Fundamentals of Information Systems Security

THIRD EDITION

Bilgi Sistemleri Güvenliğinin Temelleri

3. BASIMDAN ÇEVİRİ

David Kim | Michael G. Solomon

Çeviri Editörü | Dr. Öğr. Üyesi Özgü Can

nobel

Bilgi Sistemleri Güvenliğinin Temelleri

3. Basımdan Çeviri

Çeviri Editörü: Dr. Öğr. Üyesi Özgü Can

Fundamentals of Information Systems Security

THIRD EDITION

David Kim | Michael G. Solomon

JONES & BARTLETT LEARNING

nobel

BİLGİ SİSTEMLERİ GÜVENLİĞİNİN TEMELLERİ
Çeviri Editörü: Dr. Öğr. Üyesi Özgü Can
FUNDAMENTALS OF INFORMATION SYSTEMS SECURITY
David Kim - Michael G. Solomon

Yayın No. : 2389
Bilgisayar No. : 003
ISBN : 978-605-033-000-7
Basım Sayısı : 3. Basımdan Çeviri, Eylül 2019

© Copyright 2019, NOBEL AKADEMİK YAYINCILIK EĞİTİM DANIŞMANLIK TİC. LTD. ŞTİ. SERTİFİKA NO.: 40340
Bu baskının bütün hakları Nobel Akademik Yayıncılık Eğitim Danışmanlık Tic. Ltd. Şti.ne aittir. Yayınevinin yazılı izni olmaksızın, kitabın tümünün veya bir kısmının elektronik, mekanik ya da fotokopi yoluyla basımı, yayımı, çoğaltımı ve dağıtımı yapılamaz.

ORIGINAL ENGLISH LANGUAGE EDITION PUBLISHED BY Jones & Bartlett Learning, LLC 5 Wall Street Burlington, MA 01803. Fundamentals of Information Systems Security, Michael G. Solomon, David Kim, @ copyright 2016 Jones & Bartlett Learning, LLC. All rights reserved.
TURKISH language edition published by NOBEL AKADEMİK YAYINCILIK, Copyright © 2019

Genel Yayın Yönetmeni : Nevzat Argun -nargun@nobelyayin.com-
Yayın Koordinatörü : Gülfem Dursun -gulfem@nobelyayin.com-

Redaksiyon : Begüm Akcaoğlu -begum@nobelyayin.com-
Sayfa Tasarım : Emel Yıldız -emel@nobelyayin.com-
Kapak Tasarım : Mehtap Yürümez -mehtap@nobelyayin.com-
Baskı ve Cilt : Genç Ofset Sertifika No.: 32284
Süzgün Sokak No.:18/3 İskitler/Ankara

Kütüphane Bilgi Kartı

Kim. David. Solomon, G. Michael.
Fundamentals of Information Systems Security / David Kim - Michael G. Solomon
Bilgi Sistemleri Güvenliğinin Temelleri / *Çeviri Editörü: Özgü Can*
3. Basımdan Çeviri. XXVI + 548 s. 19,5x23,5 cm. Kaynakça var, dizin yok.
ISBN: 978-605-033-000-7
1. Bilgi Güvenliği 2. Bilgi Sistemleri 3. Bilgi Güvenliği Standartları

Genel Dağıtım

ATLAS AKADEMİK BASIM YAYIN DAĞITIM TİC. LTD. ŞTİ.
Adres: Bahçekapı mh. 2465 sk. Oto Sanayi Sitesi No:7 Bodrum Kat Şaşmaz-ANKARA - siparis@nobelyayin.com-
Telefon: +90 312 278 50 77 - **Faks:** 0 312 278 21 65
E-Satış: www.nobelkitap.com - www.atlaskitap.com - **Bilgi:** esatis@nobelkitap.com - info@atlaskitap.com

Dağıtım ve Satış Noktaları: Alfa Basım Dağıtım, Ana Basım Dağıtım, Arasta, Arkadaş Kitabevi, Başarı Dağıtım, D&R mağazaları, Dost Dağıtım, Güneş Dağıtım, Kitapsan, Nezih Kitabevleri, Prefix, Remzi Kitabevleri, TveK Mağazaları

Çeviri Kurulu

Çeviri Editörü

Dr. Öğr. Üyesi Özgü Can
Ege Üniversitesi - *Bilgisayar Mühendisliği Bölümü*

BÖLÜM 1 **Bilgi Sistemleri Güvenliği**

Prof. Dr. Mehmet Emin Dalkılıç
Ege Üniversitesi - *Uluslararası Bilgisayar Enstitüsü*

BÖLÜM 2 **Nesnelerin İnterneti Yaşantımızı Değiştiriyor**

Gökhan Sağırlar
University of Insubria (Università degli Studi dell'Insubria)
Dr. Öğr. Üyesi Özgü Can
Ege Üniversitesi - *Bilgisayar Mühendisliği Bölümü*

BÖLÜM 3 **Kötücül Saldırılar, Tehditler ve Güvenlik Açıkları**

Dr. Cüneyt Gürcan Akçora
The University of Texas at Dallas - *Erik Jonsson School of Engineering & Computer Science*

BÖLÜM 4 **Bilgi Güvenliği İş Sürücüleri**

Doç. Dr. Murat Osman Ünalır
Ege Üniversitesi - *Bilgisayar Mühendisliği Bölümü*

BÖLÜM 5 **Erişim Denetimleri**

Dr. Öğr. Üyesi Özgü Can
Ege Üniversitesi - *Bilgisayar Mühendisliği Bölümü*
Batuhan Erdoğdu

BÖLÜM 6 **Güvenlik Operasyonları ve Yönetimi**

Dr. Öğr. Üyesi Selma Tekir
İzmir Yüksek Teknoloji Enstitüsü - *Bilgisayar Mühendisliği Bölümü*

BÖLÜM 7 **Denetleme, Sınama ve İzleme**

Dr. Öğr. Üyesi Tuğkan Tuğlular - Dr. Ekincan Ufuktepe
İzmir Yüksek Teknoloji Enstitüsü - *Bilgisayar Mühendisliği Bölümü*

BÖLÜM 8 **Risk, Yanıt ve Kurtarma**

Dr. Ebru Çankaya
University of Texas at Dallas Department of Computer Science

BÖLÜM 9 **Kriptografi**

Dr. Öğr. Üyesi Özgü Can
Ege Üniversitesi - *Bilgisayar Mühendisliği Bölümü*

BÖLÜM 10 **Ağ ve Telekomünikasyon**

Dr. Öğr. Üyesi Enis Karaarslan
Muğla Sıtkı Koçman Üniversitesi - *Mühendislik Fakültesi*

BÖLÜM 11 **Kötücül Kod ve Aktivite**

Dr. Öğr. Üyesi Birim Balcı
Celal Baya Üniversitesi - *Bilgisayar Mühendisliği Bölümü*
Dr. Öğr. Üyesi Birol Çiloğlugil
Ege Üniversitesi - *Bilgisayar Mühendisliği Bölümü*

BÖLÜM 12 **Bilgi Güvenliği Standartları**

Dr. Öğr. Üyesi Emine Sezer
Ege Üniversitesi - *Bilgisayar Mühendisliği Bölümü*

BÖLÜM 13 **Bilgi Sistemleri Güvenliği Öğretimi ve Eğitimi**

Dr. Öğr. Üyesi Emine Sezer
Ege Üniversitesi - Bilgisayar Mühendisliği Bölümü

BÖLÜM 14 **Bilgi Güvenliği Mesleki Sertifikasyonlar**

Dr. Öğr. Üyesi Serap Şahin
İzmir Yüksek Teknoloji Enstitüsü - *Bilgisayar Mühendisliği Bölümü*

BÖLÜM 15 **ABD Uygunluk Kanunları**

Dr. Öğr. Üyesi Ali İnan
Adana Bilim ve Teknoloji Üniversitesi

Bu kitap, bilgi sistemleri güvenliği alanında kariyer yapmak isteyen okuyucularımıza, öğrencilerimize ve BT uzmanlarımıza yöneliktir. BT Güvenliğini öğrenme tutkunuz, Amerika Birleşik Devletleri'nin bilgi varlıklarını, işletmelerimizi ve vatandaşlarımızın gizlilik verilerini korumanıza yardımcı olabilir.
—David Kim

Beni birçok yönden zengin bir şekilde kutsayan Tanrı'ya.
—Michael G. Solomon

İçindekiler

Çeviri Kurulu iii
Ön Söz xxi
Teşekkür xxiii
Yazarlar xxiv
Çeviri Editörünün Ön Sözü xxv

KISIM I **Bilgi Güvenliği İhtiyacı** 1

BÖLÜM 1 **Bilgi Sistemleri Güvenliği** 2

Bilgi Sistemleri Güvenliği 3
Riskler, Tehditler, ve Zafiyetler 11
Bilgi Sistemleri Güvenliği Nedir? 12
ABD Uyum (Compliance) Yasaları Bilgi Sistemleri Güvenliği İhtiyacının İtici Gücüdür 12
Bilgi Sistemleri Güvenliğinin İlkeleri 14
Gizlilik 16
Bütünlük 17
Kullanılabilirlik 17
Tipik bir BT Altyapısının Yedi Etki Alanı 19
Kullanıcı Etki Alanı 19
İş İstasyonu Etki Alanı 22
LAN Etki Alanı 22
LAN-dan-WAN-a Etki Alanı 25
WAN Etki Alanı 28
Uzaktan Erişim Etki Alanı 32
Sistem/Uygulama Etki Alanı 36
BT Altyapısı Güvenliğindeki En Zayıf Halka 38
Etik ve İnternet 40
BT Güvenlik Politikası Çerçevesi 40
Tanımlar 41
Temel BT Güvenlik Politikaları 41
Veri Sınıflama Standartları 42
BÖLÜM ÖZETİ 44
ANAHTAR KAVRAMLAR VE TERİMLER 44
BÖLÜM 1 DEĞERLENDİRME 45

BÖLÜM 2 **Nesnelerin İnterneti Yaşantımızı Değiştiriyor** 47

Nesnelerin İnterneti'nin Gelişimi 49

TCP/IP Dünyasına Dönüşüm 50

IoT'nin İnsan Hayatına ve Ticari Hayata Etkisi 51

İnsanlar Nasıl İletişim Kurmaktan Hoşlanmaktadır? 52
Yaşamlarımızı Etkileyen IoT Uygulamaları 52

Fiziksel İşletmelerden E-Ticarete Gelişim 55

İşletmelerin Neden İnternet ve IoT Pazarlama Stratejileri Olmalıdır 57

Mobil IP 58

Mobil kullanıcılar ve Kendi Cihazını Getir 58

Mobil Uygulamalar 59

IP Hareketliliği 60

IoT'nin Yarattığı Yeni Sorunlar 62

Güvenlik 62
Mahremiyet 63
Birlikte çalışabilirlik ve Standartlar 65
Yasal ve Mevzuat Sorunları 67
E-ticaret ve Ekonomik Kalkınma Sorunları 68

BÖLÜM ÖZETİ 69

ANAHTAR KAVRAMLAR VE TERİMLER 70

BÖLÜM 2 DEĞERLENDİRME 70

BÖLÜM 3 **Kötücül Saldırılar, Tehditler ve Güvenlik Açıkları** 72

Kötücül Faaliyet Artmakta 73

Neyi Korumaya Çalışıyorsunuz? 74

Müşteri Verileri 74
BT ve Ağ Altyapısı 75
Fikri Mülkiyet 76
Mali Durum ve Mali Veriler 76
Hizmet Kullanılabilirliği ve Verimlilik 77
İtibar 78

Kimi yakalamaya çalışıyorsunuz? 78

Saldırı Araçları 79

Protokol Çözümleyiciler 80
Port Tarayıcılar 80
İşletim Sistemi Parmak İzi Tarayıcıları 80
Güvenlik Açığı Tarayıcıları 80
İstismar Yazılımları 81
Otomatik Numara Çevirici 81

Parola Kırıcılar 82
Tuşa Basma Kaydedicileri 82
Güvenlik İhlali Nedir? 83
Hizmet Reddi Saldırıları 83
Dağıtık Hizmet Reddi Saldırıları 84
Web'de Uygunsuz Gezinme Davranışları 84
İzinsiz dinleme 85
Arka Kapılar 85
Veri Değişiklikleri 86
Diğer Güvenlik Zorlukları 86
Riskler, Tehditler ve Güvenlik Açıkları Nelerdir? 88
Tehditlerin Hedefleri 89
Tehdit Türleri 90
Kötücül Saldırı Nedir? 92
Doğum Günü Saldırıları 93
Brute-Force Parola Saldırıları 93
Sözlük Parola Saldırıları 94
IP Adres Yanıltması 94
Ele Geçirme 94
Yeniden Gönderme Saldırıları 95
Ortadaki Adam Saldırıları 95
Yerine Geçme 96
Ortam Dinleme 96
Sosyal Mühendislik 96
Telefon şebekesine girme 97
Oltalama 97
Web Sitesi Trafiğinin Yönlendirilmesi 98
Kötücül Yazılım Nedir? 99
Virüsler 99
Solucanlar 100
Truva Atları 100
Rootkitler 101
Casus Yazılım 101
Saldırıların Genel Türleri Nelerdir? 102
Sosyal Mühendislik Saldırıları 103
Kablosuz Ağ Saldırıları 104
Web Uygulama Saldırıları 104
Önlem Nedir? 106
Kötücül Yazılımı Önlemek 106
Sisteminizi Güvenlik Duvarları ile Koruma k 108
BÖLÜM ÖZETİ 108
ANAHTAR KAVRAMLAR VE TERİMLER 109
BÖLÜM 3 DEĞERLENDİRME 110

BÖLÜM 4 **Bilgi Güvenliği İş Sürücüleri 112**

Risk Yönetimini Tanımlamak 113

Bir BIA, BCP ve DRP Gerçekleştirmek 115

İş Etki Analizi 115
İş Sürekliliği Planı 116
Felaket Kurtarma Planı (DRP) 118

Riskleri, Tehditleri ve Güvenlik Açıklarını Değerlendirme 122

Bilgi Güvenliği Açığını Kapatmak 123

Hukuka Uygunluğa Bağlı Kalmak 124

Kişisel Verileri Gizli Tutmak 127

Mobil Çalışanlar ve Kişisel Olarak Sahip Olunan Cihazların Kullanımı 129

BYOD Endişeleri 129
Uç Nokta ve Cihaz Güvenliği 130

BÖLÜM ÖZETİ 131

ANAHTAR KAVRAMLAR VE TERİMLER 132

BÖLÜM 4 DEĞERLENDİRME 132

KISIM II Günümüz Bilgi Sistemlerini Güven Altına Almak 135

BÖLÜM 5 **Erişim Denetimleri 136**

Erişim Denetiminin Dört-Parçası 137

Erişim Denetiminin İki Türü 138

Fiziksel Erişim Denetim 138
Mantıksal Erişim Denetim 138

Yetkilendirme Politikaları 140

Kimlik Tanımlama için Yöntemler ve Yönergeler 141

Kimlik Tanımlama Yöntemleri 141
Kimlik Tanımlama Yönergeleri 141

Kimlik Denetleme için Süreçler ve Gereksinimler 142

Kimlik Denetleme Türleri 142
Tek Oturum Açma 151

İzlenebilirlik için Politikalar ve Prosedürler 154

Günlük Dosyaları 154
İzleme ve Değerlendirme 154
Verilerin Tutulması, Ortam Araçlarının İmha Edilmesi, Uygunluk Gereksinimleri 154

Erişim Denetimin Biçimsel Modelleri 156

İsteğe Bağlı Erişim Denetim 157
İşletim Sistemi-Tabanlı DAC 157

Zorunlu Erişim Denetim 159
İsteğe Bağlı Olmayan Erişim Denetim 160
Kural Tabanlı Erişim Denetim 160
Erişim Denetim Listeleri 160
Rol-Tabanlı Erişim Denetim 161
İçeriğe-Bağlı Erişim Denetim 163
Kısıtlandırılmış Kullanıcı Ara Yüzü 163
Diğer Erişim Denetim Modelleri 164

Erişim Denetimde İhlallerin Etkileri 166

Erişim Denetimlere Yönelik Tehditler 167

Erişim Denetimin İhlallerinin Etkileri 168

Kimlik Bilgileri ve İzinlerin Yönetimi 169

Merkezi ve Merkezi Olmayan Erişim Denetim 169

AAA Sunucularının Türleri 169
Merkezi Olmayan Erişim Denetim 172
Mahremiyet 172

BÖLÜM ÖZETİ 177

ANAHTAR KAVRAMLAR VE TERİMLER 177

BÖLÜM 5 DEĞERLENDİRME 178

BÖLÜM 6

Güvenlik Operasyonları ve Yönetimi 181

Güvenlik Yönetimi 182

Erişimin Denetlenmesi 182
Belgeleme, Prosedürler ve Kılavuzlar 183
Felaket Değerlendirmesi ve Kurtarma 183
Güvenliğin Dış Kaynaklardan Edinilmesi 184

Uygunluk 185

Olay Günlükleri 186
Uygunluk İrtibatı 186
İyileştirme 186

Mesleki Etik 187

Etik Konusunda Yaygın Yanlış Düşünceler 187
Etik Kurallar 188
Personel Güvenlik Prensipleri 189

Bir BT Güvenlik Politikası İçin Altyapı 192

Politikalar 192
Standartlar 194
Prosedürler 194
Dayanaklar 195
Kılavuzlar 196

Veri Sınıflandırma Standartları 196

Bilgi Sınıflandırma Amaçları 197
Sınıflandırma Ömekleri 197
Sınıflandırma Prosedürleri 197
Güvence 198

Konfigürasyon Yönetimi 199

Donanım Envanteri ve Konfigürasyon Çizelgesi 199

Değişiklik Yönetim Süreci 200

Değişiklik Denetim Yönetimi 200
Değişiklik Denetim Komiteleri 201
Değişiklik Denetim Prosedürleri 202
Değişiklik Denetim Problemleri 203

Uygulama Yazılımı Güvenliği 203

Sistem Yaşam Döngüsü 203
Uygulama Yazılımının Test Edilmesi 205

Yazılım Geliştirme ve Güvenlik 208

Yazılım Geliştirme Modelleri 209

BÖLÜM ÖZETİ 212

ANAHTAR KAVRAMLAR VE TERİMLER 213

BÖLÜM 6 DEĞERLENDİRME 213

BÖLÜM 7

Denetleme, Sınama ve İzleme 216

Güvenlik Denetlemesi ve Analizi 217

Güvenlik Denetimleri Riske Odaklanır 218
Neyin Kabul Edilebilir Olduğunun Belirlenmesi 219
İzin Seviyeleri 219
Güvenlik Denetleme Alanları 220
Denetlemelerin Amacı 220
Müşteri Güveni 221

Denetleme Planınızı Tanımlama 223

Planın Kapsamını Belirleme 223

Denetleme Karşılaştırmalı Değerlendirme 224

Denetleme İçin Veri Toplama Yöntemleri 226

Güvenlik Denetleme Alanları 226
Denetimlerin Gözden Geçirilmesi ve Kimlik Yönetimi 227

Denetleme Sonrası Faaliyetler 228

Çıkış Mülakatları 228
Veri Analizi 228
Denetleme Raporunun Oluşturulması 228
Bulguların Sunulması 229

Güvenlik İzleme 229

Bilgisayar Sistemleri için Güvenlik İzleme 230
İzleme Sorunları 231
Günlük Tutma Anormalileri 232
Günlük Yönetimi 232

Yakalanacak Günlük Bilgilerinin Türleri 233

Güvenlik Denetimlerini Doğrulama 234

Saldırı Tespit Sistemi (Intrusion Detection System - IDS) 234
Analiz Yöntemleri 236
HIDS 237
Katmanlı Savunma: Ağ Erişim Denetimi 237
Kontrol Denetlemeleri: Saldırı Tespiti 238
Ana Bilgisayar İzolasyonu 238
Sistem Güçlendirme 238
Antivirüs Yazılımları Değerlendirmek 241

Güvenlik Sistemlerini İzleme ve Sınama 241

İzleme 241
Test Yapmak 241

BÖLÜM ÖZETİ 249

ANAHTAR KAVRAMLAR VE TERİMLER 249

BÖLÜM 7 DEĞERLENDİRME 249

BÖLÜM 8

Risk, Yanıt ve Kurtarma 251

Risk Yönetimi ve Bilgi Güvenliği 252

Risk Terminolojisi 253
Risk Bileşenleri 254
Risk Yönetiminin Amacı 254

Risk Yönetim Süreci 255

Riskleri Tanımlama 256
Risk Değerlendirmesi 259
Riske Yanıtın Planlanması 263
Risk Yanıt Planının Uygulanması 265
Riske Yanıtının İzlenmesi ve Denetimi 269

İş Süreklilik Yönetimi 270

Terim bilgisi 271
Maksimum Tolere Edilebilir Aksama Süresinin Hesaplanması 272
İş Etki Analizi 273
Plan Değerlendirmesi 274
Planın Test Edilmesi 274

Veri ve Uygulamaların Yedeklenmesi 276

Yedekleme Türleri 276

Ayrıcalıklı Olay Yönetimi 277
Hazırlık 278
Tanımlama 278
Bildirim 278
Yanıt 279
Kurtarma 280
Takip etme 280
Belgeleme ve Raporlama 280
Felaketten Kurtarma 280
Felaketten Kurtarma Planını Etkinleştirme 281
Azaltılmış/Değiştirilmiş Ortamda Çalışmak 281
Hasarlı Sistemlerin Geri Yüklenmesi 282
Felaketten Kurtarma Sorunları 282
Kurtarma Alternatifleri 282
Geçici veya Alternatif İşlem Stratejileri 283
BÖLÜM ÖZETİ 285
ANAHTAR KAVRAMLAR VE TERİMLER 286
BÖLÜM 8 DEĞERLENDİRME 287

BÖLÜM 9 **Kriptografi 288**

Kriptografi Nedir? 289
Temel Kriptografik İlkeler 290
Kriptografinin Kısa Tarihi 291
Bilgi Güvenliğinde Kriptografinin Rolü 292
Kriptografi için İş ve Güvenlik Gereksinimleri 295
İç Güvenlik 295
İş İlişkilerinde Güvenlik 295
Herkese Yarar Sağlayan Güvenlik Önlemleri 296
Kriptografik İlkeler, Kavramlar, ve Terminoloji 296
Kriptografik Fonksiyonlar ve Şifreler 296
Şifreleme Türleri 299
Yer Değiştirme Şifrelemeleri 300
Yerine Koyma Şifrelemeleri 300
Birleşik ve Üssel Şifreleme 302
Simetrik ve Asimetrik Anahtar Kriptografisi 303
Simetrik Anahtar Şifreleme 303
Asimetrik Anahtar Şifreleme 304
Kriptanaliz ve Kamusal'a Özel Anahtarlar 305
Anahtarlar, Anahtar Uzayı ve Anahtar Yönetimi 308
Kriptografik Anahtarlar ve Anahtar Uzayı 308
Anahtar Yönetimi 309
Anahtar Dağıtımı 310
Anahtar Dağıtım Merkezleri 310

Dijital İmzalar ve Özet Fonksiyonlar 311

Özet Fonksiyonlar 311
Dijital İmzalar 311

Bilgi Sistemi Güvenliğinde Kriptografik Uygulamalar ve Kullanım Alanları 312

Diğer Kriptografik Araçlar ve Kaynaklar 313
Simetrik Anahtar Standartları 314
Asimetrik Anahtar Çözümleri 316
Özet Fonksiyonu ve Bütünlük 318
Dijital İmzalar ve İnkar Edememe 320

Sertifikaların ve Anahtar Yönetiminin Prensipleri 321

Modern Anahtar Yönetim Teknikleri 321

BÖLÜM ÖZETİ 323

ANAHTAR KAVRAMLAR VE TERİMLER 324

BÖLÜM 9 DEĞERLENDİRME 324

BÖLÜM 10

Ağ ve Telekomünikasyon 326

Açık Sistemler Ara Bağlantısı Referans Modeli 327

Ana Ağ Türleri 329

Geniş Alan Ağları 329
Yerel Alan Ağları 332

TCP/IP Nedir ve Nasıl Çalışır? 334

TCP / IP'ye Genel Bakış 334
IP Adresleme 335
Ortak Bağlantı Noktaları 336
Ortak Protokoller 336
İnternet Kontrol Mesajı Protokolü 336

Ağ Güvenliği Riskleri 338

Risk Kategorileri 338

Temel Ağ Güvenliği Savunma Araçları 341

Güvenlik Duvarları 341
Sanal Özel Ağlar ve Uzaktan Erişim 345
Ağ Erişim Kontrolü 347

Kablosuz Ağlar 347

Kablosuz Erişim Noktaları 348
Kablosuz Ağ Güvenlik Denetimleri 348

BÖLÜM ÖZETİ 351

ANAHTAR KAVRAMLAR VE TERİMLER 351

BÖLÜM 10 DEĞERLENDİRME 352

BÖLÜM 11 **Kötücül Kod ve Aktivite 354**

Kötü Amaçlı Yazılımların Özellikleri, Mimarisi ve İşleyişleri 355

Kötü Amaçlı Yazılımların Ana Türleri 356

Virüs 356
İstenmeyen elektronik posta (Spam) 363
Solucanlar 364
Truva Atları 366
Mantık Bombaları 367
Aktif İçerik Zafiyetleri 367
Kötü Amaçlı Eklentiler 367
Enjeksiyon 368
Robot Ağlar (Botnets) 369
Hizmeti Engelleme Saldırıları 369
Casus Yazılım 371
Reklam Yazılımı 372
Oltalama 372
Tuş vuruşu kaydedicileri 373
Aldatmacalar ve Efsaneler 373
Anasayfa Ele geçirme 374
Websayfası İçeriğinin Bozulması 374

Zararlı Kod Tehditlerinin Kısa Bir Tarihçesi 375

1970'ler ve Erken 1980'ler: Akademik Araştırma ve UNIX 375
1980'ler: İlk PC Virüsleri 376
1990'lar: İlk LAN Virüsleri 376
1990'ların Ortası: Akıllı Uygulamalar ve İnternet 377
2000'lerden Günümüze 377

Ticari İşletmelere Olan Tehditler 378

Tehdit Türleri 378
Çalışanlardan Kaynaklanan İç Tehditler 379

Bir Saldırının Anatomisi 379

Saldırganları Ne Motive Eder? 380
Bir Saldırının Amacı 380
Saldırıların Çeşitleri 380
Bir Saldırının Aşamaları 382

Saldırı Önleme Araçları ve Teknikleri 387

Uygulama Savunmaları 388
İşletim Sistemi Savunmaları 388
Ağ Altyapısı Savunması 389
Güvenli Kurtarma Teknikleri ve Uygulamaları 390
Etkili Yazılım En İyi Uygulamalarının Gerçekleştirilmesi 390

Saldırı Tespit Araçları ve Teknikleri 390

Antivirüs Tarama Yazılımı 391
Ağ İzleyicileri ve Çözümleyicileri 391
İçerik/Bağlam Filtreleme ve Kaydedici Yazılımlar 391
Bal Küpleri ve Bal Ağları 392

BÖLÜM ÖZETİ 393

ANAHTAR KAVRAMLAR VE TERİMLER 393
BÖLÜM 11 DEĞERLENDİRME 393

KISIM III **Bilgi Güvenliği Standartları, Eğitim, Sertifikasyonlar ve Kanunlar** 395

BÖLÜM 12 **Bilgi Güvenliği Standartları** 396

Standart Kuruluşları 397
Ulusal Standartlar ve Teknoloji Enstitüsü 397
Uluslararası Standartlar Teşkilatı 398
Uluslararası Elektroteknik Komisyonu 400
World Wide Web Konsorsiyumu 401
İnternet Mühendisliği Görev Grubu 401
Elektrik ve Elektronik Mühendisleri Enstitüsü 403
Uluslararası Telekominikosyan Birliği Telekominikasyon Sektörü 404
Amerikan Ulusal Standartlar Enstitüsü 405
Avrupa Telekomünikasyon Standartları Enstitüsü Siber Güvenlik Teknik Komitesi 406
ISO 17799 (Geri çekilmiş) 407
ISO/IEC 27002 408
Ödeme Kartı Endüstrisi Veri Güvenliği Standardı 409
BÖLÜM ÖZETİ 410
ANAHTAR KAVRAMLAR VE TERİMLER 411
BÖLÜM 12 DEĞERLENDİRME 411

BÖLÜM 13 **Bilgi Sistemleri Güvenliği Öğretimi ve Eğitimi** 412

Kendi Kendine Çalışma Programları 413
Eğitmen Tarafından Yönlendirilen Programlar 416
Sertifika Programları 416
Sürekli Eğitim Programları 418
Lise Sonrası Eğitim Programları 419
Ön lisans Derecesi 420
Lisans Derecesi 420
Yüksek Lisans Derecesi 421
İşletme Yüksek Lisansı 423
Doktora Programı 424
Bilgi Güvenliği Eğitim Programları 425
Güvenlik Eğitimi Gereksinimleri 426
Güvenlik Eğitimi Kurumları 427
Güvenlik Farkındalığı Eğitimi 428
BÖLÜM ÖZETİ 430

ANAHTAR KAVRAMLAR VE TERİMLER 430
BÖLÜM 13 DEĞERLENDİRME 431

BÖLÜM 14 **Bilgi Güvenliği Mesleki Sertifikasyonlar** 433

ABD Savunma Bakanlığı/Askeri Yönerge 8570.01 434
ABD DoD/Askeri Yönerge 8140 434
ABD DoD / NSA Eğitim Standartları 436
Satıcı-Bağımsız Profesyonellik Sertifikaları 437
Uluslararası Bilgi Sistemleri Güvenliği Sertifika Konsorsiyumu A.Ş. 438
SSCP® 438
CISSP® 438
CAP® 439
CSSLP® 439
CCFP® 439
HCISPP® 439
CCSP® 440
Ek (ISC)² Meslek Sertifikaları 440
Küresel Bilgi Güvenliği Sertifikası / SANS Enstitüsü 440
Sertifikalı İnternet Web Yöneticisi 441
CompTIA 441
ISACA® 443
Diğer Bilgi Sistemleri Güvenlik Sertifikaları 443
Satıcıya-Özel Profesyonellik Sertifikaları 443
Cisco Sistemleri 444
Juniper Ağ Teknolojisi 447
RSA 447
Symantec 447
Juniper Ağ Teknolojileri 448
Check Point 449
ANAHTAR KAVRAMLAR VE TERİMLER 450
BÖLÜM 14 DEĞERLENDİRME 450

BÖLÜM 15 **ABD Uygunluk Kanunları** 452

Uygunluk Kanunen Gereklidir 453
Federal Bilgi Güvenliği 456
2002 Tarihli Federal Bilgi Güvenliği Yönetimi Kanunu 456
2014 Tarihli Federal Bilgi Güvenliği Modernizasyon Kanunu 458
Ulusal Standartlar ve Teknoloji Enstitüsü'nün Rolü 459
Ulusal Güvenlik Sistemleri 461
Sağlık Sigortası Taşınabilirlik ve Sorumluluk Kanunu 461

Amaç ve Kapsam 461
HIPAA Mahremiyet Kuralının Temel Gereksinimleri 462
HIPAA Güvenlik Kuralının Başlıca Gereksinimleri 464
Gözetim 464
Geniş Kapsamlı Düzenlemeler 466

Gramm-Leach-Bliley Kanunu 467

Amaç ve Kapsam 469
GLBA Mahremiyet Kuralı'nın Başlıca Gereksinimleri 470
GLBA Tedbirler Kuralı'nın Başlıca Gereksinimleri 471
Gözetim 472

Sarbanes-Oxley Kanunu 472

Amaç ve Kapsam 473
SOX Kontrol Sertifikasyonu Gereksinimleri 473
SOX Kayıtları Saklama Gereksinimleri 475

Aile Eğitim Hakları ve Mahremiyet Kanunu 476

Amaç ve Kapsam 476
Başlıca Gereksinimler 477
Gözetim 478

Çocukları İnternetten Koruma Kanunu 478

Amaç ve Kapsam 478
Başlıca Gereksinimler 479
Gözetim 480

Ödeme Kartı Endüstrisi Veri Güvenliği Standardı 480

Amaç ve Kapsam 481
Öz Değerlendirme Anketi 481
Başlıca Gereksinimler 482

Bilgi Güvenliği Uygunluğu Kanunlarını Anlamlandırmak 486

BÖLÜM ÖZETİ 487

ANAHTAR KAVRAMLAR VE TERİMLER 488

BÖLÜM 15 DEĞERLENDİRME 488

DİPNOTLAR 489

EK A **Cevap Anahtarı 491**

EK B **Standart Kısaltmalar 493**

EK C **CompTIA Security + Sertifikası Almak 495**

Anahtar Terimler Sözlüğü 498

Kaynakça 522

Dizin 527

Ön Söz

Bu Kitabın Amacı

Bu kitap Jones & Bartlett Learning'in (*www.issaseries.com*) Bilgi Sistemleri Güvenliği ve Güvencesi (*Information Systems Security & Assurance* - ISSA) Serilerinin bir parçasıdır. BT Güvenliği, Siber Güvenlik, Bilgi Güvencesi ve Bilgi Sistemleri Güvenliği dersleri ve müfredatları için tasarlanan bu seri, bu kritik konu alanındaki en güncel düşüncelerin ve eğilimlerin kapsamlı ve tutarlı bir şekilde ele alınmasını sağlamaktadır. Bu başlıklar, temel bilgi güvenliği ilkelerini gerçek dünyadaki uygulamalar ve örneklerle dolu olarak sunmaktadır. Sertifikalı Bilgi Sistemleri Güvenlik Uzmanları (*Certified Information Systems Security Professionals* - CISSP'ler) ve deneyimli siber güvenlik danışmanları tarafından hazırlanan bu kitap bilgi güvenliğinin tüm yönleri hakkında kapsamlı bilgi sunmaktadır. Alanında önde gelen teknik uzmanlar tarafından kelime kelime incelendiğinde, bu kitaplar sadece güncel değil, ileri görüşlüdür - sizi sadece bugünün değil, yarının da siber güvenlik sorunlarını çözme konumuna getirmektedir.

Bu kitabın bilgi güvenliğinin temelleri üzerine olan I. Kısmı, dijital dünyaya ve Nesnelerin İnterneti'ne (*Internet of Things* - IoT) dönüşüm ile ilgili yeni risklere, tehditlere ve güvenlik açıklıklarına odaklanmaktadır. Bireyler, öğrenciler, eğitimciler, işletmeler, organizasyonlar ve hükümetler iletişim kurma, kişisel bilgileri ve medyayı paylaşma ve iş yapma biçimini değiştirdi. IoT'in vizyonuyla yönetilen internet ve genişbant iletişimler günlük hayatımıza girdi. Bu dijital devrim, bilgi sistemleri güvenliğine bir ihtiyaç yarattı. Özel verilerin korunmasını ve güvenliğinin sağlanmasını ve sorumlulukların azaltılmasını gerektiren son uygunluk kanunları sayesinde, bilgi sistemleri güvenliğine şu an olduğundan daha fazla farkına varılmamıştır.

II. Kısım, CompTIA'nın Security+ profesyonel sertifikasyonundan uyarlanmıştır. CompTIA Security+ en yaygın kabul gören, başlangıç düzeyinde, satıcıdan bağımsız BT güvenlik bilgi ve becerileri profesyoneli sertifikasyonudur. Temel bilgi birikimi ve BT güvenliğindeki en iyi uygulamalar için bir karşılaştırmalı değerlendirme olarak, Security+ profesyonel sertifikası, ağ güvenliği, operasyonel güvenlik ve uygunluk için temel ilkeleri içerir. Ayrıca, uygulama, veri ve ana bilgisayar güvenliği, tehditler ve güvenlik açıkları, erişim denetimi, kimlik yönetimi ve kriptografi konularını da kapsayan Security+ sertifikası, BT güvenliği kariyeri için sağlam bir temel sağlar.

Bu kitabın III. Kısım'ı, bilgi güvenliği standartları, eğitim, mesleki sertifikalar ve son zamanlardaki uygunluk kanunları hakkında daha fazla bilgi isteyen okuyucular ve öğrenciler için bir kaynak sunmaktadır. Bu kaynaklar, bilgi sistemleri güvenliğinde eğitim ve kariyer olanakları hakkında ek bilgi isteyen öğrenciler ve bireyler için idealdir.

Öğrenme Özellikleri

Bu kitabın yazı stili pratik ve konuşma dilindedir. Bilgi güvenliği kavramlarının ve prosedürlerinin adım adım örnekleri kitap boyunca sunulmaktadır. Her bölüm bir öğrenme hedefleri açıklamasıyla başlar. Çizimler hem materyali netleştirmek hem de sunumu çeşitlendirmek için kullanılmıştır. Kitapta yer alan Notlar, İpuçları, Bilginize, Uyarılar ve Ek Bilgi Kutuları, okuyucuyu tartışılan konuyla ilgili ek yararlı bilgiler konusunda uyarmaktadır. Bölüm değerlendirmeleri, kitabın arkasında verilen çözümlerle, her bölümün sonunda yer almaktadır.

Materyallerin hızlı bir şekilde gözden geçirilmesi veya ön izlemesinin yapılması ve öğrencilerin sunulan kavramların bağıl önemliliğini anlamalarına yardımcı olmak için kitapta bölüm özetleri yer almaktadır.

Okuyucu Kitlesi

Kitap, lisans veya lisansüstü bilgisayar bilimleri uzmanları veya bilgi bilimi uzmanları, 2 yıllık temel bir teknik geçmişe sahip teknik kolej veya üniversite öğrencileri veya BT güvenliği hakkında temel bilgileri olan ve bilgilerini genişletmek isteyen okuyucular için uygundur.

Teşekkür

Bu kitap, Jones & Bartlett Learning'in (www.issaseries.com) hazırladığı Bilgi Sistemleri Güvenliği ve Güvencesi (Information Systems Security & Assurance - ISSA) Serisi'nin amiral gemisi kitabıdır. ISSA serisi, mezunları iş gücüne hazır olacak bir bilgi sistemleri güvenliği ve bilgi güvencesi lisans programı sunmak için uygulamalı bir yaklaşıma ihtiyaç duyan yüksek okullara ve üniversitelere yönelik BT güvenliği ve bilgi güvencesi müfredatları ve eğitim materyali için hazırlanmıştır.

Tüm ISSA serisi, bilgi sistemleri güvenliği uzmanları, danışmanları ve bilgi sistemleri güvenliği alanındaki tanınmış öncü kişiler tarafından geliştirilmiştir; bu kişilerin tümü her kelimeye, cümleye, paragrafa ve bölüme katkıda bulunmuştur. Katılanların gösterdiği özveri ve azim, tek bir tutku ve ortak bir hedef tarafından yönlendirildi: Günümüz bilgi sistemleri güvenlik uygulayıcısını eğitmeye yardım etmek. Bilgi sistemleri güvenlik uygulayıcılarına iş ve beceri odaklı hazırlık sağlamak için, en güncel ders kitaplarını, eğitim materyalini, uygulamalı laboratuvarları oluşturdular.

Bu çabayı ve dünyanın en iyi bilgi sistemleri güvenlik içeriğini ve müfredatını oluşturmayı destekleyen Jones & Bartlett Learning'e vizyonu ve sabrı için teşekkür ederim. Michael Solomon ve Jeff Parker'a ve son 6 aylık gelişim sürecinde bu kitap ve ISSA Serisi'ne katkıda bulunan tüm Jones & Bartlett Learning ekibine teşekkür ederim.

Son ama en önemlisi olarak, her zaman yanımda olan ve olacak olan karım MiYoung Kim'e teşekkür etmek istiyorum. Seni her geçen gün daha çok seviyorum.

David Kim

David Kim'e ve ilgili editöryal yorumlar sağlayan ve kitabın içeriğini daha iyi ayarlamaya yardımcı oldukları için tüm Jones & Bartlett Learning ekibine teşekkür ediyorum. Hepiniz süreci çok daha kolay hale getirdiniz ve kitaba çok büyük bir değer kattınız. Birçok farklı konuyu araştırmada yardım ettikleri için Stacey ve Noah'a çok teşekkürler.

Michael G. Solomon

Yazarlar

David Kim, Washington DC'nin büyükşehir alanı dışında bulunan Security Evolutions, Inc.'in (*SEI; www.security-evolutions.com*) başkanıdır. SEI, dünya genelinde kamu ve özel sektör müşterileri için yönetim, risk ve uygunluk danışmanlık hizmetleri sunmaktadır. SEI'nin müşterileri arasında sağlık kurumları, bankacılık kurumları, hükümetler ve uluslararası havaalanları bulunmaktadır. SEI'nin BT güvenlik danışmanlığı hizmetleri arasında güvenlik riski değerlendirmeleri, güvenlik açığı değerlendirmesi, uyumluluk denetimleri ve işletmeler için katmanlı güvenlik çözümleri tasarımı yer almaktadır. Ek olarak, mevcut hizmetler arasında iş sürekliliği ve felaket kurtarma planlarının geliştirilmesi yer almaktadır. Bay Kim'in BT ve BT güvenlik deneyimi, 30 yıldan fazla teknik mühendislik, teknik yönetim ve satış ve pazarlama yönetimini kapsamaktadır. Bu deneyim, LAN/WAN, ağlararası iletişim, kurumsal ağ yönetimi ve ses, video ve veri ağı altyapıları için BT güvenliğini içermektedir. Amerika Birleşik Devletleri'ndeki öğrencilere siber güvenlik öğretmekten hoşlanan başarılı bir yazar ve yarı zamanlı yardımcı profesördür.

Michael G. Solomon, CISSP, PMP, CISM, tam zamanlı bir güvenlik ve OpenEdge konuşmacısı, danışman, yazar ve güvenli BT ortamlarını sağlama ve sürdürme konusunda lider ekiplerde uzmanlaşmış bir oyun uzmanıdır. 1987'den beri BT uzmanı ve danışmanı olarak, birçok büyük organizasyon için projeler yürütmüştür ve çok sayıda kitap yazmış ve eğitim kursuna katkıda bulunmuştur. 1998'den 2001'e kadar Kennesaw Eyalet Üniversitesi Bilgisayar Bilimi ve Bilgi Bilimleri (*Computer Science and Information Sciences - CSIS*) bölümünde öğretim görevlisi olarak çalışmıştır ve halen Cumberlands Üniversitesi'nde Bilgisayar Bilimi ve Güvenliği dersleri vermektedir. Michael aynı zamanda Emory Üniversitesi'nde Bilgisayar Bilimi ve Bilişimi alanında doktora adayıdır.

Çeviri Editörünün Ön Sözü

Günümüzde yaşanmakta olan hızlı teknolojik gelişmeler, kişilerin iş, eğlence ve günlük hayatlarında yeni fırsatlar yaratmış ve her an geniş bir bilgi hazinesine ulaşılabilmelerini sağlamıştır. Tarih boyunca, bilgi her zaman çalınmış, takas edilmiş, kişisel kazanç, açgözlülük ya da kişisel hırslar için kullanılmıştır. Bilgi, günümüzde de dünyanın en önemli kaynaklarından biridir ve "yeni petrol" olarak kabul edilmektedir. Bu nedenle, 21. yüzyılın bu değerli kaynağının en uygun şekilde korunması gerekmektedir. Bilgi güvenliği farkındalığının artması ile birlikte, kurumlar verilerini korumak amacıyla bilgi güvenliği yöntemlerini uygulama başlamış, kişiler de kişisel verilerinin korunmasına yönelik önlemler almaya başlamışlardır. Bilginin ve sistemin korunmasını sağlayan bilgi güvenliğinin uygulanması, kişilerin ve kurumların bilgilerini korumaları ve işlerini yürütebilmeleri için önemlidir. Bilgi sistemleri güvenliği ise sadece bilgisayar bilgisinin güvenliği ile ilgilenmez, aynı zamanda her türlü veri ve bilgiyi de korumaktadır.

Bilgi sistemleri güvenliği, bilgilerin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin sağlanması ile ilgili süreç ve metodolojileri ifade etmektedir. Ayrıca, yetkilendirilmemiş kişilerin sisteme girmesini veya erişmesini engelleyen erişim denetim yöntemleri, kötücül yazılımlar, tehditler, zafiyetler, güvenlik ihlallerinin tespiti, düzeltilmesi ve belgelenmesi, risk değerlendirmesi ve yönetimi, kriptografik sistemler de bilgi sistemlerinin güvenliğinin sağlanmasında kullanılan diğer güvenlik yöntemleridir.

Nesnelerin birbirine bağlandığı ve kişilerin "her zaman online" olduğu çağımızda, güvenliğin önemi artmış ve güvenlik en kritik çalışma alanlarından biri olmuştur. Bu kitap, bilgi sistemleri güvenliğinde yer alan yöntemler ile ilgili temel kavramları ve ayrıntılarını okuyucuya sunmaktadır. Kitap ayrıca, bilgi güvenliği standartları, eğitim, mesleki standartlar ve kanunlar kapsamında da ayrıntılı bir kaynak sunmaktadır. Güvenlik mühendisliğinde kariyer yapacak olan kişiler için bu kitap temel bir başvuru kaynağı olacaktır. Ayrıca, güvenlik alanına ilgisi olan lisans ve lisansüstü öğrenciler için de bir rehber niteliğindedir.

Kitabın çevirisinde, kitabın orijinaline sadık kalan bir dil seçilmiştir. Literatürde sık kullanılan terimlerin Türkçe çevirileri ile birlikte İngilizce karşılıkları da verilerek okuyucunun her iki dil kapsamında da terimlere olan farkındalığının arttırılması hedeflenmiştir.

Kitabın çevirisinde yer alarak dilimize kazandırılmasında katkı veren tüm meslektaşlarıma emeklerinden dolayı teşekkür ederim. Bilgisayar Mühendisliği ve Güvenlik Mühendisliği'ne katkı verecek olduğuna inandığım bu kitabın çevrilmesini öneren ve bu süreçte katkı veren tüm Nobel Yayınevi çalışanlarına da minnetlerimi sunarım.

Çok değerli annem Mine Can ve babam Fedai Can'a sonsuz teşekkürler..

Dr. Özgü Can
28 Ağustos 2019

KISIM I

Bilgi Güvenliği İhtiyacı

BÖLÜM 1 Bilgi Sistemleri Güvenliği 2

BÖLÜM 2 Nesnelerin İnterneti Yaşantımızı Değiştiriyor 47

BÖLÜM 3 Kötücül Saldırılar, Tehditler ve Zafiyetler 72

BÖLÜM 4 Bilgi Güvenliği Sektörünün Sürücüleri 112

BÖLÜM

1

Bilgi Sistemleri Güvenliği

İnternet ilk çıktığı zamana göre dramatik bir biçimde değişmiştir. Az sayıda üniversitenin ve devlet kurumlarının kullandığı bir araçtan üç milyardan daha fazla kullanıcıya sahip dünya çapında bir ağa doğru büyümüştür. Büyürkende insanların haberleşme ve iş yapma biçimlerini değiştirmiş, birçok fırsat ve fayda getirmiştir. Bugün internet büyümeye, yeni ve değişik yollarla genişlemeye devam etmektedir. İnternet başladığında, bu ağa bağlı cihazların çoğunluğu gerek kişisel kulanım için gerekse şirket içi kullanım için olan bilgisayarlardan oluşuyordu. Buna karşın, son yıllarda, bilgisayarların yanı sıra, akıllı telefonlar, akıllı arabalar, ev aletleri, yiyecek otomatları ve akıllı binalar gibi artan çeşitlilikte cihazlar internete bağlanmakta ve veri paylaşabilmektedir.

Bugün internet olarak bildiğimiz şey hızla **Nesnelerin İnterneti**'ne (***Internet of Things - IoT***) doğru genişlemekte ve günbegün yaşantımızı etkilemektedir. İnternet 1969'da resmi olarak başlamış olsa da insanların internete bağımlı hale gelmesi yenidir. Bugün, insanlar günlük yaşamlarının normal bir parçası olarak internet ve siber uzay ile etkileşimde bulunmaktadır. Bu etkileşim kişisel kullanım ve iş kullanımını içermektedir. Kullanıcılar, şimdilerde, hem özel verilerinin güvenliği hem de iş verilerinin güvenliğinini düşünmek zorundadır. Güvenlik tehditleri internete bağlı cihazlarınızın kişisel ya da iş kullanımından kaynaklanabilmektedir. Zeki ve saldırgan olan siber suçlular, teröristler, ve dolandırıcılar gölgelerde gizlenmektedirler. Bilgisayarlarınızı ya da cihazlarınızı internete bağlamak onları anında saldırılar için hedef konumuna sokmaktadır. Bu saldırılar kurbanlarda hüsran ve sıkıntılar doğurmaktadır. Kişisel bilgileri çalınmış (**kimlik hırsızlığına** (***identity theft***) maruz kalmış) herkes bu sıkıntılara şahitlik edebilmektedir. Daha kötüsü, bilgisayarlar ve ağa bağlı cihazlara yapılan saldırılar **e-ticaret**'e (***e-commerce***) dayalı ulusal ekonomi için tehdit oluşturmaktadır. Daha da önemlisi, siber saldırılar ulusal güvenliği tehdit etmektedir. Örneğin, terörist saldırganlar elektrik şebekelerini çökertebilmekte ve askeri iletişimi kesintiye uğratabilmektedir.

Siz bir fark yaratabilirsiniz. Dünyanın bilgisayar güvenliğinden anlayan ve bilgisayarları ve ağları suçlular ve teröristlerden koruyabilecek insanlara ihtiyacı vardır. Unutmayın, herşey hassas verilerinizin güvenliğini sağlamakla ilgilidir. Hassas veriniz varsa, onu korumak zorundasınız. Başlamanız için; bu bölüm, siber saldırıları anlamak ve durdurmak için gerekli bilgi sistemleri güvenliği kavramlarının ve terimlerinin tanımlarını size sunmaktadır.

1. Bölüm Konular

Bu bölüm aşağıda verilen konuları ve kavramları içermektedir:

- Yetkisiz erişimler ve veri ihlalleri nelerdir
- Bilgi sistemleri güvenliği nedir
- Bilgi sistemleri güvenliğinin ilkeleri nelerdir
- Bir BT (Bilgi Teknolojileri) altyapısının yedi etki alanı nelerdir
- Bir BT altyapısında en zayıf halka nedir
- Bir BT güvenlik politika çerçevesi riski nasıl azaltır
- Bir veri sınıflandırma standardı bir BT altyapısının güvenlik ihtiyaçlarını nasıl etkiler

1. Bölüm Hedefler

Bu bölümü tamamladığınız zaman, yapabilecekleriniz:

- Yetkisiz erişimin nasıl veri ihlaline yol açabileceğini tanımlamak
- Kullanılabilirlik, bütünlük ve gizlilik gereksinimlerinin tipik bir BT altyapısının yedi etki alanını nasıl etkilediğini anlatmak
- Yedi etki alanında yaygın olarak bulunan riskleri, tehditleri ve zafiyetleri tanımlamak
- Yedi etki alanı içerisinde geçerli katmanlı bir güvenlik yaklaşımı belirlemek
- Yaygın tehdit ve zafiyetlerinden kaynaklanan riskleri azaltmaya yardımcı olacak bir BT güvenlik politikası çerçevesi geliştirmek
- Bir veri sınıflandırma standardının yedi etki alanını nasıl etkilediğini anlatmak

Bilgi Sistemleri Güvenliği

Günümüzün **interneti** 2 milyardan fazla kullanıcılı dünya çapında bir ağdır. Dünya üzerindeki neredeyse her hükümeti, işyerini, ve kuruluşu içermektedir. Fakat, aynı ağda bu kadar çok kullanıcıya sahip olmak, tek başına, interneti oyun kurallarını değiştiren bir yenilikçi yapmak için yeterli değildir. Bu kullanıcıların bilgisayarlar üzerinden belgeleri ve kaynakları birbirine bağlamak için bir tür mekanizmaya ihtiyaçları vardır. Bir başka deyişle, bilgisayar *A*'da bulunan bir kullanıcı bilgisayar *B* üzerindeki bir dosyayı açmak için kolay bir yola ihtiyaç duymaktadır. Bu ihtiyaç, ağda bulunan makineler üzerindeki belge ve kaynakların nasıl ilişkilendirileceğini tanımlayan bir sistemi doğurmuştur. Bu sistemin adı **World Wide Web (WWW)**'dir. Siz onu **siber uzay (*cyberspace*)** veya kısaca Web olarak biliyor olabilirsiniz. Web'i şöyle düşünün: İnternet iletişim ağlarını birbirlerine bağlamaktadır. Web, ağa bağlı bilgisayarlar üzerinde bulunan web sitelerinin, web sayfalarının, ve sayısal içeriğin bağlantısıdır. Siber uzay, dünya çapındaki bu elektronik erişim alanı içindeki erişilebilir kullanıcılar, ağlar, web sayfaları ve çalışan uygulamaların tümüdür.

Amerika Birleşik Devletleri'nde Yakın Geçmişteki Veri İhlalleri (2013-2015)

Son birkaç yıl içerisinde Amerika Birleşik Devletleri'nde rapor edilen **veri ihlallerinde (*data breaches*)** dramatik bir artış görülmüştür. Kamu sektörü ve özel sektör, her ikisi de bu ihlallere kurban gitmiştir. **TABLO 1-1**, yakın geçmişteki veri ihlallerinin, etkilenen kuruluşun ve veri ihlalinin o kuruluş üzerindeki etkisinin bir özetini listelemektedir.

TABLO 1-1 Amerika Birleşik Devletleri'nde Yakın Geçmişteki Veri İhlalleri, 2013-2015.

KURULUŞ	VERİ İHLALİ	VERİ İHLALİNİN ETKİSİ
Adobe Systems Incorporated: Yazılım Abone Veritabanı	Adobe, 3 Ekim 2013'de yaşanan bir ihlalde, bilgisayar korsanlarının 150 milyon hesap bilgisini yayınladığını ve şifrelenmiş müşteri kredi kartı verisini çaldığını duyurmuştur. Aynı zamanda, bilinmeyen sayıda Adobe kullanıcı hesabının sisteme giriş için kullanılan kimlik bilgilerinin gizliliği de ihlal edilmiştir.	Bilgisayar korsanları 3 milyon kredi kartı kaydını çalmış ve 160.000 Sosyal Güvenlik Numarasına (***Social Security Number*** - SSN) erişmiştir. Adobe, ihlalden etkilenen müşterilerine bir yıl süre ile ücretsiz kredi izleme hizmeti teklif etti.
Anthem, Inc.: Blue Cross Blue Shield müşteri veritabanı	Anthem, 4 Şubat 2015'de kriminal bilgisayar korsanlarının sunucularına yasa dışı olarak girdiğini ve hesap sahiplerinin kimlik bilgilerini içeren potansiyel olarak 37,5 milyonun üzerinde kaydı sunucularından çaldığını açıklamıştır. Anthem, 24 Şubat 2015'de kişisel bilgileri etkilenmiş olan kurbanların sayısını 78,8 milyon insana yükseltmiştir. Veri ihlali, Anthem'in sağlık sigortası planlarını pazarlamakta kullandığı, Anthem Blue Cross, Anthem Blue Cross and Blue Shield, Blue Cross and Blue Shield of Georgia, Empire Blue Cross and Blue Shield, Amerigroup, Caremore, and UniCare gibi bir çok markayı kapsamaktadır.	Verileri çalınan bireyler, tüm hayatları boyunca bu kimlik hırsızlığından kaynaklanan problemlerle karşılaşabileceklerdir. Anthem, siber saldırıları kapsayan 100 Milyon Dolarlık bir sigorta poliçesini American Group One'dan satın almıştır.

KURULUŞ	VERİ İHLALİ	VERİ İHLALİNİN ETKİSİ
Excellus BlueCross BlueShield: Blue Cross Blue Shield müşteri veritabanı	Şirketin BT sistemlerinin Aralık 2013'de başlayacak şekilde ihlal edilmesiyle 10 milyondan fazla üyenin kişisel verileri açığa çıkmıştır. Şirketin verdiği bilgiye göre, Excellus ihlalinden etkilenen bireyler arasında Excellus'un yukarı Newyork bölgesindeki 31 ilçede tedavi görmüş diğer Blue Cross Blue Shield planlarının üyeleri de bulunmaktadır. İfşa edilen veri içinde isimler, adresler, doğum günleri, Sosyal Güvenlik Numaraları, sağlık sigortası poliçe numaraları ve banka hesap numaraları ile tazminat talep verileri ve klinik bilgiler bulunmaktadır.	Excellus aleyhine açılan davada, sağlık sigortacısı şirketin müşterilerinin hassas verilerini ve verileri sistemlerinde depolanan müşterilerini korumak için gerekli yasal yükümlülüklerini yerine getirmekte başarısız olduğu öne sürülmüştür. Ayrıca, davada Excellus'un olayı kamuoyuna bildirmeden bir ay öncesinden veri ihlalini bildiği de iddia edilmiştir.
Hilton Hotel & Resorts: Seyahat endüstrisi müşteri ve kredi kartı veritabanı	Birçok bankanın, ülke genelinde Hilton mülklerinde bir kredi kartı ihlalinden şüphelenmesinden sonra, Hilton bazı satış noktası sistemlerinde kötücül yazılım bulunduğunu belirten bir sızma olayını kabul etmiştir. Hilton çalınan verinin kart sahibi isimlerini, ödeme kartı numaralarını, güvenlik kodlarını ve son kullanma tarihlerini içerdiğini, fakat adres ve kişisel kimlik numaralarını içermediğini söylemiştir.	Hilton ödeme kartı bilgilerini hedef alan yetkilendirilmemiş kötücül yazılımı tespit edip kökünü kurutmak ve sistemlerinin güvenliğini güçlendirmek için harekete geçmiştir. Şirket, etkilenen müşterilerine bir yıl ücretsiz kredi hesabı izleme hizmeti önermiştir.
Target Corp.: Ülke çapındaki perakendecinin müşteri ve kredi kartı veritabanı	Aralık 2013'de Target sistemlerinde meydana gelen bir veri ihlali 110 milyon kadar müşteriyi etkilemiştir. İfşa olan müşteri bilgisi; isimler, telefon numaraları, e-posta ve posta adreslerini içermektedir.	Target, ihlal nedeniyle finans kuruluşlarında meydana gelen zararı karşılamayı kabul etmiştir fakat perakendeci ortaya çıkan ihtilaf üzerinde MasterCard ile bir anlaşma sağlayamamıştır.

(devam ediyor)

TABLO 1-1 Amerika Birleşik Devletleri'nde Yakın Geçmişteki Veri İhlalleri, 2013-2015. (Devam)

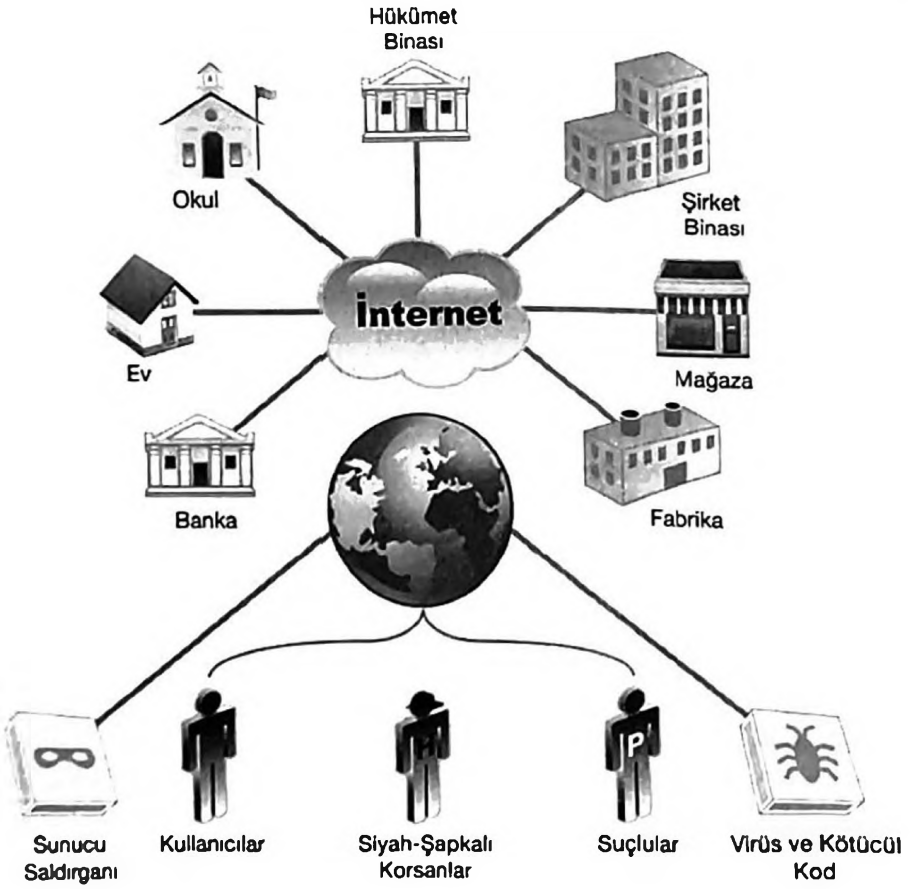
KURULUŞ	VERİ İHLALİ	VERİ İHLALİNİN ETKİSİ
Experian Information Solutions, inc., ve T-Mobile USA, Inc.: Kredi için başvuran T-Mobile müşterilerinin veritabanı	Experian, 15 Eylül 2015'de saldırganların kredi için başvuran 15 milyon T-Mobile müşterisinin kişisel verilerini barındıran bir Kuzey Amerika iş birimi sunucusunu ihlal ettiğini ortaya çıkarmıştır. T-Mobile bu bilgiyi kredi çeklerini işlemek ya da finans sağlaması için Experian ile paylaşmıştır. Sosyal Güvenlik ve kredi kartı bilgileri ifşa olmuştur. Dahili Gelirler Servisi (***Internal Revenue Service*** - IRS) bu veri ihlalinin bir sonucu olarak 13.673 Amerikan vatandaşının 65 milyon dolarlık düzmece bireysel vergi iadesi başvurusu yolu ile mağdur edildiğini doğrulamıştır.	T-Mobile, taşıyıcının (***carrier***) iş ortağı seçimine rağmen, kendisinin değil ama üçüncü parti bir ortağın eylemleri nedeni ile itibar ve finansal kayıp yaşamaktadır.
Sony Pictures Entertainment: Gizli dosyalar, e-postalar ve çalışanların verisi	24 Kasım 2014'de kendilerini Barış Gardiyanları ***(Guardians of Peace)*** olarak adlandıran bir bilgisayar korsanı grubu Sony Pictures film stüdyosundan gizli bilgi sızdırmıştır. Bilgi sızıntısı Sony Pictures çalışanlarına ve ailelerine ait kişisel bilgiler, çalışanlar arası e-postalar, Sony yöneticilerinin maaş bilgileri, henüz gösterime girmemiş filmlerin kopyaları ve diğer bilgileri içermektedir. Aralık ayında, FBI Barış Gardiyanlarının Kuzey Kore hükümeti adına hareket ettiğini tespit etmiştir.	2 Ocak 2015'de Amerikan başkanı Barack Obama, spesifik olarak bu siber saldırıya ve süregelen Kuzey Kore politikalarına atıfta bulunarak, Kuzey Kore hükümetine ve bir Kuzey Kore silah tüccarına karşı ilave yaptırımlar yürürlüğe koyan bir başkanlık emri yayınlamıştır. Obama ayrıca kongreye Sony olayı benzeri siber suçlara daha iyi yanıt vermek ve vatandaşların mahremiyetlerini korurken bu tür suçları benzer çevrim dışı suçlarla uyumlu bir şekilde yargılayabilmek için mevcut yasaları güncelleyen bir yasa tasarısı sunmuştur.

KURULUŞ	VERİ İHLALİ	VERİ İHLALİNİN ETKİSİ
U.S. Office of Personnel Management: ABD Federal Hükümetinin bir Birimi	Haziran 2015'de ABD Personel Yönetimi Ofisi (Office of Personnel Management - OPM) yaklaşık 22 milyon insanı etkileyen bir veri ihlalinin hedefi olduğunu duyurmuştur. Veri ihlali OPM tarafından Nisan 2015'de farkedilmiştir. Federal yetkililer olayı Amerika Birleşik Devletler tarihindeki en büyük hükümet verisi ihlalleri arasında tanımlamıştır. İhlalde hedef alınan veri Sosyal güvenlik numaralarının yanı sıra isimler, tarihler, doğum yerleri ve adresler gibi kişileri tanımlayan bilgileri içermektedir. Saldırı, başlangıçta düşünülenden daha derine gitmiştir ve muhtemelen detaylı güvenlik kontrolleri ile ilişkili kişisel geçmiş bilgisi hırsızlığını da kapsamaktadır.	Veri ihlali, rahatlıkla 40 yıl sürebilecek çok büyük bir karşı istihbarat tehdidi yaratmıştır. Kişisel geçmiş soruşturma veritabanında yer alan her beş bekar federal çalışanından en az dördünün izlenmesi gerekecektir. Evli ya da birden fazla evlenenlerde ise etkilenen insan sayısı 14 kişide en az 12'dir.
The Wendy's Co.: Ulusal hazır yemek perakendecisinin müşteri ve kredi kartı veritabanı	Aralık 2015'de bir şeylerden şüphelenmeye başlayan, Ohio kökenli burger zinciri, ülke genelindeki Wendy's dükkanlarında kullanılan kredi kartlarında olağandışı hareketlere ilişkin raporları incelemeye başlamıştır. Şirket zarar tespiti için siber güvenlik uzmanlarından oluşan bir ekibi işe aldı ve kolluk kuvvetleriyle bu suçun soruşturulması konusunda işbirliği yapmaktadır Wendy's yerlerinde işlem yapmış 6.000 kadar müşteri etkilenmiş olabilir.	Soruşturma yenidir ve devam etmektedir fakat kart ihlalleri restoran endüstrisinde giderek daha yaygın hale gelmektedir. Lokanta zincirleri, büyük olasılıkla eski teknoloji kullanımları nedeniyle saldırılara özellikle açıktır.

Siber uzaya bağlandığınız zaman, ne yazık ki, aynı zamanda kapıyı bir sürü kötü insana da açmış olursunuz. Bu insanlar, sizi bulmak ve verilerinizi çalmak istemektedirler. Kullanıcıları hayatlarının her alanında destekleyen bir Nesnelerin İnterneti (IoT) yaratan ve internete bağlanan her bilgisayar ya da cihaz tehlikededir. Dış uzay gibi, olgunlaşan internet de yeni bir sınır boyudur. Bir internet hükümeti veya merkezi otoritesi yoktur. İnternet zorluklarla ve kuşkulu davranışlarla doludur: Bu kuşkulu davranışlar sadece son üç yılda gördüğümüz veri ihlalleri dikkate alındığında bile bellidir. Amerika Birleşik Devletleri'nde, resmi ve özel sektörler yetkisiz erişimler ve veri ihlali saldırıları ile tehlikeye düşürülmüştür. Bu son saldırılar, kişiler, organize siber suçlular ve diğer ülkelerden saldırganlar tarafından yapılmıştır. ABD çıkarlarına karşı yapılan siber saldırıların sayısı artmaktadır.

Nesnelerin İnterneti'nin (IoT) şimdi, kişisel cihazlar, ev cihazları ve motorlu taşıtları da ağa bağlamasıyla, çalmak için her zamankinden daha çok veri bulunmaktadır. Tüm kullanıcılar bilgilerini saldırganlardan korumak zorundadırlar. **Siber güvenlik (*cybersecurity*)** ulusal güvenliğini korumak isteyen her hükümetin görevidir. Veri güvenliği bilgi varlıklarını ve hassas verilerini (örn., Sosyal Güvenlik Numaraları, kredi kartı numaraları, ve benzeri) koruması gereken her kuruluşun sorumluluğudur. Ve kendi sahip olduğumuz veriyi korumak hepimizin görevidir. **ŞEKİL 1-1** bu yeni sınır boyunu göstermektedir.

Siber uzayı oluşturan bileşenler otomatik olarak güvenli değildir. Bu bileşenler kablolama, fiziksel ağlar, işletim sistemleri ve bilgisayarların internete bağlanmak için kullandığı yazılım uygulamalarını içermektedir. Sorunun kalbinde **İletim Kontrol Protokolü/İnternet Protokolü (*Transport Control Protocol/Internet Protocol - TCP/IP*)** haberleşme protokolündeki güvenlik eksikliği yatmaktadır. Bu protokol internet üzerindeki bilgisayarların haberleşmek için en çok



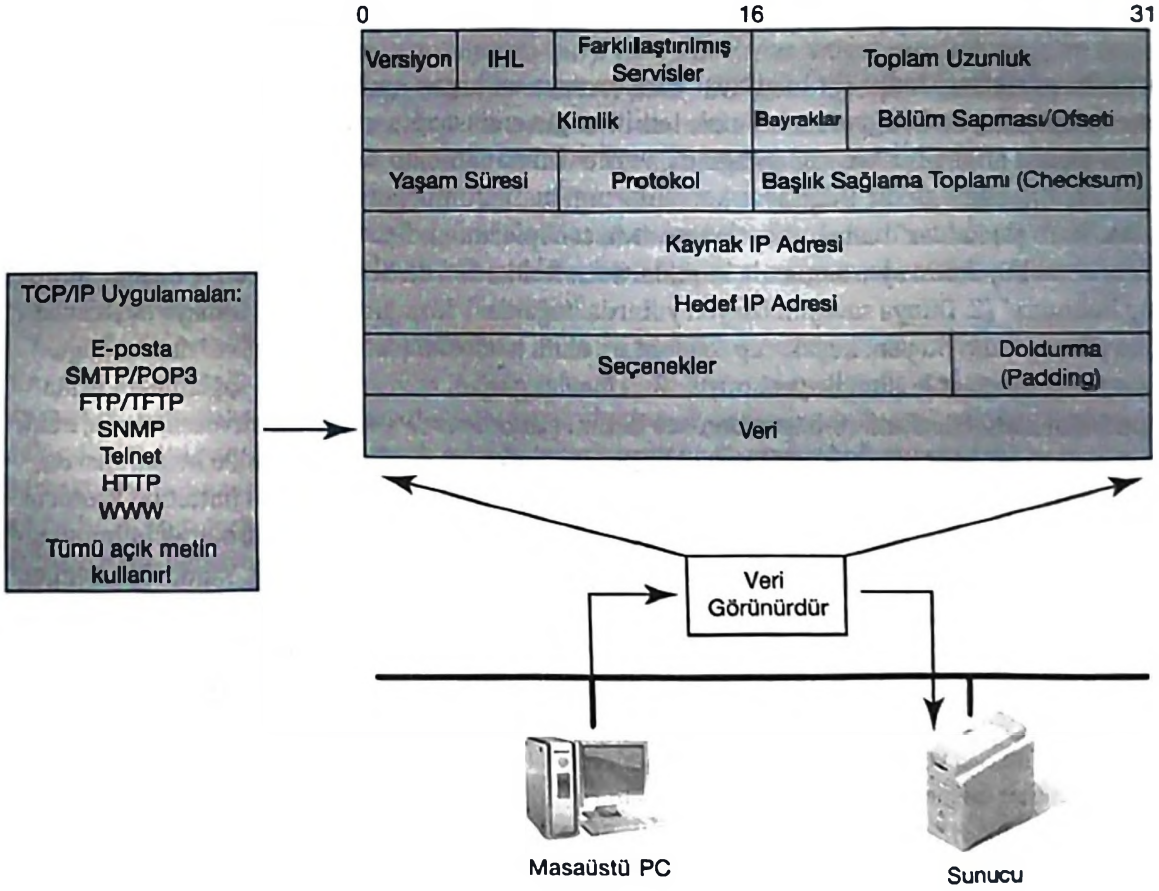
ŞEKİL 1-1
Siberuzay: yeni sınır boyu

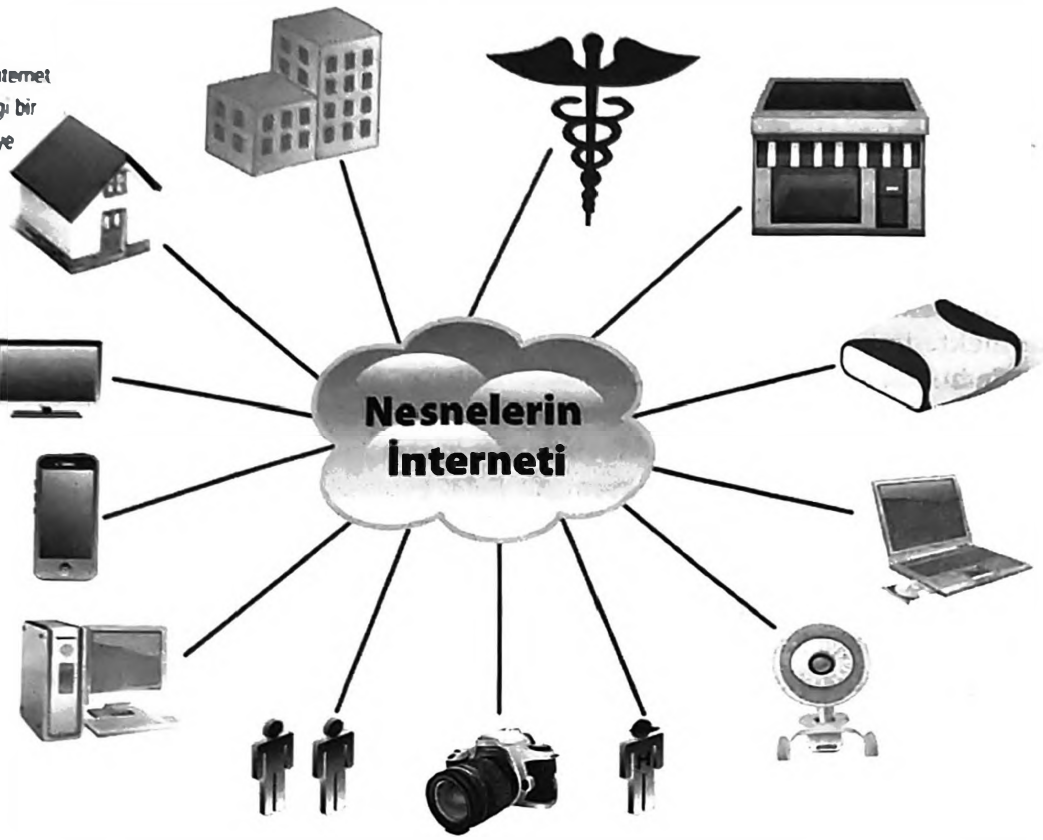
kullandıkları dildir. (**Protokol** haberleşme için kullanılan bir kurallar ve yöntemler listesidir.) TCP/IP tek bir protokol değildir fakat bir ağ üzerinden haberleşmek için geliştirilmiş bir protokol takımıdır. En önemli iki protokolünün adını taşıyan, TCP/IP'de takımı oluşturan protokoller herhangi iki bilgisayarın haberleşmesine izin vermek için birlikte çalışmaktadırlar. TCP/IP ağa bağlı bilgisayarlar arasında veri göndermek için iletileri öbeklere veya paketlere ayırmaktadır. Sorun, her IP paketindeki verinin herkesin kullanabileceği basit yazılımlar ile okunabilir durumda olmasıdır. Verinin bu okunabilir durumu **açık metin** ***(cleartext)*** olarak bilinmektedir. Bu, veriyi daha güvenli kılmak için bir TCP/IP paketi içinde gönderilen veriyi gizlemeniz ya da şifrelemeniz gerektiği anlamına gelmektedir. **ŞEKİL 1-2** TCP/IP paket yapısı içerisindeki veri alanlarını göstermektedir.

Bütün bunlar şu soruyu akla getirmektedir: İnternet bu kadar güvensiz ise neden herkes internete bu kadar istekle bağlanmıştır? Yanıt, Web'in 1990'ların ortalarından 2000'li yılların başlarına kadar yaşanan muazzam büyümesidir; internete bağlanmak herkese Web'e ve Web'in çok sayıdaki kaynaklarına anında erişim imkanı vermiştir. Kolay evrensel bağlantının cazibesi bağlanma taleplerinin itici gücü olmuştur. Bu talep ve ardından gelen büyüme, yüksek hızlı iletişim maliyetlerini düşürmeye yardımcı olmuştur. Ev halkı, ticarethaneler ve hükümetler uygun fiyatlı yüksek hızlı internet erişimine sahip olmuştur. Kablosuz ve hücresel bağlantıların giderek daha yaygın ve uygun fiyatlı olması ile bağlı kalmak, nerede olursanız olun ve hangi cihazla bağlanmış olursanız olun, daha kolay olmuştur. **ŞEKİL 1-3** IoT'nin dünyayı nasıl sayısal olarak bağlanmış bir bütün haline

ŞEKİL 1-2

TCP/IP haberleşmeleri açık metindir





ŞEKİL 1-3
Nesnelerin İnterneti (Internet of Things - IoT) herhangi bir şeyden-herhangi bir şeye bağlantıyı destekler.

getirdiğini göstermektedir. Bir bilgisayar korsanı veya saldırgan herhangi bir IP-bağlı cihaza yetkisiz erişim sağlayabileceğinden, IoT risk, tehdit ve güvenlik açığı sorunlarını büyütmektedir. Bir IP-bağlı cihaza erişim bir kez sağlandığında, veriler çalınabilmekte veya saldırgan isterse bu cihaz hasara uğratılabilmektedir. Bilgisayar korsanlarının bu "karanlık kötü adam (*dark villain*)" doğası onların "kara şapkalılar" olarak etiketlenmesinin sebeplerindendir.

İnternetin büyümesi aynı zamanda kuşaklararası farklardan da beslenmektedir. **Y Kuşağı** kültürü, "baby boomers" (2. Dünya savaşını izleyen yıllarda doğanlar) kuşağının emekli olmaya başlaması ile öne çıkmaktadır. Bu yeni kuşak, cep telefonları, **akıllı telefonlar (*smartphones*)**, ve "daima-bağlı (*always-on*)" İnternet erişimi ile yetişmiştir. Bu cihazlar gerçek zamanlı iletişim sağlamaktadırlar. Günümüzün kişisel iletişimi IP-üzerinden-ses iletimi (*Voice over IP* - VoIP), metin mesajlaşma, anlık mesajlaşma (*Instant Messaging* - IM), ve sohbetin yanı sıra sesli ve görüntülü video konferansı da içermektektedir. Bu gerçek zamanlı, Oturum Başlatma Protokolü-etkin (Session Initiation Protocol (SIP)-enabled) uygulamalar genel olarak **birleşik iletişim (*unified communication*)** olarak bilinmektedir. Birleşik iletişim uygulama örnekleri Google Chat™ anlık mesajlaşma servisi, Yahoo! Messenger, WebEx™, GoToMeeting™, ve Skype™ for Business'in çevrimiçi buluşma özelliklerini içermektedir.

Bu sırada, bir **bilgi güvenliği (*information security*)** savaşı şiddetle sürmektedir. Siber uzay savaş alanıdır ve düşmanlar hali hazırda kale duvarlarının içindedirler. İşi daha da kötü hale getiren ise düşmanın hem yerel alan ağlarında hem de dünyanın öbür ucunda olması yani her yerde olmasıdır. Düşman sizin hassas verinizi aramaktadır. Bu nedenle, saldırgan için oyunun adı yetkisiz erişim sağlamaktır. **Yetkisiz erişim (*unauthorized access*)** saldırganın, sizin yetkilendirilmiş oturum açma kimliğinizi ve parolanızı sizin izniniz olmadan elde etmesi anlamına gelmektedir. Saldırgan, size ait bu giriş bilgilerini kullanarak, erişim izniniz olan tüm sistem ve uygulamalara erişim hakkı kazanmaktadır.

Eğer yetkisiz erişim sağlandı ise, yasal kullanıcının erişim denetimlerine bağlı olarak, hassas verilere erişilebilmekte ve indirilebilmektedir. Bu sebeple, bilgi teknolojisi altyapıları uygun güvenlik kontrollerine ihtiyaç duymaktadır. Bu güvenlik savaşı, bilgi sistemleri güvenliği ve bilgi güvencesi (*information assurance*) uzmanları – güvenlik ve ticari çıkarları savunmak için yeni bir siber savaşçı türü için muazzam bir talep yaratmıştır.

Riskler, Tehditler, ve Zafiyetler

Bu kitap siber uzayın tehlikelerini ortaya koymakta ve bu tehlikelerle nasıl başedileceğini tartışmaktadır. **Bilgi sistemlerinde *(information systems)*** ve BT altyapılarında sıklıkla karşılaşılan tehlikelerin nasıl tanınacağını ve onlarla nasıl savaşılacağını açıklamaktadır. Bilgisayarların nasıl daha güvenli hale getirileceğini anlamak için, önce riskler, tehditler ve zafiyetler kavramlarını anlamanız gerekmektedir.

Risk bir varlığa kötü bir şey olacak olması olasılığıdır. Bir varlığa etki edecek bazı olaylara maruz kalma düzeyidir. Bu varlık, BT güvenliği bağlamında, bir bilgisayar, bir veritabanı, veya bir bilgi parçası olabilmektedir. Aşağıda bazı risk örnekleri verilmektedir:

- Veri kaybı
- Bir afetin binanızı yıkması sebebiyle uğradığınız iş kaybı
- Yasa ve yönetmeliklere uymamak

Tehdit bir varlığa hasar verebilecek herhangi bir eylemdir. Bilgi sistemleri hem doğal hem de insan kaynaklı tehditlerle karşı karşıya kalmaktadır. Sel, deprem, ve şiddetli fırtına tehditleri, kuruluşların afetlerin verdiği hasardan kurtulmak ve işlerine devam edebilmek için planlar yaratmalarını gerektirmektedir. Bir **iş sürekliliği planı *(business continuity plan - BCP)*** bir kuruluşun işlevlerine, kuruluşun işini devam ettirebilmesi için o işleve ne kadar ihtiyaç duyduğuna göre öncelik atamaktadır. Bir **afet kurtarma planı *(disaster recovery plan - DRP)*** bir işyerinin yangın veya fırtına gibi bir büyük felaketten sonra nasıl tekrar ayakları üzerine kalkabileceğini tanımlamaktadır. Bir bilgisayar sistemi insan kaynaklı tehditler virüsler, kötücül kodlar, ve yetkisiz erişimi içermektedir. Bir **virus**, bir sistem, uygulama veya veriye zarar vermek amacıyla yazılmış bir bilgisayar programıdır. **Kötücül kod *(malicious code)***, veya **kötücül yazılım *(malware)*** örneğin bir sabit diski silmek gibi spesifik bir eyleme neden olmak için yazılmış bir bilgisayar programıdır. Bu tehditler kişilere, işyerlerine veya kuruluşlara zarar verebilmektedir.

Bir **zafiyet/güvenlik açığı *(vulnerability)*** bir tehditin gerçekleşmesine ya da bir varlık üzerinde etki etmesine olanak sağlayan bir zayıflıktır. Zafiyetin ne olduğunu anlamak için ateş yakmayı düşünün. Ateş yakmak mutlaka kötü bir şey değildir. Izgarada yemek pişiriyorsanız, ateş yakmanız gerekmektedir. Izgara, ateşi içinde tutacak şekilde tasarlanmıştır ve uygun kullanılırsa tehlike oluşturmamaktadır. Öte yandan, bir bilgisayar veri merkezi içinde ateş yakmak büyük olasılıkla hasara yol açacaktır. Ateş, ızgara için bir zafiyet değildir fakat bilgisayar veri merkezi için bir zafiyettir. Bir tehdit tek başına her zaman hasara neden olmaz; o tehditin gerçekleşebilmesi için bir *zafiyet* olmalıdır.

Zafiyetler genellikle yasal yükümlülüklerle sonuçlanabilmektedir. Bir tehditin gerçekleşmesine sebep olan bir zafiyet soruşturma ve yasal işleme yol açmaktadır. Bilgisayarlar faydalı olmak için yazılımları çalıştırmak zorundadır ve yazılımları da insanlar yazdığı için yazılım programları kaçınılmaz olarak hatalar içermektedirler. Bu nedenle, yazılım satıcıları, yazılımlarından kaynaklanan zafiyetlerin getireceği yasal yükümlülüklerden kendilerini korumak için **Son Kullanıcı Lisans Sözleşmesini (*End-User License Agreement* - EULA)** kullanırlar. Bu sözleşme kullanıcı paketi açıp yazılımı kurduğunda devreye girmektedir. Tüm yazılım satıcıları EULA sözleşmelerini kullanmaktadır. Bu, BT sistemlerini ve verileri koruma yükünün dahili (*internal*) bilgi sistemleri güvenliği uzmanlarına ait olduğu anlamına gelmektedir.

Son Kullanıcı Lisans Sözleşmeleri (EULA'lar)

EULA'lar kullanıcı ile yazılım satıcısı arasındaki lisans sözleşmeleridir. EULA'lar yazılım satıcılarını kusurlu yazılım davranışları sebebiyle ortaya çıkacak tazminat taleplerinden korumaktadır. EULA'lar genellikle garanti koşullarını içermektedir. Bu, yazılım satıcılarının, bilgisayar korsanlarının kötüye kullanabileceği yazılım hatalarından ***(bugs)*** ve zayıflıklarından doğan yükümlülüklerini sınırlamaktadır.

Burada Microsof'un EULA'sından, şirketin yazılımı için sadece "sınırlı" garantiler verdiğini ifade eden bir alıntı verilmektedir. Bu EULA ayrıca, yazılım ürününün "olduğu gibi ve tüm hatalarıyla" sunulduğunu bildirmektedir.

DISCLAIMER OF WARRANTIES. THE LIMITED WARRANTY THAT APPEARS ABOVE IS THE ONLY EXPRESS WARRANTY MADE TO YOU AND IS PROVIDED IN LIEU OF ANY OTHER EXPRESS WARRANTIES (IF ANY) CREATED BY ANY DOCUMENTATION OR PACKAGING. EXCEPT FOR THE LIMITED WARRANTY AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, MICROSOFT AND ITS SUPPLIERS PROVIDE THE SOFTWARE PRODUCT AND SUPPORT SERVICES (IF ANY) AS IS AND WITH ALL FAULTS, AND HEREBY DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS....

Microsoft'un EULA'sı ayrıca kendi mali yükümlülüklerini, yazılımın fiyatı ya da 5$ ile, hangisi daha büyükse, sınırlamaktadır.

LIMITATION OF LIABILITY. ANY REMEDIES NOTWITHSTANDING ANY DAMAGES THAT YOU MIGHT INCUR FOR ANY REASON WHATSOEVER (INCLUDING, WITHOUT LIMITATION, ALL DAMAGES REFERENCED ABOVE AND ALL DIRECT OR GENERAL DAMAGES), THE ENTIRE LIABILITY OF MICROSOFT AND ANY OF ITS SUPPLIERS UNDER ANY PROVISION OF THIS EULA AND YOUR EXCLUSIVE REMEDY FOR ALL OF THE FOREGOING (EXCEPT FOR ANY REMEDY OF REPAIR OR REPLACEMENT ELECTED BY MICROSOFT WITH RESPECT TO ANY BREACH OF THE LIMITED WARRANTY) SHALL BE LIMITED TO THE GREATER OF THE AMOUNT ACTUALLY PAID BY YOU FOR THE SOFTWARE PRODUCT OR U.S.$5.00. THE FOREGOING LIMITATIONS, EXCLUSIONS AND DISCLAIMERS (INCLUDING SECTIONS 9, 10 AND 11 ABOVE) SHALL APPLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EVEN IF ANY REMEDY FAILS ITS ESSENTIAL PURPOSE.

Bilgi Sistemleri Güvenliği Nedir?

Güvenlik terimini parçalara ayırarak tanımlamak daha kolaydır. Bir bilgi sistemi, kişiler veya kuruluşlar için bilgi toplamak, işlemek ve depolamak için birlikte çalışan, donanım, işletim sistemi, ve uygulama yazılımından oluşmaktadır. Bu nedenle, **bilgi sistemleri güvenliği *(information systems security)*** bilgi sistemlerini ve üzerlerindeki veriyi koruyan faaliyetler topluluğudur. Birçok ABD yasası ve uluslararası yasa, bu tür güvenlik güvencelerini şu anda zorunlu kılmaktadır. Kuruluşlar bu ihtiyacı doğrudan karşılamak durumundadırlar. **ŞEKİL 1-4** bir BT altyapısında yaygın olarak bulunan bilgi türlerini incelemektedir.

ABD Uyum (Compliance) Yasaları Bilgi Sistemleri Güvenliği İhtiyacının İtici Gücüdür

Siber uzay, insanlar ve kuruluşlar için yeni tehditler getirmektedir. Kişiler kendi mahremiyetlerini korumalıdır. İşletmeler ve kuruluşlar hem kendi fikri mülkiyetlerini hem de işledikleri kişisel ve özel verileri korumaktan sorumludurlar. Çeşitli yasalar, kuruluşların özel ve gizli verileri korumak için güvenlik kontrolleri kullanmasını gerektirmektedir. Aşağıdakiler, yakın zamanda çıkan bilgi güvenliği ile ilişkili ABD yasaları arasındadır:

- **Federal Bilgi Güvenliği Yönetim Yasası (Federal Information Security Management - FISMA)** — 2002'de yasalaşan FISMA federal hükemet bünyesindeki sivil dairelerin federal işlemleri destekleyen kaynaklar üzerinde güvenlik kontrolleri sağlamasını gerektirmektedir.

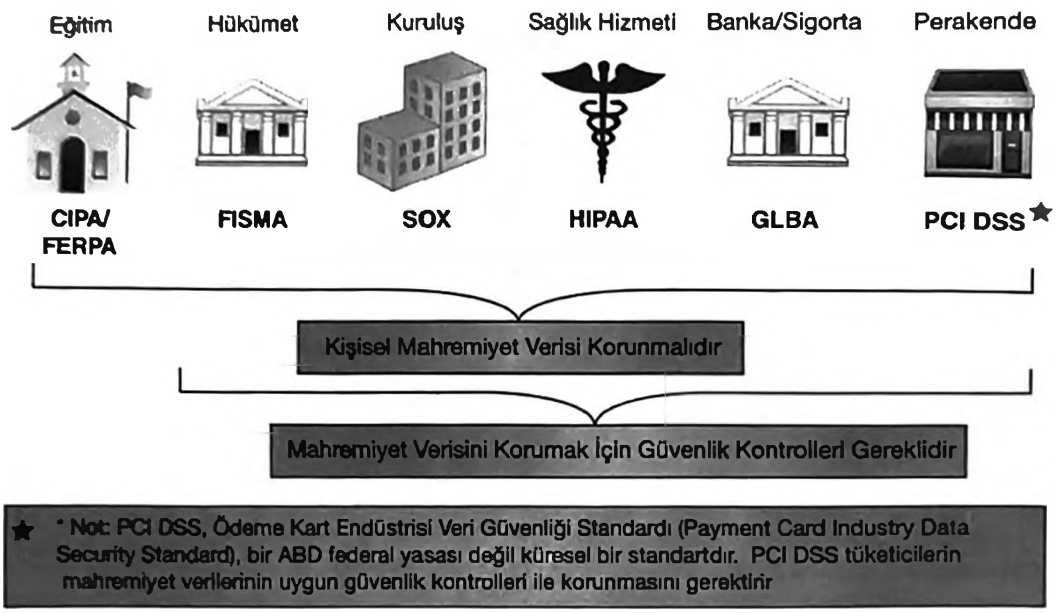


- Bireylerin Mahremiyet Verileri
  - İsim, adres, doğum tarihi
  - Sosyal Güvenlik Numarası
  - Banka ismi, hesap numarası
  - Kredi kartı hesap numarası
  - Hizmet hesap numarası
  - İpotek hesap numarası
  - Sigorta poliçe numarası
  - Menkul kıymetler ve aracılık hesap numaraları
- Kurumsal Fikri Mülkiyeti
  - Ticari sırlar
  - Ürün geliştirme
  - Satış ve pazarlama stratejileri
  - Mali kayıtlar
  - Telif hakları, patentler, vb.
- Çevrimiçi (*Online*) B2C and B2B İşlemleri
  - Çevrimiçi bankacılık
  - Çevrimiçi sağlık hizmeti ve sigorta tazminat talepleri
  - E-ticaret, e-devlet, hizmetler
  - Çevrimiçi eğitim ve transkriptler
- Hükümet Fikri Mülkiyeti
  - Ulusal Güvenlik
  - Askeri ve Savunma Bakanlığı (*Department of Defense* - DoD) stratejileri

ŞEKİL 1-4
Neyi güvenli hale getiriyoruz?

- **Federal Bilgi Güvenliği Modernizasyon Yasası (*Federal Information Security Modernization Act* - FISMA)** — 2014'de yasalaşan FISMA, FISMA 2002'yi modern tehditleri yanı sıra güvenlik kontrolleri ve en iyi uygulamalar bağlamında güncellemek için getirildi.
- **Sarbanes-Oxley Yasası (SOX)** —2002'de yasalaşan SOX halka açık şirketlerin doğru ve güvenilir mali raporlar yayınlamalarını gerektirmektedir. Bu yasa kişisel bilginin güvenceye alınmasını gerektirmemektedir fakat finansal raporlamanın gizliliği ve bütünlüğü için güvenlik kontrollerini gerektirmektedir.
- **Gramm-Leach-Bliley Yasası (GLBA)** — 1999'da yasalaşan GLBA, her tür finans kuruluşunun müşterilerinin kişisel mali bilgilerini korumasını gerektirmektedir.
- **Sağlık Sigortası Taşınabilirlik ve Sorumluluk (*Health Insurance Portability and Accountability Act* - HIPAA)**— 1996'da çıkan HIPAA, sağlık hizmeti veren kuruluşların hasta mahremiyetini korumak için güvenlik ve mahremiyet kontrolleri gerçekleştirmelerini gerektirir.
- **Çocukların İnternetten Korunması Kanunu (*Children's Internet Protection Act* - CIPA)**— 2000'de geçen ve 2011'de güncellenen CIPA, devlet okullarının ve halka açık kütüphanelerin bir internet güvenliği politikası kullanmasını gerektirmektedir. Bu politika aşağıdaki konulara çözüm getirmelidir:
  - Çocukların internette uygunsuz konulara erişimini sınırlamak
  - E-posta, sohbet odaları, ve diğer elektronik iletişim programlarını kullanırken çocukların güvenliğini garanti etmek
  - Çocukların çevrimiçi bilgisayar korsanlığı ve diğer yasa dışı faaliyetlerini kısıtlamak
  - Çocuklar hakkında kişisel bilgilerin izinsiz olarak dağıtılmaması ve açıklanmaması
  - Çocukların zararlı içeriğe erişiminin kısıtlanması
  - Çocukların sosyal medyanın kullanımı ve tehlikeleri konusunda uyarılması

ŞEKİL 1-5
ABD Uyum yasaları bilgi sistemleri güvenliği ihtiyacının itici gücüdür.



- **Aile Eğitim Hakları ve Mahremiyet Yasası (Family Educational Rights and Privacy Act - FERPA)**— 1974'de yasalaşan FERPA, öğrencilerin kişisel verilerini ve okul kayıtlarını korumaktadır.

ŞEKİL 1-5 bu yasaları ilgili endüstrilere göre göstermektedir.

Bilgi Sistemleri Güvenliğinin İlkeleri

Çoğu insan kişisel bilginin güvenli olması gerektiği konusunda hemfikirdir. Fakat, "güvenli bilgi" gerçekte ne anlama gelmektedir? Güvenli olan bilgi üç ana ilkeyi veya özelliği sağlamaktadır. Eğer bu üç ilkeyi sağlayabiliyorsanız, güvenli bilgi gereksinimlerini sağlamış olursunuz. Bu üç ilke aşağıdaki gibidir:

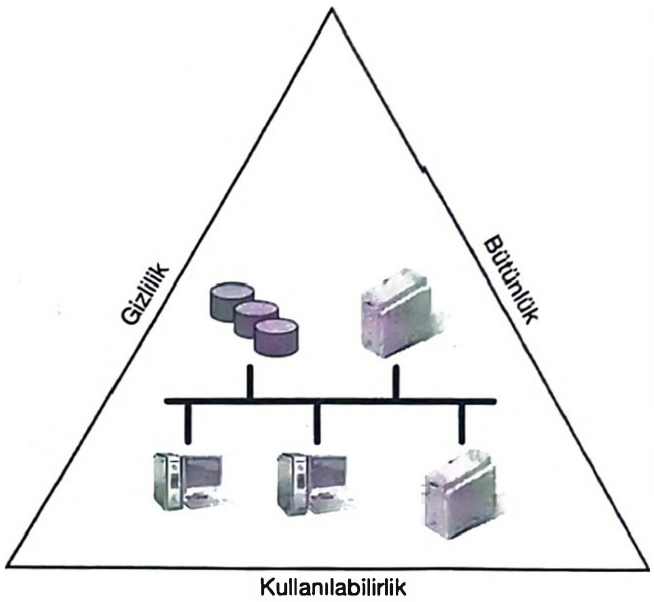
- **Gizlilik *(Confidentiality)*** – Sadece yetkili kullanıcılar bilgiyi görebilmektedir.
- **Bütünlük *(Integrity)*** – Sadece yetkili kullanıcılar bilgiyi değiştirebilmektedir.
- **Kullanılabilirlik *(Availability)*** – Bilgi yetkili kullanıcıların talep ettikleri her zaman erişilebilirdir.

ŞEKİL 1-6 bilgi sistemleri güvenliğinin üç ilkesini göstermektedir. Bir güvenlik kontrolü tasarladığınız ya da kullandığınız zaman bu üç ilkeden bir veya birkaçında bir sorun çözüyorsunuz demektir.

Güvenlik konularına çözüm ararken, **C-I-A** (Confidentiality – Integrity - Availability) üçgenini kullanmalısınız. Tipik bir BT altyapısı için, kuruluşunuzun güvenlik temel hedeflerini bu üçlüyü kullanarak tanımlamalısınız. Bir kez tanımlandığında, bu hedefler koruduğunuz verinin türüne göre güvenlik kontrollerine ve gereksinimlerine dönüşecektir.

Teknik İPUCU

Bazı sistem güvenlik uzmanları bu ilkeleri, genellikle CIA olarak bilinen Amerikan Merkezi İstihbarat Ajansı (U.S. Central Intelligence Agency) ile karışmaması için A-I-C olarak adlandırmaktadır.



ŞEKİL 1-6
Bilgi sistemleri güvenliğinin üç ilkesi.

Kimlik hırsızlığı her yıl 50 milyar dolara varan mali kayıplara sebep olmaktadır ve yaklaşık olarak 15 milyon ABD vatandaşını etkilemektedir. Kimlik hırsızlığı ABD'li tüketiciler için önemli bir tehdittir. Bir kişinin kimliği bir çok bileşenden oluşmaktadır. Bu bileşenlerin kısmi bir listesi aşağıda verilmektedir:

- Ad soyad
- Posta adresi
- Doğum tarihi
- Sosyal Güvenlik Numarası
- Banka ismi
- Banka hesap ismi
- Kredi kartı hesap numarası
- Elektrik/Su vb. abone numarası
- Tıbbi kayıt numarası
- İpotek hesap numarası
- Sigorta poliçe numarası
- Menkul kıymetler ve yatırım hesabı numaraları

Örneğin, bir sahtekar banka hesaplarınıza sadece isminiz, ev adresiniz, ve Sosyal Güvenlik Numaranızı kullanarak erişebilmektedir. Çöpe atılan banka hesap özetleri veya hesap numaraları vicdansız bir kişi tarafından geri alınması, kişisel verinizin ve mali hesap bilgilerinizin kötüye kullanımını kolaylaştırmaktadır. Çöpe atmadan önce dokümanları belge parçalayıcısından geçirmek kayıp olasılığını azaltmaktadır.

Bu tehdit basit mali kayıpların çok ötesine uzanmaktadır. Kimlik hırsızlığı sizin (ABD'de Fair Isaac Corp. - **FICO**) kişisel kredi notunuza zarar vermektedir. Bu bankalardan ev ve ihtiyaç kredisi almanızı engelleyebilmektedir. Kişisel kredi tarihçenizi temizlemek yıllar alabilmektedir. FICO halka açık bir şirket olup, Equifax, Experian, ve TransUnion gibi Amerika Birleşik Devletleri'nde tüketici kredisi raporu veren en büyük üç kuruluşun kullandığı bilgileri sağlamaktadır.

Gizlilik

Gizlilik (*Confidentiality*) genel bir terimdir. Bilgiyi hakkı olanlar dışındaki herkesten korumak anlamına gelmektedir. Gizli bilgi aşağıdakileri içermektedir:

- Kişilerin özel verileri
- İşletmelerin fikri mülkiyetleri
- Ülkeler ve hükümetler için ulusal güvenlik

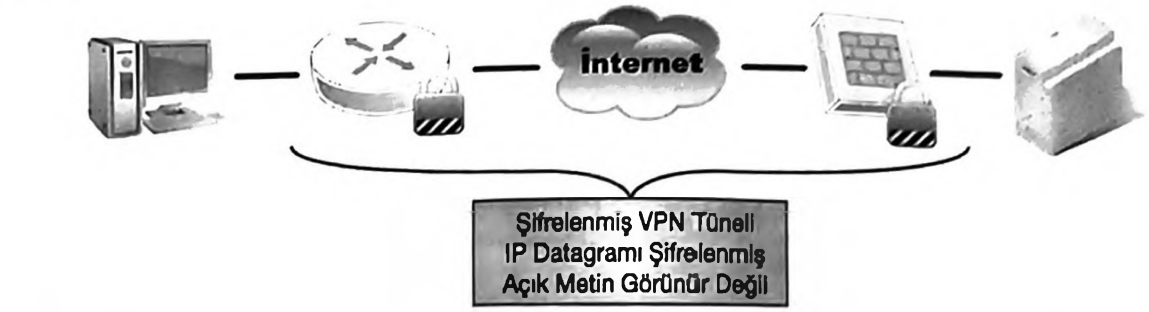
Vatandaşların kişisel verilerini koruyan ABD uygunluk yasaları, işletmeler ve kuruluşların gizliliği garanti etmek için uygun güvenlik kontrollerine sahip olmalarını gerektirmektedir.

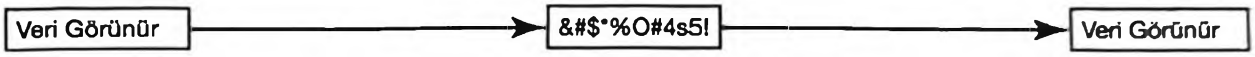
E-ticaret'in büyümesi ile daha çok insan kredi kartları ile çevrimiçi satın alma yapmaktadır. Bu durum, insanların e-ticaret web sitelerine kişisel verilerini girmelerini gerektirmektedir. Tüketiciler kişisel kimlik bilgilerini ve özel verilerini korumak için dikkatli olmalıdırlar. Yasalar kuruluşların müşterilerinin kişisel verilerini korumak için güvenlik kontrolleri kullanmalarını zorunlu tutmaktadır. Bir **güvenlik kontrolü** bir kuruluşun riski azaltmak için yaptığı bir şeydir. Bu tür kontrollere örnekler aşağıda verilmektedir:

- Çalışanlar için yıllık güvenlik farkındalık eğitimi vermek. Bu, personele kişisel verilerin doğru kullanımını hatırlatmaya yardımcı olmaktadır. Ayrıca, kuruluşun güvenlik politikaları çerçevesi, standartları, ve yönergeleri konusunda farkındalığı arttırmaktadır.
- Bir **BT güvenlik politika çerçevesi** *(IT security policy framework)* oluşturmak. Bir politika çerçevesi, güvenlik kontrollerinin nerede kullanılacağını belirlemektedir.
- Bir BT altyapısı için katmanlı bir güvenlik çözümü tasarlamak. Kişisel verileri ve fikri mülkiyeti koruyan veya bloke eden ne kadar çok katman veya bölme varsa verileri ve mülkiyeti bulmak ve çalmak o kadar zorlaşmaktadır.
- Websiteleri ve BT altyapısı üzerinde periyodik güvenlik risk değerlendirmesi, denetim, ve sızma testleri yapmak. Bu, güvenlik uzmanlarının kontrolleri uygun yerleştirdiklerini doğrulama şeklidir.
- İnternet giriş ve çıkış noktalarında güvenlik olayı ve kaza izlemeyi etkinleştirmek. Bu ne geliyor ve ne gidiyoru görmek için bir mikroskop kullanmak gibidir.
- Otomatikleştirilmiş iş istasyonu ve sunucu antivirüs ve kötücül yazılım koruması kullanmak. Bu, virüsleri ve kötücül yazılımları bilgisayarınızın dışında tutmanın yoludur.
- Hassas sistemler, uygulamalar ve veriler için bir oturum açma kimliği ve parolanın ötesinde daha sıkı erişim kontrolleri kullanmak. Oturum açma kimliği ve parolalar kullanıcının yalnızca tek bir kontrolüdür. Daha hassas sistemlere erişimde, kullanıcının kimliğini doğrulamak için ikinci bir test olmalıdır.
- Bilgisayarlarınızdaki ve sunuculardaki yazılımların zayıflıklarının güncelleme ve güvenlik yamaları ile en aza indirilmesi. Bu işletim sistemi ve uygulama yazılımının güncel tutulması için uygun yoldur.

Özel verilerin korunması veri gizliliğini garanti edilmesi işlemidir. Kuruluşlar bu iş için uygun güvenlik kontrollerini kullanmak zorundadırlar. Bazı örnekler aşağıda verilmektedir:

- Gizli verileri korumak için kuruluş genelinde geçerli politikalar, standartlar, prosedürler, ve yönergeler tanımlanmalıdır. Bunlar kişisel bilginin nasıl ele alınıp işleneceğini gösteren komutlardır.
- Verileri BT altyapınız boyunca nasıl işleyeceğinizi tanımlayan bir **veri sınıflandırma standartı *(data classification standard)*** seçilmelidir. Bu verileri güvende tutmak için hangi kontrollere ihtiyaç olduğunu gösteren bir yol haritasıdır.
- Gizli veri içeren sistem ve uygulamalara erişim, sadece o verileri kullanmaya yetkili olanlarla sınırlandırılmalıdır.





ŞEKİL 1-7
Açık metinin şifreli metine şifrelenmesi.

- Kriptografi teknikleri kullanarak gizli verileri saklamak ve o verileri yetkisiz kullanıcılara karşı görünmez tutmak.
- Halka açık internet üzerinden geçen verileri şifrelemek
- Veritabanları ve veri depolama cihazlarında tutulan verileri şifrelemek

Bir ağ üzerinden başka bilgisayarlara veri göndermek, sizin gizli verileri yetkisiz kullanıcılardan korumak için özel adımlar atmanız gerektiği anlamına gelmektedir. **Kriptografi** veriyi gizleme ve yetkisiz kullanıcılardan uzak tutma uygulamasıdır. Şifreleme ***(encryption)*** veriyi açık metin halinden şifreli metin ***(ciphertext)*** haline dönüştürme işlemidir. Açık metin veri, herkesin okuyabileceği formattaki veridir. Şifreli metin ise açık metnin şifrelenmesi sonucu karıştırılmış biçimdeki veridir. Bu işlemin bir örneği **ŞEKİL 1-7**'de gösterilmektedir.

Veri mahremiyeti öyle önemlidir ki yerel ve eyalet hükümetleri federal yasaları genişletecek biçimde verileri koruyan yasalar geçirmeye başlamışlardır.

Bütünlük

Bütünlük (*Integrity*) verinin geçerlilik ve doğruluğu ile ilgilenmektedir. Bütünlüğü olmayan veri – yani, geçersiz veya doğru olmayan veri – kullanışlı değildir. Veri ve bilgi, bazı kuruluşlar için fikri mülkiyet varlıklarıdır. Örnekler arasında telif hakları, patentler, gizli formüller ve müşteri veritabanları bulunmaktadır. Bu bilgilerin değeri büyük olabilmektedir. Yetkisiz değişiklikler, verilerin değerini düşürmektedir. Bu nedenle, bütünlük bir sistem güvenliği ilkesidir. **ŞEKİL 1-8**, veri bütünlüğü ve bu verilerin kullanılabilir olup olmadığı ile ne denmek istendiğini göstermektedir. Özellikle de veriler iş operasyonları için kritik öneme sahipse, sabotaj ve veri bütünlüğünün bozulması bir kuruluşa yönelik ciddi tehditlerdir.

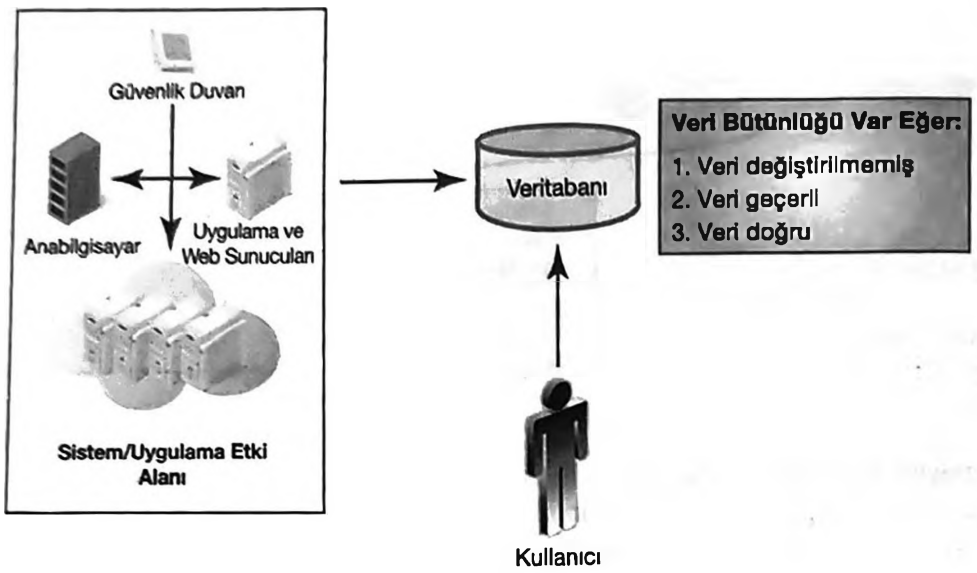
Kullanılabilirlik

Kullanılabilirlik (*Availability*) günlük hayatta yaygın bir terimdir. Örneğin, siz muhtemelen internet hizmetinin, TV hizmetinin, veya cep telefonu hizmetinin kullanılabilirliğine dikkat ediyorsunuzdur. Bilgi güvenliği bağlamında, kullanılabilirlik genellikle kullanıcıların bir

⚠ UYARI

Açık metin biçimindeki bir e-postada asla özel bilgilerinize yer vermeyiniz. E-posta trafiğinin İnternet üzerinde açık metin olarak iletilmekte olduğunu hatırlayınız. Bu durum sizin verilerinizin bu e-postayı gören herkese tümüyle görünür olduğu anlamına gelmektedir. Ayrıca, eğer bir web sitesi bir telefon ya da benzer yollarla doğrulanamayan güvenilir bir sunucu değilse bu web sitelerine asla kişisel verilerinizi girmeyiniz. Şifreleme kullanmayan bir web sitesine veya web uygulamasına asla kişisel veriler girmeyin (örneğin, bir web sitesinde veya uygulamada ***Güvenli Hiper Metin Aktarım Protokolü (Hypertext Transfer Protocol Secure - HTTPS)*** şifrelemesinin etkin olup olmadığını doğrulamak için tarayıcınızda kilit simgesini arayın).

ŞEKİL 1-8
Veri Bütünlüğü



sistem, uygulama veya verinin ulaşılabilir ve kullanılabilir olduğu zaman miktarı olarak ifade edilmektedir. Yaygın kullanılabilirlik süresi ölçütleri aşağıdakileri içermektedir:

- **Çalışma süresi (*Uptime*)**— Çalışma süresi, bir sistemin, uygulamanın veya verinin erişilebilir olduğu toplam zaman miktarıdır. Çalışma süresi genellikle verilen bir takvim ayı için saniye, dakika ve saat cinsinden ölçülmektedir. Çalışma süresi sıklıkla mevcut zamanın bir yüzdesi olarak ifade edilmektedir, örneğin, yüzde 99,5 çalışma süresi.
- **Aksama süresi (*Downtime*)**—Arızalı süre, bir sistem, uygulama veya verinin erişilebilir olmadığı toplam zaman miktarıdır. Arızalı süre de bir takvim ayı için saniye, dakika ve saat cinsinden ölçülmektedir.
- **Kullanılabilirlik (*Availability*)**—Kullanılabilirlik K = (Toplam Çalışma Süresi) / (Toplam Çalışma Süresi + Toplam Aksama Süresi) formülü ile hesaplanmaktadır.
- **Arıza için ortalama süre (*Mean time to failure - MTTF*)**—MTTF belli bir sistemde arızalar arasında geçen ortalama süredir. Yarı-iletkenler ve elektronik parçalar kolay bozulmaz ve çok büyük MTTF değerlerine (25 ya da daha fazla yıl vb.) sahiptir. Konnektörler, kablolama, fanlar ve güç kaynakları gibi fiziksel parçalar, aşınma ve yıpranmanın onları parçalayabileceği gerçeği dikkate alındığında, çok daha düşük MTTF değerlerine (beş yıl ya da daha az) sahiptirler.
- **Onarım için ortalama süre (*Mean time to repair - MTTR*)**—MTTR, bir sistem, uygulama, veya bileşeni onarmak için gerekli olan ortalama süredir. Amaç sistemi en kısa sürede ayağa kaldırmaktır.
- **Arızalar arası ortalama süre (*Mean time between failures - MTBF*)**—MTBF, işlem sırasında bir BT sisteminin arızaları arasında geçen tahmini zamandır.
- **Kurtarma süresi hedefi (*Recovery time objective - RTO*)**—RTO, bir kesintiden sonra bir sistem, uygulama, ya da verinin geri kazanılarak tekrardan kullanılabilir duruma getirilmesi için gereken zamandır. İş sürekliliği planları tipik olarak kritik görev sistemler, uygulamalar ve veri erişimi için bir RTO tanımlamaktadır.

Aylık Kullanılabilirliği Nasıl Hesaplarız

Verilen bir 30 günlük takvim ayı için, toplam çalışma süresi miktarı eşittir:

30 gün × 24 saat/gün × 60 dakika/saat = 43.200 dakika

28 günlük bir takvim ayı (Şubat) için, toplam çalışma süresi miktarı eşittir:

28 gün × 24 saat/gün × 60 dakika/saat = 40.320 dakika

Aşağıdaki formülü kullanarak

Kullanılabilirlik = (Toplam çalışma süresi) / (Toplam çalışma süresi + Toplam aksama süresi)

30 dakika planlanmış aksama (ya da servis dışı) süresi ile 30 günlük bir takvim ayı için kullanılabilirlik faktörü:

Kullanılabilirlik = (43.200 dakika) / (43.200 + 30 dakika) = 0,9993 veya %99,93

olarak hesaplanmaktadır.

Telekomünikasyon ve internet hizmet sağlayıcıları müşterilerine **servis seviyesi anlaşmalar (*service level agreement* - SLA)** sunmaktadırlar. Bir SLA, geniş alan ağları (*wide area network* - WAN) ve internet erişim hatları için asgari aylık hizmet kullanılabilirliğini garanti eden sözleşmedir. SLAlar WAN servisleri ve adanmış internet erişim hatlarının kullanımına eşlik etmektedirler. Kullanılabilirlik, bir aylık çalışma süresi servis seviyesi taahhüdünü ölçmektedir. Yukarıda verilen aylık kullanılabilirlik örneğinde görüldüğü gibi 30 günlük bir takvim ayında 30 dakikalık bir servis dışı süresi yüzde 99,993 bir kullanılabilirliğe eşittir. Servis sağlayıcılar genellikle yüzde 99,5 ile yüzde 99,999 kullanılabilirlik arasında değişen SLAlar önermektedirler.

Tipik bir BT Altyapısının Yedi Etki Alanı

Tipik bir BT altyapısında bilgi güvenliğinin üç ilkesi ne rol oynar? İlk olarak, tipik bir BT altyapısı nasıl görülür, ona bakalım. İster bir küçük işletme, büyük bir hükümet organı veya halka açık şirket olsun, çoğu BT altyapıları **ŞEKİL 1-9**'da gösterilen yedi etki alanından oluşmaktadır: Kullanıcı, İş istasyonu, LAN, LAN-WAN, WAN, Uzak Erişim, ve Sistem/Uygulama etki alanları.

Genellikle, bu yedi etki alanı tipik bir BT altyapısında mevcuttur. Her biri uygun güvenlik kontrollerini gerektirmektedir. Bu kontroller C-I-A üçlüsünün gereksinimlerini karşılamak zorundadır. Aşağıda bu yedi etki alanı ve günümüz BT ortamlarında sıklıkla bulacağınız risklere, tehditlere, ve zafiyetlere genel bir bakış verilmektedir.

Kullanıcı Etki Alanı

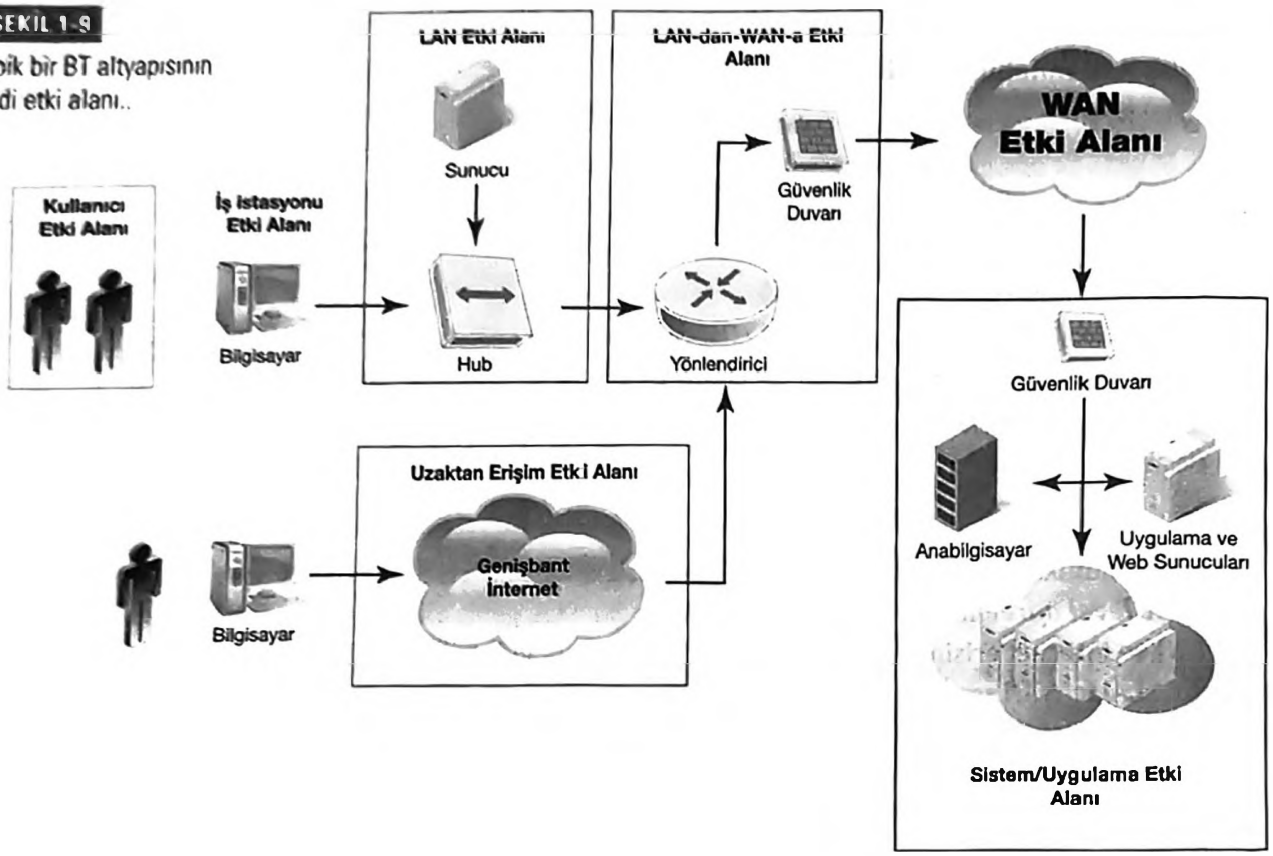
Kullanıcı Etki Alanı bir kuruluşun bilgi sistemlerine erişen insanları ifade etmektedir.

Kullanıcı Etki Alanı Rolleri, Sorumlulukları, ve İzlenebilirlik

Aşağıda, Kullanıcı Etki Alanında neler olması gerektiğine ilişkin genel bir açıklama verilmektedir:

- **Roller ve görevler**—Kullanıcılar, sistemlere, uygulamalara ve verilere, kendileri için tanımlanmış erişim haklarına göre erişebilmektedirler. Çalışanlar personel yönergelerine ve politikalarına uymalıdır.

ŞEKİL 1-9
Tipik bir BT altyapısının yedi etki alanı..



Kullanıcı Etki Alanı **kabul edilebilir kullanım politikası (*acceptable use policy* - AUP)** belgesini bulacağınız yerdir. Bir AUP, kullanıcıların kuruluş-mülkiyetindeki BT varlıkları üzerinde ne yapmalarına izin verildiğini ve izin verilmediğini tanımlamaktadır. Çalışanların uymaları gereken bir kurallar kitabı gibidir. Bu kuralların ihlali işten atılmaya temel oluşturabilmektedir. Burası katmanlı bir güvenlik stratejisi için ilk savunma katmanının başladığı yerdir.

- **Sorumluluklar (*Responsibilities*)**—Çalışanlar BT varlıkları üzerindeki kullanımlarından sorumludurlar. Birçok kuruluş için çalışanlarına bir AUP sunmak, yeni yasal düzenlemeler ışığında yapılacak en iyi uygulamadır. Kuruluşlar, personel, taşeronlar veya diğer üçüncü taraflar için kuruluş içi bilgiyi gizli tutmaları için sözleşme imzalamayı zorunlu tutabilmektedir. Bazı kuruluşlar hassas görevlere getirilecek personel için güvenlik soruşturmasını zorunlu tutabilmektedir. Bölüm müdürü veya insan kaynakları müdürü, genellikle çalışanların bir AUP belgesi imzalamalarından ve belgeye uygun davrandıklarını takipten sorumludurlar.
- **İzlenebilirlik (*Accountability*)**—Genellikle, bir kuruluşun insan kaynakları bölümü doğru çalışan güvenlik kontrollerini uygulamaktan sorumludur. Bu kontroller hassas verilere erişim yetkisi verilecek kişiler için yaptırılmalıdır.

Kullanıcı Etki Alanında Yaygın olarak Bulunan Riskler, Tehditler, ve Zafiyetler

Kullanıcı Etki Alanı bir BT altyapısındaki en zayıf halkadır. Bilgisayar güvenliğinden sorumlu olan herkes, bir kimseyi kuruluşun sistemini, uygulamalarını, veya verilerini tehlikeye atmak için neyin teşvik ettiğini anlamak zorundadır. **TABLO 1-2**, Kullanıcı Etki Alanında yaygın olarak bulunan riskler ve tehditlerin yanı sıra onları engellemek için kullanabileceğiniz planları listelemektedir.

TABLO 1-2 Kullanıcı Etki Alanı için riskler, tehditler, zafiyetler, ve azaltma planları

RİSK, TEHDİT, VEYA ZAFİYET	AZALTMA
Yetkisiz erişim	Kullanıcılarda, olta (*phishing*) e-postalar, hile bahaneleri, klavye kaydediciler, oturum açma kimliği ve parola bilgilerini elde etmek için bir BT çalışanı veya kuryeyi taklit eden sahtekarlar konularında farkındalık yaratılmalıdır.
Kullanıcı farkındalığı eksikliği	Güvenlik farkındalığı eğitimi düzenlenmeli, güvenlik farkındalığı posterleri asılmalı, afişlere hatırlatıcılar eklenmeli ve çalışanlara hatırlatma e-postaları gönderilmelidir.
Politikalara karşı kullanıcı duyarsızlığı	Yıllık güvenlik farkındalığı eğitimi düzenlenmeli, uygun kullanım politikaları yürürlüğe koyulmalı, personel yönerge ve el kitabı güncellenmeli, performans değerlendirmeleri sırasında konu gündeme getirilmelidir.
Güvenlik politikası ihlalleri	Çalışan izlemeye alınmalı, AUP belgesi ve çalışan el kitabı gözden geçirilmeli, performans değerlendirmeleri sırasında konu gündeme getirilmelidir.
Kişisel resim, müzik, ve videolar içeren USB sürücü ve CDlerin kullanımı	CD sürücü ve USB portları iptal edilmeli. Sisteme sokulan medya sürücüleri, dosyalar, ve e-posta eklentileri için otomatik olarak antivirüs taraması etkinleştirilmelidir. Bir antivürüs tarama sistemi bilgisayarınızın sabit diskindeki tüm yeni dosyaları virüslere karşı gözden geçirmektedir. Eklentisi olan e-postalar için antivirüs taraması kurulmalıdır.
Kullanıcının resim, müzik ve video indirmesi	**İçerik filtreleme (*Content filtering*)** ve e-posta eklentileri için antivirüs tarama etkinleştirilmelidir. İçerik filtreleyen ağ cihazları AUP tanımlamalarına uygun olarak spesifik alan isimlerine izin verecek veya ret edecek şekilde yapılandırılmıştır.
Kullanıcının sistemi, uygulamayı, veya verileri tahrip etmesi	Kullanıcıların erişimleri sadece kendi işlerini yapmak için gerekli olan sistem, uygulama, ve verilerle sınırlanmalıdır. Yazma/silme izinleri sadece veri sahibine verilmelidir.
Kuruluşa saldırılar veya kızgın çalışanların sabotajları	Çalışanın normal dışı davranışları, düzensiz iş performansı, ve BT altyapısının mesai saatleri dışı kullanımı takip edilmeli ve gözlemelidir. AUP izleme ve uyumunu temel alan BT erişim kontrol kilitleme prosedürleri başlatılmalıdır.
Kötü giden çalışan romantizmi	Çalışanın normal dışı davranışları ve BT altyapısının mesai saatleri dışı kullanımı takip edilmeli ve gözlenmelidir. AUP izleme ve uyumunu temel alan BT erişim kontrol kilitleme prosedürleri başlatılmalıdır.
Çalışan şantajı veya gaspı	Çalışanın normal dışı davranışları ve BT altyapısının mesai saatleri dışı kullanımı takip edilmeli ve gözlenmelidir. Hassas görevlerde çalışan ve hassas verilere erişen personel için Saldırı Tespit Sistemi/Saldırı Önleme Sistemi (*Intrusion Detection System/Intrusion Prevention System* - IDS/IPS) izlemesi etkinleştirilmelidir. IDS/IPS güvenlik cihazları içeri gelen ve dışarı giden trafik için IP veri akışlarını incelemektedir. Bir IDS/IPS üzerinde programlanmış alarm ve uyarılar normal dışı trafiği tespit etmeye yardım etmekte ve politika tanımlamalarına göre IP trafiğini engellemektedir.

İş İstasyonu Etki Alanı

Bir **iş istasyonu (*workstation*)** bir masaüstü bilgisayar, bir dizüstü bilgisayar, bir özel-amaçlı terminal, veya ağınıza bağlanan başka herhangi bir cihaz olabilir. İş istasyonu bilgisayarları genellikle ince istemciler veya kalın istemcilerdir. Bir **ince istemci *(thin client)*** bir yazılım veya ağ üzerinde çalışan, sabit diski olmayan ve uygulamaları, verileri ve tüm veri işleme işleri için bir sunucuya gereksinim duyan gerçek bir bilgisayardır. İnce istemciler yaygın olarak büyük kuruluşlarda, kütüphanelerde, ve okullarda kullanılmaktadırlar. Buna karşın, bir **kalın istemci *(thick client)*** sabit diski de içeren çok özellikli donanım ve uygulamalardır ve veriyi yerel olarak işlemekte, sunucuya sadece dosyaları depolamak için gitmektedir. Sıradan bir PC, kalın istemciye bir örnektir. İş istasyonları olarak kabul edilebilecek diğer cihazlar **kişisel dijital yardımcılar *(personal digital assistants - PDA'lar)***, akıllı telefonlar, ve tablet PC'lerdir. Mobil cihazlarla ilgili daha fazla detayı "Uzaktan Erişim Etki Alanı" bölümünde bulabilirsiniz.

İş İstasyonu Etki Alanı Rolleri, Sorumluluklar, ve İzlenebilirlik

Bu bölümde İş İstasyonu Etki Alanında nelerin bulunacağı konusuna genel bir bakış sunulmaktadır:

- **Roller ve görevler**—Bir kuruluşun personeli verimli olabilmek için gerekli erişime sahip olmalıdır. Donanımı yapılandırmak, sistemleri güçlendirmek ve antivirüs dosyalarını doğrulamak görevler arasında bulunmaktadır. **Sistemi sertleştirmek (*hardening*)** bilinen tüm tehditlere karşı kontrollerin yerleştirilmiş olduğundan emin olma sürecidir. Güçlendirme faaliyetleri tüm bilgisayarların en son yazılım revizyonlarına, güvenlik yamalarına, ve sistem yapılandırmalarına sahip olduğundan emin olmayı içermektedir. İş istasyonu Etki Alanı ilave savunma katmanlarına da ihtiyaç duymaktadır; bu taktiğe **derinlemesine savunma (*defense in depth*)** adı verilmektedir. Bir başka yaygın savunma katmanı, BT altyapılarına bu etki alanından yapılacak girişleri korumak için iş istasyonu oturum açma kimliklerinin ve parolalarının kullanılmasıdır.
- **Sorumluluklar**—Bir kuruluşun masaüstü destek grubu İş İstasyonu Etki Alanından sorumludur. Tanımlı standartların uygulanmasını temin etmek kullanıcı iş istasyonları ve verilerin bütünlüğünü korumak için kritik öneme sahiptir. BT güvenlik personeli İş İstasyonu Etki Alanındaki kontrolleri korumak zorundadır. Genellikle, insan kaynakları bölümleri çalışanlar için uygun erişim kontrollerini onların görevlerine göre tanımlamaktadır. Ardından, BT güvenlik bölümü sistemlere, uygulamalara ve verilere erişim haklarını bu tanımlara göre atamaktadır.
- **İzlenebilirlik**—Bir kuruluşun BT masaüstü sistemler yöneticisi genellikle çalışanlara İş İstasyonu Etki Alanında en kapsamlı kullanım olanağını sağlamak konusunda yetkili ve sorumlu kılınmaktadır. BT güvenlik direktörü İş İstasyonu Etki Alanının politikaya uygunluğunu temin etmekle görevlidir.

İş İstasyonu Etki Alanında Yaygın olarak Bulunan Riskler, Tehditler, ve Zafiyetler

İş istasyonu Etki Alanı sıkı güvenlik ve erişim kontrolleri gerektirmektedir. Burası kullanıcıların sistemlere, uygulamalara, ve verilere ilk eriştiği yerdir. İş İstasyonu Etki Alanı erişim için bir oturum açma kimliği ve parola gerektirmektedir. **TABLO 1-3** İş İstasyonu Etki Alanında yaygın olarak bulunan riskler, tehditler ve zafiyetler ile birlikte bunlara karşı korunma yollarını listelemektedir.

LAN Etki Alanı

Bir **yerel alan ağı (local area network - LAN)** birbirlerine ya da ortak bir bağlantı ortamına bağlanmış bir bilgisayarlar topluluğudur. Ağ bağlantı ortamı telleri, fiber-optik kabloları, veya radyo dalgalarını içerebilmektedir. LANlar genellikle işleve veya bölüme göre organize edilmektedir.

TABLO 1-3 İş istasyonu Etki Alanı için riskler, tehditler, zafiyetler, ve azaltma planları

RİSK, TEHDİT, VEYA ZAFİYET	AZALTMA
İş istasyonuna yetkisiz erişim	Erişim için iş istasyonları üzerinde parola koruma etkinleştirilmelidir. Kullanılmadığı zamanlarda otomatik ekran kilitleme etkinleştirilmelidir. Kullanıcılar için sistem yöneticisi **(admin)** hakları devre dışı bırakılmalıdır.
Sistemlere, uygulamalara, ve verilere yetkisiz erişim	Katı erişim kontrol politikaları, standartları, prosedürleri ve yönergeleri tanımlanmalıdır. Hassas veri içeren uygulamalara erişim için ikinci bir seviye veya doğrulama katmanı gerçekleştirilmelidir (örneğin, **iki adımlı kimlik doğrulama**)
Masaüstü veya dizüstü bilgisayar işletim sistemi yazılım zafiyetleri	Bir iş istasyonu işletim sistemi **zafiyet penceresi (*vulnerability window*)** politikası ve standardı tanımlanmalıdır. Zafiyet penceresi, bir iş istasyonunun bilinen bir zafiyete karşı yama yapılana kadar maruz kaldığı zaman boşluğudur. Süregelen güvenlik işlemlerinin bir parçası olarak sık sık **zafiyet değerlendirme (*vulnerability assessment*)** taramaları yapılmalıdır.
Masaüstü veya dizüstü bilgisayar uygulama yazılım zafiyetleri ve yazılım yama güncellemeleri	Bir iş istasyonu uygulama **yazılım zafiyet (*software vulnerability*)** politikası ve standardı tanımlanmalıdır. Uygulama yazılımı ve güvenlik yamaları tanımlanmış politikalar, standartlar, prosedürler, ve kılavuzlara göre güncellenmelidir.
Kullanıcı iş istasyonunun ve dizüstü bilgisayarının virüsler, kötücül koddan, ya da kötücül yazılımdan etkilenmesi	İş istasyonu antivirüs ve kötücül kod politikaları, standartları, prosedürleri ve yönergeleri kullanılmalıdır. Uygun koruma ile kişisel iş istasyonlarını tarayan ve güncelleyen otomatik antivirüs koruma çözümü aktif edilmelidir.
Kullanıcının kuruluş bilgisayarlarına CD, DVD, veya USB sürücü takması	Tüm CD, DVD ve USB portları devre dışı bırakılmalıdır. Takılan ve dosya barındıran tüm CD, DVD ve USB sürücüleri için otomatik antivirüs taraması etkinleştirilmelidir.
Kullanıcı tarafından İnternet'ten indirilen resim, müzik ve videolar	İçerik filtreleme ve İnternet giriş ve çıkış noktalarında antivirüs tarama kullanılmalıdır. Tüm yeni dosyalar için iş istasyonu otomatik taramaları etkinleştirilmeli ve bilinmeyen dosya tipleri karantinaya alınmalıdır.
Kullanıcının AUP ihlali, kuruluşun BT altyapısı için güvenlik riskleri yaratmaktadır	Tüm çalışanlar için yıllık güvenlik farkındalık eğitimi zorunlu tutulmalıdır. Yıl boyunca güvenlik farkındalığı kampanyaları ve programları düzenlenmelidir.
Çalışanlar ve kullanıcılar işyerinde kendi akıllı telefon veya tabletlerini kullanmak istemektedirler, bu da kuruluşun Kendi Cihazını Getir (Bring Your Own Device - BYOD) altyapı desteği sağlamasını gerektirmektedir	Çalışanların kendi kişisel akıllı telefonlarını veya mobil cihazlarını kullanmalarına izin veren bir BYOD politikası ve prosedürü geliştirilmelidir. BYOD politika ve prosedürleri, genel olarak kuruluşa, kullanıcının akıllı telefon veya mobil cihazındaki verileri cihazın kaybolması ya da çalışanın ilişiğinin kesilmesi durumunda silmesine izin vermektedir.

LAN'a birkez bağlanıldığında, bilgisayarınız sistemlere, uygulamalara, muhtemelen internete ve verilere erişebilmektedir. BT altyapısında üçüncü bileşen LAN Etki Alanıdır.

LAN Etki Alanının fiziksel kısmı aşağıdakilerden oluşmaktadır:

- **Ağ arayüz kartı (*Network interface card - NIC*)**—Bilgisayar ile LAN fiziksel ortamı arasındaki arayüzdür. NIC kendisine ait benzersiz bir donanım tanımlayıcı olarak çalışan 6-byte'lık bir Ortam Erişim Kontrol (*Media Access Control* - MAC) katmanı adresine sahiptir.
- **Ethernet LAN**—Bu, 10/100/1.000 Mbps Ethernet ağı için geliştirilmiş **IEEE 802.3 CSMA/CD** standardı üzerine inşa edilmiş bir LAN çözümüdür. **Ethernet** en popüler LAN standardıdır. Günümüzün LAN standardı **Elektrik ve Elektronik Mühendisleri Enstitüsü (*Institute of Electrical and Electronics Engineers - IEEE*)** 802.3 **Taşıyıcı Duyarlı Çoklu Erişim/Çarpışma Tespiti (*Carrier Sense Multiple Access/Collision Detection - CSMA/CD*)** spesifikasyonudur. Ethernet, kampüs ve kent Ethernet omurgası bağlantıları için 10-Mbps, 100-Mbps, 1-Gbps, 10-Gbps, 40-Gbps ve şu anda 100-Gbps hızlarında mevcuttur.
- **Korumasız bükümlü-çift kablolama (*Unshielded twisted-pair cabling*)**—Bu, 100Mbps/1Gbps/10Gbps Ethernet LAN anahtarlarına fiziki olarak bağlanmak için RJ-45 konektörler ve jaklar kullanan iş istasyonu kablolamasıdır. Günümüzde, yüksek hızlı veri iletişimini desteklemek için, kuruluşlar Kategori 5 veya Kategori 6 UTP iletim ortamı kullanmaktadırlar.
- **LAN Anahtarı (*LAN switch*)**—Bu iş istasyonlarını fiziki bir Ethernet LAN'ına bağlayan bir cihazdır. Bir anahtar, her bir iş istasyonuna maksimum üretilen iş ve performansı verecek şekilde, iş istasyonlarına ve sunuculara adanmış Ethernet LAN bağlantısı sağlamaktadır. İki tip LAN anahtarı vardır. Bir **Katman 2 anahtar** MAC katmanı adresini incelemekte ve yönlendirme kararlarını MAC katmanı adres tablosuna göre vermektedir. Bir **Katman 3 anahtar** ağ katmanı adresini incelemekte ve paketleri yönlendirme protokolünün yol belirleme kararlarına göre yönlendirmektedir. Bir katman 3 anahtar bir yönlendirici *(router)* ile aynıdır.
- **Dosya sunucusu ve yazdırma sunucusu**—Bunlar şirket ya da bölüm içi dosya paylaşımı ve veri depolama sağlayan yüksek güçte bilgisayarlardır. Yazdırma servisleri bölüm içinde ortak yazıcı kullanımını desteklemektedir.
- **Kablosuz erişim noktası (*Wireless access point - WAP*)**—Kablosuz **LAN'lar (*wireless LAN'lar*-WLAN'lar)** için, radyo telsizleri IP paketlerini WLAN NIC'den bir **kablosuz erişim noktasına (WAP)** iletmek için kullanılmaktadır. WAP, mobil dizüstü bilgisayarların bağlanması için WLAN sinyalleri göndermektedir. WAP korumasız bükümlü-çift kablo üzerinden geriye LAN anahtarına bağlanmaktadır.

Ethernet anahtarları, tipik olarak, her iş istasyonu için 100-Mbps veya 1-Gbps bağlantı sağlamaktadır. Bugün, Ethernet LAN anahtarları 100-Mbps ve 1-Gbps masaüstü hızları ve 10-Gbps ve 40-Gbps omurga bağlantı hızlarını desteklemektedir. Bu omurga bağlantıları genellikle fiber optik kablolama kullanmaktadır.

LAN Etki Alanının mantıksal kısmı aşağıdakilerden oluşmaktadır:

- **Sistem yönetimi (*System administration*)** – Kullanıcı LAN hesaplarının, oturum açma kimliği ve parola erişim kontrolleri (kullanıcı bağlantı bilgisi) ile kurulması.
- **Dizin ve dosya servislerinin tasarımı** – Kullanıcının erişim hakkının olacağı sunucular, dizinler ve klasörler.
- **İş istasyonu ve sunucu TCP/IP yazılım ve iletişim protokollerinin yapılandırılması/konfigürasyonu** – Bu, IP adreslemesi, **IP varsayılan ağ geçidi yönlendiricisi, alt-ağ maske adresi (*IP default gateway router, subnet mask address*)**, vb. ile ilgilidir. IP varsayılan ağ geçidi yönlendiricisi, LAN'ın giriş/çıkış noktası olarak çalışmaktadır. Alt-ağ maske adresi IP ağ numarası ve IP makine *(host)* numarasını belirlemektedir.

- **Sunucu disk depolama alanı tasarımı; kullanıcı verisinin yedeklenmesi ve kurtarılması**—Kullanıcı veri dosyaları için verinin günlük yedeklendiği ve arşivlendiği LAN disk depolama alanı sağlanmasıdır. Verinin kaybolması veya bozulması durumunda veri dosyaları yedekleme dosyalarından geri kazanılabilmektedir.
- **Sanal LAN'ların (VLAN'lar) Tasarımı**—Katman 2 ve Katman 3 LAN anahtarlar ile Ethernet portları, gerçekte farklı fiziki LAN'lar üzerinde bulunmalarına rağmen aynı VLAN üzerinde yer alacak şekilde yapılandırılabilmektedir. Bu, iş istasyonları ve sunucuları aynı Ethernet LAN veya yayımlama etki alanında *(broadcast domain)* olacak şekilde yapılandırmakla aynı olmaktadır.

Kullanıcılar kendi bölümlerinin LAN'larına ve görev gereksinimlerine göre diğer uygulamalara erişmektedir.

LAN Etki Alanı Rolleri, Sorumluluklar ve İzlenebilirlik

Bu bölümde LAN Etki Alanında nelerin bulunacağı konusuna genel bir bakış sunulmaktadır:

- **Roller ve görevler**—LAN Etki Alanı hem fiziksel ağ bileşenleri hem de kullanıcılar için servislerin mantıksal yapılandırmasını içermektedir. Fiziksel bileşenlerin yönetimi aşağıdakileri içermektedir:
  - Kablolama
  - NIC'ler
  - LAN anahtarları
  - Kablosuz erişim noktaları (WAP'lar)

  LAN sistem yönetimi, kullanıcı hesaplarının ana listelerini ve erişim haklarını korumayı kapsamaktadır. LAN Etki Alanında, iki aşamalı kimlik doğrulama gerekli olabilmektedir. İki-aşamalı doğrulama, kullanıcının kimliğini ikinci kez onaylattığı bir geçide benzemektedir. Bu işlem yetkisiz fiziksel erişim riskini azaltmaktadır.
- **Sorumluluklar**—LAN destek grubu LAN Etki Alanından sorumludur. Bu, hem fiziksel bileşenleri hem de mantıksal elemanları içermektedir. LAN sistem idarecileri bölümün dosya ve yazdırma servislerini sürdürmek ve desteklemek, ve kullanıcılar için erişim kontrollerini yapılandırmak zorundadır.
- **İzlenebilirlik**—LAN yöneticisinin görevi LAN Etki Alanındaki verinin kullanımı ve bütünlüğünü maksimize etmektir. Genellikle, BT güvenlik direktörü LAN Etki Alanının politikaya uyumunu garanti etmelidir.

LAN Etki Alanında Yaygın olarak Bulunan Riskler, Tehditler, Zafiyetler

LAN Etki Alanı, aynı zamanda güçlü güvenlik ve erişim kontrollerine gereksinim duymaktadır. Kullanıcılar şirket genelinde sistemlere, uygulamalara ve verilere erişebilmektedirler. Burası üçüncü savunma katmanının gerekli olduğu yerdir. Bu savunma BT altyapısını ve LAN Etki Alanını korumaktadır. **TABLO 1-4**, LAN Etki Alanında yaygın olarak bulunan riskler, tehditler ve zafiyetler ile birlikte uygun risk azaltıcı stratejileri de listelemektedir.

LAN-dan-WAN-a Etki Alanı

LAN-dan-WAN-a Etki Alanı BT altyapısının bir geniş alan ağına ve internete bağlandığı yerdir. Maalesef, internete bağlanmak kötü adamlara kırmızı halı sermeye benzemektedir. İnternet açıktır, kamusal alandadır ve herkes tarafından kolayca erişilebilmektedir.

TABLO 1-4 LAN Etki Alanı için riskler, tehditler, zafiyetler ve azaltma planları

RİSK, TEHDİT, VEYA ZAFİYET	AZALTMA
LAN'a yetkisiz erişim	Kablo dolapları, veri merkezleri, ve bilgisayar odalarının güvenliğinin sağlandığından emin olunmalıdır. Uygun bir görevli kimliği olmayan kişilere izin verilmemelidir.
Sistemlere, uygulamalara ve verilere yetkisiz erişim	Katı erişim kontrol politikaları, standartlar, prosedürler ve yönergeler tanımlanmalıdır. Hassas sistemlere, uygulamalara ve verilere erişim için ikinci bir kimlik denetimi seviyesi kullanılmalıdır. Kullanıcıların LAN klasörlerine erişimleri ve spesifik dokümanlar için okuma/yazma/silme hakları ihtiyaç halinde kısıtlanmalıdır.
LAN sunucu işletim sistemi yazılım zafiyetleri	Sunucu/masaüstü/dizüstü zafiyet penceresi politikaları, standartları, ve yönergeleri tanımlanmalıdır. Yazılım açıklarını bulmak için periyodik olarak LAN Etki Alanı zafiyet değerlendirmeleri yapılmalıdır. Bir zafiyet değerlendirmesi, yazılımın içindeki kusur ve hataları belirleyen bir yazılım gözden geçirme faaliyetidir. Bu kusur ve hatalar yazılım yama ve düzeltmeleri yüklendiğinde yok olmaktadır.
LAN sunucu uygulama yazılım zafiyetleri ve yazılım yama güncellemeleri	Yazılım yamalarının vakit geçirmeden yüklenmesini zorunlu kılan katı bir yazılım zafiyet penceresi politikası tanımlanmalıdır.
WLAN'lardaki dolandırıcı kullanıcılar tarafından gerçekleştirilen yetkisiz erişim	Kablosuz erişim için parola isteyen WLAN **ağ anahtarları (network keys)** kullanılmalıdır. WAP'lardaki yayımlama **(broadcasting)** kapatılmalıdır. WLAN erişimi onaylanmadan önce ikinci seviye kimlik doğrulama **(authentication)** yapılmalıdır.
WLAN üzerinden veri iletiminin gizliliğinin ihlal edilmesi	İş istasyonu ve WAP arasında gizliliği sağlamak için şifreleme gerçekleştirilmelidir.
Farklı donanım, işletim sistemi ve yazılıma sahip LAN sunucularının yönetim ve sorun gidermeyi güçleştirmesi	LAN sunucu ve yapılandırma standartları, prosedürleri ve yönergeleri oluşturulmalıdır.

İnternet trafiğinin büyük çoğunluğu açık metin halindedir. Bu, trafiğin görünür olduğu ve mahrem olmadığı anlamına gelmektedir. Ağ uygulamaları iki yaygın taşıma protokolü kullanmaktadır: İletim Kontrol Protokolü (*Transmission Control Protocol* - TCP) ve Kullanıcı Veri Bloğu İletişim Kuralı (*User Datagram Protocol* - UDP). TCP ve UDP'nin her ikisi de (trafiğin ait olduğu) uygulama ya da işlevi belirlemek için port numaralarını kullanmaktadır; bu port numaraları bir TV'deki kanallar gibi iş görmekte, hangi istasyonu izlediğinizi belirlemektedir. Bir paket TCP veya UDP ile gönderildiğinde, o paketin ait olduğu port numarası paket başlığında yer almaktadır. Birçok servis belli bir port numarası ile ilişkilendirildiği için, port numarasını bilmek onun ne tür bir paket olduğunu açığa çıkarmaktadır. Bu, iletmekte olduğunuz şeyi dünyaya ilan etmeye benzemektedir.

Aşağıda çok kullanılan TCP ve UDP port numaralarına örnekler verilmektedir:

- **Port 80: Hiper Metin Aktarım Protokolü (*Hypertext Transfer Protocol - HTTP*)**—HTTP web tarayıcıları ile web siteleri arasındaki açık metin veri iletişimi protokolüdür.
- **Port 20: Dosya Aktarım Protokolü (*File Transfer Protocol - FTP*)**—FTP dosya aktarımı yapmak için kullanılan bir protokoldür. FTP bağlantı temelli bir veri iletimi için TCP'yi kullanmaktadır ancak parola da dahil olmak üzere veriler açık metin biçimindedir. *Bağlantılı*

(connection-oriented) olmak, dosya aktarımının bütünlüğünü arttırmak için paketlerin tek tek numaralanması ve alındıklarında teyit edilmeleri anlamına gelmektedir.

- **Port 69: Önemsiz Dosya Aktarım Protokolü (*Trivial File Transfer Protocol - TFTP*)**—TFTP dosya aktarımı yapmak için kullanılan bir protokoldür. TFTP bağlantısız *(connectionless)* veri iletimi için UDP'yi kullanmaktadır ancak veriler açıkta gitmektedir. Bu protokol küçük dosyaların hızlı iletimi içindir ancak her paketin iletimini garanti etmemektedir.
- **Port 23: Terminal Ağı (*Telnet*)**—Telnet bir başka cihaza uzaktan terminal erişimi gerçekleştirmek için kullanılan bir ağ protokolüdür. Telnet TCP'yi kullanmaktadır ve verileri açıkta göndermektedir.
- **Port 22: Güvenli Kabuk (*Secure Shell - SSH*)**—SSH bir başka cihaza uzaktan terminal erişimi gerçekleştirmek için kullanılan bir ağ protokolüdür. SSH, iletişimin gizliliğini korumak için veri iletimini şifrelemektedir.

Çok kullanılan, 0 ile 1023 arasındaki port numaralarının tam bir listesi İnternet Atanmış Numaralar Yetkilisi (*Internet Asigned Numbers Authority*-IANA) tarafından muhafaza edilmektedir. IANA küresel alan isim servisleri, IP adresleri ve diğer kaynakların birlikte çalışmasına yardımcı olmaktadır. Çok kullanılan port numaraları *www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml.* IANA web sitesinde bulunabilir.

TCP/IP protokol takımı *güvenlikten yoksun olduğundan*, bu aileden protokollerle çalışırken güvenlik kontrollerine daha fazla ihtiyaç vardır. LAN-dan-WAN-a Etki Alanı tipik bir BT altyapısı için dördüncü savunma katmanını temsil etmektedir.

LAN-WAN Etki Alanı Rolleri, Sorumlulukları ve İzlenebilirlik

Bu bölümde LAN-dan-WAN-a Etki Alanında nelerin bulunacağı konusuna genel bir bakış sunulmaktadır:

- **Roller ve görevler** – LAN-dan-WAN-a Etki Alanı hem fiziksel parçalar hem de güvenlik araçlarının mantıksal tasarımını içermektedir. Bir BT altyapısında güvenliği sağlamanın en karmaşık olduğu alanlardan biridir. Kullanıcılara mümkün olduğunca çok erişim sağlarken, güvenliği korumanız gerekmektedir. Fiziksel kısımların servise kolay erişim verecek şekilde idare edilmesine ihtiyaç vardır. Güvenlik araçları politika tanımlarına uyacak şekilde yapılandırılmalıdır.

  Bu, kullanılabilirliği *(availability)* en iyi hale getirmekte, veri bütünlüğünü sağlamakta ve gizliliği korumaktadır. LAN-dan-WAN-a Etki Alanında roller ve görevler aşağıdakilerin yönetimini ve yapılandırmasını içermektedir:
  - **IP yönlendiriciler (*IP routers*)** – Bir IP yönlendirici, IP paketlerini İnternet'e ve WAN'a ulaştırmak (hem göndermek hem de almak) için kullanılan bir ağ cihazıdır. Yönlendiricide alınan yol belirleme kararları IP paketlerini yönlendirmektedir. Yapılandırma işleri IP yönlendirme ve erişim kontrol listelerini (*access control lists* – ACL'ler) içermektedir. ACL'ler bir filtre gibi trafiğe engel olmak veya izin vermek için kullanılmaktadırlar.
  - **IP durum denetlemeli güvenlik duvarları (*IP Stateful firewalls*) – Durum denetlemeli bir IP güvenlik duvarı,** gelen *(inbound)* IP paketlerini IP, TCP, ve UDP paket başlıklarına göre yapılandırılmış çeşitli ACL tanımlarına göre filtreleyen bir güvenlik cihazıdır. Durum denetlemeli bir güvenlik duvarı filtreleme için IP, TCP ve UDP paket başlıklarını inceleyebilmektedir.
  - **Arındırılmış bölge (*Demilitarized zone - DMZ*)** – DMZ, LAN-dan-WAN-a Etki Alanı içerisinde gelen ve giden IP trafiği için bir tampon bölge olarak davranan bir LAN segmentidir. Web sunucuları, **vekil sunucular *(proxy servers)***, ve e-posta sunucuları

gibi harici sunucular IP trafiğinin daha fazla izolasyonu ve taranması için bu bölgede konumlandırılabilmektedir.

- **Saldırı tespit sistemleri (*Intrusion Detection Systems - IDS*)** – Bir IDS güvenlik aracı IP data akışını yaygın saldırı ve kötü niyetli örüntüler açısından incelemektedir. IDS'ler pasif olup en fazla bir alarm tetikleyecek kadar ileri giderler fakat trafiği aktif bir şekilde engellemezler.
- **Saldırı engelleme sistemleri (*Intrusion Prevention Systems - IPS*)** – Bir IPS bir IDS'le aynı şeyi yapmaktadır, fakat zararlı olarak tespit edilen IP veri akışlarını engelleyebilmektedir. IPS'ler gerçek iletişim oturumunu sonlandırabilmekte, kaynak IP adresine göre filtreleyebilmekte ve hedef makineye erişimi engelleyebilmektedir.
- **Vekil sunucular (*Proxy servers*)** – Bir vekil, bir iş istasyonu ile dış hedef arasında aracı olarak hareket etmektedir. Trafik bir vekil gibi davranan aracı sunucuya gitmektedir. Veri, vekil güvenlik duvarları veya uygulama ağ geçidi güvenlik duvarı tarafından BT altyapısına yönlendirilmeden önce analiz edilebilmekte ve uygun şekilde taranabilmektedir.
- **Web içerik filtresi (*Web content filter*)** – Bu güvenlik cihazı, alan isimlerinin veya alan isimleri içindeki anahtar kelimelerin filtrelenmesine dayalı olarak içeriğin BT altyapısına girişini engelleyebilmektedir.
- **E-posta içerik filtresi ve karantina sistemi** – Bu güvenlik cihazı e-postaların veya bilinmeyen dosya eklerinin içinde bulunan içeriği uygun antivirüs taraması ve karantina kullanarak engelleyebilmektedir. İnceleme sonrasında, e-posta ve ekler kullanıcıya iletilebilmektedir.

- **Güvenlik bilgi ve olay yönetimi (Security Information and event management - SIEM)** – SIEM, DMZ VLAN, güvenlik duvarları, IDS/IPS, ve diğer güvenlik cihazlarını da kapsayacak şekilde LAN-dan-WAN-a Etki Alanındaki BT varlıklarını gizlilik, bütünlük ve kullanılabilirliği en üst düzeye çıkarmak amacıyla izlemeyi ve belirli durum ve koşullar tarafından tetiklenen güvenlik olaylarını ve alarmları gözlemeyi içermektedir.
- **Sorumluluklar** – LAN-dan-WAN-a Etki Alanından ağ güvenliği grubu sorumludur. Bu hem fiziksel hem de mantıksal elemanları içermektedir. Grup üyeleri tanımlanmış güvenlik kontrollerini uygulamaktan sorumludurlar.
- **İzlenebilirlik** – Kuruluşunuzun WAN ağ yöneticisi LAN-dan-WAN-a Etki Alanını yönetmekle görevlidir. Genellikle, BT direktörü LAN-dan-WAN-a Etki Alanı güvenlik politikaları, standartları, prosedürleri, ve yönergelerinin kullanımını garanti etmektedir.

LAN-dan-WAN-a Etki Alanında Yaygın olarak Bulunan Riskler, Tehditler, ve Zafiyetler

LAN-dan-WAN-a Etki Alanı, internete bağlanmanın riskleri ve tehditleri düşünüldüğünde, katı güvenlik kontrollerine ihtiyaç duymaktadır. Bu etki alanı tüm verilerin BT altyapısına girip çıktığı yerdir. LAN-dan-WAN-a Etki Alanı, tüm kuruluş için internet erişimi sağlamakta ve WAN için giriş ve çıkış noktası gibi davranmaktadır. Bu, aynı zamanda internet giriş/çıkış *(ingress/egress)* noktası olarak bilinmektedir. LAN-dan-WAN-a Etki Alanı, dördüncü savunma katmanının gerekli olduğu yerdir. **TABLO 1-5**, LAN-dan-WAN-a Etki Alanında yaygın olarak bulunan riskleri, tehditleri ve zafiyetleri uygun risk azaltma stratejileri ile birlikte listelemektedir.

WAN Etki Alanı

Geniş Alan Ağı (*Wide Area Network* - WAN) Etki Alanı, uzak yerleri birbirine bağlamaktadır. Ağ maliyetleri düştükçe, kuruluşlar daha hızlı internet ve WAN bağlantıları alabilir hale gelmektedir. Bugün telekomünikasyon servis sağlayıcıları aşağıdakileri satmaktadırlar:

- **Ulusal optik omurgalar**—Özel optik omurga ağları için optik omurga gövdeleri.
- **Uçtan uca IP aktarımı**—Servis sağlayıcının IP ağ altyapısını kullanarak IP hizmetleri ve bağlantı.

TABLO 1-5 LAN-WAN Etki Alanı için riskler, tehditler, zafiyetler ve azaltma planları

RİSK, TEHDİT, VEYA ZAFİYET	AZALTMA
Yetkisiz ağ sorgulaması ***(probing)*** ve port taraması	Tüm LAN-WAN Etki Alanı içinde, dış IP'ye sahip tüm cihazlar üzerinde ***ping***, ***prob*** gönderme ve port tarama devre dışı bırakılmalıdır. Ping, İnternet Kontrol Mesaj Protokolü (***Internet Control Message Protocol*** - ICMP) yankı-istek ***(echo-request)*** ve yankı-yanıt ***(echo-reply)*** mesajlarını kullanmaktadır. IDS/IPS ile sorgulama, tarama ve izleme için kullanılan IP port numaralarına izin verilmemelidir.
LAN-dan-WAN-a Etki Alanı üzerinden yetkisiz erişim	Saldırı tespit ve önleme için katı güvenlik izleme kontrolleri uygulanmalıdır. Gelen IP trafiği üzerindeki anomaliler ve kötü-niyetli trafik izlenmelidir. Eğer trafik kötücül ise anında engellenmelidir.
Halka açık dış IP'ler ve İnternet bağlantıları üzerinde Hizmet Reddi (***Denial of Service*** - DoS)/Dağıtık Hizmet Reddi (***Distributed Denial of Service*** - DDoS) saldırıları	Bir yarı-açık TCP SYN paketleri akışı İnternet Servis Sağlayıcı (***Internet Service Provider*** - ISP) hattı üzerinde ISP bağlantısına flood saldırısı başlattığında yukarı yönde (***upstream***) ISP'ler DoS/DDoS saldırı önlemesi ve IP paketlerinin düşürülmesi çabasına ortak olmak zorundadırlar.
IP yönlendirici, güvenlik duvarı, ve ağ cihazı işletim sistemi yazılım zafiyetleri	Katı bir sıfırıncı gün zafiyet penceresi tanımı belirlenmelidir. Güvenlik düzeltmeleri ve yazılım yaması gerektiren aygıtlar hemen güncellenmelidir.
IP yönlendirici, güvenlik duvarı, ve ağ cihazı yapılandırma dosyası hataları veya zayıflıkları	LAN-dan-WAN-a Etki Alanındaki katmanlı güvenlik çözümü üzerinde yapılandırma sonrası sızma testleri yapılmalıdır. Gelen ve giden trafik test edilmeli ve açıkları giderilmelidir.
Uzak kullanıcıların kuruluşun altyapısına erişebilme ve hassas verileri indirebilme kabiliyeti	Kuruluşun veri sınıflandırma standardı uygulanmalı ve uygulatılmalıdır. Erişim kontrol listelerinde yer alan kaynak IP adresleri kullanılarak giden trafik reddedilmelidir. Uzaktan indirmeye izin veriliyorsa gerektiğinde şifrelenmelidir.
Bilinmeyen kaynaklardan bilinmeyen dosya tipinde eklentiler indirilmesi	Bilinmeyen kaynaklardan bilinmeyen tipte dosya indirilmesine karşı dosya aktarım izleme, tarama, ve alarm kullanılmalıdır.
Yerel kullanıcılara ulaşan bilinmeyen e-posta eklentileri ve gömülü URL bağlantıları	Bilinmeyen dosya türleri için e-posta sunucusu ve eklenti antivirüs ve e-posta karantinaya alma kullanılmalıdır. İçerik filtreleme politikalarına dayalı olarak alan adı web sitesi erişimi durdurulmalıdır.
Web'de sörf yapan ve işlerine odaklanmayan yerel kullanıcılar nedeniyle oluşan verimlilik kaybı	İnternet giriş/erişim noktalarında alan-ismi içerik filtreleme kullanılmalıdır.

- **Çok bölgeli WAN bulut servisleri** – Çok bölgeli *(multisite)* servisler için, Çoklu Protokol **Etiket Anahtarlama (Multi protocol Label Switching - MPLS)** WAN servisleri gibi IP servisleri ve bağlantı önerilmektedir. MPLS, WAN'daki uç noktalar arasında sanal bağlantılar yapmak için etiketler *(label)* veya *tag*'ler kullanmaktadır.
- **Metropol Ethernet LAN bağlantısı** - Şehrin alan ağı içinde sunulan Ethernet LAN bağlantısıdır.
- **Adanmış İnternet erişimi** – Genellikle bir kuruluş içinde paylaşılan geniş bant internet iletişim bağlantısıdır.

- **Yönetilen Servisler** – 24 × 7 × 365 yönlendirici yönetimi ve güvenlik cihazları yönetimidir.
- **Servis seviyesi anlaşmalar (*Service-level agreements* - SLA'lar)** – Kullanılabilirlik, paket kaybı ve sorunları gidermek için tepki süresi *(response time)* gibi aylık servis hizmetleri için sözleşme taahhütleridir.

WAN Etki Alanı genel BT altyapısı için beşinci güvenlik katmanını temsil etmektedir. WAN servisleri, müşterilerin yönlendirici ve güvenlik duvarları için adanmış internet erişimi ve yönetilen servisleri içermektedir. Servis kesilmesine karşı kullanılabilirlik ve tepki süreleri için yönetim anlaşmaları yaygındır. WAN hizmetini kullanılabilir tutmak için ağlar, yönlendiriciler ve donanım sürekli izlenmeli ve yönetilmelidir.

WAN Etki Alanı Rolleri, Sorumlulukları, ve İzlenebilirlik

Burada WAN Etki Alanı içinde nelerin olabileceği konusuna genel bir bakış sunulmaktadır:

- **Roller ve görevler** - WAN Etki Alanı hem fiziksel bileşenler hem de yönlendirici ve iletişim araçlarının mantıksal tasarımını içermektedir. Bir BT altyapısında güvenliği sağlamak bakımından ikinci en karmaşık alandır. Hedeflenen, giren ve çıkanın güvenliğinden emin olunurken kullanıcılara mümkün olan en fazla erişimi sağlamaktır. WAN Etki Alanındaki roller ve görevler aşağıdakilerin yönetilmesini ve yapılandırılmasını içermektedir:
  - **WAN iletişim hatları** - Bunlar binanızda sona eren dijital veya optik bir servis olarak sağlanan fiziksel iletişim bağlantılarıdır. Geniş bant bağlantı hızları aşağıdaki değerler arasında değişebilmektedir:
    - Dijital servis için DS0 (64 Kbps)'dan DS1 (1.544 Mbps)'e ve DS3 (45 Mbps)
    - Optik servis için OC-3 (155 Mbps)'den OC-12 (622 Mbps)'e ve OC-48 (2.488 Mbps)
    - Fiziksel mesafeye bağlı olarak 10/100/1000 Mbps Metro Ethernet LAN bağlantısı
  - **IP ağ tasarımı** – Bu, IP ağının ve adres şemasının mantıksal tasarımıdır. Bu, ağ mühendisliğini, alternatif yol tasarımlarını, ve IP yönlendirme protokolünün seçimini gerektirmektedir.
  - **IP durum denetlemeli güvenlik duvarı** – Bu, IP paketlerini filtrelemek ve istenmeyen IP, TCP, ve UDP paketlerinin ağa girişine veya çıkışına engel olmak için kullanılan bir güvenlik cihazıdır. Güvenlik duvarları LAN segmentlerini korumak için iş istasyonları veya yönlendiricilere yüklenebilmekte veya bağımsız cihazlar olarak görev yapabilmektedirler.
  - **IP yönlendirici yapılandırılması** - Bu, uzak konumlara IP bağlantısı için kullanılan WAN omurgası *(backbone)* ve geliştirilmiş yönlendiriciler *(edge routers)* için gerçek yönlendirici yapılandırma bilgisidir. Yapılandırma IP ağ tasarımı ve adresleme şemasının üzerine inşa edilmelidir.
  - **Sanal özel ağlar (*virtual private networks* - VPN)** – VPN, bir uç noktasından diğerine adanmış bir şifreli tüneldir. VPN tüneli ortak interneti kullanan bir uzak iş istasyonu ile bir VPN yönlendirici arasında veya güvenli bir tarayıcı ile bir **Güvenli Soketler Katmanı Sanal Özel Ağ (Secure Sockets Layer Virtual Private Network - SSL-VPN)** web sitesi arasında yaratılabilmektedir.
  - **Çoklu protokol etiket anahtarlama (*Multiprotocol Label Switching* - MPLS)** - MPLS müşterilerin performansı maksimize etmesine olanak sağlayan bir WAN yazılım özelliğidir. MPLS, IP paketlerini belirlenmiş uç noktaları arasındaki sanal tünellerden hızlı aktarım için etiketlemektedir. Bu, Katman 1/Katman 3 üstüne bindirmeli ağ *(overlay network)* biçimidir ve uzun ömürlü bir akış yapılandırıldığında veya dinamik olarak belirlendiğinde, yönlendirme işlevleri yol belirleme işlemini atlamaktadır.

- **Basit Ağ Yönetim Protokolü (Simple Network Management Protocol - SNMP) ağ izleme ve yönetimi**—SNMP ağ cihazlarında izleme, alarm ve performans için kullanılmaktadır.
- **Yönlendirici ve ekipman bakımı**—Donanım ve *firmware* güncellemelerini gerçekleştirmek, yeni işletim sistemi yazılımı yüklemek ve yönlendiriciler ve filtreleri yapılandırmak için bir gerekliliktir.

- **Sorumluluklar**—WAN Etki Alanından ağ mühendisi veya WAN grubu sorumludur. Bu hem fiziksel hem de mantıksal elemanları kapsamaktadır. Ağ mühendisleri ve güvenlik uygulamacıları tanımlanmış güvenlik kontrollerini tanımlanmış politikalara göre ayarlamaktadırlar. IP ağ mühendisliğinin karmaşıklığı nedeniyle birçok grubun günümüzde WAN ve yönlendiricilerinin yönetimini servis sağlayıcılardan (dışardan) destek olarak aldığına dikkat etmek gerekir. Bu hizmet, sistemin kullanılabilirliğini ve problemlerin çabuk çözüleceğini garanti altına alan SLA'ları içermektedir. Bir WAN bağlantı kesintisi olduğunda, müşteriler servis sağlayıcılarının **ağ operasyon merkezini (*network operations center* - NOC)** ücretsiz bir telefon hattından aramaktadırlar.
- **İzlenebilirlik**—Kuruluşunuzun BT ağ yöneticisi, WAN Etki Alanını korumak, güncelleştirmek ve teknik destek sağlamak zorundadır. Genellikle, BT güvenlik direktörü şirketin WAN Etki Alanı güvenlik politikaları, standartları, prosedürleri ve yönergelerini karşıladığını garanti etmektedir.

Bazı kuruluşlar halka açık interneti kendi WAN altyapısı olarak kullanmaktadırlar. Bu daha ucuz olmasına rağmen, internet mesajların teslimatını veya güvenliğini garanti etmemektedir.

WAN Etki Alanında (İnternet) Yaygın olarak Bulunan Riskler, Tehditler ve Zafiyetler

Telekomünikasyon servis sağlayıcıları uçtan uca iletişim için WAN bağlantısı sağlamakla görevlidir. Servis sağlayıcılar önce kendi ağ altyapılarının güvenliğini sağlama sorumluluğunu üstlenmek zorundadırlar. WAN iletişim servislerine kaydolan müşteriler, hizmet sözleşmelerindeki sorumluluk şartlarını, koşullarını ve sınırlamalarını gözden geçirmelidir. Bu önemlidir çünkü kuruluşlar, yönlendirici yönetimi ve güvenlik yönetimi ile ilgili görevlerinin nerede başlayıp nerede bittiğini anlamalıdırlar.

Bir WAN hizmetleri sözleşmesinin en kritik yönü, servis sağlayıcıların sorun giderme, ağ yönetimi ve güvenlik yönetimi servislerini nasıl sağladığıdır. WAN Etki Alanı, beşinci savunma katmanının gerekli olduğu yerdir. **TABLO 1-6**, riskleri, tehditleri ve WAN Etki Alanının internet segmentinde bulunan zafiyetleri ve uygun risk azaltma stratejilerini içermektedir.

Telekomünikasyon servis sağlayıcıları WAN bağlantı hizmetleri satmaktadırlar. Bazı sağlayıcılar günümüzde güvenlik yönetim hizmetlerini de sağlamaktadır. Aşağıdaki bölümde, WAN bağlantı riskleri, tehditler ve zafiyetler ve risk azaltma stratejileri sunulmaktadır.

WAN Etki Alanında (Bağlantı) Yaygın olarak Bulunan Riskler, Tehditler ve Zafiyetler

Telekomünikasyon şirketleri müşteri IP trafiğini hazırlamak ve aktarmaktan sorumludurlar. Bazen bu IP trafiği, kuruluş çapında paylaşılan genişbant erişimi sağlayan özel internet erişimi ile birlikte gelmektedir. Eğer, kuruluşlar WAN altyapılarını dış kaynaktan temin ediyorsa, yönetim ve güvenlik, bu dış kaynak servis sağlayıcısını da kapsayacak şekilde genişletilmelidir. Kuruluşlar güvenlik politikalarını ve ihtiyaçlarını, kendi güvenlik sağlayıcısının gereğini yapması için tanımlamalıdır. **TABLO 1-7**, WAN Etki Alanı içinde bulunan bağlantı ile ilişkili riskleri, tehditleri, zafiyetleri ve uygun risk azaltma stratejilerini listelemektedir.

TABLO 1-6 WAN Etki Alanı (Internet) için riskler, tehditler, zafiyetler ve azaltma planları

RİSK, TEHDİT, VEYA ZAFİYET	AZALTMA
Açık, kamusal alanda, bağlanmak isteyen herkes tarafından kolayca erişilebilmektedir	Kabul edilebilir kullanım politikaları "RFC 1087: Etik ve İnternet *(Ethics and the Internet)*" belgesine uygun olarak uygulanmalıdır. Sistemlere yetkisiz erişim, BT altyapılarına yönelik kötü niyetli saldırılar ve kötü niyetli kesintilerden kaynaklanan maddi kayıplarla ilgili yeni yasalar için öncülük edilmelidir.
İnternet trafiğinin çoğu açık metin olarak gönderilmektedir	Şifreleme ve VPN tünelleri olmadan özel iletişim için İnterneti kullanımı yasaklanmalıdır. Veri sınıflandırma standardınız varsa, politikalar, prosedürler ve yönergeler hassasiyetle uygulanmalıdır.
Gizli dinlemeye (eavesdropping) karşı zayıf	Uçtan uca güvenli IP iletişim için şifreleme ve VPN tünelleri kullanılmalıdır. Veri sınıflandırma standardınız varsa, politikalar, prosedürler ve yönergeler izlenmelidir.
Kötücül saldırılara karşı zayıf	Katmanlı LAN-dan-WAN-a güvenlik önlemleri, IP durum denetlemeli güvenlik duvarlarıyla DMZ, güvenlik izlemesi için IDS/IPS ve bilinmeyen e-posta dosya ekleri için karantina devreye alınmalıdır.
DoS, DDoS, TCP SYN taşkını, ve IP adres yanıltması *(spoofing)* saldırılarına karşı zayıf	TCP SYN "açık bağlantılar" ve ICMP (yankı isteği) ping paketlerini engellemek için dış IP durum bilgisi tutan güvenlik duvarlarına ve IP yönlendirici WAN arabirimlerine filtreler uygulanmalıdır. İnternet servis sağlayıcınızı *(Internet Service Provider* - ISP) IP yönlendirici WAN arayüzlerine CERT Advisory CA-1996-21 uyarınca uygun filtreleri yerleştirmesi konusunda uyarmalısınız. Bu; *www.cert.org/advisories/CA-1996-21.html* adresinde bulunabilir.
Bilgi ve verilerin bozulmasına karşı zayıf	VPN'lerle IP veri iletimleri şifrelenmelidir. Test edilmiş kurtarma prosedürleri ile veriler yedeklenmeli ve veriler şirket dışında konumlanmış veri kasalarına kaydedilmelidir (çevrimiçi veya fiziksel veri yedekleme).
Doğası gereği güvenli olmayan TCP/IP uygulamaları (HTTP, FTP, TFTP, vb.)	Verilerin düzgün bir şekilde taşınması ve TCP/IP uygulamalarının kullanılması için veri sınıflandırma standardınıza bakmalısınız. Doğru şifreleme olmadan TCP/IP uygulamaları hiçbir zaman gizli veriler için kullanılmamalıdır. Bir ağ yönetimi VLAN'ı oluşturulmalı ve ağ yönetimi için kullanılan TFTP ve SNMP trafiği normal trafikten ayırılmalıdır.
Bilgisayar korsanları, saldırganlar ve suçluların **Truva atları *(trojans)*, solucanlar *(worms)***, ve kötücül yazılım e-postaları	LAN-dan-WAN-a Etki Alanındaki tüm e-posta ekleri tür, virüs ve kötü amaçlı yazılımlar için taranmalıdır. Daha fazla güvenlik incelemesi yapılıncaya kadar bilinmeyen dosya ekleri ayrılmalı ve karantinaya alınmalıdır. Çalışanlara bilinmeyen taraflardan gelen gömülü URL bağlantıları ve e-posta ekleri gibi tehlikeler hatırlatılmalı, bağlantıları tıklarken ve dosyalar açarken dikkat etmelerini sağlamak için güvenlik bilinci eğitimi verilmelidir.

Uzaktan Erişim Etki Alanı

Uzaktan Erişim Etki Alanı *(Remote Access Domain)*, uzak kullanıcıları kuruluşun BT altyapısına bağlamaktadır. Uzaktan erişim, sahada veya evde çalışan personel (örneğin, dış satış temsilcileri, teknik destek uzmanları veya sağlık uzmanları) için kritik önem taşımaktadır. Küresel erişim, internete, e-postaya ve diğer iş uygulamalarına, **Kablosuz Bağlantı (*Wireless Fidelity*, Wi-Fi)** erişim noktası bulabileceğiniz herhangi bir yerden bağlanmayı

TABLO 1-7 WAN Etki Alanı (Bağlantılı) için Riskler, Tehditler, Zafiyetler ve Azaltma Planları

RİSK, TEHDİT, VEYA ZAFİYET	AZALTMA
Aynı servis sağlayıcı yönlendiricisi ve altyapısı üzerinde WAN IP trafiğinin akması	Gizli veri aktarımları, VPN tünellerini kullanan servis sağlayıcı WAN üzerinden şifrelenmelidir.
Yüksek WAN servis kullanılabilirliğini korumak	WAN hizmet kullanılabilirliği SLA'ları edinilmelidir. Yüzde 100 kullanılabilirlik gerekliyse, yedek İnternet ve WAN bağlantıları uygulamaya koyulmalıdır.
WAN performansını ve verimliliğini en üst düzeye çıkarma	Uzak sistemlere, uygulamalara ve verilere erişirken WAN optimizasyon ve veri sıkıştırma çözümleri kullanılmalıdır. Güvenlik politikaları ile uyumlu bir şekilde, giden yönlendirici WAN arayüzlerinde erişim kontrol listeleri (*access control lists* - ACL'ler) etkinleştirilmelidir.
SNMP ağ yönetimi uygulamaları ve protokollerinin (ICMP, Telnet, SNMP, DNS, vb.) kötü amaçlı kullanımı	Ayrı WAN ağ yönetimi VLAN'ları oluşturulmalıdır. SNMP yönetici ve yönlendirici IP adreslerinin LAN-dan-WAN-a Etki Alanı üzerinden geçişine izin veren katı güvenlik duvarı ACL'leri kullanılmalıdır.
24 x 7 x 365 SNMP alarmları ve güvenlik izleme	Güvenlik otperasyonları ve izleme dışardan hizmet olarak alınmalıdır. Servisler, yönetilen güvenlik dahil edilecek şekilde genişletilmelidir.

kolaylaştırmaktadır. Uzaktan Erişim Etki Alanının olması gereklidir ancak kullanımı tehlikelidir. Uzaktan Erişim Etki Alanı, internetten birçok risk ve tehdit getirmektedir.

Bugünün mobil çalışanı aşağıdakilere gereksinim duymaktadır:

- **Kesintisiz cep telefonu hizmeti** - Mobil çalışanlar, ofis ve destek ekipleriyle irtibat kurmak için cep telefonu servisine ihtiyaç duymaktadır.
- **Kritik iletişimler için gerçek zamanlı erişim** - Cep telefonlarında metin mesajlaşma veya **anlık mesajlaşma** (***instant messaging*** - **IM**) **sohbetinin** kullanımı kısa sorulara hızlı yanıtlar sağlamakta ve kullanıcıların o anda yaptıkları işi tamamen kesmesini gerektirmemektedir.
- **Bir mobil cihazdan e-postaya erişim** - E-postaların cep telefonları, akıllı telefonlar, tabletler, PDA'lar veya **BlackBerry** cihazlarıyla entegrasyonu, kullanıcılara önemli e-posta mesajlarına hızlı bir şekilde yanıt verme olanağı sunmaktadır.
- **Geniş bant Wi-Fi İnternet erişimi** - Bazı ülke çapında servis sağlayıcılar günümüzde Wi-Fi genişbant erişim kartları sunmaktadır. Büyük metropol alanlarında kablosuz erişim imkanına izin vermektedirler.
- **Yerel Wi-Fi bağlantı noktası (*hotspot*)** - Wi-Fi bağlantı noktaları havaalanları, kütüphaneler, kafeler ve perakendeciler dahil olmak üzere çok sayıda bulunmaktadır. Çoğu ücretsizdir, ancak bazıları kullanıcıların erişim için ödeme yapmasını gerektirmektedir.
- **Ev ofisine geniş bant İnternet erişimi** - Evden çalışan personel geniş bant internet erişimine ihtiyaç duymaktadır. Bu servis genellikle VoIP telefon ve dijital TV hizmetleri ile birlikte verilmektedir.
- **Bir şirketin BT altyapısına güvenli uzaktan erişim** - Uzaktan çalışanlar, tüm IP veri aktarımlarını halka açık internet üzerinden şifrelemek için güvenli VPN tünellerine ihtiyaç duymaktadırlar. Bu durum, eğer özel verilere uzaktan erişilecekse kritik bir önem taşımaktadır.

Bu etki alanının kapsamı, internet ve IP iletişim yoluyla uzaktan erişimle sınırlıdır. Uzaktan Erişim Etki Alanının mantıksal yapılandırması, IP ağ mühendisliği ve VPN çözümleri

gerektirmektedir. Bu bölüm birçok uzaktan kullanıcı için önemli olan bireysel uzaktan erişime ve büyük ölçekli uzaktan erişime yöneliktir. Uzaktan Erişim Etki Alanı, tipik bir BT altyapısı için altıncı savunma katmanını temsil etmektedir.

Uzaktan Erişim Etki Alanı için Roller, Sorumluluklar, ve İzlenebilirlik

Burada Uzaktan Erişim Alanında ne olması gerektiği konusunda genel bir bakış sunulmaktadır:

- **Roller ve görevler**—Uzaktan Erişim Etki Alanı, mobil kullanıcıları halka açık internet yoluyla BT sistemlerine bağlamaktadır. Mobil kullanıcının internete bağlanabilecek nitelikte bir uzaktan erişim IP cihazı olmalıdır. Dizüstü bilgisayarlara ilave olarak, mobil kullanıcılar akıllı telefonlar, tabletler, ve elde taşınır bilgisayarlar olarak PDA'lar kullanabilmektedirler. Bu cihazlarda bulunan mobil yazılım, telefon görüşmeleri, sesli posta, e-posta, metin mesajlaşma, ve uzaktan web taramasını mümkün kılmaktadır.

Uzaktan Erişim Etki Alanında gerekli olan roller ve görevler aşağıda listelenen unsurların yönetim ve tasarımını içermektedir:

- **Cep telefonları, akıllı telefonlar, PDA'lar ve BlackBerry üniteleri**—Şirket tarafından verilen cihazlara, tanımlanmış politikalara göre güncel ürün yazılımı, işletim sistemi yazılımı ve yamalar yüklenmelidir. Politika, bu ekipman üzerinde parolaların kullanılmasını gerektirmelidir.
- **Dizüstü VPN istemci yazılımı**—Kuruluşlar, LAN-dan-WAN-a Etki Alanı ve uzak kullanıcı dizüstü bilgisayarları arasında VPN tünellerini kullandığında, o kuruluşların özel gereksinimlerini karşılayan ve o kuruluşun diğer yazılımlarıyla uyumlu çalışan VPN yazılımının seçilmesi gerekmektedir.
- **Güvenli tarayıcı yazılımı**—Güvenli Hiper Metin Aktarım Protokolü (*Hypertext Transfer Protocol* - HTTPS) kullanan web sayfaları güvenli tarayıcılara ihtiyaç duymaktadır. HTTPS, güvenli tarayıcılar ve güvenli web sayfaları arasındaki veri aktarımını şifrelemektedir.

Arka-kapı analog telefon hatları ve modemlerden gelen risk

Bazı bakım firmaları, ekipmanlara ulaşmak için analog telefon hatlarını ve modemleri kullanmaktadırlar. Bu, IP veya SNMP protokollerinin kullanılmaması anlamına gelmektedir. Bu önemli bir kolaylık olmasına rağmen, BT sistemine güvenli olmayan bir arka kapı sağlamaktadır. Saldırganlar, bir analog modem parolasının etrafından dolaşabilen araçlar kullanmaktadırlar. Bir arka kapı analog telefon hattına bağlı bir analog modem ile donatılmış kullanıcı iş istasyonları için dikkatli olunmalıdır. Şirketiniz, BT personelinin ve yazılım geliştiricilerinin bu arka kapıları kurduklarını bilmiyor olabilir. Analog modemler genellikle az güvenlik denetimine sahip oldukları için bu bir risk olabilmektedir.

Aşağıdaki listelenen maddeler bu riskleri ve tehditleri azaltmanın en iyi yollarından bazılarıdır:

- Tek bir analog telefon hattı, özel birim santrali (**private branch exchange** - PBX) veya VoIP telefon sistemi kullanılmadan sisteme sokulmamalıdır.
- Tek bir analog telefon hattının kurulmadığından emin olmak için yerel telefon hizmeti şirketleri ile birlikte çalışılmalıdır.
- Kimliği belirsiz aramaların (diğer bir deyişle, arayanın kimliği ekranda "bilinmeyen" olarak görülen çağrılar) telefon sistemine girmesi engellenmelidir.
- Hatalı telefon numaraları ve anormal çağrı kalıpları için PBX ve VoIP telefon sistemlerinden gelen çağrı detay kaydı (**call-detail record** - CDR) raporları izlenmelidir.

- **VPN yönlendiriciler, VPN güvenlik duvarları veya VPN yoğunlaştırıcılar**—Uzaktan erişim VPN tünelleri, VPN yönlendirici, VPN güvenlik duvarı veya VPN yoğunlaştırıcıda (*concentrator)*, genellikle LAN-dan-WAN-a Etki Alanı içerisinde sona ermektedir. Tüm veriler, VPN istemcisi (uzak dizüstü bilgisayar) ile VPN yönlendiricisi, güvenlik duvarı veya yoğunlaştırıcı arasında şifrelenmektedir - *tünel (tunnel)* adı da buradan gelmektedir.
- **Güvenli Soketler Katmanı (*Secure Sockets Layer* - SSL)/VPN web sunucusu**—SSL güvenli bir web sayfası ile güvenli bir tarayıcı arasında 128-bit şireleme kullanmaktadır. Bu şifrelenmiş VPN tüneli uzak web sayfasının veri paylaşımı için uçtan uca gizlilik sağlamaktadır.
- **Kimlik doğrulama sunucusu (*Authentication server*)**—Uzaktan erişim talep eden kullanıcıları doğrulamak için ikinci seviye kimlik doğrulama gerçekleştiren bir sunucudur.
- **Sorumluluklar**—Genellikle ağ mühendisi veya WAN grubu Uzaktan Erişim Etki Alanından sorumludur. Bu hem donanım bileşenlerini hem de mantıksal elemanları içermektedir. Ağ mühendisleri ve güvenlik uygulamacıları politikalara göre güvenlik kontrollerini hayata geçirmekten sorumludurlar. Bu sorumluluklar, Uzaktan Erişim Etki Alanı için donanım ve mantıksal uzaktan erişim bağlantısının bakımı, güncellenmesi ve sorunlarını gidermeyi içermektedir. Bu sorumluluklar aşağıdakilerin yönetimini gerektirmektedir:
  - IP yönlendiriciler
  - IP durum denetlemeli güvenlik duvarları
  - VPN tünelleri
  - Güvenlik izleme cihazları
  - Kimlik doğrulama sunucuları
- **İzlenebilirlik –** Kuruluşunuzun WAN ağ yöneticisi Uzaktan Erişim Etki Alanından sorumludur. Genellikle, BT güvenlik direktörü Uzaktan Erişim Etki Alanı güvenlik planlarının, standartlarının, yöntemlerinin ve yönergelerinin kullanıldığından emin olmalıdır.

Uzaktan Erişim Etki Alanında Yaygın olarak Bulunan Riskler, Tehditler ve Zafiyetler

Uzaktan erişim tehlikelidir ancak mobil çalışanlar için gereklidir. Bu, satış temsilcileri, danışmanlar ve destek personeli gibi mobil bir iş gücüne dayanan kuruluşlar için geçerlidir. Kuruluşlar maliyetleri düşürdükçe, birçok kuruluş personelini evden çalışmaya teşvik etmektedir. Bu durumda, WAN halka açık internettir. Bu bağlantıları güvenli hale getirmek en öncelikli iştir. Kullanıcıları doğrulamak ve verileri şifrelemek için kuruluşun sıkı veri sınıflandırma standardı kullanılmalıdır.

Uzaktan erişim güvenlik kontrolleri aşağıda listelenen maddeleri kullanmalıdır:

- **Tanımlama (*Identification*)**—Bir kullanıcı adı, oturum açma kimliği veya hesap numarası gibi kimlik bilgilerini verme sürecidir.
- **Kimlik doğrulama (*Authentication*)**—Uzak kullanıcıların, kullanıcının iddia ettiği kişi olduğunu kanıtlayan süreçtir. En yaygın kimlik doğrulama yöntemi, bir parola sağlamaktır. Birçok kuruluş, **belirteç *(token)*** (donanım veya yazılım), biyometrik parmak izi okuyucu veya akıllı kart gibi ikinci seviye doğrulama hizmetleri kullanmaktadır. Bir belirteç, rastgele bir sayı gönderen bir donanım aygıtı veya kullanıcıya bir sayıyı metin olarak mesaj atan bir yazılım belirteci olabilmektedir. Biyometrik parmak izi okuyucu, kullanıcının parmak izi sistemde saklanan parmak iziyle eşleştiğinde erişime izin vermektedir. Akıllı kart, bir belirtece benzer şekilde davranan bir kredi kartına benzemektedir. Akıllı kartın, kullanıcıyı bir akıllı kart okuyucu üzerinden doğrulayan bir mikro işlemci yongası vardır.
- **Yetkilendirme (*Authorization*)**—Belirli bir kullanıcıya, bir kuruluşun BT varlıklarını, sistemlerini, uygulamalarını ve verilerini kullanma haklarını verme sürecidir.

TABLO 1-8 Uzaktan Erişim Etki Alanı için Riskler, Tehditler, Zafiyetler ve Azaltma Planları

RİSK, TEHDİT VEYA ZAFİYET	AZALTMA
Kaba kuvvet (Brute-force) kullanıcı kimliği ve parola saldırıları	Periyodik olarak değiştirme (örneğin, her 30 veya 60 günde) gerektiren kullanıcı kimliği ve parola politikaları oluşturulmalıdır. Giriş şifreleri kullanılmalı, şifreler sekiz karakterden daha uzun olmalı ve şifreler sayı ve harf içermelidir.
Çoklu oturum açma denemeleri ve erişim kontrolü saldırıları	Oturum açma denemeleri girişimi için otomatik engelleme ayarlanmalıdır (örneğin, üç oturum açma girişimi başarısız olduktan sonra kullanıcı erişimi engellenmelidir).
BT sistemlerine, uygulamalara ve verilere yetkisiz uzaktan erişim	Hassas verilere, uygulamalara ve verilere birinci seviye (örneğin, kullanıcı kimliği ve parola) ve ikinci seviye (örneğin, belirteçler, biyometrikler, ve akıllı kartlar) kimlik doğrulama güvenliği uygulanmalıdır.
Özel veri veya gizli verinin uzaktan ifşa edilmesi	Veritabanları veya sabit disklerdeki tüm özel veriler şifrelenmelidir. Veri çalınırsa, veri şifreli olduğu için hırsız onu kullanamaz veya satamaz.
Mevcut veri sınıflama standartlarını ihlal eden veri sızıntısı	Kuruluşun veri sınıflandırma standardına uygun olarak veri sızıntısı güvenlik izleme araçları ve izleme de dahil olmak üzere, LAN-dan-WAN-a Etki Alanında güvenlik önlemleri uygulanmalıdır.
Mobil çalışanın dizüstü bilgisayarının çalınması	Çalışanın özel veya gizli veriye erişimi varsa sabit disk üzerindeki veriler şifrelenmelidir. Kayıp ya da çalınan bir dizüstü bilgisayar, kullanıcısı tarafından bildirildiğinde gerçek zamanlı cihaz kilitleme kuralları uygulanmalıdır.
Mobil çalışanın belirtecinin, diğer kimlik doğrulamasının çalınması	Bir belirteç kaybolursa veya bir kimlik doğrulama aracı tehlikeye düştüyse gerçek zamanlı cihaz kilitleme kuralları uygulanmalıdır.

- **İzlenebilirlik**—Kullanıcı eylemlerini kaydetme işlemidir. Kaydedilen bilgiler çoğunlukla kullanıcıları sistem olayları ile ilişkilendirmek için kullanılmaktadır.

TABLO 1-8, Uzaktan Erişim Etki Alanı riskleri, tehditleri ve zafiyetleri ile birlikte risk azaltma stratejilerini listelemektedir.

Sistem/Uygulama Etki Alanı

Sistem/Uygulama Etki Alanı tüm kritik önem taşıyan sistemleri, uygulamaları ve verileri tutmaktadır. Yetkili kullanıcılar bu etki alanındaki birçok bileşene erişebilmektedir. Güvenli erişim, ikinci seviye kontrolleri gerektirebilmektedir.

İkinci seviye kimlik doğrulamasını gerektirebilecek uygulamalara örnekler aşağıda verilmektedir:

- **İnsan kaynakları ve bordro –** Sadece bordro bölümünde çalışan personelin bu özel verilere ve gizli bilgilere erişmesi gerekmektedir.
- **Muhasebe ve finans –** Üst düzey müdürler, sağlıklı iş kararları vermek için muhasebe ve finansal verilere erişmeye ihtiyaç duymaktadır. Mali verileri güvence altına almak, erişimi sadece veriye erişime gereksinim duyanlar ile sınırlandıran benzersiz güvenlik kontrollerini gerektirmektedir. Halka açık şirketler, güvenlik gerektiren Sarbanes-Oxley (SOX) uyum yasalarına tabidir.
- **Müşteri ilişkileri yönetimi (*Customer relationship management* - CRM) -** Müşteri hizmetleri temsilcileri, müşteri satın alma geçmişi ve kişisel veriler içeren bilgiye gerçek zamanlı olarak erişmek zorundadır.

Teknik İPUCU

Güvenlik kontrolleri, özel verileri ve fikri mülkiyet haklarını korumaktadır. Verileri şifrelemek, sahte kullanıcıları durdurabilmektedir. Veri arayan bilgisayar korsanları, insanların bunları nerede sakladığını ve nasıl bulacaklarını iyi bilmektedir. Verileri veritabanlarında ve depolama aygıtlarında şifrelemek, ek bir güvenlik katmanı sağlamaktadır.

- **Satış siparişi girişi** - Satış uzmanları, satış siparişi girişi ve sipariş izleme sistemine erişmek zorundadırlar. Kişisel müşteri verileri güvenli bir şekilde tutulmalıdır.
- **ABD askeri istihbarat ve taktikleri** - Savaş alanında kararlar alan ABD askeri komutanları son derece hassas bilgiler kullanmaktadırlar. Bu bilgilere erişim ABD Savunma Bakanlığı (DoD) veri sınıflandırma standartlarını karşılamalıdır.

Sistem/Uygulama Etki Alanı, savunmanın yedinci katmanını temsil etmektedir.

Sistem/Uygulama Etki Alanı Rolleri, Sorumluluklar, ve İzlenebilirlik

Bu bölümde Sistem/Uygulama Etki Alanında neler bulunması gerektiği konusuna genel bir bakış sunulmaktadır:

- **Roller ve görevler –** Sistem/Uygulama Etki Alanı, donanım, işletim sistemi yazılımı, uygulamalar ve verilerden oluşmaktadır. Bu etki alanı, donanım ve onun mantıksal tasarımını içermektedir. Bir organizasyonun görev kritik uygulamaları ve fikri mülkiyet varlıkları burada bulunmaktadır. Bu etki alanı fiziksel ve mantıksal olarak güvence altına alınmalıdır.

  Sistem/Uygulama Etki Alanı kapsamını riskleri azaltma konusuna sınırladık. Bunlar arasında aşağıdaki maddeler bulunmaktadır:

  - **Bilgisayar odalarına, veri merkezlerine ve kablo dolaplarına fiziksel erişim**—Personelin güvenli alana girmesine izin vermek için prosedür ayarlanmalıdır.
  - **Sunucu mimarisi**—Sunucu kullanımlarını birleştirmek ve maliyetleri düşürmek için blade sunucular ve rafları kullanan birleşik bir sunucu tasarımı uygulanmalıdır.
  - **Sunucu işletim sistemleri ve çekirdek ortamlar**—Yazılım güncelleştirme ve yamaları yüklenerek işletim sistemi yazılımlarının saldırıya açık olma süresi azaltılmalıdır.
  - **Sanallaştırma sunucuları**—Fiziksel ve mantıksal sanal ortamları ayrı tutulmalı ve katmanlı güvenlik çözümleri buluta genişletilmelidir. Sanallaştırma, bir fiziksel sunucu kullanarak birçok işletim sistemi ve uygulamasının yüklenmesini sağlamaktadır.
  - **Uygulama sunucularının sistem yönetimi**—Kullanıcılar için sürekli sunucu ve sistem yönetimi sağlamaktadır.
  - **Veri sınıflandırma standardı**—Verilerin doğru şekilde işlenmesine ilişkin veri sınıflandırma standartları, prosedürleri ve yönergeleri gözden geçirilmelidir. Taşınırken ve depolanırken özel verilerin güvenliği sağlanmalıdır.
  - **Yazılım geliştirme yaşam döngüsü (*Software development life cycle* - SDLC)**—Yazılım tasarlarken ve geliştirirken güvenli yazılım geliştirme yaşam döngüsü taktikleri uygulanmalıdır.
  - **Test ve kalite güvencesi**—Güvenlik açıklarını ve yazılım zayıflıklarını doldurmak için sağlam yazılım testleri, nüfuz etme *(penetration)* testleri ve kalite güvence yöntemleri uygulanmalıdır.
  - **Depolama, yedekleme ve kurtarma işlemleri**—Veri sınıflandırma standardında belirtilen veri saklama, yedekleme ve kurtarma planları takip edilmelidir.

- **Veri arşivleme ve saklama**—Politikalar, standartlar, prosedürler ve yönergeler dijital depolama ve saklama gereksinimleriyle karşılaştırılmalıdır.
- **İş sürekliliği planı (*Business continuity plan* - BCP)**—Bir iş etki analizi (*business impact analysis* - BIA) çalışması yapılmalıdır ve hangi bilgisayar kullanımlarının iş sürekliliği için kritik olduğuna karar verilmelidir. Her bir sistem için RTO'lar tanımlanmalıdır. İşin devam etmesi için en önemli olan şeylere odaklanan bir BCP hazırlanmalıdır..
- **Felaketten kurtarma planı (*Disaster Recovery Plan* - DRP)** - BCP'ye dayalı bir felaketten kurtarma planı hazırlanmalıdır. Önce en önemli bilgisayar sistemleri için DRP öğeleri başlatılmalıdır. Bir DRP ekibi ve uzak veri merkezi kurulmalıdır.

- **Sorumluluklar**—Sistem/Uygulama Etki Alanı sorumluluğu, sistem ve uygulamalar direktörü ve yazılım geliştirme direktörünün üzerindedir. Bu etki alanı aşağıdaki unsurları içermektedir:
  - Sunucu sistemlerinin yönetimi
  - Veritabanı tasarımı ve yönetimi
  - Sistem ve uygulamalar için erişim haklarının tasarımı
  - Yazılım geliştirme
  - Yazılım geliştirme proje yönetimi
  - Yazılım kodlama
  - Yazılım testi
  - Kalite güvencesi
  - Üretim desteği

- **İzlenebilirlik**—Sistem ve uygulamalar direktörü ve yazılım geliştirme direktörü, kuruluşun üretim sistemlerinden ve kullanımlarından sorumludur. BT müdürü genellikle Sistem/Uygulama Etki Alanı güvenlik politikalarının, standartlarının, prosedürlerinin ve yönerge ilkelerinin uygunluğundan sorumludur.

Sistem/Uygulama Etki Alanında Yaygın olarak Bulunan Riskler, Tehditler, ve Zafiyetler

Sistem/Uygulama Etki Alanı, kuruluşun verisinin adeta bir hazine olduğu yerdir. Bunlar kişisel müşteri verileri, fikri mülkiyet hakları veya ulusal güvenlik bilgileri olabilmektedir. Bunlar, bir BT sistemi içinde saldırganların en çok aradığı bilgilerdir. Bu hazineyi korumak her organizasyonun amacıdır. Veri kaybı, Sistem/Uygulama Etki Alanındaki en büyük tehdittir.

Bir veri sınıflandırma standardıyla, veri türleri benzer gruplar halinde izole edilebilmektedir. Veriler ne kadar önemliyse o kadar derin gizleyip saklamak gerekmektedir. Uzun süre depolanacak verilerin şifrelenmesi değerlendirilmelidir. **TABLO 1-9**, Sistem/Uygulama Etki Alanı için yaygın olan riskler, tehditler ve zafiyetler ile birlikte risk azaltma stratejilerini listelemektedir.

BT Altyapısı Güvenliğindeki En Zayıf Halka

Kullanıcı, güvenlik açısından en zayıf halkadır. Bilgi sistemleri güvenlik uzmanları bile hatalar yapabilmektedir. İnsan hatası, herhangi bir organizasyon için büyük bir risk ve tehdittir. Hiçbir grup, herhangi bir kişinin davranışını tamamen kontrol edememektedir. Bu nedenle, her organizasyon kötü niyetli kullanıcılar, eğitimsiz kullanıcılar ve dikkatsiz kullanıcılar için hazırlıklı olmalıdır.

TABLO 1-9 Sistem/Uygulama Etki Alanı için Riskler, Tehditler, Zafiyetler ve Azaltma Planları

RİSK, TEHDİT VEYA ZAFİYET	AZALTMA
Veri merkezlerine, bilgisayar odalarına ve kablo dolaplarına izinsiz erişim	Tesisleri güvenli hale getirmek için personel ve ziyaretçiler için politikalar, standartlar, prosedürler ve yönergeler uygulanmalıdır.
Bakımların gerçekleştirilmesi için sunucuların kesinti süresi	Sunucuları, depolamayı ve ağ oluşturmayı bir araya getiren bir sistem oluşturulmalıdır.
Sunucu işletim sistemleri yazılım zafiyeti	Sunucu işletim sistemi ortamları için zafiyet penceresi tanımlanmalıdır. Güçlendirilmiş sunucu işletim sistemleri kullanılmalıdır ve bakımları düzenli olarak yapılmalıdır.
Doğası gereği güvenli olmayan bulut hesaplama sanal ortamlar	Ayrı VLAN'larda sanal güvenlik duvarları ve sunucu segmentasyonu uygulanmalıdır. Sanal bir güvenlik duvarı, sanal ortamlarda kullanılan yazılım tabanlı bir güvenlik duvarıdır.
İstemci/sunucu ve web uygulamalarının güvenlik açığı içermeye yatkınlığı	Çalıştırmadan önce sıkı yazılım ve web uygulaması testleri ve penetrasyon testleri yapılmalıdır.
Sistemlere yetkisiz erişim	İkinci seviye kimlik doğrulamanın sıkı kullanımı ile ilgili veri sınıflandırma standartları izlenmelidir.
Bireylerin kişisel verilerinin tehlikeye düştüğü veri ihlalleri	Özel veri öğeleri farklı veritabanlarına ayrılmalıdır. Arşivleme amacıyla, veritabanları ve depolama aygıtlarında yatan hassas veriler şifrelenmelidir.
Verilerin kaybolması veya bozulması	Aylık veri arşivleme için günlük veri yedekleme ve kurum dışı veri depolama yapılmalıdır. Belirlenmiş kurtarma süresi hedeflerine (RTO'lar) uygun veri kurtarma prosedürleri tanımlanmalıdır.
Yedeklenen medyanın yeniden kullanılmasıyla yedeklenen verilerin kaybedilmesi	Uzun süreli depolama için tüm veriler dijital verilere dönüştürülmelidir. Tanımlanmış RTO'lara dayalı olarak yedeklemeler kurum dışı veri kasalarında tutulmalıdır.
Kritik iş fonksiyonlarının kurtarılmasının potansiyel olarak yararlı olamayacak kadar uzun zaman alması	Kritik uygulamalarda işlemlerin devamlılığı (kullanılabilirliği) için taktik adımlar sağlayan bir iş sürekliliği planı geliştirilmelidir.
Felaketten sonra uzunca bir süre BT sistem kesintilerinin sürmesi	Operasyonları sürdürmek için görev, kritik uygulama ve verilerin geri kazanılmasına özgü bir felaketten kurtarma planı geliştirilmelidir.

Aşağıda belirtilen stratejiler, riskin azaltılmasına yardımcı olabilmektedir:

- Her bir iş başvurusunun geçmişi dikkatlice kontrol edilmelidir.
- Her personel için düzenli bir değerlendirme yapılmalıdır.
- Hassas sistemlere, uygulamalara ve verilere erişim farklı personel pozisyonları arasında dönüşümlü yapılmalıdır.
- Sağlam uygulama ve yazılım testleri uygulanmalı ve kalite kontrolü yapılmalıdır.
- Tipik bir BT sisteminin yedi etki alanı boyunca düzenli olarak güvenlik planları gözden geçirilmelidir.
- Yıllık güvenlik kontrol denetimleri yapılmalıdır.

Saygın ve etkili bir meslek oluşturmak için, bilgi sistemleri güvenlik uzmanları etiğe ve mesleki davranış kurallarına uygun hareket etmelidir. Bu bölüm, bu öğretinin neden mesleğin temelini oluşturduğunu açıklamaktadır.

Yorumlar için İstek (Request for Comments/RFC) 1087: Etik ve İnternet

IAB (***Internet Architecture Board – İnternet Mimari Kurulu***) Politika Bildirgesi

İnternet, genel kullanım kolaylığı ve erişilebilirliğinin bir sonucu olan ulusal bir tesistir.
Bu kritik kaynağın sorumsuzca kullanılması, teknik topluluğa hizmet etmeye devamı açısından, muazzam bir tehdit oluşturmaktadır. Bu sistemin ABD hükümet sponsorları, hükümet kaynaklarını akıllıca ve etkin bir biçimde tahsis etmek için kamuoyuna güven verme sorumluluğuna sahiptir. Bu sistemin desteklenme gerekçesi, büyük çaplı yıkıcı ihlallerin ortaya çıkması durumunda zarar görür. İnternete erişim ve kullanım bir ayrıcalıktır ve bu, sistemin tüm kullanıcıları tarafından bu şekilde değerlendirilmelidir.
IAB, Ulusal Bilim Vakfı Ağ Bölümü İletişim Araştırmaları ve Altyapı Bölümü Danışma Paneli'nin ***(Divison Advisory Panel of National Science Foundation Division of Network, Communications Research and Infrastructure)*** görüşlerini kuvvetle desteklemekte olup aşağıdaki faaliyetler kasıtlı olarak yapıldığında, etik olmayan ve kabul edilemez olarak nitelendirmektedir:

(a) İnternet kaynaklarına yetkisiz erişim sağlamaya çalışmak,

(b) İnternet'in amaçlanan kullanımını kesintiye uğratmak,

(c) Bu tür eylemler yoluyla kaynakları (insanlar, kapasite, bilgisayar) israf etmek,

(d) Bilgisayar tabanlı bilgilerin bütünlüğünü yok etmek, ve / veya

(e) Kullanıcıların gizliliğinden ödün vermek.

Etik ve İnternet

Herhangi bir hava trafik kontrolörü olmadığını ve uçakların serbestçe uçtuğunu düşünün. Kalkış ve inişler son derece tehlikeli olacaktır. Muhtemelen çok daha fazla kaza olacaktır. Böyle bir durum ciddi bir karışıklık yaratacaktır.

İnanılması zor fakat, siber uzayda *(cyberspace)* hava trafik kontrolörleri gibi işlev gören bir makam bulunmamaktadır. Daha da kötüsü, çevrim içi insan davranışları çoğu kez normal sosyal ortamlardan daha az olgundur. Siber uzay bugünün kötü adamları için yeni bir oyun alanı haline gelmiştir. Bu nedenle, sistem güvenlik uzmanlarına yönelik olarak talep hızla artmaktadır.

ABD hükümeti ve İnternet Mimari Kurulu (*Internet Architecture Board* - IAB), ABD vatandaşlarına yönelik internet kabul edilebilir kullanımı ile ilgili bir politika belirlemiştir. Bununla birlikte, bu bir yasa ya da bir görev değildir; çünkü siber uzay küresel olup kesin sınırları olmadığından bu politika uygulanabilir değildir. Kullanımı, sağduyu ve kişisel dürüstlüğe dayanmaktadır. Yukarıdaki kutuda verilen açıklama, IAB'nin etik ve internet standartlarını sunmaktadır.

Etik, kişisel dürüstlük meselesidir. Güvenlik mesleği, doğru olanı yapmak ve yanlış olanı durdurmaktır; interneti kullanmak herkesin paylaştığı önemli bir ayrıcalıktır. İnternet, sınırları, kültürel önyargıları olmayan önyargısız bir iletişim aracıdır. Kullanıcıların internete bağlanma hakkı vardır. Bu hak, minnettarlık duyulacak bir şeydir. Ne yazık ki, kötü adamlar suç işlemek ve sorun yaratmak için siber uzayı kullanmaktadır. Bu durum, sistem güvenlik uzmanlarına yönelik küresel bir ihtiyaç yaratmaktadır.

BT Güvenlik Politikası Çerçevesi

Siber uzay, kullanıcıların güvenliği konusunda bazı güvenceler olmaksızın gelişmeye devam edemez. Yasalar, kuruluşların kişisel verilerini mahrem tutmalarını gerektirmektedir. İşletmeler, herhangi birinin, şirket verilerini çalabilecekleri bir internet üzerinde etkin bir şekilde çalışamazlar.

BT güvenliği, herhangi bir kurumun hayatta kalabilmesi için çok önemlidir. Bu bölüm size bir BT güvenlik politikası çerçevesi *(security policy framework)* tanıtmaktadır. Çerçeve, riskleri ve tehditleri azaltacak politikalar, standartlar, prosedürler ve yönergelerden oluşmaktadır.

Tanımlar

Bir BT güvenlik politikası çerçevesi dört temel bileşeni içermektedir:

- **Politika (*Policy*)** - Bir politika, bir kuruluştan sorumlu kişilerin bir dizi eylem veya yön belirlediklerini gösteren kısa bir yazılı ifadedir. Bir politika, üst yönetimden gelir ve kuruluşun tamamı için geçerlidir.
- **Standart (*Standard*)** - Bir standart, donanım, yazılım ve bunların nasıl kullanılacağına ilişkin ayrıntılı bir yazılı tanımdır. Standartlar, BT sistemi boyunca tutarlı güvenlik denetimlerinin kullanılmasını sağlamaktadır.
- **Prosedürler (*Procedures*)** - Bunlar, politikaların ve standartların nasıl kullanılacağıyla ilgili yazılı talimatlardır. Güvenlik kontrolleri için bir eylem planı, kurulum, test ve denetimi içerebilmektedir.
- **Yönergeler (*Guidelines*)** - Bir yönerge, politikayı, standartları veya prosedürleri kullanmak için önerilen bir eylem yoludur. Yönergeler, kullanıma ilişkin olarak spesifik veya esnek olabilmektedir.

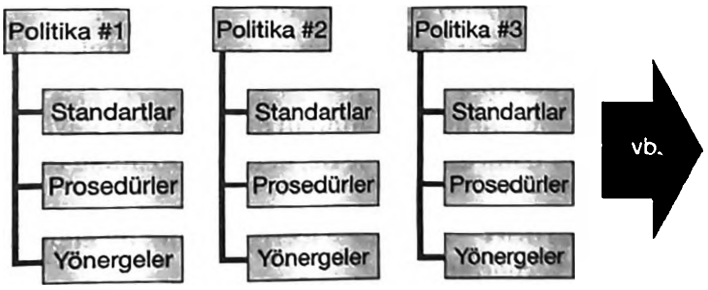
ŞEKİL 1-10, hiyerarşik bir BT güvenlik politikası çerçevesinin bir örneğidir. Politikalar bir kuruluşun tamamı için geçerlidir. Standartlar belirli bir politikaya özeldir. Prosedürler ve yönergeler kullanımın tanımlanmasına yardımcı olmaktadır. Her bir politika ve standart içinde, tipik bir BT altyapısının yedi etki alanının etkisini belirleyiniz. Bu, BT altyapısı boyunca rolleri, sorumlulukları ve izlenebilirliği tanımlamanıza yardımcı olacaktır.

Temel BT Güvenlik Politikaları

Kuruluşunuzun BT güvenlik politikası çerçevesinin odak noktası, riskleri, tehditleri ve zafiyetleri azaltmaktır. Politika tanımını ve standartları pratik tasarım gereksinimleriyle ilişkilendirmek önemlidir. Bu tasarım gereksinimleri en iyi güvenlik kontrollerinin ve önlemlerin düzgün şekilde uygulanmasını sağlayacaktır. Politika bildirimleri *(statements)*, standartlar, prosedürler ve yönergelere atıf yapmanın yanı sıra sınırlar belirlemelidir. Politikalar, yasa ve yönetmeliklere uymak için güvenlik kontrollerinin ve önlemlerinin nasıl kullanılması gerektiğini tanımlamaktadır.

Bazı temel BT güvenlik ilkelerine örnekler aşağıda listelenmektedir:

- **Kabul edilebilir kullanım politikası (*Acceptable use policy* - AUP)** - AUP, kuruluşa ait BT varlıklarının kullanımı ile ilgili olarak izin verilen ve verilmeyen eylemleri tanımlamaktadır. Bu politika Kullanıcı Etki Alanına özgüdür ve bir kuruluş ile çalışanları arasındaki riski azaltmaktadır.



ŞEKİL 1-10
Hiyerarşik BT güvenlik politikası çerçevesi.

Güvenlik Farkındalığı Politikası - Bu politika tüm personelin, kuruluşun güvenlik politikası kapsamında güvenliğin ve davranış beklentilerinin öneminin farkına varmasını nasıl sağlayacağını tanımlamaktadır. Bu politika, Kullanıcı Etki Alanına özgüdür ve kuruluşun güvenlik farkındalık tutumunu değiştirmeniz gerektiğinde devreye girmektedir.

- **Varlık sınıflama politikası** - Bu politika, bir kuruluşun veri sınıflandırma standardını tanımlamaktadır. Hangi BT varlıklarının kuruluşun misyonu için kritik olduğunu söylemektedir. Genellikle kuruluşun sistemlerini, kullanımlarını ve veri önceliklerini tanımlamakta ve tipik bir BT altyapısının yedi etki alanı içerisindeki varlıklarını belirlemektedir.
- **Varlık koruma politikası** - Bu politika, kuruluşların kritik öneme sahip BT sistemleri ve verileri için bir öncelik tanımlamasına yardımcı olmaktadır. Bu politika, bir kuruluşun **işletme etki analizi (*business impact analysis* - BIA)** ile uyumludur ve bir felâket sonrası kuruluşun faaliyetine devam etme kabiliyetini tehdit eden riskleri ele almak için kullanılmaktadır.
- **Varlık yönetim politikası** – Bu politika, güvenlik işlemlerini ve tipik bir BT altyapısının yedi etki alanı içerisindeki tüm BT varlıklarının yönetimini içermektedir.
- **Zafiyet değerlendirme ve yönetimi** - Bu politika, üretim işletim sistemi ve uygulama yazılımı için kuruluş genelinde zafiyet penceresi tanımlamaktadır. Bu politikadan kuruluş genelinde zafiyet değerlendirme ve yönetim standartları, prosedürleri ve yönergeleri geliştirilmektedir.
- **Tehdit değerlendirme ve izleme** - Bu politika, kuruluş çapında bir tehdit değerlendirmesi ve izleme otoritesi tanımlamaktadır. Bu politikanın, LAN-dan-WAN-a Etki Alanı ve AUP uyumluluğu ile ilgili belirli ayrıntıları da içermesi gerekmektedir.

Kuruluşların BT güvenlik politikası çerçevelerini kendi ortamlarına uyarlaması gerekmektedir. Birçok kuruluş, BT kurulumlarının güvenlik değerlendirmesini yaptıktan sonra, politika tanımlarını gördükleri açıklara ve maruz kaldıkları güvenlik tehditlerine göre biçimlendirmektedir. Politikalar genelde kuruluşun üst düzey yönetimi ve hukuk bürosunun incelemesi ve onayını gerektirmektedir.

Veri Sınıflama Standartları

Bir veri sınıflandırma standardının hedefi ve amacı, bir kuruluşun farklı veri türlerini nasıl ele alması ve ne şekilde koruma altına alması gerektiği konusunda tutarlı bir tanım sağlamaktır. Güvenlik denetimleri farklı veri türlerini korumaktadır. Bu güvenlik kontrolleri tipik bir BT altyapısının yedi etki alanı içerisindedir. Prosedürler ve yönergeler, veri güvenliğini sağlamak için tipik bir BT altyapısının yedi etki alanı içerisindeki verilerin nasıl ele alınacağını tanımlamalıdır.

Son uyum yasalarına göre işletmeler ve kuruluşlar için, veri sınıflandırma standartları tipik olarak aşağıdaki ana kategorileri içermektedir:

- **Kişisel veri**—İnsanlar hakkında kişisel olarak tutulması gereken verilerdir. Yasal uyumluluk için kuruluşlar uygun güvenlik kontrolleri kullanmalıdır .
- **Gizli**—Kuruluşa ait bilgi veya verilerdir. Fikri mülkiyet, müşteri listeleri, fiyatlandırma bilgileri ve patentler gizli verilere örnektir.
- **Yalnızca dahili kullanım**—Bir kuruluş tarafından dahili olarak paylaşılan bilgi veya verilerdir. Gizli bilgi ya da veriler dahil edilemese de, iletişim kuruluşu terk etmeye yönelik değildir.
- **Herkese açık etki alanı verileri**—Web sitesi içeriği, teknik incelemeler ve benzerleri gibi halkla paylaşılan bilgi veya verilerdir.

ABD Federal Hükümet Veri Sınıflandırma Standardı

ABD hükümeti, 13526 nolu Başkanlık Emri uyarınca Savunma Bakanlığı (Department of Defense - DoD) da dahil olmak üzere tüm federal devlet kurumları için bir veri sınıflandırma standardı belirlemektedir.

Başkan Barack Obama, bu icra emrini 9 Aralık 2009'da imzalamıştır. ABD hükümeti ve vatandaşları bilginin serbest dolaşımından yararlanmalarına rağmen, bilgi güvenliğinin sağlanması ulusal güvenlik, savunma veya askeri eylem için esastır.

Aşağıda belirtilen noktalar ABD federal hükümet veri sınıflandırma standartlarını tanımlamaktadır:

- **Çok gizli (*Top secret*)** - Sınıflandırma yetkilisinin, açıklanması halinde ulusal güvenliğe ölümcül hasar verebileceğini değerlendirdiği bilgilere uygulanmaktadır.
- **Gizli (*Secret*)** - Sınıflandırma yetkilisinin açıklandığı takdirde ulusal güvenliğe ciddi zarar verebilir olduğunu değerlendirdiği bilgilere uygulanmaktadır.
- **Hizmete özel (*Confidential*)** - Sınıflandırma yetkilisinin açıklandığı takdirde ulusal güvenliğe zarar verebilir olduğunu değerlendirdiği bilgilere uygulanmaktadır.

Kamu alanı bilgisi sınıflandırılmamış sayılırken, veri sınıflandırma standardının bir parçası değildir. ABD hükümeti sınıflandırılmamış (maruz kalınması halinde ulusal güvenliğe tehdit oluşturmayan) ve denetimli sınıflandırılmamış (sadece resmî kullanım için, hassas fakat sınıflandırılmamış ve güvenlik güçleri için hassas) verilerin ele alınmasına ilişkin kurallara sahiptir. Bu kuralların İcra Emri 13562'ye dahil olmadığını ve Başkan George W. Bush'un idaresi tarafından kullanılan daha önceki standartlara dayandığı dikkat alınmalıdır.

Kuruluşunuzun veri sınıflandırma standardına bağlı olarak, en yüksek hassaslık derecesine sahip verileri depolama aygıtlarında ve sabit sürücülerde olsa bile şifrelemek gerekebilmektedir. Örneğin, uzaktan erişim için ortak internet kullanırken şifreleme ve VPN teknolojisi kullanmak gerekebilmektedir. Ancak, dahili LAN iletişimi ve sistemlere, uygulamalara veya verilere dahili erişim, şifreleme kullanmayı gerektirmeyebilir.

Kullanıcıların, müşterilerin kişisel verilerine girmeleri kısıtlanabilmekte ve yalnızca belirli veri parçalarına erişebilmelerine izin verilebilmektedir. Müşteri hizmetleri temsilcileri, bir müşterinin tüm kişisel verilerine erişmeden müşteri hizmeti sağlayabilmektedir. Örneğin, müşterinin Sosyal Güvenlik numarası veya hesap numaralarının bütününü görülmeyebilmekte; yalnızca son dört basamak görünebilmektedir. Hassas veri öğesinin bazı karakterlerini gizleme yöntemi **maskeleme (masking)** olarak adlandırılmaktadır.

Teknik İPUCU

Kuruluşlar BT güvenlik politikası çerçevesini tanımlamaya bir varlık sınıflandırma politikası tanımlayarak başlamalıdır. Bu politika, karşılık olarak, kendini bir veri sınıflandırma standardı ile doğrudan karşılaştırmaktadır. Bu standart bir kuruluşun verilerini güvence altına alma ve koruma biçimini tanımlamaktadır. Veri sınıflandırma standardınızdan yararlanarak, tipik bir BT altyapısının yedi etki alanından herhangi birinde kişisel veya gizli verilerin dolaşıp dolaşmadığının değerlendirilmesi gerekmektedir. Verilerin nasıl sınıflandırıldığına ve kullanıldığına bağlı olarak, BT altyapısı boyunca uygun güvenlik kontrollerinin kullanılması gerekmektedir.

BÖLÜM ÖZETİ

Bu bölümde bilgi sistemleri güvenliği ve sistem güvenliği mesleği tanıtılmıştır. Tipik bir BT altyapısı için ortak bir tanım gördünüz. Yedi etki alanı içindeki riskleri, tehditleri ve zafiyetleri öğrendiniz. Bu etki alanlarının her biri, riskleri, tehditleri ve zafiyetleri azaltmak için stratejilerin kullanılmasını gerektirmektedir. BT güvenlik politikası çerçevelerinin, yetkili politikalar tanımlayarak kuruluşlarda riskin azaltılmasına nasıl yardımcı olabileceğini gördünüz. Ayrıca, veri sınıflandırma standartlarının kuruluşlara farklı veri türlerini işleme yöntemleri için bir yol haritası sunduğunu öğrendiniz. Ancak güvenlik kontrollerini kim uygulayacaktır?

Kalifiye BT güvenlik uzmanları, uygun güvenlik kontrollerini ve önlemlerini tasarlamalı ve uygulamalıdır. Bir BT güvenlik uzmanı olarak, en üst düzey insan bütünlüğü ve ahlakına sahip olmalısınız. Güvenlik profesyonelleri için birkaç profesyonel güvenlik sertifikası bulunmaktadır. CompTIA'nın Security+ mesleki sertifikası giriş seviyesi BT güvenlik profesyonellerine temel oluşturmaktadır. $(ISC)^2$, **Uluslararası Bilgi Sistemleri Güvenlik Sertifikasyon Konsorsiyumu (*International Information Systems Security Certification Consortium*)**, daha tecrübeli profesyoneller için **Sertifikalı Bilgi Sistemleri Güvenlik Profesyoneli CISSP® (*Certified Information Systems Security Professionals CISSP®*)** sertifikası sunmaktadır. CISSP® profesyonel sertifikasyonunu edinmek için gerekli olanlar: Sertifikasyon sınavını geçmek, bilgi sistemi güvenlik alanında en az beş yıllık çalışma tecrübesine sahip olmak, etik kurallara uymak ve sertifikasyonunuzu korumak için sürekli mesleki eğitim (CPE) kredileri göndermektir.

ANAHTAR KAVRAMLAR VE TERİMLER

Acceptable use policy - Kabul Edilebilir Kullanım Politikası (AUP)
Application gateway firewalls - Uygulama ağ geçidi güvenlik duvarları
Availability – Kullanılabilirlik
Biometric – Biyometrik
BlackBerry – BlackBerry
Business continuity plan - İş sürekliliği planı (BCP)
Carrier Sense Multiple Access/Collision Detection – Taşıyıcı Duyarlı Çoklu Erişim/Çarpışma Tespiti (CSMA/CD)
Certified Information Systems Security Professionals - Sertifikalı Bilgi Sistemleri Güvenlik Profesyoneli (CISSP)
Children's Internet Protection Act – Çocukların İnternetten Korunması Kanunu (CIPA)
Ciphertext – Şifreli metin
Cleartext – Açık metin
Confidentiality – Gizlilik
Content filtering – İçerik filtreleme
Cryptography – Kriptografi
Cybersecurity – Siber güvenlik
Cyberspace – Siber uzay
Data breach – Veri ihlali
Data classification standard – Veri sınıflandırma standardı
Defense in depth – Derinlemesine savunma
Demilitarized zone – Arındırılmış bölge (DMZ)
Disaster Recovery Plan – Felaketten Kurtarma Planı (DRP)
Downtime – Aksama süresi
E-commerce – E-ticaret
Encryption – Şifreleme
End-User License Agreement – Son-Kullanıcı Lisans Sözleşmesi (EULA)
Ethernet – Ethernet
Family Educational Rights and Privact Act – Aile Eğitim Hakları ve Mahremiyet Yasası (FERPA)
Federal Information Security Management Act 2002 – Federal Bilgi Güvenliği Yönetim Yasası (FISMA)
Federal Information Security Modernization Act 2014 – Federal Bilgi Güvenliği Modernizasyon Yasası (FISMA)
FICO
File Transfer Protocol – Dosya Aktarım Protokolü (FTP)
Generation Y – Y Kuşağı
Gramm-Leach-Bliley Act – Gramm-Leach-Bliley Yasası (GLBA)
Hardening – Sertleştirme
Health Insurance Portability and Accountability Act – *Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası* (HIPAA)
Hypertext Transfer Protocol – Hiper Metin Aktarım Protokolü (HTTP)
Hypertext Transfer Protocol Secure – Güvenli Hiper Metin Aktarım Protokolü (HTTPS)
Identity theft – Kimlik hırsızlığı
IEEE 802.3 CSMA/CD
Information security – Bilgi güvenliği
Information systems – Bilgi sistemleri
Information systems security – Bilgi sistemleri güvenliği
Instant messaging chat – Anlık mesajlaşma sohbeti (IM)

ANAHTAR KAVRAMLAR VE TERİMLER (*devam ediyor*)

Institute of Electrical and Electronics Engineering – Elektrik ve Elektronik Mühendisleri Enstitüsü (IEEE)
Integrity - Bütünlük
International Information Systems Security Certification Consortium – Uluslararası Bilgi Sistemleri Güvenlik Sertifikasyon Konsorsiyumu $(ISC)^2$
Internet - İnternet
Internet of Things – Nesnelerin İnterneti (IoT)
Intrusion detection system/ *intrusion prevention system* – Saldırı tespit sistemi/sızma önleme sistemi (IDS/IPS)
IP default gateway router – IP varsayılan ağ geçidi yönlendiricisi
IP stateful firewall – IP durum denetlemeli güvenlik duvarı
IT security policy framework – BT güvenlik politikası çerçevesi
Layer 2 switch – Katman 2 anahtar
Layer 3 switch – Katman 3 anahtar
Local area network – Yerel alan ağı (LAN)
Malicious code – Kötücül kod
Malware – Kötücül yazılım
Masking – Maskeleme
Mean time between failures - Arızalar arasındaki ortalama süre (MTBF)
Mean time to failure – Arıza için ortalama süre (MTTF)
Mean time to repair – Onarım için ortalama süre (MTTR)
Multiprotocol Label Switching – Çoklu Protokol Etiket Anahtarlama (MPLS)
Network interface card – Ağ arayüz kartı (NIC)
Network keys – Ağ anahtarları
Network operations center – Ağ operasyon merkezi (NOC)
Personal digital assistant – Kişisel dijital yardımcı (PDA)
Ping - Paket İnternet Yoklayıcısı
Protocol – Protokol
Proxy firewalls – Vekil güvenlik duvarı
Proxy server – Vekil sunucu
Recovery time objective – Kurtarma süresi hedefi (RTO)
"RFC 1087: Ethics and the Internet" – "RFC 1087: Etik ve İnternet"
Risk – Risk
Sarbanes-Oxley Act-Sarbanes-Oxley Kanunu (SOX)
Secure Sockets Layer virtual *private network* – Güvenli Soketler Katmanı Sanal Özel Ağ (SSL-VPN)
Security control – Güvenlik kontrolü
Service level agreement – Servis seviyesi anlaşmalar (SLA)
Simple Network Management *Protocol* – Basit Ağ Yönetimi Protokolü (SNMP)
Smartphone – Akıllı telefon
Software vulnerability – Yazılım zafiyeti/güvenlik açığı
Subnet mask address – Alt ağ maske adresi
Telnet-Telnet
Thick client – Kalın sunucu
Thin client – İnce sunucu
Threat - Tehdit
Token - Belirteç
Transmission Control Protocol/ *Internet Protocol* – İletim Kontrol Protokolü/İnternet Protokolü (TCP/IP)
Trivial File Transfer Protocol – Önemsiz Dosya Aktarım Protokolü (TFTP)
Trojan – Truva atı
Two-step authentication – İki adımlı kimlik denetleme
Unified communications – Birleşik iletişim
Uptime – Çalışma süresi
Virtual LAN – Sanal LAN (VLAN)
Virtual private network – Sanal özel ağ (VPN)
Virus - Virüs
Vulnerability - Zafiyet/Güvenlik Açığı
Vulnerability assessment – Zafiyet değerlendirme
Vulnerability window – Zafiyet penceresi
Wireless access point – Kablosuz erişim noktası (WAP)
Wireless Fidelity – Kablosuz Bağlantı (Wi-Fi)
Wireless LAN – Kablosuz LAN (WLAN)
Workstation – İş istasyonu
World Wide Web-Dünya Çapında Ağ (WWW)
Worm – Solucan

BÖLÜM 1 DEĞERLENDİRME

1. Bilgi güvenliği, bilginin güvence altına alınmasına özeldir; buna karşın bilgi sistemleri güvenliği, bilgiyi barındıran sistemlerin güvenliğine odaklanmaktadır.
   A. Doğru
   B. Yanlış

2. Yazılım üreticileri yazılım satarken sorumluluklarını aşağıdakilerden hangisini kullanarak sınırlandırırlar?
   A. Son Kullanıcı Lisans Sözleşmesi
   B. Gizlilik Sözleşmesi
   C. Yazılım geliştirme sözleşmesi
   D. Hatasız yazılım ve kod geliştirerek sorumluluğu ortadan kaldırmak
   E. Hiçbiri

3. Bilgi sistemleri güvenliğinin ---------- ilkesi kurtarma süresi hedefi ile ilgilenmektedir.
   A. Gizlilik
   B. Bütünlük
   C. Kullanılabilirlik
   D. Hepsi
   E. Hiçbiri

4. Halka açık bir şirket veya ABD federal devlet kurumuysanız, bir veri ihlali olayında bu veri ihlalini kamuoyuna ilan etmeli ve etkilenen kişilere bu veri ihlalini bildirmelisiniz.
   A. Doğru
   B. Yanlış

5. Müşteri hizmetleri temsilcilerinin kişisel müşteri verilerine erişiminin gerekli olduğu kuruluşlar, aşağıdaki güvenlik denetimlerinden hangisini kullanarak müşteri gizliliğini en iyi şekilde koruyabilir ve diğer müşteri verilerine erişmeyi kolaylaştırabilir?
   A. Müşteri hizmetleri temsilcilerinin kişisel müşteri verilerine erişimini engelleyerek
   B. Müşteri kişisel verileri ayrıntılarına erişimi engellemek ve yalnızca Sosyal Güvenlik numaralarının veya hesap numaralarının son dört hanesine erişime izin vermek
   C. Tüm müşteri verilerini şifrelemek
   D. Müşteri veritabanına erişim için iki seviyeli doğrulama kullanmak
   E. Hepsi

6. Bir BT altyapısında en zayıf halka _____ dır.
   A. Sistem/Uygulama Etki Alanı
   B. LAN-WAN Etki Alanı
   C. WAN Etki Alanı
   D. Uzaktan Erişim Etki Alanı
   E. Kullanıcı Etki Alanı

7. Aşağıdaki güvenlik kontrollerinden hangisi kötücül e-posta eklerini azaltmada yardımcı olmaktadır?
   A. E-posta filtreleme ve karantinaya alma
   B. E-posta ekleri anti-virüs taraması
   C. E-posta kaynağının saygın olduğunu kullanıcılarla doğrulama
   D. Bilinmeyen eklere sahip tüm gelen e-postaları tutmak
   E. Hepsi

8. _____ kullanarak gizliliği güvence altına alabilirsiniz.
   A. Kabul edilebilir bir kullanım politikası
   B. Bir veri sınıflandırma standardı
   C. Bir BT güvenlik politikası çerçevesi
   D. Uzaktan erişim için bir sanal özel ağ
   E. Güvenli erişim kontrolleri

9. Gizli bilgileri bir e-posta iletisinde herkese açık internet aracılığıyla gönderiyorsanız, e-posta iletişimini şifrelemek gerekmektedir.
   A. Doğru
   B. Yanlış

10. Güvenlik politikalarını, standartları, prosedürleri ve yönergeleri kullanmak, kuruluşların riskleri ve tehditleri azaltmasına yardımcı olmaktadır.
   A. Doğru
   B. Yanlış

11. Bir veri sınıflandırma standardı genellikle hangi politika tanımının bir parçasıdır?
   A. Varlık koruma politikası
   B. Kabul edilebilir kullanım politikası
   C. Güvenlik açığı değerlendirme ve yönetim politikası
   D. Güvenlik farkındalığı politikası
   E. Tehdit değerlendirme ve izleme politikası

12. Bir veri ihlali genellikle aşağıdakilerin hangisinden sonra gerçekleşmektedir?
   A. Sistemlere ve uygulamalara yetkisiz erişim sağlanması
   B. Güvenlik açığı değerlendirme taraması
   C. Konfigürasyon değişikliği talebi
   D. Yeni bir veri merkezinin hayata geçirilmesi
   E. Bir web uygulama güncellemesinin yapılması

13. Kullanılabilirliğin maksimize edilmesi esas olarak _____ minimize edilmesi ile ilişkilidir.
   A. Bir felaket sonrası kurtarma sırasında gerçekleşen hizmet dışı kalma süresi
   B. Bir sistem veya uygulamayı onarma için geçen ortalama süre
   C. Bir iş süreklilik planını hayata geçirirken oluşan hizmet dışı kalma süresi
   D. Kurtarma süresi hedefi
   E. Hepsi

14. Aşağıdakilerden hangisi bir ABD uygunluk yasası veya eylemi değildir?
   A. CIPA
   B. FERPA
   C. FISMA
   D. PCI DSS
   E. HIPAA

15. İnternet IP paketleri ile açık metin arasındaki ilişkinin benzeri şifrelenmiş IP paketleri ile _____ arasındadır.
   A. Gizlilik
   B. Şifreli metin
   C. Sanal özel ağlar
   D. Kriptografi algoritmaları
   E. Hiçbiri

BÖLÜM

2

Nesnelerin İnterneti Yaşantımızı Değiştiriyor

Nesnelerin İnterneti (***Internet of Things*** - IoT), bağlanabilirlik ve iletişim konuları için günümüzün yeni trend konusudur. Bu yeni trend, sosyal, hukukî, kişisel mahremiyet ve güvenlik açısından birçok problem ortaya çıkarmaktadır. İnternet bizlere ilk olarak küresel bağlantı kazandırmıştır. Bu bağlantı; kişiler ve işletmeler arası iletişimde köklü değişimlere neden olmuştur. Günümüzde, internet kullanıcıları "her zaman online ***(always-online)***" ve her zaman internete bağlıdırlar (örneğin, ***hiper bağlıdırlar(hyper-connected)***). **Sosyal medya** gerçek zamanlı erişim ve iletişimin ana aracısı konumundadır. Facebook®, Twitter®, LinkedIn®, Pinterest®, Google+®, Instagram® vb. servis ve uygulamalar insanların iletişim şeklini değiştirmişlerdir.

Günümüzde internet teknolojisi kişi ve işletmeler arası her tür iletişim için ara katmanlar sunmaktadır, bunlardan bazıları aşağıda listelenmektedir:

- **VoIP—** Kişiler arası gerçek zamanlı ses iletişimi.
- **IM chat —** Gerçek zamanlı sohbet programları için anlık mesaj.
- **Sesli konferans —** Birden fazla kişi arasında gerçek zamanlı telekonferans görüşmeleri.
- **Video konferans—** Birden fazla kişi arasında gerçek zamanlı, 2 yönlü (ses ve görüntü) görüşmeler.
- **İş birliği —** Birden fazla kişi arasındaki sesli konferans ve video konferanslar esnasında gerçek zamanlı belge paylaşımı ve düzenlenmesi.
- **Dijital medya —** Sosyal medyaya yüklenen ve paylaşılan ses kayıtları, resimler ve videolar.

İnternet, insanların işletmelerin iletişim şeklini değiştirmiştir. IoT teknolojisinin gelişmesinin sonucunda milyarlarca cihaz internete bağlanmaya çalışmaktadır. Bunda en büyük etken, neredeyse gerçek zamanlı olarak internete erişmenin önemli görüldüğü nesnelerin (örneğin, tüketim malları, ev eşyaları, arabalar, kamyonetler, trafik ışıkları, bina ve tesis sensörleri, kritik altyapı cihazı vb.) çokluğudur.

IoT avantajları ve dezavantajlarıyla birlikte gelmektedir. IoT yaşantımızı, çalışmamızı ve tüm eylemelerimizi köklü bir şekilde değiştirmektedir. Örneğin, restoranları telefonla arayıp rezervasyon yaptığınız günleri hatırlıyor musunuz? Şimdilerde ise kolaylıkla e-mail göndererek rezervasyon yaptırılabilmektedir. Aile tatiliniz için tatil acentasıyla buluşma ayarladığınız günleri hatırlıyor musunuz? Şimdilerde ise internet üzerinden, online olarak, ve de daha önce aynı tatili yapmış ailelerin değerlendirmelerini okuyarak, kolaylıkla kendi tatilinizi araştırıp satın alabilmektesiniz. İş görüşmeleri ve toplantıları için seyahat etmek zorunda olduğunuz günleri hatırlıyor musunuz? Şimdilerde ise ses ve video konferansları aracılığıyla görüşebilmekte, iş birliği uygulamaları ile belge paylaşımı ve düzenlemesi yapabilmektesiniz. Bu gibi değişimler işletmelerin para ve zamandan tasarruf etmelerini sağlamaktadır.

IoT'nin üstesinden gelmesi gereken beş kritik problem vardır:

- **Güvenlik (*Security*):** İnternet şu anki hali ile bile birçok kötü niyetli kişiler ve buna karşın oldukça az yasal uygulamalar nedeniyle Vahşi Batı'ya dönüşmüş durumdadır. Bununla birlikte, IoT milyarlarca nesneyi daha internete bağlayacaktır.
- **Mahremiyet (*Privacy*):** Bunlar kimin verileri? Üretilen verilerin, bilgilerin, medyaların fikri haklarını kim elinde bulunduruyor? Mahremiyet politikası bildirimi nedir ve ne için önemlidir?
- **Bilikte çalışabilirlik (*Interoperability*):** IoT'ye bağlı milyarlarca cihazın iletişim kurabilmesine ve birlikte çalışabilmesine olanak sağlayacak protokolleri nasıl tanımlayacağız?
- **Yasal ve Mevzuat Uyumluluk (*Legal and regulatory compliance*):** IoT yasal ve mevzuat uyumluluk konuları her zaman IoT uygulamaları kadar hızlı gelişmemektedir.
- **Ortaya çıkan sosyal ve ekonomik sorunlar:** Ülkelerin ve insanların IoT'nin getirdiği politik, çevresel ve ekonomik problemleri ve bu problemlerin nasıl üstesinden gelinilebileceğini öğrenmesi gerekmektedir.

2. Bölüm Konular

Bu bölüm aşağıda verilen konuları ve kavramları içermektedir:

- Nesnelerin İnterneti (IoT) 1990'lardan günümüze nasıl gelişmiştir
- İnternet, işletme ve insanlar arası iletişimi nasıl TCP/IP dünyasına taşımıştır
- IoT'nin insanlar, işletmeler ve yaşantılarımız üzerinde etkileri neler olacaktır
- İşletmeler, fiziksel yapılardan e-ticaret'e, IoT'ye doğru nasıl gelişmiştir
- Neden günümüz işletmeleri İnternet ve IoT pazarlama stratejisine ihtiyaç duymaktadır
- Mobil IP, IoT dünyasının sürdürülmesine nasıl katkı vermektedir
- IoT'nin yarattığı temel konular nelerdir

2. Bölüm Hedefler

Bu bölümü tamamladığınız zaman, yapabilecekleriniz:

- Nesnelerin İnterneti (IoT)'nin 1990'lardan günümüze nasıl geliştiğini açıklamak
- İnternet ve IoT'nin iş dünyası ve insanlar üzerindeki etkisini bilmek
- Fiziksel yapıdaki işletmelerin e-ticaret ve IoT stratejisini kullanarak e-işletme modellerine nasıl dönüştüğünü anlamak
- Mobil IP'in IoT'nin hem kişisel hem de işletme ortamlarını içerecek şekilde nasıl katkı verdiğini açıklamak
- IoT'nin ortaya çıkardığı yeni zorlukları listelemek

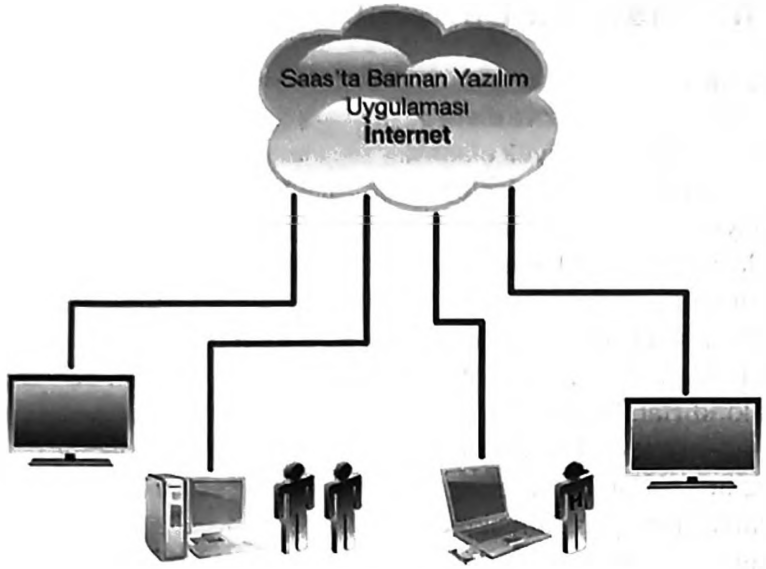
Nesnelerin İnterneti'nin Gelişimi

İnternetin hızlı gelişimi ve evrimi, fiber omurgasına sahip ağların ülke çapında yayılmasıyla mümkün olmuştur. Daha hızlı bağlantılar ve daha büyük bant genişlikleri insanların diğer nesneler ile etkileşime geçebilmesi için daha büyük olanaklar meydana getirmektedir. Mobil kullanıcıya kadar genişleyen yüksek hızlı ağlar sonsuz olanaklar yaratmaktadır. Ülke çapında hücresel ve kablosuz İnternet Servis Sağlayıcıları (*Internet Service Provider* - ISP) sayesinde günümüzde tüketiciler ve işletme kullanıcıları geniş bant bağlantıdan faydalanmaktadırlar. 1990'ların sonlarına doğru gelişen fiber optik altyapı sayesinde, ISP'ler Amerika Birleşik Devletler'i genelindeki hücresel ağlara bağlanarak etki alanlarını genişletmişlerdir. Bu durum da internete bağlanan telefon ve tablet gibi mobil uç noktaların sayısını arttırmıştır. İnsanlar, işletmeler ve onların araçları şu anda internete bağlanmaktadırlar. Ebeveynler kreşlerdeki veya oturma odasındaki çocuklarını güvenli kameralar ile takip edebilmektedir. İşletmeler işlemlerini güvenli bir şekilde internet aracılığıyla yürütmektedir. Satış otomatları kendilerine entegre olan hücresel telefon ağları sayesinde güvenli bir biçimde kredi kartı işlemi yapabilmektedir. Akıllı telefonların veya tabletlerin hücresel veya kablosuz olarak internete bağlı olanları da güvenli kredi kartı işlemleri yapan yazılımları çalıştırabilmektedir. Mobil ödemeler için kredi kartı ödemeleri de mevcut durumdadır. Bölgesel sağlık hizmetleri tele-tıp, güvenli video konferans ve iş paylaşımı kullanarak sağlanabilmektedir. İnternete bağlanabilen her cihaza sahibi tarafından erişim sağlanabilmektedir.

Nesnelerin İnterneti (*Internet of Things* – IoT) terimi ilk olarak 1999'da kullanılmıştır. Kevin Ashton, İngiliz teknoloji tahmincisi, bu terimi internete bağlanabilen her türlü objeyi tarif etmek için kullanmıştır. Ashton'a göre IoT, fiziksel dünya içerisindeki nesnelerin internete bağlanmasını ve sahibinin yetkisi dahilinde herhangi bir şeyden herhangi bir şeye bağlanabilirliği ifade etmektedir. Aynı zamanda, **radyo frekansı ile tanımlama (*radio frequency identification* - RFID)** teknolojisi tedarik zinciri yönetimi işleminde ürünlerin hareketlerini ve teslimatlarını takip etmek için geliştirilmiştir. Günümüzde, IoT terimi çeşitli nesnelerin, sensörlerin, araçların ve gündelik eşyaların birbirlerine nasıl bağlandıklarını ve erişilebilir olduklarını tanımlamak için kullanılmaktadır. IP kullanabilecek cihazları internete bağlama fikri yeni bir fikir olmamasına karşın, IoT ile yapılabilecekler hakkındaki vizyon hız kazanmaktadır. IoT uygulamalarının hızı yavaşlamamakta, aksine hızlanarak artmaktadır. Bu durum da yukarıda açıklanan problemleri yaratmaktadır.

Teknoloji ve pazar eğilimlerinin temeli IoT ile atılmıştır ve IoT'nin gelişim yönüne doğru devam etmektedir. Bu sistemdeki en temel sorun; cihaz geliştirmenin ve cihazların bağlanabilirliklerini arttırmanın her zaman güvenlik, mahremiyet ve mevzuata uygunluk gibi önemli ilkelerin önünde görülmesidir. IP'ye bağlı bu cihazları nasıl koruyacağız? Bütün cihazların internete bağlanması gerçekten iyi bir fikir midir? IoT'yi güçlendirici teknoloji ve pazar trendleri aşağıda listelenmektedir:

- **IP-temelli ağ iletişimi küresel olarak uygulanmaktadır**—İnternet herhangi bir kullanıcıya, işletmeye veya cihaza küresel bir bağlanabilirlik kazandırmıştır.
- **Bağlanabilirlik her yerdedir**—Geniş bant internet bağlanabilirliği küresel olarak şehirlerde birçok halka açık yerde ve müşterilere (barlar, restoranlar vb.) bir fayda olarak ücretsiz bir şekilde sağlanmaktadır.
- **Daha küçük ve daha hızlı hesaplama**—Daha küçük yarı iletkenler ve daha hızlı çipler daha hızlı hesaplama ve daha küçük boyutlu cihazların oluşması ile sonuçlanmıştır.
- **Bulut hesaplama büyümektedir**—Bulut servisleri veriye ve içeriğe daha hızlı ve kolay erişim imkanı sunmaktadır.



ŞEKİL 2-1
Hizmet olarak Yazılım (Software as a Service - SaaS) uygulama dağıtım modeli

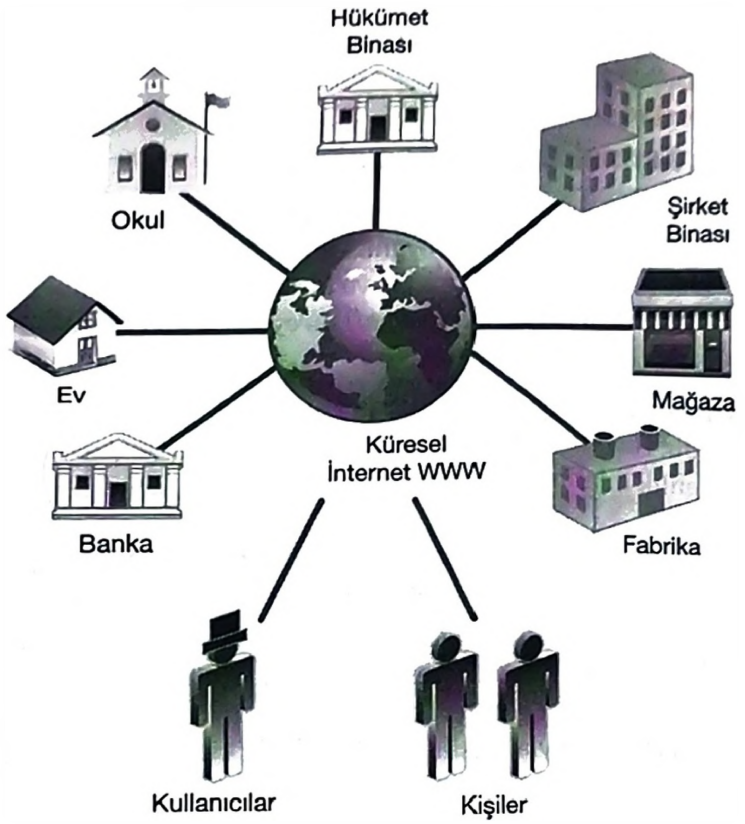
- **Veri analizi gelişmeye katkı sunmaktadır**—İnternet verisi analizi üzerinden cihazların internete nasıl, ne zaman ve neden bağlandıklarının ve iletişime geçtiklerinin analizinin servis ve performans artımı için yakalanması ve çalışılmasıdır.

IoT nesnelerin bağlanması için bir yol sağlamaktadır. Bu bağlanabilirlik hem kişisel hem de ticari hayatı kapsamaktadır. IoT uygulamaları güvenli bulut altyapılarında geliştirilmekte ve depolanmaktadır. Bu, internet sayesinde bire çok *(one-to-many)* teslimat modelini desteklemektedir. **Uygulama servis sağlayıcıları (*application service providers* - ASP)** bulut altyapısında ve internette barındırılan uygulamalar geliştiren yazılım şirketleridir. Bu modelde kullanıcıların yazılımı satın almasına, dizüstü bilgisayarlarına ve iş istasyonlarına bu yazılımı kurmalarına ihtiyaç yoktur; kullanıcılar bunun yerine bulut üzerinde depolanmış olan uygulamaları güvenli bir web tarayıcı ile kullanmaktadırlar. Bu model, **Hizmet Olarak Yazılım (*Software as a Service* - SaaS)** olarak ifade edilmektedir. ŞEKİL 2-1 SaaS tarafından barındırılan uygulama dağıtım modelini göstermektedir.

Amazon Web Servisleri (*Amazon Web Services* - AWS) gibi bulut barındırma *(hosting)* şirketlerinin gelişimi ile bulut uygulamalarının geliştirilmesi de hızlanmıştır. Hem kişisel hem ticari senaryolar için Nesnelerin İnterneti uygulamaları oluşturulmaya başlamıştır. ASP'lerin SaaS uygulamaları geliştirmeleriyle yeni online e-işletmeler doğmuştur. Fiziksel mağazaya ihtiyaç duyulan günler artık geride kalmıştır. Artık World Wide Web'de internet mağazasına sahip olmak gerekmektedir. Online olarak varlık gösteremeden küresel müşterilere ve tedarikçilere erişmek mümkün değildir. İnternet pazarlaması, World Wide Web'de var olmak, ve **arama motoru optimizasyonunu (*search engine optimization* - SEO)** maksimize etmek günümüz IP-bağlantılı dünyasında çok önemli iş gereksinimleridir.

TCP/IP Dünyasına Dönüşüm

Kişisel ve işletmeler arası iletişimde e-posta nasıl en çok kullanılan iletişim aracı haline gelmiştir? iTunes nasıl bir numaralı online müzik dağıtım sitesi haline gelmiştir? Cep telefonları ve internet, iletişimimizi nasıl etkiledi? Bu değişimler işletmeleri nasıl etkiledi? Cevap, İletim



ŞEKİL 2-2
İnternet ve TCP/IP hayatlarımızı nasıl değiştiriyor.

Kontrol Protokolü/İnternet Protokolü'ne (*Transmission Control Protocol/Internet Protocol* - TCP/IP) geçişin hayatımızı değiştirmiş olmasıdır. İnsanlar, aileler, işletmeler, eğitimciler ve devlet artık eskisinden farklı bir şekilde iletişim kurmaktadır ve neredeyse herkesin internete erişimi vardır. **ŞEKİL 2-2** TCP/IP'nin ve internetin günlük yaşamımızı nasıl değiştirdiğini göstermektedir.

IoT'nin İnsan Hayatına ve Ticari Hayata Etkisi

İnsanlar teknolojiyi kullanmayı ve internete bağlı olmayı tercih etmektedir. Bu seçim günlük yaşantımızı sosyal, kişisel ve ticari olarak değiştirmiştir. İnternet kişisel, sosyal ve ticari yaşamlarımızı etkilemektedir. Her sabah uyandığımızda hava durumunu, haberleri ve sosyal medyayı takip etmek için internete erişimi olan cihazları kullanıyoruz. Ofise gittiğimizde iş e-postalarımızı kontrol ediyor ve cevap veriyoruz. İnternet öncesi -30 yıl önceki "karanlık çağlarda"- insanlar sabit telefon hatlarını kullanmaktan ve analog ekipmanlı televizyonları izlemekten memnunlardı. Bilgiye anlık erişim sağlayabilecek bir World Wide Web yoktu. Haberler televizyonda, radyoda ya da gazetelerdeydi. İnsanlar ile anlık olarak konuşabilmek için sabit telefon hatlarına ihtiyaç duyuluyordu. Çağrı cihazlarının ve ses ve mesaj sistemlerinin geliştirilmesi gerçek zamanlı erişime, bilginin saklanmasına ve iletilmesine olanak sağlamıştır. Sonuç olarak, çağrı cihazlarının yerini cep telefonları aldı ve nerede olurlarsa olsunlar insanların herhangi birine erişebilmeleri olanağı sağlandı.

1990'ların ortasından itibaren internete erişimin ve World Wide Web'in kullanılmasının yaygınlaşması ve çok kolaylaşması ile herkesin hayatını değiştirdi. İnsanlar arası iletişim ve hemen arkasından ticari iletişim de internete taşındı.

İnsanlar Nasıl İletişim Kurmaktan Hoşlanmaktadır?

Sosyal medya bireylerin aileleriyle, arkadaşlarıyla ve iş ortaklarıyla nasıl iletişim kurduğunu belirlemektedir. Sosyal medya paylaşımlarının yaygınlaşması (örneğin, profesyonel bağlantılar için LinkedIn ve kişisel bağlantıları için Facebook) iş ve kişisel çizgi arasındaki ayrımı belirsizleştirmektedir. Günümüzün hiper-bağlı *(hyper-connected)* bireyleri temel olarak iki şekilde iletişim kurmaktadır:

- **Gerçek zamanlı iletişim:** Birisiyle anlık olarak konuşmak gerektiğinde gerçek zamanlı iletişim tercih edilmektedir. Hayati öneme sahip bir acil durum, hisse veya senet alımı gibi finansal işlemler, bir güvenlik ihlaline cevap verilmesi bu iletişim biçimine örnek olarak verilebilmektedir.
- **Sakla ve ilet iletişimler (*Store-and-forward communications*):** Anlık olarak cevap gerekmeyen durumlarda sakla ve ilet iletişimi kullanılabilmektedir. Bu iletişim neredeyse gerçek zamanlı olarak gerçekleşmektedir. Sesli mesajlar ve e-postalar bu iletişim biçimine örnektir. İki türlü iletişimde mesajı daha sonra teslim için saklamaktadır. Sesli mesajlar ses dosyalarına dönüştürülüp e-posta olarak gönderilebilmektedir. Bu durum, tüm mesajların (hem ses hem de e-posta) e-posta yardımıyla erişilebildiği **birleşik mesajlaşmaya (*unified messaging* - UM)** örnektir.

Yaşamlarımızı Etkileyen IoT Uygulamaları

İnsanlar arası iletişimin temelleri oluşturulduktan sonra, IoT uygulamaları için olanaklar bu temelin üstüne oluşturulmuştur. Sonraki bölümde günlük hayatımızı etkileyebilecek genel IoT uygulamaları listelenmektedir:

IoT'nin İnsanlar Üzerindeki Etkisi

- **Sağlık izleme ve güncelleme**—Sensörler insanların yaşamsal istatistiklerini görüntüleyebilmekte ve arka planda çalışan uygulamalara veya mobil uygulamalara bu verileri güvenli bir şekilde gönderebilmektedir. İnsan odaklı yeni IoT uygulamaları insanların performansları hakkında gerçek zamanlıya yakın izleme imkanı sağlayabilmektedirler (örneğin, atletlerin antrenman sırasındaki performanslarını izleme, diyabet hastalarının kan şekeri seviyelerini takip etme veya kolesterol hastaları için yemesi tavsiye edilen menü önerileri sunan bir izleme).
- **Ev güvenliği ve akıllı ev kontrol sistemleri**—Ev sahipleri, ev güvenlik sistemlerine, ev video kamera sistemlerine ve enerji tasarrufu sağlayabilmek için ısıtma ve klima sistemlerinde gerçek zamanlıya yakın olarak erişime sahip olabilmektedir. Ebeveynler evde değilken de çocuklarına göz kulak olabilmektedirler. Evin su, elektrik, gaz ve enerji tüketimlerinin görüntülenmesi masraflardan tasarruf etmek için yardımcı olabilmektedir.
- **Online aile üyeleri takvimleri**—Aileler, ebeveyn/çocuk koordinasyonu gerektiren planları yapmak için bu araçları kullanabilmektedirler. Bu, özellikle okul dönemlerinde çocuklarına şoförlük yapan aileler için hayati bir öneme sahiptir. Aile yemekleri, tatiller ve çocukların ulaşım ihtiyaçları bu şekilde daha verimli olarak koordine edilebilmektedir.

- **Küresel konumlama sistemi (global positioning system - GPS) ile aile üyelerinin takip edilmesi ve izlenmesi:** Çocukları hakkında endişelenen ebeveynler GPS takibi ve izlemesini akıllı telefonlarını ve mobil uygulamaları kullanarak aktif duruma getirebilmektedirler. GPS takip uygulamaları ebeveynlerin gerçek zamanlıya yakın olarak çocuklarının konumlarını bulmalarına olanak sağlamaktadır.
- **Online bankacılık, fatura ödeme, finansal işlemler:** Ev sahipleri online bankacılık uygulamalarını kullanarak kendi hesapları üzerinden tüm fatura ödemelerini otomatik hale getirebilmektedir. Çek yazma, kağıt fatura, posta üzerinden fatura ödemeye artık gerek kalmamaktadır. Günümüzde çoğu işletme, kredi kartı veya elektronik hesap yoluyla güvenli, online e-ödemeleri kabul etmektedir.
- **Ev eşyaları, gıda ve servisler için online e-ticaret alışverişleri:** Ev sahipleri artık online olarak alışveriş yaparak ürünleri mağazalardan almaya veya kapılarına kadar getirtme olanaklarına sahiptirler. Marketler zamanı olmayan ebeveynlerin gıda alışverişi ihtiyaçlarını online olarak karşılamaktadırlar. Tatil alışverişlerinin temel şeklinin online alışverişler olması ile müşterilerin uzun kasa kuyrukları beklemelerine ve stres yapmalarına gerek kalmamıştır. Günümüzde devletin, işletmelerin ve bireylerin dijital dünyaya taşınmalarından dolayı, bireyler internete bağlı oldukları sürece iş ilişkilerini ve işlemlerini evlerinden gerçekleştirebilmektedir. Eve pizza servis etme bile restoranların teslimat tekniklerinin gelişmesine sebep olmuş, böylelikle restoranlar tüm aileye yetebilecek ölçekteki yemekleri sıcak ve yemeye hazır biçimde servis edebilecek noktaya gelmişlerdir.
- **Akıllı bilgisayarlara sahip otomobiller ve "her zaman açık *(always-on)*" Wi-Fi internet erişimi:** Araba alırken bilinmesi gereken özellikler artık yakıt sarfiyatı gibi özelliklerin ötesinde bir şekilde gelişmiş ve birçok ileri özellik ve fonksiyon eklenmiştir:
  - "Her zaman açık" Wi-Fi internet erişimi
  - Ellerin serbest kaldığı *(hands-free)* Bluetooth bağlanırlığı
  - Lojack® araba konumlayıcısı
  - Uzaktan kontak başlatıcı
  - Öndeğerlendirme analizi için, araç servis randevusuna gitmeden önce üreticinin sistemine güvenli bir şekilde yüklenebilecek olan araç sistem kontrol bilgileri.

IoT'nin İşletmeler Üzerindeki Etkisi

Artık IoT'nin günlük yaşantımıza etkisini daha iyi biliyoruz, peki IoT'nin işletmelere etkisi nasıl? IoT işletmelerin ürünlerini ve servislerini nasıl satması ve pazarlaması gerektiğini değiştirmektedir. Daha da önemlisi, işletmeler IoT'nin getirdiği yeni olanaklarla ilgilenmektedirler. ASP'ler internet startup'larının IoT temelli ürün, servis ve çözümler sağlayan yeni dalgasıdır. IoT uygulamalarının ilerlediği yön, son kullanıcılar için akıllı telefonlarından ya da tablet cihazlarından iletişim kurabildikleri bulut temelli uygulamalar ve mobil uygulamalardır. İşletmelerin benimsemeye başladığı bazı IoT uygulamaları aşağıda listelenmektedir:

- **Perakende Satış Mağazaları:** Marketler, bankalar, restoranlar ve üreticiler müşterileri için World Wide Web'e sahip olmalılardır. Online katalog sistemi ve güvenli elektronik ödeme metotlarının mağazadan teslim alma ve kapıya kadar teslimat imkanlarıyla birleşmesiyle, müşteriler internete bağlı akıllı telefonlarından, tabletlerinden ya da bilgisayarlarından her zaman alışveriş yapabilmektedirler.

İnternet Topluluğu (Internet Society)

İnternet Topluluğu (*www.internetsociety.org/who-we-are/mission*) İnternet'in vizyon ve misyon görevlerinde insan odaklı özünü betimlemiştir:

Vizyon Görevi: İnternet herkes içindir.

Misyon Görevi: İnternet'in dünya genelinde tüm insanların faydasına kullanılması için açık geliştirimi, gelişimi ve kullanımı desteklemek.

İnternet Topluluğu bu misyonu gerçekleştirebilmek için:

- İnternet standartlarının, protokollerinin, yönetiminin ve teknik altyapısının açık geliştirimini destekler.
- Özellikle gelişmekte olan ülkelerde, nerede ihtiyaç varsa eğitimi destekler.
- İnternet'in gelişimi için liderliğin ve katılımın önemli olduğu alanlarda profesyonel gelişimi destekler ve topluluk oluşturur.
- İnternet ile ilgili güvenilir bilgiler sağlar.
- İnternet'in teknik, ticari, sosyal, ve diğer konularda gelişimini, geliştirimini ve kullanımını etkileyen konuları tartışmak için forumlar düzenler.
- Kendi kendine yönetimi etkin kılan uluslararası iş birliği, topluluk, ve kültür için bir ortam oluşturulmasını teşvik eder.
- İnternete dünya genelinde tüm insanların yararına pozitif bir araç olarak destekleyecek işbirliği çabaları için bir merkez noktası olarak hizmet eder.
- İnsani, eğitimsel, sosyal ve diğer bağlamlarda stratejik girişimler ve sosyal yardım çabaları için yönetim ve koordinasyon sağlar.

- Ürünlerin ve servislerin teslimat masrafları müşterilerin online alışveriş yapmasıyla beraber oldukça azalmıştır. Bu durum bir paradigma değişimine sebep olmuş, geleneksel fiziksel mağazalar yerine online e-ticaret portallarının geliştirilmesini sağlamıştır. Müşteriler her zaman ve her yerden alışveriş yapabilir hale gelmişlerdir. Self-servise sahip olan portallar, müşterilerinin online alışveriş yaparken artık müşteri temsilcisi ile IM sohbet gerçekleştirmesini desteklemektedir. İşletmeler siparişleri direkt olarak envanter yönetim sistemleriyle ilişkilendirebilmektedirler. Tedarik zinciri işlemleri, verilen gerçek zamanlıya yakın satış sipariş erişimleriyle üretim ve dağıtım işlem akışı boyunca optimize edilebilmektedir.
- **Sanal çalışma ortamı:** Profesyonel hizmet veren işletme ve şirket çalışanları önemli bir toplantı veya sunum olmadığı sürece fiziksel olarak ofise gitmek zorunda değillerdir. Günümüzde IoT iki yönlü video konferans ve iş birliği sistemleri dahil olmak üzere, farklı lokasyonlarda bulunan çalışanlar arasında her türlü iletişim biçimini desteklemektedir. Günümüzün IoT teknolojisi çocuk bakımından sorumlu olan ebeveynlerin evdeyken de üretken olabilmelerini sağlamaktadır. Çalışanlar zamandan tasarruf edebilmekte, ulaşım ve yiyecek masrafını azaltabilmekte, verimi arttırabilmekte ve iş arkadaşlarıyla iş birliği içerisinde efektif bir çalışma sergileyebilmektedirler.
- **Hizmet sektörü/çevresel/altyapı izleme için uzak sensörler:** Elektrik ölçümlerinin, su kullanımının, suyun pH seviyesinin, karbonmonoksit ölçer, ya da gaz sızıntısı sensörlerini izlemek isteyen işletmeler IoT'den yararlanabilmektedirler. Özellikle alarm durumunda ya

da güvenlik ile ilgili alarm belirteçlerinin arttığı durumlarda gerçek zamanlıya yakın sensörlere erişim olduğunu hayal edin. Hizmet sektörü, kritik altyapı sistemlerine veya çevresel sistemlere sahip olan herhangi bir işletme internete bağlı sensörlerden ve ölçer-okuma cihazlarından faydalanabilmektedir. Bu erişim, bireylerin fiziksel olarak ilgili konumu ziyaret etmesi ve ölçer cihazı okuması ihtiyacının yerini almaktadır.

- **Şehir ve kamu servisi trafik izleme uygulamaları:** Akıllı şehirler gerçek zamanlıya yakın trafik durumlarını izleyebilmekte ve raporlayabilmekte ve yoğun saatlerdeki trafik akışı durumlarını gerçek zamanlıya yakın güncelleme yaparak akıllı arabalar tarafından erişilebilen mobil uygulamalara yönlendirebilmektedir.
- **IoT, B2C (İşletmeden müşteriye) servis teslim modelini değiştiriyor:** Şirketler müşterilerine teslimat yapma modellerini internet aracılığıyla değiştirmektedirler. İşletmeden **müşteriye (*business-to-consumer* – B2C)** dönüşümü, ürünlerine ve servislerine ulaşılmasını sağlayan yeni web uygulamaları ve mobil uygulamalar öncülüğünde gerçekleşmektedir. İhtiyacınız ya da istediğiniz ne olursa olsun, işletmeler müşteriye yani size yapmış oldukları paketleme, teslim ve satış işlemlerini nasıl yaptıklarını dönüştürmektedirler. Dijital devrimden önce kaset ya da CD almak için mağazalara gittiğinizi hatırlıyor musunuz? Artık kaset ya da CD mağazası yok! Dijital müzik artık farklı müzik dağıtım siteleri aracılığı ile online olarak dağıtılmaktadır. Eğitim şirketleri, eğitmen tarafından yürütülen kursları videolar, ses kayıtları, ve öğrenci etkileşiminin olduğu eğitimlere dönüştürmektedir. Müşterinin ürünleri açıklamak için yapılan bilgilendirmeler de artık adım adım işlemleri açıklayan YouTube videoları ile yapılmaktadır. Bu tür müşteri deneyimi IoT'nin getirdiği bir dinamikliktir. Bu dinamiklik müşterinin sizin ürününüzü ya da servisinizi kullanması için iyi, hızlı ve daha etkili bir yoldur. YouTube videolarını kullanmanın maliyeti de neredeyse hiç yoktur. Bu eğitimler, müşterinin ürün ile ilgili montaj talimatlarını hızlı ve kolay bir şekilde uygulayarak deneyimini arttırmasını sağlamaktadır. IoT uygulamaları tüm müşteri deneyim ve teklifleri için interneti kullanmaktadır. Bu durum, sık alışveriş yapan müşterilere e-posta ile kupon ve fiyat teşvikleri sunan internet ve sosyal medya pazarlama kampanyalarını içermektedir. Satış ve diğer özel servisler online olarak kayıt olan kayıtlı müşterilere gerçek zamanlıya yakın Kısa Mesaj Servis (*Short Message Service* - SMS) metin mesajları olarak gönderilmektedir.
- **Yeni "Hizmet olarak Her şey (Anything as a Service)" IoT uygulamaları:** Yeni IoT ve mobil uygulamalar geliştirildikçe işletmeler kendilerini işletmenin IoT servisi sunmasına olanak veren **Hizmet olarak Her Şey (*Anything as a Service* - AaaS)** teslimat modeline uyarlamaktadır. Hizmet olarak Her şey, ne yapıyor olursanız olun, bu işin içeriğe ve bilgiye web sitesinden erişilebilecek güvenli bir bulut temelli çözüm haline dönüştürülebileceğini belirtir. Takvimler, sağlık hizmeti hatırlatmaları, kuru temizleme, market alışverişi, bebek bakıcılığı, vergi hazırlama servisleri, ürünlerin ya da servislerin bulunması veya herhangi bir şeyin bulunması artık internet ile yapılabilmektedir. Yeni ürünler ya da servisleri dönüştüren veya bulan işletmeler geleceğin ticari IoT ortamında hizmet olarak IoT teklifini kazanacaklardır.

Fiziksel İşletmelerden E-Ticarete Gelişim

İnternet insanların iletişiminden çok daha fazla şeyi değiştirmiştir. Aynı zamanda, işletmelerde de devrim yaratmıştır. Fiziksel işletmeler artık küresel bir erişime sahiptir. E-ticaret işletmelerin nasıl sattıklarını ve internet de işletmelerin nasıl pazarlama yaptıklarını değiştirmiştir.

E-ticaret nedir? Ürünlerin ve servislerin internet üzerinden satılmasıdır. Online müşteriler ürünleri ve servisleri sağlayıcının internet sitesinden alırlar. Ödeme yapmak için kişisel verileri girip, kredi kartı veya cari hesapları ile işlem yaparlar.

E-ticaret iki tip iş modelini desteklemektedir: **işletmeden müşteriye (*business-to-consumer* - B2C) ve işletmeden işletmeye (*business-to-business* - B2B):**

- **İşletmeden müşteriye (*Business-to-Consumer* - B2C)** - İşletmeler müşterileri için ürün ve servisleri web siteleri üzerinden direkt olarak satabilecekleri online mağazalar yaratmaktadırlar, örneğin *www.amazon.com*.
- **İşletmeden işletmeye (*Business-to-Business* - B2B)** – İşletmeler, özellikle tedarik zinciri alışları ve teslimleri için diğer işletmeler ile satışları yürütebilecekleri online sistemler geliştirmektedirler.

E-ticaret sistemleri ve uygulamaları katı bir **gizlilik, bütünlük, ve kullanılabilirlik (*confidentiality, integrity, availability* - CIA)** güvenlik kontrolleri talep etmektedir. Organizasyonlar bilgilerini internet üzerindeki saldırganlardan korumak için katı güvenlik kontrolleri kullanmalıdırlar. Özellikle kişisel verilerin ve kredi kartı bilgisinin internet üzerinden iletildiği durumlarda bu çok daha önemlidir. Ödeme Kartı Endüstrisi Veri Güvenlik Standardı (***Payment Card Industry Data Security Standard* - PCI DSS)** ile uyumlu olmak için, işletmeler güvenlik değerlendirmeleri yapmalı ve doğru kontrol yöntemlerini kullanarak kredi kartı sahiplerinin bilgilerini korumalıdırlar. İnternet neredeyse bir gecede küresel bir pazarlama alanı yaratmıştır. Kimse böyle bir değişimi ya da bunun etkisini öngörememiştir. İnternet her zaman her yerde olunca, reklam, satış ve pazarlama artık sadece televizyon, radyo, gazeteler, dergiler ve posta ile sınırlandırılmamıştır. Pazarlama, yeni müşteriler bulma, bu müşterileri tutma ve daha iyi ürünler ve servisler sağlamadır. İnternet sunduğu online imkanlar ile bu faaliyetleri mümkün kılmaktadır. İnternet işletme zorluklarını değiştirmiştir. Yeni zorluklar aşağıda listelenmektedir:

- İnternet yoluyla işletmeyi büyütme
- Geleneksel işletme modellerini e-işletmeye çevirme
- Güvenli ve yüksek erişimli web siteleri ve e-ticaret portalları geliştirme
- İnternet erişimli müşteri servis stratejileri geliştirme
- İnternet pazarlama ile yeni müşteriler bulma

Amazon, Dell, Apple, Western Union, eBay, Priceline.com, Domino's Pizza ve UPS gibi firmaların hepsi e-işletme modelleri yaratmışlardır. Bu firmaların herbirisi, internet sitelerini küresel müşterilerine ulaşmak için ana yol olarak görmektedirler. Müşterileri, web sitelerine entegre edilmiş olan müşteri servis sunumu sayesinde ürünleri satın alabilmektedirler. Self-servis bu oyunun adıdır. Birçok online aktivite, örneğin hesap yönetimi, self-servis olarak yapılabilmektedir. VoIP ve IM sohbet kullanarak müşteri servis temsilcilerine gerçek zamanlı erişim, yüksek değerli müşteriler için deneyimin arttırılmasını sağlayabilmektedir.

E-işletme stratejisi nedir? E-işletme stratejisi, işletmelerin fonksiyonlarını ve işlemlerini internet erişimli olarak değiştirmektedir. E-işletme stratejileri internet üzerinden ürünlerin ve servislerin satılmasını ve pazarlanmasını içermektedir. Bir e-işletme stratejisi genel olarak aşağıdaki unsurları içermektedir:

- **E-ticaret Çözümü**—Güvenli bir işlem içerisinde ürünlerin ve servislerin satın alınabilmesi için online katalog ve sistem oluşturulması olabilmektedir.
- **İnternet pazarlama stratejisi**—İnternet pazarlama stratejileri, arama motorunun sonuçları sıralamasına yardım etmek için görmülü üst etiketleri *(embedded meta tags)* ve anahtar kelimeleri içeren arama motoru optimizasyonunu (*search engine optimization* - SEO); pazarın, bilgi web sitelerinden ve tanıtım belgelerinden *(white paper)* müşteri bilgisini istediği müşteri

yaratmayı; reklam ve indirim kuponlarının direkt olarak muhtemel alıcılara e-posta ile iletildiği toplu e-posta gönderimleri (e-mail blasts) ve kullanıcı ilgisine göre direk satışları ve pazarlamayı içeren itici pazarı *(push marketing)* içermektedir.

- **E-müşteri servis teslimat stratejisi**—Bu, self-servis ve online müşteri servisi stratejisidir.

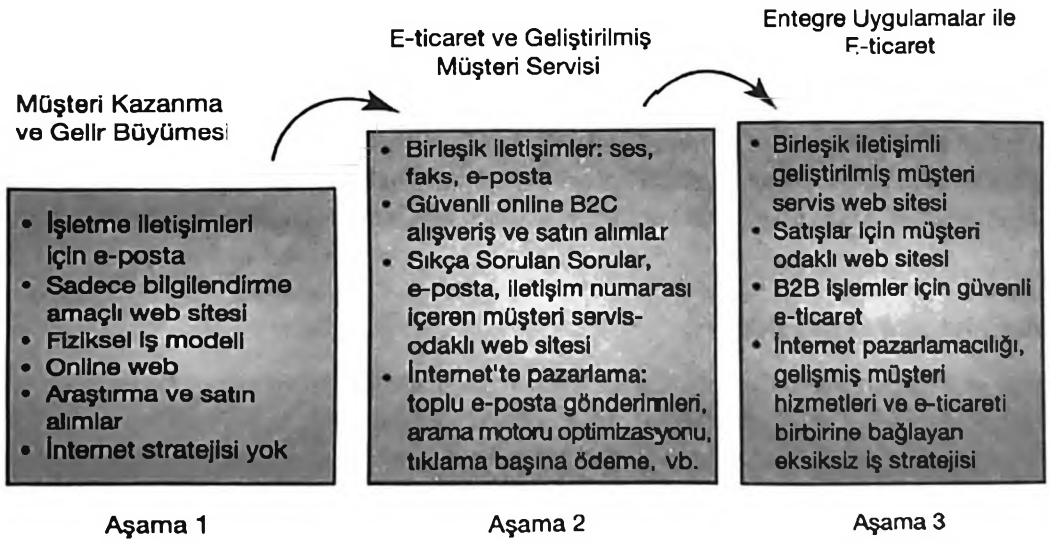
Ödeme ve kredi kartı işlemlerinin işlenmesi—Güvenli online ödeme ve kredi kartı işlemleri müşterilerin kişisel bilgilerini yetkisiz erişimlerden korumak için tam bir arka uç *(back-end)* sistem güvenlik kontrolleri ile şifrelenmelidir.

İşletmelerin Neden İnternet ve IoT Pazarlama Stratejileri Olmalıdır

E-işletme stratejisi geliştirmek bir internet sitesi oluşturmaktan çok daha fazla şey içermektedir. Herhangi bir e-işletme sahibi internet aracılığıyla küresel yeni iş partnerlerini ve müşterilerini nasıl bulacağını anlamalıdır. E-işletme planı veya buraya nasıl geçilebileceğine dair bir planı olmayan işletme, internet konusunda bilgi sahibi rakipleri karşısında kaybedecektir. İnternet pazarlama stratejisi, bir işletmenin başarısındaki anahtar parçalardan biridir. Önemli olan web sitelerinize daha fazla ilgi çekmeniz ve bu ilgiyi tutabilmenizdir. İnternet pazarlama stratejileri, arama motoru stratejilerini, ortak pazarlama anlaşmalarını, talep gören ve taze içerikleri kullanmaktadır. Günümüzün küresel marketinde, tek bir model olarak sadece fiziksel işletme modellerinin kullanımı güncelliğini yitirmiştir. İşletmelerin, müşterilere bilgiye, ürünlere ve servislere sürekli erişim imkanı sunan online e-işletme varlığı olmalıdır. **ŞEKİL 2-3**, World Wide Web üzerinden e-işletme modeline dönüşüm işlemlerini göstermektedir.

İşletmeler iş modellerinde interneti içerdikçe online riskler, tehditler ve güvenlik açıkları ile daha fazla karşı karşıya kalmaktadır. internete bağlanmanın, kendinizi bilgisayar korsanlarına ve siber hırsızlara açmak anlamına geldiğini unutmamalısınız. Güvenli web uygulamaları, güvenli ön-uç *(front-end)* ve arka-uç *(back-end)* sistemleri, kişisel müşteri verisinin şifrelemesi her organizasyonun riskleri azaltmak için gerçekleştirmesi gereken kritik güvenlik kontrolleridir.

Bu durum, fiziksel mağazalara ihtiyaç olmadığı ya da tamamen gereksiz olduğu anlamına gelmemektedir. İronik bir biçimde, büyük bir online mağaza olan Amazon ilk gerçek dünya perakende mağazasını 2015 yılının sonunda açmıştır. Gelecek yıllarda daha fazla fiziksel mağaza açacak



ŞEKİL 2-3
Web üzerinde bir e-işletme modeline dönüşüm.

olmasının planlaması da, fiziksel mağazaların önümüzdeki yıllarda e-ticaret ve kapsamlı bir müşteri deneyimi ile birlikte var olmaya devam edeceğini göstermektedir.

Mobil IP

İletişim araçları da insanların iletişim için kullandığı teknikler gibi değişime uğramıştır. İletişimde önceki değişimler yeni bilgisayarlara uyum sağlanması ve ağlara bağlanmayı içermektedir. Ses iletişimi genellikle telefonlar kullanılarak gerçekleştirildi. Uzun yıllar boyunca, telefonlar ses iletişimini destelemekten biraz daha fazlasını gerçekleştirdi. Geçtiğimiz yıllarda, kişisel iletişim cihazları ve mobil telefonlar oldukça güçlü bir hale gelmiştir. Cep telefonu kullanımı, insanların hareket kabiliyetlerini *(mobility)* genişletmek için cep telefonlarını kullanmaya başlamaları ile 1990'larda patlamıştır. Günümüzün mobil telefonları, akıllı telefonları ve PDA'ları birçok küçük bilgisayarın gücü ve esnekliği ile eşleşecek şekilde gelişmiştir. PDA, hafif, elde tutulan, genellikle kalemi ile kullanılan ve takvim, adres defteri, vb. uygulamaları ile kişisel bir elektronik ajandadır. Yazılım yayıncıları taşınabilir cihaz pazarını hedefleyen birçok program çıkarmışlardır. Tabletler, akıllı telefonlar ve netbooklar hafif taşınabilir cihaz ihtiyacını ortaya çıkarmıştır. Sayısı gittikçe artan kişiler günlük kullanım için büyük dizüstü bilgisayarlar yerine bu cihazları taşımaktadırlar.

Mobil kullanıcılar ve Kendi Cihazını Getir

Her büyüklükteki organizasyonu etkileyen en önemli eğilimlerden biri de kişisel iletişim cihazlarının kullanımının artmasıdır. Kullanıcıların kişisel cihazlarına bağlılığı artınca, çalışanlar işteyken de bağlantılarını korumayı beklemektedirler. Bu cihazlara izin veren organizasyonlar, bu cihazların kullanımını politika aracılığı ile hala kontrol etmek zorundadırlar. Bu politika **Kendi Cihazını Getir (*Bring Your Own Device* - BYOD)** olarak bilinmektedir. Böyle bir politikaya sahip organizasyonlar çalışanlarının ve taşeronlarının ofislerindeki ağa bağlanmak için kendilerinin kişisel olarak seçmiş ve temin etmiş oldukları cihazlarını kullanmalarına izin vermektedir. Bu uygulama, organizasyonların kısıtlı modelleri tedarik edip çalışanların şahsi kullanımına sunma ihtiyacını ortadan kaldırmıştır. Kimi uzmanlar böyle bir yaklaşımı "iş anlayışı *(business sense)*" açısından alım maliyetlerini ve işlemsel harcamaları düşürmesi, kullanıcıların ve uygulamaların desteklenmesi nedenleri ile desteklemekte fakat diğerleri BYOD'un önemli güvenlik sorunlarına kapı açacağını itiraf etmektedir.

Kullanıcılar çok fonksiyonlu ve bağlı küçük cihazları tercih etmektedirler. Geçtiğimiz on senede, dizüstü bilgisayarlar daha küçük, hafif ve daha güçlü bir hale gelmişlerdir. Birçok masaüstü bilgisayarın performansına erişebilecek kadar güçlenmişlerdir. Kullanıcılar da dizüstü bilgisayarlarına güvenmekte ve işlerini masalarından her yere götürebilmenin keyfini çıkarmaktadırlar. Kullanıcılar, aynı zamanda, ofislerinden ayrılabilmeyi ve hala e-postalarına bağlanabilmeyi ve artan ofis uygulamalarını sevmişlerdir. Kullanıcılar masaüstü bilgisayarlardan mobilite ve özgürlük

Mobil telefon, akıllı telefon veya PDA?

Mobil cihazlar geliştikçe artık onları açıklayabilmek için gerekli terimlere sahip olduk. Günümüzde mobil telefon *(mobile phone)*, kullanıcının telefon görüşmeleri yapabilmesi ve metin mesajları gönderip alabilmesine izin veren mobil cihazdır. Telefon özelliklerine sahip olmayan fakat bir mobil işletim sistemi ile programları yürütebilen diğer cihazlara PDA'ler denmektedir. Hem mobil telefonların hem PDA'ların özelliklerini birleştiren cihazlara da genellikle akıllı telefonlar *(smartphones)* denmektedir.

talep etmeye başladılar. Bilgisayar üreticileri, kullanıcıların ağır bir cihazı yanlarında taşımadan her zaman bağlantılı olabilmek için artan isteklerinden dolayı daha küçük ve hafif dizüstü bilgisayarlar üretmeye başladılar.

Akıllı telefon ve PDA üreticileri de bu isteğe dikkat ettiler. Cihazlarını daha hızlı ve güçlü, daha bilgisayara benzer yapmaya başladılar. İşletme kullanıcıları arasında artan pazardaki en önemli liderlerden biri BlackBerry'di. 1999'da ilk BlackBerry aracı tanıtılmıştır. Kullanıcıların tek bir araç ile arama yapabilmesine, e-postalarına bakabilmesine ve planlarını yönetebilmesine olanak sağlamıştır. Aynı zamanda, kullanıcılar bazı uygulamalar çalıştırıp işlerinin bir kısmını dizüstü bilgisayarları olmadan da gerçekleştirebilir duruma gelmişlerdir. Bu gelişmeyi, Apple'ın popüler IPhone® ile başlayan iOS ürünleri takip etmiştir. İlk IPhone 2007 yılında piyasaya çıkmıştır. İlk Android telefon, yeni Android işletim sistemini kullanan T-Mobile G1™, 2008 yılında piyasaya çıkarılmıştır. Pazardaki bu üç ağır oyuncu ile pazardaki en fazla mobil kullanıcıya sahip olma oyunu başlamıştır.

Buradaki soru: "Mobil cihazları kullanmayı gerçekten kim ister?" idi. Bu sorunun cevabı ise: "Neredeyse herkes!" oldu. İnsanlar mobil cihazları şahsi ve profesyonel yaşamları için istemişlerdir. Bu trend, BYOD politikasının önemine işaret etmiştir. Mobil cihazların, yazılımların ve servislerin tedariki kullanıcıların taleplerini ancak karşılamıştır. Her yeni cihazın ve yazılımın piyasaya sürülmesi ile mobil kullanıcılar mobil teknolojilerin daha fazla kullanım alanını keşfetmişlerdir. Mobil hesaplama, geleneksel sistemlerin gücüne ve uygunluğuna erişmeye başlamıştır. Fakat, en azından hala bulunmakta olan üç sorun vardır: Ağ hızı, kullanılabilirlik ve güvenlik.

Mobil araçlar ve uygulamalar için birçok kullanım şekli vardır. İlk uygulamaların bazıları genellikle oldukça basit web uygulamalarıydı. Kullanıcılar mobil cihazlarındaki web tarayıcılarını kullanarak web sunucularına bağlanmaktaydılar. Daha sonra çıkan akıllı telefonlar ve PDA'lar sürekli ağ bağlantısı gerektirmeyen yerel uygulamaları *(native applications)* desteklemişlerdir. Bazı uygulamalar sabit ağ bağlantısına ihtiyaç duyarken bazıları ise ihtiyaç duymamıştır. Örnek olarak, çalışanların zaman çizelgesi bilgisini merkezi sunucuda saklayan bir uygulama verilebilir. Mobil cihaz ağa bağlanıp sunucu ile senkronize olmalıdır fakat sabit bir bağlantı kurmasına ihtiyaç yoktur. Sabit network bağlantısına ihtiyaç duymayan uygulamalar, örneğin uçak ya da diğer uzak konumlarda, mobil veri ile çalışmaya imkan vermektedir.

Mobil cihazların ilk kullanım şekillerinden biri işi iş yeri dışına taşıyabilmek olmuştur. Mobil çalışanlar, uygulamaların mobil cihazlara geçmesindeki öncüler olmuşlardır. İlk kullanılan uygulamalar, e-posta ve planlamaları yönetmeye yardımcı olan genel uygulamalardır. Tıp uzmanları da hızlıca kendi ihtiyaçlarını karşılayacak mobil hesaplamanın avantajlarını fark etmişlerdir. Tıbbi tedavi ve tıbbi bilgi yönetimi uzun bir süredir birbiri ile alakalı görevlerdi. Tıbbi uzmanların, en iyi tedaviyi uygulayabilmek için, hastaların kişisel sağlık bilgilerini içeren çizelgelerine ve dosyalarına erişme ihtiyaçları vardır ve bunu hızlı bir şekilde gerçekleştirmelidirler. Hastaneler, klinikler ve uygulamalar hasta verisinin yönetilebilmesi için oldukça önemli miktarda zaman ve para harcamıştır. Son zamanlarda, tıbbi kayıtların elektronik olarak saklanmasına yönelik yapılan zorlama bu veriye erişimi daha da önemli hale getirmiştir. Doktorlar, hemşireler ve diğer yetkilendirilmiş tıp personelinin talep edildiğinde hasta verilerine erişimi ve bu verileri güncellemesi mobil cihazlar ile olanaklı bir duruma gelmiştir.

Mobil Uygulamalar

Birçok organizasyon, web uygulamalarını etkinleştirerek yeni mobil kullanıcıların isteklerini çözmeye çalışmıştır. Birçok mobil cihaz sınırlı web tarayıcısına sahiptir ve az sayıda uygulama çalıştırabilmektedir.

Bu yaklaşım daha önceleri uygulamaları yalnızca ev bilgisayarı ile kullanan birçok kullanıcıya yeni uygulamalar sağlanmıştır. Maalesef, fonksiyonellik çoğu zaman yetersiz kalmıştır. Web tarayıcıları için yazılmamış olan uygulamalar çoğu zaman kullanıcılar için kafa karıştırıcı ve sinir bozucu olmuştur. Birçok uygulama mobil kullanıcılara kötü arayüz sunmasından dolayı başarısız olmuştur.

Mobil araç üreticileri, yazılım geliştiricileri, servis sağlayıcıları mobil kullanıcıları desteklemeye başlamış ve bazı sorular sormaya başlamışlardır. Sormaya başladıkları en temel sorular: "Mobil uygulamaları kim kullanıyor?" ve "Kim mobil uygulamaları kullanmak ister?" olmuştur. Birçok farklı alanlardan farklı kullanıcıların mobil uygulamaları kullandıklarını fark etmişlerdir. İlk önce uyum sağlayanlar arasında tıp personeli vardır.

Tıbbi uygulamalar mobil cihazların ilk günlerinde mobil uygulamalar için iyi bir eşleşme olmuştur. Tıbbi personel sürekli olarak hastalarla ve hasta bilgileriyle etkileşimde olmak durumundadır. Örneğin, bir hastanın aynı gün içinde birçok farklı doktor, hemşire ve uzman tarafından muayene edilmesi gerekebilmektedir. Her tıbbi görevlinin hasta hakkında bazı bilgilere erişmesi gerekmektedir. Hasta bilgisi nüfus bilgilerini, hasta geçmişini, hastalık teşhisini ve tedaviyi içermektedir. Hastaya iyi bir tedavi sağlanabilmesi için hastayla ilgilenen herkesin bu bilgilere erişimi olması gerekmektedir. Her odaya bir bilgisayar yerleştirmek hem zor hem de pahalıdır, bu nedenle tıbbi görevliler ve hastaneler birçok bilgisayara ve ağ altyapısına yatırım yapmaya gerek olmadan mobil cihazların ilgili bilgiye erişimi sağlayabileceğini fark etmişlerdir. Hastayla ilgilenen herkes bir mobil araç taşımakta ve gerekli olan bilgilere kolaylıkla erişebilmektedir.

IP Hareketliliği

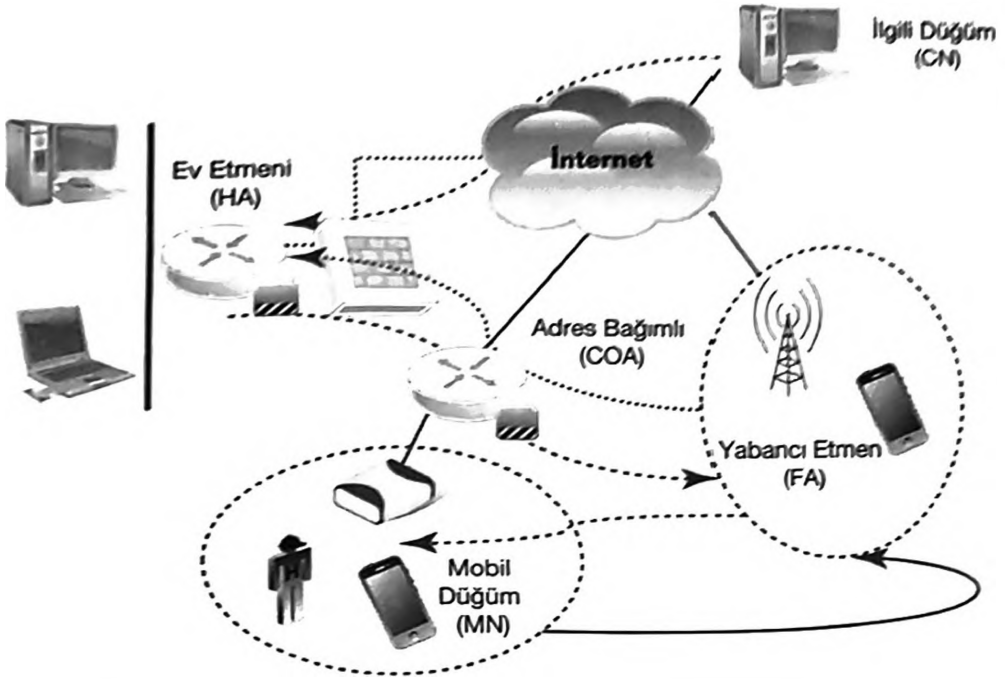
Günümüzün 4G teknolojisi gerçek anlamda IP iletişimini sağlamaktadır. Bu teknoloji önceki teknolojilere göre çok büyük bir gelişim olmuştur. Her 4G araç özgün bir IP adresine sahiptir ve ağda kablo ile bağlı herhangi bir cihaz gibi görünmektedir. Bu da, mobil cihazların diğer IP cihazları ile herhangi bir adres çevrimi yapmadan birbirleriyle etkileşim kurabilmelerine izin vermektedir. Buradaki tek kısıt mobil cihazın işlem gücündedir. Mobil cihazlar gittikçe daha hızlandığından aradaki fark azalmaktadır.

Mobil cihazlar artık fiziksel bir sınırlandırmaya tabi olmadan kablolu cihazlar gibi işlem yapabilmektedirler. Bu durum, hem bir avantaj hem de potansiyel bir tehlikedir. Geleneksel ağ yönetimi, cihazların nerede olduğu bilgisinin bilinmesi temellidir. Sabit bir konumu olmayan cihazların takibi ve güvenliğinin sağlanması zordur.

Mobil kullanıcılar ağa ofislerinde kablo ile bağlandıkları gibi bağlanmak istemektedirler. **IP hareketliliği (*Mobile* IP)** bunu mümkün kılmaktadır. Kullanıcılar, IP hareketliliğini kullanarak farklı LAN segmentlerinde bağlantıları kopmadan hareket edebilmekte ve standart TCP/IP kullanımında bir

Listeden birden fazla öğe seçmek

Bir uygulamanın mobil cihazla eşleşmesine örnek bir zorluk olarak listeler gösterilebilir. Yazdığınız yasal bir uygulamanın kullanıcılara pizzalarına ne tür malzemeler eklemek istediğini sorduğunu varsayalım. Klasik bir web uygulaması birden fazla seçim yapabilmeyi kullanıcılar için kolay hale getirmektedir. Microsoft Windows kullanıcıları Control (ctrl) tuşuna basılı tutup birden fazla seçim yapabilmektedirler. Fakat, bu kolay eylem IPhone'lar, IPad®'ler veya Android araçlarında zordur, çünkü Control tuşu yoktur, bu nedenle yazılım geliştiricilerinin mobil cihaz kullanıcılarına pizzaları için birden fazla malzeme seçmelerine izin verecek farklı yollar bulması gerekmektedir.



ŞEKİL 2-4
IP hareketliliği iletişimleri

1. Mobil düğüm (MN) yabancı etmene (FA) bağlanır.
2. FA adres bağımlısı (COA) MN'ye atar.
3. FA, COA'yı ev etmenine (HA) gönderir.
4. İlgili düğüm (CN) MN'ye mesaj gönderir.
   a. CN'nin MN'ye mesajı öncelikle HA'ya gider.
   b. HA mesajı COA'ya iletir.
   c. FA mesajı MN'ye iletir..

kesintiye neden olacak bu olaydan etkilenmeden bağlı kalmaktadırlar. Kullanıcılar hareket ettikçe cihazlarının bir ağdan diğerine geçtiğini fark etmeyecektir. Kullanıcılar, mobil cihazları ağın kapsama alanında kaldıkları sürece ağ bağlantılarını koruyacaklardır. Ağ cihazı hücresel bağlantı ve Wi-Fi bağlantısı arasında değişim yapmak durumunda kalabilmektedir ve hala şeffaf bağlantıları *(transparent connections)* sağlamaktadır.

ŞEKİL 2-4, IP hareketliliğinin bir çok mobil cihazın bir ağdan diğerine bağlantı kopmaksızın geçmesini garanti etmek amacıyla birlikte çalışan bir çok varlık için nasıl şeffaf bağlantı sağladığını göstermektedir.

- **Mobil düğüm (*Mobile node* - MN)** – Bir ağdan diğer ağa hareket eden mobil cihazdır. MN, ağdan bağımsız olarak sabit bir IP adresine sahiptir.
- **Ev etmeni (*Home agent* - HA)** - Standart yönlendiricilerden fazla özelliklere sahip olan bir yönlendiricidir. HA yönettiği MN'leri takip etmektedir. MN yerel ağı terk ettiğinde HA onun paketlerini MN'in mevcut ağına yönlendirmektedir.
- **Yabancı etmen (*Foreign agent* - FA)** – HA ağından farklı bir ağa bağlı olan ek özelliklere sahip bir yönlendiricidir. FA MN'ye yerel bir adres atar. MN, IP hareketliliğini destekleyen başka bir ağa bağlandığında kendini FA'ya tanıtır.
- **Adres bağımlı (*Care of address* - COA)** - MN yeni bir ağa bağlandığında onun yerel adresidir. FA, COA'yı MN'ye atar ve MN bağlandığında onu HA'ya gönderir. Birçok durumda, COA aslında FA adresidir. HA, MN ile ilgili herhangi bir paketi COA'ya gönderir. FA paketleri alır ve MN'ye iletir.
- **İlgili düğüm (*Correspondent node* - CN)** - Bu düğüm MN ile iletişim kurmak isteyen düğümdür.

Bir MN'nin ev ağını terk ettiğini ve başka bir ağa bağlandığını varsayalım. MN yeni bir ağa bağlanınca, FA, COA'yı HA'ya gönderir. Daha sonra, bir CN,MN ile iletişime geçmek ister. CN, MN'nin IP

adresine bir mesaj gönderir. Ağ paketi MN'nin ev ağına yönlendirir. HA paketi alır ve COA'ya iletir. FA, paketi MN'ye iletir.

IoT'nin Yarattığı Yeni Sorunlar

Bu bölümün başında IoT'nin üstesinden gelmesi gereken beş sorunu görmüştünüz:

- **Güvenlik (*Security*)**—Kişisel ve profesyonel hayatınız için IoT'yi etkinleştirirseniz kötü adamları nasıl uzak tutacaksınız?
- **Mahremiyet (*Privacy*)**—Ailenizin kimlik ve mahrem verisini hırsızlardan ya da yetkilendirilmemiş erişimden nasıl koruyacaksınız?
- **Birlikte çalışabilirlik ve standartlar (*Interoperability and standards*)**—IoT üreticileri ve ASP geliştiriciler cihazların güvenli bir şekilde haberleşmesini nasıl garanti etmektedirler?
- **Yasal ve Mevzuat Uyumluluk (*Legal and regulatory compliance*)**—ürünlerin ve servislerin ödemesini içeren IoT ile ilgili işletme işlemlerine ilişkin yasal, vergi ve mevzuat gereksinimlerine uluslararası, federal, ve eyalet seviyesinde ne tür bir rol ile katkı verilmektedir?
- **E-ticaret ve ekonomik kalkınma sorunları**—World Wide Web'de de iş yapan kurumlar için ekonomik kurallar nelerdir? IoT bağlanabilirliği ve bilgi paylaşımı küresel olarak nasıl yayılmalıdır?

Güvenlik

Güvenlik üçlüsünün gizlilik, bütünlük, ve kullanılabilirlikten (*confidentiality, integrity, availability* - CIA) oluştuğunu hatırlayın. Bir kişi ya da kurum güvenliği göz önünde bulundurmadan internete bağlanırsa ne olacaktır? Çalınabilecek değeri olmayan ya da hassas bir yapısı olmayan bir şey olsa bile bağlanır mıydınız? Kullanıcılar ve işletmeler internete bağlanmadan önce ne yapmalıdırlar? Aynı sorular IoT üzerinden bağlanan cihazlar için de geçerlidir. Varlık *(asset)* ve varlığın içerisindeki bilgi size ait, bu nedenle kendi kişisel hayatınızı, evinizi, ve işletme içeriğinizi internete bağlarsanız neyin riskte olduğuna siz karar vereceksiniz. internete kimlik bilgilerinizi, sosyal ve aile hayatınızı, ev ve profesyonel hayatınızı bağlayabilmek için yüksek derecede güvene sahip olmanız gerekir. Veya varlıklarınızı internete bağlamak için savunma stratejisi olarak kendi güvenlik kontrollerinizi etkinleştirebileceğinize dair yüksek derecede güvene sahip olmanız gerekir. Savunma stratejiniz ne olursa olsun, riskler, tehditler ve güvenlik açıkları her yerde bulunmaktadır. O zaman güven ne zaman devreye girmektedir? İnsan olarak tabi olduğumuz etik değerler internet için de geçerli mi? Kabul edilebilir veya kabul edilemez davranışlar nelerdir, ve kim ya da hangi kurum bunları kabul edilebilir ya da kabul edilemez olarak tanımlamaktadır?

İnternet mevcut durumda korsanlar ve kötü niyetli kişilerle doludur. Güvenlik ve veri ihlalleri her gün gerçekleşmektedir. Günümüzde insanlar ve işletmeler IoT aracılığı ile daha da fazla cihaza bağlanmak istiyorlar. Bu mevcut durumda gerçekleşmektedir. Her geçen gün internete bağlı cihaz ve insan daha fazla olmaktadır. İşletmeler online varlıklarını genişletmekte ve yeni uygulamalar geliştirerek internet aracılığı ile satmaktadır. Yazılım ürünleri ve dağıtımları artık CD veya DVD ile yapılmamaktadır. Yazılım lisansı bir kez online olarak ödendikten sonra yazılım cihaza hemen indirilebilmekte ve kurulmaktadır. İnsanlar elektronik cihazlara ve gerçek zamanlı bağlantıya daha bağımlı hala gelmektedir. İnternete bağlılıkta ve IoT cihazlarına erişimde artan

bu bağımlılık devam etmekte ve daha da artmaktadır. İnsanların ve işletmelerin IoT'ye bağlılıkları arttıkça korsanların ve kötü niyetli kişilerin de verilere erişme ve çalma olanağı artmaktadır. Bu nedenle, güvenlik IoT'nin üstesinden gelmesi gereken en büyük sorundur. Kim idareci kurum olarak davranacaktır? İnsanlar ve işletmeler IoT ile etkileşim kurarken hangi politikalara, prosedürlere veya davranış kodlarına uyulması gerekmektedir? Güvenlik tüm insanları, devletleri ve işletmeleri etkileyen küresel sorunlara sahiptir.

Aşağıda listelenenler IoT cihazlarının güvenlik sorunlarını özetlemektedir:

- Sensör veya tüketici ürünleri (internete bağlı TV) gibi IoT cihazları büyük miktarlara yayılmıştır. Uygulamanın önemine göre, eğer bir saldırı olursa bir güvenlik açığı birçok uç noktayı etkileyecektir.
- IoT araçları her zaman her yerdedir *(ubiquitous)* ve büyük miktarda kullanıcı ya da ev eşyası popülasyonunu etkilemektedir. Örneğin, eğer bir saldırı tekrar edilebilirse ve uç noktalara iletilebilirse internete bağlı elektrik sayaçları kritik bir altyapı güvenlik açığı ile karşılaşacaktır.
- Güncellenmeyen ve düzenli bakımı yapılmayan IoT cihazları güvenlik açıklarına neden olup ağ ve işletmenin giriş noktası haline gelebilirler. Bu durum, üreticilerin bir ürünün ya da yazılım uygulamasının destek süresinin duyurdukları **Yolun Sonu (*End of Life* - EOL)** durumuna eşdeğerdir.
- IoT güncellemelerinin dağıtımları ve yayımları zor olabilmektedir, bu da IoT cihazlarının veya uç noktaların iyileştirilmelerinde aksaklıklar yaratmaktadır. Wi-Fi erişime ve bütünleşik bilgisayarlara sahip olan arabalar üretici tarafından sağlanacak olan yazılım yamalarına ve güncellemelerine ihtiyaç duyarlar. Bu bakım, bir yazılım güvenlik açığının iyileştirilmesi gereken tüm arabalar için gerçekleştirilmelidir.
- IoT cihazları, genellikle kullanıcılara ya da cihaz sahiplerine cihazın iç özellikleri ya da cihazın nasıl çalıştığı ve internete nasıl bağlandığı ile ilgili bilgi sağlamamaktadır. IoT cihaza uzaktan erişime sahip olan üreticiler ya da servis sağlayıcıları kullanıcının izni olmadan araçtan veri ya da bilgi çekebilirler. Ürün garantisinin kontrolü ve servis sağlayıcısıyla IoT cihazının iletişiminin ve veri paylaşımının kontrolü kullanım anlaşmasının bir parçası olmalıdır.
- IoT cihazları genellikle fiziksel olarak güvenli değillerdir ve ev dışında kamu kullanımına açık alanlara yerleştirilebilirler. Evinizin elektrik paneli, kablolu TV'si veya fiber optik kablo noktaları genellikle çok güvenli değildir. Kamusal Wi-Fi'a bağlı IoT cihazlarında ya da açık Wi-Fi ağlarında güvenlik yetersizdir.
- Çevresel IoT cihazları, bilimsel nedenler ya da araştırma nedenleri ile okuma ve ölçüm yapmak için genellikle dışarıda açıktırlar. Eğer bir IoT cihazı IP veri ağına giriş noktası olarak davranabiliyorsa, tek bir cihazdaki güvenlik açığı eğer ağda birden fazla IoT cihazı varsa tüm cihazları etkileyebilecektir.

Mahremiyet

Ailenizin kimlik ve mahremiyet verisini kimlik hırsızlığına neden olabilecek bir hırsızlıktan ya da yetkisiz erişimden nasıl korursunuz? Ülkenizdeki bir birey olarak mahremiyet haklarınızı biliyor musunuz? Bu mahremiyet hakları internet ve IoT cihazlarını da kapsıyor mu? IoT cihazlarınızdaki verilerin sahibi kim? Mahremiyetin birçok katmanı vardır. Birincisi sizsiniz ve sizin kimliğiniz ve kişisel verileriniz. Daha sonra, mahremiyet eşinize ya da diğer aile üyelerinize doğru genişlemektedir. Aileler, tüm aile üyelerinin mahrem verilerinin gizli olarak tutulduğundan emin olmak için bir mahremiyet stratejisine ihtiyaç duyarlar. Bir aile üyesinin kişisel verisinin sızması diğer aile üyelerinin kişisel verilerinin de ele geçirilmesine neden olabilecektir.

Kullanıcılar, interneti ve IoT cihazlarını kullanırken belli bir seviyede güvene sahip olmalıdırlar. Asıl önemli olan mahremiyete saygı duyulmasıdır. Kullanıcının hakları net olarak tanımlanmalı ve tüm IoT cihazlarına da açık bir biçimde tanıtılmalıdır. IoT, mahremiyet kavramı, kişisel verinin ne olduğu ve kişisel verinin sahibinin kim olduğu hakkında yeni endişeler yaratmaktadır. IoT cihazındaki verinin sahibi kimdir, cihazın sahibi olan kişi mi (yani siz) veya cihazın üreticisi midir? Verinin üst verisinin ***(metadata)*** sahibi kimdir? Üst veri IoT cihazının sahibine mi aittir ya da kullanıcı ürünü satın aldığında ürün garantisi ve yazılım lisans anlaşmasında belirtildiği üzere internet aracılığı ile bu üstveriyi toplayan cihaz üreticisine mi aittir? IoT cihazının kullanım örüntüsü *(patterns)* ve bilgisi üretici için yararlı bilgilerdir. Ancak bu veriler sizin verileriniz midir? Veri ve verinin sahibinin kim olduğu tanımlaması siz ürünü satın almadan ve cihazı internete bağlamadan önce açık bir şekilde anlaşılmalıdır.

IoT yeni ve ilginç mahremiyet sorunları ortaya çıkarmaktadır. Bu sorunların hem IoT cihazının üreticisi hem de bu cihazın kullanıcısı birey tarafından tamamen anlaşılması ve incelenmesi gerekmektedir. Aşağıda belirtilen mahremiyet sorunlarının cihaz üreticileri tarafından ele alınması, kullanım hakkı ve son kullanıcı yazılım lisans anlaşmasında tanımlanması gerekmektedir:

- **Mahremiyet politikası açıklaması:** Üreticinin mahremiyet politikası açıklamasında belgelenen kullanıcının mahremiyet haklarının yasal olarak tanımıdır. Bu mahremiyet politikası açıklaması kullanıcı tarafından mahremiyet verisinin girildiği herhangi bir online forma eşlik etmelidir.
- **Veri, üst veri, veya analitik veri kullanımı ve hakların tanımlanması:** Verinin, üst verinin, ya da analitik verinin ne olduğunun, bunların ne için kullanılabileceğinin ve bu verilerin kullanımı için kullanıcıdan izin alınmasının gerekip gerekmediğinin gerçek tanımıdır.
- **Kullanıcının, üreticiye ya da uygulama servis sağlayıcısının mahremiyet politikası açıklamasına onay (*consent*) verme yeterliliği:** Kullanıcılar açıklamayı online olarak okumalı, mahremiyet politikası terimlerini ve koşullarını kabul ya da reddebilmelidirler. Kullanıcı bir kez onay verdiğinde, bu onayın geri alınması genellikle çok zordur. Bazı şirketler

BİLGİNİZE

Eğer sağlığınızı takibe düşkün biriyseniz ve bir mobil uygulama aracılığıyla online kalori ve sağlık performansı izleme servisine kaydolduysanız ne olur? IoT bağlantılı olan buzdolabınız, online gıda alışverişleriniz ile birlikte çalışarak ne yediğinizi izler ve yediklerinizin kalorisini hesaplar. Aynı zamanda, kullandığınız online restoran rezervasyon sistemini kalori ve sağlık performans izleme uygulamasına bağlamaya karar verebilirsiniz. Restoranda sipariş verdiğinizde, yemeğiniz ve kalorisi otomatik olarak günlük kalori hesabınız içerisinde hesaplanır. Üstelik, siz egzersiz yaptıkça ve kalori yaktıkça sizin IoT fitnes kalori izlemeniz sizin online kalori ve sağlık performans izleme uygulamanıza gerçek zamanlı güncellemeler yapar. Sizin kalorinizi ve sağlık performans verinizi barındıran kalori ve sağlık performans ASP'si, veriniz üzerinde analiz gerçekleştirir ve veriniz ile ilgili yeni üst veri yaratır. Bu üst veri sağlık hizmetleri ile ilgili araştırmacılarına ya da sağlıklı yiyecek üreticilerine satılmaktadır. Eğer bu veri, örneğin yaşınız, kilonuz ve coğrafik konumunuz gibi demografik bilgi içeriyorsa, **kimliksizleştirilmiş veri (de-identified data)** olarak kabul edilse de sizin hakkınızda oldukça fazla bilgiye sahiptirler.

Üst verinin ya da veri hakkındaki verinin sahibinin kim olduğu mahremiyet alanında çok yaygın bir konudur. Bu muhtemelen henüz tam olarak incelenmemiş ve çözülmesi gereken bir numaralı mahremiyet sorunudur. Genel olarak, insanlar mahremiyet haklarını bilmez, ve kullanıcıların bu haklarını tam olarak anlamaları önemlidir. Bu konu, kullanıcının neleri yapmakla ilgili rahat olduğu ile IoT cihazının üreticisine ne kadar güven duyduğu arasında ince bir çizgi yaratır.

bu onayın kaldırılması için online olarak hiçbir yetenek sunmadan sizden resmi bir yazı yazmanızı istemektedir.

- **Mahremiyetin etki alanına karar vermek:** Eğer sizin, akıllı telefonunuzun ya da mobil IP cihazınızın konum belirleme takibine ve diğer uygulama servis sağlayıcısının sizin ve sizin nereye gittiğiniz bilgisini kullanmasına onay verdiyseniz, bu sizin mahremiyet haklarınızı ihlal etmekte midir? Eğer bu verilerin toplandığından bile haberiniz yoksa ne olacaktır? Ev içi mahremiyetin ihlal edilmesinin bir anlamı vardır fakat bu durum evinizdeki internete bağlı IoT cihazlarına da genişletilebilir mi? Mahremiyetin etki alanları mahrem veriniz ya da üst veri yeni veri oluşturmak için diğer veriler ile kümelendiğinde *(aggregated)* ya da ilişkilendirildiğinde *(correlated)* bulanıklaşmaktadır. IoT cihazlarının insanlar hakkında çok ayrıntılı bilgi toplayabildiği unutulmamalıdır. Veri profilleri yaratılabilir, böylelikle dışarıya sızmasını istemeyeceğiniz ya da yeni tehditler ve başka bir şahıs tarafından kullanılmasını istemeyeceğiniz davranış örüntüleriniz yaratılabilir.

Bu mahremiyet sorunlarına ek olarak, aşağıda IoT hukuk uzmanlarının ve mahremiyet danışmanlarının arasında incelemesi ve anlaşması için yeni sorular sunulmaktadır:

- Veri kaynağını, veri toplayıcılarının haklarını ve verinin kullanımını nasıl belirleyeceğiz?
- Mahrem veriyi kişiye bağlamadan, mahrem verinin kimliksizleştirilmesini içeren mutlu bir orta yol var mıdır?
- Bir kullanıcı ya da işletme iyi bir mahremiyet durumunu ya da tercihini nasıl bilecektir?
- Mevcut sosyal bağlamlar ve kabul edilebilir davranışlar IoT'ye genişletilecek mi?
- Mahremiyete göre (temel gereksinimler kümesi ile birlikte) bir tasarım geliştirebilir ve IoT'nin tümü için mahremiyetin standart bir gerçekleştirimi olarak devreye sokabilir miyiz?

Bu gibi sorular, özellikle yasal ve mevzuat uyumluluk bakış açısıyla dikkatli bir analiz ve risk azaltıcı çözümler gerektirmektedir. ABD federal ve eyalet mahremiyet yasaları, kişisel veriyi kullanan, elinde tutan, saklayan ve yayınlayan varlıkların belirli güvenlik ve mahremiyet gereksinimlerine uymalarını beklerken vatandaşların kişisel verilerini korumak içindir.

Birlikte çalışabilirlik ve Standartlar

Birlikte çalışabilirlik *(interoperability)* ve standartlar, uyumlu bir IoT cihazı, bağlanabilirlik ve iletişim ortamı gerçekleştirimi için kilit bir öneme sahiptir. Bunlar olmadan, uygulama servis sağlayıcıları, IoT cihazı üreticileri ve müşteriler, IoT cihazlarının gerçekleştiriminden ve bağlantılarını sağlamaktan vazgeçeceklerdir. İnternet Servis Sağlayıcıları (*Internet Service Provider* - ISP) ve son kullanıcı müşteriler, uçtan uca IP iletişimleri için birlikte çalışabilirliği sağlamak için TCP/IP sürüm 4 iletişim protokolünü kullanmayı kabul etmişlerdir. Cihazdan cihaza işlevselliği sağlamada IoT cihaz bağlanabilirliği ve güvenlik için ortak bir birlikte çalışabilirlik ve standartlar temasını izlemek önemlidir. ***İnternet Mühendisliği Görev Gücü* (*Internet Engineering Task Force* – IETF)** dahil olduğu sürece, IoT çözümleri için birlikte çalışabilirlik ve standartlar takip edilebilir. İnternet Topluluğu'nun *(Internet Society)* dört temel prensibi – bağlan, konuş, paylaş, ve yenilik yap *(innovate)* – IoT yeniliğinin başarısını sürdürebilmenin anahtarıdır.

Tam olarak birlikte çalışabilir bir IoT ortamı, herhangi bir IoT'ye bağlı cihazın başka bir IoT'ye bağlı bir cihaz ile konuşmasına izin vermektedir. Bu iletişim doğrudan ya da paylaşılan bir sunucu veya iletişimin merkezi bir noktası olarak davranan uygulama üzerinden dolaylı olarak gerçekleşebilir. Burada önemli olan, bilginin nasıl toplandığı, saklandığı ve kullanıldığıdır. Birlikte çalışabilirlik, benzer işletim sistemlerini (*operating systems* - OS), iletişim protokollerini ve verinin güvenli bir

şekilde bir sunucuya ya da güvenli bir bulutta barındırılan uygulama sunucusuna iletilmesi için metotları gerektirir. Standardizasyon, ortak protokollerin benimsenmesi ve şifrelemeyi/deşifrelemeyi içeren iletim şemaları standartlaştırılmış gerçekleştirimleri gerektiren önemli gereksinimlerdir.

Birlikte çalışabilirlik eğer düzgün bir şekilde ele alınmazsa önemli ekonomik etkileri vardır. Bu üreticilerin ve uygulama yazılım sağlayıcılarının istemediği bir durumdur. Üreticiler ve uygulama yazılım sağlayıcıları, destekledikleri IoT cihazlarının ve uygulamalarının fiyatlarının düşmesini ve böylelikle uygun bir fiyatlandırma ile geniş bir kullanıcı ve işletme kitlesinin IoT'den yararlanmasını istemektedirler. Birlikte çalışabilirlik, kullanıcılar ve işletmeler için IoT gerçekleştirim maliyetlerini düşürmektedir. Açık standartların gerçekleştirimi ve birlikte çalışabilirlik gereksinimleri daha fazla IoT cihazının bağlanabilmesine olanak sağlayacaktır. Bu durum, IoT dağıtımları için kârlılık IoT dağıtım maliyetini ödemek için ayrıldığından, ekonomik değeri, ya da yatırım kârlılığını arttırmaktadır. 2015'te yayınlanmış olan McKinsey Küresel Enstitüsü *(McKinsey Global Institute)* raporuna göre 2025 yılında birlikte çalışabilirliğin ekonomik faydaları ve finansal etkileri trilyonları bulacaktır.

IoT cihazlarının gerçekleştirimi ve erken gelişimi için IoT araçlarının geliştirilmesi için birlikte çalışabilirlik, standartlar, protokoller ve tanımlamalar gereklidir. Aşağıda birlikte çalışabilirlik ve standartlar ile birlikte ele alınması gereken önemli zorluklar listelenmektedir:

- **Bazı üreticiler tescilli IoT cihazları ve çözümleri tasarlamak ve dağıtmak istemektedirler:** Bu, erken benimseyen müşterileri ve işletmeleri kendi ürünlerine bağlama stratejisidir. Bu durum, bilgi paylaşımına izin vermeyen ve ağ geçidi *(gateway)* kullanımı gerektiren ya da bilgi paylaşımı için aracı çözümler gerektiren teknoloji silolarını yaratmaktadır. Eğer veriler paylaşılabilir formattaysa uygulamaların IoT cihaz verilerini paylaşması mümkündür. Uyumsuz IoT cihazları ve uygulamaları arasında veri paylaşımı için, uygulama program arayüzleri (*application program interface* – API'ler) veya diğer yazılım arayüzlerine gerek olabilmektedir. Bu durum, IoT'nin gerçekleştirimini ve kabul edilebilirliğini engellemektedir.
- **IoT cihazları ve uygulamaları içerisine operasyonel, teknik, fonksiyonel ve güvenlik özelliklerini uygulamanın getirdiği maliyet faktörü:** Bir pazara açılma stratejisinin tasarlanması ve gerçekleştiriminde maliyet her zaman bir kilit faktördür. IoT cihaz bağlanabilirliği için kitlelerin büyük hacimli alımlar yapacağını bilerek fiyat düşük ve karşılanabilir tutulmalıdır. Sağlayıcılar ve üreticiler, ürünün piyasaya hemen sürülmesine karşın IoT cihazı içerisine birlikte çalışabilirliğinin maliyetini eklemelidir.
- **Pazara sürüm süresi riski:** Pazara ilk çıkan olmanın küresel çapta IoT cihaz pazarında bir avantajının olduğunun hiç şüphesi yoktur. Teknoloji yaratıldığından beri sağlayıcılar ve üreticiler bu oyunu oynamaktadırlar. Birlikte çalışabilirlik ve standartlar dönemecinde ne kadar hızlı ilerlediğiniz, tescilli ya da açık standartlar temelli IoT teknoloji dağıtımlarının kullanımına ilişkin çoğu kullanıcı ve iş camiasının nerede olduğuna bağlıdır. Pazara sürüm süresinin gerilimi olmadığında, riske girme ve ürün pazara sürmeden önce birlikte çalışabilirliğin ve standartların küresel olarak uygulanması ve kabul edilmesi sorunları olmayacaktır.
- **Eski teknoloji riski:** IoT sağlayıcılarının, üreticilerinin ve yazılım geliştiricilerinin her biri, IoT teknik çözümlerini ve tam anlamıyla tanımlanmış ve uygulanmakta olan birlikte çalışabilirliği ve standartları olmayan IoT ürünlerini geliştirirken risk almaktadırlar. Bu durum, açık ve geniş çapta kullanılabilir standartlar ya da tescilli çözümler ve tekniklerin kullanılması için erken tasarımı zorlamaktadır. Açıkçası, mimariniz ne kadar açık ve esnek olursa, IoT cihaz ve çözümlerinin geliştirilmesinin tasarımı aşamasında teknik birlikte çalışabilirlik ve standart teknoloji kararlarının uygulanması ve değiştirilmesi o kadar kolaydır.

- **IoT cihazları için birlikte çalışabilirlik ve standartların yokluğu kötü IoT cihazlarından oluşan bir ortamı yaratabilir:** IoT cihazları arasında birlikte çalışabilirlik ve standartlar olmadıkça, iletişim ve bilgi paylaşımı eksikliği olacaktır. Bu durum, cihazların iletişim kuramayabileceği ve bilgi paylaşamayabileceği birçok IoT ortamına neden olabilecektir. Bu durum, birden fazla IoT cihazı ve sadece bu cihazların bağlanabileceği ve bilgi paylaşabileceği farklı IoT ağları ile daha fazla sorunlar yaratacaktır. Eğer IoT cihazları birbirleriyle iletişim kuramayacak ve bilgi paylaşamayacaksa IoT vizyonunun amacı nedir? Burada IoT birlikte çalışabilirlik ve standartlarının benimsenmesi için önemli bir sorun yatmaktadır. Konfigürasyon güncellenmeleri otomatik, basit ve IoT cihazları arasında tamamen birlikte çalışabilir olmalıdır. Güncellenmiş firmware gönderim yeteneği, işletim sistemi yazılımı, ve diğer IoT cihaz yazılımı olmadan cihazlar eskimiş duruma gelecektir. Bu durum, güvenlik açıkları olan veya üretim IP ağına bağlı eskimiş IoT cihazlarına sahip olma riskini arttıracaktır. Uzaktan konfigürasyon yeteneği tüm IoT cihazları ve sistemleri için birlikte çalışabilirlik ve standartları sürükleyecektir.

Yasal ve Mevzuat Sorunları

IoT cihazlarının kamu erişimine açık internette yerleşmesi mevzuat ve yasal açıdan bazı önemli endişeleri ortaya çıkarmaktadır. Bu endişelerden bazıları daha önce hiç oluşmamıştır. Amerika Birleşik Devletleri genelindeki artık tüm dikey endüstriler için mevzuat uygunluğunun geçerli olması ile, kullanıcılar ve işletmeler IoT merkezli cihazları ve çözümleri uyumlu bir şekilde nasıl dağıtmaktadırlar? Bu durum, uyumluluk kanunu altındaki dikey endüstriler (örneğin, sağlık hizmeti için HIPAA, yüksek eğitim için FERPA, federal devlet için FISMA, bankacılık ve finans için **Federal Finansal Kurumlar İnceleme Konseyi (*Federal Financial Institutions Examination Council* - FFIEC)** ve güvenli kredi kartı işlem süreçlerinin izlenmesinde bir standart olan PCI DSS v3.1.1.) için ilginç bir soru ortaya çıkarmaktadır.

Mevzuat uygunluğu ile endişe duyulan konular hassas verinin düzgün bir şekilde ele alınması ve verinin gizliliğinin sağlanmasıdır. Bu mevzuat uygunluğu kanunları ile kullanıcı ve bireyler için hassas veriler özgün olarak tanımlanmaktadır. Fakat IoT cihazlarının verileri ile ilgili durum nedir? IoT cihazları iletişim kurmak için interneti kullanmaktadır. Sunucunun nerede olduğuna ya da IoT uygulamasının nerede bulunduğuna bağlı olarak, sizin IoT veriniz fiziksel ağlardan geçmekte ve devlet sınırlarını aşmaktadır. Bu durum, kişisel verilerinizin hem yaşadığınız ülkedeki hem de IoT'yi barındıran firmanın bulunduğu ülkedeki mahremiyet kanunlarının bir öznesi olduğu anlamına gelmektedir. Verilerin bu hareketi hızlı bir şekilde hukuksal bir soruna neden olmaktadır. Eğer IoT verisi mevzuat uyumluluğu altında korunması gereken kişisel ya da hassas veri olarak sınıflandırılmışsa, IoT sağlayıcısının ya da çözüm sağlayıcısının güvenlik kontrolleri gereksinimlerine ve ihtiyaç duyulan veri koruma kanunlarına bağlı kalması gerekmektedir. Bu ülkelerarası veri hareketi internet için yeni değildir. Yeni olan, IoT cihazlarının IoT cihazınızdaki verilerinizi diğer sistemler ve uygulamalar ile sizin yetkilendirmeniz ya da bilginiz dışında paylaşabileceği ve iletişim kurabileceğidir. Bu durum, sizin bilginizin ya da onayınız olmadığı zamanlarda verinin ülkelerarası dolaşabilmesinden dolayı mahremiyet sorununu karmaşıklaştırmaktadır.

IoT cihazınızdaki verileri kim toplamaktadır? IoT cihazlarınızdan davranış örüntülerinizi kimler toplamaktadır? Bu veriyi toplayan, IoT cihazınız ve davranışsal veriniz ile ne yapmaktadır? Bu durum, IoT veri ayrımcılığı ile birlikte yepyeni bir hukuki ve mahremiyet sorunudur. IoT cihazınızdan toplanan veriler sizin ve sizin IoT cihazınızı kullanımınız ile ilgili özel bir hikaye anlatmaktadır. Bu veriler, iyi amaçlarla kullanılabileceği gibi sizin aleyhinizde ayırımcı bir şekilde

de kullanılabilecektir. Üçüncü parti kullanım hakkı şartlarına bağlı olarak, IoT sağlayıcıları ve ASP'ler sizin verinizi ya da üst veriyi size karşı ayırımcı olacak bir şekilde kullanıyor olabilir. Bunlar, sizin nerede tatil yaptığınız ya da ne yediğiniz veya eğlenmek için nelerden hoşlandığınız hakkındaki verileri içerebilmektedir. Üst veri biriktirilebilir ve sizin harcama alışkanlıklarınızı içeren demografik piyasa verisi arayan başka şirketlere satılabilir. Bu veriler diğer şirketler için ne kadar değerlidir? IoT veya cihaz takip uygulamasının sağlayıcısının sizin üst veri bilginizi satmaya hakkı var mıdır? Farklı ülkelerdeki diğer bireyler ile küresel olarak ilişki kurulduğunda, bu kişinin mahremiyetine hangi kanunlar uygulanmaktadır, örneğin, güvenlik kontrolleri gerekli midir değil midir?

Son olarak, IoT cihazlarının sorumlukları nelerdir? Eğer IoT cihazınız sağlık izleme ve alarmlar için kullanılıyorsa fakat kusurlu çalışma *(malfunction)* durumu varsa? Eğer hatalı bir IoT cihazı nedeni ile bir kişi yaralanırsa ya da ölürse, sorumluluğun tahdidi IoT cihaz üreticisinin mi, ASP'nin mi, veya kimindir? Üreticiler IoT cihazlarının sahipleri tarafından nasıl kullanacağını bilemezler. Eğer cihaz bir suça ya da soyguna yardım etmek, suç işlemek veya soygun gerçekleştirmek için kullanılırsa? Eğer bir bilgisayar korsanı bir evin IoT güvenlik sistemini ve video kamera sistemini ele geçirirse ve daha sonra evin sahipleri evde yokken bu evi soyarsa, bu soygundan ve mal kaybından kim sorumludur? Eğer güvenlik açığı olan bir IoT cihazı diğer BT sistemlerini (IT systems), uygulamaları ve veriyi ele geçirmek için kullanılırsa? Bu örnekler, IoT cihazlarını kullanarak gerçek hayatta karşılaşılabilecek potansiyel sorumlulukları göstermektedir. Mevcut sorumluluk kanunları ve koruma, kamuya açık internete bağlı olan IoT cihazlarını kapsamayabilir. Biz bu yasal ve mevzuata uygunluk eğrisinden nasıl uzak durabiliriz? Bu kolay bir görev değildir. IoT cihazlarının ve gerçekleştirimlerinin hukuki etkilerini değerlendirmede öncelikle kişilerin mahremiyet haklarının ele alınması gerekmektedir. Bu durumu, IoT cihaz üretimi ve çözümlerinde yer alan işletmelerin sorumluluk bakış açısından neyin kabul edilebilir ve neyin kabul edilemez olduğunun anlaşılması izlemelidir.

E-ticaret ve Ekonomik Kalkınma Sorunları

IoT, internete bağlanmaya çalışan az gelişmiş ülkeler için e-ticareti ve ekonomiyi etkinleştiricidir. IoT teknolojisinin, ülkeleri e-ticarete hazır uluslara dönüştürmesi nedeni ile gelişmekte olan ekonomiler üzerinde önemli bir etkisi vardır.

IoT'yi bünyesinde barındıran endüstriyel ve kritik altyapı çözümleri, az gelişmiş ülkelerin küresel internet ve e-ticaret varlığını arttırmasına yardımcı olabilir. Bu durum, tarımı, enerjiyi, su seviyelerini, endüstrileşmeyi, çevresel ve doğal kaynakların yönetimini izleyen kritik IoT altyapı çözümlerinin gerçekleştirimini içermektedir. IoT, şehirlere, ülkelere, ve ekonomik gelişimini ve büyümesini hızlandırmak için kritik altyapı teknolojileri dağıtan ülkelere yardımcı olabilir.

Gıda, su, tarım, ve çiftçilik, IoT cihazları ve sensörler tarafından desteklenmekte, ve ülkelerin tarım ve gıda işleme için yeni altyapılar kurmalarında yardımcı olmak üzere izleme yapılmaktadır.

İlerlemeyi takip etmek ve izlemek için IoT'yi kullanmak, kritik bir altyapı oluştururken halkları ve işletmeleri için temel gereksinimleri sağlarken hükümetler için uygulanabilir bir çözümdür. Aşağıda IoT'nin ülkelere getirdiği e-ticaret ve ekonomik kalkınma örnekleri verilmektedir.

- **Altyapı kaynakları:** Bir ülke içerisinde IoT'nin kurulumunda temel olarak bir iletişim altyapısına ve genişbant internet ağına ihtiyaç vardır. Bu, küresel pazarda IoT cihaz bağlanabilirliği ve iletişimi için temel yapıdır.

IoT Kritik Altyapısı

Yeni bir su tedarik yönetim sistemi gerçekleştiren ülkeler taze su tedariklerinin sağlandığından ve su tedariklerinin ihtiyacı olan kişilere ulaştığından emin olmak için uygun bir sensör izleme ve takibine ihtiyaç duymaktadır. Tarım ve çiftçilik sulamaya bağlıdır ve IoT'den faydalanabilir. Sensörler, gerçek-zamanlıya yakın veriyi su yönetim sistemine ve personele sağlayarak hem su tedariklerini hem de suyun kalitesini izleyebilmektedir. Bu IoT altyapısını tüm bölgenin taze su tedariğini yönetmek için kullanmak uygun nüfus ve zirai büyümeyi destekleyebilir. Su yönetimi için bir kez gerçekleştirildiğinde, diğer benzer kritik altyapı servisleri (örneğin, atık su yönetimi vb.) benzer gerçekleştirim yolunu izleyebilir. Bu IoT temeli ülkenin ekonomik kalkınmasını ve e-ticaret yol haritasını destekleyebilir. Tarım ve diğer doğal kaynaklar, ülkenin IoT ve uluslararası ticari e-ticaret stratejisinin bir parçası haline gelebilir. Doğal kaynaklar, su, tarım, doğal kaynaklar ya da mineraller vb. gibi ne olursa olsun, IoT temel yapısı ülkenin ekonomik kalkınmasına ve e-ticaret stratejisine yardım edebilir.

- **Temel Yatırımlar:** Kritik altyapılara yatırım yapmaya yönelen ülkeler, dağıtımları hızlandırma ile ilgili mevzuat ve yasal sorunlar ile uğraşan diğer ülkelerden öne sıçrayabilir.
- **Teknik ve endüstriyel gelişim:** Yeni teknolojilerin ve ekonomik çözümlerin interneti ve IoT'yi anahtar bir ekonomik sürücü olarak kullanması için yeni yeteneklere ihtiyaç duyulmaktadır: IoT teknolojisi ve endüstri birlikte çalışabilirliği ve standartlar olgunlaştıkça IoT cihaz dağıtımı, ve kullanıcı ve işletme benimsenmesi de olgunlaşacaktır.
- **Politika ve mevzuat tanımları:** Ülkeler ve gelişen ekonomiler, güvenlik ve mahremiyetin dağıtımın bir parçası haline gelmesine yardımcı olmak için politikalar ve yönergeler oluşturmak ve uygulamak üzere konumlandırılmıştır.

Uluslararası e-ticaret ile uğraşırken diğer hususlar ortaya çıkmaktadır. Yurt dışı ve uluslararası e-ticaret için vergileri ödemekten ve bu vergileri teslim etmekten kim sorumludur? Bu tür sorular, özellikle IoT ülkeler ve uluslararası sınırların ötesine geçtiğinde cevaplara ihtiyaç duymaktadır.

BÖLÜM ÖZETİ

Bu bölümde, iletişimdeki değişimleri ve internetin insanlar ve işletmeler üzerindeki etkisini öğrendiniz. Bu etki bizi IP'ye bağlı herhangi bir cihazın internete bağlanabildiği Nesnelerin İnterneti'ne (Internet of Things - IoT) yönlendirdi. Bu gelişim internet ve onun patlayan büyüme ve popülerliği ile yaratılmıştır. Bu gelişim kişisel ve profesyonel hayatlarımızı ve iş yapma şeklimizi değiştirdi. Daha fazla kullanıcı ve bu kullanıcıların cihazları internete bağlandığında, bilginin IoT evreni üzerinde paylaşımı ve kullanımı için daha fazla imkan vardır. Bu durum, IoT ile insan ve kişisel etkileşimi ve işletmelerin yeni yenilikçi (innovative) ürünler ve hizmetler

sağlayarak uygulama servis sağlayıcılara dönüştüğü IoT ile profesyonel ya da ticari etkileşimi içerebilir.

Bu yeni IoT işletme zorlukları ve sorunları, güvenlik, mahremiyet, birlikte çalışabilirlik ve standartlar, yasal ve mevzuat sorunları ve e-ticaret ve ekonomik kalkınma olmak üzere internet ve IoT'ye bağlı cihazların insan ile etkileşiminin tüm yönlerini içermektedir. Küresel işbirliği ve IoT birlikte çalışabilirlik ve standartlar alanına katılım, IoT sağlayıcılarının, üreticilerinin ve ASP'lerin tümünün geleceğin piyasasına yönelik IoT cihazlarının ve çözümlerinin geliştirilmesi ve gerçekleştirilmesi için ortak bir platformda olmasını sağlayacaktır. Bu küresel işbirliği olmadan, İnternet Topluluğu (Internet Society) tarafından tanımlanan IoT vizyonunun uygulanması zor olacaktır.

ANAHTAR KAVRAMLAR VE TERİMLER

Anything as a Service (AaaS) – Hizmet olarak Herşey
Application service provider – Uygulama servis sağlayıcıları (ASP)
Audio conferencing – Sesli Konferansı
Bring Your Own Device– Kendi Cihazını Getir (BYOD)
Business-to-business – İşletmeden işletmeye (B2B)
Business-to-consumer – İşletmeden müşteriye (B2C)
Collaboration – İşbirliği
Confidentiality, integrity, and availability – Gizlilik, bütünlük, ve kullanılabilirlik (C-I-A)
De-identified data – Kimliksizleştirilmiş veri
Digital media – Dijital medya
End of life – Yolun sonu (EOL)
Federal Financial Institutions Examination Council - Federal Finansal Kurumlar İnceleme Konseyi (FFIEC)
IM chat – Anlık mesajlaşma sohbeti
Internet Engineering Task Force - İnternet Mühendisliği Görev Gücü (IETF)
Internet of Things – Nesnelerin İnterneti (IoT)
Interoperability – Birlikte çalışabilirlik
Metadata – Üst veri
Mobile IP – IP Hareketliliği
Payment Card Industry Data *Security Standard* - Ödeme Kartı Endüstrisi Veri Güvenlik Standardı (PCI DSS)
Privacy – Mahremiyet
Radio frequency identification - Radyo frekansı ile tanımlama (RFID)
Real-time communications – Gerçek zamanlı iletişimler
Search engine optimization – Arama motoru optimizasyonu (SEO)
Security – Güvenlik
Social media – Sosyal medya
Software as a Service – Hizmet olarak Yazılım (SaaS)
Store-and-forward communications – Sakla-ilet haberleşme
Unified messaging – Birleşik mesajlaşma
Video conferencing – Video konferans
Voice over IP – IP üzerinden ses (VoIP)

BÖLÜM 2 DEĞERLENDİRME

1. İnternet açık, tüm gezegen tarafından paylaşılan kamusal bir ağdır. İsteyen herkes bir bilgisayar ve geçerli bir internet bağlantısı ve tarayıcı ile internete bağlanabilir.
   A. Doğru
   B. Yanlış

2. Aşağıda verilenlerden hangileri IoT endüstrisinin üstesinden gelmesi gereken bir zorluktur?
   A. Güvenlik ve mahremiyet
   B. Birlikte çalışabilirlik ve standartlar
   C. Yasal ve mevzuata uygunluk
   D. E-ticaret ve ekonomik kalkınma
   E. Hepsi

3. Hangi fenomen uç nokta cihaza gerçek zamanlıya yakın, yüksek hızlı genişbant bağlanabilirliği sürdürmesine yardım etmiştir?
   A. İnternet bağlantısı
   B. E-posta
   C. VoIP
   D. Sosyal medya paylaşımı
   E. Hepsi

4. Aşağıdakilerden hangisi IoT bağlantılı bir otomobil gerektirir?
   A. Ev kontrolleri ve sistemleri için gerçek zamanlıya yakın erişim
   B. GPS konum bulma uygulamaları üzerinden çocuklarınızın nerelerde olduğunu izleme kabiliyeti
   C. Faturaları zamanında ödemeyi hatırlatan gerçek-zamanlı alarmlar
   D. Direk teslimatlı online e-ticaret ve online alışveriş
   E. Trafik durumu için gerçek-zamanlı güncellemeleri sağlayan trafik izleme sensörleri

5. Aşağıdakilerden hangisi IoT'nin ticari hayatlarımıza etkilerindendir?
   A. E-ticaret
   B. Sipariş girişi ile entegre tedarik zinciri
   C. Şirketler artık gerçek zamanlı güncellemeler ile ürünler ve servisler için teslimat servisleri önermektedir
   D. Tüketicilere online olarak ürün ve servis yorumlarını sağlayan ve müşteri memnuniyeti hakkında daha fazla bilgi veren müşteri yorumları
   E. Hepsi

6. Aşağıdakilerden hangisi uzaktan çalışmaya yardım etmektedir?
   A. Mevcudiyet/kullanılabilirlik
   B. Anlık mesajlaşma
   C. Video konferans
   D. İşbirliği
   E. Hepsi

7. Aşağıdakilerden hangisi IoT dağıtımlarının üstesinden gelmesi gereken bir güvenlik zorluğudur?
   A. IP trafik hareketliliğinin tıkanması
   B. Diğer IoT cihazlarıyla güvenli iletişim
   C. Bir güncelleme mesajını gönderemeyen bir IoT cihazının sorumluluğu
   D. IoT cihazlarında yazılım lisansının fiyatlandırılması
   E. Mahremiyet verisinin kullanımı paylaşım anlaşması

8. Birleşik mesajlaşma kullanıcılar için hareket halindeyken hangi işlevleri sağlamaktadır?
   A. Ses dosyalarına dönüştürülen ve yolda iken oynatılması için kullanıcının posta kutusuna e-posta olarak gönderilen ses mesajları
   B. Birden çoka *(one-to-many)* iletişimler
   C. Çoktan çoka *(many-to-many)* iletişimler
   D. VoIP iletişimleri ve mesajlaşma
   E. SIP iletişimleri ve mesajlaşma

9. Aşağıdaki uygulamalardan hangisi yüz yüze eğitim ihtiyacını ortadan kaldırabilecektir?
   A. Ses/video konferansı
   B. İş birliği
   C. Anlık Mesajlaşma
   D. Mevcudiyet/Kullanılabilirlik
   E. Hepsi

10. E-ticaret sistemleri neden en gelişmiş güvenlik önlemlerine ihtiyaç duymaktadır?
   A. PCI DSS standardıdır.
   B. Kişisel müşteri verileri web sitelerine girilmektedir.
   C. Kredi kartı verisi web sitelerine girilmektedir.
   D. Müşteriyi elde tutma güvenli online alışverişlerde güveni gerektirir.
   E. Hepsi

11. Aşağıda verilenlerden hangisi IoT dağıtımları tarafından çözülmesi gereken bir zorluk değildir?
   A. Güvenlik
   B. Kullanılabilirlik
   C. Yasal ve Mevzuat
   D. E-ticaret ve ekonomik kalkınma
   E. Mahremiyet

12. Genellikle, araştırma amacıyla kullanılacak ya da paylaşılacak veri _____ dir/dır.
   A. Şifrelenmeli
   B. Özetlenmeli
   C. Kimliksizleştirilmeli
   D. Maskelenmeli
   E. Açık metin olarak tutulmalı

BÖLÜM

3

Kötücül Saldırılar, Tehditler ve Güvenlik Açıkları

Bu bölümde **kötücül amaçlı** bir saldırı yapmak için kullanılan yazılım hakkında bilgi edineceksiniz. Bu yazılımlara **kötücül yazılım (*malware*)** denmektedir. Ayrıca saldırıların farklı türlerini öğreneceksiniz. İnternet yeni ve henüz oturmamış bir alandır. Bu alanda bilgilerinizi çalmaya çalışan birçok kötü insan bulunmaktadır. Eğer cihazlarınız veya hassas bilgileriniz İnternete açık ise kayıp veya zarar riskiniz olacaktır. Günlük yaşamınızdan farklı olarak, siber dünyada herkesin uymak zorunda olduğu yasalar yoktur. Size zarar verecek faaliyetler ve hırsızlıklar gündelik olaylardır. Bu tür olaylar şirketleri, kişileri ve hatta devletleri de etkilemektedir. 2014 yılının sonunda Sony Pictures Entertainment'in hacklenmesinde olduğu gibi, bu tür suçlar genelde cezasız kalmaktadır.

Kötücül saldırılar her yıl milyarlarca dolarlık zarara neden olmaktadır. Neyse ki, birçok şirket ve sizin gibi kişiler Bilgi Teknolojileri - BT (*Information Technologies* - BT) varlıklarını saldırılardan korumak için çaba sarf etmektedir. Bu bölümde, güvenlik açıklarını tanımlamayı, kurumunuzu tehditlerden korumayı ve bilgisayarınızı kötücül saldırılardan güvende tutmayı öğreneceksiniz.

3. Bölüm Konular

Bu bölüm aşağıda verilen konuları ve kavramları içermektedir:

- Siber saldırıların küresel kapsamı nedir
- Neyi korumaya çalışıyorsunuz
- Kimi yakalamaya çalışıyorsunuz
- Bilgisayar sistemlerine saldırıda hangi tür araçlar kullanılmaktadır
- Bir güvenlik ihlali nedir
- Riskler, güvenlik açıkları ve tehditler nelerdir
- Kötücül yazılım nedir
- Kötücül yazılım saldırısı nedir
- Sosyal mühendislik saldırısı nedir
- Kablosuz ağ saldırısı nedir
- Web uygulaması saldırısı nedir
- Karşı tedbirler nelerdir

3. Bölüm Hedefleri

Bu bölümü bitirdiğiniz zaman, yapabilecekleriniz:

- Kötücül yazılımları tanımak ve önlemler almak
- Genel saldırıları tanımak, uygun önlemeleri geliştirmek
- Sosyal mühendisliği fark etmek ve risklerini ortadan kaldırmak
- Kablosuz ağlardaki tehditleri ve saldırıları türlerini tanımak
- Web uygulamalarındaki tehditleri ve saldırı türlerini tanımak

Kötücül Faaliyet Artmakta

Muhtemelen siber saldırıların haberlerini izlemiş, TV'de komik reklamlarını görmüş veya gazetelerde manşet başlıklarını fark etmişsinizdir. Bir örnek: Yakın bir zamanda, bir üniversite öğrencisi Amerika Birleşik Devletleri başkan yardımcısı adayının e-posta hesabına sızdığı için 20 yıl hapse çarptırıldı. Benzer bir olayda, bir tekstil firması olan TJX şirketi milyonlarca müşterisinin kredi kartı numarasının çalınmasına neden olduğunu kabul etti. Komik bir ticari reklam filminde saf bir çalışan "zararsız" bir e-posta bağlantısına tıklayarak bütün şirkete bir virüs saldırısı başlatmaktadır. Etrafınızdaki her alanda, bilişim güvenliği çalışanlarının durdurmak zorunda olduğu kötücül saldırıları göreceksiniz. Haberler son zamanlardaki veri ihlalleri ile doludur. Hiçbir şirket veya kişi dijital verilerin veya dijital kimlik bilgilerinin çalınmasının getirdiği risklerden korunmuş değildir.

Bu tür saldırılar habercilerin ve kamunun dikkatini çekse de, çoğu zaman siber saldırıların kurbanları başlarına geleni hiç kimseye duyurmazlar. Dünya genelindeki sistemler her gün tehdit altındadır. Çoğu durumda bu tür saldırılardan haberdar olanlar yalnızca güvenlik uzmanları ve BT çalışanlarıdır. Güvenlik uzmanları, sistemleri tehditlerden korumak ve gerçekleşen kötücül saldırıların etkilerini de hafifletmekle sorumludurlar. Bilgisayar sistemlerini korumanın en etkili yollarından biri sistemdeki açıkların BT altyapısında hızlıca ve etkili bir biçimde giderilmesini sağlamaktır.

TABLO 3-1, Bloomberg Business tarafından Nisan 2013 yılında belirlenen en fazla saldırı gerçekleştiren ilk 10 ülkeyi göstermektedir. 2013 yılında Çin yüzde 41 ile dünyanın en fazla saldırı gerçekleştiren ülkesidir. ABD yüzde 10 ile ikinci sıradadır. Unutmayalım ki, saldırının başlatıldığı yeri bulmak zor olabilmektedir. Özellikle, **botnetler** kullanılıyorsa daha da zor olmaktadır. Botnet, uzaktaki bir bilgisayar korsanının *(hacker)* kontrol ettiği birbirine internet üzerinden bağlı bir grup bilgisayardır. Uzaktaki bilgisayar korsanı başka bir ülkede yaşasa dahi bu botnet ile birbirine bağlı bilgisayarları kullanarak bir saldırı başlatabilmektedir. Bu durumda, saldırıyı gerçekleştireni bulmak ve yakalamak zor olabilmektedir.

NOT

Bazı durumlarda saldırganlar **geçişli erişim** (***transitive access***) kullanarak hedefteki sistemin veya kullanıcının güvenini kazanırlar. Geçişli erişim saldırgan tarafından kullanıldığında, ilk önce hedefteki kişinin güvendiği bir cihaz veya servis ele geçirilir. Bu durumda, hedefteki sistem, kaynak cihazı ya da servisi tanıyorsa ve güveniyorsa yersiz bir güven hissine kapılmaktadır. Saldırganlar güvenilen servis veya cihazdan bir saldırı planlayarak bu güveni kendi çıkarları için kullanırlar.

TABLO 3-1 En fazla saldırı düzenleyen 10 ülke, 2013.

KAYNAK	SALDIRI PAYI (%)
Çin	%41
ABD	%10
Türkiye	%4,7
Rusya	%4,3
Tayvan	%3,7
Brezilya	%3,3
Romanya	%2,8
Hindistan	%2,3
İtalya	%1,6
Macaristan	%1,4

Bloomberg Business Verilerine Göre En Çok Saldırı Düzenleyen 10 Ülke 2013.

Neyi Korumaya Çalışıyorsunuz?

Kısaca, değerli varlıklarınızı korumaya çalışıyorsunuz. Bir **varlık (*asset*)** değer taşıyan herhangi bir şey olabilir. Bir organizasyondaki her şeyin bir değeri olsa da, *varlık* kelimesi genellikle ciddi değeri olan öğeler için kullanılmaktadır. Bir kurumun varlıkları aşağıdakileri içerebilmektedir:

- **Müşteri verisi** – İsim, adres, telefon, sosyal güvenlik numarası (*Social Security Number* – SSN), doğum tarihi, kart sahibinin verileri, korunan sağlık bilgisi kayıtları.
- **BT varlıkları ve ağ altyapısı** – Donanım, yazılım ve hizmetler.
- **Fikri mülkiyet** – Patentler, yazılım kodu, formüller veya mühendislik planları gibi hassas veriler.
- **Mali durum ve mali veriler** – Banka hesapları, kredi kartı bilgileri ve mali işlem verileri.
- **Servis kullanılabilirliği ve verimlilik** – Hesaplama servislerinin ve yazılımlarının insanların ve makinelerin verimliliğini desteklemesi kabiliyeti.
- **İtibar** – Şirket çalışanlarının yasa ve kurallara uyumu (kurumsal uyum) ve marka imajı.

Bu varlık türlerine ayrı ayrı bakalım ve kötücül saldırılara nasıl maruz kalabileceklerini tartışalım.

Müşteri Verileri

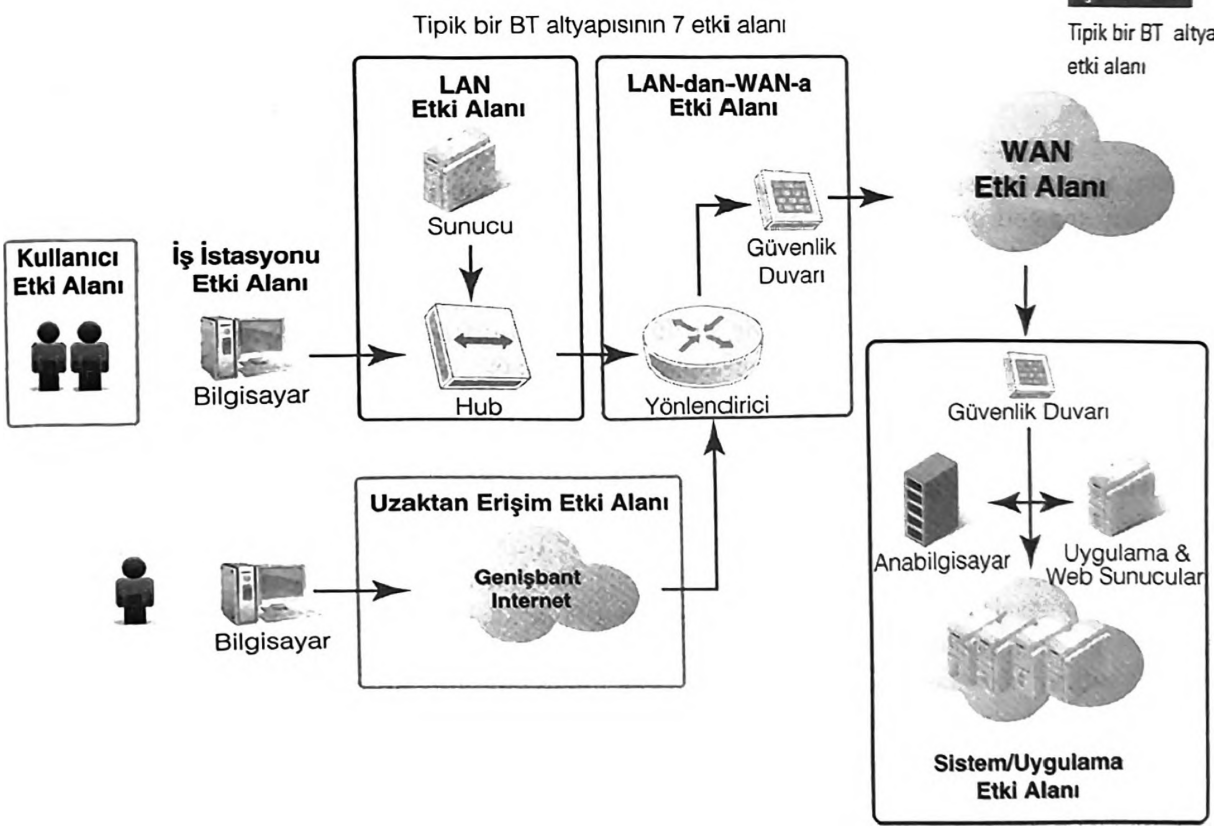
Medya kaynakları bir veri ihlalinde çalınan bilgileri haber yapmayı çok severler. Müşteri kişisel verisinin, kart sahibi bilgilerinin veya elektronik ortamda korunan kişisel sağlık hizmetleri veri unsurlarının kaybolması etkileri nedeniyle kısa sürede manşetlere taşınmaktadır. Günümüzün dijital çağında, müşterinin kişisel verileri başka bir şahıs tarafından çalınmaya ve istismara açıktır. Kimlik bilgileri çalınarak başka bir kişi taklit edildiğinde oluşan duruma **kimlik hırsızlığı (*identity theft*)** denmektedir. Müşteri kişisel verileri müşterinin adı ve soyadı, ev adresi, telefon numarası, doğum tarihi, sosyal güvenlik numarası veya kart bilgilerini içerebilir.

BT ve Ağ Altyapısı

Yazılım ve donanım bir kurumun bilişim altyapısının temel bileşenleridir. **ŞEKİL 3-1** genel bir BT altyapısı çerçevesinin yedi etki alanını göstermektedir. Her etki alanının parçaları bir ağa veya internete bağlanabilir. BT altyapısının internete bağlı olması nedeni ile BT altyapısının hem içerisine hem de dışarısına yönelik tehditler olabilmektedir.

Veriye zarar veren yeni tehditler, **zırhlı virüsler (*armored virüs*), fidye yazılımları (*ransomware*)** ve **kötücül kripto-kilitleyici yazılımlarını (*cryptolocker malware*)** içermektedir; bu zararları düzeltmek veya değiştirmek şirketlere zaman ve maliyete mal olabilir. Zırhlı virüsler, kodlarının tersine mühendislikle (*reverse engineering*) okunmasını ve kötücül yazılım için bir antivirüs oluşturmayı zorlaştıran güçlendirilmiş koda (*hardened code*) sahiptirler. Fidye yazılımları, bir zaman saatiyle bağlantılı yeni bir malware formudur ve kurban kuruluşu verilerinin silinmesini önlemek için fidye ödemeye zorlar. Kripto kilitleyici, deşifreleme (decryption) anahtarlarını elde etmek için kurban fidye ödeyinceye kadar kritik dosyaları veya verileri şifreleyen özel bir fidye yazılımı biçimidir. Kritik donanım ve yazılım sistemlerine yönelik kötücül saldırılar, kuruluşlar içerisinde geniş çaplı sorunlara neden olabilir. Bu sorunlar kritik verilerin kaybolmasını veya mali bilgilerin veya fikri mülkiyetin çalınmasını içerebilir. Korunmayan BT ve ağ altyapısı varlıkları, saldırganlara ve siber suçlulara hassas kaynaklara erişmek için en geniş açıklıkları sunabilir. Bu erişim kolaylığı, internete bağlı varlıkları saldırıların en sık yapıldığı ilk nokta haline getirir. Bu durum, katmanlı bir güvenlik yapısı oluşturmak için en değerli varlıklarınızı BT altyapısının erişilmesi en zor kısımlarına

ŞEKİL 3-1
Tipik bir BT altyapısının yedi etki alanı



koymanız gerektiği anlamına gelmektedir. Katmanlı güvenlik savunmaları yeni, **çok biçimli kötücül yazılımların (*polymorphic malware*)** gelişmişliği göz önüne alındığında kritik bir öneme sahiptir. Çok biçimli kötücül yazılım, şekil değiştirip farklı biçimlere girebileceği ya da değişebileceği için anti virüs ve kötücül yazılımla mücadele uygulamaları ile tespit edilmesi ve temizlenmesi zorlaştığından zararlıdır.

NOT

Şubat 2016'da Hollywood Presbiteryen Kilisesi Tıp Merkezi kripto-kilitleyici kötücül yazılım kullanan bir fidye yazılımının kurbanı oldu. Bir kripto-kilitleyici yazılım kritik önemdeki dosyaları şifreleyerek sistemi kilitler ve şifreleme anahtarını vermek için fidye talep eder. Hollywood şifreleme anahtarını elde etmek için 17000 doları Bitcoin ile ödemeyi seçti. Hastane fidyeyi ödemeye ve normal işlemlerine dönmeye karar verdi. Bu durumda, bir veri ihlali oluşmasa da kritik önemdeki dosyalar şifrelendikleri ve kullanılamaz hale geldikleri için bu olay bütün bilgisayar sistemlerinin kontrolünün tamamıyla kaybedilmesiyle sonuçlandı.

Fikri Mülkiyet

Fikri mülkiyet (*intellectual property*) pek çok kurumun temel taşıdır. Fikri mülkiyet kurumun bir varlığıdır. Bu varlık, özgün bir üretim süreci veya müşteri verisi gibi gerçek bir veri de olabilir. Fikri mülkiyet örnekleri olarak patentler, ilaç formülleri, mühendislik planları, bilimsel formüller ve tarifler verilebilir. Örneğin, bir restoran zincirinin yiyecek hazırlamak ve teslimatı hızlı bir biçimde yapmak için özgün bir sürece sahip olduğunu düşünelim. Eğer piyasadaki rakipleri sahip olunan bu süreci öğrenirlerse, restoran rekabet üstünlüğünü kaybedebilir. Dijital dünyada veri en değerli varlıktır. Ne kadar veriniz varsa o kadar değerlisiniz. Ayrıca, eğer verinizin üst verisi (*metadata*) varsa, verinize ek değer katabilir.

Haber manşetlerinde neler okuyorsunuz? Veri ihlalleri ya da veri kayıpları hayatın her alanında her gün gerçekleşmektedir. Bu tür kayıplar, kimlik hırsızlığı, iş hırsızlığı ya da fikri mülkiyetin çalınmasını içermektedir. Veri ihlalleri sıklıkla gerçekleşmektedir. Bir bilgi sistemleri güvenliği uzmanı olarak göreviniz, varlıklarınızda bir veri ihlali olmasını önlemektir. Bu sizin bir numaralı hedefinizdir.

BT güvenliği açısından temel sorun, fikri mülkiyet hırsızlığından korunmak ve bunun rakiplere ya da kamuya açıklanmasını önlemektir. Fikri mülkiyetin çalınması, kurumun rekabet avantajını etkisiz bir duruma getirebilir. Örneğin, Alpha İlaç Şirketi isimli bir şirketin, piyasaya sürdüğünde 10 milyar dolar kazanmayı hedeflediği yeni bir ilacı 2 milyar dolar yatırım yaparak geliştirdiğini düşünün. Şirket ilacı tam piyasaya sürecekken, Beta İlaç Şirketi'nin Alpha'nın formüllerini ele geçirip kendi versiyonu olan ürünü piyasaya aceleyle sürdüğünü düşünün. Alpha, ARGE yatırımları ve yeni ilaç geliştirmek için önemli meblağlar harcamasına rağmen ilk pazar avantajını kaybedecektir. Fikri mülkiyetin korunması her kurumun en fazla önem verdiği konudur.

Mali Durum ve Mali Veriler

Mali varlıklar her kurumun en önemli varlıkları arasındadır. Bu varlıklar çeşitli biçimler alabilirler. Bunlar; banka hesapları, ticaret hesapları, alım hesapları, şirket kredi kartları ve diğer para ve kredi kaynakları gibi finansal varlıklar olabilmektedir. Alternatif olarak, bu varlıklar gerçek mali varlıklara erişime izin veren veriler de olabilir. Mali veriler, müşteri kredi kartı numaralarını, kişisel mali verileri veya yatırım hesapları ya da bankacılık için kullanılan kullanıcı adları ve parolalar olabilir. Diğer mali veri örnekleri, banka ve şirketlerin kendi aralarındaki finansal veri transferlerinde kullandıkları işlem verisini içermektedir. Bunlar, elektronik ödemeler ya da para transferleri için kullanılan elektronik veri değişimi (*electronic data interchange* – EDI) numaralarını veya otomatik takas merkezi (*automated clearinghouse* – ACH) işlemlerini içerebilmektedir.

Mali varlıkların kötücül saldırılar nedeniyle kaybı tüm kurumlar için en kötü senaryodur. Bu durum sadece fiziksel kayıplara neden olmamakta, ayrıca kurumun şöhretine ve marka imajına da uzun vadeli etkileri olabilmektedir.

Hizmet Kullanılabilirliği ve Verimlilik

Bilgisayar uygulamaları kurumların iş ilişkilerinin yönetiminde yardımcı olan özgün hizmetler sunarlar. Kurum her ihtiyaç duyduğunda bu kritik hizmetlerin kullanılabilir olması önemlidir. Bir hizmetin arıza veya bakımı nedeniyle sunulamadığı süreye *kesinti (downtime)* denir. Kesinti, kasıtlı ya da kasıtsız olabilmektedir. Çoğu zaman, sistem yöneticileri kasıtlı kesintileri önceden

Zengin Ol ya da Uğrunda Öl Operasyonu

Mayıs 2010'da, 28 yaşındaki Albert Gonzalez birçok bilinen perakende firmasının güvenliğini aşarak milyonlarca kredi kartı numarası çaldığı için mahkeme tarafından federal hapishanede 20 yıl hapse çarptırıldı. Gonzalez numaraları çaldıktan sonra, gölge "tarama *(carding)*" web sitelerini kullanarak bu numaraları satıyordu. Basit bir paket koklayıcı *(sniffer)* kullanarak, Gonzalez kart numaraları işlem verisini gerçek zamanlı olarak çalmayı başardı. Daha sonra, kart numaralarını Letonya ve Ukrayna gibi (önceden Sovyetler Birliği'nin parçası olan) ülkelerde bulunan gizli *(blind)* sunucularda tutuyordu. Gonzalez, "Zengin Ol ya da Uğrunda Öl Operasyonu" adını verdiği bu faaliyetlerle, çalınmış kredi kartı bilgilerini satarak müsrif bir hayat tarzının keyfini sürdü. Gizli Servis en sonunda Gonzalez'i izleyerek yakalasa da, "Zengin Ol ya da Uğrunda Öl Operasyonu" iki yıldan fazla sürmüştü. Bu süre içerisinde, TJX, Office Max, Barnes & Noble, Heartland ve Hannaford gibi büyük perakendeciler karşıladıkları zararlar ve ödedikleri tazminatlarla 200 milyon dolardan fazla kayba uğradılar. Bu o zamana dek görülen en büyük bilişim suçları davasıydı.

İlk bakışta "Zengin Ol ya da Uğrunda Öl Operasyonu" kolay karar verilecek bir dava gibi görünüyordu. Bir saldırgan birtakım siber suçlar işledi, güvenlik güçleri saldırganı yakaladılar ve mahkemeler saldırganın cezasını verdiler. Gonzalez hatasının ve suçunun cezasını çekti, kurumlar ve milyonlarca kredi kartı sahibi de adalete kavuştu. Yine de bütün suç siber suçluda değildi. Birçok siber saldırıda, kurban da saldırının başarılı olmasını kolaylaştırmaktadır. Neredeyse tüm siber saldırılar bilinen teknikleri kullanmaktadır ve aslında kurumlar sistemlerini bilinen saldırılardan koruyabilirler. Bir saldırıyı önlemede başarısız olmak, saldırıya davetiye çıkarır.

Bu noktayı vurgulamak için, hissedarlar, banka ortakları ve TJX müşterileri firma aleyhine bir dizi toplu dava açtılar. Bu davalar, TJX'in güvenlik uygulamalarındaki "üst düzey eksikliklerin" Albert Gonzalez ve suç ortaklarının neden olduğu zararlarda şirketi kısmen de olsa sorumlu hale getirdiğini iddia ediyordu. Dava dosyaları, örneğin, Gonzalez'in TJX ağına yerleştirdiği paket yoklayıcısının yedi aydan fazla bir süre fark edilmediğini belirtiyordu. Dava dosyaları ayrıca, TJX'in, kendi yüksek hızlı ağı kullanılarak TJX'in sunucularında saklanan 80 GB büyüklüğünde verinin taşınmasını fark etmediğini belirtiyordu. Son olarak, TJX'in ödeme kartı işleme ortakları tarafından yapılan bir denetim, TJX'in güvenli ödeme kartı işlemleri için 12 gereksinimden dokuzuna uymadığını buldu. TJX'in temel bilgi güvenlik politikaları o kadar etkisizdi ki, şirket Gonzalez'e tek suçlama dahi yapamadı ve sonrasında şirkete acılan davalardan birkaçında uzlaşma yoluna gitti.

Dava sürecinde ihlallerin boyutu ile ilgili ayrıntılar ortaya çıkınca, TJX müşterilerin ve medyanın giderek artan öfkesine maruz kaldı. TJX'in ihlali öğrenmesi ile kamuya bildirmesi arasında yaklaşık altı hafta olduğunu öğrenen müşteriler kızarak tepki gösterdiler. Haber kanalları TJX'i bilgisiz ve ilgisiz bir şirket olarak gösteren hikâyeler yayınladılar. Tüketici örgütleri insanları açık bir şekilde TJX mağazalarında alışveriş yapmamaları konusunda uyardılar. Zengin Ol ya da Uğrunda Öl Operasyonunun ardından TJX'in itibarı ve marka imajı yıprandı. Sonuçta, Zengin Ol ya da Uğrunda Öl Operasyonundan alınacak asıl ders, suçun kendisi değil de, aciz bir güvenlik politikasının suçun ilk etapta işlenmesinde nasıl da asıl sorumlu olduğudur.

planlarlar. Örneğin, sunucular işletim sistemi güncellemelerine veya yamalarına ihtiyaç duyduğunda, sistem yöneticileri sunucular üzerinde ilgili işlemleri problem çıkarmadan gerçekleştirebilmek için sistemleri kasıtlı olarak çevrim dışı *(offline)* duruma getirirler. Yöneticiler kasıtlı kesintiyi planladıklarında, bu planlamanın kurumdaki etkisini en aza indirmeye çalışırlar. Sistem yöneticileri kesintinin etkisini, işletmenin kritik işlemlerini aksatmayacak şekilde yönetmeye çalışırlar. Siz de, örneğin kritik bir yazılımın hafta sonu güncellenmesi ya da e-posta sistemleri gibi sistemlere yamaların gece yarısı uygulanması gibi kasıtlı kesinti senaryolarını biliyorsunuzdur.

Kasıtsız kesinti genellikle teknik arızalar, insan hataları veya saldırılar nedeniyle oluşmaktadır. Teknik arıza ve insan kaynaklı hatalar kasıtsız kesintinin en yaygın nedenleridir. Kötücül saldırılar nedeniyle oluşan kesinti daha az yaygın olsa da, araştırmalar bu saldırıların hızla arttığını göstermektedir. Kötücül saldırılar BT altyapısının yedi etki alanından herhangi birinde gerçekleşebilir ve kesintiye neden olabilir. Kötücül saldırılar genellikle, Kullanıcı, iş istasyonu, LAN ve LAN-dan-WAN-a etki alanlarını hedeflemektedirler.

Fırsat maliyeti (*opportunity cost*) bir şirketin kesinti nedeniyle kaybettiği para miktarıdır. Kesinti ister kasıtlı ister kasıtsız olsun, her iki türlü de sistem kullanılabilirliğini etkilemektedir. Bazı kurumlar fırsat maliyetine **gerçek kesinti maliyeti** de **(*true downtime cost*)** demektedir. Fırsat maliyeti genellikle kesinti nedeniyle kurumda yaşanan üretim kaybını ölçmektedir. Örneğin, büyük bir hava yolu şirketinin rezervasyon sunucularının çalışmadığını düşünün. Sunucular çalışmadığında, müşteriler bilet alamazlar. Bu kesintinin fırsat maliyetini satılamayan biletlerin toplam ücreti olarak ölçebilirsiniz. Kasıtsız kesintinin fırsat maliyeti genellikle kasıtlı kesintinin fırsat maliyetinden çok daha fazladır. Fırsat maliyeti bilgi güvenliği uzmanları için ciddi bir sorundur. Bu maliyet, siber suçlar ve kötücül saldırılarla mücadelede kaybedildiği tahmin edilen yıllık 1 trilyon doların büyük bir kısmını oluşturmaktadır.

NOT

Bir veri ihlali politikası ve usulü, bir veri ihlalini yönetmek için kuruluşunuzu hazırlayacaktır. Bu tür bir politika, müşteriler, düzenleyici kurumlar ve sigorta şirketleri ile iletişimi içermektedir. Eğer kuruluşunuz yasalara uygunluk gereksinimleri altındaysa, veri ihlali bildirimi için yasal zorunluluklara tabii olabilirsiniz. Hukuk personeli de dahil olmak üzere yönetici kadro, gerçekleşen bir veri ihlali ile ilgili olarak kuruluşun yönetim kuruluna özel tavsiyelerde bulunurlar. Bir veri ihlalinin düzgün bir şekilde ele alınması, ilgili hukuki tavsiyelerle birlikte yapılmalıdır.

İtibar

Bilgi güvenliği uzmanlarının korumaya çalıştıklarının en önemlilerinden biri kurumun itibarı ve marka imajıdır. Güvenlik açıkları ve zararlı saldırılar nedeniyle sahip oldukları varlıklar tehlikeye düşen şirketler kamuoyunda oluşan ciddi olumsuz sonuçlarla karşılaşmaktadırlar. Örneğin, kullanıcı kredi kartı verisinin çalınmasına ve bu verinin uluslararası ölçekte dağılmasına izin veren bir güvenlik açığı şirketin itibarına ve marka imajına ciddi zarar verecektir. Şirket çabucak önlem alsa ve sorunu etkili bir biçimde çözse de, şirkete ve markalarına yönelik kamudaki olumsuz algı uzun süre kalabilecektir. Diğer sonuçların yanı sıra, bu durum, kurumun gelir, net değer ve piyasa değerinde bir düşüşe neden olabilir.

Kimi yakalamaya çalışıyorsunuz?

Popüler kullanımlarda ve medyada, **bilgisayar korsanı (*hacker*)** terimi genellikle bir bilgisayar sistemine yetkilendirilmeden giren birisini tanımlar. Çoğu durumda, bilgisayar korsanı ağ üzerinden ya da bir yazılım çatlağı *(software crack)* yoluyla uzaktaki bir bilgisayarın kontrolünü ele geçirmeye çalışmaktadır. Medya ve kamuoyu ayrıca terörizm, vandalizm, kredi kartı dolandırıcılığı, kimlik hırsızlığı, fikri mülkiyet hırsızlığı veya başka birçok suç biçiminden biri için teknolojiyi kullanmaktan dolayı suçlanan kişileri tanımlamak için *bilgisayar korsanı* terimini kullanmaktadır. Bilgisayar

dünyasında *bilgisayar korsanı* kelimesi genellikle, bilgisayar sistemleriyle ilgili olarak, bir şeyi nasıl değiştireceğini araştırmayı ve öğrenmeyi seven bir kişiyi tanımlamaktadır. Bilgisayar korsanları, iyi ya da kötü, uzman ve tamirci olarak kabul edilmektedirler ancak basının bu terime olumsuz bir anlam yüklemesi nedeniyle bilgisayar korsanları sıklıkla bazı tartışmalara konu olmaktadırlar.

Bu kitap, bilgisayar korsanlarını aşağıdaki gibi sınıflandırarak bu terimle ilgili karışıklığı gidermeye çalışmaktadır:

- **Siyah şapka bilgisayar korsanları (*Black-hat hackers*)** – Bir **siyah şapka bilgisayar korsanı,** teknik hünerlerini göstermek için BT güvenliğini kırmaya çalışmakta ve yetkilendirmesiz olarak sistemlere girmeye çalışmaktadır. Siyah şapka bilgisayar korsanları güvenlik açıklarından yararlanmak için genellikle özel yazılım araçları geliştirmekte ve kullanmaktadırlar. Siyah şapka bilgisayar korsanları genellikle sistemlerdeki açıklardan faydalanmaktadırlar fakat buldukları güvenlik açıklarını genellikle bu sistemlerin yöneticilerine bildirmeye çalışmamaktadırlar. Güvenlik kavramının aksine, bilgi işlem kaynaklarının ücretsiz ve açık olarak kullanılmasını teşvik etme eğilimindedirler.
- **Beyaz şapka bilgisayar korsanları (*White-hat hackers*)** – Bir **beyaz şapka bilgisayar korsanı** ya da **etik bilgisayar korsanı,** güvenlik açıklarını tanımlamak ve sızma testi *(penetration test)* gerçekleştirmek için yetkisi olan bir bilgi sistemleri güvenliği uzmanıdır. Siyah şapka bilgisayar korsanları ve beyaz şapka bilgisayar korsanları arasındaki fark, beyaz şapka bilgisayar korsanlarının güvenlik zayıflıklarını düzeltmek için belirlemesi, siyah şapka bilgisayar korsanlarının güvenlik zayıflıklarını sadece eğlencesine ve bu zayıflıkları kullanmak için bulmasıdır.
- **Gri şapka bilgisayar korsanları (*Gray-hat hackers*)** – Bir **gri şapka bilgisayar korsanı,** bir gün siyah şapka bilgisayar korsanı olabileceği gibi beyaz şapka bilgisayar korsanı da olabilecek, yetenekleri ortalama seviyede olan kişilerdir. Bir diğer ortak tanıma göre, keşfedilen güvenlik açıklarını belirleyen ancak kullanmayan, ancak yine de güvenlik açıklarını açıkça ifşa etmediği için bir ödül bekleyen bir bilgisayar korsanıdır. Bu tip bilgisayar korsanları için ortak-bir tanım bulunmamaktadır.

Bilgisayar korsanları, **kırıcılardan** *(cracker)* farklıdır. Bir kırıcının düşmanca bir niyeti vardır, gelişmiş yeteneklere sahiptir ve mali kazançla ilgilenebilir. Kırıcılar ağlara ve bilgi kaynaklarına yönelik en büyük tehdidi temsil etmektedir. Bu tehditler genellikle dolandırıcılık, veri hırsızlığı, verilerin tahrip edilmesi, erişimin engellenmesi ve diğer kötücül faaliyetleri içermektedir. Bununla birlikte, bilgisayar korsanlarının faaliyetleri de hasar ve kayba neden olabilmektedir.

NOT

Bir başka saldırgan türü **betik keratalarıdır (*script kiddies*).** Bir betik keratası, bilgisayar korsanı olmaya çalışan **özenti *(wannabe)***, herhangi bir yaştaki az yetenekli ya da yeteneksiz bir kişidir. Bu kişi, bir siber saldırı gerçekleştirmek için, gerçekleştirdiği adımların anlamını tam olarak anlamaksızın, sadece talimatları izlemekte ya da "yemek kitabı" yaklaşımını kullanmaktadır.

Saldırı Araçları

Bir kurumun varlıklarını ve BT alt yapısını korumak için saldırganların nasıl düşündükleri konusunda biraz fikir sahibi olmanız gerekmektedir. Bir saldırının nasıl düzenlendiği ve hangi araçların kullanıldığını bilmek bir savunma planı yapmaya yardımcı olacaktır. Aslında, birçok kurum sistemleri üzerindeki zayıflıkları bulmak için saldırganların kullandığı araçların aynısını kullanmaktadır. Kendi sisteminizdeki zayıflıkları saldırganlardan önce bulmak her zaman daha iyidir ancak bu zayıflığı bir an önce gidermek daha da önemlidir.

Bilgisayar suçluları ve siber saldırganlar, kullanılabilir zayıflıkları bulmak için birtakım donanım ve yazılım araçlarını ve asıl saldırıyı gerçekleştirmek için de başka araçlar kullanmaktadır. Bu araçlar ve teknikler aşağıdakileri içerebilmektedir:

- Protokol çözümleyiciler *(protocol analyzers)*
- Port tarayıcılar *(port scanners)*

- İşletim sistemi parmak izi tarayıcıları *(OS fingerprint scanners)*
- Güvenlik açığı tarayıcıları *(vulnerability scanners)*
- İstismar yazılımı *(exploit software)*
- Otomatik numara çeviricileri[1] *(wardialers)*
- Parola kırıcılar *(password crackers)*
- Tuşa basma kaydedicileri *(keystroke loggers)*

Protokol Çözümleyiciler

Bir **protokol çözümleyicisi** (***protocol analyzer***) veya **paket koklayıcı** (***packet sniffer***) (veya sadece koklayıcı), bir bilgisayarın LAN veya kablosuz bir ağda olsun veya olmasın, ağ trafiğini izleyip yakalamasını sağlayan bir yazılım programıdır. Saldırganlar şifreleri ve açık metin verileri yakalayabilmekte ve bozabilmektedir. Protokol çözümleyicileri yazılım, donanım veya hem yazılım hem de donanım birleşimi şeklinde olabilmektedir. Koklayıcılar **karışık modda** (***promiscuous mode***)[2] çalışırlar; bu da her veri paketinin koklayıcı tarafından görülebileceği ve yakalanabileceği anlamına gelmektedir. Koklayıcılar çerçeve *(frame)* ve IP veri paketini çözmekte, şifrelenmemişse verileri açık metin olarak görmenize olanak tanımaktadır.

Port Tarayıcılar

Bir **port tarayıcı** (***port scanner***), IP sunucu cihazları ndaki etkinleştirilmiş açık portları taramak için kullanılan bir araçtır. Bir port numarasını bir hizmetle yaygın şekilde ilişkili bir kanal olarak düşününüz. Örneğin, Port 80 http web trafiği için, Port 21 Dosya Transfer Protokolü *(File Transfer Protocol – FTP)*, ve Port 23 Telnet içindir. Artık RFC 3232 olarak bilinen Yorumlar için İstek (Request for Comments – RFC) 1700, en yaygın TCP/UDP bağlantı noktası numaralarını ve hizmetleri listelemektedir. (Port numaralarının tam listesi için, İnternet Atanan Numaralar Yetkilisi'ne [Internet Assigned Numbers Authority – IANA] bakınız.) Port tarayıcıları, IP sunucu cihazında etkinleştirilen açık portları veya uygulamaları ve hizmetleri tanımlamak için kullanılmaktadır. Bu, saldırgana saldırıda kullanılabilecek değerli bilgiler sağlamaktadır.

İşletim Sistemi Parmak İzi Tarayıcıları

Bir **işletim sistemi parmak izi tarayıcısı** (***Operating System – OS fingerprint scanner***) bir saldırganın bir IP sunucu cihazına değişik türlerde paketler göndererek gelen cevaplardan hedef cihazın işletim sistemini (Operating System - OS) tahmin etmesini sağlayan bir yazılımdır. Ağ protokolleri genel olarak standart olsa da, farklı işletim sistemi satıcıları uygun gördükleri şekilde bunları hayata geçirebilirler. İşletim sistemi parmak izi tarayıcısından gönderilen paketler, iş istasyonlarında, sunucularda ve ağ cihazlarında kullanılan çeşitli işletim sistemlerinden gelen farklılıkları ayırt edecektir. Bir IP sunucu cihazı yanıt verdiğinde, OS parmak izi tarayıcısı hangi işletim sisteminin cihaza yüklendiğini tahmin edebilmektedir. Bir saldırgan, hangi OS ve sürümün yüklendiğini bildikten sonra, uygulanabilir yazılım güvenlik açıklarını ve istismarlarını kullanabilmek için daha fazla şansı olacaktır. Bir yazılım güvenlik açığı *(software vulnerability)*, programdaki bir hata veya zayıflıktır. Bir istismar *(exploit)* saldırganın bir güvenlik açığı bulduğunda yapabileceği bir şeydir.

Güvenlik Açığı Tarayıcıları

Bir **güvenlik açığı tarayıcısı** (***vulnerability scanner***) bir IP sunucu cihazında var olan güvenlik açıklarını tanımlamak ve mümkün olduğunda doğrulamak için kullanılan bir yazılım programıdır. Bu bilgiden, bir güvenlik açığı tarayıcısı veri tabanındaki bilinen yazılım güvenlik açıklarını bulduğu şeyle karşılaştırır. Güvenlik açığı tarayıcısı bilinen tüm yazılım güvenlik açıklarını listelemekte ve bunları kritik, büyük ya da küçük olarak önceliklendirmektedir:

---

[1] *Editörün Notu*: Bir modeme bağlanan telefon numaralarını bulmak için kullanılan, genellikle başkalarının bilgisayarlarına izinsiz olarak girmek isteyen biri tarafından kullanılan bir programdır.

[2] *Editörün Notu*: Ağ kartının çalışma modlarından bir tanesidir. Ağ kartının, hedefi neresi olursa olsun aynı alt ağdaki (subnet) tüm paketlerin bir kopyasını kendi üzerine almasıdır.

Bilinen yazılım açıklarının ve etkilenmelerin tam ve güncellenmiş bir listesi için https://cve.mitre.org adresini inceleyiniz. Yaygın Güvenlik Açıkları ve Etkilenme (*Common Vulnerabilities & Exposures – CVE*) listesi, ABD Ulusal Güvenlik Bakanlığı *(U.S. Department of Homeland Security)* adına, Mitre Şirketi tarafından tutulmakta ve yönetilmektedir. Bu liste günümüzde **Ulusal Güvenlik Açıklar Veri tabanı (*National Vulnerability Database* – NVD)** olarak bilinmektedir.

NOT

NVD (https://nvd.nist.gov), Güvenlik İçerik Otomasyon Protokolü'nü (*Security Content Automation Protocol* – SCAP) kullanarak temsil edilen ABD hükümetinin standartlara dayalı güvenlik açığı yönetim verileri deposudur. Bu veriler güvenlik açığı yönetimi, güvenlik ölçümü ve uyumluluğunun otomatikleştirilmesini sağlamaktadır. NVD, güvenlik kontrol listeleri, güvenlikle ilgili yazılım kusurları, hatalı yapılandırmalar, ürün adları ve etki metrikleri veri tabanları içermektedir.

İstismar Yazılımları

Bir istismar yazılımı (*exploit software*) bilinen yazılım açıklarını, verileri ve kod betiklerini birlikte kullanarak bir IP aygıtındaki veya bilgisayar sistemindeki zayıflıkları istismar eden bir yazılımdır. Bazı tür kötücül amaçları gerçekleştirmek için kullanılabilen bir programdır. Bu kötücül amaçlar, hizmet reddi saldırıları, izinsiz erişim saldırıları, brute-force parola saldırıları (*brute-force password attack*) ve arabellek taşması (*buffer overflow*) saldırılarını içerir. Unutmayınız ki, yazılım güvenlik açıkları sistemde yazılım hatası (*software bug*), arka kapı açığı (*backdoor vulnerability*), kısa süreli program arızası (*glitch*) gibi zayıflıklar yaratmaktadır.

Bir saldırgan güvenlik açıkları değerlendirmesi yaparken ve **izinsiz sızma testi (*intrusive penetration test*)** gerçekleştirirken istismar yazılımlarını kullanacaktır. Güvenlik açığı değerlendirmesi bir açığı belirleyebilir, sızma testi ise bu açığı istismar etmeye çalışarak açığın varlığını teyit edecektir. Bu nedenle, sızma testi kötücül ağ trafiğine neden olur. Sızma testi siyah şapka veya beyaz şapka bilgisayar korsanlarının bir bilgisayar sistemine veya IP cihazına sızmak için gerçekleştirdiği eylemdir. Bu hem sisteme erişimi, hem de siyah şapka bilgisayar korsanlarının çoğunun en çok istediği şey olan veriye erişimi elde etmeye yol açabilir. Bir beyaz şapka bilgisayar korsanı, izin verilirse, keşfedilen bir güvenlik açığının gerçekten var olduğunu ve bunun sistemi kritik bir riske maruz bıraktığını doğrulamak için sızma testi yapabilir. Beyaz şapka bilgisayar korsanı daha sonra sızma testi sonuç değerlendirme raporunun bir parçası olarak maruz kalınan risklerin giderilmesi için yollar önerir.

Otomatik Numara Çevirici

Bir **Otomatik Numara Çevirici (*wardialer*)** telefon numaralarını arayıp karşı tarafta bir bilgisayar bulmaya çalışan bir bilgisayar programıdır. Program otomatik olarak belli bir aralıktaki telefon numaralarını arayarak çalışır. Daha sonra karşı tarafta bir modeme başarıyla bağlanabildiği numaraları kaydeder ve bir veri tabanına girer. Otomatik Numara Çeviriciler dijital telefonların, IP telefonların ve IP üzerinden arayıcı (*Voice over IP* - VoIP) telefonların yaygınlaşmasıyla gittikçe demode olmakta ve ortadan kalkmaktadır. VoIP'den önce, saldırganlar Otomatik Numara Çeviricileri kullanarak özel santrallere (*Private Branch Exchange* - PBX) erişerek çevir sesi almaya ve böylece uluslararası telefonları ücretsiz aramaya çalışırlardı. Ek olarak, bir saldırgan Otomatik Numara Çevirici kullanarak analog modem sinyallerini bulmaya ve uzaktaki bir BT altyapısında bulunan bir sisteme erişim izni almaya çalışır.

Ayrıca, bazı Otomatik Numara Çeviriciler hem bir bilgisayarda çalışan işletim sistemini ayırt edebilir, hem de otomatik sızma testleri gerçekleştirebilir. Bu durumlarda, Otomatik Numara Çevirici önceden belirlenmiş bir listede bulunan yaygın kullanılan kullanıcı adlarını ve şifreleri deneyerek sisteme girmeye çalışır.

Ağa sızmaya çalışan bir saldırgan Otomatik Numara Çevirici kullanarak olası hedefleri belirleyebilir. Eğer program otomatik sızma testi sağlamıyorsa, saldırgan modemi şifresiz kullanıcı adları ile veya kolay kırılacak parolalarla hacklemeye çalışabilir. Bir ağ sistemi yöneticisi ticari bir Otomatik Numara Çevirici kullanarak kurum ağında bulunan izinsiz kurulmuş modemleri tespit edebilir. Bu izinsiz modemler saldırganlara kurumun iç ağına kolay erişim izni sağlayabilir. Bulunup kontrol edilmeli ya da ortadan kaldırılmalıdırlar.

Otomatik numara çevirmek oldukça eski bir yöntem olsa da hala bilgisayara giriş noktaları bulmada faydalıdır. Birçok bilgisayar ağı ve ses sistemi telefon hatlarına bağlı modemlere sahiptirler. Bu modemler çoğu zaman destek hattına doğrudan erişim için veya ağdaki erişim kısıtlamalarını geçmeye çalışan kişiler tarafından takılmışlardır. Bugünün internet ile birbirine bağlı sistemlerinde dahi diğer bilgisayarlardan gelecek çağrılara cevap vermeye hazır bir kaç modem olabilir. Bir bilgisayara modem kullanarak başarıyla bağlanmak kurum ağının diğer kısımlarına da olası bir erişim noktası sağlayacaktır.

Parola Kırıcılar

Parola kırmanın amacı unutulan veya bilinmeyen parolaları bulmaktır. Bir **parola kırıcı (*password cracker*)** iki amaçtan birine hizmet eden yazılım programıdır: **Brute force parola saldırısı (*Brute-force password attack*)** ile bir sisteme izinsiz giriş yapmak veya bir bilgisayar sisteminde kriptografik hash ile kaydedilmiş parolaları geri kurtarmak. **Kriptografik hash** büyük bir miktar veriyi tek bir (uzun) sayıya dönüştüren bir algoritmadır. Matematiksel olarak hashlendiğinde, hash değeri verinin bütünlüğünü (*integrity*) teyit etmekte kullanılabilir. Brute force parola saldırısı denemesinde ise bir saldırgan kırılan (*cracked*) parola sisteme giriş izni verinceye dek her olası karakter kombinasyonunu denemektedir. Sözlük saldırıları (*dictionary attacks*) deneme yanılma saldırılarının bir alt kümesidir. Bir **sözlük parola saldırısında (*dictionary password attack*)**, bilgisayar korsanları gerçek kelimeleri de içeren (saldırının adı da buradan gelir) kısa ve basit birleşimleri denerler çünkü bu tür parolalar çok yaygındır.

Tuşa Basma Kaydedicileri

Bir tuşa basma kaydedici (*keystroke logger*) kullanıcının klavyede bastığı her tuşu bir kayıt dosyasına kaydedebilen bir takip yazılım veya donanımıdır. Tuşa basma kaydedici daha sonra almak için dosyayı yerel dizine kaydedebilir veya belirli bir alıcıya gönderebilir. İşverenler tuşa basma kaydedicilerini çalışanların iş bilgisayarlarını sadece iş amaçlı kullanmalarını sağlamak amacıyla kullanabilirler. Fakat, casus yazılımları da (*spyware*) parola gibi bilgileri bilinmeyen üçüncü kişilere göndermek için tuşa basma kaydedicileri içerebilirler. (Bu bölümün devamında casus yazılımları öğreneceksiniz). Bir donanım parçası olarak, tuş kaydedici kullanıcının klavyesi ve bilgisayarı arasında bağlantı görevi gören pil büyüklüğünde bir cihazdır. Bu cihaz sıradan bir klavye aparatına benzediği için, bir kişinin davranışlarını takip etmek isteyen birinin bu cihazı açıkça görünür bir yerde saklaması kolaydır. Ayrıca, iş bilgisayarlarının klavyeleri genellikle bilgisayarın arkasına takılır, bu kaydedicinin fark edilmesini daha da zorlaştırır. Kullanıcı klavye tuşuna bastıkça, kaydedici her basılan tuşu alır ve bu bilgiyi metin olarak kendi içindeki küçük bir belleğe kaydeder. Daha sonra, tuşa basma kaydedicisini takan kişi geri dönmeli ve cihazın topladığı bilgiye erişmek için cihazı fiziksel olarak kaldırmalıdır.

Bir tuşa basma kaydedici yazılım programı genellikle kötücül Truva atı (*Trojan*) programları gibi gizlenir. Bu zararlı yazılım bir URL adresi, PDF dosyası veya ZIP dosyası ile hedefe iletilebilir. Saldırgan bir bilgisayara ağ üzerinden erişebildiği sürece, yürütülebilir (*executable*) dosyalar da dâhil olmak üzere her dosyayı transfer edebilir. Çoğu saldırgan sosyal mühendislik (*social engineering*) kullanarak kullanıcıları bu indirilen programları çalıştırmaya ikna eder. Kullanıcıların kendileri de farkında olmadan tuş kaydedicileri casus yazılımlar olarak indirebilirler ve bunlar daha sonra saldırganlar tarafından rootkit'in bir parçası olarak çalıştırılabilirler. (Rootkitler hakkında bu bölümün devamında daha fazla bilgi edineceksiniz.) Tuşa basma kaydedici program bir kullanıcının her bastığı tuşu kaydeder ve periyodik olarak bu kayıt bilgisini programı kuran kişiye internet üzerinden gönderir.

Güvenlik İhlali Nedir?

Bilgisayarları saldırılardan korumak için atılan en girişken adımlara rağmen, saldırganlar bazen başarılı olabilirler. Gizlilik (*confidentiality*), bütünlük (*integrity*) ve kullanılabilirlik (*availability*) prensiplerinden herhangi birinin ihlaline neden olan her olay bir **güvenlik ihlalidir (*security breach*)**. Bazı güvenlik ihlalleri sunulan hizmetleri kasten sekteye uğratır. Bazıları ise kaza sonucudur ve yazılım veya donanım arızaları nedeniyle oluşur. Bir güvenlik ihlali ister kaza sonucu ister kötücül olsun, bir kurumun hem iş yapabilme kabiliyetini hem de güvenilirliğini etkiler.

Güvenlik ihlallerine neden olabilecek olaylar aşağıdakileri içerir:

- Hizmet reddi *(Denial of Service – DOS)* saldırısı
- Dağıtık hizmet reddi *(Distributed Denial of Service – DDOS)* saldırısı
- Web'de uygunsuz gezinme davranışları
- İzinsiz dinleme *(Wiretapping)*
- Arka kapı (*backdoor*) kullanarak kaynaklara erişim
- Kaza sonucu oluşan veri değişiklikleri

Hizmet Reddi Saldırıları

Hizmet reddi (*Denial of Service* - DOS) saldırıları sistem kesintisi (*downtime*) veya bir kullanıcının sisteme erişememesi ile sonuçlanır. DOS saldırıları bilişim sistemleri güvenliğinin hizmet kullanabilme ilkesini etkiler. Bir DOS saldırısı büyük miktarda gereksiz işler yaptırıp bir bilgisayarı meşgul tutarak kullanılmasını engelleyen koordine edilmiş bir saldırıdır. Bu gereksiz ve fazla iş, sistemin asıl yapması gereken işleri yapamamasına neden olur. Bir disk dolduğunda, sistem kullanıcıya hesabını açtırmadığında, bir bilgisayar çöktüğünde veya bir işlemci çok fazla yavaşladığında bunun sonucu hizmet reddidir, saldırının adı da buradan gelir. Hizmet reddi saldırıları genelde tek bir bilgisayardan başlatılır. Bir hizmet reddi saldırısını tespit edince, kolayca durdurulabilirsiniz.

İki yaygın hizmet reddi saldırı türü şunlardır:

- **Mantık saldırıları (*Logic attacks*)** – Mantık saldırıları yazılım hatalarını kullanarak uzaktaki sunucuların performansını ciddi olarak azaltır veya çökertir. Bu tür saldırıların çoğunu kullandığınız yazılımı en son yamaları yükleyip güncel tutarak engelleyebilirsiniz.
- **Taşkın saldırıları (*Flooding attacks*)** – Taşkın saldırıları kurbanın bilgisayarının işlemcisini, belleğini veya ağ kaynaklarını büyük sayıda gereksiz istek göndererek sıradan isteklere cevap veremez hale getirir.

DOS saldırılarına karşı en iyi savunmalardan biri saldırı önleme sistemi *(Intrusion Prevention System - IPS)* yazılımlarını veya cihazlarını kullanmaktır. Saldırı tespit sistemleri *(Intrusion Detection System - IDS)* yazılım ve cihazları ayrıca hizmet reddi saldırılarını tespit edebilir ve bu tür saldırılar gerçekleşirken sizi uyarırlar. Bir önlem alınmazsa, hizmet reddi saldırıları kısa sürede sunucuları, masa üstü bilgisayarları ve ağ donanımını boğabilirler ve kurumunuzdaki bilişim hizmetlerini durma noktasına getirebilirler. Bazı durumlarda, bu saldırılar bütün alt yapıyı felç edebilirler.

Çoğu DOS saldırıları bir yazılım hatası veya güvenlik açığından ziyade genel sistem mimarisindeki zayıflıkları hedef alırlar. Saldırganlar TCP ve ICMP *(Internet Control Message Protocol)* gibi yaygın kullanılan internet protokollerini kullanarak hizmet reddi saldırılarını başlatabilirler. Bu protokollerden birini kullanarak başlatılan hizmet reddi saldırıları bir veya daha fazla ağ sunucusunu ve cihazını gereksiz veri paketleri ile boğarak ve ağ hizmetlerinin durumu hakkında yanlış bilgiler sağlayarak çökertebilirler. Buna *paket taşkını (packet flood)* denir.

Paket taşkını başlatmanın popüler bir yolu **SYN taşkınıdır (*SYN flood*)**. SYN başka bir cihazla TCP/IP iletişimi başlatmak için kullanılan bir TCP kontrol bitidir. Normalde, bağlantı kurmak için SYN bitini alan cihaz (hem SYN hem de ACK bitleriyle) hemen cevap verir ve teyit bekler. Bir SYN taşkınında, saldırgan hedefteki bilgisayara bağlanmak için çok fazla bağlantı isteği gönderir fakat, ACK biti asla alınmaz. Hedef bilgisayar her gelen isteği kaydeder ve belleğindeki bir yerel bağlantı tablosunda bağlantı için bir yer ayırır. Hedef bilgisayar daha sonra teyit için saldırgana geri mesaj gönderir ama saldırgan teyidi aldığını asla bildirmez. Bellekte kaydedilen bütün bu bitler çok küçüktürler, ama zaman geçtikçe birikirler ve sonunda bağlantı tablosunu saldırının kurbanı olan bilgisayarın belleğinde başka işlemler için yer kalmayıncaya dek doldururlar. Bu sırada, gerçek kullanıcılar hedefteki bilgisayara bağlanamazlar çünkü SYN taşkını bağlantı tablosunu doldurmuştur. Saldırının kurbanı olan bilgisayar var olan bağlantı istekleri zaman aşımına uğrayıncaya dek devre dışı kalır.

Bir başka popüler teknik **smurfing**'dir. Smurfing saldırısı hedefteki bilgisayarda ağ trafiği baskını yaratmak için doğrudan yayın (*direct broadcast*) kullanır.

Hem iç hem de dış saldırganlar hizmet reddi saldırıları başlatabilirler. Yine de, saldırıların çoğu bilinmeyen dış kaynaklardan gelir. Ağa sızmayı engelleme sistemleri (IPS/IDS) genellikle bu saldırıları tespit etmekte etkilidirler.

NOT

RFC 2827 güvenlik yöneticileri için faydalı bir bilgi kaynağıdır. RFC 2827 gelen trafiği filtrelemeyi kullanarak çoğu zaman sahte IP adreslerini kullanan hizmet reddi saldırılarını önlemek için bir metot sunar.

Güvenlik çalışanları saldırganların kendi sistemlerini kötücül amaçlarla kullanamamalarını sağlamak için düzenli olarak agresif tedbirler almalıdır. Ayrıca, artık bazı web içerik sağlayıcıları ve ağ cihazı üreticileri temel yapılandırma tablolarında DOS saldırılarını engellemek için tasarlanmış yeni kurallar bulundurur. Saldırganların bilgisayarlarınıza erişmelerini engellemek tüm zamanınızı alabilir, fakat bu sarf edilen çabaya değecektir.

Dağıtık Hizmet Reddi Saldırıları

Dağıtık hizmet reddi saldırısı (*Distributed Denial of Service Attacks* - DDOS) kullanıcının sisteme erişebilmesini de etkileyen bir hizmet reddi saldırısı türüdür. Bir DDOS saldırısı bilgisayarları aşırı yükler ve gerçek kullanıcıların erişimini engeller. DDOS saldırıları hizmet reddi saldırılarından kapsam olarak ayrışır. DDOS saldırısında saldırgan internete bağlı yüzlerce hatta binlerce bilgisayarı ele geçirip bu sistemlere otomatik saldırı birimleri yükler. Saldırgan daha sonra birimlere bir hedef sitesini sahte mesajlarla boğmaları talimatını verir. Bu mesajlar siteyi aşırı yükler ve asıl trafiği engeller. Burada asıl nokta saldıran birimlerin sayısıdır. Saldırgan saldırıyı birçok bilgisayara dağıtarak daha fazla zarara neden olur.

Büyük şirketler ve üniversiteler DDOS saldırıları başlatan saldırganların cazip hedefleridir. Araştırmacıların tahminlerine göre saldırganlar ağlara her hafta binlerce DDOS saldırısı başlatırlar. Bu tehdit o kadar ciddidir ki bu saldırıları durdurmak güvenlik ürünleri üretenler de dâhil olmak üzere birçok şirketin ilk önceliğidir. DDOS saldırılarını durdurmak DOS saldırılarını durdurmaktan daha zordur çünkü farklı kaynaklardan gelirler. Bilgisayarları DDOS saldırılarından korumak farklı güvenlik seviyeleri gerektirir. Hem hizmet reddi hem de DDOS saldırıları birçok biçimde ve değişik şiddet seviyelerinde olabilirler ve milyonlarca dolarlık gelir kaybına neden olabilirler.

Web'de Uygunsuz Gezinme Davranışları

Kurumun kabul edilebilir kullanım politikasının *(Acceptable Use Policy – AUP)* ihlal edilmesi, mesela bir çalışanın web'de uygunsuz sitelerde gezinmesi, kendi başına güvenlik ihlali olabilir. Kurumlar

hangi davranışların kabul edebilir hangisinin kabul edilemez olduğunu açıkça ifade eden bir kullanım politikasına (AUP) sahip olmalıdırlar. Kabul edilemez kullanım, yetkisiz kullanıcıların okumamaları gereken veri veya bilgiler için dosyaları veya dizinleri aramalarını veya basitçe, yasak web sitelerini ziyaret etmelerini içerebilir. Kurumun kabul edilebilir kullanım politika belgesi güvenlik ihlaline neden olan eylemleri listeler.

İzinsiz dinleme

Saldırganlar telefon ve veri iletişim hatlarına gizlice girebilirler. **Telefon dinleme (wiretapping), saldırganın hatta değişiklik yapması durumunda aktiftir. Yetkilendirilmemiş bir kullanıcının, içeriği değiştirmeden yalnızca iletimi dinlemesi durumunda ise pasif olabilir.** Pasif dinleme *(passive intrusion)*, daha sonra gerçekleşecek aktif bir saldırı için verinin kopyalanmasını da içerebilir.

Aktif dinlemenin iki yöntemi aşağıdaki şekildedir:

- **Hatlar arasında dinleme (*Between-the-lines wiretapping*)** – Bu tür dinleme gerçek kullanıcıların gönderdiği mesajları değiştirmez fakat kullanıcı duraksadığında iletişim hattına ilave mesajlar sokar.
- **Hattı değiştirerek dinleme (*Piggyback-entry wiretapping*)** – Bu tür dinleme iletişim hattına girerek orijinal mesaj yakalar ve değiştirir ve mesajı sunucu (host) gibi davranan başka bir bilgisayara gönderir.

İzinsiz dinleme genellikle ses ve telefon dinlemesi ile ilişkilendirilse de, saldırganlar iletişim hattını veri iletişimini yakalamak için de kullanabilirler. Veri iletişimin yakalanması, yine de, daha çok koklama (*sniffing*) olarak adlandırılır (yine de Sniffing basit izinsiz dinlemeden öte, kablosuz iletişimin yakalanmasını içerir).

Arka Kapılar

Yazılım geliştiriciler, programlarında bazen **arka kapı (*backdoor*)** adı verilen gizli erişim metotları bulundururlar. Arka kapılar geliştiricilere ve destek personeline güvenlik kontrolleri ile uğraşmadan sisteme kolay giriş izni sağlarlar. Fakat sorun şu ki arka kapılar her zaman gizli kalmazlar. Bir saldırgan bir arka kapıyı keşfettiğinde, bunu kullanarak parolalar, şifreleme vb. var olan güvenlik mekanizmalarını atlatarak sisteme girebilir. Gerçek kullanıcılar kullanıcı kimliği ve parola kullanarak sisteme girerken saldırganlar arka kapıları kullanarak normal erişim kontrollerini sorunsuz geçerler.

Saldırganlar bir sistemin güvenliğini sisteme kendi arka kapı programlarını kurarak da tehlikeye atabilirler. Saldırganlar bu tür arka kapıları yöneticilerin bir bilgisayar sistemini korumak için koydukları kontrolleri aşmak için kullanırlar. **Netcat** adı verilen program günümüzde en çok kullanılan arka kapı araçlarından biridir.

Rootkitler normal denetim metotlarından saklanabilmeleri için tasarlanan kötücül yazılım programlarıdır. Bunlar bir saldırganın bir bilgisayar sistemine erişebilmesini sağlarlar. Saldırganlar root yetkisine veya sistem yöneticilerinin erişim yetkilerine sahip olunca rootkitler kurarlar. Geleneksel rootkitler kritik programları değiştirerek saldırganlara arka kapı erişimi verirler ve saldırganların sistemde gizlenebilmelerini sağlarlar. Şirketin yazılım bileşenlerinin yerini aldıkları için rootkitler uygulama seviyesindeki Truva atı arka kapılarından daha güçlüdürler. Rootkitler hakkında bu bölümün sonunda daha fazla bilgi alacaksınız.

> **NOT**
>
> Neredeyse bütün ağ cihazı satıcıları cihazlarını varsayılan bir kullanıcı adı ve parola ile piyasaya sürerler, cihazın kurulumunda bu bilgileri değiştirmeniz gerekir. Yeni cihazların kullanımında bu kullanıcı adı ve parolayı değiştirmeyişiniz sisteminizde herkesin bildiği bir arka kapıya – ciddi bir güvenlik açığına! – neden olur.

Veri Değişiklikleri

Kasten veya kasıtsız olarak değiştirilen veri, bilişim sistemleri güvenliğinin bütünlük (*integrity*) ilkesini etkiler. Bu ayrıca bir güvenlik ihlali olarak kabul edilir. Birden fazla süreç temel veri bütünlüğü koşullarına dikkat etmeden aynı anda veriyi değiştirmeye çalışırsa bitmemiş veri değişiklikleri oluşabilir. Başka bir örnek, veriyi tutacak kayıt alanının yeterince büyük olmaması nedeniyle verilerin bir kısmının kırpılarak kaybedilmesidir. Bu durum, birçok programlama dilinde oluşabilir ve tespiti zordur. Ancak, sonuçları çok önemli olabilir. Veri değişikliği sorunlarından kaçınmanın en iyi yolu veriyi kaydetmeden önce doğrulamak ve kullandığınız programların katı veri bütünlüğü ilkelerine uymalarını sağlamaktır.

Diğer Güvenlik Zorlukları

Güvenli ve emin iletişimi sağlamanın diğer zorlukları spam, hileler, casus yazılımlar ve hatta web tarayıcılarının kaydettiği yerel bilgilerden kaynaklanabilir. Bu zorlukların birkaçının bir arada bulunduğu durumlar da mümkündür.

Spam ve Spim

Spam istenmeyen e-postadır. **Spim** ise istenmeyen anlık iletiler ve chat mesajlarıdır. Çoğu spam ve spim ticari reklamlardır, genellikle kolay yoldan zengin olma teknikleri, ne olduğu belirsiz ürünler ve diğer gereksiz hizmetlerdir. Spam göndermenin maliyeti azdır, çünkü alıcı spamle ilgili giderlerin çoğunu yüklenir. İnternet servis sağlayıcıların ve internetteki hizmetlerin spam iletmesinin bir maliyeti vardır. Çok fazla sayıda istenmeyen mesajla başa çıkmak pahalıdır. İnternet sağlayıcıları bu masrafları kullanıcılara yüklerler. Ayrıca, spam mesajları kullanıcıları aldıkları mesajları inceleyip istenmeyenleri silmek için zaman harcamaya zorlar.

E-posta spam'i ve IM chat spim'i e-posta adresleri ve IM/chat hesapları bilinen kişisel kullanıcıları hedef alır. Çoğu zaman spam ve spim göndericileri özel veya herkese açık tartışma gruplarının e-posta listelerindeki veya IM chat forumlarındaki üyelere mesajlar gönderirler. Spam göndericiler için bir diğer popüler yöntem, yazılım kullanarak bilindik kullanıcı adı ve alan adlarından e-posta adresleri yaratmak ve mesajları bu adreslere göndermektir. Örneğin, bir spam programı mehmet@yahoo.com adresine veya M harfi ile başlayan tüm isimlerin yahoo.com adreslerine e-postalar gönderir. Spim aynı yöntemi takip eder, fakat e-posta değil de anlık ileti mesajları kullanır.

Spam göndericilerin çok kullandığı bir teknik içinde 'abonelikten çık' linki bulunduran bir e-posta mesajını birtakım adreslere göndermektir. Asıl amaç e-posta adresinin kullanımda olup olmadığını bulmaktır. Yani, linke tıklayan kullanıcıları abonelikten çıkarmak yerine, spam göndericiler basitçe hesabın kullanıldığına karar verirler ve hesap daha çekici bir hedef haline gelir. Benzer şekilde, spam üreten yazılımlar genellikle e-posta hesaplarının listelerini tutarlar. Yazılımı üretenler bu adreslerin sisteme isteyerek "üye olan" kullanıcılara ait olduğunu öne sürerler fakat bunlar aslında haber gruplarından ya da mail listelerinden aşırılmış adreslerdir. Spamciler sıklıkla e-posta hesaplarını istek olursa sistemden sildiklerini iddia ederler fakat neredeyse asla silmezler.

NOT

Eğer aldığınız bir mesajın sahtekârlık içerdiğinden şüpheleniyorsanız, Snopes (www.snopes.com) adında bir web sitesini ziyaret ederek mesajı araştırabilirsiniz. Çoğu zaman Snopes'ta size gelen mesajla eşleşen bir başlık bulacaksınız. Snopes her hile hakkında tam bilgiye sahip değildir, fakat araştırmanıza başlamak için uygun bir yol sağlayabilir.

Spam artık sadece can sıkıcı bir detay değil. Spam'i engellemek bilişim güvenliği için kritik önemdedir. Son zamanlarda spam, suçluların kişisel ve şirketlere ait bilgileri elde etmesi ve

Truva atı veya diğer zararlı yazılımları bilgisayarlara yüklemeleri için kullanılan bir yol haline geldi. Üstelik bazı spam türlerini, mesela çocuk pornosu ile ilgili olanları, bulundurmak suçtur.

Siber suçlarla savaşmak için kurumlar spam ile başa çıkmalıdırlar. Bir **oltalama (*phishing*)** e-postası, alıcıyı e-postanın eklerinde gömülü halde bulunan bir URL bağlantısına tıklaması için kandırmaya çalışan sahte veya düzmece bir e-postadır. Daha önceki bölümde de belirtildiği gibi, kötücül yazılımlar, Truva atları ve tuşa basma kaydediciler oltalama e-postalarına gömülmüş olabilirler. Bu e-postayı alan bir kişi farkında olmadan URL bağlantısına tıklayarak veya e-postaya ekli dosyaları açarak kötücül yazılımı etkinleştirebilir. Bu tür olaylarla savaşmak için anti virüs, casus yazılım önleyici ve kötücül yazılım önleyici uygulamalar gerekir.

Aldatmalar

Bir **aldatma (*hoax*)**, alıcıyı kandırmak veya aldatmak için tasarlanan bazı eylemlerdir. Bu bağlamda, aldatmalar genellikle e-posta mesajlarıyla yayılırlar. Çoğu zaman, bu mesajlar çok tahrip edici yeni virüsler hakkında uyarılar içerirler. Bu aldatma mesajları sisteminize virüsler veya Truva atları gibi otomatik olarak bulaşmasa da, bunlarla uğraşmak zaman alıcıdır. Aslında, gerçek virüslerle ve Truva atı olaylarıyla uğraşmaktan daha fazla zamanı bu tür aldatmaların gerçek olmadığını açığa çıkarmak için harcayabilirsiniz.

Aldatmalar ile başa çıkmanın en iyi yolu kullanıcılardan kendilerine gelen mesajları diğer kişilere iletmemelerini istemektir. Size gelen şirin bir mesajı bir veya iki arkadaşınıza göndermeniz sorun olmaz. Fakat doğruluğu belli olmayan bir uyarıyı ya da yardım isteğini adres defterinizdeki herkese göndermek ve alıcılardan da bu mesajı *kendi* adres defterlerindeki herkese göndermelerini istemek, zaten herkesin gelen kutusunu gereksiz yere dolduran kargaşayı daha da artıracaktır. Bu tür e-postaları alan kişiler bildikleri herkese bu mesajları iletmemelidirler.

Çerezler

Bir web sunucuya bir kullanıcının geçmişini izlemede yardımcı olmak için, web tarayıcılar kullanıcının hard diskinde bu web sunucusunun bir çerez saklamasına izin verirler. **Bir çerez (*cookie*)**, geçmişte bir web sitesine yapılan ziyaretlerden edinilmiş ayrıntıları saklayan basit bir metin dosyasıdır. Çerezler değerlidirler çünkü HTTP durumsuz (*stateless*) bir protokoldür, bu nedenle bir veri dosyası çerezi kullanılarak son ziyaretin küçük bir kaydı tutulur. Bu kayıtlar kullanıcının kullanıcı adı, kullanıcının girdiği kredi kartı bilgileri ve benzeri diğer bilgileri içerebilir. Daha sonra, kullanıcı web sunucuya bir istek gönderdiğinde, sunucu kullanıcıdan bilgileri yeniden girmesini istemek yerine çereze erişebilir.

Çerezler bazen tartışmalı bir konudur, çünkü bir web sunucusunun bazı dosyaları kullanıcının hard diskinde kaydetmek için kullanıcının bilgisayarına iletmesine izin verirler. Çerezler yazı dosyaları oldukları için, yine de, genellikle kendi başlarına bir zarara neden olamazlar. Çerezler kendileri doğrudan kötücül eylemlere kalkışamazlar. Çerezler virüsleri yayamazlar veya kullanıcının hard diskindeki diğer bilgilere erişemezler. Yine de bu çerezlerin bir güvenlik sorununa neden olmayacağı anlamına gelmez. Çerezler bir kullanıcının hard diskinden bilgi toplayamasalar da, belirtildiği gibi, bazen kredi kartı detayları gibi mahrem bilgileri kaydedebilirler.

Çerezlerle ilgili asıl problem, bilgiyi şifrelenmemiş metin dosyalarında tutmalarıdır. Bu da bilgisayarınıza erişimi olan herkesin çerezlerinizin içeriğini okuyabilmesi demektir. Bir çerez bir takım kolaylık sağlayabilse de, örneğin daha önce internette aradığınız uçuşları hatırlasa da, sizin mahremiyetinizi de kolayca tehlikeye atabilir. Güvenli bir şekilde tasarlanmış çoğu web sitesi kredi kartı numarası gibi bilgileri asla bir çerezde tutmaz fakat bazı web siteleri özensizdirler. Bilgisayarınızdaki çerezlerde hangi bilgilerin tutulduğunu asla tamamıyla bilemezsiniz. Çerezlerde kişisel bilgilerin tutulmasını engellemenin en iyi yolu sadece güvendiğiniz web sitelerinin çerez bulundurmasına izni vermektir.

Web sitelerinde daha fazla gezindikçe, bilgisayarınızda muhtemelen daha fazla çerez bulacaksınız. Aslında, kullanıcılar bilgisayarlarında yüzlerce çerezle baş başa kalabilirler, bu durum can sıkıcı bir hal alabilir. Neyse ki bu çerezleri istediğiniz an silebilirsiniz. Ayrıca, her şeyden önce web tarayıcınızın çerezlere izin vermesini engelleyebilirsiniz. Talimatlar için tarayıcınızın yardım bilgilerini kontrol ediniz.

Riskler, Tehditler ve Güvenlik Açıkları Nelerdir?

Riskler, tehditler ve güvenlik açıkları beraber oluşurlar. *Risk* kötü bir şeyin gerçekleşme olasılığıdır. Bir *tehdit (threat)* bir varlığa zarar verecek veya tehlikeye atacak herhangi bir eylemdir. Bir *güvenlik açığı/zafiyet (vulnerability)* ise tasarımdaki veya yazılım kodundaki zayıflığın kendisidir. İstismar edilebilecek bir güvenlik açığı bir tehdittir.

Eğer bir sistemde güvenlik açığı varsa, tehdit ihtimali de vardır. Bir açığın getirdiği herhangi bir tehdit olumsuz bir olayın gerçekleşmesi riskini yaratır. Tehditleri tamamen yok edemezsiniz fakat açıklara karşı kendinizi koruyabilirsiniz. Böylece, tehditler hala var olsalar da, güvenlik açıklarını kullanamazlar. Varlıkları saldırı riskinden korumanın kilit noktası mümkün olan en fazla sayıda güvenlik açığını ortadan kaldırmak veya etkilerini gidermektir.

Bir BT altyapısında çok fazla tehdit ve açık bulabilirsiniz. **TABLO 3-2**, BT altyapısının yedi alt etki alanının her birinde bulunabilen bazı yaygın tehditleri listelemektedir.

TABLO 3-2 Bir bilişim altyapısının yedi etki alanındaki yaygın tehditler ve güvenlik açıkları

ETKİ ALANI	YAYGIN TEHDİTLER VE GÜVENLİK AÇIKLARI
Kullanıcı etki alanı	Güvenlik hakkında duyarlılığın veya dikkatin eksikliği Kullanılabilir kullanım politikasının kaza sonucu ihlali Bilinçli yapılan kötücül eylemler Sosyal mühendislik
İş istasyonu etki alanı	İzinsiz kullanıcı girişi Kötücül yazılımların sisteme sokulması Kurulan yazılımdaki zayıflıklar
LAN etki alanı	Yetkisiz ağ erişimi Gizli verilerin şifrelenmeden iletilmesi Kötücül yazılımın yayılması
LAN-dan-WAN-a etki alanı	Dışarıdan ağ içindeki kaynaklara yetkisiz erişim ve temas Kötücül yazılımların sisteme sokulması İnternet bağlantısı olmaması nedeniyle üretim kaybı
WAN etki alanı	Gizli bilgilerin şifrelenmeden iletilmesi Bilinmeyen kaynaklardan gelen kötücül saldırılar Hizmet reddi saldırıları Yazılımda bulunan zayıflıklar
Uzaktan Erişim etki alanı	Sistem erişimine ve gizli bilgilere Brute-force parola saldırıları Kaynaklara uzaktan yetkisiz erişim Uzaktan erişimde veya kaybedilen kayıt cihazlarından verinin sızması (data leakage)
Sistem/Uygulama etki alanı	Kaynaklara yetkisiz fiziksel veya mantıksal erişim (physical or logical access) Sunucu işletim sisteminde veya uygulama yazılımında zayıflıklar Hatalar, yanlışlar ve felaketler sonucu veri kaybı (data loss)

BİLGİNİZE

Tehditleri ve güvenlik açıklarını bulmak ve bunlara cevap vermek karmaşık bir süreç olabilir. Bazı durumlarda, bir tehdidi ortadan kaldırmak çok pahalı veya çok zaman alıcı olabilir. Amacınız mümkün olduğu kadar fazla tehdidin gerçekleşmesini engellemektir fakat ayrıca bazı varlıkları koruma masrafının varlıkların kendi ederinden daha fazlaya gelip gelmeyeceğini dikkatlice değerlendirmelisiniz. Varlıkların gerçek değerinden daha fazla zamanı ve parayı tehditleri fark edip engellemeye harcamamalısınız.

Tehditler bir kişiden, bir grup kişiden veya bir kurumdan gelebilir. İster kasıtsız ister kötücül olsun, bir hesaplama cihazına (*computing device*) yönelen bir tehdit, bir kişinin veya bir kurumun varlık veya kaynaklarına olumsuz etkisi olan herhangi bir eylemdir. Bu varlık bir donanım, yazılım, veri tabanları, dosyalar, veri veya fiziksel ağın kendisi olabilir.

Güvenlik açısından bir tehdit önem arz eder. Bilgisayar güvenliğinin hedefi tehditlerle başa çıkmada gerekli metotları, teknikleri ve tavsiyeleri sunmaktır. Ağ sistemi yöneticilerine, tasarımcılara, geliştiricilere ve kullanıcılara istenmeyen sistem özelliklerinden ve zayıflıklarından kaçınmaları için gerekli olan politikaları geliştirerek bu hedefe ulaşabilirsiniz.

Tehditleri belirleyebilir, önem ve etkilerine göre sıralayabilirsiniz. Tehditleri neden olacakları para kaybı, itibara verecekleri zarar, tazminat ve ne kadar sıklıkla oluşabilecekleri gibi kıstaslarla sıralayabilirsiniz. Her kurum, kurumun yaptığı işe ve bu işe olan etkisine bağlı olarak bir tehdidi diğer bir kurumdakinden daha yüksek veya daha alçak bir sıraya koyabilir.

En yaygın tehditler, özel bir sıralama olmaksızın, aşağıdakileri içerir:

- Kötücül yazılım
- Donanım veya yazılım hatası
- Sistemin içindeki saldırgan
- Cihaz hırsızlığı
- Dışarıdaki saldırgan
- Doğal afet
- Endüstriyel casusluk
- Terörizm

Her tehdit kötücül olmayabilir. Bazı tehditler kasten olsa da, bazıları kaza sonucu oluşabilir. Kaza sonucu oluşan tehditler donanım hatalarını ve denetim eksikliği nedeniyle oluşan yazılım hatalarını içerir. Yine de, bu kaza sonucu oluşan tehditlerin sonuçları kötücül tehditler kadar zarar verici olabilir. İster kaza sonucu, ister kötücül olsun, güvenlik ihlallerini en aza indirmek için her çabayı sarf etmelisiniz. Genel hedefiniz, ağ ve bilgisayar sistemini her tür saldırıdan korumak ve kişilerin veya kurum varlıklarının hırsızlığını, tahribatını ve bozulmasını engellemektir.

Tehditlerin Hedefleri

En çok beğendiği arama motorunu kullanarak, bir saldırgan neredeyse her protokolün, işletim sisteminin, uygulamanın, cihazın veya donanım ortamının güvenliğini aşmak için gerekli yöntemleri bulabilir. Bu nedenle, bütün tehditleri yakından izlemelisiniz. Bir sonraki tehdidin nereden geleceğini asla bilemezsiniz. Saldırgan profesyonel bir siber suçlu veya bulunduğunuz binadaki bir kişi olabilir. En iyi yöntem bütün tehdit hedeflerini düzenli olarak ve dikkatlice izlemektir.

Bir izleme planı oluşturmadaki ilk adım tehdidin bilişim altyapısının yedi etki alanından hangisinde oluşabileceğini belirlemektir. TABLO 3-3, genel tehditleri ve bu tehditlerin bilişim altyapısının neresinde oluştuğunu listelemektedir.

Bu listeden, bir saldırganın büyük sorunlara neden olmak için çok imkâna sahip olduğu açıkça görülmelidir. Ayrıca, çoğu tehdit hedefinin farklı kategorilerde ortaya çıktığını fark etmelisiniz. Bütün etki alanları üzerinde kapsamlı bir güvenlik planının hazırlanmasının gerekliliği açıkça görülmelidir.

Tehdit Türleri

Bilgiyi korumak için, bilginin gizliliğini (*confidentialty*), bütünlüğünü (*integrity*) ve kullanılabilirliğini (*availability*) korumalısınız (CIA). Üç ana tehdit türü bu prensiplerden her birini doğrudan tehdit etmektedir. Bunlar aşağıdaki şekildedir:

- İfşa (*disclosure*) tehditleri
- Değişim (*alteration*) tehditleri
- Hizmet reddi (*denial*) veya tahribat (*destruction*) tehditleri

İfşa Tehditleri

Ağ kaynakları üzerinde tutulan veya ağ kaynakları arasında iletim halinde olan gizli ve mahrem bilgilere yetkisiz kullanıcıların her erişiminde **ifşa (*disclosure*)** oluşur. İfşa, ayrıca tıbbi kayıtlar veri tabanı gibi gizli ve mahrem bilgiler içeren bir cihaz veya bir bilgisayar kaybedildiği veya çalındığı

TABLO 3-3 Bir bilişim altyapısının yedi etki alanındaki tehdit hedefleri.

ETKİ ALANI	TEHDİT HEDEFİ
Kullanıcı etki alanı	Çalışanın kendi karakteri ve davranışı. Kabul edilebilir kullanım politikasının ihlalleri hedeflenir.
İş istasyonu etki alanı	İş istasyonları, diz üstü bilgisayarları, mobil cihazlar ve bunların güvenlik açıkları hedeflenir. Bu bölüm bilişim altyapısına giriş noktasıdır.
LAN etki alanı	Windows Aktif Dizin/Bölüm Kontrolörü, dosya sunucuları, yazıcı sunucuları. Ayrıca, IP veri ağı LAN bölümünün bir parçasıdır ve kimlik ve doğrulama saldırılarının hedefidir.
LAN-dan-WAN-a etki alanı	DMZ VLAN'lar veya adanmış uzaktan bağlantılar genellikle burada sonlandırılır. Dünyaya açık IP cihazları, güvenlik katmanının (perimeter) güvenlik duvarları da (firewall) dâhil olmak üzere, IDS/IPS ve uzaktan VPN sonlandırmaları buradadır.
WAN etki alanı	IP yönlendiricileri *(router)*, TCP IP yığınları ve tampon bellekleri, güvenlik duvarları, ağ geçitleri (*gateway*), anahtar ar (*switch*) ve WAN servis sağlayıcıları hedeftirler.
Uzaktan Erişim etki alanı	Sanal özel ağ (Virtual private network - VPN), iki faktörlü kimlik denetleme (*two-factor authentication*), mobil ve uzaktan çalışanlar için erişim sistemleri genellikle desteklenir ve hedeftir.
Sistem/Uygulama bölümü	Web ve uygulama sunucuları, işletim sistemleri ve uygulamaları. Mahrem veriler içeren arka-uç (*back-end*) veri tabanı sunucuları ve veri tabanı tabloları hedeftir.

durumlarda oluşabilmektedir. Saldırganların yasadışı olarak veriyi elde etmek veya değiştirmek için kullandıkları iki teknik aşağıdaki gibidir:

- **Sabotaj (*Sabotage*)** – Sabotaj mala zarar verilmesi veya normal hizmetlerin engellenmesidir. Teknik olarak, sabotaj bilişim güvenliğinin hizmet sunabilme ilkesine saldırır.
- **Casusluk (*Espionage*)** – Casusluk bilgileri, genellikle başka bir devlete yardımcı olmak için, çalma eylemidir. Teröristler ve düşman güçleri aynı zamanda mahrem devlet bilgilerini gelecekteki ataklarında kullanmak için çalmaya kalkışabilirler.

> **NOT**
>
> *Bilgi sızması (information leak)* bir kişinin gerekli yetkiye sahip olmaksızın bilgiyi kasten başkalarına dağıttığı her durumdur.

Sabotaj sessiz bir saldırı değildir fakat casusluk hiçbir görünür iz bırakmadan yapılabilir.

Çoğu kurumda, kaydedilen bilginin çok büyük bir kısmı kamuya açık değildir. Bu bilgi, kullanıcının bilgisayarında bulunan kişisel bilgileri veya büyük bir veri tabanında saklanan mahrem kayıtları içerebilir. Bu bilgilerin ifşasının etkileri farklı olabilir. Örneğin, bir kullanıcının kişisel bilgilerinin açıklanması kullanıcıyı utandırırken, bir yurttaşın mahrem kayıtlarının ifşası ciddi sonuçlara neden olabilir. Ayrıca, eğer devlet sırrını veya istihbarat dosyalarını ilgilendiriyorsa, bilginin ifşası daha fazla probleme bile neden olabilir.

Bilişim güvenliği çalışanları ifşa tehditleri ile başa çıkmak için çok fazla zaman harcarlar. Özellikle, Amerikan hükümeti kritik güvenlik alanlarında problem oluşturabilme potansiyelleri yüzünden ifşa tehditlerine çok yakından odaklanır. Bu tür tehditlerle başa çıkmanın en zor yanlarından biri yetkilendirilmemiş kişilerin korunmayan veriyi çaldıktan sonra eylemleri hakkında hiçbir iz bırakmamalarıdır. Bu nedenle, güvenlik araştırmaları ve geliştirmeleri ifşa tehditlerine ve karşı tedbirlere odaklanmıştır.

Değiştirme Tehditleri

Bir değiştirme tehdidi (*alteration threat*) verinin bütünlüğünü hedef alır. Bu saldırı türü, kasıtlı veya kasıtsız olarak, bir sistemde tutulan verilere yetkisiz değişiklikler yaparak sistemi tehlikeye sokar. Bu değişim veri ağ cihazında kayıtlıyken veya iki kaynak arasında transfer edilirken oluşabilir. Kasıtlı değişimler genellikle kötü niyetlidir. Kasıtsız değişimler genellikle kaza sonucudur. İnsanlar, bilgisayarların ve cihazların tutarlılığını etkileyecek hatalar yapabilirler ve çoğu zaman yaparlar. Değişimler kasıtlı olmasa bile yine de güvenlik problemleri yaratırlar.

Sistem yapılandırmasına yapılan değişiklikler bir ağ kaynağının bütünlüğünü de ihlal edebilir. Bu değişiklik yetkisiz bir kişi bir varlığı kurcaladığı zaman veya yetkisi olan bir kişi öngörülemeyen sonuçları olan bir değişiklik yaptığı zaman meydana gelebilir. Örneğin, bir kullanıcı veri tabanı dosyalarını, işletim sistemlerini, uygulama yazılımını ve hatta donanım cihazlarını değiştirebilir. Değişiklikler ağ üzerindeki bir kaynakta bilgi oluşturmayı, değiştirmeyi, silmeyi ve yazmayı içerebilirler. Bu değişiklikleri takip etmeyi veya denetlemeyi içeren teknikler geliştirmek iyi bir fikirdir. Bu sayede kimin ne zaman, nerede ve nasıl değişiklikler yaptığı hakkında bir kayda sahip olabilirsiniz. Ayrıca, değişiklik yönetim sistemleri (*change management systems*) kimlerin değişiklik yapabileceğini, bu değişiklikleri nasıl yapabileceklerini ve dosyaları nasıl değiştirebileceklerini sınırlandırabilir. Varlıkları sadece yetkili kişilerin ve sadece yetki verilen şekillerde değiştirebilmeleri çok önemlidir.

Tehdit gerçekten bir DoS tehdidi mi?

İsteklere geç cevap verilmesi her zaman hizmet reddi saldırısı yüzünden değildir. Bu durum, ağ kullanım limitinin aşılması yüzünden olabilir. Aşırı talep (oversubscription) ağın tasarlanandan daha fazla bilgisayar ve süreç tarafından kullanıldığını ifade eder. Bir başka deyişle, kullanıcılar ağı gerektiğinden fazla kullanıyorlardır. Ağ cihazı satıcıları bu tekniği müşterinin zararına olarak gelir artırmada kullanırlar. Bir başka ihtimalde, hizmet sağlayıcının kullanıcının ağdaki bazı kaynaklara ulaşamamasına neden olması olabilir. Örneğin, hizmet sağlayıcı ağdaki önemli kaynakları sistem güncellemesi veya web sitesi değişikliği gibi nedenlerle devre dışı bırakmış olabilir. Başka bir suçlu da *kısma (throttling)* adı verilen, yöneticilerin ağdaki trafiği yavaşlatmak ve azaltmak için kullandıkları bir teknik olabilir veya sorun basit bir kullanıcı hatası olabilir.

Önceden hazırlanmak değiştirme tehditlerinin şiddetini azaltabilir. Örneğin, sizde verinin bir kopyası veya yedeği varsa, güvenlik ihlalinin etkisi yedeğin bulunmadığı duruma göre daha az şiddetli olur. Yine de, verinin geri kazanılması (*recovery*) en son çaba olmalıdır. Çok daha iyi bir yöntem değiştirme saldırısının gerçekleşmesini ilk baştan engellemektir. Bilginizi korumak, bu bilgiyi tamir etmekten veya geri kurtarmaktan her zaman daha iyidir.

Red veya Tahribat Tehditleri

Red (*denial*) veya tahribat (*destruction*) tehditleri varlıkları ve kaynakları kullanılamaz veya ulaşılamaz hale getirirler. Veriyi yok eden veya kullanılamaz hale getiren her tehdit bilişim güvenliğinin kullanılabilirlik ilkesini ihlal eder. Bir red veya tahribat saldırısı yetki sahibi bir kullanıcının bir kaynağa erişimini geçici veya kalıcı bir şekilde engellediğinde başarılı olmaktadır.

Bir DoS saldırısı red veya tahribat tehdidine bir örnektir Bu bölümde daha önce öğrendiğiniz gibi, genelde kötücül olan bir DoS saldırısı, yetkili kullanıcıların bilgisayar ve ağ kaynaklarına erişimini engeller. Birçok kurum DoS saldırılarının muhtemel kurbanlarıdır. Aslında internete bağlı her cihaz DoS tehditlerine açıktır. Bu saldırı türü bloke edilen varlığın veya kaynağın önemine göre küçük veya çok büyük bir tehlike oluşturabilir. Örneğin, bir saldırganın bir sunucudaki belirli bir portu bloke ettiğini düşünelim. Eğer bu port kritik önemdeki bir kaynak için değilse etkisi çok küçük olabilir, fakat eğer port şirketinizin web sitesine kullanıcı girişinin doğrulanmasını destekliyorsa, müşterilerinizin sisteme dakikalarca veya saatlerce girmesini engelleyebilecektir. Bu durumda etkisi çok ciddi olabilecektir.

UYARI

Bir DoS saldırısı kritik önemde olmayan bir portu baskına uğratsa da, gelen büyük miktardaki trafik sunucuyu çökertebilir veya o kadar yavaşlatır ki sunucu gelen geçerli isteklere zamanında cevap veremez. Bu durumda, DOS saldırısı hala başarılı olmaktadır.

Kötücül Saldırı Nedir?

Bir bilgisayar sistemine veya ağa yapılan bir **saldırı *(attack)*** sistemde bulunan bir güvenlik açığını istismar ederek başarılı olur. Dört genel saldırı kategorisi vardır. Bir saldırı aşağıda belirtilen dört kategoriden hepsi veya birkaçının birleşiminden oluşabilir:

- **Uydurmalar (*Fabrications*)** – Uydurmalar, hiçbir şeyden şüphelenmeyen kullanıcıları aldatmak için bir takım hileler oluşturmaktır.
- **Engellemeler (*Interceptions*)** – Engelleme, bir iletişime kulak misafiri olmak ve bu iletişimi yetkisiz bir kullanım için başka bir yere yönlendirmektir.

- **Kesintiler (*Interruptions*)** – Bir kesinti, bir iletişim kanalında kopmaya neden olur ve verinin iletimini engeller.
- **Değişiklikler (*Modifications*)** - Bir değişiklik, iletimde veya dosyada bulunan verinin değiştirilmesidir.

Daha önce öğrendiğiniz gibi, güvenlik tehditleri aktif veya pasif olabilir. Her iki tür de bilişim altyapısı için olumsuz sonuçlara neden olabilir. Aktif bir saldırı veri akımının (*data stream*) değiştirilmesini veya bilgisayar ve ağ sistemlerini yetkisiz erişimin elde edilmesini içerir. Bir aktif saldırı fiziksel bir sızmadır. Pasif bir atakta saldırgan sisteme değişiklikler yapmaz. Bu tip saldırılar sadece veri iletimini takip eder ve dinler.

Aktif tehditler aşağıdakileri içerir:

- Doğum günü saldırıları *(Birthday attacks)*
- Brute-force parola saldırıları *(Brute-force password attacks)*
- Sözlük parola saldırıları *(Dictionary password attacks)*
- IP adres yanıltması *(IP address spoofing)*
- Ele geçirme *(Hijacking)*
- Yeniden gönderme saldırıları *(Replay attacks)*
- Ortadaki adam saldırıları *(Man-in-the-middle attacks)*
- Yerine geçme saldırıları *(Masquerading)*
- Sosyal mühendislik *(Social engineering)*
- Oltalama *(Phishing)*
- Telefon şebekesine yasa dışı girme *(Phreaking)*
- Web sitesi trafiğinin yönlendirilmesi *(Pharming)*

Bu tür saldırılar sıklıkla görülür ve çok yaygındırlar. Bu saldırılar bilişim sistemleri güvenliği çalışanlarının radar ekranlarında her yıl daha da artan bir sayıda görünürler. Şimdi bu kötücül saldırıların en yaygın biçimlerinden birkaçının tanımını yapacağız.

Doğum Günü Saldırıları

Saldırganlar özetlenmiş *(hash)* bir parola dosyasını ele geçirince bir **doğum günü saldırısı (*birthday attacks*)** gerçekleştirilir. Bir doğum günü saldırısı, tek yönlü özetlere (*one-way hashes*) yapılan brute-force saldırısını kolaylaştıran bir kriptografik saldırı türüdür. Olasılık teorisindeki doğum günü problemine (*birthday problem*) dayanan matematiksel bir saldırı biçimidir.

Brute-Force Parola Saldırıları

En çok denenen ve çalışan saldırı metotlarından bir tanesi brute-force parola saldırılardır (*brute-force password attacks*). Bir brute-force parola saldırısında saldırgan çalışan bir parola buluncaya kadar farklı parolaları bir sistem üzerinde dener. Genellikle saldırgan parola, kullanıcı kimliği ve güvenlik kodunun bütün birleşimlerini bir eşleşme buluncaya dek deneyen bir yazılım programı kullanır. Saldırı kısa bir sürede ve seri olarak gerçekleşir. Bu saldırı tipine *brute-force parola saldırısı* denir, çünkü saldırgan basitçe bütün şifreleri denemeye çalışır. Beceri veya gizliliğe gerek yoktur - sadece kod kırılıncaya dek brute-force vardır.

Bugünün büyük ölçekli bilgisayarları ile milyonlarca parola birleşimini çok kısa bir sürede denemek mümkündür. Yeterince zaman verilir ve yeterince bilgisayar kullanılırsa çoğu algoritmayı kırmak mümkündür.

Sözlük Parola Saldırıları

Bir sözlük parola saldırısı (dictionary password attack) kullanıcıların kötü parolalar seçeceklerini göz önüne alan basit bir saldırı türüdür. Bir sözlük parola saldırısında, bir parola kırıcı program sözlükteki bütün kelimeleri alır ve her bir kelimeyi parola olarak kullanarak sisteme giriş yapmaya çalışır.

Kullanıcılar genellikle yaygın olarak kullanılan kelimeleri parola olarak seçmek gibi kötü bir tercih yaparlar. Karmaşık parolaları zorunlu hale getiren bir parola politikası sözlük saldırılarına karşı en iyi savunmadır. Kullanıcılar rakamların ve sayıların birleşiminden oluşan parolalar kullanmalıdırlar ve parolalar kullanıcı hakkında hiçbir kişisel bilgi içermemelidir.

IP Adres Yanıltması

Adres yanıltması (*spoofing*) bir kişi, program veya bilgisayarın kendisini bir başka kişi, program veya bilgisayar gibi gösterip bir kaynağa erişim kazanmaya çalıştığı bir saldırı türüdür. Yaygın bir adres yanıltması saldırısı, sahte bir ağ adresi kullanarak kendisini farklı bir bilgisayar olarak göstermeye çalışmaktır. Bir saldırgan bir bilgisayarın ağ adresini hedefteki ağda bulunan yetkili bir bilgisayarın adresi ile değiştirir. Eğer hedefin yerel yönlendiricisinin yöneticisi, yönlendiriciyi dışarıdan gelen ama ağın içindeki adreslere sahip olan trafiği filtreleyip engelleyecek şekilde yapılandırmamışsa, saldırı başarılı olabilir. IP adres aldatması, bir saldırganın içerideki korunan kaynaklara erişimini sağlayabilir.

Adres çözümleme protokol zehirlenmesi (*Address Resolution Protocol – ARP poisoning*), adres aldatması saldırısına bir örnektir. Bu saldırıda, saldırgan değişik bir MAC adresi ile sahte ARP mesajları göndererek hedefteki bir cihazın, örneğin bir sunucunun, MAC adresini taklit eder. Bu, sunucudan gönderilen ağ trafiğinin ikiye katlanmasına neden olur. Başka bir ağ tabanlı saldırı türü **Christmas (XMAS) saldırısıdır.** Bu tür bir saldırı, bayrakları (flag), TCP başlık bitleri 1 olarak ayarlanmış IP yönlendiricileri ve ağ sınırındaki yönlendiricileri şaşırtmak için ayarlanmış gelişmiş TCP paketleri gönderir ve böylece IP yönlendiricisini bir Nel (Christmas) ağacı gibi aydınlatır.

NOT

CERT tarafından hazırlanan bir IP adres aldatması saldırısı raporunda, kaynak IP adresi değiştirilmiş paketler oluşturularak saldırılar yapıldığına dair haberlerin CERT Koordinasyon Merkezine ulaştığı yazıldı. Bu istismar kişilerin taklit edilmesine ve hedefteki sistemde artırılmış yetkilerle erişime neden olmaktadır. Bu, saldırganların hesaba giriş bilgilerini ele geçirip içeride her istediklerini yapabilmeleri demek olur.

Ele Geçirme

Ele geçirme (*Hijacking*) saldırganın iki makine arasındaki iletişimi ele geçirdiği ve bu makinelerden biri gibi davrandığı saldırı türüdür. Ele geçirme saldırısının birkaç türü vardır:

- **Ortadaki adam ele geçirmesi (*Man-in-the-middle hijacking*)** - Bu tür saldırılarda, birazdan detaylıca tartışacağımız gibi, saldırgan bağlantıyı ele geçirerek kendisini bağlantının herhangi bir ucundaki kişi olarak sunmak için bir program kullanır. Örneğin, Ayşe ve Ahmet iletişim kurmak istediğinde, saldırgan Ahmet ile konuşurken Ayşe gibi, Ayşe ile konuşurken de Ahmet gibi davranır. Ne Ayşe ne de Ahmet saldırgan ile konuştuklarının farkında değillerdir. Saldırgan böylece önemli miktarda bilgi edinebilir ve hatta Ayşe ve Ahmet arasında veri akarken bu veriyi değiştirebilir. Bu saldırı türü, saldırganın mesajlara erişebilmesini veya mesajları yeniden iletmeden önce değiştirebilmesini sağlar. Ortadaki adam saldırıları sistemin içindeki bir tehditten gelebilir. Bu içerideki tehdit *(insider threat)* bir çalışandan, sözleşmeli birisinden veya kurum içerisindeki güvenilir birisinden gelebilir.
- **Tarayıcı veya URL ele geçirmesi (*Browser or URL hijacking*)** – Bir **tarayıcı veya URL ele geçirme saldırısında** kullanıcı istediğinden farklı olarak, genellikle saldırgan tarafından oluşturulmuş,

BİLGİNİZE

Oturum ele geçirme saldırısı bir oturumda karşıdaki kişinin kimliğini belirlemenin önemini ortaya koyar. Oturuma sızan kişinin oturumun geri kalan kısmında asıl kullanıcılardan birinin yerine geçebilmesi mümkündür. Bu nedenle, bütün iletişim boyunca verinin kaynağının kimliğinin denetlendiği bir mekanizmaya ihtiyaç vardır. Aslında, bir bağlantıdaki her iki tarafın da kimliğinin denetlendiği *ortak kimlik denetleme (mutual authentication) sistemi* denilen süreç, oturumun fark edilmeden çalınması ihtimalini azaltabilir. Yine de, en güçlü kimlik denetleme sistemleri dahi oturum çalma saldırılarını engellemekte her zaman başarılı değildir. Bu, bütün iletişimi şifrelemeniz gerektiği anlamına gelir.

sahte bir web sitesine yönlendirilir. Bu, kullanıcıya saldırganın siteyi değiştirdiği izlenimini verir, fakat aslında saldırgan sadece kullanıcının tarayıcısını farklı bir siteye çekmiştir. Bu tür bir saldırı aynı zamanda **yazım hatası (*typo squatting*)** olarak bilinir. Saldırganlar bu saldırıyı kullanarak kullanıcıları kandırıp parola gibi gizli bilgileri oltalayabilirler. (Bu oltalama saldırılarını az sonra öğreneceksiniz.)

- **Oturum ele geçirme (*Session hijacking*) - Oturum ele geçirmede** saldırgan iki ağ bilgisayarı arasında var olan bir bağlantıyı ele geçirmeye çalışır. Bu saldırının ilk adımında saldırgan bağlantıyı izlemek için LAN üzerindeki bir ağ cihazının, örneğin bir güvenlik duvarının veya başka bir bilgisayarın, kontrolünü eline alır. Bu, saldırganın alıcı ve verici tarafından kullanılan sıralı numaraları öğrenmesini sağlar. Bu numara sıralamasını öğrendikten sonra, saldırgan sistemde iletişim halindeki taraflardan birinden geliyormuş gibi görünen bir trafik oluşturur. Bu gerçek kullanıcılardan birinin oturumunu çalar. Çalınan oturumu başlatan asıl kullanıcıdan kurtulmak için saldırgan iletişim halindeki cihazlardan birine çok fazla sayıda paket göndererek aşırı yükler ve böylece cihazın oturumu biter.

Yeniden Gönderme Saldırıları

Yeniden gönderme saldırıları (*replay attacks*) bir ağda veri paketlerini ele geçirip bunları yetkisiz bir durumu oluşturmak için yeniden sisteme göndermeyi içerir. Çoğaltılmış (*duplicate*), doğrulanmış *(authenticated)* IP paketlerinin alımı servisleri aksatabilir ya da bazı diğer istenmeyen sonuçlara neden olabilir. Saldırganlar eski mesajları veya eski mesajların bazı kısımlarını sistem kullanıcılarını kandırmak için yeniden gönderme saldırılarında kullandıkları zaman sistemler ele geçirilebilir. Bu durum, saldırganların bir sisteme yetkisiz girişlerine izin veren bilgiler elde etmelerine yardımcı olabilir.

Ortadaki Adam Saldırıları

Bir ortadaki adam saldırısı (*man-in-the-middle attack*) pek çok ağ türü tarafından kullanılan çok atlamalı *(multi-hop)* süreçten faydalanır. Bu tür saldırıda, saldırgan iki taraf arasındaki mesajları diğer tarafa iletmeden önce ele geçirir.

Web yanıltması *(web spoofing)* kullanıcının belirli bir web sunucusuyla güvenli bir oturuma sahip olduğunu düşündüğü bir tür ortadaki adam saldırısıdır. Gerçekte, güvenli oturum web sunucusuyla değil saldırganla kurulmuştur. Saldırgan daha sonra web sunucusuyla güvenli bir bağlantı kurar ve görünmeyen bir ortadaki adam gibi davranır. Saldırgan kullanıcı ile web sunucusu arasındaki trafiği idare eder. Böylelikle, kullanıcıyı parolalarını, kredi kartı bilgilerini ve diğer gizli bilgilerini vermesi için kandırır.

Saldırganlar ortadaki adam saldırılarını bilgi çalmak, DoS saldırıları düzenlemek, iletilen veriyi bozmak, bir kurumun iç bilgisayar ve ağ kaynaklarına ulaşmak ve ağdaki oturumlara yeni bilgileri sokmak için kullanabilirler.

Yerine Geçme

Yerine geçme (*masquerading*) saldırısında, bir kullanıcı veya bilgisayar başka bir kullanıcı veya bilgisayar yerine geçer. Yerine geçme saldırıları, genellikle IP adres aldatması veya yeniden gönderme gibi aktif saldırı biçimlerinden birini içerir. Saldırganlar doğrulama sıralarını *(authentication sequences)* kaydedip bunları yeniden sisteme sokarak uygulamalara veya işletim sistemlerine girebilirler. Örneğin, bir saldırgan zayıf bir web uygulamasına gönderilen kullanıcı adlarını ve parolaları izleyebilir. Saldırgan, bu ele geçirilen giriş bilgilerini kullanarak web uygulamasına girebilir ve kullanıcıymış gibi davranabilir.

NOT

Yerine geçme saldırıları diğer yetkilerin çalınmasını da içerebilir. Örneğin, çoğu saldırgan İnternet abonelerinin ağ paketlerini ele geçirerek kablosuz ağdan bedava yararlanır. Yakaladıkları paketlerdeki veriyi kullanarak kendilerini İnternet abonesi gibi gösterirler ve kablosuz ağa ücret ödemeden bağlanırlar.

Ortam Dinleme

Ortam dinleme *(eavesdropping)* veya koklama *(sniffing)*, ağdaki bir birimin ağ ara yüzünü *karışık (promiscuous)* modunda ayarlaması ve geçen bütün paketleri daha sonra analiz etmek üzere kopyalaması halinde oluşur. Karışık mod, bir ağ cihazının adresi kendi ağ adresiyle eşleşmese dahi gelen her ağ paketini yakalayıp okumasına izin verir. Diğer kullanıcıları uyarmaksızın, sisteme donanım ve yazılım ekleyerek iletim ortamının o bölümündeki bütün paketleri izlemek ve analiz etmek mümkündür. Ortam dinleme saldırıları uydu, kablosuz, mobil ve diğer iletim metotlarını içerir.

Sosyal Mühendislik

Saldırganlar bir BT altyapısındaki kaynaklara erişmek için sıklıkla **sosyal mühendislik (*social engineering*)** denen bir aldatma tekniğini kullanırlar. Neredeyse bütün olaylarda, sosyal mühendislik yetkili kullanıcıları kandırarak yetkisiz kullanıcıların istediği şeylerin yaptırılmasını içerir. Sosyal mühendislik saldırısının başarısı insanların yardımcı olma dürtülerine bağlıdır.

Sosyal mühendislik, güvenlik ihlali konularında insan faktörünü devreye sokar ve bir silah olarak kullanır. Çalınan veya taklit edilen çalışan veya satıcı kimlikleri güvenlikli yerlere giriş hakkı sağlayabilir. Saldırgan daha sonra önemli varlıklara erişim elde edebilir. Çalışanların, teknik servise veya sözleşmeli çalışanlara yardımcı olma isteğinden faydalanarak, bir saldırgan bir kurumun güvenliğini aşabilir ve erişim hakkı kazanabilir.

Bir kurumun dışarıyla iletişim kuran ilk çalışanları, örneğin resepsiyonistler ve yönetici asistanları, çoğu zaman sosyal mühendislik saldırılarının hedefleridir. Kurumun yapısı hakkında biraz bilgisi olan saldırganlar, yeni, eğitim almamış çalışanları ve güvenlik politikasından pek anlar gibi görünmeyen kişileri de hedef alacaktır.

Sosyal mühendislik saldırılarını durdurmak zor olabilir, fakat saldırıların etkisini azaltmak için bazı teknikler vardır:

- Çalışanların güvenli bir ortam konusunda temel bir eğitim almalarını sağlayınız.
- Bir bilgisayar kullanım ve güvenlik politikası geliştiriniz.
- İç ve dış teknik destek süreçleri hakkında katı bir politika uygulayınız.

- Bütün çalışanların kimliklerinin doğrulanmasını gerektiriniz.
- Dizinlerde, ilan sayfalarında, web sitelerinde ve kamuya açık veri tabanlarında bulunan herkesin erişebileceği verinin miktarını sınırlandırınız.
- Uzaktan erişim kullanıyorsanız çok dikkatli olunuz. Kimlerin ağınıza girdiğini bilmek için çok güçlü kimlik doğrulama teknikleri kullanınız.
- Güvenli mail alma ve gönderme teknikleri için çalışanlarınıza eğitim veriniz.
- Gizli veya hassas dokümanları ince şeritlere ayırarak yok ediniz.

Telefon şebekesine girme

Telefon şebekesine girme veya kısaca **şebekeye girme (*phreaking*)**, telefon sistemleri, telefon şirket donanımları ve genel telefon hatlarına bağlı sistemleri araştıran, bunlar üzerinde çalışan ve bunlarla deneyler yapan kişilerin eylemlerini tanımlayan argo bir terimdir. Şebekeye girme telefon sisteminde var olan hataları ve sorunları istismar etme sanatıdır.

Oltalama

Dolandırıcılık internet üzerinde gün geçtikçe büyüyen bir sorundur. **Oltalama (*Phishing*)** bir saldırganın kurbanını kredi kartı numaraları, parolalar, doğum tarihi, banka hesabı numarası, ATM şifresi veya Sosyal Güvenlik Numarası gibi gizli bilgilerini vermek için kandırdığı bir dolandırıcılık türüdür.

Oltalama saldırıları e-posta veya anlık iletiler ile kimlik hırsızlığı yapmaya çalışmaktır. Bu mesajlar, güvenilen bankalar veya finansal kurumlar gibi gerçek kaynaklardan geliyormuş gibi görünürler ve kişisel bilgiler için acil bir istek içerirler. Oltalama mesajları genellikle (banka, kredi kartı gibi) önemli hesap bilgilerinin hemen değiştirilmesini ister. Mesaj kurbana istenen bilgiyi ya doğrudan göndermesi ya da verilen bir linke tıklayarak girmesini talimat verir. Linke tıklamak kurbanı sahte bir web sitesine götürür. Bu web sitesi resmi siteye tıpatıp benzer, fakat saldırganın kendi yaptığı bir sitedir. Bu sayfaya girilen kişisel bilgiler asıl kuruma değil saldırgana gider.

Oltalama saldırılarının bir başka türü de hedef odaklı oltalamadır (spear phishing). Hedef odaklı oltalama, e-posta veya anlık iletiler kullanarak belirli bir kurumu hedef alır, gizli veriye yetkisiz erişimi hedefler. Sıradan oltalama mesajlarında olduğu gibi hedef odaklı oltalama mesajları da güvenilir bir kaynaktan geliyormuş gibi görünür.

Her tür oltalama saldırısından korunmanın en iyi yolu şüpheli bir e-postadaki linke tıklamamaktır. Bir e-posta veya anlık ileti ile istendi diye kişisel bilgileri önünüze gelen bir web sitesine girmek çok kolay olabilir. Eğer bu isteğin doğru olduğunu düşünüyorsanız herhangi bir bilgiyi girmeden önce şirketin müşteri hizmetleri destek hattını aramalısınız. Eğer şirketi arayacaksınız, şüpheli mesajda verilen hiçbir telefon numarasını kullanmayınız. Mesajda verilen web adresi doğru görünse dahi, mesajdaki linke tıklamak yerine web adresini tarayıcınıza kendiniz yazarak giriniz.

NOT

Bugün gerçekleşen çoğu sosyal mühendislik aktivitesinin kökeni telefon hattına giren kişiler (phreakers) tarafından üretilen stratejilerdir. Nitekim günümüzde kullanılan bir kaç sosyal mühendislik saldırısının adı bu sosyal mühendislik öncülerine ithafen "ph" harfleri ile başlamaktadır.

NOT

Kötücül yazılıma karşı olan programlar ve güvenlik duvarları çoğu oltalama dolandırıcılığını tespit edemez, çünkü bunlar şüpheli kod içermezler. Bazı spam filtreleri oltalama mesajlarını engellemezler, çünkü bu mesajlar geçerli kaynaklardan geliyor gibi görünürler.

Bir Oltalama Dolandırıcılığı Nasıl Tespit Edilir?

Sadece gelen e-posta mesajında tıkladığınız linke bakarak oltalama dolandırıcılığını tespit etmek zor olabilir. Fakat göndericinin adresindeki bazı ipuçları dolandırıcılığı ortaya çıkarabilir. Şunlara dikkat ediniz:

- Oltalama yapanlar genellikle gerçek adreslerdeki karakterleri benzer karakterler ile değiştirirler. Örneğin, Paypal.com adresindeki küçük L harfi yerine 1 (rakam olarak) kullanabilirler (Paypa1.com).
- Oltalama hileleri o kadar gelişti ki artık oltacılar gerçek bağlantıları hatta asıl sitenin güvenlik sertifikasını kullanıyormuş gibi görünebilirler. Bir bağlantıya tıklamadan önce bağlantının sizi nereye götüreceğine dikkat ediniz. Eğer alan adı tuhaf görünüyorsa bağlantıya tıklamayınız. Bunun yerine, asıl web sitesinin müşteri hizmetlerini veya teknik destek hattını arayarak bağlantının geçerli olup olmadığını sorunuz. Bu yaklaşım zaman alabilir fakat bağlantılara hiç kontrol etmeden tıklamaktan daha güvenlidir.
- Bazı oltacılar gerçek şirketlerin adresine benzeyen alan adlarını satın alırlar - örneğin *walmartorder.com* gibi. Asıl şirket Wal-Mart'tır fakat şirketin alan adında order kelimesi geçmemektedir.
- Bir başka taktik de aynı alan adını .com uzantısı yerine .org uzantısıyla kullanmaktır. Bu alan adını kullanan dolandırıcılar daha sonra milyonlarca e-posta gönderip müşterilerden hesap bilgilerini, doğum tarihlerini, Sosyal Güvenlik numaralarını ve diğer bilgilerini doğrulamalarını isterler. Kaçınılmaz bir şekilde, bazı bilgisayar kullanıcıları bu mesajlara cevap verirler. Bütün alan adını dikkatlice kontrol ediniz!

Oltalama Dolandırıcılığını Önleme Çalışma Grubu (*Anti Phishing Working Group* - APWG) sahtekârlık ve kimlik hırsızlığı gibi e-posta dolandırıcılıklarının neden olduğu sorunları ortadan kaldırmaya çalışan endüstri tabanlı küresel bir yasa uygulama birliğidir. Daha fazla bilgi edinmek için APWG web sitesini www.antiphishing.org adresinde ziyaret edebilirsiniz. Ayrıca, Federal Ticaret Komisyonu (FTC) web sitesi (www.ftc.gov) tüketiciler için oltalama aktivitelerini ve kimlik hırsızlığı sorunlarını bildirebilecekleri bir form ve e-posta adresi bulundurmaktadır.

Web Sitesi Trafiğinin Yönlendirilmesi

Web sitesi trafiğinin yönlendirilmesi (*pharming*) alan adı değiştirerek kişisel ve finansal bilgileri elde etmeye çalışan bir saldırı türüdür. Fakat, web sitesi trafiğinin yönlendirilmesi saldırısı kurbanlarını geçerli sitelere benzeyen sahte sitelere çekmek için mesajlar kullanmaz. Bunun yerine alan adı sunucusunda *(Domain Name Server - DNS)* bulunan bir alan adını "zehirler". Bu sürece **DNS zehirlenmesi (*DNS poisoning*)** denir. Sonuç olarak, bir kullanıcı zehirlenmiş sunucunun web adresini kendi adres çubuğuna girdiğinde saldırganın sitesine ulaşır. Kullanıcının tarayıcısı hala gerçek web adresini gösterir ki bu durum web sitesi trafiğinin yönlendirilmesinin tespitini zorlaştırmakta ve sonuçlarını daha da ciddi hale getirmektedir. Oltalama e-posta ve anlık ileti yoluyla kişileri teker teker dolandırmaya çalışırken; web sitesi trafiğinin yönlendirilmesi, alan adını değiştirerek büyük insan gruplarını dolandırır.

Kötücül Yazılım Nedir?

Bütün yazılımlar iyi amaçlara hizmet etmezler. Bazı yazılımlar bir veya daha fazla hedef bilgisayara sızar ve bir saldırganın talimatlarını izlerler. Bu talimatlar zarar vermeyi, güvenlik yetkilerini yükseltmeyi, mahrem verileri ifşa etmeyi ve hatta veriyi silip değiştirmeyi içerebilir. Bu tür yazılıma **kötücül yazılım (*malicious software*)** veya kısaca **malware** denir. Kötücül yazılımın amacı sistemi zarara uğratmak ve çalışmasını aksatmaktır. Kötücül yazılımın etkileri bir masaüstü bilgisayarını yavaşlatmaktan çökertmeye, kredi kartı numaraları hırsızlığına ve daha kötü şeylere kadar uzanabilir. İnternette gezinmek, e-posta okumak, müzik veya diğer dosyaları indirmek kişisel bir bilgisayara kötücül yazılım bulaştırabilir – bu genellikle kullanıcının bilgisi olmadan gerçekleşir.

Kötücül yazılım iki temel kategoride yer alır: bulaşıcı *(infecting)* programlar ve saklanan *(hiding)* programlar. Bulaşıcı programlar aktif olarak kendilerini diğer bilgisayarlara kopyalamaya çalışırlar. Bunların asıl amacı bir saldırganın talimatlarını yeni hedeflerde çalıştırmaktır. Bu tür zararlı yazılımlar aşağıdakileri içerir:

- Virüsler
- Solucanlar *(worms)*

İsimlerinin ima ettiği gibi, saklanan programlar bilgisayarda saklanırlar ve saldırganın talimatlarını fark edilmeden gerçekleştirirler. Saklanan kötücül programlar aşağıdakileri içerir:

- Truva Atları *(Trojan Horses)*
- Rootkitler *(Rootkits)*
- Casus yazılım *(Spyware)*

Gelecek bölümler kötücül yazılımın her bir türünü tanımlayacaktır.

Virüsler

Bir bilgisayar *virüsü* kendisini başka bir bilgisayardaki bir programa kopyalayan veya iliştiren bir yazılım programıdır. Virüsün amacı programı asıl geliştiren kişinin tasarlamadığı talimatları çalıştırmak için diğer bilgisayarı kandırmaktır. Kullanıcılar virüs bulaşmış dosyaları ağdaki diğer bir bilgisayardan, bir flash bellekten veya internetteki bir hizmetten kopyalar. Bundan farklı olarak kullanıcılar evdeki bilgisayarlarında bulunan virüsleri getirip, internete ve diğer ağ hizmetlerine erişimi olan taşınabilir bilgisayarlarında çalışabilirler.

Bir bilgisayar virüsü biyolojik bir virüse benzer şekilde çalışır. Bir programa "bulaşır" ve bulaştığı programın kendisini diğer bilgisayarlara kopyalamasına neden olabilir. Virüs herhangi bir programa bağlı olmadan var olamaz ve bir hedeften diğerine bulaşıcı bir biçimde yayılır.

Kaydedilen ilk bilgisayar virüsü araştırmacı Bob Thomas tarafından 1971 yılında yazılan Creeper virüsüydü. Creeper kendisini ağdaki diğer bilgisayarlara kopyalayıp ekranlarında "Benim adım Creeper, yakalayabiliyorsanız yakalayın beni!" mesajını gösteriyordu. Thomas bu kendini çoğaltan, deneysel virüsü ağdaki bilgisayarların bu tür programlardan nasıl etkilendiklerini görmek için tasarladı. Creeper sisteme sokulduktan kısa bir süre sonra araştırmacılar Creeper'ı bulmak ve yok etmek için Reaper programını ortama saldılar.

Günümüzde bilinen yüz binlerce virüs her tür programa bulaşmaktadır. Virüslerin asıl endişelendirici yanı kendilerini sıklıkla kullanılan programlara bulaştırmalarıdır. Kullanıcılar bu virüslü programları çalıştırdıklarında, aslında kendi parolaları ve yetkileri ile virüs kodunu

çalıştırmaktadırlar. Virüs yetkilerini artırmak zorunda kalmaz; virüs bulaşmış programı çalıştıran kullanıcı virüse kendi yetkilerini ve izinlerini kullandırtmış olur.

Zamanla, virüsler daha akıllı hale geldiler. Örneğin, bazı virüsler kötücül yazılımı tespit eden programların virüs tanıma fonksiyonlarını devre dışı bırakarak kendilerini koruyabilirler. Virüsler bulaştıkları dosyaların boyutlarını artırdıkları için kolayca tespit edilebilirler. Buna önlem olarak bazı virüsler bulaştıkları dosyaların boyutlarını virüs bulaşmadan önceki kadar göstererek denetimden kurtulmaya çalışırlar. Böylece, hiçbir şey değişmemiş gibi görünür.

Solucanlar

Bir *solucan (worm)* kullanıcıların girdilerine veya eylemlerine ihtiyaç duymadan kendisini çoğaltarak kopyalarını, genellikle bir ağ üzerinden, diğer bilgisayarlara gönderebilen bağımsız *(self-contained)* bir programdır. Solucanın amacı, basitçe, ağı gereksiz yere kullanarak ağın bant genişliğini azaltmak veya başka zararlı eylemlere kalkışmak olabilir. Solucanla virüs arasındaki fark solucanın bulaşmak için üzerinde yaşayacağı bir programa ihtiyaç duymamasıdır. Solucan tek başına *(standalone)* bir programdır.

NOT

Bir arabellek taşması (*buffer overflow*) çalışan bir programın veri için ayrılan bellek alanının dışında bir yere veri kaydettiği bir durumdur. Bir programın beklediğinden fazla veri kaydederek, programa çalıştığı anlardaki davranışını değiştirecek talimatlar ekleyebilirsiniz. Arabellek taşmaları çok çeşitlidir ve her zaman programcının girilen veriyi kontrol etmeden içeri alması yüzünden oluşur.

Dünyada "kontrolsüzce" yayıldığı tespit edilen ilk solucan Morris solucanıydı. Robert Tapan Morris bu solucanı 1988'de yazdı. Morris solucanı bir arabellek taşması *(buffer overflow)* açığına saldırmaktaydı. Morris solucanın asıl gayesi Unix işletim sistemi sürümlerine sahip olan bilgisayarlara bulaşarak internette yayılmak ve bu sayede internetin boyutlarını tahmin etmekti. Yine de, solucan yazarının tahmininden daha hızlı yayıldı. Sonunda, solucan bilgisayarlara birçok defa bulaştı ve bulaştığı bilgisayarları kullanılamayacak kadar yavaşlattı. Morris solucanı medyanın ilgisini çeken ilk kötücül yazılım oldu ve Amerika Birleşik Devletlerinde 1986 Bilgisayar Kullanımı ve Sahtekârlığı Yasası *(U.S. 1986 Computer Use and Fraud Act)* kapsamında verilen ilk cezayla sonuçlandı.

Truva Atları

Bir **Truva Atı (*Trojan horse*)**, aynı zamanda **Truva** da denir, kendisini faydalı bir programmış gibi gösteren kötücül bir yazılımdır. Adı *Aeneid*[3]'deki meşhur Truva atından gelir. Bu şiirde, Truva ile 10 yıldır savaşta olan Yunanlar büyük bir tahta at yapıp Truvalılara "hediye" olarak verirler. Truvalılar atı, bir barış teminatı olarak görüp, şehrin içine alırlar. O gece Truvalılar uyurken atın oyuk karnında saklanan Yunanlı askerler dışarı tırmanırlar ve şehir kapılarını açıp Yunan ordusunun kalan kısmını şehre alırlar. Yunanlılar o gece Truva'yı tamamıyla mağlup ederler.

Benzer bir şekilde, Truva atı programları dış görünüşlerini kullanarak kullanıcıları kendilerini çalıştırmaları için aldatırlar. Bu programlar faydalı işler yapıyormuş gibi görünürler, fakat aslında kötücül kod içerirler. Program çalışmaya başladığında, saldırı talimatları kullanıcının izni ve yetkisi olmadan yürütülür.

İlk bilinen Truva atı programı 1974'te yaratılan Animal'dır. Animal kendisini basit bir soru cevap oyunu olarak gösterip kullanıcılara bir hayvan adı seçtirir ve adı tahmin edebilmek için sorular sorardı. Ancak, soru sormaya ek olarak, program kendisini kullanıcının yazma yetkisinin olduğu bütün dizinlere kopyalardı.

3 *Editörün Notu*: Aeneid ya da Aeneis, Romalı şair Vergilius'un Roma İmparatorluğu'nun destanı sayılan epik destanıdır.

Günümüz Truva atları kendilerini kopyalamaktan çok daha fazlasını yapmaktadırlar. Truva atları mahrem bilgileri saklayan, bilgisayarlara arka kapılar açan veya aktif olarak dosya indiren veya gönderen programlar içerebilirler. Yapabilecekleri şeylerin listesi sınırsızdır.

Rootkitler

Rootkitler diğer kötücül yazılımlara göre daha yeni bir türdür. 1990 yılına dek görülmediler. Bir rootkit bir veya daha fazla programı değiştirerek veya bunların yerine geçerek saldırısının izlerini gizler. Rootkitler izlerini gizlemek için genellikle işletim sisteminin parçalarını değiştirseler de, aslında bilgisayarın boot komutlarından işletim sisteminde koşan uygulamalara dek her seviyede var olabilirler. Rootkitler bir defa kurulduklarında, başka saldırılar başlatmaları için saldırganların sızılmış bilgisayarlara kolay bir şekilde erişimlerini sağlar.

> **İPUCU**
>
> Rootkitler genellikle diğer kötücül programlarla beraber çalışırlar. Örneğin, malware.exe isimli bir programın Windows üzerinde çalıştığını düşününüz. Basit bir rootkit Windows Görev Yöneticisini başka bir yönetici ile yer değiştirerek malware.exe isimli dosyanın gösterilmemesini sağlayabilir. Sistem yöneticileri artık kötücül programın çalıştığını bilemezler.

Rootkitler birçok işletim sistemi için yazılmışlardır, bunlara Linux, Unix ve Microsoft Windows dâhildir. Çok fazla türde rootkit olduğu için ve bir defa makineye kurulduklarında kendilerini çok iyi gizledikleri için, rootkitleri tespit etmek ve kaldırmak çok zor olabilir. Buna rağmen, rootkitleri tespit etmek ve kaldırmak güvenli bir sistem için çok önemlidir. Host tabanlı bir saldırı tespit programı *(host based-IDS)* rootkit aktivitesini tespit etmede yardımcı olabilir.

Sisteminizde bir rootkit tespit ederseniz, en iyi çözüm işletim sistemini orijinal kaynağından yeniden kurmanızdır. Bu, kullanıcı ve uygulama verilerini daha önce aldığınızı var saydığımız kopyalardan yeniden kurmanız ve yenilemenizi gerektirir. Eğer sisteminizin dokümanlarını iyi tutmadıysanız, bunları yapmak daha zor olabilir. Bir saldırganın rootkit kurmasını sağlayacak yetkisiz bir erişimi engellemek, kurulmuş bir rootkiti kaldırmaya çalışmaktan daha etkilidir.

Casus Yazılım

Casus yazılım (*spyware*) özellikle bilginin gizliliğini *(confidentiality)* tehdit eden bir kötücül yazılım türüdür. Bu yazılım kullanıcının izni olmadan internet bağlantısı üzerinden bilgi toplar. Casus yazılım internetten indirilen, ücretsiz olan kamuya açık yazılım *(freeware)* veya paylaşılan *(shareware)* yazılım programlarının, Truva atına benzer bir şekilde, gizli bir bileşeni olarak gelir. Casus yazılım ayrıca uçtan uca *(peer-to-peer)* dosya paylaşımı ile de yayılır. Casus yazılımlar 1990'ların sonundan beri varlar ve 2000'den sonra daha popüler oldular. İnternetin hızlı büyümesi saldırganların hiçbir şeyden haberi olmayan daha fazla kullanıcının bilgisini toplamasını kolaylaştırdı.

> **NOT**
>
> Yazılımla beraber gelen kullanım şartları sözleşmeleri kullanıcıları bazen istenen yazılımın yanında bir de casus yazılım kurulacağı konusunda uyarırlar. Fakat, ağır hukuki terimlerle dolu oldukları için bu sözleşmeler çoğu zaman okunmazlar.

Casus yazılım bir defa kurulduktan sonra, kullanıcının internet üzerindeki davranışlarını gözetler. Casus yazılım e-posta adresi ve hatta parolalar ve kredi kartı numaraları gibi bilgileri de toplayabilir. Casus yazılım daha sonra elde ettiği veriyi yazılımı yazan kişiye iletir. Yazılımı yazan kişi bu bilgiyi, basitçe, reklam veya pazar araştırması için kullanabilir ama isterse bu bilgiyle kimlik hırsızlığını kolaylaştırabilir.

Bilgi çalmaya ek olarak, casus yazılım hem elde ettiği veriyi üçüncü partilere iletmeye çalışırken internet bağlantısını kullanarak hem de bilgisayarın kaynaklarını kullanarak kullanıcıdan

Reklam Yazılımı

Reklam yazılımı (*Adware*) casus yazılıma benzer fakat **kişileri ayırt edebilecek bilgileri (Kişisel Tanımlama Bilgisi, *Personally Identifiable Information* - PII)** iletmez. PII kişileri ayırt etmeye yarayan bilgilerdir. PII örnekleri sürücünün ehliyet numarası, Sosyal Güvenlik numaraları (TC Kimlik Numarası) ve kredi kartı numaraları vb. bilgileri içerir. Reklam yazılımının topladığı bilgiler pazarlama kampanyalarını geliştirmek için kullanılır. Örneğin, reklam yazılımı, satın alma alışkanlıklarına göre uyarlanmış açılır pencereler (pop-up) sağlamaya yardımcı olabilir veya pazar araştırması amacıyla kullanılabilir.

Bir **açılır pencere (*popup*)** tarayıcıda en üstte açılan bir pencere türüdür. Bu pencereler genellikle reklam içerir. Açılır pencereler tam anlamıyla reklam yazılımı olmasalar da, çoğu reklam yazılımı kullanıcılarla iletişim kurmak için bu pencereleri kullanır. Bazı yazılım ürünleri açılır pencereleri engellemek için bir seçenek sunar.

Casus ve reklam yazılımları, hızlı ve artan bir şekilde bilgisayarlar için oldukça yaygın tehditlere dönüştüler. Bazı uzmanlar bilgisayarların %90'dan fazlasına bu yazılımların çoktan bulaşmış olduğunu tahmin ediyor. Neyse ki, bazı yazılım sağlayıcıları casus ve reklam yazılımlara karşı yazılımlar üretmektedirler. Aslında, anti virüslerin ve genel kötücül yazılımla mücadele programlarının çoğu casus ve reklam yazılımları da tespit edip kaldırıyor. Kurumunuzun ihtiyaçları doğrultusunda bu programları inceleyip size en uygun olanını bulmak zor olduğu kadar önemli de bir görevdir.

çalma gerçekleştirir. Birden fazla casus yazılım çalıştıran bilgisayarlar temiz bilgisayarlara göre oldukça yavaş çalışırlar. Ayrıca, casus yazılım bellek ve diğer sistem kaynaklarını kullandığı için sistemlerde düzensizliğe ve hatta çökmelere neden olabilir.

Casus yazılım bağımsızca yürütülebilen *(executable)* bir program olduğu için, aşağıda verilen listedekileri de içeren bazı işlemleri gerçekleştirebilmektedir:

- Basılan tuşları izlemek
- Sabit diskteki *(hard disk)* dosyaları taramak
- Sohbet *(chat)* programları ve kelime işlemciler *(word processors)* gibi diğer uygulamaları izlemek
- Diğer casus yazılım programlarını kurmak
- Tarayıcı çerezlerini okumak
- Web tarayıcıdaki varsayılan ana sayfayı değiştirmek

Saldırıların Genel Türleri Nelerdir?

Saldırganın hedefine ve amacına bağlı olarak birçok saldırı türü saldırganın gereksinimine ve yeteneğine uygun olabilir. Bu saldırılar üç kategoride özetlenebilir:

- **Kullanılabilirliğe yönelik saldırılar** - Bu saldırılar, hayati önemdeki bir sistemin, uygulamanın veya verinin erişimini ve çalışmasını etkiler.
- **İnsanlara yönelik saldırılar** - Bu saldırılar, hile ve zorlama ile diğer bir kişinin bilgi paylaşmasını veya bir eylemi gerçekleştirmesini (örneğin, şüpheli bir URL linkine tıklamasını veya bilinmeyen bir e-posta adresinden gelen e-posta eklentisini açmasını) içerirler.
- **BT varlıklarına yönelik saldırılar** - Bu saldırılar, sızma testleri, yetkisiz erişim, yetkilerin artırılması, parola çalınması, veri silinmesi veya bir veri ihlali gerçekleştirmeyi içerirler.

Sosyal Mühendislik Saldırıları

Sosyal mühendislik, kişileri zorlayarak veya kandırarak bir şeyi yaptırma veya bir bilgiyi ifşa etmesini sağlama sanatıdır. Günlük hayatımızda bunu her zaman kullanırız. Çocuklar ebeveynlerinden izin almak veya istedikleri bir şeyi yaptırmak için sosyal mühendisliği kullanırlar. Bir eş olarak, eşinizi sizin yapmanız gereken küçük işleri yapmaya ikna edebilirsiniz. Suçlular ve sahtekârlar da bundan farklı değildir: Sosyal mühendislik taktiklerini insanlardan kendileri veya başkaları hakkında bilgi almak için kullanırlar. Bu, kimlik hırsızlığı için kişisel bilgileri toplamada anahtar noktadır. Bilgisayar korsanları ayrıca, bilişim sistemleri ve uygulamaları hakkında bilgi vermeye ikna etmek için seçilen çalışanlar üzerinde sosyal mühendislik taktiklerini denerler ve bu sayede erişim izni kazanırlar.

Bilgisayar korsanları ve sisteme giren kişiler kurbanlarına çok farklı sosyal mühendislik taktikleri uygularlar. Kurumunuza veya size karşı kullanılabilecek sosyal mühendislik taktiklerinin bir özeti aşağıda listelenmektedir:

- **Otorite** – Kurumdaki yüksek bir pozisyonu kullanarak bir kişiyi bilgiyi vermeye ikna etmek veya zorlamak.
- **İttifak/sosyal kanıt** – "Herkes böyle yapıyor" diyerek bir şeyi yapmanın doğru ve kabul edilebilir olduğunu söylemek.
- **Çöp karıştırma** – İnce kıyılarak çöpe atılmış belgelerden kimlik hırsızlığı için kullanılabilecek hassas ve gizli bilgiler bulmaya çalışmak.
- **Yakınlık/Beğenme** – Kurbanla sık sık iletişim kurup yakınlık ve aşinalık kurmak (örneğin, bir kargo görevlisi zamanla ofis çalışanı ile samimiyet kurabilir) ve bu sayede tanınan kişiye yardımcı olması için kurbanı cesaretlendirmek.
- **Hileler** – Yanlış veya sahte bir izlenim yaratarak bir kişiye bir şey yaptırmak veya kişiyi bilgi vermeye ikna etmek.
- **Taklit** - Bir kişinin (mesela bir teknik destek çalışanı, bir kargocu veya bir banka temsilcisi) yerine geçmek.
- **Korkutma** – Güç kullanarak bir kişiye bir şey yaptırmak veya bir şeyi açıklamasını sağlamak.
- **Yetersizlik** – Bir şeye sahip olmamakla veya bir şeye erişim hakkını kaybetmekle korkutarak kişiye bir iş yaptırmak veya bir bilgiyi açıklamaya zorlamak.
- **Omuz sörfü (*Shoulder surfing*)** –Veri giren kişinin omuzunun üstünden bilgisayar ekranına bakmak.
- Öndeki kişinin **yakınından gitmek** – Bir kişinin hemen arkasından yürüyerek güvenli bir kapıdan veya giriş bölgesinden gizlice geçmek.
- **Güven** – Zaman içinde bir güven bağı oluşturup daha sonra bu güven bağı ile kişiye bir şey yaptırmak ya da kişiden bir bilgiyi öğrenmek.
- **Aciliyet/Öncelik** – Öncelikli veya acil stres durumunu kullanarak birisinden bilgi almak veya bir işe zorlamak (örneğin, ara holde bir yangın olduğunu söylemek ön kapıdaki güvenlik görevlisini masasından ayırabilir).
- **Telefonla kişisel bilgilerin el geçirilmesi** – Telefonla bir oltalama saldırısı gerçekleştirerek, (tatlı sözlerle) konuşarak kişisel bilgi edinmeye çalışmak veya kurbanı bir işe zorlamak.
- **Balina avı** – En üst düzey kullanıcıyı veya en değerli çalışanları, yani "büyük balık" veya "balina" gibi görülen kişileri hedef almak (çoğu zaman *hedef odaklı oltalama (spear phishing)* denir).

Kablosuz Ağ Saldırıları

Kablosuz ağ saldırıları kablosuz ağ üzerinde trafiği izlemek, paket yakalamak ve sızma testleri yapmak gibi saldırıları içerir. Hem kamuya açık hem de özel alanlardaki artan kablosuz ağ kullanımını göz önünde bulundurursak mobil kullanıcı her zaman tehdit altındadır. Kablosuz ağlar bilişim alt yapınızda ağa erişim noktası olarak ele geçirilebilirler. Gerekli kablosuz ağ güvenlik kontrollerinin hayata geçirilmesi, kablosuz ağlarda oluşacak risklerin, tehditlerin ve güvenlik açıklarının giderilmesi için anahtar bir rol oynar. Bilgisayar korsanları ve ağa sızmaya çalışan kişiler tarafından kablosuz ağlara sızma ve saldırma girişimlerinde birçok farklı taktik kullanılmaktadır.

Kablosuz ağ saldırılarının bir özeti aşağıdaki gibidir:

- **Bluejacking** – Bluejacking, kullanıcının telefonu ve kulaklığı arasındaki Bluetooth kablosuz iletişim bağlantısının kırılması ve ele geçirilmesidir.
- **Bluesnarfing** – Bluetooth cihazları arasındaki paket trafiğinin izlenip kopyalanmasıdır.
- **Kötü ikiz** – Özel veya herkese açık bir kablosuz ağmış gibi davranarak ağa bağlanmaya çalışan her kullanıcının paketlerini izlemek.
- **IV saldırısı** – İletilmekte olan bir şifrelenmiş IP paketinin başlangıç vektörünü *(Initialization Vector - IV)* değiştirerek zaman içerisinde genel şifreleme anahtarını kırma çabasıdır.
- **Frekans bozumu/Araya girme (*Jamming/Interference*)** – Kablosuz erişim noktaları ile aynı frekansta radyo dalgaları göndererek kablosuz iletişime karışmak ve bozmak, böylece normal kullanıcılara verilen hizmeti sekteye uğratmak.
- **Yakın alan iletişim saldırısı** – Çok yakın mesafeden (bir kaç santimetreden) mobil işletim sistemli iki cihazın iletişiminin arasına girmek.
- **Paket koklamak (*Packet sniffing*)** – Bir kablosuz ağın IP paketlerini yakalamak ve Wireshark® gibi araçlar kullanarak TCP/IP paket verilerini analiz etmek.
- **Yeniden gönderme saldırıları (*Replay attacks*)** – Kimlik doğrulama işlemi yapıyormuş gibi önceki bir IP paket akışını bir sunucuya yeniden göndererek sunucuyu kandırmak.
- **Sahte erişim noktaları** – Yetkisiz bir ağ cihazını kullanarak, hiçbir şeyden şüphelenmeyen kullanıcılara kablosuz ağ hizmeti sunmak.
- **War chalking** – Kablosuz erişim noktalarının ve ağlarının fiziksel ve coğrafi konumlarının bir haritasını çıkarmak.
- **War driving** – Fiziksel olarak bölgelerin veya iş merkezlerinin etrafında dolaşarak açık ve herkes tarafından kullanılabilir ağ bağlantıları sunan kablosuz erişim noktaları ve ağları aramak.

Bu belirli saldırılara ilaveten, bilgisayar korsanları hedef tarafından kullanılan kablosuz şifreleme tekniklerindeki zayıflıkları da kullanabilirler: WEP *(Wireless Encryption Protocol – Kablosuz Şifreleme Protokolü)*, WPA *(Wi-Fi Protected Assets – Wi-Fi Korumalı Varlıklar)* ve WPS *(Wi-Fi Protected Setup – Wi-Fi Korumalı Kurulum)*.

Web Uygulama Saldırıları

Web **uygulama saldırıları (*application attacks*)**, internete açık ara yüzü bulunan web sunucularına, uygulamalara ve veri tabanlarına sızma testleri yapmayı içerir. E-ticaret, müşteri veya üye web siteleri ve portallarının sayısının hızlı artışı nedeniyle gizli verilere, hassas verilere ve fikri eserlere erişim çok fazladır. Bilgisayar korsanları ve sisteme sızmak isteyenler, uygulamalara sızmak ve saldırmak için çok farklı taktikler kullanmaktadırlar.

İnternet üzerinde herkesin erişimine açık olan web uygulamaları, aşağıdakileri içeren web uygulama saldırıları ile karşılaşmaktadır:

- **Rastgele/uzaktan kod yürütmek (*Arbitrary/remote code execution*)** – Yetkili erişime veya sistem yöneticisinin erişim haklarına sahip olunursa, saldırgan uzaktaki sistemde keyfi olarak komutlar çalıştırabilir ya da bir komutu yürütebilir.
- **Arabellek taşması (*Buffer overflow*)** – Arabelleğin kabul edebileceğinden fazla veriyi göndermeye çalışmak, daha fazla açığın oluşabileceği bir durum yaratılmasıdır.
- **İstemci-tarafı saldırısı (*Client-side attack*)** – Bir iç ağda bulunan kullanıcının iş istasyonunda veya diz üstü bilgisayarında bulunan kötücül yazılımı kullanarak, internetteki (korunan ağın dışındaki) kötücül bir sunucu veya uygulama ile birlikte hareket etmek.
- **Çerezler (*Cookies*) ve eklentiler (*Attachments*)** – Çerezleri ve diğer eklentileri (veya içerdikleri bilgileri) güvenliği ihlal etmek için kullanmaktır.
- **Çapraz site betikleme (*Cross site scripting – XSS*)** - Bir web uygulama sunucusuna betikler enjekte edip, saldırıları istemci tarafına yöneltmektir. Bu saldırıda, web uygulamasına değil de sunucunun kullanıcılarını kullanarak sunucuya erişen diğer bilgisayarlara saldırı başlatılır.
- **Dizin gezme/komut enjekte etme (*Directory traversal/command injection*)** - Bir web uygulama sunucusunu istismar ederek, root dosya dizinine korunan ağın dışından erişim sağlamak, sunucuda komut çalıştırmak ve sunucudaki verilerin kopyasını almaktır.
- **Başlık manipülasyonu (*Header manipulation*)** - Çerezleri ve tarayıcı URL adres bilgilerini çalmak ve başlığı geçersiz ve yanlış komutlarla değiştirerek güvensiz bir iletişim veya eylem yaratmaktır.
- **Tamsayı taşması (*Integer overflow*)** – Sistemin izin verdiği en büyük tamsayıyı aşan bir matematiksel arabellek taşması oluşturmaktır. Bu, finansal veya matematiksel uygulamaların donmasını veya bir güvenlik açığı oluşturmasını sağlayabilir.
- **Hafifletilmiş Dizin Erişim Protokolü'ne enjeksiyon (*Lightweight Directory Access Protocol - LDAP*)** – Sahte ya da taklit kimlikler yaratarak, ve LDAP komutlarını ve paketlerini yanlış ID'ler için kimlik doğrulaması yapmak ve bir web uygulamasına kimlik doğrulaması yapmak.
- **Yerel paylaşılan nesneler (*Local shared objects - LSO*)** – Tarayıcının yapılandırma ayarları ile silinemeyen **flash çerezlerini** (adlarını Adobe Flash Oynatıcısından alırlar) kullanmak. Flash çerezler ayrıca kullanıcının sildiği veya engellediği sıradan tarayıcı çerezlerini yerlerine geri koyabilirler.
- **Kötücül eklentiler (*Malicious add-ons*)** – Yasal programların veya uygulamaların üzerinde ek kötücül yazılım çalıştıran takılabilir *(plug-in)* ve eklenti *(add-on)* yazılımları kullanmaktır.
- **SQL enjeksiyonu (*SQL injection*)** – Yapısal Sorgulama Dili (*Structured Query Language* - SQL) komutları enjekte ederek arka uç *(back-end)* SQL veri tabanından bilgi ve veri almaktır.
- **Suyun başı saldırısı (*Watering-hole attack*)** – Hedefteki bir kullanıcıyı sıklıkla ziyaret edilen bir web sitesine çekerek, kullanıcının bu web sitesine yüklenmiş kötücül kod veya yazılıma farkına varmadan tıklayarak bir saldırı başlatmasını sağlamaktır.
- **XML enjeksiyonu (*XML injection*)** – XML etiketlerini *(tags)* ve verilerini bir veri tabanına enjekte ederek veri almaya çalışmaktır.
- **Sıfırıncı-gün (*Zero-day*)** - Henüz belirli bir savunmanın bulunmadığı yeni bir güvenlik açığını veya yazılım hatasını kullanma.

Önlem Nedir?

Kurumunuzu bilgisayar saldırılarından korumanın basit önlemleri yoktur. Güvenlik açıklarını tespit eden, saldırıları engelleyen ve başarılı saldırıların etkilerine başarıyla cevap verebilen karşı önlemler üzerinde yoğunlaşmalısınız. Bu kolay değildir fakat hiçbir şey yapmamaktan daha iyidir. Bilgisayar ve ağ saldırılarıyla başa çıkmak BT alanında iş yapmanın bedelidir.

Zeki saldırganlar ve izinsiz giren kişiler, bilgisayarlara ve ağ kaynaklarına saldırmak için yeni metotlar icat etseler de, bu metotların çoğu zaten bilindiktir ve birkaç uygun araçla yok edilebilirler. En iyi strateji, güvenlik açıklarını tespit etmek ve saldırıları daha olmadan engellemek için açıkların sayısını azaltmaktır.

Saldırıları önlenmek en büyük önceliğiniz olmalıdır. Buna rağmen, bazı saldırılar başarılı olacaktır. Sizin bu saldırılara olan tepkiniz saldırının kendisi kadar saldırgan, proaktif ve reaktif (tepkisel) olmalıdır. Saldırılara, bilgisayar ve ağ kaynaklarını hızlıca yenileyerek, kurumunuzun savunmasındaki boşlukları kapatarak ve suçluları cezalandırmak için gerekli kanıtları toplayarak karşılık verebilirsiniz. Elbette, bir saldırıdan öğrendiğiniz dersleri ağı benzer saldırılardan korumakta kullanmalısınız.

Saldırılara karşılık vermek için planlama, politika oluşturma ve olay yeri inceleme amaçlı çalışmalar yapmanız gerekir. Neyse ki, güvenlik güçleri, olay yeri inceleme uzmanları, güvenlik danışmanları ve bağımsız çalışan uzman ekipler size hem güvenlik ihlaline cevap vermede hem de suçluları yakalamada yardımcı olabilirler. Ayrıca birçok kurum güvenlik ihlalleri ile başa çıkmak üzere uzman ekipler bulundurur. Bu **güvenlik olay müdahale ekipleri (*security incident response team - SIRT*)** ihlalleri tespit etme ve bunların verdiği zararı en aza indirip saldırının kanıtlarını sonraki adli safhalar için koruyabilme konularında bilgilidirler.

Gelecek bölümleri okudukça birçok karşı önlem hakkında bilgi sahibi olacaksınız. Başlangıç olarak, bu bölüm size BT altyapınızı korumak için alabileceğiniz en yaygın bir kaç önlemi tanıtacak. Bu önlemlerden bazılarını aynı zamanda tehditlere, güvenlik açıklarına ve devam eden kötü niyetli saldırılara müdahale etmek için de kullanabilirsiniz.

Kötücül Yazılımı Önlemek

Kötücül yazılım hem kişisel ağlara hem de şirket ağlarına saldırılar için bir platform sunar. Kötücül yazılım karşıtı önlemler bu saldırılara karşı ilk savunma hattıdır. Bulunduğunuz ortama zararlı yazılımların sokulmasını engellemek için adımlar atmalısınız. Kötücül yazılıma engel olmak, kötücül yazılımın verdiği zararı telafi etmekten her zaman daha iyidir. Kötücül yazılıma engel olmak için bir güvenlik programı geliştirmelisiniz.

Kötücül yazılımı engellemek için atılabilecek altı genel adım aşağıda listelenmektedir:

- Kullanıcıların sisteminize kötücül yazılım yüklemelerini engellemek için bir eğitim (bilgi güvenliği farkındalığı) programı oluşturunuz.
- Kötücül yazılım problemleri hakkında düzenli olarak bilgi verici bültenler yayınlayınız.
- Kötücül yazılım karşıtı uygulamalar kurulmamışsa, bilinmeyen veya güvenilmeyen hiçbir kaynaktan dosya transferi yapmayınız. (Bu kötücül yazılım karşıtı programlar hakkında birazdan bilgi alacaksınız.)
- Üretim ortamına dâhil etmeden önce, yeni programları ve şüpheli dosyaları önce karantina altına alınmış -ağınızın hiçbir yerine bağlı olmayan- bir bilgisayarda test ediniz veya açınız.

- Anti-malware yazılım kurunuz. Bu yazılımın ve verisinin güncel olduğundan emin olunuz. Kötü niyetli kullanıcıların sisteme kötücül yazılım sokmalarına engel olmak ve var olan kötücül yazılımları tespit etmek için düzenli olarak güvenlik taraması yaptırınız.
- Güvenli bir giriş ve kimlik doğrulama sistemi kullanınız.

Kötücül yazılımlar ile başa çıkmada başka bir önemli taktik kötücül yazılım konusundaki gelişmeleri yakından takip etmektir. Haftalık bilgisayar dergilerini okuyarak veya US-CERT veya Ulusal Siber Güvenlik İttifakı (National Cyber Security Alliance - NCSA) gibi organizasyonlara katılarak en son kötücül yazılımlar hakkında bilgi alınız. Ayrıca, kötücül yazılımlar hakkında bilgi almak için aşağıdaki web sitelerini sık sık ziyaret ediniz:

- **Ulusal Siber Güvenlik İttifakı – (*National Cyber Security Alliance* – NCSA)** – *www.staysafeonline.org.*
- **Birleşik Devletler Bilgisayar Acil Durum Hazırlık Takımı – (*United States Computer Emergency Readiness Team* – US-CERT)** – *http://us-cert.gov*

Ayrıca, sisteminizdeki anti-malware (kötücül yazılımla mücadele programını) kullanarak, iş istasyonlarına ve mail sunucularına sokulan bütün dosyaları tarayınız. (Bu tür yazılımların genel adı anti-virüs yazılımlarıdır fakat bugünün anti-virüs yazılımları genellikle sadece virüslerle uğraşmazlar. Bu nedenle, anti-malware demek daha doğrudur.) Çoğu yönetici anti-malware programlarını ağın birçok noktasında kullanır. Bu programlar aşağıdakileri içerir:

- **BitDefender** – *www.bitdefender.com.*
- **Kaspersky Antivirüs** – *www.kaspersky.com.*
- **Webroot Antivirüs**– *www.webroot.com.*
- **Norton Antivirüs** – *www.symantec.com/norton/antivirus.com.*
- **Eset Nod32 Antivirüs** – *www.eset.com.*
- **Avg Antivirüs** – *www.avg.com.*
- **G DATA Antivirüs** – *www.gdatasoftware.com.*
- **Avira Antivirüs** – *www.avira.com.*
- **McAfee Endpoint Protection** – *www.mcafee.com.*
- **Trend Micro** – *www.trendmicro.com.*
- **Microsoft Security Essentials** – *www.microsoft.com/security_essentials.*

Bazı anti-malware yazılımları bir dosya tarafından gerçekleştirilen eylemleri inceleyerek dosyanın kötücül yazılım olup olmadığına karar verir. Bu tür anti-malware programları sezgisel *(heuristic) analiz* denen bir yöntem kullanarak programların kötücül yazılım gibi "davranıp davranmadıklarını" inceler. Diğer bazı programlar, programları ve dosyaları bilinen kötücül yazılımlarla karşılaştırarak kötücül yazılım tespit ederler. Sorun şudur ki, bu yazılımlar yeni yaratılmış kötücül yazılımların davranışlarını hemen tanıyıp karşı tedbirler alamayabilirler. Anti-malware programı, imza veri tabanını bu yeni türleri içerecek biçimde güncellemelidir. Saldırganlar sürekli yeni kötücül yazılımlar yarattıkları için, anti-malware programınızın güncel olması çok önemlidir. Etkili bir yöntem sisteme her giriş yaptığınızda anti-malware programını güncelleyip sistemde tarama yaptırmaktır.

NOT

Anti-malware programlarının kullanıcı yorumlarını Web'de bulabilirsiniz. Bu konuda diğer kullanıcıların yorumlarını bulunduran iki popüler site www.star-reviews.com ve http://anti-virus-software-review.toptenreviews.com'dir. Gereksinimleri ve kullanım koşulları sizinkilere benzer olan kişilerin yazdıkları yorumlar, kurumunuz için ürün seçmede size yol gösterebilir.

Unutmayınız ki sisteminizdeki bir kötücül uygulamayı tespit edip imha etseniz dahi, bu kötücül yazılım kurumun başka bir kısmında sisteme yeniden bulaşmak veya saldırmak için pusuda bekliyor olabilir. Bu durum özellikle ortak çalışma alanları için geçerlidir; virüs içeren dosyalar ana sunucuda tutulup ağ üzerinden dağıtılıyor olabilir. Bu bulaşma-tespit-kaldırma-imha süreci siz kötücül yazılımı bütün sistemden atıncaya dek defalarca tekrarlanabilir. Sisteminizin herhangi bir yerinde kötücül yazılım bulursanız, depolama cihazları da dâhil olmak üzere bütün sisteminizi taramalısınız.

Sisteminizi Güvenlik Duvarları ile Korumak

Bir **güvenlik duvarı (firewall)** ağ üzerinden geçen trafiği inceleyip, sizin yapılandırma ayarlarında belirlediğiniz kurallara göre geçen trafiği reddeden veya kabul eden bir program veya bu amaç için ayrılmış bir donanım cihazıdır. Bir güvenlik duvarının temel görevi, farklı güven seviyelerine sahip olan bilgisayar ağları arasındaki trafik akışını düzenlemektir, iç ağın internetle buluştuğu yer olan LAN-dan-WAN-a bölümü ile WAN bölümü arasındaki trafik gibi.

Birçok ticari güvenlik duvarı bulunmaktadır. Önemli güvenlik duvarı üreticileri aşağıda listelenmiştir:

- **Palo Alto Networks** – *www.paloaltonetworks.com.*
- **Cisco Systems** –*www.cisco.com.*
- **SonicWall** – *www.sonicwall.com.*
- **WatchGuardTechnologies** – *www.watchguard.com.*
- **Check Point** – *www.checkpoint.com.*
- **ZyXel** – *www.zyxel.com.*
- **NetGear** – *www.netgear.com.*
- **Juniper Networks** – *www.juniper.net.*
- **DLink** – *www.dlink.com.*
- **MultiTech Systems** – *www.multitech.com.*

BÖLÜM ÖZETİ

BT altyapısının ve varlıklarının yedi etki alanındaki riskler, tehditler ve güvenlik açıkları her gün karşılaşılan sorunlardır. Kurumların ve kişisel kullanıcıların kendilerine ait olan riskleri, tehditleri ve güvenlik açıklarını tespit edip, bunların getireceği sorunlarla başa çıkmak için planlar geliştirmeleri gerekmektedir.

Çok farklı tehdit türleri bulunmaktadır. Bunlar, gizlilik tehditlerini, bütünlük tehditlerini ve kullanılabilirlik tehditlerini içermektedir. Ek olarak, kötücül saldırı tehdidi bulunmaktadır. Kötücül saldırılar, yerine geçme, IP adres aldatması, oturum ele geçirme, yeniden gönderme, ortadaki adam, sözlük parola saldırıları gibi aktif tehditler olabilir. Pasif tehditler, ortam dinlemesi ve izlemesini içerebilir. Virüsler, en yaygın ve en sık karşılaşılan saldırı türüdür. Anti-malware yazılımı virüs saldırıları ile başa çıkmanın en etkili yöntemidir. En kolay hedef, güvenlik tehditlerinden haberdar olmayan kullanıcılardır. İnternete bağlanan kullanıcıların sayısı arttıkça bu tehdit hedefleri

artmaktadır. Genel olarak hedefler, bilgisayar sistemlerini, ağ bileşenlerini, yazılımı, elektrik sistemlerini ve veri tabanlarını içerir. Siyah şapka bilgisayar korsanları,beyaz şapka bilgisayar korsanları, gri şapka bilgisayar korsanları, betik kerataları ve kırıcılar saldırıları başlatabilirler.

ANAHTAR KAVRAMLAR VE TERİMLER

Adware – Reklam yazılımı
Application attacks – Uygulama saldırıları
Arbitrary code execution – İsteğe bağlı kod yürütme
Armored virüs – Zırhlı virüs
Address resolution protocol (ARP) poisoning – Adres çözümleme protokol zehirlenmesi (ARP)
Asset - Varlık
Attack - Saldırı
Backdoor – Arka kapı
Birthday attack – Doğum günü saldırısı
Black-hat hacker – Siyah şapka bilgisayar korsanı
Bluejacking - Bluejacking
Bluesnarfing - Bluesnarfing
Botnets – Botnetler
Brute-force password attack – Brute force parola saldırısı
Buffer overflow – Arabellek taşması
Christmas attack – Christmas saldırısı
Client-side attack – İstemci tarafı saldırısı
Command injection – Komut enjeksiyonu
Cookie - Çerez
Cracker - Kırıcı
Cross-site scripting (XSS) – Çapraz site betikleme
Cryptographic hash -Kriptografik özet
Cryptolocker – Kripto kilitleyici
Denial of service (DoS) – Hizmet reddi
Dictionary password attack – Sözlük parola saldırısı
Directory traversal – Dizin gezme
Disclosure - İfşa
Distributed denial of service (DDoS) – Dağıtık hizmet reddi
DNS poisoning – DNS zehirlenmesi
Dumpster diving – Çöp karıştırma
Ethical hacker – Etik bilgisayar korsanı
Evil twin – Kötü ikiz
Exploit software – İstismar yazılımı
Familiarity - Yakınlık
Firewall – Güvenlik duvarı
Flash cookies – Flash çerezler
Gray-hat hacker – Gri şapka bilgisayar korsanı
Hacker – Bilgisayar korsanı
Header manipulation – Başlık manipülasyonu
Hijacking – Ele geçirme
Hoax - Aldatma
Identity theft – Kimlik hırsızlığı
Impersonation – Taklit etme
Insider threat – İçerideki tehdit
Integer overflow – Tamsayı taşması
Intellectual property – Fikri mülkiyet
Intrusive penetration testing – İzinsiz sızma testi
IV attack – IV saldırısı
Jamming – Frekans bozumu
Keystroke logger – Tuşa basma kaydedicisi
LDAP injection – LDAP enjeksiyonu
Local shared objects (LSO) – Yerel paylaşılan nesneler (LSO)
Malicious add-ons – Kötücül eklentiler
Malicious software – Kötücül yazılım
Malware – Kötücül yazılım/ Malware
Man-in-the-middle attack – Ortadaki adam saldırısı
Masquerade attack – Yerine geçme saldırısı
National Vulnerability Database (NVD) – Ulusal Güvenlik Açıkları Veritabanı (NVD)
Near field communication attack – Yakın alan iletişim saldırısı
Netcat - Netcat
Operating system (OS) fingerprint scanner – İşletim sistemi (OS) parmak izi tarayıcısı
Opportunity cost – Fırsat maliyeti
Packet sniffer – Paket koklayıcı
Password cracker – Parola kırıcı
Personally identifiable information (PII) – Kişisel tanımlama bilgisi
Pharming – Web sitesi trafiğinin yönlendirilmesi
Phishing - Oltalama
Phreaking – Telefon şebekelerine yasadışı girme
Polymorphic malware – Çok biçimli kötücül yazılım
Popup – Açılır pencere
Port scanner – Port tarayıcı
Promiscuous mode – Karışık mod
Protocol analyzer – Protokol çözümleyici
Ransomware – Fidye yazılımı
Remote code execution – Uzaktan kod yürütme

ANAHTAR KAVRAMLAR VE TERİMLER, *devamı*

Replay attack – Yeniden gönderme saldırısı
Rogue access points – Sahte erişim noktaları
Rootkit - Rootkit
Scarcity – Yetersizlik
Script kiddie – Betik keratası
Security breach – Güvenlik ihlali
Security incident response team (SIRT) – Güvenlik olay müdahale ekibi (SIRT)
Session hijacking – Oturum ele geçirme
Shoulder surfing – Omuz sörfü
Smurfing - Smurfing
Sniffer – Koklayıcı
Social engineering – Sosyal mühendislik
Spam – Spam
Spear phishing – Hedef odaklı oltalama
Spim - Spim
Spoofing - Yanıltma
Spyware – Casus yazılım
SQL injection – SQL enjeksiyonu
SYN flood – SYN taşkını
Tailgating – Öndeki kişinin yakınından gitmek
Transitive access – Geçişli erişim
Trojan – Truva atı
True downtime cost – Gerçek kesinti maliyeti
Trust - Güven
Typo squatting – URL kaçırma/Sahte URL
Urgency – Aciliyet/Öncelik
URL hijacking – URL ele geçirmesi
Vishing – Telefonla kişisel bilgilerin ele geçirilmesi
Vulnerability scanner – Güvenlik açığı tarayıcısı
Wannabe – (Bilgisayar korsanı omaya çalışan) Özenti
War chalking – War chalking
War driving – War driving
Wardialer – Otomatik numara çevirici
Watering hole attack – Suyun başı saldırısı
Whaling – Balina avı
White-hat hacker – Beyaz şapka bilgisayar korsanı
Wiretapping – Telefon dinleme
Xmas attack – Christmas/ Noel saldırısı
XML injection – XML enjeksiyonu
Zero-day – Sıfırıncı gün

BÖLÜM 3 DEĞERLENDİRME

1. Korsanların asıl amacı BT varlıklarına sızarak bozmak ve muhtemelen veri çalmaktır.
   A. Doğru
   B. Yanlış

2. Aşağıdakilerden hangisi fikri mülkiyeti en iyi tanımlamaktadır?
   A. Bir işletmenin telif hakkını aldığı şeyler
   B. İşletmenin sahip olduğu bütün patentler
   C. Bir işletim sürecinin nasıl yapıldığı bilgisi
   D. Müşteri listeleri
   E. Hepsi

3. Aşağıdakilerden hangisi korsanlık için çok az yeteneğe sahip olan bir kişiyi ifade etmektedir?
   A. Siyah şapka bilgisayar korsanı
   B. Betik keratası
   C. Kırıcı
   D. Gri şapka bilgisayar korsanı
   E. Hepsi

4. Bir _____ ağdaki paketleri yakalamaya yarayan bir yazılım aracıdır.

5. Hangi saldırı türü gerçek kullanıcıların sistemdeki bir kaynağa erişememelerine neden olur?
   A. Dağıtık hizmet reddi saldırısı
   B. Sosyal mühendislik
   C. Ortadaki adam
   D. Oltalama e-postaları
   E. SQL enjeksiyonu

6. Bir SYN taşkını saldırısı hedefi geçersiz veya yarı açık TCP bağlantı istekleri ile boğar.
   A. Doğru
   B. Yanlış

7. Aşağıdakilerden hangisi bir sosyal mühendislik örneğidir?
   A. SQL enjeksiyonu
   B. XML enjeksiyonu
   C. Güvenlik tasarımı
   D. Kişiyi taklit etme
   E. Hepsi

8. Kötücül yazılıma karşı koruma için aşağıdaki karşı tedbirlerden hangisi en iyisidir?
   A. Anti-virüs/anti-malware koruması
   B. Veri sızmasını önleme
   C. Dizüstü bilgisayarların ve iş istasyonlarının tüm kurumda aynı özelliklere sahip olması
   D. Güvenlik farkındalığı eğitimi
   E. Hepsi

9. War driving herkese açık veya şifresiz kablosuz ağlar aramayı içerir.
   A. Doğru
   B. Yanlış

10. Aşağıdakilerden hangisi hizmet sunabilmeyi etkiler?
   A. Çapraz site betikleme
   B. SQL enjeksiyonu
   C. Dağıtık hizmet reddi saldırısı
   D. Paket yoklayıcı
   E. Hiçbiri

11. Hangi saldırı türü ağdaki veri paketlerini yakalayıp yetki almadan bir iş yapmak için bunları yeniden iletmeyi içerir?
   A. Ortadaki adam
   B. SYN taşkını
   C. Yeniden oynatma
   D. Smurfing
   E. SQL enjeksiyonu

12. Bir _____, bir varlığa zarar verebilecek herhangi bir eylemdir.

13. Bir _____, bir bilgisayara veya bir ağa bir tehdidin zarar vermesini mümkün hale getirecek herhangi bir zayıflıktır.

14. Hangi kötücül yazılım türü kendisini çoğaltıp kopyalarını, genellikle bir ağ üzerinden, diğer bilgisayarlara gönderen bağımsız *(self-contained)* bir programdır?
   A. Virüs
   B. Solucan
   C. Truva atı
   D. Rootkit
   E. Çerez manipülasyonu

15. Hangi kötücül yazılım türü şifreleme anahtarını vermek için kullanıcıyı veya kurumu para ödemeye zorlar?
   A. Virüs
   B. Truva atı
   C. Mantık bombası
   D. Kripto-kilitleyici kötücül yazılım
   E. Kâbusunuz olan virüs

BÖLÜM

4 Bilgi Güvenliği İş Sürücüleri

Her kurum iş hedeflerini karşılamak için görevlerini yerine getirmektedir. Hedefler olmadan, kurumların bir amacı yoktur. Kurumunuzdaki iş hedeflerinizi destekleyen elemanları tanımlamak zorundasınız.

Bu elemanlar kurumunuzun **iş sürücüleridir (*business drivers*)**. İş sürücüleri, iş hedeflerini destekleyen insan, bilgi ve koşulları içermektedir. Bilgi güvenliği etkinlikleri, uygunluk ve fikri mülkiyetin korunmasına yönelik çabalar dahil olmak üzere birçok ortak iş sürücüsünü doğrudan desteklemektedir. Güvenlik etkinlikleri aynı zamanda iş sürücülerini olumsuz etkileyebilir, bu da iş hedeflerinizi karşılamayı zorlaştırır.

Bazı dış gereksinimler kurumunuzun kendi görevlerini nasıl yerine getirdiğini yönlendirebilir. Bu gereksinimler, kanunlardan, düzenlemelerden, endüstri taleplerinden veya kendi standartlarınızdan gelebilir. Her kurumun uymak zorunda olduğu bazı gereksinimler vardır. Kurumunuzun gereksinimleri karşılamak için birden çok yolu vardır. Birçok yönetmelik, iş kesintilerini veya olağanüstü durumları idare etmek için planlar geliştirmenizi gerektirebilir. Gerçekte, bir kesilmeden sonra operasyonları eski durumuna getiren çoğu etkinlik birçok gereksinimi karşılamaktadır.

Uyumluluk gereksinimlerini karşılamak için her zaman farklı kontroller düşününüz. Güvenlik etkinliklerinin, işletmenize yön veren amaçlarınız üzerindeki etkisini dengelemeniz bilgi güvenliğinizi korumanız için önemlidir. Bu bölümde, güvenlik ilişkili iş sürücüleri hakkında ve bunların bütün iş sürücülerini nasıl etkilediğini öğreneceksiniz.

4. Bölüm Konular

Bu bölüm aşağıda verilen konuları ve kavramları içermektedir:

- Risk yönetimi nedir
- BIA, BCP ve DRP birbirinden nasıl farklıdır ve aynıdır
- Risklerin, tehditlerin ve güvenlik açıklarının bir kurum üzerindeki etkileri nasıl tanımlanır
- Bilgi güvenliği boşluğu nasıl kapatılır
- Risk nasıl azaltılır ve kanunlar, yönetmelikler ve gereksinimlerle uyumluluk nasıl başarılır
- Kişisel veri nasıl gizli tutulur
- Mobil çalışanların ve kişisel cihazların kullanımının riski nasıl azaltılır

4. Bölüm Hedefler

Bu bölümü tamamladığınız zaman yapabilecekleriniz:

- Risk yönetimini ve kurumların risk yönetimine yaklaşım yollarını tanımlamak
- BIA, BCP ve DRP'yi birbirlerinden ayırt etmek ve bunları birbirleriyle karşılaştırmak
- Risklerin, tehditlerin ve güvenlik açıklarının BT altyapısı üzerindeki etkilerini tanımlamak
- Kabul edilebilir bir riski veya yükümlülüğü tanımlamak
- Bilgi güvenliği boşluğunu risk azaltma stratejilerine bağlı olarak küçültmek
- Uyumluluk kanunlarına ve yönetime (politikalar, standartlar, yöntemler ve yönergeler) bağlı kalmak
- Riski, devam eden güvenlik operasyonlarının bir parçası olarak yönetmek ve azaltmak
- BT altyapınız için tanımlanan CIA hedefleriyle nasıl uyum sağlayacağınızı belirlemek
- Mobil çalışanlar ve kişisel olarak sahip olunan cihazların kullanımı ile ilgili riskleri tanımlamak

Risk Yönetimini Tanımlamak

Risk yönetimi (*risk management*), risklerin tanımlanması, değerlendirilmesi, önceliklendirilmesi ve ele alınması sürecidir. Güvenlik konusunda ciddi olan herhangi bir kurum, risk yönetimini devam eden bir süreç olarak görür.

Risk yönetimi sadece bir kere yaptığınız bir şey değildir. Risk yönetimi sürecinin her bir parçası ayrıdır ancak birçok kez gerçekleşebilir ve gerçekleşecektir. Risk yönetimi, kurumunuzda en çok etkisi olabilecek riskleri planladığınızı garantiye almaktadır. Güvenli bir kurumun, olaylar olmadan önce riskleri ele almak için mevcut planları vardır. Böylece, güvenliği stratejik iş hedefleriyle uyumlu hale getiren kurumlar, iş başarısını riski azaltarak sürdürebilir.

Her işletme, fikri mülkiyet, altyapı ve tesisler veya çalışanlar olmak üzere varlıklara veya kaynaklara sahiptir. Risk, belirsiz bir olayın bir veya daha fazla kaynağı etkileme olasılığıdır. Pek çok insan riskleri olumsuz etkiler açısından görmektedir. Bununla birlikte, **Proje Yönetimi Enstitüsü (*Project Management Institute* - PMI)** tarafından yürütülen proje yönetimi için en iyi uygulamalar yönergesi olan **Proje Yönetimi Bilgi Tabanı (*Project Management Body of Knowledge* - PMBOK)**, riskin etkilerinin olumlu veya olumsuz olabileceğini belirtmektedir. PMI, risk yönetimi felsefesini, aşağıdakileri aynı anda yaparak proaktif bir yaklaşıma dayandırır:

- Olumsuz risklerin etkilerini azaltmak
- Olumlu risklerin etkilerini çoğaltmak

Risklerin geleneksel görünümünü düşününüz. **ŞEKİL 4-1** riskler, tehdiler ve güvenlik açıkları arasındaki geleneksel ilişkileri göstermektedir.

Şekilde gösterildiği gibi, risk denklemi aşağıdaki gibidir:

Risk = Tehditler × Güvenlik Açıkları



ŞEKİL 4-1 Riskler, tehditler, ve güvenlik açıkları.

Bir *tehdit (threat)*, herhangi bir olayın meydana gelme sıklığıdır. Bir çok durumda, tehdit denklemindeki olaylar olumsuzdur veya aykırı olaylardır. *Güvenlik açığı (vulnerability)*, belirli bir tehditin başarılı bir şekilde gerçekleşmesi olasılığıdır. Bir tehdit olasılığının ve güvenlik açığının olma olasılığının çarpımı, belirli bir olayın *riskini* belirlemektedir. Riskler, belirli varlıklar ve kaynaklar için geçerlidir. Eğer risk olasılığını varlığının değeri ile çarparsanız, sonuç belirli bir riske maruz kalmaktan dolayı beklenen kayıptır.

Birçok insan riski hiçbir zaman olumlu bir şey olarak düşünmez. Bununla birlikte, belirsizlik *(uncertainty)* olumsuz *veya* olumlu etkileri olan olaylar ile sonuçlanabilir. Örneğin, kurumunuzun yazılım satıcınız tarafından öngörülen kullanılabilirliğe bağlı olarak son kullanıcılarınıza yeni bir yazılım dağıtmayı planladığını varsayalım. Risk yönetimi planınız hem erken hem de geç gerçekleşecek bir yazılım dağıtımına verilen yanıtları ele almalıdır. Eğer yazılımı erkenden alırsanız, ya daha kapsamlı bir sınama gerçekleştirirsiniz ya da kuruluma erken başlarsınız. Eğer yazılım sağlayıcınız yazılımı size teslim etmede gecikirse, öngörülen kurulum tarihini kaçırabilirsiniz. Zamanlamanızla uyuşmayan bir teslim tarihinin hem olumlu hem de olumsuz etkilerini ele almak için planlarınız olmalıdır.

Bir **risk metodolojisi (*risk methodology*)**, riski nasıl yöneteceğinizin bir tanımıdır. Kurumunuzun hayata geçireceği risk metodolojisi, yaklaşımı, gerekli bilgiyi ve her bir riski ele almak için teknikleri içermelidir. Yaklaşım, risk metodolojisi sürecinin adımlarını nasıl yürüteceğinizi tanımlamaktadır. Örneğin, yaklaşım, risk analizinin belirli aralıklarla gerçekleştirileceğini belirtebilir. Bu analizi yürütmek için gerekli araçlar, riskleri tanımlayan, sınıflandıran ve sıralayan belgeleri içerebilir. Bu yaklaşım, PMI'nın PMBOK'u ile uyumludur. PMI yaklaşımı her şeyi yapmanın tek yolu değildir, genel olarak risk yönetimi de dahil olmak üzere proje yönetimine kuralcı bir yaklaşım getirmektedir.

Risk tanımlama sürecinin sonucu, tespit edilen risklerin bir listesidir. PMI bu listeyi **risk kayıtçısı (*risk register*)** olarak tanımlamaktadır. Risk kayıtçısı birçok farklı türde bilgi içerebilir, ancak en azından aşağıdaki listelenenleri içermelidir:

- Riskin bir tanımı
- İlgili olay meydana gelirse beklenen etki
- Olayın meydana gelme olasılığı
- Riski azaltmak için atılabilecek adımlar
- Olayın gerçekleşmesi durumunda atılması gereken adımlar
- Riskin derecesi

Kurumunuzun herhangi bir riski yanıtlama yeteneği, potansiyel riskleri ne kadar iyi tanımladığınız ile başlamaktadır. Risk kayıtçısı girdisi isterken yaratıcı olunuz. Birden fazla bakış açısı

kullanmak size daha kapsamlı bir yanıt planı verecektir. Aşağıdaki listelenenler de dahil olmak üzere birçok yerde risk kayıtçısına girdiler isteyebilirsiniz:

- Risk tanımlama beyin fırtınası toplantıları
- Resmi anketler
- Gayri resmi anketler ve yorumlar için talepler
- Yorum ve geri bildirim toplamak için bir forum içeren "öğle yemeği ve öğrenme" oturumları gibi teşvik edilen etkinlikler

Kurumunuzun üst yönetiminin desteğine sahip olduğunuzdan emin olmak çok önemlidir. Yönetimin desteği olmadan, muhtemelen iyi bir risk yönetimi planı oluşturmak için gerekli adımları atma yetkiniz yok demektir. Bu risk tanımlama faaliyetlerinde baştan itibaren tam yönetim desteğine sahip olmanın avantajlarından yararlanacaksınız. Yönetim, sonradan akla gelen bir düşünce olarak değerlendirilmemelidir.

Bilgi toplama süreci devam ettikçe, gittikçe daha fazla insan sürece katılmaya başlamalıdır. Bununla birlikte, daha büyük gruplar, katılımcıları kurumunuzdaki güvenlik açıkları hakkında konuşmaktan vazgeçirebilir. Misillemeden veya başkalarının kendilerini şikayetçi olarak göreceğinden korkabilirler. Özellikle bir tekniğin, **Delphi metodu**'nun, ihtiyacınız olan gerçek sonuçları ürettiğini anlayabilirsiniz. Bu metot, görüş ve bilgi toplamak için birden fazla turda resmi anonim anketlerin kullanılmasına yönelik bir yaklaşımdır. Anketler anonim olduğu için, yöntem gerçek yanıtları teşvik etmektedir. Bir panel, anket yanıtlarının her turunu incelemekte ve bir önceki turun sonuçlarına dayanan yeni bir anket oluşturmaktadır. Birden fazla tur, endişe uyandıran alanlara odaklanmanıza ve birtakım konu uzmanlarından ayrıntılı bilgi toplamanıza izin vermektedir.

Risk yönetiminin ne olduğunu artık bildiğinize göre, risklerin bir BT altyapısının yedi etki alanının her birine nasıl uygulanacağını değerlendirmek önemlidir. Bu süreç, Kullanıcı, İş İstasyonu, LAN, LAN-dan-WAN-a, WAN, Uzaktan Erişim ve Sistem/Uygulama etki alanlarının bir risk, tehdit ve güvenlik açığı analizi veya değerlendirmesi ile başlamaktadır. Bir risk analizi ve risk değerlendirmesi gerçekleştirmek daha sonraki bir bölümde anlatılmaktadır.

Bir BIA, BCP ve DRP Gerçekleştirmek

Risk yönetiminin önceliği, gerçekleşen tehditleri önlemektir. Kayıba neden olan her olayı öngörmek ve önlemek mümkün değildir. Bu durum, herhangi bir kurumun normal ticari işlemleri kesintiye uğratacak bir olayla karşılaşma ihtimalinin hala devam ettiği anlamına gelmektedir. Bilgi güvenliği, herhangi bir yetkili kullanıcının bilgiye ihtiyaç duyduğu durumlarda tüm bilgilerin kullanılabilir olmasını gerektirmektedir. Kuruluşun BT kaynaklarını korumak ve olayların normal iş fonksiyonlarını kesintiye uğratmaması için yöntemler ve teknikler geliştirmeniz ve uygulamanız gerekir.

İş Etki Analizi

Kesintileri gidermek için planlar geliştirmenin ilk adımı, kurumunuz için çok önemli olan iş fonksiyonlarını tanımlamaktır. Kurumunuzun bazı faaliyetleri işletmenin işleyişi için kritik önem taşımakta, ve bazıları da taşımamaktadır. Bir olay, kuruluşunuzun işlemleri yürütme becerisini kesintiye uğrattığında, önce en önemli işlemleri geri yüklemek önemlidir. Bunu yapmadan önce bu işlevlerin neler olduğunu belirlemelisiniz.

Bir *iş etki analizi* (*business impact analysis* - BIA), bir kurumun işlevlerini ve faaliyetlerini kritik veya kritik olmayan olarak sınıflandıran bir resmi analizdir. BIA, iş sürekliliği ve felaket kurtarma için bir yol haritası tanımlamaya yardımcı olmaktadır. İşletmeyi çalıştırmak için kritik işlevler gereklidir. Eğer kritik bir işlevi yerine getiremezseniz, kabul edilemez bir hasara neden olur. Kritik olmayan işlevler önemli olabilir ve bunlar yoksa onları gözden kaçırmış olabilirsiniz, ancak bunların yokluğu bir kurumun işi yürütmesini durdurmaz. Bir BIA, kritik faaliyetleri önem temelinde düzenlemekte ve büyük bir kesinti olması durumunda kuruma hangi işlevlerin hangi sırada geri yükleneceklerini belirlemesinde yardımcı olmaktadır. BIA'lar ayrıca, risk yönetimi ve olay müdahale planlaması ile kurumlara yardımcı olur.

BIA'da her kritik işlev, kendi kurtarma hedefleri ve her bir işlev için gerekliliklerin açıklaması da dahil olmak üzere, kendi bölümünde tam olarak tanımlanmıştır. Kurtarma hedefleri ve gereksinimleri aşağıdaki şekilde ifade edilmiştir:

- **Kurtarma noktası hedefi (*Recovery point objective* - RPO)**—Zaman olarak ölçülen RPO, kabul edilebilir maksimum veri kaybı miktarıdır. İşlevin niteliğine bağlı olarak, personel üyeler, verileri yeniden yaratabilir veya tekrar girebilir. RPO, verilerin nasıl yedekleneceği, kurtarma politikaları ve kayıp önlemenin mi veya kayıp düzeltmenin mi daha iyi bir seçenek olduğu konusunda yönlendirme sağlamaktadır.
- **Kurtarma zamanı süresi (*Recovery time objective* - RTO)**—RTO, işlevi kurtarmak için izin verilen maksimum süreyi ifade eder. Daha az resmi kurtarma planlarının pek çoğu RTO'yu gözden kaçırmaktadır. Zaman kritik bir faktör olabilir ve kurtarma süresi için gereksinimlerin belirlenmesi en iyi kurtarma seçeneklerini belirlemeye yardımcı olmaktadır.
- **İş kurtarma gereksinimleri**—Bu gereksinimler, belirtilen kurtarma işlevinin gerçekleşmesi için halihazırda yerine getirilmesi gereken diğer tüm iş fonksiyonlarını tanımlamaktadır. İş kurtarma gereksinimleri, kurtarma sırasının belirlenmesine yardımcı olmaktadır.
- **Teknik kurtarma gereksinimleri**—Teknik kurtarma gereksinimleri, her kritik iş fonksiyonunu desteklemek için gerekli teknik ön koşulları tanımlamaktadır. Çoğu durumda, teknik kurtarma gereksinimleri hangi BT altyapısı bileşenlerinin bulunması gerektiğini belirlemektedir.

Bir kurum için kritik olan operasyonların ve işlevlerin devam edebilmesinin sağlanması kurumun hayatta kalması için çok önemlidir. BIA, yalnızca hangi işlevlerin kritik olduğunu değil, aynı zamanda önemli iş fonksiyonlarının ne kadar hızlı bir şekilde büyük bir kesintinin ardından tam çalışmaya dönmesi gerektiğini de belirlemeye yardımcı olacaktır. BIA ayrıca, her bir işlevi tam çalışmaya döndürmek için kaynak gereksinimlerini belirleyecektir. BIA'lar, genel olarak, her etkinliği veya fonksiyonu destekleyen fiziki altyapının herhangi bir veri ile birlikte tahrip edildiği bir en kötü durum senaryosunu varsaymaktadır. Herhangi bir kesinti süresini planlamayı seçebilirsiniz, ancak birçok BIA'da, restorasyon planları, birincil kaynaklara erişimin en az 30 gün boyunca mümkün olmayacağını varsaymaktadır. Başka bir deyişle, eksiksiz bir BIA, normal altyapı kullanılamadığında uzun bir süre iş yapmak için gerekli gereksinimleri gösterecektir.

İş Sürekliliği Planı

Bir *iş sürekliliği planı* (*business continuity plan* - BCP), kritik iş faaliyetlerine veya fonksiyonlarına ara veren herhangi bir olaya yapısal bir yanıt vermek için hazırlanmış yazılı bir plandır. Bir BIA

gerçekleştirmek, BIA'nın bir BCP'nin gerekli olduğu kaynakları tanımlamasından dolayı bir BCP oluşturmaya yönelik önemli bir ilk adımdır.

Bir kurumun hayatta kalmasında kritik olmayan kaynaklara yönelik olarak bir BCP geliştirilmesi için genellikle hiçbir sebep yoktur. BCP, öncelikle, işletmenin yaşayabilirliğini etkileyen bir kesinti olduğunda, kritik iş faaliyetlerini yürütmeye devam etmek için gerekli olan süreçleri, kaynakları, ekipman ve cihazları ele almaktadır.

Herhangi bir BCP'nin en önemli kısmı, insanlar her zaman önce gelir anlayışı ile önceliklerin ayarlanmasıdır. İstisna yoktur. İş kesintilerini ve felaketleri ele alan herhangi bir plan, kurum personelinin güvenliğini ve refahını en yüksek önceliğe yerleştirmelidir. Diğer tüm endişeler ikincildir. İyi dengelenmiş bir BCP için öncelikler sırası aşağıdaki şekilde olmalıdır:

- İnsanların güvenliği ve esenliği
- Kritik iş fonksiyonlarının ve operasyonların sürekliliği, ister yerinde ister dışında olsun, ister manuel ya da BT sistemlerine bağımlı olsun
- Bir BT altyapısının yedi etki alanı içerisindeki BT altyapı bileşenlerinin sürekliliği

Bir sonraki kategoriye geçmeden önce her kategorinin ihtiyaçlarını belirlemelisiniz. Koşullar insanlar için tehlikeli ise, bu insanlar verimli bir şey yapamazlar. Personeliniz güvende olmasına rağmen binanız hasar görürse, sunucuların veya ağ donanımının yerini değiştiremezsiniz. Hasarın onarılmasını ya da kurumun altyapı bileşenlerini geri yüklemek üzere taşınmasını beklemelisiniz. İş süreci kesintilerinden kaçınmak için planlar geliştirirken kaynak önceliği sırasını aklınızda tutmalısınız.

Resmi bir BCP sadece birçok kurum için yararlı değildir, bazı durumlarda gerekli olmaktadır. Mevzuat ve yönetmelikler, sistemlerin güvenliğini sağlamak için genellikle bir BCP'ye gerek duymaktadır. Bugünün kurumları BT kaynaklarına artan bir biçimde güvenmekte ve iş yapmak için eksiksiz bir BT altyapısına gerek duymaktadır. Bu şirketler için sistemin aksama *(downtime)* maliyeti çok büyük olabilir. Aksama süresi ile ilişkili doğrudan ve dolaylı maliyetler aşağıdakileri içeren çeşitli kategorilerde mevcut olabilir:

- Kayıp müşteriler
- Kayıp gelir
- Kaybedilen pazar payı
- Ek harcamalar
- Zarar gören itibar

Organizasyonlar, acil durum ve kurtarma planlarını kapsamlı bir bakış açısından değerlendirmelidir. Planlar, başkalarının dışlanması için bireysel kaynaklara odaklanamaz. Acil durum ve kurtarma planlarının her bir bileşeni genellikle belirli kaynakları ele alıyor olmasına rağmen, bunu daha geniş bir bağlamda yapmaları gerekmektedir. Plan geliştirme sırasında daha geniş bağlamı göz önünde tutmak, yalnızca bozuk bir kaynağı düzeltmek yerine, bir organizasyonun risklerini belirlemenizi sağlamaktadır.

NOT

Doğrudan (*direct*) maliyetler, kan düşüren acil giderlerdir. Dolaylı (*indirect*) maliyetler, müşteri kaybı gibi genel gelir akışını etkilemektedir, ancak masraf kayıtları olmadığından hesaplamak daha zordur. Dolaylı maliyetler söz konusu olduğunda, potansiyel satışların asla gerçekleşmemesi olasılığı bir etkidir.

Eksiksiz bir BCP'nin unsurları aşağıdakileri içermelidir:

- Dağıtım politikasını, standartlarını, prosedürlerini ve yönergelerini tanımlayan politika bildirimi
- Tanımlanmış roller, sorumluluklar ve izlenebilirliklere sahip proje ekibi üyeleri
- Acil müdahale prosedürleri ve hayatın, güvenliğin ve altyapının korunması
- Durum ve hasar tespiti
- Kaynak kurtarma ve geri kazanma
- İşlemlerin ve iş kurtarmanın kısa süreli veya uzun vadeli acil durum modları için alternatif olanaklar veya öncelikler

Özetle, bir BCP, bir kurumun kritik iş fonksiyonlarının az ya da hiç kesintiye uğramadan devam etmesini sağlamak için gereken tüm faaliyetleri yönetmektedir. BCP, işlemleri desteklemek için gerekli altyapı bileşenlerinin bulunduğunu varsaymaktadır. Maalesef, bu durum bir felâket sonrasında her zaman böyle değildir. Bir yangın veri merkezinizi yok ettiğinde ne olur? Bu durumda ticari faaliyetlere nasıl devam edersiniz? Cevap, başka bir plana ihtiyacınız olduğudur: bir *felaket kurtarma planı* (*disaster recovery plan* - DRP).

Felaket Kurtarma Planı (DRP)

Felaket kurtarma planı (*disaster recovery plan* - DRP), bir felâket sonrası kaynakları kurtarmak için gereken eylemleri yönetmektedir. Bir DRP, bir BCP'nin parçasıdır. BCP tarafından gerekli görülen kaynakların kullanılabilir durum için onarılmasını sağlamak gerekmektedir. DRP, kritik iş fonksiyonlarını desteklemek için gerekli olan kaynaklara zarar verebilecek olayları belirleyerek BCP'yi genişletmekte ve desteklemektedir. BCP zaten her iş fonksiyonunu desteklemek için gerekli olan kaynakların bir listesini içermektedir. DRP'yi geliştirmede bir sonraki adım, her bir kaynağa neler olabileceğini düşünmektir.

BCP ve DRP: Fark Nedir?

Bir BCP ve bir DRP arasındaki fark nedir? BCP, afetlerden nasıl kurtulacağınızı belirtmemekte, yalnızca kesintiler için belirtmektedir. Genel olarak, bir *kesinti (interruption)*, bir veya daha fazla iş sürecini kısa bir süre için bozabilecek küçük bir olaydır. Bunun tersine, bir *felaket (disaster)*, çoklu iş süreçlerini uzun bir süre için etkileyen bir olaydır. Ayrıca, felaketler genellikle iş süreci kesintisini çözmeden önce ele almanız gereken önemli miktarda kaynak hasarına neden olmaktadır.

Tehdit Analizi

Bir tehdit (threat) analizi, kritik kaynaklara yönelik tehditleri tanımlamayı ve belgelemeyi içermektedir. Bir felaketten kurtarmadan önce, hangi felaket türlerinin mümkün olduğunu ve hangi tür hasarlara neden olabileceklerini düşünmelisiniz. Örneğin, veri merkezi yangınından kurtulmak, grip salgınından kurtulmaktan farklıdır. Bazı ortak tehditler aşağıdakileri içermektedir:

- Yangın
- Sel

- Kasırga
- Hortum
- Hastalık
- Deprem
- Siber saldırı
- Sabotaj
- Hizmet kesintisi
- Terörizm

Hastalık dışında, bu tehditlerin her biri bir kuruluşun altyapısına zarar verme potansiyeline sahiptir. Buna karşılık, hastalık doğrudan personeli etkilemektedir. Hastalığı çeşitli çözümlerle çözebilirsiniz. Bununla birlikte, hastalık, kurtarma planlarını gerçekleştirmekle görevli kişileri etkiliyorsa, kurtarma başarısız olabilir.

Bu tehditlerin birer birer gerçekleşmesi gerekmediğini unutmayınız. Bir tehdit başka bir tehdide neden olabilir. Örneğin, bir ofise kirli su getiren bir sel, personelinizi iş yapamaz duruma getirecek bir hastalığa neden olabilir. Başka bir örnek olarak, bir kasırga veya deprem bir yangınla sonuçlanabilir. Her zaman, felaketlerin yalnızca tek bir olay olarak değil, gruplar halinde oluşabileceğini varsaymalısınız.

Etki Senaryoları

Potansiyel tehditleri tanımladıktan sonra, kapsamlı bir DRP oluşturmanın bir sonraki adımı, muhtemel etki senaryolarını belgelemektir. Bunlar DRP'nin temelini oluşturmaktadır. Çoğu organizasyonda, daha küçük sorunlara odaklanmak yerine en geniş ve kapsamlı felaketi planlamak, daha kapsamlı bir plan ile sonuçlanmaktadır. Daha küçük konulara odaklanmanın daraltılması, daha geniş bir stratejiyi dikkate almayan bir DRP ile sonuçlanabilir. Aynı anda birden fazla kaynağın kaybından kurtarmak için daha geniş bir strateji gereklidir. "Binanın Kaybı (*Loss Of Building*)" gibi bir etki senaryosu muhtemelen tüm kritik iş fonksiyonlarını ve verilen herhangi bir tehditten kaynaklanan en kötü potansiyel sonucu kapsayacaktır. Bir DRP, bir kurumda birden fazla bina varsa, ek etki senaryoları içerebilir.

Eksiksiz bir DRP aynı zamanda, ilave edilmiş, daha özgün etki senaryolarını da içerebilir. Örneğin, planınız bir binadaki belirli bir katın kaybolmasını ele alan bir senaryo içerebilir. Birçok plan, bir konumdan diğerine geçmek için gerekli olan kaynakları önemsemez. Planınızın her bir adımını gerçekleştirmek için gerekli olan kaynakları ihmal etmeyiniz. Ekipmanınızı alternatif bir konuma taşımak için yeterince büyük bir kamyona erişiminiz olmadığı için başarısız olan bir kurtarma planı çok sağlam bir plan değildir.

Kurtarma Gereksinimi Dokümantasyonu

Analiz aşamasını tamamladıktan sonra, uygulama aşamasını başlatmak için iş gereksinimlerini ve teknik gereksinimleri belgelemelisiniz. Bir felâket sırasında muhtemelen, varlık listelerini ve bunların kullanılabilirliğini içeren varlık bilgilerine erişmeniz gerekecektir. Her bir varlığın bir sahibi vardır. Bir varlığın sahibi afet yardım ekibine o varlık için erişim izni vermelidir. Genellikle, BCP ve DRP'nin, iş sürekliliğini sağlamak veya iş fonksiyonlarını ve işlemlerini kurtarmak için görevlerini ve işlevlerini yönetmede tam yetkiye sahip ekip liderleri vardır. BCP ve DRP ekipleri, dahili ve harici iletişimlerin tüm yönlerini ele almak için genellikle icra yönetimi, hukuksal ve halkla ilişkiler personel üyelerini içermektedir.

Varlık bilgileri önceden BCP'de tanımlanmalı ve sağlanmalıdır. Bu bilgiler, olağanüstü felaket kurtarma ekibi için hazır bulunmalı ve aşağıdakileri içermelidir:

- Tüm tesis varlıklarının eksiksiz ve doğru envanteri
- BT varlıkları, donanım, yazılım, lisanslar, sözleşmeler ve bakım anlaşmalarının eksiksiz ve doğru envanteri
- Alternatif ofis olanaklarının ve öncelikli konumların eksiksiz ve doğru listesi
- İş ortakları, satıcılar, servis sağlayıcılar ve tedarikçilerin eksiksiz ve doğru listesi ve iletişim bilgileri
- Felaket kurtarma ekibi üyesi iletişim bilgileri-iş ve kişisel
- Kritik iş fonksiyonları ve işlemleri ve gerekli BT sistemleri, uygulamalar, kaynaklar ve veri kurtarma
- Kurtarma ve kullanım için yedeklenmiş verilerin geri getirimi
- Ayrıntılı BT sistemi, uygulama ve veri kurtarma prosedürleri
- Felaket kurtarma ekibi üyeleri, manuel ve geçici çözümler için ihtiyaç duyulan kaynaklar
- Kurtarma süresi hedefleri (*recovery time objectives* - RTO) ve bu ölçüte ulaşmak için gereken adımlar

Felaket Kurtarma

Tüm personelin herhangi bir felakete karşı doğru bir müdahale konusunda eğitilmesi önemlidir. Personel için genel yanılgı, personelin kurtarma sürecine başlamaya çok hevesli olmasıdır. Kurumunuz bir DRP geliştirmek için zaman ve kaynak ayırmış olsa da, plana değil de felakete tepki gösterdiğinizden emin olmalısınız. Bir felâkete müdahale etmede kritik adımlar aşağıdakileri içermektedir:

- **Öncelikle herkesin güvenliğini sağlayın** - Başka hiçbir kaynak insanlar kadar önemli değildir.
- **Kurtarmadan önce felakete tepki verin** - Gerekli tepki ve sınırlama eylemleri felaketin niteliğine bağlıdır ve kurtarma çabasıyla hiçbir ilgisi olmayabilir.
- **Etkilenen tüm taraflarla iletişim kurmayı da içeren DRP'yi takip edin** - İnsanlar güvendeyse ve felakete karşılık verdiyseniz, kurtarma eylemlerini takip edebilirsiniz.

Felaket kurtarma DRP'nin bir uzantısıdır. Ortak sistem hizmet kesilmeleri veya kesintilerinden kurtarma sorununu gidermektedir. Bir felaket genellikle genel bir hizmet kesintisinden daha büyüktür, ve kaynaklar basit kurtarma çözümlerini yürürlüğe koymak için mevcut olmayabilir. Örneğin, çoğu veritabanı yönetim sistemi birincil veritabanını çoğaltılmış bir kopyadan hızlı bir şekilde kurtarmanıza olanak tanımaktadır. Bununla birlikte, bir felaket veritabanı sunucu bilgisayarınızın tahrip edilmesiyle sonuçlanırsa, veritabanı verilerinizi geri yükleyebilmeniz için önce sunucuyu kararlı bir duruma (*stable state*) getirmeniz gerekecektir.

Bir felaket, veri merkezinizi kullanılamaz hale getirebilir, böylece işlemlerinizi yeniden konumlandırmanıza neden olur. Böyle bir hareket için dikkatli planlar yapmak onu uygulanabilir yapmaktadır. Veri merkezinizi başka bir konuma taşımak büyük bir girişim gibi gelmese de, çok fazla ayrıntı içermektedir. Bu nedenle planlama için çok fazla gayret sarf etmeniz gerekir.

NOT

Bazı endüstrilerde işbirliği anlaşmaları zorunludur. Örneğin, bankaların diğer bankalarla işbirliği anlaşmaları yapmaları gerekmektedir. Ayrıca, müşterilerine kesintisiz hizmet sunmak için diğer bankaların olanaklarını kullanma yeteneklerini düzenli olarak test etmeleri gerekmektedir.

TABLO 4-1 Felaket kurtarma için veri merkezi alternatifleri.

SEÇENEK	TANIM	YORUMLAR
Sıcak bölge (*Hot site*)	Çevre hizmetlere, donanıma, yazılıma ve orijinal veri merkezini sıkça yansıtan (*mirror*) verilere sahip tesis	En pahalı seçenek, en az sistem değişikliği zamanı
Ilık bölge (*Warm site*)	Çevre hizmetleri ve temel bilgisayar donanımına sahip tesis	Bir sıcak bölgeden daha ucuzdur, ancak işletim sistemleri, yazılımlar, veriler ve yapılandırmaları yüklemek için daha fazla zaman gerekmektedir
Soğuk bölge (*Cold site*)	Temel çevre hizmetlerine sahip, ancak altyapı bileşenleri olmayan tesis	En düşük maliyetli seçenek ancak tüm donanım, yazılım ve verilerin yeni bölgede yüklenmesi gerektiği için en uzun sistem değişikliği zamanı maliyetine sahiptir.
Mobil bölge (*Mobile site*)	Sıcak bir bölge veya soğuk bir bölge olarak çalışabilen gerekli çevresel hizmetlere sahip römork	Çok esnek, oldukça kısa sistem değişikliği zamanı, büyüklük ve kapasiteye bağlı olarak çok çeşitli maliyetler

Donanım ve yazılımı yüklemeniz gerekmektedir ve ağ ve telekomünikasyon gereksinimleri vardır. **TABLO 4-1**, felaket kurtarma için birkaç yaygın veri merkezi seçeneğini listelemektedir.

Başka bir şirketle karşılıklı yardım anlaşması yapmanız sizin avantajınıza olabilir, buna göre her şirket bir felâket durumunda yedekleme kaynakları sağlamayı kabul etmektedir. Anlaşma, bilgisayar kaynaklarına veya geçici bir veri merkezi olarak kullanmak üzere bir fiziksel alana çalışma saatleri dışında erişmeyi içerebilir. İşbirliği anlaşması yaparken tüm şartları dikkatlice inceleyiniz. Bir veri merkezi için temel kritik işlevler sağlamak basit görünebilir ancak telekomünikasyon hizmeti gibi bazı kaynakları bir konumdan diğerine geçirmek kolay olmayabilir. Ayrıca, mevcut konumunuza alternatif herhangi bir konumun ne kadar yakın olduğunu göz önünde bulundurun. Önerilen alternatif konumunuz ana konumunuza çok yakınsa, bir sel veya deprem gibi büyük bir felaket her ikisini de etkileyebilir.

Felaket kurtarma, kurumsal bilgi işlem işleminin giderek daha önemli bir yönü haline gelmektedir. İş ortamları daha karmaşık hale geldikçe, daha fazla şey ters gidebilir. Kurtarma planları, ayakta kalabilmek için daha karmaşık hale gelmiştir. DRP'ler birçok faktöre bağlı olarak bir kurumdan diğerine değişmektedir. Bunlar, kurumun türünü, ilgili süreçleri ve ihtiyaç duyulan güvenlik seviyesini içermektedir. Birçok işletme, bir felâket için hazırlıksız kalmakta veya yeterli düzeyde hazırlığa sahip olmamaktadır. Tekrarlayan hatırlatmalara rağmen birçok şirketin DRP'si yoktur. DRP'ye sahip olanların neredeyse yarısı planlarını hiç denememiştir ki aslında bu durum plan yapmadığınız durum ile aynıdır.

Etkinlik ve eksiksizlik için DRP'nizi doğrulamak ve doğruluğunu test etmek çok önemlidir. Bir DRP'nin ilk sürümünün eksiksiz ve doğru olması nadiren görülmektedir. Eksiklikleri belirlemek için DRP'nizi test etmelisiniz. Eksiklikler belirlendikten sonra, DRP'yi düzeltmeniz gerekmektedir. Bu tür testlerde yardımcı olması için bir felaket kurtarma firmasıyla çalışabilirsiniz. Bu testler basit incelemelerden bütünlüklü felaket simülasyonlarına kadar değişebilir. En etkili testler, bilgisayar sistemleri arasında yazılım aktarımını ve alternatif bir konumda iletişim kurabilmenizi sağlamayı içeren gerçek afetleri simüle etmektedir.

Aşağıda çeşitli DRP testleri yer almaktadır:

- **Kontrol listesi (*Checklist*) testi**—Bu test, DRP testinin en basit türüdür. Bir kontrol listesi testinde, her katılımcı DRP kontrol listesindeki adımları izlemekte ve geri bildirim sağlamaktadır. DRP eğitimi ve farkındalığı için kontrol listesi testlerini kullanabilirsiniz.
- **Yapılandırılmış gözden geçirme**—Yapılandırılmış gözden geçirme, bir kontrol listesi testine benzemekte, ancak DRP ekibi bir felaketi simüle etmek ve DRP'nin etkinliğini değerlendirmek için rol yapmayı (*role playing*) kullanmaktadır. Bu tür testler aynı zamanda masaüstü egzersizi (*tabletop exercise*) veya konferans odası testi (*conference room test*) olarak da bilinmektedir.
- **Simülasyon testi**—Bir simülasyon testi, yapılandırılmış gözden geçirmeden daha gerçekçidir. Bir simülasyon testinde, DRP ekibi rol yapmayı kullanmaktadır ve canlı operasyonları etkilemeksizin simüle edilmiş bir felaketin etkilerini mümkün olduğunca takip etmektedir.
- **Paralel test**—Paralel bir test, birincil veri merkezini kesintiye uğratmaksızın alternatif bir veri merkezinde tam işleme kapasitesi sağlayarak DRP'nin etkinliğini değerlendirmektedir.
- **Tam kesinti testi**—Bu test, tek eksiksiz testtir. Tam kesinti testleri, birincil veri merkezini kesintiye uğratmakta ve işlem kapasitesini alternatif bir bölgeye aktarmaktadır.

DRP'lerin tüm yönleri duyarlı değildir. Bir DRP'nin bazı kısımları önleyicidir ve öncelikle bir felaketin olumsuz etkilerinden kaçınmayı amaçlamaktadır. Bir DRP'nin önleyici bileşenleri aşağıdakilerden bazılarını içerebilir:

- Disk sistemlerinin yerel yansıtması (*mirroring*) ve bağımsız disklerin yedek dizisi (*redundant array of independent disks* - RAID) veya depolama alan ağı (*storage area network* - SAN) depolama sistemi gibi veri koruma teknolojisinin kullanılması
- Güç dalgalanmalarının hassas elektronik ekipman üzerindeki etkisini en aza indirgemek için aşırı gerilim koruyucuları
- Elektrik kesilmesi durumunda sistemlerin devam etmesini sağlamak için kesintisiz güç kaynağı (*uninterruptible power supply* - UPS) ve/veya bir yedek jeneratör
- Yangın önleme sistemleri
- Antivirüs yazılımı ve diğer güvenlik kontrolleri

Riskleri, Tehditleri ve Güvenlik Açıklarını Değerlendirme

Kapsamlı BCP'leri ve DRP'leri geliştirmede ilk adımlardan biri, kurumunuzun kritik kaynaklarıyla ilgili riskleri, tehditleri ve güvenlik açıklarını tam olarak değerlendirmektir. Çevrenizi olası her tehditten koruyamazsınız, bu nedenle önceliklendirmeniz gerekmektedir. Riskleri bilene kadar hangi düzeltmelerin gerekli olduğunu bilemezsiniz.

Riski değerlendirmek için pek çok yaklaşım bulunmaktadır. Her kurum, süreci kendi özgün şekliyle yürütür. Risk değerlendirme sürecinde sıfırdan başlamak yerine, mevcut birçok metodolojiden birini kullanabilirsiniz. Bunlardan en az biri muhtemelen kuruluşunuz için iyi bir seçenektir. Çeşitli teklifleri araştırmaya zaman ayırmak, tüm süreci daha etkin ve verimli hale getirebilir. **TABLO 4-2**, genel risk değerlendirme yöntemlerini listelemektedir.

TABLO 4-2 Genel risk değerlendirme yöntemleri.

İSİM	TANIM	DAHA FAZLA BİLGİ İÇİN
Bilgi Teknolojisi Sistemleri için Risk Yönetimi Rehberi *(Risk Management Guide for Information Technology Systems)* (NIST SP800-30)	Özel Yayın 800 serisi raporların bir parçası olan bu ürünler, bilgisayar güvenliği kapsamında risk yönetiminde ve risk değerlendirmesinde nelere dikkat etmeniz gerektiğini belirten ayrıntılı bir rehberlik sağlamaktadır. Raporlar, kontrol listelerini, grafikleri, formülleri ve ABD mevzuat konuları ile ilgili referansları içermektedir.	*http://csrc.nist.gov*
CCTA Risk Analizi ve Yönetimi Metodu (*CCTA Risk Analysis and Management Method* - CRAMM)	CRAMM, Birleşik Krallık devleti tarafından geliştirilen bir risk analizi yöntemidir. Birleşik Krallık devlet örgütlerinin en iyi uygulamaları, CRAMM yönteminin ve aracının ilk sürümlerinin temelini oluşturmaktadır. Dünya genelinde insanlar CRAMM kullanmıştır; aynı zamanda Birleşik Krallık devletinin tercih ettiği risk analizi yöntemidir. CRAMM, büyük kuruluşlar için en uygun çözümdür.	
Operasyonel Kritik Tehdit, Varlık ve Güvenlik Açıkları Değerlendirmesi (*Operationally Critical, Threat, Asset, and Vulnerability Evaluation* - OCTAVE)	OCTAVE yaklaşımı, güvenlik için risk-tabanlı stratejik değerlendirme ve planlama tekniğini tanımlamaktadır. OCTAVE kendi kendini idare eden (self-directed) bir yaklaşımdır. OCTAVE'ın iki sürümü vardır: OCTAVE ve OCTAVE-S. OCTAVE büyük kurumlar için çok uygundur; OCTAVE-S ise 100'den az kişiden oluşan kurumlar için iyi çalışmaktadır.	*www.cert.org/resilience/products-services/octave/index.cfm*
ISO/IEC 27005 "Bilgi Güvenliği Risk Yönetimi" (*Information Security Risk Management*)	Bilgi güvenliği risk yönetimini genel bir biçimde tanımlayan bir ISO standardıdır. Belgeler, bilgi güvenliği risk değerlendirmesi yaklaşımları ve olası tehditler, güvenlik açıkları ve güvenlik kontrolleri listelerini içermektedir.	*www.iso.org*

Bilgi Güvenliği Açığını Kapatmak

Tüm iyi çabalara rağmen, hiçbir güvenlik kontrolü topluluğu mükemmel değildir. Denetimin olmadığı bazı güvenlik açıkları daima vardır. Yürürlükte olan güvenlik kontrolleri ile tüm güvenlik açıklarını gidermek için ihtiyaç duyduğunuz kontroller arasındaki fark **güvenlik farkı (*security gap*)** olarak adlandırılmaktadır.

Fark analizi (*gap analysis*), kurumunuzun **güvenlik politikasını (*security policy*)** sağladığınızdan emin olmanıza yardımcı olmak için değerli bir araçtır. BT güvenlik bakış açısından, bir güvenlik politikası, kurumunuz için bir risk azaltma tanımını veya çözümünü tanımlamaktadır. Fark analizi, tanımlanmış tüm tehditleri belirlemek için, yürürlükteki güvenlik denetimlerinin ve ihtiyacınız olan denetimlerin karşılaştırılmasıdır. Fark analizi aktiviteleri devam etmelidir. Bunlar, gündelik uygulamaların en güncel tehdit değerlendirmesi ile karşılaştırılarak düzenli olarak

gözden geçirilmesini içermelidir. En az bir kontrol ile belirtmediğiniz tehditler, güvenliğinizdeki eksiklikleri belirtmektedir.

Fark analizi gerçekleştirmek, bir kurumun BT ortamlarının genel güvenliğini ölçmek için etkili bir yöntemdir. Buna ek olarak, fark analizi, güvenlik uygulamalarının gerçek gereksinimlerle uyumlu olduğuna dair güvence sağlayabilir. Fark analizi faaliyetlerini birçok farklı türde gerçekleştirebilirsiniz. Resmi araştırmalar ya da resmi olmayan anketler olabilirler. Analizi etkileyen faktörler, kurumunuzun büyüklüğü, faaliyet gösterdiğiniz sektör, maliyet, çabalar ve analizin derinliğini içermektedir.

- Güvenlik politikasının uygulanabilir unsurlarını ve diğer standartları tanımlamak
- Politika, standart, prosedür ve yönerge belgelerini birleştirmek
- Politikaların, standartların, prosedürlerin ve yönergelerin uygulanmasının gözden geçirilmesi ve değerlendirilmesi
- Tüm donanım ve yazılım bileşenleri için envanter bilgisini toplamak
- Kullanıcılarla politikalar hakkında bilgi ve uyumu değerlendirebilmek için röportaj yapmak
- Mevcut güvenlik ortamını yürürlükteki politikalarla karşılaştırmak
- Çözüm için belirlenen eksikliklere öncelik verilmesi
- Politikalara uyacak çözümleri belgelemek ve uygulamak

Bir fark analizinin önemli bir yönü, farkın nedenini belirlemektir. Bir farkın olması gerçeği, yeterli güvenlik denetiminin eksikliği anlamına gelmektedir, ancak neden bu fark vardır? Herhangi bir organizasyonda güvenlik farklarının yaygın olarak görülen birkaç nedeni bulunmaktadır:

- Uyumsuz davranışa neden olan güvenlik eğitimi eksikliği
- Kasıtlı veya hatalı güvenlik politikası ihmali
- Kontrol veya politika değişikliğinin istenmeyen sonucu
- Uygun risk analizi yapılmadan donanım veya yazılımın eklenmesi veya değiştirilmesi
- Uygun risk analizinden yoksun yapılandırma değişiklikleri
- Mevzuat, yönetmelik veya kontrol değişikliklerini gerektiren endüstri standartları gibi dış gereksinimlerdeki değişiklikler

Gördüğünüz gibi, güvenlik farklarının çoğu kullanıcı eylemleriyle yakından ilgilidir. Farkları kapatmak için atabileceğiniz ilk adımlardan biri, güvenlik konularında personeli tamamen eğitmeyi sağlamaktır. İyi eğitimli insanlar BT ortamınızı güvenleştirmede en iyi müttefiklerinizdir. Güvenlik çalışmalarınız daha gelişmiş hale geldiğinde ve kurumunuzun personeli güvenlik ile ilgili daha fazla bilgili olduğunda, daha az güvenlik açığı ile karşılaşırsınız.

Hukuka Uygunluğa Bağlı Kalmak

Son 30 yıl, bilgisayar gücünde ve bilgisayarların kullanılış biçiminde bir patlama görmüştür. Ağa bağlı kaynaklara, donanıma ve yazılıma olan güvenin artması, kaynakların kötücül kullanımı için bir çok yeni fırsat yaratmıştır. Bilgi, kurumlar için değerli bir varlık ve saldırganlar için çekici bir hedef haline gelmiştir. Bilgi ile ilgili suç büyüdükçe, kurumları ve bireyleri suç faaliyetlerinden korumak için kanunlar ve yönetmelikler de gelişmiştir.

Günümüzün kurumları giderek artan bir şekilde, elektronik bilginin mahremiyetini korumak için çıkartılan çeşitli kanunların öznesi olmaktadır. Her kurum kanunlara ve düzenlemelere uymak zorundadır; ancak bir kuruluşun öznesi olduğu belirli kanunlar ve yönetmelikler, kuruluşun bulunduğu konuma, kullandığı bilgilerin türüne ve faaliyet gösterdiği sektörlere bağlıdır.

Aşağıda verilen liste, kuruluşların BT işlemlerini nasıl gerçekleştirdiklerini etkileyen en kapsamlı kanunların ve düzenlemelerin bir çoğunu özetlemektedir:

- **Sarbanes-Oxley Kanunu (*Sarbanes-Oxley Act* - SOX)**—Temmuz 2002'de kanun haline gelen Sarbanes-Oxley, kurumsal yönetimin ve mali uygulamaların düzenlenme biçiminde kapsamlı değişiklikler yaptı. Birkaç kamu mali skandalının doğrudan bir sonucu olarak, SOX, kamu şirketlerinin denetçisi rollerinde muhasebe firmalarını izlemek, düzenlemek, denetlemek ve disipline etmekten sorumlu olan Halka Açık Şirketler Muhasebe Gözetim Kurulu'nu (*Public Company Accounting Oversight Board* - PCAOB) kurdu. SOX ayrıca, denetçinin bağımsızlığını, kurumsal yönetimi, iç denetim değerlendirmesini ve gelişmiş mali bildirim konularını içeren politikaları belirlemektedir.
- **Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (*Health Insurance Portability and Accountability Act* - HIPAA)**—14 Nisan 2006'da yürürlüğe giren HIPAA, doktorların, hastanelerin ve diğer sağlık hizmeti sağlayıcılarının kişisel tıbbi bilgileri nasıl işleyeceğini kontrol etmektedir. HIPAA, tüm tıbbi kayıtlar, faturalandırma ve hasta bilgilerinin hastanın mahremiyetini koruyacak şekilde kullanılmasını gerektirmektedir. HIPAA ayrıca, tüm hastaların kendi tıbbi kayıtlarına erişebilmelerini, hataları veya eksiklikleri düzeltmelerini ve kişisel bilgilerin nasıl kullanıldığı konusunda bilgilendirilmelerini garanti etmektedir. Etkilenen her kişinin HIPAA'nın gereksinimlerinin farkında olduğundan emin olmak için, hastalar tıbbi bilgi gönderdikleri zaman mahremiyet prosedürlerinin bildirimlerini almalıdır.
- **Federal Finansal Kurumlar İnceleme Konseyi (*Federal Financial Institutions Examination Council* - FFIEC)**—FFIEC, güvenlik kontrolleri ve olgunluk değerlendirmeleri için bir standart oluşturmuştur. Bu, doğal bir risk profili değerlendirmesi ve bir siber güvenlik olgunluk değerlendirmesi içermektedir. Finansal kurumlar, bu iki ölçütü kullanarak kendi mevcut risk profillerini ve kendi mevcut siber güvenlik seviyelerini kendi kurumları içerisindeki kendi öz değerlendirmelerini temel alarak değerlendirebilirler.
- **Federal Bilgi Güvenliği Yönetim Yasası (*Federal Information Security Management Act* - FISMA)**—FISMA, bilgi güvenliğinin ABA'nin ulusal güvenliğine ve ekonomik sağlamlığına yönelik önemini resmi olarak kabul etmektedir. FISMA 2002'de yürürlüğe girmiştir ve her federal ajansın, güvenlik bilinci oluşturma çalışmalarını, bilgisayar kaynaklarına güvenli erişimi, değişmez kabul edilebilir kullanım politikalarını, resmi olay müdahalesini ve beklenmedik durum planlamasını da içeren resmi bilgi güvenliği programlarını geliştirmesini ve sürdürmesini gerektirmektedir.
- **Federal Bilgi Güvenliği Modernizasyon Yasası (*Federal Information Security Modernization Act* - FISMA)**—FISMA 2014, 2002'de yürürlüğe giren orijinal FISMA'nın güncellemesidir. Bu, orijinal FISMA'nın ilk değişikliğidir. FISMA 2014 güncellemeleri aşağıdakileri içermektedir:
  - Federal bilgi sistemleri için güvenlik politikaları ve uygulamalarının gerçekleştirimini yönetmek için Ulusal Güvenlik Bakanlığı (*Secretary of the Department of Homeland Security* - DHS) Sekreteri'ne yetki verirken, Yönetim ve Bütçe Dairesi (*Office*

of Management and Budget - OMB) direktörünün yetkisini gözetim ile yeniden belirtmektedir.

- Ajansların, kongreye büyük güvenlik olaylarını yedi gün içinde bildirmesini gerektirmektedir. OMB, büyük bir olayı neyin oluşturduğu konusunda yönerge geliştirmekten sorumlu olacaktır.
- Üst düzey yetkililerin bilgi güvenliği görevlerini yerine getirdiğinden ve tüm personelin kurum bilgi güvenliği programlarına uyduğunu garantileyen, güvenlik yönetimi için bütçesel planlamaya bakan kurumlara daha fazla sorumluluk vermektedir.
- Tehditlere, güvenlik açıklarına, olaylara, büyük olaylar anında sistemlerin uyumluluk durumuna ve kişisel olarak tanımlanabilir bilgileri (*personally identifiable information* - PII) içeren olaylara ilişkin verilere odaklanan raporlama yönergelerini değiştirmektedir.
- Verimsiz ya da zahmetli raporlamayı ortadan kaldırmak için OMB Genelgesi A-130'un revizyonu için çağrıda bulunmaktadır.
- Kurumların, periyodik risk değerlendirmelerini, güvenlik prosedürlerinin test edilmesini ve güvenlik olaylarının tespitini, raporlanmasını ve yanıtlanmasını içeren bilgi güvenliği programlarındaki otomatik araçların kullanımını sağlamaktadır.

- **Gramm-Leach-Bliley Kanunu (GLBA)** - GLBA, finans sektöründeki bilgi güvenliği endişelerini ele almaktadır. GLBA, finansal kurumların müşterilerine, şirketin müşteriyle ilgili hangi bilgileri topladığını, bilgilerin kiminle paylaşıldığını ve şirketin bu bilgileri nasıl koruduğunu açıklayan bir gizlilik bildirimi sunmasını gerektirmektedir. Şirketler, iş yapmak için bir anlaşmaya başlamadan önce müşterilere bu gizlilik bildirimini sağlamalıdır.
- **Ödeme Kartı Endüstrisi Veri Güvenliği Standardı (*Payment Card Industry Data Security Standard* - PCI DSS v3.2)** - Kanun olmasa da PCI DSS v3.2, kredi kartı bilgilerini işleme koyan veya depolayan herhangi bir kuruluşu etkilemektedir. PCI Güvenlik Standartları Konseyi'nin kurucu ödeme markaları - American Express, Discover Finansal Hizmetler, JCB, MasterCard, Visa International gibi - tutarlı küresel veri güvenliği ölçütlerini teşvik etmek için PCI DSS v3.2'yi geliştirdi. PCI DSS v3.2, güvenlik yönetimi, ilkeler, prosedürler, ağ mimarisi, yazılım tasarımı ve diğer kritik koruyucu ölçütler için gereksinimleri içeren kapsamlı bir güvenlik standardıdır.
- **Aile Eğitimi Hakları ve Mahremiyet Kanunu (*The Family Education Rights and Privacy Act* - FERPA)** - Bu federal kanun öğrenci eğitim kayıtlarının mahremiyetini korumaktadır. Kanun, ABD Eğitim Bakanlığı'nın uygulanabilir bir programı kapsamında fon alan tüm okullar için geçerlidir. FERPA'ya göre, okullar bir öğrencinin eğitim kayıtlarında yer alan herhangi bir bilgiyi yayımlamadan önce bir ebeveyn veya hak sahibi öğrenciden yazılı izin almalıdır.
- **2001 yılının ABD Vatanseverlik (*Patriot*) Kanunu** - 11 Eylül 2001'de New York'taki Dünya Ticaret Merkezi (*World Trade Center*) ve Washington D.C.'deki Pentagon saldırılarından 45 gün sonra geçen Vatanseverlik Kanunu, ABD kolluk kuvvetlerinin ABD ve diğer ülkelerdeki terörle mücadele etmelerini sağlamak için yetkisini önemli ölçüde genişletti. Kolluk kuvvetlerinin, yürütülmekte olan bir soruşturma ile ilgili bilgilere erişme yeteneğini genişletmektedir. Politikasında neleri içermesi gerektiği, onaylanmış onamın bir

ebeveynden ne zaman ve nasıl isteneceği ve çocuğun çevrimiçi mahremiyet ve güvenliğini koruması için bir operatörün hangi yükümlülüklerinin olduğunu tanımlamaktadır.

- **2000 yılının Devlet Bilgi Güvenliği Reformu Kanunu (Güvenlik Reform Kanunu) (*Government Information Security Reform Act – Security Reform Act*)** - Bu düzenleme, sınıflandırılmamış ve ulusal güvenlik sistemlerinin güvenliğinin yönetimine ve değerlendirilmesine odaklanmaktadır. Bu kanun, mevcut OMB güvenlik politikalarını resmileştirmiş ve 1987 Bilgisayar Güvenlik Kanunu'nda yer alan güvenlik sorumluluklarını yeniden düzenlemiştir.
- **2003 yılının California Veritabanı Güvenlik İhlali Kanunu (SB 1386) (*California Database Security Breach Act*)** - Bu California kanunu, SB 1386, diğer birçok benzer eyalet kanunu ile birlikte müşteri verilerini elektronik ortamda depolayan herhangi bir şirketin, herhangi bir güvenlik ihlali olduğunda müşterilere bunu bildirmesini gerektirmektedir. Birisi bilgisayar sistemini ihlal eder ve şifrelenmemiş bilgileri çalarsa, şirket etkilenen müşterilere derhal haber vermelidir. Benzer diğer kanun taslakları finansal kuruluşların kamuya açık olmayan kişisel istemci bilgilerini, grup şirketleri ve üçüncü kişilerle paylaşma kabiliyetini sınırlamaktadır.

Hangi kanunların ve düzenlemelerin kendileri için geçerli olduğunu anlamak ve uyulacak gerekli kontrolleri benimsemek her kurumun kendi sorumluluğundadır. Bu çalışma genellikle dikkat gerektirmektedir ve kuruluşun uyumlu kalmasını sağlamak için denetimler ve değerlendirmeler ile sonuçlanmaktadır.

NOT

Bir **mahremiyet politikası** (***privacy policy***), bir kurumun sizin ile ilgili topladığı verilerle ne yaptığını ve neden bu verileri topladığını tanımlamaktadır. Mahremiyet politikaları aynı zamanda verilerinizin üçüncü taraflarla paylaşılmasını veya üçüncü taraflara satılmasını istemiyorsanız yapmanız gerekenleri de açıklamaktadır.

Kişisel Verileri Gizli Tutmak

Önceki bölümlerde gördüğünüz uyumluluk gereksinimlerinin çoğunda veri gizliliği ele alınmaktadır. Güvenlik kontrollerinin en önemli sınıflarından biri, bilgiyi gizli tutan sınıflardır. Kullanılabilirlik ve bütünlüğün sağlanması önemlidir, ancak en çok ilgiyi gizlilik çekmektedir. Bunun nedeni gizlilik ihlalini geri alamamanızdır. Yani, birisi gizli verileri görüntülediğinde, bu verileri o kişinin hafızasından kaldırmanın bir yolu yoktur. Kurumunuzun veri varlıklarını korumak için bilgi güvenliğinin üç ilkesinin her birine dikkat etmelisiniz. ŞEKİL 4-2 bilgi güvenliğinin üç ilkesini göstermektedir.

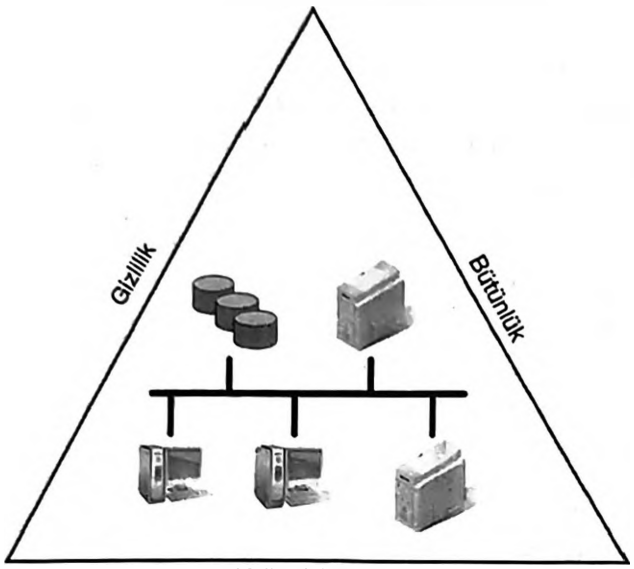
Verilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak için farklı teknikler öğreneceksiniz. En üst düzeyde, yetkili kullanıcılar tarafından kullanılabilir olduklarında ve yetkisiz kullanıcılar tarafından kullanılamadığında veriler güvenlidir. Verilerinizin güvenliğini tam olarak sağlamak için önce birçok ayrıntıyı içermeniz gerekecektir. Gizliliğin korunması kesinlikle tekrar eden bir konu olacaktır. Aslında, gizliliği sağlamak için birçok kontrol, veri güvenliğinin diğer boyutlarını da sağlamaktadır.

Çeşitli güvenlik kontrolleri hakkında daha fazla bilgi edinirken, veriyi yetkisiz kullanıma karşı korumak için güvenlik kontrollerinin birlikte nasıl çalıştıklarını göreceksiniz. Verinin güvenliğini sağlamak için kullanılan birçok strateji, kimlik doğrulamayı, yetkilendirmeyi ve izlenebilirliği içeren üç yönlü bir yaklaşım kullanmaktadır. Bu üç teknik, yalnızca yetkili kullanıcıların kaynaklara ve verilere erişebilmelerini sağlamaktadır.

NOT

Bilgi sistemi etkinliğini izleme bağlamında, **izleme** (***accounting***) terimi, olayları günlük (log) dosyalarına kaydetmek anlamına gelmektedir. Kullanıcıların eylemlerini izlemek ve olayları araştırmada yararlı olan bir olay dizisini belirlemek için bilgisayar olay izlemeyi kullanabilirsiniz.

ŞEKİL 4-2
Bilgi güvenliğinin üç ilkesi.



Ayrıca, erişim oluştuktan sonra erişim sorunlarını gidermek için yeterli bilginin alındığından emin olurlar. Güvenlik olaylarına ilişkin araştırmalar, geçmiş olayları yeniden yapılandırmak için izleme bilgilerine dayanmaktadır.

Üç yönlü yaklaşımın temel amacı, korunan herhangi bir kaynağın yetkisiz kullanımını önleyerek güvenliği sağlamaktır. Birçok kimlik doğrulama ve erişim denetimi bu görevi yerine getirmeye yardımcı olabilir. Öğreneceğiniz kimlik doğrulama denetimlerinin bazıları aşağıdakileri içermektedir:

- Parolalar ve kişisel kimlik numaraları (*personal identification number* - PIN'ler)
- Akıllı kartlar ve belirteçler
- Biyometrik cihazlar
- Dijital sertifikalar
- Meydan okuma-cevap el sıkışmaları
- Kerberos kimlik doğrulaması
- Bir kerelik şifreler

NOT

Düzenleyici bir uyum yasası kapsamındaki işletmeler ve kurumlar, düzenlenen verilere karşı düzenlenmemiş verileri ele almalıdır. Düzenleyici bir uyumluluk gereksinimi altındaki veriler, genellikle bu verilerin, uyulması zorunlu erişim denetimleri, gerçek zamanlı izleme ve dinlenme, depolama ve aktarmada veri şifrelemesi gibi uygun güvenlik denetimlerini içermiş olması gerektiği anlamına gelmektedir. Veri gizliliği, düzenleyici bir uyum yasası altındaki kurumlar için en önde gelen ticari zorluktur. Doğru veri gizliliği güvenlik kontrolleri, bir veri ihlali veya veri kaybı tehdidini azaltabilir. Düzenlemelere uymak için uygun denetimleri kullanmayan herhangi bir kurum, kendilerine karşı verilen cezalara veya cezai kovuşturmaya tabi olabilir.

Bir kullanıcının kimliğini doğruladıktan sonra, erişim denetimleri, korunan kaynağa yalnızca yetkili kullanıcıların erişebildiğini garantilemeye yardımcı olmaktadır. Öğreneceğiniz yetkilendirme denetimleri aşağıdakileri içermektedir:

- Kimlik doğrulama sunucusu kuralları ve izinleri
- Erişim kontrol listeleri
- Saldırı tespit ve önleme
- Fiziksel erişim kontrolü
- Bağlantı ve erişim politikası filtreleri
- Ağ trafiği filtreleri

Bu iki liste, kurumunuzun veri güvenliğini sağlamaya yardımcı olan güvenlik kontrollerinin bazılarına kısa bir bakış sunmaktadır.

Mobil Çalışanlar ve Kişisel Olarak Sahip Olunan Cihazların Kullanımı

Şirketler ve kurumlar için yeni ortaya çıkan bir diğer iş sürücüsü mobilitedir. **Mobilite (*mobility*)** uzaktaki çalışanların ve personelin neredeyse gerçek zamanlı olarak BT altyapısına bağlanmalarına izin vermektedir. Bunun anlamı, hızlı ve etkili iletişimlerin işletmelerin verimliliği, satışları, geliri ve kârı arttırmalarına yardımcı olabileceğidir. Hiper bağlantılı mobil çalışanlar artık "her zaman çalışır (*always on*)" durumdadır. Bu, kurum genelinde verimliliği yürütmeye yardımcı olmaktadır. Müşterileri ziyaret eden dış satış temsilcileri gibi olan bu mobil yol savaşçılarının[1] (*road warriors*) yaygınlığı, kurumun BT altyapısına giriş işleminin kullanıcının uç nokta cihazı ile İş İstasyonu Etki Alanı aracılığıyla bağlanan Kullanıcı Etki Alanı'ndaki kullanıcı tarafından gerçekleştirildiği göz önüne alındığında kurum için kritik bir risk unsuru oluşturmaktadır. Verilen duruma bağlı olarak, uç nokta cihazı, bir dizüstü bilgisayardan veya bir tabletten bir akıllı telefona kadar herhangi bir şey olabilir. Bu cihazların her biri kendi risklerini, tehdit ve güvenlik açıklarını ortaya çıkarmaktadır. Mobilite, işletmelerin ve kuruluşların, Kendi Cihazınızı Getirin (*Bring Your Own Device*-BYOD) stratejisini benimsemelerini sağlayan iş sürücüsüdür. BYOD, örneğin bir dizüstü bilgisayar veya akıllı telefon gibi kişisel olarak sahip olunan cihazları iş için olduğu kadar kişisel kullanım için de kullanan personeli belirten bir terimdir.

NOT

İşletmeler ve kurumlar kişisel BT varlıklarının ticari amaçla kullanımı konusunda bir karar vermelidir. Bu, e-posta eki olarak hassas verileri içerebilecek veya içermeyebilecek iş e-postaları için kişisel akıllı telefonlarını kullanan çalışanları içermektedir. Mobilite, iş dünyasının ve kişisel BT varlıklarının yakınlaşmasını sağlamaktadır. Sosyal medyanın kullanımı, iş ve kişisel iletişimlerin ve bilgi paylaşımının yakınlaşmasını yönlendiriyor. Çalışanlara dizüstü bilgisayar ve akıllı telefon sağlamak için gereken yatırım, bazı işletmeler veya kurumlar için yüksek maliyetli olabilir. Birçok organizasyon artık, dizüstü bilgisayarlar veya akıllı telefonlar gibi kişisel olarak sahip olunan cihazlar ile ilgili olarak işletme bilgilerinin gizliliğini sağlamak için politikalar ve prosedürler uyguluyor. Kişisel BT varlıklarını kullanan çalışanlar, genellikle, kurumun kabul edilebilir kullanım politikasına, e-posta ve internet kullanım politikasına ve BYOD politikasına uymak zorundadırlar. BYOD politikası, cihazın kaybolması veya çalınması durumunda veri temizleme ya da veri silme işlemini gerçekleştirmek için yetkilendirme gerektirebilir.

BYOD Endişeleri

BYOD'un kurumsal ortamlara ve hükümet ortamlarına kabul edilmesi, çözülmesi gereken özgün bir iş zorluğu yaratmıştır. Bu zorluk, BT varlığının çalışana ait olduğu gerçeğini temel almaktadır. Ne olursa olsun, BT varlığı ve onun kullanıcısı, kuruluşun mobilitesi, BYOD'a ve kabul edilebilir kullanım politikasına hala uymak zorundadır. Aşağıda belirtilen unsurlar bir BYOD politika tanımında yaygın olarak ele alınmaktadır:

- **Veri sahipliği (*Data ownership*)**—Kişiler, resimler veya e-postalar gibi kişisel veriler, çalışanların fikri mülkiyetindedir. İş e-postaları ve tüm ekler, kuruluşun fikri mülkiyetindedir. Bu ayrım, bir BYOD politikasında açıkça tanımlanmalıdır.
- **Destek mülkiyeti (*Support ownership*)**—Çalışan, geri ödeme kuruluş tarafından onaylanmadıkça BT varlığına ve tüm destek ve bakım sorumluluklarına sahiptir.
- **Yama yönetimi (*Patch management*)**—Yazılım güncellemeleri ve yamalar önerilmektedir ve kurum tarafından tanımlanan politika tanımı aracılığı ile çalışan tarafından çalışanın kendi cihazı üzerinde gerçekleştirilmelidir.
- **Antivirüs yönetimi (*Antivirus management*)** — Kuruluşun fikri mülkiyetine erişen herhangi bir BT varlığına, (BYOD politikası tarafından tanımlandığı şekilde) uygun bir antivirüse/kötücül yazılıma karşı koruma yüklenmiş olmalıdır.

[1] Editörün notu: Taşınabilir bilgisayar teknolojisi talep eden iş yolcusu için kullanılan pazarlama ifadesi

- **Adli Bilim (*Forensics*)**—Çalışanlar, kişisel olarak sahip oldukları BT varlıkları eğer resmi bir olay müdahale soruşturmasının bir parçasıysa, varlık hakkında kapsamlı bir adli bilim araştırması yapmak için BT varlığına el konabilir.
- **Mahremiyet (*Gizlilik*)**—Çalışanlar mahremiyetlerini kaybetmemek ve korumakla yükümlüdür; bununla birlikte, kurumun kabul edilebilir kullanım politikası ve veri temizleme ve veri silme tanımları, işi yürütmek için kendi kişisel olarak sahip oldukları cihazları kullanmaya karar vermeden önce çalışanlar tarafından tam olarak anlaşılmalıdır.
- **İşe alım/işten çıkarma (*Onboarding/offboarding*)**—BYOD politikası, İK işe alım işlemi sırasında açıklanmalı ve kabul edilmelidir. Politika ayrıca, kişisel olarak sahip olunan BT varlığının, çalışanların işten çıkarılmasından ve erişim denetimlerinin kaldırılmasından önce ele alınmasını (örneğin, veri temizleme, veri silme, vb.) içermelidir.
- **Kurumsal politikalara uyum**—Kişisel olarak sahip olunan BT varlıklarının kullanımı, çalışanların kabul edilebilir kullanım politikası da dahil olmak üzere diğer tüm politika ve prosedürlere uymalarını gerektirmektedir.
- **Kullanıcı kabulü**—Çalışanın, iş verisi ile kişisel verinin ayrılmasının yanı sıra (BYOD politikasının gerektirdiği gibi) veri temizleme ve silme işlemini kabul etmesi gerekmektedir.
- **Mimari/altyapı değerlendirmeleri**—Kişisel olarak sahip olunan herhangi bir BT varlığının kullanımı, kurumun BT standartlarını karşılamalıdır ve güvenliği desteklemek için yeni yazılım yüklemeyi gerektirebilir.
- **Hukuki endişeler**—Çalışanlar, özellikle yasal bir sorun veya olay soruşturması söz konusuysa (örneğin, adli bilim araştırması) kurumun politikalarına ve prosedürlerine uymayı kabul etmek zorundadır.
- **Kabul edilebilir kullanım politikası**—Çalışanlar, özellikle kurumun kabul edilebilir kullanım politikası olmak üzere tüm kurumsal politika ve prosedürlere uymak zorundadır.
- **Bütünleşik kamera/video**—BYOD politikası, kişisel olarak sahip olunan herhangi bir BT öğesinin kamera ve video yeteneklerinin kullanımını ele almalıdır. Bu resimlerin ve videoların içeriği, kabul edilebilir kullanım politikasına uymak zorundadır. Genellikle, çalışanlar fotoğraf ve video dahil olmak üzere tüm kişisel veri yedeklemelerinden sorumludur.

Uç Nokta ve Cihaz Güvenliği

Mobilite ve BYOD, uç nokta veya cihaz güvenliği kontrollerini etkinleştirmeye ihtiyaç duymaktadır. Aşağıdaki tartışma, mobilite ve BYOD ortamlarıyla genel olarak ilişkili olan riskleri, tehditleri ve güvenlik açıklarını azaltabilecek uç nokta cihazı güvenlik kontrollerini sunmaktadır:

- **Tam cihaz şifrelemesi**—Dizüstü bilgisayarların, tabletlerin ve akıllı telefonların veri şifrelemesi ile donatılmasını gerektirmektedir, böylece cihazın kaybolmasından veya çalınmasından doğacak risk azalacaktır.
- **Uzaktan silme**—Kurumun cihazın kaybolması veya çalınması durumunda verilerin veya e-postaların uzaktan silinmesini başlatmasını sağlayan bir yazılım yükleyiniz.
- **Kilitleme**—Kilitleme zamanlayıcıları olan, kurumun İş İstasyonu Etki Alanı güvenlik politikalarına ve prosedürlerine uyan cihaz ekran koruyucularını gerektirmektedir.

- **Ekran kilitleri**—Cihazın sahibinin cihaza erişim için bir parola girmesini gerektiren parola-korumalı-ekran-kilidi fonksiyonunu gerektirmektedir.
- **Küresel konumlama sistemi (*Global positioning system* - GPS)**—Eğer cihaz bir iletişim ağına bağlıysa, cihazın fiziksel konumunu belirlemek için uydu ve/veya hücresel iletişimleri kullanan bir GPS kurunuz.
- **Uygulama kontrolü**—Uygulama kontrolü veya cihaz kontrolü sağlayan bir yazılım yükleyiniz.
- **Bellek bölümleme**—Kişisel ve iş amaçlı olarak paylaşılan cihazların, kişisel verileri iş verilerinden fiziksel olarak ayırmak için bölümlenmiş belleğe sahip olmasını gerektirmektedir.
- **Varlık takibi**—BT altyapısına bağlı olan tüm BT varlıklarının, ister kişisel olarak sahip olunsun ister kurumun mülkiyetinde olsun, kurum tarafından BT varlıkları olarak izlenmesini gerektirmektedir.
- **Envanter kontrolü**—Çalışanlar tarafından sahip olunan tüm mobil cihazların BT varlığı envanteri olarak kaydedilmesini gerektirmektedir. Böylelikle, uygun değişim yönetimi ve olay tepkisi tüm uç nokta cihazlarına uygulanabilir
- **Mobil cihaz yönetimi**—Mobil cihaz yönetimi (*mobile device management*-MDM) yazılım etmeninin (kurumların kişisel olarak sahip olunan bir cihazdan işletme verilerini izlemesine, kontrol etmesine, veri temizlemesine veya veri silmesine izin veren bir yazılım uygulaması) herhangi bir mobil cihaza kurulmasını gerektirmektedir.
- **Cihaz erişim kontrolü**—Kişisel olarak sahip olunan tüm aygıtların kurumun BYOD politikasına uygun olmasını ve BT varlığının kendisine erişebilmesi için uygun cihaz erişim denetimleri, e-posta erişimi için erişim denetimleri ve BT altyapısına uzaktan erişim için erişim denetimlerine sahip olmasını gerektirmektedir.
- **Çıkarılabilir depolama (*Removable storage*)**—Kurumun BYOD politikasında ve kabul edilebilir kullanım politikasında tanımlanan çıkarılabilir depolama veya veri yedeklerinin kullanımını gerektirmektedir. Kişisel verilerin yedeklenmesi çalışanların sorumluluğundadır. İş verilerinin veri yedekleri, politika tanımına göre çalışanın veya kurumun sorumluluğundadır.
- **Kullanılmayan özelliklerin devre dışı bırakılması**—BYOD politikasına ve kabul edilebilir kullanım politikası tanımına bağlı belirli uygulamaların ve özelliklerin kullanımına izin vermeyiniz, örneğin; hassas verilerin kısa mesajlarda kullanımı.

BÖLÜM ÖZETİ

Bu bölümde, güvenliğin veriyi gizli tutmanın bir yolundan daha fazla olduğunu öğrendiniz. Güvenlik, herhangi bir kurumun ayrılmaz bir parçasıdır. BCP ve DRP hazırlığı, bir kurumun bir felaket durumunda bile temel iş fonksiyonlarını gerçekleştirebilmesini ve verilerini de içeren tüm varlıklarını koruyarak bunu gerçekleştirebilmesini sağlamaktadır. Sağlam bir güvenlik altyapısı, kurumun gerekli kanunları, yönetmelikleri ve diğer güvenlik gereksinimlerini yerine getirmek için gerekli

kontrolleri uyguladığına dair güvence sağlamaktadır. Kısacası, güvenlik, bir kurumun yaşayabilir olmasını sağlamakta ve iş yürütebilmesine izin vermektedir.

Ek olarak, bu bölümde bilgi sistemleri güvenliği için iş sürücüleri sunulmuştur. Bulunduğunuz iş türüne veya dikey sanayiye bağlı olarak, uyumluluğun, güvenliğin ve mahremiyetin tamamı uygun güvenlik denetimlerini uygulamak için gerekli olan sürücü gereksinimleridir. Düzenlenen verilerin gizliliği akılda kalan bir iş sürücüsüdür. Mobilite ve kişisel olarak sahip olunan BT varlıklarının kullanımı, kurumların çalışanları için BYOD varlıklarının kullanımına izin verme şeklini de yönlendirmektedir.

ANAHTAR KAVRAMLAR VE TERİMLER

Accounting - İzleme
Antivirus - Antivirüs
Business drivers – İş sürücüleri
California Database Security Breach Act (SB 1386) - California Veritabanı Güvenlik İhlali Kanunu (SB 1386)
Children's Online Privacy Protection Act (COPPA) – Çocukların Çevrimiçi Mahremiyetini Koruma Kanunu
Delphi method – Delphi yöntemi
Disaster recovery plan (DRP) – Felaket kurtarma planı (DRP)
Gap analysis – Fark analizi
Government Information Security Reform Act (Security Reform Act) – Devlet Bilgi Güvenliği Reformu Kanunu (Güvenlik Reform Kanunu)
Mobile device management (MDM) – Mobil cihaz yönetimi (MDM)
Mobility – Mobilite
Patch - Yama
Privacy policy – Mahremiyet politikası
Project Management Body of Knowledge (PMBOK) - Proje Yönetimi Bilgi Tabanı
Project Management Institute (PMI) - Proje Yönetimi Enstitüsü (PMI)
Recovery point objective (RPO) - Kurtarma noktası hedefi (RPO)
Recover time objective (RTO) - Kurtarma süresi hedefi (RTO)
Remote wiping – Uzaktan silme/temizleme
Removable storage – Çıkarılabilir depolama
Risk management – Risk yönetimi
Risk methodology – Risk metodolojisi
Risk register – Risk kaydı
Security gap – Güvenlik farkı
Security policy – Güvenlik politikası
USA Patriot Act – ABD Vatanseverlik Kanunu
User acceptance – Kullanıcı kabulü

BÖLÜM 4 DEĞERLENDİRME

1. Risk yönetimi olumsuz bir olay meydana geldiğinde buna tepki vermektedir.
   A. Doğru
   B. Yanlış
2. BT güvenliği açısından bir risk, olumlu veya olumsuz bir etki ile sonuçlanabilir.
   A. Doğru
   B. Yanlış
3. PMI'ye göre, tanımlanan risklerin listesini hangi terim tanımlamaktadır?
   A. Risk kontrol listesi
   B. Risk kaydı
   C. Risk metodolojisi
   D. Azaltma Listesi
   E. Hepsi

4. İş etki analizinin (BIA) temel amacı nedir?
   A. Görev kritik iş fonksiyonlarını tanımlamak, kategorilere ayırmak ve öncelik vermek
   B. İş sürekliliği ve felaket kurtarma planlaması için bir yol haritası sağlamak
   C. Kurulumlara risk yönetimi ile ilgili yardımcı olmak
   D. Kurumlara olaylara müdahale planlaması ile ilgili yardımcı olmak
   E. Hepsi

5. Aşağıdaki terimlerden hangisi, bir üretim BT sistemini, uygulamasını ve veriye erişimi kurtarmak için gereken süreyi tanımlamaktadır?
   A. Kurtarma noktası hedefi
   B. Kurtarma süresi hedefi
   C. Riske maruz kalma süresi
   D. Üretim kurtarma süresi
   E. Hiçbiri

6. Kurtarma noktası hedefi (RPO), üretime geri dönüştürülebilen _____ kurtarması için son noktayı tanımlamaktadır.
   A. Sistem
   B. Uygulama
   C. Üretim
   D. Veri
   E. Hiçbiri

7. Bir kullanıcının sistemlere, uygulamalara ve veriye erişebilmesi için kimlik doğrulamasında aşağıdaki çözümlerden hangisi kullanılmaktadır?
   A. Parolalar ve PIN'ler
   B. Akıllı kartlar ve belirteçler
   C. Biyometrik cihazlar
   D. Dijital sertifikalar
   E. Hepsi

8. Hangi risk yönetimi yaklaşımı BT kurumuyla birlikte çalışan işletme birimleri ile bir dağıtılmış yaklaşım gerektirmektedir?
   A. OCTAVE
   B. CRAMM
   C. NIST SP800-33
   D. ISO 27005
   E. Hiçbiri

9. NIST SP800-30 standardı, risk yönetimi gerçekleştirmek için bir _____ yönetim çerçevesi standardıdır.
   A. Risk
   B. Tehdit
   C. Güvenlik Açığı
   D. Güvenlik
   E. Hiçbiri

10. Hangi terim bir dönem boyunca maksimum veri kaybı miktarını belirtmektedir?
    A. RAI
    B. ROI
    C. RTO
    D. RPO
    E. Hiçbiri

11. Çalışanlara kendi dizüstü bilgisayarlarını veya akıllı telefon cihazlarını kullanmalarına ve BT altyapısına bağlanmalarına izin veren kurumlar aşağıda belirtilen hangi politikayı tanımlamaktadır?
    A. RTO
    B. MDM
    C. BYOD
    D. AUP
    E. Hiçbiri

12. BYOD ve mobilite için kurumsal kaygılar aşağıdakilerden hangisi?
    A. Veri sahipliği
    B. Mahremiyet
    C. Kaybedilen veya çalınan cihaz
    D. Veri silme
    E. Hepsi

13. ___, ABD'de, düzenlenmiş sağlık hizmeti bilgilerini yöneten güvenlikle ilgili bir kanundur.

14. ABD'de güvenlikle ilgili hangi kanun özellikle finansal endüstri için verilerin güvenliğini yönetmektedir?
    A. GLBA
    B. COPPA
    C. HIPAA
    D. FERPA
    E. Hiçbiri

15. Aşağıdaki iş sürücülerinden hangisi işletmelerin ve kurumların güvenlik gereksinimlerini ve uygulamalarını etkilemektedir?
    A. Mobilite
    B. Yasal uygunluk
    C. Verimlilik iyileştirmeleri
    D. Her zaman çalışır (*always-on*) bağlantı
    E. Hepsi



KISIM II

Günümüz Bilgi Sistemlerini Güven Altına Almak

Bölüm 5 Erişim Denetimleri 136

Bölüm 6 Güvenlik Operasyonları ve Yönetimi 181

Bölüm 7 Denetleme, Sınama ve İzleme 216

Bölüm 8 Risk, Yanıt ve Kurtarma 251

Bölüm 9 Kriptografi 288

Bölüm 10 Ağlar ve Telekmünikasyon 326

Bölüm 11 Kötücül Kod ve Etkinlik 354

BÖLÜM

5 Erişim Denetimleri

ERİŞİM DENETİMLERİ (*Access Controls*), otomobiller, evler, bilgisayarlar hatta akıllı telefonlarınız gibi cihazlara erişim sağlamak ve kısıtlamak için kullanılan yöntemlerdir. Erişim denetimleri ile ilk deneyiminiz, çocukken kardeşlerinizden birini odanızdan dışarı kilitlemeniz veya okulda kullandığınız kilitli dolaplar olabilir. Benzer bir örnek, arabanızın anahtarının *sadece* arabanıza uygun olması ve bu sayede sadece sizin arabanızı o anahtarla açacağınız ve çalıştırabileceğinizdir. Benzeri bir durum yaşadığınız ev ya da apartman için de geçerlidir. Aynı zamanda, birçok insan tabletinin veya akıllı telefonunun kilidini açmak için özel bir kod kullanmaktadır. Bu kod olmadan kimse o tableti veya akıllı telefonun kilidini açamaz. Veya belki televizyonunuzda bile bazı kanalları bir güvenlik kodu olmadan görüntüleyemezsiniz.

Erişim denetimi, sadece izin verilen kişiler tarafından bir kaynağın kullanılmasını sağlayarak, o kaynağı koruma işlemidir. Erişim denetimleri, bir kaynağı yetkisiz kullanımdan korumaktadır. Banka veya kredi kartınız için olan **kişisel bilgi numaraları (*personal information number* - PIN)** da aynı eviniz veya arabanız için olan anahtar kilit sistemleri gibidir. Erişim denetimlerini tanımlamanın bir diğer yolu da, bir kaynağın bir tehdide karşı korunması için yerine getirilmiş önlemler olmasıdır. Erişim denetimleri, bir kaynağa sadece "izin verilen" kullanıcıların eriştiğinden emin olmanızı sağlayan araçlardır.

İşletmeler, erişim denetimlerini çalışanlarının ne yapıp yapamayacağını yönetmek için kullanmaktadırlar. Erişim denetimleri, kullanıcıların (insanlar veya bilgisayar süreçleri) kim olduğunu, bu kullanıcıların neler yapabileceklerini, hangi kaynaklara erişebileceklerini ve hangi işlemleri gerçekleştirebileceklerini tanımlamaktadır. Erişim denetim sistemleri, bu hedefi gerçekleştirmek için parolalar, şifre üreteçleri (akıllı anahtar) (*hardware token*), biyometriler, ve sertifikalar dahil olmak üzere çeşitli yöntemler kullanmaktadırlar. Erişim izni, binalar ve odalar gibi fiziksel varlıklara verilebilmektedir. Erişim izni aynı zamanda bilgisayar sistemlerine ve veriye de verilebilmektedir.

5. Bölüm Konular

Bu bölüm aşağıda verilen konuları ve kavramları içermektedir:

- Erişim denetiminin dört parçasının neler olduğu
- Erişim denetiminin iki türünün neler olduğu
- Bir yetkilendirme politikasının nasıl tanımlandığı
- Kimlik tanımlama *(identification)* yöntemlerinin ve yönergelerinin neler olduğu

- Kimlik denetleme *(authentication)* süreçlerinin ve gereksinimlerinin neler olduğu
- İzlenebilirlik *(accountability)* politikalarının ve prosedürlerinin neler olduğu
- Erişim denetiminin biçimsel modellerinin neler olduğu
- Erişim denetimlerine yönelik tehditlerin neler olduğu
- Erişim denetim ihlallerinin etkilerinin neler olduğu
- Merkezi *(centralized)* ve dağıtık/merkezi olmayan *(decentralized)* erişim denetimlerin neler olduğu

5. Bölüm Hedefler

Bu bölümü tamamladığınız zaman, yapabilecekleriniz:

- Erişim denetim kavramlarını ve teknolojilerini tanımlayabilme
- Erişim denetiminin biçimsel modellerini açıklayabilme
- Kimlik tanımlamasının erişim denetim tarafından nasıl yönetildiğini açıklayabilme
- Erişim denetim sistemi geliştirme ve sürdürülebilirliğini sağlama

Erişim Denetiminin Dört-Parçası

Bir varlığın korunabilmesi için, öncelikle koruyan kişinin hedef kullanıcı hakkında bilgiye sahip olması gerekmektedir. **Erişim denetiminin** dört parçası aşağıda verilmektedir:

- **Kimlik Tanımlama (*Identification*)**—Varlığa ulaşmak isteyen kim?
- **Kimlik Denetleme/Kimlik Doğrulama (*Authentication*)**—İstekte bulunan kişinin kimliği doğrulanabiliyor mu?
- **Yetkilendirme (*Authorization*)**—İstekte bulunan kişi kesin olarak nelere ulaşabilir? Ve ne yapabilir?
- **İzlenebilirlik (*Accountability*)**—Bir bireyin eylemleri nasıl izlenebilir? Veriye veya sistemlere erişen veya bunlarda değişiklik yapan bir kişinin kimliğinin tanımlanabildiğinden emin olmamız gerekmektedir.
  İleriki raporlamalar ve araştırmalar için, kullanıcılarla eylemleri birbirleriyle ilişkilendiren bu süreç **izlenebilirlik** olarak bilinmektedir.

Bu dört parça iki aşamaya bölünmüştür:

- **Politika tanımlama aşaması**—Bu aşama, kimin erişim yetkisinin olduğunu ve hangi sistemleri veya ve kaynakları kullanabileceğini belirlemektedir. Yetkilendirme tanımlama süreci bu aşamada çalışmaktadır.
- **Politika yürütme aşaması**—Bu aşama, birinci aşamada tanımlanan yetkilendirmelere dayanarak erişim isteklerini onaylamakta veya reddetmektedir. Kimlik tanımlama, kimlik denetleme, yetkilendirmenin yürütülmesi ve izlenebilirlik süreçleri bu aşamada çalışmaktadır.

Erişim Denetiminin İki Türü

Erişim denetimleri genel olarak iki kategoriden birine ayrılmaktadır:

- **Fiziksel erişim denetimler**—Bu denetimler fiziksel kaynaklara erişimi denetlemektedir. Bu kaynaklar, binalar, otoparklar ve korunan bölgeleri içerebilirler. Örneğin, ofisinizin kapısı için bir anahtarınız vardır. Bu anahtar, ofisinize *fiziksel* erişimi kontrol etmektedir.
- **Mantıksal (logical) erişim denetimler**—Bu denetimler bir bilgisayar sistemini veya ağa erişimini denetlemektedir. Şirketiniz, muhtemelen şirket bilgisayarınıza oturum açmanız için özgün bir kullanıcı adı ve parola girmenizi istemektedir. Bu kullanıcı adı ve parola, sizin organizasyonunuzun bilgisayar sistemini ve ağ kaynaklarını kullanmanıza izin vermektedir.

NOT

Bazen *erişim denetimi* ve *erişim denetimleri* arasındaki fark kafa karıştırıcı olabilmektedir. *Erişim denetimin* kaynakları korumak için yapılan bir şey olduğunu hatırlayınız. Yetkisiz erişimden kaynaklarınızı korumanın yolu farklı türlerde *erişim denetimler* kullanmaktır.

Fiziksel Erişim Denetim

Genellikle, bir organizasyonun tesis yöneticisi **fiziksel erişim denetimden** sorumludur. Bu kişi size sizin çalışan numaranızla programlanmış olan bir güvenlik kartı (aynı zamanda **akıllı kart (*smart card*)** olarak da bilinir) verir. Bu kartı otoparka giden kapıyı açmak için veya gerekli katta asansörden inmek için bir kart okuyucusundan geçirmeniz gerekmektedir. Ayrıca ofisinize giden bir kapının kilidini açmak için bu kartı geçirmeniz gerekebilir. Bu kart çalışan olduğunuz için bu yerlere girişinizi sağlamaktadır. Bir çalışan olarak, organizasyonun yetkilendirme politikası size belirli yerlere fiziksel olarak erişim sağlamaktadır. Yetkilendirilmiş kartı olmayan insanlar ön kapıyı geçememelidir. Eğer sizin organizasyonunuz ofis binasını başka bir organizasyonla paylaşıyorsa, çalışma saatlerinden sonra bu binaya erişiminiz için ikinci bir kartınız bile olabilir. Bu kartlar *fiziksel* kaynaklara erişimi denetlemektedir.

Mantıksal Erişim Denetim

Güvenlik yöneticileri, **mantıksal erişim denetimlerini** bir sisteme kimin girebileceğini ve bu kişilerin hangi görevleri gerçekleştirebileceğini belirleyebilmek için kullanmaktadır. Bir sistem yöneticisi ayrıca kadrolu personelin bir sistemi nasıl kullanabileceğini ayarlamak için mantıksal erişim denetimlerini kullanabilmektedir. İnsan kaynakları (İK) sistemi için sistem kontrol örnekleri aşağıdakileri içermektedir:

- **Hangi kullanıcıların sisteme erişebileceğine karar verirler**—İK çalışanları, İK sunucularında depolanan hassas bilgiye erişim hakkına sahip olan tek çalışanlar olabilirler.
- **İlgili sistemde kullanıcının ne yaptığını takip etme**—Belirli İK çalışanları, belgeleri görüntüleme iznine sahip iken, diğer bazı İK çalışanları ise bu belgeleri düzenleme iznine sahip olabilir.
- **İlgili sistemde kullanıcının davranışlarını kısıtlama veya ayarlama**—Erişimi kısıtlanmış bir belgeyi tekrar tekrar görüntülemeye çalışan bir İK personelinin, bütün sisteme erişimi engellenebilir.

Bu izinler, mantıksal kaynaklara (veya sistem kaynaklarına) erişimi denetlemektedir.

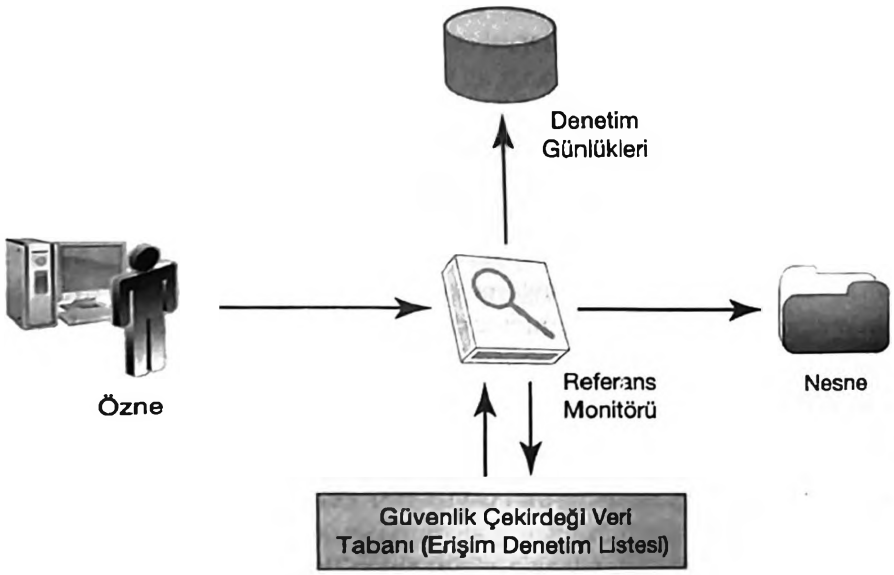
Güvenlik Çekirdeği

Güvenlik çekirdeği (*security kernel*), bilgisayar sistemleri için erişim denetimini yürüten işlem ortamının donanımın, yazılımın ve firmwarein merkez parçasıdır. Güvenlik çekirdeği, merkezi bir erişim denetim noktası sağlamakta ve **referans monitörü (*reference monitor*)** kavramını uygulamaktadır. Bütün erişim istekleri için aracılık yapmakta ve sadece uygun kurallar veya koşullar sağlandığında erişime izin vermektedir. Örneğin:

1. Özne bir nesneye erişim izni ister. Güvenlik çekirdeği bu isteği engeller.
2. Güvenlik çekirdeği, kendi içerisindeki kurallar tabanına bakar, bu aynı zamanda **güvenlik çekirdeği veri tabanı (*security kernel database*)** olarak da bilinir. Bu kuralları erişim haklarını belirlemek için kullanmaktadır. Erişim yetkileri organizasyonunuzun tanımladığı politikalara göre belirlenmektedir.
3. Çekirdek tanımlanmış erişim kurallarına göre ya erişime izin verir ya da erişimi reddeder. Sistem tarafından yürütülen bütün erişim istekleri, ileride izlenmesi ve analiz için kullanılmak üzere günlüklerde *(log)* kayıt altına alınır.

ŞEKİL 5-1, özneden belirli bir nesneye (bu durumda, bir dosya) gelen bir erişim isteğini göstermektedir. Referans monitörü gelen erişim isteğini engeller. Erişim, güvenlik çekirdeği veri tabanındaki kurallara göre onaylanmaktadır. Bu kural tabanı, bir **erişim denetim listesi (*access control list* – ACL)**, bir dizin veya başka bir erişim izinleri havuzu *(repository)* olabilir. Eğer kurallar erişim isteğine izin veriyorsa, referans monitörü erişime izin verir ve bir günlük girdisi oluşturur.

Herhangi bir sistemin erişim denetiminin tüm güvenliği, işletim sisteminin güvenliğine bağlıdır. Birçok popüler işletim sistemi (örneğin, Windows®, Linux®/UNIX®, OS X®) kapsamlı güvenlik özellikleri sağlamaktadır. Bu özellikler, sistem yöneticilerinin çok güvenli sistemler yaratmasına izin vermektedir. Bununla birlikte, bir çok mobil cihazın popüler işletim sistemi (örneğin, Android™ ve iOS®) bu güvenlik özelliklerinin bazılarından yoksundur. Bir tartışma, mobil aygıtların sunucular veya tam özellikli istemci bilgisayarlar ile aynı düzeyde güvenlik özelliklerine sahip olmaya ihtiyacı olmadığıdır. Fakat, mobil cihazlar gittikçe daha güçlü hale geldikçe, daha sıkı güvenlik gereksinimine olan ihtiyaç artmaktadır. Bazı bilişim ortamları, çoğu işletim sisteminin sağladığı güvenlik garantilerinden daha fazlasına ihtiyaç duymaktadır. Devlet sunucularındaki gizlilik dereceli/



ŞEKİL 5-1
Erişim denetimin uygulanması.

sınıflandırılmış *(classified)* bilgiler gibi aşırı hassas bilgileri işleyen sistemler daha fazla güvenlik denetimine ihtiyaç duymaktadır. Birçok işletim sistemi, bu tür sistemlerin ek güvenlik ihtiyaçlarını karşılamak için ek denetimler içermektedir. **Güvenilir işletim sistemleri (*trusted operating systems* - TOS)** olarak da anılan bu işletim sistemleri, devletin özel gereksinimlerini karşılamak için özellikler sağlamaktadır. TOS tasarımında en çok kullanılan kriter setlerinden biri, bu bölümün ilerleyen kısımlarında okuyacağınız Ortak Ölçütler *(Common Criteria)*'dir.

Erişim Denetim Politikaları

Bir **erişim denetim politikası (*access control policy*)**, belirli bir grup kullanıcının belirli bir kaynaklar kümesinde belirli bir eylem kümesini gerçekleştirmesine olanak veren bir kurallar kümesidir. Eğer kullanıcılar yetkilendirilmemişse, bu kullanıcıların sistem fonksiyonlarına ve sistem kaynaklarına erişimleri yoktur. Erişim denetim politikaları, güvenlik risklerini düşürmek ve denetlemek için kullanılmaktadır. Hem otomatik süreçler hem de insanlar erişim denetim politikalarını kullanmaktadır.

Erişim denetim politikalarını iyi yönetmek için, erişim denetiminin dört merkezi bileşenini çok iyi anlamalısınız:

- **Kullanıcılar (*Users*)**—Bunlar, başka insanlar veya süreçler için bazı servisler gerçekleştiren sistemi veya süreçleri kullanan kişilerdir. Kullanıcılar için kullanılan daha genel bir terim özneler *(subjects)*'dir.

> **İPUCU**
>
> Erişim denetim kavramları ile ilgili birçok tartışmada, kullanıcı için özne *(subject)*, kaynak için *nesne (object)* terimleri kullanılmaktadır. Bunun yanında, bir öznenin gerçekleştirmeye çalıştığı erişim eylemi anlamına gelen *istek (request)* terimi ile de karşılaşabilirsiniz.

- **Kaynaklar (*Resources*)**—Sistemdeki korunan nesnelerdir. Kaynaklara sadece yetkili kişiler tarafından erişilebilmektedir. Kaynaklar sadece yetkilendirilen şekillerde kullanılabilir.
- **Eylemler (*Actions*)**—Sadece yetkili kişilerin kaynaklar üzerinde gerçekleştirebildikleri eylemlerdir.
- **İlişkiler (*Relationships*)**—Kullanıcılar ve kaynaklar arasında var olan isteğe bağlı bulunan koşullardır. İlişkiler, yetkili bir kullanıcıya verilen *okuma, yazma, yürütme* gibi izinlerdir.

Yetkilendirme Politikaları

Erişimi denetlemenin ilk adımı, yetkilendirme kurallarını tanımayan bir politika yaratmaktır. **Yetkilendirme (*authorization*)**, kimin hangi bilgisayara ve hangi ağ kaynaklarına erişiminin olduğuna karar verme sürecidir. Birçok organizasyonda, yetkilendirme, iş rolüne, geçmiş araştırmasına ve varsa, devlet gereksinimlerine dayanarak yapılmaktadır. Bu koşullara ya da politikalara, öncelikle ya bir grup üyelik politikası veya bir yetki seviyesi politikası tarafından karar verilmektedir.

En ayrıntılı yetkilendirme politikası, her bir kullanıcıyı tek tek temel almaktadır. Bu tür politikalarda, her kullanıcının kendine atanmış ayrıcalıkları vardır. Bu **kullanıcıya atanmış ayrıcalıklar (*user assigned privileges*)**, sistem yöneticilerinin onaylanan kaynak erişimini çok ayrıntılı bir düzeyde tanımlamasına izin vermektedir. Ancak, kullanıcı tabanlı bir kimlik denetimi yaklaşımını sürdürmek oldukça zordur. Bu tür bir kimlik denetleme güncel kalabilmek için oldukça fazla sistem yönetim zamanı gerektirmektedir.

Bir **grup üyelik politikasında (*group membership policy*)**, yetkilendirme, kullanıcıların hangi grupta veya gruplarda olduğu ile tanımlanmaktadır. Grup tabanlı ayrıcalıkları atamak, benzer kullanıcıları birbirleriyle gruplayarak sistem yöneticilerinin iş yükünü azaltmaktadır. Örneğin, belki sadece BT bölümü çalışanlarının güvenlik kartları bilgisayar donanımlarının saklandığı odaya erişim sağlıyordur. Siz bu BT grubunun bir üyesi değilseniz, sizin güvenlik kartınız yeni bir monitör

(ekran) almak için ilgili odaya girmenize izin vermez. Eğer bilgisayar donanımlarının saklandığı odaya erişmek istiyorsanız, ilk BT bölümü ile iletişime geçersiniz ve onlar da BT grubunun bir üyesini size yardım etmesi için atarlar.

Bir **yetki-seviyesi politikasında (*authority-level policy*)**, belirli kaynaklara erişim için daha yüksek seviyede bir yetkiliye gereksinim vardır. Örneğin, belki sadece BT grubunun üst seviyedeki bir üyesinin sunucuların olduğu odaya giriş izni vardır. Sunucular genellikle bilgisayar monitörlerinden daha değerli olduğundan, bir politika sadece üst düzey bir personel üyesinin sunucu odasına erişimi olduğunu belirtebilir.

Kimlik Tanımlama için Yöntemler ve Yönergeler

Bir yetkilendirme politikasında yetkilendirme kurallarını bir kez tanımladıktan sonra, kuralları yürütebilirsiniz. Kullanıcının her bir kaynağa erişim isteğinde, erişim denetimler yetkilendirme politikasına göre erişime izin verir veya reddeder.

Bir yetkilendirme politikasını yürütmenin ilk adımı kimlik tanımlamadır. **Kimlik tanımlama (*identification*)**, bir öznenin bir sistem veya kaynağa erişim istemek için kullandığı yöntemdir. Özne bir kullanıcı, süreç veya başka bir varlık olabilir. Özneleri tanımlamak için yaygın olarak kullanılan birkaç yöntem vardır. Kullanılacak yöntem, güvenlik gereksinimlerinize ve bilişim ortamınızın kabiliyetlerine bağlıdır. Bir sonraki kısımda, bir öznenin kendini sisteme nasıl tanıttığı ile ilgili çeşitli yöntemleri ve yönergeleri öğreneceksiniz.

Kimlik Tanımlama Yöntemleri

Kullanıcı adı (*username*), bir kullanıcıyı sisteme tanıtmanın en yaygın yöntemidir. Bir kullanıcı adı, kullanıcı kimliği *(user ID)*, hesap numarası veya başka bir atanmış tanımlayıcı formunda olabilir. Bazı uygulamalar kullanıcıyı, çoğunlukla plastik kredi kartı formunda olan **akıllı kart (*smart card*)** kullanımı ile tanımlamaktadır. Akıllı kartlar, özneler için karışık kimlik tanımlama bilgilerini, uzun parolaları hatırlamalarına gerek kalmadan kolaylaştırmaktadır. Bir satın alma işlemi sırasında kredi kartınızı elektronik bir kart okuyucusundan geçirdiğiniz gibi bir akıllı kartı da otoparklara, binalara veya odalara erişim sağlayan bir kart okuyucusundan geçirebilirsiniz.

Biyometriler (*biometrics*) öznelerin kimliklerini tanımlamak için kullanılan başka bir erişim denetim metodudur. Biyometriler, insanları bir ya da daha fazla fiziksel veya davranışsal özellikleri ile ayırt etmek için kullanılmaktadır. Biyometri örnekleri olarak, parmak izleri, yüz veya ses tanıma, DNA eşleşmesi, el yazısı, retina taramaları ve hatta bir insanın yazma şekli verilebilir.

> **NOT**
>
> ABD Gümrük ve Sınır Koruma (*U.S. Customs and Border Protection* - CBP) programı, programın yetkilendirilmiş üyelerini tanımak için iki farklı tür biyometri kullanmaktadır. CBP, sık yolculuk yapan kişilerin normal gümrük sırasında beklemeden ve hızlıca otomatikleştirilmiş kioskları kullanabilmeleri için, bu yolcuları önceden yetkilendiren birkaç farklı program tanımlamıştır. Seçilmiş ABD ve Kanada sınır geçişlerinde bulunan NEXUS kioskları kullanıcıları tanımlamak için retina taraması kullanmaktadır. ABD'deki birçok uluslararası havaalanında bulunan Küresel Giriş kioskları kullanıcıları tanımlamak için parmak izi tarayıcılarını kullanmaktadır.

Kimlik Tanımlama Yönergeleri

Bir bilgisayar sisteminde yürütülen bütün **eylemlerin (*actions*)** belirli bir kullanıcı ile ilişkilendirildiğinden emin olmak için, her kullanıcının özgün bir tanımlayıcısı olmalıdır. Bu, her kullanıcının diğer kullanıcılardan farklı bir kullanıcı hesabının olmasının önemli olduğu anlamına gelmektedir. Hesap politikanız, eş değer hesapları *(generic account)* ve kullanıcı hesabı paylaşımını yasaklamalıdır. Özgün bir tanımlayıcı (ID), aynı isme sahip birden fazla kullanıcıyı birbirinden ayırmaya

olanak tanımaktadır. İleride gerçekleştirilecek olan raporlama ve analiz işlemleri için kullanıcılarla eylemleri ilişkilendirme sürecine **izleme (*accounting*)** denir. Özneleri tanımlamak için kullanılan veriyi güncel tutmalı ve bu veriyi yakından izlemelisiniz. Kurumdan ayrılan veya uzun bir süre aktif olmayan kullanıcıların özgün tanımlayıcılarını (ID'lerini) yetkisizleştirmelisiniz *(disable)*. Standart adlandırma kuralları uygulamalısınız; bunlar iş fonksiyonları ile ilişkili olmamalıdır. Özgün tanımlayıcılar (ID) atama süreci belgelenmelidir ve güvenli olmalıdır.

Kimlik Denetleme için Süreçler ve Gereksinimler

Bu bölümde şimdiye kadar, yetkilendirme kurallarını tanımlama ile ilgili yöntemleri ve kullanıcıları tanımlamayı öğrendiniz. Bir sonraki aşama kimlik denetlemedir. Erişim denetimin bu kısmında, kullanıcı, kimlik tanımlama sırasında sağladığı kimliği doğrulamakta veya ispatlamaktadır. **Kimlik denetleme (*authentication*)** "Kullanıcılar söyledikleri kişiler mi?" sorusunun cevabını vermektedir. Kimlik denetleme, erişim gerçekleştirmek isteyen öznenin erişim verilen özne ile aynı olduğunu ispatlamaktadır. Kimlik denetleme olmadan, kullanıcıların iddia ettikleri kişi olup olmadıklarını kesinlikle bilemeyiz.

Kimlik Denetleme Türleri

Beş farklı tür kimlik denetleme vardır:

- **Bilgi (*Knowledge*)**—Bildiğiniz bir şeydir, örneğin, parola *(password)*, uzun parola *(passphrase)*[1] veya kişisel kimlik numarası (*personal identification number* - PIN).
- **Sahiplik (*Ownership*)**—Sahip olduğunuz bir şeydir, örneğin, akıllı kart, anahtar, rozet veya belirteç *(token)*.
- **Karakteristik (*Characteristics*)**—Size özgü bir özelliktir, örneğin, parmak izi, retina veya imza. Genellikle buradaki karakteristikler fiziksel olduğundan, bu tür bir kimlik denetleme bazen *olduğunuz bir şey (something you are)* olarak tanımlanmaktadır.
- **Konum (*Location*)**—Bulunduğunu bir yerdir, örneğin, bir kaynağa erişmeye çalıştığınızda bulunduğunuz fiziksel konumdur.
- **Eylem (*Action*)**— Yaptığınız şey veya onu nasıl yaptığınızdır, örneğin, klavyede yazma şekliniz.

> **UYARI**
>
> Kullanıcı adı ve parolanın kombinasyonu, iki aşama gerektirse de tek faktörlü kimlik denetleme olarak bilinmektedir. Bu, daha hassas sistemlere, uygulamalara veya verilere erişim için yeterli olabilir de olmayabilir de. Bu durumda iki faktörlü veya çok faktörlü (*multifactor*) kimlik denetleme sağlamanız, bir binaya girmek için bir kartı (sahip olduğunuz bir şey) okuyucudan geçirmeniz, değerli bir kaynağın güvenliğini sağlamak için bir PIN (bildiğiniz bir şey) girmeniz gerekebilir.

Kimlik denetlemenin her türü tek başına iken kolaylıkla ihlal edilebilir. Tek kategoride bir denetim kullanmaya **tek faktörlü kimlik denetleme (*single-factor authentication*)** denir. Kritik ve hassas bilgileri içeren sistemler bu onaylama türlerinden en az ikisini kullanmalıdır. Bu tekniklerden iki veya daha fazla kategoride kullanılmasına **iki faktörlü kimlik denetleme (*two-factor authentication*)** denir ve bir tane kullanılmasından daha fazla güvenlik sağlar.

Bilgi ile Kimlik Denetleme

Bilgi (*Knowledge*) ile kimlik denetleme, parola, passphrase veya PIN gibi sizin bildiğiniz bir şeye dayalıdır. Sıkça değiştirilmeyen statik parolalar çok nadir görülür. Bilgisayar sistemlerinde onaylamanın en eski ve en yaygın metodu parolalardır. Aynı zamanda da en zayıf olanıdır. Değerli

[1] *Editörün Notu: Normal paroladan daha uzun ve daha güçlü bir paroladır. Harfler, sayı ve rastgele karakterler içerir.*

kaynaklarınızı korumak için, sadece parolaları kullanmamalısınız. Bir kaynağın değeri arttıkça, onu koruyan erişim denetimin de dayanıklılığı artmalıdır. Değerli kaynaklar için minimum gereksinim iki faktörlü kimlik denetlemesidir.

Saldıran kişiler genelde, kaba kuvvet saldırısı (*brute-force attack*) veya sözlük saldırısı (*dictionary attack*) kullanarak parolaları kırabilirler. Bu metotlar çok kısa veya sözlükteki kelimeleri içeren parolalar gibi zayıf parolaları kolayca kırabilirler.

- **Kaba kuvvet saldırısı (*brute-force attack*)** bütün karakterin her türlü kombinasyonunu deneyerek yapılır. Modern parola kırıcıları harflerin, sayıların ve özel karakterlerin her kombinasyonunu denemezler. Onun yerine, en başta entropiyi (rastgeleliğin bir ölçütü) ölçerler. Ondan sonra, önce düşük entropili kelimeleri, sonra orta entropili kelimeleri ve en son yüksek entropili kelimeleri test ederler.
- **Sözlük saldırısı (*dictionary attack*),** bir sözlükteki bütün kelimeleri özetleyip (*hashing*) (genellikle 01, 02, 4u vb. gibi son eklerle desteklenirler) sonrasında sistem parolasını özetlenmiş değer (*hash value*) ile karşılaştırıp bir eşleşme bularak çalışır. Bilgisayar korsanları, ismi tersinden yazma veya karakterlerin basitçe değiştirilmesi (e yerine 3, 0 yerine o, $ yerine s vb. gibi) gibi birçok alışılagelmiş aldatmacayı iyi bilirler.
- Sistemlerin çoğu parolanın özelenmiş halini depoladıkları için, saldıran kişiler bu sözlük kelimelerini önceden hesaplayıp (*precompute*), bir tablo oluştururlar. Ondan sonra, özetlenmiş versiyonu oluşturan kelimeyi bulmak için, depolanan parolanın özetlenmiş versiyonunu ararlar. **Rainbow tabloları (*rainbow tables*)** olarak bilinen bu tablolar, yaygın biçimde mevcuttur. Örneğin, AccessData'ya ait olan Forensic Toolkit® (FTK®), içinde bir milyon kelime bulunan bir rainbow tablosunu içermektedir. FTK'nın sitesine göre, bu tablo kullanıcı parolalarının yüzde 28'ini keşfedebilmektedir.

> **İPUCU**
>
> Daha kısa bir parola ömrü, kullanıcı için daha fazla koruma anlamına gelmektedir. Kullanıcılar için daha güçlü parola denetimleri oluşturmak için 30 günlük bir şifre değiştirme politikası kullanmayı dikkate alın. Daha kısa bir parola ömrü, saldırganın parolanın süresi dolmadan önce parolanın gizliliğini ihlal etme ve kullanma şansının düşmesi demektir.

Parola Hesap Politikaları: En iyi parola uygulamaların desteklenmesine ek olarak, hesap politikanız açık parola gereksinimlerini içermelidir. Aşağıdakiler önerilen hesap parola politika gereksinimlerine örnek bir listedir. (Bu maddelerin özelliklerini organizasyonunuz için değiştirebilirsiniz ve değiştirmelisiniz.)

- Karmaşıklık
  - Parola minimum 8 alfanümerik karakter içermelidir.
  - Parola büyük ve küçük harf ve sayı kombinasyonlarını içermelidir.
  - Parola ilk yedi karakteri içerisinde minimum bir tane özel karakter içermelidir.
  - Parola ilk ve son karakter pozisyonlarında sayısal olmayan bir harf veya sembol içermelidir.
  - Parola kullanıcı adı içermemelidir.
  - Parola asla yakın bir arkadaş veya akraba ismi içermemelidir.
  - Parola asla çalışan ID'si, sosyal güvenlik numarası (*social security number*), doğum tarihi, telefon numarası veya kolayca tahmin edilebilecek herhangi bir kişisel bilgi içermemelidir.
  - Parola asla İngilizce sözlükten alışılagelmiş kelimeler içermemelidir (veya kullanıcının aşina olduğu başka bir dilin sözlüğü).

En İyi Parola Uygulamaları

En görülebilir güvenlik politikası kullanıcı hesabı politikasıdır. Bu her kullanıcının karşılaşması gereken bir politikadır. İyi bir kullanıcı hesabı politikası kullanıcı adları ve parolalar için net gereksinimler belirler. Bir hesap politikasının eş değer hesapları yasaklaması gerektiğini gördünüz. Hesap politikanız ayrıca iyi parola için başarılı yöntemleri de içermelidir.

- **Güçlü parolalar oluşturun**—Parolanız taviz veremeyecek kadar karışık olmalıdır. Minimum uzunluk gereksinimlerini karşılamalıdır. Bir sözlükte olan bir kelimeyi asla parolanız olarak kullanmamalısınız. Parolanız kişisel bilgilerinize dayalı olmamalıdır. Bilgisayar korsanlarının çok geniş kelime ve isim sözlüklerini kullanan güçlü parola kıran araçlara erişimi vardır. Daha güvenli parolalar bir anlam ifade etmeyen ama akılda kalması kolay olanlardır. Örneğin, bir şiirin veya şarkının ilk kelimelerinin ilk harflerinden oluşan parolalar yaratabilirsiniz. Veya bazı karakterleri yıldız işareti (*), dolar işareti ($), "at" sembolü (@), küme parantezi ({}), matematiksel semboller (+) gibi sembollerle saklayabilirsiniz. Bunları tahmin etmesi ve kırması çok zordur. Hatırlatma: Kırma araçları (*cracking tools*) tersinden yazılan kelimeleri, bazı harfler için basit harf değişimlerini (örneğin Mouse'un M0us3 olması gibi) kontrol ederler.
- Çok gerekli olmadığı sürece bir parolanın yazılı halini *saklamayın*. Yazılı bir kopyayı saklamak istiyorsanız, onu güvenli bir yerde saklayın. Başka bir seçenek olarak, aslını yazmak yerine parolanız için bir ipucu yazın. İhtiyaç olmadığı zaman geldiğinde her türlü yazılı kopyayı yok edin.
- **Asla bir başkasıyla parolanızı paylaşmayın**—Güvendiğiniz biri bile olsa, parolanız gizli kalmalıdır.
- **Başka önemli kullanıcı hesapları için başka parolalar kullanın**—Bütün hesaplarınız için aynı şifreyi kullanmak, arabanız, eviniz, posta kutunuz ve banka kasanız için aynı anahtarı kullanmaya benzer. Eğer anahtarı kaybederseniz, saldıran kişinin her şeye erişimi olur. Başka sistemler için başka parolalar kullandığınız zaman, bir parolanız çalınsa bile, sadece bir sistemden taviz vermiş olursunuz. Bu strateji, izinsiz giren kişilerin (*intruder*) diğer sistemlerdeki hesaplara ve verilere erişim sağlamasını engeller. Bunun yanında, birbirine benzeyen parolaları da kullanmaktan sakının. Örneğin, çocuklarınızın ismini kullanan parolalar. Aynı veya benzer parolayı birden fazla sistem için kullanırsanız, parolalarınızdan birini belirleyen izinsiz giren kişinin diğerlerini tahmin etmesi kolaylaşır.
- **Eğer parolanızın riskte olduğunu düşünüyorsanız, hemen değiştirin**—Size ilk kullanım için atanan parolaları da hemen değiştirin. İdeal olarak, her 30 günde bir parolanızı değiştirin.
- **Bilgisayarlarınıza parolalarınızı kaydederken dikkatli olun**—Bazı diyalog kutuları (uzaktan erişim veya telefon bağlantıları vb. için olanlar) parolaları kaydetmek veya hatırlamak için size seçenek sunarlar. Bu seçenekleri seçmek büyük bir tehdit oluşturmaktadır çünkü biri diyalog kutusunu açtığında parola otomatik olarak listelenmiştir.

- Parolalar kurgu ürünü bir karakter veya bir yer dahil olmak üzere asla sıkça kullanılan düzgün isimler bulundurmamalıdır.
- Parolalar asla *qwertyxx* gibi harflerden oluşan basit desenler içermemelidir.
- Son kullanma tarihi; parolaların her 30 günde bir süresi dolar ve değiştirilmelidir.
- Kurtarma (*Recovery*): Unutulan parolalar, diğer kimlik denetleme bilgileri sağlandıktan sonra organizasyonun iç parola kurtarma yazılımı ile kurtarılabilir.

- Engellemek (*Disablement*): Bir kullanıcı o organizasyonla ilişkisini keser kesmez veya ona sağlanan erişime ihtiyacı kalmayınca, kullanıcının kullanıcı hesabı anında engellenmelidir.
- Geçmiş (*History*): Parola geçmişi saklanmaktadır ve parolanızı geçmiş 10 parolanızdan herhangi biri yapamazsınız.

Uzun parola (Passphrase) Kullanımı: Bir **uzun parola,** paroladan biraz daha farklıdır. Daha uzundur ve tahmin etmesi daha zordur, bu nedenle daha güvenli olarak düşünülür. Birden çok kelime içerdiği için, bir passphrase sözlük ataklarına karşı daha güvenlidir. Çoğunlukla, passphrase'ler genel ve özel anahtar yetkilendirmesi için kullanılmaktadır. Kullanıcı sadece kendinin bildiği bir passphrase kullanır ve kullanıcı bu passphrase bilgiye erişmek üzere özel bir anahtarı (*private key*) açmak için kullanır. Çoğu zaman kullanıcı passphrase'i parolaya dönüştürür. Ancak, bir sistem bir algoritmaya bağlı olarak bir passphrase'i parolaya otomatik olarak dönüştürmek üzere programlanabilir. Bir passphrase bir paroladan daha güçlüdür ama yazması biraz daha uzun sürer. Passphraseler, statik olmalarına rağmen, parolaların kaba kuvvet saldırılarından etkilendiği kadar etkilenmezler.

NOT

Kritik olmayan kaynaklar için kullandığınız parolaların aynı olması gayet normaldir. (Örneğin, çevrimiçi haberler sayfasındaki makalelere ulaşmak.) Sadece aynı parolayı kritik kaynaklarda oturum açmak için kullanmayın.

Hesap Kilitleme Politikaları: Birçok sistem, belirli bir hatalı oturum açma denemesinden sonra o kullanıcının ID'sini engellemeye programlanmıştır. Birçok durumda, kullanıcı hesapları, üç ile beş arası denemeden sonra engellenmektedir. Bir hesap eylemini tetikleyen hatalı oturum açma sayısına eşik (*threshold*) denir. Kullanıcı, birkaç dakika, bir iki saat veya güvenlik yöneticisi hesabı sıfırlayana kadar hesaba erişim sağlayamayabilir. Bu yöntem, saldıran kişilerin parolayı tahmin etmeye çalışırken birçok deneme yapmasına karşı koruma sağlar. Ancak, bu aynı zamanda izinsiz giren kişilerin kullanıcıların bir grup yanlış parola girerek—hizmet reddi saldırısının (DoS) bir formu—erişimini engellemesine de olanak tanır.

Bilginize

Organizasyonunuz otomatik bir parola sıfırlama süreci kullanmıyorsa, bilişim danışmanı (*help-desk*) personeliniz parola sıfırlama isteklerinin en sık gelen istekler olduğunu görecektir. Bilişim danışmanı personeli böyle bir istek aldığında, onların kullanıcılardan kimliklerini doğrulayan bilgi alması gerekmektedir. Örneğin; kullanıcı, ehliyet veya çalışan ID'si gibi bir kanıt sağlamalıdır. Eğer istek yüz yüze yapılmamışsa, bilişim danışmanı kullanıcının kimliğini doğrulayan bir çeşit sorgulama kullanmalıdır. Örneğin, "Annenizin kızlık soyadı nedir?" . Güçlü bir kimlik doğrulamanın yoksunluğu saldıran kişiye herhangi bir kullanıcı hesabının şifresini değiştirmek için istek verme ve hesaba istediğinde erişme olanağı sağlar.

Oturum açma olaylarını denetlemek sızmayı tespit etme çabalarınıza her ne kadar yardımcı olsa da dikkatli olun. Başarısız denetimler sistemlerinizi DoS ataklarına açık bırakabilir. Bir DoS atağı iki yöntemden biri şeklinde olur:

- Saldıran kişiler güvenlik günlüğünü (*security log*) doldururlar, büyük olasılıkla sistemin çökmesine veya diğer kullanıcıların oturum açmasına engel olmasına neden olurlar.
- Saldıran kişiler vakaların üstüne yazılmasına (*overwritten*) neden olurlar. Bunu ağınızda sürekli yanlış kullanıcı adı ve yanlış parola girerek oturum açma denemeleriyle ya parlar. Kasıtlı olarak denetim olaylarının üstüne yazarak, etkili bir şekilde atak eylemlerinin kanıtlarını silerler.

Hesap kilitleme (*account lockout*) politikası yazarken dikkatli olun. Kısıtlayıcı bir politika, organizasyonunuza bir atak olmasını engelleme şansını arttırır. Ama zorlu bir hesap kilitleme politikası ile siz istemeden yetkili kullanıcıların hesabını kilitleyebilirsiniz ve bu çok korkutucu ve masraflı bir durumdur. Bir hesap kilitleme politikası uyguladığınızda, eşiği yüksek tutun ki yetkili kullanıcılar parolalarını yanlış girdiklerinde hesapları kilitlenmesin.

Oturum Açma Olaylarını Denetleme: Bu bölümün ileriki kısımlarında denetimi öğreneceksiniz ama burada da bahsetmeye değer. İşlem ortamınıza kimlerin eriştiğini takip etmenin bir metodu oturum açma olaylarını **denetlemektir** (***audit***). Bu yöntem size, bir kullanıcının bir bilgisayarda oturum açma ve kapama kayıtlarını sağlar. Eğer yetkisiz bir kullanıcı başka bir kullanıcının kullanıcı adı ve parolasını çalarsa ve bir bilgisayardan oturum açarsa, o güvenlik açığının ne zaman olduğunu belirleyebilirsiniz. Oturum açma olayları kategorisindeki başarısız olayları denetlediğinizde (***başarısızlıkları denetleme*** **(failure auditing)** olarak da bilinir), başarısız olayın, yetkisiz kullanıcıların veya saldıran kişilerin bir bilgisayarda veya sistemde oturum açmayı denemelerinden kaynaklanıp kaynaklanmadığını görebilirsiniz. Bu saldırı tespitine bir örnektir.

Sahiplik ile Kimlik Denetleme

Sahiplik (***ownership***) ile kimlik denetleme doğrulamanın ikinci türüdür. Bu akıllı kart, anahtar, rozet veya belirteç (*token*) gibi sahip olduğunuz bir şeydir. Belirteçler senkronize veya asenkronize olabilir.

Senkronize Belirteçler: Senkronize belirteç onaylama sunucusundaki ve cihazdaki sayıyı hesaplayan bir algoritma kullanır. Numarayı cihazın ekranında gösterir. Kullanıcı, tıpkı parola kullanılması gibi oturum açma kimlik denetleyicisi olarak bu sayıyı kullanır.

Zaman tabanlı senkronizasyon sisteminde, o anki zaman girdi değeri olarak kullanılır. Belirteç ekranında görüntülenen yeni bir dinamik parola (genellikle dakikada bir) oluşturur. Erişim sağlamak için parola kullanıcının çalışma istasyonundaki PIN ile birlikte girilir. Belirteç klavyesine ihtiyaç yoktur. Bu sistem sadece belirteçteki saatin onaylama sunucusundaki saat ile aynı olmasını gerektirir. Eğer saat senkronizasyon dışına çıkarsa, sunucu iki taraftaki zamanın da üç veya dört dakika sapmasını tespit etmek için arama yapar. Eğer aradaki fark çok artarsa, saatleri tekrar senkronize etmelisiniz.

NOT

Senkronize belirteçler, PIN ve parolanın ikisinin de otomatik olarak girilmesini sağlayan yakınlık cihazlarında (*proximity devices*) kullanılırlar.

Olay tabanlı senkronizasyon sistemi, bir sayacın değerinin her kullanımda bir arttırılması ile zaman senkronizasyon problemini önlemiştir. Sayaç girdi değeridir. Kullanıcı tek seferlik bir parola yaratılması için bir tuşa basar ve bu parolayı ve kendi PIN'ini çalışma istasyonunda erişim sağlamak için girer. Olay tabanlı senkronizasyon sistemleriyle ilgili yaygın bir sorun, kullanıcının belirteç ile bir parola yaratıp sistemde oturum açarken bu parolayı kullanmaması ve sunucudaki sayacın belirteçteki sayaçla senkronizasyon dışı kalmasından ortaya çıkar.

Sürekli (***continuous***) **senkronizasyon** kullanıcıların kimliklerinin sürekli olarak doğrulanması gereken sistemler tarafından kullanılır. Bu genellikle erişim denetim sistemiyle sürekli iletişim halinde olan yakınlık kartları veya diğer cihazlar ile yapılır. Eğer kullanıcı masaüstünden uzaklaşırsa ve erişim denetim dedektörünün menzilinden uzaklaşırsa, sistem masaüstünü kilitler.

Asenkron belirteçler: Belirteç tabanlı cihazların iki türünden ikincisi **asenkron belirteçtir.** Kredi kartı boyutundaki bir hesap makinesine benzer. Kimlik denetleme sunucusu kullanıcının girdiği kimlik

sorma (*challenge*) sayısını bildirir. Belirteç, kimlik denetleme sunucusunun sağladığı değere bir yanıt hesaplar. Kullanıcı sunucuya belirteç üzerinde gösterilen değer ile karşılık verir. Bu sistemlerin birçoğu belirteci kötüye kullanımdan korumak için, kullanıcının kimlik sorma işinden önce PIN girmesini gerektirir.

Bir asenkronize belirteç cihazı, kimlik denetleme servisi ve kimlik denetlemeye çalışan uzak varlık arasında bir diyalog içeren kimlik sorma-yanıt verme teknolojisini kullanır. Bu nümerik bir klavye gerektirir. **ŞEKİL 5-2** asenkron belirteç kimlik sorma yanıt verme sürecini göstermektedir.

1. Kullanıcı, kimlik denetleme sunucusu üzerinden erişim istek eder. (Örnek: KullanıcıID)
2. Kimlik denetleme sunucusu kullanıcıya kimlik sorma numarası gönderir.
3. Kullanıcı kimlik sorma numarası ile akıllı telefonundaki PIN'i girer.
4. Akıllı telefon kriptografik cevabı hesaplar. (Örnek: "parola")
5. Kullanıcı "parola"yı kimlik denetleme sunucusuna yollar.
6. Kimlik denetleme sunucusu uygulama sunucusuna erişim izni verir.

Aşağıda asenkronize kimlik sorma karşılık verme oturumunun aşamaları verilmiştir:

1. Kullanıcı oturum açma isteğini başlatır.
2. Kimlik denetleme sunucusu kullanıcıya bir kimlik sorma (*challenge*) (girdi değerindeki rastgele bir sayı) sağlar.
3. Kullanıcı sunucudan alınan kimlik sormayı ve sadece hesaplama cihazındaki (kredi kartı boyutundaki bir hesap makinesi veya bir bilgisayardaki veya bir akıllı telefondaki bir yazılım) kullanıcının bildiği gizli PIN'i girer.
4. Belirteç (veya yazılım) kimlik sormaya, belirtecin ekranında gözüken, bir yanıt (parola) yaratır.
5. Kullanıcı, kimlik denetleme sunucusuna doğru parolayı sağlar.
6. Erişime izin verildi. Asenkronize belirteç cihazı ve doğru PIN olmadan, kimlik sormaya doğru bir cevap yaratılamaz.



ŞEKİL 5-2
Asenkronize belirteç kimlik sorma-cevaplama

USB belirteçleri **açık anahtar altyapısı (*public key infrastructure* - PKI)** kullanır. Örneğin, güvenilen sertifikasyon otoritesi tarafından imzalanmış bir sertifika ve tek seferlik parola sağlamazlar. Bir **USB belirteci (USB *token*)**, bilgisayarınızın USB portuna taktığınız bir donanım cihazıdır. Cihaz sizin dijital imzanızla kodlanmıştır. Bununla bir şey yazmanıza gerek kalmaz. Belirteçteki dijital imzanızın varlığı, sahiplik kanıtı (*proof of possesion*) (size ait olan bir şey) sağlamanız için yeterlidir.

NOT

Akıllı kartlarla ilgili bir sorun, bazı kullanıcıların onları okuyucunun içinde başıboş bırakmalarıdır. Bu, akıllı kart okuyucunun içinde bulunduğu sürece her kullanıcının yetkili kullanıcı olması demektir.

NOT

Bütün akıllı kartlar fiziksel olarak bir okuyucuya yerleştirilmek zorunda değildir. Temassız veya yakınlık akıllı kartları, okuyucunun yanındayken çalışan gömülü radyo frekansı (*radio frequency* - RF) alıcı vericisi içerir.

NOT

Ortak Kriter hakkında daha fazla bilgi için, *www.commoncriteriaportal.org* sitesini ziyaret edin.

Bir akıllı kart, bir kart okuyucusu aracılığıyla kabul eden, saklayan ve bilgi gönderen bir veya daha fazla çipi içeren kredi kartı şeklindeki bir belirteçtir. Akıllı kartta bulunan bilgi, kimlik denetleme bilgisini sağlar. Birçok akıllı kart gömülü mikro işlemciye güç vermek için bir okuyucu kullanır. Kullanıcı iletişime başlamak için kartı okuyucuya yerleştirir.

Akıllı kartların önemli bir avantajı, kullanıcı kimlik denetleme sürecinin kullanıcı konumunda, akıllı kart ve okuyucu arasında gerçekleşmesidir. ID'ler ve kimlik denetleme verisi uzak bir sunucuya iletilmemektedir, bu sayede "güvenilir yol (*trusted path*)" problemi önlenir (ID'ler ve kimlik denetleme bilgileri uzak bir sunucuya iletildiğinde, hassas bilgi koklayıcılara (*sniffers*) veya gizli dinleyicilere (*tappers*) açık edilebilir). Bir akıllı kart ile, okuyucu kimlik denetleme sunucusu ile el sıkışmasını (*handshake*) sürdürür ve kimlik denetleme için direkt olarak doğrular. Sonra, **Ortak Kriter (*Common Criteria*)** olarak da bilinen, **Bilgi Teknolojileri Güvenlik Değerlendirmesi için Ortak Kriter (*Common Criteria for Information Technology Security Evaluation*)** ile güvenilir yol uyumu sağlar. Ortak Kriter çerçevesi, kullanıcıların, sağlayıcıların (*vendor*) ve test laboratuvarlarının birlikte çalışmalarını ve bilgi sistemi ürünlerini belirtme, uygulama ve hesaplama çabalarını resmi olarak paylaşmalarını sağlar.

Son olarak, birçok organizasyon hassas tesisler veya otoparklar gibi yasaklı bölgelere erişimi denetlemek için manyetik şeritli kartlar (*hafıza kartları (memory cards)* olarak da bilinirler) kullanmaktadır.

Karakteristikler/Biyometrikler ile Kimlik Denetleme

Biyometrikler, hem tanılama (fiziksel biyometrikler) hem de onaylama (mantıksal biyometrikler) için kullanılmaktadır. Biyometrikler, bir kişinin anatomik veya fiziksel eylemlerinin çeşitli özgün parçalarını ölçmeyi içerir. Bu bölümde öğreneceğiniz ortak biyometrik ölçüler iki kategoriye ayrılır:

- **Statik (örneğin, psikolojik) ölçüler**—Olduğunuz şey(ler). Psikolojik biyometrikler, parmak izlerini tanımayı, iris tanecikliği, retina kan damarları, yüz görünüşü, el geometrisi vb. gibi.
- **Dinamik (örneğin, davranışsal) ölçüler**—Yaptığınız şey(ler). Davranışsal biyometrikler, ses tonunun değişmesini, tuş darbelerini ve imza hareketlerini içerir. Bu tür biyometriklerin bazen kendi içinde kategorilere ayrıldığını not ediniz (eylem ile kimlik denetleme).

Biyometrikler ile İlgili Endişeler: Biyometrikler ile ilgili üç temel endişe vardır:

- **Kesinlik/Doğruluk (*Accuracy*)**—Biyometrik cihazlar mükemmel değildir. Her birinde en az iki hata oranı vardır. Yanlış reddetme oranı (*false rejection rate* - FRR), geçerli olan öznelerin

reddedilmesi oranıdır. Yanlış kabul oranı (*false acceptance rate* - FAR), geçersiz öznelerin kabul edilme oranıdır. FRR ve FAR arasında bir ödünleşme (bir şeyi elde etmek için diğerinden vazgeçme) (*tradeoff*) vardır. İki oranın da aynı olduğu noktalara çapraz hata oranı (*crossover error rate* - CER) denir. CER, sistemin kesinliğinin yüzde olarak ölçüsüdür. Pratikte, çok hassas kaynakları koruyan biyometrik cihazlar, yüksek seviyede yanlış reddedilme oranı kabul etmeye ayarlanmıştır. Daha az hassas kaynakları koruyan sistemler, potansiyel olarak yetkisi olmayan kişilere sistemi çok yavaşlatmamak adına erişim verebilir.

- **Kabul edilebilirlik**— Retina taramaları gibi bazı biyometrik ölçümler, imza dinamikleri gibi başka biyometrik ölçümlere göre bazı kullanıcılara karşı daha reddedicidir. Eğer kullanıcılar bir sistemi kullanmakta rahat edemiyorlarsa, kullanmayı reddedebileceklerini not etmek önemlidir.
- **Tepki süresi**—Her biyometrik cihazın, sistemin bir kimliği kontrol etmek ve yanıt vermek için süreye gereksinimi vardır. Çok uzun süre alan bir sistem çalışmıyor olabilir. Örneğin, havaalanı güvenliklerindeki yüz tanımaları ele alınız. Eğer sistem bir yolcuyu tanımak için beş dakikadan fazlasını istiyorsa, yolcu kontrol yeri kuyrukları şu anda olduklarından daha uzun bir hale gelecektir. Birçok kontrol yeri için tepki süresi hızlı olmalıdır. Çok yavaş olan bir şey, üreticiliği ve erişimi sekteye uğratır.

Biyometrik Türleri: Aşağıdakiler de dahil olmak üzere, birçok biyometrik türü vardır:

- **Parmak izi**—Bu, parmağınızın ucundaki girintilerin ve çıkıntıların desenlerini kaydeder.
- **Avuç içi izi**—Bu, avuç içinizin fiziksel yapısını inceler. Bir kullanıcıyı doğrulamak için, hem el izlerinin hem de parmak izlerinin doğruluğunun (*accuracy*) son derece fazla olduğu düşünülmektedir. Sistemin tepki süresi 5-7 saniyedir ve insanlar bunları kabul etmeye yatkındır.
- **El geometrisi**—Bu biyometrik türüyle, bir kamera bir elin avuç içinin ve kenarlarının 45 derecelik bir ayna ile fotoğrafını çeker. Analiz; parmakların uzunluğu, genişliği, kalınlığı ve konturu kullanılarak yapılır. Sistemin tepki süresi 1-3 saniyedir ve insanlar bunları da kabul etmeye yatkındır.
- **Retina taraması**—Bu tür biyometrik, düşük seviyeli bir ışık kaynağı ve kamera kullanarak *retina* olarak bilinen gözün arka kısmındaki kan damarlarını analiz eder. Retina taraması, kimlik denetleme ve yetkilendirme için çok kesindir. Ancak, retina taraması diyabet, hamilelik ve kalp krizleri gibi bir kişinin fiziksel durumundaki değişime karşı hataya yatkındır. Bu durumların ortaya çıkması, o kişilerin sisteme tekrar kayıt olmalarını gerektirir. Birçok insan bunu elverişsiz ve sağlığa zararlı ve özel medikal verilerini açık etmek zorunda hissettikleri için, retina taramalarını sevmezler. Tepki süresinin ortalaması 4-7 saniyedir.
- **İris taraması**—Bu tür biyometrik ince çizgilerin, çukurların, çatlakların, lekelerin ve liflerin vb. gibi şeylerin neden olduğu iris olarak da bilinen, gözün renkli kısmındaki özgün desenleri küçük bir video kaydedicisi kullanarak kaydeder. İris taramaları onaylama ve yetkilendirme için çok kesindir. İris tarama cihazları oturumun ele geçirilmemesi (*session hijacking*) için devamlı takip etme yeteneği sağlamaktadır. Tepki süresi 1-2 saniyedir. İris taramaları kabul görmektedir.

- **Yüz tanıma**—Yüz tanıma biometrikleri ile, video kameralar gözler arasındaki uzaklık, çene ve yanak şekli, burnun uzunluğu ve genişliği, elmacık kemiği ve göz girintileri vb. gibi yüzün belirli özelliklerini ölçer. 14 ortak özellik ölçülebilecek 80 kadar tanesi arasından seçilir. Bu özellikler yüz ile ilgili bir veri tabanı oluşturmak için kullanılır. Yüz tanıma kimlik denetleme için kesindir, çünkü yüz açısı kontrol edilebilir. Ancak ilerleyen bir kalabalıkta tanılama için o kadar kesin değildir. Yüz tanıma, pasif ve elverişli olduğu için, sürekli bir kimlik denetleme verebilir.
- **Ses deseni**—Ses desen biometrikleri ile, ses kayıt cihazları ve diğer sensörler, nazal tonlar, gırtlak ve boğaz titreşimleri ve sesteki hava basıncı gibi yediye kadar parametreyi yakalarlar. Ses deseni kimlik denetleme için kesin değildir çünkü sesler bir yazılım aracılığı ile kopyalanabilir. Doğruluk (*accuracy*) arka plandaki ses ile azaltılabilir. Birçok kullanıcı bu tip biometriği kabul eder. Tepki süresi 14 saniyeye kadar değişir. Bu kadar uzun tepki süresi nedeniyle günlük kullanımda çok popüler değildir.
- **Tuş darbesi dinamikleri**—Burada kullanıcı seçilen cümleyi bir referans şablonuna tuşlar. Tuş darbesi dinamikleri, her tuşa basmanın bekleme süresini (*dwell time*) (bir tuşa ne kadar süre basıldığı) ve uçuş süresini (*flight time*) (iki tuş darbesi arasındaki süre) ölçer. Tuş darbesi dinamikleri çok kesin olarak düşünülür. İki faktörlü kimlik denetlemenin yerine geçmek için uygundur. Biri oturum açarken teknolojiyi kullanmak kolay olduğundan, ID süreçlerinden bilmeniz gereken bir şey ile sahip olmanız gereken bir şeyi birleştirir. Tuş darbesi dinamikleri iyice kabul edilmiştir ve daimi kimlik denetleme verebilir.
- **İmza dinamikleri**—Bu tür biometrik ile, kalem darbe hızı, yönü ve basıncı bir kalemdeki, kopya kalemindeki (*stylus*) veya yazma tabletindeki sensörler kullanılarak kaydedilir. İmza dinamikleri kesindir ve kullanıcılar tarafından kabul edilmiştir.

Biometriklerin Avantajları ve Dezavantajları: Biometrikler aşağıdaki avantajları sunarlar:

- Bir kişi kimlik denetleme için fiziksel olarak orada olmalıdır.
- Hatırlayacak bir şey yoktur.
- Biometriklerin sahtesini yaratmak zordur.
- Kayıp ID'ler veya unutulmuş pasaportlar sorun değildir.

Biometriklerin negatif yanları da vardır. Aşağıdakileri içerir:

- Fiziksel karakteristikler değişebilir.
- Fiziksel olarak engelli insanlar, parmak izi, el geometrisi veya imza tabanlı sistemleri kullanırken zorluk çekebilirler.
- Bütün teknikler eşit olarak etkili değildir ve genellikle hangi tekniğin verilen kullanım için en iyisi olduğuna karar vermek zordur.
- Tepki süresi yavaş olabilir.
- Gereken cihazlar pahalı olabilir. Kimlik denetleme için çok fazla zaman gerektiren metotlarda, girişlerde ve erişimlerde dar boğaz olmaması için organizasyon fazla sayıda kimlik denetleme cihazı sağlamak zorunda kalabilir.

Mahremiyet Sorunları: Biyometrik teknolojiler, sadece bir insan hakkında veri toplamayı içermez. Biometrik, insanlar için *içsel (intrinsic)* olan bilgileri toplar. Her kişi bir sınava girmelidir ve bu sınav dijital olarak kaydedilir ve depolanır. Bu veriye yetkisiz erişim yanlış kullanıma sebep olabilir. Biometrikler buna ek olarak, bir kişinin hareketlerini ve eylemlerini izler. Son olarak, kaydedilmiş ve tekrar oynatılan veri bir kişinin başka bir kişiymiş gibi davranmasına olanak tanır ve kimlik hırsızlığı riski yaratır.

Konum ile Kimlik Denetleme

Bir kullanıcının fiziksel konumu, kimlik denetleme için güçlü bir gösterge olabilir. Konum, bir kaynağa erişim veya ret vermeyi önermek için ek bilgi sağlayabilir. Örneğin, bir kullanıcının bir kart okuyucusuna hesap kartı numarasıyla PIN sağladığını düşünün. Kart okuyucusu Topeka, Kansas'ta bir benzin pompasında konumlanmaktadır. PIN'i sağlayan kullanıcı Tampa, Florida'da konumlanmaktadır. Ayrı konumlar, hesaplara erişimi reddetmek için yeterli şüpheyi uyandırabilir. Başka bir yandan, bir taksi zaman planlama uygulaması, kullanıcının konumunu, kullanıcının taksi çağırdığı konumda olup olmadığını doğrulamak için istek edebilir. Başka yöntemlerde de olduğu gibi, konum ile kimlik denetleme sadece çok faktörlü kimlik denetlemelerinde kullanılmalıdır.

Eylem ile Kimlik Denetleme

En yeni onaylama metotlarından biri bir kullanıcının eylemlerine dayalıdır. Bunun biometriklerin bir alt kümesi olup olmadığı ile ilgili bir kafa karışıklığı vardır. Biyometrik kısmında zaten bütün detayları inceledik ama, eylem ile kimlik denetlemenin bazen ayrı bir kategoriye ayrıldığından da haberdar olun. Buna *yaptığınız bir şey* denir. Bu tür kimlik denetleme, bir şeyi nasıl yaptığınız ile ilgili örüntüleri ya da ince ayrıntıları saklar. Birçok insan tahmin edilebilir bir hızda yazar ve belirli tuşlar arasında duraklar. Bu desenler saklanabilir ve kimlik denetleme sırasında kullanılabilir.

Tek Oturum Açma

Tek oturum açma (*single sign-on* - SSO) stratejisi kullanıcılarına bir bilgisayarda ya da ağda bir kere oturum açmalarına ve kimlik ve yetkilendirme tanıtımlarının (*credential*) kullanıcıların yetkili oldukları bütün bilgisayarlara ve sistemlere girmelerine izin vermesini sağlar. Kullanıcıların, birkaç kullanıcı adı veya parola girmelerine gerek yoktur. SSO sistem çökmelerinde büyük rol oynayan insan hatasını azaltır. Çok istenmesine rağmen devreye sokulması zordur.

SSO'nun Avantajları ve Dezavantajları

SSO'nun avantajları aşağıda listelenmektedir:

- Etkili bir oturum açma sürecidir. Kullanıcı sadece bir kere oturum açar.
- Daha güçlü parolalar sağlar. Sadece bir parolayı hatırlamak gerektiğinde, kullanıcılar genellikle daha güçlü parolalar kullanmaya istekli oluyorlar.
- Sürekli ve belirgin yeniden kimlik denetleme (*reauthentication*) sağlar. SSO sunucusu iş istasyonuyla (*workstation*) temas halinde kalarak onun eylemlerini izler. Bu, kullanıcı giriş noktasının yanındaki sistemin tamamında sürekli olarak uygulanabilecek zaman aşımı eşiğini sağlar. Bir iş istasyonu veya uç nokta (*endpoint*) belirli bir süre aktif olmayınca, bağlantısı kesilebilir.

Kerberos Anahtar Dağıtımı Merkez Sunucusu

Kerberos anahtar dağıtım merkez (*key distribution center* - KDC) sunucusu iki fonksiyona hizmet eder:

- **Kimlik denetleme sunucusu (*authentication server* - AS) olarak hizmet eder**—Kimlik denetleme sunucusu, bir kullanıcıyı, kullanıcının parolasına dayalı daha önceden verilmiş gizli bir anahtar yardımıyla onaylar. Bu KDC ile paylaşılmış ve KDC'nin veri tabanında depolanmış bir simetrik anahtardır. Kullanıcıdan servis için bir istek alındığında, kullanıcı iş istasyonuyla bundan sonra olan bütün konuşmalar bu paylaşılan anahtar ile şifrelenir. Kullanıcı KDC'ye bir parola yollamaz. Bunun yerine, kimlik denetleme, kullanıcının iş istasyonundaki Kerberos yazılımının kimlik denetleme sunucusundan gelen bileti deşifre etmek için paylaşılan anahtarı yaratacak parolayı istek ettiği zaman olur. Bilet, istenilen kimlik denetleme sunucusuyla iletişim kurmak için gereken oturum anahtarını içerir. Eğer yanlış parola verilirse, bilet deşifre edilemez, erişim denemesi başarısız olur.
- **Bilet-onaylama sunucusu (*ticket-granting server* - TgS) olarak hizmet eder**—Bilet-onaylama sunucusu kullanıcı doğrulandıktan sonra, aynı veya farklı uygulamalar için daha fazla bilet almak için yöntemler sağlar, bu sayede bu aşamanın bir gün içinde defalarca kez tekrarlanmasına gerek kalmaz. Biletler genelde bir günde veya birkaç saatte geçerliliğini yitirir.

Bu, sistemi bir kullanıcının iş istasyonunu kimlik denetimi yapılmamış ve asıl kullanıcı gibi davranabilecek bir kullanıcıya bırakmasından korur.

- Başarısız oturum açma girişimi eşikleri ve kilitlemeleri sağlar. Bu, kaba kuvvet kullanarak onaylı kullanıcı adı ve parola kombinasyonunu belirlemeye çalışan izinsiz giren kişiye karşı korur.
- Merkezi yönetim sağlar. Prosedürlerin ve politikaların devamlı uygulamasını garantiler.

SSO'nun dezavantajları aşağıdakileri içerir:

- Ele geçirilmiş bir parola izinsiz giren kişiye, parolanın sahibinin erişiminin olduğu her yere erişim vermektedir. Dinamik parolaların ve/veya iki faktörlü kimlik denetlemenin kullanımı bu problemi azaltabilir.
- Statik parolalar çok sınırlı bir güvenlik sağlamaktadır. İki faktörlü kimlik denetleme veya en kötü ihtimalle tek seferlik (dinamik) parolanın kullanımı, SSO kullanan bir kullanıcıdan istek edilmektedir.
- SSO'yu özgün bilgisayarlara veya ağdaki eski sistemlere eklemek zor olabilir.
- Betikler/Komutlar (*scripts*) yönetmeyi kolaylaştırmasına rağmen, veriyi açık ederler. Betikler, hassas sistemlere ve verilere iki faktörlü kimlik denetleme sağlamaz.
- Kimlik denetleme sunucusu sisteme erişim için tek arıza noktası (*single point of failure*) haline gelebilir.

Kimlik denetleme sistemleri bazı ortak servis gereksinimleri paylaşırlar. Hepsi kullanıcıların (özneler) kaynaklara (nesneler) erişim istek etmesi için bazı metotlar sağlar. Daha sonra, isteğin onaylanması veya reddedilmesi için bazı yöntemler sağlarlar. SSO kimlik denetlemesini ele almak için bir yöntem, merkez sunucu kullanmaktır. Kullanıcı bütün istekleri için merkez sunucu ile iletişime geçer. Bir başka yaklaşım **birliktir (*federation*)**. Birleştirilmiş kimlik denetleme sistemleri, kullanıcı tanıtımlarını (*credentials*) birkaç sunucu arasında paylaşır. İlgili başka bir yaklaşım ise, **geçişli güven (*transitive trust*)** kimlik denetlemesidir. Bu modelde, ilk oturum açma kimlik bilgileri, istek ile diğer güvenilen sunuculara iletilmektedir. Bir kimlik denetleme sunucusu sadece

güvendiği başka bir sunucu ile kullanıcı kimlik bilgilerini paylaşacaktır. Bu, birlikten sadece çok az daha farklıdır. Birleştirilmiş sistemde, kimlik denetleme sunucusu grubu statiktir. Geçişli güven ortamlarında, güvenilir sunucular grubu zamanla oluşur ve her kullanıcı ve istek için farklı olabilir. Güvenilir grubun içindeki sunucular bir kullanıcının izlediği erişim isteği yoluna bağlıdır.

SSO Süreçleri

SSO süreçlerinin örnekleri Kerberos, SESAME ve LDAP metotlarını içerir.

Kerberos: Kerberos, güvenli olmayan bir ağda birbirleriyle haberleşen düğümlerin birbirlerine güvenli bir şekilde kimliklerini ispatlamasına olanak sağlayan bir bilgisayar ağı onaylama protokolüdür. Kerberos, aynı zamanda Kerberos protokolünü uygulayan Massachusetts Institute of Technology (MIT) tarafından yayımlanan bir ücretsiz yazılım çiftleridir. Tasarımı öncelikle istemci/sunucu modelini hedeflemiştir ve ortak kimlik denetimi sağlar, kullanıcı ve sunucu birbirlerinin kimliklerini onaylar. Kerberos protokol mesajları, gizlice dinleme (*eavesdropping*) ve yeniden gönderme (*replay*) saldırılarına karşı korunmaktadır.

Başlamak için, kullanıcı ID'sini ve erişim isteğini iş istasyonundaki Kerberos istemci yazılımı üzerinden **anahtar dağıtım merkezine (*key distribution center* - KDC)** yollar. KDC'nin kimlik denetleme sunucusu kullanıcının ve istek yapılan servisin KDC veri tabanında olduğunu doğrular ve bir bilet gönderir. Bilet, zaman damgasının istek yapılan servis için yapıldığı kullanıcıya özgü bir anahtardır. Eğer bilet kullanılmadan zamanı dolarsa, çalışmayacaktır. Biletin içinde kullanıcı ID'si ve oturum anahtarı ve bununla beraber nesne için nesnenin KDC ile paylaşılan anahtarı ile şifrelenmiş bilet bulunmaktadır.

Kerberos ile güvenlik dikkatli bir yürütmeye ve bakıma bağlıdır. Zaman damgalarıyla kimlik bilgilerinin tekrar kullanım tehdidini azaltarak, kimlik denetleme tanıtımları için yaşam süreleri olabildiğince düşürülmelidir. KDC fiziksel olarak korunmalıdır çünkü, o —özellikle kimlik denetleme sunucusu— potansiyel tek arıza noktasıdır (*single point of failure*). Fazla/yedek kimlik denetleme sunucuları riski azaltabilir. KDC güçlendirilmelidir, bu, onun güvenlik altına alınmış bir işletim sistemine ve uygulamaya sahip olması demektir. Herhangi bir Kerberos olmayan ağ eylemine izin vermemelidir.

> **NOT**
>
> Akıllı kartlar SSO hizmetleri sağlayabilir. Sürekli bir kimlik denetleme sisteminde bir akıllı kartın varlığı, kullanıcıya SSO olarak görünebilir. Tüm kimlik denetleme değişimleri kullanıcıya şeffaftır. Akıllı kart kimlik denetleme sistemi için uygun olduğu sürece, kullanıcının kaynaklara erişmek için herhangi bir kimlik bilgisi sağlaması gerekmez.

SESAME: Çok-Sağlayıcılı Bir Ortamdaki Uygulamalar için Güvenli Avrupa Sistemi (*The Secure European System for Applications in a Multi-Vendor Environment* - SESAME) Avrupa Komisyonu tarafından desteklenen araştırma ve geliştirme projesidir. SESAME, Kerberos'taki bazı zayıflıklara çözüm olması amacıyla geliştirilmiştir. Kerberos'un aksine, değiş tokuş edilen bilgiyi koruyarak hem simetrik hem de asimetrik anahtarları kullanarak anahtar yönetimini iyileştirmiştir. Temelde Kerberos'un bir uzantısıdır. Açık anahtar kriptografisi ve rol tabanlı erişim denetim özelliklerini sunmaktadır.

LDAP: Hafifletilmiş Dizin Erişim Protokolü (***Lightweight Directory Access Protocol* - LDAP),** dağıtık dizin servislerini tanımlamak ve kullanmak için bir protokoldür. LDAP'nin sağladığı çekirdek servislerden biri erişim tanıtımlarını (*credentials*) yönetmesidir. LDAP, yöneticilerin, ağdaki bilgisayarların ve cihazların oturum açma ve erişim tanıtımlarını yönetmesini kolaylaştırır. LDAP, SSO çözümü sağlamamasına rağmen bu protokolün birçok SSO çözümünde kullanıldığını göreceksiniz. LDAP rutin olarak ağlar arasında hassas bilgi değişimi yaptığından mesajları güvelik altına almak çok önemlidir. LDAP mesajlarının güvenli olduğundan emin olmanın en önemli ortak

yollarından biri de Güvenli LDAP (secure LDAP) kullanmak veya SSL üzerinden LDAP (LDAPS) kullanmaktır. LDAP'ın bu versiyonu bütün mesaj değişimleri için ağ üzerinde sadece SSL/TLS kullanır.

İzlenebilirlik için Politikalar ve Prosedürler

Bu noktaya kadar kullanıcı kimliklerinin nasıl tanımlandığını (1. adım), kimlik denetiminin nasıl yapıldığını (2. adım) ve kullanıcıların nasıl yetkilendirildiğini (3. adım) gördünüz. Şimdi sıra erişim denetimin son kısmında; izlenebilirlik. **İzlenebilirlik (*accountability*)**, sisteme veya veriye kimin değişiklik yaptığını öğrenmek için bir eylemi bir kişiye veya bir sürece kadar takip etmedir. Bu hataları ve yanlışları takip etmek kadar, denetlemeler ve sorgulamalar için de çok önemlidir. İzlenebilirlik, "Kullanıcıları sistemde yaptıklarından sorumlu tutabilir misiniz?" sorusuna cevap verir.

Günlük Dosyaları

Günlük dosyaları (*log files*), izlenebilirlik için anahtar bileşendir. Günlük dosyaları, kimlerin sistemde oturum açtıklarını, ne zaman oturum açtıklarını ve hangi bilgileri ve kaynakları kullandıklarının detayını veren kayıtlardır. Bilgisayarların ilk zamanlarında günlükler birkaç kullanıcı tarafından paylaşılan sistemlerde kullanılıyordu. Kullanıcıları sistemi kullandıkları zaman kadar ücretlendirmek gerekiyordu ve günlükler bu veriyi takip ediyordu. Günlük dosyaları, internet kullanımının saatlik olarak ücretlendirildiği zamanlarda CompuServe ve AOL gibi şirketler tarafından kullanıyordu. Günümüz ağlarında, birçok faturalandırma ya sabit bir ücrettir ya da bant genişliği kullanımını temel almaktadır. Zaman tabanlı faturalandırma görülmemektedir. Günümüzde günlükleme faturalandırmadan daha fazlası için kullanılmaktadır. Aynı zamanda bir sisteme erişimi tespit etmek (*detect*), önlemek (*prevent*) veya izlemek (*monitor*) için değerli bir araçtır.

İzleme ve Değerlendirme

Kullanıcı erişim aktivitelerini izini sürmenin (*trace*) ana nedenlerinden biri kuşkulu eylemleri tespit etmek ve onlara karşılık verebilmektir. Bu, sizin eylem günlüklerinizi izleyen ve şüpheli bir eylem bulduğunda sizi uyaran bir yazılım kullanmanız gerektiği anlamına gelmektedir. Sürekli izleme, güvenli erişim denetim sisteminin önemli bir parçasıdır. Ama bütün şüpheli hareketler her zaman açık değildir. Bazı zamanlarda hesap politikası güvenlik açıklarını saptamanın tek yolu kullanıcı eylemlerini bir süre boyunca incelemektir. Hesap politikanız, kullanıcı hesaplarının periyodik olarak incelenmesi gereksinimini içermelidir. Bu incelemeler kullanıcı erişim tanımlamalarının doğruluğunu onaylamaya yardımcı olur. Aynı zamanda düzgün olmayan eylemleri ve gereksiz izinleri bulmaya yardımcı olur. Tabii ki, her politika herhangi bir güvenlik açığına karşılık izlenecek adımları ana hatları ile belirtmelidir. Güvenlik açıklarına nasıl karşılık verileceğinin bilinmesi, onları önceden bulmak kadar önemlidir.

Verilerin Tutulması, Ortam Araçlarının İmha Edilmesi, Uygunluk Gereksinimleri

Günümüzdeki birçok yasa organizasyonların çeşitli verilerini güven altına almasını gerektirmektedir. Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (*Health Insurance Portability and Accountability Act* - HIPAA), veri güvenliğini gerektiren yasalardan birine örnektir. Bir diğer örnek

ise, Adil ve Doğru Kredi İşlem Kanunu'dur (*Fair and Accurate Credit Transactions Act* - FACTA). FACTA iş amaçlı müşteri verisi tutan herhangi bir varlığın o veriyi gözden çıkarmadan önce yok etmesini gerektirir.

Bunlar ve benzer kanunlar, düzgün güvenlik kontrolleriyle mahremiyet verilerinin korunumunu gerektirirler. Bu kanunlar, veriyi kullanmanın, saklamanın ve imha etmenin doğru yollarını ana hatları ile belirtirler. Bu kurallar ve düzenlemeler izlenmezse, izinsiz giren kişiler, örneğin hassas veriyi almak için çöplüklere dalabilirler.

Prosedürler

Organizasyonlar farklı seviyelerde kısıtlamalar ve bilgisayar ortamının farklı yerlerinde sağlanan erişim kontrolleri farklı çeşitlerde uygulayabilirler. Erişim denetimlerin bir kombinasyonu sisteme, katmanlı, derinliğine savunma (*defense-in-depth* - DiD) bir koruma sağlar. Bir DiD yaklaşımı atakların başarılı olmasını zorlaştırır çünkü saldırı yapan kişi birçok güvenlik denetimini açık etmek zorundadır. Katmanlı sistemde, bir güvenlik denetimini başarılı bir şekilde atlatan saldırgan birçok diğer denetimle karşı karşıya gelmelidir. Güvenlik personeli her kritik kaynağı birden çok denetimle koruduğuna emin olmalıdır. Tek denetimle bir kaynağı korumaya asla güvenmeyin.

Güvenlik Denetimleri

Bir **güvenlik denetimi** bir kaynak için olan bir riskten kaçınmak, riski durdurmak veya azaltma amacına sahip herhangi bir mekanizmadır. Birkaç tip güvenlik kontrolü vardır; bunlar amaçlarına göre farklı farklı çalışırlar. Birçok organizasyonun kaynaklarını korumak için güvenlik kontrollerinin çeşitli karışımlarına ihtiyacı vardır. TABLO 5-1'de güvenlik kontrollerinin en yaygın türleri listelenmiştir.

Ortam Araçlarının İmha Edilmesi Gereksinimleri

Güvenlik ilgisinin çoğu, aktif olan kaynakları korumaya odaklanmıştır. Birçok organizasyon verinin hala artık kullanılmayan ortam (*media*) araçlarında veya hatta çöpte olabileceği gerçeğini gözünden kaçırır. Hiçbir verinin, organizasyonun dışında, kullanılmayan ortam araçları içinde sızmayacağını garantilemek önemlidir. Ortam araçlarının imha edilmesi gereksinimleri, saldırganların dosyalara, hafızaya veya başka korunan veriye ellerini sürmesine engel olmalıdır. Birçok organizasyon, sadece orijinal veri hassas değil ise, ortam araçlarının tekrar kullanımına müsaade eder. Başka bir uç örnek ise, nükleer bir silahın planlarını içeren bir ortam aracının tekrar kullanıma uygun olmamasıdır. Eğer ortam aracını etkisiz hale getirmeden önce veriyi imha etmezseniz, yasayı çiğneyebilirsiniz.

> **NOT**
>
> Yok etme yöntemleri; CD'leri, sabit sürücüleri, USB sürücüleri, DVD'leri, kağıt belgeleri, flaş bellekleri ve diğer ortam aracı formlarını parçalama, yakma veya ufalamayı içerir.

Ortam aracını fiziksel olarak yok etmeniz her zaman gerekli değildir. Bir başka yöntem **mıknatıslık giderme bobini** (***degausser***) kullanmaktır. Bir mıknatıslık giderme bobini, manyetik depolama ortam aracındaki veriyi manyetik alan yaratarak siler. Veri, mıknatıslık giderme bobininden geçtiğinde veriyi tekrar oluşturmak için yeterli manyetik malzeme kalmaz. Eğer ortam aracındaki bilgi çok hassas değildiyse, herhangi bir ortam aracını başka verileri depolamak için kullanabilirsiniz. Ancak, eğer ortam aracında çok hassas veri varsa, yok edilmesi gerekmektedir.

Ortam aracına zarar vermeden veriyi yok etmenin başka bir metodu ise tekrarlı yazmaktır. Tekrarlı olarak rastgele karakterler verinin üzerine yazdırılınca, çoğunlukla veri yok olur. Bu yönteme **üzerine yazma** (***overwriting***) denir. Bu süreç eğer üzerine yazılacak veri azsa ve üzerine yazma da

TABLO 5-1 Güvenlik Denetim Türleri.

DENETİM TÜRÜ	AÇIKLAMA
Yönetimsel	Bunlar, yönetim tarafından onaylanan ve çalışanlara kural formunda iletilen politikalardır. Bunlar, kullanıcıları sorumlulukları hakkında bilgilendiren ilk savunma hattıdır. Örnekler parola uzunluğu hakkındaki politikaları içerir.
Mantıksal/Tekniksel	Bunlar otomatik olarak kontrol edilen ve uygulanan politikalardır. Bu, insan hatasını azaltır. Örneğin, bir bilgisayar parolaları kontrol ederek kurallara uyulduğundan emin olur.
Donanım	Bu, ağ cihazlarında Ortam Erişim Denetimi (*Media Access Control* - MAC) filtreleme, iki adımlı kimlik denetlemesi için akıllı kart kullanımı ve radyo frekansı tanımlama (*radio frequency identification* - RFID) etiketleri gibi güvenlik belirteçleri gibi kimlikleri kontrol eden ve doğrulayan ekipmanı içerir. Bu örnekte, MAC bir ağın her bir düğümünü benzersiz olarak tanımlayan bir donanım adresidir. Ortam Erişim Denetimi, daha sonra bölümün ilerleyen kısımlarında tartışılan zorunlu erişim denetimleri (*mandatory access controls*) ile aynı değildir.
Yazılım	Bu denetimler işletim sistemine ve uygulama yazılımlarına gömülüdür. Bunlar, Microsoft Windows'un standart NTFS izinlerini, oturum açma gerektiren kullanıcı hesaplarını ve servis veya protokol türlerini kısıtlayan kuralları içerir. Bu maddeler genelde ID ve doğrulama aşamasının parçalarıdır.
Fiziksel	Bunlar, güvenlik görevlileri, ID rozetleri, çitler ve kapı kilitleri gibi kaynaklara fiziksel erişimi engelleyen cihazlardır.

hızlıysa iyi çalışır. Fazla miktardaki veri veya yavaş yazan cihazlar bu tür bir veri yok edimini bir üretim ortamında kullanışlı olamayacak kadar yavaş yaparlar.

Erişim Denetimin Biçimsel Modelleri

Tekniksel denetimlerin en görünen türlerinin bazıları bilgisayar kaynaklarına erişimi koruyanlardır. Birçok kullanıcı erişim denetim kısıtlamalarıyla karşı karşıya gelmiştir. Örneğin, yanlış bir parola giren herhangi bir kullanıcının erişimi reddedilmiştir.

Farklı kaynaklara erişimi kısıtlamanın birçok yolu olduğu için, iyi erişim denetimler tasarlamak için modellerden yararlanmak faydalıdır. Aşağıdakileri de içeren çeşitli biçimsel (formel) erişim denetim modeli vardır:

- **İsteğe bağlı erişim denetim (*Discretionary access control* - DAC)**—DAC ile, kaynağın sahibi olan kimin içeri gireceğine ve kimin izinleri gerektiği gibi değiştireceğine karar verir. Sahip olan kişi başkalarına bu işi verebilir.
- **Zorunlu erişim denetim (*Mandatory Access control* - MAC)**—MAC ile, bir sisteme veya herhangi bir kaynağa erişim izni kaynağın hassasiyeti ve öznenin güvenlik seviyesi ile belirlenir. Başka birine verilemez. Bu MAC'i DAC'dan daha güçlü yapar.
- **İsteğe bağlı olmayan erişim denetim (*Nondiscretionary access control*)**—İsteğe bağlı olmayan erişim denetim, sistem yöneticisi tarafından değil, güvenlik yöneticisi tarafından yakından izlenir.
- **Kural tabanlı erişim denetim (*Rule-based access control*)**— Verinin sahibi tarafından korunan bir kurallar listesi, hangi kullanıcıların nesnelere erişimi olacağını belirler.

Diğer modeller Biba, Clark-Wilson ve Bell-La Padula tabanlıdır. Bu modeller gizlilik veya bütünlüğü korumak için erişim denetimlerin ve izinlerin kullanımını açıklar.

İsteğe Bağlı Erişim Denetim

Ortak Kriterler **isteğe bağlı erişim denetimini (*discretionary access control* - DAC)** aşağıdaki şekilde tanımlamaktadır:

> Öznelerin ve/veya bulundukları grupların kimliklerine dayalı olarak nesnelere erişimi kısıtlama yoludur. Denetimler belirli bir erişim iznine sahip olan öznenin başka bir özneye bu izni iletebilme yeteneğine (belki dolaylı yoldan) sahip olması şeklinde isteğe bağlıdır.

Ortak Kriterler aynı zamanda aşağıdakileri de belirtmektedir:

> Çok gizli veya hassas bilgileri işleyen sistemler için tanımlanan güvenlik politikaları, isteğe bağlı erişim denetim kurallarının uygulanması için koşulları içermelidir. Bu, onların denetime ve bilgiye ihtiyacı olduğu saptanan kişilerin erişimini kısıtlayan tutarlı kural topluluklarını içermesi anlamına gelmektedir.

Bu tanımlamalar hem kamu hem de özel sektördeki organizasyonların hassas bilgilerini işlemek için geçerlidir.

İşletim Sistemi-Tabanlı DAC

İşletim sistemlerinin öncelikle dosyalar, hafıza ve uygulamalar gibi sistem kaynaklarına erişimi denetleme sorumlulukları vardır. Güvenlik yöneticilerinin en temel işlerinden biri erişim denetimin sürekliliğini sağlamaktır. Erişim denetimler, sadece yetkili kullanıcıların kaynaklara erişebildiğini garantilediğinde etkilidirler. Erişim denetimler, kullanıcıların sadece ihtiyaçları olan kaynaklara ulaşabildiklerini garantilediklerinde etkindirler. Hem etkili hem de etkin erişim denetimler yaratmak zorlayıcı olabilir. Organizasyonlar ihtiyaçlarına göre erişim denetimleri nasıl tasarlayacaklarına ve sürekliliğini nasıl sağlayacaklarına karar vermelidirler. Aşağıda erişim denetim politikalarını geliştirirken kurumların nelere dikkat etmesi gerektiği hakkında birkaç nokta listelenmiştir:

- **Erişim denetim metotları**—Günümüzdeki işletim sistemleri bireysel kullanıcılar (kura tabanlı) ve/veya bir grup kullanıcı (rol-tabanlı) için erişim denetim ayarları içermektedir. Hangi metodu kullanacağınız organizasyonun boyutuna ve bireyler veya roller için gereken özel erişim haklarına göre değişmektedir.
- **Yeni kullanıcı kayıtlanması**—Yeni kullanıcılar bir organizasyona getirildiklerinde, onların kullanıcı hesapları yaratılmalıdır. Ancak bu işlem hızlı bir şekilde yapılmalıdır ki, yeni gelen kişiler işlerini yapabilsinler. Kullanıcı kayıtlanması standart haline getirilmiş, etkin ve kesin olmalıdır.
- **Periyodik inceleme**—Zamanla, kullanıcılar belirli projeleri bitirmek veya özel bir görevi yerine getirmek için genellikle özel izinler alırlar. Bu izinler zaman zaman incelenmeli ve gerekmediklerinde sonlandırılmalıdır. Bu inceleme, uygunluk (*compliance*) ve denetleme (*auditing*) problemlerini kişilerin sadece gereken alanlara erişmesini sağlayarak çözmektedir.

En Düşük Erişim Hakkının, Görevler Ayrılığının ve Bilinmesi Gerekenin Engellenmesi

En düşük erişim hakkı (*least privilege*) bir kullanıcıya görevlerini tamamlaması için minimum erişim izni vermektir. Başka bir ifadeyle, kullanıcılara işlerini yapmak için yeterli yetki verilmesi demektir, başka bir şey değil. En düşük erişim hakkının sürekliliğini sağlamak zordur ama veriyi gereğinden fazla yetkilendirmeden korumaktadır.

Görevler ayrılığı (*separation of duties*) bir görevi, toplam görevin sadece bir parçasını yürütmesine izin verilen farklı insanlar tarafından gerçekleştirilen özgün eylemlere bölme işidir. Bu prensip insanların kendi işlerini hem yaratıp hem de onaylamasını önler. Görevler ayrılığı, bir görevi tamamlamak için başka insanların iş birliğini gerektirerek dolandırıcılığı veya hataları önlemek için önemli bir araç olabilir. İkili kontrol görevler ayrılığı için önemli bir araç olabilir. Bir kapıdaki iki tane kombinasyonlu kilit veya bir kişinin yönetmesi için birbirinden çok uzak olan konsollardaki tuşların aynı anda dönmesini gerektiren bir füze kontrol sistemi buna örnek olarak verilebilir.

Bilinmesi gereken (*need to know*), insanların görevlerini yerine getirmeleri için ihtiyaç duymadıkları bilgiye erişmelerini engelleme kavramıdır. Bilinmesi gereken temelinde erişim sağlanması, verilerin uygunsuz bir şekilde ele geçirilmesi veya bilgilerin yanlış bir şekilde dağıtılması olasılığını azaltabilir.

En düşük erişim hakkı, görevler ayrılığı ve bilinmesi gereken aşağıdaki şekilde engellenebilir:

- **Gizli anlaşma (*Collusion*).** Kullanıcılar denetimlerden kaçınmak için birlikte çalışırlar **(gizlice anlaşırlar - *colluding*)** ve birbirlerine yetkilendirilmemiş görevlerin yerine getirilmesinde yardımcı olurlar. İş rotasyonu gizlice anlaşma riskini azaltmaktadır.
- **Gizli kanallar (*Covert channels*).** Bunlar bilgiyi organizasyon politikasına karşı gelerek gizli (*covert*) yollarla iletmektir. İki tane ana gizli kanal vardır; zamanlama (bir sistemden diğerine sinyal gönderme) ve depolama (veriyi korunmayan veya düzgün olmayan bir yerde depolama).

Uygulama Tabanlı DAC

Uygulama tabanlı DAC, bağlama (*context*) veya içeriğe (*content*) dayalı olarak erişimi reddeder. Uygulama sadece o anki kişi için yetkilendirilmiş seçenekleri gösterir. Örneğin, bir bankomat (*automatic teller machine* - ATM) menüsü belirli bir kullanıcıya sadece ona uygun olan seçenekleri göstererek erişimi kısıtlar. Güvenlik denetimlerini, kullanıcı bağlamı veya kaynak içeriği temelli bu tür DAC'ler kullanarak uygulayabilirsiniz:

Bilginize

Güvenli Bilgisayar Sistem Değerlendirme Kriterleri (*Trusted Computer System Evaluation Criteria* - TCSEC) hem DAC hem de MAC için tanımlamalar sağlar. Bu tanımlamalar, hassas bilgiyi koruma ihtiyacı olan hem kamu hem de özel sektör organizasyonlarının ihtiyaçlarına uygundur. TCSEC, Birleşmiş Devletler Savunma Bakanlığı'nın Rainbow Serileri'nde (*U.S. Department of Defense's Rainbow Series*) önemli bir standarttır. 1980'ler ve 1990'larda basılan Rainbow Serileri, bilgisayar güvenliği standartları ve kılavuzlarının bir koleksiyonudur. Serideki her kitabın kapağı farklı renkte olmasından dolayı her kitabın kısa ismi farklıdır. TCSEC turuncu bir kapağa sahipti ve genellikle *Turuncu Kitap (The Orange Book)* olarak bilinirdi. Ortak Kriterler 2005 senesinde *Turuncu Kitap'ın* yerine geçmiştir.

- Bağlam tabanlı bir sistemde erişim, kullanıcının kendi veri kayıtlarında tanımlı olan kullanıcı ayrıcalıklarına dayalıdır. Bu onay çoğunlukla belirli bir iş rolünde veya fonksiyonunda çalışan kişilere verilir.
- İçeriğe bağlı bir sistemde, bir tablodaki veri öğelerinin değeri veya hassaslığına bağlı olarak erişim verilir. Bu sistem erişilen verinin içeriğini kontrol eder ve örneğin, Bölüm A'nın müdürü Bölüm alanında sadece A olan çalışan kayıtlarını görebilir, ancak ilgili alanda başka bir değer varsa onlara ait kayıtları göremez.

İzin Seviyeleri

İzin seviyeleri (*permission levels*) bir öznenin bir sistemdeki, uygulamadaki, ağdaki veya diğer kaynaklardaki haklarını belirtir. Bir DAC ortamında, yetkilendirme sistemi herhangi bir öznenin hangi nesnelere ulaşabileceğini görmek için izin seviyelerini kullanır. İzin seviyeleri aşağıdakilerden herhangi biri olabilir:

- **Kullanıcı tabanlı**—Bir kullanıcıya atanan izinler genellikle o kullanıcıya özeldir. Bu durumda, kurallar kullanıcı ID'sine veya başka bir özgün tanımlayıcıya dayalı olarak belirlenir.
- **İş tabanlı, grup tabanlı veya rol tabanlı erişim denetim (*role-based access control* - RBAC)**—Aynı veya benzer iş rollerine sahip olan tüm insanlara ortak izin topluluklarına dayalı olarak izinler atanır.
- **Proje tabanlı**—Bir grup insan (örneğin, bir proje takımı) bir proje üzerinde çalıştıkları zaman, onlara o projeyle ilgili belgelere ve verilere erişim hakkı verilir.
- **Görev tabanlı**—Görev tabanlı erişim denetim, bir kişinin belirli fonksiyonları yürütmesini kısıtlar ve genellikle ortak bir kullanım hakkı verir. Bir diğer ifadeyle, eğer bir kişi bir görevin bir parçasını yürütecekse, o kişiye göreve bağlı olan diğer parçaları yürütme izni verilmeyebilir. Bu, görevler ayrılığı (separation of duties) ve bilinmesi gereken (need-to-know) kavramlarına dayalıdır.

Zorunlu Erişim Denetim

Zorunlu erişim denetim (*mandatory access control* - MAC), kaynaklara erişimi kısıtlamanın başka bir yöntemidir. Kısıtlama seviyesini o kaynağın ne kadar hassas olduğuna bağlı olarak belirlersiniz. Bu bir sınıflama etiketiyle (*classification label*) temsil edilir. Bireyler bundan sonra hassas bilgiye erişim için resmi olarak yetkilendirilmelidirler (örnek, izin (*clearance*) alma). Çok gizli (*classified*) bilgileri (veya diğer gizli bilgiler) işlemek için kullanılan sistemlerde tanımlanan güvenlik politikaları MAC kurallarını uygulatmak için koşullar içermelidir. MAC kuralları, kimin hangi bilgiye erişebileceğini denetleyen kurallar topluluğu içermelidir.

> **NOT**
>
> Unutmayın: Hassaslık etiketleri veya sınıflandırmalar bütün nesnelere (kaynaklara) uygulanır. Ayrıcalık yada izin seviyesi etiketleri bütün öznelere (kullanıcılar veya programlar) atanmıştır.

Zorunlu erişim denetimde, sistem ve sahip olan kişi erişime izin vermek için birlikte karar alırlar. Sahip olan kişi bilinmesi gereken (*need-to-know*) unsurunu verir. Ayrıcalığı veya hassas materyal için izin seviyesi olan bütün kullanıcıların bütün hassas bilgiye erişime ihtiyaçları yoktur. Sistem özne ve nesneyi bu bölümde daha sonra ele alınacak olan Bell-La Padula gizlilik modeline göre karşılaştırır. Bu karşılaştırmaya dayalı olarak, sistem erişime ya izin verir ya da erişimi reddeder.

Geçici ayırma (*temporal isolation*), erişimi belirli zamanlarla kısıtlar. İlk önce nesnelerin hassasiyet seviyesini sınıflamaktadır. Sonra, bu nesnelere sadece belirli zamanlarda erişim izni verir. Geçici ayrım genellikle rol tabanlı erişim denetimle birlikte kullanılır. Geçici ayrım, daha genel

olarak **günün belirli saati kısıtlamaları (*time-of-day restrictions*)** şeklinde açıklandığını görebilirsiniz. Kullanılan terim ne olursa olsun, ikisi de basitçe erişimi belirli zaman aralıklarında kısıtlamak anlamına gelmektedir.

İsteğe Bağlı Olmayan Erişim Denetim

İsteğe bağlı olmayan erişim denetimde (*nondiscretionary access control*), erişim kuralları güvenlik yöneticisi tarafından sıkı bir şekilde yönetilmektedir. Bu erişim kuralları, kendi dosyaları için sistem sahibi veya sıradan kullanıcılar tarafından yönetilmemektedir.

İsteğe bağlı olmayan erişim denetim birçok işletim sisteminde kullanılabilir. Bu strateji isteğe bağlı erişim denetimden daha güvenlidir. Sistem, kullanıcının organizasyon içi politikalar ile uygunluğuna güvenmez. Örneğin, kullanıcılar iyi tanımlanmış dosya koruma kurallarına uysalar bile, bir Truva atı programı korumayı denetimsiz erişime izin vermek üzere değiştirebilir. Bu tür bir açık verme durumu isteğe bağlı olmayan erişimde mümkün değildir.

Güvenlik yöneticilerinin, isteğe bağlı olmayan erişim denetimde, hassas dosyaların bütünlük için yazma-korumalı olduklarından ve gizliliği korumak için sadece yetkilendirilmiş kişiler tarafından okunabildiğinden emin olmak için yeterli kontrol gücü vardır. Bozulmuş bir programın kullanılması şansı azaltılmıştır çünkü, kullanıcılara sadece net bir şekilde izin verilmiş programları çalıştırma izni verilmiştir.

İsteğe bağlı olmayan erişim denetim, sistem güvenliğinin uygulandığından ve kurcalamaya dayanıklı (*tamperproof*) olunduğundan emin olmaya yardımcı olur. Eğer organizasyonunuz çok hassas bilgileri yönetmek istiyorsa, isteğe bağlı olmayan erişim denetim kullanmayı ciddi bir şekilde düşünmelisiniz. Gizliliği ve bütünlüğü korumada DAC'dan çok daha iyi bir iş yapmaktadır. Çoğu zaman kullanıcı olan verinin sahibi olan kişi erişim kararlarını veremez. Bu sizin fazladan bir yönetici yükü eklenmeden MAC'in bazı yararlarından faydalanmanıza izin verir.

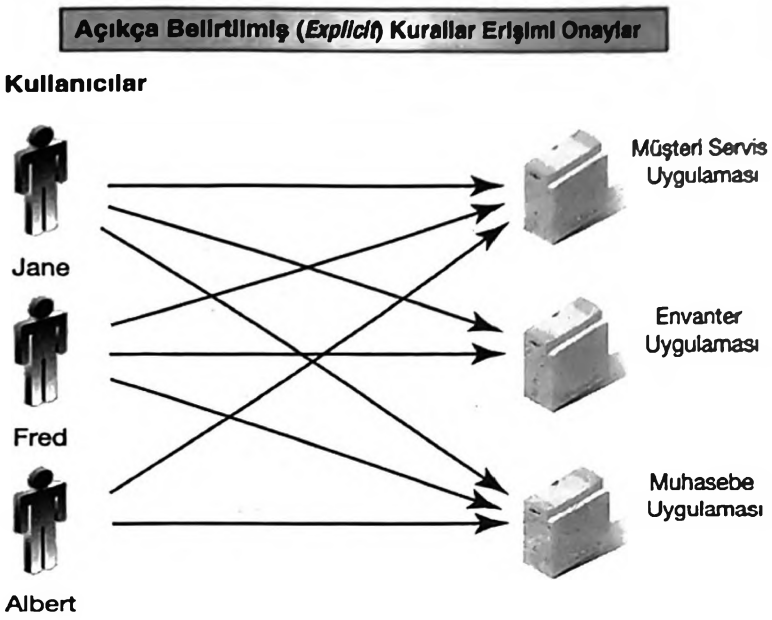
Kural Tabanlı Erişim Denetim

Kural tabanlı bir sistemde (*rule-based system*), erişim kime erişim verileceğine karar veren bir kural listesine dayalı olarak verilir. Verinin sahibi olan kişiler kuralları yaratırlar veya kurallara izin verirler. Kullanıcılara verilen okuma, yazma, yürütme gibi ayrıcalıkları belirtirler.

Kural tabanlı erişim denetimin (*rule-based access control*) başarısı verinin sahibi olan kişilere olan güvenin seviyesine dayalıdır. Bu tür bir erişim denetim, yönetimin çoğunu verinin sahibi olan kişiye verir. Teknik ve güvenliği düşünen kullanıcılar için bu tür erişim denetimler iyi çalışır. Çok kullanıcılı ya da gerekli teknik yeteneği ve eğitimi olmayan kullanıcıların olduğu ortamlarda o kadar iyi çalışmaz. **ŞEKİL 5-3** bireysel kuralların her kullanıcının izinlerini nasıl denetlediğini göstermektedir.

Erişim Denetim Listeleri

Birçok işletim sistemi listeleri veya izinleri nesnelerle ilişkilendirmek için birkaç seçenek sağlar. Bu listelere **erişim denetim listeleri (*access control lists* - ACL)** denir. Farklı işletim sistemleri farklı ACL-tabanlı (*ACL-enabling*) seçenekler sunar. Örneğin, Linux ve OSX okuma, yazma ve yürütme izinlerine sahiptir. Bunlar dosya sahiplerine, gruplara ve küresel kullanıcılara uygulanabilir. Windows hem paylaşma hem de güvenlik izinlerine sahiptir, ikisi de ACL'lere erişim kuralları



ŞEKİL 5-3
Kural tabanlı erişim denetim

tanımlama olanağı verir. Paylaşım izinleri, kaynaklara bir ağ paylaşımından erişmek için kullanılır. Güvenlik izinleri, kullanıcı yerel olarak oturum açtığında kaynaklara erişmek için kullanılır. Bazı Windows izinleri aşağıdakileri içerir:

- **Paylaşma izinleri**—Tam, değişim, okuma ve reddetme
- **Güvenlik izinleri**—Tam, düzenle (*modify*), dosya içeriklerini listele, okuma yürütme, okuma, yazma, özel ve reddetme

Hem paylaşma hem de güvenlik izinleri için reddetme diğer bütün izinleri geçersiz kılar (*override*). Ancak, eğer bir kaynak için herhangi bir ACL yoksa ne olur? Birçok yetkilendirme sistemi eğer izin verme kuralı yoksa, erişimi otomatik olarak reddet anlamına gelen *gizli engelleme (implicit deny)* kullanır. Bu yaklaşım daha kısıtlayıcıdır ama daha güvenlidir.

Çok sayıda seçeneği olduğu için Windows ACL'lerinin daha ince tanecikli (*fine-grained*) bir yapıya sahip olduğu söylenir çünkü daha yüksek bir seviyede denetime izin verir. ŞEKİL 5-4 bir ACL'i göstermektedir.

Rol-Tabanlı Erişim Denetim

Erişim denetim bir başka türü de **rol-tabanlı erişim denetimdir (*role-based access control* - RBAC)**. Bir RBAC politikası erişim denetim onaylarını kullanıcıya atanan işlere dayanarak yapar. Güvenlik yöneticisi her kullanıcıya bir veya daha fazla rol atar. Bazı işletim sistemleri roller yerine grupları kullanmaktadır. Kaynak sahibi olan kişi hangi kaynaklara hangi rollerin erişebileceğine karar verir. Microsoft Windows RBAC'i yönetmek için global grupları kullanır. ŞEKİL 5-5 RBAC'i göstermektedir.

Bir role erişim kurallarını atamadan önce, organizasyonunuzda rolleri tanımlamalı ve açıklamalısınız. Rolleri, onaylamaları (*approvals*), rol hiyerarşisini ve kısıtları (*constraints*) tanımlama sürecine **rol mühendisliği (*role engineering*)** denir. Organizasyonunuz için net bir rol açıklama listesiyle

ŞEKİL 5-4

Bir erişim denetim listesi

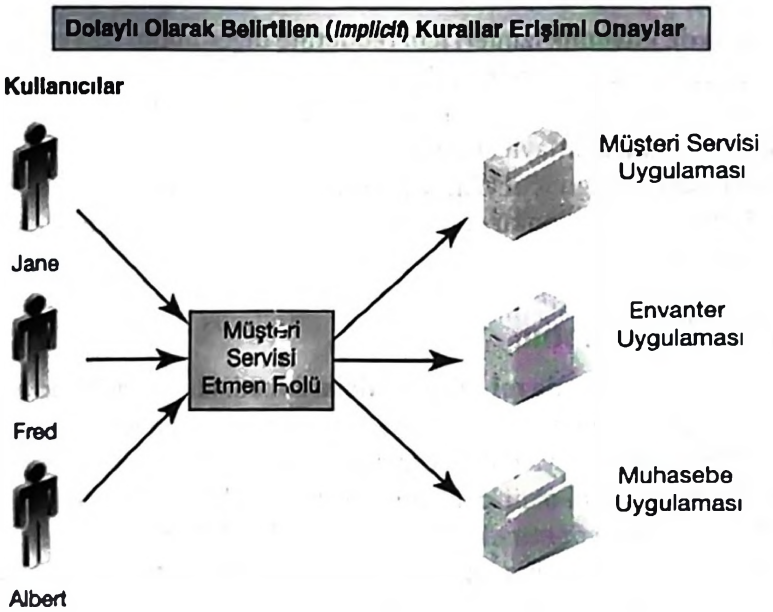
Hal	
Hal Kullanıcısının Dizini	Tam Kontrol
Kevin Kullanıcısın Dizini	Dizini Yazma
Kara Kullanıcısının Dizini	Erişim yok
Yazıcı 001	Yürütme
Kevin	
Hal Kullanıcısının Dizini	Yazma
Kevin Kullanıcısın Dizini	Tam Kontrol
Kara Kullanıcısının Dizini	Erişim yok
Yazıcı 001	Erişim yok
Kara	
Hal Kullanıcısının Dizini	Yazma
Kevin Kullanıcısın Dizini	Tam Kontrol
Kara Kullanıcısının Dizini	Erişim yok
Yazıcı 001	Yürütme
Yazıcı 002	Yürütme

başlamak RBAC'in anahtarıdır. RBAC'in diğer erişim denetim metotlarına göre asıl avantajı onun organizasyonun yapısını temsil etmesi ve organizasyon içinde kontrol politikaları ile uygunluğu zorlamasıdır.

ŞEKİL 5-5'teki Jane ve Fred'in Envanter uygulamasına erişimi olması ama Albert'in olmaması gerektiğini düşünün. Ancak, şekilde gösterildiği gibi Albert'in bu uygulamaya erişimi *vardır*; bir bilinmesi-gereken ihlali. Bu hata rollerin fazla genelleştirilmesinden dolayı olmuştur. Rollerin fazla genelleştirilmesi bireylere istenilenden fazla erişim verilmesine yol açabilir. Rolleri atarken,

ŞEKİL 5-5

Rol-tabanlı erişim denetim



bir kullanıcıya bir rol veya küçük bir grup kullanıcıya bir rol atamayı düşünün. Windows'un "izni reddet (*deny permission*)" seçeneği bir rolü etkisiz hale getirebilecek bir kural yaratmayı mümkün kılar. Bu Albert'in fazladan olan izin problemini çözer. Bu karar riske dayalıdır. Bir kullanıcıya idari giderleri düşürmek için benzer ayrıcalıklarda bir rol verilmiş ve kullanıcıya kullanıcının bilmesi gerekeninden fazla erişim izni verilmiş olabilir.

İçeriğe-Bağlı Erişim Denetim

ŞEKİL 5-6 içeriğe bağlı erişim denetimin (*content-dependent access control*) nasıl veriyi koruyabileceğini göstermektedir. İçeriğe bağlı erişim denetim veride ne olduğunu temel almaktadır. Veriye bakıp onu kimin görebileceğine karar veren erişim denetim mekanizması (işletim sisteminin değil uygulamanın bir parçası olan arabulucu program) gerektirir. Sonuç şu ana kadar gördüğünüz erişim denetimlerden daha iyi bir taneciklilikliktir (*granularity*). Erişim basitçe dosya seviyesinde değil, dosyadaki kayıt seviyesinde denetlenmektedir. Ancak, bunu yapmanın maliyeti daha fazladır çünkü bir arabulucu program gerektirir. Arabulucu program erişilen nesnedeki bilgiyi kullanır. Örneğin, kayıtta ne olduğu. Karar çoğunlukla, eğer/o zaman (*if-then*) sorusuna dönüşür. Örneğin, "Eğer güvenlik bayrağı evet ise, o zaman kullanıcının güvenlik seviyesini kontrol et." Yöneticilerin belirli çalışanlarla ilgili veri görüntülemek için maaş bordrosu veri tabanına erişmesi gerekebilir ama diğer yöneticilerin çalışanlarının verilerine erişimleri olmayabilir.

Kısıtlandırılmış Kullanıcı Ara Yüzü

Kısıtlandırılmış kullanıcı ara yüzü (*constrained user interface*) ile bir kullanıcının belirli sistem kaynaklarına girişi —veya ara yüz kurması— iki şey ile kısıtlanır: Kullanıcının hakları ve izinleri kısıtlıdır ve kısıtlar ara yüzü sağlayan cihaz veya programın içine konulmuştur. ATM veya kamu erişimli kiosk tarayıcısı kullanıcılarına sadece belirli fonksiyonlara, dosyalara veya diğer kaynaklara erişmesine müsaade eder. Yetkilendirilmemiş kaynaklara erişim isteği yeteneğini kısıtlayarak erişimlerini sınırlar. Örneğin, bazı sistemler erişime uygun olmayan simgeleri grileştirirler. Kullanıcıları kısıtlamanın çeşitli yöntemleri aşağıdaki gibidir:



ŞEKİL 5-6
İçeriğe bağlı erişim denetim.

- **Menüler**—Kullanıcıları bazı verilerden uzak tutmanın bir yolu onları o verinin olduğundan habersiz bırakmaktır. Kullanıcı oturum açtığında, menüsü kapanmış bölgeleri içermez.
- **Veri tabanı görünümleri**—**Görünüm tabanlı erişim denetim (*view-based access control* - **VBAC**)** olarak da bilinen bu yaklaşım, genellikle ilişkisel veri tabanlarında kullanılır. Veri tabanı sistemi her kullanıcı için o kişinin görebileceği veriyi limitleyen bir görüntü oluşturur. Günümüzdeki birçok veri tabanı, veri tabanlarını birkaç parçaya bölmek için yollar sağlamaktadır. Bu özellik **çok kiracılı (*multitenancy*)** olarak bilinir ve farklı kullanıcı gruplarının birbirlerinin verilerini görmeden veri tabanlarına erişmelerini sağlar. Bu yetenek, paylaşılan uygulama ve veri tabanlarında bulut kullanmak isteyen organizasyonlar için çok önemlidir.
- **Fiziksel olarak kısıtlanmış kullanıcı ara yüzleri**—Ara yüz mekanizması kullanıcıya sınırlı sayıda seçenek sunar. Örneğin, bir ATM'nin belirli bir sayıda basılacak tuşu vardır. Bu onu **fiziksel olarak kısıtlanmış bir kullanıcı ara yüzü (*physically constrained user interface*)** yapar.
- **Şifreleme**—Bu yaklaşım sistemde depolanan bilgiye erişmek veya bilgiyi okumak için deşifreleme anahtarı gerektirdiğinden kullanıcıları kısıtlar. Şifreleme aynı zamanda kullanıcıdan kredi kartı detayları gibi bilgileri saklar.

Diğer Erişim Denetim Modelleri

Diğer erişim denetim modelleri günümüzdeki erişim denetimleri şekillendirmeye yardımcı olmuştur. En başarılı erişim denetim modelleri arasında Bell-La Padula modeli, Biba bütünlük modeli, Clark ve Wilson bütünlük modeli ve Brewer ve Nash modeli bulunmaktadır. İlerleyen kısımlarda her bir modeli öğreneceksiniz.

Bell-La Padula Modeli

Bell-La Padula modeli verinin gizliliğine ve çok gizli bilgiye erişimin denetimine odaklanmıştır. Bu model bir sonraki kısımda anlatılacak olan ve verinin bütünlüğünü korumak için kuralları açıklayan Biba bütünlük modelinden farklıdır. Bell-La Padula modelinde sistem öznelere ve nesnelere ayrılmıştır ve sistemin o anki hali **durum (*state*)** olarak adlandırılmıştır. Model güvenli bir durumu açıklamaktadır. Model her durum değişiminin güvenliği korumasını, güvenli bir durumdan güvenli bir duruma geçmesiyle garantilemektedir. Bu süreç, modelin güvenlik görevlerini yerine getirdiğinden emin olmaktadır. Bell-La Padula modeli bilgisayar ağı sistemindeki izin verilebilir durumları özellik olarak alan durum makinesi kavramı üzerine kurulmuştur. Bir durumdan diğer bir duruma geçiş, **geçiş fonksiyonları (*transition functions*)** olarak tanımlanmıştır.

Biba Bütünlük Modeli

1977'de, Kenneth J. Biba bütünlük seviyelerine dayalı bilgisayar sistemlerinde bütünlüğe değinmek için ilk modeli tanımlamıştır. **Biba bütünlük modeli (*Biba integrity model*)** sadece verinin gizliliğine değinen Bell-La Padula modelindeki bir zayıflığı düzeltmiştir. Biba bütünlük modeli üç kısımdan oluşur:

- İlk kısım, bir öznenin kendinden daha düşük bir bütünlük seviyesine sahip olan bir nesneyi okuyamayacağını söyler. Verilen bütünlük seviyesindeki bir özne sadece aynı veya daha yüksek bütünlük seviyesindeki nesneleri okuyabilir. Bu basitçe **bütünlük aksiyomu (*integrity axiom*)** olarak bilinmektedir.

- İkinci kısım, bir öznenin kendisinden daha yüksek seviyedeki bir nesneyi değiştiremeyeceğini söyler.
- Üçüncü kısım, bir öznenin kendinden daha yüksek bütünlük seviyesi olan başka bir özneden servis isteyemeyeceğini söyler. Verilen bütünlük seviyesindeki bir özne, sadece kendi seviyesiyle aynı veya kendi seviyesinden daha düşük olan bir özneyi çağırabilir.

Clark ve Wilson Bütünlük Modeli

1987'de David Clark ve David Wilson tarafından yayımlanan **Clark ve Wilson bütünlük modeli** (***Clark and Wilson integrity model***), kullanıcılar sisteme alındıklarında ve kendilerinin izin verilmediği şeyleri yapmaya çalıştıklarında ne olduğuna odaklanır. Aynı zamanda, içerden gelen bütünlük tehditlerine de bakar. Bu iki bileşen Biba'nın modelinde eksikti. Bu model, yazılımın yapmaya tasarlandığı şeyi yapıp yapmadığına bakar. Bu büyük bir bütünlük sorunudur. Clark ve Wilson bütünlük modeli üç bütünlük sorununa değinir:

- Yetkilendirilmemiş kullanıcıların değişiklik yapmasını engeller (Biba sadece bu bütünlük hedefine değinmiştir).
- Yetkilendirilmiş kullanıcıların uygun olmayan değişiklikler yapmasını engeller.
- İçsel ve dışsal tutarlılığı korur.

Clark ve Wilson modeli veri üzerinde doğru biçimlendirilmiş (*well-formed*) işlemler ve kısıtlamalar tanımlar. Örneğin, bir ticari sistem yeni bir lüks araba satışı için sadece $40.000 fiyatının girilmesine izin vermelidir. Satışa $4.000 veya $400.000 girilmesi mümkün olmamalıdır. Bu içsel tutarlılığı korur. İçsel tutarlılık her zaman sistemin beklenildiği gibi çalıştığından emin olur.

> **NOT**
>
> Bu model bir ticari bütünlük modeli olarak bilinir. Askeri kullanım için kullanılan önceki modellerin aksine, bu model işletmeler için tasarlanmıştır.

Clark ve Wilson bütünlük modelinde öznenin erişimi, programı (doğru biçimlendirilmiş bir işlem) yürütme izni ile denetlenmektedir. Böylelikle, yetkisi olmayan kişiler programı yürütemez (ilk bütünlük kuralı). Yetkili kişiler her bir kişinin belirli, özgün değişiklikler yapmasını sağlayan farklı programlara erişebilirler (görevler ayrılığı). Bu modelin iki önemli parçası aşağıdaki gibidir:

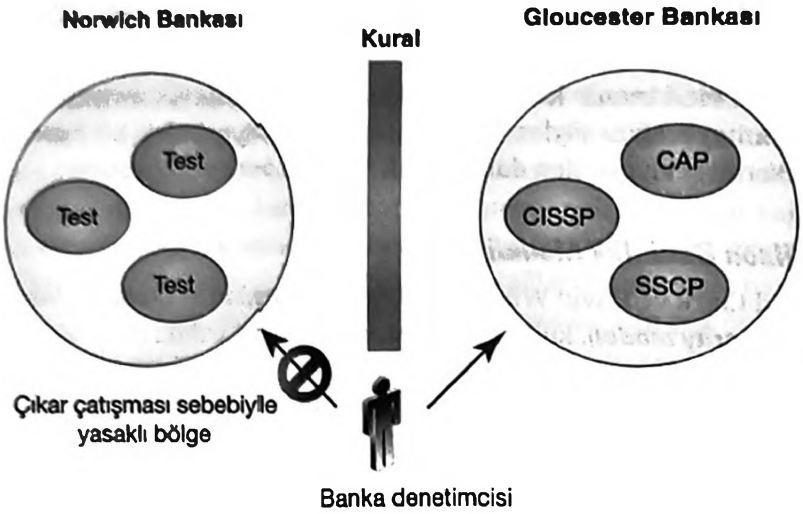
- Bu üç erişim varlığı —özne, program ve nesne— erişim üçlüsünü oluşturmak için bir araya gelirler.
- Bütünlük bağlama (binding) ile uygulatılır. Özneden programa ve programdan nesneye bağlamaları bütünlüğü uygulatır. Bu görevler ayrılığını yaratır. Bu durum, sadece yetkilendirilmiş işlemlerin gerçekleştirilebileceğinden emin olmayı sağlar.

Brewer ve Nash Bütünlük Modeli

Brewer ve Nash modeli (***Brewer and Nash integrity model***), adil yarışmayı garantilemek için, 1989'da yayımlanan matematiksel bir teoriye dayandırılmıştır. Dinamik olarak değişen erişim denetimleri uygulamak için kullanılmıştır. Rakip organizasyona ait olan aynı entegre veri tabanındaki nesnelerde kullanıcıların hileli değişiklik yapmadıklarından emin olmak için, rakip kişilerin verilerini birbirinden ayırabilir. Bu model, çıkar çatışmaları olduğunda, kullanıcıların veya müşterilerin veriyi kullanmasını engellemek için de kullanılır.

Çin Seddi (*Chinese Wall*) güvenlik politikası, bir duvarı veya bariyeri tanımlar ve hiçbir öznenin veya nesnenin duvarın diğer tarafına geçememesini sağlayan bir kural topluluğu geliştirir. **ŞEKİL 5-7** çalışan bir Çin Seddini göstermektedir. Şekil, bir denetleme firmasının rakip firmaların

ŞEKİL 5-7
Brewer ve Nash Bütünlük Modeli



NOT

Denetimler çıkar çatışmalarını engelleyemez. Çıkar çatışmaları verinin kendisine değil, bireylerin pozisyonlarına bağlıdır.

denetimlerini nasıl elden geçirdiğini göstermektedir. Bu örnekte, Gloucester Bankası'yla ilgili olan veri üzerinde çalışan bir denetimcinin, Norwich Bankası'ndaki herhangi bir veriye erişmesi yasaklanmıştır. Denetimci her iki banka için de denetleme yapan firmada çalışmasına rağmen, denetim firmasındaki içsel denetimler çıkar çatışması yaratabilecek iki bölge arasındaki erişimi engellemektedir.

Bu model, çıkar çatışmalarının tanındığından ve bu kişilerin erişmemeleri gereken veriden faydalanmalarını engellediğinden emin olmaktadır. Örneğin, eğer bir kullanıcıya bir firmanın verisi için izin verildiyse, o firmanın rakipleri olan firmaların verileri otomatik olarak yasaklı bölge olabilmelidir.

Erişim Denetimde İhlallerin Etkileri

Erişimi denetlemedeki başarısızlığınız rakiplerinize avantaj verebilir. Bu rakip askeri bir güç, rakip istihbarat ile ilgilenen bir firma hatta komşunuz bile olabilir. Aşağıdaki liste oluşabilecek bazı kayıpları listelemektedir:

- Özel bilginin açık edilmesi
- Verinin bozulması
- Firma istihbaratının kaybolması
- Tesislere, çalışan personele veya sistemlere verilebilecek zarar
- Ekipmana verilebilecek zarar
- Sistem ve iş süreçlerinin hata vermesi

Bütün ayrıcalıklı olayların (*incident*) etkisi aynı değildir. Bazılarını fark etmek diğerlerini fark etmekten daha kolaydır. Örneğin, ticari istihbarat da dahil olmak üzere ticari sırlarının açık edilmesine bağlı olan kayıplar, genellikle uzun bir süre fark edilmez. Verinin bozulması nedeni ile karşılaşılan kayıplar fark edildiği zaman, bir veri tabanını ve o veri tabanına ait bütün yedeklemeleri işe yaramaz bir duruma getirebilir. Verinin bozulması sistemlerde ve iş süreçlerinde kolayca hatalara neden olabilir.

Hizmet reddi (DoS) saldırılarının bazı türleri kısa ömürlüdür. Hızlıca bulunurlar ve ciddi bir hasara yol açmadan durdurulabilirler. DoS saldırılarının diğer türlerinin gelişmesi daha uzun sürer. Bir işletmenin müşterilerine hizmet etme yeteneklerini etkileyebilirler. Müşteriler işletmelerini başka bir yere taşıyabilirler. Bu tür DoS saldırıları bir organizasyona daha ciddi zararlar verir.

Erişim Denetimlere Yönelik Tehditler

Erişim denetimlerin zorlukları birçok biçimde olabilir. Bu liste asla tamamen bitmez. Her zaman yeni tehditler gelişir. Eşler arası/Uçtan uca (*peer-to-peer* - P2P) kullanıcılarının Belgelerim dizinini yanlışlıkla birbirleriyle paylaşmasıyla oluşan eşler arası riski buna bir örnektir. Bu durum, hassas belgeleri diğer kullanıcılara açık edebilir.

Erişim denetimler aşağıdakiler de dahil olmak üzere birçok durumda ihlal edilebilir:

- **Fiziksel erişim elde etme**—Eğer izinsiz giren kişinin fiziksel bir cihaza erişimi varsa, mantıksal erişim denetim basitçe anlamsız kalır. Veri, hak olmadan kopyalanabilir veya çalınabilir. Fiziksel erişime sahip olan biri, donanıma veya yazılıma tuş darbesi günlükçüleri (*keystroke loggers*) yükleyebilir veya donanıma zarar verebilir. Örneğin, bu kişi bir DoS atağı başlatabilir. CD'ler, DVD'ler, USB bellekler veya sabit sürücüler gibi küçük çıkarılabilir medya araçları fiziksel erişim riski yaratmaktadır. Bu cihazlardan birine veriyi kopyalamak kolaydır. Akıllı telefonlar ve mobil cihazlar başka bir ortak risktir. Günümüzün mobil cihazları arasında kameralar, ses ve görüntü kaydı yapabilen cihazlar bulunmaktadır.
- **Gözlemleme ile gizlice dinleme**—Bazen güvenlik personeli verinin görülmesine izin vererek en bariz güvenlik açığını gözden kaçırabilir. Yetkili bir kullanıcının masasındaki veya ekranındaki veriler casusluğa müsaittir. Doğru politikaları ve prosedürleri uygulatmak bu tür bir veri kaybına engel olabilir.
- **Güvenliği atlamak**—Veriye her türlü erişim güvenlik açığına neden olabilir. Geliştiriciler, örneğin bir web sitesi üzerinden erişim gibi sadece bir yöntem ile erişimi düşünebilirler. Ama saldırı yapan kişiler o yerdeki güvenliği kolayca atlatabilirler. Bilgi güvenliği takımı, bir sürücüyü eşleme (*mapping a drive*) veya sunucunun klavyesinden oturum açma gibi diğer yolları da göz önünde bulundurmalıdır.
- **Donanımı ve yazılımı kullanma**—Saldırı yapan kişiler genellikle kontrol ettikleri sisteme programlar yüklemeye çalışırlar. Bu programlara genelde **Truva Atları** (***Trojan horses***) denir. Ağ yöneticisi veya iş istasyonu sahibi, saldırı yapan kişinin orda olduğunu bile anlamayabilir.
- **Ortamları (media) tekrar kullanma veya kullanımdan çıkarma**—Saldırı yapan kişiler kullanımdan çıkarılmış veya tekrar kullanılmış ortamlardan silinmiş veya değiştirilmiş bilgiyi kurtarabilirler. Belgeleri parçalara ayırmak ve ortamları çöpe atmaktansa fiziksel olarak yok etmek daha güvenli ve daha ucuzdur.
- **Elektronik olarak gizlice dinleme**—Saldırı yapan kişiler, ağ kabloları hattına girerek (*wiretapping*) gizlice dinleyebilir. Bazı ortamlar diğerlerine göre gizlice dinlemeye karşı daha dayanıklıdır. Örneğin, fiber optik kablo bakır kablodan daha güvenlidir. Ancak, hiçbir ortam tam bir koruma sağlamaz. Mobil cihazlara ve kablosuz erişim noktalarına olan ilginin artması gizlice dinleme riskinin de artmasına yol açmıştır. Güvensiz erişim noktalarına mobil cihazlarını bağlayan kullanıcılar saldırı yapan kişiler için kolay hedeflerdir.
- **İletişimi kesme**—Gizlice dinlemenin başka bir çeşidi ise veri iletişimlerinin fiziksel olarak arasına girmektir. Buna **koklama** (***sniffing***) denir. Koklama ile, saldırı yapan kişiler

ağ trafiğini akarken yakalarlar. Koklama genelde, **ortadaki-adam (man-in-the-middle)** saldırısında kullanılır. Saldırı yapan kişi kendini iki kurban arasına koyar ve iki kişi arasındaki mesajları alır ve aktarır. Saldırı yapan kişi iki kurbanın birbiriyle güvenli bir bağlantı üzerinden konuşuyormuş hissi verecek bir durum yaratır. Gerçekte ise, saldırı yapan kişi bütün konuşmanın kontrolüne sahiptir.

- **Ağlara erişmek**—Ağlar genelde korunmasız bağlantılara sahiptir. Birçok organizasyon ağlarını ihtiyaçları olduğundan daha fazla ağ girişi/bağlantı noktası (*drop* - duvarlardaki dişi bağlantılar) ile kurarlar. Bu gelecekteki büyüme durumunda daha fazla kullanıcı ekleyebilmelerini sağlar. Bu kullanılmayan bağlantı noktaları genelde aktif bağlantılardır. Saldırganlar, bu bağlantıları ağ erişimi elde etmek için kullanabilirler. Organizasyonlar kablosuz erişim noktaları ekledikçe ağ erişim riskleri artar. Ağ erişimini kolay yapmak yasal kullanıcılara fayda sağladığı gibi, saldırı yapan kişilere de fayda sağlar. Organizasyonlar bütün ağ erişim noktalarını dikkatlice izlemeli ve kısıtlamalıdır.
- **Uygulamaları kullanma**—Birçok program ve modülde ortak olarak bir programlama zayıflığı olarak bilinen **arabellek taşması (*buffer overflow*)** zayıflığı vardır. Bu saldırı yapan kişinin girdi alanına beklenenden çok karakter girip zararlı koda bütün uygulamada izin vermesiyle oluşur. Uygulamalardaki zayıflıkları açık etmenin başka birçok yolu vardır ve saldırı yapan kişiler uygulamaları açık etmek için her zaman yeni yolların arayışı içerisindedirler.

Erişim Denetimin İhlallerinin Etkileri

Saldırı yapan kişilerin erişim denetimleri açık etmek için kullandıkları bazı yolları gördünüz. Ama saldırı yapan kişi başarılı olursa ne olur? Erişim denetimin ihlalinin etkileri nelerdir? Erişim denetim ihlalinin bir organizasyon üzerinde yaratabileceği zararlı etkiler aşağıdakilerdir:

- Müşteri güveninin kaybı
- İş fırsatlarının kaybı
- Organizasyona dayatılan yeni mevzuatlar ve düzenlemeler
- Kötü reklam
- Daha fazla dikkatsizlik
- Finansal cezalar

NOT

Bilgilendirme yasalarının eyalet bazında bir özetini aşağıdaki URL'de bulabilirsiniz: www.ncsl.org/research/ telecommunications-and-informationtechnology/ security-breach-notificationlaws. aspx.

Örneğin, Egghead Yazılım 2000 yılının yazında, gönüllü olarak bir ihlali bildirmişlerdir ve bu bildirinin olduğu bir sene içinde Amazon'a satılmıştır. İhlalden sonra, müşteriler firmaya kredi kartlarını verme konusunda güvenmemişlerdir. Egghead'in ürünlerini satın almada tereddüt etmişlerdir. Firmalar dünyası bunu dikkate almıştır. Sonuç olarak, diğer firmalar ihlalleri bildirmeyi bırakmışlardır. Sonunda, devlet, firmaları finansal veri erişim ihlallerini açıklamak zorunda bırakacak yeni yasalarla duruma el atmıştır.

Kaliforniya 2003 yılında, Kaliforniya'da iş yapan veya bu eyalette oturan kişilerle iş yapan firmaları etkileyen zorunlu bir açıklama yasasını yürürlüğe koymuştur. Yasa, bu eyalette yaşayan kişileri **kişisel kimlik tanımlama bilgilerinin (*personally identifiable information* - PII)** açıklanmasından korur. PII genellikle kötü kişilerin kimlik çalmak için kullandığı bilgilerdir. Bununla birlikte, bu yasanın fikri mülkiyet hırsızlığı gibi diğer

izinsiz girişleri kapsamadığını unutmayın. Ama yeni yasalar ihlalleri durdurmadı. Veri ihlali hala oluyor ve bunlardan bazıları haberlerde manşet oluyor. Son zamanlarda en çok haber niteliği taşıyan veri ihlalleri arasında Target, Home Depot, Blue Cross Blue Shield, Harvard Üniversitesi, Birleşik Devletler Ordusu Ulusal Muhafızı (*U.S. Army National Guard*) ve Birleşik Devletler Personel Yönetim Ofisi (*U.S. Office of Personnel Management*) gibi yerlerde gerçekleşen veri ihlalleri bulunmaktadır. Erişim ihlalleri problemi birçok organizasyonu etkilemektedir.

Kimlik Bilgileri ve İzinlerin Yönetimi

Erişim denetimi hakkında öğrendikçe, büyük bir olasılıkla erişim denetim kararları için gereken tüm bilgileri nasıl saklamak gerektiğini düşündünüz. Kullanıcılara kayıt olma, geçerli kimlik ve kimlik denetimi bilgilerini sağlama için izin vermelisiniz. Daha sonra, erişim izinlerini tanımlamanız, izinleri kullanıcılarla ilişkilendirmeniz ve bakım için izin vermeniz gerekir. Aslında, tüm bu görevler **kimlik bilgisi yönetiminin (*credential management*)** bir parçasıdır. Kimlik yönetim sistemleri, erişim kontrolü ile ilişkili bilgileri toplama, yönetme ve kullanma becerisi sağlar. Ancak kimlik bilgilerini yönetmek sadece ilk adımdır. Ayrıca izinleri ve erişim kurallarını yönetmek de gereklidir. Microsoft, yöneticilerin erişim denetimlerini yönetmesine yardımcı olmak için **Grup Politikası (*Group Policy*)** adı verilen bir özellik sunmaktadır. Bir **Grup Politikası Nesnesi (*Group Policy Object* - GPO)**, bir grup bilgisayara verimli bir şekilde uygulanabilen kullanıcılar veya bilgisayarlar için bir ayar topluluğudur. GPO'nun özellikleri, Windows yöneticilerinin pek çok kullanıcı veya bilgisayara kolayca uygulanabilen ayarları tek bir yerde tanımlamasına olanak tanımaktadır.

Merkezi ve Merkezi Olmayan Erişim Denetim

Merkezi erişim denetim, bir ortak varlığın –bir birey, departman veya cihaz gibi—sistemlere veya ağa kimin girebileceğine karar verdiği bir erişim kontrolü yaklaşımıdır. Erişim denetimler, yerel seviyeden ziyade merkezi olarak yönetilir. Sahipler hangi kullanıcıların hangi nesnelere ulaşabileceğine karar verir. Merkezi yönetim, sahiplerinin direktiflerini destekler. Merkezi kimlik doğrulama hizmetleri **kimlik denetleme, yetkilendirme ve izleme (*authentication, authorization, and accounting* - AAA)** sunucuları kullanılarak uygulanmakta ve uygulatılmaktadır.

> **NOT**
> Merkezi erişim denetiminin yönetilmesi genellikle daha basittir, ancak dezavantajı ise, eğer başarısız olursa, çok sayıda kullanıcının etkilenecek olması ve bilgisayar sistemine giremeyecek olmasıdır.

AAA sunucularını kullanmanın yararları aşağıdakileri içermektedir:

- Kullanıcı hesapları tek bir ana bilgisayarda tutulduğu için daha az yönetim süresi gerektirir.
- Tasarım hatalarını azaltır çünkü farklı erişim cihazları benzer formatlar kullanır.
- Güvenlik yöneticisi eğitimini kolaylaştırır, çünkü sadece bir sistem öğrenilir.
- Tüm erişim talepleri tek bir sistem tarafından ele alındığından uygunluk denetimlerini iyileştirir ve kolaylaştırır.
- Yardım masası çağrılarını azaltır çünkü kullanıcı arayüzü tutarlıdır.

AAA Sunucularının Türleri

İlerleyen kısımlarda, AAA sunucularının önde gelen türlerini göreceksiniz: En bilineni RADIUS olmak üzere, TACACS+, DIAMETER ve SAML'dır.

RADIUS

Uzaktan Aramalı Kullanıcı Kimlik Denetleme Hizmeti (*Remote Authentication Dial-In User Service* - RADIUS) en popüler AAA hizmetidir. İki yapılandırma dosyası kullanan bir kimlik denetleme sunucusudur:

- İstemci adresini ve işlem kimlik denetlemesi için paylaşılan gizliyi içeren bir istemci yapılandırma dosyası
- Kullanıcı kimliği ve kimlik denetleme verilerinin yanı sıra bağlantı ve yetkilendirme bilgisini içeren bir kullanıcı yapılandırma dosyası

RADIUS kimlik denetleme sürecinde aşağıdaki adımları izler:

1. Ağ erişim sunucusu (*network access server* - NAS), kullanıcının UDP erişim isteğini deşifreler.
2. NAS kaynağın kimliğini doğrular.
3. NAS kullanıcı dosyasına karşı isteği doğrular.
4. NAS, erişime izin vererek ya da erişimi reddederek veya daha fazla bilgi isteyerek cevap verir.

TACACS+

Terminal Erişim Denetleyici Erişim Denetim Sistemi+ (*Terminal Access Controller Access Control System Plus* - TACACS+), tek bir yapılandırma dosyası kullanan bir İnternet Mühendisliği Görev Gücü (*Internet Engineering Task Force* - IETF) standardıdır:

- Sunucu işlemlerini denetlemek
- Kullanıcıları ve özellik/değer eşlerini tanımlamak
- Kimlik denetleme ve yetkilendirme prosedürlerini denetlemek

TACACS+, başlangıçta açık bir standart olarak yayınlanmadan önce Cisco Systems tarafından geliştirilmiştir. Cisco, daha önce orijinal **Terminal Erişim Denetleyici Erişim Denetim Sistemi (*Terminal Access Controller Access Control System* - TACSCS)** protokolünü kendi tescilli versiyonu olan **Genişletilmiş Terminal Erişim Denetleyici Erişim Denetim Sistemini (*Extended Terminal Access Controller Access Control System - XTACACS*)** geliştirmek için genişletmişti. TACACS+, XTACACS'ın bir sonraki adımıydı. Seçenekler (*Options*) bölümü, işlem ayarlarını, paylaşılan gizli anahtarı ve izleme (*accounting*) dosya adını içerir. TACACS +, kimlik denetleme işleminde şu adımları izler:

1. İstemci, TCP kullanarak, başlığı açık metin halinde ve kullanıcı ID'si, parola ve paylaşılan anahtarı içeren gövdeyi şifrelenmiş halde olmak üzere bir servis isteği gönderir.
2. Cevap, gerektiğinde bağlantı yapılandırması için bir izin/red ile birlikte özellik/değer çiftlerini içerir.

DIAMETER

DIAMETER (kısaltma değildir) RADIUS tabanlıdır. Ancak, RADIUS sadece çok akıcı veya mobil iş gücü içinde çalışır. DIAMETER bu şekilde kısıtlanmamıştır. Sabit veya statik bir iş gücü içinde de gayet iyi çalışır. DIAMETER aşağıdakilerden oluşur:

- **Temel protokol**—Temel protokol bütün uzantılar tarafından kullanılan mesaj formatını, aktarımı, hata raporlamasını ve güvenliği tanımlar.
- **Uzantılar**—Uzantılar (*extensions*) kimlik denetlemenin, yetkilendirmenin veya izleme işlemlerinin belirli türlerini yürütür.

DIAMETER aynı zamanda **Kullanıcı Veri Bloğu İletişim Kuralı (*User Datagram Protocol* - UDP)** kullanır. UDP kullanan bilgisayar uygulamaları, İnternet Protokolü (Internet Protocol - IP) ağındaki diğer ana bilgisayarlara **veri bloğu (*datagram*)** olarak bilinen mesajları gönderir. UDP bunu özel iletişim kanallarına veya veri yollarına ihtiyaç duymadan yapar. Bu nedenle, UDP'nin servisi güvenilir değildir çünkü veri blokları sırası bozularak varabilirler. Ayrıca çoğaltılabilirler ya da eksik olabilirler. UDP, bu sorunları düzeltmek için yalnızca uygulamalara güvenir. Bu, UDP'ye bu sorunları kendi kendine çözerek harcayacağı değerli zamanı ve değerli kaynakları kazandırır. Bu, UDP'yi daha hızlı hale getirir, bu nedenle UDP genellikle akış ortamı (*streaming media*) ve çevrimiçi oyunlar için kullanılır.

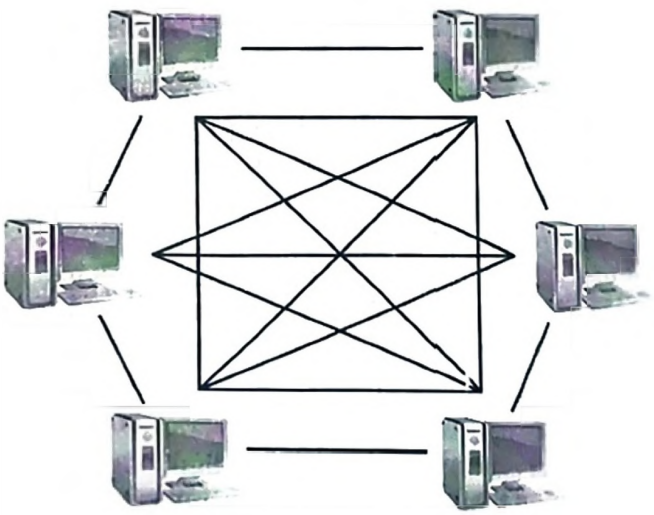
DIAMETER, UDP'yi istemci/sunucu modunda kullanmak yerine P2P modunda kullanır. Bir P2P modunda, bir kullanıcı başka bir kullanıcıya sabit sürücüsüne direk erişim izni verir. Erişim izni veren kullanıcının da diğer kullanıcının sabit sürücüsüne erişim izni vardır. Merkezi bir yapı yoktur. **ŞEKİL 5-8** P2P modunda bağlanmış bilgisayarların örneğini göstermektedir.

Bir istemci/sunucu modunda, yapı merkezileştirilmiştir. Bir istemci (bir kullanıcı) belirli bir bilgiye erişim istek etmek için bir sunucuya bağlanır. ŞEKİL 5-9 istemci/sunucu modunda bağlanmış bilgisayarların örneğini göstermektedir.

Bu, sunucuların istekleri başlatmasına ve iletim hatalarını yerel olarak ele almasına olanak tanır, bu da bir veri paketinin bir ağ bağlantısında hareket etmesi için gereken süreyi (gecikme) kısaltır ve performansı artırır. Kullanıcı istek komutunu, oturum ID'sini ve kullanıcının kullanıcı ID'si ve parolasını içeren bir yetkilendirme isteği gönderir. Bu yetkilendirme isteği bir ağa bağlı depolama (*network-attached storage* - NAS) cihazına gönderilir. NAS, kullanıcının kimlik bilgilerini onaylar. Eğer onaylanırsa, NAS cevap paketi gönderir. Cevap paketi, istenen hizmet için özellik/değer çiftlerini içerir. Oturum ID'si özgün olarak bağlantıyı tanımlar ve yüksek yoğunluklu kurulumlarda yinelenen bağlantı tanımlayıcıları ile RADIUS sorununu çözümler.

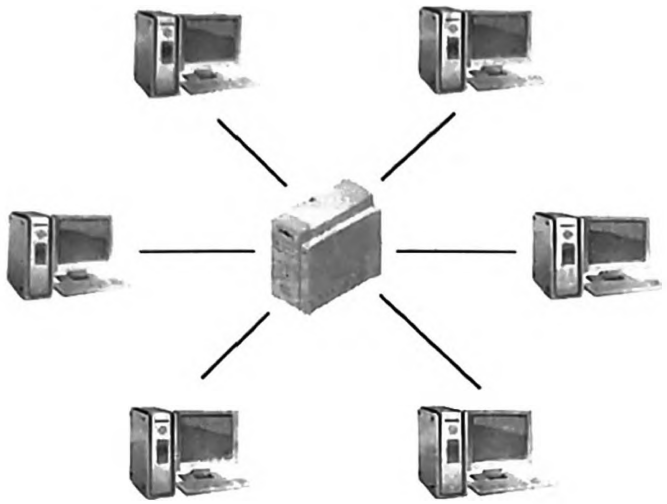
SAML

Güvenlik Bildirim Biçimlendirme Dili (*Security Assertion Markup Language* - SAML) hem kimlik denetleme hem de yetkilendirme verilerinin değiştirilmesi için kullanılan açık bir standarttır. SAML, XML tabanlıdır ve dağıtık sistemlerde erişim denetim ihtiyaçlarını desteklemek için tasarlanmıştır. SAML, genellikle web uygulaması erişim denetiminde kullanılmaktadır. SAML, tam bir merkezi AAA sistemi değildir. Bir veri formatı belirtimidir. SAML'ı bu bölüme dahil ettik, çünkü SAML kullanan sistemler güvenlik belirteçlerinin (*token*) dağıtımı için güvenilen merkezi bir otoriteye dayanır.



ŞEKİL 5-8
P2P modu.

ŞEKİL 5-9
İstemci/sunucu modu



Merkezi Olmayan Erişim Denetim

Başka bir erişim denetim yaklaşımı ise erişim denetim kararlarını ve yönetimi yerel olarak elden geçirmektir. Bu yaklaşım **merkezi olmayan/dağıtık erişim denetim (*decentralized access control*)** olarak bilinmektedir. Bu, örneğin sistem kullanıcılarına en yakın olan departman yöneticileri gibi, erişim denetimin insanların elinde olduğu anlamına gelir. Erişim istekleri bir merkezi varlık tarafından işlenmemektedir.

Bir yandan, merkezi olmayan erişim denetim genellikle kafa karışıklığına neden olur. Neden? Çünkü bu, standartlaştırmanın kaybedilmesine ve üst üste binen haklara (*overlapping rights*) yol açabilir. Bu erişim denetim tasarımında boşluklara neden olabilir. Bir diğer yandan, merkezi olmayan bir yaklaşım tek arıza noktası (*single point of failure*) problemini giderir. Merkezi denetim yapan gövdenin yerel durumlara etkili olarak cevap verememesi algısını ortadan kaldırır.

Merkezi olmayan erişim denetimin en yaygın iki örneği açık metin halinde kullanıcı adı ve parola kullanan **Parola Doğrulama Protokolü (*Password Authentication Protocol* - PAP)** ve **Meydan Okuma–El Sıkışma Kimlik Denetleme Protokolü (*Challenge-Handshake Authentication Protocol* - CHAP)**'dür. CHAP, PAP'tan daha güvenlidir çünkü gizlice dinleme tabanlı yeniden gönderme saldırılarının üstesinden gelmek için parolayı tek kullanımlık bir kimlik numarası ile özetler (*hash*). Akıllı telefonların ve tabletlerin sayısındaki patlama devam ettikçe, güvenli erişim sağlama ihtiyacı da artmaktadır. Mobil cihazlar için erişim denetimler gelişmektedir. Mobil kullanım için tasarlanmış nispeten iki yeni yaklaşım vardır. **Açık Kimlik Denetleme için Girişim (*Initiative for Open Authentication* - OATH)**, güçlü kimlik denetlemesi için bir referans mimarisi geliştirmek için devam eden bir girişimdir. OATH projesine 30'un üzerinde kuruluş katkıda bulunmaktadır. OATH, mobil cihaz kimlik denetlemesini desteklemek için çeşitli standartlar geliştirmiştir. Birincisi, **HMAC-tabanlı tek kullanımlık parola (*HMAC-based one-time password* - HOTP)** algoritmasıdır. HOTP, bir kimlik denetleme sunucusu kullanarak bir kullanıcının kimliğini denetlemek için çok güvenli bir yöntem sağlar. **Zaman tabanlı tek kullanımlık parola (*time-based one-time password* - TOTP)** algoritması HOTP'ye bir örnektir. Yeniden gönderme saldırılarına (*replay attacks*) karşı olan güvenlik açığını azaltmak için bir zaman damgasını bir özetlenmiş (hashed) değer ile birleştirir. OATH, hem merkezi hem de merkezi olmayan/dağıtık erişim denetim modellerini destekleyen bir referans çerçevesi önermektedir.

Mahremiyet

En görünür güvenlik endişelerinden biri **mahremiyet (*privacy*)** ile ilgili olanlardır. Kimlik hırsızlığı ve mahremiyeti korumanın önemine olan bilincin artması, mahremiyeti garanti altına almak

için yeni yasalarla ve standartlarla sonuçlandı. Kişisel mahremiyet, büyüyen bu sorunun sadece bir parçasıdır. Organizasyonlar mahremiyet ihlallerinin tehlikelerine karşı daha da bilinçlenmeye başlamışlardır. Organizasyonlar, aşağıda belirtilenler nedeni ile endişe duyduklarından, genellikle çalışanlarını elektronik olarak izlerler:

- Taciz davalarındaki yükümlülük
- Çalışan hırsızlığından dolayı oluşan çok büyük kayıplar
- Çalışanların işle alakalı olmayan başka şeylerle uğraşmasından dolayı oluşan verimlilik düşüşü

Elektronik izleme, iş yerinde kendi mahremiyet sorunlarını yaratır. Ülkeye veya yargılanma bölgesine bağlı olarak çalışanları izlemenin yasal seviyeleri büyük ölçüde değişebilir.

Mevcut düşünce, çalışanların makul bir mahremiyet beklentisine sahip olmaları için iki şeyi belirlemeleri gerektiğidir:

- Kişisel bir mahremiyet beklentisi olmalıdır.
- Bu kişisel mahremiyet beklentisi mantıklı olmalıdır.

İki maddeden biri eksikse, korunan bir çıkar oluşturulamaz. Bu, eğer bir çalışan e-posta mesajı gibi bir şeyin özel olduğu ile ilgili bir beklentiye girdiyse, bu kişinin iş vereninin yasal olarak bu mahremiyeti ihlal edemeyeceği anlamına gelir. Bununla birlikte, firma çalışanlarını firma ağı üzerinden gönderilen e-postaların takip edildiği ile ilgili bilgilendirirse, o zaman çalışan bundan sonra mahremiyet beklentisi içerisinde olduğunu iddia edemez. Başka bir deyişle, firma siber sahipliğini (*cyberdominion*) belirttikten sonra, çalışanların orada mahremiyet hakkı kalmaz.

Şirketler, çalışanların yapabilecekleri için neyin kabul edilebilir olduğu ve nelerin izlenildiği ile ilgili politikalarını açık bir şekilde bildirmelidir. Birçok durumda, çalışanlar kurumsal sistemleri kullanırken *herhangi bir* mahremiyet bekleyemezler. Bir kuruluşun kabul edilebilir kullanım politikası (*acceptable use policy* - AUP), diğer şeylerin yanı sıra mahremiyet için uygun beklentileri belirleyen önemli bir belgedir.

Oturum açma ekranları sistemlerin ve cihazların kullanıcılarına yasal haklarını bildiren mesajlardır. Bunlar sistemlerinizde ve cihazlarınızda kullanılmalıdır. Oturum açma ekranları aşağıdakileri kazanmak için kullanılır:

- Çalışanın izlenmek için rızası
- Hesabın kötüye kullanımı durumunda oluşabilecek potansiyel disiplin işlemleriyle ilgili çalışanın farkındalığı
- Depolanan dosyaların ve kayıtların geri erişimi için çalışanın rızası

Oturum açma ekranları kurumsal sistemleri kullanan çalışanların herhangi bir mahremiyet beklentisini yasal olarak ortadan kaldırmak için kullanılmaktadır.

İş Yerinde İzleme

2007'de Amerikan Yönetim Derneği (*American Management Association* - AMA) tarafından yapılan "Elektronik İzleme ve Gözetleme (*Electronic Monitoring & Surveillance*)" başlıklı bir araştırma "Kuruluşların %73'ünün e-postaları otomatik olarak izlemek için teknolojik araçlar kullandığını ve işverenlerin %40'ının e-postaları manuel olarak okumak ve değerlendirmek için bir bireyi atadıklarını" bulmuştur. Buna ek olarak, "%66'sı internet bağlantılarını [izliyor]", "şirketlerin %65'inin uygun olmayan web sitelerine olan bağlantıları engellemek için yazılım kullanıyor."

İş yerinde izleme aşağıdakileri içerir, ancak bunlarla sınırlı değildir:

- Posta veya e-posta açma
- Otomasyon yazılımı ile e-postaları kontrol etme

NOT

Politikalar tek başına yeterli değildir. İş verenler çalışanlarına ne yapabileceklerini ve yapamayacaklarını açıkça anlatmalıdır. Bunu yapmanın en iyi yolu eğitimdir. Sistemler veya politikalar değiştiğinde, bu değişiklikler çalışanlara anlatılmalıdır.

- Telefon günlüklerini kontrol etme veya telefon konuşmalarını kaydetme
- Ziyaret edilen web sitelerini kontrol etme
- Kredi kayıt bürolarından bilgi alma
- Satış noktası (*point-of-sale* - PoS) terminalleri ile bilgi toplama
- Kapalı devre televizyonlar ile (*closed-circuit televisions* - CCTV) eylemleri kaydetme

İş verenler, çalışanlarının yaptıkları işin miktarını ve kalitesini kontrol etmek için çalışanlarını izlemektedir. İş verenler genellikle çalışanlarının eylemlerinden sorumludur, bu nedenle çalışanlarının düzgün davrandıklarından emin olmaları gerekir.

Personelin izlemeyi anladığından emin olmak için, bir işveren açık bir davranış kuralına veya politikasına sahip olmalıdır. Çalışanlar politikayı izlemedikleri takdirde, kendilerine karşı cezai işlem uygulanabileceğini bilmelidirler.

Bulut Bilişim

Kuruluş gelişimindeki en güçlü trendlerden biri, paylaşılan hizmetleri bilişim ortamlarına dahil etmektir. **Bulut bilişim (*cloud computing*)**, bir ağ üzerinden iletilen bilişim hizmetlerini kullanma uygulamasıdır. Bilişim servisleri kuruluşun ağında veya başka bir ağa ait olan sunucuların sağladığı yerlerde konumlanmış olabilir. Farklı kullanıcı ortamlarının ihtiyaçlarını karşılamak için çeşitli bulut modelleri vardır. Bulut hizmetleri genellikle aşağıdaki kategorilerden birine girer:

- **Özel bulut (*Private cloud*)**—Ağın altyapısı dahil olmak üzere, hizmetleri sağlamak için gereken bütün donanım ve yazılım sadece tek bir kuruluş için işletilmektedir. Bileşenler kuruluş veya bir üçüncü parti sağlayıcı tarafından yönetilebilir. Asıl altyapı kuruluşun ağında veya bu ağın dışında olabilir.
- **Topluluk bulutu (*Community cloud*)**—Bu tür altyapı çeşitli kuruluşlara hizmet vermektedir. Farklı kuruluşlar bulut ortamını paylaşır ve özel ihtiyaçları için kullanır. Altyapı, katılımcı kuruluşlardan biri veya üçüncü bir parti tarafından yönetilebilir.
- **Genel bulut (*Public cloud*)**—Bu tür bulut altyapısı ilgisiz kuruluşlar veya bireyler tarafından kullanılabilir. Genel bulutlar genel kullanıma açıktır ve bir üçüncü parti sağlayıcı tarafından yönetilmektedir.
- **Hibrit bulut (*Hybrid cloud*)** — Bu tür bulut altyapısı, özel, topluluk ve genel bulutları içeren, birden fazla türde bulutun bileşenlerini içerir. Hibrit bulutlar daha kısıtlayıcı ortamların

Bilginize

Bulut bilişim yeni güvenlik endişeleri ortaya çıkarmıştır. Ödeme Kartları Endüstrisi Veri Güvenliği Standardı (*Payment Card Industry Data Security Standard* - PCI DSS) bulut güvenliği endişelerini doğrudan ele alan bir belge yayınlar. Bu belge genel olarak bulut bilişim ve bulut güvenlik endişeleri için iyi bir kaynaktır. Bu belgeyi https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf adresinde bulabilirsiniz.

sınırlarını genişletmek için yararlıdır. Genellikle, iş yükünü çeşitli altyapı veya bölümler arasında dağıtarak esneklik ve yük dengelemesi sağlamak için kullanılırlar.

En genel durumda, bir **bulut servis sağlayıcısı (*cloud service provider* - CSP)**, raflarca sunucu bilgisayarıyla birçok veri merkezinin sürekliliğini sağlar. Her sunucu birden fazla sanal makine çalıştırır ve aynı anda birçok istemciye hizmet sağlayabilir. CSP'ler müşterilerine internet üzerinden farklı hizmetler sunar. Ortak bulut hizmetleri aşağıdakileri içerir:

- **Hizmet olarak Altyapı (*Infrastructure as a Service* - IaaS)** —IaaS, kullanıcılara fiziksel veya sanal bir makineye erişim sağlar. Kullanıcılar kendi işletim sistemlerini seçmeli ve yüklemelidir. Daha sonra, makinenin bütün parçalarını sanki bir yerel bilgisayarmış gibi yönetebilirler.
- **Hizmet olarak Platform (*Platform as a Service* - PaaS)** —PaaS, kullanıcıya, bir dizi popüler işletim sisteminden herhangi birini çalıştıran fiziksel veya sanal bir makineye erişim sağlar. PaaS ile, IaaS'den farklı olarak, CSP işletim sistemini ve arkadaki donanımı yönetir. Yerel bir sunucuya bağlanmak yerine, kullanıcı buluttaki sanal bir sunucuya bağlanır. Bağlantı kurulduktan sonra, kullanıcı bulut oluşumuna diğer herhangi bir bilgisayar gibi davranır. Kullanıcı, sunucu sanki yerel veri merkezindeymiş gibi sunucuya yazılım yükleyebilir ve çalıştırabilir.

Hizmet olarak Yazılım (*Software as a Service* - SaaS) –SaaS modelinde, kullanıcılar bulut istemcilerinden yazılıma erişir. En temel bulut istemcisi web tarayıcısıdır. Kullanıcıların herhangi bir yazılımı yüklemesine veya yönetmesine gerek yoktur. Tek yapmaları gereken, doğru sunucuya bağlanmak ve yazılımı sanki kendi yerel ağlarında çalıştırıyormuş gibi kullanmaktır. SaaS'ın bazı popüler örnek arasında Google Apps™, Microsoft Ofis 365™ ve Salesforce® bulunmaktadır.

Geleneksel kurum içi yazılımlara göre bulut hizmetlerini kullanmanın birçok avantajı vardır. Bu avantajların birçoğu maliyet tasarruflarını içerir. Bu avantajlar aşağıdakileri içerir:

- **Bir veri merkezinin sürekliliğini sağlamaya gerek kalmaz**—CSP bir çok veri merkezinin sürekliliğini sağlar ve internette herhangi bir yerde sunulan hizmetlerin kullanılabilirliğinin tüm lojistiklerini ve detaylarını idare eder.
- **Bir felaketten kurtarma sitesinin sürekliliğini sağlamaya gerek kalmaz**—CSP zaten birden fazla sitede hizmetlerin ve verinin sürekliliğini sağladığından, bulutta verinin çok sayıda kopyası her zaman bulunmaktadır.
- **Performans ve bağlanabilirlik sorumluğu için dış kaynaktan sağlanan sorumluluk**—Bütün müşterilerin yapması gereken tek şey internete erişimlerinin olmasıdır. CSP, her şeyin sözleşmelerinde söz verildiği şekilde çalıştığından emin olmaktan sorumludur.
- **İsteğe bağlı konfigürasyon**— Bulut müşterileri, güncel ihtiyaçlara göre satın aldıkları bilişim gücünü ve depolama alanını artırabilir ve azaltabilir. Bu durum, kuruluşları kullanılmayan donanımın sürekliliğini sağlamak zorunda bırakmayarak, kuruluşların önemli miktarda paradan tasarruf etmelerini sağlar. Bu aynı zamanda, kuruluşların artan isteklere yeni sunucular satın almak ve onları kurmak zorunda kalmadan cevap verebileceği anlamına da geliyor.

Bulut bilişim kendi dezavantajlarına da sahiptir. Örneğin, hizmetleri kuruluşun dışına taşımak bütün ortamı kontrol etmeyi zorlaştırır. Bulut dezavantajları aşağıdakileri içerir:

- **Mahrem veriyi gizli tutmada daha büyük zorluk**—Bulutta depolanan veri (hem yetkilendirilmiş kullanıcılara hem de saldırganlara) daha erişilebilirdir. Bulut ortamları aslında

güvenilmezdir. Verinin sahibi olan kişiler, erişim denetimlerin verilerini korumak için yeterli olduğundan emin olmak için ek önlemler almalıdır.

- **Gizli verinin sızması için daha büyük tehlike**—Bulut bilişimin avantajlarından biri, CSP'nin verinizin her zaman kullanılabilir olmasını sağlamasıdır. Bunu yapmasının bir yolu, verinin güncel birçok kopyasını farklı konumlarda tutmasıdır. Gizli verinin her bir ek kopyası, verinin yetkilendirilmemiş kullanıcılara sızması olasılığını arttırmaktadır.
- **Sürekli ağ erişimi için daha fazla istek**—Bulut hizmetlerine erişim, bu hizmetlere olan ağ bağlantısına bağlıdır. Bu, güvenilir veya hızlı internet erişimine sahip olmayan bir kullanıcının bulut hizmetleriyle ilgili zorluklarla karşılaşabileceği anlamına gelir. Bu endişe en fazla, güvenilir kapsama alanının içinde veya dışında gezinen mobil kullanıcıları veya güvenilir internet erişimi olmayan kullanıcılar içindir.
- **Müşterilerin dış sağlayıcılara güvenme ihtiyacının artması**— Bir CSP'ye gizli verileri yayınlamak, bu sağlayıcıya bir miktar güven gerektirir. Üçüncü bir partiye hassas veriler için güvenmek bazı yasaları, düzenlemeleri veya sağlayıcı gereksinimlerini ihlal edebilir. Veriyi bir buluta taşımadan önce, dış gereksinimlerden kaynaklanan bütün kısıtlamaları dikkatlice incelemelisiniz. En güvenli politika, bulutu güvenilmeyen bir ortam olarak ele almak olsa da, CSP'nizle bazı temel düzeyde güvene sahip olmanız gerekir.

Kuruluşların bugün karşılaştığı en zor sorunlardan biri, gizli verileri bulutta güvende tutmaktır. Temel zorluk, verilerin kuruluşun altyapısındaki güvenilir bir konumdan güvenilmeyen bir bulut ortamına taşınmasıdır. Kullanıcılar bulut hizmetlerine bağlanabileceğinden, soru şudur, kimliklendirme, yetkilendirme ve kimlik denetlemesinden kim sorumlu olmalıdır? **Bulut Güvenliği Birliği (Cloud Security Alliance - CSA)**, bulut bilişimini güvenli bir şekilde kullanmak için en iyi uygulamaları desteklemek misyonuna sahip bir sivil toplum kuruluşudur. CSA, bulut güvenliği hakkında *Bulut Bilişimde Kritik Odak Noktaları için Güvenlik Rehberi (Security Guidance for Critical Areas of Focus in Cloud Computing)* adında bir rehber yayınladı. Rapor bulut bilişimdeki zorlukları şu şekilde tanımlıyor:

> Bulut bilişim çağında bilgi yönetimi tüm kurumları etkileyen zorlu bir sorundur; hatta görünürde aktif olarak bulut tabanlı projelerde çalışmayanlar için bile. İçsel veriyi ve bulut geçişlerini (*cloud migration*) yönetmekle başlar, veriyi dağılmış, organizasyonlar arası uygulamalarda ve hizmetlerde güven altına almaya kadar uzar. Bulut çağında bilgi yönetimi ve veri güvenliği, hem yeni stratejileri hem de yeni teknik mimarileri gerektirir.

NOT

CSA bulut bilişim güvenliği konularını öğrenmek için değerli bir kaynaktır. CSA web sitesi *https://cloudsecurityalliance.org* adresinde yer almaktadır. Bulut Bilişimde Kritik Odak Noktaları için Güvenlik Rehberi *(Security Guidance for Critical Areas of Focus in Cloud Computing)* raporunun en son versiyonunu *https://cloudsecurityalliance.org/group/security-guidance/* adresinden indirebilirsiniz.

Bulut ortamlarında erişim denetimi yönetme problemine kolay bir çözüm yoktur. Araştırmacılar, kurumlar üzerindeki yükü hafifletmek için yeni yollar araştırıyorlar. Bugün en iyi yaklaşımlar, bu bölümde öğrendiğiniz mevcut kavramları genişletmektir. Erişim denetimlerin bazılarının bulut ortamlarında var olması muhtemeldir. En önemli kural, her zaman bir derinliğine savunma (*defense-in-depth*) stratejisi kullanmaktır. Herhangi bir kaynağı korumak için asla tek bir denetime güvenmeyin.

BÖLÜM ÖZETİ

Bu bölümde, erişim denetimlerinin belirli kaynaklara erişime izin verme veya erişimi engelleme yolları olduğunu öğrendiniz. Kuruluşlar, personelin yapabileceklerini ve yapamayacaklarını yönetmek için erişim kontrollerini kullanır. Erişim denetimler, kullanıcıların kim olduklarını, ne yapabileceklerini, hangi kaynaklara erişebileceklerini ve hangi işlemleri yapabileceklerini belirler. Erişim denetim sistemleri parolalar, donanım belirteçleri, biyometrikler ve sertifikalar dahil olmak üzere çeşitli teknolojileri kullanır. Erişim, binalar veya odalar gibi fiziksel varlıklara verilebilir. Erişim aynı zamanda bilgi sistemlerine de verilebilir.

Erişim denetiminin dört parçasının kimlik tanımlama, yetkilendirme, kimlik denetleme, ve izlenebilirlik olduğunu öğrendiniz. Bu dört parça, iki aşamaya ayrılabilen bir erişim denetim süreci yaratmaktadır: Politika tanımlama aşaması ve politika yürütme aşaması. Erişim için kimin yetkilendirileceğine ve bu kişilerin hangi sistemleri ya da kaynakları kullanmalarına izin verileceğine öncelikle nasıl karar vermeniz gerektiğini öğrendiniz. Daha sonra, ilk aşamada tanımlanan yetkilendirmelere dayanarak erişimin nasıl verildiğini veya verilmediğini öğrendiniz. Ayrıca, erişim denetiminin formel modellerini, erişim denetim metodolojilerini ve zorluklarını ve erişim denetim ihlallerinin etkilerini öğrendiniz.

ANAHTAR KAVRAMLAR VE TERİMLER

Access control – Erişim denetim
Access control list (ACL) - Erişim denetim listesi (ACL)
Access control policy - Erişim denetim politikası
Accountability - İzlenebilirlik
Accounting -İzleme
Actions - Eylemler
Asynchronous token - Asenkron belirteç
Audit – Denetleme
Authentication – Kimlik denetleme
Authentication, authorization, and accounting (AAA) – Kimlik denetleme, yetkilendirme ve izleme
Authority-level policy - Yetki seviyesi politikası
Authorization - Yetkilendirme
Bell-La Padula model - Bell-La Padula modeli
Biba integrity model - Biba bütünlük modeli
Biometrics - Biometrikler
Brewer and Nash integrity model - Brewer ve Nash bütünlük modeli
Brute-force attack – Kaba-kuvvet saldırısı
Buffer overflow – Arabellek taşması
Challenge-Handshake Authentication Protocol (CHAP) - Meydan Okuma–El Sıkışma Kimlik Denetleme Protokolü (CHAP)
Characteristic - Karakteristik
Clark and Wilson integrity model - Clark ve Wilson bütünlük modeli
Cloud computing - Bulut bilişim
Cloud Security Alliance (CSA) - Bulut Güvenliği Birliği (CSA)
Cloud service provider (CSP) - Bulut Servis Sağlayıcısı (CSP)
Colluding - Gizlice anlaşmak
Collusion - Gizli anlaşma
Common Criteria for Information Technology Security Evaluation (Common Criteria) - Bilgi Teknolojileri Güvenlik Değerlendirmesi için Ortak Kriterler (Ortak Kriterler)
Constrained user interface - Kısıtlandırılmış kullanıcı ara yüzü
Continuous authentication – Sürekli kimlik denetleme
Covert channels - Gizli kanallar
Credential management - Kimlik bilgisi yönetimi
Crossover error rate (CER) – Çapraz hata oranı (CER)
Datagrams – Veri bloğu
Decentralized access control - Merkezi olmayan/dağıtık erişim denetim
Degausser - Mıknatıslık giderme bobini
DIAMETER - DIAMETER
Dictionary attack - Sözlük saldırısı
Discretionary access control (DAC) - İsteğe bağlı erişim denetim (DAC)
Event-based synchronization system - Olay tabanlı senkronizasyon sistemi
Federation - Birlik
Group membership policy - Grup üyeliği politikası
Group Policy - Grup Politikası
Group Policy Object (GPO) - Grup Politikası Nesnesi (GPO)
HMAC-based one-time password (HOTP) - HMAC tabanlı tek kullanımlık parola (HOTP)
Identification – Kimlik tanımlama
Initiative for Open Authentication (OATH) - Açık Kimlik Denetleme için Girişim (OATH)

ANAHTAR KAVRAMLAR VE TERİMLER, *devam*

Key distribution center (KDC) - Anahtar dağıtım merkezi (KDC)
Knowledge - Bilgi
Least privilege – En düşük erişim hakkı
Lightweight Directory Access Protocol (LDAP) - Hafifletilmiş Dizin Erişim Protokolü (LDAP)
Log files - Günlük dosyaları
Logical access control - Mantıksal erişim denetim
Man-in-the-middle (MITM) - Ortadaki adam saldırısı (MITM)
Mandatory access control (MAC) - Zorunlu erişim denetim (MAC)
Multitenancy – Çok kiracılı
Need to know – Bilinmesi gereken
Overwriting - Üstüne yazma
Ownership - Sahiplik
Passphrase – Passphrase/Uzun parola
Password Authentication Protocol (PAP) – Parola Doğrulama Protokolü (PAP)
Personal identification numbers (PINs) - Kişisel kimlik numaraları (PINler)
Physical access control - Fiziksel erişim denetim
Physically constrained user interface - Fiziksel olarak kısıtlandırılmış kullanıcı ara yüzü
Privacy - Mahremiyet
Public key infrastructure (PKI) - Açık anahtar altyapısı (PKI)
Rainbow tables – Rainbow tabloları
Reference monitör - Referans monitörü
Relationships - İlişkiler
Remote Authentication Dial-In User Service (RADIUS) - Uzaktan Aramalı Kullanıcı Kimlik Denetleme Hizmeti (RADIUS)
Resources - Kaynaklar
Role-based access control (RBAC) - Rol tabanlı erişim denetim (RBAC)
Secure European System for Applications in a Multi- Vendor Environment (SESAME) - Çok-Sağlayıcılı Bir Ortamdaki Uygulamalar için Güvenli Avrupa Sistemi (SESAME)
Secure LDAP - Güvenli LDAP
Security Assertion Markup Language (SAML) - Güvenlik Bildirim Biçimlendirme Dili (SAML)
Security control - Güvenlik denetimi
Security kernel - Güvenlik çekirdeği
Security kernel database - Güvenlik çekirdeği veri tabanı
Separation of duties - Görevler ayrılığı
Single sign-on (SSO) - Tek Oturum Açma (SSO)
Single-factor authentication - Tek faktörlü kimlik denetleme
Smart card - Akıllı kart
Sniffing - Koklama
State - Durum
Synchronous token - Senkronize belirteç
Temporal isolation - Geçici ayırma
Terminal Access Controller Access System (TACACS)- Terminal Erişim Denetleyici Erişim Sistemi (TACACS)
Terminal Access Controller Access System Plus (TACACS+) - Terminal Erişim Denetleyici Erişim Sistemi Artı (TACACS+)
Threshold - Eşik
Time-based one-time password (TOTP) - Zaman tabanlı tek kullanımlık parola (TOTP)
Time-based synchronization System - Zaman tabanlı senkronizasyon sistemi
Time of day restrictions - Günün belirli saati kısıtlamaları
Transition functions - Geçiş fonksiyonları
Transitive trust – Geçişli güven
Trojan horses - Truva atları
Trusted Operating Systems (TOS) - Güvenilir İşletim Sistemleri (TOS)
Two-factor authentication - İki faktörlü kimlik denetleme
USB token - USB belirteci
User assigned privileges - Kullanıcıya atanmış ayrıcalıklar
User Datagram Protocol (UDP) - Kullanıcı Veri Bloğu İletişim Kuralı
Username - Kullanıcı adı
View-based access control (VBAC) - Görünüm tabanlı erişim denetim (VBAC)
XTACACS (Extended Terminal Access Controller Access System) - Genişletilmiş Terminal Erişim Denetleyici Erişim Denetim Sistemi (XTACACS)

BÖLÜM 5 DEĞERLENDİRME

1. Erişim denetimler belirli öğelere erişimi denetlemek için kullanılan politikalar ya da prosedürlerdir.
   A. Doğru
   B. Yanlış

2. Aşağıdaki cevaplardan hangisi erişim denetimin yetkilendirme bileşenini en iyi açıklamaktadır?
   A. Yetkilendirme, öznenin bir sisteme erişim isteği için kullandığı yöntemdir.
   B. Yetkilendirme, bir kuruluş denetlendiğinde uygun bilginin kullanılabilirliğinden emin olmak için gereken politikaları ve prosedürleri yaratma ve sürekliliğini sağlama sürecidir.
   C. Yetkilendirme, erişim isteğinde bulunan öznenin, erişim verilen özneyle aynı olduğunu doğrulama veya ispatlamadır.
   D. Yetkilendirme, erişim için kimin onaylandığının ve hangi kaynaklar için onaylandıklarının belirlenmesi sürecidir.

3. Aşağıdakilerden hangisi erişim denetimin kimlik tanımlama bileşenini en iyi açıklamaktadır?
   A. Kimlik tanımlama, erişim isteğinde bulunan öznenin, erişim verilen özneyle aynı olduğunu doğrulama veya ispatlamadır.
   B. Kimlik tanımlama, öznenin bir sisteme erişim isteğinde bulunmak için kullandığı yöntemdir.
   C. Kimlik tanımlama, erişim için kimin onaylandığının ve hangi kaynaklar için onaylandıklarının belirlenmesi sürecidir.
   D. Kimlik tanımlama, bir kuruluş denetlendiğinde uygun bilginin kullanılabilirliğinden emin olmak için gereken politikaları ve prosedürleri yaratma ve sürekliliğini sağlama sürecidir.

4. Aşağıdakilerden hangisi erişim denetimin kimlik denetleme bileşenini en iyi açıklamaktadır?
   A. Kimlik denetleme, erişim isteğinde bulunan öznenin, erişim verilen özneyle aynı olduğunu doğrulama veya ispatlamadır.
   B. Kimlik denetleme, bir kuruluş denetlendiğinde uygun bilginin kullanılabilirliğinden emin olmak için gereken politikaları ve prosedürleri yaratma ve sürekliliğini sağlama sürecidir.
   C. Kimlik denetleme, erişim için kimin onaylandığının ve hangi kaynaklar için onaylandıklarının belirlenmesi sürecidir.
   D. Kimlik denetleme, öznenin bir sisteme erişim isteğinde bulunmak için kullandığı yöntemdir.

5. Aşağıdakilerden hangisi erişim denetimin izlenebilirlik bileşenini en iyi açıklamaktadır?
   A. İzlenebilirlik, erişim isteğinde bulunan öznenin, erişim verilen özneyle aynı olduğunu doğrulama veya ispatlamadır.
   B. İzlenebilirlik, öznenin bir sisteme erişim isteğinde bulunmak için kullandığı yöntemdir.
   C. İzlenebilirlik, bir kuruluş denetlendiğinde uygun bilginin kullanılabilirliğinden emin olmak için gereken politikaları ve prosedürleri yaratma ve sürekliliğini sağlama sürecidir.
   D. İzlenebilirlik, erişim için kimin onaylandığının ve hangi kaynaklar için onaylandıklarının belirlenmesi sürecidir.

6. Fiziksel erişim denetimler binalar veya kapılı otoparklar gibi kaynaklara fiziksel erişimi engeller.
   A. Doğru
   B. Yanlış

7. Bir ağda oturum açtığınızda, önünüze kullanıcı adı, parola, belirteç, akıllı kart veya biometriklerin bir kombinasyonu sunulur. Daha sonra, sistem tarafından yetkilendirilirsiniz veya erişiminiz reddedilir. Bu bir _____ örneğidir.
   A. Fiziksel erişim denetim
   B. Mantıksal erişim denetim
   C. Grup üyelik politikası
   D. Biba bütünlük modeli
   E. Hiçbiri

8. Erişim denetimler birçok biçimde, kısıtlama seviyesinde veya bilişim ortamı içerisinde farklı seviyelerde gerçekleştirilemez.
   A. Doğru
   B. Yanlış

9. Aşağıdakilerden hangisi erişim denetimin formel bir modeli için bir örnektir?
   A. İsteğe bağlı erişim denetim (DAC)
   B. Zorunlu erişim denetim (MAC)
   C. İsteğe bağlı olmayan erişim denetim
   D. Clark ve Wilson bütünlük modeli
   E. Hepsi

10. Fiziksel erişim, güvenliği atlatmak ve gizlice dinlemek erişim denetimlerin nasıl _____ olabileceğinin örnekleridir.
   A. Çalınmış
   B. İhlal edilmiş
   C. Denetlenmiş
   D. Yetkilendirilmiş

11. Erişim denetimlerin zorlukları aşağıdakilerin hangisini/hangilerini içermektedir?
   A. Dizüstü bilgisayar kaybı
   B. Donanımın kullanımı
   C. Gizlice dinleme
   D. Uygulamaların kullanımı
   E. Hepsi

12. Bir kaynağın sahibi olan kişi, ihtiyaç duyulduğunda erişimleri belirlediği ve izinleri değiştirdiğinde, bu durum _____ olarak bilinir.
    A. Zorunlu erişim denetim (MAC)
    B. İsteğe bağlı erişim denetim (DAC)
    C. İsteğe bağlı olmayan erişim denetim
    D. İçeriğe bağlı erişim denetim
    E. Rol tabanlı erişim denetim

13. Bir sistemde güvenlik açıklarını tanımlama, belirleme ve önceliklendirme sürecine _____ denir.
    A. Güvenlik açığı politikası
    B. Güvenlik açığı önleme
    C. Güvenlik açığı yetkilendirmesi
    D. Güvenlik açığı değerlendirmesi

14. Güvenlik çekirdeği, bilgisayar sistemlerinin erişim denetimini yerine getirir.
    A. Doğru
    B. Yanlış

15. Konu mahremiyete gelince, kuruluşlar aşağıdakilerden hangisi hakkında endişe duyarlar?
    A. Taciz davalarındaki yükümlülük
    B. Çalışan hırsızlığından dolayı oluşan çok büyük kayıplar
    C. Çalışanların çevrimiçi olarak alışveriş yapması ya da iş ile ilgili olmayan görevlerle uğraşmasından dolayı oluşan verimlilik düşüşü
    D. Hepsi

BÖLÜM

6

Güvenlik Operasyonları ve Yönetimi

Güvenlik uzmanları güvenlik operasyonlarının ve yönetiminin sıkı bir güvenlik programının temelini yaratmadaki rolünü anlamalıdırlar. Bir güvenlik uzmanı olarak rolünüz bir koçun rolüne benzer. Varlıklarınızın ya da "oyuncularınızın" güçlü ve zayıf yönlerinin tespit edilmesinde personeliniz ile birlikte çalışırsınız. Hedefiniz oyunu kazanmaktır. Güvenlik uzmanının dünyasında, "oyun" kurumunuzun kaynaklarını güvence altına almaktır. "Rakipleriniz" ise verilerinizi çalmaya ve size karşı kullanmaya çalışan yetkilendirilmemiş kullanıcılardır.

Koç olarak, stratejiler kitabına sahipsiniz. Bu stratejileri rakiplerinizin ellerinden uzak tutmanız gerekir. Ayrıca stratejilerinizin endüstrinin kuralları ve yönetmelikleri ile uyumlu olduğunu garanti etmeniz gerekir. Onları meydan okumaya hazırlamak için oyuncularınızı eğitmelisiniz. Onlara bir takım olarak birlikte çalışmalarını ve oyunu kazanmalarını sağlayacak yetenekleri vermelisiniz.

Başarılı iseniz kurumunuz bir şampiyonlar takımı gibi düzgün çalışacaktır. Herkes misyonu ve onu tamamlamak için nasıl birlikte çalışılacağını anlayacaktır. Başarısız olursanız takımınız kafası karışmış görünecektir. Her oyuncu sonuçlarından haberdar olmadan kendi işini yapıyor görünecektir. Bilmeniz gereken bir sonraki şey, kurumunuzun bilgilerinin rakiplerinizin eline geçeceğidir. Ticari sırlarınız sır olmaktan çıkacak, kurumunuz bozuk şeyleri düzeltmeye çalışırken çok fazla para harcayacak, siz ve çalışanlarınız kendinizi kadro dışı hatta başka işler ararken bile bulabilirsiniz.

Bu derste, güçlü bir sistem yönetimi takımını geliştirmek üzere gerekli yetenekleri öğreneceksiniz.

6. Bölüm Konular

Bu bölüm aşağıda verilen konuları ve kavramları içermektedir:

- Güvenlik yönetiminin ne olduğu
- Uygunluğun ne olduğu
- Mesleki etiğin ne olduğu
- Bir BT güvenlik politikası altyapısının ne olduğu
- Veri sınıflandırma standartlarının neler olduğu
- Konfigürasyon yönetiminin ne olduğu
- Değişiklik yönetim işleminin ne olduğu

- Sistem yaşam döngüsünün (*system life cycle* - SLC) ve sistem geliştirme yaşam döngüsünün (*system development life cycle* -SDLC) ne olduğu
- Yazılım geliştirmenin güvenlik ile nasıl ilgili olduğu

6. Bölüm Hedefler

Bu bölümü tamamladığınız zaman, yapabilecekleriniz:

- Güvenlik altyapısını yönetmek
- Politikaları yaratmak ve desteklemek
- Veriyi sınıflandırmak
- Güvenlik programlarını geliştirmek ve sürdürebilmek
- Sistemlerdeki büyük ve küçük değişiklikleri yönetmek
- Güvenlikte kullanıcı farkındalığını desteklemek
- Mesleki etiği anlamak ve kullanmak

Güvenlik Yönetimi

Bir kurum içerisindeki **güvenlik yönetimi (*security administration*)** kurumun güvenlik planını planlama, tasarlama, gerçekleştirme ve izlemeden sorumlu kişiler topluluğudur. Bir yönetim takımını oluşturabilmenizden önce kurumunuz bilgi varlıklarını tanımlamalıdır. Kurumunuzun varlıklarını tanımlamasının ve belgelendirmesinin ardından her birinin sorumluluğunu bir kişiye ya da pozisyona atamalısınız. Varlıklarınızın listesini ve her birinden sorumlu kişiyi bildiğiniz zaman takımı oluşturabilirsiniz. Bu yönetim takımı o zaman her bir varlığın hassasiyetini ve dolayısıyla korunması için nasıl bir planlama yapabileceğini belirler.

Erişimin Denetlenmesi

Bir kurumun güvenlik yönetim takımının temel görevi sistemlere ya da kaynaklara erişimi denetlemektir. Erişim denetiminin dört yönü vardır:

- **Tanımlama (*Identification*)-** Kullanıcılar tarafından kim olduklarına dair yapılan bildirimler.
- **Kimlik denetimi (*Authentication*)-** Sözkonusu bildirimin kanıtlanması.
- **Yetkilendirme (*Authorization*)-** Geçerli bir kullanıcının ya da sürecin sistem üzerinde sahip olduğu izinler.
- **İzlenebilirlik (*Accountability*)-** Yetkilendirilmiş ve yetkilendirilmemiş kullanıcıların sisteme erişimi sırasında yaptıklarının izlenmesi ya da günlük oluşturulması.

Sistem güvenliği takımı kurumunuzun kaynaklarını korumak için yürürlüğe konabilecek en iyi güvenlik kontrollerini belirleyerek adı geçen çabalara rehberlik eder.

Belgeleme, Prosedürler ve Kılavuzlar

Güvenlik yönetim takımı kurumunuzun güvenlik programının planlanması, tasarımı, gerçekleştirimi ve izlenmesi işleri ile ilgilenir. Varlıkları korumak için en iyi kararları vermede güvenlik yönetimine girdi olarak sağlanması gereken çok çeşitli dokümantasyona gereksinim vardır. En yaygın dokümantasyon gereksinimleri arasında aşağıdakiler yer almaktadır:

- **Hassas varlıklar listesi**—Kurumun korumak için önlemler aldığı varlıkları nelerdir? Liste, bilgisayarları, ağ bileşenlerini, veritabanlarını, dokümanları ve saldırıya maruz kalabilecek herhangi başka bir varlığı içerebilir.
- **Kurumun güvenlik süreci**—Hepsi bir arada nasıl çalışır?
- **Güvenlikten sorumlu kişilerin yetkisi**—Hangi yönetici hangi varlıklarından ve hangi eylemlerden sorumlu ya da yetkilidir?
- **Kurum tarafından benimsenen politikalar, prosedürler ve kılavuzlar**—İletilmesi gereken bilgiler nelerdir, nasıl ve ne zaman iletilir?

Güvenlik yönetim takımı kurumunuzun mevcut politikalara uygunluğunu garanti etmek üzere bulmacanın bütün parçalarını bir araya getirir. Bir kurum iki seviyede kurallara uymak zorundadır:

- **Mevzuata uygunluk**—Kurum kanunlara ve resmi yönetmeliklere uymak zorundadır.
- **Kurumsal uygunluk**—Kurum kendi politikalarına, iç denetimlerine, kültürüne ve standartlarına uymak zorundadır.

Sonuç olarak, güvenlik yönetim takımının dokümantasyonu, prosedürleri ve kılavuzları uygunluğa ve uygunluk izlemesine odaklanır. Kurumun çok çeşitli kuralları ve yönetmelikleri takip ettiğini garanti etmelidirler.

Felaket Değerlendirmesi ve Kurtarma

Güvenlik yönetim takımının sorumlulukları bilgisayarlarınızı ve ağlarınızı etkileyen olayların ele alınmasını içerir. Bu olaylar arasında acil durumlar, felaketler ve diğer kesintiler yer alır. Güvenlik yönetim takımı herhangi bir güvenlik arızası ile ilgilenmek üzere acil müdahale ekibi oluşturur. Bu takım acil durumlara müdahale etmek ve güvenlik açıklarını soruşturmaktan sorumlu kişilerden meydana gelmektedir. Güvenlik yönetim takımı tarafından yönetilen bir başka takım **acil operasyonlar grubudur**. Bu grup doğal felaketler, ekipmanların bozulması ve diğer potansiyel acil olaylar meydana geldiğinde hassas verilerin korunmasından sorumludur.

Acil müdahale ekiplerinin, acil operasyonlar grubunun ve sistem yöneticilerinin tüm çabalarına rağmen bütün sistemler arızaya ve saldırılara açıktır. Güvenlik yönetim takımı kurumun bir olaya hızlı ve etkili bir şekilde yanıt döndürebilmesini garanti eder.

Güvenliğin Dış Kaynaklardan Edinilmesi

Çok sayıda kurum güvenlik izleme ve analizinin idaresi için dış firmalara dayanır. Bu, dış kaynak firmasının işini izlemenizin ya da acil durumların idaresinde birlikte çalışmanızın gerekebileceği anlamına gelir. Bu yaklaşımın hem olumlu hem de olumsuz yanları vardır:

- **Olumlu yanlar**—Bir güvenlik yönetim firması her gün güvenliğe ve sadece güvenliğe odaklandığı için yüksek seviyeli bir uzmanlığa sahiptir. Basitçe ifade etmek gerekirse kendi kurumunuzun sahip olamayacağı uzmanlığa ve deneyime sahip olacaktır.
- **Olumsuz yanlar**—Dış kaynak kullanımının iki temel olumsuz yanı mevcuttur: İlki, dış kaynak firması kurumunuzu iyi tanımıyor olabilir ve kurum içi bilgilere sahip olmayabilir. İkinci olarak, dış kaynak kullanımı ile kurum içi yetenekler geliştiremezsiniz ve dolayısıyla belirsiz olarak bu hizmetler için para ödemeye devam etmeniz gerekecektir.

Dış Kaynak Kullanımı ile İlgili Hususlar

Güvenlik yönetim takımı her ikisinin de özel güvenlik gereksinimleri üzerinde anlaştığını garanti etmek üzere dış firma ile yakın bir şekilde çalışmalıdır. Verinin entegre edilmesi ya da üçüncü şahıslar ile işlenmesi yeni tehditler oluşturur. Verinin ya da süreçlerin (ya da her ikisinin) kendi veri merkezlerinizin dışına taşınması güven sorularını gündeme getirir. Bir başka kuruma fikri mülkiyetinizi korumasında nasıl güvenebilirsiniz? Dış kaynak kullanımında çok sayıda ilgi noktası olmasına rağmen, temel ilgi noktaları aşağıda yer almaktadır:

- **Mahremiyet**—Üçüncü şahıs mahremiyet politikanızı devam ettirmeyi kabul etmekte midir? Verinin toplanma, kaydedilme, işlenme ve ortadan kaldırılma şeklini nasıl denetlemeyi planlamaktadır?
- **Risk**—Verinin bir güven sınırı üzerinden transfer edilmesinde başka hangi riskler yer almaktadır? Yeni riskler nasıl ele alınacaktır? Dış kaynak kullanımının yeni risklerini yönetmekten kim sorumludur?
- **Veri güvenliği**—Veri gizliliğini ve bütünlüğünü yetkisiz erişimden hangi kontroller korumaktadır? Erişim denetimleri iç denetimler ile uyumlu mudur? Verinin kullanılabilirliği (*availability*) nasıl korunmaktadır? Arıza süresini en aza indirgemek için yedekler ve fazlalık (*redundancy*) önlemleri hazır mıdır? Yedekler ve fazlalık veri kopyaları nasıl korunmaktadır?
- **Sahiplik**—Verinin, altyapının ve araçların sahibi kimdir? Her bir bileşenden kim sorumludur?
- **Politikalara bağlılık**—Her üçüncü şahıs güvenlik politikalarınızın ve prosedürlerinizin devam ettirilmesini taahhüt etmekte midir?

Dış kurumlara dış kaynak kullanımı yapıldığında, çok çeşitli sözleşme tipleri yaygındır. Bu sözleşmeler az önceki sorulara cevapların resmileştirilmesine yardım eder. Bir dış kaynak kullanımı ilişkisinin nasıl çalıştığını tanımlayan en yaygın sözleşmelerin listesi aşağıdakileri içerecektir:

- **Hizmet-seviyesi sözleşmesi (*Service-level agreement* - SLA)**—Bu tip sözleşme, kurumunuz ve dış firma arasında firmanın sağlayacağı özel hizmetleri detaylandıran resmi bir sözleşmedir. Bir SLA içinde detaylandırılan güvenlikle ilgili hizmetlere ait bazı örnekler aşağıdakileri içerir:
  - Potansiyel güvenlik açıkları nasıl ve ne zaman iletilmektedir
  - Günlükler ve olaylar nasıl raporlanmaktadır
  - Gizli veri nasıl ele alınmaktadır
  - Güvenlik sistemi çalışabilirlik süresi (*uptime*) gereksinimleri nelerdir (örneğin, bütün kritik güvenlik sistemlerinin yüzde 99.99 güvenilirliğe sahip olmasına gerek duyabilirsiniz)

SLA gerek kurum gerekse de dış firmanın beklentilerini aktarmalıdır. SLA her iki tarafın da gereksinimlerini tahmin etmelidir. Güvenlik yönetim takımının her üyesi kendi bölümünün risklerini en ince ayrıntısına kadar analiz etmelidir. Hesaba katılmayan herhangi bir riskin kurumunuza veri kaybı ya da onarım harcamaları şeklinde maliyet çıkarması olasıdır. Bunu bir otomobilin bakımına benzer olarak düşünebilirsiniz: Düzenli yağ değişimleri, yanan conta kapaklarından daha ucuzdur. Motorun bakımı, tamirinden ucuzdur.

- **Sonu açık sipariş sözleşmesi (*Blanket purchase agreement* - BPA)**—Yinelenen tedarik ve hizmet gereksinimlerini karşılamaya elverişli bir yöntem olarak BPA yinelenen ürün ve hizmet siparişlerini karşılamak üzere nitelikli tedarikçilerden önceden onaylanmış hesaplar yaratır. BPA'lar yinelenen satın alma süreçlerini kolaylaştırmada çok faydalı olabilir.
- **Mutabakat bildirisi/İyi niyet sözleşmesi (*Memorandum of understanding* - MOU)**—Niyet mektubu olarak da bilinen MOU iki ya da daha fazla taraf arasında ortak eylemlerle sonuçlanan ortak ilgi alanlarını ifade eden bir sözleşmedir. MOU'lar genel olarak resmi bir sözleşmeden daha az yaptırım gücüne sahip fakat sözlü bir anlaşmadan daha resmidir.
- **Birbirine bağlı güvenlik sözleşmesi (*Interconnection security agreement* - ISA)**—Sıklıkla MOU'nun bir eklentisi olan ISA birbirine bağlı varlıkların teknik gereksinimlerini belgeleyen bir sözleşme olarak hizmet eder. Bu tip dokümanlar çoğu zaman birbirine bağlı kurumların güvenlik sorumluluklarını ve teknik gereksinimlerini belirtmekte kullanılır.

Uzlaşma süreci ve sözleşmelerin yaratılması iş partneri **işe uyum** sürecinin ilk adımlarından biridir. Kurumunuz veri ya da işlenmesinde dış kaynak kullanımına karar verdiği zaman güvenlik etkisini ve sorumluluklarını dikkatli bir şekilde düşünmelisiniz. İşe uyum süreci bir sorun oluşmadan önce acil durum planlaması için zaman sağlar. Ayrıca, tüm taraflar için hedeflerin ve beklentilerin net bir şekilde iletilmesi olanağını da sağlar. Benzer şekilde, dış kaynak kullanımı ilişkilerini sonlandırdığınızda takip edilecek bir **işten ayrılma uyum sürecini** tanımlamalısınız. İşten ayrılma uyum süreci, veri ve diğer varlıkların denetiminin aktarılmasını, iletişimin sonlandırılmasını ve açık işlemlerin tamamlanmasını tanımlar. Bu süreç, dış kaynak kullanımı ilişkisi bittiği anda herhangi bir veri ve işleme kalıntısının kalmadığını garanti etmek için gereklidir.

Uygunluk

Kurumunuzun güvenlik politikası, güvenlik aktivitelerine yaklaşım tarzınızı belirler. Ayrıca, uymanız gereken kuralları ifade eder. Bir güvenlik politikasını trafik kuralları gibi düşünebilirsiniz. Trafik kuralları yollarda belli derecede düzeni ve emniyeti devam ettirir. Eğer bu kurallar uygulanmazsa, yollar tehlikeli hale gelir. Bir bilgi güvenliği politikası da çok farklı değildir. Uygulanmadığında, güvenlik politikanız pek iyi değildir. Bu, uygunluk (*compliance*) kavramının resme girdiği yerdir. Politikalar uygulandığında kurumunuz o politikalara uygun olur. Uygunluğu garanti etmek için üç araç kullanılmaktadır:

- Olay günlükleri
- Uygunluk irtibatı
- İyileştirme

Olay Günlükleri

Olay günlükleri (*event logs*) işletim sisteminizin ya da uygulama yazılımınızın yarattığı eylemlerin kayıtlarıdır. Bir olay günlüğü, hangi kullanıcının ya da sistemin veriye ya da bir kaynağa ne zaman eriştiğini kaydeder. Olay günlüklerini bir halk kütüphanesinin kitap teslim alımlarını takip ettiği sisteme benzer düşünebilirsiniz. Bir kitap geciktiğinde ya da kaybolduğunda, kütüphane kitabı en son alan kişiyi tespit etmek üzere kayıtlarını kontrol eder. Kurumunuzda bir bilgi güvenliği açığı oluştuğunda olay günlüğü sisteme ne olduğunun ve ne zaman gerçekleştiğinin belirlenmesine yardımcı olur. Suçluyu takip etmenize veya sorunu çözmenize yardım eder. Olay günlüklerinin kaydettiği bilgi miktarını değiştirebilirsiniz. Her olayı kaydetmek çok büyük miktarda disk alanı gerektirir ve bilgisayarlarınızı yavaşlatabilir. Ayrıca, günlük dosyalarının okunmasının daha güç olması anlamına gelir. Öte yandan, çok az sayıda olayın kaydedilmesi önemli ayrıntıları kaçırmanıza neden olabilir. Güvenlik problemlerini soruşturmak üzere gelecekte ihtiyaç duyacağınız tüm eylemleri kaydetmeniz önemlidir. Olay günlüklerinize erişimin denetlenmesi de ayrıca önemlidir. Bir saldırganın sisteminizin gizliliğini ihlal edebilir olup saldırının izlerini silmesini istemezsiniz.

Uygunluk İrtibatı

Kurumlar ve güvenlik politikaları daha büyük ve daha karmaşık oldukça uygun kalmak güçleşir. **Uygunluk irtibatı (*compliance liaison*)** tüm personelin kurumun politikalarından haberdar olmasını ve politikalara uygun hareket etmesini garanti eder. Kurum içerisindeki farklı bölümlerin farklı güvenlik fikirleri ve gereksinimleri olabilir. Uygunluk irtibatı her bir bölüm ile o bölümün uygunluğu anladığını, gerçekleştirdiğini ve izlediğini garanti etmek üzere birlikte çalışır. Uygunluk irtibatı ayrıca bölümlere bilgi güvenliğini günlük operasyonlarına nasıl dahil edeceklerini anlamalarında yardımcı olur. Uygunluk irtibatının bir diğer önemli rolü dış kaynak kullanım hizmet sağlayıcıları ile ilgilenmektir. Birlikte işlerlik belgelerinin yaratılması zahmetine katlandıktan sonra belirlediğiniz kuralların takip edildiğini garanti etmeniz gerekir. Uygunluk irtibatı herhangi bir dış kaynak kullanım sözleşmesi boyunca anlaşma gereksinimlerini gözden geçirir. Bu gözden geçirme, hizmet sağlayıcının mevcut anlaşmalar ile uygunluk içerisinde olup olmadığının doğrulanmasına yardım eder.

İyileştirme

Güvenlik açıklarının azaltılması bilgisayarlarınıza ve ağlarınıza karşı saldırı riskini zayıflatır. Bazı durumlarda en iyi çözüm davetsiz misafiri engellemek ve bir kaynağa erişimi reddetmektir. Diğer durumlarda, güvenlik açığını ortadan kaldırmak mümkündür. **İyileştirme (*remediation*)** bozulan ya da hatalı bir şeyin tamir edilmesidir. Bilgisayar sistemlerinde iyileştirme, güvenlik açıklarının saptanması ile ilgilidir.

Elbette bazı problemler diğerlerinden daha önemlidir. Yüksek risk taşıyan sorunları düşük riskli olanlardan önce düzeltmelisiniz. Mümkünse en iyi seçenek güvenlik açıklarını ortadan kaldırmaktır. Eğer bir güvenlik açığını etkili bir şekilde ortadan kaldıramıyorsanız, bir sonraki en iyi adım saldırganın güvenlik açığından faydalanma yeteneğini ortadan kaldırmaktır. Varlıklarınızı saldırıdan korumak için her zaman güvenlik politikaları tasarlamalısınız. Uygunluk, bilgi teknolojisi sistemlerinin güvence altına alınmasında son derece önemlidir.

Mesleki Etik

Güvenlik uzmanlarının üstleneceği en önemli rollerden biri uygun davranış konusunda liderliktir. Kişiler, liderlerine güvenmedikleri takdirde kurallara uymayacaklardır. Her saygıdeğer meslek, kendine ait etik ve davranış kurallarına sahiptir. Bu kurallara bağlılık herhangi bir mesleğin üyelerinin saygınlığını arttırır. Bu bakımdan güvenlik mesleği diğer mesleklerden farklı değildir. Güvenlik uzmanlarının davranışlarını yönetecek kesin etik kuralların olması önemlidir. Güvenlik sertifikasyon kurumlarının çoğu benimsedikleri etik kuralları yayımlar. Aslında, çoğu sertifikasyon adaylar sertifikasyona yeterlik kazanmadan önce adayların belirli etik kurallara bağlılığını gerektirir. Örneğin, hem $(ISC)^2$ hem de CompTIA katı etik kılavuzları sağlar. Bununla birlikte, kılavuzlar onları benimseyip uygulamadığınız sürece etkili değildir. Aşağıda güçlü etik uygulamalar için ipuçları bulacaksınız:

- **Örnek olun**—Günlük aktivitelerinizde güçlü etik ilkeleri gösterin. Kullanıcılar öncülüğünüzü takip edeceklerdir. Etik konusunda ciddi iseniz, kullanıcılarınız etik konusunda daha ciddi olacaktır.
- **Etik kılavuzlarını ve standartlarını benimsemeyi cesaretlendirin**—Güvenlik uzmanları etik sınırlarını bilmeli ve bu sınırlara bağlı kalarak örnek olmalıdırlar. Bu, sıklıkla zor kararların verilmesi ve iyi bir örnek olunması anlamına gelir. Kurumunuzu kendi etik kurallarını tanımlaması konusunda zorlamalısınız. Bu, personelin etik ve sorumlu çalışmasına yardım eder.
- **Kullanıcıları güvenlik farkındalık eğitimleri ile bilgilendirin**—Kullanıcıların etik sorumluluklarının farkında olup anladıklarından emin olun.

Etik Konusunda Yaygın Yanlış Düşünceler

Basitçe etik yönelimli kurallar listesi yazmak yeterli değildir. Güvenlik uzmanlarının günlük hayatlarında gerçekten etik olmaları önemlidir. Etik kurallara bağlılıkta ilk adım çoğu bilgisayar kullanıcısını etik olmayan davranışlara yönelten en yaygın varsayımları anlamaktır. Bu yaygın varsayımların bazılarını aşağıda bulabilirsiniz:

- Kullanıcılar, bilgisayarların kötüye kullanımı önleyeceğini varsayarlar. Yetkisiz erişim elde edebiliyorlarsa, bu kendilerinin değil kurumun hatasıdır.
- Kullanıcılar, bazı hukuk sistemlerinde konuşma ve ifade özgürlüğünün bir şekli olarak güvenlik açıklarını araştırmanın hakları olduğuna inanmaktadırlar.
- Kullanıcılar, eylemlerinin sadece küçük bir zarara neden olabileceğini düşünürler. Küçük bir zararın kimseyi rahatsız etmeyeceğini düşünürler.
- Kullanıcılar, sisteme kolay girilebiliyorsa bunu yapmanın uygun olduğunu düşünürler.
- Kullanıcılar, sebepleri zarar vermek değilse bir sisteme izinsiz girişin uygun olduğunu düşünürler. Sisteme izinsiz giriş yaparak para kazanmıyorlarsa veya başka bir şekilde kendilerini ilerletmiyorlarsa suç işlemiyor olmaları gerektiğini düşünürler.
- Kullanıcılar, bilginin ücretsiz olması gerektiğini düşünürler. Herhangi birinin sistemini bilgi elde etmek için gözden geçirmenin uygun olduğunu düşünürler.

Etik Kurallar

Etik kurallar profesyonelliğin garanti edilmesine yardım eder. Yayımlanmış çok sayıda kural bilgi güvenliğine uygulanır. Örneğin, **İnternet Mimarisi Kurulu (*Internet Architecture Board* - IAB)'nun** yayımlamış olduğu tebliğler güvenlikle ilgili etik kuralların çoğunun tavrını özetler. Bu tebliğler, IAB'nin neyi etik ve uygun davranış olarak değerlendirdiğini açıklar.

İnternet Mimarisi Kurulu (IAB) Politika Raporu

IAB etik olmayan ve kabul edilemez uygulamalar listesi sağlamıştır. 1989'da IAB internet etiği hakkında politika raporu yayınlamıştır. Bu belgenin başlığı RFC 1087'dir. İnternet kullanımının etiği üzerine ilk raporlardan birisi olmasına rağmen bugün hala geçerlidir. RFC 1087 (*https://tools.ietf.org/html/rfc1087*) kasıtlı olarak aşağıdakilerden herhangi birini gerçekleştiren bir aktivitenin etik dışı ve kabul edilemez olduğunu bildirir:

- "İnternet kaynaklarına yetkilendirilmemiş erişim kazanmaya uğraşmak"
- "İnternetin tasarlanan kullanımını bozmak"
- "Bu tür eylemler üzerinden kaynakları (insan, kapasite, bilgisayar) boşa harcamak"
- "Bilgisayar tabanlı bilginin bütünlüğünü ortadan kaldırmak"
- "Kullanıcıların gizliliğini ihlal etmek"
- "İnternet çapında deneylerin gerçekleştiriminde ihmale yol açmak"

Belgenin anahtar noktası şudur: İnternete erişim bir hak değil, *ayrıcalıktır*.

Mesleki Gereksinimler

Herhangi bir meslekte kurallar ve yönetmelikler mesleki etiği uygulatır. Bu kurallar onay organlarından geliyor olabilir. Kuralları ihlal ederseniz sertifikanızı ya da lisansınızı kaybetme riski ile karşı karşıya kalırsınız.

Diğer bağlamlarda kanunlar ve yönetmelikler etik davranış gerektirir. Örneğin, Ekonomik Kalkınma ve İşbirliği Örgütü (*Economic Cooperation and Development* - OECD) 30 ülkeden fazla ülkenin kuruluşudur. Hedefi ekonomik işbirliği ve büyümedir. 1980 yılında sekiz gizlilik prensibi yaratmıştır. Bu prensipler dünya gizlilik mevzuatının büyük bir bölümünün temelini oluşturur. Özetle bu prensipler aşağıdakileri ifade eder:

- Bir kurum sadece gereksinim duyduğu bilgiyi toplamalıdır.
- Bir kurum sahip olduğu bilgiyi paylaşmamalıdır.
- Bir kurum sahip olduğu bilgiyi güncel tutmalıdır.
- Bir kurum sahip olduğu bilgiyi sadece toplama amacına uygun olarak kullanmalıdır.
- Bir kurum sahip olduğu bilgiye artık gereksinim duymuyorsa bilgiyi uygun şekilde ortadan kaldırmalıdır.

NOT

OECD ile ilgili daha fazla bilgi için www.oecd.org adresini ziyaret ediniz. Özgün OECD Gizlilik Yönergeleri'ni ve onların günümüz ortamlarındaki uygulamasını *www.oecd.org/sti/ieconomy/49710223.pdf* adresinde bulabilirsiniz.

Teknik TAVSİYE

Öğrendiğiniz gibi, birçok sertfikasyon kurumu etik kurallarına uyum gerektirmektedir. (*ISC*^{2} *Etik Kuralları'nı https://www.isc2.org/ethics/default.aspx* adresinde bulabilirsiniz. CompTIA Aday Etik Kuralları (*Candidate Code of Ethics*) *https://certification.comptia.org/testing/test-policies/continuing-education-policies/candidate-code-of-ethics* adresindedir.

Personel Güvenlik Prensipleri

Sistemlerinizi güvenli hale getirmek için tasarlayabileceğiniz bütün teknik çözümler için, insan bileşeni en büyük zorluğunuz olarak kalmaya devam eder. Küçük bir eğitimin ne kadar mesafe aldıracağı sizi şaşırtabilir. Personeliniz güvenlik risklerinin hem kendilerine hem de kuruma nasıl zarar verebileceğinin farkında olurlarsa, size disiplinli yönetiminizde yardımcı olmaları daha muhtemeldir.

Bir kullanıcının neyi yapıp neyi yapmaması gerektiğini bilmek önemlidir. Bu hedefi gerçekleştirmenin en iyi yolu iyi tanımlanmış iş tanımları, iş rolleri ve sorumlulukları yaratmaktır. Kişilerin neyi yapıyor olması gerektiğini bilirseniz onların yapmamaları gereken aktiviteleri tespit etmeniz kolaylaşır. Eğer onların rolleri ve sorumlulukları şüpheli ise kötü davranışı işaretlemek zorlaşır, kişilerin yaptıklarının yanlarına kar kalmasının daha muhtemel olması anlamına gelir.

Bilgiye ve varlıklara erişimin en aza indirilmesi önemli bir güvenlik kontrolüdür. Halihazırda, personel güvenliğine ilişkin bazı kavramlar hakkında bilgi edindiniz. Bu kavramlar çok önemlidir ve yeniden gözden geçirilmeye değer. Personelinizi doğrudan etkileyen herhangi bir güvenlik kavramına dikkat edin. Kişiler kurumunuzdaki en önemli varlıklardır. Onların kurumunuzun güvenliğinin sürdürülmesine nasıl katkı sağlayacaklarını bilmeleri hayati önem taşır.

Erişimin Kısıtlanması

Kullanıcılara erişimin nasıl verileceğine karar verirken ana kavramlardan biri erişimin kısıtlanmasıdır. Kullanıcılara sadece görevlerini gerçekleştirmelerine yetecek erişim hak seviyelerinin verilmesi fikri *en düşük erişim hakkı (least privilege)* prensibi olarak isimlendirilir. Her zaman bu prensibi kullanın. Aksi takdirde, yetkilendirilmemiş kullanıcıların erişmemeleri gereken bilgiye erişimine izin verme riski taşırsınız. Örneğin, zayıf erişim denetimleri bir satış görevlisinin çalışan maaşlarını görmesine izin verebilir.

Bilinmesi gereken (need-to-know) gereksinimi, en düşük yetki prensibi ile ilişkili bir başka kavramdır. Bu, kişilerin erişim yetkilerine bakılmaksızın sadece işlerini gerçekleştirmek için sadece gereksinim duydukları bilgiye erişmeleri gerektiğini bildirir. Dolayısıyla, kullanıcılar çok gizli erişim yetkisine sahip olsalar dahi çok gizli bilgilerin tümüne erişmeleri gerektiği anlamına gelmez. Sadece işlerini yapmak için gereksinim duydukları bilgiye erişmeleri gerekir.

Görevler Ayrılığı

Görevler ayrılığı (*seperation of duties*) bir görevin farklı kullanıcıların gerçekleştirmesi gereken alt görevlere bölünmesidir. Bu, tek bir kullanıcının çok önemli bir görevi bir başka kullanıcının yardımı ya da onayı olmadan gerçekleştiremeyeceği anlamına gelir. Başka bir şekilde ifade etmek gerekirse: Sisteme zarar vermeyi planlayan bir kullanıcı başkalarından yardım almak zorundadır. Bir komplonun organize edilmesi ve gizlenmesi zordur. Örneğin, görevler ayrılığı bir çalışanın yeni bir tedarikçi yaratamamasını *ve* bu tedarikçiye çek kesememesini garanti etmeye yardımcı olur. Bu bir çalışanı Acme Danışmanlık adına bir banka hesabı açmaktan, çalışan sistemde Acme Danışmanlık adında bir tedarikçi yaratmaktan ve Acme Danışmanlık'a $1000'lık bir çek kesmekten alıkoyar.

İş Rotasyonu

Kurumunuzu personelle ilişkili güvenlik ihlallerinden korumanın bir diğer yolu **iş rotasyonu** kullanmaktır. İş rotasyonu, çalışanları çeşitli sistemler ve görevler arasında sırayla çalıştırarak riski en aza indirger. Bu, çok sayıda çalışanın sahtekarlıkta bulunmak üzere komplo kurmasını engeller. Ayrıca, yöneticilere hangi kullanıcıların hangi eylemleri ne zaman yapmaya yetkili olduklarını izleme fırsatı verir. Diğer güvenlik önlemleri başarısız olduğunda iş rotasyonu güvenlik açığının daha fazla zarara uğratmadan bulunmasına olanak sağlar. İş rotasyonu ayrıca çok sayıda çalışan belirli işlere dair yetenekleri öğreneceğinden, eğitilmiş bir yedekleme sağlar.

Zorunlu İzinler

İş rotasyonuna oldukça benzer şekilde zorunlu izinler sahtekarlığı tespit etmek için fırsat sağlar. Kullanıcılar izinde olduklarında ortamınıza erişimlerini askıya almalısınız. Bu onların evden çalışarak izlerini örtme girişimlerini önler. Örneğin, Amerikan bankacılık kurallarına göre belirli banka çalışanları ardışık iki hafta izin almak zorundadır. Yakın zamana kadar kanun yöneticilerin izindeki çalışanları ile işle ilgili konularda irtibat kurmalarını yasaklıyordu. Bu kural sistemlere sadece-okuma erişimi izni vermesi için esnetildi, böylece çalışanlar en azından e-posta yazışmalarını takip edebilirler. Bununla birlikte, izinde iken işle ilgili aktivitelere hala katılamazlar.

Güvenlik Eğitimi

Katı güvenlikte personel çok önemli olduğu için geliştirebileceğiniz en iyi güvenlik kontrollerinden birisi güçlü bir güvenlik eğitimi ve farkındalık programıdır. Güvenlik eğitimi tüm çalışanların desteğinin kazanılmasına yardım eder. Onlar kendi işlerine ilişkin politikalara uyulmasında harekete geçen güvenlik savunucuları olurlar. Güvenlik açıklarından kaçınmak konusunda dikkatli olurlar. Çalışanlarınızı eğitmelisiniz, sonra belirli aralıklarda onları yeniden eğitmelisiniz. Bu yinelenen eğitimler, çalışanların bilgisini tazeler ve onlara güvenliğin önemini hatırlatır. İyi eğitilmiş personel güvenli bir ortam ile saldırılar ve hatalar koleksiyonu arasında bir fark yaratabilir.

Çalışanlar bir kuruma yönelik özellikle insan faktöründen kaynaklanan güvenlik tehditlerinin farkında olmalıdırlar. Bu tehditler arasında dolandırıcılık teknolojilerinin kurulması, zayıf parolaların seçilmesi ve oltalama saldırıları yer alır. Bu tip tehditlerin önemlerinin fark edilmesi hususunda çok sayıda kurum personelini eğitmede başarısız olduğundan yaygın olarak görülürler. Zayıf parolaların kişisel ve ticari bilgileri nasıl tehlikeye atacağının basitçe açıklanması çoğu zaman kullanıcıları daha güçlü parolalar yaratmada cesaretlendirebilir.

Güvenlik Farkındalığı

Bir güvenlik farkındalığı programı güvenlik politikanızın gereksinimlerini ve beklentilerini ele almalıdır. Güvenlik politikası güvenlik kontrolleri için yetki sağlar ve eylemler gerektirir. En iyi savunma şekillerinden biridir. Çalışanların bir güvenlik kontrolüne uymaları onu zorlayan politikayı bildikleri durumda daha olasıdır. Bir politikanın her bölümünün neden gerekli olduğunun açıklanmasına ek olarak, program politika ihlalleri durumunda cezaları açıklamalıdır.

Bir farkındalık programı resmi bir eğitim programından farklıdır. Çoğu kullanıcı güvenliğin ne olduğunu ve neden gerekli olduğunu anlamaz. Güvenlik farkındalık programlarını (posterler, e-postalar ve çalışan bültenleri ve diğer araçlar) aşağıdakileri gerçekleştirmek için kullanabilirsiniz:

- Kullanıcılara güvenlik hedeflerini öğretmek
- Kullanıcıları güvenlikteki yönelimler ve tehditler konusunda bilgilendirmek
- Kullanıcıları güvenlik politikalarına uymaları konusunda harekete geçirmek

Çalışanlar genel olarak şirket için en iyisini isterler. Bununla birlikte, güvenlik üretkenliklerine engel oluyor görünürse işlerini daha hızlı tamamlamak için çoğunlukla güvenlik önlemlerini atlarlar. Örneğin, Bob adındaki bir çalışanın haftasonu evde iken ofiste bulunan Sue adındaki başka bir çalışandan bir telefon aldığını farz edin. Sue, bir projeyi tamamlayabilmesi için Bob'un

parolası ile bir dosyaya ya da bir sisteme giriş yapması gerektiğini söylüyor. Çalışanlarınıza parolalarını paylaşmanın risklerini ne kadar sıklıkla hatırlatırsanız hatırlatın birçok çalışan böyle bir durumda parolalarını teslim etmekte hala hızlı olacaktır. Güvenlik politikalarını takip etmenin önemini kuvvetlendirmek sizin işinizdir. Üretkenlik problemlerini nasıl çözeceklerini ve yine de yüksek seviyeli bir güvenliği sürdürebilmeyi öğretmek sizin işinizdir.

Farkındalık programları personele güvenlik politikaları hakkında hatırlatma yapabilir. Bu programlar ayrıca güvenlik politikasının personel tarafından ne kadar iyi takip edildiğini ölçebilir. Programlar personele güvenlik vakaları ile nasıl ilgilenecekleri konusunda pratik tavsiye sağlar. İyi bir program personeli güvenliğin kendi kişisel sorumlulukları olduğu konusunda ikna eder. Çalışanlarınıza davranışlarını güvenliğin günlük alışkanlıklarının bir parçası olması şeklinde değiştirmelerinde yardımcı olabilirsiniz.

Politikaları takip etmeyen çalışanlarınızı not edin. Bu bilgiyi çalışanlarınıza bir eğitim oturumunda işlerine özgü senaryolar sunmak için kullanabilirsiniz. Çalışanlarınıza "..... olsa ne yapardınız?" sorularını sorun. Topladığınız bilgi, farkındalık programınızdaki boşlukları tespit etmenize yardım eder. Programınızı bu bilgi ile uygun hale getirin.

Sosyal Mühendislik

Bilgisayar sistemleri üzerinde en popüler saldırı çeşitlerinden biri sosyal mühendisliği içerir. Sosyal mühendislik güvenlik kontrollerini aşmak için insanların kandırılması veya kullanılmasıdır. Birçok kişi yardımsever olmak istediğinden bir saldırgan için sisteme erişimi olan birini yapmaması gereken bir şeyi yapması için ikna etmek çok zor değildir. Güvenliğin en kritik alanlarından biridir. Daha fazla çalışana sistemlere ve veriye erişim hakkı verdikçe güvenlik açığı riski yükselir. Teknik çözümler, yetkili bir kullanıcıyı yetkilendirilmemiş bir kullanıcıyı aramakta ya da telefon üzerinden hassas veriyi okumakta durdurmayacaktır. Sosyal mühendislikten kaçınmanın en iyi yolu personelinizin sosyal mühendislik girişimlerini tanıma ve bu saldırılarla nasıl uğraşılacağını bilme konusunda eğitilmesini garanti etmektir. Güvenlik eğitiminiz aşağıdakileri içeren en yaygın sosyal mühendislik saldırı çeşitlerini kapsamalıdır:

- **Gözdağı vermek**—Bilgi için birine tehdit ya da usanç ile zorbalık etmek.
- **Tanıyor havasına girmek**—Yöneticilerin ya da üstlerin isimlerini vererek başka bir kişiyi üst bir yetkilinin bilgiye erişim izni verdiği konusunda ikna etmek.
- **Yardım için başvurular**—Bir kişiyi merhamet hissi ya da güç belki de mantıksız bir durumu anlaması üzerinden çekmek. Duygusal başvurunun hedefi normal prosedürleri atlamak veya özel bir değerlendirme kazanmaktır. Ödül gibi bir özendirici ile birleştiğinde bu tür mühendislik çok etkilidir. Örneğin, dolandırıcının engelli bir kişiye para transfer etmesine yardım etmeniz durumunda size para göndermeyi taahhüt ettiği bir dolandırıcılığı düşünün. Maalesef, bu tür duygusal başvuru her yıl birçok kişiyi kandırmaktadır.
- **Oltalama**—Sosyal mühendislikte teknoloji gayet iyi çalışır. Örneğin, oltalamayı (*phishing*) ele alın. Bir oltalama saldırısında dolandırıcılar saygıdeğer bir kurumun yapıtını andıran bir e-posta ya da web sayfası yaratırlar. Dolandırıcılar hassas bilgilerinizi paylaşacağınız şeyin saygıdeğer bir kurum olduğuna inanmanızı isterler. Onlar bu bilgiyi finansal bilgilerinize erişim elde etmek ya da kimliğinizi çalmak üzere kullanırlar. Bir oltalama saldırısı hassas bilgilerinizi yakalama çabası içerisinde sorular soran bir anket şeklini de alabilir.

> **NOT**
>
> Güncel oltalama teknikleri ve sahtekarlık uyarıları ile ilgili daha fazla bilgi için *www.fraudwatchinternational.com/phishing* adresine bakınız.

Bir BT Güvenlik Politikası İçin Altyapı

Her şirket kanunlar, yönetmelikler, gereksinimler, rekabetçiler ve ortakların karmaşık birleşimi içerisinde çalışır. Ek olarak moral, emek ilişkileri, üretkenlik, maliyet ve nakit akışı bir şirketin nasıl işlediğini etkiler. Bu ortam içerisinde yönetim genel bir güvenlik bildirimi ve yönergeleri geliştirmeli ve yayınlamalıdır. Güvenlik takımının perspektifinden bir güvenlik programı bu yönergeleri politikalar ve onların standartlar, prosedürler, dayanaklar ve kılavuzlar gibi destekleyici bileşenleri üzerinden ele alır. **ŞEKİL 6-1** bir güvenlik politika ortamının bileşenlerini göstermektedir.

Her bileşenin uygunluk izleme, güvenlik farkındalığı, eğitim, erişim denetimi, gizlilik, olaya yanıt, sistem günlüğü analizi vb. ile ilgili olan güvenlik uzmanı için kendine özgü bir gereksinimi vardır.

Güvenlik politikanız kurumunuzun tavrını ve kültürünü belirler. Bir güvenlik uzmanı olarak sıklıkla politika niyetinizi uygulamanız gerekecektir. Kurumunuzun güvenlik politikasının ayrıntılarını anlamalısınız. Politika değerlerin ve yönün yüksek seviyeli bildirimidir. Kurumunuzun standartları, dayanakları, prosedürleri ve kılavuzları güvenlik politikanızı gerçekleştirir.
Güvenlik uzmanının rolü bu bileşenler için destek sağlamaktır. Bu destek, personeli politikalar, eğitim ve yaptırım konusunda bilgilendirmeyi içerir. Herhangi bir güncelleme ya da değişiklikte rolünüz vardır. **ŞEKİL 6-2** tipik bir güvenlik politikası hiyerarşisini göstermektedir.

Politikalar

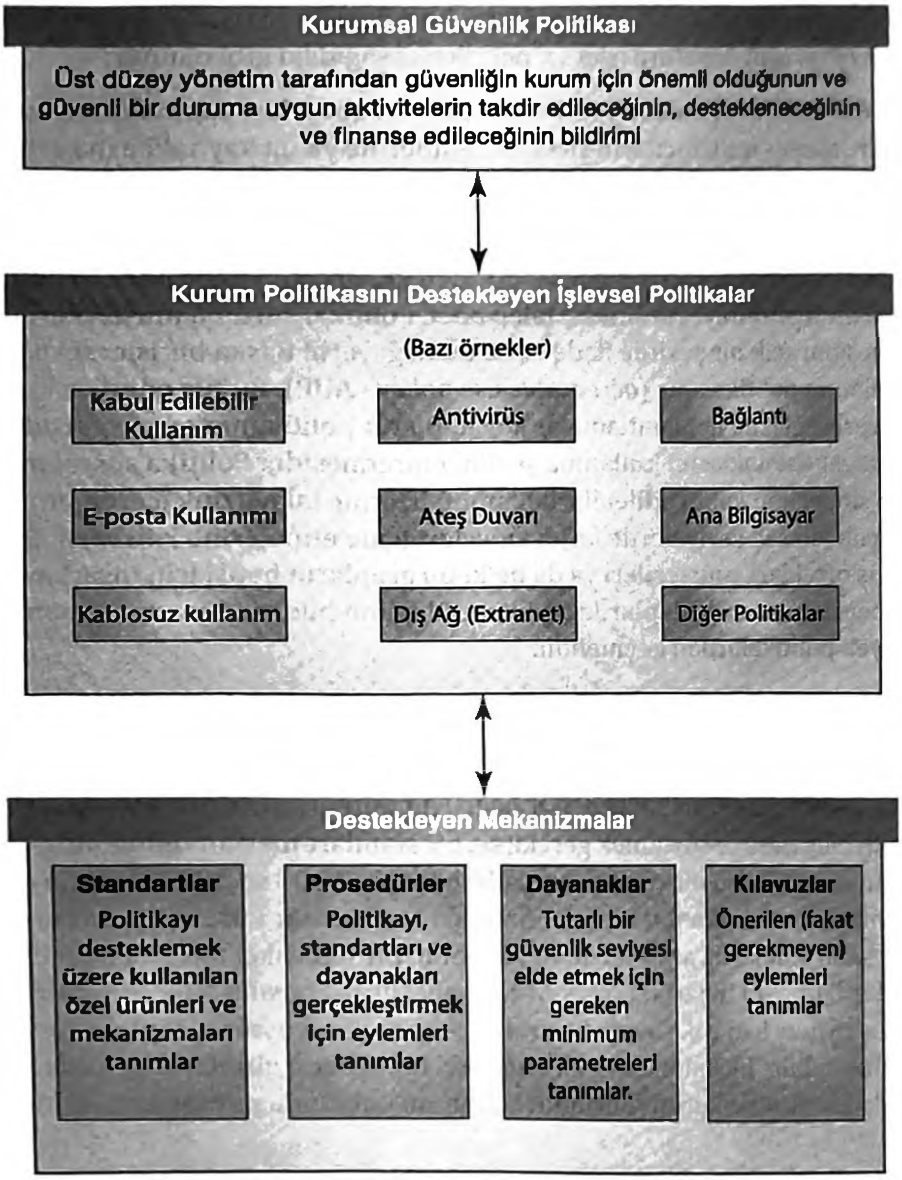
Yazılmış güvenlik politikaları yönetimin amaç ve hedeflerini belgeler. Şirketin güvenlik ihtiyaçlarını ve bu ihtiyaçları karşılamada politikaların yükümlülüğünü açıklar. Bir güvenlik politikası anahtar gerçeklerin kısa bir özeti olarak okunmalıdır. Eğer politika çok karmaşıksa yönetim onu benimsemede ve onaylamada sıkıntı yaşar.

Örneğin, iyi bir kurumsal güvenlik politikası basitçe "Güvenlik kurumumuzun geleceğine esastır" ya da "Ürünlerimizdeki güvenlik en önemli görevimizdir"de olduğu gibi okunabilir. Bu tip bildirim yöneticilere karar verme gereksinimlerinde kılavuzluk sağlar. Güvenlik politikası ayrıca kurumunuza kanunlar, yönetmelikler, bakım ve durum tespiti standartlarına ne kadar uyduğunun değerlendirilmesinde yardım eder. Güvenliğe ilişkin herhangi bir politikanın ana amacı riski azaltmaktır. Politika, kuruma çabalarını belli bir alana odaklamasında yardımcı olur.

Politikalar okunmazsa, kullanılabilir değilse, uygulatılmazsa ve güncellenmezse fazla değer taşımaz. Politikalarınızı her çalışanın erişebileceği bir yerde ilan edin. Örneğin, politikaları çoğunlukla dinlenme odalarında ilan edilmiş görürsünüz. Politikalar özellikle yeni kanun ve yönetmeliklere ayak uydurmada güncel olmalıdır. Çalışanlarınızla yılda en az bir defa onların en son



ŞEKİL 6-1
Güvenlik politikası ortamı.



ŞEKİL 6-2
Güvenlik politikası hiyerarşisi.

politikalar konusunda güncel olduğunu garanti etmek üzere bir araya gelmelisiniz. Her çalışan ile yapılan bu gözden geçirmenin kaydını muhafaza edin.

Bir güvenlik politikası tüm çalışanlara kurumun değer verdiği varlıkları ve prensipleri anlamada yardımcı olur. Personelinizin, net bir politika ile kurumun varlıklarına saygı göstermesi daha muhtemeldir. Personelin politikaları sadece kurumun ciddiye aldığı kadar ciddiye alacağını hatırlayın.

İşlevsel bir politika bir kurumun e-posta, uzaktan erişim ve internette dolaşma gibi belirli işlevsel alanlarda güvenliğe yönelik yönetim doğrultusunu beyan eder. Bu işlevsel politikalardan sorumlu olan bölümler onları yazar. Örneğin, insan kaynakları, bilişim teknolojisi, operasyonlar ve hizmetlerin her biri kendine özgü işlevsel politikaları üretecektir. İşlevsel bir politika "istek" ve "gereklilik" gibi güçlü bir dil kullanmalıdır. Birçok insan "gerekir" gibi bir terimi emir yerine

sadece bir tavsiye olarak değerlendirecektir. Zayıf sözcük seçimleri güçlü sözcükler kadar dikkat çekmeyecektir. Örneğin iyi bir erişim denetimi işlevsel politikası aşağıdaki gibi okunur:

> "Tüm yetkilendirilmiş kullanıcıların sadece yetkilendirildikleri görevleri yapmalarına izin verilmelidir. Yetkilendirilmemiş kullanıcıların şirket sistemlerine ya da kaynaklarına erişimi olmamalıdır."

İşlevsel politikanın bir örneği **mahremiyet politikasıdır.** Bir mahremiyet politikası kurumunuzun kişiler hakkındaki bilgileri nasıl topladığını, kullandığını ve ortadan kaldırdığını ifade eder. Kişisel bilgi veren birçok tüketici güçlü bir mahremiyet politikası talep eder. Politika, kuruma müşterilerin kişisel bilgilerini nasıl kullanacağını açık bir şekilde ifade etme olanağı verir. Başka bir işlevsel politika örneği, kabul edilebilir kullanım politikasıdır (*acceptable use policy* - AUP). Bu tür politika, kurumun varlıklarının kullanımına vereceği izne net kısıtlamalar koyar. Bu tür politikanın en yaygın odağı personelin kurumun bilgisayar kaynaklarını kullanma şeklini emretmesidir. Politika sosyal medyanın ya da hatta belirli web sitelerinin kabul edilebilir kullanımı üzerine kılavuzluk içerebilir.

Politikalar kurumların çok yüksek seviyelerde farklı amaçları ifade etmelerine izin verir. Bu amaçlar kendi çalışanları, iş ortakları, müşterileri ya da belki bu grupların hepsi için tasarlanmış olabilir. Kurumun tavrını belirler ve farklı alanlardaki yükümlülüğünü bildirir. Kurum personelinin tüm kararları yüksek seviyeli politikalardan geçmelidir.

Standartlar

Standartlar bir kurum genelinde güvenlik risklerini ele almak için kullanılan donanım ve yazılım çözümlerine dair emredilmiş gereksinimlerdir. Standartlar belirli bir antivirüs ürününe ya da parola üretim belirtecine işaret edebilir. Basitçe söylemek gerekirse, bir standart mevcut olduğunda, bu, kurumun bir politika hedefine ulaşmak için bir çözüm - ve sadece bu çözümü - seçtiği anlamına gelir.

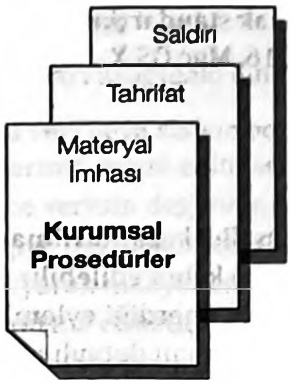
Standartların benimsenmesi birçok avantaj taşır. Çoğunlukla standartlar kuruma tasarruf ettirir, çünkü tedarikçilerle toplu satın alımlarda arabuluculuk yapabilir. Bir tedarikçi tek kullanıcı lisansını $29.95 satabilir. Bununla birlikte, aynı tedarikçi çok sayıda lisansı lisans başına $24.95 satabilir. Eğer o kurum bir standarda uymak için çok sayıda lisansa gereksinim duyuyorsa, toplu satın alım şirkete binlerce dolar kazandırabilir. Ek olarak, birçok tedarikçi toplu satın alımlarla ücretsiz eğitim sunar. Bu, kuruma zaman kazandırır ve kurumu ürünün kullanımı hakkında personelini eğitme sıkıntısından kurtarır.

Her durum için kendi standartlarınızı geliştirmek zorunda değilsiniz. Hükümet, sanayi veya diğer sektörlerin yarattığı standartları benimseyebilir ve kendi standardınız gibi kullanabilirsiniz. Standartlar ayrıca kurum genelinde ortak bir taban kurar. Bu bütün bölümlerin aynı görüşte olmasına yardım eder. Standartlar uyumlu kalması için her bölümün kılavuzunun olmasını garanti eder.

Standartların ana dezavantajı güvenlik açığıdır. Eğer seçilen ürün kusurlu ise, ürünün kurulumunun ardından tüm kurum risk altında olacaktır. Tedarikçi ürünü desteklemiyor ise ya da bakımı ve lisansı çok pahalı ise tek bir standart işe yaramayabilir. Standartlar için ürünleri değerlendirirken alternatifleri inceleyin. Yaptığınız her seçimin, bir sorun oluştuğunda bir destek garantisi ile geldiğinden emin olun.

Prosedürler

Prosedürler bir güvenlik gereksinimi, süreci ya da hedefini gerçekleştirmek üzere adım adım sistematik eylemlerdir. Eldeki en güçlü araçlardan biridir. İş yapış şeklinize dair dokümantasyon sağlar ve çok önemli bilgilerin çalışanlarınızın sadece kafasında kalmamasını garanti eder. Prosedürler



ŞEKİL 6-3
Sistematik eylemler

parolaların değiştirilmesi, vakalara yanıt verilmesi ve yedeklerin yaratılması gibi şeyleri kapsar. **ŞEKİL 6-3** birkaç örnek prosedür göstermektedir.

Prosedürler bir politika niyetinin uygulanmasını garanti eder. Bir görevi tamamlamak üzere bir adımlar serisini takip etmenizi gerektirir. Aşağıdakiler tüm prosedürler için doğrudur:

- Bir krizde hataları azaltırlar.
- Önemli adımları kaçırmamanızı garanti ederler.
- Süreç içerisinde güvence kontrolleri yürütmek için yer sağlarlar.
- Politikalar ve standartlar gibi zorunlu gereksinimlerdir.

Dayanaklar

Birçok durumda belirli tip bilgisayarlar ve cihazlar için temel konfigürasyonların tanımlanması faydalıdır. Örneğin, standart bir iş istasyonu için bileşenlerin ve konfigürasyon ayarlarının listelendiği bir dokümana sahip olmak bütün yeni iş istasyonlarının aynı olduğunu garanti etmeyi kolaylaştırır. Güvenlik personeli minimum güvenliği uyguladıklarını garanti etmek üzere çoğunlukla **dayanaklar (*baselines*)** olarak adlandırılan basit konfigürasyonlar yaratır. Dayanaklar sistemin çok sayıda uygulamaları ve farklı ürünler üzerinde minimum güvenlik seviyesinin var olduğundan emin olmaya yardım eden kıyaslama noktalarıdır. Dayanaklar mevcut sistemlerin minimumları karşılamaya devam ettiğini kıyaslamak için olduğu kadar yeni bilgisayarlar ya da cihazlar yapılandırmada da faydalıdır. **ŞEKİL 6-4** basit bir kurumsal dayanak konfigürasyonunu göstermektedir.

Dayanaklar kurum genelinde sabit bir güvenlik seviyesi yarattıklarından emin olmak için güvenlik cihazlarının nasıl uygulanacağını söyler. Farklı sistemlerin ya da platformların güvenlik problemlerini ele almakta farklı yolları vardır. Dayanaklar sistem yöneticilerine her platform için güvenliğin nasıl kurulacağını söyler. Bu, sabit bir güvenlik seviyesinin elde edilmesine yardım eder.

Dayanaklar farklı güvenlik ürünleri, işletim sistemleri ve uygulamalar yolu ile sunulan seçeneklerin çok iyi bir seviyelendiricisidir. Bu, daha fazla sayıda karma ürün güvenlik pazarına girdikçe daha önemli hale gelmektedir. Bu ürünler hizmetleri çok işlevli cihazlar ile birleştirir. Kurumlar



ŞEKİL 6-4
Dayanak kurumsal konfigürasyonu.

kullanımdaki her işletim sistemi için sıklıkla dayanak standartlar yaratır. Windows 8, Windows 10, Windows Server 2012 R2, Windows Server 2016, Mac OS X, Linux vb. için farklı dayanaklarınız olabilir.

Kılavuzlar

Kurumlar çoğunlukla bir güvenlik programına yapısallık kazandırılmasına yardım etmek için **kılavuzlar** kullanır. Kılavuzlar satın alma önerilerini ve kabul edilebilir ürün ve sistem kullanımlarını ana hatlarıyla belirler. Kılavuzlar basitçe kurumun önerdiği eylemlerdir. Bu kılavuzlar genellikle bir kurumun güvenlik programı tarafından tanımlanan detaylı rapor, en iyi uygulamalar ya da diğer formatlar şeklinde bulunur.

Kılavuzlarda kullandığınız dili dikkatlice seçmelisiniz. Birkaç yanlış sözcük bir kılavuzu şirket standardına dönüştürebilir. Örneğin, şirketin genel müdürü tarafından emredildiği şekliyle aşağıdaki kapsayıcı ifade örneğini düşünelim:

"Bu şirket ISO 27001 standardının önerilerini takip edecektir."

Bu ifade ISO 27001'i kurum içerisinde zorunlu kılar. Böyle cesur bir ifadede bulunmadan önce niyetinizin bu olduğundan emin olun.

Veri Sınıflandırma Standartları

Zorunlu erişim denetimi (*mandatory access control* - MAC) bir nesneye belirli bir sınıflandırmanın atanmasını içerir. Bilgiyi sınıflandırma çoğunlukla belirli tür veri için geçerli olan yönetmeliklere dayanır. Örnekler arasında kişisel bilginin, finansal bilginin ve sağlık bilgisinin korunması yer alır.

Veriyi sınıflandırmak sahibinin veya sahibinin atadığı birinin görevidir. Bu kişiyi *verinin sahibi* olarak adlandırabilirsiniz. Benzer bir terim olan *sistemin sahibi* altyapıyı yöneten kişi ya da gruplara işaret eder. Sistem sahipleri çoğunlukla değişim ya da konfigürasyon yönetimini denetler. Sistem sahipleri veri sınıflandırmayı *denetlemez*.

Erişim yetkisi (*clearance*) ve sınıflandırma (*classification*) arasındaki farkı anlamak önemlidir. Yetkilendirme *kullanıcılara* erişim yetkisi verir. Veri sahibi *veriyi* sınıflandırır. Sistemler erişim denetimini öznenin sınıflandırılan bir nesneye doğru erişim yetkisinin olduğunu tespit ederek uygular. İşletim sistemleri erişim kısıtlamalarını genellikle en düşük erişim hakkı (*least privilege*) ya da bilinmesi gereken (*need-to-know*) prensipleri doğrultusunda uygular.

Kurumlar bilginin sınıflandırmasında üç kriteri dikkate alır:

- **Değer**—Bilginin değerini çok sayıda farklı ölçüt ile tanımlayabilirsiniz: Kurum için değeri, rakipler için değeri, yerine koyma ya da kaybetme maliyeti ve kurumun itibarı için değeri.
- **Hassasiyet**—Hassasiyet bilginin bütünlüğüne veya ifşasına dair açıklığın kurum üzerindeki etkisinin ölçüsüdür. Kurumlar hassasiyeti çok sayıda yol ile ölçebilir, bunlar arasında mali yükümlülük ya da cezalar, itibar, güvenilirlik ya da pazar payının kaybedilmesi yer alır.
- **Kritiklik**—Kritiklik bilginin, kurumun misyonu için öneminin ölçüsüdür. Bilgi kaybedildiğinde kuruma ne olacaktır?

Bilgi Sınıflandırma Amaçları

Bilgiyi sınıflandırmanın amaçları aşağıdaki gibidir:

- Bilgi ifşa edildiğinde ya da veri veya sistem bozulduğunda işyerinin yüz yüze kalacağı riske dayalı bilgi koruma gereksinimlerinin tespit edilmesi
- Kurum politikası gereğince verinin değerinin tespit edilmesi
- Hassas ve/veya kritik bilgiye uygun koruma/denetimler sağlandığının garanti edilmesi
- Sadece hassas bilgiyi koruyarak maliyetlerin düşürülmesi
- Kurum genelinde sınıflandırma etiketlerinin standardize edilmesi
- Çalışanların ve diğer yetkili personelin koruma gereksinimleri konusunda uyarılması
- Gizlilik kanunu ve yönetmeliklerine uyulması

Kurumlar bilgiyi sınıflandırmaktan çok büyük fayda elde edebilirler:

- Hassas ya da kritik olarak sınıflandırılan veri, verinin sınıflandırmasına uygun bir koruma seviyesi alır.
- Kurum artırılmış denetimleri sadece en çok gereken yerlere uygulayarak maliyetleri için daha fazla değer elde eder. Örneğin, pahalı bir mücevher mağazasının, pahalı olmayan bir mücevher mağazasının ve bir taklit mücevher mağazasının fiziksel güvenlik maliyetlerini karşılaştırın. Bu mağazalardan hiçbiri bir diğerinin güvenlik sistemini kullanarak verimli bir şekilde işletilemeyecektir. Tüm kurumlar yüksek, orta ve düşük değerde veriye sahiptir. Her derecelendirme değeri farklı bir güvenlik seviyesini garanti eder.
- Uygun işaretlemeler sınıflandırılmış verinin koruma gereksiniminin personel tarafından tanınmasını sağlar.

Sınıflandırma Örnekleri

Amerikan hükümeti Sınıflandırılmamış (Undassified), Kısıtlanmış (Restricted), Özel/Gizli (Confidential) ve Gizli (Secret), Çok Gizli (Top Secret) derecelerini içeren hiyerarşik bir derecelendirme serisi kullanır. Özel sektör açık (düşük), özel (orta) ve gizli (yüksek) olmak üzere çeşitli kategoriler kullanır.

Hükümet derecelendirmeleri iyi bilinmektedir ve standardize edilmiştir. Şirketlere ilişkin derecelendirmeler daha az bilinmektedir ve standart değildir. Bu özel sektör için sorunlar yaratır. Örneğin, bir çalışan iş değiştirdiğinde yeni işveren "özele (*private*)" "gizlinin (*confidential*)" üzerinde değer biçebilir. Eski işinde işvereni "özele (*private*)" "gizlinin (*confidential*)" altında değer biçmiştir. Bu kafa karıştırıcıdır. Hatta aynı şirketin içerisinde olduğunda daha kafa karıştırıcıdır. Bir güvenlik uzmanının işinin bir parçası bu tutarsızlıkları tespit etmek ve düzeltmek üzere önerilerde bulunmaktır.

> **NOT**
>
> Bölümlere ayrılmış bilgi normal sınıflandırma sisteminin ötesinde özel yetki gerektiren verilerdir. Prosedürlerinizin bu tür bilgileri doğru şekilde ele almak için gerekli adımları içermesi önemlidir.

Sınıflandırma Prosedürleri

Sınıflandırma prosedürleri etkili veri sınıflandırması için çok önemlidir. Bu prosedürleri gerçekleştirmeden önce ilk olarak kapsamlarını ve süreçlerini belirlemeniz çok önemlidir. Sınıflandırma *kapsamı*, sınıflandırmanız gereken veriyi; sınıflandırma süreci ise sınıflandırılmış veriyi nasıl ele alacağınızı belirler. Tüm kaynaklarınızı uygun şekilde etiketlemeli ve işaretlemelisiniz. Güçlü prosedürlere bağlı kalarak, yaklaşmakta olan denetlemelere (*audit*) hazır olacaksınız.

Sınıflandırma planınızın kapsamını belirlemek üzere kurumunuzun verilerini değerlendirmek için bir iş etki analizi yapmalısınız. Bu verinizin değerini ve kurumunuzun işlemleri için kritikliğini belirler. Verinin değeri aşağıdakilere göre belirlenir:

- Ayrıcalıklı sahiplik (ticari sırlar)
- İşe yararlık (yararlılık)
- Veriyi yaratma ya da yeniden yaratma maliyeti
- Mali yükümlülük (koruma yönetmelikleri)
- Çevirilebilirlik/devredilebilirlik (finansal bilgi)
- İşlemsel etki (veri hazır değilse)
- Bilgiye yönelik tehditler
- Riskler

İş etki analizinin sonuçlarına bağlı olarak gerekli sınıflandırma seviye sayısını tespit etmelisiniz. Ayrıca her seviyenin başlığını kurum genelinde kullanım için standardize edeceksiniz. Bu bilgiyi başlangıç sınıflandırmasını atamaktan sorumlu bilgi sahiplerine gönderin. Bu sınıflandırıcılar ilgili yönetmelikleri, müşteri beklentilerini ve iş kaygılarını anlamalıdır. Hedef, sınıflandırılmış bilginin ele alınmasında tutarlı bir yaklaşımın kazanılmasıdır.

Sınıflandırıcılarınızın veriyi tutarlı bir şekilde ele alması için eğitim programı yaratmayı faydalı bulabilirsiniz. Sahip, sınıflandırmaların hala güncel olduğundan emin olmak üzere periyodik gözden geçirilmesinden de ayrıca sorumludur. Bu gözden geçirme kanun koyucular ya da düzenleyiciler yeni hükümet yönetmelikleri getirdiklerinde özellikle kritik olur. Son olarak, sahip artık özel olarak ele alınması gerekmeyen bilginin gizlilik sınıfının kaldırılmasından sorumludur. Hükümet kurumları sıklıkla belirli sayıda yıldan sonra bilginin otomatik olarak gizlilik sınıfını kaldırdığını ilan eder.

Hassas bilgi içeren tüm cihazları kurumun sınıflandırma politika ve prosedürlerine göre işaretlemelisiniz. Bu, personelin kullanılacak özel ele alma ölçütlerini bilmesinin tek yoludur. Manyetik ve optik cihazları hem elektronik olarak hem de basit etiketler ile etiketlemelisiniz. Basılı haldeki dokümanlar, dışında kapak üzerinde ve içinde sayfalarda etiketler gerektirir.

Güvence

İç ve dış denetçiler kurumun bilgi sınıflandırma durumunu düzenli denetleme sürecinin bir bileşeni olarak gözden geçirmelidirler. Onlar ayrıca sınıflandırma politika ve prosedürlerine uygunluk seviyesini de değerlendirmelidirler. Bu, kurumun tüm parçalarının sürece bağlılığını garanti eder. Bu gözden geçirme bilginin gereğinden fazla sınıflandırılmış olduğu durumları ortaya çıkarabilir.

Bilgi güvenliği personeli iş istasyonlarını ve kullanıcıların gizli materyalleri korumasız bırakabilecekleri diğer alanları düzenli olarak ziyaret etmelidir. Onlar ayrıca ihlaller gerçekleştiğinde uygun raporların müdürlere ve yöneticilere teslim edilmesini garanti etmelidirler. İdeal olarak çalışan performans değerlendirmeleri çalışanların bilgiyi kötüye kullandığı durumları içermelidir. Bu, personelin bu sürecin önemini anlamasına yardımcı olur. Kurum, kullanıcıların *hiçbir zaman* hassas bilgiyi başıboş bir masada ya da iş istasyonunda ekranda açık bir görüntüde bırakmamalarını ifade eden **temiz masa/temiz ekran politikasını** uygulamayı düşünmelidir.

Konfigürasyon Yönetimi

Ağa bağlı bir bilgisayar ortamındaki herhangi bir bileşenin uzun süre değişmez kalması olağan dışıdır. Kurumlar yaygın olarak sistem yaşam döngüsü boyunca otomatik bir sistemin donanımına, yazılımına, üretici yazılımına, dokümantasyonuna, test planlarına ve test dokümantasyonuna değişiklikler yapar. Tüm konfigürasyon değişikliklerinin sadece denetimli bir süreç içerisinde olması önemlidir. Denetimsiz konfigürasyon değişiklikleri sıklıkla anlaşmazlıklar ve hatta yeni güvenlik açıkları ile sonuçlanır. Bilgisayar ve cihaz konfigürasyonlarına yapılan tüm değişikliklerin yönetim sürecine *konfigürasyon yönetimi* denir.

Bir güvenlik uzmanının perspektifinden konfigürasyon yönetimi bir değişikliğin güvenlik üzerindeki olası etkisini değerlendirir. Sistemin, uygulamanın ya da dokümantasyonun gizliliğini, bütünlüğünü veya kullanılabilirliğini etkileyecek midir? Bir güvenlik uzmanı olarak iki kat işiniz vardır:

- Tüm sistem değişikliklerini uygun şekilde gözden geçirdiğinizden emin olun.
- Konfigürasyondaki değişikliğin güvenlik için istenmeyen sonuçlara neden olmayacağından emin olun.

Değişikliğin ortamınızı beklendiği şekilde etkilediğinden ve ortamınızın yetki verilmiş şekliyle işletildiğinden emin olmak için tüm değişiklikleri denetleyin.

Donanım Envanteri ve Konfigürasyon Çizelgesi

Birçok kurum kendisine kimin sahipliğinde, hangi bölümlerin ya da sistemlerin kullanımında neyi olduğunu söyleyen bir donanım envanterinden yoksundur. Bu bir güvenlik programında ciddi bir boşluktur. Bir yangın, ekipman hatası ya da hırsızlık durumunda bu dokümantasyon eksikliği yanıtı yavaşlatır ve işlemsel kaybı genişletir. Ayrıca, düzgün konfigürasyon yönetimini imkansız değilse de son derece güç hale getirir. Etkilenen her cihazı bulamıyor, güncelleyemiyor ve test edemiyorsanız, yeni bir yamayı, servis paketini ya da sürümü yayma kararı karmaşık olacaktır.

Donanım Konfigürasyon Çizelgesi

Donanım bileşenlerinin güncel bir konfigürasyon haritasına ya da planına sahip olmalısınız. Bu, tüm sistemleri dayanağa göre yapılandırdığınızdan emin olmanıza yardım eder. Ayrıca, bir sistem ya da ağ üzerinde gerçekleştirilen işin uygun şekilde gözden geçirilmesini de garanti eder, böylece herhangi bir güvenlik özelliğini atlamadan doğru değişiklikler yapabilirsiniz. Bir donanım konfigürasyon çizelgesi aşağıdakileri içermelidir:

- Ağın tamamlanmış diyagramı, bir değişikliğin sırasını planlamanıza ve oluşturabileceği hafif dalgalanmaları görmenize yardım eder.
- Bütün yazılım konfigürasyonlarını kopyalar, böylece bir cihaz için planlanan değişiklik ve güncellemeleri diğer cihazlar üzerindeki etkileri bakımından inceleyebilirsiniz. Bu konfigürasyonlar yönlendirici, anahtar ve ateş duvarı konfigürasyonları gibi öğeleri içermelidir.

Yama ve Servis Paketi Yönetimi

Düzenli olarak mevcut tedarikçi güncellemelerini ve servis paketlerini aramaya çalışmalısınız. Bu süreç eğer farklı satıcılardan birçok tipte yazılım ve donanımınız varsa karışık olabilir. Buna rağmen bilinen bütün güvenlik açıklarının ele alınması gereklidir. Yamaların tüm bilgisayarlara ve cihazlara

sistem kesintisine neden olmadan taşınmasından emin olmak için kurumun bir yama yönetim sistemine sahip olması gerekir. Her yamayı taşımadan önce diğer sistemleri ya da fonksiyonları devre dışı bırakmamasından emin olmak için test etmelisiniz.

Değişiklik Yönetim Süreci

Değişiklik ve konfigürasyon denetimini bir aktivite ikilisi olarak tartışmak yaygındır fakat gerçekte onlar bir spektrumun iki ucudur. Karışıklık elbette belirli bir aktivitenin birinden diğerine geçmesinde yatar. İkisi arasında keskin bir çizgi çizmek güçtür, çünkü farklı kurumların farklı karmaşıklıkları çizgiyi farklı yerlerde çizer:

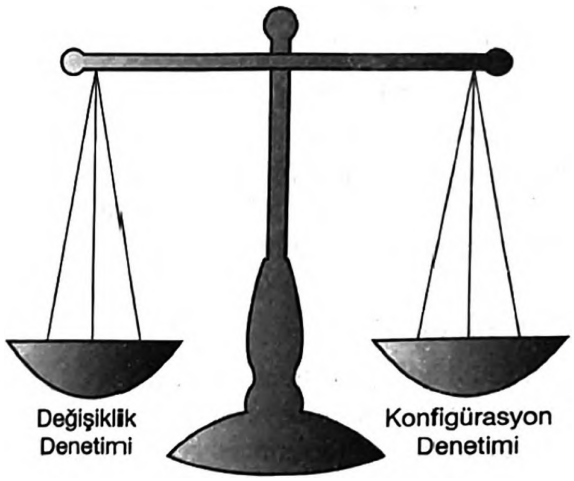
- **Konfigürasyon denetimi** bir sistem cihazı için dayanak (*baseline*) ayarların yönetimidir. Dayanak ayarlar güvenlik gereksinimlerini karşılamalıdır. Onları ancak ön onay ile ve dikkatli bir şekilde gerçekleştirmeniz gerekir.
- **Değişiklik denetimi** konfigürasyon üzerindeki değişikliklerin yönetimidir. Yönetilmeyen değişiklikler güvenlik operasyonlarını ve denetimlerini etkileyebileceğinden risk oluşturur. Uygun olmayan bir değişiklik, sistem ya da ekipmanı da devre dışı bırakabilir. Değişiklik denetimi üretim sistemine yapılan değişikliklerin test edilmiş, belgelenmiş ve onaylanmış olduğunu garanti eder. Değişikliğin kendisi değişikliği doğru yaptığınızı ve yönetime raporladığınızı garanti eden bir değişiklik denetim sürecini takip etmelidir.

ŞEKİL 6-5 değişiklik ve konfigürasyon denetimi arasındaki dengeyi göstermektedir.

Değişiklik Denetim Yönetimi

Değişiklik denetim yönetimi, değişiklik denetimi için etkilenen bütün bölümlerin dahil olduğu planlı bir yaklaşım geliştirir. Amaç, değişime dahil olan bütün kişilere faydayı maksimize etmek ve başarısızlık riskini minimize etmektir.

Etkili olması için değişiklik yönetimi çok disiplinli olmalıdır ve kurumun bütün yönlerine dokunmalıdır. Bununla birlikte, bir kurum tüm esnekliğini kaybedecek kadar kısıtlanmamalıdır. Değişiklik yönetimi kurumların yeni teknolojileri, ilerlemeleri ve değişiklikleri benimsemesine izin vermelidir.



ŞEKİL 6-5

Değişiklik ve konfigürasyon denetiminin birbirini tamamlayan dengesi.

Değişiklik yönetimi bilgi sistemleri üst yöneticisi ya da BT direktörü ve iş bilişim güvenlik yöneticisi tarafından onaylanmış yazılı bir politika gerektirir. Politika, değişiklik yönetimine ilişkin bütün rolleri, sorumlulukları ve prosedürleri tanımlamalıdır. Hatırlanması gereken önemli şeyler aşağıdadır:

- Değişiklik yönetim prosedürlerini ve standartlarını etkili bir şekilde aktarmalısınız. Onlar, politikanın desteğinde işletme genelinde kullanacağınız teknikleri ve teknolojileri tanımlamalıdır.
- Değişiklik yönetimi reaktif ya da proaktif olabilir. **Reaktif değişiklik yönetimi** ile yönetim iş ortamındaki değişikliklere yanıt verir. Değişikliğin kaynağı dışsaldır. Bazı örnekler arasında yönetmelikler, müşteri beklentileri ve tedarik zinciri yer alır. **Proaktif değişiklik yönetimi** ile yönetim istenilen bir hedefi elde etmek için değişimi başlatır. Bu durumda değişikliğin kaynağı yeni bir teknolojinin benimsenmesi gibi içseldir.
- Kurumunuz değişiklik yönetimini farklı yollarla yürütebilir. Sürekli olarak, düzenli bir plan temelinde, sürüm temelinde ya da lüzum gördüğünüzde programdan programa gerçekleşebilir.

Potansiyel Güvenlik Etkisi İçin Değişikliklerin Gözden Geçirilmesi

Değişim bir işletme için risk yaratır. Yerleşmiş güvenlik özelliklerini atlatabilir ve kesinti ya da sistem arızası ile sonuçlanabilir. Yeni sistemleri nasıl kullanacaklarının öğrenilmesi için çalışanlara yoğun yeniden eğitim gerektirebilir. İçerdiği risk nedeniyle değişiklik denetim sürecine güvenlik personelini dahil etmelisiniz.

Resmi değişim denetim süreci BT sistemlerinin bütünlüğünü korumalı ve üretim ortamındaki tüm değişikliklerin uygun şekilde test edilmiş, planlanmış ve bildirilmiş olduğunu garanti etmelidir. Değişim denetim komitesinin üyeleri tahminlemek, planlamak, gözden geçirmek ve kurumun üretim ortamını hazırlamak için toplantılara ve forumlara katılmalıdır.

Değişiklik Denetim Komiteleri

Bir değişiklik yönetim komitesine bir üst yönetici ya da işletme süreç sahibi liderlik etmelidir. Bu komite, sistemlere ve ağlara önerilen tüm değişiklikleri denetlemelidir. Komite değişiklikleri ve değişiklik gerçekleştirme planını onaylar. Böylelikle bir sistem, uygulama ya da ağa uygun bir gözden geçirme, kaynak ve dokümantasyon olmadan değişiklik yapamazsınız.

BT ile işbirliği içerisinde değişiklik denetleme komitesi (bazı durumlarda *değişiklik denetleme kurulu* olarak adlandırılır) bilişim kaynaklarını ve uygulamalar ve veritabanları içerisindeki veriyi korumak üzere gözetim sağlar. Değişim sürecinin bir parçası olarak asli üyeler BT kurumlarındaki mevkidaşları ile yaklaşan planları gözden geçirir ve bütün değişiklikleri uygun şekilde değerlendirdiğinden emin olur. Ayrıca, gerekli güvenlik kontrollerinin uygulanıp değerlendirildiğini garanti ederler. Bulgularını kurumun bütün parçalarına iletirler.

Özetle, değişiklik denetim komitesinin ana hedefleri tüm değişikliklerin aşağıdaki gibi olduğunu garanti etmektir:

- Uygun şekilde test edilmiş
- Yetkilendirilmiş

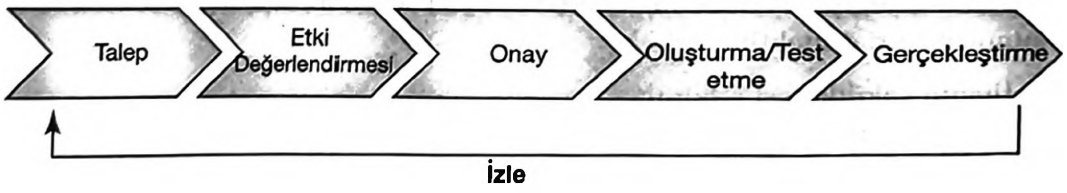
- Planlanmış
- Bildirilmiş
- Belgelenmiş

Sıkı değişiklik denetimi uyguladığınızda bir üretim problemine neden olmuş olması muhtemel en son değişiklikleri tespit etmek kolaylaşır. Bu, problem çözümleme sürecini kolaylaştırır ve ortamınızı daha güvenli hale getirir.

Değişiklik Denetim Prosedürleri

Değişiklik denetim prosedürleri bir değişikliğin doğru adımları takip etmeden gerçekleşmemesini garanti eder. Bu, bir sisteme yetkilendirilmemiş değişikliklerin gizlice sokulmasına izin veren kapsam genişlemesi (*scope creep*) gibi problemlerden kaçınmanıza yardım eder. Ayrıca, gözetim eksikliği, test eksikliği ya da uygun yetkilendirme olmadan yapılan değişikliklerden kaynaklanan problemlerden de kaçınmanıza yardım eder. **ŞEKİL 6-6** değişiklik denetim prosedürlerinin sırasını göstermektedir.

1. **İstek**—İstek aşamasında önerilen tüm değişiklikleri yazılı olarak tanımlamalı ve değişiklik talebini değişiklik denetim komitesine gözden geçirmesi için teslim etmelisiniz. Onay almadan sisteme hiçbir zaman değişiklik yapmamalısınız.
2. **Etki değerlendirmesi**—Etki değerlendirme aşaması değişikliğin bütçe, kaynaklar ve sistemin ya da projenin güvenliği üzerindeki etkisini değerlendirir.
3. **Onay**—Onay (veya bazı durumlarda onaylamama) aşaması değişiklik değişiklik denetim komitesi tarafından değişikliğin resmi olarak incelenmesi ve kabul edilmesidir (veya reddesilmesi).
4. **Oluşturma/Test etme**—Oluştur/Test et aşaması kabul edilen değişiklik dokümanına göre değişikliğin esas geliştirimi ya da oluşturulmasıdır. Sonrasında değişikliği diğer sistemler ya da bileşenler için beklenmeyen problemlere neden olmamasını garanti etmek üzere test etmelisiniz. Test etme regresyon testini ve değiştirilmiş ürünün ayrıntılı bir gözden geçirmesini içerebilir.
5. **Gerçekleştirme**—Değişikliği test edip sürüm için kabul ettiğinizde kurulum sürecini planlayabilirsiniz. Bu, yeterli bir görevler ayrılığının (*separation of duties*) hiçbir kişinin uygun gözden geçirme ve gözetim olmadan değişiklik yapamayacağını garanti ettiği yerdir. En son engel, değişikliği başarıyla gerçekleştirdiğinizin yönetime bildirilmesidir.
6. **İzleme**—Bu aşamada tüm sistemleri sistem, program, ağ ve diğer kaynakların doğru çalıştığından emin olmak üzere izlemelisiniz. Herhangi bir kullanıcı problemini ya da talebi kurumunuzun problem çözüm prosedürlerini kullanarak ele almalısınız. İzleme ileriki değişiklikler için gereksinimi tespit edebilir. Bu, değişiklik denetim sürecini yeniden başlatır.



ŞEKİL 6-6

Değişiklik denetim prosedürleri.

Değişiklik Denetim Problemleri

Sıkı değişiklik denetim prosedürleri problemleri tespit etmeye ve gerektiği takdirde kurtarma yolları sağlamaya yönelik bileşenleri içerir. Başarılı bir değişiklik denetim programı değişiklik denetim sürecinin kalitesini garanti etmek üzere aşağıdaki elemanları içermelidir:

- **Meslektaş denetimi**—Bu bir eşgörevlinin ya da başka bir uzmanın yürürlüğe koymanızdan önce tüm değişiklikleri tekrar gözden geçirmesini garanti eder. Eşgörevliler çoğunlukla test aşamasına kalmadan önce problemleri yakalayabilirler.
- **Vazgeçilen planlar**—Bu, eğer değişiklik düzgün çalışmıyorsa sistemi bilinen iyi bir durumuna geri yüklemek üzere bir planın varlığını garanti eder. En iyi denetim prosedürlerine rağmen yanlışlıkla istenmeyen etkilere sahip değişiklikler yayınlayabilirsiniz. Bozucu bir değişiklikten vazgeçmeyi ya da değişikliği geri almayı bilmelisiniz.
- **Dokümantasyon**—Dokümantasyonu gerçek sistem tasarımını yansıtması için güncel tutmalısınız. Alan dışında yedek kopyalar da tutmalısınız. Dokümantasyon sistemin nasıl işlemesi gerektiğinin anlaşılması için gereklidir.

Uygulama Yazılımı Güvenliği

Kritik ilgi alanlarından biri uygulama yazılımıdır. Saldırganlar yazılım geliştirme sürecinin karmaşıklığını ve çoğunlukla sürecin sonucunun zayıflıklar içeren bir uygulama olduğunu bilirler. Güvenli yazılımın yazılması güç olabilir. Yazılımın sadece yapması gerekenleri yaptığını garanti edecek yapısal bir süreç kadar sürecin her aşamasında güvenliğe özen gösterilmesini gerektirir. Sistem ve yazılım geliştirme sürecini tanımlayan ve denetleyen farklı popüler yöntemler mevcuttur. Yazılım geliştirme sürecini anlamak çok az sayıda zayıflığa sahip yazılım geliştirmek için önemlidir. En popüler yöntemlerin ikisine aşina olmalısınız, **sistem yaşam döngüsü (*system life cycle* - SLC)** ve **sistem geliştirme yaşam döngüsü (*system development life cycle* - SDLC)**. Bu süreçlerdeki adımlar, SLC'nin operasyonları ve yok etmeyi (*disposal*) içermesi ve SDLC'nin üretime geçiş ile sonlanması dışında çok benzerdir.

Bazı kurumlar için bakım ve yeni geliştirmenin geliştiriciler tarafından yapılması onları SDLC'nin bir parçası yapar. Diğerleri için, özelleşmiş bakım takımlarının bakım ve geliştirmeyi yapması onları SLC'nin bir parçası yapar. Giderek daha çok kurum SDLC terimini uygulama ve sistem yazılımı için değişim ve bakım sürecinin tamamı olarak tanımlar.

Sistem Yaşam Döngüsü

Bu bölüm SLC'de kullanılan ortak adımları kapsar. Güvenlik uzmanının her bir adıma daha fazla dahil olabilmesi, gereken güvenliğin sisteme başlangıçtan yerleştirilmesini daha mümkün kılacaktır. SLC -ve güvenliği başlangıçta oluşturma- için temel gerekçelendirme maliyetin düşürülmesi ya da maliyetten kaçınılmasıdır:

- Daha az sayıda yama ve düzeltme dağıtmanız gerekeceğinden ticari yazılım ürünlerinin müşterileri daha düşük maliyetler görecektir. Ek olarak, saldırganların yazılımda bulup kullandığı zayıflıklar nedeniyle daha az sayıda kayıp olacaktır.
- Ticari yazılım tedarikçileri daha az sayıda destek personeli ve daha düşük garanti ve ürün bakım maliyetine gereksinim duyacağından daha düşük maliyetler görecektir.

SLC'de kullanılan ortak adımlar aşağıdaki gibidir:

1. **Proje başlatma ve planlama**—Başarılı bir projenin ilk gereksinimlerinden biri gereken tüm kaynakların hazır olmasıdır. Gereksinim duyacağınız kaynaklar dikkate almanız ve projeye entegre etmeniz gereken alanları temsil etmelidir. Rolünüz projeye en başından itibaren güvenliği yerleştirmek konusunda tavsiye sağlamaktır. Bu, proje bütçelerini, sistem tasarımını, bakımı ve proje zaman çizelgesini içerir. Burada ilk olarak tehditleri, güvenlik açıklarını, riskleri ve kontrolleri ele almalısınız.
2. **İşlevsel gereksinimler ve tanım**—Bu "ne yapmalı?" aşamasıdır. Gereksinimleri her zaman olumlu sözcükleri kullanarak ifade edin: Program bazı veriyi işlemeli ya da bazı fonksiyonu yerine getirmelidir. Veri, spesifikasyonları karşılamazsa programın ne yapması gerektiği veya yapacağı hakkında düşünmeniz gerekecektir. Yazılım beklenmeyen bir girdi aldığında ne olur? Çok fazla karakter mi var? Eksik alan var mı? Kullanıcılar gecikmeli iletimler mi görüyor? Bu faktörleri dikkate almadaki başarısızlık çok sayıda güvenlik aksilikleri yaratır.
3. **Sistem tasarım spesifikasyonu**—Bu aşamada proje fonksiyonlara ve modüllere ayrılır. Bunun için sistemin üzerinde koşacağı donanım tipini göz önünde bulundurmalısınız. Buradaki güvenlik problemleri donanımın ve ağın fiziksel güvenliğini içerir. Güvenlik ayrıca olası tüm platformları hesaba katmalıdır. Örneğin, projenin Linux ya da Windows ile sınırlı olduğunu söylemek yeterli değildir. Her platform çok çeşitli versiyona yer verir ve çevre birimleri, yonga seti ve sürücülerin neredeyse sonsuz kombinasyonu üzerinde çalışır.
4. **Oluştur (geliştir) ve belgele**—Kodlama standartları standart kütüphanelerin fonksiyon çağrılarını içermelidir. Ayrıca kriptografi, hashing ve erişim denetimi gibi öğeler için endüstri standardı çözümleri de içermelidir. Geliştirilmekte olan kodun güvenliğini sağlamanız gerekir, öyle ki koda sadece geliştiricilerin erişiminin olması ve dolayısıyla sadece bilinmesi gereken (*need-to-know*) temelinde erişim izni vermelisiniz. Geliştiriciler bile sadece görmeleri gereken parçalara erişim sahibi olmalıdır. Kopyaları, etrafta basılı ya da CD'ler veya USB bellek çubukları gibi bilgisayarca okunur formda bırakmamalısınız.
5. **Kabul testi**—Fonksiyonel (işlevsel) tasarım aşamasında bir test planı yaratmalısınız. Bu plan yeni programların gerekli güvenliği ve uygulanabildiği yerde gizliliği sağladığından emin olmak için test etmeyi içerir. Testlerden sorumlu olan kişiler geliştiriciler olmamalıdır. Ek olarak, geliştiriciler için gecikmiş dağıtım tarihleri test için ayrılan zamanı etkilememelidir.
6. **Gerçekleştirme (üretime geçiş)**—Bu geçiş sırasında geliştiriciler kullanıcılara ve yardım masası personeline eğitim ve desteğin verilmesi üzerine çalışıyor olacaktır. Her iki gruba da güvenlik özelliklerinin dikkatli bir şekilde açıklanması gerekir. Bazı kurumlarda, geliştiriciler kodun bakım personeline devrinin yönetimine de yardım edecektir.
7. **Operasyonlar ve bakım**—Sistem ile problemler olduğunda; bakım, operasyonlar ve yardım masası personelinin ilk bilenler olacağı muhtemeldir. Gelen problemleri izlemeleri ve sonuçların yönetime raporlanmasına hazır olmaları gerekir. Bu prosedür değişiklik yönetim sürecini çalıştırır. Bu personel, değişiklik talebi, yazılım arızası ve güvenlik zayıflığı ya da açıklığı arasındaki farkları anlaması için eğitime gereksinim duyar. Ek olarak, bu olayların her birinin nasıl ele alınması gerektiğini bilmelidir.

8. **Yok etme (*Disposal*)**—Zamanla, bileşen parçaları ömürlerinin sonuna varacaktır. Yedek sistemi yükseltmeniz ya da küçük olanı yenisi ile değiştirmek için daha büyük bir disk edinmeniz gerekecektir. Araçları sterilize etmek ve daha sonra maliyet etkin bir şekilde yok etmek için prosedürlere sahip olduğunuza emin olmalısınız. Geçmişte, kurumlar bir diski silip yeniden satıyor olurlardı. Bugün, kullanılmış küçük bir diskin değeri çoğunlukla onu DBAN gibi bir araç ile güvenli bir şekilde silme ve daha sonra basitçe diski ortadan kaldırma maliyetinden düşüktür.

Uygulama Yazılımının Test Edilmesi

Güvenlik uzmanları çoğunlukla yeni sistemlerin test edilmesine ya da varolan sistemlerin yükseltilmesine yardım ederler. Bu testler beklenen ve beklenmeyen tüm eylemleri test etmenizi ve hataları doğru bir şekilde ele almanızı garanti etmek için yeterince tam olmalıdır. Testleri sistem üzerindeki maksimum yükü, işlem hacmini, bellek tahsisini, ağ bant genişliğini ve yanıtlama süresini içerecek şekilde test etmek için de uygulamalısınız. Testlerde üretim verisini ya da hassas veriyi kullanırsanız bu veriyi güvenli tutmak için adımlar attığınızdan emin olun.

Girdi doğrulama saldırıları (*input validation attacks*) çok yaygın olduğundan güvenlik personeliniz testlerin girdi güvenlik açıklarını yakaladığından emin olmak için yazılım test personeli ile birlikte çalışmalıdır. Girdi güvenlik açıkları için test tiplerinden biri **fuzzing** olarak adlandırılır. Fuzzing, yazılımın beklenmeyen veriyi nasıl ele aldığının görülmesi için yazılıma rastgele girdi sağlama uygulamasıdır. Fuzzing, test görevlisinin kötü girdiyi düşünmeye çalışması yerine, girdi güvenlik açıklarının tespit edilmesine yardım edebilir.

Sistemlerin Temin Edilmesi

Yeni güvenlik açıklarının bir ortamda ilerleme yollarından biri istenmeyen yan etkilere neden olan bir değişim sonucudur. Ortamınıza yapılan herhangi bir değişikliği yeni güvenlik açıkları ortaya çıkarmadığından emin olmak için iyice değerlendirmelisiniz. Bu değerlendirmeyi yeni donanım ve yazılım için de yapın. Yeni ekipman temini güvenlik uzmanının çok önemli bir rolüdür fakat bu süreç iyi idare edilmezse toplam güvenliği düşürebilir. Yeni ekipman temin etmeniz gerektiğinde hangi ürünlerin gereksinimlerinizi karşılayacağını dikkatlice değerlendirmelisiniz. Yeni ekipmanın ortamınızda yeni güvenlik açıkları ortaya çıkarmadığından emin olmak için aşağıdakileri yapmalısınız:

- Mevcut farklı çözümleri değerlendirin.
- Tedarikçileri bakım, destek ve eğitim açısından değerlendirin.
- Değerlendirme sürecini basitleştirdiğinizden emin olmak için Ortak Kriterleri kullanın.
- Tedarikçi sözleşmelerini ve hizmet seviyesi sözleşmeleri (SLA) izleyin.
- Ekipmanı doğru bir şekilde kurun ve proje sonunda resmen kabul edin.
- Adil bir satın alma sürecini garanti etmek için kurumun temin prosedürlerini takip edin.
- Yaşam süresinin sonuna varan ekipmanı tespit etmek için sistemleri ve ekipmanı izleyin böylece yenisiyle değiştirme planlamasını yapabilirsiniz.

Ortak Kriterler

Yeni ekipman temini güvenlik açıklarına yol açabileceğinden sürecin resmileştirilmesi anlamlıdır. Sistemleri ve ekipmanı değerlendirmek için resmi bir yaklaşıma duyulan ihtiyaç, birbirinden farklı standart kümelerine sebep olmuştur. Amerikan hükümeti doküman kapaklarındaki koyu renkler

nedeniyle Gökkuşağı Serisi (*Rainbow Series*) olarak bilinen bilgisayar güvenliği standartları serisi yaratmıştır. *Kırmızı Kitap (Red Book)* güvenilir bir ağ altyapısının (*trusted network infrastructure* - TNI) bileşenlerini tanımlar. *Turuncu Kitap (Orange Book)* derecelendirilmiş bir sistemde erişim denetiminin ve gizliliğin sürdürülmesi hakkında konuşur. Her ikisi de bir değerlendirme seviyeleri serisi (C2, B3, vb.) kullanır ve tedarikçilerin ürünleri bu seviyelerle karşılaştırılarak değerlendirilir. Gökkuşağı Serisi'nin geliştiricileri resmi olarak TCSEC olarak adlandırılır.

Diğer hükümetler kendi eş değerlerini yaratmıştır. Bazıları TCSEC ile başlamış ve değişiklikler yapmıştır. Sonunda bütün bunlar ITSEC olarak birleşmiştir. Birleşik Devletler, Birleşik Krallık, Kanada, Almanya, Fransa ve Hollanda hükümetleri ITSEC'i bir başlangıç noktası olarak kullanmıştır. Sonrasında Ortak Kriterler denilen yeni bir temin standardı geliştirmişlerdir.

Ortak Kriterler 1'den (en düşük) 7'ye (en yüksek) numaralandırılan gittikçe zorlaşan değerlendirme güvence seviyeleri (*evaluation assurance level* - EAL) serisidir. Değerlendirme laboratuvarları tüm dünyaya dağıtılmıştır. Bir endüstri içerisindeki (örneğin, ateş duvarı tedarikçileri) öncü tedarikçiler toplu olarak standart, ideal ve mükemmel bir çözüm yaratır. Herhangi bir tedarikçi ürününü bir standart karşısında değerlendirtebilir. Bir EAL derecesi tedarikçinin talebinin tanımlı bir test seviyesinde toplu standarda uyduğunu garanti eder. Ürünün dokümantasyonu, geliştirimi ve başarımının tümü değerlendirme taleplerine uymalıdır.

Veri Politikaları

Her veri belli bir noktada yararlılığının sonuna ulaşır. Veriye artık gereksinim duymadığınızda ya da veriyi kullanamadığınızda ne yaparsınız? En iyi eylem basitçe veri politikalarınızdaki kılavuzu takip etmektir. Elbette bu halihazırda veri politikalarına sahip olmanız gerektiği anlamına gelir. Veri yönetimini kapsayan politikalar verinizin yaşam döngüsü boyunca geçişlerini de kapsamalıdır. Sıkı bir veri politikası ortadan kaldırma kadar saklama ve depolamayı da kapsayan bölümler ya da hatta tam dokümanlar içermelidir.

Veri politikalarının saklama ve depolama bölümleri farklı tiplerdeki verinin ne kadar süre tutulacağını belirtmelidir. Bazı veri öğelerinin diğerlerine göre yararlılık ömürleri daha uzundur. Araştırma amaçlı tarihsel veri tutmanız gerekiyorsa politikanız nasıl depolanması gerektiğinden bahsetmelidir. Güvenlik politikanız depolanan veriyi de kapsayacak şekilde genişletilmelidir.

Fakat veriye artık gereksinim duymadığınızda ne yaparsınız? Aracı yeniden kullanıma hazır hale getirmek için verinin üzerine yazabilirsiniz (*silme (wiping)* denilen süreç) ya da aracı imha edebilirsiniz. Seçiminiz aracın yararlılığına ve verinin hassasiyetine bağlıdır. Aşırı hassas veri için veriyi silmek ve silinen verinin tamamını ya da parçasını kurtarabilecek birinin ellerinden uzak tutmak için aracı imha etmeniz daha güvenlidir.

Ekipmanın ortadan kaldırılması gerektiğinde herhangi gizli bir veriyi açığa çıkarmamak için güvenli bir şekilde ortadan kaldırdığınızdan emin olmalısınız. Sizin için aşağıdakileri içeren birçok seçenek mevcuttur:

- **Digavsing/Mıknatıslamanın giderilmesi**—Manyetik araçlara güçlü bir manyetik kuvvetin uygulanması bütün elektronikleri genellikle kullanılmaz hale getirir.
- **Fiziksel imha**—Verinin saklandığı araçların fiziksel olarak imha edilmesi herhangi gizli bir materyali yok etmenizi garanti eder.
- **Verinin üzerine yazmak**—Bu seçenek araçları ortadan kaldırmaz. Burada gerçek araç imhasına, uygulanabilir bir alternatif olarak dahil edilmiştir. Arka arkaya araçtaki verinin üzerine yazmak verinin kurtarılabilme şansını azaltır. Bununla birlikte, kararlı bir kişinin silinen verinin bir kısmını kurtarabilme ihtimali kalmaya devam eder.

Teknik TAVSİYE

Ortak kriter için resmi isim ISO/IEC 15408'dir.

Sertifikasyon ve Akreditasyon

Temin ve yok etme arasında bilişim ortamınızdaki bileşenlerin gereksinimleriniz için yeterli olduğunu garanti etmeniz gerekecektir. **Sertifikasyon** belirtilen güvenlik gereksinimlerini karşıladığından emin olmak için bir sistemin yaşam döngüsü boyunca gözden geçirilme sürecidir. **Akreditasyon** yetkilendiren görevli tarafından sistemin gerçekleştirim riskinin kabul edildiği resmi anlaşmadır. Süreç aşağıdaki oyuncuları içerir:

- **Yetkilendiren görevli**—Sertifikasyon raporunu gözden geçirip gerçekleştirim için sistem kabulü kararını verecek üst yöneticidir. **Yetkilendiren görevli (*authorizing official* - AO)** sistemin ajans misyonuna, varlıklarına ve kişilere oluşturabileceği riski resmi olarak bildirir ve kabul eder.
- **Sertifikalandıran**—Sistem için güvenlik testini uygulamaktan ve değerlendirmeden (ST+E) sorumlu kişi ya da takımdır. **Sertifikalandıran** ayrıca sistemin işletim riski üzerine AO için rapor hazırlar.
- **Sistem sahibi**—Sistemin günlük operasyonlarından sorumlu olan ve sistemin AO tarafından belirlenen şartlar ile uyumlu olarak işlemeye devam ettiğini garanti eden kişi **sistem sahibidir**.

Sertifikasyon: Sertifikasyon kurumun sistemi doğru bir şekilde gerçekleştirdiğinin güvencesini sağlamak üzere sistemin teknik değerlendirmesidir. Sistem güvenlik kontrollerinin etkili bir şekilde çalıştığından emin olmak için başlangıç tasarım gereksinimlerini karşılamalıdır. Sertifikalandıran ya da sertifikalandıran takımı bu görevi gerçekleştirir. Sertifikalandıranın, doğrulama sürecini ve uygunluk ispatı için gereken testleri uygulama yeteneğine sahip olması gerekir. Bir sistemin sertifikasyonu aşağıdaki anlama gelir:

- Sistem teknik gereksinimleri karşılamaktadır.
- Sistem işlevsel gereksinimleri karşılamaktadır.
- Sistem düzgün operasyon güvencesi sağlamaktadır.

Onay vermek için sürece dahil olan kişi ilk olarak teknik ve işlevsel gereksinimleri bilmelidir. Ayrıca, satın alınması için önerilen ya da üretime konması için kabul edilen sistemin yeteneklerini bilmelidir. Bunlar, yazılım ya da donanım gereksinimleri olabilir. Onları bir dakikada 100 kullanıcıya kimlik denetimi yapma yeteneği veya yüzde 99.99 hizmet zamanı garantisi gibi miktar ve kalite açısından değerlendirebilirsiniz. Gereksinimlerinizi ağırlık ya da enerji tüketimi gibi BT olmayan faktörlere dayandırabilirsiniz. Akreditörler tüm gereksinimleri incelemelidir. Bir güvenlik uzmanı olarak bu görevlerin gerçekleştirimi ya da yönetiminin çoğu size kalacaktır.

Son olarak, sertifikalandıranlar yeni sistemin her spesifikasyonu karşılaması ya da spesifikasyonların ötesine geçmesinden emin olmak üzere bu listeleri karşılaştırmalıdır. Sistemin bunu yaptığından emin olduklarında yönetim onayı önerirler. Bu, sistemin kurum için doğru olduğu ya

da mevcut en iyi çözüm olduğu anlamına gelmez. Sertifikasyon sadece, ürünün teknik ve fonksiyonel spesifikasyonları karşıladığı ve söz verdiği gibi işlediği anlamına gelir.

Akreditasyon: Akreditasyon bir sistemi onayladıktan sonra olur. Akreditasyon sistemin resmen kabul yönetim sürecidir. Akreditör ya da tayin edilmiş onay makamı sertifikasyon raporlarını gözden geçirir ve operasyonel ortam bazında sistemi operasyon için kabul eder. Bu süreci iki şekilde tanımlayabilirsiniz:

- Akreditasyon yönetimin riski resmi kabulüdür.
- Akreditasyon yönetimin gerçekleştirme iznidir.

Yeni Sertifikasyon için Tetikleyiciler: Sertifikasyon ve akreditasyon süreçleri bir sistemin güvenlik gereksinimlerini sadece bugün karşılamasını değil, fakat yaşam döngüsünün operasyonlar ve bakım aşamaları boyunca da karşılamaya devam etmesini garanti eder. Akreditasyon sonrası aşama kabul edilebilir bir risk seviyesi sürdürmesinde sistemi işletip yönetmeye devam etmek için gerekli aktiviteleri listeler. Bu gereksinimi karşılamak üzere aşağıdaki gerekçeler nedeniyle riski devamlı olarak değerlendirmelisiniz:

- Yeni ürünler, yeni süreçler, birleştiriciler ya da elden çıkarmalar nedeniyle işletme gereksinimleri değişir.
- Daha önce akredite edilmiş ürünler (çözümler) işletmenin gereksinimlerini artık karşılamayabilir.
- Tedarikçiler sıklıkla ürünleri yükseltir (*upgrade*) ya da yenileri ile değiştirir ve bu yenisiyle değiştirmelerin yeniden onaylanması ve akredite edilmesi gerekir.

Yazılım Geliştirme ve Güvenlik

Bu bölümün başında, güvenli yazılım geliştirmenin önemi hakkında öğrendiniz. Yazılım geliştirme, güvenlik perspektifinden özel bir ilgiye gereksinim duyar. Uygulamalar kullanıcıların, müşterilerin ve saldırganların veriye erişmesi için en yaygın yolu temsil eder. Bu, güvenlik politikanızı uygulatmak ve hem veri hem de sistem süreçlerinin gizliliği ve bütünlüğü dahil olmak üzere yönetmeliklere uygunluğu garanti etmek üzere yazılım geliştirmeniz gerektiği anlamına gelir. Kurumunuzun benimsediği geliştirme modeli ne olursa olsun uygulamanın aşağıdaki görevleri uygun şekilde gerçekleştirdiğinden emin olmalısınız:

- Uygulamaya kullanıcı kimlik denetimini kontrol eder.
- Kullanıcı yetkilendirmesini kontrol eder (yetki seviyesi).
- Sistem arızası durumunda veritabanı bütünlüğünü kurtarmak için prosedürlere sahiptir.
- Hataları ve olağan dışılıkları tutarlı bir şekilde ele alır ve herhangi bir hatanın ya da olağandışılığın ele alınmadan ilerlemesine izin vermez. Ele alınmayan olağan dışılıklar bir uygulamanın güvenliğini azaltabilir. Tüm hataların ve olağan dışılıkların standart yanıtlar ile ele alınması için yaklaşımlar planlayın. Kullanıcılara tutarlı bir hata yanıtı verin ve net açıklamalar ve yönergeler sağlayın. Kullanıcılarınıza doğru seçimler yapmaları için yetki verin.
- Bütün girdileri doğrular (ilk önce doğrulamadan bir kaynaktan herhangi bir girdiyi asla kabul etmez). Eğer veri doğrulamada başarısız olursa atın; temizlemeye çalışmayın! Bu, istemci ve sunuculardaki verileri doğrulamak zorunda olduğunuz anlamına gelir. Sunucuda yeniden doğrulamak verinin geçerli olduğundan emin olmanın tek yoludur. Zayıf doğrulamaya bağlı olan bazı saldırılar aşağıdakileri içerir:

- **Çapraz site betiği (*Cross-site scripting - XSS*)**—Bu, saldırganın istemci tarafı betik kodunu web uygulamasına girdi olarak verdiği saldırıdır. Bu sayede diğer kullanıcılar tarafından kod görüntülenecek ve istemci yazılımı betik komutlarını çalıştıracaktır. XSS saldırısı kullanıcıların sunucuya olan güvenini istismar eder.
- **Çapraz site istek sahtekarlığı (*Cross-site request forgery - XSRF*)**—XSS saldırısına benzer şekilde, saldırgan girdi betiğini görüntüleyen güvenilir bir kullanıcının web sunucusuna kötü niyetli komutlar göndermesine neden olan bir betik kodu sağlar. XSRF saldırısı sunucunun bir kullanıcıya olan güvenini istismar eder.
- **SQL-Yapısal Sorgu Dili enjeksiyonu (*Structured Query Language (SQL) injection*)** —Saldırganın veriye yetkilendirilmemiş erişim yapmak ya da yetkilendirilmemiş komutlar çalıştırmak için kötü niyetli SQL ifadeleri sağladığı saldırı tipidir.

- Güvenli konfigürasyon dayanakları tanımlar. Uygulamanızı son kullanıcılara sürdüğünüzde, güvenli bir dayanak ya da başlangıç noktası tanımlayan belgelenmiş konfigürasyon ayarlar kümesi sağlar.
- Uygulamanızı sertleştirmek üzere kılavuzluk sağlar. Güvenli bir dayanak sağlamaya ek olarak, uygulamanızı güvenli tutacak konfigürasyon ayarlarını değiştirmek üzerine kılavuzluk sunar. Ayrıca, daha ileri konfigürasyon ayarları ya da uygulamanızın güvenliğini artıracak dışsal kontrollerin eklenmesi üzerine kılavuzluk sağlamalıdır.
- Sık sık yamalar sağlar ve uygular. Ortamınız için en son güvenlik yamalarını uyguladığınızdan emin olun. Ayrıca, uygulamalarınızın kullanıcılarına yamaları uygulamanın uygun bir yöntemi ile birlikte sık sık güvenlik yamaları sağlamalı ve yamalama sürecini yönetmelidir.

Kurum içi geliştirilen yazılımın; kaynak kodu, nesne kodu ve çalışma zamanı yürütülebilirleri (*runtime executables*) olacaktır. Bunları yönetmeniz ve politikalar, standartlar ve prosedürler ile korumanız gerekir. Örneğin:

- Kaynak kodu yetkilendirilmemiş kullanıcıların erişiminden korumalısınız.
- Kaynak kodu üzerindeki değişiklikleri versiyon kontrol sistemleri ile izlemelisiniz, böylece bir önceki versiyona geri dönüş hatasız olur.
- Programcılar, üretim sistemlerini doğrudan güncelleyememelidir (programcılardan teste, daha sonra testten üretime).

Yazılım Geliştirme Modelleri

Güvenli yazılım geliştirme, yazılımın yaratılması ve değiştirilmesi için biçimsel bir model gerektirir. Bu süreç yazılım geliştirme aktivitelerine, belli başlangıç ve bitiş tarihleri ve gerekli teslimatlar kümesi olan projeler gibi kılavuzluk yapmak için en iyi endüstri uygulamalarını kullanan yazılım geliştirme yaşam döngüsü ya da SDLC olarak bilinir. Şu anda, en geniş çapta kabul gören iki yazılım geliştirme modeli aşağıdakileri içerir:

- Şelale modeli. Kapsamlı planlamanın herhangi bir geliştirmeden önce geldiği geleneksel proje yönetimi uygulamalarına dayalıdır. Proje süresince ilerleme iyi tanımlanmış bir yol boyunca yol alır.
- Çevik geliştirme yöntemi. Çok kısa aktivite sprintlerine bağlı olan yeni proje yönetimi yaklaşımları ailesidir. Çevik, gereksinimlerin değiştiği ve sıklıkla tekrar gözden geçirildiği çok dinamik ortamlarda iyi çalışır.

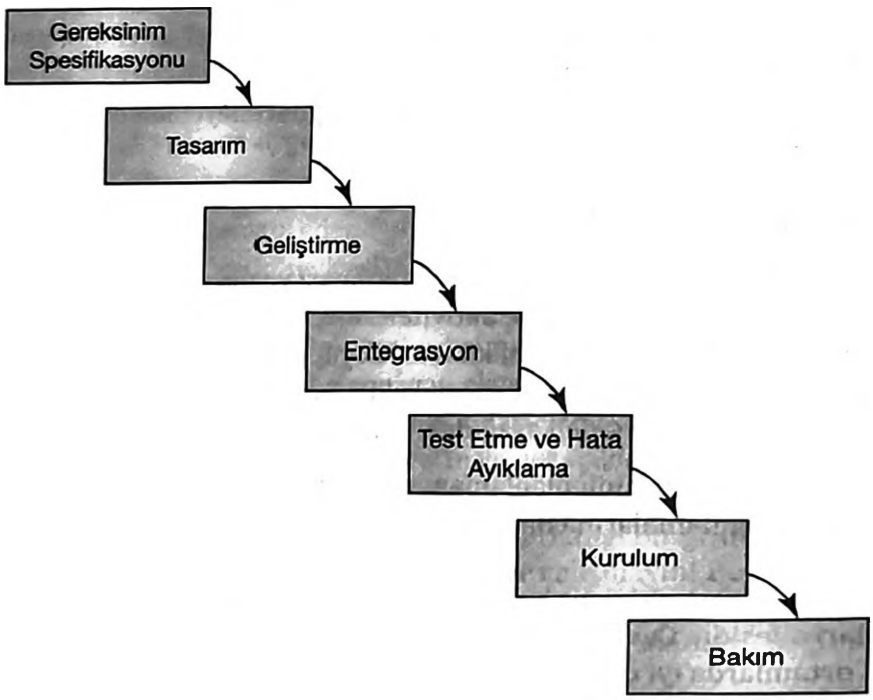
Teknik TAVSİYE

SQL enjeksiyonunu ortak bir saldırı olarak tanıyabilirsiniz. Açık Web Uygulama Güvenliği Projesi (*Open Web Application Security Project*) www.owasp.org uyarınca, SQL Enjeksiyonu güvenlik açığı web uygulamalarındaki en yaygın yinelenen güvenlik açıklarından biridir. Büyüyen veritabanları ve veriye daha hızlı duyulan ihtiyaç, *NoSQL* veritabanları olarak adlandırılan ilişkisel olmayan veritabanlarında büyümeye yol açmıştır. NoSQL veritabanları SQL enjeksiyon saldırılarına karşı özellikle savunmasız olmasa da, bu onları daha güvenli bir şekilde düşünmeniz gerektiği anlamına gelmez. NoSQL veritabanları bile enjeksiyon saldırılarına karşı savunmasızdır.

Şelale Modeli

Şu anda çok sayıda yazılım geliştirme yöntemi, modellerini **ŞEKİL 6-7**'de gösterilen **şelale modeline** (***waterfall model***) dayandırır. Bu, yazılım geliştirme için ardışık bir süreçtir. Önceden öğrendiğiniz SDLC ve SLC'yi içerir. Şelale modelinde ilerleme aşağıya doğru şelale gibi akar. Şelale modelinin esası hiçbir aşamanın önceki aşama tamamlanmadan başlamamasıdır. Aşamalar aşağıdaki gibidir:

1. Gereksinim spesifikasyonu
2. Tasarım
3. Geliştirme
4. Entegrasyon
5. Test etme ve hata ayıklama
6. Kurulum
7. Bakım



ŞEKİL 6-7
Şelale modeli.

Temel şelale modeli imalat ve inşaat endüstrilerinden kaynaklanmıştır. Geç gözden geçirmelerin büsbütün fahiş fiyat olmasa bile çok maliyetli olması yüksek derecede yapısal fiziksel ortamların bir özelliğidir. Winston W. Royce bu modeli 1970'te tasarladığında hiçbir biçimsel yazılım geliştirme yöntemi yoktu. Bu donanım yönelimli model yazılım geliştirmeye uyarlandı.

Bu modelin fark edilen eksiklikleri nedeniyle, şelale modelinin modifikasyonlarını bulacaksınız. Yazılım geliştirme modellerinin çoğu şelale modeline benzer en azından birkaç aşama kullanır. Modelin önemi bir sonraki aşamaya geçmeden önce her aşamanın tamamlanmasından emin olunmaya odaklanmasındadır. Büyük geliştirme ortamlarında bu oldukça zor olabilir ancak her zaman yazılımınızı uygun şekilde planlamak ve tasarlamak için zaman harcayın. Hemen programları yazmaya başlamayın!

Çevik Yazılım Geliştirme

Geleneksel yazılım geliştirme yönetimi hala büyük ölçüde şelale modelinin birkaç varyasyonuna dayanır. 1990'larda bazı kurumlar yazılım endüstrisinin farklı yönlerde değişmeye başladığını fark etti. Daha karmaşık yazılımların daha etkin bir şekilde geliştirilmesi için artan talep yazılım geliştirme yönetiminin yeni yöntemlerine yol açtı. Büyük projeleri uzun teslim planları ile yönetmek yerine çok sayıda kurum daha duyarlı olmanın yollarını aradı. Yazılımları küçük parçalar halinde geliştirebilmeyi istediler. Daha küçük geliştirme döngülerine doğru bu hareket sonunda **çevik geliştirme (*agile development*)** yöntemi olarak bilinir hale geldi.

Çevik, uzun proje planları yerine küçük proje iterasyonlarına ya da sprintlere dayalı olan yazılım geliştirme yöntemini gevşek bir şekilde tanımlar. Çevik kullanan kurumlar daha küçük teslimatları daha sık olarak üretir ve büyük bir projeyi tamamlanan ayrı parçaları açısından değerlendirebilir. **Sprintler** genellikle 1 ila 4 hafta sürer. Bu her ay bir defa ya da daha sık olarak teslimatın varlığı demektir. Sık teslimata odaklanma büyük bir yazılım ürününün zamanla olgunlaştıkça parçalarının görülmesini ve kullanılmasını mümkün kılar.

Çevik heveslilerinin düzenlenen ilk toplantısı 2001'de idi. Bu yeni tip yazılım geliştirmeyi araştıran çeşitli kurumlar işbirliği yapmak ve fikir alışverişinde bulunmak üzere temsilcilerini Snowbird, Utah'da bir toplantıya gönderdiler. Katılımcılar çevik hareketin temel belgesini yarattılar: Çevik Yazılım Geliştirme için Manifesto (*Manifesto for Agile Software Development*). Bu manifesto, yazarlarının basit yöntemlere olan yönelimini ortaya koyan kısa bir dokümandır. Çevik Yazılım Geliştirme için Manifesto bütünü ile (*http://www.agilemanifesto.org/*) aşağıdaki gibidir:

> Biz yazılım geliştirmenin daha iyi yollarını yazılım geliştirerek ve diğerlerine yazılım geliştirmelerinde yardım ederek ortaya çıkarıyoruz. Bu çalışma sayesinde şunlara değer vermeye başladık:
>
> - Süreçler ve araçlardan öte bireyler ve etkileşimlere
> - Kapsamlı dokümantasyondan öte çalışan yazılıma
> - Sözleşme müzakeresinden öte müşteri işbirliğine
> - Bir planın takip edilmesinden öte değişime yanıt vermeye
>
> Yani, sağdaki öğelerin değeri olmasına rağmen soldakilere daha fazla değer veriyoruz.

ŞEKİL 6-8 çevik yöntemin arkasındaki temel fikri göstermektedir. Şelale yönteminin aksine, çevik yinelemeli olarak tasarlanmıştır. Etrafındaki devir süresi tek bir sprinttir. Bütün bir yazılım projesini yaratmak çok sayıda sprint gerektirir. Her sprint zamanın belli bir noktasında sonlanır ve bir teslimata sahip olmalıdır. Teslimat çalışan yazılım gibi takımın gösterebileceği bir şey olmalıdır. Çalışan yazılıma odaklanılması takımın sonuçlara odaklanmasına yardım eder.

ŞEKİL 6-8
Çevik yazılım geliştirme yöntemi.



NOT

Çevik Yazılım Geliştirme Manifestosu ve genel olarak çevik yöntemi hakkında daha fazla bilgiyi *http://agilemanifesto.org* adresinde bulabilirsiniz. Çevik hakkında bilgi edinmek için bir başka bir iyi başlangıç noktası *www.agile-process.org* adresidir.

Çevik, yazılım geliştirme projeleri yönetiminin popüler bir tekniğidir. Süre giden iletişimi cesaretlendiren ve kısa geliştirme döngülerine değer veren kurumlarda iyi işleme eğilimi vardır. En başından yazılımı güvenliği göz önünde bulundurarak geliştirmeye başlamak önemlidir. Çevik yöntemler geliştiricilerin güvenlik için planlamasını ve daha sonra her sprintin sonunda güvenlik için test yapmasını cesaretlendirir. Güvenli yazılım geliştirme -kurum güvenliğe değer verip destekliyorsa- toplam geliştirme emeğinin ayrılmaz bir parçası olabilir. Bir kurumun kullandığı geliştirme yöntemine bakılmaksızın güvenliğe gösterilen özen herhangi bir yöntemden daha önemlidir.

BÖLÜM ÖZETİ

Bu bölümde, güvenlik uzmanlarının herhangi sıkı bir güvenlik programının temelinin güvenlik operasyonları ve yönetimi olduğunu anlaması gerektiğini öğrendiniz. Güvenlik yönetiminin bir kurumun güvenlik planını planlamak, tasarlamak, gerçekleştirmek ve izlemek için nasıl çalıştığını öğrendiniz. Her sıkı güvenlik planı için mesleki etiğin esas olduğunu

öğrendiniz. Güvenlik programının uyumlu olduğundan emin olmak için ne yapmanız gerektiğini öğrendiniz. Güvenlik programınızı şekillendirmek için planınızın politikalarınız, standartlarınız, kılavuzlarınız ve prosedürleriniz ile nasıl birlikte çalıştığını öğrendiniz. Veri sınıflandırma standartlarının karar verme sürecini nasıl etkilediğini öğrendiniz. Sistem değişikliklerini yönetmek için konfigürasyon yönetimini kullanmayı ve değişiklik yönetim sürecini konfigürasyon denetiminin ve değişiklik denetiminin nasıl etkilediğini öğrendiniz. Sistem yaşam döngüsünün (SLC) sekiz ortak adımını, sistem geliştirme yaşam döngüsünü (SDLC) ve bu adımların maliyeti nasıl düşürdüğünü öğrendiniz. Yazılım geliştirme yöntemlerinin neden özel güvenlik değerlendirmesi gerektirdiğini öğrendiniz. Son olarak, güvenlik programınızın başarısında kullanıcı farkındalığının nasıl merkezi olduğunu öğrendiniz.

ANAHTAR KAVRAMLAR VE TERİMLER

Accreditation-Akreditasyon
Agile development-Çevik geliştirme
Authorizing official (AO)- Yetkilendiren görevli (AO)
Baseline - Dayanak
Blanket purchase agreement (BPA)– Sonu açık sipariş sözleşmesi (BPA)
Certification- Sertifikasyon
Certifier - Sertifikalandıran
Change control - Değişiklik denetimi
Change control committee - Değişiklik denetimi komitesi
Clean desk/clear screen policy - Temiz masa/temiz ekran politikası
Compliance liaison – Uygunluk irtibatı
Configuration control - Konfigürasyon denetimi
Cross-site request forgery (XSRF) – Çapraz-site istek sahtekarlığı (XSRF)
Cross-site scripting (XSS) - Çapraz site betiği (XSS)
Emergency operations group - Acil operasyonlar grubu
Event logs - Olay günlükleri
Functional policy – İşlevsel politika
Fuzzing - Fuzzing
Guideline - Kılavuz
Interconnection security agreement (ISA) - Birbirine bağlı güvenlik sözleşmesi (ISA)
Internet Architecture Board (IAB) - İnternet Mimarisi Kurulu (IAB)
Job rotation - İş rotasyonu
Memorandum of understanding (MOU) Anlaşılma memorandumu (MOU)
Offboarding - İşten ayrılma uyum süreci
Onboarding - İşe uyum süreci
Privacy policy – Mahremiyet politikası
Proactive change management - Proaktif değişiklik yönetimi
Procedure - Prosedür
Reactive change management - Reaktif değişiklik yönetimi
Remediation - İyileştirme
Security administration Güvenlik yönetimi
Service-level agreement (SLA) - Hizmet seviyesi sözleşmesi (SLA)
Sprint - Sprint
SQL injection - SQL enjeksiyonu
Standard - Standart
System development life cycle (SDLC) - Sistem geliştirme yaşam döngüsü (SDLC)
System life cycle (SLC) - Sistem yaşam döngüsü (SLC)
System owner - Sistem sahibi
Waterfall model - Şelale modeli

BÖLÜM 6 DEĞERLENDİRME

1. Güvenlik yönetimi bir kurumun güvenlik planının planlanması, tasarımı, gerçekleştirimi ve izlenmesinden sorumlu kişiler topluluğudur.
   A. Doğru
   B. Yanlış

2. Güvenlik programının gerektirdiği dokümantasyon:
   A. Güvenlik süreci
   B. Kurum tarafından benimsenen politikalar, prosedürler ve kılavuzlar
   C. Güvenlikten sorumlu kişilerin yetkisi
   D. Hepsi
   E. Hiçbiri

3. Bir kurumun hem düzenleyici standartlara hem de kurumsal standartlara uyumlu olması gerekmez.
   A. Doğru
   B. Yanlış

4. _____ kurumunuz ile dış bir firma arasında, firmanın sağlayacağı özel hizmetleri detaylandıran resmi sözleşmedir.
   A. Güvenlik olay günlüğü
   B. Vaka yanıtı
   C. Hizmet seviyesi sözleşmesi (SLA)
   D. Uygunluk raporu

5. Hangi yazılım test yöntemi yazılımın beklenmeyen veriyi nasıl ele aldığını görmek için rastgele girdi sağlar?
   A. Enjeksiyon
   B. Fuzzing
   C. Geçerli hata girdisi
   D. Sınır girdisi

6. 1989'da IAB internet etiği hakkında bir politika raporu çıkardı. Bu belge _____ olarak bilinir.
   A. OECD
   B. RFC 1087
   C. $(ISC)^2$ Etik Kurallar Ölçütleri
   D. CompTIA Aday Etik Kuralları
   E. Hiçbiri

7. _____ kullanıcılara sadece görevlerini gerçekleştirmelerine yetecek erişim hak seviyelerinin verilmesi gerektiği bir kavramdır.
   A. Zorunlu izinler
   B. Görevler ayrılığı
   C. İş rotasyonu
   D. En düşük yetki prensibi
   E. Hiçbiri

8. Aşağıdakilerden hangisi bir sosyal mühendislik örneğidir?
   A. Yardım için duygusal başvuru
   B. Oltalama saldırısı
   C. Gözdağı vermek
   D. Birini tanıyor havasına girmek
   E. Hepsi

9. Politika kurumunuzun tarzını ve kültürünü belirler.
   A. Doğru
   B. Yanlış

10. _____, kurum genelinde bir güvenlik riskini ele almak için donanım ve yazılım çözümlerinin standardizasyonu ile ilgilenir.
    A. Politikalar
    B. Standartlar
    C. Prosedürler
    D. Dayanaklar

11. Aşağıdakilerden hangisi prosedürler için doğrudur?
    A. Bir kriz durumunda hataları artırır.
    B. Süreç içerisinde güvence kontrollerinin yürütülmesine yer sağlar.
    C. Önemli adımlar çoğunlukla atlanır.
    D. Hiçbiri
    E. Hepsi

12. Veri sınıflandırma veriye sahip olan kişinin sorumluluğudur.
    A. Doğru
    B. Yanlış

13. Bilgi sınıflandırmanın hedefleri arasında aşağıdakilerden hangisi yer alır?
    A. Kurum politikası gereğince verinin değerinin tespit edilmesi
    B. Bilgi koruma gereksinimlerinin tespit edilmesi
    C. Kurum genelinde sınıflandırma etiketlerinin standardizasyonu
    D. Gizlilik kanunu, yönetmelikler ve diğerlerine uyumlu olma.
    E. Hepsi

14. Konfigürasyon yönetimi sistem yaşam döngüsü boyunca otomatik bir sistemin donanımına, yazılımına, üretici yazılımına, dokümantasyonuna, test planlarına ve test dokümantasyonuna yapılan değişikliklerin yönetimidir.
    A. Doğru
    B. Yanlış

15. Değişiklik yönetim süreci _____ denetimini ve _____ denetimini içerir.
    A. Erişim yetkisi, derecelendirme
    B. Doküman, veri
    C. Donanım envanteri, yazılım geliştirme
    D. Konfigürasyon, değişiklik

16. Giderek daha çok kurum _____ terimini uygulamalar için değişim ve bakım sürecinin tamamı olarak tanımlar.
    A. Sistem geliştirme yaşam döngüsü (SDLC)
    B. Sistem yaşam döngüsü (SLC)
    C. Sistem bakım yaşam döngüsü (SMLC)
    D. Hiçbiri

17. Yazılım geliştirirken uygulamanın aşağıdakilerden hangisini yaptığından emin olmalısınız?
    A. Düzenleme kontrollerine, aralık kontrollerine, geçerlik kontrollerine ve diğer benzer kontrollere sahiptir
    B. Kullanıcı yetkilendirmesini kontrol eder
    C. Uygulamaya kullanıcı kimlik denetimini kontrol eder
    D. Sistem arızası durumunda veritabanı bütünlüğünü kurtarmak için prosedürlere sahiptir.
    E. Hepsi

18. Farklı tipte yazılım geliştirme yöntemleri vardır fakat geleneksel yöntemlerin çoğu _____ dayanır.
    A. Modifikasyon
    B. Şelale
    C. Geliştirici
    D. Entegrasyon

BÖLÜM

7

Denetleme, Sınama ve İzleme

Denetimleri yerleştirdikten sonra bile güvenli sistemler için planlama bitmez. Eğer gerçekten kendinizi veri ihlallerinden korumak istiyorsanız, her tür saldırıya karşı hazır olduğunuzdan emin olmalısınız. Bunu yapmak için düzenli olarak sisteminizi değerlendirmeniz gerekmektedir. Veri ihlallerinden kaçınmak için önemli değerlendirmelerinden biri, *güvenlik denetlemesidir* (*security audit*). Bir bilgisayar sistemini incelediğinizde, çalışmasının güvenlik hedeflerinizi nasıl sağladığını incelersiniz. Basitçe söylemek gerekirse, bir sistemi incelediğinizde, sistemdeki unsurların plana göre çalışıp çalışmadığını gözlersiniz. Denetlemeler, bazen de gereksinimlere uygunluğunu doğrulamak için herhangi bir anda sistemin mevcut yapılandırmasına da bakar.

Bir sistemi elle ya da otomatize bir bilgisayar yazılımı ile denetleyebilirsiniz. Elle yapılan/manuel testler aşağıdakileri kapsar:

- Personelinizle görüşmek
- Zafiyet taramaları yapmak
- Uygulama ve işletim sistemi erişim denetimlerini değerlendirmek
- Sisteme fiziksel erişimleri analiz etmek.

Otomatize edilmiş testler ile denetleme yazılımı, önemli dosyalar ve ayarlardaki herhangi bir değişiklik hakkında bir rapor oluşturur. Bu dosyalar ve ayarlar, hesaplama/bilgi işlem cihazları, işletim sistemleri veya uygulama yazılımları ile ilgili olabilir. Hesaplama/bilgi işlem cihazları kişisel bilgisayarları, mobil cihazları, sunucuları, ağ yönlendiricilerini ve ağ anahtarlarını kapsayabilir. Uygulama yazılımları, kullanıcılara servis sağlayan herhangi bir hesaplama/bilgi işlem cihazı üzerinde çalışan bir yazılım olabilir.

Elbette, bir sistemi denetlemenizden çok önce, sistemin kurallarını ve gereksinimlerini belirleyen politikaları ve yönetmelikleri oluşturmanız gerekir. Bu nedenle, bir şeyin işe yarayıp yaramayacağını belirleyebilmeniz için öncelikle bunun *nasıl çalışması gerektiği* konusunda bilgi vermeniz gerekir. Bu, sisteminizi *değerlendirmek* olarak bilinir. Sisteminizin tüm bileşenlerini değerlendirir ve her birinin nasıl çalışması gerektiğini belirlersiniz. Bu temel beklentilerinizi belirler. Bunu yaptıktan sonra sistemi inceleyebilirsiniz. Her şeyin planlandığı gibi çalıştığını görmek için sistemin performansı ile temel beklentilerinizi karşılaştırırsınız.

7. Bölüm Konular

Bu bölüm aşağıda verilen konuları ve kavramları kapsamaktadır:

- Güvenlik denetlemesi ve analizi nedir
- Denetleme planınızı nasıl tanımlamanız gerekir
- Denetleme ölçütleri nelerdir
- Denetleme verilerini nasıl toplamanız gerekir
- Hangi denetleme sonrası faaliyetlerini gerçekleştirmeniz gerekir
- Güvenlik izlemesi nasıl gerçekleştirilir
- Hangi tür günlük bilgilerini yakalamanız gerekir
- Güvenlik denetimlerini nasıl doğrulamanız gerekir
- Güvenlik sistemlerinizi nasıl izlemeniz ve sınamanız gerekir

7. Bölüm Hedefler

Bu bölümü tamamladığınız zaman, yapabilecekleriniz:

- Güvenlik denetlemelerinin usul ve esaslarını açıklayabilme
- Günlük yönetimi ve bir saldırı tespit sistemi veya saldırı önleme sistemi gibi sistem izleme dahilinde olan yöntemleri değerlendirebilme
- Sistem performansı için metrikleri ayarlayabilme
- Bir kuruluşun güvenlik uyumluluğunu değerlendirebilme

Güvenlik Denetlemesi ve Analizi

Güvenlik denetlemesinin amacı, sistemlerinizin ve güvenlik denetimlerinin beklendiği gibi çalıştığından emin olmaktır. Sistemlerinizi değerlendirirken aşağıdakileri denetim etmeniz gerekir:

- **Güvenlik politikaları, iş etkinlikleri için uygun ve yeterli midir?** Bilgi güvenliğinin amacı, işin misyonunu desteklemek ve karşılaştığı risklerden korumaktır. Güvenlikle ilgili olarak, en sık görülen risklerden biri, veri ihlalidir. Kuruluşunuzun politikaları ve destekleyici belgeleri, onu etkileyen riskleri tanımlar. Destekleyici belgeler, kuruluşunuzun yönetmeliklerini, standartlarını ve temelini içerir. Denetleme gerçekleştirirken, "Politikalarımız anlaşıldı ve takip edildi mi?" sorusunu sorarsınız. Denetlemenin kendisi yeni politikalar belirlememektedir. Ancak, denetçiler yeni düzenlemelere veya diğer gereksinimlere ilişkin tecrübe veya bilgiye dayalı önerilerde bulunabilir.

- **Politikalarınızı destekleyen denetimler bulunuyor mu?** Güvenlik denetimleri, kuruluşunuzun stratejileri ve misyonuyla doğru bir şekilde uyumlu mu? Denetimler politikalarınızı ve kurum kültürünüzü destekliyor mu? Eğer bir denetimi bir politika ile doğrulayamıyorsanız, muhtemelen onu kaldırmalısınız. Bir denetim "güvenlik için" olarak belirtilmiş ise, ancak herhangi başka bir açıklaması bulunmuyorsa, bu denetimi kaldırmalısınız. Güvenlik bir kâr merkezi değildir ve kendi iyiliği için asla var olmamalıdır. Güvenlik bir destek bölümüdür. Amacı, kuruluşun varlıklarını ve gelir akışını korumaktır.
- **Etkili bir şekilde denetimlerin uygulanması ve bakımı var mı?** Kuruluşunuz geliştikçe ve tehditler olgunlaştıkça, denitimlerinizin bugün karşılaştığınız riskleri karşılamasını sağlamak önemlidir.

Eğer bu soruları evet olarak yanıtlayabiliyorsanız, iyi durumdasınızdır. Ancak, bu soruları evet olarak yanıtlayamıyorsanız, endişelenmeyin. Bu bölümde, bu becerilerinizi geliştireceksiniz.

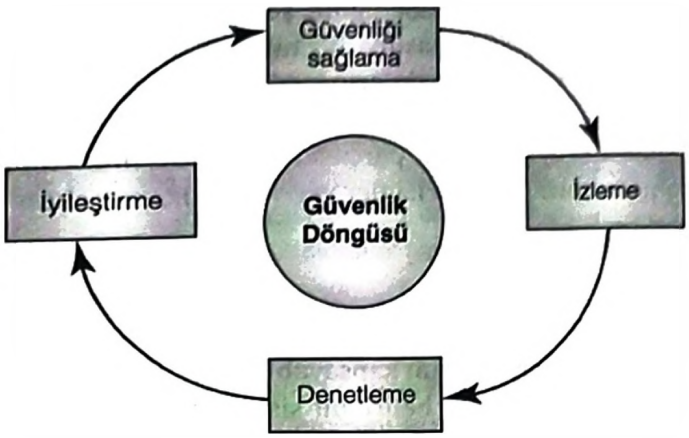
Güvenlik Denetimleri Riske Odaklanır

Güvenlik denetimleri, kuruluşunuz için bir risk oluşturabilecek faaliyetlere sınırlar koyar. Denetimlerinizin geçerli ve etkili olduğundan emin olmak için güvenliği düzenli olarak incelemelisiniz. Bu güvenlik incelemesi aşağıdaki faaliyetleri içermektedir:

- **İzleme (*Monitor*)**—Sistemdeki hareketleri ve değişiklikleri yakalamak için tüm denetimleri inceleyin ve ölçün.
- **Denetleme (*Audit*)**—Güvenlik politikasının ve denetimlerinin ne kadar iyi olduğuna dair bağımsız analiz sağlamak için günlükleri ve genel çevreyi inceleyin.
- **İyileştirme (*Improve*)**—Denetleme sonuçlarındaki güvenlik programını ve denetimlerini iyileştirmek için önerilerinizi ekleyin. Bu adım, yönetim tarafından kabul edilen, önerilen değişiklikler için geçerlidir.
- **Güvenliği sağlama (*Secure*)**—Yeni ve mevcut denetimlerin, amaçlanan güvenlik düzeyini sağlamak için birlikte çalıştığından emin olun.

Güvenlik denetimleri bilgisayarlarınızı ve ağınızı korumasına rağmen her birinin gerekli ve etkili olduğunu doğrulamanız gerekir. Her denetim kuruluşunuzu belirli bir tehdide karşı korumalıdır. Tanımlanmış bir tehdit içermeyen bir denetim, kuruluşunuzu daha fazla güvenli hale getirmeyen ek bir katmandır. Yerinde bulunan bütün güvenlik denetimlerinin, belirli tehditlere işaret ettiğini dikkatlice doğrulayın. Aynı tehdidi işaret eden çok sayıda denetime sahip olmak iyidir, sadece her denetimin en az bir tehdidi işaret ettiğinden emin olun.

Hatırlayın ki risk, bir tehdidin gerçekleşme olasılığı olarak tanımlanır. Beklenen zararı, risk olasılığının varlık maliyeti ile çarparak hesaplayabilirsiniz. Riskleri belirleme, denetimlerin geçerliliğini ölçmenize olanak tanır. Bir tehdite karşılık potansiyel bir zarardan daha fazla maliyeti olan bir denetim kullandığınızda, kuruluşunuzun kaynaklarını boşa harcıyor olabilirsiniz. Kuruluşunuzun kaynaklarını boşa harcamaktan kaçınmanın en iyi yollarından biri, güvenlik gözden geçirme döngüsünü izlemenizi sağlamaktır. **ŞEKİL 7-1**, güvenlik gözden geçirme döngüsündeki adımların birlikte birbirini nasıl tamamladığını göstermektedir.



ŞEKİL 7-1
Güvenlik gözden geçirme döngüsü

Neyin Kabul Edilebilir Olduğunun Belirlenmesi

Doğru güvenlik denetimlerini yerine getirmeye yönelik ilk yöntem, hangi eylemlerin kabul edilebilir olduğunu belirlemektir:

- Kuruluşunuzun güvenlik politikası kabul edilebilir ve kabul edilemez eylemleri tanımlamalıdır.
- Kuruluşunuz, standartlar organları tarafından geliştirilen veya onaylanan standartlara dayalı kendi standartlarını oluşturabilir.
- Politika belgesi tarafından izin verilen iletişim ve diğer eylemler *kabul edilebilir*.
- Güvenlik politikasında özellikle yasaklanan iletişim ve diğer eylemler *kabul edilemez*. Kalan diğer iletişim ve diğer eylemler de kabul edilemez olabilir. Gizli bilgileri açığa çıkarabilecek, bir sistem bütünlüğüne zarar verebilecek veya sistemi kullanılamaz hale getirebilecek herhangi bir eylem, politikanın özellikle yasaklamamasına rağmen kabul edilemez.

İzin Seviyeleri

Kuruluşunuz için uygun izin seviyesi, kuruluşunuzun ihtiyaç ve politikalarına bağlıdır. Kuruluşunuzun gerekli izin seviyesini güvenlik yapısıyla eşleştirmeniz esastır. Bunu yapmazsanız, çok fazla veri kaybedebilirsiniz ve itibarınız zedelenebilir. Güvenlik denetimleriniz gerekenden daha katıysa, kullanıcıların güvenlik denetimlerini atlamaya çalıştıklarını da görebilirsiniz. En yaygın izin seviyeleri aşağıdaki gibidir:

- **Ayrım Gözetmemek (*Promiscuous*)**—Herşey serbest. Bu izin seviyesi pek çok ev kullanıcısı tarafından kullanılır ancak saldırganların işini kolaylaştırır.
- **İzinli (*Permissive*)**—Özellikle yasaklanmamış herhangi bir şey İYİDİR. Bu izin seviyesi, çoğu kamuya açık internet siteleri, bazı okullar ve kütüphaneler ve birçok eğitim merkezi için uygundur.
- **Tedbirli (*Prudent*)**—Makul bir listeye izin verilir. Diğerlerinin hepsi yasaktır. Bu izin seviyesi birçok işletme için uygundur.
- **Paranoyak (*Paranoid*)**—Çok az şeye izin verilir; diğerlerinin hepsi yasaklanmış ve dikkatle izlenmiştir. Bu izin seviyesi yüksek güvenlikli tesisler için uygundur.

Kullandığınız izin seviyelerine bakılmaksızın, "beklediğiniz şeyleri incelemek" önemlidir. Bu ifade, denetlemenin tüm yönleri için geçerlidir. Basitçe, bir bilgisayarın tedbirli izin seviyelerini kullanmasını beklerseniz, kullanıcı haklarına ve izinlerine yakından bakın. Yerinde olan denetimlerin yapmaları gereken şeyleri yaptığından emin olun. Kullanıcı hakları ve izin yorumları, herhangi bir güvenlik denetlemesinin ayrılmaz bir parçasıdır. Yerinde, mükemmel güvenlik denetimleriniz olsa bile, kullanıcılarınıza sınırsız izinler veriyorsanız, gerçekten sisteminizi pek güvende tutmuyorsunuz demektir.

Güvenlik Denetleme Alanları

Denetlemeler, tüm birimleri veya iş fonksiyonlarını kapsayabilecek kadar geniş bir alana sahip olabilir. Bunun yanısıra, dar olabilirler ve sadece belirli bir sistemi veya denetimi işaret edebilirler. Bir denetleme yönetimi, en iyi denetimlerin yerine getirilip getirilmediğinin ve ne kadar iyi çalıştıklarının bağımsız olarak değerlendirilmesini sağlar. Bu, yönetimin, bu riskleri anlamasına ve bunları ele almasına yardımcı olur.

Örneğin, yüksek düzeyli bir güvenlik politikası denetlemesi, güvenlik ilkesinin güncelliğini, ilgisini, tebliğ edilmesini ve uygulanmasını sağlamak üzere gözden geçirilmesidir. Bu denetleme türü, politikanızın, kuruluşunuzun kültürünü yansıtmasını sağlar. Bu denetlemeler, kullanıcıların veya müşterilerin denetimleri kabul edip etmediğini veya gerçek dışı gördükleri denetimleri atlatmaya çalışıp çalışmadıklarını da belirleyebilir. Buna ek olarak, bu tür bir denetleme, altyapınızın uygulamanızın verilerini ne kadar iyi koruduğunu test eder. Uygulamanın yalnızca yetkili kullanıcılara erişimi sınırlandırdığını ve yetkisiz kullanıcıların görmemesi gereken verilerin gizlenmesini (şifrelenmesini) sağlar.

Ayrıca kuruluşunuzun tüm güvenlik duvarlarını, yönlendiricilerini, ağ geçitlerini, kablosuz erişim noktalarını ve diğer ağ aygıtlarını, amaçlandığı gibi çalıştığından ve yapılandırmalarının güvenlik ilkesine uygun olduğundan emin olmak için denetlemelisiniz. Son olarak, denetlemeler teknolojilerin kendilerini test edebilir. Ağa bağlı tüm bilgisayarlarınızın ve cihazlarınızın politikalarınıza göre birlikte çalışıp çalışmadığını tespit eder. Denetim süreçlerinin değişimine bağlı olarak, kurallarınızın ve konfigürasyonlarınızın güncel ve belgelenmiş olduğunu temin eder.

Denetlemelerin Amacı

Denetleme, risk yönetim programınızı gözden geçirme ve programın kuruluşunuzdaki riskleri doğru bir şekilde tanımlandığını ve azalttığını (veya başka bir şekilde belirttiğini) teyit etme imkanı verir.

Bir denetleme, denetimlerin aşağıdaki maddeleri sağladığına bakar:

- **Uygun olduğu**—Güvenlik denetimi seviyesi, hedeflediği risk için uygun mu?
- **Doğru kurulduğunu**—Güvenlik denetimi doğru yerde ve iyi çalışıyor mu?
- **Amaçlarına hitap ettiğini**—Güvenlik denetimi, ele alınması tasarlanan riski gidermede etkili midir?

Denetçilerin oluşturduğu denetleme raporu, organizasyonun süreçlerini, altyapısı veya diğer denetimleri gerektiğinde iyileştirme veya değişiklikler önermelidir. Denetlemeler, olası sorumluluk, ihmal ve zorunlu yasal uygunluk nedeniyle gereklidir. Denetlemeler, sorunları ortaya çıkarabilir ve uygunluğun güvencesini verebilir. Birçok yargılama, kanun gereğince denetleme gerektirir.

Ne sıklıkta denetleme yapmalısınız?

Denetleme sıklığı önemli bir husustur. Bazı denetlemelerin yalnızca talep üzerine gerçekleşmesi gerekir. Bunlara, olay sonrası denetleme ya da bir düzenleyici kurum gibi harici bir makam tarafından istenen bir denetleme dahildir. Diğer denetlemeler bir programa göre yapılmalıdır. Çoğu yönetmelik, yıllık veya üç aylık denetleme gerektirir. İç gereksinimler, denetlemeleri daha sıklaştırabilir. Örneğin, özenli kuruluşlar genellikle sunucu günlüklerini haftalık olarak denetlemektedir ve IDS/IPS gündelik olarak günlükler oluşturmaktadır. Güvenlik politikanız, denetleme planınız için denetleme kategorilerini ve sıklık gereksinimlerini içermelidir.

Kanunlar ve yönetmelikler, belirli sayıda çalışan istihdam eden veya belirli bir endüstriden olan bazı şirketlerin hem iç hem de dış denetlemesini gerektirir. Bu denetlemeleri yapması gereken endüstriler, finansal hizmetler kuruluşlarını ve kişisel tıbbi kayıtları yürüten herhangi bir kuruluşu içerir. İç ve dış denetlemeleri gerektiren Amerikan federal kanunları veya tedarikçi standartları arasında Sarbanes-Oxley Yasası (*Sarbanes-Oxley Act* - SOX), Sağlık Sigortası Taşınabilirlik ve Sorumluluk Verebilirlik Yasası (*Health Insurance Portability and Accountability Act* - HIPAA) ve Ödeme Kartı Endüstrisi Veri Güvenliği Standardı (*Payment Card Industry Data Security Standard* - PCI DSS) bulunur. Kişisel Bilgi Koruma ve Elektronik Belgeler Yasası (*Personal Information Protection and Electronic Documents Act* - PIPEDA), kuruluşların e-ticaret işlemlerinde kişisel bilgilerini nasıl topladığını, kullandığını veya açıklamasını koruyan bir Kanada yasasıdır. Aynı zamanda denetleme gereksinimlerini de içerir.

Bir denetleme, bir kuruluşun yeteri kadar eğitimli ve yetenekli bir personele sahip olmadığını bulabilir. Bu, şirketin güvenlik programlarını yeterince gözetleyemediği ve varlıklarını yeterince yönetemediğini gösterebilir. Denetleme, bir organizasyonu daha iyi personel eğitimi sağlamaya teşvik edebilir. Öte yandan, bir denetleme, bir kuruluşun gereksinimlerini karşılayıp karşılamadığını doğrulayabilir.

Birçok yeni yönetmelik, şirket varlıklarının yanlış yönetilmesinden veya dolandırıcılıktan ötürü yönetimi şahsen sorumlu tutar. Geçmişte, bu hatalardan dolayı çoğunlukla şirketler sorumluydu; şimdi ise bireyler sorumludur. Kendisini ve çalışanlarını korumak için gerekli tüm gereksinimlere uymak için her türlü çabayı göstermek kuruluşun çıkarlarına olacaktır.

Müşteri Güveni

Müşteriler genelde yalnızca güvendiği kuruluşlarla iş yapar. Müşteriler sisteminizi güvenlik açısından sürekli incelediğinizi biliyorsa, hassas bilgileri sizinle paylaşmaya daha istekli olabilir.

Birçok şirketler arası iş yapan hizmet sağlayıcıları, müşteri güvenini oluşturmak için denetleme standartlarını kullanmaktadır. Amerikan Yeminli Mali Müşavirler Enstitüsü Denetleme Standartları Kurulu (*Auditing Standards Board of the American Institute of Certified Public Accountants*), 1993'te Denetleme Standartları No.70 (*Statement on Auditing Standards Number 70* - SAS 70) ile ilgili bir bildiri yayınladı. Bu, kendi türünün ilk standardıydı ve birçok hizmet kuruluşu için denetleme rehberliği sağlamıştır. SAS 70, sigorta ve tıbbi hasar işlemcileri, telekominikasyon servis sağlayıcıları, yönetilen servis sağlayıcıları ve kredi kartı işlem işlemci şirketleri gibi kuruluşlar için geliştirildi. İki tip SAS 70 denetlemesi vardı: Tip I ve Tip II. Bir SAS 70 Tip I denetlemesi, hizmet denetçisinin çevre denetim hedeflerine ulaşmak için hizmet kuruluşu tanımının ve denetimlerin uygulanmasının değerlendirmesini kapsar. Bir SAS 70 Tip II denetlemesi, Tip I denetlemesindeki bilgileri ve ayrıca hizmet denetçisinin, tanımlanan denetimlerin etkili bir şekilde uygulanıp yürütülmediğinin

değerlendirmesini içerir. SAS 70 kendi kapsamında genel olmasına rağmen, standart bugünkü hizmet organizasyonlarında karşılaşılan yeni sorunların çoğunu ele alamadı. Örneğin SAS 70, ortak yerleşim desteğini veya bulut tabanlı hizmetler sunmayı desteklemez. SAS 70, Haziran 2011'de resmi olarak emekli oldu.

2011'de Atama Görevleri Standartlarına İlişkin Açıklamalar No.16 (*Statement on Standards for Attestation Engagements Number 16* - SSAE 16), SAS 70'in yerini aldı. SSAE 16, SAS 70'in kapsamını genişletti ve hizmet kuruluşları için denetleme ve raporlama standatlarının başında geldi. SSAE 16, denetimleri ve süreçleri doğrularken denetçilere rehberlik eder. SSAE 16 aynı zamanda, düzenlenen denetleme raporlarının incelenen denetimlerin tasarımı ve etkinliği ile ilgili açıklamaları içermesini de gerektirir. Bu raporlar, kuruluşun spesifik denetimlerini tanımlayan ayrıntılar sağlar. Örneğin, bir veri merkezinde yer kiralamaya çalışan bir şirket, veri merkezinden SSAE 16 veya SAS 70 denetleme sonuçlarını iletmesini isteyebilir.

SAS 70'in ve şu anki SSEA 16'nın sonuçlarına olan güven birçok organizasyonda artmıştır. AICPA, hizmet organizasyonlarının artan karmaşıklıklarını farkına varmış ve hizmet organizasyonları için üç farklı denetleme raporlaması seviyesi yaratmıştır. Hizmet Organizasyonu Kontrolü (*Service Organization Control* - SOC) çerçevesi, üç denetleme raporlarının seviyesini ve içeriğini tanımlar. **TABLO 7-1**, SOC raporlarını ve her birinin özelliklerini listeler.

SOC 1, SOC 2 ve SOC 3 raporları, bir kuruluşun denetçileri için önemli araçlardır. SOC 1 raporu öncelikli olarak, finansal raporlama üzerindeki iç denetimlere (*Internal Controls over Financial Reporting* - ICFR) odaklanmaktadır. Bu tür bir rapor genellikle, kullanıcı organizasyonu için finansal tablolar hazırlamak ve finansal raporlama gerekliliklerini tarafından üretilen verilerin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak için uygun denetimleri uygulamak için kullanılır. SOC 2 ve SOC 3, öncelikli olarak güvenlikle ilgili denetimleri ele alıyor. Bu raporların güvenlikle ilgili denetimleri, günümüzün teknoloji hizmet sağlayıcı kuruluşların başarısı için kritik önem taşır. SOC 2 ve SOC 3 raporlarının başlıca farkı hitap ettikleri kitlelerdir. SOC 2 raporları iç ve diğer yetkili paydaşlar için oluşturulmuştur; SOC 3 raporları ise halkın kullanımına yöneliktir.

NOT

SAS 70 hakkında daha fazla bilgi için bkz. *http://sas70.com*. SSAE 16 hakkında daha fazla bilgi için *http://ssae16.com* adresini ziyaret edin. SOC 1, SOC 2 ve SOC 3 raporları hakkında daha fazla bilgi için bkz. *www.ssae16.org/white-papers*.

TABLO 7-1 Hizmet Organizasyonu Kontrolü (Service Organization Control - SOC) raporları.

RAPOR TİPİ	İÇERİK	HEDEF KİTLE
SOC 1	Finansal raporlama için iç denetimler	Kullanıcılar ve denetçiler. Bu, Sarbanes-Oxley (SOX) veya Gramm-Leach-Bliley Yasası'na (Gramm Leach Bliley Act - GLBA) uymaları gereken kuruluşlar için yaygın olarak uygulanmaktadır.
SOC 2	Güvenlik (gizlilik, bütünlük, kullanılabilirlik) ve mahremiyet denetimleri	Yönetim, düzenleyiciler, paydaşlar. Bu, genellikle servis sağlayıcılar, barındırılan veri merkezleri ve yönetilen bulut bilişim sağlayıcıları için uygulanır.
SOC 3	Güvenlik (gizlilik, bütünlük, kullanılabilirlik) ve mahremiyet denetimleri	Halka açık. Bu, genellikle SOC 2 servis sağlayıcılarının müşterilerinin, kuruluşun müşteri özel verilerini ve uyumluluk yasası gereksinimlerini (HIPAA ve GLBA gibi) karşılamakta olduğunu doğrulamak ve onaylamak için gereklidir.

Denetleme Planınızı Tanımlama

Denetleme faaliyetlerini planlarken, denetçi öncelikle hedefleri tanımlamalı ve hangi sistemlerin veya iş süreçlerinin gözden geçirileceğini belirlemelidir. Denetçi, incelenmesi gereken güvence alanlarını da tanımlamalıdır.

Bir denetçi, denetlemede yer alacak personeli de —hem kendi ekibinden hem de incelenen kuruluştan— tespit etmelidir. Bu insanlar, denetlemenin ilerlemesini sağlamak için bilgi toplayacak ve bir araya getirecektir. Denetçi, herkesin doğru becerilere sahip olduğundan, katkıda bulunmaya hazır olduğundan ve ihtiyaç duyulduğunda erişilebilir olduğundan emin olmalıdır.

Bazı denetçiler geçmişteki sorunlar hakkında bilgi sahibi olmak için önceki denetlemeleri gözden geçirir. Diğer denetçiler ise, önceki sonuçlardan önyargı oluşturmamak adına önceki denetlemeleri gözden geçirmemeyi tercih eder.

Planın Kapsamını Belirleme

Gözden geçirmenin sınırlarını projenin başında tanımlamalısınız. Gözden geçirmenin hangi alanları kapsayacağını belirlemek önemlidir. Geçerli denetlemede gözden geçirilmemiş alanların başka bir denetlemeye tabi tutulacağından ve bu alanlar için sorumluluk yüklenecek olacağınızdan emin olmalısınız. Tüm sistemlerin ve ağların açıkça belirlenmiş bir sahibinin olması gerekir. Bazı durumlarda denetleme kapsamı tek bir kuruluşun ötesine geçer. Kuruluşunuz veri veya işlemlerini dışarıdan alıyorsa, kuruluşunuz dışında var olan varlıkları da denetlemeye eklemeniz gerekebilir. Birlikte işlerlik anlaşması yoluyla eriştiğiniz bileşenleri denetlemeniz gerekebilir. Denetlemenin kapsamını belirlemek, dış kuruluşlarla etkileşimi gerektirebilir.

> **NOT**
>
> Kaynak kısıtlamaları nedeniyle bir kuruluşun her bölümünü denetlemek ve tüm dış kaynak ortaklarıyla bağlantı kurmak mümkün olmayabilir. Denetçiler, en yüksek risk alanlarına öncelik vermelidir.

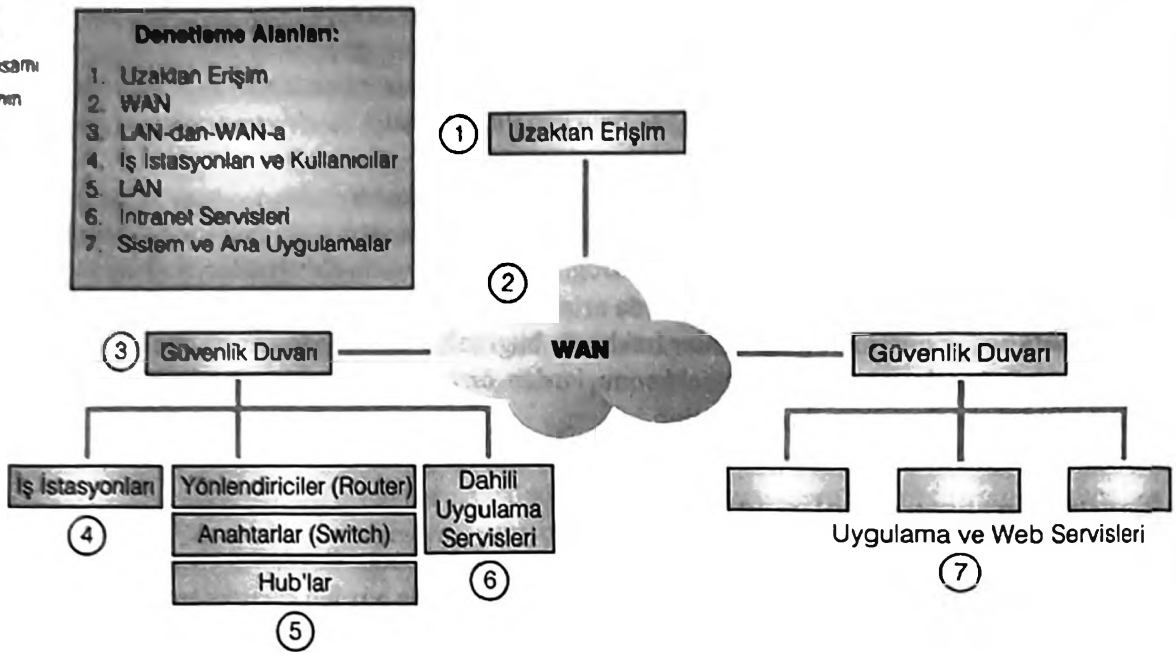
Bu noktada, denetlemenin devam edeceğini kime bildirmeniz gerektiğine karar vermeniz gerekir. Çoğu durumda, kullanıcılar onları incelediğinizi biliyorsa, daha önce göz ardı ettikleri kurallara uymaya başlayabilirler. Bir denetleme hakkında bilgi sahibi olmak kullanıcı davranışını değiştirirse, denetlemeniz doğru olmayacaktır. Öte yandan, personeli bilgilendirmeden bir denetleme yapmaya çalışmak, kritik bilgilere erişimi sınırlandırarak işi zorlaştırır. Bu dengeyi olay/vaka bazında değerlendirmelisiniz. **ŞEKİL 7-2**, denetleme kapsamının BT (Bilgi Teknolojileri) altyapısındaki yedi etki alanının tamamına nasıl yayıldığını göstermektedir.

Bir denetçi, herhangi bir denetleme faaliyeti yürütmeden önce uygun bir şekilde bir denetleme planlamak için zaman ayırmalıdır. Planlama, incelenecek dosyaları ve belgeleri listelemekten çok daha fazlasıdır. Aslında, denetçiler genellikle denetleme için hazırlanan önemli miktarda iş yapar. Planlama ve yürütme aşamalarında bir denetçiden neler bekleyebileceğiniz aşağıda belirtilmiştir:

- **Ortamları ve Sistemleri Araştırma**—Bir denetçi, denetleme faaliyetlerine başlamadan önce ortamları ve sistemler arasındaki bağlantıları anlamayı isteyecektir.
- **Belgelerin incelenmesi**—Bir denetçi, hem planlama sırasında hem de asıl denetlemenin bir parçası olarak sistem dokümantasyonlarını ve yapılandırmalarını gözden geçirmek isteyecektir. Denetlemeler harici ortaklar içerdiğinde, birlikte çalışma anlaşması gereksinimlerinin gözden geçirilmesi gereklidir. Bu belgeler, dış kaynak ortakları için üzerinde anlaşılmış uyumluluk gerekliliklerini belirtmektedir.

ŞEKİL 7-2

Denetleme kapsamı ve BT altyapısının yedi etki alanı



- **Risk analizi çıktısını gözden geçirin**—Bir denetçi, risk analiz çalışmalarının bir ürünü olan sistem kritik derecelendirmelerini anlamak isteyecektir. Bu, raporlama aşamasında sistemlerin azaltmaya uygun sıraya yerleştirilmesine yardımcı olur.
- **Sunucu ve uygulama günlüklerini gözden geçirin**—Bir denetçi günlükleri inceleyerek programlarda, izinlerde veya yapılandırmalarda değişiklik olup olmayacağını sorgulayabilir.
- **Ayrıcalıklı olay günlüklerini gözden geçirin**—Bir denetçi, sorun eğilimleri hakkında fikir edinmek için güvenlik olayı günlüklerini gözden geçirmek isteyebilir.
- **Penetrasyon testlerinin sonuçlarını gözden geçirin**—Bir kuruluş penetrasyon testleri uyguladığında, test eden bulunan zayıf yönleri içeren bir rapor hazırlar. Denetçinin bu raporu gözden geçirmesi ve denetlemenin tüm öğelerini ele aldığından emin olması gerekir.

Denetleme Karşılaştırmalı Değerlendirme

Bir **karşılaştırmalı değerlendirme (*benchmark*)**, sisteminizin güvenli bir şekilde yapılandırılıp yapılandırılmadığını belirlemek için karşılaştırılma amaçlı kullanılan bir standarttır. Denetlemedeki tekniklerden biri, farklılıkları belirlemeye yardımcı olmak için bir bilgisayarın veya aygıtın geçerli ayarını bir karşılaştırma ölçütüyle kıyaslamaktır.

Bu bölümde, sistemleri, iş süreçlerini veya güvenlik denetimlerini gözden geçirmeyi veya denetleme yapmanın genel yollarını bulacaksınız. Bu örneklerin tümü iyi uygulama örnekleridir. Genellikle bir işi veya iş sürecini denetleme prensipleri olarak kullanılırlar. Kuruluşunuzun yönetimi, aşağıdaki örneklerden birini resmen kabul etmiş olabilir. Bu, kuruluşunuzun, devlet düzenlemelerine veya mevzuata tabi olması durumunda özellikle doğru olabilir. Eğer öyleyse, değerlendirme deneyleri, denetlemenizin ana gidişatını yönlendirir. Aksi takdirde, denetçi, üst yönetimin onayı ile bir denetlemenin nasıl gerçekleştirildiğine karar verir.

- **ISO 27002**—ISO 27002, bilgi güvenliği yönetimi için iyi yönergeler sunan en iyi uygulamalar (*best-practices*) belgesidir. Bir kuruluşun uygunluk talebinde bulunması için, tüm hükümlerin

yerine getirildiğini doğrulamak için bir denetleme gerçekleştirmesi gerekir. ISO 27002, bilgi güvenliği standartlarını tanımlayan büyüyen bir standart paketi olan ISO 27000 serisinin bir parçasıdır.

- **NIST Siber Güvenlik Çerçevesi (*Cybersecurity Framework* - CSF)**—Amerika Ulusal Standartlar Enstitüsü NIST, CSF çerçevesini ilk olarak 2014 yılında, artan siber güvenliğe yönelik olarak ABD Başkanlık emriyle yayımlanmıştır. Kritik altyapı bileşenleri üzerinde yoğunlaşmaktadır ancak birçok genel sistem için de geçerlidir. Yol haritası, denetçilerin iş sürücülerini ve güvenlik gereksinimlerini toparlamasına yardımcı olabilecek sistemleri güvence altına alacak yapılandırılmış bir yöntem sağlar. NIST aynı zamanda bilgi sisteminin birçok yönünü kapsayan bir dizi özel yayın yayınlamaktadır. Örneğin, NIST SP 800-37 standardı, ABD hükümeti bilgi sistemleri için denetleme de dahil olmak üzere en iyi uygulamaları tanımlayan bir standarttır.
- **Bilgi Teknolojisi Altyapı Kütüphanesi (*Information Technology Infrastructure Library* - ITIL)**—Bu, BT altyapısını, gelişimini ve operasyonlarını yönetmek için kullanılan bir dizi kavramlar ve politikalar bütünüdür. ITIL, her biri ayrı bir BT yönetimi konusunu kapsayan bir dizi kitapta basılmıştır. ITIL, kapsamlı bir denetim listeleri, görevler ve herhangi bir BT organizasyonunun kendi ihtiyaçlarına göre düzenleyebileceği yönetmeliklerle, bir dizi önemli BT uygulamalarına ilişkin ayrıntılı bir açıklama sunar.

NOT

NIST SP 800, en iyi pratik belgeler dizisidir. Web sitesi, http://csrc.nist.gov/, önce listelenen en yeni belgelerle düzenlenir. Düzeltmeler numarayı değiştirmediğinden, düşük numaralı öğeler hala geçerli olabilir.

ISACA ve İç Denetçiler Enstitüsü (*Institute of Internal Auditors*) gibi diğer kuruluşlar, yaygın olarak kullanılan denetleme çerçevelerini geliştirmiştir. Kuruluşunuz kendi içinde bir dizi kurallar hazırlayabilir veya başka bir yerde geliştirilen bir denetleme çerçevesini benimseyip ve özelleştirebilir. İşte bu tür çerçevelere ilişkin iki örnek:

- **COBIT**—Bilgi ve İlgili Teknolojiler için Denetim Amaçları (*Control Objectives for Information and related Technology* - COBIT), BT yönetimi için en iyi uygulamalardan biridir. 1996'da Bilgi Sistemleri Denetimi (*Information Systems Audit* - ISA), Kontrol Birliği (*Control Association* - ISACA) ve BT Yönetim Enstitüsü (*IT Governance Institute* - ITGI) tarafından oluşturuldu. COBIT, yöneticilere, denetçilere ve BT kullanıcılarına genel olarak kabul edilen ölçütleri, göstergeleri, süreçleri ve iyi uygulamaları verir. COBIT'i, bilgi teknolojisinin kullanımından en fazla fayda sağlamaya yardımcı olmak ve bir şirkete uygun BT yönetimi ve denetimi geliştirmek için kullanabilirsiniz.
- **COSO**—İç Denetçiler Enstitüsü (*Institute of Internal Auditors* - IIA), Treadway Komisyonu'nun Sponsor Kuruluşları Komitesini (*Committee of Sponsoring Organizations* - COSO) oluşturur. Bu gönüllü kuruluş, idari yönetim ve yönetim kuruluşlarına, kurumsal yönetim, iş ahlakı, iç denetim, kurumsal risk yönetimi, dolandırıcılık ve finansal raporlamanın kritik yönleri hakkında rehberlik etmektedir. COSO ortak bir iç denetim modeli oluşturmuştur. Birçok şirket ve diğer kuruluşlar denetim sistemlerini değerlendirmek için kullanmaktadır.

Bir kanun veya yönetmelik bunu yasaklamazsa, kuruluşlar kendilerine en uygun denetleme yöntemini seçme konusunda özgürdür. Burada bahsedilen seçeneklerden birini kullanabilir veya başka bir kuruluştan ya da ticaret grubundan gelen yönergeleri kullanabilirler. Kendi belgelerini bile geliştirebilirler. Hangi yöntem gereksinimlerinize en iyi uyuyorsa, ilk denetlemenizi yapmadan önce takip etmeniz gereken bir denetleme yönteminiz olduğundan emin olun.

Denetleme İçin Veri Toplama Yöntemleri

Verileri analiz edebilmeniz için, bu verileri tanımlamanız ve toplamanız gerekir. Aşağıda gösterildiği gibi, veri toplamanın birçok yolu vardır:

- **Anketler**—Hazırlanan anketleri hem yöneticilere hem de kullanıcılara yöneltebilirsiniz.
- **Röportajlar**—Bunlar, tüm tarafların operasyonları hakkında fikir edinmek için kullanışlıdır. Röportajlar genellikle değerli bilgi kaynakları ve tavsiyelerdir.
- **Gözlem**—Bu, kağıt üstündeki yönetmelikler ile işin gerçekten nasıl yapıldığı arasındaki ayrımı yapmak için kullanılan girdiyi belirtir.
- **Yapılacak işler listeleri**—Bu hazırlanan belgeler, bilgi toplama sürecinin tüm alanları kapsadığından emin olmanıza yardımcı olur.
- **Belgelerin gözden geçirilmesi**—Bu belgeler ile geçerli, ilintili ve tam olma değerlendirilir.
- **Yapılandırmaların gözden geçirilmesi**—Bu gözden geçirme, değişim denetim yönetmeliklerini ve kuralların, denetimlerin ve düzenin uygunluğunun değerlendirilmesini içerir.
- **Politikanın gözden geçirilmesi**—Bu gözden geçirme, politikanın ilgililiğinin, geçerliliğinin ve tamlığının değerlendirmesini içermektedir.
- **Güvenlik testlerinin yapılması**—Zafiyet testi ve penetrasyon testinden oluşan bu sınama; ağlar, uygulamalar veya güvenlik bileşenleri içinde güvenlik açıkları olup olmadığını belirlemek için teknik bilgi toplamayı içerir.

Güvenlik Denetleme Alanları

Denetleme sürecinin bir parçası, politika tablolarının tüm kilit alanlar için mevcut olmasını sağlamaktır. Denetçiler, politikanızın ele almadığı önemli alanları ortaya koyar. Bundan sonra, tüm personelin politikaları, yönetmelikleri ve standartları takip edip etmediklerini denetlerler.

Erişim denetim politikasını desteklemek için bir parola standardına (minimum karakter ve karmaşıklık) ve bir parola yönetmeliğine (parolaları ayarlama, değiştirme ve sıfırlama yönergeleri) ihtiyacınız olacaktır. Birçok kuruluş, parola politikalarını sistem erişim ilkeleri olarak kullanmaktadır. Bu tehlikeli bir hatadır. Aşağıdakine benzer bir şey söyleyen ayrı bir erişim denetimi politikası geliştirmelisiniz:

> Yetkili kullanıcılar yalnızca yetkili olduklarını yapabilmelidir. Yetkisiz kullanıcıların herhangi bir şey yapmaları yasaklanmalıdır.

Parolalar çoğu zaman saldırıların hedefi olduğundan, parolaların kullanımı azalıyor. Bunun yerine, pek çok kuruluş kimlik doğrulamak için belirteçleri, akıllı kartları veya biyometrikleri kullanmaya başlıyor. (Elbette, daha önceki bir bölümde öğrendiğiniz gibi, bu kimlik doğrulama türlerinin bir kombinasyonu daha da iyidir.) BT ortamınız değiştikçe, politikalarınızın da değiştiğinden emin olun. Sistemlerin yarısı akıllı kartlar kullandığında tüm erişim denetim politikalarının parola gücünü

NOT

Denetleme süreci, kuruluşunuzun daha güvenli olmasını sağlamak için tüm tarafların birlikte çalıştığı bir işbirliği düzenlemesi olmalıdır. Bunu "biz onlara karşı" olarak görmemeniz gerekir. Denetçilerin ve denetlenen kuruluşun her ikisi de aynı amaca yönelik olarak çalışmalıdır: daha güvenli bir ortam.

belirlemesini istemezsiniz. Kapsamlı bir denetleme, güvenlik politikanızın güncel olduğunu ve mevcut ortamınızı yansıtıyor olmasını sağlar. Güncelliğini yitirmiş olan tüm politikaları saptamanız ve kaldırmanız gerekir.

TABLO 7-2, bir güvenlik denetlemesine mutlaka eklemeniz gereken kritik alanların birkaçını göstermektedir.

Denetimlerin Gözden Geçirilmesi ve Kimlik Yönetimi

Güvenlik denetimlerinin etkili, güvenilir ve istediğiniz gibi çalıştığından emin olmasını sağlamak önemlidir. İzleme ve inceleme yapmadan, bilgi güvenliği programınızın etkili olduğuna veya personelin gereken özeni gösterdiğine dair herhangi bir güvenceye sahip olamazsınız. Bir kimlik yönetim sistemini incelerken, bu kilit alanlara odaklanmalısınız:

- **Onay süreci**—Erişim talepleri kim tarafından onaylanır?
- **Kimlik doğrulama mekanizmaları**—Belirli güvenlik gereksinimleri için hangi mekanizmalar kullanılır?
- **Parola politikası ve uygulanması**—Kuruluşun etkili bir parola politikası var mıdır ve eşit olarak herkese uygulanmakta mıdır?
- **İzleme**—Kuruluş, yetkisiz erişimi tespit etmek için yeterli izleme sistemine sahip midir?
- **Uzaktan erişim sistemleri**—Tüm sistemler güçlü kimlik doğrulama ile düzgün bir şekilde korunmakta mıdır?

> **NOT**
>
> Denetçiler, denetleme sırasında, ne bulduklarını kontrol etmek için rutin olarak yönetimle konuşurlar. Denetçiler hata yapabilir ve bu, yönetimin yanlış anlaşılmaları düzeltme ve denetçilerin nihai raporunu sunmadan önce durumlarını bildirme imkânı verir.

TABLO 7-2 Bir denetleme planına dahil etmeniz gereken alanlar.

ALAN	DENETLEME HEDEFİ
Antivirüs yazılımı	Güncel, evrensel uygulama
Sistem erişim politikaları	Teknoloji ile güncel
Saldırı tespiti ve olay izleme sistemleri	Günlük değerlendirmeleri
Sistem güçlendirme politikaları	Erişim noktaları, servisler
Kriptografik kontroller	Şifre anahtarı yönetimi, kullanım (hassas verilerin ağ şifrelemesi)
Beklenmedik durum planlaması	İş sürekliliği planı (*Business continuity plan* - BCP), felaket kurtarma planı (*disaster recovery plan* - DRP) ve operasyon planının sürekliliği (*continuity of operations plan* - COOP)
Donanım ve yazılım bakımı	Bakım anlaşmaları, hizmet, gelecekteki ihtiyaçların tahmini
Fiziksel güvenlik	Kapılar kilitli, güç kaynakları görüntüleniyor
Erişim denetimi	Bilinmesi gereken (*need-to-know*), en düşük erişim hakkı (least *privilege*)
Yapılandırma yönetimi için kontrol süreçlerinin değiştirilmesi	Dokümante edilmiş, yetkilendirilmemiş değişiklikler yok
Medya koruması	Medya yaşı, etiketleme, depolama, ulaşım

Denetleme Sonrası Faaliyetler

Denetleme faaliyetleri tamamlandıktan sonra denetçilerin hala yapması gereken çok iş vardır. Bu ek denetçi görevleri arasında; çıkış mülakatları, veri analizi, denetleme raporunun oluşturulması ve bulguları yönetime sunma bulunur.

Çıkış Mülakatları

Denetçi, denetleme raporlamasında sonradan gelecek olan kişiye önemli konuları ve tavsiyeleri bildirmek için kilit personelle bir çıkış mülakatı yapar. Bu, yönetimin ciddi sorunlarda hızlı tepki vermesini sağlar. Bu erken uyarıların yanı sıra, denetçiler nihai rapordan önce ayrıntı vermemelidir. Yaparlarsa, örgütün güvenlik hazırlığına yanlış bir yön verebilirler.

Veri Analizi

Denetçiler, veri transferi işlemine izin verilirse, topladıkları verileri kurumdan uzakta, kurum dışında analiz eder. Bu, denetçinin öğrendiği her şeyi gözden geçirmesini ve gözlemleri standart bir rapor formatıyla sunmasını sağlar. Dışarıda gerçekleştirilen analiz, denetçilerin kurum içinde bulunduklarında sıklıkla karşılaştıkları baskılardan kaçınmalarını sağlar. Her organizasyon olumlu bir denetleme raporu almak ister ve bu arzu bazen bir denetçi için ince bir baskıya dönüşür. Denetlemeye tabi tutulan organizasyondan farklı bir yerde veri analizi yapmak, tarafsız analizin yapılmasına yardımcı olabilir.

Denetleme Raporunun Oluşturulması

Denetleme raporları genellikle en az üç geniş bölüm içerir:

- **Bulgular**—Bunlar genellikle standart ölçütlere uyma düzeyine göre listelenir. Denetleme; bulgularının belirtilen bir politikayla veya sektörün en iyi uygulamaları ile karşılaştırır, kuruluşun iyileştirilmesi gereken yerlerini tanımlar.
- **Öneriler**—Denetçiler, buldukları risklerin nasıl düzeltileceği yönünde öneride bulunur. Ayrıca personelin bir politikaya veya sürece nasıl uymadığını da söyler. Raporların çoğunda, öneriler öncelikle en önemli konuları ele alır. Denetleme önerileri şunları içermelidir:
  - **Gerçekleştirme için zaman çizelgesi**—Değiştirme önerilerin ucu açık olmamalıdır. Her öneri için önerilen bir son teslim tarihi olmalıdır.
  - **Risk seviyesi**—Denetleme, kuruluşun her bulgu ile karşılaştığı risk seviyesini netleştirmelidir.
  - **Yönetim yanıtı**—Denetçiler, yönetimin denetleme raporunun taslak bir kopyasına cevap verme fırsatı vermelidir. Daha sonra bu yanıtı nihai raporda belirtmelidir. Bu yanıt genellikle sorunları açıklığa kavuşturuyor ve denetimlerin neden kullanılmadığını veya taslak metindeki önerilerin gerekli olmadığını açıklıyor olmalıdır. Yanıt, denetimlerdeki boşlukları gidermek için eylem planları da içerebilir.

NOT

Çoğu denetleme raporu doğrudan konuya girer. Bir denetleme raporu genellikle bir özetle başlar ve detaylar gelir. Özet, kuruluşun liderliğinin dışında bir yol bulur, bu yüzden güvenlik zayıflıklarını ortaya çıkarmamak için dikkatli olmanız gerekir. Özel veya gizli bilgileri yalnızca raporun ayrıntılar bölümüne eklemelisiniz ve bu bilgileri her zaman uygun bir şekilde etiketlemelisiniz.

- **Takip**—Gerektiğinde denetçiler, kuruluşun tavsiyelere uyduğundan emin olmak için takip eden bir denetleme programlamalıdır.

Bulguların Sunulması

Denetçiler denetleme raporunu tamamladığında bulguları kuruluşa sunar. Kuruluşunuzun yapısına ve boyutuna bağlı olarak, bulguların sunumu resmi bir toplantı şeklinde olabilir veya yalnızca raporu tek bir kişiye teslim etmeyi içerebilir. Denetleme bulgularını nasıl elde ettiğinize bakılmaksızın, denetlenen kuruluşun raporu incelemesi ve gerekli değişiklikleri yapması önemlidir. Bulgular, düzenleyici gereksinimlere veya mevcut bütçeye dayalı değişikliklere neden olabilir.

Güvenlik İzleme

Bir güvenlik programının ilk amacı, bir kuruluşun güvenlik duruşunu belirlemektir. Güvenlik politikası güvenlik duruşunu tanımlar ancak güvenlik programı bu politikayı eylemler halinde yerine getirir. Bir güvenlik duruşu, bir kuruluşun başlangıç yapılandırmalarını nasıl belgelediğini, eylemleri nasıl takip ettiğini ve algılanan sorunları nasıl düzelttiğini tanımlar. İzleme (*monitoring*), herhangi bir güvenlik programının önemli bir parçasıdır. İzlemenin birincil amacı anormal davranışları tespit etmektir. Sonuçta, algılayamadığınız davranışları düzeltemezsiniz! Güvenlik izleme sistemleri, saldırı tespit sistemi (*Intrusion Detection System* - IDS) gibi teknik nitelikte olabilir veya idari konumda olabilir, örneğin kapalı devre TV'de çalışanların veya müşterilerin davranışlarının gözlemlenmesi.

Anormal veya kabul edilemez bir davranış tespit ettiğinizde, bir sonraki adım onu durdurmaktır. Hem açık hem de gizli izinsiz eylemleri durdurmak hem bir sanat hem de bir bilimdir. **Açık eylemler (*overt acts*)** aşikar ve kasıtlıdır. **Gizli eylemler (*cover acts*)** saklı ve bilinmezdir.

Çoğu saldırgan, bulundurduğunuz izleme denetimlerinden kaçınmaya çalışacaktır. Aslında, güvenlik izleme denetimlerinin varlığı birçok saldırganı caydırabilir. Öte yandan, çok fazla izleme cihazına sahip olmak mümkündür. Güvenlik izleme, güvenlik ihlallerini önlemek için yeterince belirgin fakat baskıcı bir otoriteyi çağrıştırmamak için yeterince gizli olmalıdır.

Güvenlik izleme için bazı araçlar ve teknikler aşağıdakileri içerir:

- **Dayanak noktaları**—Bir şeyi anormal olarak tanımak için, önce normalin neye benzediğini bilmelisiniz. Dün veya hatta geçen hafta ne kadar disk alanının kullanıldığını bilmediğiniz sürece, bir sistemin disk alanının yüzde 80 oranında dolu olduğunu bildiren bir rapor görmek, size hiçbir şey söylemez. Yani, her hafta ek bir yüzde 1 disk kullanan ve alarmı veren bir sistem ile geçen ay yüzde 40 olan fakat aniden kullanımda ikiye katlanan bir sistemden çok farklıdır. Güvenlik izleme için dayanak noktaları önemlidir.
- **Alarmlar, uyarılar ve eğilimler**—Alarmlar ve uyarılar, bir kapı açılma uyarısı veya bir yangın alarmı gibi olası bir güvenlik olayını personele bildiren güvenlik olaylarına verilen yanıtlardır. Tespit edilen güvenlik olaylarını rapor etmek, güvenli bilgi sistemlerini korumak için gereklidir. Bir alarm ve uyarı arasındaki fark, varlığın durumuna bağlıdır. Bir alarm kurulu değilse, kapının açılması bir uyarı üretir. Bununla birlikte, bir alarm kuruluysa, kapının açılması bir alarm üretir. Bu, ev alarm sisteminiz gibi çalışır. Gün boyunca, bir kapının açılması sistemin bir ses tonu (uyarı) oluşturmasına neden olabilir, ancak geceleri kapı açıldığında bir alarm tetiklenir. Çalışanların tekrarlanan yanlış alarmları hızlı bir şekilde yok sayacağının farkında olun. Örneğin, komşunuzun araba alarmı tekrar tekrar çalarsa, her seferinde pencereye

gitmezsiniz. Bu da, çalışanlar muhtemelen gerçek bir olaya cevap vermeyeceklerdir anlamına geliyor. Bu nedenle, uyarıları ve alarmları depolamak, olayların zaman içinde nasıl gerçekleştiğini göstermeyi mümkün kılar. Bu tür analiz eğilimleri belirlemeye yardımcı olur. Eğilim analizi, denetmenlerin yalnızca bireysel etkinliklere odaklanmalarından fazlasına yardımcı olur.

- **Kapalı devre televizyon (TV)**— Uygun bir şekilde kullanılan bir kapalı devre TV, TV kameralarının gördüklerini izlemesi ve kaydetmesi gerekir. Kameraları görüntüleyen güvenlik görevlilerinin belli eylemleri veya davranışları izlemek üzere eğitildiğinden emin olmalısınız. Personeliniz ayrıca yerel yasalar konusunda eğitilmiş olmalıdır; birçok ülke, ırk veya etnik kökene dayalı profillemeyi yasaklar.
- **Düzensiz davranışı yakalayan sistemler**—Örneğin, IDSler ve honeypot tuzakları; başka bir deyişle, bir ağdaki uygunsuz etkinlikle ilgili bilgi toplamak için altyapı kurulmuş olmalıdır.

Bilgisayar Sistemleri için Güvenlik İzleme

Tıpkı birçok fiziksel izleme denetim türü olduğu gibi, bilgisayar ve ağ sisteminin etkinliğini izlemek için birçok yol da vardır. Kötü amaçlı faaliyetleri saptamak için bilgiişlem ortamınızı birçok açıdan görüntüleyen denetimleri seçmelisiniz. Sisteminizde, hem olay gerçekleşirken hem de olaydan sonraki etkinlikleri izlemenize yardımcı olacak birçok araç bulunmalıdır.

Gerçek-zamanlı izleme (*real-time monitoring*), gerçekleşen olaylarla ilgili bilgi sağlar. Bu tür izleme, proaktif bir güvenlik durumunun sürdürülmesinde önemlidir. Gerçek zamanlı izleme denetimlerinden gelen bilgileri, olayları içerecek şekilde kullanabilir ve kuruluşunuzun ticari faaliyetlerini koruyabilirsiniz. Bir ağ saldırı tespit sistemi gerçek zamanlı izleme denetiminin bir örneğidir. Ağ trafiğini ağınız boyunca dolaşırken izler ve yakalar. Bu tip denetim örnekleri arasında aşağıdakiler bulunur:

- **Ana bilgisayar IDS**—Bir ana bilgisayar saldırı tespit sistemi (*Host Intrusion Detection System* - HIDS), bir bilgisayar etkinliğini gerçekleşirken "farketmek" için mükemmeldir. IDS kuralları şüpheli etkinliği neredeyse gerçek zamanlı olarak saptamaya yardımcı olur.
- **Sistem bütünlüğünü izleme**—Tripwire (tetikleyici mekanizma) gibi sistemler, yetkisiz değişiklikler için bilgisayar sistemlerini izlemenizi ve neredeyse gerçek zamanlı olarak yöneticilere raporlamanızı sağlar.
- **Veri kaybını önleme (*Data Loss Prevention* - DLP)**— DLP sistemleri, yetkisiz son kullanıcıların hassas bilgileri paylaşmasını önlemek için iş kurallarını kullanarak bu hassas bilgileri sınıflandırır. DLP'nin koruduğu veriler genelde ifşa edildiği takdirde bir kuruluşu risk altına sokabilecek verilerdir. Örneğin, DLP sistemleri, kullanıcıların hassas veriler için Dropbox gibi harici depolama hizmetleri kullanmalarını engeller.

Gerçek zamanlı olmayan izleme, geçmiş etkinlik kayıtlarını tutar. Olayları anında tespit etmek ve olaylara anında cevap vermek kritik olmadığında bu türden bir izleme kullanabilirsiniz. Bu tip denetim örnekleri arasında aşağıdakiler bulunur:

- **Uygulama günlüğü**—Hassas verilere erişen veya bu verileri değiştiren tüm uygulamalar, verileri ne zaman ve kimin kullandığını veya değiştirdiğini kaydeden günlüklere sahip olmalıdır. Bu günlükler, gizlilik düzenlemelerine ilişkin uyumluluğu belgelemeyi, kayıtlarla ilgili sorunların veya hataların incelenmesini ve işlemlerin izlenmesini destekler.

- **Sistem günlüğü**— Bu türden kayıtlar, sisteme erişenlerin kayıtları ile sistem üzerinde gerçekleştirdikleri işlemleri kayıt eder.

Aşağıda, günlüğünü tutmanız gereken faaliyetlerin kısmi bir listesi verilmektedir:

- **Ana bilgisayar tabanlı etkinlikler**—Bunlara; sistemdeki değişiklikler, erişim talepleri, performans verileri ile açılışlar ve kapatmalar dahildir.
- **Ağ ve ağ cihazları**— Bunlar; erişim, trafik türü ve örüntüleri, zararlı yazılımlar ve performans verilerini içerir.

İzleme Sorunları

Günlük tutmanın maliyeti vardır. Sistem veya uygulama etkinliğini günlüğe kaydetmeyi seçtiğinizde, bu bilgiyi bir yerde saklamanız gerekir. Birçok organizasyon çok fazla bilgi ürettikleri için günlük tutmayı kapatır. Sonuçta, günlükleri gözden geçirmek için yeterli personel yoksa, tüm bu verilerin toplanmasının nedeni nedir? Günlük verilerini otomatik olarak analiz etmenin bir yolu olmadan, günlük yalnızca disk alanı kullanır. Başka bir değer sağlamaz. Diğer zorluklar arasında, günlük verisinin kalitesizliği ve saldırıların karmaşıklığı bulunur. Genelde, günlükleri analiz etmek için personelin kaybettiği zamanın değerini görmek zordur.

NOT

Kuruluşlar, veriler ağ üzerinden iletilirken tüm hassas verilerin şifrelendiğinden emin olmak için trafiği izlemelidir.

Bazı kuruluşları agresif izleme faaliyetinden korkmasına neden olan diğer izleme sorunları şunları içerir:

- **Mekansal dağılım.** Saldırılar geniş bir alanda birçok saldırgandan geliyorsa, günlüklerle bu saldırıları yakalamak zordur. Daha da kötüsü, saldırganlar farklı yöneticiler tarafından yönetilen ve geniş bir alana yayılmış bir dizi bilgisayar kullanabilir.
- **Anahtarlamalı ağlar.** Anahtarlar ve sanal LAN'lar aracılığıyla çok parçalı ağlarda trafiği yakalamak zor olabilir. Bölünmüş günlük dosyalarından gerçekte olanları yeniden yapılandırmak günlük tutmaktan daha büyük bir iştir.
- **Şifreleme.** Verileri şifrelemek, günlük üzerinden izlemeyi zorlaştırır, çünkü izleme araçları bir etkinliğin şüpheli olup olmadığına karar vermek için tüm veriyi göremez. Şifrelenmemiş parçalar kullanılabilir ancak gerisi neredeyse görünmezdir. Verileri çeşitli düzeylerde şifreleyebilirsiniz:
  - **Veri Bağlantısı Katmanı şifrelemesi (*Kablolu Eşdeğer mahremiyet (Wired Equivalent Privacy* – WEP) ve Wi-Fi Korumalı Erişim (Wi-Fi *Protected Access* – WPA)).** Bu tür şifreleme ile Veri Bağlantı Katmanı'nın üstündeki her şeyi şifrelersiniz. Kablosuz güvenlik için WEP şifrelemesi asla kullanılmamalıdır; bunun yerine, WPA kullanın.
  - **Ağ Katmanı şifreleme (IPSec *ve diğer bazı tünel protokolleri*).** Bu tür bir şifreleme ile Ağ Katmanı'nın (*Network Layer*) üstündeki her şeyi şifrelersiniz.
  - **Uygulama Katmanı şifreleme (SSL ve SSH ve *diğerleri*).** Bu şifreleme türü Aktarım Katmanı'nın (*Transport Layer*) üstündekilerini şifreler.

Günlük Tutma Anormalileri

İzlemenin önemli bir özelliği, günlük girdilerindeki gerçek saldırılar ile yalnızca gürültü veya küçük bir olay olan etkinlik arasındaki farkı belirlemektir. Bunu yaparken, her tür izleme iki temel tür hata yapar:

- **Yanlış pozitif**—Tip I hataları olarak da bilinen **yanlış pozitiflikler (*false positives*)**, kötü niyetli görünen ancak gerçek güvenlik olayları olmayan uyarılardır. Bu yanlış alarmlar idari çaba sarf eden dikkati dağıtıcı şeylerdir. Çok fazla yanlış alarm, yöneticinin gerçek saldırıları görmezden gelmelerine neden olur. Bununla mücadele etmek için, sık olmayan veya insan hatası "saldırıları" kaydetmemeye karar verebilirsiniz. Sıklıkla gerçekleşmediği veya önceden tanımlanmış bazı ölçütleri karşılamadığı sürece, bir olayı yok sayan **kırpma seviyeleri (*clipping levels*)** oluşturarak bunu yapabilirsiniz. Örneğin, başarısız bir oturum açma girişimi, kısa bir süre içinde birkaç kez gerçekleşmediği sürece fazla ilgi çekmemelidir. Başarısız oturum açma işlemleri için ortak bir kırpma seviyesi beştir. Bu, sistem, bir kullanıcı oturum açma işleminin arka arkaya beş kez başarısız olacağı her durumda bir alarm tetikleyeceği anlamına gelir. Kırpma seviyeleri, yanlış pozitif hata sayısını azaltmaya yardımcı olur.
- **Yanlış negatifler**—Diğer izleme hata tipi, denetimin şüpheli davranışları yakalamadaki başarısızlığıdır. **Yanlış negatifler (*false negatives*)**, Tip II hataları olarak da bilinirler, alarm sisteminin ciddi bir saldırıyı tespit etmedeki başarısızlığını gösterir. Belki de olay fark edilmedi, ya da belki de alarm olayın aslında ciddi olduğu halde ciddi olmadığı düşüncesiyle kapatıldı. Bazı izleme denetimlerinde yanlış negatifler, denetimin hatalı yapılandırılmasının bir sonucudur. Denetim, çevreye karşı daha duyarlı olmalı ve daha çok şüpheli etkinlik bildirmelidir.

Günlük Yönetimi

Günlük tutmak, güvenlik personeli için merkezi bir faaliyettir. Günlük dosyaları, sistemin normal ve anormal sistem faaliyetlerine dair kanıt sağlamanıza yardımcı olabilir. Ayrıca denetimlerinizin, işlerini ne kadar iyi yaptığına dair değerli bilgiler sağlayabilirler. Güvenlik ve sistem yöneticileri doğru bilgileri sakladıklarından ve bu bilgilerin güvenliğinden emin olmak için birkaç şey değerlendirmelidir.

Öncelikle, günlükleri korumak ve bunları kapsamlı bir analiz için kullanışlı tutmak için günlükleri merkezi bir lokasyonda saklamalısınız. Bir sürü depolama alanı bulundurun ve günlük dosyası disk alanı gereksinimlerinizi görüntüleyin. Bir günlük dosyası dolarsa, üç kötü seçenekle karşı karşıya kalırsınız:

- Günlük tutmayı durdurun
- Eski kayıtların üzerine yazın
- İşlemeyi durdurun (kontrollü ya da olağan dışı bir şekilde sonlandırın)

Saldırganlar bazen bu hatalarından birine neden olmak için günlük dosyalarını bilerek doldururlar. Günlük dosyalarınız için depolama aygıtı, bu olasılığı önlemek için yeterince büyük olmalıdır. Buna ek olarak, günlüğe kaydetme ayarlarınız, yapay olarak düşük günlük dosyası boyutu kısıtlamalarını dayanmamalıdır.

Sistem ve günlükler arasındaki etkinlikleri birbirine bağlamak için ağınızdaki bilgisayarlar ve aygıtlar senkronize edilmiş saatlere sahip olmalıdır. Ağ Zaman Protokolü (*Network Time Protocol* - NTP), onu destekleyen tüm bilgisayarlar ve aygıtlar için zamanı eşitler. Çoğu modern yönlendiriciler ve sunucular bunu yapar. Uluslararası hükümet tarafından işletilen NTP sunucuları, zaman temin etmek için tarafsız bir üçüncü taraf sağlar.

NOT

NTP sunucularının bir listesini bulmak için bakınız http://tf.nist.gov/tf-cgi/servers.cgi.

Günlük Dosyalarını Tutmak

Düzenleme, politika veya günlük hacmi, ne kadar çok günlük kaydettiğinizi belirleyebilir. Bir günlük dosyası dava konusu ise, dava bitene kadar dosyayı saklamak zorundasınız. Davalar devam etmiyorsa, bir şirket günlük miktarı ve saklama konusunda kendi kararlarını verebilir. Bu kuralın istisnaları yasalara veya düzenlemelere dayanabilir. Davalar başladığında, bu günlüklerdeki verileri sağlamak, şirketin katlanması gereken pahalı bir süreçtir. Bir şirket, günlüklerde toplanan verilerin sayısını yalnızca ihtiyaç duyulan şeye sınırlandırarak ve bu verileri yalnızca yararlı oldukları sürece muhafaza ederek dava maliyetlerini azaltabilir.

Bazı durumlarda, yönetmelikler ne kadar süre veri tutmanız gerektiğini belirtebilir. Örneğin, Ödeme Kartı Endüstrisi Veri Güvenliği Standardı (PCI DSS), günlüklerin en az bir yıl tutulmasını gerektirir. Yazılı bir saklama standardına sahip olmak en iyisidir. Bu yolla, gerekliyse, kanıtları yok etme girişiminde bulunmak yerine günlükleri normal ticari uygulamalarınızın bir parçası olarak sildiğinizi mahkemede açıklayabilirsiniz.

Üzerine yazmayı veya değiştirmeyi önlemek için, bazı sistemler günlükleri bir CD-ROM'a veya salt yazabileceğiniz diğer bir aygıta yazarlar. Günlükleri değişiklik veya okuma erişiminden korumak bir saldırganın saldırı izlerini temizlemesini zorlaştırır. Kolay erişilebilen günlük dosyaları, bir saldırganın saldırıya bağlı günlük dosyası girdilerini kaldırmasını kolaylaştırır. Günlük dosyaları ayrıca, sıklıkla, kullanıcılar veya bilgiler hakkında, ihtiyacınız olabilecek gizli bilgiler içerir. Tüm günlük dosyalarınızı yetkisiz erişime, silinmeye veya değişikliklere karşı koruduğunuzdan emin olmalısınız.

Yakalanacak Günlük Bilgilerinin Türleri

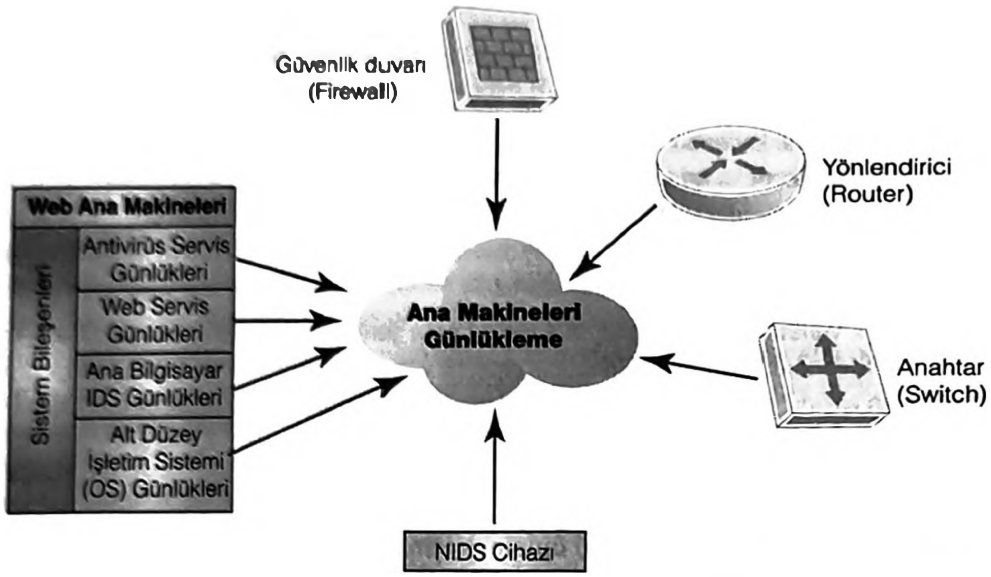
Sisteminizdeki, ağlarınızdaki ve uygulamalarınızdaki tüm etkinlikleri kaydetmek için kuruluşunuza çok sayıda günlük gerekebilir. Güvenlik denetlemesini desteklemek için tutmanız gereken dört ana günlük türü şunlardır:

- **Olay günlükleri (*Event logs*)**—Genel işletim sistemi ve uygulama yazılımı olayları.
- **Erişim günlükleri (*Access logs*)**—Kaynaklara erişim talepleri.
- **Güvenlik günlükleri (*Security logs*)**—Güvenlikle ilgili olaylar.
- **Denetim günlükleri (*Audit logs*)**—Denetleme faaliyetlerine ek girdi sağlayan tanımlı olaylar.

ŞEKİL 7-3'te gösterildiği gibi, tüm şüpheli etkinlikleri, hataları, yetkisiz erişim girişimleri ve hassas bilgilere erişimi kaydetmelisiniz. Sonuç olarak yalnızca olayları takip etmeyeceksiniz, ayrıca kullanıcılarınızı faaliyetlerinden sorumlu tutacaksınız.

Güvenlik Bilgi ve Olay Yönetimi (*Security Information and Event Management - SIEM*) sistemi, kuruluşların günlük dosyalarındaki dramatik büyümeyi yönetmelerine yardımcı olur. Olayları yakalamak ve analiz etmek için ortak bir platform sağlar. Kuruluşlar, günlükleri için güvenlik duvarları, IDS'ler ve IPS'ler, web sunucuları ve veritabanı sunucuları gibi kaynaklardan toplarlar. Buna ek olarak, birçok kuruluş bu sistemlerin birden fazla markasına veya sürümüne sahiptir. SIEM toplama ve analiz araçları, günlük verilerini oluşturulan formatta alır ve bu verileri ortak bir biçimde standardize eder. Sistem kolay erişim için standart günlük mesajlarını bir veritabanında saklar. Günlük dosyası bilgilerinize erişmek ve analiz etmek için SIEM sağlayıcı tarafından sağlanan raporları veya özel raporları çalıştırabilirsiniz.

ŞEKİL 7-3
Günlük bilgisi türleri



İşletim sistemi, uygulama yazılımı ve ağ aygıtı satıcıları ürünleri değiştirdikçe, yeni günlük dosyası biçimleri önceki ürünlerden farklı olabilir. Kuruluşunuz günlük dosyalarını işlemek için bir SIEM sistemi kullanıyorsa, bu tür biçim değişiklikleri kritik değildir. Daha önce ve sonraki dönemi kapsayan raporlar üretme özelliğini sınırlamaksızın, yeni ürünlerdeki dosyaları aynı veritabanına ekleyebilirsiniz.

SIEM sistemleri, kullanıcı etkinliğini izler ve kullanıcıların yalnızca politikaya uygun hareket etmesini sağlar. Bunun anlamı, SIEM sistemleri düzenleyici uyumu sağlamanın değerli bir metodudur. Ayrıca, yalnızca geçerli kullanıcı hesaplarının sistem üzerinde etkin olmasını sağlamak için kimlik yönetimi planlarıyla entegre olabilirler.

Güvenlik Denetimlerini Doğrulama

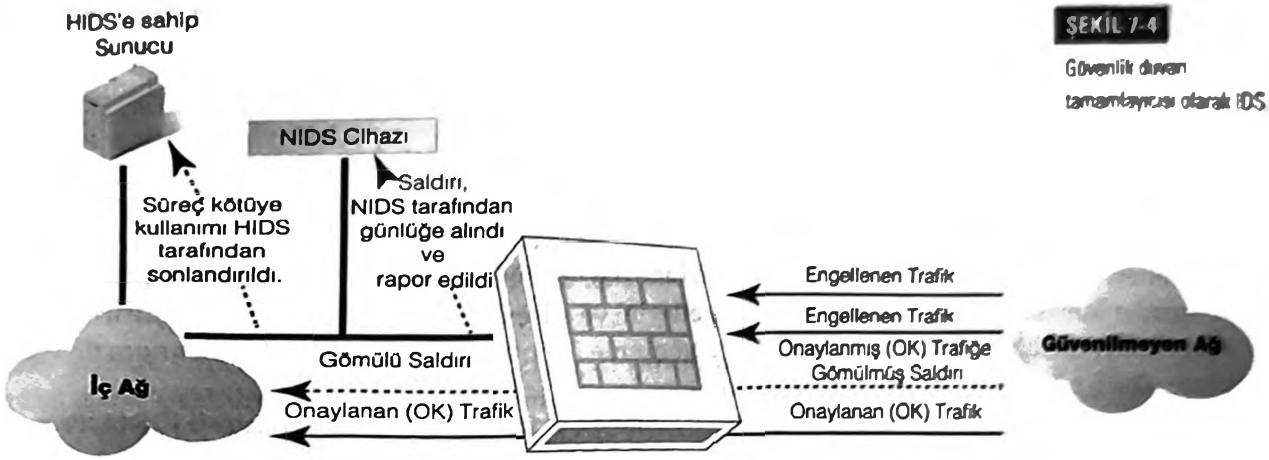
İzleme denetimlerinden biri olan belirli bir sınıf, çok iyi bir güvenlik katmanı sağlayabilir. Bu denetim sınıfı, alışılmadık veya şüpheli davranışları saptamak için ağ ve sistem etkinliğini görüntüler. Bu sınıftaki bazı denetimler, tespit edilen şüpheli etkinliklere yanıt verebilir ve olası bir saldırıyı durdurabilir. İzleme etkinliği denetimleri, saldırı tespit sistemleri (*intrusion detection systems* - IDS), saldırı önleme sistemleri (*intrusion prevention systems* - IPS) ve güvenlik duvarlarını içerir.

NOT

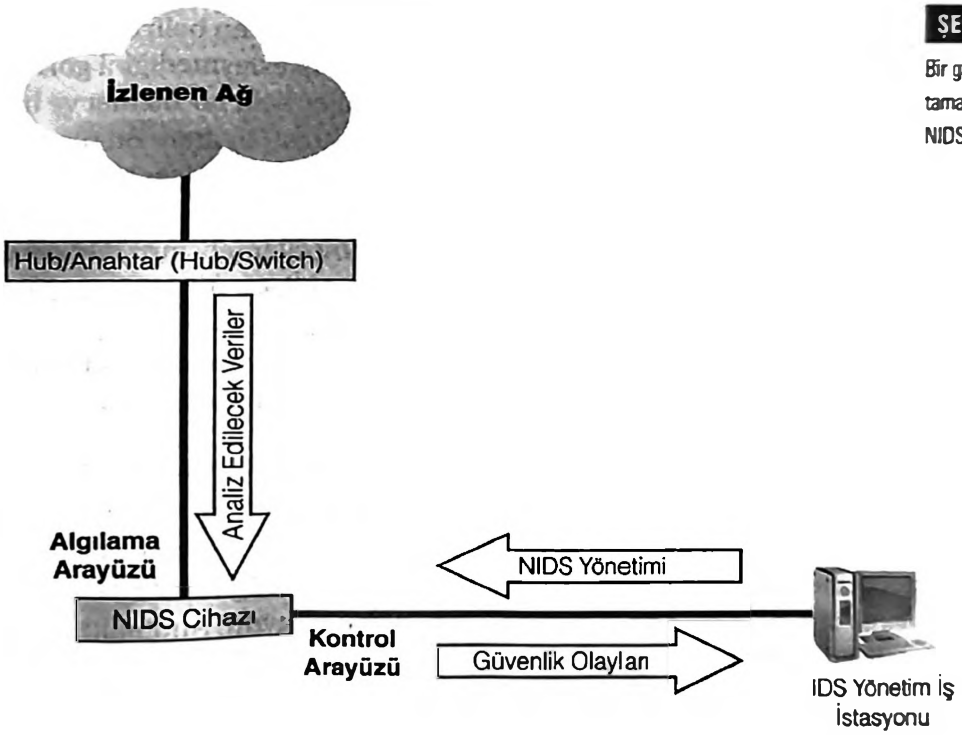
Birincil güvenlik kontrol türlerinin iki tipi, önleyici ve tespit denetimlerdir. IDS ve IPS her kontrol türünü temsil eder. Bir tespit denetim, tanımlanan bir olayın ne zaman gerçekleştiğini basitçe tespit eder, oysa önleyici denetim, olayın meydana gelmesini önler. Her iki denetim türü de önemlidir.

Saldırı Tespit Sistemi (Intrusion Detection System - IDS)

Katmanlı savunma, saldırıları önlemek için birden fazla denetim gerektirir. En yaygın katmanlı savunma mekanizmalarından biri, yüksek güvenlik sağlamak için bir güvenlik duvarının arkasına bir IDS yerleştirmektir. Bir ağ saldırı tespit sistemi (*network intrusion detection system* - NIDS), kötü niyetli etkinliği tespit etmek için güvenlik duvarından geçen trafiği izler. Bu bölümün ilerleyen sayfalarında açıklanan ana bilgisayar tabanlı bir saldırı



ŞEKİL 7-4
Güvenlik duvarı tamamlayıcısı olarak IDS



ŞEKİL 7-5
Bir güvenlik duvarı tamamlayıcısı olarak temel NIDS

tespit sistemi (*host-based intrusion detection system* - HIDS) - belirli bir bilgisayara veya cihaza yönelik trafikte aynı şeyi yapar. HIDS daha dar bir görme açısına sahip olduğu için çok spesifik etkinlikleri algılamak için ayarlama yapabilirsiniz. NIDS'in aksine HIDS, kuruluş içinden çıkan trafiği de görür. **ŞEKİL 7-4**, bir NIDS ve bir HIDS aygıtı içeren bir ağı gösterir.

ŞEKİL 7-5'de gösterildiği gibi bir NIDS'i bir anahtara veya hub'a bağlayabilirsiniz. IDS, anahtar üzerindeki tüm trafiği yakalar ve yetkisiz faaliyeti saptamak için analiz eder. Bu analizi, IDS'deki cihaz türüne bağlı olarak çeşitli şekillerde yapabilirsiniz.

NOT

Yöneticiler genellikle izlem.ı bağlantı noktasında bir IP adresi olmadan NIDS'i yapılandırırlar. Bu, yabancının NIDS'e paket göndermesine ya da doğrudan NIDS'e adres atamasını son derece zorlaştırır. Yöneticiler aygıta farklı bir alt ağda olması gereken başka bir arayüz üzerinden ulaşırlar.

IDS'yi, yöneticinin izlemesi ve yönetmesini sağlayan bir yönetim konsoluna bağlarsınız. İdeal olarak, IDS ağdan algılanamaz. Bu, saldırganların, IDS'nin ağdaki yerini belirleyemeyeceği anlamına gelir. IDS üzerindeki yönetim portuna ağdan erişilemez; bu da bir saldırganın IDS yapılandırmasını değiştirmesini önler.

Analiz Yöntemleri

İzleme ve algılama aygıtlarının, ne zaman bir alarm veya uyarı vermesi gerektiğini bilebilmesi için faaliyetleri incelemesi ve analiz etmesi gerekir. Cihazlar, trafiği ve faaliyeti analiz etmek için çeşitli yöntemler kullanabilir. Bazı yöntemler, ağ paketlerini ve adreslerini kurallar ile karşılaştırırken, bazıları faaliyet sıklığını ve türünü inceler. Bu iki yönteme örüntü -veya imza-tabanlı ve anomali- veya istatistiksel- tabanlı IDS'ler denir.

Kural tabanlı algılama olarak bilinen yöntemi kullanan **örüntü (veya imza) tabanlı IDS (*pattern -or signature- based IDS*)** çalışma yöntemi, bilinen trafik saldırılarının faaliyet örüntüleri (imzalar) ile mevcut trafiği karşılaştırmak için örüntü eşleştirmesine ve durum bilgisi eşleştirmeye dayanır. Örüntü eşleştirme sistemleri, *imzalar* olarak bilinen belirli bayt dizilerinin bilinen saldırıların imzasıyla eşleşip eşleşmediğini görmek için paketleri tarar. Genellikle örüntüler belli bir hizmet ve bağlantı noktasıyla (kaynak veya varış noktası) ilgilidir. Bu tür denetimlerden kaçınmak ve algılamadan sakınmak için birçok saldırgan saldırılarını değiştirir. Bilinen en yeni saldırıları algılayabilmeniz için imza dosyalarınızı sık sık güncellemelisiniz. **Duruma dayalı eşleme (*stateful matching*)** basit örüntü eşleştirmesinin gelişmişidir. Tek tek paketleri aramak yerine trafik akışında çeşitli paketlerde görünen belirli dizileri arar. Örüntü eşlemeden daha ayrıntılı olmasına rağmen, duruma dayalı eşleştirme hala yanlış pozitif üretebilir. Örüntü eşleme gibi, duruma dayalı olan eşleştirme yalnızca bilinen saldırıları algılayabilir. Sıkça imza güncellemelerine ihtiyaç duyar.

> **NOT**
>
> Yanlış pozitifler, örüntü eşleştirmeyle ilgili bir sorundur, çünkü bu sistemler, özellikle örüntü taneciklilikten (granularity) yoksun ise (örn. benzersiz değilse) yakın benzerlikler bildirir.

Anomali tabanlı IDS'ler (*anomaly-based IDS*) bazen *profil tabanlı sistemler (profile-based systems)* olarak adlandırılır ve mevcut etkinliği, normal (beklenen) etkinliğin kayıtlı profilleriyle karşılaştırır. Bunlar, yalnızca "normal etkinlik" tanımımızın doğruluğu kadar doğrudur. Normal sistem işlemini tanımladıktan sonra IDS, mevcut etkinliği normal etkinlik olarak düşündüğünüzle karşılaştırır. IDS'in anormal olduğunu düşündüğü her şey, analiz ve yanıt için bir adaydır. Anomalileri algılamanın daha yaygın yöntemleri şunlardır:

- **İstatistiksel tabanlı yöntemler**—Bunlar normal trafik ve ağ etkinliklerinin dayanak çizgilerini oluşturur. Cihaz bir sapmayı yakaladığında bir uyarı oluşturur. Bunlar bilinmeyen saldırıları yakalayabilir, ancak normal faaliyetin belirlenmesi zor olduğundan yanlış pozitifler ortaya çıkabilir.
- **Trafik tabanlı yöntemler**—Bunlar, trafiğe dayalı beklenen davranıştan kabul edilemez bir sapmayı tanımladıklarında bir uyarı sinyali verir. Ayrıca bilinmeyen saldırıları ve sel saldırılarını da tespit edebilirler.
- **Protokol örüntüleri**—İmzasız saldırıları tespit etmenin diğer bir yolu, protokollerden sapmalar aramaktır. Protokol standartları, İnternet Mühendisliği Görev Gücü (*Internet Engineering Task Force* - IETF) tarafından yayınlanan Yorumlar için Rica (*Request for Comments* - RFC) metni tarafından sağlanmaktadır. RFC'ler hakkında daha fazla bilgiyi *www.ietf.org/rfc.html* adresinden edinebilirsiniz. Bu tespit türü, iyi tanımlanmış protokoller için çalışır; ancak, iyi tanımlanmamış protokoller için yanlış pozitif sonuçlara neden olabilir.

HIDS

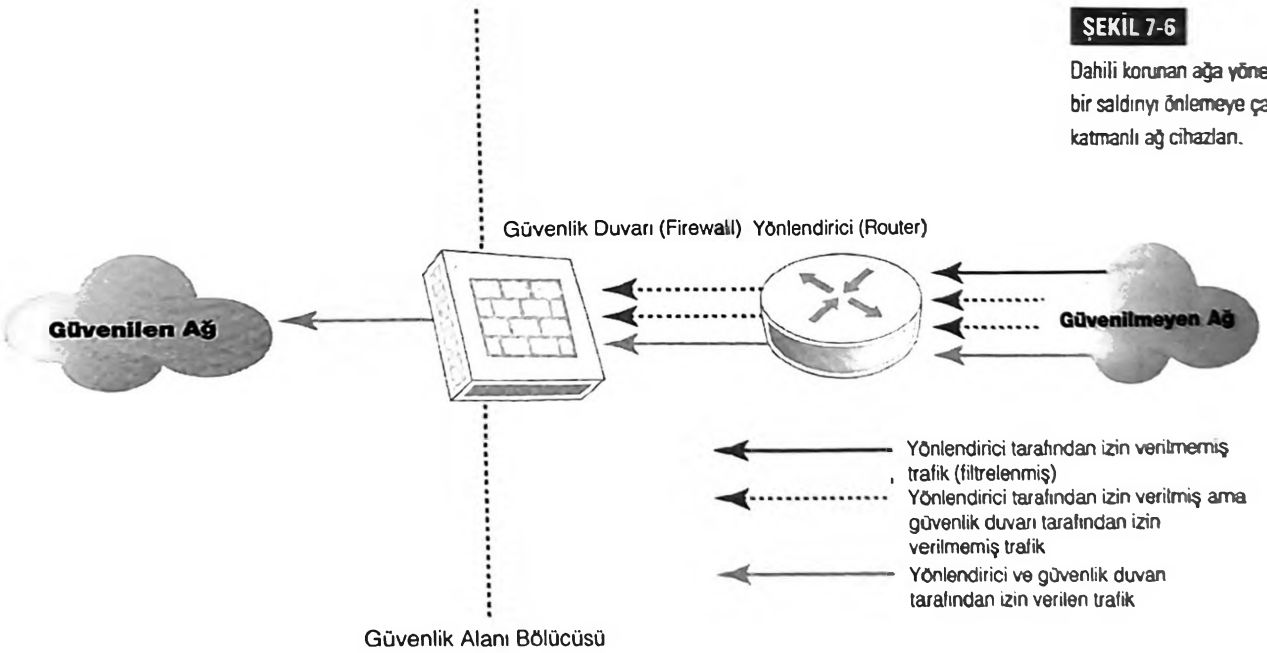
HIDS teknolojisi, bir bilgisayarın içindeki hassas süreçleri izleyerek tüm sistemin korunmasına katkıda bulunur. HIDS sistemleri genellikle aşağıdaki özelliklere sahiptir:

- Bunlar genellikle sunucu bilgisayarlarında çalıştırılacak yazılım süreçleri veya hizmetlerdir.
- Normalde izin verilmemesi gereken kalıplar veya davranışlar için sistem çağrılarının veya belirli süreçlerin (örneğin, veritabanı ve web sunucuları) yolunu keser ve incelerler.
- HIDS hayalet programları, ihlalin durdurulması veya rapor edilmesi gibi önceden tanımlanmış bir işlemi gerçekleştirebilir.

HIDS'lerin de NIDS'lerden farklı bir bakış açısı vardır. Bir HIDS, ağın içinden çıkan uygun olmayan trafiği tespit edebilir. Ayrıca, belirli bir makine veya kullanıcıya özgü bir anormalliği de tespit edebilir. Örneğin, yüksek hacimli bir posta sunucusundaki tek bir kullanıcı herhangi bir günde (veya saatte) bir kullanıcı için normal iletilerin 10 katından fazla ileti yollayabilir. HIDS farkına varacaktır ve bir uyarı verir ancak bir NIDS bu olayı fark etmeyebilir. Bu durum NIDS için, sadece artan ağ trafiği gibi görünür.

Katmanlı Savunma: Ağ Erişim Denetimi

En iyi savunma birden çok denetim katmanına sahip olmaktır. Bu, sisteminizi yalnızca tek bir denetime kıyasla daha çok saldırıdan koruma şansını artırır. **ŞEKİL 7-6**, ağ aygıtlarının dahili korunan ağa yönelik bir saldırıyı önlemeye yönelik nasıl birden fazla katmanda çalıştığını göstermektedir. Yönlendirici (*router*), bazı trafiği tespit edip filtrelerken, güvenlik duvarı (*firewall*) istenmeyen trafiği tespit eder ve durdurur.



ŞEKİL 7-6
Dahili korunan ağa yönelik bir saldırıyı önlemeye çalışan katmanlı ağ cihazları.

Kontrol Denetlemeleri: Saldırı Tespiti

NIDS, çok katmanlı bir savunma stratejisinde önemli bir bileşendir. **ŞEKİL 7-7**, bir NIDS'in dışarıdan gelen saldırıları ve içeriden kötüye kullanımını nasıl görüntüleyebildiğini göstermektedir. Ağın dışındaki bir NIDS, güvenlik duvarının karşılaştığı saldırı türleri hakkında fikir verir. Dahili NIDS (*internal NIDS*), güvenlik duvarının alabileceği saldırı tiplerini tespit eder. Bu cihazı ayrıca bir IPS olarak da kurabilirsiniz. Bu şekilde cihaz yalnızca potansiyel bir saldırıyı tespit etmekle kalmaz aynı zamanda saldırıyı durdurmak için trafiği filtrelemek için kurallarını değiştirebilir. Bu cihazlar ayrıca HIDS cihazlarıyla da çalışır. NIDS sisteminizi kötü niyetli ağ trafiğinden korumaya yardımcı olurken, HIDS ana makinenin kendisine teşebbüs edilen etkinlik türünü görecektir.

Ana Bilgisayar İzolasyonu

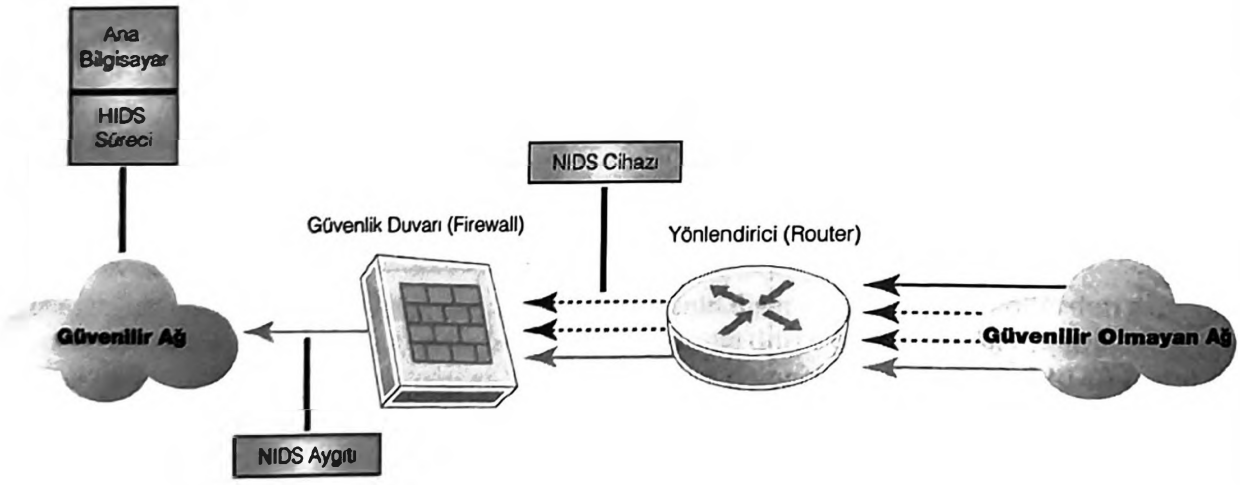
Bazı sunucuların veya ana bilgisayarların internete açık olması gerekir. Web sunucuları bu tür ana bilgisayarlara örnektir. Herhangi bir kullanıcının web sunucunuza erişebilmesini istiyorsanız -ancak herkesin dahili ağınıza erişmesini istemiyorsanız- basit çözüm, internete bağlı olan ana bilgisayarları ağınızın geri kalanından ayırmaktır. Ana bilgisayar yalıtımı, bir veya daha fazla ana bilgisayarı iç ağlarınızdan izole eder ve bir arındırılmış bölge (*DeMilitarized Zone* - DMZ) oluşturur. **ŞEKİL 7-8**, İki izole edilmiş ana bilgisayara sahip bir DMZ'yi gösterir. Bir DMZ, bir kuruluşun dış hizmetlerini içeren, daha büyük ve güvenilir olmayan bir ağa, genelde internete sahip olan fiziksel veya mantıksal bir alt ağdır. Güvenilmeyen internetten gelen dış trafik yalnızca belirli şirket hizmetlerine erişebilecek DMZ'ye izin verilir. DMZ'deki web uygulamaları daha sonra güvenilir iç ağa erişir ancak dış kullanıcının doğrudan dahili ağa girmesini önler.

Sistem Güçlendirme

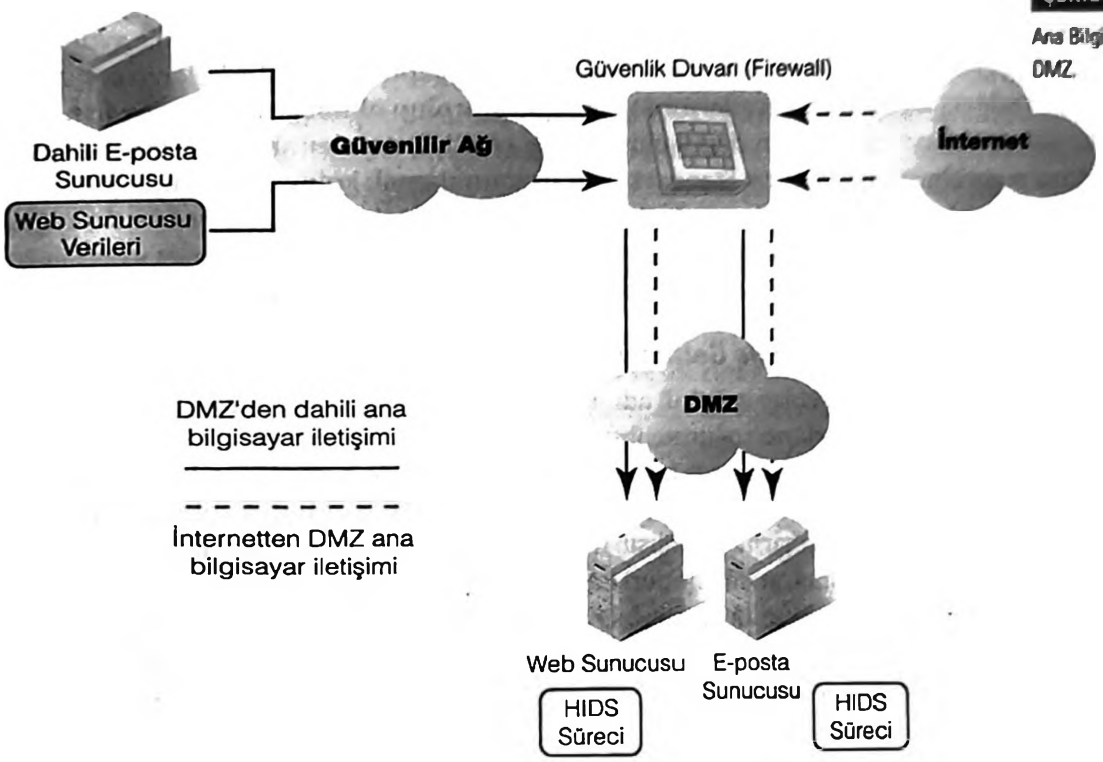
Hiçbir bilgisayar tamamen güvenli değildir. Aslında, çok az işletim sistemi veya uygulama yazılımı paketini yüklediğinizde güvenlidir. Güvenlik yöneticilerinin, bilgisayarları ve aygıtları olabildiğince güvenli hale getirmek için donanım ve yazılım yapılandırmalarını değiştirmek için **güçlendirme**

ŞEKİL 7-7

Dış saldırıları görüntülemek için NIDS cihazlarını kullanma.



ŞEKİL 7-8
Ana Bilgisayar izolasyonu ve DMZ



(***hardening***) denilen bir süreçten geçmeleri önemlidir. **Güçlendirilmiş bir yapılandırmaya (*hardened configuration*)** sahip bir bilgisayar veya aygıt, aşağıdaki minimum eylemleri gerçekleştirdiğiniz bir bilgisayardır:

- Gereksiz hizmetler kapatıldı veya devre dışı bırakıldı ve hala çalışmakta olanlar kapatıldı.
- Yönetim arayüzleri ve uygulamaları güvenli hale getirildi.
- Agresif parola politikaları ile parolalar korundu.
- Gereksiz kullanıcı hesapları devre dışı bırakıldı.
- Mevcut en yeni yazılım yamaları uygulandı.
- Herhangi bir yetkisiz değişikliğe karşı tüm bilgisayarlar ve cihazlar güvence altına alındı.

Güçlendirme sistemlerine ek olarak, ağınızı da güçlendirmeniz önemlidir. Güçlendirilmiş ağlar için pek çok fırsat vardır, ancak sadece birkaç adım ağlarınızı (ve ağ aygıtlarınızı) daha güvenli hale getirmek için uzun bir yol kat etmeniz gerekiyor. Bu adımlar şunları içerir:

- Kullanılmayan ağ arayüzlerini devre dışı bırakma
- Kullanılmayan uygulama hizmeti bağlantı noktalarını devre dışı bırakma
- Aygıt erişimini sınırlamak için MAC filtrelemesi kullanma
- 802.1x, Bağlantı Noktası-tabanlı Ağ Erişim Denetimi (*Port-based Network Access Control* - PNAC) gerçekleştirme

Çalışmaya açmadan önce tüm sistemleri güçlendirebilirsiniz. Bir sistemi neredeyse çalışmaya başlamadan önce güçlendiremiyorsanız, kesinlikle sistemin zayıflığı ile sonuçlanacaktır.

Dayanak Noktası Yapılandırması Kurmak

Bir bilgisayarı veya aygıtı güçlendirdikten sonra, güçlendirilmiş yapılandırma ayarlarını kaydetmeniz gerekir. Bu şekilde, güçlendirilmiş yapılandırmayı bilinen, güvenli yapılandırmalarla karşılaştırabilirsiniz. Ayrıca, gelecekteki yapılandırma ayarlarını da bir değişiklik olup olmadığını görmek için orijinal ayarlar ile karşılaştırabilirsiniz. Bir taban çizgisi oluşturmak, çeşitli sistemler arasında güvenliğin tutarlı olduğuna emin olmayı kolaylaştırır. Standart ayarları tanımlamak kolay olduğunda, bireysel sistem farklılıklarını çok daha kolaylıkla kontrol edebilirsiniz. Örneğin, eğer bir hizmet ya da uygulamanın temel yapılandırmasının sizin standartlarınıza uyduğunu biliyorsanız, bu hizmet ya da uygulamalara bireysel bir bilgisayarda izin verip vermeyeceğinize karar verebilirsiniz.

Gerekli Olmayan Hizmetleri Etkisiz Hale Getirmek

Bilgisayarları güçlendirmek için en kolay ve etkili adımlardan biri, gereksiz hizmet ve programları kapatmaktır. Saldırganlar, bilgisayarların çoğunun ihtiyaç duyduklarından daha fazla hizmet ve program çalıştırdıklarını biliyor. Örneğin, birçok sunucu bilgisayarı, bir web sitesine ev sahipliği yapmadığı halde web sunucusu çalıştırır. Saldırganlar, bu ihtiyaç duyulmayan hizmetleri arayıp bu hizmetlerdeki saldırıya açık zayıf noktaları ortaya çıkarmaya çalışır. Gereksiz hizmetleri devre dışı bırakmalısınız. Bundan daha da iyisi, ihtiyacınız olmayan hizmetleri kaldırın. Saldırganlar, var olmayan programlara saldıramazlar. İhtiyaç duyulmayan güvenlik duvarı bağlantı noktalarını kapatın ve mobil kod, telnet ve FTP gibi belli hizmetleri sınırlandırın. Güvenlik duvarlarını, özel olarak izin verilmeyen her şeye engel olacak şekilde ayarlamalısınız. Bu, saldırganların gizlice yeni ve beklenmeyen hizmetleri eklemelerini durduracaktır.

Tüm yönlendiricileri (*router*) ve diğer ağları güçlendirmelisiniz. Yönlendiricileri, izinsiz yönetici erişimleri ve değişikliklerine karşı koruyun. Ağ aygıtları parolasız ya da varsayılan bir parola ile gelir. Ağınıza herhangi bir aygıt bağlamadan önce varsayılan parolaları değiştirmeniz gerekmektedir. Bu aygıt parolalarını diğer parolalarınız gibi yönetin. Parolalarınız karmaşık olmalı ve düzenli olarak değiştirilmelidir. Ağ aygıtlarına yapılan tüm değişiklikleri belgelemeniz ve değişikliği yapan yönetici kullanıcının kimliğini günlükte tutmanız zorunludur. Düzenli aralıklarla yapılandırma günlüklerinizi, muhtemelen bir SIEM uygulaması kullanarak incelemelisiniz.

Güçlendirilmesi gereken öğeler yalnızca sunucular ve ağ aygıtları değildir, iş istasyonlarını unutmayın. İş istasyonlarının standart yapılandırma ve erişim denetimlerine ihtiyacı vardır. Kurumlar, iş istasyonları için güçlendirilmiş bir imaja sahip olmalıdır. Yeni bir işletim sistemi kurup, kopyasını alarak ve bu kopyayı güçlendirerek standart bir imaj oluşturabilirsiniz. Gereksiz hizmetleri kaldırın ve virüs önler yazılımlar ve kişisel güvenlik duvarları gibi güvenlik ürünlerini ekleyin. Bu imaj, aynı zamanda, kelime işlemcisi, hesap çizelgesi ve tarayıcı eklentileri gibi şirket standardı olan yazılımları da içermelidir. İmajın sizin kurumunuzun iş istasyonlarının standartlarını karşıladığını doğruladığınızda, bu imaja tüm yeni masa üstü ve diz üstü bilgisayarlar için başlangıç noktası olarak kullanabilirsiniz. Bu işlem güvenlik uyumluluğu konusunda emin olmanıza yardım edebilir ve bakım zamanını düşürebilir.

Sunucuları fiziksel olarak koruyun, örneğin kilitli bir odada saklayarak. Tüm bilgisayar ve aygıtlara en güncel yamaların uygulandığına emin olun. Şirketin bilgisayarlarında ve aygıtlarında kurulu olan tüm ürünlerin, tüm sağlayıcıları tarafından yayınlanan yamalarının takibini yapmak için üçüncü parti bir yama yönetim yazılımı kullanabilirsiniz. Bazı ürünler otomatik "telefon-ev" yama yönetimine dahi sahiptir.

Çoğunlukla, internet bağlantısına maruz kalan sunucular için en iyi çözüm, bu sunucuların başka hiçbir amaç için kullanılmadığına emin olmaktır. Örneğin, DMZ'nizde bulunan ve web sunucusu olarak görev yapan bir bilgisayar başka hiçbir hizmet vermemelidir.

Antivirüs Yazılımları Değerlendirmek

Bir sistem denetlemesi, kurumunuzun kullandığı virüs-önler ve diğer kötücül yazılım önleme programlarının değerlendirmesini içermelidir. Bu değerlendirme, tüm yazılım ürünlerinin ve bu ürünlerin verilerinin güncel olduğunu garantilemelidir. Tüm ağ aygıtları ve bilgisayarlar üzerinde belli aralıklarla virüs-önler taramalarını gerçekleştirin. Düzenli aralıklarla tüm sistemler üzerinde tam tarama gerçekleştirin. Tüm uygulama sunucularını, iş istasyonlarını ve ağ geçitlerini tarayın.

Güvenlik Sistemlerini İzleme ve Sınama

Kapalı bir ortamı güvenli hale getirmek ve güvence altına almak zordur. Bir güvenlik uzmanı olarak sizin ana göreviniz kurumunuzun hassas verilerini saldırganlardan korumaktır. Kapalı bir sistemi güvence altına almak halihazırda zor iken, ağınız internete bağlandığında bu iş çok daha zor bir hale gelir. Yalnızca internete bağlanarak bile, saldırganlara kırmızı bir halı sermiş olursunuz. Sizin işiniz sistemlerinize erişimi denetlemek için stratejileri oluşturmak ve yerleştirmektir. Sisteminizi tamamen güvence altına almanın imkansız olduğunu unutmayın. Bilgi güvenliği ile ilişkili birçok risk olmasına rağmen, en yaygın iki risk şunlardır:

- Yetkisiz erişimle dışarıdan gelen saldırganlar, kötü amaçlı kodlar, Trojanlar ve kötü amaçlı yazılımlar
- Kurumunuzun içinden, kurumunuza zarar verebilecek yetkisiz insanlara sızan hassas bilgiler

İzleme

Hassas bilgilerin kuruluşunuzdan sızmasını nasıl engelleyebilirsiniz? Her zaman istenen sonucu verecek bir yöntem yoktur ancak görüntüleme önemlidir. Tabii ki, sisteminizdeki her IP paketini izleyemezsiniz. İnsanları bezdiren, sıkıcı bu iş için eğitseniz bile, yeteri kadar insanı ayakta tutamazsınız. Bunun yerine, bir saldırı tespit sistemi veya IDS ile trafiğini görüntülemelisin. Bir IDS'in hedefi, daha fazla araştırma yapabilmek için anormal trafiği saptamaktır. Saldırı önleme sistemleri veya IPS'ler, kötü amaçlı trafiği aktif bir şekilde engelleyerek IDS'lerin ötesine geçerler. Bir IDS olası yetkisiz etkinliğe karşı sizi uyarır; bir IPS bunu engeller. Tabii ki, bir IDS veya IPS kullanmadan önce, normal trafik için temel bir tanım oluşturmanız gerekir.

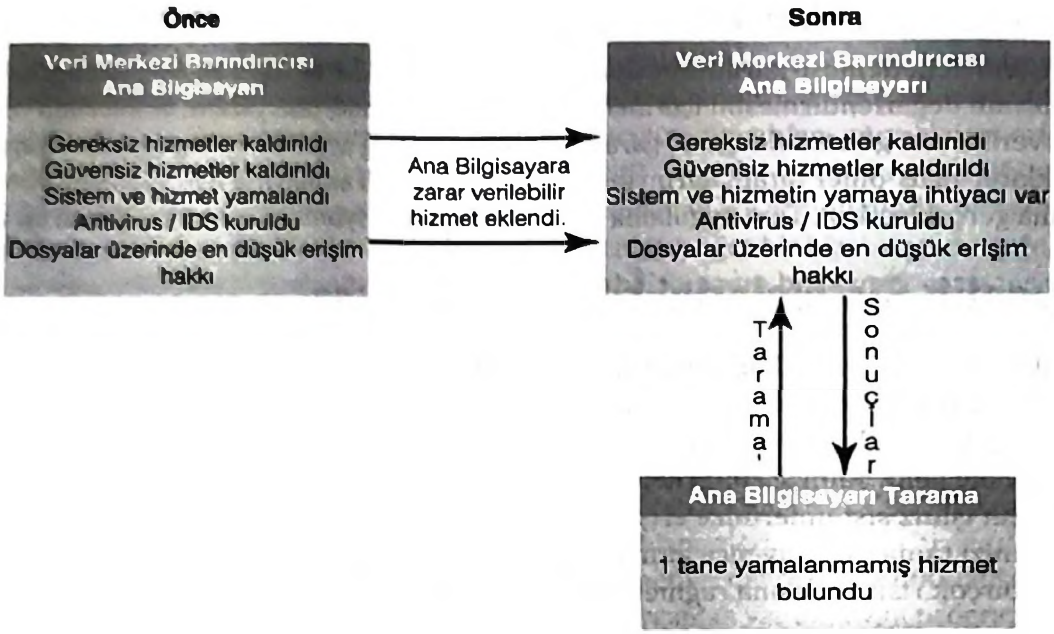
Test Yapmak

Sisteminizi görüntülemenin yanı sıra, sisteminizi de sınamalısınız. Herhangi bir güvenlik testinin ana amacı, bir sistemdeki düzeltilmemiş güvenlik açıklarını belirlemektir. Bir seferde bir sistem güvenli olabilir, ancak yeni bir hizmet veya uygulamanın eklenmesi sistemi zayıflatabilir. Test için yeni güvenlik açıklarını keşfederek onları hedefe koymanız gerekir. **ŞEKİL 7-9** güvenlik testinin ana hedeflerini göstermektedir.

Testlerinizin sıklığı, sistemin değişim oranı, sistemin hassaslığı veya kritikliği gibi faktörlere bağlıdır. Ayrıca, politika ve yönetmelik testleri zorunlu kılar. En yaygın test çizelgesi tetikleme noktalarından birkaçı şöyledir:

- Güvenlik sertifikası aşamasında
- Büyük sistem değişikliklerinden sonra (yeni teknoloji yükseltmeleri, uygulama değişiklikleri).

ŞEKİL 7-9
Güvenlik testi.



NOT

Zafiyet (Güvenlik açığı) testi (*Vulnerability testing*) bir sistemin zayıf yönlerini bulmaya çalışır. Penetrasyon testi (*Penetration testing*), keşfedilen bir güvenlik açığından yararlanmak için odaklanmış bir saldırıdır. Saldırganlar, penetrasyon testi gerçekleştirenler ile aynı adımları takip eder; ikisi arasındaki fark, saldırganların sisteme girmek için onayları olmamasıdır. Aşağıdakiler, bu testlerin farklılıklarına dikkat çekmek için her test türünün kısa bir özetidir.

Zafiyet testinin hedefleri şunları içerir:

- Güvenlik açığını belirleme (pasif olarak)
- Eksik güvenlik denetimi veya yanlış konfigürasyonu belgelendirme
- Kimliği doğrulanmış ve kimliği doğrulanmamış kullanıcılar ile ilgili güvenlik açıklarını inceleme

Penetrasyon testinin hedefleri şunları içerir:

- Tehditleri tanımlama
- Denetimleri atlatma
- Güvenlik açıklarından faydalanma

- Yeni tehditler ortaya çıktığında
- Sistem denetlemeleri sırasında
- Periyodik olarak, sistemin niteliğine bağlı olmak kaydı ile
- Kritik sistemlerde yılda bir kez

Listedeki diğer öğelerden hiçbiri bir testi tetiklemiyorsa yılda en az bir kez yapmalısınız. Bazı şirketler, bir risk analizine bağlı olarak daha kısa veya daha uzun test aralıkları seçebilir.

Test Yol Haritası

Test etme konusunda mükemmel bir çözüm mevcut değildir ve her güvenlik uzmanının aynı yolu takip etmesi mümkün değildir. **ŞEKİL 7-10**, güvenlik testi için bir yol haritasını göstermektedir. Şekilde görüldüğü gibi, güvenlik testi, sisteminizin güvenliğini tam olarak görmek için birkaç ortak aktiviteden oluşur. En yaygın faaliyetler şunlardır:

- **Keşif**—Bu etkinlik, sistemin organizasyonu, sistemleri ve ağları hakkında olabildiğince öğrenmek üzere incelenmesini içerir. Ağ yöneticileri tarafından dikkate alınmayan Whois ve Dig gibi açık kaynaklar, saldırganlar tarafından kullanıldığında bir sorun oluşturur.
- **Ağ haritalama**—Bu aşamada, kuruluşun sistemlerinde ve ağlarında çalışan düzenlemeleri ve hizmetleri belirlemek için araçlar kullanır.



ŞEKİL 7-10
Güvenlik testleri farklı yollardan ilerleyebilir.

- **Zafiyet Testi**—Zafiyet (güvenlik açığı) testi, bir sistemdeki tüm zayıf noktaları bulmak ve hangi yerlerin saldırı noktaları olabileceğini belirlemekle ilgilidir.
- **Penetrasyon Testi**— Bu aşamada, sistemdeki bir zayıflıktan yararlanmaya ve bir saldırganın başarıyla ona sızabileceğini kanıtlamaya çalışırsınız.
- **Faaliyetleri Azaltma**— Penetrasyon testlerinde veya zafiyet testlerinde bulunan zayıf noktaları azaltmaya veya bunları ortadan kaldırmaya yönelik herhangi bir eylemdir.

Test Hedeflerinin Oluşturulması

Test yönetmeliklerinizi çalıştırmadan önce, test hedeflerinizi belirlemeniz önemlidir. Güvenlik testleri, denetimlerinizin güvenlik açıklarını ne kadar iyi kontrol ettiğini değerlendirmekle ilgilidir. Öncelikle, açıkları tespit edin ve bunları, sisteminiz için ne kadar kritik olduklarına göre sıralayın. Daha sonra, diğer zaman dilimleriyle karşılaştırmak için bir zaman noktasındaki (anlık görüntüdeki) testi belgeleyin. Günün saatine veya etkinlik hacmine bakılmaksızın güvenlik denetimlerinizin düzgün şekilde çalıştığından emin olun. Sonra denetçi denetlemesine hazırlanın. Bu, BT personelinizin gerçek denetlemelere hazırlık için zafiyet analizi kullanarak kendi yönetmeliklerini ayarlamasını ve test etmesini sağlar. Son olarak, güvenlikteki boşlukları bulun. Bu adım, gizli test uzmanının (aşağıda tartışılacak), sisteme zarar verilmesi ve saldırının tespit edilmesi olasılıklarını belirlemesini sağlar.

Keşif Yöntemleri

Keşif, pek çok testin ilk ve en temel adımıdır. Keşif safhasında, sosyal mühendislik gibi teknikler yoluyla veya organizasyonun web sitesini araştırarak bilgi toplarsınız. Saldırganlar, bir organizasyon hakkında bilgi toplamak için mümkün olduğunca çok keşif kullanır. Bu aşamada, saldırganların ne yaptığını anlamalı ve daha sonra sizin hakkınızda bilgi toplamak için olanaklarını sınırlamalısınız.

Sosyal mühendislik (*social engineering*), yalan söylemek için süslü bir deyimdir. Gizli bilgileri paylaşmak veya hassas sistemlere erişmek için birini kandırmayı gerektirir. Çoğu durumda, saldırgan asla mağdurla yüz yüze gelmez. Bunun yerine, saldırgan bir çalışana telefon açıp bir sistem yöneticisi olarak tavır takınabilir. Düşünüldüğünden daha çok, saldırganlar çalışanları hassas bilgileri paylaşmaları için kandırıyor. Sonuçta, çalışanların düşüncesi, parolanızı bir yöneticiye vermekte ne yanlış olabilir ki? Kullanıcılarınızı sosyal mühendislik saldırılarını tanıması için eğitmelisiniz.

Başka bir keşif aracı Whois servisidir. Bu hizmet, saldırganlara yardımcı olabilecek, yöneticilerin adları ve telefon numaraları gibi bilgileri sağlar. **ŞEKİL 7-11** bir Whois isteğinin çıktısını göstermektedir.

Bölge aktarımı (*zone transfer*), bölgenin içeriğini isteyen bir DNS sunucusunun benzersiz bir sorgusudur. Bölge, sunucunun yönettiği alan adıdır. Yöneticiler genellikle bu aracı, aynı kuruluştaki DNS sunucularını senkronize etmek için kullanır. Bölge aktarmalarına kısıtlama olmaksızın izin verirseniz, saldırganlar bu bilgiyi hem ağınızın içindeki hem de dışındaki sunucuların adlarını ve türlerini anlamaya çalışabilir. Bu türden bilgi sızıntısından en iyi savunma, DNS sunucunuzu kilitlemektir.

NOT

Kuruluşlar, alan adı (*domain*) kayıtlarının geçmesine izin vermekten kaçınmak için çok dikkatli olmalıdır. Başka biri değiştirip kendisininmiş gibi kullanabilir. Böyle bir eylem organizasyonun itibarına büyük zarar verebilir. Bu tür bir sosyal mühendislik, olağan çeşitlilikten biraz daha karmaşıktır.

Ağ Haritalama Yöntemleri

Ağ haritalama (*network mapping*) keşfin genişletilmiş bir türüdür. Ağ haritalama, ana bilgisayarlar ve ana bilgisayar adresleri ile mevcut hizmetler de dahil olmak üzere bir ağ hakkında ayrıntılı bilgi keşfeder. Bu, saldırganların belirli türde sistem, uygulama, hizmet ve yapılandırmaları tespit etmesine olanak tanır. **ŞEKİL 7-12**, ağ haritalamasının sağlayabileceği bazı bilgileri göstermektedir.

Bir saldırgan, bir ağ düzenini keşfetmek için İnternet Kontrol Mesaj Protokolü (*Internet Control Message Protocol* – ICMP; aynı zamanda *ping* olarak da bilinir) paketlerini kullanabilir. Bu saldırganın bir saldırı hazırlamasına avantaj sağlar. **ŞEKİL 7-13**'de gösterildiği gibi, ping paketlerini engellemek, Tony yönlendiricisinde görüldüğü gibi, saldırganın ağ hakkında bilgi edinmesini engelleyebilir. Tabii ki, bu da aynı zamanda yöneticinin ağdaki sorun giderme için bu değerli aracı kullanabilmesini engeller.

ŞEKİL 7-14, bir saldırganın TCP/SYN taramalarını kullanarak hedef bir ana bilgisayarda bulunan hizmetleri nasıl keşfedebileceğini göstermektedir. Saldırgan paketleri ortak bağlantı noktalarına gönderir ve yanıttan ana makinenin bu hizmetleri kabul edip etmediğini belirleyebilir.

Saldırganlar potansiyel bir kurbanın hangi işletim sisteminde çalıştığını bilmelidir. Bir sisteme saldırma yaklaşımı, hedef işletim sistemine göre değişir. **İşletim sistemi parmak izi (*operating system fingerprint*)** ile, bir saldırgan, hangi işletim sisteminin ve sürümünün bir bilgisayarda çalıştığını öğrenmek için bağlantı noktası haritalamasını kullanır. Bu aynı zamanda bir saldırganın güvenlik açığı bulunan bilgisayarları keşfetmesine yardımcı olabilir çünkü yamaları olmayabilir ya da bilinen açıkları olabilir. **ŞEKİL 7-15**, işletim sistemi parmak izinin saldırganlara nasıl değerli bilgiler sağlayabileceğini göstermektedir.

Gizli Test Uzmanı Gizli Olmayan Test Uzmanına Karşı

Hem içeriden hem de dışarıdan personeli içerebilecek güvenlik testlerini gizli olmayarak ya da gizli olarak gerçekleştirebilirsiniz. Kullandığınız personel ve yöntemler yönetmeliklere veya kuruluş personelinin beceri düzeyine bağlı olabilir. **ŞEKİL 7-16**, çeşitli test uzmanlarını gösterir.

networksolutions.com Arama

ŞEKİL 7-11
Whois arama sonuçları

Tescil yapan

WHOIS Sunucusu: whois.networksolutions.com
URL: http://networksolutions.com
Tescil yapan: NETWORK SOLUTIONS, LLC.
IANA ID: 2
Kötüye Kullanım İletişim E-postası:: abuse@web.com
Kötüye Kullanım İletişim Telefon Numarası: +1.8003337680

Durum

Alan Adı Durumu: clientDeleteProhibited

Alan Adı Durumu: clientTransferProhibited
https://www.icann.org/epp#clientTransferProhibited
Alan Adı Durumu: clientUpdateProhibited
https://www.icann.org/epp#clientUpdateProhibited
Alan Adı Durumu: serverDeleteProhibited
https://www.icann.org/epp#serverDeleteProhibited
Alan Adı Durumu: serverTransferProhibited
https://www.icann.org/epp#serverTransferProhibited
Alan Adı Durumu: serverUpdateProhibited
https://www.icann.org/epp#serverUpdateProhibited

Önemli Tarihler

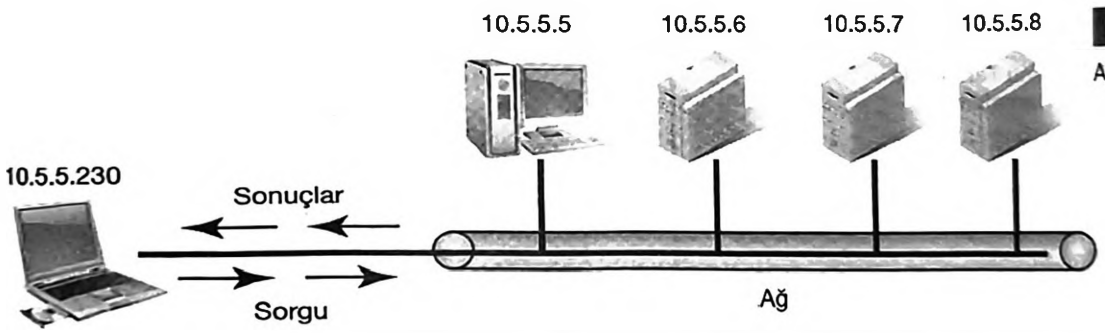
Güncelleme Tarihi: 2015-01-28
Oluşturulma Tarihi: 1998-04-27
Kayıt Sona Erme Tarihi: 2025-04-27

İsim Sunucuları

NS1.NETSOL.COM
NS2.NETSOL.COM
NS3.NETSOL.COM

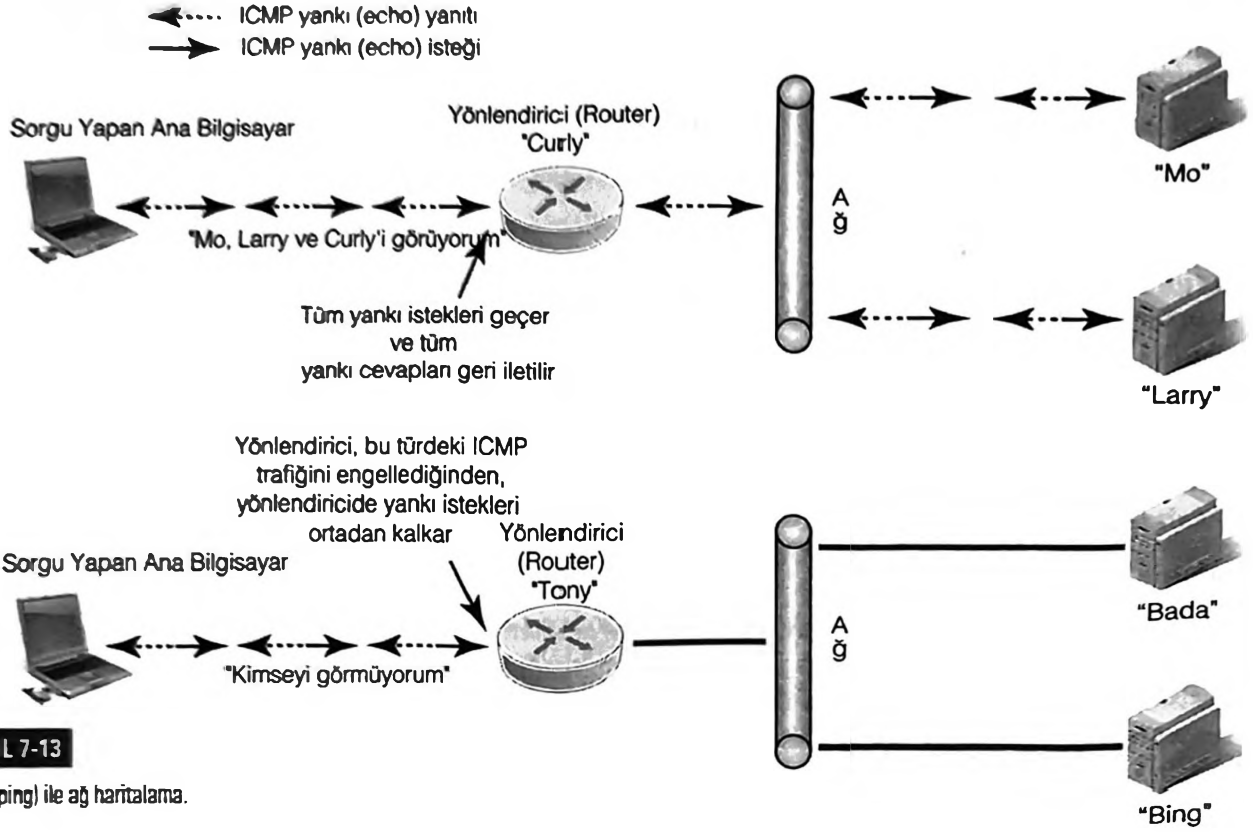
İşlenmemiş WHOIS Kaydı

Alan Adı:: NETWORKSOLUTIONS.COM
Kayıt Alan Kimliği: 4548132_DOMAIN_COM-VRSN
Tescil yapan WHOIS Sunucusu: whois.networksolutions.com
Tescil yapan URL: http://networksolutions.com
Güncelleme Tarihi: 2015-01-28T23:20:59Z
Oluşturulma Tarihi: 1998-04-27T04:00:00Z
Tescil Kayıt Sona Erme Tarihi: 2025-04-27T04.00.007



ŞEKİL 7-12
Ağ Haritalama

Ana Bilgisayar Adı	IP	Servisler	İşletim Sistemi (OS)
user-5	10.5.5.5	http, netbios, ftp	Windows Server 2008
server-6	10.5.5.6	http, netbios	Windows Server 2012
server-7	10.5.5.7	telnet, smtp	Linux
server-8	10.5.5.8	dns, finger, telnet	Solaris

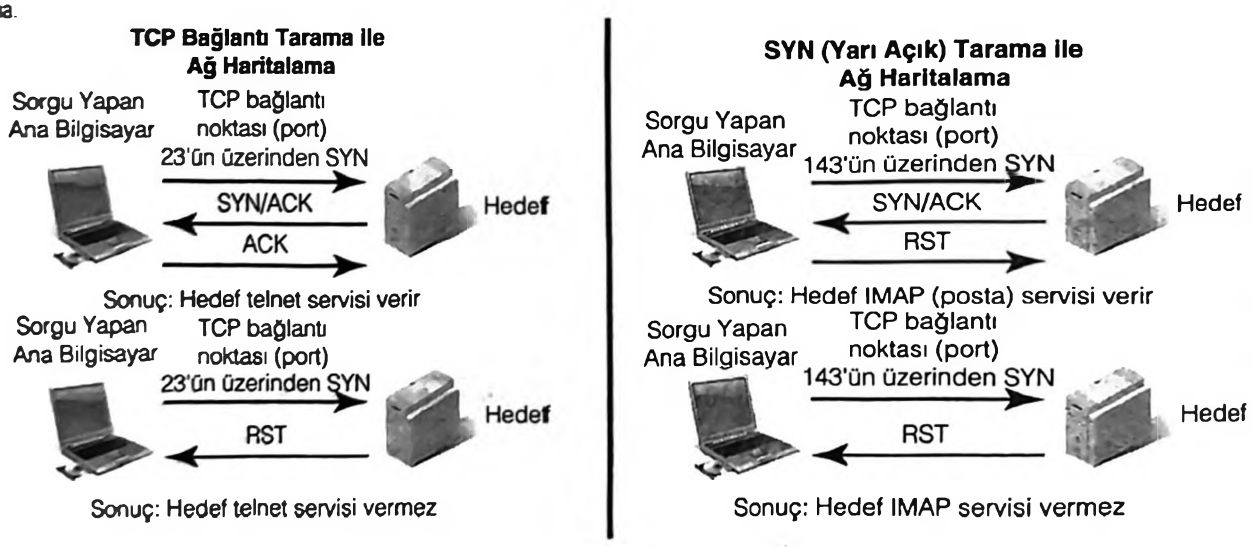


ŞEKİL 7-13

ICMP (ping) ile ağ haritalama.

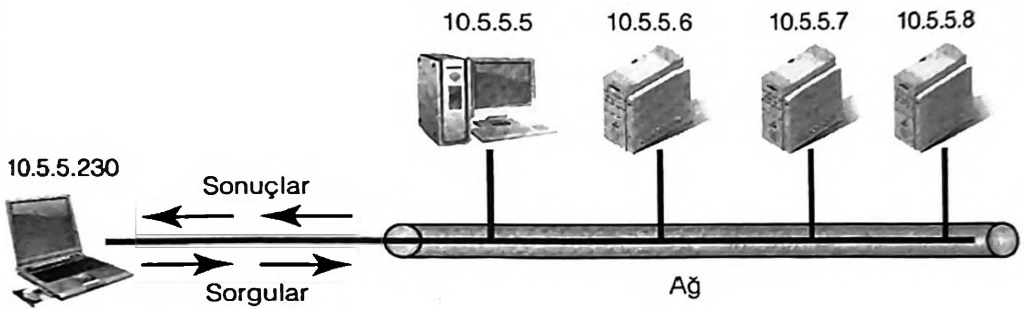
ŞEKİL 7-14

TCP / SYN taramaları ile ağ haritalama.



Testi kimin yaptığına bakılmaksızın, test etkinliklerinin potansiyel etkisini göz önüne almanız gerekir:

- **Zarar görme olasılığına dikkat edin**—Bazı testler bir sistemin çökmesine neden olabilir. Diğer testlerin etkisi daha az olacaktır. Potansiyel olarak etkilenen tüm tarafların hangi testleri uygulayacağınızın farkında olduğundan emin olun. Herhangi bir test, hizmeti aksatma veya zorluklara neden olma olasılığı varsa, tüm taraflardan anlaştığınızdan emin olun. Testler—hatta güvenli testler—bir sistemi çökertirse, kurtarmak için daima planınız olsun.
- **Günün saatine ve haftanın gününe dikkat edin**—Az yoğun zamanlarda test yapmak cazip olabilir ama birçok kullanıcıyı etkilemeyecektir ve bu gerçekçi bir senaryo olmayabilir. Alternatif olarak, çalışma saatleri dışında daha tehlikeli testler ve yoğun saatlerde ise daha güvenli testler yapılır.

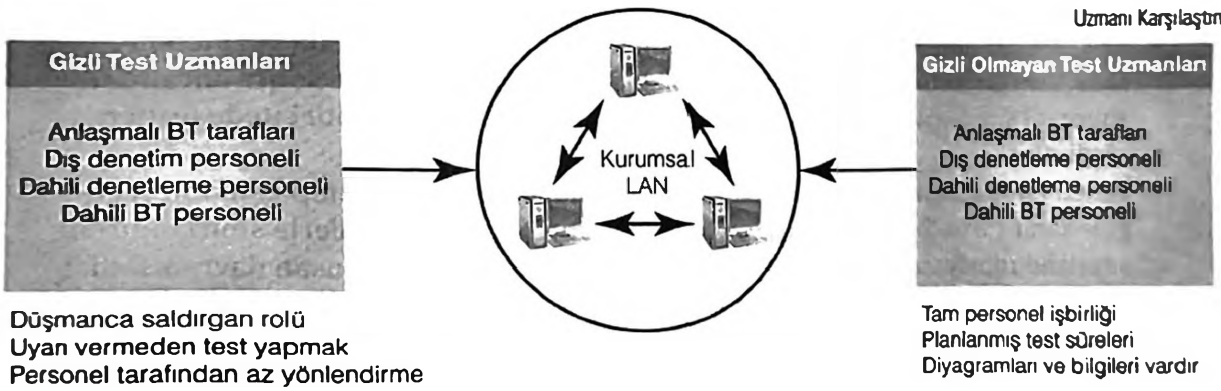


ŞEKİL 7-15
İşletim sistemi parmak izi.

Bağlantı noktası haritalayanlar "ne düşünüyor":

- 10.5.5.5, TCP/IP iletişimlerinin yapılandırılma biçimine dayalı olarak Windows Server 2003'e benziyor.....
- 10.5.5.6, Windows Sunucu 2008'e benziyor, çünkü bir FIN gönderdiğimde bir RST ile yanıt vermedi ve http başlığına göre IIS 5'i çalıştırıyor ....
- 10.5.5.7 Linux'a benziyor, çünkü FIN'e yanıt olarak bir RST gönderdi ve TCP/IP iletişimleri Linux gibi davranıyor....

ŞEKİL 7-16
Gizli Test Uzmanı Bilinir Test Uzmanı Karşılaştırması.



Düşmanca saldırgan rolü
Uyarı vermeden test yapmak
Personel tarafından az yönlendirme

Tam personel işbirliği
Planlanmış test süreleri
Diyagramları ve bilgileri vardır

Test Yöntemleri

Kara kutu testinde (*black-box testing*), doğrudan bir programın mimarisi veya tasarım bilgisine sahip olmayan test yöntemleri kullanılır. Bu terim, ya test kullanıcısının kaynak koduna sahip olmadığını veya kaynak kodunun ayrıntılarının test edilenle alakalı olmadığını gösterir. Başka bir deyişle, kara kutu testi, yazılımın dışarıdan görünür davranışına odaklanır. Örneğin, gereksinimler, protokol belirtimleri, API'ler veya hatta denenmiş saldırılar temel alınabilir.

Buna karşın, **beyaz kutu testi (*white-box testing*)**, uygulamanın tasarımı ve kaynak kodu bilgisi üzerine kuruludur. Gerçekte, beyaz kutu testleri genellikle kaynak koddan türetilir. Örneğin, bu testler kaynak kodunda bulunan belirli yapıları hedefleyebilir veya belirli bir kod kapsamı elde etmeye çalışabilir.

Gri kutu testi (*gray-box testing*), kara kutu testi ve beyaz kutu testi arasında bir yerde bulunur. Programın içerikleri hakkında sınırlı bilgi kullanır. İlke olarak, bu, testi yapan kişinin kaynak kodun bazı bölümlerini bildiği anlamına gelir. Pratikte, genellikle testi yapan kişinin sadece, belirtimlere veya gereksinimlere göre daha ayrıntılı tasarım belgelerine erişimi olduğu anlamına gelir. Örneğin, testler bir mimari diyagrama veya programın davranışının duruma dayalı bir modeline dayanabilir.

Güvenlik Testi İpuçları ve Teknikleri

Test işlemine başlamadan önce şu noktaları göz önünde bulundurun:

- **Doğru aracı seçin**—Yazılımınızı test etmek için en iyi araçları seçmek, nelerin test edileceğine ve test planının testlerin nasıl yürüteceğini belirlemesine bağlıdır. Araç işlevlerinin çakıştığını unutmayın.
- **Araçlar hata yapar**—İlk sonuçlara şüphe ile yaklaşmalısınız. Yanlış pozitif veya yanlış negatifleri izleyin. Algılama yöntemleri genellikle tutarlı olmadığı için araç sonuçları değişebilir.
- **Sistemlerinizi koruyun**—Testlerin yanlış zamanda veya yanlış bir şekilde yapılması sistemlere zarar verebilir. Sistemlerinizi korumaya özen gösterin.
- **Testler olabildiğince gerçek olmalıdır**—Testler ağlarda ve sistemlerde, sistem işlemlerini bozmadan mümkün olan oranda çalıştırılmalıdır. Testlerinizi olabildiğince gerçek yapmaya çalışırken şu noktaları göz önünde bulundurun:
  - Önce bir sistem üzerinde önemli bir etkisi olmayan veya çökmesi muhtemel olmayan bir dizi test gerçekleştirmelisiniz. Ardından, testlerin tespit ettiği zayıf noktaları düzeltin. Bundan sonra, kesintinin en az etkili olacağı zamanlarda normal çalışmayı kesebilecek testler yapabilirsiniz.
  - En kritik sistemlerde, bu testleri iş süreklilik planı testi ile aynı anda yürütebilirsiniz. Örneğin, tam kesinti testini başarılı bir şekilde uyguladıktan sonra ancak alternatif sitede çalışmaya devam ederken, birincil siteyle alternatif sitede testleri sürdürün.
  - Penetrasyon testinin bir parçası olarak sosyal mühendisliğin eklenip eklenmeyeceğine karar verin. Test yapan kişi ve yönetim, testin teknik yöntemlerle sınırlandırılıp sınırlandırılmayacağına veya test yapan kişinin erişebilmek için insan davranışından yararlanmaya çalışması gerekip gerekmediğine karar verecektir. Sosyal mühendislik testleri gerçekleştirmek zor olabilir ancak iyi yapıldıysa ek güvenlik açıklarını ortaya çıkarabilir.

BÖLÜM ÖZETİ

Bu bölümde, güvenlik denetlemesi hakkında bilgi edindiniz. Denetlemenin daha güvenli sistemler yaratmanıza yardımcı olmak için nasıl kullanıldığını öğrendiniz. Bu denetlemelere neden ihtiyaç duyulduğunu, sorumluluk ve hesap verebilirlik kültürünü nasıl oluşturduklarını keşfettiniz. Kapsamı da dahil olmak üzere denetleme planını nasıl tanımlayacağınızı ve güvenli sistemleri geliştirmenin nasıl yürüdüğünün farkına vardınız. Denetleme ölçütlerini ve denetleme planınızın temelini oluşturmaya nasıl yardımcı olduğunu öğrendiniz. Ayrıca, kaliteli bir denetleme gerçekleştirmek için ihtiyaç duyduğunuz bilgileri toplamaya nasıl yardımcı olabileceğiniz de dahil olmak üzere veri toplama yöntemlerinden öğrendiniz. Ayrıca, denetleme sonrası faaliyetleri ve bunların denetlemeyi tamamlamanıza nasıl yardımcı olduklarını incelediniz. Sistemlerinizi izlemeye yardımcı olmak da dahil olmak üzere günlük biriktirmeyi ve analizini incelediniz. Ayrıca günlük yönetimi hakkında bilgi edindiniz. Yakalamanız gereken günlük bilgileri türleri ve bunları etkili bir şekilde yakalamanıza yardımcı olan araçlar hakkında bir anlayış geliştirdiniz. Son olarak, güvenlik sistemlerini izlemeyi ve test etmeyi öğrendiniz.

ANAHTAR KAVRAMLAR VE TERİMLER

Anomaly-based IDS - Anomali-tabanlı IDS
Benchmark - Karşılaştırmalı Değerlendirme
Black-box testing - Kara-kutu testi
Clipping level – Kırpma seviyesi
Covert act – Gizli eylem
False negative – Yanlış negatif
False positive – Yanlış pozitif
Gray-box testing – Gri kutu testi
Hardened configuration – Güçlendirilmiş yapılandırma
Hardening - Güçlendirme
Mitigation activities – Azaltıcı faaliyetler
Network mapping – Ağ haritalama
Operating system fingerprinting – İşletim sistemi parmak izi
Overt act – Açık eylem
Pattern- or signature-based IDS – Örüntü - ya da imza- tabanlı IDS
Penetration testing – Penetrasyon testi
Real-time monitoring – Gerçek-zamanlı izleme
Reconnaissance - Keşif
Security Information and Event Management (SIEM) system - Güvenlik Bilgi ve Olay Yönetimi
Stateful matching – Duruma dayalı eşleme
Vulnerability testing – Zafiyet (Güvenlik açığı) testi
White-box testing – Beyaz kutu testi
Zone transfer – Bölge aktarımı

BÖLÜM 7 DEĞERLENDİRME

1. Söz konusu riskten daha fazla maliyeti olan bir denetim kullandığınızda, kötü bir yönetim kararı veriyorsunuz demektir.
   A. Doğru
   B. Yanlış

2. Aşağıdakilerden hangisi fazla sıkı olmayan bir izin seviyesine bir örnektir?
   A. Tedbirli
   B. Hoşgörülü
   C. Rastgele
   D. Paranoyak
   E. Hepsi

3. Bir denetleme, güvenlik denetimlerinin uygun olup olmadığını, doğru kurulduğunu ve _____ inceler.
   A. Güncel olduğunu
   B. Amaçlarına hitap ettiğini
   C. İzin verilmiş olduğunu
   D. Uygun maliyetli olduğunu

4. Bir _____, sisteminizin sektörün beklentileri ile ne kadar örtüştüğünü ölçmek için kullanılan bir standarttır.
   A. Kontrol amacı
   B. Yapılandırma
   C. Ölçüt
   D. Politika

5. Aşağıdakilerden hangisi denetleme sonrası faaliyetleri içerir?
   A. Bulguları yönetime sunmak
   B. Veri analizi
   C. Çıkış görüşmeleri
   D. Denetçinin bulgularının gözden geçirilmesi
   E. Hepsi

6. Güvenlik izlemede kullanılan araç ve tekniklerden bazıları ana çizgileri, alarmları, kapalı devre TV'yi ve honeypot tuzaklarını içerir.
   A. Doğru
   B. Yanlış

7. _____, olayları derhal algılamak ve yanıtlamak kadar kritik olmadığında kullanılır.
   A. Gerçek zamanlı olmayan izleme
   B. Mantıksal bir erişim denetimi
   C. Gerçek zamanlı izleme
   D. Hiçbiri

8. Günlük girişlerini yakalamak ve analiz etmek için ortak bir platform _____'dır.
   A. Saldırı tespit sistemi (*Intrusion Detection System* - IDS)
   B. Honeypot tuzağı
   C. Güvenlik Bilgi ve Olay Yönetimi (Security Information and Event Management - SIEM) sistemi
   D. HIPAA
   E. Hepsi

9. _____ yöntemlerinde IDS, mevcut trafiği, örüntü eşleme ve durum bilgisi eşlemesi yoluyla bilinen bir ağ saldırılarına eşlik eden etkinlik örüntüleriyle karşılaştırır.
   A. İmza tabanlı
   B. Anomali tabanlı
   C. Sezgisel tarama
   D. Hepsi

10. Ana bilgisayar izolasyonu iç ağların izolasyonu ve bir _____ oluşturulmasıdır.
    A. HIDS
    B. DMZ
    C. IDS
    D. IPS

11. Güçlendirilmiş bir yapılandırma, gereksiz hizmetleri etkinleştiren bir sistemdir.
    A. Doğru
    B. Yanlış

12. Sistemin; kuruluşun organizasyonu, sistemleri ve ağları hakkında olabildiğince bilgi edinilmesi için gözden geçirmesi, _____ olarak bilinir.
    A. Penetrasyon testi
    B. Zafiyet testi
    C. Ağ haritalama
    D. Keşif

BÖLÜM

8

Risk, Yanıt ve Kurtarma

KURUMLAR SÜREKLİ BİR ŞEKİLDE değişime ayak uydurmak durumundadırlar: Örneğin şirket hisse sahipleri çeşitli şekillerde kurumlara yeni baskılar getirmekte, ülke yönetimi yeni kanunlar ve standartlar koyarak kurumları zorlamaktadırlar. Öte yandan kurumlar tedarikçileri ile müşterilerini birarada tutabilmek için tedarik zincirini yakından takip etmek ve rekabet ortamında kalıcı olabilmek için hedeflerini gerçekleştirmek üzere stratejiler belirlemek zorunda kalmaktadır. Bu değişken ortama ayak uydurabilmek çoğu zaman şirketlerin personel, Bilgi İşlem organizasyonu ve lojistik planlarini siklikla degistirmesini gerektirmektedir ki bu değişim, risk faktörünü arttırır. Bir kurumun yapısı bu organizasyonun kültürünü yansıtır, ve bu kültür kurumun bilgiyi, bu bilgiyi yaratıp kullanan insan gücü ve altyapısını korumaya yönelik davranışını etkiler.

Bir kurumun risk yönetim tarzı, kurum varlıklarına değer verme şekline yansır. Herhangi bir risk faktörünün yeterince ciddi olmadiği düşünüldüğünde kurumlar bu riski gidermek üzere yatirim yapmayı tercih etmeyecektir. Bir kurumun değerli kaynaklarını korumak üzere harcamaya hazır olduğu kaynak miktarı, riski etkiler. Bazı durumlarda kurumlar riskin yeterince ciddi olduğunu farketseler dahi yeterli bütçeye sahip olmadıklarından riski gözardı etmek zorunda kalabilirler. Bazı durumlarda ise kurumlar "kullan at" kültürünü benimseyerek kısa vadeli kazanç peşinde olduğundan uzun vadeli risk faktörlerini dikkate almayabilir, hatta sıkıntılı durumlarda faaliyetlerini tamamen sonlandırabilirler. Böyle durumlarda gereken standartlara erişmek için mümkün olan en az çaba gösterilir. Öte yandan kurum uzun vadeli başarı hedefliyorsa, etkin maliyet politikaları benimseyerek riski azaltmaya calışacaktır. Bahsedilen her bir strateji, belirli kurumlar için faydalı olabilir. Bu hususta yapılabilecek tek yanlış, risk yönetimi harcamalarını şirket kültürü ile eşleştirememektir. Örneğin "kullan-at" prensibini benimseyen bir kurum, sürdürülebilir risk planı için yatırım yapmamalıdır.

8. Bölüm Konular

Bu bölüm aşağıda verilen konuları ve kavramları içermektedir:

- Risk yönetimi ve veri güvenliği ilişkisi
- Risk yönetim süreci nedir
- Risk değerlendirmesi nedir
- Risk değerlendirmesine yönelik nicel ve nitel yaklaşımlar arasındaki farklar nelerdir
- Risk yönetim stratejisi nasıl belirlenmelidir
- Risk yönetim stratejisi belirlerken hangi faktörler ve önlemler göz önünde bulundurulmalıdır

- Üç farklı etkinlik kontrol çeşidi nedir ve güvenlik yaşam döngüsüne nasıl entegre olurlar
- İş Süreklilik Planı (*business continuity plan* - BCP) nedir ve kurumlar işletmelerinin sürdürülebilirliğini devam ettirerek bu planı nasıl uygulayabilirler
- Felaketle mücadelede yedeklemenin rolü nedir
- Felaketten kurtarma planı (*disaster recovery plan* - DRP) nedir
- Felaketten kurtarma planının temel adımları nelerdir

8. Bölüm Hedefler

Bu bölümü tamamladığınız zaman, yapabilecekleriniz:

- Risk yönetiminin temel prensiplerini anlamak
- Ayrıcalıklı olaylara nasıl yanıt verileceğini ve bu olayların nasıl analiz edileceğini anlamak
- İş süreklilik planını kullanarak beklenmedik durumların nasıl önlenebileceğini veya bu tür durumlardan nasıl en az zararla kurtulunabileceğini anlamak

Risk Yönetimi ve Bilgi Güvenliği

Risk yönetimi, bilgi güvenliğinin temel yapıtaşlarından biridir. Bir kurumun başarılı ya da başarısız her bir faaliyeti risk taşır. Bu süreçte risk yönetimine verilen önem, genel olarak kurumun iş dünyasında başarılı veya başarısız olmasını etkiler. Bu durum her bir risk faktörünün saf dışı edilebilmesinden çok, kurumun farklı risk yönetim alternatifleri arasından fayda ve maliyet dengesini belirleyebilmesine bağlıdır. Örneğin, kurumsallaşmış bir hastane işletmesiyle ilgili her türlü risk faktörünü en az düzeye indirebilmek için çabalar. Diğer yandan, az sayıda çalışanı olan yeni bir işletme daha fazla risk alıp cazip finansal getirilerden faydalanmaya daha hevesli olabilir.

Güvenlik personeli, kurumun diğer çalışanlarıyla biraraya gelerek risk faktörlerini birlikte belirlemeli ve risk yönetim çözümlerini birlikte uygulamalıdır. Bu aşamada iki temel risk yönetim ilkesi dikkate alınmalıdır:

- Bir varlığı korumak için o varlığın gerçek değerinden daha fazla harcama yapılmamalıdır. Bu durum pratikte, göründüğünden daha karmaşık olabilir. Güvenlik açıkları müşterinin güvenini sarsabilir. Başarılı bir güvenlik saldırısı ivedi zararın yanında müşterinin rakip şirketlere yönelmesine yol açabilir. Tüm bunlar esas maliyetin zararın hemen ardından harcanan miktardan daha fazla olmasına yol açar.
- Karşılığı olan bir risk içermeyen bir karşı önlem, bir problem arayan çözümdür; maliyete gerekçe göstermek zordur.

Güvenlik personeli, bilgi güvenliği ile ilgili riskin (*risk*) tanımı, riske verilen yanıt (*response*) ve kurtarma (*recovery*) konularında önemli rol oynar. Bu sebeple güvenlik personeli risklerin tanımlanması konusunda yardımcı olmalıdır. Bu faktörlerden bazıları öyle önemlidir ki, kurumun iş hayatını terk etmeye sürükleyebilir. Örneğin veri sızdırılması şirketin itibarının sarsılmasına, satışların düşmesine,

hatta ödenmesi gereken cezalar sebebiyle çok miktarda para kaybetmesine sebep olabilir. Güvenlik personeli ayrıca şirketin istenmeyen bir durumla karşılaşması durumunda operasyonlarını sürdürebilmesi için gereken planın hazırlanıp yürütülmesinde yardımcı olmalıdır. Bu tür plana iş süreklilik planı (*business continuity plan* - BCP) adı verilir. Aksaklıklar kaçınılmazdır ve her kurumun başına gelebilir. Güvenlik personeli olarak aksaklıklara karşı plan yapmak görevlerinizden biri olmalıdır. Bu amaçla şirket altyapısına hasar veren faktörleri gidermeye yönelik bir felaketten kurtarma planı (*disaster recovery plan* - DRP) hazırlanmalıdır. Güvenlik personeli olarak amacınız bir kesintinin ardından sistemi tekrar kullanıma hazır hale getirmek ve kaybolan veya zarar gören veriyi kurtarmaya çalışmaktır. Bunun yanında bir önemli görev de kurtarma sürecini hatasız biçimde yürütebilmektir.

NOT

Lütfen *http://csrc.nist.gov/publications/PubsSPs.html* adresinden erişebileceğiniz NIST SP 800 serisi güvenlik alıştırmalarını inceleyiniz. Bu adres sizin bilgi güvenliği konusunda edinmeniz gereken temel bilgileri içermektedir. Daha ileri düzeydeki güvenlik personeli, daha detaylı maddelerdeki bilgileri kullanmalıdır..

Risk Terminolojisi

Risk yönetimi; risk faktörlerini tanımlayıp her bir risk faktörü için ne yapmak gerektiğini kararlaştırmaktır. Risk yönetiminde ilk adım, risk faktörlerini tanımlamak ve değerlendirmektir. Peki risk nedir ve nasil değerlendirilir? Risk yönetimini anlamaya calişmadan önce konu ile ilgili birkaç terimi anlamak gereklidir. Aşağıdaki terimler risk değerlendirme türlerini veya risk tanımlama ve tartışma yöntemlerini açıklamaktadır:

- **Tehdit (*Threat*)**- Bir **tehdit**, olma olasılığı olan (genelde kötü) bir şeydir. Tehdit veri merkezini yıkan bir hortum veya müşteri verilerinin yüklü olduğu veritabanını çalan bir hırsız olabilir.
- **Güvenlik açığı (*Vulnerability*)** - Bir **güvenlik açığı**, bir tehdide maruz kalmaya yol açan durumdur. Bazi sistem açıkları sistemin en zayıf noktaları iken, bazıları başka aktivitelerin (örneğin çalışanların şirket ağına bağlanmak üzere akıllı telefonlarını kullanmasına izin vermek) yan etkileri olabilir.
- **Risk (*Risk*)** - **Risk,** belirli bir tehdidin belirli bir güvenlik açığı sebebiyle gerçekleşmesi olasılığıdır. Birçok risk olası hasara ve olumsuz sonuçlara yol açar. Öte yandan her risk kötü olmayabilir. Bazı riskler olumlu sonuçlara yol açabilir. Bir tehdidin zarar verme (veya olumlu etkileme) kapasitesi, ilgili riskin seviyesini belirler.
- **Etki (*Impact*)** – **Etki,** bir güvenlik açığını hedef alan bir tehdidin sebep olabileceği zararın miktarıdır. Örneğin bir virüs yazılımı yerleştiği bilgisayar sistemindeki tüm verileri etkileyebilir.

NOT

Birçok kişi riski olumlu bir faktör olarak düşünmez. Ancak belirsizlik bazen olumlu, bazen olumsuz sonuçlara yol açabilir. Örneğin, şirketinizin yazılım üreticisinin tedarik edebilirliğine bağlı olarak kullanıcılarına yeni bir yazılım sağlamak üzere plan yapıyor olduğunu farz edin. Bu durumda risk yönetim planınız hem erken hem de geç yazılım dağıtımı olasılıklarına göre planlanmalıdır. Eğer yazılım erken elinize geçerse, ya daha fazla test yapabilir, ya da yazılımı erken dağıtabilirsiniz. Eğer tedarikçi yazılımı geç teslim ederse, planladığınız dağıtım tarihini ertelemek zorunda kalabilirsiniz. Bu durumda planlanan takvime uymayan teslim tarihinin olumlu ve olumsuz etkilerini göz önüne alan bir plan yapmalısınız..

Bir tehdit gerçekleştiğinde, kurum bir olay ya da kötü olay sonucuyla karşılaşır. **Olay (*event*)**, şirkete doğrudan etkisi olan ölçülebilir bir olgudur. Bazı olayların çok az etkisi olurken bazıları kötü olay seviyesine yükselebilir. **Ayrıcalıklı olay (*incident*)**, güvenlik politikasını ihlal eden veya ihlal etme konusunda tehdit eden bir olgudur. Bir çalışanın kurum deposundan hırsızlık yapması ayrıcalıklı olaya örnektir. Ayrıcalıklı olaylar, bir önlem alınmasını gerekli kılar.

İlerleyen kısımlarda *kontroller*, *önlemler* ve *korunmalar* hakkında daha çok bilgi aktarılacaktır. Aralarında küçük farklılıklar

olmasına rağmen birçok insan bu terimleri birbirinin yerine kullanmaktadır. Bu terimlerin her biri ya bir güvenlik açığını ya da bir tehdidin etkisini azaltarak riski küçültmeye çalışır. **Kontroller (*controls*)**, hem korunmaları hem de önlemeleri içerir. Kontroller, davranışı sınırlandıran ya da kısıtlayan eylemlerdir. **Korunmalar (*safeguards*)** kontrollerdeki boşlukları ve zayıflıkları doldurmaya çalışarak tehditlerin gerçekleşmesini önlemeye çalışırlar. **Önlemler (*countermeasures*)** belirli bir tehdide karşılık verir ya da tehdidi adresler. Örneğin, yangın ihtimaline karşı su fiskiye sistemi döşemek bir önlemdir.

Risk Bileşenleri

Varlıklar, güvenlik açıkları ve tehditler risk bileşenleridir ve her biri bir formül ile ifade edilmekten çok bütünün parçasıdırlar. Varlıklar değer olarak artıp eksilebilirler. Kurumun etkin (proaktif) tedbirleri, güvenlik açıklarını bulup gidermeyi hedeflemelidir. Yeni tehditler ortaya çıktığında kendilerini mevcut tehditlere ekleriler. Tüm bu faktörler zamanla değişirken, risk de değişir. Bu sebeple periyodik olarak riskin yeniden değerlendirmesi yapılmalı, yeni veya değişen riskler belirlenmelidir.

Tehditlerin daima dışarıdan geldiği doğru bir varsayım değildir. 2014 yılında *CSO Magazine*, The CERT Program, Price Waterhouse Cooper, Deloitte, Microsoft, ve ABD Gizli Servisi son *Siber Güvenlik İzleme Araştırması (Cybersecurity Watch Survey)*'nı yayınlamışlardır. Bu rapora göre şirket içi saldırılar, rapor edilen saldırıların %28'ini oluşturmaktadır. Diğer kaynaklar, FBI'ın raporu ve Verizon'ın 2015 *Veri İhlali Araştırmaları Raporu (Data Breach Inverstigations Report)* gibi, şirket içi saldırıların tüm saldırıların %20'sini kapsamakta olduğunu belirtmektedir. Ancak, bu saldırıların etkileri oransal olarak daha zarar verici olmaktadır. Bunun yanında şirket içi saldırılar gün geçtikçe daha karmaşık hale gelmektedir. 2013 yılında Ulusal Havacılık ve Uzay Dairesi (*National Aeronautics and Space Administration* - NASA) kurum için veritabanını kapatarak uzaktan erişim politikalarını sıkılaştırmıştır. Tüm bu eylemler, yabancı uyruklu bir çalışanın olası fikir hakkı hırsızlığı yaptığı şüphesinin bir sonucudur.

NOT

Siber Güvenlik İzleme Araştırması (*Cybersecurity Watch Survey*)'na *www.cert.org/insider-threat/research/cybersecurity-watch-survey.cfm*? adresinden erişebilirsiniz. CERT Bölümü, Carnegie Mellon Üniversitesi bünyesindeki Yazılım Mühendisliği Enstitüsü'nün bir parçasıdır. CERT Insider Threat Center, *www.cert.org/insider-threat/cert-insider-threat-center.cfm* adresinde yer alan kapsamlı bir çevrimiçi kaynağa sahiptir. Verizon 2015 Veri İhlali Araştırmaları Raporu (Data Breach Inverstigations Report)'na *www.verizonenterprise.com/DBIR/2015/* adresinden erişebilirsiniz.

Yeni tehditler her zaman için mevcuttur. Birleşik Devletler Bilgisayar Acil Hazırlık Takımı (*United States Computer Emergency Readiness Team* - US-CERT) yeni tehditleri e-posta aracılığıyla bildirmektedir. Bu kurumun Teknik Siber Güvenlik Uyarıları (*Technical Cyber Security Alerts*), Siber Güvenlik Bültenleri (*Cyber Security Bulletins*), veya Siber Güvenlik Uyarıları'na (*Cyber Security Alerts*) *www.us-cert.gov/ncas/alerts* adresinden üye olabilirsiniz. Üye olduktan sonra, düzenli e-posta uyarıları alacaksınız. Aynı zamanda, haber akışına üye olabilir veya Twitter üzerinden takip edebilirsiniz.

Risk Yönetiminin Amacı

Risk yönetiminin amacı, kötü bir olay gerçekleşmeden önce olası problemleri belirlemektir. Erken tanımlama ilgili risk faktörlerine tepki göstermek zorunda kalmadan önce bu risk faktörlerini yönetmeyi sağladığından önemlidir. Riskleri aşağıdaki maddeleri göz önünde bulundurarak tanımlamak önemlidir:

- Ayrıcalıklı olaya yol açmadan önce
- Riski idare etme eylemlerini başlatmak ve planlamak için uygun zamanda (kontroller ve önlemler)
- Bir ürün, sistem veya projenin yaşam süreci boyunca sürekli bir şekilde

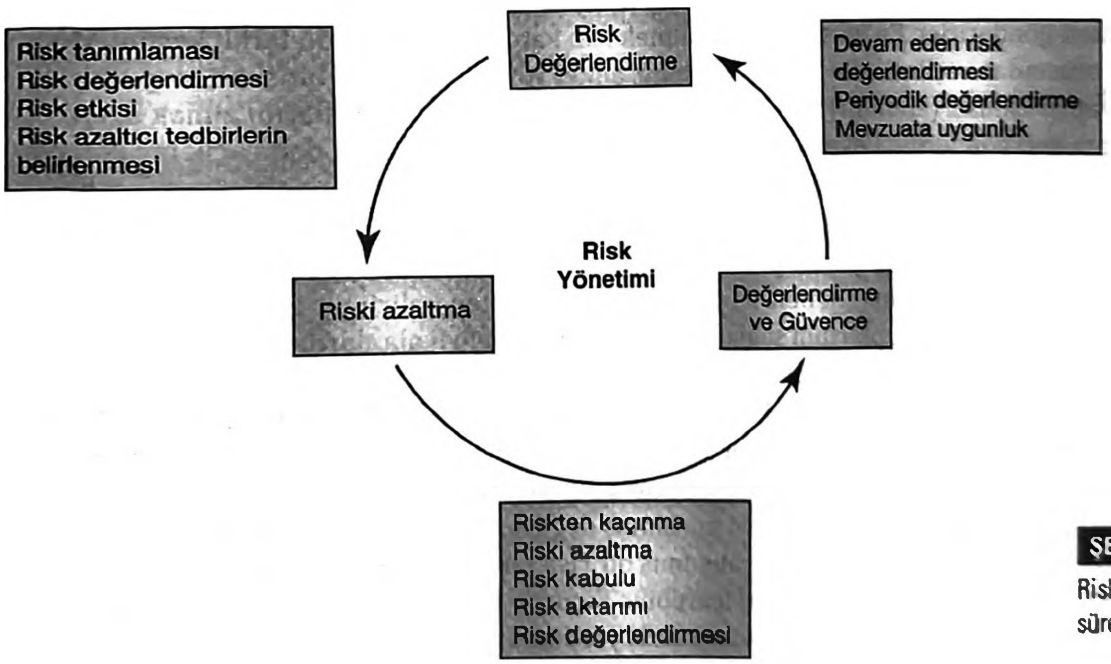
Bir riskin gerçekleşme olasılığı hiçbir zaman sıfıra indirgenemez. Bir kurumun risk kültürünü tanımlamanın ardından, risk faktörleri değerlendirilerek kuruma ciddi etkisi olabilecek olanlar öncelikli olarak ele alınmalıdır. Bunun yanında risk ile başa çıkma maliyetlerinin rasyonalize edilmesi gereklidir. Pek çok durumda az miktarda risk azalımının maliyeti yüksek olmaktadır. Risk yöneticisinin görevlerinden biri, kabul edilebilir risk seviyesini belirleyip gerekli kontrolleri uygulayarak mevcut risklerin bu seviyeye çekilmesini sağlamaktır. Ayrıca risk yöneticisi, bazı risk yönetim etkinliklerini yeni risklerin belirlenmesi üzerine odaklayarak bu risklere olumsuz bir olaya yol açmadan önce müdahale edebilir. Bu sürecin bir kısmı sürekli bir şekilde risk faktörlerinin yeniden değerlendirilerek gereken tedbirlerin alınmasından ibaret olmalıdır.

Risk Yönetim Süreci

ŞEKİL 8-1 risk yönetim sürecini göstermektedir. Risk yönetimi aslında sonu olmayan bir süreçtir. Tüm döngüyü periyodik olarak ziyaret etmek, mevcut tehditlere hazırlıklı olmak açısından çok önemlidir. Bu süreç, kurum için risk yönetim adımlarının nasıl yürütüleceğini tanımlar. Örneğin, risk analizinin belirli aralıkla yapılacağı belirlenmiş olsun. Bu analizi yürütmek üzere kullanılacak araçlar risk faktörlerini tanımlayacak, sınıflandıracak ve sıralayacak belgeleri içermelidir. Bu yaklaşım, Proje Yönetim Enstitüsü'nün (*Project Management Institute* - PMI) Proje Yönetimi Bilgi Tabanı (*Project Management Body of Knowledge* - PMBOK) ile tutarlıdır. Her ne kadar PMI tek yaklaşım olmasa da, genel olarak proje yönetimi ve buna bağlı olarak risk yönetimi hakkında faydalı bilgiler sunar.

Risk yönetim süreci aşamaları şöyle sıralanmaktadır:

- **Riskleri tanımlama**—Risk yönetiminde ilk adım olan riskleri tanımlamadır. Ne yanlış gidebilir? Bu sorunun cevapları yangın, sel, deprem, yıldırım, elektrik veya diğer hizmet kesintisi, grev ve ulaşım aksaklıklarını içerebilir. Her bir tehdit için senaryolar geliştirilerek tehditlerin değerlendirilmesine çalışılmalıdır.



ŞEKİL 8-1
Risk yönetim süreci

- **Riskleri değerlendirme**—Bazı riskler diğerlerinden daha fazla kayıba yol açma olasılığına sahiptirler. Dahası, her risk her fiziksel konumdaki her kurum için geçerli olmayabilir. Örneğin, Montana'daki ve Moskova'daki şirketlerin hortum riskinden korunmasına gerek yoktur. Olası riskler göz önünde bulundurulduğunda senaryoya ve fiziksel konuma bağlı olarak risk etkisi daha az ya da çok olabilir. Risk değerlendirmesi hangi risklerin en ciddi olduğunu tespit etmektir.
- **Riske verilecek yanıtı planlama**—En yüksek öncelikli risklerle başlayarak her bir risk için potansiyel yanıtların ne olacağı araştırmalıdır. Şirketin üst yönetiminin yönlendirmesi ışığında, her bir risk için en az zararla sonuçlanacak yanıtlar belirlenmelidir.
- **Risk yanıtlarının gerçekleştirimi**—Bir önceki adımda her bir risk için belirlenen yanıtların gerçekleştirimi için eyleme geçilmesidir.
- **Risk yanıtlarının izlenmesi ve kontrol edilmesi**—Her şeyin planlandığı gibi ilerlediğinden emin olmak için her bir risk yanıtı izlenir ve ölçümler yapılır. Bu aşama pasif izleme ve günlük tutma ile birlikte bir kontrolün nasıl davrandığını görmek için aktif testi içerebilir.

NOT

"Film konusu" risklerine zaman ve para harcamaktan kaçınmak önemlidir. Senaryo yazarları imkansız senaryolar yaratabilir ve onları mümkün hatta muhtemel gösterebilir. Bu sahte tehditlere karşı korunmak için para harcamak neredeyse her zaman bir israftır. Bunun yerine, gerçekçi olasılıklara odaklanın.

Riskleri Tanımlama

Risk yönetimi sürecinde ilk adım farklı risklerin tanımlanmasıdır. Şirketler risk tanımlamak için pek çok farklı yöntem kullanmaktadırlar. Bu yöntemlerden her biri, farklı yaklaşımlarla aynı problemi –mümkün oldukça çok sayıda risk tanımlama –çözmeye çalışır. Her bir yaklaşımda temel strateji, farklı kaynaklar kullanarak kapsamlı bir risk listesi hazırlamaktır. Yaygın risk tanımlama yöntemlerinden bazıları aşağıda sıralanmıştır:

- **Beyin fırtınası**—Bu yöntemde grup toplantısı sırasında katımcılardan yapısal olmayan veri toplanır. Toplantı yöneticisi tüm katılımcıları önerilerini çekinmeksizin belirtmeye teşvik etmelidir.
- **Anketler**—Bu yöntemi kullanan şirketler katılımcılara önceden hazırlanmış bir dizi sorudan oluşan anketi gönderirler. En iyi sonucu alabilmek için katılımcılar şirketin farklı kesimlerinde çalışanlar arasından seçilmelidir. Delphi yöntemi, anket yönteminin özel bir şekli olup bu yöntemde cevaplar isimsiz (anonim) ve karışık bir şekilde toplanarak yorumlarını almak üzere katılımcılara geri gönderilir. Cevapları anonim olarak toplama yaklaşımı, daha açık bir iletişim ortamı yaratır.
- **Mülakatlar**—Grup olarak ya da birebir uygulanabilen mülakatlar, risklerin detayları hakkında bilgi toplamak için etkin bir yöntemdir.
- **Çalışma grupları**—Bu yöntem belirli bir iş alanından seçilen belirli bir grubun fikrini almaya yöneliktir. Çalışma gruplarının sağladığı geribildirim, belirli alanlardaki risklerin belirlenmesine büyük ölçüde yardım eder.
- **Kontrol Listeleri**—Pek çok kurum kendi kullanımları ya da genel dağıtım için kullanılmak üzere risk kontrol listeleri hazırlar. Benzer kurumlar veya amaçlar için hazırlanmış kontrol listeleri ilgili risklerin kapsamlı bir şekilde ele alınmasına yardımcı olur.
- **Geçmişe ait bilgiler**—Bir kurum yeni kurulmuş değilse, elinde geçmişe ait birikmiş bilgiler olacaktır. Bu bilgi üzerinde önceden çalışılmış bir risk tanımlama sürecine, ya da geçmişte yolunda gitmeyen bir sürece ait belgeleri içerebilir. Kaynağı her ne olursa olsun, geçmişe ait bilgiler mevcut risklerin tanımlanması konusunda yardımcı olabilir.

Pek çok şirket riskleri tanımlamak için birden fazla yöntem kullanmaktadır. Siz de şirketiniz için en uygun yöntemi kullanmalısınız. Hangi yöntemin en iyi olduğuna karar vermek için de farklı faaliyet alanlarından mümkün oldukça çok sayıda kişiyi bu riskleri belirleme sürecine dahil etmelisiniz. En iyisi, şirketinizin başa çıkabileceğinden daha fazla sayıda risk belirlemektir. Her ne kadar bu çözüm akılcı bir çözüm gibi görünmese de, önemli riskleri tamamen göz ardı etmekten daha iyidir. Çok sayıda risk tanımlama yöntemi kullanıp şirketiniz için en uygun yöntemler birleşimini belirlemelisiniz.

Risk tanımlama sürecinin sonunda tanımlanmış riskler listesi elde edilir. PMI bu listeyi **risk kaydı (*risk register*)** olarak adlandırmaktadır. Risk kaydı ek olarak çok sayıda bilgi içerebilir ancak aşağıdaki bilgiler bu listede yer alması gereken minimum bilgilerdir:

- Riskin tanımı
- İlgili olay gerçekleştiğinde beklenen etki
- İlgili olayın gerçekleşme ihtimali
- Riski azaltmak için atılacak adımlar
- Eğer risk gerçekleşirse atılacak adımlar
- Riskin derecelendirilmesi

Gelişmekte Olan Tehditler

Risk tanımlama faaliyetlerinin bir kısmı yeni ve gelişmekte olan tehditler üzerine yoğunlaşmalıdır. Bu tür tehditler pek çok farklı alanda ve iç ya da dış kaynaklı olabilir. Gelişmekte olan tehditlerin bazıları aşağıdaki listede sunulmuştur:

- Yeni teknoloji
- Kurum kültüründe veya çevresinde meydana gelen değişiklikler
- Teknolojinin izinsiz kullanımı (Örneğin; kablosuz iletişim teknolojileri, hileli modem, akıllı telefonlar, tabletler veya lisanssız yazılım kullanımı)
- Kanun ve düzenlemelerdeki değişiklikler
- İşlerin yürütülmesine dair değişiklikler (Örneğin; dışarıdan kaynak temini, küreselleşme)

Etkin bir güvenlik personeli, yeni tehditleri izleyerek yeni bir risk incelemesinin gerekli olup olmadığını belirlemelidir. Gelişmekte olan tehditlerin en yaygın olduğu iki alan bulut servisleri ve sanallaştırmadır. Şirketler veri işleme sürecini bulut hizmet tedarikçilerine devretmeye (*outsourcing*) başladıkça yeni tehditlerle karşı karşıya kalmaktadırlar. Bazı tehditler doğrudan bulut hizmet tedarikçileri ile ilgili iken, bazıları sanallaştırmanın iç veya dış kullanıcıları ile ilgilidir. Bu tehditlerden bazıları aşağıda listelenmiştir:

- Sanallaştırma sınırlarının ihlali
- Dışarıya devredilen kaynaklar için erişim denetimlerinin bulunmaması
- Bulut veya sanallaştırma hizmetlerinin güvenilirliği
- Bulut hizmet tedarikçisinin (*cloud service provider* - CSP) kilitlenmesi
- Güvenli olmayan uygulama program arayüzleri (*application program interface* - API)

- Kötü niyetli iç kullanıcılar
- Hesabı ele geçirme

Her ne kadar bu tehditler her ortam için geçerliyse de, bulut ve sanal ortamlar işlerin sıklıkla dış kaynaklara devredilmesi sebebiyle daha fazla miktarda risk taşımaktadırlar. Bulut ve sanal hizmetler söz konusu olduğunda daima yeni tehditleri göz önünde bulundurmak gerekmektedir.

Durağan Ortamlar

Yakından takip edilmesi gereken bir diğer tehdit grubu durağan ortamlara aittir. **Durağan ortamlar (*static environments*)**, başlangıçtan itibaren çok değişmeyen ortamlardır. Normal veya dinamik ortamlar sıklıkla değişirken durağan ortamlar kurulduğu gibi kalma eğilimindedirler. Bazı durağan sistem örnekleri aşağıda sıralanmıştır:

- **Danışmalı Kontrol ve Veri Toplama Sistemi (*Supervisory Control and Data Acquisition - SCADA*)**—SCADA sistemleri daha çok endüstriyel ortamlarda görülür. SCADA sistemleri üretim sektöründe; güç dağıtımında; yağ, su ve gaz dağıtımında; fiziksel araçların kontrolünde ve izlenmesinde kullanılırlar. Bu sistemler çoğunlukla üretici tarafından işletim sisteminin durağan versiyonu kullanılarak, bir yazılım yığını yaratmak üzere üretilirler. SCADA sistemlerinin gömülü yazılım katmanları arasında güvenlik açıkları belirlenmesi durumunda bu sisteme yama yapılması kolay değildir.
- **Gömülü Sistemler**— Bu sistemler genellikle daha geniş bir cihazın içine yerleştirilmiş küçük bilgisayarlardır. Bilgisayarı meydana getiren bileşenler, cihazın diğer parçalarını da taşıyan bir düzeneğin içine yerleştirilir. Bu tür cihazlar başka donanım ya da mekanik parçalar da içerebilir. Örneğin, bir robot vakum cihazı, hareketlerini kontrol eden bir gömülü sistem içerir. Gömülü bilgisayara erişim kolay olmadığından, güvenlik yamalarını güncellemek de kolay olmaz.
- **Mobil Araçlar (*Android*, iOS, *Windows*)**—Mobil işletim sistemi yamaları ve güncellemeleri yaygın ve kolay uygulanabilir olsa da pek çok kullanıcı cihazlarını gereken sıklıkta güncellemez. Kötü güncelleme tecrübeleri kullanıcıları gereken güncellemeleri yapmaktan alıkoyabilir. Bu durum yama yapılmamış mobil uç noktaların tehdit altında kalmasına yol açar. Ek olarak, birçok mobil cihaz bağlandıkları kurumun kontrolü dışındadır.
- **Ana bilgisayarlar**—Bu büyük boyutta bilgisayarlar çoğunlukla büyük kurumların veri merkezlerinde bulunurlar. Büyük çapta veri işleme amacıyla kullanılırlar ve yüksek maliyetlidirler. Bu sistemlerin aksaması (*downtime*) çok maliyetli olup tavsiye edilmez. Bu sebeple güvenlik yamalarını yüklemek için sistem aksama penceresini beklemek en uygun çözümdür. Ana bilgisayarlar bazı durumlarda gelişmekte olan tehditlerin etkisi altında işlerler.
- **Oyun konsolları**—Bu tür bilgisayarlar grafik uygulamalarını etkin bir biçimde işletebilen sistemlerdir. Günümüzde oyun konsolları sıklıkla internete bağlı olarak calışır ve düzenli olarak yeni tehditlere maruz kalırlar. Üreticiler oyun konsolları için güvenlik yamaları sağlar fakat tüm kullanıcılar sistemlerini güncellemek konusunda yeterli özeni göstermez. Birçok kullanıcı konsollarını açar ve oyun oynamaya başlamayı ister.
- **Taşıt sistemleri** —Durağan sistemlerin son çeşidi olan bu kategorideki sistemler, gömülü sistemlere bir örnektir. Günümüzde gittikçe artan sayıda taşıt koşulları monitör etme, internet bağlantısı, gerçek zamanlı yönlendirme ve hatta taşıtın temel işleyişi ile ilgili (Örneğin; otomatik

park etme veya sürücüsüz otomobiller) kontroller sağlayan sistemler ile donatılmaktadır. Güvenliği artırmak adına taşıtın işleyişine müdahale eden sistemler yeni taşıtlarda standart halini almaya başlamaktadır. Örneğin, kilitlenmeyen fren sistemi ve çarpışma önler sistemler pek çok taşıt sisteminde yer almaktadır. Bu tür sistemlerin güncellenmesi veya yama yapılması, taşıtın bakım yapılan yetkili servise götürülmesi gerekliliği nedeni ile zordur. Eğer üreticiler güncelleme işlemlerini çok kolaylaştırırsa, saldırganlar bu sistemlere kolaylıkla zararlı kod yerleştirebilir.

Risk tanımlama sürecinin bir kısmı bu durağan sistemleri göz önünde bulundurarak gerçekleştirilmelidir. Bu sistemler de diğer bütün sistemler gibi tehditlerle karşı karşıya kalırlar. Her ne kadar durağan sistemlere yönelik tehditleri belirlemek daha zor olsa da, güvenli bir sistemin tüm bileşenlerinin güvenli olmasına bağlı olduğu unutulmamalıdır.

Risk Değerlendirmesi

İyi bir risk değerlendirmesi şirketin risk ortamını yöneticilerine onların anlayacağı bir dille açıklamaya çalışmalıdır. Bu değerlendirmede, ne tür risklerin bir şirketi işlevsellikten alıkoyacağı belirlenmelidir. Bazen BT çalışanları şirketin BT alt yapısını korumak konusunda öyle duyarlı hale gelirler ki, sistemlerinin şirketin temel hedeflerini gerçekleştirmek üzere kullanıldığını unutabilirler. Risk değerlendirme sürecinde "Bu benim sistemlerim ve altyapım için ne anlam taşıyor?" sorusundan çok, "Bunun şirket için anlamı nedir?" ve "Bunun şirket için değeri nedir?" sorularına odaklanmak gerekmektedir.

> **NOT**
>
> Ayrıcalıklı olayların gerçekleşmesi kaçınılmazdır. Felaket planlaması (bu bölümün ilerleyen kısımlarında incelenmiştir) ile birlikte uygulanan risk yönetimi (riskin tanımlanması, değerlendirilmesi ve yanıt verilmesi), bir şirketin hayatta kalması veya başarısız olması arasındaki fark anlamına gelmektedir.

Riske tepki göstermek için birçok alternatif olsa da risk değerlendirmesinin temel sebebi en uygun yanıt seçeneklerinin belirlenmesini sağlayacak veriyi toplamaktır. Bu da maliyete, verimliliğe, üretkenliğe etki, ve kullanıcı kabulü gibi pek çok parametreye bağlıdır.

Risk Değerlendirmesine Yönelik İki Yaklaşım: Nitel ve Nicel

Risk değerlendirmesine iki farklı şekilde yaklaşabilirsiniz:

- **Nitel risk değerlendirmesi—Nitel risk değerlendirmesi (*qualitative risk assessment*),** riskleri gerçekleşme olasılığına ve iş faaliyetleri üzerindeki etkisine göre sıralar. Etki, gerçekleşen bir tehdidin yaratacağı tesirdir. Etki genellikle düşük (önemsiz) ile yüksek (felakete yol açan) seviyeler arasında derecelendirilir. Nitel risk analizi çoğunlukla öznel (kişiye bağlı) olsa da, pek çok kritik riskin belirlenmesine yardımcı olur. Bu tür risk analizi şirketin farklı bölümlerinde çalışan kişilerin sağlayacağı verilere ihtiyaç duyar ve bu kişilerin sağlayacağı göreceli verilerle belirlenir. Örneğin, nitel bir değerlendirme hangi risklerin diğerlerinden daha kötü olduğunu sorar. Bu, iş birimlerinin ve teknik uzmanların bir olayın diğer bölümler ve faaliyetler üzerindeki etkilerini anlamalarına izin verir.

- **Nicel risk değerlendirmesi—Nicel risk değerlendirmesi (quantitative risk assessment)** riski parasal olarak tanımlamaya çalışır ve her bir risk faktörü için dolar cinsinden değer ataması yapar. Nitel risk değerlendirmesine göre daha objektiftir. Bu yöntemin dezavantajlarından biri, bazi risklerin parasal değerinin belirlenmesinin güçlüğüdür. Bunlar, itibar ve önlemlerin kullanılabilirliğini içermektedir. Özellikle gelecekte gerçekleşebilecek olayların maliyetini önceden hesaplamak çoğu zaman zordur. Diğer yandan, nicel risk değerlendirmesinin otomatikleştirilmesi nitel risk değerlendirmesine göre daha kolaydır.

ŞEKİL 8-2
Nitel ve nicel risk analizi karşılaştırması

Nicel	Sayısal-Temelli (Somut) Veri	Finansal Veri Nesneljective
Nitel	Senaryo-Temelli (Soyut) Veri	Senaryo-Tabanlı Öznel

Nicel analiz, ilgili riske bir dolar miktarı ataması yapar. Nitel analiz ise riskleri, etkilerinin ve/ya da olasılıklarının önemini temel alarak tanımlar. **ŞEKİL 8-2** Nitel ve nicel risk analizlerini karşılaştırmaktadır. Bu yaklaşımlardan hiçbiri kendi başına mükemmel değildir. Başarılı bir risk analizi çoğu zaman her iki yöntemi de içerir.

Birçok durumda adı geçen iki yöntem birleştirilebilir. Nitel risk analizi, istenmeyen bir durumun kurum içinde yaratacağı etkinin daha iyi anlaşılmasını sağlar. Ayrıca, olası zararın etkisini azaltmak amacıyla kurum bünyesindeki bölümlerin biraraya gelip ortak hareket etmesi için gereken iletişim ortamını sağlar. Ancak nitel risk analizi, nicel risk analizi tarafından sağlanan güvenilir finansal veriyi sağlamaktan yoksundur. Bu maliyet bilgisine genellikle, önlemlerin maliyetini gerekçelendirilmek için ihtiyaç duyarsınız. Bu nedenle, her iki analiz yöntemini birden dikkate almalısınız.

Nicel Riskin Hesaplanması. Nicel riskin hesaplanması için, kuruma ait her bir varlığın ne değerde olduğunu ve bir kayıp ile karşılaşma olasılığınızın ne olduğunu bilmelisiniz. Bu, olayın **kayıp beklentisi (*loss expectancy*)** dir. Bunu hesaplamak çoklu adımlardan oluşan bir süreçtir:

1. **Varlık değerinin (*Asset value* - AV) hesaplanması**—Varlık, bir kurum için değeri olan herhangi bir bileşendir. Varlıklar dokunulabilir (bina gibi) veya dokunulamaz (şirket saygınlığı gibi) olabilir. Risk değerlendirme sürecindeki ilk adım kurumun her bir varlığının ve değerinin belirlenmesidir. Varlık değeri donanım ve sistemlerin yenilenme maliyetlerini dikkate almalıdır. Aynı zamanda, üretkenlik kaybı, şirket saygınlığı yitimi, müşteri güveninin kaybı gibi faktörleri de içermelidir.
2. **Maruz kalma faktörünün (*Exposure factor* -EF) hesaplanması**—Bu aşamada beklenmedik bir olay gerçekleştiğinde kaybedilecek varlık değeri yüzdesi hesaplanır. Örneğin, her taşıt kazası sonucunda taşıt hurda haline gelmez. Bu sebeple sigorta şirketleri herbir kaza bildirimi için olası kayıp yüzdesini hesaplar. Bu amaçla her bir taşıt modeli ve yılı için bilinen tamir maliyetini kullanarak kaza bildirimi başına maruz kalma faktörünü tahmini olarak hesaplarlar. Bu tahmin belirli bir kaza bildirimi için doğru olmasa da (şans eseri değilse), yüzlerce ve hatta binlerce taşıt kaza bildirimi için gruplandırma yapıldığında doğru olacaktır.
3. **Tekil kayıp beklentisinin (*Single loss expactancy* - SLE) hesaplanması**—Tekil bir kayip maliyeti, önceki iki değer kullanılarak hesaplanabilir. Eğer bir sigorta şirketi son model bir taşıt için EF değerini %20 olarak hesaplamışsa, her seferinde yeni bir kaza bildirimi yapıldığında aracın varlık değerine bakıp bu değeri EF ile çarparak ödenmesi gereken maliyeti kolaylıkla hesaplayabilir. Bu, sigorta şirketinin sigorta primlerini doğru bir biçimde hesaplamasına ve şirketin para kaybetme riskini azaltmasına izin verir.
4. **Belli bir kaybın yıllık gerçekleşme sıklığını belirleme**—Bu miktar **yıllık gerçekleşme oranı (*annualized rate of occurence*)** (ARO) veya risk **olasılığı** olarak da adlandırılır. Bazı durumlarda ARO'lar birden büyük olabilir. Örneğin, Buffalo ya da Berlin'de yil içinde kar

fırtınası olma olasılığı pek çok kez iken başka coğrafyalarda bu olasılık daha düşük olabilir. Örneğin, bir depoda yangın çıkma olasılığı her 20 senede bir olabilir. Beklenmedik bir olayın ne sıklıkta gerçekleşeceğini tahmin etmek çok kolay olmayabilir. Bu hesaplamanın doğru olması için içsel ve dışsal faktörler göz önünde bulundurulmalıdır. Öte yandan geçmişe ait veri her zaman için geleceği doğru şekilde tahmin edemez. Örneğin, içsel bir tehditten kaynaklanan bir ayrıcalıklı olayın gerçekleşmesi, çalışanların huzursuz olduğu zamanlarda veya kontrat görüşmeleri sırasında, diğer her zamandan daha olasıdır.

5. **Yıllık kayıp beklentisinin (*Annualized loss expectancy* - ALE) belirlenmesi** —ALE, SLE (ayrıcalıklı olay gerçeklestiğinde yaşanan kayıp) ile ARO değerlerinin çarpılması ile hesaplanır. ALE, kurumun riskin olası bütün etkilerini belirlemesini sağlar. Daha seyrek gerçekleşen olaylar için, ALE SLE'den cok daha az olacaktır. Örneğin, bir olayın gerçekleşme olasılığı her 10 yılda bir ise ARO 0.10 veya %10 olacaktır. Eğer SLE 1000$ ise ALE sadece 100$ (1,000$ x 0.10) olacaktır. Diğer yandan, ARO 20 ise, yani beklenmeyen olayın gerçekleşme olasılığı her yıl 20 defa ise, bu durumda ALE 20,000$ (1,000$ × 20) olacaktır.

TABLO 8-1 nicel risk değerini hesaplamada kullanılacak formülleri içermektedir. Nicel risk değerini hesaplamanın amacı, bir önlem için harcanabilecek maksimum miktari belirlemektir. Önlemlerin maliyeti, ALE'den az olmalıdır.

Şu örneği düşünün. Şirketinizde 100 kullanıcı laptop kullanıyor olsun. Bilgisayar, yazılım ve veri maliyetlerinden oluşan toplam maliyet değerinin her bir laptop icin 1,500$ olduğunu varsayalım. Son iki yılda şirkette her yıl altı bilgisayarın kaybolduğunu düşünelim. Bu bilgi sizin SLE, ARO ve ALE'yi hesaplamanızı sağlar:

- SLE 1,500$'dır.
- ARO 6'dır.
- ALE 9,000$'dır.

Bilgisayar sistemlerinin çalınmaya karşı korunmasına önlem olarak donanım kilitleri satin alınmasının önerildiğini varsayalım. Bisiklet sürücülerinin bisikletlerini bisiklet parke yerine kilitlemesi gibi, kullanıcılar da bu kilitleri sahipsiz bilgisayarları mobilyaya kilitlemek için kullanabilirler. Eğer bu kilitler toptan satın alınırsa her bir kilidin maliyeti 10$ olsun. Ek olarak, eğer bu kilitler satın alınıp kullanılırsa, yıllık kayıp riskinin altı taneden bir taneye düşeceğini varsayın. Bu maliyet etkin bir önlem midir?

- Önlemin maliyeti 1,000$'dır (10$ × 100 bilgisayar)
- Yeni ARO 1'dir.
- Yeni ALE 1,500$'dır.

TABLO 8-1 Nicel riskin belirlenmesi.

HESAPLANAN DEĞER	FORMÜL
Tekil kayıp beklentisi (SLE)	AV × EF = SLE
Yıllık gerçekleşme oranı(ARO)	ARO = Yıllık olay sayısı
Yıllık kayıp beklentisi (ALE)	SLE × ARO = ALE

NOT

Riskin her iki ölçekte de nerede yer alacağını belirlemek için uzman görüşüne başvurulmalı, eğer uzman görüşleri farklıysa fikir birliğine varılmaya çalışılmalıdır. Bu tür analizde şirketin saygınlığı ve halkın ilgisi gibi dokunulamaz faktörler de göz önünde bulundurulmalıdır..

Açıkca görülmektedir ki bu önlem maliyet etkin bir denetimdir. Önerilen tedbirle şirket yılda 9.000$ kaybetmek yerine 1.000$ harcamakta ve sadece 1.500$ kaybetmektedir. Bu durumda toplam harcanan miktar 2.500$ olacaktır. Buna karşılık, önlem maliyeti için örneğin 20.000$ ayrılırsa, 9.000$'ı kaybetmemek icin 20.000$'lık önlem yatırımı yapmak maliyet etkin bir çözüm olmayacaktır.

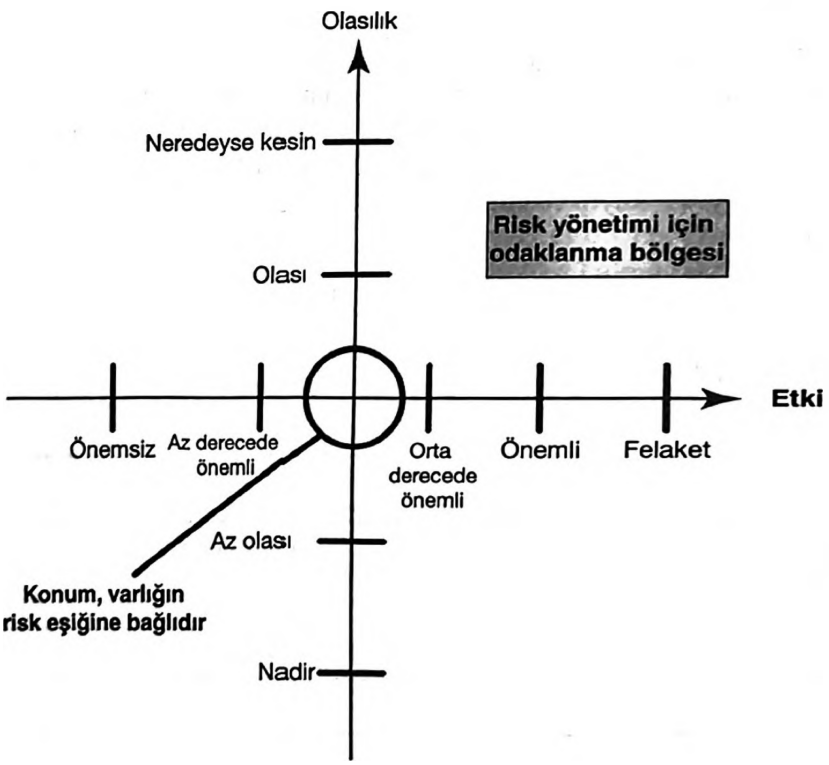
Nitel Risk Analizi. Her risk iki temel ölçek kullanılarak değerlendirilebilir:

- **Olasılık** – Bazı olaylar—Örnegin çalışanların işe gelişi esnasında kart okuyucunun hatalı çalışması - daha seyrek gerçekleşirken diğer bazı olaylar - örneğin bir çalışanın hasta olduğunu rapor edip işe gelememesi - daha sıklıkla yaşanır.
- **Etki**—Bazı olaylar—Örnegin bir bilgisayarın açılışı sırasında sorun yaşanması -şirketin üretkenliği üzerinde farkedilir bir etki yaratmazken diğer bazı olaylar- Örneğin üretim sisteminin arızalanması- çok daha büyük etki yaratır.

Olması muhtemel olaylar her iki ölçeğe göre değerlendirilip, **SEKİL 8-3**'te gösterilen çizelge üzerine yerleştirilmelidir.

Bu şekil üzerinde yer alan "Risk yönetimi için odaklanma bölgesi" çeyrek dairesi, olasılığı yüksek ve gerçeklestiği durumda etkisi fazla olacak riskleri içerir. Bu sebeple bu kategorideki riskler öncelikli olarak ele alınmalıdır. Eğer karşı tedbirler ilk bu risklere

SEKİL 8-3
Nitel risk analizi



yönelik tasarlanırsa, riskin olasılığını ve olumsuz etkisini azaltabilir. Risk yönetimi faaliyetlerinizi yalnızca üst sağ kadranla sınırlandırmamalısınız ancak riske yanıt çabalarınızın odaklanması gereken yer burasıdır. Risk azaltma, aktarım, kabul veya kaçınma —bir sonraki bölümde ele alınmaktadır— üst sağ kadrandaki riskleri azaltır. Bir hatırlatma olarak, amaç, riski ortadan kaldırmak değil, bunun yerine riski kabul edilebilir bir düzeye indirmektir.

Riske Yanıtın Planlanması

Risk yönetim sürecinin sonraki iki aşaması olası risklerin her biri ile başa çıkmak üzere bir plan geliştirmek ve bu planı uygulamaktır. Risk yönetim stratejilerini geliştirirken en yaygın tepkilerin ne olduğu bilinmelidir: Her olumsuz risk azaltılabilir, aktarılabilir, kabul edilebili, veya kaçınılabilir.

- **Azaltma**—Bu yaklasim, tanimlanan riskleri farkli denetimler kullanarak azaltmaya calisir. Bu denetimler idari, teknik veya fiziksel olabilir. Örneğin anti-virüs yazilimi yüklemek bilgisayarlara virüs bulaşma riskini azaltır.
- **Aktarma**—Bu yaklaşım, kurumun riski baska varlıklara aktarmasıdır. Sigortalama, aktarma yoluyla riski azaltmanın yaygın yöntemlerinden biridir. Bu şekilde bir kurum riski belirli bir prim karşılığında sigorta şirketine "satar". Bazı durumlarda ise risk aktarma ile kurumun fazla sorumluluktan kurtulması sağlanmaya çalışılır. Örneğin, bir otel bir park yeri şirketi ile anlaşarak park yerinin yönetim işini transfer edebilir. Bu durumda park edilen araçlarda gerçekleşecek kayıplar otelin değil park yeri şirketinin sorumluluğu altında olacak, olası bir hırsızlık durumunda otel bir dava ile karşı karşıya kalmayacaktır.
- **Kabul Etme**—Bu yaklaşımda kurum riski kabul eder. Kurum riskin varlığını kabul eder ve riski azaltma maliyeti, risk sebebiyle yaşanacak olası kaybın maliyetinden daha fazladır. Bu durum kendi kendini sigortalama ya da sigorta indirimi kullanmayı da kapsar. Bir kurumun kabul etmeye razı olduğu risk, üst yönetimin riski kabullenme konusundaki isteğine bağlıdır. Örneğin bir doktor meslek hatası sigortası satın alarak kayıp riskinin sigorta indirimine eşit olduğu ödeme düzeyini kabul edebilir. Fakat meslekte hata yapma olasılığının az olduğunu düşünerek daha yüksek prim ödemeyi gereksiz bulabilir.
- **Kaçınma**—Riskten kaçınma riski almamaya karar vermek demektir. Bir şirket risk seviyesinin çok yüksek olması durumunda bir iş sahasından çekilebilir veya böyle bir yeni iş sahasina girmekten kaçınabilir. Kaçınma stratejisi söz konusu olduğunda yönetim potansiyel kayıp olasılığının, riskli etkinliği sürdürmekle edinilecek kazançtan daha fazla olduğuna karar verir. Örneğin, bir şirket siyasi belirsizliğin olduğu bir ülkede yeni bir şube açmaktan vazgeçebilir.

Olumlu riskler için, her bir riskten yararlanabilir, riski paylaşabilir, geliştirebilir veya kabul edebilirsiniz:

- **Yararlanma**—Olumlu bir riskten yararlandığınızda, bu riske yanıt verdiğinizde ortaya çıkan bir fırsattan yararlanırsınız. Örneğin, kuruluşunuzun belirli bir riski ele almanıza yardımcı olmak için kuruluşunuzda kullanılmak üzere eğitim materyalleri geliştirdiğini varsayalım. Bu eğitim materyallerini diğer kuruluşlara ambalajlayarak ve pazarlayarak riski kullanabilirsiniz.

- **Paylaşma**—Olumlu bir risk paylaşıldığında, bu risk ile ilgili fırsatlara üçüncü şahıslar da dahil edilmiş olur. Örneğin bir başka kurumla biraraya gelerek bilgisayar lisansı satın almak, toplam sipariş miktarının büyüklüğü sayesinde her iki şirketin de önemli bir indirimden faydalanmasını sağlayabilir. (Bu durumda risk lisans maliyetinin değişme olasılığıdır.)
- **Geliştirme**—Olumlu bir risk geliştirildiğinde, risk ile ilgili olumlu etki olasılığı artırılmaya çalışılır. Örneğin, erken tamamlanıp teslim edilmesi halinde 20.000$ ikramiye verileceği belirtilmiş bir yazılım dağıtım sözleşmeniz olduğunu varsayalım. Olumlu riski geliştirmek için - kendi programınıza uymayan yazılım teslim tarihini -taşeron bir firma ile 5.000$ tutarında bir anlaşma yaparak yazılımın planlanandan erken tarihte bitirilmesini sağlayabilirsiniz.
- **Kabullenme**—Olumlu bir riski kabul ettiğinizde, riskin potansiyel etkileri olumlu olduğundan ve değer kattığından, bunu ele almak için hiçbir adım atmazsınız. Örneğin, şirketiniz yeni iş istasyonlarının kurulumunu yarı zamana indiren yeni bir otomatik yedekleme ve yapılandırma hizmet programı satın almış olsun. Yardımcı program yeni olduğu için, kullanımının öğrenilmesi biraz zaman alabilir; bu da kuruluşunuzun yeni iş istasyonlarının kurulum zamanından tasarruf etmesine yardımcı *olamayacağı* anlamına gelir. En kötüsü, yeni yardımcı programı öğrenmenin ve bunları kurulumları yönetmek için kullanmanın, kurulumu el ile yapmakla aynı miktarda zaman alacağı belirlendi. Ancak, pozitif riski fark ederseniz, kurulumları planlanandan daha erken bitirirsiniz.

Kabul Edilebilir Risk Miktarı / Artakalan Risk

Riskin kabul edilebilir miktarı aktivitelerin ve önlemlerin nasıl tanımlanacağını belirler. Bu miktar için üst sınır, kurumun karşılayabileceği en yüksek risk etkisi maliyeti değeridir. Alt sınır, artakalan risk ile başa çıkmak için gereken önlemlerin artan maliyetini gösterir. **Şekil 8-4**, risk yönetiminin temel hedefinin kabul edilebilir bölge içinde kalabilmek olduğunu göstermektedir.

Şekil 8-4'teki üst çizelge, bir kurumun belirli bir riske maruz kalma miktarını belirtmektedir. Bu durumda mevcut önlemler, riski maksimum kabul edilebilir artakalan risk seviyesinden kabul edilebilir sınıra indirgeyemezler. Alt çizelge, maksimum artakalan risk seviyesini kabul edilebilir sınıra indirgeyecek önerilen önlemleri göstermektedir.

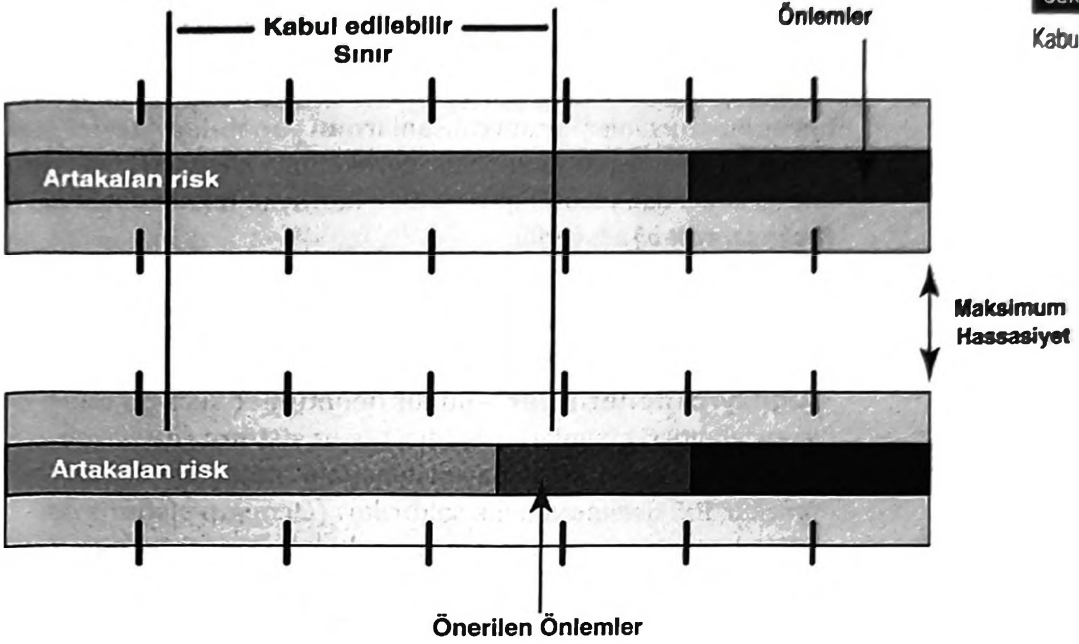
Toplam risk (*total risk*), tüm işletme varlıklarının birleşik risk değeridir. **Artakalan risk (*residual risk*)** ise önlemler ve denetimler yürürlüğe girdikten sonra geride kalan risk değeridir:

Risk – Azaltıcı kontroller = Artakalan Risk

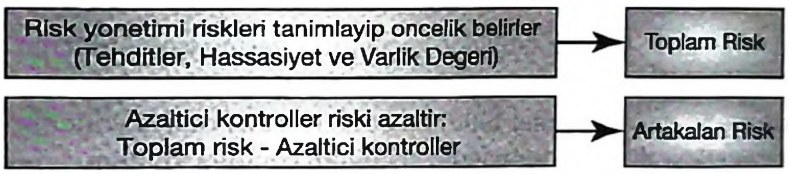
Önlemleri ve denetimleri uygulamak riski azaltsa da tamamen ortadan kaldırmaz. Bir taşıt sigorta örneğinde olduğu gibi yeni bir taşıt satın aldığınızda, galeriden çıkar çıkmaz taşıtın değeri sürüldükçe azalmaya başlar, çünkü artık kullanılmaya başlanmıştır. Eğer bir kaza sonucu taşıt hurda olursa, sigorta şirketi taşıtın satın alındığı fiyatın tamamını ödemeyebilir. Taşıt için ödediğiniz fiyat ile sigorta şirketinin ödeyeceği zarar karşılığı miktar arasındaki fark artakalan risktir. Benzer diğer örnekler sigorta indirimi ya da yangın alarmı, yangın söndürücü sistem kurulumu ve eğitim oturumlarının ardından kalan (ve azalan) yangın riskidir. Toplam risk ile artakalan risk arasındaki fark **ŞEKİL 8-5**'te görülmektedir.

NOT

Riski tamamen yok etmek mümkün değildir. Kurumlar, kabul edebilecekleri risk sınırını belirlemek durumundadırlar. Bu kabul edilebilir sınırdır.



SEKİL 8-4
Kabul edilebilir risk sınırı



SEKİL 8-5
Toplam risk ve artakalan risk

Artakalan risk kabul edilebilir bir düzeye ayarlanmalıdır.

Kurum, artakalan risk maliyetini kabul etmeye hazırlıklı olmalıdır. Bazı durumlarda riski tamamıyla yok etmek mümkün olmadığı ya da çok maliyetli oldugu icin soz konusu olmayabilir. Eğer bu maliyet çok yüksekse çözüm ya riskli davranıştan vazgçcmek, ya da farklı bir karşı tedbir kullanmaktır.

Risk Yanıt Planının Uygulanması

Güvenlik kontrolleri kurumun riskten kaçınmak, riske karşı tepki göstermek, ya da kayıpları ve sistemin faaliyet dışı kaldığı zamanları en aza indirgemeye yönelik faaliyetleri kapsar. İç Denetçiler Enstitüsü (*Institute of Internal Auditors*) tarafından tanımlandığı üzere:

> Denetim ortamı, bir kurumun risk yönetimi karşısında alacağı tavrı belirleyerek çalışanlarının denetim farkındalığını etkiler. Bu ortam disiplin ve yapılanma sağlayarak kurum içi içsel denetim bileşenlerinin temelini oluşturur. Denetim ortamı faktörleri bütünlüğü, ahlaki değerleri, kurum çalışanlarının becerilerini, yönetim felsefesini ve isleyiş tarzını, yönetimin çalışanları arasındaki yetki belirleme ve çalışanları örgütleme ve geliştirme yöntemlerini içerir.

NOT

NIST, NIST SP 800-53a'da üç denetim kategorisi önermektedir. Bu üç NIST denetim kategorileri:

- **Yönetim denetimleri.** Bu denetimler risk sürecinin tamamını yönetmek üzere kullanılır. Güvenlik denetimlerinin gözden geçirilmesi ve genel güvenlik planının geliştirilip sürdürülmesi yönetim denetimlerine örnektir.
- **İşlevsel denetimler.** Bu denetimler işlevsel personelin uygulayıp yönetebileceği fiziksel güvenlik ve acil muüdahale gibi denetimlerdir.
- **Teknik denetimler.** Bu denetimler kimlik tanıma sistemleri ya da denetim geçmişleri için günlük dosyaları gibi bilgisayar program çıktılarından oluşur.

Bazı denetimler, güvenliğin faaliyet aşamasını - insanların neler yaptıklarını - yönetir. Bu tür denetimlere **yönetimsel denetimler (*administrative controls*)** adı verilir. Yönetimsel denetimler, kurum işletiminin politika ve yönetmeliklere uygunluğunu sağlamaya çalışırlar. Bu denetimler kurum çalışanlarının yapabileceklerini, yapması gerekenleri ya da yapmaması gerekenleri kapsar. Bilgisayar sistemi tarafından yürütülüp yönetilen kontrole **teknik denetim (*technical control*)** adı verilir.

Faaliyet aşaması denetimleri yönetimsel veya teknik olabilir. Bu denetimler güvenlik programının yaşam döngüsü ile aşağıdaki şekilde ilişkilendirilirler:

- **Algılayıcı denetimler**—Bu tür denetimler sistemi etkileyen tehditleri tanımlarlar. Saldırı tespit sistemi (*intrusion detection system* - IDS) **algılayıcı denetime (*detective control*)** bir örnektir. IDS sisteme yönelik saldırıları (Örneğin sisteme dair bilgi edinmeye çalışan port tarama saldırıları gibi) tespit eder. Daha sonra, IDS bu aktiviteleri günlükler.
- **Önleyici denetimler**—Bu tür denetimler tehditlerin sistem hasssasiyeti ile buluşmasını önlemeye yöneliktir. **Önleyici denetime (*preventive control*)** ilişkin bir örnek saldırı önleme sistemleri (*intrusion prevention system* - IPS)dir. IPS, bir saldırıyı bloke etmek için ayarlanan bir IDS'dir. IPS basitçe aktiviteyi kaydetmek yerine yapılandırma ayarlarını değiştirerek kötücül aktiviteyi önler.
- **Düzeltici denetimler**—Bu tür denetimler tehdidin etkilerini azaltmaya yöneliktir. Örneğin kötücül yazılım (*malware*) etkisi altındaki bir işletim sistemini yeniden yüklemek bir **düzeltici denetim (*corrective control*)** uygulamasıdır. Adli bilişim ve beklenmedik bir olaya tepki verme de düzeltici kontrollerin diğer yaygın örnekleridir.
- **Caydırıcı denetimler**—Bu tür denetimler bir ihlale yol açabilecek faaliyetleri caydırmaya yöneliktir. Caydırıcı denetimler ile önleyici kontroller arasında ince bir fark vardır. Caydırıcı denetimlerde şüphelinin bir etkinlikte bulunmayacağı varsayılır, önleyici denetimlerde ise etkinliğin olmasına izin verilmez. Caydırıcı denetimler işini bilen bir kullanıcı risk içeren bir aktivite gercekleştireceği zaman faydalıdır. Caydırıcı denetim bir uyarının ardından aktivitenin gerçekleştirilmesine izin verirken önleyici denetim buna izin vermez. Özetle, önleyici ve caydırıcı denetimlerden hangisinin seçileceğine karar verilmesi, sağlanacak fayda ve güvenlik arasında sağlanacak denge ile ilişkilidir.
- **Telafi edici denetimler**—Bu tür denetimler gerçekleştirilmesi zor ya da çok pahalı olan tercih edilen bir denetim yerine bir tehdidi ele almak için tasarlanmışlardır.

Önlemlerin Seçimi: Bu bölümde daha önce bahsedildiği üzere *denetim (control), korunma (safeguard)* ve önlemler (countermeasure) birbiri yerine kullanılabilen terimler değildir. *Denetim* bir davranışı kısıtlar. *Korunma* ve önlemler bir etkinliğin yönetimini ya da kısıtını belirleyen denetimlerdir. Örneğin, değerli eşyaların saklanması için kullanılan bir kasa denetimdir. Kasayı koruyan bekçi bir koruyucudur. Değerli eşyaların çalınmasına karşı yapılan sigorta bir önlemdir. Önlem, belirli bir ayrıcalıklı olaydan kaynaklanacak kayıpları ele almaktadır.

Fiziksel Güvenliğin Korunması

Kurum için özel bir risk sınıfı da fiziksel güvenliktir. Aslında iyi bir fiziksel güvenlik, sağlam bir güvenlik planı için gereklidir. Pek çok bilgi işlem güvenlik personeli fiziksel güvenliği göz ardı ederek tamamen teknik güvenlik denetimleri üzerine yoğunlaşmaktadır. Risk yönetim programı dahilinde her zaman en iyi güvenlik denetimleri ele alınmalı, tüm kritik bilgi işlem varlıklarının her zaman fiziksel güvenliğinin sağlandığından emin olunmalıdır. Aşağıda güvenli bir bilgi işlem ortamını yürütebilmek için gereken en yaygın çevresel ve fiziksel denetimlerin kısmi listesi verilmektedir:

- **Isıtma, havalandırma ve iklimlendirme (*Heating, ventilating, and air conditioning* - HVAC)** —Bu sistemler bilgi işlem parçalarının gerektiği şekilde işleyebilmesi için gereken hava akımı, ısıtma ve nem bileşenlerini sağlarlar. Her ne kadar çok basit görünse de, bilgi işlem sistemini desteklemek üzere bu sistemler iyi tasarlanmalı ve etkin bir biçimde çalışmalıdır. Veri merkezi tasarımı sıcak koridor (bilgi islem parcasının ısınan havasını almak üzere) ve soğuk koridor (bilgi işlem parçalarına soğuk hava akımını sağlamak üzere) bileşenlerini içermelidir. Bunun yanında ISH sistemleri en az seviyede enerji kullanarak masrafları minimum düzeyde tutan ve gereken tüm servisleri sağlayacak şekilde tasarlanmalıdırlar. Tüm çevresel kontroller monitör edilerek sistemin gerektiği şekilde çalışıp istenen sıcaklık ve nem seviyesini koruduğundan emin olunmalıdır.
- **Yangın tedbirleri** —Bu kontroller farklı türdeki yangınların söndürülüp yayılmasının önlenmesi için gereken yangın söndürme cihazlarından oluşur.
- **Elektromanyetik enterferans/parazit (EMI) kalkanı** —Bu kontroller kablolama sistemi veya bina malzemelerinin etrafına döşenen elektromanyetik sızıntıyı önleyici araçları kapsar.
- **Işıklandırma**—Tüm gerekli alanların ışıklandırılması faaliyetlerini kapsar.
- **Sinyalizasyon** —Uygun sinyalizasyon ile hangi bölgelerin erişilebilir, hangilerinin yasak olduğu belirlenmelidir.
- **Çit** —Fiziksel bariyerler döşeyerek bilerek veya bilmeden yapılan fiziksel saldırılar önlenmeye çalışılmalıdır.
- **Barikatlar** —Fiziksel setler saldırganları caydırmaya ve taşıt girişini engellemeye yönelik kontrollerdir.
- **Korumalar** —Fiziksel bir varlık, saldırıyı engelleyebilir ve insanlar değişen koşullara hızlı bir şekilde tepki verebilir.
- **Hareket detektörleri** —Önceden tanımlanmış küçük bir alanda bir hareket tespit ettiğinde uyarı yapan araçlardır.
- **Kamera sistemi** —Bir kurumun pek çok bölgesini merkezi bir noktadan gözleyip daha sonra incelemek üzere kaydeden sistemlerdir.
- **Kilitle**—İzinsiz personelin fiziksel erişimini engelleyen araçlardır. Kapı veya kablo kilidi, kasa ya da kilitli kabinetler şeklinde olabilirler.
- **Tuzaklar** —Arasında bir boşluk olan iki grup odadan ibaret denetim sistemleridir. Herhangi bir kişinin hedef odaya ulasması için önce ilk grup odayı geçip bu grubun kapısını kilitlemesi, ardından ikinci grup odanın kilidini açması gerekir. Tuzaklar güvenli bir alana ulaşmak için uygun bir fiziksel erişim denetimi sağlar.

- **Erişim listeleri** — Bu denetimler belirli bir fiziksel kaynağa erişim hakkı olan personelin listesini içerir.
- **Yakınlık okuyucusu** —Gerekli cihazı ya da akıllı kartı taşıyan kullanıcıların bilgilerini okuyarak güvenli bölgelerdeki kaynaklara erişim sağlayan okuyuculardır.
- **Biyometrik** —Bazı fiziksel karakteristiklere ya da aktiviteye göre erişim denetimi sağlayan denetim turudur.
- **Korumalı erişim (kablolama)** —Erişimi bağlayıcı kablolamaya indirgeyerek güvenli bilgi işlem bileşenlerine kısıtlı erişim sağlayan denetimlerdir.
- **Alarm** —Bir denetim tarafından yaratılan ve listelenen olaylardan herhangi biriyle karşılaşıldığında tetiklenen sinyallerden oluşan sistemlerdir.

Çevresel ve fiziksel denetimler sadece güvenlikle ilgili değildir. Bu denetimlerden pek çoğunun rol aldığı en önemli faaliyetlerden biri personel güvenliğidir. Yukarıda listelenen denetimlerden her biri personel için güvenli bir ortamın oluşturulmasına yardım eder. Buna ek olarak güçlü bir personel güvenlik planı aşağıdaki bileşenleri içermelidir:

- **Kaçış planı** —Bu temel personel güvenlik planı, tehlike bölgesinden nasıl uzaklaşılıp nereye gidileceğini belirtir.
- **Kaçış rotası** —Kaçış planına ek olarak personel bir tehlike anında kaçış için kullanılacak en uygun yolu bilmelidir. En ideali, kaçış rotalarının önceden belirlenen bir noktada buluşmasını sağlayarak yönetimin kayıp personel olup olmadığını belirlemesini sağlamaktır.
- **Alıştırma** —Personel güvenlik planının her bir maddesinin üstünden geçildiği alıştırmalar gerçek bir tehdit anında nasıl davranılacağını belirlemek açısından çok önemlidir.
- **Denetim testi** —Her ne türde olursa olsun tüm denetimler periyodik olarak test edilerek her birinin tasarlandığı gibi çalıştığından emin olunmalıdır.

Neredeyse sınırsız sayıda olası önlem bulunmaktadır. Bir önlemin açık bir biçimde tanımlanmış bir hedefi olmalı, bir risk ile ilişkilendirilip bir güvenlik açığını azaltmaya yönelik olmalıdır. Bir maruz kalma (risk) olmayan bir önlem (veya kontrol), bir sorun arayan bir çözümdür. Önlemlerin temel amaçlarından bazıları aşağıdakileri içermektedir:

- Bilinen işletilebilir yazılım boşluklarını gidermek
- İşlevsel süreçler ve erişim denetimleri (veri ve sistem) geliştirip uygulamaya koymak
- Şifreleme hizmeti sunmak
- Fiziksel güvenliği artırmak
- Güvenilir olmayan ağlar ile iletişimi kesmek

Kurum içinde çalışan herkes kendi güvenlik sorumluluklarından haberdar olmalıdır. Kurum bünyesinde bazı kişiler için güvenlik tam zamanlı iş anlamına gelmekte iken diğerleri cok sık olmayan sorumlulukları yerine getirmekle sorumludur, çıkarken kapıyı kilitlemek gibi. Kurum içinde sorumlu olunabilecek bazı güvenlik sorumlulukları aşağıdakileri içermektedir:

- Ekstra/ziyaretçi hesaplar silme
- Sistem yöneticilerine yönelik eğitim (özel amaçlı eğitim)
- Herkese yönelik eğitim (genel eğitim)
- Virüs tarama programları yükleme
- IDS/IPS ve ağ tarama programları yükleme

Önlemlerin Fiyatlandirmasi: Önlemler ele alınırken çok sayıda faktör göz önünde bulundurulmalıdır:

- **Ürun maliyeti**— Ürun maliyeti ürünün tavan fiyatı, ekstra özelliklerinin fiyatı ve hizmet seviyesi anlaşması ya da yıllık bakım maliyeti toplamından oluşacaktır.
- **Uygulama masrafı**—Bu tür masraf, altyapıda gerçekleştirilen degişikler, ürünün geliştirilmesi, tasarım ve eğitim ile ilgili masraflarını kapsar. Yeni donanım kurulumu için tabanın güçlendirmeye yönelik masraf uygulama maliyetine bir örnektir.
- **Uygunluk masrafı**—Önlem ait olduğu ortamla birebir uyumlu olmalıdır. Örneğin Windows tabanlı bir kurum, Linux tabanlı bir önlemi yüklemeden önce eğitim ve birlikte calışabilirlik sorunlarından kaynaklanacak ek masrafları dikkatlice gözden geçirmelidir.
- **Çevresel masraflar**—Eğer bir önlem için çok miktarda enerji harcanması gerekiyorsa, kurumun elektrik sisteminin bu miktar enerjiyi sağlayıp sağlayamayacağı ve yaratılan aşırı ısınmanın giderilip giderilemeyeceği belirlenmelidir.
- **Test masrafı**—Test süreci zaman ve para gerektirse de kurum için zorunludur. Öte yandan unutulmamalıdır ki test aksamalara da yol açabilir. Bu sebeple tüm bu masraflar gözönünde bulundurulmalıdır.
- **Verimlilik etkisi**—Pek çok denetim verimliliği olumsuz yönde etkiler: Örneğin danışma masasına yapılan artan sayıda başvuru, ağırlaşan cevap süresi gibi.

> **İpucu**
> Unutmayın: Bir önlemin maliyeti, bir teknoloji parçasının alım fiyatından daha fazladır.

Riske Yanıtının İzlenmesi ve Denetimi

Bir kontrol veya önlemin yürürlüğe konulmasıyla ilgili en önemli nokta, temel hedefleri karşıladığından emin olunmasıdır. Risk yönetim sürecindeki son aşama yürürlüğe konulan önlemleri izlemek ve denetlemektir. Bir önlem hedeflenen yararı sağlamıyorsa kurum için hiçbir değeri yoktur.

Bir önlemi değerlendirirken ilk sorulması gereken "Bu önlem hangi sorunu çözmek için kullanılacak?" sorusudur. (Risk yönetim planı bu soruyu açıklıkla cevaplıyor olmalıdır.) Daha sonra, "Bu önlem gerçekten adı geçen sorunu çözebilecek mi?" sorusu ile devam edilmelidir. Bu noktada aşağıdaki maddeler dikkate alınmalıdır.

- **Önlemler kurumun yeni risklerle karşı karşıya kalmasına yol açabilir**—Örneğin, bir önlemin uygulamaya konulması, kurum içinde gerekli güvenliğin sağlandığı yanılsamasına düşülmesine neden olabilir. Ya da kritik bir sistemde önlemin kendisi yeni kırılma noktası haline gelebilir. Bu sebeple, önlemin sürekli bir biçimde izlenmesi, uyum ve tasarımının gerektiği gibi olduğundan emin olunması ve düzenli bakımının yapılması gereklidir.
- **Önlem programlarının sertifikalandırılması ve ilgili yetki onayının alınması gereklidir**—Hiçbir sistem, denetim ya da uygulama değişim denetim sürecinden geçmeden hayata geçirilmemelidir. Bu kural aynı zamanda mevcut üretim sistemlerini de kapsar.

Herhangi bir kurulum veya değişiklik gerçekleştirilmeden önce tüm denetim ve önlemler dikkatlice gözden geçirilmelidir. Çünkü, aksi halde sistem yöneticileri sistemi yanlış yapılandırabilir, ya da başka hatalar yapabilirler.

- **En iyi uygulamalar takip edilmeli ve gereken özen gösterilmelidir**—İyi bir risk yönetim programı denetleyicilere, güvenlik risklerine karşı sağduyulu ve özenli bir şekilde yaklaşıldığını gösterir. Sıklıkla yapılan değerlendirmelerle tedbirlerin planlandığı gibi işlediğinden emin olunmalıdır.

İş Süreklilik Yönetimi

Bir kuruluşun, bir aksamaya (*disruption*) tepki vermesi, onun hayatta kalmasını oldukça belirleyebilir. Kötü planlama, riski büyük ölçüde artırır. Kötü planlama ile bir kuruluş uygun şekilde yanıt veremez ve normal işlemlere geri dönemez. Aksamalar için planlama yapmak, aşağıdakilerin her ikisini de içeren iş sürekliliği yönetiminin (*business continuity management* - BCM) bir parçasıdır:

- **İş süreklilik planı (*Business continuity plan* - BCP)**—Bu plan, bir aksamadan sonra kritik iş sürecinin devam etmesini sağlamaya yöneliktir. Aksamalar küçük boyutlu (Örneğin elektrik kesintisi), ya da büyük boyutlu (Örneğin kurum binasını kullanılmaz hale getiren hava olayları) olabilir.
- **Felaketten kurtarma planı (*Disaster recovery plan* - DRP)**—Bu plan bir aksamadan sonra toparlanmak ve kurumun normal işleyisini sürdürebilmesi için gereken altyapıyı tamir etmek amacıyla gereken adımları belirler.

BCM, BCP ve DRP'nin yanında kriz yönetimi, ayrıcalıklı olay müdahale yönetimi ve risk yönetimini de kapsar.

Bir **aksama (*disruption*)**, ani gelişen ve planlanmamış bir olaydır. Kurumun kritik iş fonksiyonlarını yerine getirmesini engeller ve büyük çapta hasara ya da kayba yol açar. Büyük çaplı aksama örnekleri aşağıdakileri içermektedir:

- **Kötü hava koşulları**—2012'deki Sandy fırtınası buna bir örnektir.
- **Suç unsuru taşıyan faaliyetler**—Bu kategoride kredi kartı bilgileri ya da diğer müşteri bilgilerinin çalınması sıralanabilir.
- **Ayaklanma / terörist eylemler**—Bu kategorinin bir örneği 2014 yılında Missouri'deki halk protestoları sırasında yaşanmıştır.
- **İşlevsel**—2012'de Hindistan'da yaşanan büyük çaplı elektrik kesintisi sırasında dünya nüfusunun %9'u etkilenmiştir.
- **Uygulama hataları**—Amazon E2 bulut servisinin 2011 yılındaki arızası ve Microsoft bulut servisinin 2014'teki arızası bu kategoriye birer örnektir. Bu bulut servisleri üzerinden işi yapan firmalar, arıza giderilinceye kadar hizmetlerini başka şekillerde vermek durumunda kalmışlardır.

BCM'nin amacı, ayrıcalıklı olayların sayısını azaltmak ve islemlerin devamlılığını sağlamaktır. Tüm tedbirlere rağmen ayrıcalıklı bir olay gerçekleşirse ilk yapılması gereken, kişilerin güvenliğinin sağlanmasıdır. Bu aşamada hasarı gidermek ikincil derecede önceliklidir.

Terim bilgisi

Bir güvenlik personeli olarak aşağıdaki terimlerin tanımını bilmelisiniz:

- **İş etki analizi (*Business impact analysis* - BIA)**—Bu analiz ne tür olayların hangi sistemler üzerinde etki yaratacağı üzerinde odaklanır. BIA'nın odağı bilgi sistemleri departmanı ve altyapısı ile sınırlı kalmamalıdır; tedarik zincirine yönelik bir olayla (depo yangını, tır şöförlerinin greve gitmesi, vb.) karşılaşan bir şirket, teknoloji ile doğrudan ilgisi olmayan büyük çapta bir hasarla karşı karşıya kalabilir. Bazı senaryolar bazı departmanları, kritik bazı senaryolar ise tüm işyerini etkiler. BIA hakkında bu bölümün ilerleyen kısımlarında daha detaylı bilgi bulabilirsiniz.
- **Kritik iş fonksiyonu (*Critical business function* - CBF)**—BIA'nın beklenmedik bir olayın etkileyeceği iş alanlarını tanımlamasının ardından bu sistemler en kritik olandan en az kritik olana doğru sıralanmalıdır. Bu sıralama, kritik bir fonskiyonun yokluğu durumunda kurumun faaliyetlerine devam edip edemeyeceğini ve edebilirse ne kadar devam edebileceğini belirler.
- **Maksimum tolere edilebilen aksama süresi (*Maximum tolerable downtime* - MTD)**—MTD, bir işletmenin belirli bir kritik sistem olmadan yaşayabileceği en uzun zamandır. Büyük çaplı bir aksama, CBF'yi onun MTD değerinden daha uzun süreli faaliyet dışı bırakan beklenmedik bir olaydır. Felaket planı ve azaltma çözümlerinin her biri, kendi MTD'leri içinde CBF'leri kurtarabilmelidir. En kısa süreli MTD değerine sahip sistemler ve faaliyetler, kurum için en kritik olanlardır. Bir sonraki bölüm bu konuyu daha detaylı bir şekilde işlemektedir.
- **Kurtarma süresi hedefi (*Recovery time objective* - RTO)**—RTO, CBF'yi eski haline döndürebilmek için gereken süredir. RTO, MTD'den daha az ya da en çok MTD'ye eşit olmalıdır.
- **Kurtarma noktası hedefi (*Recovery point objective* - RPO)**—Beklenmedik olaylar veri kaybına sebep olabilirler. Her bir iş kolu için katlanılabilir veri kaybı hesaplanmalıdır. Kurtarma süreci bu aşamada belirlenen minimum değerleri karşılayabilmelidir. Eğer bir işyeri bir işgünü büyüklüğünde veri kaybını göze alıyorsa, bu iş yeri için gecelik yedekleme kabul edilebilir bir çözüm olabilir. Ancak eğer veri kaybından tamamıyla kaçınılması gerekiyorsa, yedek sistem sunucusu ve yedek bellek çözümleri gerekebilir.
- **Acil durum operasyon merkezi (*Emergency operations center* - EOC)**—EOC, felaket sırasında toparlanma ekibinin toplanıp çalışacağı yerdir. Pek çok kurum birden fazla **acil durum operasyon merkezine** sahiptir. Örneğin, bir bina yangında kullanılması için yakınınızda olabilir. Başka bir bina ise - örneğin, bir deprem veya bölgesel elektrik kesintisi durumunda kullanılmak üzere- önemli bir mesafe uzaklığında olabilir.

MTD ve RTO birlikte şu şekilde calışırlar: Bir veri merkezinde güç kaynağının kesilmiş olduğunu varsayın. Alternatif siteye (RTO) geçmek altı saat sürer. İş yeri arızalı bir veri merkezi ile dokuz saat işlevselliğini sürdürebilir. Bu durumda henüz bir felaket yerine ancak bir olaydan söz edilebilir. Eğer güc kaynağının üç saat içinde tekrar çalışması bekleniyorsa (MTD - RTO), iş yerinin bir aksama ya da felaket ilan etmesine gerek yoktur. Buna karşılık üç saat sonunda güç kaynağı halen arızalı ise, iş yeri büyük çaplı bir aksama olduğunu kabul etmeli ve ona göre davranmalıdır.

İpucu

Cihazların ne sıklıkla başarısız olabileceğini göz önüne aldığınızda, bilmeniz gereken birkaç başka terim daha vardır. Bu terimlere aşina olun:

- **Arızaya kadar geçen ortalama süre (*Mean time to failure* - MTTF)**—Bir cihazın arızalanmadan önce çalışacağı süre.
- **Arızalar arasındaki ortalama süre (*Mean time between failures* - MTBF)**—Arızalar arasındaki süre (arızaların onarıldığını varsayar).
- **Tamir için gereken ortalama süre (*Mean time to repair* - MTTR)**—Bir cihazı tamir etmek ve hizmete geri göndermek için gereken ortalama süre.

Bu örnekte üç saatlik zaman kritiktir. İş yerinin bu kritik üç saatlik süre içinde işlemlerini alternatif sahaya transfer etmediğini, bunun yerine dört saat beklediğini varsayın. Yeni sahaya transfer toplam altı saat süreceğinden, iş yeri toplam 10 saatlik hizmet kaybı yaşayacaktır. Bu rakam dokuz saatlik MTD'den fazladır. Bu değer belirlenmiş olan MTD değerini temel almakta olduğundan, bir saatlik fark çok fazla görünmeyebilir. Veri merkezi başka kurumlara da hizmet veriyor olabilir. Hizmet seviyesi anlaşmaları, daha uzun kesintiler için para cezaları olmak üzere dokuz saatten fazla kesintileri belirler. Bu ekstra saat, organizasyona on binlerce dolara (hatta daha fazlasına) neden olabilir.

Elbette ki MTD'den daha uzun süre hizmet dışı kalmaktan kaçınmanın en iyi yolu, hiç hizmet dışı kalmamaktır. BCM'nin önemli hedeflerinden biri, gerekli kontrolleri sağlayarak hizmet dışı kalmaktan kaçınmaya çalışmaktır. Bilgi Teknolojileri - BT (*Information Technology* - IT) acil durum planı hizmet dışı kalındığında bileşenlerin nasil idare edileceğine odaklanırken, yüksek derecede erişilebilirlik planı kritik bileşenlerin her zaman nasıl ayakta tutulacağını belirlemeye çalışır. Yüksek derecede erisilebilirlik planı kritik bileşenlerin tanımlanması ve bu bileşenlerin arızalanması durumunda tüm işyerinin hizmet dışı kalmasının önlenmesine çalışır. Arızalanması halinde isleyişte aksaklığa yol açabilecek her bir bileşen **tek arıza noktası (*single point of failure* - SPOF)** olarak adlandırılır. BCM'nin hedeflerinden biri, tüm kritik SPOF'lari yok etmektir. Örneğin şirketiniz tek bir internet servis saglayıcısı (*Internet service provider* - ISP) kullanıyor olsun. Eğer bu ISP ile şirketiniz arasındaki bağlantı arızalanırsa internet bağlantınız kesilecektir. Bu SPOF ile ilgili sorunu çözmenin bir yolu, birincil ISP'ınız yanında bir başka ISP'den de internet hizmeti satın almaktır. Aynı hizmeti sağlayan iki veya daha fazla bileşenin kurulumu **yedek (*redundancy*)** olarak adlandırılır, bir kuruluşun aksaklıklardan kaçınma yeteneğini artırmaya yardımcı olur (bu durum aynı zamanda **hata toleransı (*fault tolerance*)** olarak da adlandırılır.)

NOT

Kurumlar çoğu zaman fazlalık bileşenler kullanarak hata toleransı (*fault tolerance*) sağlar. Hata toleransı sağlamanın yaygın yolları aşağıda sıralanmıştır:

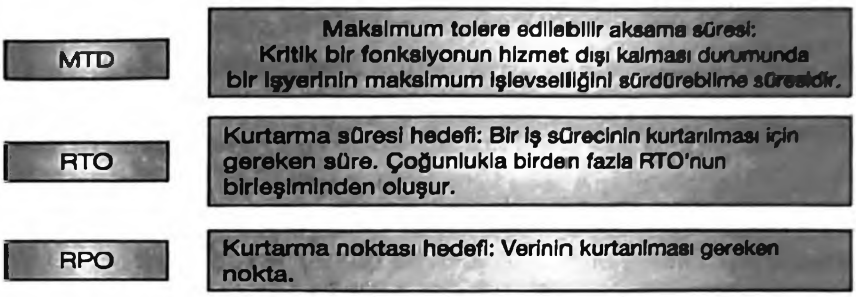
- **Ucuz Diskler Yedek Dizisi (*Redundant Array of Inexpensive Disks* - RAID)**— Bunlar, tek bir disk sürücüsü olarak görünen ancak dizideki bir disk sürücüsünün arızalanması durumunda birden çok veri kopyasını depolayan birden çok disk sürücüsüdür. RAID, farklı seviyelerde uygulanabilir.
- **Kümeleme** – İki ya da daha fazla bilgisayarı birbirine bağlayarak tek bir bilgisayar gibi davranmalarını sağlamaktır. Eğer bir kümenin bir bileşeni arizalanırsa, diğer küme(ler)deki bileşen(ler) arıza olmaksızın faaliyete devam ederler.
- **Yük dengeleme** – Hizmet isteklerine iki veya daha fazla sunucu kullanarak cevap verme işlemidir. Sunuculardan biri meşgul iken diğer sunucular isteklere cevap verir. Yük dengeleme sunucuları kümeleme bilgisayarlarında olduğu gibi birbirine bağlı değillerdir ve mesajlaşma haricinde birbiriyle iletişimde bulunmazlar.
- **Çoklu sunucular ya da araçlar** – Yük dengelemenin daha genel bir uygulaması olan bu kategoride farklı sunucular aynı isteklere cevap vermeye çalışırlar. Bir araçtaki arıza hizmetin kesilmesine yol açmaz. Yedek sunucular ya da cihazlar işlemeye devam eder.

Maksimum Tolere Edilebilir Aksama Süresinin Hesaplanması

Maksimum tolere edilebilir aksama süresini (*maximum tolerable downtime* – MTD) iş gereksinimlerine göre belirlersiniz. Bu süre çok sayıda entegre fonksiyonun RTO değerlerine bağlıdır. E-ticaret faaliyetleri için bir web sitesini barındıran bir kurumu ele alalım. Web sunucuları ağ hizmetleri, ISP kullanılabilirliği ve elektrik bileşenlerinin varlığına bağlıdır. Bu bileşenlerden her birinin kendi ayrıcalıklı olaya bağlı RTO değeri bulunacaktır fakat bu değerler MTD ile doğrudan ilgilidir.

Örnegin web sitesinin MTD değeri dört saat ise, ağ hizmetleri, ISP kullanılabilirliği ve elektrik bileşenlerinin her birinin RTO değerleri dört saatten az olmallıdır. Kurtarma sürecinin bir kısmı paralel gerçekleşse bile bir kısmı seri olarak yapılmak zorunda olabilir. Bu örnekte güç kaynağı arızası giderilmeden ağ hizmetleri arızası giderilemez. Ancak güç kaynağı onarıldığında ağ hizmetleri ve ISP kullanılabilirliği eş zamanlı olarak geri getirilebilir.

RPO ile tolere edilebilir veri kaybı ifade edilmektedir. Bu değer iş etki analizi veya hükümet emri sonucu elde edilebilir. Örneğin eczacılık ile ilgili araştırma verilerinin saklanması ile



SEKİL 8-6
Maksimum tolere edilebilir aksama süresinin hesaplanması (MTD)

ilgili kanun ve yönetmelikler gibi. **SEKİL 8-6** MTD, RTO ve RPO değerlerinin nasıl hesaplanacağını göstermektedir.

İş Etki Analizi

Bir iş etki analizi (*business impact analysis* - BIA), belirli bir olayın işletmenin işleyişi üzerinde zaman içindeki etkisini belirler. BIA kurtarma stratejisinin ve CBF'lerin belirlenmesini sağlar. Güvenlik personelinin bu aşamada sorması gereken iki soru vardır:

- İşi ne etkileyebilir?
- Bu işi nasil etkileyecek?

Başarılı bir BIA, bağlamı, kritik iş fonksiyonlarını ve güvendiği süreçleri eşleştirir. Adreslenmesi zor olan veya daha az belirgin olanlar da dahil olmak üzere tüm etkileri göz önünde bulundurmalısınız. Farklı olaylar farklı kurtarma stratejileri gerektirir. Muhasebe departmanındaki bir yangın, muhasebe işlemlerinin dış kaynak kullanımı ve geçici idare merkezlerinde temin edilmesini gerektirebilir. Bodrumdaki bir sel, bir hizmet bürosu planını aktive edebilir. Bir deprem veya kasırga yeni bir tesise kalıcı bir şekilde taşınılmasına yol açabilir.

İş etki analizi üç temel sebeple gerçekleştirilir:

- Kurumun tüm işlevselliği ile ilgili olmak üzere her bir iş ünitesi ya da kaynağının değerini belirlemek
- Bir iş kurtarma planı geliştirmek üzere kritik ihtiyaçları belirlemek
- Aksamaların ardından kurum faaliyetlerini yeniden hayata geçirmek üzere yapılacak işlerin sırasını ve önceliğini belirlemek

Etkinin Hızı

Bazı ayrıcalıklı olaylar zaman icinde daha etkin hale gelirler. Örneğin kritik bir işlem ünitesinin yavaş yavaş bozulması sonunda bir felakete yol açabilir, ya da bir bilgisayar odasına sürekli yeni donanım eklenmesi bir süre sonra elektrik kaynağını hizmet dışı bırakıp kesintiye veya yangına sebep olabilir.

Bazı sistemler yılın belli zamanları daha önemlidir: Mesela ısınma için gaz sağlayan bir firma kış aylarında daha yoğun olacaktır. Bu sebeple kış ayları boyunca en küçük bir kesinti, firmanın hizmet anlaşmalarını tehlikeye sokacaktır. Aynı firma, iş yükünün en düşük seviyede olduğu yaz ayları boyunca çok daha ciddi arızaları (daha uzun MTD) karşılayabilecektir.

Kritik Bağımlılıklar

BIA, kurumun hangi kritik işlemlerini desteklemesi gerektiğini tanımlamalıdır:

- Bilgi işleme
- Personel

- İletişim
- Araç gereç
- Hizmetler
- Diğer kurumsal faaliyetler
- Satıcılar
- Tedarikçiler

Aksama Süresinin Hesaplanması

BIA kritik veri ve sistemleri tanımlamalıdır. Sistemlerin önemi ve verilerin önemi her zaman aynı değildir. Bir sistem içerdiği verilerden daha kritik olabilir ve bunun tersi de geçerlidir. Gerçekten önemli olan, işin dayandığı sistemler ve verilerdir.

IEA sırasında gözönünde bulundurulması gereken sorunlar aşağıda sıralanmıştır:

- **Kişiler**—Ayrıcalıklı olay ve etkileri hususunda kişiler nasıl haberdar edilecek? Çalışanlar nasıl olay yerinden uzaklaştırılıp transfer edilecek ve paraları ödenecek? Eğer kritik personel çalışamaz duruma gelirse bunun yerine kim görevlendirilecek? (Bu durum **yedekleme planlaması** (***succession planning***) olarak adlandırılır.)
- **Sistemler**—Bilgi işlem ve telekomünikasyon altyapınızın hangi bölümlerini hemen kopyalamanız gerekir? Ne kadar süren bir süreniz var - bir dakika, bir saat, bir gün?
- **Veri**—İşletmeniz için hangi veriler kritiktir? Kaybedilen kritik verileri nasıl kurtaracaksınız?
- **Mülkiyet**—İşletmeniz için hangi öğeler gereklidir? Araç, sarf malzemesi ve özel formlar gibi şeylerin hepsi kurtarılabilir veya kolayca değiştirilebilir olmalıdır.

Aksama süresinin etkilerinin değerlendirilmesi BIA'da bir planlama adımıdır. Ne yapılması gerektiğini ve bu dört kategoride açıklanan hedefleri gerçekleştirmek için hangi sırada olduğunu belirlenmesine yardımcı oluyorsunuz. Bunun nasıl yapılacağını anlamak BCM'nin temel görevidir.

Plan Değerlendirmesi

Sistemler ve uygulamalar için BCP'yi ve envanter ve yapılandırma listelerini güncellemeli ve düzenli olarak korumalısınız. Bazı firmalar bunu yıllık olarak yapıyor. Diğerleri farklı dönemleri seçer. Planlanan değerlendirmelere ek olarak, şirketteki tüm önemli değişiklikler bir incelemeyi tetiklemelidir. Güncel bir plana sahip olmanın açık faydasının yanı sıra, test ve planlama iyileştirmeleri yeni çalışanları eğitmek için mükemmel yollardır. Yeni çalışanların uygulamalı bir süreçten geçirilmesi, onlara prosedürleriniz ve ortamınız hakkında daha fazla bilgi verir.

Planın Test Edilmesi

Kapsamlı bir test yapmadan BCP veya DRP'yi kabul etmemelisiniz. Bu, planın çalışmasını ve CBF, MTD, RPO ve RTO hedeflerini karşılamanızı sağlamanıza yardımcı olur. Testin her aşaması, hem sınama gerçekleştirmek hem de gerçek bir felaketle başa çıkmak için gereken güvenlik ve teknik kaynakların devam eden ihtiyacını dikkate almalıdır.

Kontrol Listesi Testi

Bir **kontrol listesi testi** (***checklist test***), yöneticilerin ve iş sürekliliği ekibinin, iletişim numaralarının güncel olduğundan ve planın şirketin önceliklerini ve yapısını yansıttığından emin olmak için planın basit bir incelemesidir. Bu tür bir kontrol masa başı kontrolüdür. Her ekip üyesi, kendi masasında otururken planın kendi kısmını kontrol eder. Kişi listelerini (*contact list*) kontrol etmenin yanı sıra, ekip üyeleri bölümlerindeki değişikliklerin planı etkileyip etkilemediğini inceler. Ayrıca, planlarını güncellemeye ihtiyaç duyup duymayacaklarını görmek için departmanlarında beklenen değişikliklere bakmaktadırlar.

Yapılandırılmış Gözden Geçirme Testi

Yapılandırılmış bir gözden geçirme testi, bir masabaşı faaliyetidir. Bu test sırasında her bir bölümü temsil eden üyeler aşağıdaki görevleri yerine getirmelidirler:

- Planın kendi paylarına düşen kısmını diğer takımlara sunmak
- Planın hedeflerini bütünlük ve doğruluk açısından gözden geçirmek
- Planın kapsamını ve yaptığı varsayımları belirlemek
- Çakışmaları ve boşlukları tespit etmek
- Kurum organizasyonunu ve raporlama/iletişim yapısını gözden geçirmek
- Test, bakım ve eğitim ihtiyaçlarını belirlemek
- Planın etkinliğini değerlendirmek üzere senaryo tabanlı alıştırmalar yapmak
- Planın gözden geçirilmesi için düzenli bir şekilde toplantılar yapmak

Son adımda, takım üyeleri belirli bir olay türü için planı yürütüyormuş gibi davranmalıdır. Yapılandırılmış gözden geçirmenin amacı, her bölümün planlarında boşluklar veya çakışmalar gibi hataları bulmaktır. Boşluklar (*gaps*), bir bölümün kritik bir görevin bir başka bölüm tarafından yerine getirileceğini varsayması halinde ortaya çıkar. Çakışmalar (*overlaps*), iki bölümün aynı kaynağın özel (veya çoğunluk) kullanımına sahip olacağını düşündükleri durumlardır; örneğin, iki bölüm, yedek masaüstü bilgisayarların üçte ikisine sahip olacaklarını düşünmektedir.

Simulasyon Testi

Simulasyon testi kağıt üzerinde bir testten çok daha fazlasıdır. Gözden geçirmeden daha fazla planlama gerektirir. Operasyonlara/prosedürlere katılan kurum personelinin tamamı bu testte aktif olarak yer alır. Test aşağıdaki maddeleri tanımlar:

- Personelin tepkisi ve yanıt zamanı
- Verimsizlikler veya daha önce tanımlanmamış güvenlik açıkları

Simülasyonu, sadece planda tanımlanan önlemleri kullanarak yerinde yürütmelisiniz. Simülasyon testi, plan geliştirmeye henüz katılmamış olan birçok çalışanı içerir. Örneğin hafta sonu gibi, şirketin kapalı olduğu bir günde simülasyon yapmak yaygındır.

Simülasyon testinin amacı eksiklikleri tanımlamaktır. Testi mümkün olduğunca yapmalısınız. Örneğin, kritik bir dosya eksikse, dosya ana siteden oluşturulmalı veya alınmalı ve test devam etmelidir. Değerlendirme için yerinde düzeltmeleri kaydettiğinizden ve daha sonrası için

güncellemeyi planladığınızdan emin olun. Test sadece tamamlandığında ya da devam etmek imkansız hale geldiğinde sona ermelidir.

Paralel Test

Çoğu kuruluş **paralel testleri** alternatif sitede yürütmektedir. Paralel bir test, işlemin ana sitede durmaması dışında, tam kesinti testi ile aynıdır (bir sonraki bölümde anlatılmıştır). Paralel testlerle ilgili olarak birkaç önemli nokta aşağıda belirtilmiştir:

- Paralel test işlevsel bir testtir. Bu sebeple İnsan Kaynakları, Halkla İlişkiler, satın alma, hizmet gibi bolumlerden temsilcileri icermez.
- Paralel test alternatif sitenin etkin hale getirilmesini gerektirdiğinden, yüksek maliyetli bir testtir. Bu sebeple üst yönetimin onayını alması gerekir.
- Test sonuclari, asıl sitedeki isleyis ile karşılaştırılmalıdır.
- Boşluk analizi, ilgilenilmesi gereken zayıflık veya düşük performans sorunlarının ortaya çıkarılmasına yardımcı olur.
- Genellikle denetçiler başarıyı izlemek ve paralel çalışma verilerinin normal operasyonel verilerine karıştırılmamasını sağlamak için her adımda yer alırlar.

Tam Kesinti Testi (Full-Interruption Test)

Bu tür testi gerçekleştirmenin en yaygın yolu alternatif sitedir. İşlerin yürütülmesini fazlasıyla kesintiye uğrattığı için az sayıda firma bu testi uygulamaya isteklidir. Test sırasında, test süresi boyunca orijinal sistemi kapatmanız gerekir. İş operasyonlarına devam etmek için yalnızca alternatif sitede mevcut olan süreçleri kullanabilirsiniz.

> **⚠ Uyarı**
>
> Bu test yüksek risk taşımaktadır! Tam kesinti testi yapmak aslında bir felaket yaratabilir. Tüm diğer test türlerini başarıyla çalıştırdıktan sonra, tam kesinti testini yürütmelisiniz. Testten önce üst düzey yönetim onayı almalısınız.

Veri ve Uygulamaların Yedeklenmesi

Kurtarma, yalnızca şirketin veri ve uygulamalarının yedeklerine erişimi olduğunda mümkündür. Planlar, yedek depolama ortamı, konum ve erişim ile ilgilenmeyi içermelidir. Teyp yedekleme, yedekleme için geleneksel tercihtir ve hala en yaygın olanıdır. Ancak, teypten veri geri getirimi cok yavaştır, ve coğu sistem için RTO değeri teypten veri getirme zamanından daha azdır. Bu tür siteler genellikle depolama alanı ağı (*storage area network* - SAN), veya **uzak günlük kaydı (*remote journaling*)** gibi site dışı ağ tabanlı depolama veya ağa bağlı sunucu (*network attached server* - NAS) gibi disk tabanlı çözümleri kullanır. Uzak günlük kaydında, sistem çevrimiçi işlemlerin bir kaydını bir site dışı yere yazar. Günlük, veritabanının bir kopyasını günceller. Birincil site düşerse, site dışı kopya geçerli olur.

Yedeklemeler, veri, dokümantasyon ve ekipman gibi gerekli kaynakların fazladan kopyalarını sağlar. Birincil site bozulursa bir yedekleme sitesini etkinleştirebilirsiniz. Benzer şekilde, bir yedek teybi muhtemelen farklı bir sitede yeniden kaydedebilirsiniz. Sonra süreç kaldığı yerden devam edebilir.

Yedekleme Türleri

Yedeklemeler ve geri yüklemeler yavaş işlemlerdir. İşletmeler, bunları işlemek için üç alternatife sahiptir:

- **Tam yedekleme (*Full backup*).**—Adından da anlaşıldığı üzere bu tür yedeklemede her şey yedekleme ortamı üzerine kopyalanır. Bu medya çoğu zaman teyp olsa da, CD, DVD ya da disk de olabilir.

Yedekleme (*Backup*) ve Yedek (*Redundancy*) Arasındaki Fark

Birincil kaynak başarısız olursa yedek veya hata toleransı seçenekleri, alternatif kaynaklar sağlar. Başka bir deyişle, bir sistem bir arızayla karşılaşabilir ancak bunu tolere edebilir ve çalışmaya devam edebilir. Ancak, yedeklerin yedeklemelerin yerine konamayacağını bilmeniz gerekir.

Örneğin, RAID 1 yansıtması (*mirroring*), verileri bir yerine iki diske yazar. Bir disk arızalanırsa, sistem çalışmaya devam edebilir. Veriler ikinci diskte hala mevcuttur. Ancak RAID ile korunan bir sunucunuz olduğunu varsayın. Sunucuda bir felaket hatası tüm sürücüleri yok ederse, veriler kaybolur. Yedeklemeniz yoksa, veriler sonsuza kadar silinir.

Benzer şekilde, kümelenmiş sunucular kurabilirsiniz, böylece birincil sunucu başarısız olursa bekleme sunucuları birincil sunucunun yerine geçer. Bir servis hata toleransı için bir kümeyi kullansa da, yine de yedeklemeye ihtiyacınız var.

- **Diferansiyel yedekleme (*Differential backup*).**—Bu tür yedekleme ile ağ trafiğinin en hafif olduğu gün, örneğin Pazar günü, tam bir yedekleme yaparak başlarsınız. Pazartesi'den cumartesiye, pazar gününün tam yedeklemesinden bu yana yapılan değişiklikleri günlük olarak yedeklersiniz. Hafta ilerledikçe, her gecenin yedeği (diferansiyel) biraz daha uzun sürmektedir.
- **Artan yedekleme (*Incremental backup*).** —Yine, ağ trafiği hafifken tam bir yedekle başlarsınız. Sonra, her gece, sadece o günün değişikliklerini yedeklersiniz. Hafta ilerledikçe, her gece (artan) yedekleme yaklaşık aynı miktarda süre alır.

Diferansiyel yedeklemelere göre artan hafta içi yedeklemeleri oluşturmak daha hızlıdır. Ancak bu bunun bir maliyeti vardır. Verileri geri yüklemek için yedekleme imajlarını (*backup images*) kullanmanız gerekiyorsa, diferansiyel yedeklemeleri kullanan sistemlerin yalnızca tam yedeği ve ardından en son farklılığı geri yüklemesi gerekir. Artan yedekleme kullananların, tam yedeklemeyi geri yüklemeleri ve geri yüklemeyi tamamlamak için her günün artan yedeklemelerini yüklemeleri gerekir.

Sadece verilerden başka öğeleri de yedeklemelisiniz. Bunlar arasında yönlendirici, anahtar ve diğer ağ aygıtı yapılandırmaları, kullanıcı erişim izinleri ve yapılandırmaları (ör. Active Directory) ve sunucu/iş istasyonu işletim sistemleri ve yapılandırmaları bulunur. Bunu daha yönetilebilir hale getirmek için, çoğu büyük şirket, istek üzerine yeniden yüklenebilecek, iş istasyonları için standart bir temel yapılandırmaya sahiptir. Bunları güncel tuttuğunuz sürece (yamalı ve sabit (*fixed*)), bu ilgi çekici bir çözümdür.

Ayrıcalıklı Olay Yönetimi

Bir hatırlatma olarak, bir ayrıcalıklı olay (*incident*), güvenlik politikasının gerçek veya tehdit altında bir ihlali ile sonuçlanan bir olaydır. Bir ayrıcalıklı olay meydana geldiğinde, bir kurumun cevap vermesi gerekir. Ayrıcalıklı olay yönetim süreci aşağıdaki adımları içerir:

- Hazırlık
- Tanımlama
- Bildirim

İpucu

Aksama sürelerini en aza indirmenin genellikle aksama süresinden kaçınmak olduğunu unutmayın. Çoğu zaman aksama süresinden kaçınmanın en basit yolu, tüm bilgisayarların ve cihazların en son güvenlik düzeltmeleriyle yamalandığından emin olmaktır. Yama, sistemlerinizi birçok saldırı türüne daha dayanıklı hale getirir ve yedeğe ve diğer hata tolerans tekniklerine daha az bağımlı hale getirir.

- Yanıt
- Kurtarma ve takip etme
- Belgeleme

Bu adımların her biri aşağıdaki alt bölümlerde açıklanmıştır.

Hazırlık

Bir ayrıcalıklı olay yanıt programındaki ilk adım, çeşitli ayrıcalıklı olaylara en iyi nasıl yanıt verileceğini ve **ayrıcalıklı olay yanıt ekibinin (*incident response team* - IRT)** nasıl kurulacağını planlamaktır. IRT, meydana gelen ayrıcalıklı olaylara müdahale etmek için eğitim ve dokümantasyona sahip olacaktır. IRT üyeleri birbirleriyle rahatça iletişim kurabilmeli ve her ayrıcalıklı olayı profesyonel bir şekilde ele almalıdır. Planlama aşamasının kalitesi, IRT'nin ayrıcalıklı olayları ne kadar iyi yönetebileceğini belirler.

Tanımlama

Gerçekte bir ayrıcalıklı olayı ele almanın ilk adımı, bir ayrıcalıklı olayın gerçekte gerçekleşip gerçekleşmediğini tespit etmektir. Bütün olaylar ayrıcalıklı olay değildir. Ayrıcalıklı olayın ciddi olup olmadığını veya yaygın, iyi huylu bir ayrıcalıklı olay olup olmadığını öğrenmelisiniz. Bu bir triyajdır, olaya öncelik vermektir. Bir alarmdan, bir kullanıcıdan şikayetten, bir güvenlik tedarikçisinden bir uyarıdan veya bir günlük analizinden bir ayrıcalıklı olayın ilk bildirimini alabilirsiniz. Herhangi bir ayrıcalıklı olaya tepki gösterecek prosedürlere sahip olduğunuzdan emin olun.

Bildirim

Siz veya başka bir IRT üyesi genellikle bir ayrıcalıklı olayın farkında olan ilk kişilerden biri olacağınızdan, nasıl tepki vereceğinizi bilmeniz gerekmektedir. İlk yanıtlayıcı olarak, ayrıcalıklı olayı başından düzgün bir şekilde ele almanız önemlidir. Amaç, ayrıcalıklı olayı kontrol altına almak ve eğer mümkünse durumu iyileştirmektir. Durumu daha da kötüleştirmemeye özen gösterin. Olayın yanlış bir pozitif olup olmadığını öğrenmelisiniz. Birkaç yanlış pozitifin gerçek olaylara karşı duyarsızlaşmanıza neden olmamasını sağlamaya dikkat edin. Bağımsız olarak alınan bir dizi görünüşte bireysel olay bir yanıtı haklı çıkaramayabilir. Ancak, olaylar topluca ele alındığında önemli olabilirler.

Olayların nasıl ve ne zaman ileteceğinizi ve kime bildireceğinizi bilmelisiniz. Bu, yanıt senaryolarını planladığınızda ve ayrıcalıklı olay cevap takım üyelerini eğitirken iyi sonuç verir.

Mahkemeler ve Kanıtlar: Adli Süreç

Zaman zaman, bir ayrıcalıklı olay sivil veya hatta ceza davası için gerekçe olacaktır. Bu nedenle, kanıtların kusurlu olmadığından ya da kabul edilmediğinden emin olmak için tüm araştırmaları dikkatli bir şekilde yapmalısınız. Her zaman önce kısa süreli verileri toplayın. Kısa süreli veriler, yakın gelecekte değişebilen verilerdir. Kısa sürme sırası (ve veriyi toplamanız gereken sıra):

1. RAM
2. Takas ve sayfalama dosyaları

3. Disk üzerindeki dosyalar
4. Günlükler
5. Arşivlenmiş veri

Bir ayrıcalıklı olay mahkemede sonuçlanmasa bile, mahkeme eyleminin tehdidi şirketin ihtiyaçlarını karşılamak için yeterli olabilir. Örneğin, birisini yargılamak yerine, şirket bu kişiyi istifaya zorlamayı tercih edebilir.

Ülkelerin yasaları değişebilir ancak şu kural neredeyse her yerde geçerlidir: Eğer delillere erişim engellenirse bu durum geri döndürülemez.

Tüm genel hukuku benimseyen ülkelerde (ve medeni hukuku takip eden birçok ülkede) kanıtların güvenilir olduğu gösterilmelidir. Başka bir deyişle, olaydan sonra kanıtın değiştirilmediğini kanıtlamalısınız. Bu, mümkün olduğunca erken bir sistem imajı yakalamanız ve ardından tüm analizleri imajın kopyasında yürütmeniz gerektiği anlamına gelir. Bunu yapmak, orijinal kanıtları yanlışlıkla değiştirmemenizi sağlar. Daha sonra, herhangi bir ağ trafiğini ve günlükleri, video veya diğer ortamlarla birlikte uygun zaman damgalarıyla yakalayabilirsiniz. Bir gözaltı zinciri kanıtın nasıl toplandığını ve belgelendiğini gösterir. Belge, ortaya çıkarılmasından itibaren kanıtlarla temas eden herkesi listeler. Belge, kanıtın nasıl ele alındığını, kanıta ne yapıldığını ve değişmeden nasıl korunduğunu gösterir.

Tüm kanıtların geçerli olduğunu ve toplandıklarında olduğu gibi aynı durumda olduğunu göstermek için, özetler (hash) oluşturabilir, ekran görüntülerini alabilir ve hatta olayın tanıklarını ve toplama aktivitelerini kullanabilirsiniz. Adli tıp işlemlerinde kullanılan tüm zaman ve harcamaların ayrıntılı kayıtlarını tuttuğunuzdan emin olun. Kanıt toplamak için gereken çalışmaları ölçmeniz gerekebilir. Son olarak, toplanan tüm verilere sahip olduğunuzda, toplanan verilerin hepsinden yararlı bilgiler elde etmek için analiz tekniklerini, özellikle yeni ortaya çıkan büyük veri tekniklerini kullanabilirsiniz.

Yanıt

Bir ayrıcalıklı olayı belirledikten sonra, bir sonraki aşama hasarı sınırlamaktır. Bu adımın önemli bir yönü de önlemedir. Birçok olay hızla büyür ve genişler, muhtemelen diğer sistemleri, bölümleri ve hatta iş ortaklarını etkiler. Ayrıcalıklı olay yanıt planı, gereksiz yere hizmet kesintisine yol açmadan ayrıcalıklı olayın yayılmasını durdurmak için atılması gereken adımları belirtmelidir. Örneğin, bir virüs bir sisteme bulaştığında, tehdidi önlemenin basit bir yolu sistemin ağ bağlantısını kesmektir.

Bir planın olması şarttır. Olasılıklar, bir ayrıcalıklı olayın ortasında en iyi eylem planını doğru tahmin etmede zayıftır. Unutmayın, zamandan yararlanan ve olayın önemini sonradan anlayan insanlar, ayrıcalıklı olaydan sonra yanıtınızı değerlendirecektir. Önceden onaylanmış bir yanıt planı, daha iyi ve daha etkili bir yanıta dönüşürken aynı zamanda suçu azaltmanızı sağlayacaktır.

Uygun kurtarma prosedürlerini gerçekleştirebilmeniz için ayrıcalıklı olayın kaynağını ve türünü tanımlamak önemlidir. Belirtileri ortadan kaldırmak problemi çözmeye yetmez. Yanıt verenler, hasarın kapsamını öğrenmek zorundadırlar ve eğer hasar çok şiddetli ise, felaket kurtarma planının başlatılmasını tavsiye edebilirler. Ayrıcalıklı olay yönetiminin önemli bir bileşeni gelecekteki olayları önlemektedir. Ayrıcalıklı olay sırasında toplanan günlükler ve belgeler korunmalı ve gelecekteki analizler için kullanılabilir durumda olmalıdır.

Kurtarma

Ayrıcalıklı olayı kontrol altına aldıktan ve kaynağını eledikten veya engelledikten sonra, kurtarma süresidir. Sistemi normal kullanımına getirmeden önce, ayrıcalıklı olayın tekrar etmemesi için kullanılan güvenlik açığını ele almalısınız. Zarar görmemiş uygulama ve veri yedeklemelerini kullanarak sistemleri yeniden oluşturmanız gerekebilir. Yeniden bulaşmayı önlemek için sistemden kötücül içeriği temizlemeniz gerekebilir.

Takip etme

Ayrıcalıklı olaydan ders almak, yönetimin ayrıcalıklı bir olayı gelecekte daha etkili bir şekilde önlemek veya tepki vermek için yeni prosedürler ve kontroller oluşturmasını sağlayacaktır. IRT'nin gelecekteki ayrıcalıklı olaylar için kullanabileceği değerli bilgileri yakalamak için her bir ayrıcalıklı olayın bir öğrenilen dersler değerlendirmesinin yapılması önemlidir.

Belgeleme ve Raporlama

Ayrıcalıklı olay yanıt sürecindeki her adımı belgelemenin önemini göz ardı etmeyin. Oluşturduğunuz belgeler gelecekteki ayrıcalıklı olayların kalitesi için çok değerli olabilir. Hangi eylemlerin iyi sonuç verdiğini ve hangilerinin işe yaradığını belgelemeniz durumunda, olay yanıt planınızı iyileştirebilirsiniz. Ayrıcalıklı olay yanıt belgelerini biriktirirken, değerli bir kaynak oluşturursunuz. Bu yanıtı, ayrıcalıklı olay yanıt planınızda ve normal güvenlik politikalarınızda ve yordamlarınızda değişiklik yapmak için kullanabilirsiniz. Örneğin, veri merkezindeki yetkisiz personel ile ilgili birçok olayı belgelemek, daha iyi denetimlere ihtiyaç duyulduğunu gösterebilir. Ayrıcalıklı olay yanıtını belgelemek için kazandığınız bilgileri kullanın. Bu, kuruluşunuzu daha güvenli hale getirebilir.

Felaketten Kurtarma

Felaketten kurtarma planı (*disaster recovery plan* - DRP) üç görevi yerine getirir:

- BCP/DRP'nin koordine edileceği ve uygulanacağı alternatif bir yer olarak bir acil durum operasyon merkezi (*emergency operations center* - EOC) kurar.
- Bir EOC yöneticisi belirler.
- Bu yöneticinin ayrıcalıklı bir olayı ne zaman felaket olarak bildirmesi gerektiğini belirler.

Bir DRP, kritik kararları önceden vermenizi sağlar. Böylece, gerçek bir felaketin aciliyeti olmadan kararları yönetebilir ve gözden geçirebilirsiniz. Bu planları önceden oluşturmazsanız, siz ve yöneticilerinizin büyük baskı altında iken en iyi tahmin kararlarını vermek zorunda kalacaksınız.

DRP'ler uzun vadeli, zaman alıcı ve pahalı projelerdir. Büyük bir şirketin DRP'si on milyonlarca dolara mal olabilir. Üst yönetimin sadece destek vermekle kalmayıp, etkili ve iyi test edilmiş bir DRP üzerinde ısrar etmesi önemlidir.

Süreç bir iş analizi ile başlar. Kritik fonksiyonları ve maksimum tolere edilebilir aksama sürelerini tanımlar. Ardından planı tetikleyebilecek çok çeşitli senaryolarla ilgilenmek için stratejileri tanımlar. Bir güvenlik uzmanı olarak, büyük olasılıkla felaket planlama ve felaket kurtarma ekiplerinin bir üyesi olarak ekipte yer alacaksınız.

Felaketten Kurtarma Planını Etkinleştirme

Bir güvenlik uzmanı olarak, işin gerektirdiği ağları ve sistemleri yeniden inşa ederek bir kriz durumunda iş operasyonlarını yeniden kurmada önemli bir rol oynayacaksınız. Kurtarma işlemi iki ana aşamadan oluşur. İlk aşama iş operasyonlarını geri yüklemektir. Çoğu durumda kurtarma, alternatif bir sitede olabilir. Mevcut yedek verilerden, yedek donanımlardan ve satıcılardan temin edilebilecek herhangi bir donanımdan hızlı bir şekilde ağ kurmanız gerekebilir.

İkinci aşama, operasyonları felaketten önce orijinal hallerine geri döndürmektir. Normal işlemlere dönmek için, birincil siteyi yeniden oluşturmanız gerekir. Normal siteye geri dönüş ve alternatif sitenin kapanması, BCP/DRP'nin "Ev Sitesine Dönüş" kısmının bir parçası olmalıdır.

Kurtarma ve onarım ekiplerini etkinleştirin. Ekipler, insanlar ve veriler birincil siteye dönmeden önce işlerini yapacaklar. Güvenlik profesyonelleri genellikle ağ altyapısının hasarlı kısımlarını yeniden inşa etmek için onarım ekibinde bulunurlar. Güvenlik profesyonelleri, güvenlik seviyelerini önceki güvenlik seviyelerine eşleştirecekler ya da artıracaklar. Yeni ekipmana ihtiyacınız varsa, güvenliği artırmak için bu fırsatı kullanın.

NOT

Unutmayın: Bir felaket (*disaster*), kritik iş fonksiyonunun (*critical business function* - CBF) maksimum tolere edilebilen aksama süresinden (*maximum tolerable downtime* - MTD) daha uzun bir süre çalışmasını engelleyen bir olaydır.

Azaltılmış/Değiştirilmiş Ortamda Çalışmak

Bir kriz sırasında, denetimler, destek ve süreçler gibi normal şartların çoğu mevcut olmayabilir. Yedekleme ve hataların uzlaştırılması da dahil olmak üzere, sistemlerin güvenli çalışmasını sağlamak için hızlı bir şekilde adapte olmalısınız. Bu konuda akılda tutulması gereken birkaç nokta aşağıda belirtilmektedir:

- Görevler ayrılığı veya harcama limitleri gibi normal süreçleri askıya almak isteyebilirsiniz. Bu durumu, ek kontroller veya ek denetim (*audit*) ile telafi etmelisiniz. DRP, belirli insanlara veya belirli görevlere ek ayrıcalıklar veya harcama yetkisi vermelidir.
- Bazı sistemler çökerse, kullanıcılar alternatif sistemlerin veya erişimin nasıl kullanılacağı konusunda daha fazla teknik desteğe veya kılavuza ihtiyaç duyabilirler. BIA'lar, kurtarma ihtiyaçlarının bir parçası olarak minimum kurtarma kaynaklarını belirlemiş olmalıdır.
- Bir felaket ve kurtarma sırasında, farklı donanım platformlarındaki servislerin ortak sunucular üzerinde birleştirilmesi iyi olabilir. Bu kurtarmayı hızlandırabilir. Ancak, taşınmanın ve kurtarmanın sorunsuz geçtiğinden emin olmak için bu işlemi dikkatli bir şekilde yönetmelisiniz.
- Alternatif sitede çalışırken, veri ve sistemlerin yedeklerini almaya devam etmelisiniz. Bu, kurtarma sitesi başarısız olursa yeni felaketleri önleyebilir.

NOT

DRP'ler sigorta oranlarını düşürebilir ve bir DRP'nin hazırlanması risk yönetimi çabalarına yardımcı olabilir.

Felaketten Kurtarmanın Temel Adımları

Felaket kurtarma için temel adımlar (önem sırasına göre):

1. Bireylerin güvenliğini sağlayın.
2. Hasarı kontrol altına alın.
3. Hasarı değerlendirin ve kurtarma işlemlerini DCP ve BCP'ye göre başlatın

Hasarlı Sistemlerin Geri Yüklenmesi

Hasarlı sistemleri yeniden inşa etmeyi planlamanız gerekir. Yapılandırma çizelgelerini, envanter listelerini ve yedekleme uygulamalarını ve verilerini nereden alacağınızı bilmeniz gerekir. Sistemin yalnızca geçerli kullanıcılara izin verdiğinden emin olmak için erişim kontrol listeleriniz olmalıdır. Aşağıdaki noktaları aklınızda bulundurun:

- Yeniden yapılandırma başladığında, yönetici, işletim sistemlerini ve uygulamaları en güncel yamalarla güncellediğinden emin olmalıdır. Yedekler veya kurulum diskleri genellikle geçerli olmayan eski sürümleri içerir.
- Sistemi yeniden kurduktan sonra, verileri RPO'ya geri yüklemeniz gerekir. Bu, uzlaştırıcı (*reconciling*) kitaplar ve kayıtları içerir. İşletim sistemlerinin ve uygulamaların güncel ve güvenli olduğundan emin olmalısınız.

Bazı kuruluşlar kurtarma planlarında erişim denetim izinlerine bakmaktadır. Kullanıcıların yeni sistemlere girmelerine izin vermek için erişim denetimi kurallarını, dizinleri ve uzaktan erişim sistemlerini etkinleştirmeniz gerekir. Planı yaparken, herhangi bir satıcı yazılımının alternatif işlemcilerde çalıştığından emin olun. Bazı satıcılar ürünlerini yalnızca belirli bir CPU üzerinde çalışacak şekilde lisanslar.

Felaketten Kurtarma Sorunları

Burada bir DRP'nin bakım ve uygulamasında sıklıkla göz ardı edilen felaket kurtarma sorunlarının kısa bir listesi bulunmaktadır:

- **Jenaratörler**—Tüm yakıtın taze olduğundan emin olun ve bir krizde yakıt tedariki için sözleşmelerin guncel olduğunu garantileyin. Jeneratörler, rutin bakım almalı ve çalıştırılmaya hazır olduklarından ve beklenen sistem yükünü taşıyabileceklerinden emin olmak için periyodik olarak çalıştırılmalıdır.
- **Hasarlı sitenin güvenliği**—Birincil (hasarlı) siteyi daha fazla hasar veya yağmalardan korumalısınız.
- **Yeniden Giriş**—Hasar görmüş siteyi, kalifiye eleman ile kontrol edilerek insanların bu siteye yeniden girmesinin guvenli olup olmadığı belirlenmelidir.
- **Donanımın ve yedek parçaların taşınması**—Plan, insanların, donanımların ve yedek verilerin alternatif siteye güvenli bir şekilde taşınmasını sağlamalıdır.
- **İletişim ve ağlar**—Düzenli telefon hizmeti genellikle krizde başarısız olur. Özellikle, kilit ekip üyeleri arasında alternatif bir iletişim yöntemine ihtiyacınız olabilir.

Kurtarma Alternatifleri

Bir iş sürekliliği koordinatörü, her bir alternatifin kritik iş işlevlerini, RTO'yla karşılaştırıldığında operasyonel hazırlığını ve ilgili maliyeti destekleme yeteneğini dikkate alır. Koordinatör, çalışma alanı, güvenlik gereksinimleri, BT ve telekomünikasyon için tanımlamaları inceler.

Bir işletme (veya işletmenin bir kısmı) kurtarma için taşınması gerektiğinde genellikle üç seçenek dikkate alınır:

- İşletme tarafından işletilen, örneğin ikincil bir işlem merkezi gibi, özel bir site
- Sıcak site veya mobil hizmet noktası gibi ticari olarak kiralanan bir tesis
- Bir iç veya dış tesisle anlaşma

Dış ticaret sağlayıcıları birçok kuruluşa hizmet sunmaktadır. Bu, bir felaket olduğunda, bir ticari sağlayıcının birçok müşterisinin etkilenebileceği anlamına gelir. Bu olursa, hangi önceliğe sahip olacaksınız? Test süresi, bildirim, ücretler ve minimum/maksimum kurtarma günleri gibi şeyler için seçeneklerinizi (fiyatlar ile birlikte) öğrenin. Çalışma alanı, güvenlik gereksinimleri, BT ve telekomünikasyon özelliklerinin kritik iş işlevlerinize uygun olduğundan emin olun. Dinlenme ve duş olanakları ile ikram hizmetleri de dahil olmak üzere personel için uygun konaklama imkanlarının mevcut olduğundan emin olun.

İşletmenizin tercih ettiği seçenek ne olursa olsun, BT departmanının görevi, gerekli tüm ekipmanın alternatif sitede mevcut olduğundan emin olmaktır. Bu, kurtarma dosyalarında tanımlanan kritik dosyaları, belgeleri ve diğer öğeleri içerir. Diğer öğeler arasında ek yama kabloları, USB sürücüler veya BT personelinin günlük olarak kullanabileceği diğer ortak öğeler yer alabilir.

Geçici veya Alternatif İşlem Stratejileri

İşlemlerin nerede sürdürüleceği konusunda ne karar verilirse verilsin, BT altyapınızı destekleyebilmek üzere bir yere ihtiyacınız olacaktır. Maliyete ve operasyonel hale gelme süresine bağlı olarak çeşitli seçenekler mevcuttur. En yaygın kurtarma konumu seçenekleri şunlardır:

- Alternatif bir işlem merkezi veya yansıtılmış (*mirrored*) site her zaman hazır ve kuruluşun kontrolündedir. Tamamen yedekli veya çift işlemleri ve senkronize edilmiş verileri gerektirdiği için en pahalı seçenektir. Organizasyon sürekli olarak çalışır. Ek masrafları, kurtarma planlaması dışındaki iş ihtiyaçları (çift destek personeli bulundurma gibi) tarafından haklı gösterilebilir. Ancak, maliyet dağıtımları yapmak karmaşıktır.
- Sıcak bir site, işlemleri hızlı bir şekilde üzerine alan bir sitedir. Verileri yenilemeniz veya güncellemeniz gerekebileceği halde, önceden konumlandırılan tüm ekipman ve veriler vardır. İki tür sıcak site vardır. Bir tanesi şirkete ait ve adanmış. Diğeri ise ticari bir sıcak sitedir. Sıcak sitenin avantajı, hızlı bir şekilde kurtarma sağlayarak hızlı bir şekilde alternatif bilgi işlem olanakları sunabilmesidir. Dahili olarak sahip olunan bir sıcak site, diğer alternatiflerden daha pahalı olacaktır, ancak bölgesel felaket sırasında kimse bununla rekabet edemez.
- Ilık bir sitenin bazı ortak bilgi teknolojileri, iletişimleri, gücü ve HVAC'ı vardır, ancak sunucular ve iletişim gibi IT ekipmanlarını satın almanız ve teslim etmeniz gerekecektir. Verileri de almak ve yüklemek zorunda kalacaksınız. Birçok kuruluş, ılık sitelere sahiptir ve çoğu zaman bu siteyi kurum dışı veri deposu olarak kullanırlar.
- Soğuk bir site, HVAC ve güç ile boş bir veri merkezidir. En ucuz seçenektir. Faaliyete geçmek için çok zaman gerekir çünkü tüm ekipmanı ve iletişim malzemelerini satın almanız, teslim etmeniz ve yapılandırmanız gerekir. Bazı kuruluşlar, kurtarmaya sıcak bir sitede başlarlar ve kesinti uzun süre devam ederse, ılık bir siteye veya soğuk siteye transfer olurlar.

TABLO 8-2 Yaygın kurtarma sitesi seceneklerinin karsilastirilmasi.

Özellik	Sıcak Site	Ilık Site	Soğuk Site	Çoklu Siteler
Maliyet	Yüksek	Orta	Düşük	Doğrudan maliyeti yok
Bilgisayar donanımı	Evet	Evet	Hayır	Evet
Bağlantı donanımı	Evet	Evet	Hayır	Evet
Veri donanımı	Evet	Hayır	Hayır	Evet
Çalışanların varlığı	Evet	Hayır	Hayır	Evet
Hazır olana kadar gereken zaman	Dakikalar veya saatler	Saatler veya günler	Günler veya haftalar	Saniyeler veya dakikalar

TABLO 8-2 En yaygın kurtarma site seçenekleri karşılaştırılmaktadır.

Anlaşmaların İşlenmesi

Kurtarma sorunlarını çözmenin bir yolu, benzer BT yapılandırmalarına ve yedekleme teknolojilerine sahip kuruluşları bulmaktır. Bu başka bir şirket, bir koşullu taşıyıcı veya bir hizmet bürosu olabilir. Daha sonra şirketiniz bir felaketle karşılaştığında destek sağlamak için diğer kuruluşla bir anlaşma imzalarsınız. BT, güvenlik ve yasal departmanları taslak anlaşmalarını dikkatlice gözden geçirmelidir.

Çift Taraflı ya da Karşılıklı Yardım

Şirketiniz, benzer teknolojiye sahip bir şirket ile **karşılıklı yardım (*mutual aid*)** veya bir **konsorsiyum anlaşması (*consortium agreement*)** olarak bilinen karşılıklı bir anlaşmaya girebilir. Bir konsorsiyum anlaşmasında, birkaç şirket birbirini desteklemeyi kabul eder. Bu yaklaşımı dikkatlice değerlendirmelisiniz. Örneğin, her kuruluş bir başkasını desteklerken birincil işine devam edebilir mi? Ekipman ve altyapı her iki kuruluşu da destekleyebilir mi? Tüm sistemlerin ekstra yükü taşıyabildiğini ve uyumlu olduklarını onaylamak için testler yapmalısınız. Ayrıca, verilerin hassaslığını ve buna uygun olan tüm düzenlemeleri de göz önünde bulundurmalısınız. Ortakların yöneticileri veya kullanıcıları buna erişebilir. Her iki taraf da sistemlerini uyumsuz yapabilecek teknolojiyi iyileştirme veya eskiyen teknolojiyi terk etme faaliyetlerinden birbirini haberdar etmelidir.

Çift Taraflı Merkezler

Çift taraflı merkezler (*reciprocal centers*) genellikle aynı tür işleri yapan ancak doğrudan rakip olmayan işletmeleri içerir. Bunlar arasında şehirler arası hastaneler veya ciltli kitap üreten firmaların biraraya gelmesi sayılabilir. Aşinalık ve ortaklığın avantajları vardır. Sektörde ihtiyaç duyulan özel kodları, endüstri jargonunu ve özel formları paylaşabilirler. Örneğin, hastaneler "DRG kodu" terimini kullanırlar. Bu kod, ortak bir veritabanında tanı, prosedür veya hastalığa karşılık gelen bir sayıyı ifade eder.

Beklenmedik Olay

Bir kuruluş, birincil tedarik yöntemi başarısız olursa, beklenmedik olay taşıyıcıları veya beklenmedik olay tedarikçileri için sözleşme yapabilir. Bakım ücretlerini ve aktivasyon süresini dikkate almanız gerekir. Ayrıca, taşıyıcıların (*carriers*), özellikle de iletişim taşıyıcılarının (*communication*

carriers) aynı kabloyu veya yönlendirme yollarını paylaşıp paylaşmadığını kontrol etmeniz gerekir. Onlara sormak tedbirli olmaktır.

Hizmet Bürosu

Bir **hizmet bürosu** (***service bureau***), ekstra kapasiteye sahip bir servis sağlayıcıdır. Gelen çağrıları işleyen bir çağrı merkezi buna bir örnektir. Kuruluşunuz, acil kullanımı için çağrı merkezi ile sözleşme yapabilir. Bu, karşılıklı anlaşma düzenlemesine sahip olanlar ile aynı endişeleri dile getirebilir. Satıcı, işini geliştirebilir ve ekstra kapasitesini tüketebilir veya satıcı, donanımını veya yapılandırmalarını değiştirebilir.

Bulut Kullanımı

Bulut bilişim son yıllarda çok popüler hale geldi. Daha fazla kuruluşun, BT ortamlarının en azından bazılarına buluta dahil etmesi bekleniyor. Bulut bilişim sanallaştırmaya dayalı olduğundan, tüm sunucu imajlarını bir yerden diğerine kopyalamak kolaydır. Bu teknik, felaket kurtarma sitelerini çok daha uygun maliyetli hale getirmektedir. Neredeyse herhangi bir kuruluş, fiziksel bir sitenin maliyetinin çok altında bir maliyet ile bulut tabanlı bir felaket kurtarma sitesini yönetebilir.

Bu bölümde öğrendiğiniz tüm seçenekler bulutta mevcuttur. Bulut tabanlı felaket kurtarma siteleri, soğuk, ılık veya sıcak siteler olarak var olabilir. Daha da pahalı olan bir seçenek, kritik dosyaları yalnızca bulut tabanlı depolamaya yedeklemektir. Tabii ki, birincil site başarısız olursa kurtarmak için gereken zamanı düşünmelisiniz.

Genel sanallaştırma bellek kopyası (*snapshot*) özelliği olağanüstü durum kurtarma için kullanışlıdır. Uygulanan tüm yamaları içeren bir sanal makine (*virtual machine* - VM) imajı oluşturabilirsiniz. İstenen VM'nin bir bellek kopyası, bir kurtarma imajı için mükemmel bir başlangıç noktasıdır. Sanallaştırma, birincil veri merkezinizi geri yükleyene kadar işlemlerinizi desteklemek için gerektiği kadar sanal alternatif sitelerin başlatılmasını mümkün kılar. Bulut bilişim, alternatif ortamların kurulum ve bakım maliyetlerini düşürerek daha fazla kurtarma seçeneği sunar. IT ortamınızdaki herhangi bir değişikliği düşündüğünüzde yapmanız gerektiği gibi, bulutu kullanmanın güvenliği nasıl etkilediğini değerlendirin. Sanallaştırmayı kullanırken bile tüm güvenlik denetimlerini test etmeniz gerekir ancak bu yeni teknoloji kesintilere veya ayrıcalıklı olaylara yanıt vermek için birçok yarar sağlar. Felaket kurtarma için sanallaştırmayı kullanmak zorunda değilsiniz. İşlemleri etkilememesi gereken testleri yapmanız gerekiyorsa, VM imajlarını ayrılmış (*isolated*) sunucular veya **kum havuzu** (***sandbox***) olarak döndürebilirsiniz. Seçenekler çoktur. Ancak, her zaman olduğu gibi, verilerinizi nerede sakladığınızı veya işlemlerinizi gerçekleştirdiğinizden bağımsız olarak, güvenlik politikanızı karşıladığınızdan veya daha fazlasını yaptığınızdan emin olmalısınız.

BÖLÜM ÖZETİ

Bu bölümde, üç temel bilgi güvenliği ilkesini öğrendiniz:

- Kurumun karşı karşıya olduğu risklerin tanımlanması.
- Denetimleri kullanarak hasarı mümkün olduğunca engelleme.
- Önlenemeyen ayrıcalıklı olaylara tepki verebilmek için plan ve prosedürlerin hazır olması. Bu hazırlığa dair temel ilkeler ve denetimlerin kişiler, süreçler, teknoloji ve

veri bağlamında ifade edilmesi.

Bu bölümde risk yönetiminin nedenlerini ve süreçlerini öğrendiniz. Bir iş sürekliliği planının (*business continuity plan* - BCP), bir aksamanın kuruluşunuzu hizmet dışı bırakmadığından emin olmanıza nasıl yardımcı olduğunu öğrendiniz. Nicel risk değerlendirmesi ve nitel risk değerlendirmesi arasındaki fark dahil olmak üzere risk değerlendirmesi hakkında bilgi sahibi oldunuz. Risklere en yaygın yanıtları ve bunların risk azaltma stratejisi geliştirmenize nasıl yardımcı olduklarını öğrendiniz. Önlemleri ve bunları nasıl değerlendireceğinizi öğrendiniz.

Üç tür aktivite denetimini ve güvenlik yaşam döngüsüne nasıl karşılık verdiklerini öğrendiniz. Yanıtın kuruluşunuzun aksamalarla ve felaketlerle başa çıkma yeteneğini nasıl belirlediğini öğrendiniz. Üç tür yedeklemeyi ve aksamadan kurtarma için kullanabileceğiniz yedekleme modellerini öğrendiniz. Ek olarak, olay yanıtı için almanız gereken adımları ve ayrıcalıklı olay yanıtının risk, yanıt ve kurtarma işlemlerinde oynadığı rolü öğrendiniz. Son olarak, felaket kurtarma için ana adımları ve felaket kurtarma planı boyunca oynadığınız rolleri öğrendiniz.

ANAHTAR KAVRAMLAR VE TERİMLER

Activity phase controls – Faaliyet aşaması denetimleri
Administrative control – Yönetimsel denetimler
Annualized rate of occurrence (ARO) – Yıllık gerçekleşme oranı
Barricades - Barikatlar
Checklist test – Kontrol listesi testi
Clustering - Kümeleme
Compensating controls – Telafi edici denetimler
Consortium agreement – Konsorsiyum anlaşması
Control - Denetim
Corrective control – Düzeltici denetim
Countermeasure - Önlem
Detective control – Algılayıcı denetim
Deterrent control – Caydırıcı denetim
Disruption - Aksama
Emergency operations center (EOC) – Acil durum operasyon merkezi (EOC)
EMI shielding – Elektromanyetik enterferans /parazit (EMI) kalkanı
Event - Olay
Fault tolerance - Hata toleransı
Impact – Etki
Incident – Ayrıcalıklı olay
Incident response team – Ayrıcalıklı olay yanıt ekibi
Likelihood - Olasılık
Load balancing – Yük dengeleme
Loss expectancy – Kayıp beklentisi
Management control – Yönetim denetimi
Mantrap - Tuzak
Maximum tolerable downtime (MTD) – Maksimum tolere edilebilir aksama süresi (MTD)
Mean time between failures (MTBF) - Arızalar arasındaki ortalama süre (MTBF)
Mutual aid – Karşılıklı yardım
Operational control – İşlevsel denetim
Parallel tests – Paralel testler
Preventive control – Önleyici denetim
Proximity reader – Yakınlık okuyucusu
Qualitative risk assessment – Nitel risk değerlendirmesi
Quantitative risk assessment – Nicel risk değerlendirmesi
Reciprocal centers – Çift taraflı merkezler
Redundancy - Yedek
Redundant Array of Inexpensive Disks (RAID) - Ucuz Diskler Yedek Dizisi
Remote journaling – Uzak günlük kaydı
Residual risk – Artakalan risk
Risk - Risk
Risk register – Risk kaydı
Safeguard - Korunma
Sandbox – Kum Havuzu
Service bureau – Hizmet bürosu
Simulation test – Simülasyon testi
Single point of failure (SPOF) – Tek arıza noktası
Static environments – Durağan ortamlar
Succession planning – Yedekleme planlaması
Technical control – Teknik denetim
Threat - Tehdit
Total risk – Toplam risk
Vulnerability – Güvenlik açığı

BÖLÜM 8 DEĞERLENDİRME

1. Bir aksamanın ardından kritik iş süreçlerini devam ettirmek için gerekli eylemleri içeren bir plana _____ denir.
   A. Felaket kurtarma planı (DRP)
   B. İş etki analizi (BIA)
   C. İş süreklilik planı (BCP)
   D. Hiçbiri

2. Büyük bir aksamanın ardından kurtarma ve normal iş operasyonları için gerekli altyapıyı geri yüklemek için gerekli adımları açıklayan bir plan, _____ dır.
   A. Felaket kurtarma planı (DRP)
   B. İş etki analizi (BIA)
   C. İş süreklilik planı (BCP)
   D. Hiçbiri

3. Bir güvenlik açığı, bir tehdidin gerçekleştirilmesine olanak tanıyan herhangi bir risktir.
   A. Doğru
   B. Yanlış

4. Bir IDS ne tür bir denetimdir?
   A. Algılayıcı denetim
   B. Önleyici denetim
   C. Düzeltici denetim
   D. Telafi edici denetim
   E. Hepsi

5. _____, belirli bir kritik sistem olmadan bir işletmenin yaşayabileceği süredir.
   A. Kurtarma süresi hedefi (RTO)
   B. Kritik iş fonksiyonu (CBF)
   C. Maksimum tolere edilebilir aksama süresi (MTD)
   D. Hiçbiri

6. Ayrıcalıklı bir olayı yönetme süreci aşağıdakilerden hangisini kapsar?
   A. Belgeleme
   B. Yanıt
   C. Bildirim
   D. Kurtarma ve takip etme
   E. Hepsi

7. Felaketten kurtarmanın temel adımları kişilerin güvenliği, hasarın kontrol altına alınması, hasar tespiti ve kurtarma işlemlerinin başlatılmasından oluşur.
   A. Doğru
   B. Yanlış

8. Güvenlik politikanızı ihlal eden veya tehdit eden herhangi bir olay _____ olarak bilinir.
   A. Önlem
   B. Etki
   C. Risk
   D. Ayrıcalıklı olay

9. Bir risk senaryosunun açıklanması ve ardından olayların ticari faaliyetler üzerindeki etki derecesinin belirlenmesi süreci niceliksel risk analizidir.
   A. Doğru
   B. Yanlış

10. Risk azaltma çabaları uygulandıktan sonra bile devam eden risk, _____ risk olarak bilinir.
    A. Nitel
    B. Nicel
    C. Artakalan
    D. Hiçbiri

BÖLÜM

9 Kriptografi

Webster'ın *Gözden Geçirilmiş Tam Sözlüğü*'ne göre, kriptografi "gizli karakterlerle yazım eylemi ya da sanatı"dır. Hesaplamanın Ücretsiz Çevrimiçi Sözlüğü, kriptografinin "verilerin yalnızca belirli bireyler tarafından çözülebilmesi için kodlanması" olduğunu söyler. Verileri şifrelemek ve deşifrelemek için kullanılan algoritmalar veya şifreler topluca bir **kriptosistem (*cryptosystem*)** olarak adlandırılır. Şifrelerin çoğu, **düz metin (*plaintext*)** olarak adlandırılan şifrelenmemiş verileri alır ve düz metni bir gizli mesaja dönüştürmek için bir veya daha fazla anahtar kullanır. **Anahtar (*key*)**, yalnızca gönderici ve/veya alıcı tarafından bilinen bir sayı veya karakter dizisidir. Elde edilen gizli mesaj **şifreli metindir (*ciphertext*).**

Bir kriptosisteminin güvenliği genellikle şifrenin gizliliği yerine anahtarların gizliliğine bağlıdır. Güçlü bir kriptosistem, olası anahtarların geniş bir aralığına sahiptir ve bu anahtarların hepsini kaba kuvvet (brute-force) saldırısında denemeyi imkansız hale getirir. Güçlü bir sistem ayrıca tüm standart istatistiksel testlere rastgele görünen ve kodları kırmak için bilinen tüm önceki yöntemlere direnen şifreli metin üretmelidir. Kodları kırma işlemi **kriptanalizdir (*cryptanalysis*).**

Temelde, **kriptografi (*cryptography*)**, bilgiyi diğerlerinden gizleme sanatıdır. Kişisel işlemlerde olduğu kadar iş ve devlette de uygulanmış kriptografiyi bulabilirsiniz. Şifreleme, bilgiyi güvenli hale getirmenin tek yolu değildir. Bunun yerine, kriptografi BT güvenliği için bir araçlar kümesidir.

Kriptografi dört güvenlik hedefini gerçekleştirir:

- Gizlilik
- Bütünlük
- Kimlik denetleme
- İnkar edememe

BT güvenlik uzmanı, işletmelerin güvenlik hedeflerini karşılamak için bu kriptografik araçları yaratıcı bir şekilde kullanır.

Bölüm 9 Konular

Bu bölüm aşağıda verilen konuları ve kavramları içermektedir:

- Şifreleme nedir?
- Şifreleme, iş ve güvenlik gereksinimlerini nasıl ele alabilir?
- Bilgi sistemi güvenliğinde hangi kriptografik uygulamalar kullanılır?
- Kriptografik prensipler, kavramlar ve terminoloji nedir?

- Kriptografik uygulamalar, araçlar ve kaynaklar nelerdir
- Sertifikaların ve anahtar yönetiminin prensipleri nelerdir

9. Bölüm Hedefler

Bu bölümü tamamladığınız zaman, yapabilecekleriniz:

- Kriptografinin temel kavramlarını tanımlamak
- Simetrik, asimetrik ve özetleme (*hashing*) algoritmalarını tanımlamak
- Kriptografinin çeşitli kullanımlarını inceleyebilmek
- Kriptografik kullanımların zorluklarını anlayabilmek
- Sertifika yönetimini tanımlamak

Kriptografi Nedir?

Kriptografi, okunabilir bir mesajı yalnızca yetkilendirilmiş kullanıcılar tarafından okunabilen bir biçime dönüştürme sanatıdır:

- **Şifrelenmemiş bilgiler** — Anlaşılabilir biçimdeki bilgilerdir. Şifrelenmemiş bilgiler, **açık metin (*cleartext*)** olarak da adlandırılan **düz metinlerdir (*plaintext*).**
- **Şifrelenmiş bilgi** — Karıştırılmış biçimdeki bilgilerdir. Şifrelenmiş bilgi **şifreli metindir (*ciphertext*).**

Şifreleme (*encryption*), düz metnin karıştırılarak şifreli metne dönüştürülmesi işlemidir. **Şifre çözme (*decryption*)** şifreli metnin çözülerek düz metne dönüştürülmesi işlemidir.
Şifreleme, işlevlerini yerine getirmek için bilinen matematiksel işlemleri kullanır. Böyle bir süreç **algoritma (*algorithm*)** olarak bilinir. Bir algoritma, aynı sonucu aldığında aynı sonucu üreten tekrarlanabilir bir işlemdir. Bir şifre, bilgiyi şifrelemek veya şifresini çözmek için kullanılan bir algoritmadır. Bu tekrarlanabilirlik, bir kez şifrelenen bilginin şifresinin çözülebildiğinden emin olmak için önemlidir. **ŞEKİL 9-1,** iş yerindeki bir kriptosistemi gösterir.

Bilgileri şifrelemek için kullandığınız algoritmanın, bu bilgilerin şifresini çözmek için kullandığınız ile aynı olabileceğini veya olmayabileceğini unutmayın. Örneğin, şifrelemek için her bir değere X ekleyen basit bir algoritma, her bir değerin deşifre edilmesi için X değerini çıkarmak zorunda kalacaktır. Ayrıca, bazı şifreleme algoritmalarının şifre çözme algoritmaları yoktur. Bunlar **tek yönlü algoritmalar (*one-way algorithms*)** veya **özetleme fonksiyonlarıdır (*hashing functions*).** Tek yönlü bir algoritmanın çıktısı bir **özettir (*hash*).** Özetleme fonksiyonları, verileri yetkilendirilmemiş değişikliklerden korumak için yararlıdır. Kriptografinin farklı şekillerde nasıl kullanıldığını bu bölümün ilerleyen kısımlarında öğreneceksiniz.



ŞEKİL 9-1
İş yerindeki bir kriptosistem.

TEKNİK İPUCU

Kriptografik şifrelerin tümü anahtar gerektirmez. Bazı yeni kriptografik algoritma türleri, anahtarlarını diğer bilgilerden elde etmektedir. Bu yaklaşım, parola dışındaki girdileri kullanan erişim denetimlerine benzemektedir. Örneğin, **kimlik tabanlı şifreleme (*identity-based encryption - IBE*)** bir anahtar elde etmek için şifrelemeyi yapanın kimliğini kullanır. **Öznitelik tabanlı şifreleme (*attribute-based encryption - ABE*)** verileri şifrelemek ve şifresini çözmek için betimleyici (***descriptive***) öznitelikler kullanır.

En yaygın şifrelemeler, girdi olarak düz metin ve en az bir anahtar gerektirmektedir. Şifreleme, çıktılarını değiştirmek için şifreleme anahtarı kullanılır, böylece ilgili kişiler, bilgilerini aynı şifreye sahip olan başka kişilerden koruyabilir. Anahtarı değiştirerek, düz metin aynı kalsa bile, şifreleme işlevinin çıktısını değiştirirsiniz.

Şifrelemeler iki genel kategoriye ayrılır:

- Şifrelemek ve şifresini çözmek için aynı anahtarı kullananlar **özel (*simetrik*) (*private - symmetric*) anahtarlı** şifrelemeler.
- Şifrelemek ve şifresini çözmek için farklı anahtarlar kullananlar **açık/kamusal (*asimetrik*) (*public - asymmetric*) anahtarlı** şifrelemeler.

Bazen, açık anahtar ve özel anahtar terimleri, asimetrik şifrelemelerdeki iki farklı anahtarı işaret eder. Açık anahtar ve özel anahtar birlikte bir anahtar çiftidir. Karışıklığı önlemek için, şifreler için simetrik ve asimetrik adlandırma geleneği burada kullanılır. Bununla birlikte, birçok kaynağın bu şartları serbestçe değiştirebileceğini unutmayın.

Temel Kriptografik İlkeler

İPUCU

Anahtar uzatma (*key-stretching*) teknikleri, zayıf bir anahtarın kaba kuvvet (*brute-force*) saldırılarına karşı daha dayanıklı olmasını sağlar. Bir anahtar uzatma işlevi, bir anahtarı (genellikle zayıf bir anahtar) girdi olarak alır ve daha kararlı bir saldırıya dayanabilecek geliştirilmiş bir anahtar oluşturur.

Mükemmel bir şifreleme yoktur. Yeterli zaman ve kaynaklar olduğunda, bir saldırgan önünde sonunda herhangi bir şifreli metni deşifre edebilir. Kriptografinin amacı, şifreli bilginin anahtarsız bir şekilde şifresini çözmek için gereken sürenin veya zamanın korunan bilginin değerini aşmasını sağlamaktır. Böylelikle, değeri 100$ 'dan fazla olmayan bilgileri, kırılması 1000$ maliyetine sahip olan şifreleme ile etkili bir şekilde koruyabilirsiniz. Bu önemli bir kavramdır. Bu durum, kriptografik araçları ve şifrelemeleri seçmek için temel gerekçelerden birini sağlar.

Bir şifreleme için olası anahtarların sayısı **anahtar uzayıdır (*keyspace*)**. Anahtar ile ilgili herhangi bir bilgi olmadan, şifrelenmiş bir iletiye ve şifre çözme algoritmasına erişimi olan bir saldırgan, iletinin şifresini çözmek için mümkün olan her anahtarı deneyebilir. Bu kaba kuvvet saldırısıdır (*brute-force*). Anahtar uzayını yeterince büyük tutarak, kaba kuvvet saldırısının maliyetini çok yükseltirsiniz. Şifreleme algoritmasının matematiksel zayıflıklarının olmadığı varsayıldığında, büyük bir anahtar uzayı genellikle daha fazla güvenlik anlamına gelir.

Açık/kamusal (açık kaynaklı) şifrelemeler ve gizli (kapalı-kaynaklı veya tescilli) şifrelemeler bulunmaktadır. Açık şifrelemeler, dünyanın dört bir yanındaki uzmanların şifreleme algoritmalarını zayıflıklar açısından incelemelerini mümkün kılar. Uzmanlar açık kaynaklı şifrelemelere kapsamlı analizler yaparlar. Şifrenin gücünü azaltabilecek kusurları ve zayıflıkları bulurlar. Hiç kimse önemli kusurlar belirtmediyse, kamu denetimine karşı koyabilen herhangi bir şifreleme çok daha güvenlidir. Tarihte en iyi incelenen kod, 1977'de Federal Bilgi İşleme Standardı (*Federal Information Processing Standard* - FIPS) 46 olarak yayınlanan Veri Şifreleme Standardı (*Data Encryption Standard* - DES) 'dır. Modern hesaplama, tek bir matematiksel zayıflık bulmaksızın, 72 katrilyon anahtardan oluşan anahtar uzayında arama yapmıştır.

Kriptografinin Kısa Tarihi

> **UYARI**
> Her zaman kanıtlanmış şifreleme algoritmaları kullanın. Kendi algoritmalarınızı yazmaya çalışmayın. Tarih, özel olarak geliştirilmiş şifreleme algoritmalarının açık algoritmalardan daha zayıf olduğunu göstermektedir. Dünyanın dört bir yanındaki uzmanların bir algoritmanın gücünü kesin olarak doğrulamasına izin vermenin hiçbir alternatifi yoktur.

İnsanlar en az 4.000 yıl boyunca bilgileri korumak için şifreleme kullandılar. İnsanlar yazmayı öğrendiklerinde, sözlerini meraklı gözlerden korumak istediler. Bilgi güvenliği başlangıçta, gizleme kadar basitti. Bu yönteme **steganografi (*steganography*)** denir. Örneğin, efsane, 5. yüzyılda Miletos tiranı Histiaeus'un kölesinin kafa derisine yaptırdığı dövme ile mesajını gönderdiğini söyler. Elçiye müdahale eden herhangi bir düşman, bilgiyi bulamayacaktı. Ancak, bu yöntem hızlı değildi. Miletos, haberciyi gizli mesajla göndermeden önce habercinin saçının tekrar uzamasını beklemek zorundaydı. Ayrıca, yeniden kullanılabilirlik bir problemdi.

Steganografi bugün hala kullanılmaktadır. Steganografiyi kullanmanın yaygın bir yolu, dijital bir resim gibi büyük bir medya dosyasına bir mesaj yerleştirmektir. Steganografi yazılımı, bir dizi adres için bir medya dosyasındaki tek bir biti değiştirebilir. Örneğin, bir dizi byte'da bir bitin değiştirilmesi, görüntünün (imajın) insanlara nasıl göründüğünü değiştirmez. Görüntü dosyası, taşıyıcı, bize değiştirilmemiş görünür. Fakat, steganografi yazılımı taşıyıcıyı gizli bir yük (*payload*) ile yükledi. Bu veriyi gizleme metodu, veriyi tespit etmeyi, çıkarmayı daha da zorlaştırmaktadır. Çoğu şifreleme algoritması ile şifreli metinleri tanımlamak kolaydır. Sadece anlamsız görünür. Steganografi, suçlular iletişimlerini kolluk kuvvetleri yetkililerinden saklamak için steganografiyi daha sık kullandıkları için giderek artan bir endişe kaynağıdır.

Kriptanaliz bilimi ya da kodları kırma uzun yıllar boyunca önemliydi. Kraliçe I. Elizabeth, kuzeni İskoç Kraliçesi Mary'i vatana ihanet nedeni ile idam etti. Neden? Çünkü, Sir Francis Willingham, Mary'nin komplocuları ile iletişim kurduğu gizli kodu kırdı. Böylece, kriptanaliz İngiliz tarihinin seyrini değiştirdi.

20. Yüzyıl Kriptografisi

Kriptografi, I. ve II. Dünya Savaşları'nda iletişimde önemli bir rol oynamıştır. Bunlar, savaşçıların radyo kullandığı ilk büyük savaşlardı. Tüm ülkeler iletişimlerini korumak için kodları kullandı. Birçok savaşçı, rakiplerinin kodlarını başarılı bir şekilde, bazen birden çok kez kırdı. ABD ve İngiliz kod çözücüleri, Japonların Mor Şifresi'nin (*Purple Cipher*) ve Almanların Enigma'sının şifresini çözerek, askeri karar vericilere düşman planlarına ilişkin bilgi verdi. Bu kod kırıcılar, Müttefiklerin Midway Muharebesi ve İngiltere Muharebesi de dahil olmak üzere kesin askeri savaşlar kazanmasına yardımcı oldular.

Dijital bilgisayarın doğuşu, karmaşık şifreleri uygulanabilir yaptı. Dijital bilgisayarlar, genelde manuel olarak saatlerce ya da günlerce sürecek işlemleri saniyeler içerisinde gerçekleştirebilir. Sonuç olarak, modern kriptografi hızlı bir şekilde dijital ortama taşındı. 1950 yılının Mühimmat Kontrol Yasası (*Munitions Control Act*), kriptografik şifreleri ve ekipmanları özel olarak Sınıf 13B mühimmat olarak sınıflandırdı. Bu onları ihracat kontrolüne ve hükümet denetimine tabi savaş araçları haline getirdi.

1976'da Stanford Üniversitesi'ndeki Whitman Diffie ve Martin Hellman, kriptografide devrim yaratan bir makale yayınladılar. Diffie ve Hellmann, asimetrik anahtar kriptografisi kavramını tanıttılar. **Simetrik anahtar kriptografisi,** iki taraf anahtarları değiştirinceye kadar yazışmaları garanti edemez. **Asimetrik anahtar kriptografisi**, iki ayrı anahtarlı bir şifreleme kullanmaktadır. Anahtarlardan biri şifreleme, diğeri şifre çözme içindir. Karşılıklı yazışan kişiler, güvenli bir şekilde iletişim kurmak için öncelikle gizli bilgi değiş tokuşu yapmak zorunda değildir. Asimetrik anahtar kriptografisi ile düşman her şeyi engelleyebilir ve hala mesajı çözemez. Diffie ve Hellman, kendi asimetrik

tekniklerini kullanarak simetrik anahtarları değiştirmenin güvenli bir yöntemini ortaya koymuştur. Bu algoritmanın en yaygın kullanımı, iki taraf arasındaki iletişimin güvenliğini sağlamaktır. Günümüzün ağ uygulamaları, mesaj değiş tokuşu yapmak için genellikle oturumlar kurarlar. Değiştirilen mesajları korumak için güvenli bir yol, her oturum için **oturum anahtarları (*session keys*)** olarak adlandırılan benzersiz anahtarlar oluşturmaktır. **Diffie-Hellman algoritmasını** kullanarak, gönderici ve alıcı simetrik anahtarları güvenli bir şekilde değiştirmek için asimetrik şifreleme kullanır. İlk anahtar değişiminden sonra, her bir taraf daha sonra verileri şifrelemek ve şifresini çözmek için simetrik şifrelemeyi kullanabilir. Bu neden önemlidir? Çünkü, simetrik şifreleme algoritmaları, benzer güvenlik garantilerine sahip asimetrik algoritmalardan neredeyse her zaman çok daha hızlıdır.

Diffie-Hellman algoritması, kriptografide ileriye doğru büyük bir adımdı. Diffie-Hellman algoritması, anahtar üretmek için modüler aritmetik kullanan **Ephemeral modunda Diffie-Hellman (*DHE*)** ve anahtar üretmek için cebirsel eğrileri kullanan **Eliptik Eğri DHE (*ECDHE*)** dahil olmak üzere birçok ortak anahtar değişim protokolünün temelini oluşturur. Bir kriptografik anahtar, her yeni oturum için yeni bir anahtar olarak oluşturulmuşsa *ephemeral (geçici)* olarak adlandırılır. DHE ve ECDHE'nin ikisi de Diffie-Hellman değişimi için geçici anahtarları kullanır. Bu, iletişim oturumlarının daha güvenli hale getirilmesine yardımcı olur. Her yeni anahtar değişimi yeni asimetrik anahtarlar kullandığı için, her bir iletişim oturumu kurulum (*setup*) işlemi benzersizdir. Mevcut oturumun anahtarlarının gizliliği bir saldırgan tarafından ihlal edilirse, bu durum önceki herhangi bir oturum anahtarını riske atmaz. Bu özelliğe **mükemmel iletme gizliliği (*perfect forward secrecy*)** denir. Mükemmel iletme gizliliği, geçmiş oturumları gelecekteki oturum gizlilik ihlallerinden korur.

Şifrelemenin dört temel amacını göz önünde bulundurun: gizlilik, bütünlük, kimlik denetleme ve inkar edememe. Dijital bilgisayarlardan önce, klasik hesaplama, bunların her birini ele almıştır. Gönderen bir mesajı şifreleyerek, saldırganın anahtarı olmadığı ve mesajı çözmek için bir kısayol bulamadığı sürece mesajın güvende olduğundan emin olur. Bütünlük, genellikle önemsizdi. Eğer şifre çözme sonucu elde edilen çıktı anlaşılmazsa, mesajın aktarımda değiştiğini biliyordunuz. Ancak, bir sahtekâr şifreleme gereçlerini elde ederse, sahte bir mesaj geçerli bir mesaj olarak görülebilir. Hem gönderen hem de alıcı aynı kod kitabına sahip ve bununla ilgili öğeleri değiştirmiş ise kimlik denetleme -gönderenin kimliğinin kanıtlanması- yapılabilir. Bununla birlikte, kod kitabını yenilemediğiniz sürece bu bilgileri değiştirmek yavaş yavaş kitabın içeriğinin gizliliğini ihlal etti. Son olarak, inkar edememe -bir tarafın gerçekten bir mesajı oluşturduğunun kanıtlanması- simetrik anahtar kriptografisi ile mümkün değildi. Paylaşılan anahtara erişimi olan herkes bir mesaj oluşturabilir. Asimetrik anahtar kriptografisinden önce, mesajı kimin yazdığını "kanıtlayamazdınız".

Bilgi Güvenliğinde Kriptografinin Rolü

Günümüzün bilgi sistemlerinde, kriptografinin iki temel kullanımıyla karşılaşacaksınız: Aktarımdaki veriyi (*data-at-transit*) korumak ve durağan veriyi (*data-at-rest*) korumak. *Aktarımdaki veri*, yaygın olarak bir ağ bağlantısı üzerinden değiştirilen herhangi bir veriyi ifade etmektedir. *Durağan veri*, bazı depolama ortamlarında saklanan herhangi verilerdir. Durağan veri, aynı zamanda bellekteki verileri de içermektedir. Farklı kriptografik yaklaşımlar, aktarımdaki verinin ve durağan verinin güvenliğini sağlama problemini çözmeye yardımcı olabilir. Aktarımdaki veri güvenliği, genellikle iletişim güvenliği olarak adlandırılmaktadır.

İletişimi güvenceye almak için iki temel yaklaşım vardır. Birinci yaklaşım, göndermeden önce her mesajı şifrelemektir. Bu yaklaşım, mesajların iletişim işlevlerinden ayrı olarak şifrelenmesi ve şifresinin çözülmesi için bazı yazılımlar gerektirir. Diğer bir yaklaşım ise, iletişim fonksiyonlarının şifreleme ve şifre çözme işlemlerini yönetmesini sağlamaktır. İletişim yazılımı aslında, mesajlar iletildiklerinde

veya alındıklarında mesajları şifreler ve şifrelerini çözer. İkinci yaklaşım genellikle, şifreleme (ve şifre çözme) ağ yığınındaki aktarım katmanında (*transport layer*) meydana geldiğinden, **bağlantı şifreleme (*connection encryption*)** veya **aktarım şifrelemesi (*transport encryption*)** olarak adlandırılmaktadır. Aktarım şifreleme protokollerinin yaygın örnekleri arasında, web sunucuları ve tarayıcılar arasında güvenli bağlantılar oluşturmak için yaygın olarak kullanılan Güvenli Soket Katmanı (*Secure Sockets Layer* - SSL) veya Aktarım Katmanı Güvenliği (*Transport Layer Security* - TLS) ve uzak sunuculara güvenli oturum açma kurmak için kullanılan **Güvenli Kabuk (*Secure Shell* - SSH)** bulunmaktadır.

Bilgi güvenliği söz konusu olduğunda, kriptografi şu gereksinimleri karşılayabilir:

- Gizlilik
- Bütünlük
- Kimlik Denetleme
- İnkar Edememe

Gizlilik

Gizlilik (*confidentiality*), bilgiyi yetkilendirilmemiş kullanıcılardan gizli tutar. Gizliliği sağlamak için kasaları kilitleyebilir, silahlı muhafızlar görevlendirebilir veya uzak bir alanda bir kişinin kulağına fısıldayabilirsiniz. Ancak, bu taktikler çoğu zaman yeterli değildir. Kriptografi, şifreleme kodunu (*encryption cipher*) ve doğru anahtarı bilmeyen herkes için bilgiyi anlaşılmaz hale getirmektedir. Yetkilendirilmiş kullanıcılar bu bilgiyi alabilirler. Aynı zamanda, etkili bir kriptanaliz de bu bilgiyi üretebilir. Gizliliğin değeri açıktır. Gizli bilgileri içeren belirli iletişimleri açıklamak, iletişim kuran kişilere zarar verebilir veya bir düşmana yardım edebilir.

Bütünlük

Bütünlük (*integrity*), gönderen bile olsa, hiç kimsenin aktarımdan sonra bilgileri değiştirememesini sağlar. Eğer bir mesajın şifresi düzgün bir şekilde çözülmezse, bir kişi veya bir şey muhtemelen aktarım sırasında şifreli metni değiştirmiştir.

Ek olarak, kriptografi, bütünlüğü özetlemeler (*hash*) veya sağlama toplamları (*checksum*) ile yerine getirebilir. Bir **sağlama toplamı**, genellikle orijinal mesajdan çok daha küçük bir sonuç veren bilginin tek yönlü bir hesaplamasıdır. Bunu tekrarlamak zordur. Örneğin, 1-800-555-1212 numaralı telefon numarasının basit bir sağlama toplamı, her bir rakamın toplamı olan 30 olabilir. Sağlama toplamını bilerek, telefon numarasını yeniden oluşturamazsınız. Bununla birlikte, telefon numarasının sağlama toplamıyla eşleşip eşleşmediğini anlayabilirsiniz. Eğer bir rakamı değiştirdiyseniz -örneğin 1-800-555-1212'yi 1-900-555-1212 olarak değiştirdiniz- sağlama toplamı beklenen değerle artık eşleşmemektedir. Bu nedenle, verinin bütünlüğünü sorgulayabilirsiniz. Ancak, bunun pratik bir güvenlik yöntemi olmadığını unutmayın. Yanlış telefon numarasıyla doğru sağlama toplamını üretmek için verileri kolayca değiştirebilirsiniz. Bütünlük doğrulaması, tersine mühendislik yapmanın zor olduğu sağlam matematiksel süreçleri kullanma eğilimindedir. Bunlar özetlemelerdir. Bu bölümde daha sonra özetlemeler hakkında daha fazla bilgi edineceksiniz.

Kimlik Denetleme

Kimlik denetleme (*authentication*), bir varlığın kimliğini doğrular. Gönderen, gönderenin bilgisayarı, herhangi bir cihaz veya bazı bilgiler olabilir. İnsanlar, yüz görünümü, ses veya cilt dokusu gibi özelliklere dayanarak birbirlerinin kimliğini içgüdüsel olarak denetlerler. Geleneksel bir askeri kimlik doğrulama yöntemi paroladır. Eğer parolayı biliyorsanız, nöbetçi geçmenize izin verir. Eğer parolayı bilmiyorsanız, başınız derttedir. Dijital alanda, kriptografi varlıkların kimliklerinin

denetlenmesi için bir yol sağlamaktadır. En basit formu, bir kullanıcı kimliği ve parolasıdır. Bunun güçlü bir kimlik denetlemesi olmadığını unutmayın. Bu sabit bilgiyi elde eden diğer herkes, kullanıcının geçerli olduğunu düşünecek olan alıcıya aynı bilgiyi sağlayabilir.

Genel olarak, simetrik anahtar kriptografisi bu soruna sahiptir. Bir saldırgan, gönderenin ve alıcının bir şifre ve anahtar üzerinde hemfikir olduğu konuşmayı dinleyebilirse, saldırgan geçerli bir kullanıcıymış gibi davranabilir. Anahtar değişimine yönelik bu yaklaşım, veri ile aynı iletişim kanalını kullanır ve **bant içi anahtar değişimi (*in-band key exchange*)** olarak adlandırılmaktadır. Bir simetrik anahtar kriptografi dünyasında kimlik denetlemesi yapabilmek için, taraflar öncelikle anahtarları kendi aralarında güvenli bir şekilde dağıtmalıdır. Örneğin, taraflar simetrik anahtarları dağıtmak için asimetrik anahtar kriptografisini kullanabilirler. Daha sonra, izleyen yazışmalar için simetrik anahtarları kullanırlar. Anahtarları dağıtmanın daha az karmaşık bir diğer yolu, bağlantısız bir iletişim yöntemi kullanmaktır. Anahtar değişimi için, verileriniz için kullandığınızdan farklı bir iletişim kanalı kullanımı **bant dışı anahtar değişimi (*out-of-band key exchange*)** olarak adlandırılmaktadır. Fiziksel bir kurye anahtarı teslim edebilir. Bu, çok sayıda kullanıcının olduğu durumlar için pahalı ve zaman alıcıdır; bununla birlikte, tüm tarafların kimliklerinin denetlenmesinin değeri, ordu gibi ortamlarda maliyete değecek kadar büyüktür.

Asimetrik anahtar kriptografisi, kimlik denetleme yöntemlerini basitleştirmek için bir yaklaşım sunar. Gizlilik ile birlikte, asimetrik anahtar kriptografisi internet ticaretinin temel taşıdır. Ancak, kriptografi tek başına kimlik denetleme problemini çözemez. Bir çözüm, özünde kriptografi ile birlikte bir dizi kimlik denetleme ve güvenlik protokollerini kullanmaktır. Microsoft, kimlik denetlemesini kanıtlamak ve kullanıcılara bütünlük sağlamak için NT LAN Yöneticisi (*NT LAN Manager* - NTLM) protokol paketini üretti. NTLM, dağıtılmış ağ kaynakları arasında güvenli iletişimi kurmak ve yönetmek için yapı sağlamaktadır. NTLMv2, NTLM'nin daha yeni bir sürümü, güvenliği orijinal sürümün sınırlamalarının ötesinde artırmaktadır.

İnkar Edememe

İnkar edememe (*nonrepudiation*), bir tarafın önceki bir ifadeyi veya eylemi reddetmesini önlemenizi sağlar. Örneğin, bir yatırımcının borsacısına "Değeri 50'de olan XYZ'den 1.000 hisse satın al" şeklinde bir e-posta gönderdiğini varsayın. İşlem gerçekleştikten kısa bir süre sonra, XYZ hisseleri 20'ye düşer. Yatırımcı daha sonra bu satın alma emrini reddeder ve aslında bunun satmak için bir emir olduğunu belirtir. Bir kişi bu tür bir "o söyledi/o söyledi" ikilemini nasıl çözer?

Asimetrik anahtar kriptografisini kullanarak, matematiksel olarak (genellikle bir hakimin veya jürinin memnuniyeti için), belirli bir tarafın belirli bir zamanda belirli bir mesajı oluşturduğunu kanıtlayabilirsiniz. Asimetrik anahtar kriptografisinin temel ilkesi, şifreleme ve şifre çözmek için bir

Bilginize

Kamusal ve özel anahtarları karıştırmak kolaydır. Bir mesajı, mesajın gizliliğini ve bütünlüğünü korumak için şifreliyorsanız, alıcının kamusal anahtarını kullanırdınız. Sadece alıcı, ilgili özel anahtarı kullanarak mesajın şifresini çözebilir. Bununla birlikte, eğer siz, mesajı gönderen olarak, şifrelemeyi inkar edememeyi sağlamak için kullanmak istiyorsanız mesajı kendi özel anahtarınız ile şifreleyeceksiniz. Genel anahtarınıza erişimi olan herkes mesajın şifresini çözebilir, ancak başarılı bir şifre çözme mesajı sizin oluşturduğunuzu kanıtlar.

anahtar çifti kullanmasıdır. Mesajı düzenleyen kişi, anahtarlardan birini bilen tek kişidir. İnkar edilemez bir zaman damgası vardır. Mahkemedeki argüman şöyle bir şey olurdu:

"Şifreleme, mesajları gizli tutmaktan daha fazlasını yapar. Gönderenin kimliğini doğrulayabilir. Bu şifrelenmiş mesajın şifresi bu kamusal anahtarla çözülür. Sadece ilgili özel anahtarın sahibi bu mesajı oluşturabilirdi. Mesaj, güvenilir bir üçüncü taraf zaman damgası cihazı tarafından üretilen zamana dayalı bir özet içerir. Hiçbir taraf onu değiştiremezdi. Bu nedenle, şifresi çözülmüş olan bu mesajın özgün ve bilinen bu taraf kaynaklı olduğunu etkin bir kesinlikle biliyoruz. Bu inkar edememedir."

Kriptografi için İş ve Güvenlik Gereksinimleri

Bu bölümde, bilgi güvenliği ilkeleri ve kriptografinin bunları nasıl ele alabileceği hakkında bilgi edineceksiniz.

İç Güvenlik

Bazı güvenlik hedefleri, bir işletmeye değer katar. Bunlar aşağıdakileri içermektedir:

- **Gizlilik** – Gizlilik, bilgilerin yalnızca yetkilendirilmiş kişiler tarafından okunabilmesini sağlar. Yetkilendirilmemiş kişiler verilere erişemez. Örneğin, çoğu şirket maaş bilgilerini gizli tutar.
- **Mahremiyet** - Mahremiyet genellikle gizlilikle karıştırılmaktadır. Mahremiyet, bir bireyi tanımlayabilecek bilgilerin yayımlanmasını koruduğu için gizlilikten farklılık gösterir. Örneğin, belirli bir posta kodunda yaşayan bir kişinin belirli bir hastanede belirli bir günde kırık bir kol için tedavi edildiğini ve bir yüz lazerasyonu olduğunu yayımlayan bilgiler bu kişinin kimliğini ortaya çıkarabilir. Mahremiyet, bir saldırganın bir bireyi tanımlamak için mevcut bilgileri bir araya getirememesini sağlar.
- **Bütünlük** - Bütünlük, hiç kimsenin verileri değiştirmediğini veya silmediğini garanti eder. Örneğin, çek yazıcınıza gönderildikten sonra hiç kimsenin ödemeyi değiştirmediğinden emin olmak için maaş bordroları verisi bütünlüğü gerektirmektedir.
- **Yetkilendirme** - Yetkilendirme, belirli bir görevi yerine getirmek veya belirli verilere erişmek için bir kişinin onaylanması anlamına gelir. Örneğin, değişen maaş planları, yönetimden uygun yetkilendirme gerektirir.
- **Erişim denetim** - Erişim denetimi, bilgileri doğru kişilere sınırlamayı içerir. Örneğin, maaş planlarını sadece İK çalışanlarının anahtarı olan kilitli bir dosya dolabında saklayabilirsiniz.

İş İlişkilerinde Güvenlik

Bir dizi güvenlik hedefi işletmeler arasındaki veya işletmeler ile müşterileri arasındaki ilişkilere değer katmaktadır. Daha önce listelenenlere ek olarak, bu güvenlik hedefleri aşağıdakileri içerir:

- **Mesaj doğrulama** — Mesaj doğrulama, yazışma başlatan kişinin kimliğini doğrular. Örneğin, bir borsacı "ABC hesabı için XYZ'nin 1.000 hissesini satın al" mesajının ABC'den geldiğini bilmek ister.

NOT

Mahremiyet sorunları gittikçe daha önemli bir hale geldikçe, güvenlik çevrelerinde ilginç bir gerilim kaynağı daha belirgin hale gelmektedir. İnkar edememe, bir eylemin bir bireyle olumlu bir şekilde ilişkilendirilebileceği anlamına gelir. Mahremiyet, kişisel bilgileri açıklamadan eylem gerçekleştirebilmeyi ifade eder. Hangisi daha önemlidir? Henüz bilmiyoruz. Bu iki kavram temelde birbirine karşıttır ve bu tartışma devam etmektedir.

- **İmza** - Dijital imza, bir mesajı veya verileri belirli bir varlığa bağlar. Bunun, elektronik olarak çoğaltılan bir imzanın imgesi olan dijitalleştirilmiş bir imza olmadığına dikkat ediniz.
- **Alındı ve onay** - E-posta mesajları genellikle alındı ve onay kullanır. Alındı, bir varlığın bilginin geldiğini onayladığını doğrular. Onay, sağlayıcının bir servisi sağladığını doğrular.
- **İnkar edememe** - İnkar edememe, bir mesaj gönderen kişinin daha sonra bunu inkar edemeyeceği anlamına gelir. Örneğin, XYZ yüzde 50 düştükten sonra satın alma emrini yapan kişi bu emire itiraz etseydi, inkar edememe orijinal mesajın geçerli olduğunu kanıtlayabilirdi.

Herkese Yarar Sağlayan Güvenlik Önlemleri

İş ve müşteri ilişkilerinin ötesinde, belirli güvenlik hedefleri bilgi sistemlerine değer katmaktadır. Önceden listelenen bu öğelere ek olarak, bu hedefler aşağıdakileri içerir:

- **Anonimlik** - Anonimlik bir kullanıcının kimliğini gizler. Örneğin, baskıcı bir ülkedeki muhalif, yetkililerin onun kim olduğunu bilmeden bir tartışma web sitesine bilgi göndermek isteyebilir. Maalesef, suçlular ve teröristler tespit edilmekten kaçınmak için anonimlik kullanabilirler.
- **Zaman damgası** - Zaman damgası, bir üreticinin bilgiyi oluşturduğu veya gönderdiği tam zamanı sağlar. Örneğin, son dakikada vergi beyannamesi gönderen kişiler son teslim tarihini yerine getirdiklerini kanıtlamak isteyebilir.
- **İptal etme** - İptal etme, verilere erişim için yetkilendirmeyi sonlandırır. Örneğin, kredi kartını kaybeden bir kişi kartın kullanımını durdurmak için bankayı arar.
- **Sahiplik** - Sahiplik, yasal hak talep etmek için kişiyi bilgileri ile ilişkilendirir. Örneğin, çoğu belgede, bu belgeleri kimin yazdığını belirten telif hakkı bildirimleri bulunur.

Kriptografik İlkeler, Kavramlar, ve Terminoloji

Birçok farklı bilgi güvenliği hedefi vardır. Bu hedefleri anlamak, birlikte nasıl çalıştıklarını ve bazen nasıl birbirlerine karşı olduklarını anlamak önemlidir. Kriptografi dahil olmak üzere güvenlik girişimleri amaçlarının çoğunu temsil ederler. Güvenlik hedeflerinin en iyi özetlerinden biri *Uygulamalı Kriptografinin El Kitabı*'ndadır (*Handbook of Applied Cryptography*). **TABLO 9-1** güvenlik hedeflerini özetlemektedir. İş ile ilgili bir güvenlik sorununu çözmeye çalıştığınızda, bu terimleri anlamanız gerekmektedir. Daha sonra, kriptografik bir çözüm kullanıp kullanmayacağınızı anlayabilirsiniz.

Kriptografik Fonksiyonlar ve Şifreler

Kriptografik şifrelemelere dair temel bir anlayış, kriptografinin iş gereksinimlerinizi nasıl karşılayabileceğini size söyleyebilir. Her şifre, herhangi bir durum için istenen veya istenmeyen özel karakteristiklere sahiptir. Bir şifrelemeyi değerlendirirken dikkate alınması gereken ilk konu, kullanım amacıdır. Aktarımdaki veriyi mi yoksa durağan veriyi mi güvence altına almaya çalışıyorsunuz? Farklı şifrelemeler farklı problemleri diğerlerinden daha iyi çözer. Bir şifreleme seçtikten sonra, anahtar boyutu ve çalışma modu gibi konularda ek kararlar almak zorundasınız. Birçok simetrik şifreleme, seçtiğiniz moda bağlı olarak **kesintisiz şifreleme (stream cipher)** veya **blok şifreleme (*block cipher*)** olarak çalışır. **Kesintisiz şifreleme (*stream cipher*)** bir defada bir byte (veya bit) şifrelerken,

TABLO 9-1 Bilgi güvenliği hedefleri.

HEDEF	ATILACAK ADIMLAR
Mahremiyet ya da gizlilik	Tüm yetkilendirilmemiş kullanıcılardan bilgiyi gizli tutun.
Bütünlük	Yetkilendirilmemiş kullanıcıların veya bilinmeyen süreçlerin bilgileri değiştirmediğinden emin olun.
Varlık kimlik denetleme ya da tanımlama	Bir varlığın kimliğini (yani, bir kişi, bir bilgisayar terminali, bir kredi kartı, vb.) doğrulayın.
Mesaj doğrulama	Bilgi kaynağını doğrulayın; verilerin kaynağının kimliğini denetleyin.
İmza	Bilgiyi bir varlığa bağlayın.
Yetkilendirme	Bir şey yapmak ya da olmak için başka bir varlığa resmi bir yaptırım bildirin.
Doğrulama	Bilgi veya kaynakları kullanmak veya değiştirmek için süreli yetkilendirme sağlayın.
Erişim denetim	Kaynaklara erişimi ayrıcalıklı varlıklar ile sınırlandırın.
Sertifikasyon	Güvenilir bir varlık tarafından bilgiyi onaylayın.
Zaman damgası	Bir kullanıcının bilgiyi yarattığı ya da bilgiye eriştiği zamanı kaydedin.
Tanıklık	Bir nesneyi oluşturan eylemi doğrulayın veya bir nesnenin varlığını nesneyi yaratan dışındaki bir varlık tarafından doğrulayın.
Alındı	Alıcının bilgiyi aldığını onaylayın.
Onay	Sağlayıcının hizmetleri sağladığını onaylayın.
Sahiplik	Bir varlığa, bir kaynağı yasal olarak kullanma ya da başkalarına aktarma hakkı verin.
Anonimlik	Bazı süreçlerde yer almış olan bir varlığın kimliğini gizleyin.
İnkar edememe	Bir varlığın önceki sorumlulukları veya eylemleri reddetmesini engelleyin.
İptal etme	Sertifikasyonu veya yetkilendirmeyi geri çekin.

blok şifreleme (*block cipher*) bir defada tüm veri bloğunu şifrelemektedir. "En iyi" şifreleme türüne karar vermek karmaşık bir işlemdir. Birçok fark ve çok az standart cevap vardır. Şifrelemeler daha karmaşık hale geldikçe, anahtar oluşturmak ve düz metinleri şifreli metinlere dönüştürmek için yeni tekniklere güvenilmektedir.

Eliptik eğri kriptografi (*elliptic curve cryptography* - ECC) ve **kuantum kriptografi,** iki verimli araştırma alanıdır. ECC şifrelemeleri, sonlu alanlar üzerinde eliptik eğrilerin cebirsel yapılarına bağlıdır. Bu şifrelemeler, daha geleneksel olan şifrelemelere göre daha küçük anahtarlar kullanarak çok güvenli şifreli metinler meydana getirirler. Bununla birlikte, ECC yüksek bir hesaplama maliyeti getirir. Kuantum kriptografi, algoritmalarını kuantum mekaniğinin özelliklerine dayandırır. Klasik kriptografi ve kuantüm kriptografi arasındaki temel fark, şifrenin kırılmasındaki zorluktur. Klasik şifrelemeleri kırmak son derece zordur; kuantum kriptografi şifrelemelerini kırmak teorik olarak imkansızdır. Kuşkusuz kuantum kriptografi uygulamaları hesaplamasal (*computationally*) olarak pahalıdır ve "doğru" olması daha zordur. Bu nedenlerle, klasik kriptografi günümüz uygulamalarında hala baskındır.

İş Güvenlik Uygulamaları

Güvenlik ürünlerinin ve hizmetlerinin genel sınıflandırmasının bir değerlendirmesi aşağıdaki gibidir:

- Kimlik denetleme (PKI olmayan)
- Erişim denetimi/yetkilendirme
- Değerlendirme ve denetleme
- Güvenlik yönetimi ürünleri
- Perimetre/ağ güvenliği/kullanılabilirlik
- İçerik filtreleme
- Şifreleme
- Yönetim/eğitim
- Dış kaynak (outsource) hizmetler/danışmanlar

Bu ürünleri ve hizmetleri daha önce bahsedilen bilgi güvenliği hedefleri ile eşlediğinizde, hangi iş araçlarının ve hizmetlerinin hangi güvenlik amaçlarını karşıladığını görebilirsiniz. Daha sonra, kriptografinin bu hedeflerden hangilerini ele alabileceğini anlayabilirsiniz. **TABLO 9-2**, güvenlik ürünlerinin ve güvenlik hedeflerinin birbiriyle nasıl bağlantılı olduğunu göstermektedir.

Gördüğünüz gibi birçok güvenlik hedefine ulaşmak için şifreleme kullanabilirsiniz. Kriptografi, özellikle aşağıdaki yetenekleri sunmaktadır:

- **Mahremiyet ya da gizlilik**—Kriptografi, bilgileri yalnızca doğru bir şifrelemeye ve anahtara sahip bir kişi tarafından okunmasını sağlayacak şekilde karıştırmaktadır. Bu kişinin akıllı bir kriptanalist olabileceğini unutmayın.
- **Bütünlük**—Kriptografi, sağlama toplamlarını veya özetleri sağlayarak bütünlüğü korur. Verilerin değişmediğini kanıtlamak için bu değerleri bilinen bir gerçek değerler tablosuyla karşılaştırabilirsiniz.
- **Varlık kimlik denetleme ya da tanımlama**—Birinin bir mesajı kodlama veya çözme yeteneği, bu kişinin kriptografik anahtara sahip olduğu veya anahtarı hesaplama yeteneğine sahip olduğu anlamına gelir. Eğer bir iş ilişkisi bu anahtarın gizli kalmasını gerektiriyorsa, sahiplik geçerli bir kimlik kanıtıdır.
- **Mesaj doğrulama**—Varlık kimlik denetlemesine benzer şekilde, özel bir anahtar ile kodlanmış bir mesaj, mesajı yazanın kim olduğunu kanıtlar. Ayrıca, bu şart, herhangi bir iş sözleşmesinin veya resmi ilişkinin bir parçası olmalıdır.
- **İmza**—Kriptografi, dijital imza oluşturmanın bir yolunu sağlayabilir. Bu, belirli bir kişinin belirli bir mesajı gönderdiğini kanıtlayabilir.
- **Erişim denetimi**—Erişim denetimi, ayrıcalıklı kaynakların ve verilerin şifrelenmesini ve böylece sadece yetkilendirilmiş kişilerin bu kaynakların ve verilerin şifrelerini çözmesini ve bunlara erişmesini yürütmektedir.
- **Sertifikasyon**—Güvenilir bir varlık, kriptografik bir sağlama toplamı ve dijital imza ekleyerek bir mesajı veya verileri onaylayabilir.
- **Zaman damgası**—Asimetrik anahtar şifrelemesini kullanarak, güvenilir bir aygıt, saldırganların oluşturamayacağı zaman damgaları verebilir. Zaman damgası, zaman damgalı bilgilerin bir özetini güvenli, güvenilir bir saatin çıktısı ile birleştirir.
- **Tanıklık**—Üçüncü bir taraf, verinin belirli bir zamanda belirli bir formatta var olduğunu kanıtlamak için veriye kriptografik bir sağlama toplamı ekleyebilir.
- **Sahiplik**—Sahiplik, bir sahip tarafından oluşturulan ve verilere eklenen, daha sonra doğrulama için güvenilir bir üçüncü tarafa gönderilen kriptografik bir özet anlamına gelir. Bu, bir varlığı verinin sahibi olarak tanımlar.

TABLO 9-2 Güvenlik hedefleri ve güvenlik ürünleri.

HEDEF	KİMLİK DENETİMİ	ERİŞİM DENETİMİ	DEĞERLENDİRME VE DENETLEME	GÜVENLİK YÖNETİMİ	AĞ GÜVENLİĞİ	İÇERİK FİLTRELEME	ŞİFRELEME	YÖNETİM	DANIŞMANLAR
Mahremiyet veya Gizlilik		X			X		X	X	X
Bütünlük				X	X		X	X	X
Varlık kimlik denetleme veya tanımlama	X	X			X		X	X	X
Mesaj doğrulama	X				X		X		
İmza	X				X		X	X	
Yetkilendirme	X	X			X				
Onaylama		X	X	X				X	
Erişim denetimi	X	X		X	X	X	X	X	
Sertifikasyon			X	X			X		X
Zaman damgası		X			X		X		
Tanıklık			X				X		X
Alındı					X			X	
Onaylama					X			X	
Sahiplik			X				X	X	X
Anonimlik							X	X	
İnkar edememe					X		X	X	X
İptal etme	X				X		X		

- **Anonimlik**—Kriptografiyi kullanarak, bilgiyi şifrelenmiş olarak ileterek gözlemleyicilerin yorumlayamayacağı bir biçimde bir varlığın kimliğini gizleyebilirsiniz. Ayrıca, bir dizi şifrelenmiş atlama (*hop*) kullanarak ve günlüklerden (*log*) kurtularak, internet üzerinde anonim görünüşe sahip bir varlık sağlanabilir.
- **İnkar edememe**—İş ilişkisinin bir parçası olarak kabul edilen verilerin asimetrik bir anahtar imzası, gönderenin kimliğini alıcıya kanıtlayabilir.

Şifreleme Türleri

Şifrelemeler iki temel biçimdedir:

- **Yer değiştirme (*transposition*) şifrelemeleri** - Bir **yer değiştirme şifrelemesi,** verinin karakterlerini veya bitlerini yeniden düzenler.
- **Yerine koyma (*substitution*) şifrelemeleri** - Bir **yerine koyma şifrelemesi,** bitleri, karakterleri veya bilgi bloklarını diğer bitlerle, karakterlerle veya bloklarla değiştirir.

Yer Değiştirme Şifrelemeleri

Basit bir yer değiştirme şifrelemesi, karakterleri bir matristeki satırlara yazar. Daha sonra sütunları çıktı olarak okur. Örneğin, "ATTACK AT DAWN" mesajını, **ŞEKİL 9-2**'de gösterildiği gibi dört sütunlu bir matrise yazın.

Daha sonra, sütunlardaki bilgiyi okuyun: ACDTKATAWATN. Bu şifreli metin olacaktır. Anahtar, sütunların okunduğu sıra olan {1,2,3,4} olacaktır. Örneğin, {2,4,3,1} gibi başka bir anahtarla şifrelemek, farklı bir şifreleme metniyle sonuçlanacaktır - bu örnek için, TKAATNTAWACD.

Bu örnekte, şifreli metnin harf sıklığını (frekansını) içerdiğini unutmayın. Bunun nedeni, İngilizce'deki en yaygın harfler olan — E, T, A, O ve N — yer değiştirme uygulanmış şifreli metinde fazlaca görünür. Bu, kriptanalist için bunun bir yer değiştirme şifrelemesi olduğuna dair bir ipucudur.

Yer değiştirme şifrelemeleri, orijinal mesajın tüm öğelerini korur. Bu şifreleme, bilgiyi sadece daha sonra tekrar birleştirebileceği şekilde karıştırır. Bazı temel dijital yer değiştirme şifrelemeleri, verilerin sıradan okuyucu tarafından anlaşılmaz görünmesini sağlamak için bayt içindeki bitleri değiştirir. Belirtilen bu yer değiştirme şifrelemesinin bir örneği bozuk Latince[1]'dir.

Yerine Koyma Şifrelemeleri

En basit yerine koyma şifrelemelerinden biri **Sezar şifrelemesidir (*Caesar cipher*)**. Alfabedeki her harfi sabit bir sayıdaki pozisyona kaydırır, Z'den A'ya geri sarılır. Julius Caesar, bu şifrelemeyi 3 kaydırma ile kullanmıştır. Aşağıda, bir Sezar şifrelemesi kullanılarak yapılan bir şifreleme gösterilmektedir[2]:

ATTACK AT DAWN

↓

DWWDFN DW GDZQ

Sezar şifrelemesi için 25 olası anahtar olduğuna dikkat edin. (26. anahtar, karakterleri kendilerine eşler.) Ayrıca, bunun bir yer değiştirme şifrelemesi olmadığına da dikkat edin çünkü şifreleme metnindeki harfler düz metin içinde mevcut değildir.

Cap'n Crunch © kod çözücü halkası, 1960'larda çocuklar için popüler bir yerine koyma şifresiydi. Halka, özel olarak işaretlenmiş Cap'n Crunch mısır gevreği kutularının içerisindeydi. Bu halka,

ŞEKİL 9-2
Bir yer değiştirme şifrelemesi.

1	2	3	4
A	T	T	A
C	K	A	T
D	A	W	N

[1] Ç.N. Pig Latin veya Igpay Atinlay olarak bilinen, kuş dili benzeri İngilizce dilinde oynanan bir oyundur. Oyun birinci kelimenin sonuna kelimenin ilk harfi ve "ay" getirilerek oynanır. Örneğin, pig = igpay, latin = atinlay

[2] Ç.N. Bu örnekte ve bölümdeki diğer tüm örneklerde İngilizce alfabe kullanılmaktadır. İngilizce alfabe 5 tanesi sesli, 21 tanesi sessiz olmak üzere toplam 26 harften oluşur: A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z.

bir daire içine yazılmış iki alfabeden (A'dan Z'ye) oluşuyordu. İç daireyi hareket ettiremiyor ancak dış daireyi döndürebiliyorsunuz. Dış daireyi ayarlanan bir değere döndürerek, bir alfabeden diğerine bire bir bir eşleme oluşturdunuz. Şifrelemek için, iç çemberdeki istediğiniz karakteri araştırdınız ve dış çemberdeki karakteri okudunuz. Şifresini çözmek için işlemi tersine çevirdiniz. (Evet, bu bir Sezar şifresi!)

Bir **anahtar kelime karıştırılmış alfabe şifrelemesi (*keyword mixed alphabet cipher*)**, bir anahtar kelimeden, tekrar eden harflerin çıkarılmasının ardından alfabenin geri kalan harflerinden oluşan bir alfabe şifrelemesini kullanır. Örneğin, CRYPTOGRAPHY anahtar kelimesini kullanarak gerçekleştirilen bu tür şifreleme aşağıdakileri verecektir:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

↓

CRYPTOGAHBDEFIJKLMNQSUVWXZ

Böylece, ALPHABET düz metin sözcüğü CEKACRTQ olarak şifrelenecektir.

Herhangi bir yerine koyma şifrelemesi, karmaşıklığı ne olursa olsun, bu temel ilkeleri kullanacaktır. Bu kodları kırmayı zorlaştırmak için, art arda çoklu şifreleme şeması kullanabilirsiniz. Örneğin, her harfi kendi yerine koyma şemasıyla şifreleyebilirsiniz. Bu bir **Vigenère (*vee-zhen-AIR*) şifrelemesidir**. Her biri kendi kaydırma karakterine sahip çoklu Sezar şifrelemesi gibi çalışmaktadır. Örneğin, beş Sezar şifrelemesi kullanan PARTY'i anahtar olarak kullanabilirsiniz. Alfabedeki her karakterin 1 ile 26 arasında bir değere sahip olduğunu bilerek, şifreli karakteri, düz metin karakterinin değerini anahtarda karşılık gelen ilgili karakterin değerine ekleyerek hesaplayabilirsiniz. Toplam 26'dan büyükse, son değeri bulmak için 26'yı çıkarmanız yeterlidir. ATTACK AT DAWN TOMORROW mesajını şifrelemek için aşağıdakiler geçerli olacaktır:

Düz metin:	ATTACKATDAWNTOMORROW
Anahtar (düz metin uzunluğuyla eşleşmesi için tekrarlanmaktadır):	PARTYPARTYPARTYPARTYPA
Şifreli metin (anahtar kullanılarak kaydırılan karakterler):	PTKTAZAKWYLNKHKDRIHU

Bu, daha fazla güvenlik sağlar. Çıktı, çok daha rastgele görünmektedir. Anahtar uzunluğunun arttırılması genellikle yerine koyma şifrelemesinin güvenliğini arttırır.

Her harfi belirli bir sayıda pozisyon değiştirmek yerine, bir harfin başka bir harfle tek bir şekilde eşleşmesine izin vererek yerine koyma şifrelemesinin karmaşıklığını artırabilirsiniz. **Basit bir yerine koyma şifrelemesi** adı verilen bu tür şifrelemeyi, birçok gazetede **kriptogram (*cryptogram*)** adı verilen bir bulmaca olarak bulabilirsiniz. Bu durumda, A harfi 26 harften herhangi biriyle eşleşebilir, B kalan 25 harften herhangi biriyle eşleşebilir, C 24 harfe eşlenebilir, vb. Bu nedenle, kullanabileceğiniz (26 faktöriyel) veya 403.291.461,126,606,000,000,000,000 olası anahtar vardır. Buna rağmen, bu bulmacaları kırmak basit bir iştir. Bu önemli bir noktayı göstermektedir: Karmaşıklığı asla güvenlikle karıştırmamalısınız.

Bir yerine koyma şifrelemesinin güvenli olduğundan emin olmak için üç şey yapmalısınız. İlk olarak, anahtarın tekrarlamayan rastgele bir sırada olduğundan emin olun. İkincisi, anahtarın şifrelenmiş bilgi kadar uzun olduğundan emin olun. Üçüncüsü, anahtarı sadece bir kez kullanın. Böyle bir şifreleme tek kullanımlık şifrelemedir (*one-time pad*). Bu stratejinin ilk kullanımı, AT&T çalışanı Gilbert Vernam tarafından yapılan tasarımı temel alan bilgisayar sistemleridir. Bir Vernam şifrelemesi, düz metinle birleştirilmiş, sıfırlardan ve birlerden oluşan bir bit akışını (bit stream) XOR

(dışlamalı OR) fonksiyonunu kullanarak oluşturur. XOR işlemi, girişlerden biri ve yalnızca biri doğru olduğunda doğrudur. ⊕ olarak gösterilen XOR fonksiyonu aşağıdaki özelliklere sahiptir:

$0 \oplus 0 = 0$

$0 \oplus 1 = 1$

$1 \oplus 0 = 1$

$1 \oplus 1 = 0$

Bunun ≠ (eşit değil) fonksiyonuna eş değer olduğunu unutmayın. Bu yaklaşımı kullanarak, şifreli metin üretmek için bir ikili veri akışını ikili bir anahtar akışı (*keystream*) (bir anahtardaki karakterlerin akışı) ile birleştirebilirsiniz. Donanım veya yazılım, modern yerine koyma şifrelemelerini bu şekilde kullanmaktadır.

Birleşik ve Üssel Şifreleme

Bir **birleşik şifreleme (*product cipher*)**, çok sayıda şifrelemenin birleşimidir. Her biri bir yer değiştirme veya yerine koyma şifrelemesi olabilir. Veri Şifreleme Standardı (*Data Encryption Standard* - DES), 56-bit bir anahtar ile yerine koyma ve değiştirmenin 16 yinelemesinden oluşan sahip bir birleşik şifrelemedir. İlk olarak 1977'de Federal Bilgi İşleme Standardı (*Federal Information Processing Standard* - FIPS) olarak yayınlanan DES hala kullanılmaktadır. DES'in geliştiricileri, DES'in yüksek güvenlikli olduklarını düşündüler çünkü 1977'de mevcut bilgisayarların şifreli bir mesajı kırması 90 yıldan fazla zaman alırdı. Birçok sivil özgürlükçü ve komplo teorisyeni ve ayrıca profesyonel kriptograf, tasarımcıların DES'e, Ulusal Güvenlik Ajansı'nın (*National Security Agency* - NSA) mesajların şifresini kolayca çözebilmesi için algoritmada arka kapı açmasına izin veren bazı zayıf yönler getirdiğini düşünüyor. Ancak, 25 yıldan uzun bir süre sonra hiç kimse böyle bir zayıflık bulamadı. Kriptografideki ilerlemeler - büyük miktardaki şifreli metinde örüntüleri aramayı içeren **diferansiyel kriptanaliz (*differential cryptanalysis*)** dahil olmak üzere - aslında DES tasarımının ilk şüphelendiğinden daha güvenli olduğunu gösteriyor. Bununla birlikte, bilgisayar gücündeki gelişmeler 56 bitlik anahtar uzayını (72,057,594,037,927,900 anahtar) arama yapmak için daha az korkutucu hale getirmiştir. Sonunda, Elektronik Öncü Vakfı (*Electronic Frontier Foundation*) 1998 yılında, üç günden daha kısa bir sürede anahtar uzayını arayabilen Deep Crack adlı özel-amaçlı bir bilgisayar geliştirdi. Bu bölümün ilerleyen kısımlarında DES hakkında daha ayrıntılı bilgilendirileceksiniz.

Bazı şifrelemeler, bazı matematik problemlerinin çözülmesindeki zorluğa dayanmaktadır. Asimetrik anahtar kriptografisinin temeli budur. Bu şifrelemeler **alan teorisi (*field theory*)** olarak bilinen bir matematik dalını kullanır. Çok fazla matematiğe girmeden, bir **alan**, 0 dışındaki her öğenin çarpımsal bir terse sahip olduğu sayıların herhangi bir etki alanıdır. Örneğin, bütün rasyonel sayılar bir alan oluşturur. Verilen $x \neq 0$ için her zaman $1/x$'i hesaplayabilirsiniz. Alanların sonsuz olması gerekmez. Sonsuza kadar saymak yerine, belirli bir değere ulaştıktan sonra saymayı yeniden başlatabilirsiniz. Örneğin, Amerika Birleşik Devletleri'nde insanlar saati, 12 saatlik bir zamanla belirtir. Saat 10:00'dan bir saat sonrası 11:00'dir, ancak saat 12:00'den bir saat sonrası 13:00 değil 1:00'dir. Pek çok ülke 24 saatlik zaman kullanıyor, ancak tamamlama etkisi aynıdır. Bir kümedeki tam sayıların sayısı asal olduğunda işler matematiksel olarak ilginçleşmektedir. 1'den asal sayıya kadar olan tam sayılar kümesi sonlu bir alanı temsil eder.

Üssel şifreleme, bir sonlu matematiksel alan üzerinde üstelleri hesaplamayı içerir. **Rivest-Shamir-Adelman (RSA)** şifreleme şeması, çok büyük sayıların çarpanlarına ayrılmasındaki zorluğa dayanır. İki sayının çarpımı basittir, ancak çok büyük bir sayıyı çarpanlarına ayırmak çok zordur. Bu işlemin detaylarını bu bölümün ilerleyen kısımlarında daha sonra öğreneceksiniz.

Simetrik ve Asimetrik Anahtar Kriptografisi

Bu bölümde, simetrik ve asimetrik anahtar kriptografisi arasındaki farklar ve her ikisinin de karşılaştırmalı avantajları ve dezavantajları hakkında daha fazla bilgi edineceksiniz.

Simetrik Anahtar Şifreleme

Simetrik anahtar şifreleme, şifreleme ve şifre çözme için aynı anahtarı kullanır. Sonuç olarak, her iki tarafın da iletişim kurmak için öncelikle karşılıklı anahtar değiş tokuşunda bulunmaları gerekmektedir. Bu durum, bu tür kripto sistemleri için temel bir sınırlamayı belirtmektedir. Başka bir tarafa mesaj göndermeden önce, anahtarların değişimini yapmak için önce güvenli bir şekilde konuşmanız gerekmektedir. Bu tavuk ve yumurta problemi geçmişte kriptografiyi, hükümetler, ordu ve iyi finanse edilmiş kişiler hariç, büyük ve dağınık olan herhangi bir organizasyon için zorlaştırdı.

Bu sorunu örneklemek için karşılıklı yazışma yapan iki kişinin, Alice ve Bob'un, güvenli bir şekilde bilgi değişiminde bulunmak istediğini düşünün. Bu senaryoda, Alice ve Bob ABC Şirketi için çalışıyor. Yeni bir müşteri olan MNO Plastik'e bir teklif için fiyat bilgisi değişiminde bulunmak istiyorlar. Bob, müşteri tarafındadır ve şirketin iç ağına erişememektedir. Tüm bilgiler internet üzerinde gelip gitmek zorundadır.

Eva, ABC'nin deniz aşırı bir rakibi için çalışmaktadır. Görevi, ABC'nin teklifi ve açık arttırma hakkında mümkün olduğunca fazla istihbarat toplamaktır. Görevine ulaşmak için, her türlü iletişimi izleme, bozma ya da maskeleme/taklit etme yetkisine sahiptir. Buradaki aşikar olan yasal konular, tartışmanın anlaşılması için bir kenara bırakılabilir. Eva'nın, Bob'un tüm iletişimini (gelen ve giden mesajları) izleyebildiğini varsayın. Bob'un gönderdiği veya aldığı tüm mesajlar, Eva'nın kontrol ettiği bir uçtan (*node*) geçmektedir.

Problem şudur: Alice ve Bob, önceden herhangi bir şey üzerine anlaşmadıysalar güvenli bir iletişim oturumunu nasıl yaratırlar? Diyelim ki Alice ve Bob, bilgilerini şifrelemek için DES'i kullanmaya karar verdiler. DES kamuya açık bir algoritma olduğundan, Eva DES yazılımının bir kopyasını yükleyebilir. Alice, Bob'a BIGBUCKS'ı anahtar olarak kullanması için bir mesaj gönderir. Bob bu kararı kabul eder ve şifreli mesajını bu anahtarı kullanarak Alice'e gönderir. İletişimi dinleyen Eva, Bob'un mesajının şifresini çözmek için aynı anahtarı kullanır ve Bob'un bilgilerini kendi şirketine gönderir.

Alice ve Bob, anahtarları çok sayıda değiştirmeyi kabul edebilir, ancak her değiştirdiklerinde, Eva bu anahtar değişikliğini öğrenir ve buna göre ayarlanır. Simetrik anahtar kriptografisi kullanarak bu problemin üstesinden gelinemez. Her bir taraf diğerinin hangi anahtarı kullandığını bilmek için diğer tarafla anahtar değişimi yapmalıdır. Bir anahtarı özel amaçlı bir anahtarla veya bir **anahtar şifreleme anahtarıyla (*key-encrypting key*)** şifreleseniz bile, bir noktada anahtar şifreleme anahtarını değiş tokuş yapmanız gerekir. Anahtar şifreleme anahtarları, yalnızca diğer anahtarları şifrelemek için kullandığınız anahtarlardır. Anahtar şifreleme anahtarlarını değiş tokuş yapmak, bir saldırganın siz anahtarı değiş tokuş yaptığınızda anahtar şifreleme anahtarını engellemesi (*intercept*) anlamına gelir.

Bu ikilemin çözümü, Eva'nın izleyemediği farklı bir yolda ilerleyen bir mesaj gerektiriyor. Bu, güvenli bir kanal kullanan bant dışı iletişimdir (*out-of-band communication*). Diyelim ki bu durumda Alice ve Bob, DES'i kullanmayı kabul ediyor ve Alice, Bob'a onu cep telefonundan aramasını ve hangi anahtarı kullanmak istediğini söylemesini belirtiyor. Tüm internet trafiğini okuyabilen Eva, cep telefonlarını izleyemiyor. Alice ve Bob 56-bitlik bir anahtar üzerinde anlaşır ve bilgi değişimine başlarlar. Eva döngü dışındadır. Elbette, Bob iş gezisine çıkmadan önce, Alice ve Bob belirli bir anahtar kullanmayı kabul etmiş olabilirler. Bu da bant dışı iletişimdir. Bu, mesaj göndermek ve almak için kullanılan iletişim kanalı dışında gerçekleşir.

ABC Şirketi'nin şimdi yapması gereken bir seçim var. Tüm çalışanlara aynı anahtarı verebilir, bu da yazışmaları kolaylaştırır. Herhangi bir çalışan, dünyadaki herhangi bir diğer çalışanla güvenli bir şekilde iletişim kurabilir. Bu model, hoşnutsuz bir çalışan anahtarı alıp işten ayrılına ve rakip bir firma ile anlaşana kadar iyi çalışır. Şimdi ne olacak? ABC'nin yeni bir anahtar oluşturması ve yeni anahtarı dünya çapındaki herkese vermesi gerekir. Bu zaman alıcı ve pahalı olabilir.

Bunun yerine, ABC tek bir aksama noktasının kabul edilemez olduğuna karar verebilir ve her çalışana ayrı anahtar verebilir. Ancak, her iki tarafın da aynı anahtarı simetrik anahtar şifrelemeleriyle kullanması gerektiğinden, her çalışan-çalışan çiftinin kendi özgün anahtarına sahip olması gerekir. Bu nedenle, eğer 10 çalışan olsaydı, ABC'nin bu şemaya başlaması için 45 anahtar çiftine (9 + 8 + 7 + 6 + 5 + 4 + 3 + 2 + 1) ihtiyacı olacaktır. ABC'nin 100 çalışanı olsaydı, 4.950 anahtar çiftine ihtiyacı olacaktır. ABC'nin 10.000 çalışanı olsaydı, 49.995.000 anahtar çiftine ihtiyacı olacaktır! *n* yazışma yapan taraf için gereken anahtar çifti sayısı (*n* (*n* - 1)) / 2'dir. Ayrıca, bir çalışan şirkete her katıldığında veya ayrıldığında, diğer çalışanların her biri için bir anahtar çifti eklemek veya silmek zorunda kalırsınız. Açıkçası, simetrik anahtar sistemleri iyi ölçeklenemezler.

Bu, 1976 yılında Whitfield Diffie ve Martin Hellman'ın *IEEE Bilişim Teorisinde İşlemler (IEEE Transactions on Information Theory)* dergisinde "Kriptografide Yeni Yönergeler (*New Directions in Cryptography*)[3]" başlıklı makalelerini yayınlamalarına kadar kriptologlar (ve hükümetler, ordular ve işletmeler) için anlaşılmaz bir sorun olarak kaldı. Diffie ve Hellman bu makalede, ölçeklenebilirlik problemine potansiyel bir çözüm sunan yeni bir radikal yaklaşım önerdiler.

Asimetrik Anahtar Şifreleme

Diffie ve Hellman, makalenin giriş bölümünde, "Bu anahtar dağıtım probleminin getirdiği maliyetin ve gecikmenin, işletme iletişimlerinin büyük uzaktan işleme ağlarına (teleprocessing networks) aktarılmasında büyük bir engel" olduğunu belirtmektedir. Diffie ve Hellman, **kamusal anahtar kriptografisi (*public key cryptography*)** kavramını tanıttı. (Bu metinde, bu kavramın *asimetrik anahtar kriptografisi (asymmetric key cryptography)* olarak belirtildiğini unutmayın.) Kamusal anahtar kriptografisi, karşılıklı yazışan tarafların yalnızca kamusal olarak bilinen teknikleri kullanarak, bir kamusal kanal üzerinden iletişim kurmasını sağlayan bir sistemdir. Taraflar, güvenli bir bağlantı oluşturabilirler. Bant dışı bir mektup zarfın içinde bir anahtarla gelene kadar beklemelerine gerek yoktur. Tarafların ayrıca, birisinin yeni bir taraf ile güvenli bir şekilde iletişim kurmak istemesi durumunda milyonlarca anahtar çifti yayınlamaları ve bu anahtar çiftlerini yönetmeleri gerekmez. Bu bulgunun etkisi kriptografi üzerinde temel ve geniş kapsamlı sonuçlara sahiptir.

Asimetrik anahtar şifrelemeler dört temel özelliğe sahiptir:

- **Birbirinin tersi olan iki ilişkili algoritma vardır**—Bu çözüm birbiriyle ilişkili iki bileşeni içerir. Bu, şifrelemek için bir algoritmayı ve şifreyi çözmek için ise diğer algoritmayı kullandığınız anlamına gelir.
- **Bu iki algoritmanın her birinin hesaplanması kolaydır**—Bu yaklaşımı bilgisayar yazılımında çok fazla zorluk çekmeden kullanabilirsiniz. Sonuç olarak, güvenli dijital iletişim için pratik bir yaklaşım haline gelir.
- **İlk algoritmayı biliyorsanız, ikinci algoritmayı türetmek hesaplamalı olarak imkansızdır**—Bir anahtarı, ilişkili olduğu anahtarın içeriğinden ödün vermeden kullanması için herhangi birine gönderebilirsiniz. Bunlar kamusal bir anahtarın ve bu anahtarın ilişkili olduğu özel anahtarın çiftidir veya bir kamusal özel anahtar çiftidir. Kamusal anahtar kripto

[3] Ç.N. *W. Diffie ve M. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory, 22(6): 644-654, Kasım 1976.* İlgili makaleye https://ee.stanford.edu/~hellman/publications/24.pdf adresinden ulaşıp okuyabilirsiniz.

sistemleri özel anahtarlara sahip olduğundan, bu bölümün neden asimetrik anahtar adlandırma kuralına bağlı kaldığını görebilirsiniz!

- **Bazı rastgele girdiler dikkate alındığında, birbirlerinin tersi olan ilişkili anahtar çiftleri oluşturabilirsiniz**—Herhangi bir taraf kamusal özel anahtar çiftleri oluşturabilir, bir tanesini özel tutabilir ve diğerini herhangi bir tarafın kullanması için bir dizine (*directory*) gönderebilir. Özel anahtar gizli olduğundan ve hiçbir zaman iletilmediğinden, gizli bir şekilde dinleme yapan biri bu değeri öğrenemez.

Kamusal anahtar kriptografisi şu şekilde çalışır: Bob'un Alice'e bir mesaj göndermek istediğini varsayalım. Alice, güvende tuttuğu özel anahtarını ve web sitesine koyduğu kamusal anahtarını önceden yaratmıştır. Bob, "Merhaba Alice!" mesajını şifrelemek için Alice'in kamusal anahtarını kullanır. Bob daha sonra şifreli mesajı Alice'e gönderir. Bob, mesajı şifrelemek için Alice'in kamusal anahtarını kullandığı için, Alice yalnızca kendi özel anahtarıyla mesajın şifresini çözebilir. Alice'in kendi özel anahtarına erişimi olduğu için, anahtarı mesajın şifresini çözmek ve "Merhaba Alice!" mesajını okumak için kullanır. Alice, Bob'un mesajına cevap vermek isterse, yanıtını Bob'un kamusal anahtarı ile şifreler ve mesajı Bob'a geri gönderebilir.

Gündelik iş dünyasında asimetrik anahtar şifrelemelere en yakın eş değerlerden biri, bir bankadaki gecelik kasadır. Bir tüccar makbuzlarını bankaya götürür, deliği anahtarıyla açar ve parayı oluktan aşağıya bırakır. Zarf aşağı ve kasanın içine doğru kayar. Arkasını döndüğünde ve bir hırsız ona silah doğrulttuğunda ve anahtarını talep ettiğinde, tüccar anahtarı güvenle teslim edip kaçabilir. Soyguncu parayı geri almaya çalışabilir ancak zarf erişilemeyen bir yere düştüğünden, soyguncu zarfa erişemeyecektir. Ertesi sabah banka memuru, kasayı açmak, parayı almak ve tüccarın hesabına yatırmak için anahtarını kullanabilir. Her tarafın farklı bir anahtarı vardır ancak birbirleriyle ilişkilidirler. Bu işlemi banka memurunun tüccara mesajlar bırakabileceği şekilde tersine çevirdiğinizde, asimetrik veya kamusal anahtarlı kripto sistemine sahip olursunuz.

Kriptanaliz ve Kamusal'a Özel Anahtarlar

Şifreleme, düz metni, doğru yazılım ve anahtarla yetkilendirilmiş bir kişi dışındaki herkese okunamaz bir hale getirir. Ancak, veriler değerliyse, siber suçlular şifrelemeyi kırmaya çalışabilir.

Bir şifreyi iki şekilde kırabilirsiniz:

- Düz metni veya anahtarı bulmak için şifreli metni analiz etme
- Anahtarı bulmak için şifreli metni ve şifreli metnin ilişkili olduğu düz metni analiz etme

Hiçbir miktardaki şifreli metin, özgün bir düz metin elde etmek için yeterli bilgiyi vermezse, şifreleme koşulsuz olarak güvenlidir (*unconditionally secure*). Yeterli zaman ve kaynaklar verildiğinde, neredeyse tüm şifrelemeleri kırılabilirsiniz. Ancak bir şifrelemenin temel amacı, şifrelemenin kırılmasını zorlaştırarak kırılmasını hesaplamasal olarak imkansız (*computationally infeasible*) yapmaktır. Örneğin, bir kuruluşun her hafta yeni anahtarlar ürettiğini

TEKNİK İPUCU

Kırılmaz tek kriptografik şifreleme **Vernam şifrelemesi**dir. Bu şifrelemenin diğer bir ismi **tek kullanımlık şifrelemedir (one-time pad)**. Bu bölümde daha sonra bununla ilgili daha fazlasını okuyacaksınız. Vernam şifresi hakkında daha fazla bilgiyi *www.pro-technix.com/information/crypto/pages/vernam_base.html* adresinde bulabilirsiniz.

varsayalım. Bir saldırgan 13 gün içinde herhangi bir anahtarı kırabilirse, kırılan anahtarlar saldırgan kullanmaya çalıştığında işe yaramaz olur; anahtar zaten yeni bir anahtarla değiştirilmiş olurdu. Bu nedenle, bir saldırganın ekonomik olarak kıramayacağı bir şifre (korunan verilerin değerine göre) güçlüdür veya hesaplamasal olarak güvenlidir (*computationally secure*).

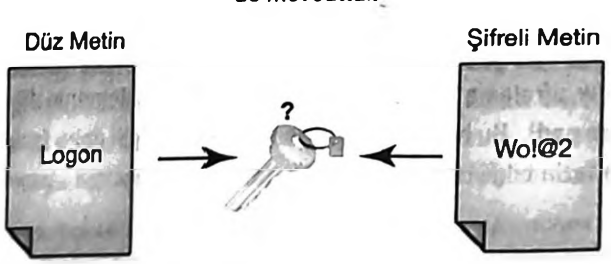
Dört temel kriptografik saldırı şekli vardır:

- **Sadece şifreli metin saldırısı (*Ciphertext-only attack* - COA)** – Sadece şifreli metin saldırısında, kriptanalist yalnızca şifreli verinin bir bölümüne erişebilir ve bu verilerin hangisi olabileceği ile ilgili olarak hiçbir seçeneğe sahip değildir. Bazı günlük gazetelerdeki kriptogram buna örnektir. Ancak, kişi bilginin içeriğini anlayarak, belirli kelimeleri veya var olan biçimlendirmenin şeklini çıkarabilir. **ŞEKİL 9-3**, sadece şifrelenmiş metin saldırısını göstermektedir. Burada, şifreli metnin bir örneği mevcuttur ancak şifreli metin ile ilişkili düz metin mevcut değildir.
- **Bilinen düz metin saldırısı (*Known-plaintext attack* - KPA)** – Bilinen düz metin saldırısında, kriptanalist, şifreleme öncesi ve sonrasında belirli bilgi parçalarına sahiptir. Örneğin, tüm güvenli oturum açmalar LOGON karakterleriyle başlayabilir ve bir sonraki aktarım ŞİFRE olabilir. Güvenli bir şifreleme, çok sayıda düz metin şifreli metin çiftine erişimi olan bir analistin saldırısına karşı direnmelidir. **ŞEKİL 9-4**, bir bilinen düz metin saldırısını göstermektedir.
- **Seçilmiş düz metin saldırısı (*Chosen-plaintext attack*)** – Seçilmiş düz metin saldırısında, kriptanalist herhangi bir bilgiyi şifreleyebilir ve çıktıları gözlemler. Kriptanalist için en iyi durum budur. Bu saldırı, şifreleme düzeneğine en fazla esnekliği (ve kavrayışı) sunar. Microsoft Office yazılım uygulamalarının eski sürümleri tarafından sunulan şifreleme buna bir örnektir. Şifrelemenin ne yaptığını anlamak için önce sadece A harfini, sonra B harfini ve buna benzer şekilde diğerlerini şifreleyebilirsiniz.

ŞEKİL 9-3
Sadece şifreli metin saldırısı (COA)



ŞEKİL 9-4
Bilinen düz metin saldırısı (KPA)



- **Seçilmiş şifreli metin saldırısı (Chosen-ciphertext attack)**—Seçilmiş şifreli metin saldırısı özel bir durumdur. Bu saldırı, asimetrik anahtar sistemlerinde ve özet fonksiyonlarında uygulanmaktadır. Seçilmiş şifreli metin saldırısında, kriptanalistler, düz metin çıktısını veya şifresi çözülmüş metnin bazı sistemler üzerindeki etkisini görmek için aynı şifreleme algoritması ve kırmaya çalıştıkları anahtar ile şifrelenmiş verileri şifre çözme cihazına gönderir. Basit bir örnek olarak, yalnızca Navahoca (*Navajo*)[4] söylenen komutlara cevap vermek için bir bekçi köpeği yetiştiren bir sahibi düşünün. Bir hırsız Navahoca bilmiyor ama bir dizi gürültü ve ses çıkarabiliyor. Köpek anlamsız sözleri (kendi perspektifinden) görmezden geliyor ama geçerli emirlere uyuyor. Yeterince saçma bir konuşma yapan hırsız, köpekten bir cevap isteyebilir (aradığı cevap olmasa bile). Köpeğin görünüşte saçma sapan olan çeşitli komutlara tepkisini gözlemleyerek, hırsız köpeğin yere yatmasını ve ölü numarası yapmasını sağlayabilir. Seçilmiş şifreli metin saldırılarının, şifreli e-postalara saldırmak için özel kullanımları vardır. İlgili matematiğin karmaşıklığı, burada tartışmak için çok büyüktür.

Simetrik ve Asimetrik Anahtar Şifrelemenin Saldırı Direnci

Kriptanalizin aşağıda belirtilenleri içeren çeşitli amaçları vardır:

- Hedef mesajın düz metnini elde etmek.
- Hedef mesajı şifrelemede kullanılan anahtarı belirlemek.
- Belirli bir şifreleme tarafından kullanılan algoritmayı elde etmek.
- Kriptografinin altında yatan genel matematik problemini çözmek.

Kriptograflar kriptanalizde birçok araç kullanırlar. Bunların, doğrusal kriptanaliz, diferansiyel kriptanaliz, kaba kuvvet (*brute force*), ayrıntılı arama ve bilgi teorisi gibi isimleri vardır. En dolaysız durumda, analist, ilişkili düz metnini elde etmek için şifreli bir mesaj kullanmalıdır. Bugün kullanılan birçok şifreleme açık kaynaktır. Bu, analistin şifreleme ve şifre çözme fonksiyonlarına yönelik mantığa erişimi olduğu anlamına gelir. Kapalı kaynak veya tescilli şifrelemelerin güvenliği, analistin mutlaka şifrelemenin nasıl çalıştığını bilmesi gerekmediği gerçeğinden kaynaklanmaktadır.

Örneğin, Amerika Birleşik Devletleri'nin, II. Dünya Savaşı'nda bir Japon Mor şifreleme cihazına erişimi yoktu. Kod kırıcılar, şifreli metindeki soluk desenleri analiz ederek makinenin nasıl çalıştığını belirlemek zorunda kaldı. Bunu çözdükten sonra, analistler mesaj trafiğinin şifresini çözmek için farklı anahtarların sırasını değiştirebilirler. Anahtarı bir kez belirlediklerinde, herkes ilgili süre için kodlanmış tüm trafiği aynı anahtarla okuyabilir.

Bazı durumlarda, analistler bir şifreleme sisteminin temelini oluşturan matematiğe saldırarak bir çözüm buldular. 1970'lerin sonlarında, bazı satıcılar, *alt küme toplamı problemi (the subset sum problem)* olarak adlandırılan sırt çantası probleminin (*the knapsack problem*) basitleştirilmiş bir sürümüne dayanan asimetrik anahtar şifrelemesi kullanan güvenlik ürünleri ürettiler. Satıcılar için ne yazık ki, Len Adelman, 1982'de Apple II bilgisayarında çalışabilecek alt küme toplamı sorunu için genel bir çözüm geliştirdi. Bir gecede, bütün bir güvenlik ürünleri sınıfı kullanılamaz oldu.

Bugün, çoğu ticari asimetrik anahtar şifrelemenin temeli, büyük sayıları çarpanlara ayırmadaki zorluktur. Örneğin, kalem ve kağıt kullanarak 757 × 769 = 582.133'ü hesaplamak oldukça kolaydır. Ancak, 582.133 sonucu verildiğinde, bu sayının iki çarpanının türetilmesi o kadar kolay değildir. Klasik yaklaşım, 2, 3, 5, 7, 11, 13 vb. gibi bir asal çarpan bulunana kadar denemektir. Bu işlem 134 tahmin sürecektir. Bu işlem her ne kadar bir bilgisayarla daha kolay olsa da, iki asal çarpanın her birinin 100 basamak olduğunu düşünün! Buna bir anlam kazandırmak için, aşağıda 100 basamaklı bir asal sayı verilmektedir:

[4] Ç.N. Navaho, Amerika Birleşik Devletleri'nin Arizona, New Mexico ve Utah eyaletlerinde yaşayan ve Navahoca (Navaho dili) konuşan Atabaskların Güney Atabaskları grubundan olan bir Kızılderili halkıdır.

6,513,516,734,600,035,718,300,327,211,250,928,237,178,281,758,494,417, 357,560,086,828,416,863,929,270,451,437,126,021,949,850,746,381

Ayrıca, bundan önceki sayı iki çarpandan yalnızca biri olacaktır.

Anahtarlar, Anahtar Uzayı ve Anahtar Yönetimi

Bu bölümde, anahtarların fonksiyonunu, anahtar uzayı boyutunun önemini ve yeterli anahtar yönetimi için gereksinimleri nasıl tanımlayacağınızı öğreneceksiniz.

Kriptografik Anahtarlar ve Anahtar Uzayı

Bir süredir anahtarlar hakkında okuyorsunuz. Fakat anahtarlar nedir? Anahtar, bir şifreleme sistemine girdi olan bir değerdir. Anahtar, mesajı belirli bir şekilde dönüştürmeye katılır. İyi tasarlanmış bir şifreleme sistemi, kullanılan her anahtar için aynı mesajın farklı çıktılarını üretir. Anahtarları şu şekilde düşünebilirsiniz: Bir şifreleme belirli bir görevi yerine getirir ve bir anahtar bunun nasıl yapılacağına ilişkin belirli yönergeleri verir.

Fiziksel anahtarlar kriptografik anahtarlara benzer ancak aynı değildir. Birçok popüler kapı kilidinde, her biri 10 olası pozisyona sahip beş kapı mandalı vardır. Bu nedenle, ev anahtarları için 10^5 veya 100.000 olası kesim vardır. Bu, ön kapınızda rastgele bir anahtar kullanan bir kişinin evinize giremeyeceğine dair makul bir güvence verir.

Bir **anahtar uzayı** (***keyspace***) tüm olası anahtar kümesidir. Her zaman olmasa da, genellikle, anahtar uzayı ne kadar büyük olursa algoritma da o kadar güvenli olur. Bir örneğe bakalım.

İki üç basamaklı kilidi olan evrak çantasının anahtar uzayı ne kadar büyüktür? Kombinasyonlar 000–000 ile 999–999 arasındadır, bu nedenle anahtar uzayında 1.000.000 anahtar vardır. Bu, bir hırsızın doğru kombinasyonu tahmin etmeden önce 1 milyon kombinasyonu denemesi gerektiği anlamına mı geliyor? Şart değil. Bir hırsız inanılmaz derecede şanslı olabilir ve ilk denemede doğru kombinasyonu tahmin edebilir. Bundan farklı olarak, bir hırsız inanılmaz derecede şanssız olabilir ve son denemede doğru kombinasyonu bulmadan önce olası tüm kombinasyonları deneyebilir. Ortalama olarak, bir saldırgan, doğru kombinasyonu anahtar uzayında yaptığı aramanın ortasında tahmin edecektir. Bu, bir saldırganın ortalama olarak 500.000 kombinasyon denemesi gerektiği anlamına mı geliyor? Her deneme iki saniye sürdüyse ve saldırgan gece gündüz aralıksız çalıştıysa, evrak çantasını açmak için 11 günden fazla zamana ihtiyacı olacaktır. Bununla birlikte, bir evrak çantasının kaba kuvvet saldırısına karşı gerçek direnci 17 dakikaya yakındır! Bu neden böyledir?

Evrak çantası algoritmasında zayıf bir şey var. Her biri 1.000 kombinasyonlu iki ayrı kilit bulunduğundan, ortalama olarak her bir alt kombinasyonu tahmin etmek için 500 deneme gerekir. Sol kombinasyonu bulduktan sonra, saldırgan sağ kombinasyona ilerler. Saldırganın en fazla 1.000 + 1.000 veya 2.000 kombinasyon denemesi gerekir. Bununla birlikte, ortalama olarak, saldırganın sadece 1.000 kombinasyon denemesi gerekecektir. Her biri iki saniyeden, bu 16 dakika 40 saniye sürecektir.

Bu, çok güzel bir şekilde, artan anahtar uzayının, veya bir anahtardaki bitlerin sayısındaki bir artışın bile mutlaka daha fazla güvenlik sağlamadığını göstermektedir. Bir evrak çantası üreticisi size altı adet üç basamaklı kilit içeren bir ürün satmak isteseydi, satın almak ister miydiniz? Şirket, evrak çantasının DES'ten daha fazla olası kombinasyona (yani anahtarlara) sahip olduğunu iddia etmekte haklı olacaktır. Bununla birlikte, şu an ne bildiğinizi bilerek, bu güvenli evrak çantasını açmanın bir saatten az süreceğini hesaplayabilirsiniz.

Anahtar Yönetimi

Bir kripto sisteminin en zor ve kritik kısımlarından biri **anahtar yönetimidir (*key management*)**. Her ne kadar bir şifrelemenin matematiği bir saldırganın çözmesi için zor olsa da, anahtar yönetimindeki zayıflıklar veya hatalar çoğu zaman bir sistemi tehlikeye atmanın bir yolunu sunar. Gördüğünüz gibi simetrik bir kripto sisteminin anahtar yönetimi zor ve karmaşık olabilir. Sonuç olarak, anahtar yönetimi bazen güvenli şifreleme için tehlikeli olabilecek kısa yollara yol açar.

II. Dünya Savaşı tarihi, zayıf anahtar yönetiminin bir kripto sistemine nasıl zarar verebileceğine bir örnek verir. 1940'dan 1948'e kadar Sovyetler Birliği, ticari telgraf hatları üzerinden gönderilen mesajları şifrelemek için tek kullanımlık şifreleme (*one-time pad*) kullandı. Teorik olarak, tek kullanımlık şifrelemeler kırılamaz. Anahtar rastlantısala çok yakındır. Anahtar koruduğu bilgi kadar uzundur ve tekrar etmez. Şifreli metinde bir örüntü tespit etmek mümkün değildir. Bununla birlikte, okuduğunuz gibi dünya çapında bir savaş ortamında uzun anahtarların dağıtılmasının ve yönetilmesinin zorluğu, şifreli anahtarların bitmesine neden oldu. Her konum kendi anahtarlarını tekrar kullanmaması gerektiğini biliyordu ancak başka bir istasyonun tek kullanımlık şifrelemesini kullanmanın zararı ne olabilir? Oldukça zararı vardır.

Şifrelemek için özel VEYA işlevini kullanırsanız, A mesajını X anahtar akışı ile şifrelemek şu şekilde olur:

$$A \oplus X = E(A)$$

Burada E(A), A'yı içeren şifreli mesajı temsil eder. Özel VEYA fonksiyonunun ilginç bir özelliğinin, kendisi ile özel VEYA işlemine giren değerin işlem sonucunun 0 olduğu ve 0 ile özel VEYA işlemine giren değerin işlem sonucunun kendisi olduğunu unutmayın. Bu mesajın şifresini çözmek için, yeniden X anahtarı ile birleştirerek mesajı ele geçirin:

$$E(A) \oplus X = A \oplus X \oplus X = A$$

Başka bir istasyonun anahtar malzemesini tekrar kullanmanın problemi, Amerika Birleşik Devletleri'nin tüm konumlardan tüm şifreli trafiği yakalamaya çalışmış olmasıdır. ABD, daha sonra mesajları ilişkilendirmeye çalışmıştır. Örneğin, 1943'te New York'tan Moskova'ya gönderilen bir mesaj, 1944'te Sydney'deki büyükelçiliğin Kahire'deki büyükelçiliğine gönderdiği bir mesajla aynı tek kullanımlık şifrelemeyi kullanmış olabilir. Aynı anahtarla şifrelenmiş iki mesajı birleştirdiğinizde ilginç bir şey olur:

$$\begin{aligned} A \oplus X &= E(A) \quad B \oplus X = E(B) \\ E(A) \oplus E(B) &= A \oplus X \oplus B \oplus X \\ &= A \oplus B \oplus \cancel{X \oplus X} \\ &= A \oplus B \end{aligned}$$

Artık B mesajını şifrelemek için A mesajını kullanabilirsiniz. Yer değiştirme şifrelemeleri konusundaki tartışmayı hatırlarsanız şifreli metin düz metindeki örüntüleri saklamaktadır. Bir mesajı diğer mesajı şifrelemek için kullanmak, aynı zamanda düz metnin istatistiksel özelliklerinin çoğunu da tutmaktır. Bu mesajları kırmanın oldukça kolay olduğu ortaya çıkmıştır. Şifreleme anahtarını değil, düz metni çözdüğünüzü unutmayın! Mesajın şifresini bir kez çözdükten sonra, şifreli metni düz metinle birleştirerek anahtarı hesaplayabilirsiniz.

Amerika Birleşik Devletleri bu projeyi Venona olarak adlandırdı. Bu mesajları 1940'lı yıllardan 1980 yılına kadar kırmaya çalıştı! Tamamı bu proje hakkında olan kitaplar vardır; ABD hükümeti 1995 ile 1997 yılları arasında ele geçirilen mesajları açıklamıştır. Julius ve Ethel Rosenberg'in

Sovyetler Birliği için casusluk yaptığını düşünmemeniz durumunda, bugün şifresi çözülmüş suçlayıcı mesajları okuyabilirsiniz.

Anahtar Dağıtımı

Anahtar dağıtım (*key distribution*) teknikleri genellikle aşağıda belirtilen üç biçimden biridir:

- **Kağıt** — Kağıt dağıtımı teknoloji kullanımını gerektirmez. Ancak, anahtarı yüklemek için bir kişinin bir şeyler yapmasını gerektirir. Bu insan rolü hataları ortaya çıkarabilir veya hoşnutsuz birine sisteme zarar vermesi için bir olanak verebilir.
- **Dijital medya** — Dijital dağıtım CD'ler veya e-posta şeklinde olabilir. Aktarımdaki anahtarları korumanız gerektiğini unutmayın. Bazı güvenli aktarım şekilleri kullanılmalıdır. Fiziksel medya için, kurcalanmaya karşı korumalı (*tamperproof*) durumlar ve kayıtlı posta, bir miktar güvence sağlar. Elektronik dağıtım için, anahtar **şifreleme anahtarı (*key-encrypting key*)** olarak bilinen üst düzey bir anahtar, aktarımdaki ve saklanmakta olan anahtarları korumalıdır. Bu, elbette, önce anahtar şifreleme anahtarını bazı alternatif güvenli düzenekler ile dağıtmanızı gerektirir. Anahtar şifreleme anahtarlarını, verileri şifrelemek için değil, yalnızca diğer anahtarları şifrelemek için kullanmalısınız. Herhangi bir anahtarın aşırı kullanılması, anahtarın tehlikeye atılmasına neden olabilir.
- **Donanım** — Bir anahtarı USB flash sürücü, akıllı kart veya başka bir çıkarılabilir depolama aygıtına sahip bir donanım aracılığıyla dağıtabilirsiniz. Bunun avantajı, kimse izlemeden anahtarları doğrudan anahtar aktarım düzeneğinden kripto cihazına aktarmanızdır. Bu bileşenlerin dışında hiçbir kopya bulunmamaktadır.

Aktarım sırasında anahtarın ele geçirilmesini önlemek için, anahtarları bölebilirsiniz. Bir anahtarı eşit sayıda iki parçaya bölmek iyi bir fikir değildir. Bir saldırgan bir parçayı yakalarsa, anahtarın diğer yarısına kaba kuvvet (*brute-force*) uygulaması çok daha kolaydır (evrak çantası örneğini unutmayın). Bu nedenle, bir K anahtarını bölme stratejilerinden biri, anahtar şifreleme anahtarı olacak başka bir rastgele J anahtarı oluşturmaktır. Şifrelenmiş bir anahtar üretmek için K ve J'yi birleştirirsiniz. Daha sonra, bu şifreli anahtarı bir kanal üzerinden gönderirsiniz. Anahtar şifreleme anahtarını başka bir kanal ile gönderirsiniz. Bir saldırgan iki mesajdan birini ele geçirirse, saldırgan temel anahtarı öğrenmez.

Kanal 1: J

Kanal 2: K ⊕ J

Tekrar birleştir: J ⊕ K ⊕ J = K

Bu şemanın her anahtar için yeni bir anahtar şifreleme anahtarı gerektirdiğini unutmayın.

Anahtar Dağıtım Merkezleri

Her bir kuruluş kendi anahtarlarını yönetecek altyapıyı oluşturmak yerine, bir dizi ana bilgisayar ortak bir **anahtar dağıtım merkezine (*key-distribution center - KDC*)** güvenmeyi kabul edebilir. Bütün taraflar KDC'ye güvenmelidir. Bir KDC ile, her varlık -kendisi ile KDC arasında- sadece bir gizli anahtar çiftine ihtiyaç duyar. Kerberos ve ANSI X9.17, KDC kavramını kullanır.

Örneğin, Alice, Bob ile güvenli bir iletişim oturumu başlatmak istiyorsa, KDC'ye şifreli bir mesaj gönderir. KDC rastgele bir oturum anahtarı seçer, hem Alice'in anahtarındaki hem de Bob'un anahtarındaki kopyaları şifreler ve her ikisini de Alice'e iletir. Alice, kendi oturum anahtarının şifresini çözer ve bunu Bob'a ileteceği mesajı şifrelemek için kullanır. Alice, mesajı Bob'un anahtarı ile

şifrelenmiş oturum anahtarıyla birlikte –Alice'in okuyamayacağı– Bob'a gönderir. Bob her iki mesajı da alır, gizli anahtarını kullanarak oturum anahtarının şifresini çözer ve Alice'in mesajının şifresini çözmek için oturum anahtarını kullanır.

Dijital İmzalar ve Özet Fonksiyonlar

Birçok iş gereksinimi için, dijital imzaların ve özet (*hash*) fonksiyonların kullanımını ve ne tür şifrelemeler kullanacağınızı anlamanız gerekir.

Özet Fonksiyonlar

Bir mesajın değerlerinin -kasıtlı olarak veya aktarım hatası yoluyla- değişmediğinden emin olmak için, tekrarlanabilir bir işlemle doğrulayabileceğiniz bilgilerin bir özetini ekleyebilirsiniz. Bu özet bir sağlama toplamıdır (*checksum*). Örneğin, sayılardan oluşan bir dizgisinin aktarım sırasında değişmediğinden emin olmak için, tüm sayıların toplamını mesajın sonuna ekleyebilirsiniz. Eğer alıcı sayıları toplarsa ve farklı bir değere ulaşırsa, aktarımda bir hata olduğunu varsayabilir ve tekrar göndermeyi talep edebilirsiniz.

Kredi kartlarında, kart numarasını doğrulayan bir özet basamağı vardır. Bu basamağı hesaplamak için kullanılan algoritma, ANSI X4.13'e dayanan LUHN formülüdür. Bir kredi kartı numarasının geçerli olup olmadığını hesaplamak için aşağıda belirtilen dört adımı izleyin:

1. Sağdaki ikinci basamak ile başlayarak, diğer her sayıyı iki ile çarpın.
2. Eğer herhangi bir iki katını almanın sonucu 10'dan büyükse (yani, 8 + 8 = 16), bu sonucun rakamlarını ekleyin. Tüm iki katına çıkarılmış sayıları ekleyin.
3. Bu toplama, son basamak hariç (sağlama toplamı) diğer tüm sayıları ekleyin.
4. Toplam ile bir sonraki 10 katı arasındaki fark kontrol basamağıdır. Örneğin, kredi kartı numarası 5012 3456 7890 123X için doğru özet sayısı 6'dır.

Bir özet, sağlama toplamı gibidir ancak sahte bir mesajın geçerli bir mesajla aynı özet sonucunu vermeyeceği şekilde çalışır. Özetler genellikle sabit bir boyuttadır. Sonuç bir özet değerdir. Özetler veriler için parmak izi görevi görür. Mesaj yaratıcıları bir özeti referans olarak yayınlayabilir, böylece alıcılar bilgilerin değişip değişmediğini görebilir. Yazılım yayıncıları genellikle özet değerlerini sağlarlar, böylece müşteriler aldıkları yazılımın bütünlüğünü kontrol edebilirler. Etkili olmak için, özetler genellikle yeterince uzun olmalıdır, böylelikle özet değeriyle eşleşen alternatif bir mesaj oluşturmak çok zaman alacaktır.

Dijital İmzalar

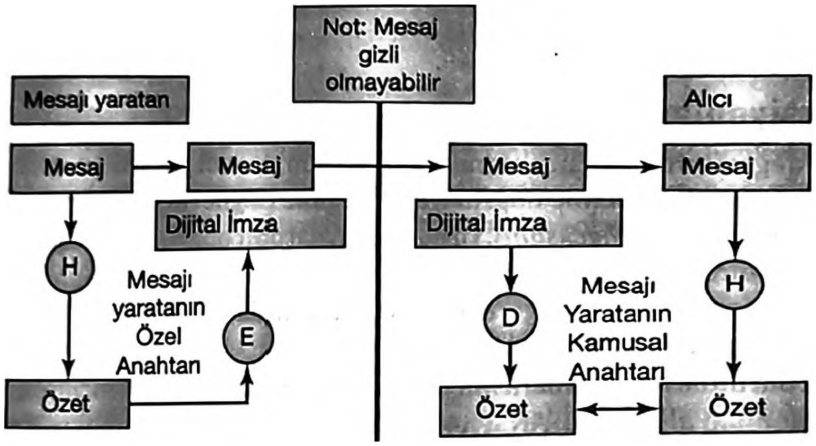
Dijital imzalar dijitalleştirilmiş imzalar değildir (el yazısı imzaların elektronik görüntüleri). Aksine, dijital imzalar bir varlığın kimliğini belirli bir mesaja veya bilgi parçasına bağlar. Mahremiyet ya da gizlilik sağlamazlar. Bir mesajın bütünlüğünü sağlar ve mesajı kimin yazdığını doğrularlar. Dijital imzalar asimetrik anahtar şifrelemesini gerektirir. **ŞEKİL 9-5**, bir dijital imzayı göstermektedir.

Asimetrik bir anahtar çiftinden özel bir anahtarla dijital imza oluşturabilirsiniz. Mesajın bir özet imzasını içerir. Bu kombinasyon, bir mesajın belirli bir varlıktan geldiği ve hiç kimsenin mesajın içeriğini değiştirmediğine dair çifte güvence sağlar. İmzalayanın kamusal anahtarına erişimi olan herkes dijital imzayı doğrulayabilir. Ancak,

ŞEKİL 9-5
Dijital İmza.



ŞEKİL 9-6
Bir dijital imzanın işleyişi.



yalnızca özel anahtarın sahibi dijital imzayı oluşturabilir. **ŞEKİL 9-6,** bir dijital imzanın nasıl çalıştığını göstermektedir.

Rivest-Shamir-Adelman (RSA) ve **Dijital İmza Algoritması (*Digital Signature Algorithm* - DSA),** kullanılan en yaygın dijital imza algoritmalarıdır. RSA'nın patenti Eylül 2000'de sona ermiştir. RSA artık kamuya açıktır. DSA, mesajın özetini **Güvenli Özet Algoritması (*Secure Hash Algorithm* - SHA)** ile imzalar. Çoğu ticari sistem RSA kullanmasına rağmen, Dijital İmza Standardı (*Digital Signature Standard* - DSS), DSA ve SHA ABD devlet standartlarıdır. Devlet ürünlerinde görünme olasılıkları daha yüksektir.

Bilgi Sistemi Güvenliğinde Kriptografik Uygulamalar ve Kullanım Alanları

Günümüzde birçok satıcı güvenlik ürünleri ve hizmetleri sunmaktadır. Aslında, birkaç bin farklı teklif bulunmaktadır. Bu ürün ve hizmetler genellikle aşağıdakileri içeren ortak kategoriler halinde düzenlenir:

- Kötücül yazılımdan koruma
- Uyumluluk / denetim
- Adli bilişim
- Kimlik (ID) yönetimi
- Fikri Mülkiyet
- Yönetilen güvenlik servis sağlayıcıları (*managed security service providers* - MSSP'ler)
- Mesajlaşma korumaları
- Yama yönetimi

- Alan savunmaları (*perimeter defense*)
- Güvenli bilgi ve olay yönetimi (*security information and event management* - SIEM) ve olay müdahalesi
- İşlem güvenliği (dijital sertifikalar, güvenli dosya transferi)
- Kablosuz güvenlik

Bu kategorilerin çoğunda kriptografi kullanımlarını bulabilirsiniz.

Kimlik denetleme araçları, belirteçleri (*token*), akıllı kartları, biyometrikleri, parolaları ve şifre kurtarma işlemlerini içerir. Bazı araçlar yaklaştırmalı kartlara (*proximity card*) ve parmak izi okuyucularına dayanır. Diğerleri, **açık anahtar altyapısı (*public key infrastructure* - PKI)** kullanıcı kimlik denetlemesi ve internet üzerinden güvenli bir şekilde parola gönderen araçlar gibi kriptografik tekniklerini kullanır. PKI, dijital sertifikalar yaratmak, yönetmek, dağıtmak, kullanmak, saklamak ve iptal etmek için gereken bir dizi donanım, yazılım, kişiler, politikalar ve prosedürler kümesidir.

Erişim denetimi ve yetkilendirme, güvenlik duvarları, zaman damgası, tek oturum açma, kimlik yönetimi ve mobil cihaz güvenliğini içerir. Bu şifreleme araçları, güvenlik duvarları ile birlikte sanal güvenlik ağlarına sahiptir ancak mutlaka güvenlik duvarlarının kendileri olması gerekmez. Ayrıca, internet üzerinden bağlantının güvenliğini sağlayabilirler ve sabit sürücülerin içeriğini şifreleyen araçlar sağlayabilirler.

Değerlendirme ve denetim araçları arasında güvenlik açığı değerlendirme tarayıcıları, penetrasyon (sızma) testi araçları, adli bilişim yazılımı ve günlük çözümleyicileri (analizcileri) bulunur. Parola kırma modüllerini içeren değerlendirme tarayıcıları ve penetrasyon testi araçları, parolaları tahmin etmeye çalışmak için kriptografik teknikleri kullanır.

Güvenlik yönetimi ürünleri, kurumsal güvenlik yönetimi, yapılandırma ve yama yönetimi ve güvenlik politikası geliştirme araçlarını içerir. Bütünlük kontrol araçları, hiçbir şeyin ve hiç kimsenin yazılımı değiştirmediğinden emin olmak için kriptografik yöntemler kullanır.

Kablosuz güvenlik araçları, verilerin aktarım sırasında korunmaları ve verilere erişimin yetkili kişiler ile sınırlandırılması için verileri şifreler. E-posta güvenlik araçları genellikle aktarımdaki ve bazen de durağan verinin şifrelenmesini içerir. İçerik filtreleme, virüsten koruma ürünleri, mobil kod tarayıcılar, web filtreleri ve spam engelleyicileri içerir. Tehdit imzalarının veritabanlarını şifreleyebilmenize rağmen, içerik filtreleme araçları genellikle şifreleme kullanmazlar.

Şifreleme araçları arasında hat şifreleme (*line encryption*), veritabanı güvenlik ürünleri, sanal özel ağlar (*virtual private network* - VPN'ler), açık anahtar altyapısı (PKI) ve kripto hızlandırıcıları bulunur. Bu ürünler, görevlerini yapmak için kriptografiyi kapsamlı olarak kullanır. Bir kripto hızlandırıcı, kriptografik rutinleri ana işlemciden hızlı şifreleme için tasarlanmış yonga setlerine sahip kartlara yükler.

Diğer Kriptografik Araçlar ve Kaynaklar

Bir güvenlik uzmanı olarak, işletme gereksinimlerinin kriptografik çözümlerle nasıl eşleştirileceğini ve uygun araç setlerini nasıl seçmeniz gerektiğini anlamalısınız. Bu bölümde, simetrik anahtarları kullanan araç setlerini tanımlamayı ve bunları en yaygın iş kullanımlarıyla eşleştirmeyi öğreneceksiniz. Asimetrik anahtar şifrelemeyi kullanabilecek araç setlerini ve bir çözüm elde etmek için gereken altyapıyı nasıl tanımlayacağınızı öğreneceksiniz. Özet fonksiyonlarının nasıl çalıştığını, özet fonksiyonlar için kullanılan şifrelemeleri nasıl tanımlayacağınızı ve bütünlüğü sağlamak için bunları nasıl kullanacağınızı öğreneceksiniz. Her gereksinimi ve her gereksinim arasındaki farkları ele almak için kriptografiyi nasıl kullanacağınızı öğreneceksiniz. Ayrıca, dijital ve dijitalleştirilmiş imzalar arasındaki farkları ve inkar edememe için kullanılan dijital imzaların korunmasına yönelik altyapı ve yasal

gereklilikleri de öğreneceksiniz. Son olarak, işletme gereksinimlerinizi destekleyen bir anahtar yönetim modelini nasıl tasarlayacağınızı öğreneceksiniz.

Simetrik Anahtar Standartları

Simetrik anahtar algoritmaları (veya standartları) en yaygın şifreleme şeklidir. Aynı anahtar, bilgiyi şifreler ve şifreyi çözer. Simetrik anahtarlar kolayca oluşturulabildiğinden ve hızlıca değiştirilebildiğinden, genellikle iki taraf arasında bilgi alışverişinde bulunmak için yalnızca bir kez kullanılırlar ve daha sonra kullanılmazlar. Bu durumda, bunlar oturum anahtarlarıdır. Asimetrik anahtar algoritmalarından farklı olarak, simetrik algoritmalar hızlı olabilir ve birçok veriyi şifrelemek için çok uygundur. Aşağıdaki kriptografik algoritmalar listesi genel olarak en zayıftan en güçlüye doğru sıralanmıştır. Daha güçlü algoritmalar her zaman zayıf algoritmalardan daha güvenlidir ancak çoğu zaman daha yüksek bir hesaplama maliyetine sahiptir. Eğer daha zayıf bir algoritma yeterli güvenlik sağlıyorsa, bu algoritma iyi bir seçim olabilir. Elbette, ihtiyaçlar değiştiğinde yeterli güvenlik sağladıklarından emin olmak için algoritma tercihlerinizi düzenli olarak gözden geçirmelisiniz. Kuruluşlar bugünlerde, aşağıdakiler dahil olmak üzere çeşitli simetrik algoritmalar kullanmaktadır:

- **Veri Şifreleme Standardı (*Data Encryption Standard* - DES)** — IBM başlangıçta DES'i Lucifer algoritması olarak geliştirmiştir. NSA algoritmayı değiştirdi ve 1977'de ulusal bir standart olarak yayınladı. FIPS PUB 46-3 tanımını güncelledi. DES, 56 bitlik bir anahtar kullanır ve 64 bitlik veri blokları ile çalışır. Algoritma, donanım kullanımı için yazılımdan daha iyidir ve birçok veriyi hızlı bir şekilde şifreleyebilir. DES algoritması kamuya açıktır. DES bir zamanlar en son teknolojiye sahip bir algoritmaydı ancak donanım yeteneklerinde ve saldırı yöntemlerinde hızlı gelişmeler ile birlikte, saldırganlar şimdi birkaç gün kadar kısa bir sürede DES'i kırabilirler. DES artık güvenli bir algoritma değildir.
- **Üçlü DES (*Triple DES* - 3DES)** — Üçlü DES, birden fazla anahtar kullanarak DES'in üç aşamasından (şifreleme, şifre çözme, şifreleme) oluşan bir protokoldür. İki veya üç anahtarın kullanılmasına bağlı olarak, anahtar uzayını 56'dan 112'ye veya 168 bit'e yükseltir. Üçlü DES, DES algoritmasının altında yatan güvenlik ve büyük ölçüde arttırılmış anahtar uzayı nedenleriyle hesaplama açısından güvenlidir. Aynı anahtarı üç kez kullanmanın, tek bir DES ile aynı sonucu verdiğine dikkat edin. Üçlü DES de FIPS PUB 46-3 içerisinde yer almaktadır ve kamuya açıktır.
- **Uluslararası Veri Şifreleme Algoritması (*International Data Encryption Algorithm* - IDEA)** — DES gibi, bu blok şifreleme 64-bit bloklar ile çalışır. 128 bitlik bir anahtar kullanır ve donanım ve yazılım konusunda DES'ten biraz daha hızlı çalışır. Ascom-Tech AG, IDEA (ABD Patenti 5,214,703) için bir patent sahibidir, ancak IDEA ticari olmayan kullanım için ücretsizdir.
- **CAST** — CAST algoritması, DES'e benzer bir yerine koyma permütasyon algoritmasıdır. DES'den farklı olarak, bu algoritmanın yazarları tasarım kriterlerini halka açıkladı. Bu 64-bit simetrik blok şifrelemesi, 40 ila 256 bit arasındaki anahtarları kullanabilir. RFC 2144, CAST-128'i tanımlar; RFC-2612, CAST-256'yı tanımlar. Patenti alınmış olmasına rağmen (ABD Patenti 5,511,123) mucitleri olan C.M. Adams ve S.E. Tavares, CAST'i ücretsiz kullanım için uygun hale getirdiler.
- **Blowfish** — Blowfish 32'den 448 bit'e değişken anahtar uzunluğuna sahip 64 bit bir blok şifrelemedir. DES veya IDEA'dan çok daha hızlıdır. Blowfish, 150'den fazla ürüne ve Linux çekirdeğinin v2.5.47'sine dahil edilmiş güçlü bir algoritmadır. Yazarı olan Bruce Schneier, Blowfish'i kamuya açık bir hale getirmiştir. Schneier'ın Twofish'i, Gelişmiş Şifreleme Standardı (*Advanced Encryption Standard*) için bir adaydı.

Bilginize

Saldırganların ortak anahtar değerlerini denediği sözlük saldırılarına karşı savunmaya yardımcı olmak için, bazı algoritmalar **tuz değeri (*salt value*)** denilen ek bir değer kullanır. Tuz değeri, şifreleme anahtarını oluşturmak için gerçek bir girdi anahtarıyla birleştirebileceğiniz rastgele bir karakter kümesidir. Tuz değeri ve girdi anahtarı kombinasyonu, ortak anahtar değerlerini kullanarak bir şifreleme anahtarının güvenliğini tehlikeye sokmayı çok daha zor hale getirmektedir.

- **Gelişmiş Şifreleme Standardı (*Advanced Encryption Standard* - AES)** — Rijndael (RAIN-doll) olarak da bilinen AES, bir blok şifrelemedir. Vincent Rijmen ve Joan Daemen AES'yi tasarladı ve FIPS PUB 197 bunu bir standart olarak yayınladı. AES algoritması, 128 bitlik bloklardaki verileri şifrelemek ve şifrelemesini çözmek için 128, 192 ve 256 bitlik şifreleme anahtarlarını kullanabilir. Şifre aynı zamanda değişken blok uzunluklarında da çalışabilir. AES hem güçlü hem de hızlıdır.
- **RC2** — RC2, Ronald Rivest tarafından tasarlanan değişen anahtar boyutlu bir blok şifrelemedir (RC, Ron'un Kodu anlamına gelmektedir). RC2, DES'in yerine bir alternatif olarak çalışır ve 64-bit bloklar ile çalışır. Kriptanalizi zorlaştırmak için şifreleme rutininin bir parçası olarak bir tuz değeri kullanır. RSA Security RC2'nin sahibidir.
- **RC4** — RSA Security tarafından üretilen RC4, sekizli (*byte-oriented*) işlemlerle çalışan değişen anahtar boyutlu bir kesintisiz şifrelemedir (*stream cipher*). İnternet tarayıcıları genellikle bir SSL bağlantısı sağlamak için RC4'ü kullanır.

Kablosuz Güvenlik

Ucuz yüksek-bant genişliği iletişim teknolojisiyle, kablosuz yerel alan ağları (*wireless local area networks* - WLAN) artık bilgisayarlara kablo bağlamak istemeyen evler ve ofisler için geçerli bir stratejidir. WLAN'lar kahve dükkanlarında ve diğer birçok kamusal alanda da yaygınlaşmaktadır. Ancak, bu kolaylık güvenliği zayıflatmaktadır.

Birçok kablosuz erişim noktası sağlayıcısı ve kullanıcısı yeni teknolojilerini tak ve çalıştır yöntemiyle kurmaktadır. Yani, kutuyu açıyorlar, parçaları birleştiriyorlar ve cihazı açıp kurulum sihirbazlarını çalıştırıyorlar. Cihaz çalışırsa, el kitabına asla dokunmazlar. Kablosuz ürünlerin içinde güvenliği var olsa da, varsayılan yapılandırma genellikle bunu etkinleştirmez. Neden? Çünkü, çoğu tüketici, bir ürünün fişini taktığında çalışmasını beklemektedir. Sonuç olarak, güvenlik sunan çoğu satıcı güvenliği müşterinin açmasını ister. Birçok müşteri hiç uğraşmaz. Bu durum büyük güvenlik problemleri yaratabilir.

802.11 Kablosuz Güvenlik. 802.11 veya Wi-Fi, kablosuz standartları 1999 yılında ortaya çıkmıştır. Wi-Fi, 802.11b için 11 Mbps'den 802.11ac için 780 Mbps'ye kadar aktarım hızlarında kablosuz iletişim sağlar. Yeni ve önerilen standartlar, maksimum aktarım oranını daha da ileriye götürmektedir. 802.11ay standardı, 100 Gbps'ye kadar veri aktarım hızlarını desteklemektedir. 802.11 tanımlamasındaki en popüler standartlar, 2.4GHz veya 5GHz bandını kullanarak veriyi aktarır. Daha yeni standartlar bant genişliğini daha geniş aralıklara genişletmektedir. En popüler standartların bant genişliğindeki veri iletişim aralıklarının yaklaşık 100 metre (802.11n için 200 metrenin üzerinde) olduğu ilan edilmiştir. Bununla birlikte, bilgisayar korsanları, yayın alımını birkaç mil arttırmak için - bir Pringles® patates cipsi kutusundan yapılanlar da dahil olmak üzere! - yüksek kazanımı olan antenler kullandılar. En uzun 802.11 kablosuz bağlantısını kimlerin oluşturabileceğini görmek için dünya çapında resmi olmayan bir tür rekabet yaşanmaktadır. Son sayımda, İsveç Uzay Şirketi rekorunu 29.7 km yükseklikte yüzen stratosferik bir balonla kaydetti. Şirket, 310 km uzaklıktaki baz istasyonu ile bağlantı sağladı.

802.11 kablosuz protokolleri, Kablolu Eş değer Mahremiyet (*Wired Equivalent Privacy* - WEP) veya daha yeni olan Wi-Fi Korumalı Erişim (*Wi-Fi Protected Access* - WPA) ile şifrelemeye izin verir. Kullanıcıların güvenli kablosuz bağlantılara başlamak için anahtar işlevi gören bir paylaşılan gizliliğe (*shared secret*) sahip olması gerekir. Çoğu kablosuz erişim noktası (*wireless access point* - WAP) genellikle kablosuz şifrelemeyi varsayılan olarak etkinleştirmediğinden, çoğu kablosuz ağ şifreleme olmadan çalışmaktadır. Herhangi bir saldırgan bu açık ağları izleyebilir ve bunlara erişebilir. 2000 yılında, Peter Shipley, taşınabilir bir kablosuz donanım ile San Francisco Körfezi bölgesinde dolaştı. Kablosuz ağların yaklaşık yüzde 85'inin şifrelenmemiş olduğunu gördü. Şifrelenenlerin yarısından fazlası ise varsayılan parolayı kullanmaktaydı. Her WAP'ın bir müşterinin erişim için bilmesi gereken kendi servis seti tanımlayıcısına (*service set identifier* - SSID) sahip olmasına rağmen, bilgisayar korsanları, menzil içindeki tüm SSID'lerin adlarını görüntüleyen NetStumbler gibi araçlara sahiptir. Windows basit bir şekilde bulunan ilk ağ sinyaline bağlanır. Sonuç olarak kablosuz şifreleme, kablosuz bir ağda güvenliği sağlamak için en asgari gereksinimdir.

UYARI

Hatırlanması gereken önemli ders, kablosuz sinyallerin bir binanın çevresinde durmadığıdır. Bu nedenle, kuruluşunuzun kablosuz iletişimini güvence altına almak için kriptografik koruma önem kazanır.

WEP, yaygın kullanımda ilk kablosuz şifreleme protokolüydü. Bununla birlikte, bazı ciddi sınırlamaları vardır. RC4 şifrelemesindeki bazı önemli anahtar programı zayıflıkları da dahil olmak üzere protokolde tasarım hataları mevcuttur. AirSnort veya WEPcrack gibi araçları kullanan bir bilgisayar korsanı, yaklaşık olarak 5 milyon ila 10 milyon şifreli paket topladıktan sonra şifreleme anahtarını tahmin edebilir. Bu zayıflıkları gidermek için mevcut standartlar ve desteklenen donanımlar da WPA'yı sunmaktadır. Kablosuz ağ trafiği için en iyi korumayı sağlamak için, her zaman WPA'yı veya WPA'nın en yeni sürümü olan WPA2'yi kullanın. Asla WEP'i kullanmayın. Tanımadığı bilgisayarları tarayan MAC adres filtrelemesini etkinleştirin. Saldırganların ilerlememesi için kablosuz LAN ile ağın geri kalanı arasına bir güvenlik duvarı yerleştirin.

Asimetrik Anahtar Çözümleri

Anahtar dağıtımının, bir kripto sisteminin geçerli kullanıcılarına anahtarlar verdiğini ve böylelikle kullanıcıların iletişim kurabildiklerini hatırlayın. Anahtarları yönetmedeki ilk adım aslında anahtarları dağıtmadan önce gerçekleşir. Bir kayıt işlemi sırasında anahtar oluşturma ve yönetme için kullanıcıların kimliği denetlenmeli ve kullanıcılar yetkilendirilmelidir. Bu, ilk etapta sadece yetkilendirilmiş kullanıcıların anahtar oluşturabilmelerini sağlar. Anahtar dağıtımına klasik çözüm, anahtarları önceden dağıtmak için güvenilir bir kanaldan bant dışı iletişimleri kullanmaktır. Bu, kayıtlı postayla, kuryeyle hatta eğer telefon hattını hiç kimsenin dinlemediğinden eminseniz telefonla olabilir. Ancak, bu strateji pahalı ve yavaştır.

Kaynakları ve planlama yeteneği olan kuruluşlar bunu gerçekleştirmek için yöntemler geliştiriyor. Örneğin, ABD Donanması, kripto sistemlerinin güvenli kaldığından emin olmak için özgün bir dağıtım sistemi kullanmaktadır. Bu sistem, kripto sistemlerinin uygun şekilde kullanılmasını sağlamak için katı izlenebilirlik ve denetim prosedürlerini içerir. Bu program, İletişim Güvenliği Malzeme Sistemi (*Communications Security Material System*) veya CMS'dir. Her komut, bir CMS sorumlusu ve bir alternatif atar. Bunlar, donanma kripto sistemleri için anahtarları almak, depolamak, denetlemek, kurmak, silmek ve imha etmekle sorumludurlar. Bu, çok fazla masraf ve gider içermektedir. Ancak, bilginin yüksek değeri bunun gerekçesini haklı göstermektedir.

Asimetrik bir anahtar dağıtım sisteminin kuryelere, arka kanallara veya pahalı depolama veya envanter planlarına ihtiyacı yoktur. Bunun nedeni, her bir tarafın öncelikle bir gizli anahtarı

paylaşmasını gerektirmemesidir. Bu, güvenli bir kanal oluşturmadan önce ilk olarak güvenli bir kanala ihtiyaç duyan tavuk yumurta problemini çözmektedir.

Anahtarın iptal edilmesi (*key revocation*), kişi artık güvenilmezse veya kişinin artık bir kripto sistemini kullanmasına izin verilmediğinde gerçekleşir. Herkesin aynı gizliliği paylaştığı simetrik bir anahtar sisteminde, anahtarın bir kopyasının güvenliğinin tehlikede olması tüm kopyalarının güvenliğini tehlikeye atar. Bu, tüm çalışanların aynı ofis anahtarına sahip olmasına benzer. Eğer bir çalışanın işine son verildiğinde anahtarı geri vermeyi reddederse, kuruluş her kilidi değiştirmeli ve yeni anahtarlar dağıtmalıdır. Birkaç işten çıkarma sonrasında, bu işlem pahalı ve zahmetli hale gelir.

Asimetrik bir anahtar ortamında, **anahtar dizini (*key directory*)** tüm kamusal anahtarların güvenilir bir deposudur. Eğer bir kişiye artık güvenilmiyorsa, dizinin yöneticisi bu kamusal anahtarı siler. Bu kişiyle iletişim kurmaya çalışan hiç kimse bu anahtarı bulamayacaktır. Bu kişi hala yayınlanan diğer kamusal anahtarları kullanarak şifreli iletişim başlatabilir. Bununla birlikte, protokol tüm mesajlar için dijital imzalar gerektiriyorsa, alıcı mesajı reddedebilecektir çünkü imzayı kontrol etmek için geçerli bir anahtar bulamayacaktır. Örneğin, *http://pgp.mit.edu/* adresinden MIT PGP Kamusal Anahtar Sunucusu'nu sorgulayabilirsiniz. Fakat anahtarları saklayan varlığın, varlığının sona ermesi durumunda ne olur? Verilerin dış kaynak kullanımının gerçekleştiği ve bulut servis sağlayıcılarında işlendiği günümüz çağında, bu her zaman gerçek bir olasılıktır. Bir **anahtar emaneti (*key escrow*)**, belirli şartlar altında bazı yetkilendirilmiş üçüncü tarafların bir anahtara erişmesine izin veren bir anahtar saklama yöntemidir. Bu koşullar, anahtar sahibinin bir anahtara erişemediği durumlardaki acil durumları içerebilir.

Özel amaçlı güvenli iletişimler, internet e-ticaretinin temelidir. Bu, kriptografinin günümüzde en sık kullanılan biçimlerinden biridir. Simetrik bir anahtar kullanmak zor olabilir. Simetrik anahtar kullanımı, her bir tarafın başka bir yöntemle iletişim kurmasını ve gizli bir anahtar üzerinde anlaşmasını gerektirecektir. Eğer böyle bir kanal varsa, neden onu kullanmıyorsunuz? Gerçekte, böyle bir kanal mevcut değildir.

Asimetrik bir anahtarla, özel amaçlı iletişimler basittir. İnternet kriptografisinin en yaygın biçimi Güvenli Soket Katmanı (*Secure Sockets Layer* - SSL) veya Güvenli Hiper Metin Aktarım Protokolü (*Hypertext Transport Protocol Secure* - HTTPS) şifrelemesidir. SSL tokalaşması, bir istemci ve bir sunucu arasında ilk güvenli iletişim oturumunu oluşturmuştur. Symantec web sitesi bu süreci iyi bir şekilde tanımlamaktadır (*www.symantec.com/connect/blogs/how-does-ssl-work-what-ssl-handshake*).

SSL Tokalaşma Protokolü (SSL *Handshake Protocol*) iki aşamadan oluşmaktadır: sunucu kimlik denetlemesi ve isteğe bağlı istemci kimlik denetlemesi. Birinci aşamada, sunucu, bir istemcinin isteğine yanıt olarak, sunucunun kamusal anahtarını içeren sertifikasını ve şifreleme tercihlerini gönderir. İstemci daha sonra sunucunun kamusal anahtarıyla şifrelediği bir ana anahtar (*master key*) oluşturur. İstemci daha sonra şifrelenmiş ana anahtarı sunucuya gönderir. Sunucu ana anahtarın şifresini çözer ve ana anahtar ile bir mesaj döndürerek kendisini istemciye doğrular. İstemci ve sunucu, bu ana anahtardan türetilen anahtarlarla sonraki verileri şifreler ve doğrular. İsteğe bağlı olan ikinci aşamada, sunucu istemciye bir çağrı gönderir. İstemci çağrıda, kendi kamusal anahtar sertifikasının yanı sıra, istemcinin dijital imzasını da göndererek kendisini sunucuya doğrular.

Dijital imzalar, bir kişinin kimliğini veya o kişinin bir mesajla ilişkisini doğrular. Bir kimlik bilgisinin geçerliliğini doğrulayabilecek bir **sertifika yetkilisinin (*certificate authority* - CA)** kullanılmasını gerektirir. İnkar edememe, bir belgedeki dijital imzayı doğrular. Mesajı kimin yolladığını kanıtlamaktadır. Bazı durumlarda, mesajı ne zaman gönderdiğinizi kanıtlamak için kurcalamaya dayanıklı (*tamperproof*) bir zaman kaynağı ile birleştirebilirsiniz. Ancak, CA'lar sadece sertifika sağlamaktan daha fazlasını yapar. Ayrıca, önemli sertifika yönetimi fonksiyonlarının eksiksiz bir paketini sunarlar. İki kritik hizmet, sertifika isteyen kullanıcıları ve sertifikaları iptal eden CA'yı içerir.

Bir kullanıcı, standart bir sertifika imzalama isteği (*certification signing request* - CSR) göndererek sertifika isteyebilir. Bir CSR standardı, birçok farklı türde programın CA'dan sertifika istemesine izin verir. Bir noktada, sertifikaların çoğunun süresi dolar veya geçersiz hale gelir. Bir CA, geçersiz ya da iptal edilmiş sertifikaların kontrolünü sertifika iptal listesindeki (*certificate revocation list* - CRL) ile veya yeni olan Çevrimiçi Sertifika Durum Protokolü'nü (*Online Certificate Status Protocol* - OCSP) desteklemek için verilerin kontrolünü gerçekleştirerek sağlar.

Özet Fonksiyonu ve Bütünlük

Güvenlik ile ilgili deneyimi olmayan birinin terimleriyle, özet fonksiyonlarının nasıl çalıştığını açıklayabilmeniz, özet fonksiyonları için kullanılan şifrelemeleri tanımlayabilmeniz ve bütünlüğü sağlamadaki kullanımlarını açıklayabilmeniz gerekir.

Özet Fonksiyonları

Özet fonksiyonları sahteciliği tespit etmeye yardımcı olur. Bir mesajın sağlama toplamını hesaplarlar ve daha sonra sonucun kurcalamaya karşı korumalı olması için bunu kriptografik bir fonksiyon ile birleştirirler. Özetler, genellikle kullanılan algoritmaya bağlı olarak bilinen sabit bir boyuttadır.

Bir sağlama toplamının, verileri sağlama fonksiyonu üzerinden yeniden çalıştırarak kolayca kontrol edebileceğiniz bir sonuç veren tek yönlü bir hesaplama olduğunu hatırlayın. Örneğin, aşağıdaki gibi bir ondalık sayı dizisi verildiğinde, basit bir sağlama toplamı, bu sayıların toplamının en sağındaki iki basamağı olabilir:

71 77 61 114 107 75 61 114 100 121

Bu nedenle, bu durumda, sayıları toplayarak 901'i elde edersiniz, 9'u atarsanız ve sağlama toplamınız 01 olur. Şimdi, bu 10 sayıdan oluşan diziyi gürültülü bir iletişim kanalı üzerinden birine gönderirseniz, gürültü bu bilginin bir kısmını bozabilir. Ayrıca sağlama toplamını da gönderirseniz, alıcı sayıların toplanıp toplanmadığını görmek için yeniden hesaplayabilir. Olmazsa, alıcı yeniden gönderim isteğinde bulunacağını bilir.

Sağlama toplamları çok basit fonksiyonlar olduğundan, sağlama toplamının bozuk bir mesaj üzerinde doğru bir şekilde ortaya çıkması mümkündür. Tabii ki, birisinin sayıları kasıtlı olarak sağlama toplamı ile aynı olacak şekilde değiştirmesi de mümkündür. Bu, sağlama toplamlarının güvenliği sağlamadığını; güvenilirliği sağladığını göstermektedir.

Bir özet, hiç kimsenin bir mesajı geçerli bir mesajın özeti ile aynı sonucu verecek şekilde oluşturamayacağı biçimde tasarlanmış bir sağlama toplamıdır. Özetler genellikle sabit bir boyuttadır. Sonuç, bir **özet değeridir (*hash value*)**. Genel olarak, özet değerleri sağlama toplamı değerlerinden daha büyüktür. Özetler verinin parmak izi olarak işlemektedir. Özetleri referans olarak kullanılabilir duruma getirebilirsiniz, böylelikle alıcı bilginin değişip değişmediğini görebilir. Yazılım yayıncıları genellikle özet değerlerini sağlarlar, böylece müşteriler aldıkları yazılımın bütünlüğünü doğrulayabilirler. Etkili olmak için, özetler genellikle, bir bilgisayar korsanının özet değeri ile eşleşen alternatif bir mesaj oluşturmak için uzun bir zamana ihtiyacı olacak kadar uzun olmalıdır.

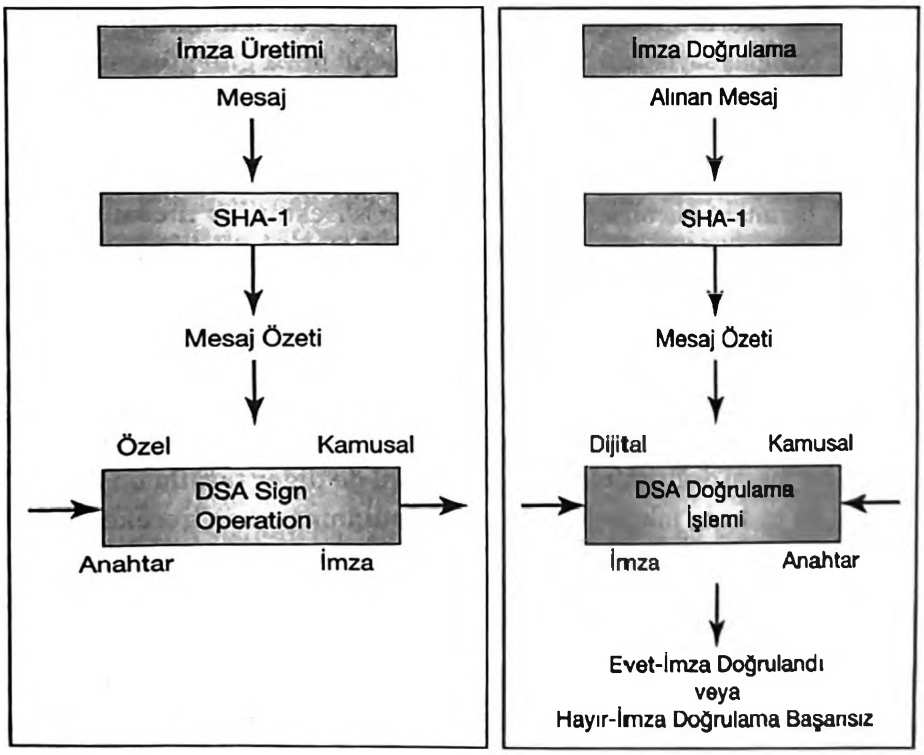
MIT'den Profesör Ronald Rivest - RSA'daki R'nin sahibi - MD5 **mesaj özeti algoritmasını (*message digest algorithm*)** geliştirdi. RFC 1321, algoritma için tanımlamaları içerir. MD5, isteğe bağlı herhangi bir uzunlukta bir girdi alır ve başka bir girdiyi bulmak suretiyle hesaplamasal olarak imkânsız bir 128 bitlik mesaj özeti oluşturur. Bu mesaj özeti kaynağı ile benzersiz bir şekilde ilişkilidir. Bir MD5 özet değerini derlenmiş kaynak kodu gibi bir bilgi ile birlikte yayınlayabilir ve daha sonra bilgiyi özet ile karşılaştırabilirsiniz. Bu, hiçbir kişinin veya virüs gibi bir işlemin bilgiyi değiştirmemiş olduğunu doğrular.

Ancak, MD5 mesaj özetinin henüz imzalı bir özet olmadığını unutmayın. Hiçbir şey, özet ile onu yaratanı tek bir şekilde ilişkilendiremez. Diğer bir deyişle, eğer bir saldırgan bir programı değiştirmek istiyorsa, saldırgan yeni bir MD5 özetini kolayca yeniden hesaplayabilir ve web sitesine her ikisini birlikte gönderebilir. Bir MD5 özetinin varlığı bir dosyanın aslına uygunluğunu (*authenticity*) kanıtlamaz; yalnızca, özeti hesapladığınızdan itibaren dosyanın değişmediğini kanıtlar.

Federal Bilgi İşleme Standardı Yayını 180-1 (*Federal Information Processing Standard Publication* - FIPS 180-1), Güvenli Özet Algoritmasını (*Secure Hash Algorithm* - SHA-1) tanımlar. SHA-1, isteğe bağlı herhangi bir uzunluktaki bir mesajdan 160 bitlik bir özet üretir. MD5 gibi, SHA-1 bir dosyanın yeniden üretilebilmesi hesaplamasal olarak imkânsız olan özgün bir parmak izini oluşturur. SHA-1 o kadar popülerdi ki, SHA-2 ve SHA-3 olarak iki ilave standart üreten gelişmelerle sonuçlandı. Ardışık her sürüm, girdi boyutu ve çıktı uzunluğu seçeneklerini artırır. Tek özet algoritmalar MD5 ve SHA değildir. Özet tabanlı mesaj doğrulama kodu (*hash message authentication code* - HMAC), özeti veya mesaj özetini oluşturmak için bir anahtar kullanan özet fonksiyonudur. RACE Bütünlük Asli Mesaj Değerlendirme Özeti (*RACE Integrity Primitives Evaluation Message Digest* - RIPEMD), çeşitli sayıdaki uygulamalar için özet değerler sağlayan bir fonksiyonlar topluluğudur.

Bir özetten bir dijital imzayı nasıl oluşturursunuz? MD5 veya SHA özetinin çıktısı, girdi olarak özel bir anahtar kullanan asimetrik anahtar algoritması için girdi sağlar. Bu şifrelemenin sonucu, dosya ile özgün bir şekilde ilişkilendirilmiş bir değerdir. Dosyayı imzalayan varlığın kimliğiyle ilgili olarak sahtekârlık yapmak ve ispatlamak hesaplamasal olarak imkânsızdır. FIPS 180-1, bu ilişkiyi gösteren **ŞEKİL 9-7**'deki şemayı içerir.

Bir kimse bir mesajı, yazılımı ya da herhangi başka bir dijital gösterimi dijital olarak herhangi birinin kolayca doğrulayabileceği şekilde imzalayabilir. Bunun, alıcının imzayı doğrulamak için anahtarı aramada kullandığı kamusal anahtar dizininin bütünlüğünü varsaydığını unutmayın.



ŞEKİL 9-7
Özet ve dijital imza algoritmaları arasındaki ilişki.

Eğer bir saldırgan dizine başarıyla girerse, her şey mümkündür. Bu noktada, tilki kümesin güvenliğini sağlamak için kefil olmaktadır.

Şifrelemenin uygulanmasını biraz daha kolaylaştırmak için çeşitli yazılım paketleri vardır. En popüler seçeneklerden ikisi PGP/GPG ve Bcrypt'dir. Oldukça İyi Mahremiyet (*Pretty Good Privacy* - PGP), aslen Phil Zimmerman tarafından yazılan ve veri iletişimi için şifreleme sağlayan bir programdır. PGP en çok e-posta mesajlarını korumak için kullanılır. GNU Mahremiyet Koruyucusu (*GNU Privacy Guard* - GPG), PGP'ye bir alternatif olarak ücretsiz olarak sunulmaktadır. GPG, PGP lisanslarını doğrulayamayan uygulamalarda yaygın olarak kullanılmaktadır. Kriptografik hizmetleri sağlayan bir diğer yaygın yazılım uygulaması Bcrypt'dir. Bcrypt, anahtarları kullanıcı parolalarından türeten bir uygulamadır. Bir kullanıcının kimliğine bağlı olarak değişen parolaları gerektiren birçok uygulamada Bcrypt kullanılır. Parola-Tabanlı Anahtar Türetme Fonksiyonu 2 (*Password-Based Key Derivation Function 2* - PBKDF2), kriptografik anahtarların türetilmesine yardımcı olan başka bir yazılım uygulamasıdır. PBKDF2, RSA Laboratuvarı'nın Açık-Anahtarlı Kriptografi Standartları'nın (*Public-Key Cryptography Standards* - PKCS) bir parçasıdır.

Dijital İmzalar ve İnkar Edememe

Örnek bir işletme durumu verildiğinde, deneyimi olmayan birinin terimleri ile dijital ve dijitalleştirilmiş imzalar arasındaki farkları nasıl belirteceğinizi anlamanız gerekir. İnkar edememeye yönelik olarak dijital imzaları tutmak için gereken altyapıyı ve yasal ihtiyaçları açıklayabilmelisiniz.

Dijital İmzalar ve Dijitalleştirilmiş İmzalar

Bu bölümün başlarında, dijital imzalar ve dijitalleştirilmiş imzalar hakkında bilgi edindiniz. İkisi arasındaki fark çok basit olsa da, birçok insan bunları karıştırır. Yeniden gözden geçirirsek, dijitalleştirilmiş bir imza, fiziksel imzanın dijital biçimde saklanan bir görüntüsüdür. Bu dosya JPG, GIF veya BMP formatında olabilir. Teorik olarak, bir dijital kamerada saklanabilir. Dijitalleştirilmiş bir imzanın temel değeri, basılmış sayfadaki el yazısı mürekkepli imza gibi görünmesini sağlamak için bazen farklı bir renkte hazır mektup formunda yazdırmaktır.

Dijital imza, oldukça farklı bir şeydir. Dijital imzanın, bir mesajın parmak izi gibi davranan güçlü bir özetinin bir kombinasyonu olduğunu hatırlayın. Bunu, simetrik veya asimetrik bir kripto sisteminden gelen gizli bir anahtarla birleştirebilirsiniz. Bu birleşim, bir mesajın belirli bir varlıktan geldiğine ve hiç kimsenin içeriği değiştirmediğine dair çifte güvence verir.

Asimetrik bir kripto sisteminde, imzalayanın kamusal anahtarına erişimi olan herkes dijital imzayı doğrulayabilir. Ancak, yalnızca özel anahtarın sahibi onu oluşturabilir. Simetrik bir kripto sisteminde, hem gönderenin hem de alıcının aynı gizli anahtara ihtiyacı vardır.

Şunu düşünün: Hangi güvenlik prensibini simetrik dijital imza ile sağlayamaz ancak asimetrik dijital imza ile yerine getirebilirsiniz? Cevap, inkar edememedir. Eğer hem gönderen hem de alıcı aynı gizli anahtara sahip ise, bir mesaj değişiminin bir tarafla değil de diğer tarafla başladığını bir başkasına kanıtlayamazsınız. Bu nedenle, inkar edememenin kanıtlanması için gereken koşullar aşağıdaki gibidir:

- Etkili bir asimetrik anahtar algoritması
- Güçlü bir özet fonksiyonu
- Bir dijital imza oluşturmak için özel şifreleme anahtarını özet değerine uygulamanın bir yolu
- Eğer istenirse, kurcalanmaya karşı korumalı veya güvenilir bir üçüncü taraf zamanlama cihazı

- Dijital imzaları doğrulamak için üzerinde anlaşmaya varılmış bir protokol
- Güvenli bir anahtar yönetim ve dağıtım sistemi
- Önceden belirlenmiş bir bütünlük seviyesi olan bir kamusal anahtar havuzu
- İsteksiz taraflardan kamusal anahtarlar üretebilmek için anahtar emanetçiliği (*key escrow*)
- Anlaşmazlıkların üstesinden gelme yöntemleri

Kurumlar, tüm bu adımları bir iş sözleşmesinin bir parçası olarak yazılı olarak açıklamalıdır. İşte ancak o zaman, inkar edememeyi uygulamaya geçirmeye hazırsınız.

Sertifikaların ve Anahtar Yönetiminin Prensipleri

Bu bölümde daha önce anahtar yönetimini öğrendiniz. Anahtar yönetimi, anahtarları olanları oluşturma, dağıtma, saklama, doğrulama, güncelleme, değiştirme ve iptal etme işlemlerini ve anahtar malzemesini (*keying material*) içermektedir.

Bu bölümde, örnek bir klasik anahtar yönetimi şeması yer almaktadır. Enigma, 20. yüzyılın en ünlü şifreleme cihazlarından biriydi. Arthur Scherbius tarafından icat edilmiş, II. Dünya Savaşı öncesi ve sırasında Almanya'nın en önemli şifreleme aracıydı. Makine, bilinen evrendeki atom sayısından daha fazla anahtar konfigürasyonuna sahipti! Uygulamada, anahtar değişiminin uygulanabilir olması için bir anahtar alt kümesi kullanılmıştır. Bununla birlikte, üç rotorlu Enigma, II. Dünya Savaşı'nın başlangıcında baş döndürücü şekilde 158.962.555.217.826.360.000 olası anahtar sundu.

Alman Enigma operatörleri aylık olarak yeni bir kod çizelgesi aldı. Bu kitap, her gün hangi anahtarı kullanacaklarını söyledi. Şimdi, eğer tüm mesajlar aynı anahtarla şifrelenmiş olsaydı, Müttefik kriptanalistler şifresini çözmek için hepsi aynı anahtarla şifrelenmiş çok sayıda şifreli metine sahip olurdu. Bu bir problem olabilirdi. Bu nedenle, anahtar protokolü yalnızca kod defterindeki anahtarı, anahtar-şifreleme anahtarı olarak kullanmanızı gerektirdi. Savaş zamanı Enigma'sında beş karıştırıcı vardı. Enigma kullanıcıları herhangi bir zamanda sadece üç karıştırıcı kullandılar. Kullanıcılar bu karıştırma çarklarının her birini 26 başlangıç pozisyonundan birine, yani alfabenin her bir harfi için bir tane olacak şekilde yerleştirebilirler. Bu nedenle, her mesaj karıştırıcının ayarlanmasıyla başlamaktadır. Gönderenler, anahtarın herhangi bir radyo parazitinden geçtiğinden emin olmak için her mesajı tekrarladı. 60 farklı olası karıştırıcı seçimi ve 26 × 26 × 26 veya 17.576 olası başlangıç konumlarıyla, kullanıcılar her günün mesajlarını 1.054.560 olası anahtardan biriyle şifreleyebilirler. İlk ayarları bilmeden, kriptanalistin 159 kentilyon anahtardan hangisini kullanacağını bilmediğini unutmayın. Enigma şifrelemesi tamamen kırılmazdı, değil mi? Almanlar öyle düşünüyordu. Yanılıyorlardı.

Polonyalı kriptografi uzmanı Marian Rejewski bunu çözdü. Burada Rejewski'nin bunu nasıl yaptığıyla ilgili ayrıntılı bilgi vermek için yeterli alan yok. Onun üstün başarılarına çeşitli kitaplardan bakabilirsiniz. Burada, Rejewski'nin çözümünün şifrelemedeki bir zayıflıktan yararlanmak için saf matematiğin parlak bir şekilde kullanılmasını içerdiğini söylemek yeterli olacaktır. Bu hikâyeden alınacak ders, bir anahtar dağıtım sisteminin güvenli görünmesi ve anahtar sayısının neredeyse sonsuz olmasına rağmen eğer şifreleme algoritmasının kendisinin zayıf yanları varsa, dünyadaki en iyi anahtar yönetim sistemi parlak bir kriptanaliste karşı bir koruma sağlamaz.

Modern Anahtar Yönetim Teknikleri

Günümüzde bilgisayarlar tüm ticari kriptografiyi yönetmektedir. Alandaki en iyi beyinlerden bazıları, bazen on yıllardır tercih edilmekte olan algoritmaları dikkatlice incelemektedir. Bu nedenle, bir saldırgan büyük olasılıkla şifrelemenizi arkasındaki matematiği kırarak yenmeyecektir. İnsan

davranışının - ve en önemlisi, insan hatasının - zayıflığa yol açma olasılığı daha yüksektir. Genellikle sebep kötü anahtar yönetimidir.

Burası, her anahtar yönetim tekniğinin teknik karmaşıklığını incelemek için uygun bir yer değildir. Bunun yerine, farklı iş uygulamaları için hangi tekniklerin uygun olduğuna bakmalısınız. Örneğin, PKI, kesinlikle etkili anahtar yönetimi gerektiren bir teknolojidir. PKI satıcıları yıllardır muazzam bir büyüme sözü verdiler. Ancak, tüm anahtar yönetim bileşenlerini kullanmanın uygulanabilirliği, büyümeyi engelledi. Bu bölümün geri kalan kısmında çeşitli modern anahtar yönetim tekniklerine kısa bir genel bakış yer almaktadır. Kuruluşunuz için hangi tekniğin en iyi sonucu verdiğine karar vermek için bu tartışmayı bir başlangıç noktası olarak kullanın.

Herhangi bir anahtar yönetim stratejisini gerçekleştirmenin en önemli yönlerinden biri güvendir. Birine güvenmelisiniz. Aksi takdirde, herhangi bir kimlik bilgisini geçerli olarak kabul etmeyeceksiniz. En yaygın güven modeli genellikle "güvenilirlik ağı (*web of trust*)" olarak adlandırılır. Bu terim, herhangi bir varlığın başlangıçta kime güveneceğini belirleyeceği bir modeli ifade eder. Buna genellikle doğrudan sorgulama ve yetkilendirme yoluyla karar verilmektedir. Bir varlık güvenilir olduğunda, kuruluş güvenilir varlığın güvendiği diğer kuruluşlara güvenir. Başka bir deyişle, "Güvendiğiniz her kim olursa ona güveniyorum." Bu model, tüm güvenilir varlıklar gerçekten güvenilir olduğunda işe yarar. Diğer model ise, her varlığın, güven uzatılmadan önce güvenilirlik kanıtı sağlamasını zorunlu kılmaktır. Güvenilirlik ağı modelinin gerçekleştirilmesi çok daha kolaydır ancak kötüye kullanıma izin verir. Güvenilmez olan herhangi bir varlık, ağdaki diğer herhangi bir düğümü ona güvenmesi için kandırabilir.

AES

ABD hükümeti şu anda sınıflandırılmamış uygulamalar için kriptografik anahtarları oluşturmak için bir standarda sahip değildir. Bununla birlikte, çalışma grupları bütünlük bilgisi ile birlikte bir düz metin anahtarını güvenli bir şekilde şifreleyecek bir AES anahtar sarmalama (*key wrap*) özelliği tanımlamaktadır. Bu yetenek, sınıflandırılmamış hükümet ortamlarında anahtar yönetimi için bir mekanizma sağlayacaktır.

IPSec

IPSec, İnternet Protokolü (*Internet Protocol* - IP) paketlerini açığa çıkmaktan veya değişikliklerden korur. Protokol mahremiyet ve/veya bütünlük sağlar. Her başlık, belirli bir şifreleme anahtarına karşılık gelen bir güvenlik parametresi endeksi (*security parameter index* - SPI) içerir. Ek olarak, başlık en fazla iki güvenlik başlığı içerebilir. Kimlik Denetleme Başlığı (*Authentication Header* - AH) bütünlük kontrolünü sağlar. Kapsüllenen güvenlik yükü (*encapsulating security payload* - ESP), paketi gizlilik için şifreler. IPSec kullanan ana bilgisayarlar, birbirleriyle bir güvenlik ilişkisi kurar. Bu, SPI sunucusunun yanı sıra hangi kripto yöntemlerinin ve anahtarlarının kullanılacağının kabulünü de içerir. Bir sonraki kısımda öğreneceğiniz İnternet Güvenlik Birliği ve Anahtar Yönetimi Protokolü (*Internet Security Association and Key Management Protocol* - ISAKMP, *ICE-a-kamp* olarak okunur), anahtar yönetim hizmetlerini sağlamaktadır.

ISAKMP

ISAKMP, popülaritesi artan bir anahtar yönetim stratejisidir. RFC 2408, ISAKMP'yi iletişim taraflarının kimliğini denetleyen, güvenlik birlikleri oluşturan ve yöneten, servisin reddi ve yeniden gönderme saldırıları gibi tehditleri azaltan, anahtar oluşturma tekniklerine yönelik prosedürler kümesi olarak tanımlamaktadır. Bütün bunlar, IP Güvenlik Hizmeti veya internet ortamındaki başka bir güvenlik protokolü aracılığıyla güvenli iletişimler kurmak ve sürdürmek için gereklidir.

Güvenlik birliği (*security association* - SA), ISAKMP anahtar yönetiminin temel unsurudur. Bir SA, çeşitli ağ güvenliği hizmetlerini gerçekleştirmek için gereken tüm bilgileri içerir. ISAKMP, SA özelliklerinin formatını kabul etmek ve SA'lar ile pazarlık etmek, SA'ları değiştirmek ve silmek için ortak bir çerçeve görevi görür. RSA ile imzalanmış bir Diffie-Hellman anahtar değişimi kullanmaktadır.

XKMS

Genişletilebilir İşaretleme Dili (*Extensible Markup Language* - XML) anahtar yönetimi özelliği (*key management specification* - XKMS), kamusal anahtarların XML ile birlikte kullanımı için dağıtılması ve kaydedilmesi için protokolleri gösterir. XML, yapılandırılmış bilgi içeren belgeler için bir işaretleme dilidir. Karmaşık yapılandırılmış belgelerin Web üzerinden paylaşılmasını destekleyen sözdizimini sağlar.

Yönetilen PKI

Bazı satıcılar kamusal anahtar yönetimi ile ilgili sorunları ele almak için yönetilen bir hizmet sunar. Hizmetler arasında merkezi anahtar üretimi, dağıtımı, yedeklemesi ve kurtarması bulunur. Anahtar yönetim altyapısı oluşturmak yerine, müşteriler bu ayrıntıları dış kaynaklardan sağlamayı seçebilir.

ANSI X9.17

Finans endüstrisi bu standardı anahtar yönetim yöntemlerini tanımlamak için yarattı. Birçok üreticinin donanım şifreleme aygıtlarında kullandığı simetrik bir anahtar değişim protokolünü tanımlamaktadır. Asimetrik anahtar değişimi bazı avantajlar sunsa da, kuruluşların X9.17 uyumlu donanıma önemli miktarda para yatırmış olmaları, onu bir süre kullanmaya devam edecekleri anlamına gelmektedir. FIPS Pub 171'e göre, X9.17 aşağıdakiler için minimum standartları belirtir:

- Yetkilendirilmemiş açıklama, değiştirme veya yerine koymayı engellemek için anahtar malzemesinin kullanım ömrü boyu kontrolü
- Kriptografik donanım veya tesisler arasında birlikte çalışabilirliğe izin vermek için anahtar malzemesinin dağıtılması
- Üretimi, dağıtımı, saklanması, girişi, kullanımı ve imhası da dahil olmak üzere anahtar malzemesinin bütünlüğünün ömrünün tüm aşamalarında sağlanması
- Anahtar malzemesinin bütünlüğü sorgulandığında anahtar yönetim işlemcisinin çalışmaması durumunda kurtarma.

Kuruluşunuz için bir anahtar yönetim ürünü veya tekniği seçtiğinizde, öncelikle ödevinizi yapın. Her yöntemin avantajları ve dezavantajları vardır. Belirli maliyetin yanı sıra devam eden bakım ve yönetim maliyetlerini de anladığınızdan emin olun.

BÖLÜM ÖZETİ

Bu bölümde, kriptografinin nasıl çalıştığını ve işletme sorunlarının çözümü için nasıl uygulandığını öğrendiniz. Anahtar kriptografik terimleri ve iş ilkelerini, bu ilkelere kriptografinin nasıl uygulanacağını ve kriptografiye dayanan güvenlik araçlarını nasıl belirlediğinizi öğrendiniz. Ayrıca, simetrik ve asimetrik şifrelemelerin kriptanalize ilişkin avantaj ve dezavantajlarını da öğrendiniz.

ANAHTAR KAVRAMLAR VE TERİMLER

Algorithm - Algoritma
Asymmetric key cryptography - Asimetrik anahtar kriptografisi
Attribute-based encryption (ABE) - Öznitelik tabanlı şifreleme (ABE)
Authentication - Kimlik denetleme
Block cipher - Blok şifreleme
Caesar cipher - Sezar şifreleme
Certificate authority (CA) - Sertifika yetkilisi (CA)
Checksum - Sağlama toplamı
Cipher - Şifreleme
Ciphertext - Şifreli metin
Cleartext - Açık metin
Confidentiality - Gizlilik
Connection encryption - Bağlantı şifreleme
Cryptanalysis - Kriptanaliz
Cryptography - Kriptografi
Cryptogram - Kriptogram
Cryptosystem - Kripto sistemi
Data Encryption Standard (DES) - Veri Şifreleme Standardı (DES)
Decryption - Şifre çözme
Differential cytpanalysis - Diferansiyel kriptanaliz
Diffie-Hellman algorithm - Diffie-Hellman algoritması
Diffie-Hellman in ephemeral *mode (DHE)* - Ephemeral modunda Diffie-Hellman (DHE)
Digital signature - Dijital imza
Digital signature algorithm (DSA) - Dijital imza algoritması (DSA)
Digitized signature - Dijitalleştirilmiş imza
Elliptic curve cryptography (ECC) - Eliptik eğri kriptografi (ECC)
Elliptic Curve DHE (ECDHE) - Eliptik Eğri DHE (ECDHE)
Encryption - Şifreleme
Hash - Özet
Hashing function - Özet fonksiyonu
Identity-based encryption (IBE) - Kimlik tabanlı şifreleme (IBE)
In-band key exchange - Bant içi anahtar değişimi
Integrity - Bütünlük
Key - Anahtar
Key directory - Anahtar dizini
Key distribution - Anahtar dağıtımı
Key escrow - Anahtar emaneti
Key management - Anahtar yönetimi
Key revocation - Anahtarın iptal edilmesi
Key-encrypting key - Anahtar şifreleme anahtarı
Key stretching - Anahtar uzatma
Keyspace - Anahtar uzayı
Keyword mixed alphabet cipher - Anahtar kelime karıştırılmış alfabe şifrelemesi
Message digest algorithm (MD5) - Mesaj özeti algoritması (MD5)
Nonrepudiation - İnkâr edememe
One-time pad cipher - Tek kullanımlık şifreleme
One-way algorithm - Tek yönlü algoritma
Open cipher - Açık şifreleme
Out-of-band key exchange - Bant dışı anahtar değişimi
Perfect forward secrecy - Mükemmel iletme gizliliği
Plaintext - Düz metin
Private (symmetric) key - Özel (simetrik) anahtar
Product cipher - Birleşik şifreleme
Public (asymmetric) key - Kamusal (asimetrik) anahtar
Public key cryptography - Kamusal anahtar kriptografisi
Public key infrastructure (PKI) - Açık anahtar altyapısı (PKI)
Quantum cryptography - Kuantum kriptografi
Revocation - İptal etme
Rivest-Shamir-Adelman (RSA) - Rivest-Shamir-Adelman (RSA) *Salt value* - Tuz değeri
Secure Hash Algorithm (SHA) - Güvenli Özet Algoritması (SHA)
Secure Shell (SSH) - Güvenli Kabul (SSH)
Security association (SA) - Güvenlik birliği (SA)
Session key - Oturum anahtarı
Simple substitution cipher - Basit yerine koyma şifrelemesi
SSL handshake protocol - SSL tokalaşma protokolü
Steganography - Steganografi
Stream cipher - Kesintisiz şifreleme
Substitution cipher - Yerine koyma şifrelemesi
Symmetric key cryptography - Simetrik anahtar kriptografisi
Timestamping - Zaman damgası
Transport encryption - Aktarım şifrelemesi
Transposition cipher - Yer değiştirme şifrelemesi
Vernam cipher - Vernam şifrelemesi
Vigenère cipher - Vigenère şifrelemesi

BÖLÜM 9 DEĞERLENDİRME

1. _____ dört güvenlik hedefine ulaşmak için bir mekanizma sunar: gizlilik, bütünlük, kimlik denetleme ve inkar edememe.
   A. Güvenlik birliği (SA)
   B. Güvenli Soket Katmanı (SSL)
   C. Kriptografi
   D. Yukarıdakilerin hiçbiri

2. Güçlü bir özet fonksiyonu, sahte bir mesajın geçerli bir mesajla aynı özet ile sonuçlanmaması için tasarlanmıştır.
   A. Doğru
   B. Yanlış

3. Düz metnin şifreli metne dönüştürülmesi işlemi _____ olarak bilinmektedir.
   A. Şifre çözme
   B. Şifreleme
   C. Düz metin
   D. Açık metin

4. Kriptografik amaçlar için kullanılan bir algoritma _____ olarak bilinmektedir.
   A. Özet B. Özel anahtar
   B. Kamusal anahtar
   C. Şifreleme

5. Şifrelemeler iki genel kategoriye ayrılır: simetrik (özel) anahtar ve asimetrik (kamusal) anahtar.
   A. Doğru
   B. Yanlış

6. Şifreleme ve şifre çözme için aynı anahtarı kullanan bir şifrelemeye _____ anahtarlı denir.
   A. Simetrik (özel)
   B. Asimetrik (kamusal)
   C. Şifreleme
   D. Özet
   E. Hiçbiri

7. _____ bir varlığın, göndericinin, göndericinin bilgisayarının, bir cihazın ya da bazı bilgilerin kimliğini doğrular.
   A. İnkar edememe
   B. Gizlilik
   C. Bütünlük
   D. Kimlik denetleme

8. Aşağıdakilerden hangisi bir kriptografik saldırının dört temel formundan birisidir?
   A. Şadece şifreli metin saldırısı
   B. Bilinen düz metin saldırısı
   C. Seçilmiş düz metin saldırısı
   D. Seçilmiş şifreli metin saldırısı
   E. Hepsi

9. Yer değiştirme ve yerine koyma şifrelemenin iki temel türüdür.
   A. Doğru
   B. Yanlış

10. Bir _____ sahteciliği tespit etmek için kullanılmaktadır.
    A. Özet fonksiyonu
    B. Sağlama toplamı
    C. Özet değeri
    D. KDC

11. 11. DES, IDEA, RC4, ve WEP _____ örnekleridir.
    A. Anahtarın iptal edilmesi
    B. 802.11b kablosuz güvenlik
    C. Asimetrik anahtar algoritmalar (ya da standartlar)
    D. Simetrik algoritmalar (ya da standartlar)

12. Bir _____ imza dijital bir formatta saklanan fiziksel imzanın bir temsilidir.
    A. Dijital
    B. Dijitalleştirilmiş
    C. Özel anahtar
    D. Kamusal anahtar

BÖLÜM

10

Ağ ve Telekomünikasyon

Bilgisayar ağları ve telekomünikasyon, günümüzde birçok ticari işletmenin ve kurumun iş altyapısının kritik parçalarıdır. **Telefon hizmeti (*telephony*)**, tüm elektronik iletişimi destekleyen servislerin geliştirilmesi ve konuşlandırılmasını içeren bir teknoloji alanıdır. Ağlar kullanılamaz haldeyken veya **hata yapma eğilimi (*prone to error*)** gösterdiğinde, birçok kurum çalışamaz hale gelecektir. Ağ güvenliği; bir kurumun ağ kullanılabilirliği, bütünlüğü ve gizliliği için hayati ihtiyaçlarını karşılamayı içerir. Ağ üzerinden iletilen veriler, kazara veya kasıtlı olarak değiştirilmekten korunmalı, yetkisiz taraflar tarafından okunamamalı, kaynak ve hedef doğrulaması yapılabilmelidir (inkar edilemezlik). Ticari ve güvenlik gereksinimleri aşağıdaki gibidir:

- Erişim denetimi
- Ağ kararlılığı ve güvenilirliği
- Bütünlük
- Kullanılabilirlik
- Gizlilik veya inkar edilemezlik

Bu bölümde ağlar ve telekomünikasyonun nasıl güvenli hale getirilebileceği incelenmektedir. Bir ağın temel unsurları tanıtılmakta ve ağları çevreleyen güvenlik sorunları açıklanmaktadır. Verinin, bilgisayar ağı boyunca dolaşırken güvenliğini sağlamak için oluşturulan bazı yapı taşları sunulmaktadır.

Bir güvenlik uzmanı olarak, ağların ve telekomünikasyonun aşağıda belirtilen unsurlarını anlamanız gerekmektedir:

- Açık Sistemler Ara Bağlantısı (*Open Systems Interconnection* - OSI) Referans Modeli
- Ağ topolojisi
- İletim Denetimi Protokolü / İnternet Protokolü (*Transmission Control Protocol/Internet Protocol* - TCP / IP) ağ oluşturma
- Kablosuz ağ oluşturma
- Ağ güvenliği

10. Bölüm Konular

Bu bölüm aşağıda verilen konuları ve kavramları içermektedir:

- Açık Sistemler Ara Bağlantısı (*Open Systems Interconnection* - OSI) Referans Modeli'nin ne olduğu
- Ana ağ türlerinin hangileri olduğu
- TCP/IP'nin ne olduğu ve nasıl çalıştığı
- Ağ güvenlik risklerinin neler olduğu
- Temel güvenlik savunma araçlarının neler olduğu
- Kablosuz ağların nasıl çalıştığı ve ağ güvenliğine hangi tehditleri oluşturduğu

10. Bölüm Hedefler

Bu bölümü tamamladığınız zaman, yapabilecekleriniz:

- OSI Referans Modeli'ni tanımlamak
- Ağ türlerini, ağ protokollerini ve ağ güvenlik risklerini anlamak
- Ağ güvenliği risklerine karşı savunmak için kullanılabilecek bazı temel araçları öğrenmek
- Kablosuz ağ oluşturmayı anlamak ve ortaya çıkarabildiği ağ güvenliği tehditlerini anlamak

Açık Sistemler Ara Bağlantısı Referans Modeli

Açık Sistemler Ara Bağlantısı (*Open Systems Interconnection* - OSI) Referans Modeli, bir ağ ve kaynaklarını kurmak ve kullanmak için bir şablondur. OSI Referans Modeli, biri ötekinin yerine konulabilir katmanlarla ağ oluşturmanın teorik bir modelidir. Bunun güzelliği, diğer katmanların nasıl çalıştığından endişelenmeden herhangi bir katman için teknoloji tasarlayabilmenizdir. Her katmanın, üst ve alt katmanlarla nasıl konuşulacağını bildiğinden emin olmak yeterlidir. **ŞEKİL 10-1** OSI Referans Modeli katmanlarının her birini göstermektedir.

OSI Referans Modeli katmanları aşağıdaki gibidir:

- **Uygulama Katmanı (*Application Layer*)**—Bu katman, son kullanıcılar ile etkileşimden sorumludur. Uygulama Katmanı, ağda etkileşim kuran bir bilgisayardaki tüm programları içerir. Örneğin, e-posta yazılımınız ağ üzerinden ileti gönderip alması gerektiğinden bu katmana dahil edilmiştir. Solitaire gibi basit bir oyun buraya uygun değildir çünkü çalışması için bir ağa ihtiyacı bulunmamaktadır.
- **Sunum Katmanı (*Presentation Layer*)**—Bu katman, verilerin kodlanmasından sorumludur. Sunum Katmanı dosya biçimlerini ve karakter gösterimlerini içerir. Şifreleme genellikle sunum katmanında gerçekleşir.
- **Oturum Katmanı (*Session Layer*)**—Bu katman, bilgisayarlar arasındaki iletişim oturumlarını sürdürmekten sorumludur. Oturum Katmanı, ağ üzerinden gerçekleşen süreçler arasında oluşan iletişimleri oluşturur, bunları sürdürür ve bağlantıyı keser.

ŞEKİL 10-1
OSI Referans Modeli



İPUCU

OSI Referans Modelinin katmanlarını hatırlamayı kolaylaştırmak için şu anımsatıcı verilebilir. Örneğin, "Uygulamayı Sunduğumuz Oturumda Aktarım Ağının Veri Bağlantısı Fiziksel dir." (İngilizce olarak: "All People Seem To Need Data Processing")

- **Aktarım Katmanı (*Transport Layer*)**—Bu katman, verilerin paketlere ayrılmasından ve ağ üzerinden uygun bir şekilde iletilmesinden sorumludur. Akış kontrolü (*flow control*) ve hata kontrolü (*error checking*) Aktarım Katmanı'nda gerçekleşir.
- **Ağ Katmanı (*Network Layer*)**—Bu katman, ağın mantıksal uygulanmasından sorumludur. Ağ Katmanı'nın çok önemli bir özelliği olan mantıksal adresleme özelliği, bu bölümün ilerleyen bölümlerinde ele alınacaktır. TCP/IP ağ oluşturmada, mantıksal adresleme bilinen IP adresleri biçimini alır.
- **Veri Bağlantı Katmanı (*Data Link Layer*)**—Bu katman, aynı yerel alan ağına (*local area network* - LAN) bağlı bilgisayarlardaki bilgileri iletmekten sorumludur. Veri Bağlantı Katmanı, Ortam Erişim Kontrolü (*Media Access Control* - MAC) adreslerini kullanır. Aygıt üreticileri, her donanım aygıtına benzersiz bir MAC adresi atar.
- **Fiziksel Katman (*Physical Layer*)**—Bu katman, ağın fiziksel çalışmasından sorumludur. Fiziksel Katman, bilgisayar dilinin ikili verileri olan birler ve sıfırlarını aktarma ortamının diline çevirmelidir. Örneğin bakır ağ kablolarında, bilgisayar verilerinin elektriksel sinyallere (*pulse*) dönüştürülmesi gerekir. Fiber optik kullanılması durumunda, verinin ışık patlamaları haline çevrilmesi gerekmektedir.

OSI Referans Modeli, geliştiricilerin her katmanda bağımsız olarak üretim yapabilmelerini sağlar. Uygulama Katmanı'nda çalışan bir e-posta programı yazarsanız, bilginin yalnızca Sunum Katmanı'na indirilmesi konusunda endişelenmeniz yeterli olacaktır. Bu durumda kullandığınız ağın ayrıntıları programınızla ilgisiz olacaktır. Diğer yazılımlar sizin için bunların çaresine bakacaktır. Benzer şekilde, Fiziksel Katman'da kablolar geliştiren bir firmaysanız, o kabloda hangi Ağ Katmanı protokollerinin geçeceği hakkında endişelenmeniz gerekmeyecektir. Veri Bağlantı Katmanı gereksinimlerini karşılayan bir kablo üretmeniz yeterlidir.

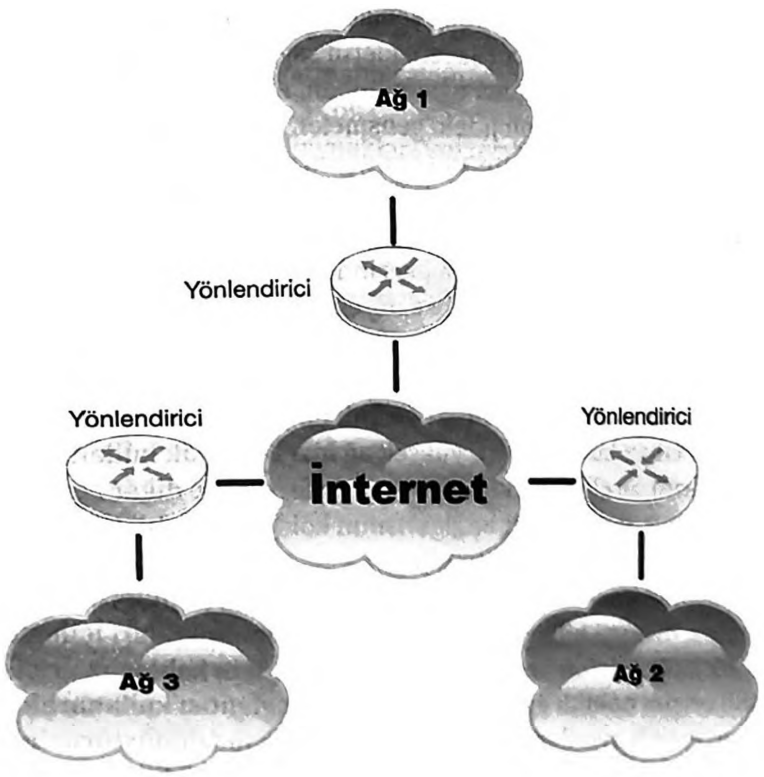
Ana Ağ Türleri

Bir güvenlik uzmanı olarak, ağ oluşturma hakkında bir çok şey öğreneceksiniz. Bilgisayar ağları ve nasıl korunacağı hakkında iyi bir bilgiye sahip olmanız, kurumunuzu ağ hatasından veya veri ihlalinden korumanız için kritik öneme sahiptir. Güvenlik alanında kullanılan birçok cihaz, ağları korumaktadır. Ağları korumayanlar da genellikle ağların işlevlerine güvenmektedir. Bu bölümde, sizin iki ana tür ağı -geniş alan ağları (*wide area networks* - WAN) ve yerel alan ağları (*local area networks* - LAN)- incelemeniz ve işlevlerini keşfetmeniz hedeflenmiştir. Ayrıca LAN'ınızı bir WAN'a bağlamanız için gereken bazı yöntemleri inceleyeceksiniz. Son olarak, en önemli ağ aygıtlarına kısaca göz atacaksınız.

Geniş Alan Ağları

Adından da anlaşılacağı üzere, WAN'lar sistemleri büyük bir coğrafi alan üzerinden bağlar. WAN'ın en bilinen örneği internettir. **ŞEKİL 10-2**'de gösterildiği gibi, internet birçok bağımsız ağı birbirine bağlar. Bu da farklı konumlardaki kişilerin birbirleriyle kolayca iletişim kurmalarına olanak tanır. İnternet, bu sürecin ayrıntılarını son kullanıcıdan gizler. Bir e-posta mesajı gönderdiğinizde, verilerin nasıl taşınacağı konusunda endişelenmenize gerek yoktur. Siz sadece göndere tıklarsınız ve ağın tüm karmaşıklıkla ilgilenmesine izin verirsiniz.

Güvenlik açısından bakıldığında, internetin açık bir ağ olduğunu unutmamak önemlidir. Veriler ağınızı terk ettiğinde veri mahremiyetini garanti edemezsiniz.



ŞEKİL 10-2
Geniş alan ağları.

Veriler, hedeflerine ulaşmak için herhangi bir yol izleyebilirler. Herhangi birisi bu verileri yol boyunca okuyabilir. İnternetteki verileri, kapalı bir zarftaki mektuptan daha çok, bir kartpostal gibi düşünün. Neyse ki şifreleme gibi bir güvenlik teknolojisi, verilerinizi internete gönderirken onun içeriğini gizlemenizi sağlar. Bu, yine bir kartpostal göndermek gibidir ancak bu sefer mesajı gizli bir kodla yazmaya benzer. Ağ şifreleme hakkında bu bölümde daha sonra daha fazla bilgi edineceksiniz.

Günümüzdeki kurumların birçoğu, interneti farklı konumları birbirlerine bağlamak ve müşterileri ile bağlantı kurmak için kullanmaktadır. Bu, konumları birbirine bağlamak için düşük maliyetli bir yoldur çünkü bir ağın internete bağlanması genellikle kolay ve ucuzdur. Ancak, internet gibi açık bir ağın kullanımından gelen güvenlik sorunlarını göz önünde bulundurduğunuzdan emin olmalısınız. Yine, şifreleme teknolojisi, interneti kullanma riskini azaltmanıza yardımcı olabilecektir.

Bazı kuruluşlar, uzak konumlarını ana merkezlerine bağlamak için kendi özel ağlarını kullanmayı tercih eder. Bazıları bunu güvenlik nedenleriyle yapmayı seçerler; diğerleri sadece özel ağların garanti edilen güvenilirliğini isterler. Bu güvenlik ve güvenilirlik nedenleriyle çok iyi bir seçenek olsa da, aynı zamanda çok pahalıdır. Bununla beraber, kendi özel WAN'ınızı geliştirmek için bir komünikasyon servis sağlayıcısı ile de çalışabilirsiniz.

Bağlantı Seçenekleri

İnternete bağlanmak için kullanabileceğiniz birden fazla yöntem vardır. Çoğu ev kullanıcısı, telekom şirketinden bir kablo modem veya bir dijital abone hattı (*digital subscriber line* - DSL) seçer. Ancak bunlar tek seçenek değildir. İnternet servis sağlayıcıları (*internet service provider* - ISP) fiber optik kullanımıyla giderek artan oranda yüksek bant genişliğine sahip internet hizmeti vermeye başlamışlardır. Bu tür bir hizmet, önceki servis seçeneklerine göre çok daha hızlı internet bağlantıları sağlamaktadır. Kablo, DSL veya fiber optik servislerine erişimi olmayan kullanıcılar; uydu veya modası geçmiş çevirmeli bağlantı (*dialup*) hizmetleri kullanarak internete bağlanmaya devam edebilirler. İnternet kullanımı arttıkça, ISP'ler bağlanma şekillerine daha fazla seçenek katmaktadır. Bir çok durumda, internete bağlanmak için mevcut seçeneklerin sayısı yaşadığınız yere bağlıdır. Daha yoğun nüfuslu alanlar, daha fazla seçenek sunma eğilimindedir. Ayrıca, internete kablosuz bir operatör ile de bağlanabilirsiniz. Kablosuz teknolojideki gelişmeler, birçok alanda hücresel bağlantıları uygun fiyatlı hale getirmekte ve servis alanı kapsamı her geçen gün artmaktadır.

Akıllı telefonlar genellikle üçüncü nesil (3G) veya dördüncü nesil (4G) ağlara bağlanmaktadır. Bu cihazların birçoğunun 802.11 standartlarını kullanarak Wi-Fi ağlarına bağlanma yeteneği de vardır. Hücresel 3G ve 4G şebekeleri, geniş bir alan üzerinden sürekli bir internet ve ses iletişimi sağlar. İnternete olan bağlantılar sürekli gibi görünse de, cihazlar aslında bir hücreden başka hücreye doğru hareket etmektedir. Bir hücreden diğerine yapılan bu teslim, kullanıcı için görünmezdir ve bağlantıların sanki sürekliymiş gibi görünmesini sağlar. Bununla birlikte, çoğu hücresel şebeke operatörü, veri aktarım sınırları tanımlar ve kullanıcılar bu sınırları aştığında erişim için ücret talep ederler. Mobil cihaz kullanıcıları, yüksek ağ hızı ve düşük kullanım maliyetleri nedeniyle Wi-Fi ağ bağlantılarını tercih etmektedir. Birçok kafe, otel ve diğer çeşitli yerde ücretsiz Wi-Fi erişimi bulmak zor değildir. Bu internet bağlantısının kolaylığı, mobil bilişimi ortalama bir kullanıcı için gerçek bir seçenek haline getirmektedir.

Bu hücresel ağlar, bireysel kullanıcılar ve ticari işletmeler için çok popülerdir. Günümüzdeki operatörler mevcut durumda, dizüstü bilgisayarlar ve mobil erişim noktaları için cihazlar sunmaktadırlar. Aslında, birçok akıllı telefon ve tablet, diğer cihazlar için kablosuz erişim noktaları gibi davranabilir. Bu mobil erişim noktalı aygıtlar, hücresel ağ bağlantısı kullanarak internete bağlanırlar ve bu bağlantıyı yeterli aygıtlar için bir Wi-Fi bağlantısına dönüştürürler. Bu da taşıyıcınızın kapsama alanında bulunduğunuz herhangi bir yerde; bir dizüstü bilgisayarı, akıllı telefonu

ve hatta başka birkaç cihazı internete bağlayabileceğiniz anlamına gelmektedir. Bu yetenek, ücretsiz Wi-Fi'yi kullanmaktan çok daha büyük bir avantaj olabilir. İnternet bağlantı hızları, 3G veya 4G kablosuz erişim cihazları kullanıldığında genellikle daha yavaştır. Bununla birlikte, bu gibi bağlantılar çok daha güvenlidir. İnternet bağlantınızı bir kafede aynı ağı kullanan bir saldırganla paylaşma konusunda endişelenmeniz gerekmez. Herkese açık Wi-Fi şebekelerinin çoğu çok güvensizdir. Sizin tüm trafiğinizi dinleyen başka birisiyle aynı ağı paylaşıp paylaşmadığınızı asla bilemezsiniz. Güvenli bir bağlantı elde etmek için biraz hız feda etmek buna değebilecektir.

İnternet servislerinin ticari işletmeler için birçok seçeneği bulunmaktadır. Şaşırtıcı bir şekilde, bunların bir çoğu ev kullanıcılarına sunulan ile aynı seçeneklerdir. Örneğin çoğu ISP, tüketici tekliflerine ek olarak ticari servisleri sunar. Bu genellikle ticari kullanıcılarının ihtiyaçlarını desteklemek için ev bağlantılarından daha yüksek bir hızdadır. Tabii ki ISP'ler, genellikle bu artan hız için daha fazla ücret talep etmektedir.

Bir anlığına OSI Referans Modeline geri dönüp bakalım. Unutulmaması gereken önemli şey, seçtiğiniz bağlanabilirlik seçeneğinin ağınızla neler yapabileceğinizi etkilememesidir. Farklılıklar, sinyalin binanıza geliş yöntemi (telefon hatları, kablo yolları veya tahsisli kablolar), hızı ve servisinizin güvenilirliği ile ilgilidir.

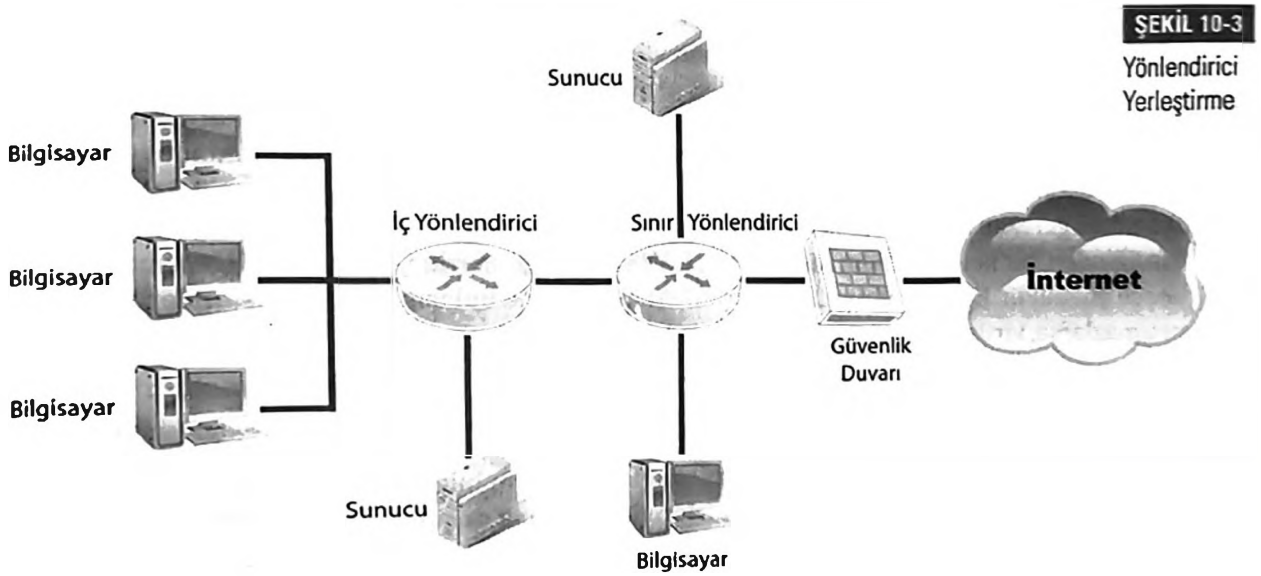
Yönlendiriciler

Bir **yönlendirici (*router*)**, iki veya daha fazla ağı bağlayan ve aralarındaki veri paketleri alışverişini seçime bağlı olarak karşılıklı alıp veren bir aygıttır. Bir yönlendirici bir LAN'ı bir WAN'a bağlar ve her paketi nereye göndereceğine karar vermek için ağ adreslerini inceler.

Ağ mimarisinde bir yönlendiricinin nasıl yerleştirildiği, yapılandırma seçeneklerini etkilemektedir. Yönlendiricileri iki temel konuma yerleştirebilirsiniz (bkz. **ŞEKİL 10-3**):

- **Sınır yönlendiricileri (*Border router*)**—Bir sınır yönlendirici, dış kaynaktan gelen doğrudan saldırıya maruz kalır. Herhangi bir yönlendiriciyi yapılandırdığınızda, bu cihazın savunmanın tek noktası mı yoksa çok katmanlı savunmanın bir parçası mı olduğu belirlenmelidir. Tabii ki, bir çokvkatmanlı savunma çok daha iyi ve daha güvenlidir. Savunmanın tek noktası olarak kullanılan yönlendirici, iç kaynakları koruyabilir ancak kendisi saldırılara açıktır.

ŞEKİL 10-3
Yönlendirici Yerleştirme



- **İç yönlendiriciler (*Internal router*)**—Bir iç yönlendirici, iç ağlarınıza gelişmiş özellikler de sağlayabilir. İç yönlendiriciler, alt ağ trafiğini ayrı tutmaya yardımcı olabilir. Trafiği bir alt ağdan uzak tutabileceği gibi, trafiği bir alt ağın içinde de tutabilirler. Örneğin, bir kuruluşun Ar-Ge departmanının ağı ile kuruluşun geri kalan ağı arasındaki konumlandırılan bir iç yönlendirici, iki ağı ayrı tutabilecektir. Bu yönlendiriciler, gizli trafiği Ar-Ge departmanı içinde tutabilir. Araştırma dışı trafiğin kurumun diğer ağlarından Ar-Ge ağına geçmesini de engelleyebilirler.

İPUCU

Yönlendiricileri nereye konumlandırdığınıza bakmaksızın, onların güvenli olduğundan emin olmalısınız.

Bir **güvenli yönlendirici yapılandırması (*secure router configuration*)**, yönlendiricinizin sadece geçerli ağ trafiğini geçerli düğümlere ve geçerli düğümlerden akmasını sağlayan bir ayarlar bütünüdür. Her bir yönlendiriciyi uygun bir şekilde yapılandırmak için zaman ayırmanız gerekir; ardından yetkisiz yapılandırma değişikliklerinin gerçekleşmediğinden emin olmak için her bir yönlendirici izlenmelidir. Saldırganlar, saldırıların daha başarılı olmasını sağlamak için ağ cihazlarını yeniden yapılandırmayı severler.

Yönlendiricileri, tüm trafiğin geçmesine izin verecek veya bazı iç kaynakları koruyacak şekilde yapılandırabilirsiniz. Yönlendiriciler, güvenlik önlemlerini ilerletmek için **ağ adresi çevirisi (*network address translation* - NAT)** ve paket filtreleme yöntemlerini kullanabilir. NAT, bir sistemin gerçek **IP adresini** gizlemek için değişen bir genel IP adresi kullanır. NAT'ın asıl amaçlarından biri, IP adreslerinin sayısal eksikliğini telafi etmekti. Günümüzde ise bir cihazın gerçek IP adresini gizleyerek güvenlikte yardımcı olmak için kullanılmaktadır. Bir saldırgan, NAT kullanan bir güvenlik duvarı arkasındaki ağ düzenini tanımlamakta daha da zorlanacaktır.

Paket filtreleme, bir yönlendirici veya güvenlik duvarı işlevidir. Yönlendirici veya güvenlik duvarı her bir veri paketi aldığı durumda filtreleme gerçekleşir. Cihaz, her gelen paketi ağ yöneticisi tarafından yapılandırılan bir kurallar listesiyle karşılaştırır. Kurallar, cihaza paketi ağa kabul etmesi veya reddetmesi gerektiğini söyler. Hiçbir kuralla eşleşmediğinde ise güvenlik duvarı paketi otomatik olarak engeller.

NAT ve paket filtreleme, yönlendiricilerinizi ağınızı savunmaya yardımcı olmak için kullanmanın iki iyi yoludur. Temel saldırılara karşı birtakım savunma sağlarlar. Bununla birlikte, hiç bir teknolojinin bir "sihirli değnek" olmadığını hatırlamak önemlidir. Ağınızı korumak için güvenlik duvarlarını ve verilerinizin güvenliğini sağlamak için bu kitapta açıklanan diğer teknolojileri kullanmalısınız.

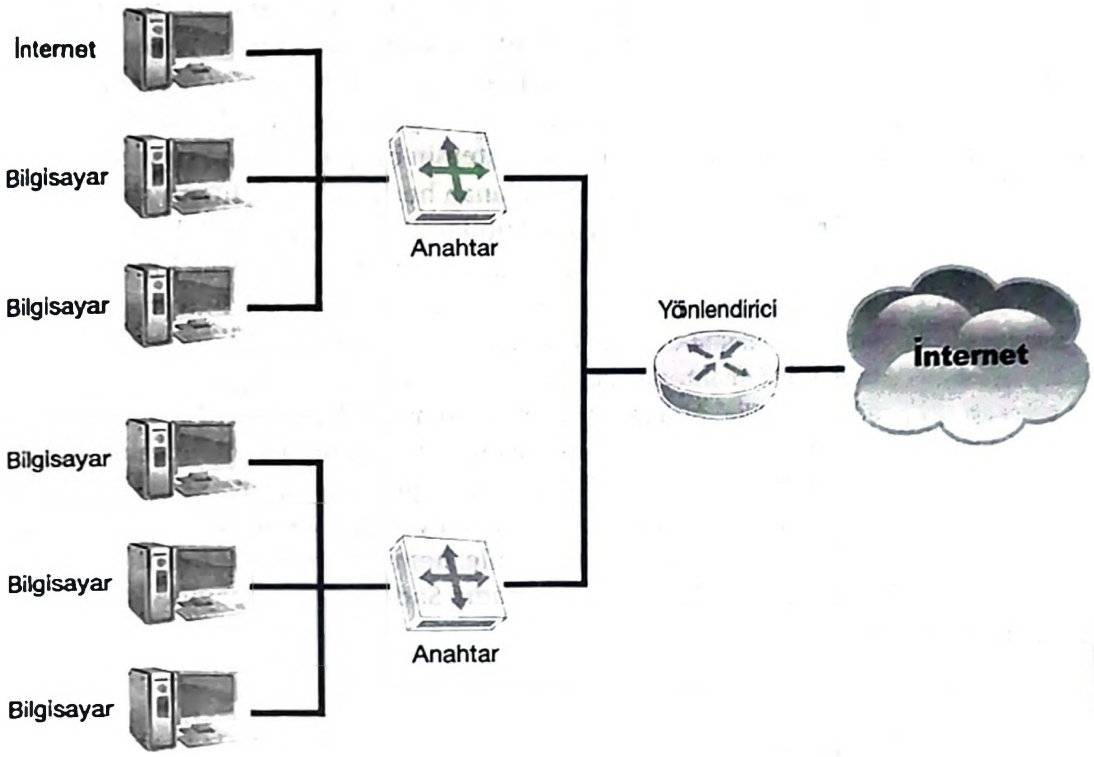
Yerel Alan Ağları

LAN'lar aynı coğrafi alanda bulunan bilgisayarlara ağ bağlantısı sağlar. Bu bilgisayarlar genellikle birbirlerine dağıtım kutuları (*hub*) ve anahtarlar gibi cihazlarla bağlanırlar. Bu ağ anahtarlama altyapısı, **ŞEKİL 10-4**'de gösterildiği gibi kurumun yönlendiricisinin arkasında bulunmaktadır.

Aynı LAN üzerindeki sistemler kendilerini birbirlerinden çoğu durumda korumaz. LAN sistemleri arasındaki gereken iş birliği, genellikle internetten izin vermeyeceğiniz türden bağlantıları gerektirdiğinden, bir nevi kasıtlıdır. Bu nedenle, LAN'daki sistemlerde iyi bir güvenliğe sahip olmak son derece önemlidir. Eğer bir virüs LAN üzerindeki bir sisteme bulaşır ve diğer sistemler kendilerini korumazlarsa, virüs LAN'daki tüm sistemlere hızlı bir şekilde yayılabilir.

Ethernet Ağları

Yaklaşık on yıl önceye kadar bir çok farklı LAN türü vardı. Şimdi neredeyse her ağ, Ethernet adı verilen tek bir teknolojiye geçiş yaptı. İlk Ethernet ağlarında, tüm bilgisayarlar tek bir kabloya bağlıydı ve ağı kullanım hakkı elde etmek için birbirleriyle yarışmak durumundaydılar. Bu, verimsiz bir çalışma şekliydi. Neyse ki, teknoloji gelişti. Modern Ethernet ağları, her sistem için adanmış



ŞEKİL 10-4
Yerel ağlar.

bir bağlantı kullanmaktadır. Bu Ethernet kablosu, her sistemi LAN'ı kontrol eden bir ağ anahtarına (*switch*) bağlar.

Ethernet standardı, bilgisayarların ağda iletişim yöntemini tanımlar. Ethernet, OSI Referans Modelinin Fiziksel ve Veri Bağlantı katmanlarını yönetir. Ethernet, bilgisayarların ağdaki birbirleriyle iletişim kurmak için MAC adreslerini nasıl kullandıklarını tanımlar. Ethernet, en yaygın kullanılan LAN teknolojisi haline gelmiştir. Rakip teknolojilerin çoğunda bile Ethernet'in üstünde çalışan farklı çeşitleri bulunmaktadır. Örneğin, **İnternet Küçük Bilgisayar Sistem Arayüzü (*Internet Small Computer System Interface* - iSCSI)**, veri depolama aygıtlarını IP kullanan ağlara bağlamak için kullanılan taşıma katmanı için bir depolama ağı oluşturma standardıdır. Optik ve elektrik ağları için iSCSI'ye bir alternatif ise **fiber kanaldır (*fibre channel*)**. Fiber kanal, aslında ilk olarak süper bilgisayarlarda depolama aygıtlarını bağlamak için kullanıldı, ancak o zamandan bu yana birçok bilgisayar türü arasında kullanılarak yaygınlaştı. **Ethernet üzerinden Fiber Kanal (*The Fibre Channel over Ethernet* - FCoE)** protokolü, fiber kanal özellikli cihazların bir Ethernet ağına bağlanmasını daha da kolaylaştırmaktadır. Bu da, katmanlı ağ protokollerinin birçok farklı türde ağ aygıtını gerçekleştirmeyi kolaylaştırmasına bir başka örnektir.

LAN Cihazları: Dağıtım Kutuları ve Anahtarlar

İki tür cihaz bilgisayarları bir LAN'a bağlar: Dağıtım kutuları[1] (*hub*) ve anahtarlar (*switch*). **Dağıtım kutuları (*hub*)** basit ağ cihazlarıdır. Farklı ağ sistemleri için Ethernet kablolarını bağlayabileceğiniz bir takım bağlantı noktaları (ya da port) içerirler. Dağıtım kutusu, herhangi bir bağlantı noktasına bir paket aldığında, bu paketi diğer tüm diğer bağlantı noktalarına otomatik olarak yeniden gönderir. Bu şekilde, dağıtım kutusuna bağlı olan her sistem, her diğer sistemin ağ üzerinde ilettiği her şeyi duyabilir. Bu da dağıtım kutusunun işini oldukça basitleştirir.

[1] *Editörün Notu*: Aynı zamanda, "göbek", "çoklayıcı" ve "dağıtıcı" olarak da isimlendirilmektedir.

Bir dağıtım kutusunun basit doğası, aynı zamanda da onun en büyük dezavantajıdır. Bir dağıtım kutusu, işittiği her şeyi yeniden göndererek çok fazla ağ tıkanıklığı (*congestion*) yaratır. Bir önceki bölümde, eski moda Ethernet ağlarında her sistemin aynı kabloya nasıl bağlandığını öğrendiniz. Sistemleri birbirine bağlamak için dağıtım kutuları kullandığınızda da aynı sonucu elde edersiniz. Her sistem, ağdaki diğer tüm sistemlerle iletişim kurar ve tek bir sistemin bir paket alma fırsatı yakalamasını zorlaştırır. Bu da ağ tıkanıklığına neden olur ve ağı kullanan herkes için ağ hızını azaltır.

UYARI

Dağıtım kutuları aynı zamanda bir güvenlik riski oluşturmaktadır. Her bilgisayar, ağdaki diğer her bilgisayarın ne ilettiğini görebilmekte, gizlice ağı dinleyenlerin istedikleri bütün paketleri kapmaları çok daha kolay olmaktadır.

Anahtarlar (*switch*) dağıtım kutularına nazaran çok daha iyi bir seçenektir. Bir anahtar, birden fazla sistemi ağa bağlayarak bir dağıtım kutusu ile aynı temel işlevi yerine getirir. Bununla birlikte, anahtarların bir başka önemli eklenmiş özelliği vardır: Akıllı filtreleme gerçekleştirebilirler. Anahtarlar, her bir bağlantı noktasına bağlı sistemin MAC adresini "bilir". Ağdan bir paket aldıklarında hedef MAC adresine bakarlar ve paketi *sadece* hedef sistemin bulunduğu bağlantı noktasına gönderirler. Bu basit özellik, büyük bir performans avantajı sağlar.

Anahtarlar günümüzde ucuz maliyetlidir ve performansı büyük ölçüde geliştirilmiştir. Bu nedenle, hemen hemen her modern ağ, sistemleri birbirine bağlamak için ağ anahtarları kullanmaktadır. Sadece çok az sayıda küçük ağlar hala dağıtım kutusu kullanmaktadır.

Sanal Yerel Ağlar

Bir sanal LAN (*virtual LAN* - VLAN), diğer etki alanlarından (*domain*) izole edilmiş herhangi bir yayın (*broadcast*) etki alanı adıdır. Yönlendiricilerde ve ağ anahtarlarında VLAN'lar oluşturulur ve yapılandırma gerçekleştirilir. VLAN, bölünmüş bir ağ kesimi olarak görülecek şekilde toplanmış mantıksal ilişkili ağ cihazlarının bir koleksiyonudur. Bu da yöneticilere, ağ kablolarını fiziksel olarak ayırmak zorunda kalmadan ağ kesimlerine ayırabilme becerisi kazandırır. VLAN'lar, mantıksal cihaz gruplarını izole ederek ağ trafiğini azaltabilir ve güvenliği arttırabilir. Örneğin, İnsan Kaynakları (İK) departmanınız için bir VLAN oluşturursanız, bir İK bilgisayarından başka bir İK bilgisayarına giden tüm hassas bilgiler, İK VLAN'ında olmayan diğer tüm bilgisayarlardan gizlenecektir.

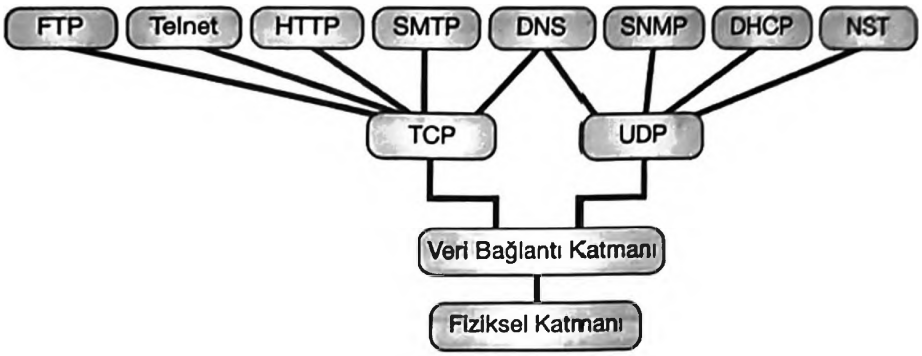
TCP/IP Nedir ve Nasıl Çalışır?

Bir Çinli konuşmacı, bir Fransız konuşmacı ve bir İngiliz konuşmacının bulunduğu bir yemek masası düşünün. Sohbet kafa karıştırıcı olsa gerek! Bu masadaki misafirler, iletişim kurmak istiyorlarsa ortak bir dil kullanmalıdır. Aynı şey bilgisayarlar için de geçerlidir. Neyse ki hemen hemen her bilgisayar, günümüzde İletim Denetimi Protokolü/İnternet Protokolü (*Transmission Control Protocol/Internet Protocol* - TCP/IP) olarak adlandırılan standart bir dil (veya protokol) konuşmaktadır.

Bir **iletişim kuralı (*protokol*)**, bilgisayarların değiş tokuş ettiği iletilerin biçimini yöneten kurallar dizisidir. Bir ağ protokolü, ağ donanımlarının ağ üzerinden veri iletmek için nasıl etkileşime girdiğini yönetir. Bu protokoller, bir sunucudan bir uç nokta cihazına veri aktarımının başından sonuna kadar iletişimi yönetir. Bu bölümde, TCP/IP'yi oluşturan protokoller ve TCP/IP ağ oluşturmanın temelleri hakkında bilgi edineceksiniz.

TCP / IP'ye Genel Bakış

TCP/IP aslında OSI Referans Modelinin Ağ ve Aktarım katmanlarında çalışan protokol paketidir. İnternet üzerindeki, birçok kurumsal ve ev ağları arasındaki tüm etkinlikleri yönetir. ABD Savunma



ŞEKİL 10-5
TCP/IP protokol paketi.

Bakanlığı, oldukça güvenilir ve hataya dayanıklı bir ağ altyapısı sağlamak için TCP/IP'yi geliştirmiştir. Tasarımda odak noktası güvenlik değil, güvenilirlikti.

Bu protokol paketi çok farklı sorumluluklara sahiptir. **ŞEKİL 10-5** TCP/IP protokol paketinin bir bölümünü göstermektedir.

IP Adresleme

Ağ Katmanı protokollerinin asıl işlevlerinden biri, bir adresleme şeması sağlamaktır. Bu katman, TCP/IP'deki adresleme şemasını içerir. **IPv4 adresleri,** ağdaki tüm aygıtları benzersiz şekilde tanımlayan dört baytlık (32 bit) adreslerdir. Geçen yüzyılın sonlarında ağ cihazlarının sayısının artmasıyla IPv4'in her cihaz için benzersiz adreslere yetemeyeceği açıktı. IPv6'nın geliştirilmesinin nedenlerinden biri de budur. IPv6 adresleri 128 bit uzunluğundadır ve eski standarttan çok daha fazla benzersiz aygıt adresi sağlayabilir. Ayrıca, IPv6 birçok ek özellik barındırır ve daha güvenlidir. Bununla birlikte, IPv6'ye geçiş süreci yavaştır, bu nedenle IPv4 hâlâ kullanılan en yaygın IP adresleme tekniğidir.

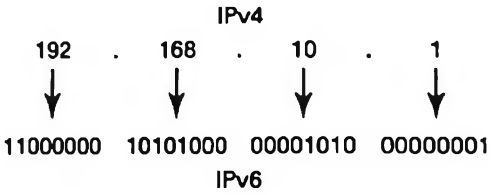
ŞEKİL 10-6, bir IPv4 ve IPv6 adresi gösterimi arasındaki farkı göstermektedir. Gördüğünüz gibi IPv4 adresleri nokta ile ayrılan dört parçalı gösterimi kullanır. Bu da, 4 baytın her birinin 0 ile 255 arasında bir tam sayı olarak temsili şeklindedir. Her IPv4 adresi, ağ adresi ve ana bilgisayar adresi kısmından oluşur. Örneğin, şekilde gösterilen IPv4 adresi 192.168.10.1, ağı tanımlayan adres kısmı 192.168 ve ana bilgisayar adres kısmı 10.1'dir. Ağ ve ana bilgisayar adresleri arasındaki ayrım, yöneticinin ağ yapılandırma şekline bağlı olarak değişebilir. **Alt ağ maskesi (*subnet mask*)** olarak bilinen bir ağ yapılandırma parametresi, belirli bir ağ için bu ayrımı tanımlar. Aynı ağ adresini paylaşan tüm ana sistemler bir **alt ağın (*subnet*)** parçasıdır. Bir alt ağ, bir ağın IP adreslerine dayalı bir bölümüdür. IPv6 adresleri IPv4'ten çok daha büyük olduğu için, IPv6 tamamen farklı bir gösterim kullanır. Şekilde görüldüğü gibi, IPv6 adresleri 16 bitlik sekiz gruba ayrılmış onaltılık değerler olarak ifade edilir.

Her bilgisayar kendi IP adresine ihtiyaç duyduğundan, adres atamalarını takip etmek zaman alıcı olabilir. IPv4'ü kullanan birçok kuruluş, her kullanıcının bilgisayarının yapılandırmasını basitleştirmek için ağın içinde **Dinamik Ana Bilgisayar Yapılandırma Protokolünü (*Dynamic Host Configuration Protocol* - DHCP)** kullanmaktadır. Bu, her bilgisayarın kendi yapılandırma bilgilerini ağ yöneticisi yerine ağdan dinamik olarak almasını sağlar. DHCP, bilgisayara IPv4

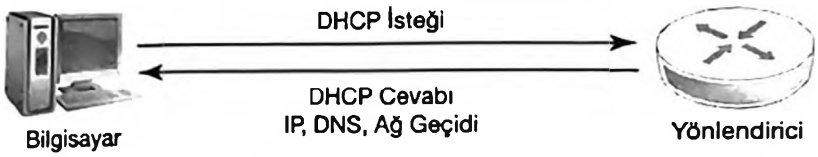
NOT

İnternet Atanmış Sayılar Yetkilisi (*Internet Assigned Numbers Authority* - IANA), kullanılabilir IPv6 adreslerinin yalnızca yüzde 20'sini kullanıma sokmuştur. Bu da halihazırda dünyadaki her kişi için yaklaşık 4,000 adet IPv6 adresi mevcut olduğu anlamına gelmektedir.

ŞEKİL 10-6
IP adresleme.



ŞEKİL 10-7
DHCP iletişimi



adresi, alt ağ maskesi ve diğer önemli iletişim bilgilerini sağlar. Ağ yöneticisinin işini basitleştirir. **ŞEKİL 10-7**'de DHCP iletişimi bir örnekle gösterilmiştir. Teknik olarak, DHCP yalnızca IPv4 ağlarıyla çalışır. DHCPv6, IPv6 adreslerini sağlar.

Ortak Bağlantı Noktaları

Ağ uygulama yazılımı, başka bir cihazla iletişim kurmak için hedef (uzaktaki) cihazın adresini bilmelidir. Ağ yazılımı yığını, iletiyi bir cihazdan diğerine ulaştırmakla ilgili tüm ayrıntıları ele alır. Uygulama yazılımının hedef adresinden fazlasını ayrıca belirtmesi gerekir. Yazılımın alıcı (hedef) cihaza, mesajı aldığında nereye göndereceğini söylemesi gerekir. Bu hedef adrese, **ağ bağlantı noktası (*network port*)** denmektedir. Bir ağ bağlantı noktası, hedef cihaza aldığı mesajları nereye göndereceğini söyleyen bir rakamdır. İstemci yazılımı ağ iletilerini belirli bağlantı noktalarına gönderir ve sunucu yazılımı gelen iletiler için ağ bağlantı noktalarını dinler. Örneğin, web tarayıcıları ve web sunucuları arasındaki hemen hemen tüm şifrelenmemiş trafik, 80 numaralı bağlantı noktasını kullanır. 80 numaralı bağlantı noktası genellikle HTTP trafiği için kullanılır. Ortak servislerin kullandığı bağlantı noktaları **TABLO 10-1**'de listelenmiştir. Hiç kimse yazılımı ortak bağlantı noktalarını kullanmaya zorlamaz, ancak çoğu yazılım istemcilerin ve sunucuların iletişimini kolaylaştırmak için standart bağlantı noktalarını kullanır.

Ortak Protokoller

En yaygın ağ protokollerinden bazılarını daha önceki bölümlerde gördünüz. Birçok kullanım için iletişim kurallarını tanımlayan çok daha fazla protokol vardır. Tanımanız gereken yaygın ağ protokollerinin (çok kapsamlı olmasa da) bir listesi **TABLO 10-2**'de verilmiştir.

NOT

IANA, tanınmış hizmetlerin ve bağlantı noktalarının numaralarının bir listesini tutmaktadır. Bu listeyi şu adreste bulabilirsiniz: *www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml*

İnternet Kontrol Mesajı Protokolü

Tüm ağ bileşenlerini yapılandırdıktan sonra, ağınızı sağlık ve performans açısından izlemeniz gerekir. **İnternet Kontrol Mesajı Protokolü (*Internet Control Message Protocol* - ICMP)**, IP için bir yönetim ve kontrol protokolüdür. ICMP, ana sistemler arasında ağın sağlığı hakkında ileti gönderir. ICMP mesajları; ulaşabileceği ana sistemlerle ilgili, ayrıca yönlendirme ve güncellemelere dair bilgi taşır.

TABLO 10-1 Yaygın Ağ Kapısı Numaraları

BAĞLANTI NOKTASI	SERVİS/KULLANIMI
20	FTP dosya transferi
21	FTP denetim
22	Güvenli Kabuk (SSH)
25	Basit E-posta Transfer Protokolü (SMTP)
53	Alan Adı Sistemi (DNS)
80	Hipermetin Transfer Protokolü (HTTP)
110	Postane Protokolü v3 (POP3)
139	NetBIOS Oturum Servisi
143	İnternet Mesaj Erişim Protokolü (IMAP)
443	Güvenli Soket Katmanı (SSL) üzerinden HTTP
3389	Uçbirim Sunucusu

TABLO 10-2 Yaygın ağ protokolleri.

PROTOKOL	YAYGIN BAĞLANTI NOKTALARI
DNS (Alan Adı Servisi)	53
FTP (Dosya Transfer Protokolü)	20 (veri), 21 (denetim)
FTPS (TLS/SSL üzerinden FTP)	989 (veri), 990 (denetim)
HTTP (Hipermetin Transfer Protokolü)	80
HTTPS (TLS/SSL üzerinden Hipermetin Transfer Protokolü)	443
iSCSI (Internet Ufak Bilgisayar Sistem Arayüzü)	860, 3260 (hedef)
NetBIOS (Ağ Temel Girdi/Çıktı Sistemi)	137, (Ad Servisi) 138, (Veri iletisi servisi) 139 (Oturum servisi)
SCP (Güvenli Kopyalama— SSH parçası)	22
SFTP (Güvenli Dosya Transferi Protokolü—SSH parçası)	22
SNMP (Basit Ağ Yönetim Protokolü)	161
SSH (Güvenli Oturum)	22
Telnet	23
TFTP (Sıradan Dosya Transferi Protokolü)	69

Teknik İpucu

SSL veya TLS (*Transport Layer Security* - Aktarım Katmanı Güvenliği) için listelenen bir bağlantı noktası numarasının olmadığına dikkat edin. Bunun nedeni, bu iki protokolün üst düzey protokoller için şifreleme sağlamak için kullanılmasıdır. Örneğin, HTTPS; SSL veya TLS üzerinden çalışan HTTP'dir. Bu da SSL veya TLS'in sadece HTTP bağlantı noktasını (80) kullanacağı anlamına gelir. İstemci tarayıcısı normalde HTTPS ile 443 numaralı bağlantı noktasını kullanarak sunucuya bağlanır. Ancak bağlantı noktasının kendisi, güvenlik açısından hiçbir şey ifade etmez. HTTP verilerini şifreleyen SSL protokolüdür. SSL, TLS'den daha uzun süredir devam etmekte ancak daha güvenli olan TLS ile yavaş yavaş yer değiştirmektedir.

İki ICMP aracı, ping ve traceroute'dur. Ping komutu, bir hedef IP adresine **ICMP yankı isteği** (***ICMP echo request***) adı verilen tek bir paket gönderir. Bu paket, "Orada mısın?" sorusunu sormaya eş değerdir. Hedef bilgisayar, bu isteğe ICMP yankı paketi ile "Evet" diyerek cevap verebileceği gibi isteği görmezden de gelebilir. Saldırganlar, bazen gelecekteki bir saldırı için hedef belirlemek için ping komutunu kullanırlar. Birçok sistem yöneticisi, bu olası güvenlik açığı nedeniyle bilgisayarlarını tüm ping isteklerini görmezden gelecek şekilde yapılandırır.

Traceroute komutu ICMP yankı isteğini, paketlerin bir ağ içinden dolaştığı yolu belirlemek için kullanır. Paketler, ağdaki bir noktadan diğerine ulaşmak için birçok farklı yol izleyebilir. Traceroute komutu; olası ağ sorunlarının kaynağını belirleyebilmeniz için, belirli bir paketin izlediği yolu görüntüler.

Saldırganlar, ICMP'yi bir ağa karşı bir hizmet reddi saldırısı oluşturmak için kullanabilir. Bu saldırı türü, bunu gerçekleştirmek için geliştirilen ilk programlardan birinin adını taşımaktadır ve **Smurf saldırısı** (***Smurf attack***) olarak bilinir. Saldırılacak ana sistem, IP kaynak adresi olarak tanımlanır. Sahte kaynak adresi içeren ICMP yankı isteği paketleri bir ağın yayın adresine gönderilir ve ağdaki ana sistemlerin bu isteğe yanıt vermesi beklenir. Saldırgan yeterince yanıt gönderimini sağlatabilirse, çevirmeli ağ bağlantısından yapılan bir saldırıdan bile bir T1 ağ bağlantısına sahip ana sistemi çökertmek mümkün olabilecektir. Neyse ki, bu saldırıya karşı ağı savunmak çok kolaydır. Yayın adreslerine gönderilen ICMP yankı isteklerini görmezden gelmek için ağı yapılandırmak yeterlidir.

Ağ Güvenliği Riskleri

İletilmekte olan herhangi bir veri, olası bir saldırı hedefidir. Bu da ağ güvenliğini önemli hale getirmektedir. Şu ana kadar bu bölümde, ağların verileri nasıl taşıdığını öğrendiniz. Smurf saldırıları ve gizlice ağ dinlemeleri gibi ağların karşı karşıya kaldığı birkaç risk hakkında da bilgi edindiniz. Bu bölümde, bazı ağ güvenliği risklerini derinlemesine inceleyeceksiniz. Ayrıca, ağınızı korumak için kullanıma alabileceğiniz bazı ağ güvenliği kontrollerini de ele alacaksınız.

NOT

Saldırganlar bunun yanı sıra ağınızdaki sistemlerin denetimini ele geçirmek isteyecektir. Bunun için ağ güvenliği açıklarını kullanacaklardır. Bu tartışma ise bu bölümün kapsamı dışındadır.

Risk Kategorileri

Ağ güvenliği riskinin üç ana kategorisi, keşif (*reconnaissance*), gizlice dinleme (*eavesdropping*) ve hizmetin reddidir (*denial of service*). Bunların her birinin bir ağda taşınan verilerin

kullanılabilirliği, bütünlüğü ve gizliliği üzerinde farklı etkileri bulunmaktadır. Ayrıca ağ güvenliğini de etkileyebilirler. Bu bölümde en yaygın ağ güvenliği risklerinin bazılarını inceleyeceksiniz.

Keşif

Ağ keşfi (*network reconnaissance*), gelecekteki bir saldırıda kullanılmak üzere bir ağ hakkında bilgi toplamaktır. Bir ülkeye saldırmak isteyen bir orduyu düşünün. Saldırı yapan ordu, başarılı olmak için çok daha fazla ileri seviyede bilgiye ihtiyaç duyar. Bir komutanın bilmek isteyebileceği bazı şeyler şunlardır:

- Savaş alanı
- Yollar, parkurlar ve su yollarının konumu
- Düşman savunma yerleri ve türleri
- Düşmanın çevresindeki zayıflıklar
- Çevresinden erişime izin verecek yöntemler
- Düşman tarafından kullanılan silah türleri

Bir ağa saldıracak kişi de benzer şekilde saldırı öncesinde birçok şeyi bilmek isteyecektir:

- Ağda kullanılan IP adresleri
- Güvenlik duvarlarının çeşitleri ve diğer güvenlik sistemleri
- Uzaktan erişim yöntemleri
- Ağdaki bilgisayarların işletim sistem(ler)i
- Ağ sistemlerindeki zayıflıklar

Normalde bu bilgileri bir saldırganın kullanımına sunmazsınız. Ne yazık ki, saldırganlar bunları elde etmek için birçok araca sahiptir. Ağınızın dışından gelen ICMP yankı isteklerini engellemenin neden önemli olduğunu öğrendiniz. Bu engelleme, saldırganların bilgi toplamak için ping ve traceroute araçlarını kullanmasını durduracaktır. Sistemleri, dışarıya mümkün olduğunca az bilgi sağlayacak şekilde yapılandırdığınızdan emin olmalısınız. Bu da ağ keşif saldırılarının etkinliğini sınırlayacaktır.

Gizlice Dinleme

Saldırganlar, ağınızda iletilen verilerin gizliliğini de ihlal etmek isteyebilirler. Ağları gizlice dinleme hakkında bilgi edinmeden önce, daha az karmaşık bir teknoloji olan telefonu ele alalım. Casus filmlerinde de gördüğünüz üzere, telefon kablolarına erişebiliyorsanız telefonu dinlemek kolaydır. Binadaki ana telekom kutusuna bir kablo bağlamanız ve aramaları dinlemek için bir mikrotelefon (ahize) takmanız yeterlidir.

Ağ dinlemeleri de aynı derecede basittir. Bir saldırganın bir kabloya fiziksel erişimi varsa, o kabloyu dinlemek için gizlice bağlantı yapabilir ve kablodan geçen tüm verileri elde edebilir. Bu saldırı türünden korunmak için birkaç seçeneğiniz var:

- Ağ kablolarına fiziksel erişimi sınırlamak.
- Ağ anahtarları kullanmak. Saldırgan, sadece gizlice bağlantı yaptığı kabloya bağlı olan bilgisayarın ağ trafiğini görebilecektir.
- İletilen hassas verileri şifrelemek. Saldırgan hala iletilen trafiği görebilecek, ancak içeriğinden anlam çıkaramayacaktır.

Ağı gizlice dinlemek, telefonu gizlice dinlemekten daha kolaydır. Ağa fiziksel olarak erişim bunu kolaylaştırır ancak gerekli de değildir. Saldırgan, ağdaki bir bilgisayarı ele geçirip ağı gizlice dinlemek için kullanabilir. Ağ anahtarları ve şifreleme kullanarak bu saldırının etkinliğini kısıtlamak mümkündür. Ayrıca, ağınızdaki sistemleri kötü amaçlı yazılımlardan korumalısınız.

NOT

Kablosuz ağ, gizlice dinlemeyi engellemeyi zorlaştıran tamamen yeni bir dünya sunmaktadır. Bu konuda daha fazlasını, bölümün sonraki kısımlarında öğreneceksiniz.

Hizmet Reddi

Saldırgan, çoğu zaman ağınıza erişmeyle ilgilenmez. Aksine, sizin ağı kullanmanızı sadece engellemek ister. Bu son derece etkili bir saldırı taktiği olabilir. Birçok ticari işletme, ağlarını kaybederse çalışamaz. Bir saldırganın bir hizmetin reddi saldırısı (*denial of service* - DoS) gerçekleştirmek için iki temel yöntemi vardır: Ağı trafiğe boğmak ve sistemi ayakta tutan bir noktayı devre dışı bırakmak.

Bir ağın trafiğe boğulması daha basit bir yöntemdir. Bir ağı, dolmadan önce yalnızca kapasitesi kadar veri taşıyabilecek bir boru olarak düşünebilirsiniz. Boruya sığamayacak kadar fazla veri gönderirseniz, ağ tıkanır ve işe yaramaz hale gelir. Saldırganlar, ağın işleyebileceğinden daha fazla veriyi ağ üzerinden göndererek bir DoS saldırısı oluşturabilirler. Bu saldırının bir çeşidi, dağıtık hizmet reddi (*distributed denial of service* - DDoS) saldırısıdır. Bu saldırıda; siyah şapka bilgisayar korsanı, farklı birçok yerden ağı trafiğe boğmak için dünyanın çeşitli yerlerinden ele geçirdiği birçok sistemi kullanmaktadır. Normal trafiği, saldırı trafiğinden ayırmak güçleşir ve ağ durma aşamasına gelir.

DDoS saldırıları yıllardır bilinmektedir. Bununla birlikte, bunlar eski tür saldırılar olarak görülmez. Saldırganlar, kurbanlarını yavaşlatmak veya devre dışı bırakmak için hala DDoS saldırıları kullanmaktadır. Eylül ve Ekim 2012'de, bilgisayar korsanlığı yetenekleri olan ve hacktivist olarak adlandırılan bir grup eylemci, birçok büyük Amerikan bankasına karşı bir dizi DoS saldırısı başlattı. Hacktivistler genellikle bazı politik konulara dikkat çekmek için, giderek daha fazla ve daha büyük ölçekli saldırıların arkasındadır. Bu saldırılar, 2012 yılının sonundan 2013 yılına kadar devam etti. Bu saldırıların hedefleri arasında ABD Bancorp, JPMorgan Chase, Bank of America, PNC Financial Services ve SunTrust Banks bulunmaktadır. Saldırılar devam ettikçe, daha fazla organizasyonu etkilemiştir. Bazı müşteriler yavaş banka web siteleri nedeniyle hayal kırıklığına uğramış, diğerleri bankalarına internet üzerinden erişememiştir. Devam eden saldırılar banka web sitelerine çevrimiçi erişimi aksatmaya devam etmektedir ancak genellikle daha önceki saldırılar kadar başarılı olamamaktadır. Bankalar daha önceki saldırılardan edindikleri deneyimlerle web sitelerini korumak için yeni denetimler eklemektedirler.

Önceki saldırılar, çoğu zaman büyük perakendecilere odaklanmıştı. Amazon.com, Walmart ve Expedia dahil olmak üzere birçok büyük internet perakendecisi, 2009'dan bu yana DoS saldırılarının kurbanıydı. Bu saldırılar, kış tatili alışveriş sezonunun ortasında üç web sitesinin hepsini yaklaşık üç saat boyunca kapattı. Müşteriler diğer perakende web sitelerine girdikçe şirketler gelir kaybetti. Yaşananlar daha da kötüye gitmektedir. Aralık 2014'te ismi bildirilmeyen bir ISP (ISS), 400GB'lık bir ağ trafiği zirvesi oluşturan bir NTP yansıtmalı DDoS saldırısı bildirdi; bu herhangi bir ISP'nin üstesinden gelebileceğinin üstünde bir trafik hacmidir. Anlaşılacağı üzere, ISP'nin müşterileri bu saldırıda internete bağlanamadı.

Teknoloji ilerlemeleri, saldırganların DoS saldırılarıyla sorunlara sebep olabilmeleri için daha fazla fırsat sunmaktadır. Oldukça yeni bir saldırı türü olan **telefon hizmet reddi (*telephony denial of service* - TDoS)** saldırısı, daha yaygın hale gelmeye başlamıştır. TDoS saldırısı, bazı kişiler veya kuruluşların telefon görüşmelerinin başarıyla başlatılmasını veya çağrı alınmasını önlemeye

kalkışmaktadır. Bu saldırılar, 2013 yılının başında daha yaygın hale geldi. Saldırganlar; asıl iletişim yöntemi olarak telefon çağrılarına bağımlı olan artan sayıda kuruluşu hedef almaktadır. Sonuç standart DoS saldırıları gibidir. Telefon iletişimini kesintiye uğratabilecek veya tamamen devre dışı bırakabilecek bu ağ saldırıları, çok büyük etkilere neden olabilir. Gelir kaybı, muhtemel para cezaları, faaliyetlerin gerçekleştirilememesi ve müşteri güveninin kaybedilmesini içeren zararlar olabilir.

Kendinizi bir DoS saldırısına karşı korumak zor olabilir. En belirgin yaklaşım, yüke dayanacak kadar yeterli internet bant genişliğine sahip olmayı sağlamaktır. Piyasadaki bazı yeni teknolojiler DDoS saldırılarına karşı savunma arayışındadır ancak bu teknolojiler kanıtlanmamıştır ve etkinliği sınırlıdır. En iyi savunma şekli, saldırıları olabildiğince erken algılamak ve gelen trafiği ağınızı kullanılamaz hale getirmeden önce engellemek için harekete geçmektir.

Temel Ağ Güvenliği Savunma Araçları

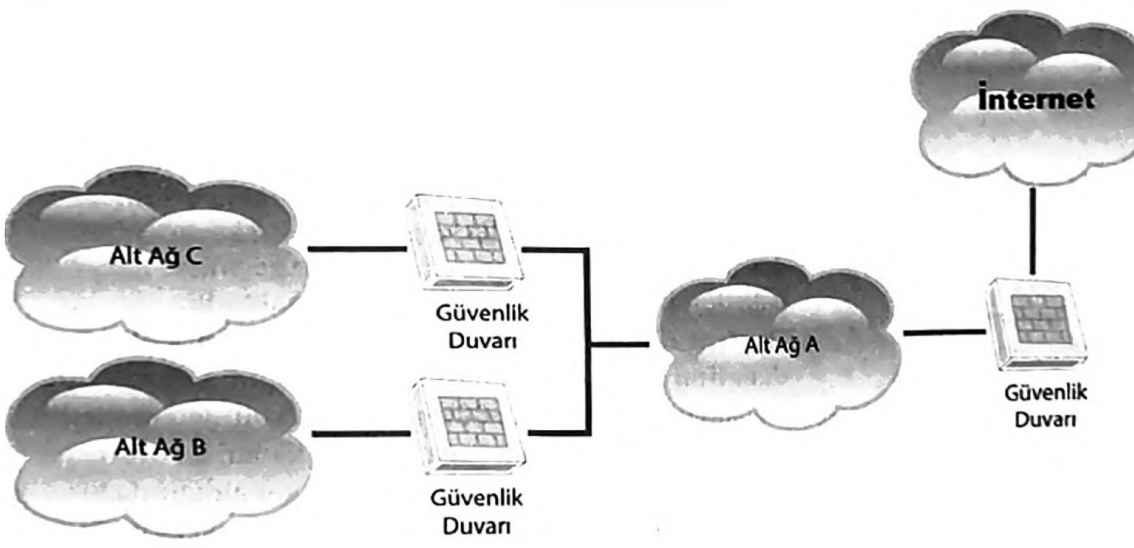
Bu tür risklere karşı savunma, bazı temel donanım ve yazılım araçları ile başlar: Güvenlik duvarları, sanal özel ağlar ve ağ giriş denetimi.

Güvenlik Duvarları

Bir **güvenlik duvarı (*firewall*)**; yetkisiz ağ trafiğinin, ağın belirli bir bölümüne girmesini veya çıkmasını önleyerek trafik akışını denetler. İç ağ ile dış dünya arasına veya iç ağın içerisinde bir güvenlik duvarı yerleştirerek, önemli şirket varlıklarına yalnızca yetkili kullanıcılar tarafından erişim yapıldığını denetleyebilirsiniz. Güvenlik duvarları; ağ güvenliği için kritik unsurlardır ancak sadece bir elemanı oldukları unutulmamalıdır. Güvenlik duvarları tüm güvenlik sorunlarını çözmeyeceklerdir, ancak çok gerekli bir caydırıcılık eklemektedirler.

ŞEKİL 10-8, ağdaki güvenlik duvarının rolünü göstermektedir. Özel ağları internetten ayırır. Farklı özel ağları da birbirinden ayırır. Bu bölümde, farklı güvenlik duvarları türlerine ve ağ topolojisinde oynadıkları rollere bakacağız.

ŞEKİL 10-8 Güvenlik Duvarları.



Güvenlik duvarları, ağları güvenli hale getirmekte güçlü araçlardır. Her bir güvenlik duvarı kurallar kullanarak yapılandırıldığından, **kural tabanlı yönetimi (*rule-based management*)** gerçekleştirmenin en yaygın yolunu sağlarlar. Kural tabanlı yönetim, nelerin kabul edilebilir ve nelerin kabul edilemez olduğunun kurallarını tanımlayarak bir ağın güvenliğini yönetmektir. **Güvenlik duvarı kuralları (*firewall rules*)**, güvenlik duvarı yapılandırmasında tanımlanan ve bu güvenlik gereksinimlerinin çoğunu uygulamayı kolaylaştıran filtrelerdir. Farklı güvenlik duvarları türleri farklı kurallar kullanır. En basit güvenlik duvarları bile **erişim denetim listelerini (*access control list*)** desteklemektedir. Bir erişim denetim listesi, belirli bir protokol ve bir veya daha fazla bağlantı noktası kullanan bir veya daha fazla ana sistemden gelen trafiği işlemek için bir kural tanımlar. Güvenlik duvarları sadece bir ana sistemin güvenliğini sağlamanın yanı sıra, trafiği, bağlantı noktalarına göre filtreleyebilir. Bu da **bağlantı noktası güvenliği (*port security*)** olarak adlandırılır. Erişim denetim listeleri çok özel kurallar içerebilir veya ana sistem serisi ve bağlantı noktası aralıkları içerebilir. Her kural, belirli ileti tiplerini nasıl işleyeceğini güvenlik duvarına bildirir. En yaygın eylemler; izin ver (*allow*) ve engelle (*deny*) şeklindedir. En güvenli ağı oluşturmak istiyorsanız, güvenlik duvarınızı açıkça izin verdiğiniz iletiler dışındaki tüm iletileri engelleyecek şekilde yapılandırabilirsiniz. Bu yaklaşıma **gizli engelleme (*implicit deny*)** denir. Bu yaklaşım çok güvenli olabilir, ancak ihtiyaç duyulduğunda yeni bağlantı noktalarını açmak gerekecek ve bu da ağ yöneticilerinin ek çaba göstermesini gerektirecektir.

Güvenlik duvarları, ağları güvenli hale getirmede birden fazla şekilde yardımcı olabilir. Daha önce gördüğünüz filtreleme özelliklerine ek olarak, güvenlik duvarları şu güvenlik özelliklerini sağlayabilir:

- **Trafiğe boğma koruması (*Flood guard*)**—Kurallar, ana sistemlerden gelen trafik bant genişliğini sınırlandırarak, herhangi bir ana sistemin ağı boğma kabiliyetini azaltabilir.
- **Döngü koruması (*Loop protection*)**—Güvenlik duvarları, ileti adreslerine bakıp bir iletinin sonsuz bir döngü şeklinde gönderilip gönderilmediğini belirleyebilir. Bu da bir tür trafiğe boğma olabilir.
- **Ağ ayırma (*Network seperation*)**—Filtreleme kuralları; trafiğin bir ağdan diğerine geçmesini önleyerek, ağlar arasında bölünmeleri yerine getirebilir.

Güvenlik Duvarı Türleri

Bir güvenlik duvarının temel işlevi oldukça basittir: Açıkça izin vermediğiniz herhangi bir trafiği engellemelidir. Güvenlik duvarları, bir ağ üzerinden gelebilecek ve gidebilecek trafik türlerini tanımlayan kurallar içerir. Güvenlik duvarı her ağ iletisi aldığında, iletiyi kendi kurallarına göre kontrol eder. İleti bir kurala eşleşirse, güvenlik duvarı iletinin geçmesine izin verir. İleti bir kurala eşleşmezse, güvenlik duvarı iletiyi engeller.

Bu temel işlevselliğin ötesinde, güvenlik duvarı teknolojisi üç ana türü içermektedir:

NOT

Güvenlik duvarları sadece engelleyici denetleme yapmaz. Ayrıca bir dedektif gibi de çalışırlar. Güvenlik duvarları, analiz edebileceğinizden çok günlük kaydı yapabilir. Yapılandırılmış bir **günlük kaydı analiz (*log analysis*)** süreci, keşif etkinliğini veya hatta daha önce meydana gelen saldırıları da tanımlamanıza yardımcı olabilir. Potansiyel sorunları belirlemek için tüm güvenlik duvarı günlük kayıtlarını düzenli olarak izlemelisiniz.

- **Paket filtreleme (*Packet filtering*)**—Bir **paket filtreleme güvenlik duvarı** çok basittir. Alınan trafiği, hangi trafiğin güvenlik duvarından geçmesine izin verildiğini tanımlayan bir dizi kuralla karşılaştırır. Bu kararı, güvenlik duvarına ulaşan her paket için yapar ve geçmişte karşılaştığı paketleri hatırlama yeteneği bulunmamaktadır.
- **Durum denetimi (*Stateful inspection*)**—Bir **durum denetimi güvenlik duvarı**, bir ağ iletişiminin durumu hakkındaki bilgileri hatırlar. Güvenlik duvarı bir iletişimde ilk paket alındıktan iletişim kapatılıncaya kadar, bu oturumu hatırlar. Bu tür bir güvenlik duvarı, her paket aldığında kurallarını kontrol etmek zorunda değildir. Yalnızca yeni bir iletişim oturumu başladığında kuralları kontrol etmesi gerekir.

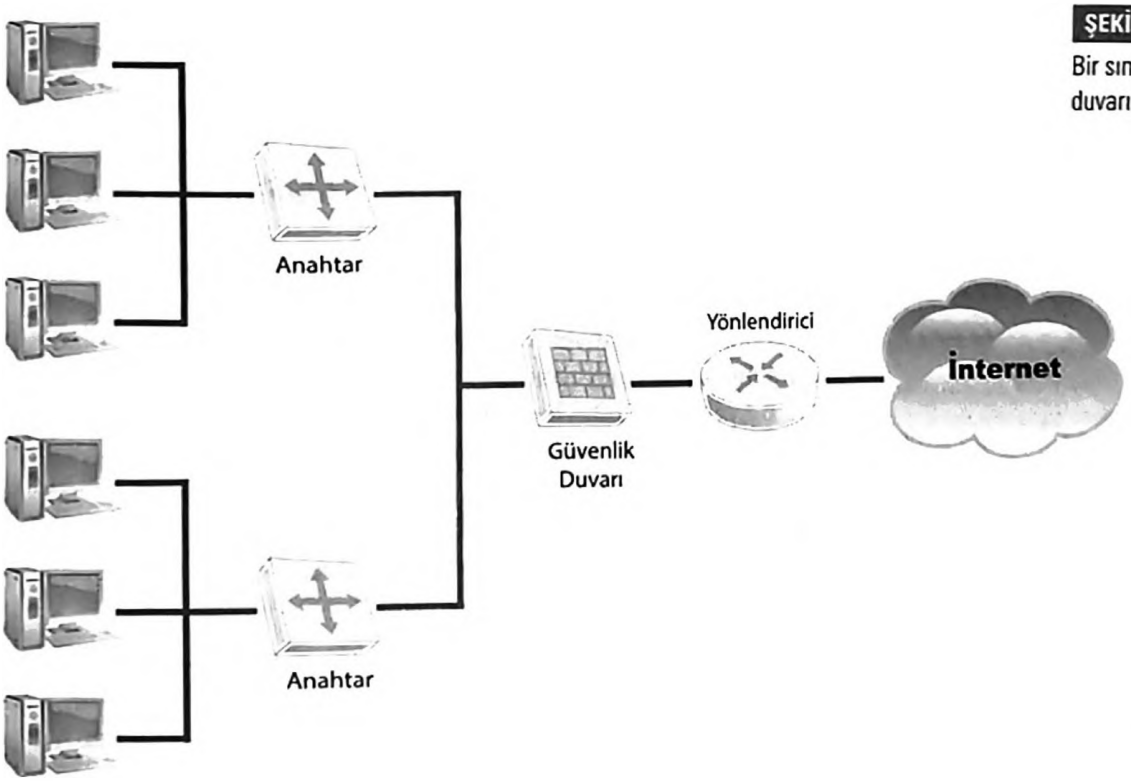
- **Uygulama vekil sunucusu (*Application proxy*)—Bir uygulama vekil sunucusu güvenlik duvarı,** durum denetim güvenlik duvarından daha ileri gider. Paketlerin, karşılıklı sistemler arasında doğrudan dolaşmasına aslında izin vermez. Güvenlik duvarı, iki iletişim kuran sistemin her biri ile ayrı bağlantılar açar ve sonrasında ikisi arasında bir aracı kurum (veya vekil sunucu) şeklinde davranır. Bu da eklenmiş bir koruma derecesine olanak tanıyacaktır çünkü güvenlik duvarı trafiğe izin verme veya reddetme kararı verirken kullanılan uygulama hakkındaki bilgileri analiz edebilecektir.

Ağınız için seçtiğiniz güvenlik duvarı türü, birçok değişik etkene bağlı olacaktır. Büyük bir ağın sınırında basit bir güvenlik duvarı yerleştiriyorsanız, temel bir paket filtresi kullanmak isteyebilirsiniz. Diğer yandan, web uygulamalarını barındıran yüksek güvenlikli bir veri merkezini koruyorsanız, bir uygulama vekil sunucusu daha uygun olabilecektir.

Güvenlik Duvarı-Yerleştirme Teknikleri

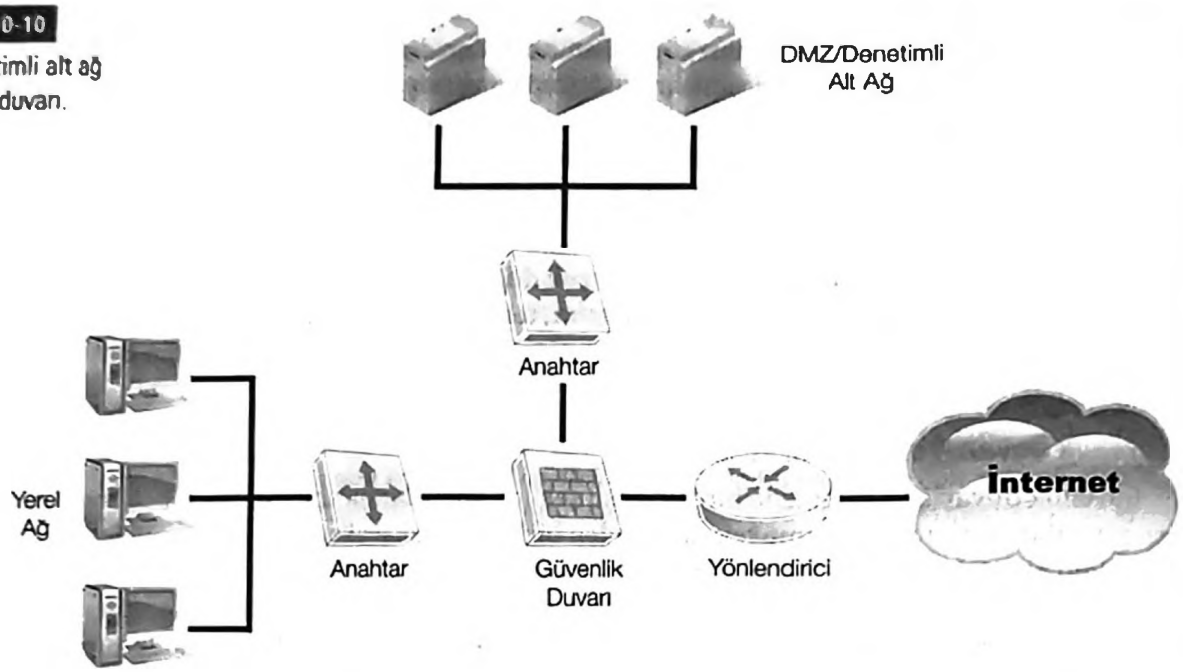
Güvenlik duvarlarını ağınızda birçok farklı şekilde konuşlandırabilirsiniz. Bu bölümde, en yaygın güvenlik duvarı yerleştirme tekniklerinden birkaçına bakacaksınız: Sınır güvenlik duvarları, denetimli alt ağ (veya DMZ) güvenlik duvarları ve çok katmanlı güvenlik duvarları. Kuruluşunuzun güvenlik gereksinimlerine bağlı olarak, bu yaklaşımlardan bir veya daha fazlası uygun olabilir.

Sınır Güvenlik Duvarı (*Border firewall*). **Sınır güvenlik duvarı,** en temel yaklaşımdır. Sınır güvenlik duvarları; **ŞEKİL 10-9**'da gösterildiği gibi, korunan ağı internetten ayırır. Bir sınır güvenlik duvarı, normalde yönlendiricinin arkasında bulunur ve yönlendiriciden özel ağa iletilen tüm iletişimi alır. Ayrıca, özel ağdan internete iletilen tüm iletişimleri de alır. Sınır güvenlik duvarları normalde ya paket filtreleme ya da durum denetimi kullanır.



ŞEKİL 10-9
Bir sınır güvenlik duvarı.

ŞEKİL 10-10
Bir denetimli alt ağ güvenlik duvarı.



Sınır güvenlik duvarları, kamu hizmetlerini barındırmayan kurumlar için en yaygın olanıdır. Web sitesi ve e-posta servislerinizi dış bir kaynaktan alıyorsanız, genel kullanıcıların ağınıza girmesine izin vermeniz hiç gerekmeyebilir. Bu durumda, gelen trafiğin çoğunu (veya bazen hepsini) basitçe engelleyebilirsiniz. Sınır güvenlik duvarı, bu senaryoda çok iyi olacaktır.

Denetimli Alt Ağ (*Screened Subnet*). Ağınıza gelen tüm trafiği engellemek çoğu zaman mümkün değildir. Genel bir web sitesini veya kendi e-posta sunucunuzu barındırıyorsanız, gelen bağlantılara sınırlı bir şekilde izin vermeniz gerekir. ŞEKİL 10-10'da gösterilen denetimli alt ağ güvenlik duvarı topolojisi, bu tür bir gereksinim için en iyi yaklaşımdır. Güvenlik duvarı, üç ağ kartına sahiptir. Biri internete bağlı ve diğeri de özel ağa bağlı olacak şekilde iki adedi, bir sınır güvenlik duvarı ile benzer şekilde kurulmuştur. Üçüncü kart, denetimli alt ağ veya arındırılmış bölge (***demilitarized zone*** - **DMZ**) olarak da bilinen özel bir ağa bağlanır.

DMZ, halka açık hizmetleri barındırmak için kullanılan yarı özel bir ağdır. Kullanıcıların bu hizmetlerden yararlanabilmesi için internetten DMZ'deki sistemlere erişimi kısıtlıdır. Güvenli bir ağ, internetten özel ağa doğrudan erişime izin vermeyecektir.

NOT
Denetimli alt ağ, günümüzde kullanılan en yaygın güvenlik duvarı topolojisidir.

Bu yaklaşım, internetten erişilen sistemlerin özel bir risk oluşturduğunu kabul eder. Saldırıların daha olası hedefleri olduklarından, başarılı saldırılara maruz kalma olasılıkları daha yüksektir. Eğer bu makineleri DMZ'ye sınırlandırırsanız sadece DMZ'deki diğer sistemleri tehlikeye atabilirler. Bir DMZ sistemine erişim kazanan bir saldırgan; o sistemi, özel ağdaki sistemlere doğrudan erişmek için kullanamayacaktır.

Çok Katmanlı Güvenlik Duvarı (*Multilayered Firewall*). Büyük ve/veya yüksek güvenlikli ortamlarda, kuruluşlar ağlarını kesimlere bölmek için genellikle birden fazla güvenlik duvarı kullanır. Böyle bir durum Şekil 10-8'de gösterilmiştir. Bu şekilde görüldüğü üzere; bir güvenlik duvarı, A, B

ve C alt ağlarını internetten korumak için sınır güvenlik duvarı olarak görev yapmaktadır. Ancak, diğer iki güvenlik duvarı, B ve C alt ağlarını birbirlerinden ve A alt ağından ayırmaktadır.

Çok katmanlı güvenlik duvarları, farklı güvenlik düzeylerine sahip ağlarda yararlıdır. Örneğin, Şekil 10-8'de genel kullanıcılar A alt ağına bağlanabilirler. Gizli bir araştırma projesinde çalışan kullanıcılar B alt ağına bağlı olabilirler. Yöneticiler C alt ağına bağlanmış olabilirler. Bu yapı; gizli proje ve yöneticilerini, genel kullanıcı topluluğundan korumayı sağlayacaktır.

Birleşik Tehdit Yönetimi (*Unified Threat Management*). Güvenlik duvarları, ağ güvenliği için o kadar önemlidir ki paket denetiminden çok daha fazlasını yapan cihazlara dönüşmüşlerdir. Çok amaçlı güvenlik duvarları, daha çok **birleşik tehdit yönetimi (UTM)** cihazları olarak adlandırılır. UTM cihazları, diğer birçok güvenlik servisinin yanı sıra filtreleme de yapmaktadır. UTM cihazlarının sağladığı bazı hizmetler şunlardır:

- **URL filtresi**—Bu özellik, IP adresi yerine URL'yi inceleyerek web trafiğini filtrelemektedir.
- **İçerik denetimi**—Cihaz, paketin geçmesine izin verilip verilmeyeceğini belirlemek için bazı veya tüm ağ paket içeriğine bakar. Bu tür bir denetim, güvenilir kaynaklardan gelen kötü amaçlı içeriğin belirlenmesine yardımcı olabilir. Bu da güvenilir bir kaynağın ele geçirilmesi durumunda olabilir.
- **Zararlı yazılım denetimi**—Özel bir içerik denetimi biçimi olan bu serviste cihaz, zararlı yazılıma dair belirtiler için paket içeriğine bakar.

Bu birleştirilmiş hizmetler, ağ paketlerini analiz etmesi gereken cihazların sayısını azaltmayı mümkün kılmaktadır. Daha az sayıda UTM cihazı, daha fazla sayıda eski cihazla aynı düzeyde güvenlik sağlayabilir. Bununla birlikte, paketleri denetleyen daha az cihaz olsa bile, UTM cihazlarının kullanımında, cihazların gerçekleştirmesi gereken yoğun miktardaki iş nedeniyle bir ağı genellikle yavaşlatır. Her bir ağ paketini, ağ yığınının çoklu katmanlarında incelemek ve analiz etmek zaman alır. Bu nedenle, bazı kurumlar bir "orta yol" yaklaşımını seçmektedir. Bir **web güvenlik ağ geçidi (*web security gateway*)**, bir UTM cihazının yaptığı şeylerin bir kısmını gerçekleştirerek tüm işletim yüküne maruz kalmaz. Kısacası; bir web güvenlik ağ geçidi, URL filtreleme gerçekleştirir, ancak paketlerin içeriğini incelemez.

NOT

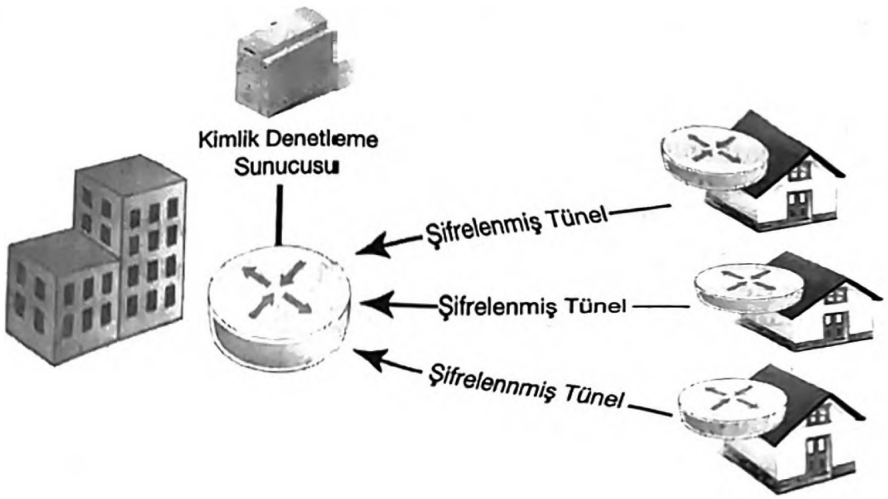
Güvenlik duvarlarının bir diğer kullanışlı özelliği ise **yük dengeleyici (*load balancer*)** olarak yapılandırılabilmesidir. Bir yük dengeleyici, tıkanıklığı önlemek için ağ trafiğini başka ağ kesimlerine dinamik olarak yönlendirebilir. Güvenlik duvarı, bilinen ağ kesimlerini izler ve hedef ana sistem için uygun olan ve kullanılabilir bant genişliği olan bir ağ kesimine trafiği yönlendirir. Bu da, talep yüksek olduğunda ağların yavaşlamasını önleyebilir.

Sanal Özel Ağlar ve Uzaktan Erişim

Evden çalışmanın mümkün olmasıyla uzaktan çalışma, bir çok kurumsal ağın ortak bir parçası haline gelmiştir. Günümüzde birçok şirket, şirket ofisine nadiren gelen çalışanlara sahiptir. Bu kullanıcılar evde ya da yolda çalışmaktadır. Buna rağmen, yine de kurumsal kaynaklara erişmeleri gerekmektedir. Bu da BT uzmanlarının istediğinden daha fazla kurumsal kaynağa internetten erişim açmak anlamına gelmektedir. Kurumsal çalışanlara ihtiyaç duydukları erişimi sağlarken, saldırganları bu potansiyel açık kapılardan uzak tutmak da hüner gerektirmektedir.

Sanal özel ağlar (*virtual private network* - VPN'ler), genel veri ağında ilettiğiniz verilerin güvenlik seviyesini artırmanın iyi bir yoludur. Genellikle bir kullanıcı ile kurumun ağı arasında gönderilen tüm verileri korumak için şifreleme kullanılır. Uzaktan erişim için VPN kullanmak güvenlik sağlar

ŞEKİL 10-11
VPN erişimi.



ve uygun maliyetlidir. İki konum arasında VPN ile tahsisli bağlantı kullanmak arasındaki maliyet farkı belirgindir. ŞEKİL 10-11, bir ağa VPN erişiminin örneğini göstermektedir.

VPN; ağ geçidi ekipmanınızın, şifreleme algoritmalarını işlemek için çok fazla işlem gücüne sahip olmasını gerektirir. Yönlendirici veya güvenlik duvarının VPN'i sonlandırmasını sağlamak yerine, özel bir **VPN yoğunlaştırıcı (*VPN concentrator*)** kullanarak bu işleme gücünü başka bir aygıta yükleyebilirsiniz.

Bir VPN'in yerleştirilmesinde, son kullanıcı bilgisayarlarının güvenliğini de göz önüne almanız gerekir. Kullanıcıların kurumsal ağa bağlanmak için kullandıkları bilgisayarları, o bilgisayara erişim kazanmış bir saldırgan için kurumun kaynaklarına açılan bir kapı olabilecektir. Bu nedenle, birçok kurum, çalışanların ev bilgisayarlarına güvenlik yazılımı yüklemelerini şart koşmaktadır. VPN erişimini, kurumunuzun sahibi olduğu ve yönettiği dizüstü bilgisayarlardan olacak şekilde de sınırlayabilirsiniz.

Bugün kullanılan üç temel VPN teknolojisi şu şekildedir:

- **Noktadan Noktaya Tünel Protokolü (*Point-to-Point Tunneling Protocol* - PPTP)**—PPTP, bir zamanlar en baskın VPN protokolüydü. Neredeyse tüm VPN'ler uzun yıllar boyunca PPTP kullandı. Çoğu işletim sisteminde PPTP desteği bulunduğu için, istemci bilgisayarlarda kurulumu kolaydır.
- **Güvenli Soket Katmanı (*Secure Sockets Layer* - SSL)**—Güvenli Soket Katmanı, web iletişimlerini şifreler ve birçok VPN şifrelenmiş iletişim sağlamak için SSL kullanır. Kullanıcılar SSL korumalı bir web sayfasına bağlanır ve oturum açar. Web tarayıcıları, onları VPN'ye bağlayan yazılımı indirir. Bu tür kullanım, sistemin önceden yapılandırılmasını gerektirmez. Bu nedenle, SSL VPN'ler hızla rağbet kazanmaktadır.
- **IPSec—İnternet Protokol Güvenliği (IPSec-Internet Protocol Security)**, konumları güvenli bir şekilde bağlamak için tasarlanmış bir protokol paketidir. Bazı IPSec VPN'leri son kullanıcılar için kullanılabilir olmasına rağmen, çoğu nlukla a kullanıcının sisteminde üçüncü parti yazılımların kurulumunu gerektirir ve popüler değildir. Birçok kuruluş, bir siteden diğerine güvenli bir şekilde internet üzerinden bağlanmak için IPSec kullanmaktadır. Gerekli IPSec VPN işlevi, yapılandırmayı kolaylaştırmak için birçok yönlendirici ve güvenlik duvarına entegre edilmiştir.

VPN'ler, bir kuruma açık bir fayda sağlamaktadır. Konumlar arasındaki tahsisli bağlantılardan ucuz ve güvenli bir alternatif bağlantı imkanı sunar. Ayrıca, kullanıcıların uzak konumlardan kurum

ağına güvenli bir şekilde bağlanmalarını sağlarlar. Bu da artan verimliliği garanti eder; çünkü çalışanlar, ihtiyaç duydukları kaynakları kurum dışında iken kolayca elde edebilmektedir.

Ağ Erişim Kontrolü

Ağ erişim kontrolü (*Network access control* - NAC) sistemleri, bir cihazın ağınıza bağlanmasına izin vermeden önce daha fazla güvenlik gereksinimleri sağlaması koşullarını eklemenizi sağlar. İki önemli görevi yerine getirirler: Kimlik denetleme (*authentication*) ve durum kontrolü (*posture checking*). NAC yeni bir teknoloji olmasına rağmen popülerliği her geçen gün artmaktadır. Pek çok kuruluş, günümüzde ağlarını kullanan hem dahili kullanıcılar hem de misafirler için NAC konuşlandırmaktadır. NAC, kablolu ve kablosuz ağlarda çalışmaktadır.

IEEE 802.1x standardı, en yaygın NAC teknolojisini tanımlar. Genellikle 802.1x veya 1x olarak anılan bu standart, istemcilerin ağa giriş kazanmak için cihazların bir NAC sistemiyle nasıl etkileşime geçebileceğini anlatır. Kullanıcıların bilgisayarlarındaki yazılımlar, ondan ağda oturum açmasını ister. NAC sistemi; kullanıcının kimlik bilgilerini doğruladıktan sonra, kullanıcıya ağa erişim izni vermek için (kablolu bir ağ için) anahtara veya (kablosuz ağ için) erişim noktasına talimat verir. Bu, NAC'ın kimlik denetleme bileşenidir.

Durum kontrolü, NAC teknolojisinin seçimli ikincil bir kullanımıdır. NAC sistemi; durum kontrolü kullanıldığında, ağa erişim izni vermeden önce kullanıcının bilgisayarının yapılandırmasının güvenlik standartlarını karşılayıp karşılamadığını kontrol eder. Sık denetlenen bazı şeyler şunlardır:

- Virüsten koruma yazılımının güncelliği
- Ana sistem güvenlik duvarının aktifliği
- İşletim sisteminin desteklenme durumu
- İşletim sisteminin yama durumu

Kullanıcılar uyumlu olmayan bir sistemi ağa bağlamaya çalışırlarsa, NAC cihazı iki seçenek sunar. Yönetici, eksikler tamamlanıncaya kadar bu tür sistemleri ağdan engellemeye karar verebilir. Alternatif olarak sistem, ana ağa erişim kazanmadan önce sistemi düzeltebileceğiniz özel bir karantina ağına bağlanabilir. **Genişletilebilir Kimlik Denetleme Protokolü (*Extensible Authentication Protocol* - EAP)**, anahtarların taşınması ve kimlik denetleme yeterlilik belgelerini tanımlayan bir kimlik denetleme çerçevesidir. EAP, yaygın olarak kablosuz ağ kimlik denetlemesinde kullanılır. **Korumalı Genişletilebilir Kimlik Denetleme Protokolü (*Protected Extensible Authentication Protocol* - PEAP)**, temelde bir TLS tünelinde çalışan EAP'dir. PEAP, kimlik denetleme alışverişi için EAP'den daha fazla güvenlik sağlar.

Kablosuz Ağlar

Kablosuz ağlar, cihazları ev içinde ve ofiste birbirine bağlamak için çok popüler hale geldi. Kablosuz ağlar; dizüstü bilgisayarları, masaüstü bilgisayarları, akıllı telefonları ve pek çok diğer cihazı bağlayabilir. Kablosuz ağ oluşturma, kullanıcıların bir ağ kablosunu takmak için bir yer bulma endişesi olmadan binadaki herhangi bir yerden çalışmasını sağlar.

Bir kablosuz ağı yapılandırmak oldukça kolaydır ve ucuzdur. Sorulması gereken soru şudur: Kablosuz teknoloji, ağınızın güvenliğinde nelere yol açar? Bir çalışanın ağa bağlanması o kadar kolaysa, başkalarının da bağlanabileceği anlamına mı gelir?

Güvenli bir kablosuz ağ kurmak (en azından herhangi bir kablolu ağı kadar güvenli bir şekilde) mümkündür. Ama bu; dikkatli planlama, yürütme ve sınama (test) gerektirir. Düzgün olarak

yapılandırılmış güçlü şifreleme, güvenli bir kablosuz ağı çalıştırmak için kritik önem taşır. Bu bölümde, kablosuz ağ teknolojisini inceleyecek ve kablosuz ağları nasıl yapılandıracağınızı ve güvenliğini nasıl sağlayacağınızı öğreneceksiniz.

Kablosuz Erişim Noktaları

Bir **kablosuz erişim noktası (*wireless access point* - WAP)**, kablolu ve kablosuz bir ağ arasındaki bağlantıdır. WAP'lar radyo yayınıdır, kablosuz cihazlardan havadan aldığı ağ bilgisini kablolu ağ ile gönderip almaktadır. Bir kablosuz erişim noktasının kapsama alanındaki herhangi bir kimse WAP ile iletişim kurabilir ve ağa bağlanmaya çalışabilir.

Güvenliğinizi baltalamak isteyen saldırganlar, kablosuz ağ ile çeşitli şeyler yapabilir. Birincisi; kablosuz ağların, kuruluşunuzun ağının alanını duvarlarınızın ötesine taşıdıklarını anlarlar. Kablolu bir ağa fiziksel erişimi kolayca kontrol edebilirsiniz ancak duvarlar ve çitler kablosuz sinyalleri durdurmaz. Bu nedenle, düzgün güvenlik içermeyen kablosuz ağlar, ağınıza bağlanmak isteyen saldırganlar için kolay bir hedef oluşturmaktadır. İkincisi; bir kablosuz ağı dinlemenin, kablolu bir ağı dinlemekten çok daha kolay olduğunu bilirler. Kablosuz ağın kapsama alanındaki herhangi bir kimse için, bu ağda gönderilen tüm verileri yakalamak çok basittir. Bu veriler şifrelenmemişse, saldırı için kolay hedeftir.

Kablosuz Ağ Güvenlik Denetimleri

Neyse ki, kablosuz ağınızı güvence altına almak için oldukça çok şey yapabilirsiniz. Bu bölümde, çeşitli kablosuz ağ güvenlik denetimi örneklerine bakacağız. Gizlice dinlemeyi önlemek için kablosuz şifrelemenin kullanılması en önemlisidir. Katma güvenlik sağlayan diğer teknikler için şu önlemler sayılabilir; hizmet kümesi tanımlayıcısı (*service set identifier* - SSID) yayıncılığının devre dışı bırakılması, **MAC adres filtrelemesinin** uygulanması ve kablosuz ağa güçlü kimlik denetlemesinin eklenmesidir.

Kablosuz Ağ üzerinden VPN

Güvenli kablosuz ağları uygulamak için en güvenli yöntemlerden biri, tüm kablosuz bağlantılar için VPN'in kullanılmasıdır. Bunu dahili kullanıcılar için yönetmek kolaydır, ancak misafirlerin VPN'e erişimini sağlamak daha zordur. Ortak bir çözüm ise en az iki ayrı kablosuz ağ oluşturmaktır; dahili ağınıza daha ayrıcalıklı haklara sahip bağlantı ihtiyacı duyan dahili kullanıcılar için VPN erişimi gerektiren bir ağ ve konuklar için VPN erişimine izin verilmeyen başka bir ağ. Konuk ağının dahili ağınıza bağlantısı çok kısıtlı haklarla olmalıdır.

Kablosuz Şifreleme

Şifreleme, kablosuz ağınızı korumak için yapabileceğiniz en önemli, tek şeydir. Dışarıdan birinin, ağ üzerinden seyahat eden bilgileri görüntülemesini şifreleme imkansız hale getirir. Şifreleme yapılmamışsa, tüm kablosuz kullanıcıların faaliyetleri, kablosuz ağınızın kapsama alanında bulunan herhangi biri tarafından görülebilir. Bir saldırganın binanızın otoparkında oturması, standart bir dizüstü bilgisayara bağlı ucuz bir antenle kablosuz ağınızda gerçekleşen her şeyi izlemesi mümkündür.

Bunlardan kaçınmak için güçlü şifreleme kullanmalısınız. Kablosuz ağların ilk günlerinde endüstri tarafından, temel şifreleme sağlayan **Kabloluya Eş değer Gizlilik (*Wired Equivalent* Privacy - WEP)** adlı bir standart geliştirildi. WEP, Ron Rivest'in seksenlerin sonunda RSA için yarattığı RC4 şifreleme

LEAP ve PEAP

Cisco Systems; kablosuz ağ anahtarları ve kimlik denetlemeyi yönetmeye yardımcı olmak için kendi **Hafif Genişletilebilir Kimlik Denetleme Protokolü (*Lightweight Extensible Authentication Protocol* - LEAP)**'nü geliştirdi. LEAP, güvenli bağlantılar kurmak için WEP veya **Geçici Anahtar Bütünlüğü Protokolü (*Temporal Key Integrity Protocol* - TKIP)**'i kullanabilir. WEP zayıflıkları iyi biliniyordu; bu yüzden TKIP, sadece WEP'i destekleyebilen mevcut donanım üzerinde çalışacak geçici bir önlem olarak ortaya çıktı.

Bölümde daha önce belirtildiği gibi; daha sonra Cisco, Microsoft ve RSA bir araya gelerek LEAP'ın zayıf yönlerini ele aldılar ve Korumalı Genişletilebilir Kimlik Denetleme Protokolü (*Protected Extensible Authentication Protocol* - PEAP)'i yarattılar. PEAP, sunucuda bir sertifika gerektirdiğinden, Hafif EAP'den farklıdır.

algoritmasına dayanır. Güvenlik analizcileri, WEP'in ilk sürümünden beri onu güvensiz hale getiren önemli kusurlar keşfettiler. Bir WEP ağındaki şifrelemeyi internette ücretsiz bulunan yazılımlarla birkaç saniye içinde kolayca kırmak mümkündür. Aslında bir kablosuz ağ üzerinde WEP'i kullanmak; muhtemelen herhangi bir şifreleme olmadan kullanmaktan daha kötüdür, çünkü güvenliğin var olduğuna dair yanlış bir his sağlar. İnsanlar, kablosuz ağların trafiği şifrelediğini düşündüklerinden dolayı güvende olduklarını hissediyorlar. Oysa ki verilerini korumak için bir şifreleme oyuncağının (Cap'n Crunch® dekoder yüzüğü gibi) eş değerini kullandıklarının farkında değiller.

Neyse ki, WEP'e bir alternatif var. Aslında, WEP'in zayıf yönlerini gidermek için çeşitli alternatifler geliştirildi. **Sayaç Modu Şifreleme Bloğu Zincirleme Mesaj Doğrulama Kodu Protokolü (*Counter Mode Cipher Block Chaining Message Authentication Code Protocol*, CCMP)**, 802.11i standardını uygulayan bir şifreleme protokolüdür. CCMP, AES standardının Sayacı Modunu kullanarak gelişmiş güvenlik sağlar. CCMP'ye ek olarak, **Wi-Fi Korumalı Erişim (Wi-Fi *Protected Access* - WPA)** standardı, ağlardaki verileri korumak için güçlü AES şifreleme kullanır ve WEP'deki güvenlik açıklarına sahip değildir. WPA, IEEE 802.11i güvenlik standardının taslak belgesine atıfta bulunmaktadır. Bu standart, WEP açıklarına bir ara çözüm olarak tasarlanmıştı. WPA, 2003 yılında kullanılmaya başlandı. Daha güvenli bir standart olan WPA2, 2004 yılında kullanıma sunuldu. Bu standardın resmi adı 802.11i-2004'dür. WPA ve WPA2'yi yapılandırmak oldukça kolaydır. WPA ve WPA2'nin temel kullanımında, paylaşılan bir gizli anahtarın ağdaki her bilgisayarın ağ yapılandırmasına girilmesi gereklidir. Daha gelişmiş kullanımlarda; her kullanıcıya benzersiz bir kullanıcı adı ve parola vererek paylaşılan gizli anahtarı değiştirebilirsiniz. Uzaktan Kimlik Denetleme Çevirmeli Giriş Kullanıcı Hizmeti (*Remote Authentication Dial-In User Service*, RADIUS) sunucusu gibi merkezi bir kimlik denetleme sunucusu kullanıldığında, bu parolalar kullanıcının normal kimlik bilgileriyle aynı olabilmektedir. RADIUS, 1991'de tanıtıldı ve uzak kullanıcı bağlantılarını yönetmek için kısa sürede popüler bir protokol haline geldi. Bu protokol; yetkilendirme (*authorization*), kimlik denetleme (*authentication*) ve izlenebilirlik (*accounting*) (AAA) servislerini yönetmek için merkezi bir yöntem sunar. Onun halefi olan Diameter, 1998'de piyasaya sürüldü. Diameter; RADIUS'dan daha fazla hareketlilik sorununu çözebildiği için kablosuz uzaktan bağlantılar üzerinde son zamanlarda daha popüler hale geldi. Örneğin, Diameter; daha iyi dolaşım (*roaming*) desteği içerir, TCP veya SCTP protokollerini kullanabilir.

İPUCU

SSID yayınını devre dışı bırakmak, küçük bir koruma sağlar ancak kusursuz değildir. Aslında; yetenekli bir saldırgan, mevcut ücretsiz yazılım araçlarını kullanarak ağınızın varlığını kolayca keşfedebilir. Bu tekniği kullanmanız, ağınızın tanıtımını yapmayarak sıradan bir saldırganın ilgisini çekmemeyi umduğunuz anlamına gelir.

SSID Yayını

Kablosuz ağlar, varsayılan olarak varlığını genele yayınlar. Ağın SSID'sini içeren duyuruları gönderirler. Bu, ağın genel adıdır. Örneğin bir kafeteryada cihazınızı açtığınızda; bu ağları daha önce gördüyseniz, bilgisayarınız kablosuz ağların mevcut olduğunu söyler. Bu bildirim, mevcut tüm ağların SSID'lerini içerir.

Kablosuz erişim noktalarınızda SSID yayınını devre dışı bırakarak, ağınızın kendisini duyurmasını engelleyebilirsiniz. SSID yayınını devre dışı bırakırsanız, ağınıza bağlanacak kullanıcıların bu ağın var olduğunu bilmeleri ve ağ adını kendilerinin belirtmeleri gerekir. Kurumsal bir ortam gibi düzenli kullanıcıların olduğu yerlerde bu çalışacaktır. Misafirlerin ağınıza erişmesine izin veriyorsanız, bu yöntem çalışmayacaktır.

MAC Adres Filtreleme

WAP'lar hangi bilgisayarların ağınıza bağlanabileceğini kontrol etmek için MAC adres filtreleri uygulamanıza da imkan sağlar. Bu teknoloji ile, WAP'ınıza kabul edilebilir MAC adreslerinin listesini sağlarsınız. Sadece onaylanan bilgisayarların ağınıza bağlanmasına izin vermeli diğer bilgisayarların ağınıza erişimini engellemelisiniz.

MAC adres filtrelemesinin en büyük dezavantajı, bakımının çok komplike olmasıdır. Ağınızda bir avuçtan fazla bilgisayarınız varsa, kabul edilebilir MAC adresleri listesini güncellemek kısa sürede büyük bir sorun haline gelecektir. 20.000 kullanıcıya sahip bir kuruluşta çalıştığınızı farz edin. Her hafta ağda 100 yeni bilgisayar görmeniz şaşırtıcı olmayacaktır. Bu cihazların gelmesiyle eski 100 bilgisayarın da ağdan ayrılmasını da hesaba katmak gerekir. Her hafta 200 MAC adresini güncellemeye çalışmayı kafanda canlandırabiliyor musun? MAC adres filtrelemeyi, anlamlı olduğu durumlarda kullanın.

Ek Kablosuz Güvenlik Teknikleri

Önceki önerilere ek olarak, kablosuz ağ cihazlarınızın donanım seçimini ve yerleştirilmesini göz önünde bulundurun. Doğru donanımın seçilmesi ve bu donanımın doğru konuma yerleştirilmesi, ağınızın güvenliğinde fark edilebilir bir etkiye yol açabilir. Özellikle, kablosuz donanım yönetiminin aşağıda belirtilen yönlerine dikkat edin:

- **Anten türleri**—Kablosuz cihaz antenlerinin, cihazın kapsama alanı üzerinde büyük bir etkisi olabilir. Harici antenler, genellikle dahili antenlerden daha uzak yerlere erişebilir. Antenler değişik şekillerde iletebilir ve alabilir. Bunlar, çok yönlü (tüm yönlerde), yarı yönlü (sınırlı yön) veya yüksek yönlü (odaklanmış yön) olabilir. Kurumunuzun kullanımı için doğru anteni seçin.
- **Anten yerleşimi**—Cihazlarınız için en iyi antenleri seçtikten sonra; antenleri dikkatlice yerleştirerek başkaları için değil, kendi istediğiniz kapsama alanını sağlayın. Çok yönlü bir anteni dış duvara yakın bir yere yerleştirdiğinizde, kablosuz ağınız binanızın dışındaki insanlara ulaşılabilir hale gelecektir.
- **Güç seviyesi kontrolleri**—Kablosuz aygıtın kullandığı gücü, yapılandırma ayarlarından değiştirebilirsiniz. Güç ayarlarını varsayılan değerlerden düşürmek, cihazın kapsama alanını azaltacaktır. Kablosuz ağlarınızın görünürlüğünü sınırlamaya çalışırken de bu ayar yardımcı olabilecektir.
- **Kısıtlanmış ana giriş sayfası**—Kısıtlanmış ana giriş sayfası, tüm yeni bağlantılar için görüntülenen bir web sayfasıdır. Kablosuz cihazınız, bağlantı doğrulanıncaya kadar tüm trafiği bu

sayfaya yönlendirebilir. Kısıtlanmış ana giriş sayfasının en yaygın kullanımı, kablosuz ağınız için bir oturum açma sayfası sağlamaktır.

- **Konum araştırma**— Kablosuz ağları korumak için teknik olmayan en önemli hususlardan biri de konumun araştırılmasıdır. Bir kablosuz ağ ile hizmet vermek istediğiniz fiziksel alanı inceleyin. Tesis zemin planları, kablosuz cihazlar için en iyi yerleşimi belirlemenize yardımcı olabilir. Fiziksel olarak cihazları yerleştirmeden önce kablosuz ağınızı planlamak için çizimler yapın.

Hiçbir ağ tamamen güvenli olmasa da doğru güvenlik denetimlerini yerine getirmek, ağlarınızı daha güvenli hale getirebilir. Ana fikir, asla tek bir denetime güvenmemektir. Her zaman katmanlı denetimler kullanın. Bilgili bir saldırganın, kurduğunuz denetimlerden bir veya daha fazlasını her zaman ele geçirebileceğini varsaymalısınız. Saldırganın verilerinizi ele geçirilebilmesi için çoklu denetimi ele geçirmesi zorunluluğunun garantilenmesi, BT altyapınızı olabildiğince güvenli hale getirmenin en iyi yoludur.

⚠ UYARI

MAC adres filtreleme, zayıf bir güvenlik mekanizmasıdır. Saldırganlar ücretsiz araçlar kullanarak ağınızdaki etkin bir MAC adresini kolayca keşfedebilir ve sonra kendi ağ ara birim kartını keşfedilen geçerli MAC adresini kullanacak şekilde ayarlayabilirler. Bu da bir tür adres yanıltmacasıdır.

BÖLÜM ÖZETİ

Bu bölümde, Açık Sistemler Ara Bağlantısı (*Open Systems Interconnection* - OSI) Referans Modelini ve bir ağın ve kaynaklarının nasıl oluşturulup kullanılacağının bir örneği olarak nasıl hizmet ettiğini öğrendiniz. TCP/IP'ye genel bakış dahil olmak üzere, Ağ Katmanı protokollerini öğrendiniz. Ağ güvenliği için bazı temel araçları öğrendiniz. Ayrıca, kablosuz ağların nasıl çalıştığını ve kurumunuzun güvenliğine nasıl tehditler oluşturduğunu öğrendiniz. Son olarak, güvenlik politikaları, standartlar ve prosedürlerin yanı sıra, BT altyapınızın ancak en zayıf halkası kadar güvenli olduğunun konusunda daha iyi bir bakış açısı kazandınız.

ANAHTAR KAVRAMLAR VE TERİMLER

Access control lists – Erişim denetim listeleri
Application proxy firewall – Uygulama vekil sunucusu güvenlik duvarı
Border firewall – Sınır güvenlik duvarı
Content inspection – İçerik denetimi
Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) - Sayaç Modu Şifreleme Bloğu Zincirleme Mesaj Doğrulama Kodu Protokolü (CCMP)
Demilitarized zone (DMZ) – Arındırılmış bölge (DMZ)
Dynamic Host Configuration Protocol (DHCP) - Dinamik Ana Bilgisayar Yapılandırma Protokolü (DHCP)
Extensible Authentication Protocol (EAP) - Genişletilebilir Kimlik Denetleme Protokolü (EAP)
Fibre channel – Fiber kanal
Fibre Channel over Ethernet (FCoE) - Ethernet üzerinden Fiber Kanal (FCoE)
Firewall – Güvenlik duvarı
Firewall rules – Güvenlik duvarı kuralları
Flood guard – Trafiğe boğma koruması
Hacktivist - Hacktivist
Hub – Dağıtım kutusu
ICMP echo request – ICMP yankı isteği
Implicit deny – Gizli engelleme
Internet Control Message Protocol (ICMP) - İnternet Kontrol Mesajı Protokolü (ICMP)
Internet Protocol Security (IPSec) - İnternet Protokol Güvenliği (IPSec)
IP address – IP adresi

ANAHTAR KAVRAMLAR VE TERİMLER , *devam*

IPv4 addresses – Ipv4 adresleri
Internet Small Computer System Interface (iSCSI) - İnternet Küçük Bilgisayar Sistem Arayüzü (ISCSI)
Lightweight Extensible Authentication Protocol (LEAP) - Hafif Genişletilebilir Kimlik Denetleme Protokolü (LEAP)
Load balancer – Yük dengeleyici
Log analysis – Günlük kaydı analizi
Loop protection – Döngü koruması
MAC address filter – MAC adres filtresi
Malware inspection - Zararlı yazılım denetimi
Network access control (NAC) - Ağ erişim kontrolü (NAC)
Network address translation (NAT) - Ağ adresi çevirisi (NAT)
Network port - Ağ bağlantı noktası
Network reconnaissance – Ağ keşfi
Network seperation - Ağ ayrımı
Open Systems Interconnection (OSI) Reference Model - Açık Sistemler Ara Bağlantısı (OSI) Referans Modeli
Packet-filtering firewall – Paket-filtrelemeli güvenlik duvarı
Point-to-Point Tunneling Protocol (PPTP) - Noktadan Noktaya Tünel Protokolü (PPTP)
Port security – Bağlantı noktası güvenliği
Protected Extensible Authentication Protocol (PEAP) - Korumalı Genişletilebilir Kimlik Denetleme Protokolü (PEAP)
Protocol - Protokol
Router - Yönlendirici
Rule-based management – Kural-tabanlı yönetim
Screened subnet – Denetimli alt ağ
Secure router configuration – Güvenli yönlendirici yapılandırması
Smurf attack – Smurf saldırısı
Stateful inspection firewall – Durum denetimi güvenlik duvarı
Subnet – Alt ağ
Subnet mask – Alt ağ maskesi
Switch - Anahtar
Telephony – Telefon hizmeti
Telephony denial of service (TDoS) - Telefon hizmet reddi (TDoS)
Temporal Key Integrity Protocol (TKIP) - Geçici Anahtar Bütünlüğü Protokolü (TKIP)
Unified threat management (UTM) - Birleşik tehdit yönetimi (UTM)
URL filter – URL filtrelemesi
VPN concentrator – VPN yoğunlaştırıcısı
Web security gateway – Web güvenliği geçidi
Wi-Fi Protected Access (WPA) - Wi-Fi Korumalı Erişim (WPA)
Wireless access point (WAP) - Kablosuz erişim noktası (WAP)
Wired Equivalent Privacy (WEP) - *Kabloluya Eş değer Gizlilik (WEP)*

BÖLÜM 10 DEĞERLENDİRME

1. Bir ağ ve kaynaklarının nasıl inşa edebileceğinin ve kullanabileceğinin temel modeli _____ olarak bilinir.
   A. Dinamik Ana Sistem Yapılandırma Protokolü (DHCP) modeli
   B. Uluslararası Standartlar Organizasyonu (ISO) modeli
   C. Açık Sistemler Ara Bağlantısı (OSI) Referans Modeli
   D. Hiçbiri

2. Bir _____'(n)ın temel işi, bir ağın sınırında bir erişim denetim politikası uygulamaktır.
   A. Güvenlik Duvarı
   B. Yönlendirici
   C. Anahtar
   D. Erişim noktası

3. Bir _____, bugünün her kurumsal ağında kritik bir unsur olup, kuruluşun kaynaklarına dünyanın her yerinden erişilmesine izin verir.
   A. Yerel ağ (LAN)
   B. Geniş alan ağı (WAN)
   C. Dinamik Ana Sistem Yapılandırma Protokolü (DHCP)
   D. Hiçbiri

4. Bir güvenli sanal özel ağ (VPN), genel ağlarda kimliği denetlenmiş ve şifrelenmiş bir kanal oluşturur.
   A. Doğru
   B. Yanlış

5. _____, ABD Savunma Bakanlığı tarafından son derece güvenilir ve hataya dayanıklı bir ağ altyapısı sağlamak için geliştirilmiş bir protokol paketidir.
   A. DHCP
   B. VPN
   C. PPPoE
   D. TCP/IP

6. Bir _____, iki veya daha fazla ağı birbirine bağlayan ve veri paketlerini seçerek aralarında değiştirmelerini sağlayan bir cihazdır.

7. Hangi basit ağ aygıtı, ağ trafiğini yalnızca hedeflenen hedefe göndermek için MAC adresini kullanarak ağ performansını artırmaya yardımcı olur?
   A. Dağıtım kutusu (*Hub*)
   B. Anahtar (*Switch*)
   C. Yönlendirici (*Router*)
   D. Ağ Geçidi (*Gateway*)

8. Güvenlik duvarlarının üç temel türü; paket filtreleme, uygulama vekil sunucusu ve durumsal denetimdir.
   A. Doğru
   B. Yanlış

9. Hangi teknoloji, kablosuz iletişimi şifrelemek için en güvenli yöntemdir?
   A. A. TCP
   B. WEP
   C. WPA
   D. UDP

10. IP adresleri, üreticiler tarafından bilgisayarlara atanır.
    A. Doğru
    B. Yanlış

11. Hangi VPN teknolojisi, kullanıcıların Web üzerinden bağlantı başlatmasına izin verir?
    A. SSL
    B. PPTP
    C. IPSec
    D. ICMP

12. OSI Referans Modelinin hangi katmanı şifreleme için sorumludur?
    A. Uygulama
    B. Sunum
    C. Oturum
    D. Ulaşım

13. DHCP, MAC adresleriyle sistemlere hizmet sağlar.
    A. Doğru
    B. Yanlış

14. Hangi güvenlik duvarı topolojisi DMZ'in uygulanmasını destekler?
    A. Savunma kalesi ana sistemleri
    B. Çok katmanlı güvenlik duvarı
    C. Sınır güvenlik duvarı
    D. Denetimli alt ağ

15. Hangi teknoloji, bir sistemin özel IPv4 adresini internetten gizlemenizi sağlar?
    A. SSL
    B. RADIUS
    C. PPTP
    D. NAT

BÖLÜM

11

Kötücül Kod ve Aktivite

KÖTÜCÜL KOD (*MALICIOUS CODE*) YA DA YAZILIM internet bağlantılı herhangi bir cihaz için bir tehdittir. Bu bölümde, kötü amaçlı kodun nasıl çalıştığını ve nasıl mücadele edebileceğinizi öğreneceksiniz. Basitçe söylemek gerekirse, zararlı yazılım, bilgisayar kullanıcısı olarak, sizin niyetiniz olmayan eylemleri gerçekleştiren herhangi bir programdır. Çoğu zaman kötücül yazılımın amacı sisteminize zarar vermektir. Kötücül yazılım internette, çimlerin arasında sürünen bir yılan gibi hareket eder. Saldırganlar kötücül yazılımı veya **kötü amaçlı yazılımı (*malware*),** şifreleri çalmak, gizli bilgileri çalmak, sisteminizden bilgi silmek (veya şifrelemek) ya da sabit diskleri yeniden biçimlendirmek için kullanırlar. Maalesef, kötü amaçlı kodu sadece virüs koruma yazılımı ile denetleyemezsiniz. Bunun nedeni, kötü amaçlı kodun virüsten daha fazlasını içermesi ve bazı kötü amaçlı yazılımların tespiti engellemesidir.

Kötücül kod, üç bilgi güvenliği özelliğine saldırır:

- **Gizlilik (*Confidentiality*)**– Kötü amaçlı yazılım kuruluşunuzun özel bilgilerini açığa vurabilir. Bu bölümde, kötü amaçlı yazılımın başka türleri olan casus yazılımlar (*spyware*) ve Truva atlarının, kuruluşunuzun özel bilgilerini nasıl yakalayabileceklerini ve yetkisiz hedeflere nasıl gönderebileceklerini öğreneceksiniz.
- **Bütünlük (*Integrity*)** – Kötü amaçlı yazılım veritabanı kayıtlarını hemen ya da belli bir süre sonra değiştirebilir. Değiştirilen verileri bulduğunuzda, kötü amaçlı yazılımın yedeklerinizi de bozduğunu görebilirsiniz. Güvenlik ihlalinden şüphelendiğiniz her an, verilerinizin bütünlüğünü doğrulamanız önemlidir. Süreç pahalı ve bütçenize uygun olmayan bir masraf olabilir .
- **Kullanılabilirlik (*Availability*)** – Kötü amaçlı yazılım dosyaları silebilir veya üzerine yazabilir veya depolama ortamına önemli zararlar verebilir. Bazı kötü amaçlı yazılım türleri, bilgilerinizi silmeden veya yok etmeden bile kullanılamaz hale getirir.

Bir güvenlik uzmanı olarak, kurum personelini veri güvenliğinin herkesin sorumluluğunda olduğuna ikna etmenin çok zor bir iş olduğunu göreceksiniz. Onlar sadece BT departmanının sorumluluğu olduğunu düşünme eğilimindedirler. Sadece bu değil, sizin güvenlik çabalarınızın onların işlerinin önünde bir engel olduğunu düşünme eğilimindedirler. Bu güvenlik çabaları, kötü amaçlı yazılım saldırılarını önlemek için kullanmanız gereken politikaları, prosedürleri ve teknolojileri içerir. Birçok veri ihlali, bir çeşit kötü amaçlı yazılım içerir. Kuruluşunuzu her tür kötü amaçlı yazılımdan korumak, sistemlerinizi büyük ölçekli veri ihlallerine karşı daha dayanıklı hale getirir.

Bölüm 11 Konular

Bu bölüm aşağıda verilen konuları ve kavramları içermektedir:

- Kötü amaçlı yazılımın ne olduğu ve sisteminize nasıl zarar verdiği
- Kötü amaçlı yazılım türlerinin neler olduğu
- Kötü amaçlı yazılımın tarihçesinin ne olduğu
- Kötü amaçlı yazılımın nasıl ticari organizasyonlar için bir tehdit olduğu
- Saldırganları neyin motive ettiği ve saldırganların neleri hedeflediklerı
- Hangi araçların ve tekniklerin saldırıları önlediği
- Hangi araçların ve tekniklerin saldırıları tespit ettiği

Bölüm 11 Hedefler

Bu bölümü tamamladığınız zaman, yapabileceleriniz:

- Kötü amaçlı yazılım ve aktiviteleri tanımlama
- Truva atı (*Trojan*), virüs, solucan (*worm*), casus yazılım (*spyware*), reklam yazılımı (*adware*), fidye yazılımı (*ransomware*) ve spam kavramlarını tanımlama
- Bireylere yönelik kötü amaçlı yazılım risklerini ve tehditlerini anlayabilme
- İşletmelere yönelik kötü amaçlı yazılım risklerini ve tehditlerini anlayabilme
- Kötü amaçlı yazılım saldırısının fazlarını anlayabilme
- Bilgisayar korsanlarının (*hacker*), kod kırıcıların(*cracker*), ve suç işleyenlerin (*perpetrator*) kim olduklarını anlayabilme
- Sosyal mühendislik kavramını tanımlayabilme
- Olay tespit araç ve tekniklerini anlayabilme
- Saldırı önleme araçlarını ve tekniklerini anlayabilme

Kötü Amaçlı Yazılımların Özellikleri, Mimarisi ve İşleyişleri

Güvenlik uzmanları kötü amaçlı yazılımları bilirler. Kötücül yazılım veya kötü amaçlı yazılım, sizin bilgisayar sisteminizde çalışan ve kullanıcının niyetlenmediği işlemleri gerçekleştiren komutlardır. Bu aktivite çeşitli biçimlerde olabilir:

- Bir saldırgan, sisteminizin yönetimini kontrolüne alır ve zarar vermek için komutlar kullanır.
- Saldırgan komutları doğrudan sisteminize gönderir. Sisteminiz bu komutları yorumlar ve yürütür.
- Saldırgan, sisteminize zarar veren veya verileri kullanılamaz hale getiren yazılım programları kullanır. Bu programlar fiziksel ortamlardan (USB sürücü gibi) ya da bir iletişim sürecinden

(internet gibi) gelebilir. Virüsler, Truva atı (*Trojan*) programları ve solucanların (*worm*) hepsi bu tür zararlı yazılım programları örnekleridir.

- Saldırganlar ağınızdaki güvenlik zayıflıklarını tanımlamak ve bunlardan yararlanmak için, yasal uzaktan yönetim araçlarını ve güvenlik yoklayıcılarını (*security probes*) kullanırlar.

Karşılaşabileceğiniz kötü amaçlı kod tehditlerinden haberdar olmalısınız. Bu anlayış, organizasyonunuzu korumak için makul önlemler geliştirmenize yardımcı olacaktır.

Kötü Amaçlı Yazılımların Ana Türleri

Teknik olmayan bir bakış açısından, çoğu bilgisayar kullanıcısı tüm zararlı kodların bir virüs olduğunu düşünür. Aslında, birçok farklı türde virüsün yanı sıra, birçok zararlı kod türü vardır. Her tip benzersiz özelliklere ve mimariye sahiptir. Kötü amaçlı kod saldırılarını tespit etmek, hafifletmek ve önlemek için etkili önlemler tasarlamanız ve uygulamanız gerekir. Bunu yapmak için, çeşitli kötü amaçlı kod türlerini ve her türün nasıl kullanıldığını anlamanız gerekir.

Bu bölümde, yaygın kullanılan saldırgan kod (*hostile code*) türlerinin özelliklerini ve işleyişini tanımayı ve tanımlamayı öğreneceksiniz. Saldırganların her türü nasıl kullandığını öğreneceksiniz, bu da uygun önlemlerin nasıl uygulanacağını anlamanıza yardımcı olur.

Virüs

Bir bilgisayar **virüsü** çalıştırılabilir diğer programlara eklenebilen veya bulaşan yürütülebilir bir programdır. Daha sonra daha çok programa bulaşmak için çoğalır. Bazı virüsler çoğaldıktan sonra yıkıcı aktiviteler de yaparlar. Kötü amaçlı yazılım karşıtı programlardan iyi olanlar, bariz ve zarar verici içeriğe sahip pek çok virüsü fark eder ve yok eder. Bir virüsün temel özelliği, çoğalabilmesi ve genellikle bir tür kullanıcı eylemi içermesidir. Tüm virüsler zarar vermez; bazıları sadece

Virüs Kod Aktivitelerinin Kanıtı

Her virüsü her zaman tanıyamasanız da, virüsleri belli eden birçok gösterge vardır. Aşağıdakilerden herhangi biri virüslü bir bilgisayarı işaret edebilir:

- Bozulan iş istasyonu veya sunucu yanıtı
- İş istasyonlarında beklenmeyen ve uzun süreli disk etkinlik düzeyleri (*churning*)
- Özellikle bilgisayarın başlatılması aşamasında kullanıcı programlarının ani yavaşlığı
- Uygulamaların sebepsiz donması veya beklenmeyen hata iletileri
- Programların tamamlanmadan durdurulmasını (*program aborts*) içeren planlanmayan donanım sıfırlamaları (*hardware resets*) ve çökmeler (*crashes*)
- Anti antivirüs alarmları
- Disk taramasından kaynaklı, artan "kayıp küme (*lost cluster*)" sonuçlarını içeren disk hata mesajları,
- Diskte veya kullanılabilir bellek alanlarında açıklanamayan azalma
- Makro virüs durumlarında, DOT dosyası olarak açılan kayıtlı belgeler
- Kaybolan veya yürütülmeyen uygulamalar (veya onların simgeleri).

can sıkıcıdır ya da kopyalamaya odaklanır. Diğer virüsler içeriklerini (*payload*) saklarlar ve bir arka kapı kurarlar. Bir **arka kapı,** erişim kontrollerini devre dışı bırakmak için gizli bir yoldur. Kaynaklara veya verilere yetkisiz erişime izin verir. Mağdur virüsü fark etmeyebilir veya zarar görmeyebilir.

Üç temel virüs türü vardır. **Sistem başlatma virüsleri (*system infectors*),** bilgisayar donanım ve yazılım başlangıç fonksiyonlarını hedef alan virüslerdir. **Dosya virüsleri (*file infectors*),** yürütülebilir programlara (COM, EXE, SYS ve Microsoft Windows içindeki DLL dosyaları gibi) saldıran ve bunları değiştiren virüslerdir. **Veri virüsleri (*data infectors*),** gömülü makro programlama yetenekleri içeren belge dosyalarına saldıran virüslerdir.

Kötü amaçlı yazılım etkinlikleri, saldırgan ve hedef arasındaki gerçek zamanlı oturumlarda etkileşimli olarak gerçekleşebilir. Alternatif olarak, uykuda kalabilirler ve önceden belirlenmiş bir zamanda veya bazı öngörülebilir olaylarda tetiklenebilirler. Yıkıcı bir eylem başlatabilirler veya sadece gözlem yapıp bilgi toplayabilirler. **ŞEKİL 11.1** bir bilgisayar virüsünün tipik yaşam döngüsünü göstermektedir.

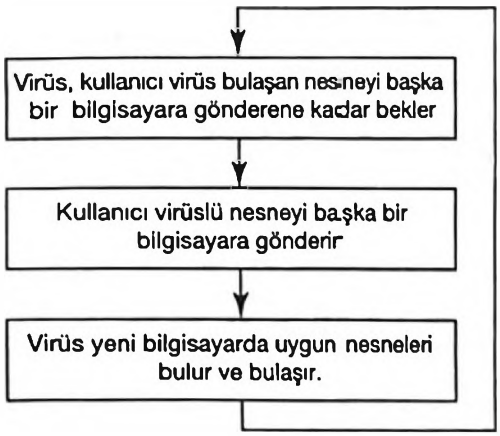
Önyükleme Virüsleri

Sistem başlatma (*Boot Record*) virüsleri, bilgisayardaki ana donanım ve sistem yazılımı bileşenlerini hedef alan virüslerdir. Virüs bulaşan bileşenler, genellikle sistem başlatma süreçleridir. Bu tür bir bulaşma (*infection*), virüsün kontrolü ele geçirmesine ve bilgisayar pek çok koruyucu kontrolü yükleyemeden çalışmasını mümkün kılar. En yaygın sistem başlatma virüsü türleri, önyükleme aygıtı Ana Önyükleme Kayıt (*Master Boot Record*) virüsleridir. Bu virüsler medya alışverişi yoluyla yayılırlar.

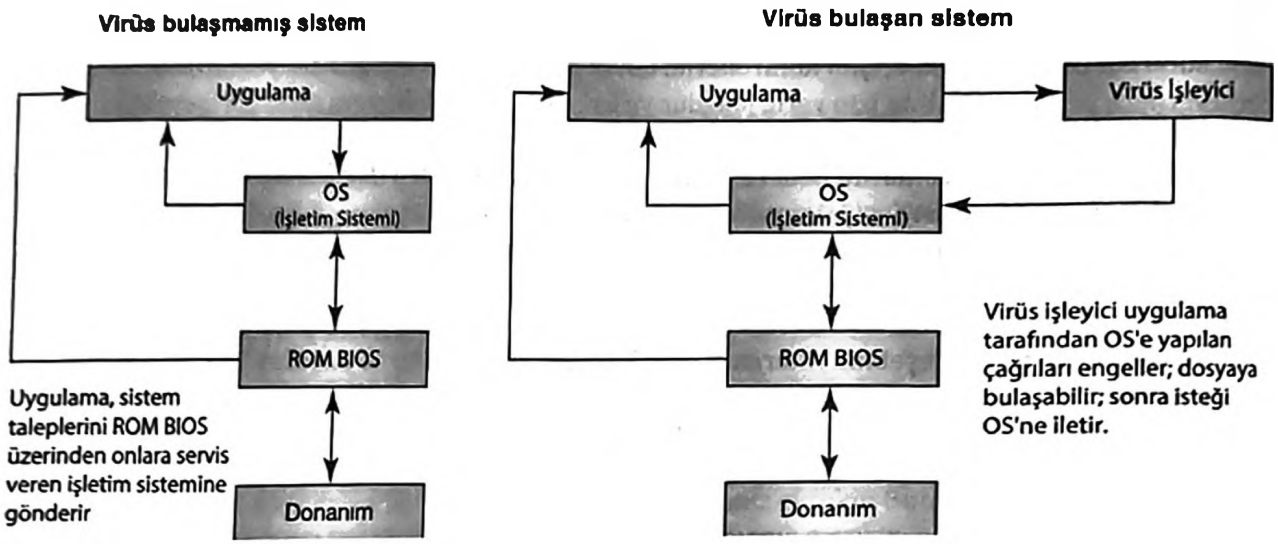
Ana Önyükleme Kayıt ve Sistem Başlatma Virüsleri

Bir Ana Önyükleme Kayıt (*Master Boot Record*) virüsü, önyükleme aygıtının orjinal Ana Önyükleme Kaydı'nı onu virüs ile ilgili kod ile değiştirerek taşır veya yok eder. Daha sonra, bootstrap programından kontrolü alabilir ve düşmanca olan amacını gerçekleştirebilir. Tipik olarak, Ana Önyükleme Kayıt virüsleri görevlerini yerine getirirler ve varlıklarını gizlemek için kontrolü yasal Ana Önyükleme Kaydı veya etkin bölüme geri verirler.

Her iki önyükleme kayıt virüs türü genellikle ROM tabanlı sistem cihazlarını baypas edebilen yönergeleri yükler. Bu seviyede yükleme, virüsün tüm normal uygulamaları ve sistem donanım isteklerini işlemesini sağlar. Bu istekler dosyaların ve dosya dizin servislerinin açılıp kapanması gibi



ŞEKİL 11-1
Bir bilgisayar virüsünün yaşam döngüsü



ŞEKİL 11-2

Sistem başlatma virüsünün çalışması

gibi fonksiyonları içerirler. Bu virüs türü, diğer zararlı kod tiplerini de çalıştırabilir ve kendi izlerini kapatabilir.

Bu ikili eylem kabiliyetine sahip bir **virüs, çok bölümlü virüs (*multipartite* virüs)** adını alır. Ardından dosya enjeksiyon kodunu (*file injection code*) da yürütebilir. **ŞEKİL 11.2**, bir sistem başlatma virüsünün bir bilgisayarı nasıl etkilediğini göstermektedir.

Dosya (Program) Virüsleri

Dosya virüsleri klasik "çoğal ve ekle (*replicate and attach*)" davranışını sergiler. Microsoft Windows tabanlı işletim sistemlerinin yaygın olarak kabül görmesinden ve popüler olmasından dolayı, en iyi bilinen dosya virüsleri bu sistemleri hedefler. Genelde .com veya .exe dosya uzantılı program dosyalarına saldırırlar. Daha yeni virüs türleri SYS, DLL ve diğer birçok Windows dosya türü ile uyumlu çalışır.

Windows bilgisayarlar ortak hedefler olmakla birlikte, kötü amaçlı yazılım saldırılarına karşı hiçbir işletim sisteminin bağışıklığı yoktur. Diğer platformlardaki saldırıların sayısı artmaktadır. Linux ve OS X (Apple'ın işletim sistemi) çalıştıran bilgisayarlar, giderek artan sayıda saldırı ile karşılaşmaktadırlar. Akıllı telefon ve tablet gibi mobil cihazlara yapılan saldırıların sayısı da hızla artmaktadır. Bu mobil cihazlar bilgisayar korsanlarına, az sayıda kullanıcı cihazlarını güvenceye almak için zaman ayırdığından, cazip gelmektedir. Symantec, kötü amaçlı yazılım aktiviteleri hakkında bol miktarda bilgi ve istatistik içeren ve karşı önlemler öneren yıllık İnternet Güvenliği Tehdit Raporu yayınlamaktadır.

BİLGİNİZE

En son Symantec İnternet Güvenliği Tehdit Raporu'nu *https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf* adresinden bulabilirsiniz.

Kötü amaçlı yazılım geliştiriciler, bu virüslerin çoğunu yüksek seviyeli dilleri kullanarak yazıp derlerler. C ve C++ dilleri, virüslerin başarılı olması için gereken gücü ve esnekliği sağlama yeteneklerinden dolayı, ortak tercihlerdir. Buna karşılık, önyükleme kayıt virüslerini yazmak için genellikle assembly dilini kullanırlar. Dosya virüslerinin kodlanması oldukça karmaşık olsa da, çoğu çalıştırılabilir programın mimarisi nispeten basittir.

Bu tür virüsler kendilerini orjinal program dosyasına eklerler. Kendisini kopyalayıp diğer dosyalara bulaşmasına ve muhtemelen bir veri yükü dağıta na kadar, bu dosyanın yürütülmesini kontrol ederler.

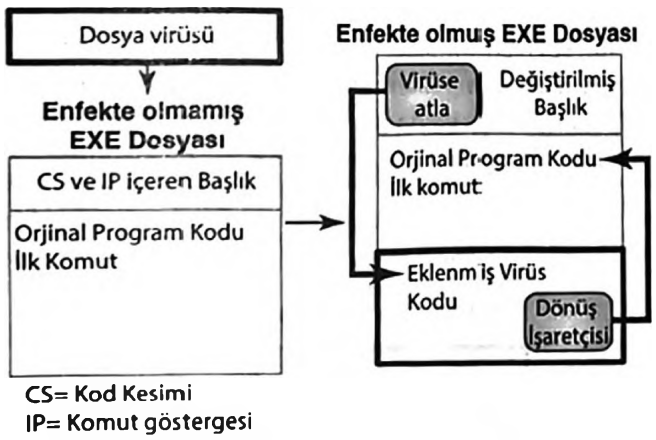
Dosya virüsünün bir türü, eşlik eden (*companion*) virüs, kendisini ana bilgisayarda yürütülen orjinal programa eklemeyen gerçekten ayrı bir program dosyasıdır. Bunun yerine, eşleşen bir dosya adına sahip ancak orjinalinden daha önce yürütülen bir uzantı ile yeni bir program oluşturur. Örneğin, Windows .exe dosyalarından önce .com dosyalarını yürütür. Bu dosyayı, gerçek program ile aynı dizin altında oluşturur. Kullanıcı programı çalıştırdığında, işletim sistemi meşru program yerine kötü amaçlı yazılımı çağırır. Virüs işini tamamladıktan sonra, orjinal programı başlatmak için ilgili komutu çalıştırır. **ŞEKİL 11.3** bir dosya virüsünün nasıl çalıştığını göstermektedir.

Makro (Veri Dosyası) Virüsleri

Makro virüsler, yazılım satıcıları popüler ofis uygulamalarına kayıt yetenekleri eklediğinde, bir sorun haline geldi. Kullanıcılar eylemlerini bir program a kaydetmek için makro kayıt yeteneklerini kullanırlar. Bu eylemlerin kaydedildiği uygulama, bu komutları veri dosyası ile birlikte depolar. Kullanıcı, daha sonra dosyayı açtığında veya önceden tanımlanmış bir tuş dizisine bastığında bu eylemleri otomatik olarak yürütebilir. Makroların asıl amacı, tekrarlı süreçleri otomatikleştirmekti. Kullanıcılar bu özelliği beğendiler çünkü uygulamaları daha uygun ve verimli kıldı. Ancak, bu makrolar kendi komutlarını uygulamak için kötü amaçlı yazılımlara bir kapı açtı.

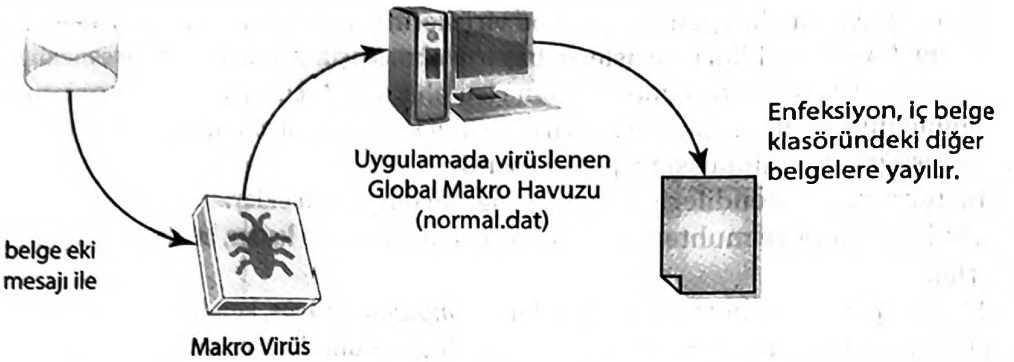
Makro virüsler bu belge dosyalarına bulaşır ve kendi komutlarını ekler. Kullanıcılar virüslü belgeyi diğer kullanıcılarla paylaştığında, kötü amaçlı yazılım yayılır ve çoğalır. Çoğu ofis uygulamasının bağlı yapısı, virüs bulaşmış belgelerin diğer bilgisayarlara ve kullanıcılara yayılmasını kolaylaştırır. Makrolar platformlar arasında kolayca hareket edebilir ve inşa edilmeleri oldukça kolaydır. Bu nedenle, makro virüsler bilgisayar korsanları arasında son derece popülerdir.

Elektronik posta bombası (*electronic mail bomb*), bir kötü amaçlı makro saldırı türüdür. Bu saldırı türü genellikle maksimum hasarı vermek üzere tasarlanmış makroları içeren bir posta eki içerir. Saldırganlar, hedefine ulaşmak üzere belge ekini adsız bir e-posta gönderme sitesi aracılığıyla



ŞEKİL 11-3
Bir dosya virüsünün çalışması

ŞEKİL 11-4
Makro virüsün çalışması



gönderebilirler. E-posta bombasını alan birinin makro virüsünü bulaştırmak için eki açması yeterlidir. Bazı durumlarda, sadece e-posta mesajının ön izlemesi bile e-posta bombasını etkinleştirir. **ŞEKİL 11. 4** bir makro virüsünün nasıl çalıştığını gösterir.

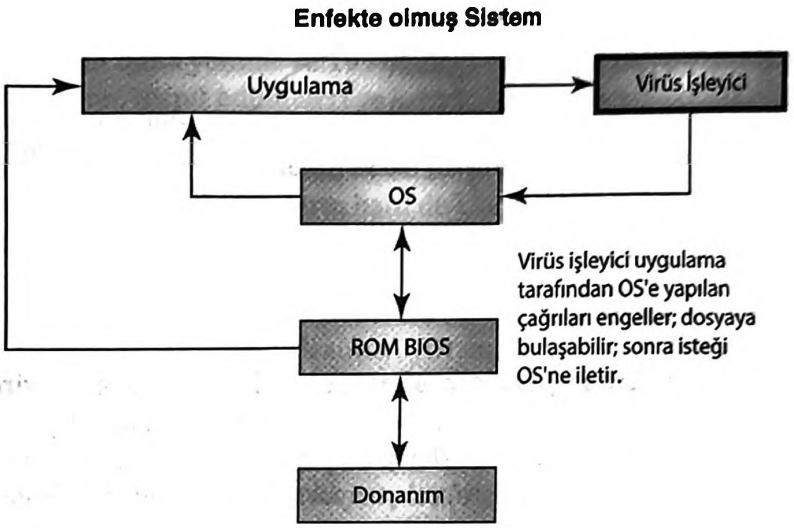
Diğer Virüs Sınıflamaları

Virüsler, antivirüs yazılımınca algılanmaktan kaçınmak ve yayılmak için bir dizi tekniğin herhangi birinden faydalanabilirler. Pek çok tek bilgisayar virüsü, her dosyaya, önyükleme sektörüne ya da bulaştığı belgeye kendi kopyalarını kopyalayarak çalışır. Virüs, sonraki enfeksiyonları, byte byte birebir kopyasını çıkararak, aynı şekilde gerçekleştirir. Bu öngörülebilir eylem bir imza modeli oluşturur. Pek çok antivirüs ve kötü amaçlı yazılım önleme programı kötü amaçlı yazılımları algılamak için bu imzayı kullanır. Bazı virüsler, mesela aşağıdaki gibi farklı davranırlar:

- **Çok biçimli virüsler (*Polymorphic viruses*)** — **Çok biçimli virüsler,** virüsün gövdesini çoğaltırken, virüs gövdesini şifreli formatta depolayan ayrı bir şifreleme makinesi içerirler. Virüs, olası tespit edilme durumu için yalnızca şifre çözme rutinini gösterir. Virüsün kontrol bölümünü şifre çözme rutininde gömer. Şifre çözme rutini, hedef sistemin kontrolünü ele geçirir ve virüsün ana gövdesini çözer, böylece çalıştırabilir. Gerçek çok biçimli virüsler, her yinelemede şifre çözme işlemini değiştirmek için ek dönüştürme motoru kullanırlar. Bu, kodun bu kısmını bile tanımlamayı daha da zorlaştırır. **ŞEKİL 11.5** çok biçimli bir virüsün bir bilgisayarı nasıl etkilediğini göstermektedir.
- **Gizli virüsler (*Stealth viruses*) —Zırhlı virüsler (Armored viruses)** olarak da adlandırılan **gizli virüsler,** kendilerini kullanıcılardan ve algılama yazılımlarından gizlemek için birtakım teknikler kullanırlar. Düşük seviyeli bir sistem servis fonksiyonu kurarak, herhangi bir sistem talebini engelleyebilir ve varlıklarını gizlemek için servis çıkışını değiştirebilirler. Gizli virüsler, boyut gizliliği, okuma gizliliği ya da her ikisine birden sahip olabilirler. **ŞEKİL 11.6** bir gizli/zırhlı virüsün nasıl çalıştığını göstermektedir.



ŞEKİL 11-5
Çokbiçimli virüsün çalışması



ŞEKİL 11-6
Gizli virüsün çalışması

BİLGİNİZE

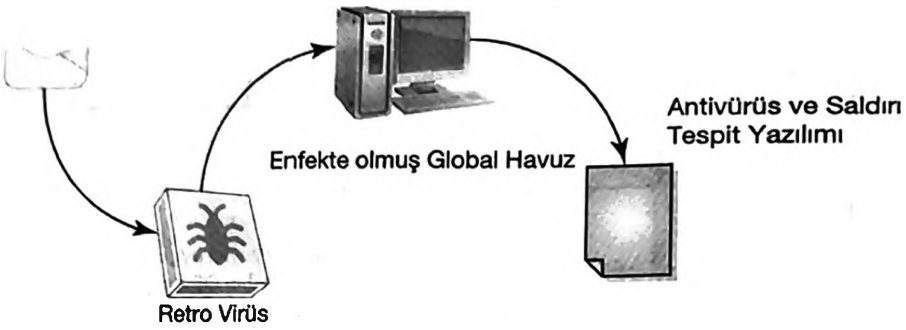
Boyut gizlemesi, virüslü bir dosyanın olduğundan büyük olduğunu gizler. Virüs, dosya bilgisi için sistem taleplerini keser ve talep sürecine geri göndermeden önce kendi büyüklüğünü cevaptan çıkarır. Okuma gizliliği, virüsün önyükleme sektörü kodunu taşıdığı gerçeğini gizler. Virüs, yeniden konumlandığı ve viral kod ile yer değiştirdiği normal önyükleme sektörü için gelen okuma/yazma taleplerini durdurur. Virüs, isteği orijinal önyükleme sektörü kodunun yeni gizli konumuna yönlendirir.

- **Yavaş virüsler (*Slow viruses*)** —**Yavaş virüsler,** virüsten koruma programlarının virüslü dosyalardaki değişiklikleri algılamasını engeller. Bu virüs sınıfı, bilgisayarın belleğinde bulunur ve virüsten koruma yazılımı bunu algılayamaz. Yürütme için, dosyaları kopyalamak veya taşımak gibi belirli görevleri bekler. İşletim sistemi dosyayı belleğe okuduğundan, virüs, çıktı dosyasına yazmadan önce girdi dosyasından okunan verileri değiştirerek tespit edilmesini çok daha zor hale getirir. **ŞEKİL 11-7** yavaş bir virüsün nasıl çalıştığını gösterir.
- **Retro virüsler** — **Retro virüsler** antivirüs imza dosyaları veya bütünlük veritabanları gibi karşı önlemlere saldırırlar. Bir retro virüs bu veri dosyalarını tarar ve onları siler ya da değiştirir, böylece virüsten koruma yazılımının işlevlerini devre dışı bırakabilir. Diğer virüsler, özellikle önyükleme virüsleri (başlangıçta hedef sistemin kontrolünü ele geçiren), eğer bulursa AV, güvenlik duvarı (*firewall*) ve saldırı tespit sistem (*Intrusion Detecton System*-IDS) yazılımını devre dışı bırakmak için, Windows kayıt defteri anahtarları ve diğer işletim sistemi anahtarı başlangıç dosyalarını değiştirir. **ŞEKİL 11.8,** bir retro virüsün nasıl çalıştığını göstermektedir.



ŞEKİL 11-7
Yavaş virüsün çalışması

ŞEKİL 11-8
Retro virüsün çalışması



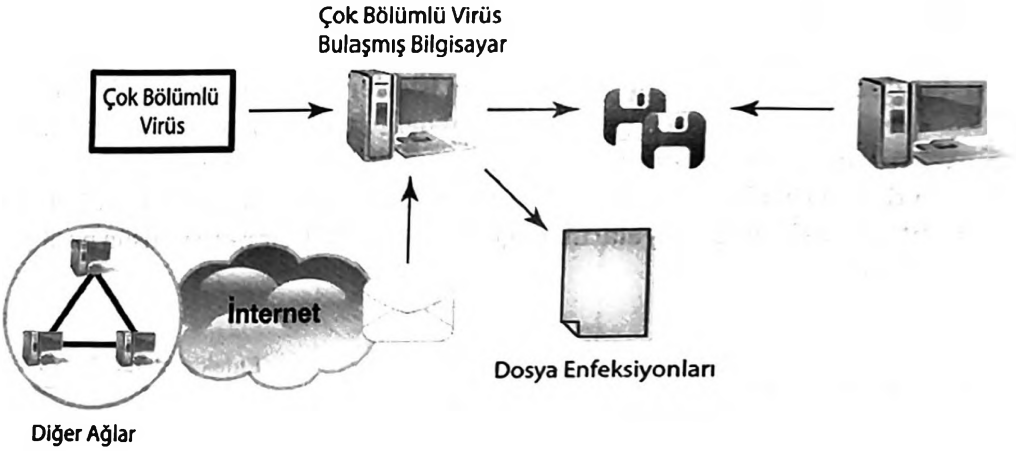
- **Platformlar arası virüsler (Cross-platfom viruses)** — **Platformlar arası virüsler** daha az yaygındırlar. Birden çok işletim sistemini hedefleyen bir dizi belgelenmiş virüs vardır (örneğin, Apple Macintosh HyperCard virüsleri). Bu platformlar ayrıca Windows öykünme/benzetim yazılımı (*emulation software*) çalıştırıyorsa, bir gerçek Windows bilgisayar olarak Windows virüslerine duyarlı hale gelir.
- **Çok bölümlü virüsler (Multipartite viruses)**—Daha önce bahsedildiği gibi, çok bölümlü virüsler çoklu davranışlar sergileyen hibrit virüslerdir. İki ana türü vardır: Ana Önyükleme Kaydı/önyükleme sektörü virüsleri ve dosyaları etkileyen virüs. Bu tür virüsler bir uygulama içinde dosya enfektörleri olarak mevcut olabilir. Virüs bulaşan uygulamanın çalıştırılması üzerine, virüs bir Ana Önyükleme Kaydı enfeksiyonunu oluşturabilir ve bu da sistemi yeniden başlattığınızda diğer dosyalara bulaşır. **ŞEKİL 11-9** çok bölümlü bir virüsün nasıl çalıştığını göstermektedir.

1994 yılında izole edilen One Half virüsü gibi bazı çok bölümlü virüsler, hem gizli hem de polimorfik özellikler sergileyebilir.

Korsanlık amaçlı programlar (Rootkits)

Korsanlık amaçlı bir program, bir bilgisayarın tehlikede olduğunu gizlemek için, bir ya da daha fazla programı modifiye eden veya yerlerini değiştiren bir tür kötü amaçlı yazılımdır. Bu programların, kendilerini gizlemek için işletim sistemlerinin parçalarını değiştirmeleri yaygındır. Bu programlar bilgisayarın önyükleme komutlarından işletim sistemindeki uygulamalara kadar her seviyede bulunabilir. Bir kez yüklendikten sonra, korsanlık amaçlı programlar saldırganlara tehlikede

ŞEKİL 11-9
Çok bölümlü bir virüsün çalışması



bilgisayarlara erişerek ek saldırı başlatma imkanı sağlarlar. Korsanlık amaçlı programlar, diğer kötü amaçlı yazılımlardan daha yenidir ve 1990'lara kadar ortaya çıkmamıştır. Ana amaçları kendilerini gizlemek olduğundan, tespit edilmeleri ve kaldırılmaları çok zor olabilir. Ancak, korsanlık amaçlı programların tespiti ve kaldırılması sistem güvenliğini korumak için çok önemlidir.

2015 yıllında, çok ciddi tipte korsanlık amaçlı programları tanımlayan raporlar ortaya çıkmaya başladı. Korsanlık amaçlı programların hard disk sürücülerinin aygıt yazılımına veya bir bilgisayarın Temel Giriş /Çıkış Sistemi (*Basic Input/Output System* - BIOS)'ne gömülebileceği keşfedildi. Bu korsanlık amaçlı programlar, işletim sisteminin yeniden yüklenmesi ve sabit diskin yeniden biçimlendirilmesinin tamamında var olmaya devam edeceklerdir. BIOS'a bir korsanlık amaçlı programın gömülmesi durumunda, mevcut disk sürücüyü tamamen yeni bir disk sürücü ile değiştirmek bile korsanlık amaçlı programı kaldıramaz. Bu yeni tip korsanlık amaçlı programlar oldukça yaygındır ve teknik beceriye sahip olmaksızın kaldırılmaları zordur. 2016 yılında, çeşitli kaynaklar, belli hedefler üzerinde denetim sağlamak için ABD Ulusal Güvenlik Ajansı'nın (*National Security Agency* - NSA) sabit disk aygıt yazılımı korsanlık amaçlı programlarını kullandığını raporlamışlardı.

Fidye Yazılımı (Ransomware)

Bir başka tip kötü amaçlı yazılım, bir bilgisayar kullanıcısından direkt olarak fon oluşturmaya çalışır. Bu tür kötü amaçlı yazılımlar da en hızlı büyüyen tehditlerden biridir. **Fidye yazılımı**, bir bilgisayara saldırır ve kullanıcının bilgisayarın verilerine erişme yeteneğini sınırlar. Bilgisayarı yavaşlatarak, yetkili kullanıcıların erişimini reddederek veya belirli programlara veya kaynaklara erişimi engelleyerek erişimi sınırlayabilir. Birçoğu, önemli dosyaları, hatta tüm diski şifreleyerek ve onları erişilemez hale getirerek çalışır.

İlk fidye yazılım programlarından biri 2013 yılında piyasaya sürülen CryptOL0cker oldu. Fidye yazılım programları o günden sonra daha karmaşık ve tehlikeli hale geldi. Saldırgan genellikle kullanıcıları kısıtlamalara karşı uyarır ve tam erişimi geri yüklemek için bir ödeme talep eder. Bu ödeme talebi veya *fidye (ransom)*, bu tip kötü amaçlı yazılımlara adını verir. Saldırgan, fidye ödediğinde kullanıcının datalarının şifresini çözmeyi veya erişimi engelleyen mekanizmaları kaldırmayı vaat eder. Pek çok bilgisayar kullanıcısı bilgisayarlarına ve sakladıkları verilere güvenir. Az sayıda bilgisayar kullanıcısı, süregelen hayal kırıklığı yaşamadan, veri ve diğer kaynaklara erişimini kaybedebilir.

İş kullanıcıları fidye yazılımlarını basit bir rahatsızlıktan çok daha fazla bulabilirler. Bir işletmenin bilgisayar sisteminin kilit parçalarına erişilememesi, DoS saldırısı ile aynı etkiye sahip olabilir. Bir fidye yazılımı saldırısı, çok kısa sürede çok büyük miktarda kardan kayba neden olabilir. Saldırganlar, büyük risklere maruz kalırken aynı zamanda büyük karlar elde edebilirler. Fidye yazılımı, kötü amaçlı yazılımlar arasında büyüyen bir trenddir. Mobil cihazlarda kullanıcı güveni, bu cihazları çekici hedefler haline getirmektedir. Bilgisayarlar ve diğer cihazlar daha mobil hale geldikçe, potansiyel fidye yazılımı saldırılarına karşı daha savunmasız hale gelmektedirler.

NOT

Peki, kötü amaçlı bir yazılım bir bilgisayarın kontrolünü nasıl ele alabilir? Kötü amaçlı yazılımlar birçok farklı teknik kullanabilir, ancak yaygın olan ikisi tembel programcılara bağlıdır. *Arabellek taşması (buffer overflow)*, bir programın bir değişkene beklediğinden daha fazla verinin yüklenmesine izin verdiği bir durumdur. Bu olduğunda, "ekstra" veriler, hafızadaki korunan verileri değiştirebilirler hatta bir programın talimatlarını değiştirebilir. Benzer bir zayıflık, bir *tamsayı taşmasıdır (integer overflow)*, yan, basit bir tamsayı değişkeninde depolanmayacak kadar büyük bir sayıya neden olan aritmetik işlemdir. Her iki durumda da, programcılar hataları üstlenmeli ve kullanıcıyı uyarmalıdır, ancak taşma meydana geldiğinde birçok program alışılmadık şekilde davranır.

İstenmeyen elektronik posta (Spam)

İstenmeyen elektronik posta (spam), ağ yöneticilerinin karşılaştığı en rahatsız edici zorluklardan biridir. Spam, genellikle sadece

virüs ya da diğer zararlı kodlar içermez, aynı zamanda ağları ve posta sunucularını tıkar ve pek çok kullanıcının zamanını ve üretkenliğini boşa harcayabilir. Pek çok virüs, virüslenmiş bir bilgisayarı istenmeyen elektronik posta robot/zombi ağının (*botnet*) bir parçası yapmak için yazılım taşımaktadır. Bu istenmeyen elektronik posta robot ağları yeni virüs sürümleri gönderir.

Çoğu spam koruma yazılımı satıcısı, tüm mesajlaşma trafiğinin yüzde 70 ila 90'ının spam olduğunu tahmin etmektedir. Basitçe söylemek gerekirse, spam herhangi bir istenmeyen mesajdır. Ancak, birçok kullanıcı hala istenmeyen e-postalar açmaktadırlar veya istenmeyen anlık mesajlar almaktadırlar. Mesajlarda, iş vaadi, piyango kazancı veya ürünlerde indirimli fiyatları görmeleri, mesajı kesinlikle "istenmeyen" olarak sınıflandırmalarını zorlaştırmaktadır.

Spam, her ölçekteki kuruluşlar için büyük bir sorun haline gelmektedir. Spam, kuruluşların çalışması gereken bant genişliğini kullanır ve çalışanların zamanını boşa harcar. Spam ayrıca virüs ve solucanlar için çoğalma alanıdır. İçerik olarak rahatsız edici olması durumunda, spam organizasyonu finansal sorumluluğa maruz bırakabilir. Neyse ki, güvenlik yöneticisinin bu mesajları ortadan kaldırmasına yardımcı olacak otomatik araçlar bulunmaktadır. Ne yazık ki, spam üreticileri çok dinamiktir ve spam tespit filtrelerini önlemek için hızlıca değişirler. İstenmeyen postaları tamamen ortadan kaldırmak çok zordur.

İstenmeyen posta önleme hizmetleri ve teknolojisinin artan dağılımına rağmen istenmeyen posta iletilerinin sayısı ve boyutu artmaya devam etmektedir. Belirgin olarak kötü amaçlı kod olmasa da, spam en azından kuruluşlara yönelik şu tehditleri temsil etmektedir:

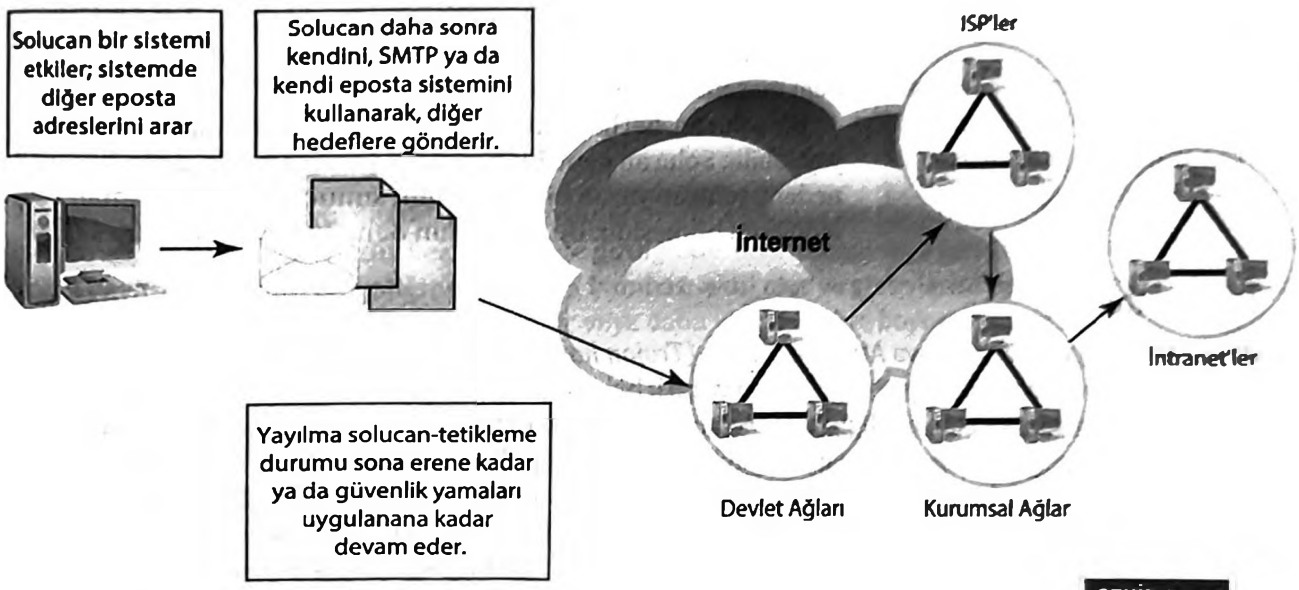
- Spam, bilgi işlem kaynaklarını (band genişliği ve CPU zamanı) tüketir.
- Spam, BT personelini ağ güvenliği için daha kritik olan faaliyetlerden uzak tutar.
- İstenmeyen elektronik posta, kötü amaçlı yazılım kodu (virüsler, düşmanca aktif içerik) için potansiyel bir taşıyıcıdır.
- İstenmeyen elektronik posta yollayanlar, cevaplanmayan elektronik postaları tekrar yollayan servislerin (remailing services) kolaylaştırılması, gerçek kaynak adreslerinin maskelenmesi ve mağdur sistemler için DoS saldırısı oluşturmak amacıyla orta düzey sistemler için teknikler geliştirmiştir.
- İstenmeyen elektronik postalardaki iptal etme (abonelikten çıkma) özellikleri, yasal hedef adresler elde etmek için yeni bir keşif saldırısı şekli sunabilirler.

Solucanlar

Solucanlar (worm), makinenin kendi iletişim protokollerini kullanarak bir makineden diğerine yayılmak için tasarlanmış bağımsız programlardır. Virüslerin aksine, hayatta kalmak ve çoğalmak için bir ana programa ihtiyaç duymazlar. Orjinal olarak, solucanlar ve virüsler arasındaki ayrım,

İstenmeyen elektronik posta (Spam) nedir?

SPAM, tüm büyük harflerle, Hormel Foods'un bir ticari markasıdır. Karışık veya küçük harflerle, bu terim istenmeyen ticari e-postaya atıfta bulunur. Spam teriminin şu andaki kullanımı, ilk olarak 1970 yılında televizyonda yayınlanan bir Monty Python komedi skecinden kaynaklanıyordu. Skeç, her yemeğin SPAM ürününü içerdiği akşam yemeğindeki garsonu canlandırdı. Karakterlerden biri ne zaman "SPAM" kelimesini söylese lokantadaki birkaç Viking tekrar tekrar "SPAM, SPAM, SPAM, SPAM!" diye tezahürat yaptı. Vikinglerin ana diyaloğu bastırması diğer karakterlerin anlaşılmasını zorlaştırdı. Sonuç olarak, *spam* terimi, ana iletiyi zorlayan herhangi bir gürültü veya diğer aşırı iletişim anlamına geldi.



ŞEKİL 11-10

Bir solucanın çalışması

solucanların yayılmak için ağı ve haberleşme bağlantılarını kullanması ve direk olarak çalıştırılabilir bir dosyaya eklenmemeleridir. *Solucan* teriminin kullanımı, solucanların, hepsi bir bilgisayar ağı üzerinden haberleşen farklı bilgisayarlar üzerinde çalışan programlar olduğu gerçeğinden kaynaklanmaktadır.

Solucanlar genellikle belli bir güvenlik açığından yararlanmak için ağa bağlı bilgisayarları araştırırlar. Genel olarak, solucanlar, ağ sorgularına ya da aktivitelerine yanıt verecek belirli bir sunucu veya yardımcı yazılım ararlar. Solucan örnekleri arasında 1988 yılının internet / Morris Worm solucanı yer almaktadır. Daha yeni solucanlar, Conficker ve Stuxnet solucanlarını, Lion solucanı gibi bir dizi Linux solucanını içermektedirler. **ŞEKİL 11-10** solucanın nasıl çalıştığını göstermektedir. Blaster,

Solucan Saldırılarının Kanıtı

Solucanlar, varlıkları ile ilgili birçok belirti bırakırlar. Aşağıdakilerden herhangi biri virüslü bilgisayarı işaret etmektedir:

- Band genişliği tüketiminde açıklanamaz bir artış
- Normal aktivite zamanlarında yüksek hacimli gelen ve giden elektronik posta
- E-posta sunucusu depolama kullanımında ani artış (bu, disk / kullanıcı bölümü alanını izlemek ve yönetmek için ayarlanan alarm eşiklerini tetikleyebilir)
- Uygun disk alanında açıklanamayan azalma
- Ortalama mesaj büyüklüğünde sıradışı bir artış ya da eklentilerin hacminde artış
- Kullanıcılar tarafından gönderilmemiş mesaj trafiğinin teslim edilmemesi için beklenmeyen SMTP veya POP3 bekletici cevapları (*deamon responses*)
- Ağ genelinde kullanıcı yanıt süresinde ani bir artış veya sunucu çiftlikleri yakınındaki tıkanma noktalarında ani tıkanıklık
- IDS veya güvenlik duvarı eşik değeri alarm aktivitelerinde ani artış.

NOT

Nimda bir başka solucan örneğidir. Bununla birlikte, birçok başka şekilde yayılabilir, bu nedenle bir e-posta virüsü ve bir çok bölmeli virüs olarak dikkate alabilirsiniz.

muhtemelen en başarılı ilk solucanlardan biriydi çünkü kullandığı işlev, DCOM, Windows'un tüm versiyonlarında -hem sunucu hem masaüstü- kullanılabiliyordu.

Bir solucan, herhangi bir kullanıcı hareketi olmadan hızla yayılabilir. Solucan genellikle sunucu yazılımına saldırır. Bunun nedeni, solucan yazan birçok kişinin sunucuların her zaman açık olduğunu bilmesidir. Bu, solucanın daha hızlı yayılmasını sağlar.

Truva Atları

Truva Atları (*trojans*), veya Truva Atı programları (*Trojan horse programs*), en büyük kötü amaçlı yazılım sınıfıdır. Truva atı, kötü niyetini gizlerken yararlı bir program gibi görünen herhangi bir programdır. Truva atının maskeleme niteliği, kullanıcıları programı indirmeye ve çalıştırmaya teşvik eder. Bir kod kırıcının (*cracker*) bakış açısından, bu yaklaşımın avantajı, Truva atının yetkili bir işlem olarak çalışmasıdır çünkü yetkili bir kişi çalıştırmaktadır. Truva atlarının başarısı, yayılmaları ve işletilmelerinin sosyal mühendisliğe bağlı olmasından kaynaklanmaktadır. Truva atı, kullanıcıları kendisini çalıştırmaları için kandırmak zorundadır. Eğer Truva atı faydalı bir program gibi gözükürse, daha çok çalıştırılma ve yayılma şansı vardır. Aslında, en başarılı Truva atları faydalı hizmetler sunarlar ve isteksiz kullanıcılar Truva Atını birçok kez çalıştırabilir. Bununla birlikte, Truva Atı her çalıştığında, diğer kötü amaçlı yazılım türlerinde olduğu gibi bazı istenmeyen eylemler de gerçekleştirir.

Birçok Truva atı e-posta mesajları veya web siteleri indirmeleri yoluyla yayılır. Geçtiğimiz yıllarda Trojan geliştiricileri, programları elektronik bülten tahtası sistemlerine ve dosya arşiv sitelerine gönderdi. Moderatörler ve kötü amaçlı yazılımdan koruma yazılımı kısa sürede kötü amaçlı programları belirleyecek ve ortadan kaldıracaktır. Daha yakın zamanlarda, Trojan programları toplu e-posta, web siteleri, sosyal ağ siteleri ve otomatik dağıtım aracıları (*bot*'lar) ile yayıldı. Trojan programları gizlenmiş olarak farklı şekillerde yayılabilirler. Trojan programlarının kötü niyetli içeriklerini belirlemek çok daha zor hale gelmiştir.

Bazı uzmanlar virüslerin sadece bir çeşit Truva atı programı olduğunu düşünmektedir. Bu görüşün biraz geçerliliği vardır. Bir virüs, yasal bir programa gizlenip onunla yayılan ne yapacağı bilinmeyen bir niceliktir. Ek olarak, herhangi bir programı bir virüs bulaştırarak Truva Atı'na

Truva Atlarının Belirtileri

Truva atları birçok belirti bırakırlar. Aşağıdakilerden herhangi biri, Truva atından etkilenmiş bir bilgisayarı gösterebilir:

- Çalışan tanınmayan yeni süreçler
- Yeni yazılımların yüklendiği (ya da yüklenmekte olduğunu) gösteren başlangıç mesajları
- Uygulamaların normal komutlara tepkisizliği,
- Normal web isteklerinin bilinmeyen sitelere olağan dışı yönlendirilmesi
- Beklenmeyen veya planlanmamış modem bağlantı etkinliği
- Olağandışı zamanlarda beklenmeyen uzaktan oturum açma veya tanıdık olmayan oturum açma bilgi istemi panelleri (bu, rutin yazılım yükseltmelerinden veya oturum sıfırlamalarından kaynaklanabilir ancak aynı zamanda Truva atı tuş kaydedici (Trojan key-logging) veya parola yakalama yazılımını da gösterebilir.
- Antivirüs tarama yazılımının veya kişisel güvenlik duvarı yazılımının ani veya beklenmedik şekilde sonlandırılması (başlangıçta veya kullanıcı yüklenmeye çalıştığında)

dönüştürebilirsiniz. Bununla birlikte, *virüs* terimi enfekte olmuş bilgisayardan daha çok bulaşıcı kod anlamına gelir. *Trojan* terimi, kendini üretmeyen kasıtlı olarak yanıltıcı veya değiştirilmiş bir program anlamına gelir.

Mantık Bombaları

Bir **mantık bombası (logic bomb)**, belirli koşulları tespit ettiğinde bir tür yazarlı yazılım fonksiyonunu çalıştıran bir programdır. Bir kez yürürlüğe girdiğinde, belirli koşul veya zamanı bekler. Belirtilen koşul veya zaman gerçekleştiğinde, mantık bombası aktif olur ve görevlerini yerine getirir. Kötü niyetli görevler anında hasara neden olabilir veya daha uzun bir süre boyunca hasara neden olan bir dizi olay başlatabilir.

Birçok mantık bombası organizasyon içinden kaynaklanmaktadır. Bir kurum içindeki insanlar genellikle BT altyapısı hakkında yabancıların bildiğinden daha fazla bilgiye sahip olduklarından, mantık bombalarını daha kolay yerleştirebilirler. Ayrıca, kurum personeli genellikle bir kuruluşun zayıf noktaları hakkında daha fazla şey bilir ve zarar vermenin daha etkili yollarını tanımlayabilir. Örneğin, bir programcı, uykuda olan diğer yazılımların içine bir programı gizleyebilir. Eğer şirket bu programcının istihdamını sonlandırırsa, programı aktive edebilir. Bu, mantık bombasının değerli dosyaları silmek veya başka şekilde zarar vermek gibi kötü niyetli faaliyetlerde bulunmasına neden olur.

Mantık bombalarını tanımlamak çok zor olabilir çünkü tasarımcı tespit edilmelerini engellemek üzere yaratır. Buna ek olarak, tasarımcı genellikle kuruluşun yetenekleri ve güvenlik kontrolleri hakkında bilgi sahibi olur ve daha az dikkat çekebilecekleri mantık bombaları yerleştirebilir.

Aktif İçerik Zafiyetleri

Aktif içerik (active content) terimi, öncelikle web sitelerinde, kullanıcılarla etkileşime geçme işlevselliği sağlayan bileşenleri ifade eder. Bu, kullanıcı web sayfasını açtığında bir şeyler yapan dinamik nesneleri içerir. Geliştiriciler, ActiveX, Basamaklı Stil Sayfaları (*Cascading Style Sheets* - CSS), React, Java, JavaScript, VBScript, makrolar, tarayıcı eklentileri, PDF dosyaları ve diğer komut dosyası dilleri dahil olmak üzere birçok teknolojiyi etkin içerik oluşturmak için kullanabilirler. Bu kod, kullanıcının tarayıcısı bağlamında çalışır ve kullanıcının oturum açma kimlik bilgilerini kullanır. Bu aktif içerik tehditleri mobil kod olarak kabul edilir, çünkü bu programlar çok çeşitli bilgisayar platformlarında çalışırlar.

Günümüzde pek çok internet sitesi, görünümlerini oluşturmak için aktif içeriğe güvenmektedir. Bu şemaların düzgün çalışması için kullanıcının sabit diske erişebilecek bu mobil kod parçalarını indirmesi gerekir. Etkinleştirildiklerinde, masaüstünüze virüslü dosya simgeleriyle doldurmak gibi şeyler yapabilirler. Bu simgeler kötü amaçlı kodun ek kopyalarını oluşturur.

Aktif içerik, uygulama makrolarından applet'lere ve arka plan komut dosyalarına kadar birçok türde gelir. Java, JavaScript, Visual Basic Komut Dosyası, ActiveX, CSS, React, makrolar, Adobe Acrobat dosyaları ve tarayıcı eklentileri, iyi tanımlanmış ve belgelenmiş etkin içerik özellikleri sayesinde kötü amaçlı yazılımlar içerebilir. Bütün bunlar kötü amaçlı yazılımın faydalanabileceği zayıf yönlere sahiptir.

Kötü Amaçlı Eklentiler

Web tarayıcıları daha güçlü hale geldikçe, yazılım geliştiriciler web tarayıcınızla birlikte çalışan daha fazla sayıda yardımcı program sağlarlar. Bu yardımcı programlar, **tarayıcı eklentileri (*browser add-ons*)**

olarak adlandırılırlar. Tarayıcı eklentileri, web tarayıcısını birçok yönden genişletebilir. Örneğin, tarayıcınıza haberler ve hava durumu uyarılarını entegre edebilirler. Bir tarayıcı eklentisi, bir web tarayıcısının işlevselliğine birçok yolla ekleme yapabilir. Maalesef, eklentiler güvenliği de azaltabilirler. Tüm eklentiler güvenilir değildir. Kötü amaçlı eklentiler, bir tür kötü amaçlı yazılım içeren tarayıcı eklentileridir. Kurulduktan sonra, birçok zararlı eylem gerçekleştirebilirler. Kendinizi kötü amaçlı eklentilerden korumanın en iyi yolu, yüklediğiniz eklentilere çok dikkat etmektir. Yalnızca güvendiğiniz kaynaklardan gelen tarayıcı eklentilerini yükleyin. Ayrıca, hangilerini kullandığınızı bildiğinizden emin olmak için yüklü olan eklentileri düzenli olarak kontrol etmelisiniz. Tanımadığınız herhangi bir eklenti bulursanız, kaldırın.

ÖNERİ

Herhangi bir tarayıcıdan kötü amaçlı eklentileri kaldırma hakkında daha fazla bilgi için *https://malwaretips.com/blogs/browser-toolbar-removal/* adresini ziyaret edin. Bu makale özellikle araç çubuklarının kaldırılmasını kapsar ancak web sitesinde kötü amaçlı yazılımlarla mücadele için faydalı birçok başka makale bulunmaktadır.

Enjeksiyon

Kötü amaçlı yazılım saldırıları gerçekleştirmek için birçok farklı teknik kullanır. Taşma tekniklerini zaten öğrendiniz. **Enjeksiyon teknikleri (*Injection techniques*)** de kötü amaçlı yazılım geliştirmede oldukça popülerdir. Kötü amaçlı bir yazılım başka bir yazılıma kasıtlı olarak geçersiz girdi sağladığında yapılan bir enjeksiyon işlemidir. Geçersiz girdi sağlamanın amacı, bir hata koşuluna ve bir saldırının gerçekleşmesine izin veren bazı durumlara neden olmaktır. Enjeksiyon zafiyetleri her zaman giriş verilerini doğru şekilde doğrulamamış olan yazılımdan kaynaklanır. En popüler enjeksiyon teknikleri şunlardır:

- **Siteler arası komut çalıştırma (Cross-site scripting - XSS):**—Bu teknik, saldırganların istemci tarafı komut dosyalarını, kullanıcıların görüntülediği web sayfalarına yerleştirmesini sağlar. Bir kullanıcı komut dosyalı bir web sayfasını görüntülediğinde, web tarayıcısı saldıran komut dosyasını çalıştırır. Bu komut dosyaları erişim kontrollerini atlamak için kullanılabilir. XSS etkileri, sitedeki verilerin ne kadar hassas olduğuna bağlı olarak önemli güvenlik riskleri oluşturabilir.
- **SQL enjeksiyonu** —Veritabanlarında saklanan verilere dayanan uygulamalara saldırmak için bir kod enkeksiyonu kullanılır. SQL ifadeleri bir giriş alanına eklenir ve uygulama tarafından yürütülür. SQL enjeksiyon saldırıları, saldırganların verileri açıklamalarını ve değiştirmelerini, veri bütünlüğünü ihlal etmelerini ve hatta verileri tahrip etmelerini ve veritabanı sunucusunu değiştirmelerini sağlar.
- **LDAP enjeksiyonu**—Bir başka enjeksiyon saldırısı, LDAP enjeksiyon saldırısı, kullanıcı girişine dayanarak LDAP oluşturan web sitelerini kendi çıkarı için kullanır. Girdiyi kontrol ederek temizlemeyen web uygulamaları, saldırganların LDAP ifadelerinin oluşturma biçimini değiştirmelerine olanak verir. Saldırgan tarafından değiştirilen LDAP deyimleri, komutu uygulayan bileşenle aynı izinlerle çalışır.
- **XML enjeksiyonu**—XML enjeksiyon saldırısı, XML uygulamasının ya da servisinin mantığını değiştirmek için kullanılan bir tekniktir. Bir XML mesajına XML içeriği enjekte etmek, bir uygulamanın mantığını değiştirebilir veya hatta bir XML belgesine kötü amaçlı içerik ekleyebilir.
- **Komut enjeksiyonu**—Bu tür bir saldırının amacı, bir ana bilgisayar işletim sisteminde komutları çalıştırmaktır. Hassas bir uygulama bu saldırının başarılı olmasını sağlar. Bu saldırılar, yalnızca bir uygulama doğrulanmamış kullanıcı girişini kabul ettiğinde ve girişi bir sistem kabuğuna geçirdiğinde mümkündür.

Herhangi bir enjeksiyon saldırısının temel amacı, saldırganın yetkisiz eylemler gerçekleştirmesine izin vermektir. Bu eylemler, verilere erişmek veya bunları değiştirmek ya da izinsiz çalıştırılmaması gereken kodları çalıştırmak olabilir. Bir bilgisayara veya aygıta başarıyla saldırma ve yetkisiz kod çalıştırma yeteneği, **isteğe bağlı kod çalıştırma (*arbitrary code execution*)** saldırısı veya **uzaktan kod yürütme (*remote code execution*)** saldırısı olarak adlandırılır.

Robot Ağlar (Botnets)

Saldırgan grupları saldırıları başlatmak için **robot ağları (*botnet*)** (robotik kontrollü ağların kısaltması) oluştururlar. Saldırganlar güvenlik açığı bulunan makinelere, bot-çobanı veya kontrol eden kişinin emrinde çeşitli işlevleri yerine getiren etmenleri bulaştırırlar. (Bir **bot-çobanı** bir robot ağ çalıştıran bilgisayar korsanıdır.) Genelde, kontrolörler İnternet Aktarmalı Sohbet (*Internet Relay Chat* - IRC) kanallarını kullanarak robot ağın diğer üyeleriyle iletişim kurarlar. IRC, internet üzerinden metin konuşmaları sağlayan bir protokoldür. Saldırganlar, kötü amaçlı yazılım ve spam dağıtmak ve kuruluşlara ve hatta ülkelere karşı DoS saldırıları başlatmak için robot ağları kullanabilir. Saldırganlar binlerce robot ağ kurmuşlardır ve bunlar sistemler için gerçek bir tehdittir. 2007 yılı boyunca, Storm robot ağı dünyanın en güçlü ikinci süper bilgisayarıydı. Robot ağlar o kadar güçlüdür ki günümüz saldırılarında çok önemli bir rol oynamaktadır. ABD bankalarına ve altyapılarına 2012 ve 2013 yıllarının sonunda tekrarlanan saldırıların başlatılması için robot ağlar kullanmıştır. Robot ağların oluşturduğu tehlike, her bilgisayar cihazının güvenliğinin sağlanmasının gerekliliğine dikkat çekmektedir. Saldırganlar, saldırıları başlatmak için her türden cihazı kullanabilir.

Hizmeti Engelleme Saldırıları

Hizmet reddi saldırısının (*Denial of Service* - DoS) amacı, bir sunucuyu ya da bir ağ kesimini kullanılamaz hale getirmektir. Başarılı bir DoS saldırısı bir sunucu veya ağ cihazını çökertir ya da yetkili kullanıcıların ağ kaynaklarına erişemeyeceği kadar çok ağ tıkanıklığı yaratır.

Standart DoS saldırıları, saldırıyı başlatmak için tek bir bilgisayar kullanır. Dağıtık hizmet engelleme (*Distributed DoS* -DDoS) saldırısı, saldırıyı gerçekleştirmek için aracı bilgisayarlar kullanır. Bu aracılar, Truva işleyici programları içeren tehlikeye girmiş sistemlerdir. Bu Truva programları daha sonra bir hedef sistem veya ağda koordineli bir saldırı gerçekleştirmek için aracılar olarak görev yaparlar. Saldırgan(lar), her biri birçok ajanı veya geri planda çalışan programları kontrol edebilen bir veya daha fazla ana işleyici sunucusunu kontrol eder. Ajanlar, bir veya daha fazla mağdur sisteme karşı paket tabanlı bir saldırıyı koordine etmek için talimatlar alırlar.

BİLGİNİZE

Robot ağlar, dağıtık hizmet reddi (DDoS) saldırıları ve istenmeyen e-postaların ana kaynağıdır. Bunlar, güvenli bilgisayarlara gizlenen ve "uyanmak" ve bazı talimatlar almak için bir komut bekleyen programlardır. Botlar saf dışı bırakılmaya karşı oldukça dirençlidir ve pek çok farklı bilgisayarda bulunduğundan algılanması zor olabilir. Robot ağ DoS saldırıları o kadar hızlı büyüyor ve yayılıyor ki, onları tanımlamaya çalışan yazarlar yetişemiyorlar. Antivirüs yazılımı, kişisel güvenlik duvarları ve kişisel IDS tedarikçisi olan F-Secure, YouTube'da *www.youtube.com/fslabs* adresinde bir dizi video ve güncelleme sunmaktadır.

Eylül ve Ekim 2012'de ve yine Şubat 2013'ten başlayarak, hack yetenekleri olan bir grup eylemci, **politik amaçlı bilgisayar korsanları (*hactivist*)** deniliyor, birkaç büyük ABD banka bilgisayar sistemine karşı bir dizi DDoS saldırısı başlattı. Tipik olarak, saldırıya uğrayan sitelerin bazı müşterileri, yavaş web siteleri nedeniyle büyük olasılıkla sinirlenebilir; diğerleri sitelere hiç erişemeyebilir. Ekim 2012'de ABD bankalarına yönelik saldırıları başlatan aynı korsan eylemciler, Aralık 2012 ve 2013'te de aynı bankaların çoğuna karşı yeni bir saldırı turu başlattılar. Saldırılar, tekrar, banka web sitelerine çevrimiçi erişimi kesintiye uğrattı ancak önceki saldırılar kadar başarılı değildi. Bankalar daha önceki saldırılardan tecrübe edinmiş ve web sitelerini korumak için yeni kontroller eklemişti.

2015 ve 2016 başlarında, bilgisayar korsanları, İslami Irak ve Suriye Devleti'ne (ISIS) ve hatta ABD başkan adayına karşı büyük çaplı başarılı saldırılar başlattılar. Hacktivistler, genel niyeti bazı siyasi veya sosyal konulara dikkat çekmek olan daha fazla sayıda geniş çaplı saldırılar düzenlemişlerdir.

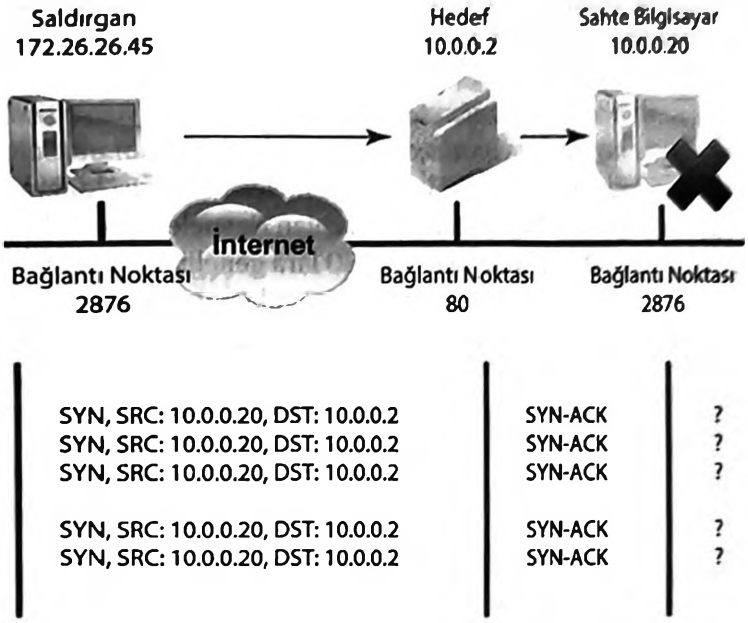
Bu saldırılarda üç taraf vardır: Saldırgan, aracı kurumlar (eylemciler ve ajanlar) ve mağdur(-lar). Aracı hedeflenen kurban olmasa da, aracı mağdurun maruz kaldığı sorunlara maruz kalabilir. DDoS saldırıları ile ilgili daha fazla bilgiyi *www.cert.org* adresindeki CERT web sitesinden bulabilirsiniz.

SYN Taşkını Saldırıları

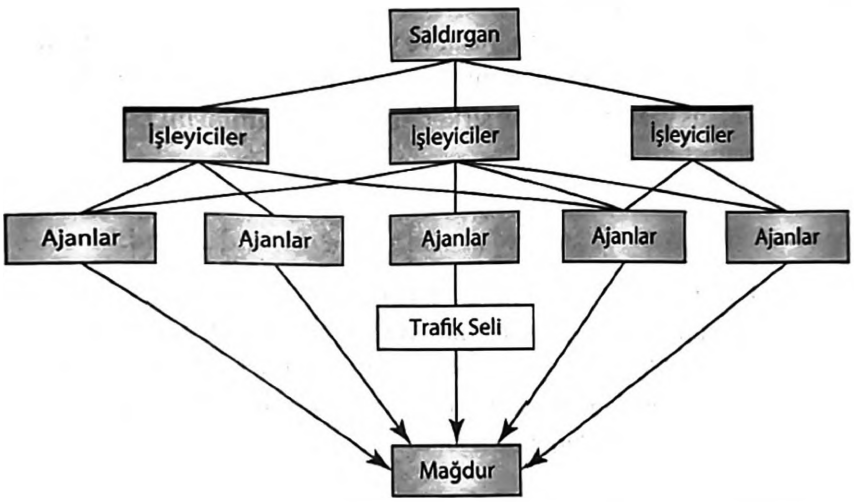
DoS saldırıları için popüler bir teknik **SYN taşkını saldırısında (*SYN Flood attack*)** olarak adlandırılır. Bir SYN taşkını saldırısında, saldırgan, mağdur bilgisayara bağlantı talebinde bulunan çok sayıda paketi yollamak için IP yanıltması (IP spoofing) kullanır. Bu istekler yasal görünmektedir ancak aslında, bağlantı kurma sürecinde belirli bir ağ mesajına cevap veremeyen bir istemci sistemine atıfta bulunmaktadır. Mağdur bilgisayar, her bağlantı isteğini kaydeder ve her bağlantı için hafızadaki yerel tablosunda bir yer ayırır. Mağdur bilgisayar daha sonra saldırgana, SYS-ACK mesajı adı verilen bir geribildirim yollar. Normal olarak, istemcinin SYS-ACK mesajına cevap vererek bağlantı kurulumunu tamamlaması bitirmesi gerekir. Ancak, saldırgan IP yanıltması yaptığı için, SYS-ACK mesajı hedef gösterilen sisteme gider. Sonuç, istemci hiçbir zaman ACK mesajını yollamaz. Mağdur bilgisayar, daha sonra tüm istekler için ACK mesajlarını bekleyerek bağlantı tablosunu doldurur. Bu arada, SYN taşkını saldırısı bilgisayarın bağlantı tablosunu doldurduğundan, hiçbir yasal kullanıcı mağdur bilgisayara bağlanamaz. Mağdur bilgisayar, bağlantı talepleri zaman aşımına uğrayana kadar kullanılamaz durumda kalacaktır. O zaman bile, saldırı sistemi, mağdur sistemin zaman aşımına uğramış bağlantıları sonlandırabileceğinden daha hızlı şekilde yeni bağlantılar talep ediyor olabilir. **ŞEKİL 11-11** bir SYS saldırısının nasıl çalıştığını göstermektedir.

Smurf Saldırıları

Bir **smurf saldırısında (*smurf attack*)**, saldırganlar DoS saldırıları oluşturmak için, uzak konumlardan sahte İnternet Kontrol Mesaj Protokolü (*Internet Control Message Protocol* - ICMP) yankı istek paketlerini IP yayın adreslerine yönlendirirler. Bu saldırılarda üç taraf vardır: Saldırgan, aracı ve mağdur. (Ayrıca aracının da mağdur olabileceğini unutmayın.) Aracı, kendi ağının IP yayın adresine yollanan bir ICMP yankı istek paketini alır. Eğer aracı IP yayın adresine yönlendirilen ICMP trafiğini filtrelemez ise, ağdaki makinelerin çoğu bu ICMP yankı istek paketini alır ve bir ICMP yankı cevap paketi geri yollar. Ağdaki tüm makineler (potansiyel olarak) bu ICMP yankı talebine cevap verdiğinde, sonuç ciddi ağ tıkanıklığı veya kesintileri olabilir. **ŞEKİL 11-12** smurf saldırısının nasıl çalıştığını göstermektedir.



ŞEKİL 11-11
SYS saldırısının çalışması



ŞEKİL 11-12
Smurf saldırısının çalışması

Casus Yazılım

Casus yazılım (*spyware*), kendisini kullanıcının bilgisayarına yükleyen, kullanıcının gezinme alışkanlıkları ve web sitesi etkinlikleri hakkında bilgi toplayan istenmeyen bir arka plan işlemidir. Bu programlar genellikle mahremiyet (*privacy*) ve gizliliği (*confidentiality*) etkiler. Kullanıcılar genellikle ücretsiz programlar yüklediklerinde yüklenirler.

Çerez (*cookie*), bir tarayıcı oturumu hakkında bilgi depolayan küçük bir metin dosyasıdır. Bir web sunucusuna olan bir kullanıcı bağlantısının sunucu tarafı, çerezlere belirli bilgileri yerleştirebilir ve ardından bu çerezi kullanıcının tarayıcısına aktarabilir. Daha sonra aynı sunucu, tarayıcıdan çerez isteyebilir ve daha önce tarayıcının sakladığı bilgileri alabilir. Bu, tarayıcı ile web sitesi arasındaki herhangi bir akıllı etkileşimde işe yarar, çünkü tarayıcı talepler arasında sunucuyla bağlantı kurmaz.

Casus yazılım çerezleri, siteler arasında bilgi paylaşan çerezlerdir. Bazı çerezler kalıcıdır ve izniniz olmadan süresiz olarak sabit diskinizde saklanır. Birden fazla siteden toplanan özel bilgileri açığa çıkarabilirler ve paylaşabilirler. Casus yazılım çerezleri, *247media, admonitor, adforce, doubleclick, engage, jlycast, sexhound, sextracker, sexlist* ve *valueclick* gibi ifadeleri içeren metinleri isimlerinde içerirler. Adobe Flash, web sitelerinin çerez kullanmasına benzer şekilde Yerel Olarak Paylaşılan Nesneleri (*Locally Shared Objects* - LSO) kullanır. Aslında, LSO'lara genellikle *Flash çerezleri (Flash cookies)* denir. LSO'lar, Flash uygulamaları kullanan web siteleri için küçük miktarda veri depolar. Bu LSO'lar, saldırganlar tarafından hassas kullanıcı verilerini depolamak ve ifşa etmek için kullanılabilir. Son yıllarda, Flash pek çok güvenlik açığı nedeniyle birçok saldırıda kullanılmıştır.

NOT

Çerezler ve e-posta ekleri, saldırganların kötü amaçlı yazılım yaymak için kullandıkları en yaygın tekniklerdir. Çerezleri kabul eden veya ekleri açan kullanıcılar, saldırganların bilgisayarlara veya mobil cihazlara kötü amaçlı yazılım yerleştirmesi için en kolay yolu sağlarlar.

Reklam Yazılımı

Reklam yazılımları (*adware*), belirli web sitelerini ziyaret ettiğinizde, açılır pencere reklamları ve afişler (*banner*) gibi sıkıntıları tetikler. Üretkenliği etkilerler ve ana sayfa ele geçirme kodu gibi etkin arka plan etkinlikleriyle birleştirilebilirler. Buna ek olarak reklam yazılımı uygulama, web sitesi ve internet etkinliği hakkında bilgi toplar ve izler.

Casus yazılım ve reklam yazılımıyla ilgili sorun, yasal ve yasadışı faaliyetler arasında ayrım yapmaktan kaynaklanır. Casus yazılım ve reklam yazılımı şirketleri, bu belirsiz durumdan tam anlamıyla yararlanmış, genellikle casus yazılım önleme şirketlerine programlarını casus yazılım olarak etiketleme konusunda dava açmıştır.

Oltalama

Oltalama (*phishing*) saldırısı, kullanıcıların, yasal olarak görünen bir web sitesine oturum açma bilgileri sağlamasına neden olur, ancak web sitesi aslında bu bilgiyi elde etmek için bir saldırgan tarafından oluşturulan bir web sitesidir. Saldırgan, örneğin finansal kurumlar için oturum açma bilgisini elde edebilirse, saldırgan mağdurdan çalabilir. Saldırganlar bu tür sitelerin yasal görünmesini sağlamak için çok karmaşık teknolojiler kullanır.

Hedef Odaklı Oltalama (Spear-Phishing)

Kimlik avı saldırısının başarı oranını artırmak için, bazı saldırganlar yasal şirketten gelen mağdur hakkında bilgi sağlar. Bu bilgiler, tahmin etme, çöpten ayıklama ("Çöp karıştırma", "Dumpster diving") veya sahte anketler gönderme de dahil olmak üzere birçok şekilde elde edilebilir.

Site Trafiğinin Yasal Olmayan bir Siteye Yönlendirilmesi

Site trafiğinin yasal olmayan bir siteye yönlendirilmesi (*pharming*) terimi, kullanıcı adı ve parolalar gibi erişim bilgilerini elde etmek için sosyal mühendislik kullanımını ifade eden *phishing* teriminden kaynaklanmaktadır. Site trafiğinin yasal olmayan bir siteye yönlendirilmesi, Alan Adı Sistemi (*Domain Name System* - DNS) sunucusu yazılımındaki bir güvenlik açığından yararlanarak gerçekleştirilebilir. DNS sunucuları, internet alan adlarının gerçek IP adreslerine çözümlenmesinden sorumlu makinelerdir. DNS sunucusu yazılımındaki güvenlik açığı bir saldırganın bir sitenin alan adını almasına ve (örneğin) o web sitesinin trafiğini başka bir web sitesine yönlendirmeyi sağlamasına olanak tanır.

Eğer trafiği alan web sitesi, bir bankanın web sitesinin bir kopyası gibi sahte bir web sitesi ise, bir bilgisayarın kullanıcı şifresini, PIN kodu veya hesap numarasını avlamak veya çalmak için kullanılabilir. Örneğin, Ocak 2005'te bir saldırgan, büyük bir New York İnternet Servis Sağlayıcısı (*Internet Service Provider* - ISP) Panix'in alan adını Avustralya'daki bir siteye yönlendirdi. Diğer tanınmış şirketler de bu saldırının kurbanı oldu. (Bunun yalnızca orijinal sitenin SSL korumalı olmadığı veya kullanıcı geçersiz sunucu sertifikalarıyla ilgili uyarıları yoksaydığı durumlarda mümkün olduğunu unutmayın.)

Tuş vuruşu kaydedicileri

Tuş vuruşu kaydedicileri (***keystroke loggers***) bir saldırganın elinde sinsi ve tehlikeli araçlardır. Yazılım veya donanım tabanlı bir tuş vuruşu kaydedicisi, tuş vuruşlarını veya kullanıcı girişlerini yakalar. Tuş vuruşu kaydedicisi daha sonra bu bilgiyi saldırgana iletir. Bu, saldırganın oturum açma bilgilerini, bankacılık bilgilerini ve diğer hassas verileri yakalamasını sağlar.

Tuş vuruşu kaydedicileriyle mücadele etmek için bazı insanlar ekran klavyelerine döndüler. Yanıt olarak, siyah şapkalı bilgisayar korsanları (*black-hat hackers*), fare ile tıklanan alan çevresindeki anlık ekran görüntüsünü alarak kötü amaçlı yazılımları dağıtmaya başladı. Böylece güvenlik ve bilgisayar korsanları arasındaki savaş her iki tarafın da yeni tehditler ve yeni çözümler geliştirmeye devam etmesiyle sürmektedir.

Aldatmacalar ve Efsaneler

Virüs aldatmacaları *(virus hoaxes)* her zaman kötü amaçlı olmamasına rağmen, doğrulanmamış uyarıların ve sahte yamaların yayılması yeni güvenlik açıklarına neden olabilir. Genellikle, aldatmaca *(hoax)* veya efsanenin *(myth)* yaratıcısının amacı, sadece hilenin ne kadar geniş ölçüde yayılabileceğini gözlemlemektir. Bu eski zincirleme mektup saldırısının (*chain-letter attack*) yeni bir sürümüdür; saldırgan, bir kişiye eğer mesajı bir düzine insana iletirse, o kişiye iyi şanslar veya mutluluk vaat eden bir mektup gönderir.

Aldatmacaları, özellikle de virüs aldatmacalarını tanımaya yönelik bazı yönergeler:

- **Uyarıyı yasal bir bileşen mi (bilgisayar güvenlik uzmanı, satıcısı vb.) gönderdi?** —Uyarıyı gönderenin, doğrulama sertifikasını ya da en azından internet kaynak adresini (*Uniform Resource Locator* - URL) kontrol edin.
- **Uyarıyı başkalarına iletme isteği var mı?**—Hiçbir yasal güvenlik uyarısı, alıcının uyarı göndereni (*advisory*) iletmesini önermez.
- **Uyarıda ayrıntılı açıklamalar veya teknik terminoloji var mı?**—Aldatmacalar genellikle alıcıyı, uyarının yasal olduğuna inandırmak ve korkutmak için teknoloji kullanırlar. Bununla birlikte, yasal bir tavsiye tipik olarak herhangi bir ayrıntıyı atlamaz. Sadece alıcıyı detaylar için yasal bir web sitesine yönlendirir. Web sitesi ayrıca koruma etkinlikleri için genellikle öneri sunar.
- **Uyarı, bir mektup zincirinin genel biçimini takip ediyor mu?**—Bu formatta bir kanca (*hook*), bir tehdit ve bir istek vardır. Kanca, alıcının dikkatini çekmek için akılda kalıcı veya etkileyici bir açılış veya konudur. Tehdit, ciddi güvenlik açıkları veya hasarlar hakkında teknik bir uyarıdır. İstek, örneğin bağlantılı bir websitesinden bir yamanın indirilmesi gibi, acil bir eylemde bulunulması için öneri veya bir uyarının dağıtılması yönünde bir ricadır.

Anasayfa Ele geçirme

Bu saldırıların işlevi, tarayıcınızın ana sayfasını saldırganın sitesine işaret edecek şekilde değiştirmektir. Ele geçirmenin iki şekli var:

- **Anasayfayı sıfırlamak için tarayıcının güvenlik açığından yararlanmak**—Birçok aktif içerik türü, kullanıcı izni olmadan tarayıcının anasayfasını değiştirebilir. Gizli yollara başvurmadan bile, kullanıcıyı beklediğinden daha fazlasını yapan bir eylem seçmeye ikna etmek kolaydır. Sırf "Etkilenen Programları Bilgisayarımdan Kaldır" yazan bir düğmeyi tıklatmanız, sadece bu eylemin gerçekleşeceği anlamına gelmez.
- **Gizlice bir tarayıcı yardımcı nesnesi (Browser Helper Object - BHO) Truva atı programı yüklemek**—Truva atı, ele geçirme kodu içerir. BHO çalıştırıldığında, tarayıcının anasayfasını korsanın istediği siteye çevirebilir. Genellikle bilgisayar korsanlığı programları, işletim sisteminin başlatma yordamlarına kendilerine bir referans koyarlar. Bu şekilde, bilgisayar her yeniden başlatıldığında, kendilerini yeniden çalıştırır. Bu ayarlardan herhangi birini değiştirmeyi denediğinizde, siz korsanlık yazılımını bulup kaldırana kadar, program bunları sürekli değiştirir.

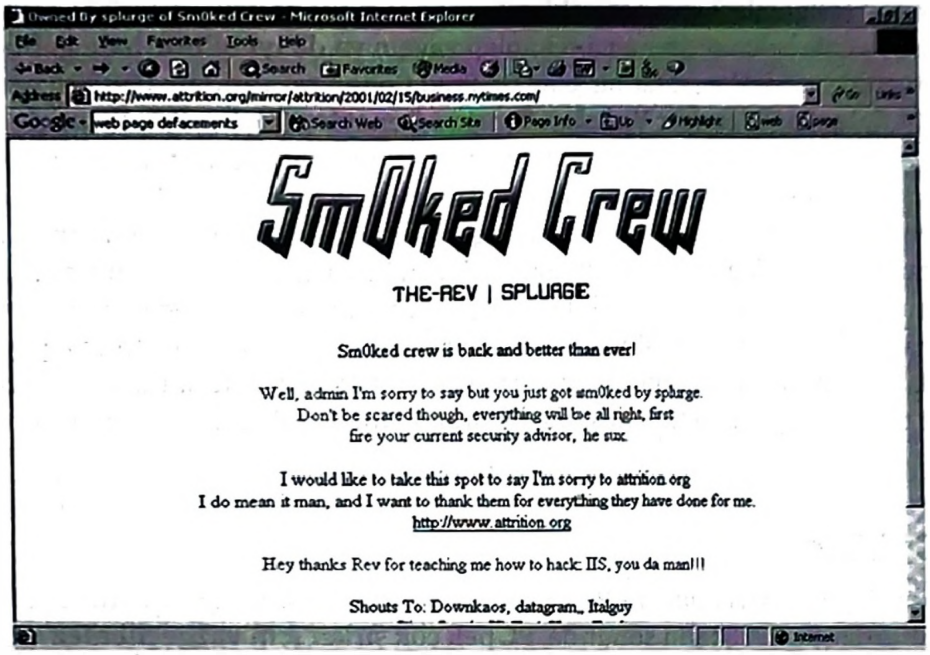
Websayfası İçeriğinin Bozulması

Web sayfası içeriğinin bozulması (web defacement) veya **web grafiti (web graffiti)** terimi, bir kişinin bir web sunucusuna yetkisiz erişime sahip olması ve sunucudaki bir sitenin ana sayfasını değiştirmesi anlamına gelir. Genellikle saldırgan, hedef sunucudaki bilinen güvenlik açıklarından yararlanır ve yönetimsel erişim kazanır. Kontrol altına alındıktan sonra, saldırgan sitedeki orijinal sayfaları değiştirilmiş sürümlerle değiştirir. Örneğin, **ŞEKİL 11-13,** bozulmuş *New York Times* web sayfasını gösterir.

Tipik olarak, içeriği bozmak grafitiyi temsil eder. Güvenlik uygulayıcılarının çoğu, bu saldırı biçimini sadece bir sıkıntı olarak görmektedir. Ancak, web sitesine virüs veya Truva atı gibi zararlı aktif içerik kodunu yerleştirme potansiyeli mevcuttur. Örneğin, Kırmızı Kod, arka kapı Truva atını kuran

Saldırganlar Web Uygulamalarına Nasıl Saldırabilir?

Bir web tarayıcısını kullanarak kullanıcıların eriştiği uygulamalara **web uygulamaları (web applications)** denir. Çoğu insan web uygulamalarını web siteleri olarak düşünür ancak gerçekte bir web sayfasından çok daha güçlüdür. Bir web uygulaması genellikle bir veritabanındaki verilere erişim sağlar ve bu verileri kullanıcıya bazı servisleri sağlamak için kullanır. Örneğin, çevrimiçi alışveriş siteleri gerçekten web uygulamalarıdır. Saldırganlar sık sık web uygulamalarını hedeflemektedir çünkü uygulama çok miktarda verilere erişim sağlamaktadır. Saldırganların kullandığı yöntemlerden biri **oturumu ele geçirme (session hijacking)** olarak adlandırılmaktadır. Oturumu ele geçirme, saldırganın bir web sunucusu ile web tarayıcısı arasındaki ağ mesajlarını yakaladığı bir saldırıdır. Genellikle bir ya da daha fazla veriyi, genellikle oturum kimliği **(session ID)**, ayıklar ve bunu web sunucusuyla iletişim kurmak için kullanır. Saldırgan, yetkili kullanıcının oturumunu devralarak yetkili bir kullanıcı gibi görünür. Saldırganın yetkili bir kullanıcı olarak maskelenme yaparken kullandığı tekniğe **başlık manipülasyonu (header manipulation)** denir. Saldırgan, web sunucusu için bir HTTP mesajı oluşturur ancak ele geçirilen oturum kimliğini içerecek şekilde HTTP başlığını değiştirir. Web sunucusu değiştirilmiş HTTP mesajını aldığında, saldırganın yetkili bir kullanıcı olduğunu düşünür. Bu, her isteğin kimliğini doğrulayamayan web uygulamaları için etkili bir saldırıdır.



ŞEKİL 11-13
Görüntüsü bozulmuş *New York Times* web sayfası

Kaynak: zdnet.com

BİLGİNİZE

Arka kapı programları genellikle bilgisayar virüslerinden daha tehlikelidir. Bunun nedeni davetsiz misafirlerin bir bilgisayarı kontrol etmek ve potansiyel olarak ağ erişimi elde etmek için bunları kullanabilmeleridir. Bu programlara genellikle *Truva atları* da denir çünkü gerçekte yaptıklarından başka bir şey yapmış gibi davranırlar. Arka kapı programları tipik olarak masum görünümlü dosya adlarına sahip e-postalara ek olarak gelir.

bir yük içeriyordu. Bu Truva atı, saldırganların web sunucusunun ön sayfasını engellemek için kullanabileceği virüslü bir IIS sunucusuna uzaktan erişime izin verdi. Bu tür saldırı riskini, güncel yazılım sürümlerini ve güvenlik yamalarını yüklediğinizden emin olarak, en aza indirebilirsiniz.

Zararlı Kod Tehditlerinin Kısa Bir Tarihçesi

Bilgisayarlı hesaplamanın ilk zamanlarında, kötü amaçlı yazılımlar kişiden kişiye verilen disketler aracılığıyla bilgisayardan bilgisayara yayılmıştır. Bu manuel yayılma metoduna *sneakernet* adı verilmiştir. Sneakernet ile bir virüsün dünya boyunca yayılması aylarca sürebilirdi. Buna karşın, günümüzün viral enfeksiyonları ağlar aracılığı ile yayılıyor ve dünyayı saniyeler içerisinde dolaşabiliyor. Virüs yazanlar topluluğu evrildikçe, gitgide daha karmaşık virüsler ortaya çıkmaya başlamıştır. Bazıları e-posta, mobil kod ya da makrolar aracılığı ile yayılabilirken, diğerleri birden fazla yolla yayılabilir.

1970'ler ve Erken 1980'ler: Akademik Araştırma ve UNIX

Kendini çoğaltan bilgisayar programları fikri onyıllardır bilinmektedir. Bu fikir erken 1970'lerden beri literatürde, bilimsel yayınlarda ve hatta deneylerde yer almaktadır. Araştırmacılar

kendini dağıtan kodlar (solucanlar) kullanarak büyük ağlarda rutin bakım görevleri gerçekleştirmek için erken girişimlerde bulunmuştur ama teknoloji yaygın ya da iyi bilinir hale gelmemiştir.

Düşmanca kod geliştirimindeki anahtar bir olay Dr. Fred Cohen tarafından 1983'te gerçekleştirilen araştırmadır. Cohen'in "Bilgisayar Virüsleri-Teori ve Deneyler (*Computer Viruses—Theory and Experiments*)" başlıklı bildirisi 1984'te yayınlanmış, bilgisayar virüsünü tanımlamış ve kendisinin ve diğerlerinin viral kodun yaşama kabiliyetini kanıtlamak için gerçekleştirdiği deneyleri açıklamıştır. Cohen çalışmasını ilk bilgisayar virüsleri gözlemlenmeden önce yayınlamıştır.

Bu dönemde internet, öncelikle üniversite bilgisayarlarını birbirine bağlayan bir ağdı. Bu ağ mevcut iletişim protokolleri kullanılarak yayılabilecek programların verebileceği zararlara açıktı. İlk büyük kötü amaçlı yazılım olayı olan Morris Solucanı'nı Kasım 1988'de yaratan ve yayan Robert Morris adındaki bir üniversite öğrencisi, bu fikri uygulamıştır. UNIX tabanlı bu solucan internetteki neredeyse tüm bilgisayarları etkilemiş, büyük oranda medya ilgisine ve pek çok manşete sebep olmuştur.

1980'ler: İlk PC Virüsleri

İlk kişisel bilgisayarlar (*personal computer* - PC) 1980'lerin başında piyasaya sürülmüştür. PC'lerin popülerliği hızlı artmıştır. 1980'lerin sonunda, PC pek çok şirket için vazgeçilemez ve satın alınabilir bir iş teknolojisiydi. Bu hızlı büyüme ayrıca, bilgisayar teknolojisini daha fazla sayıda bireye yakınlaştırmıştır.

PC işletim sistemi disk-tabanlıydı (DOS) ve çoğu yazılım ve veri dosyası disketler aracılığıyla PC'ler arasında taşınmaktaydı. Zararlı virüs kodlarının iki temel türü bu gerçeği kendi yararına kullanmıştır: Önyükleme sektörü virüsleri (*boot sector viruses*), disklerde ve bellekte bulunan işletim sistemi bileşenlerine saldırmaktadır ve dosya virüsleri (*file infector viruses*) ise çalıştırılabilir dosyalara kendileri saldırıda bulunmaktadır.

Brain (bir önyükleme sektörü virüsü), Lehigh ve Jerusalem (bir dosya virüsü) ilk virüslere örnek verilebilir. Bu virüsler öncelikli olarak disketler ve popüler bilgisayar bülten tahtaları (*bulletin board*-BBS) arşivlerinden yapılan yüklemeler aracılığı ile yayılmıştır. Diğer ilk virüslerden Elk Cloner, Apple bilgisayarlarını hedef almış ve disketler aracılığı ile yayılmıştır.

1990'lar: İlk LAN Virüsleri

Yerel alan ağları (*Local Area Networks* - LANs) 1990'ların başında iş ortamlarında yer almaya başlamıştır. Bu gelişme geleneksel dosya virüslerine yayılmaları için üretken bir ortam sağlamıştır. Bu dönemde çok az sayıda insan virüs problemini anlamıştır ve bir virüs bulmak nadir bir olaydır. İlgili kullanıcılar buldukları örnekleri toplamışlar ve bunları serbestçe dağıtarak, ünlü virüs değişim bülten tahtalarının doğmasını sağlamıştır. Bazı virüsler hasara neden olmuştur ve iş kullanıcıları problemin farkına varmaya başlamıştır. Yükleme sektörü virüsü Form5 bu dönemde en yaygın virüs olmuştur. Bu dönemin diğer iyi bilinen virüsü Eddie6 olarak da bilinen Dark Avenger'dır. Bu çok yıkıcı bir virüstü.

Bu on yılın sonunda, yerel alan ağları çoğu şirkette anahtar bir altyapı olmuştu. Aynı zamanda, internetin iletişim için kullanımı -özellikle e-posta ve veri dosyası transferi- yaygınlaşmıştı. CD-ROM'ların ortaya çıkması ile depolama teknolojisi geliştikçe, geleneksel yükleme sektörü ve dosya bozucu virüslerin görülme sıklığı azalmaya başlamıştı.

1990'ların Ortası: Akıllı Uygulamalar ve İnternet

E-postanın popülerliği, dosya eklemenin kolaylığı ile birleşerek, yıllar önce Morris tarafından uygulanan aynı teknikler kullanılarak zararlı kodların aşırı yaygın dağıtımına fırsat vermiştir: E-posta solucanları. Bu programlar bir kullanıcının sistemindeki e-posta adres dosyalarını konumlandırmakta ve genellikle masum görünen dosya ekleri olarak kılık değiştirerek kendilerinin çok sayıda kopyasını üretmektedir. Melissa ve Loveletter adlarındaki iyi bilinen e-posta solucanları bunlara örnektir. Bu ilk dönem programlarının çoğunun kullanıcıların ekleri açarak kodu etkinleştirmesini gerektirmesine karşın, solucanların daha yeni biçimleri gittikçe sayıları artan sürekli açık bilgisayarların ve sunucuların çeşitli güvenlik zayıflıklarını kullanmışlardır. Örneğin, Code Red, Microsoft web sunucularındaki (IIS) zaafiyetlerden faydalanmıştır ve çok üst düzeyde kendini kopyalama hızına sahiptir.

İnternet bireylerin ve grupların etkinliklerini fonksiyonel ve coğrafi sınırların ötesine genişletebilecekleri bir ortam sağlamaktadır. 1990'ların ortalarında, bilgisayar korsanlığı (ya da kod kırıcılığı-cracking) büyüyen bir iş güvenlik kaygısı olmuştur. Otomatik araçlar ve daha yapısal yaklaşımlar kullanarak, bu birey ve gruplar evrilmeye devam etmiştir. İnternet iletişim protokollerinin özünde olan esnekliği (*resiliency*) normal işlemleri bozmak için bir yol haline gelmiş ve popüler web sitelerine karşı DoS saldırılarına yol açmıştır.

Back Orifice ve AIDS gibi Truva atı programlarını içeren yeni zararlı kod biçimleri 1990'larda evrilmiştir. Tequila gibi çok biçimli sürümleri içeren virüs kodlarının daha esnek ve gizli başka biçimleri de evrilmiştir. Ek olarak, taşınabilirlik ve işlevsellik için tasarlanan yeni programlama dilleri ek zararlı kod biçimleri geliştirmek için yeni fırsatlar sundu. StrangeBrew Java dosyalarını etkileyen ilk virüstü. Zararsız olmakla birlikte, virüs CLASS dosyalarını kendisinin bir kopyasını içerecek şekilde değiştirmekteydi.

Popüler uygulama yazılımlarına gelişmiş programlama özelliklerinin eklenmesi ile birlikte, diğer zararlı kod biçimlerinin artışı doküman dosyalarını da bozmaya başladı. İlk makro virüsü, WM/Concept7, Ağustos 1995'te keşfedildi. Bu virüs basit bir doküman dosyasının iletimi aracılığıyla yayıldı.

2000'lerden Günümüze

Bu yeni yüzyılda kişisel ve şirket internet bağlantısallığı artmaya devam ettikçe, popüler tarayıcı teknolojilerinin yazarları sayısız eşlik edici araçlar ve eklentiler (*plugins*) eklediler. Bu araçlar ortak işlevleri otomatikleştirebilen özelleşmiş komut dosyası (*scripting*) kodları kullanmaktadır. Bunlar saldırganlara ek fırsatlar yaratan bir aktif içerik kodu nesli içermektedir.

İnternete bağlı olan bilgisayar ve cihaz sayısı, özellikle Windows ve diğer yaygın dağıtık yazılımları çalıştıran popüler sunucu platformları, yeni güvenlik zafiyetleri oluşturmuştur. İnternet solucanlarının kendini kopyalama hızı günümüzün yüksek hızlı bilgisayarları ile birleştiğinde ve aynı zamanda güvenlik açıkları için saldırgan gruplar tarafından etkileşimli yoklamaların (*probing*) artışı, işletmeler ve kullanıcı toplulukları tarafından BT güvenliğinin sürekli iyileştirilmesini, izlenmesini ve sınanmasını zorunlu kılmaktadır.

Code Red solucanı tarafından bırakılan arka kapılardan faydalanan W32/Nimda solucanı, e-posta, ağ paylaşımları ve bir bozulan web sayfası gibi çeşitli yöntemlerle kendisini yayma konusunda ilkti. Bu solucan arka kapılar için tarama yaparak istemciden web sunucusuna yayılmaktadır. Klezworm, orjinal dosyanın gizli bir kopyasını oluşturarak ve orjinal dosyayı kendisi ile yeniden yazarak çalıştırılabilir dosyaları bozmaktadır.

En son iletişim devrimi 2007'de iPhone'un ve 2008'de Android akıllı telefonunun tanıtılması ile başlamıştır. Bu ürünlerin mevcudiyeti mobil iletişimle ilgili tüketici algısında bir değişim başlattı. Mobil cihazlar daha güçlü ve daha yaygın hale geldiler. Günümüzde masaüstü bilgisayarları kullananlardan daha fazla insan mobil cihazları kullanmaktadır. Bu cihazlar bollaşmış ve neredeyse günlük hayat için zorunlu hale gelmiştir. Saldırganlar kullanıcıların mobil cihazlarda saklanan ve işlenen bilgilere ne kadar bel bağladıklarını bilmektedir. Aynı zamanda kullanıcıların çoğunun mobil cihazlarını güvenli hale getirmeyi ihmal ettiklerini de bilmektedir. Artan sayıdaki zarar görmeye açık hedefler nedeniyle, pek çok yeni zararlı kod saldırganı geleneksel bilgisayarlardansa mobil cihazları hedef almaktadır ve gittikçe daha fazla aletin ve diğer cihaz türlerinin internete bağlı olmasıyla, zararlı kodlarla ilgili problem daha da kötüleşmektedir. Saatler, buzdolapları, arabalar ve diğer cihaz türlerinin binlercesinin internete bağlanması ile birlikte, saldırganlar saldırmak için çok daha fazla fırsat görmektedir.

Ticari İşletmelere Olan Tehditler

Zararlı kodlardan gelen güvenlik tehditleri çeşitli kaynaklardan doğabilmektedir. Bunlar, bir suçlu içeren karmaşık olmayan izole durumlardan, organize gruplar tarafından pek çok hedefe yönelik yapılan karmaşık, yapısal saldırılara kadar değişebilir. Bu tehditler genellikle bir kuruluşun BT altyapısının ve kullanıcı topluluğunun dışından kaynaklanmaktadır. Bu nedenle, kuruluşlar bu saldırıları belirlemek, saldırılara tepki vermek, saldırıları azaltmak ve saldırı sonrası eski haline gelmek için kayda değer bir çaba sarfetmektedir.

Bir kuruluşun içinden kaynaklanan tehditler kamuoyunca daha az bilinse de eş değer düzeyde tehlikelidir. Bu tehditler uygun olmayan ya da yetersiz güvenlik politikalarından ve güvenli olmayan kullanıcı uygulamalarından kaynaklanmaktadır. Bu tarz içsel tehditlerin doğasını ve önemini anlamak ve etkili karşı önlem ve uygulamaları hayata geçirmek BT güvenlik uygulayıcısının sorumluluğudur.

Tehdit Türleri

Zararlı kodlar işletmeleri aşağıdaki şekillerde tehdit edebilirler:

- **Gizlilik ve mahremiyete yönelik saldırılar** — Bunlar hem bireysel hem de tüzel düzeyde kimlik hırsızlığı ve ticaret sırları ile ilgili gelişmekte olan kaygıları içermektedir.
- **Veri bütünlüğüne karşı saldırılar** — Hırsızlık, tahribat veya hassas verilerin yetkisiz manipülasyonundan kaynaklanan ekonomik zarar veya kayıp bir kuruluş için yıkıcı olabilir. Kuruluşlar bilginin doğruluğuna ve bütünlüğüne güvenmektedir. İletişimlerin kaynağının yasallığı da iletilen verilerin bütünlüğünü etkilemektedir.
- **Servislerin ve kaynakların kullanılabilirliğine yönelik saldırılar** — İşletmeler anahtar ağ servisleri sağlama aracı olarak internete giderek daha fazla bağımlı olmaktadır. Bunun bir sonucu olarak, yasal kullanıcıların bu servislere ulaşmalarını engellemeye yönelik düşmanca saldırılar, BT güvenlik uygulayıcıları arasında artan bir kaygı haline gelmiştir. Agresif önleme (*aggressive prevention*), erken tespit (*early detection*), ve hızlı kurtarma (*quick recovery*) kabul edilebilir bir hizmet seviyesi sağlamak için gereklidir.
- **Verimlilik ve performansa karşı saldırılar**— Toplu miktarda istenmeyen e-posta (*spam*), casus yazılım, kalıcı çerezler ve benzerleri, bilgi işlem kaynaklarını tüketir ve kullanıcı verimliliğini azaltır. Fidye yazılımı, fidye ödenene kadar önemli verileri erişilemez

yaparak performansı sıfıra indirebilir. Aldatmacalar gibi var olmayan kod tehditlerine gereksiz yere tepki vermek de üretkenliği etkileyebilir. Güvenlik uzmanları bu gibi tehditlerin etkilerini en aza indirmek için düzenli olarak çaba göstermelidir.

- **Yasal sorumluluk yaratan saldırılar-** — Düşünülmemiş güvenlik zafiyetleri bir kuruluşun yasal sınırlarının ötesine geçerek müşteriler, ticaret ortakları ve diğerleri için potansiyel bir sorumluluk oluşturabilir.
- **İtibar zedeleyen saldırılar** — Zararlı kod saldırıları, bir şirket veya müşterileri hakkında hassas bilgiler yayınlayabilir ya da bir şirketi küçük düşürebilir. Bu gibi saldırılar bir şirketin itibarına zarar verebilir. Bu durum, müşterilerin ve potansiyel işlerin kaybına neden olabilir.

Çalışanlardan Kaynaklanan İç Tehditler

Saldırganlar, bir hedef ağın dışından daha kötü üne sahip (*notorious*) güvenlik tehditleri başlatsalar da güvenilir bir ağın içinde bir dizi önemli güvenlik açığı bulunmaktadır. Bunlar, BT güvenlik uygulayıcısının dikkatini gerektirmektedir.

Belki de bu güvenlik açıklarının en yaygın olanı çalışanların güvenli olmayan bilgisayar uygulamaları nedeniyle ortaya çıkmaktadır. Bu uygulamalar aşağıdakileri içerir:

- Sistemler arasında güvenilmeyen disklerin veya diğer iletim ortamların, araçlarının değişimi
- Yetkisiz, kayıtsız yazılım (uygulama ve işletim sistemi) kurulumu
- İnternetten denetlenmeyen dosyaların indirilmesi
- E-posta veya diğer mesajlaşma uygulamalarına ait eklerinin kontrolsüz bir şekilde dağıtılması

Güvenlik ihlalleri mevcut ve eski çalışanlar tarafından yürütülerek, mağdur kuruluşun içerisinden de kaynaklanmaktadır. Bu ihlaller, yetersiz personel ve güvenlik politikaları veya etkili olmayan karşı önlemler nedeniyle genellikle tespit edilmemektedir. Dolayısıyla, ilgili kuruluş tarafından çoğunlukla bildirilmezler. Bu ihlaller aşağıdakileri içerebilir:

- Sistem ve ağ kaynaklarına yetkisiz erişim
- Ayrıcalık yükseltmesi *(privilege escalation)*
- Verinin çalınması, tahrip edilmesi veya yetkisiz dağıtılması
- Dış hedeflere karşı düşmanca saldırılar başlatmak için kurumsal ağ kaynaklarının kullanılması
- Çevre kontrolleri ve izinsiz giriş tespiti karşı önlemleriyle korunmayan içsel ağ bölümlerine, yanlışlıkla veya kasıtlı olarak zararlı kodun bırakılması

Bir Saldırının Anatomisi

Tehditleri anlamak ve pratik ve etkili karşı önlemler geliştirmek için, kötü niyetli kod saldırılarının amacını olduğu kadar, saldırganların neyi hedeflediğini de anlamanız gerekir. Bu bölümde, kötü niyetli kod saldırılarının ana hedeflerini nasıl belirleyeceğinizi ve her saldırı türünün temel özelliklerini ve düşmanca amaçlarını nasıl tanımlayacağınızı öğreneceksiniz. Bu bölüm aşağıdakileri kapsar:

- Saldırganları ne motive eder
- Bir saldırının amacı

- Saldırıların türleri
- Bir saldırının aşamaları

Saldırganları Ne Motive Eder?

Bir saldırgan, artık yaptığının yanına kar kalıp kalmayacağını görmek gibi basit bir niyetle, ebeveynlerinin bodrumundan kötü amaçlı yazılımlar yazan sosyal olarak dışlanmış bir birey değildir. Günümüzün saldırganları çok daha karmaşıktır. Dört temel motivasyonları vardır:

- Para isterler.
- Ünlü olmak isterler.
- Siyasi inançlarını veya sistemlerini başkalarına dayatmak isterler.
- Kızgındırlar ve onları kızdıranlardan intikam almak isterler.

Bir Saldırının Amacı

Bir saldırının dört ana amacı vardır:

- **Kullanılabilirliğin reddedilmesi**—DoS, DDoS veya fidye yazılımı saldırısı gibi bazı saldırıların amacı, yasal kullanıcıların bir sisteme veya verilere erişmesini engellemektir.
- **Veri değiştirme**—Saldırgan yerel veya ağ sürücüsündeki bir dosyaya erişmek ve bu dosyayı yeni verilerle değiştirmek, silmek veya üzerine yazmak için komutlar verebilir. Alternatif olarak, saldırgan sistem ayarlarını veya tarayıcı güvenlik ayarlarını değiştirebilir.
- **Veri dışa aktarımı**—Saldırganlar bilgisayarınızdan bilgi çalıp internet üzerinden veya e-posta yoluyla bir saldırgana iletmek isteyebilir. Örneğin, pek çok Truva atı, kullanıcı adları ve parolaları anonim bir saldırganın Web'deki e-posta adresine iletir. Saldırgan daha sonra korunan kaynaklara erişmek için parolaları kullanabilir.
- **Başlangıç noktası**—Bir saldırgan, diğer bilgisayarları etkilemek ve hedeflemek için bir başlangıç noktası olarak kullanmak üzere bir bilgisayarı hedef alabilir.

Saldırıların Çeşitleri

Dört ana saldırı türü vardır:

- Yapısal olmayan saldırılar
- Yapısal saldırılar
- Doğrudan saldırılar
- Dolaylı saldırılar

Yapısal Olmayan Saldırılar

Orta derecede yetenekli saldırganlar genellikle ağ kaynaklarına yönelik yapısal olmayan saldırılar gerçekleştirir. Saldırganın ilk niyeti çoğunlukla yasadışı erişim elde etmekten kaynaklanan - meydan okumanın heyecanı - kişisel memnuniyettir. Elde edilen herhangi bir başarı seviyesi, içeriğin bozulması veya sistemlerin yanlışlıkla çökmesi gibi daha da zararlı aktivitelere yol açabilir. Bazen yapısal olmayan bir saldırı, istenmeyen bir güvenlik açığını gün yüzüne çıkarır; saldırgan daha sonra daha

yöntemsel bir yaklaşıma geçebilir. Tüm bu faaliyetler BT güvenlik uygulayıcıları için endişe vericidir çünkü savunma önlemlerinden bir taviz verildiğini göstermektedir.

Yapısal Saldırılar

Yüksek motivasyonlu ve teknik olarak yetenekli saldırganlar, yapısal saldırılar gerçekleştirmek için karmaşık araçlar ve odaklanmış çabalar kullanırlar. Bu saldırganlar tek başlarına veya gruplar halinde hareket edebilir. Zararlı faaliyetleri belirlemek, yoklamak *(probe)*, nüfuz etmek ve yürütmek için karmaşık bilgisayar korsanlığı tekniklerini anlar, geliştirir ve kullanırlar. Bu saldırganları harekete geçiren nedenler para, öfke, yıkım veya politik hedefler olabilir.

Motivasyonlarından bağımsız olarak, bu saldırganlar ağlara ciddi hasar verebilir. Saldırganlar, tam bir hedef belirlendikten sonra genellikle aşamalar halinde yapısal saldırılar gerçekleştirir. Bir saldırı, belirli bir kuruluşu veya işletim sistemi gibi belirli bir teknolojiyi hedef alabilir.

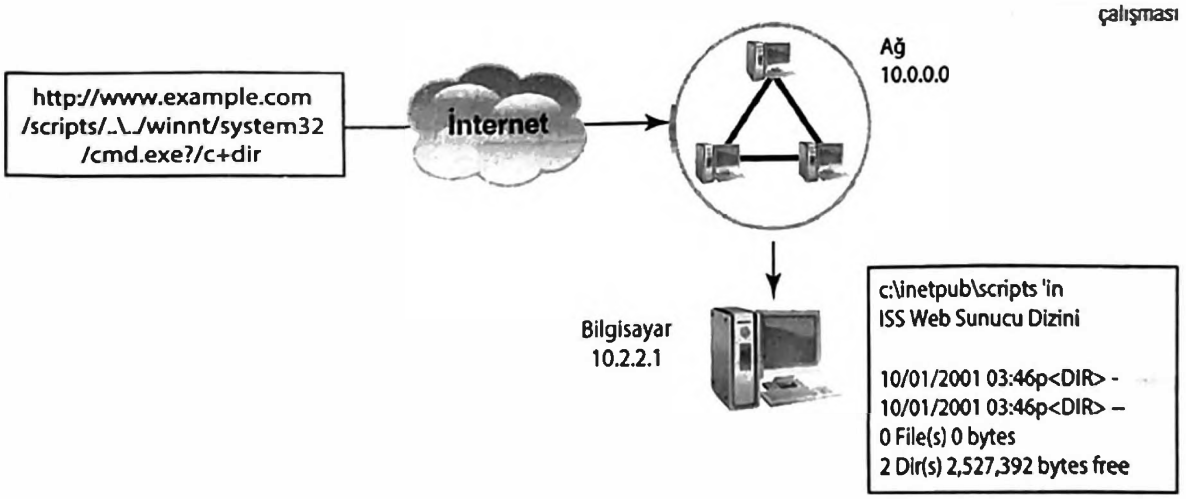
Doğrudan Saldırılar

Saldırganlar genellikle belirli kuruluşlar gibi belirli hedeflere karşı doğrudan saldırılar gerçekleştirir. Belirli donanımları kullanan ağlar, işletim sistemi sürümleri veya servisler gibi hedef sınıflarına karşı da doğrudan saldırılar düzenleyebilirler. Örnek olarak, bir kuruluştaki belirli web sunucularına karşı bir IIS Unicode saldırısı verilebilir.

Bu istismarlar (exploit) yapılandırılmamış (unstructured) olabilir - örneğin, bir betik/komut dosyası çocuğu (script kiddie) savunmasız siteleri ortaya çıkarmak için iyi bilinen bilgisayar korsanı araçlarını kullandığında ve daha sonra deneme ve yanılma yoluyla gizliliği ihlal edilmiş bir ağın etrafında rastgele istismarlar gerçekleştirdiğinde bu istismarlar yapılandırılmamıştır. Bu istismarlar, bireysel kod kırıcılar veya koordine edilmiş siber terörist gruplar tarafından düzenlenen yapısal saldırılar da olabilir ve istenilen hedeflerine ulaşmak için aşamalar aracılığıyla yöntemsel olarak ilerleyebilirler.

Tipik olarak, bir saldırgan bir hedef sisteme, parola tahmini veya oturum ele geçirme gibi uzaktan oturum açma kötüye kullanımları yoluyla erişerek gerçek zamanlı bir doğrudan saldırı gerçekleştirir. Alternatif olarak, saldırgan, bir Unicode güvenlik zafiyeti veya bir aktif içerik güvenlik zafiyeti gibi hedef işletim sistemindeki bilinen bir güvenlik açığından yararlanabilir. **ŞEKİL 11-14** bir doğrudan saldırıyı göstermektedir.

ŞEKİL 11-14
Doğrudan saldırının çalışması



Anahtar özellik saldırının gerçek zamanlı olarak gerçekleşmesidir. Saldırganın karmaşıklığına bağlı olarak, nihai amaç bir web sitesinin içeriğini bozmak olabilir. Alternatif olarak, daha kötü niyetli yapısal saldırılar için bir başlangıç olabilir. Örneğin, saldırgan, zayıf korunan bir hedef sistemi bulmaya ve ele geçirmeye çalışabilir ve ardından ele geçirilen ağdaki diğer kaynakları (dosyalar veya sistemler) istismar etmek için sisteme Truva atı programları yerleştirebilir.

Dolaylı Saldırılar

Dolaylı saldırılar, internet solucanları veya virüsler gibi önceden programlanmış düşmanca kod kötü kullanımlarının doğal bir sonucu olarak ortaya çıkmaktadır. Bu saldırılar ayrım gözetmeksizin gerçekleşmektedir. Genellikle, hızlı ve geniş bir şekilde yayılırlar. Solucan ya da virüs belirli bir sistemin veya uygulamanın güvenlik zafiyetinden yararlansa da çoğalması ve iletimi ayrım gözetmeden gerçekleşir.

Büyük olasılıkla, belirli bir hedefe yönelik bir doğrudan saldırının amacı, daha yaygın şekilde dağılmış bir topluluğa karşı dolaylı bir saldırı için bir başlangıç noktası oluşturmak olabilir. Örneğin, bir DoS kötüye kullanımı olarak bir e-posta solucanı kurmak için tek bir web sunucusunun ele geçirilmesi asıl amaçlanılan hedef olabilir.

Bir Saldırının Aşamaları

Bir saldırı geliştirmek için, saldırganların saldırının hedefini bilmeleri gerekir. Bu amaçla, bir strateji geliştirirler. Akıllı saldırganlar dedektiflerin onların kimliğini saptamasına imkân veren izler bırakmama konusuyla da ilgilidirler. Bu bölüm saldırıların aşamalarını detaylandırmaktadır. **ŞEKİL 11-15** bir saldırının aşamalarını göstermektedir.

Keşif ve Yoklama

Bir saldırının genel amacı açık olduğunda, saldırganın olası giriş noktalarını, yani güvenlik zafiyetlerini belirlemek için hedef ağı yoklaması gerekir. Bir saldırının keşif (*reconnaissance*) ve yoklama (*probing*) aşaması, belki de en önemli aşamadır. Bu aşamada, bir saldırgan, saldırının gerçekleştirilmesi için gerekli tüm bilgileri toplar. Aslında, bu aşamada toplanan bilgileri kullanmak, bir saldırının kolay olan bölümüdür. İyi bilgiler toplamak, başarılı bir saldırı girişimi için en iyi başlangıç noktasıdır. Bu aşama genellikle internette hazır olan ortak araçların kullanımını içerir. Bu araçlar genellikle altta yatan protokol paketinin bir parçasıdır ya da belirli veya potansiyel hedeflerden yararlanmak için özel olarak geliştirilmiştir.



ŞEKİL 11-15
Bir saldırının aşamaları

Bu araçlar aşağıdakileri içerebilir:

- TCP/IP protokol paketi içindeki ONS ve ICMP araçları
- Standart ve özelleştirilmiş SNMP araçları
- Bağlantı noktası tarayıcıları (port scanners) ve bağlantı noktası adresleyicileri (*port mappers*)
- Güvenlik yoklayıcıları (*security probes*)

Saldırganlar bu araçları bağımsız olarak kullanabilir. Alternatif olarak, bir saldırgan hedeflenen bir ağın tam olarak anlaşılmasını sağlamak için bunları koordine edilmiş bir takım olarak kullanabilir. Bu, kullanılan protokolleri ve işletim sistemini, çalıştırılan sunucu platformlarını, açık olan servisleri ve bağlantı noktalarını, kullanılan gerçek veya muhtemel ağ adreslemelerini ve isimlendirmelerini, vb. içerir.

İnternet ve diğer kamu kaynakları hedefleri tanımlamak için ek bilgiler sağlayabilir. Bu bilgiler, tesislerin konumunu, kilit personeli ve muhtemel iş ortaklarını içerir. Bu son bilgi önemsiz görünebilir, ancak ciddi güvenlik ihlalleri olan bir ticaret ortağı tarafından yapılan dolaylı bir saldırı olasılığı oldukça yüksektir.

DNS, ICMP ve İlgili Araçlar: Öğrendiğiniz üzere, alanı adı sunucuları (*domain name servers*), bir web sitesinin alan adını IP adresiyle eşleştiren telefon defterleri gibi çalışır. Aranabilir birkaç web sitesi, herkesin kayıtlı adresler hakkında bilgi almasını sağlar. Ek olarak, TCP/IP, hedef bir sitenin profilinin çıkartılmasında ön bilgi toplamak için kullanabileceğiniz Whois ve finger gibi keşif araçlarını destekler. **ŞEKİL 11-16**, bir Whois aramasının (*lookup*) çıktısını göstermektedir.

Ters DNS (Reverse DNS) lookup ve nslookup, aynı zamanda ONS bilgilerini arayan ve çapraz referans sağlayan ek yardımcı komutlardır. Bu servisler internette genellikle ücretsizdir. Bunları komut adının kendisini arayarak bulabilirsiniz.

İnternet Kontrol Yönetimi Protokolü (*Internet Control Management Protocol* - ICMP) ping komutu ve birbiriyle yakından ilişkili değişik araçlar, çoğu bilgisayar işletim sisteminde hazır olarak bulunmaktadır. Bu profil oluşturma araçları, saldırganların hedef sistemlerin erişilebilir olduğunu doğrulamasını sağlar. Örneğin, saldırganlar, bilgisayarlar arasında doğrudan erişilebilirliği test etmek için ping komutunu bir dizi uzantı bayrağıyla (*extension flags*) kullanabilir. Ayrıca, ping komutunu gerçek saldırı planının bir parçası olarak da kullanabilirler; örneğin, bir saldırganın güvenlik zafiyeti olan bilgisayarları çökertebilecek özel olarak oluşturulmuş ping paketleri gönderdiği bir ping saldırısı *(ping-of-death)* gerçekleştirmek için olabilir. Bir hedef ağ bulunduktan sonra, birçok saldırgan erişilebilir olabilecek diğer potansiyel bilgisayarları belirlemek için, ana ağ veya alt ağ içindeki tüm (veya bir dizi) IP adreslerinin bir ping taramasını gerçekleştirir. Bazı zamanlarda yalnızca bu bilgi, olası ağ boyutu ve topolojisini ortaya çıkarır. Ayrıca, birçok ağ yapısal bir numaralandırma düzeni kullandığından, olası sunucu ve ağ aygıtı konumlarını da işaret edebilir.

Eğer erişim kazanmak hedeflerden biriyse, bir saldırgan çevre kontrollerinin yumuşaklığını test etmek için basit bir telnet oturum açma girişiminde bulunabilir. Bir saldırgan, uzaktan komut çalıştırma için uzak yordam çağrısı (*Remote Procedure Call* - RPC) servisinin etkin olup olmadığını belirlemek amacıyla rpcinfo da kullanabilir.

SNMP Araçları: Basit Ağ Yönetimi Protokolü (*Simple Network Management Protocol* - SNMP), ağ aygıtları arasında yönetim bilgisi alışverişini kolaylaştıran bir Uygulama Katmanı protokolüdür. İletim Kontrol Protokolü/İnternet Protokolü (*Transmission Control Protocol/Internet Protocol* - TCP/IP) paketinin bir parçasıdır. SNMP, ağ yöneticilerinin ağ performansını yönetmesini, ağ sorunlarını bulup çözmesini ve ağ büyümesini planlamasını sağlar.

OpenNMS®, Solarwinds® Network Performance Monitor ve Ipswitch WhatsUp® Gold gibi pek çok popüler ağ yönetim yazılımı paketleri SNMP uyumludur. Yönetilen cihazlar, ajanlar ve ağ yönetim sistemleri için tam destek sunarlar. Ayrıca, platform, işletim sistemi sürümü ve

ŞEKİL 11-16 Bir Whois aramasının sonuçları

WHOIS information for boxtwelve.com

```
michael@primarchGazelle:~/Downloads$ whois boxtwelve.com

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: BOXTWELVE.COM
   Registrar: FASTDOMAIN, INC.
   Sponsoring Registrar IANA ID: 1154
   Whois Server: whois.fastdomain.com
   Referral URL: http://www.fastdomain.com
   Name Server: NS1.HOSTMONSTER.COM
   Name Server: NS2.HOSTMONSTER.COM
   Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Updated Date: 07-mar-2016
   Creation Date: 07-mar-2007
   Expiration Date: 07-mar-2017

>>> Last update of whois database: Wed, 11 May 2016 22:34:15 GMT <<<

For more information on Whois status codes, please visit https://icann.org/epp

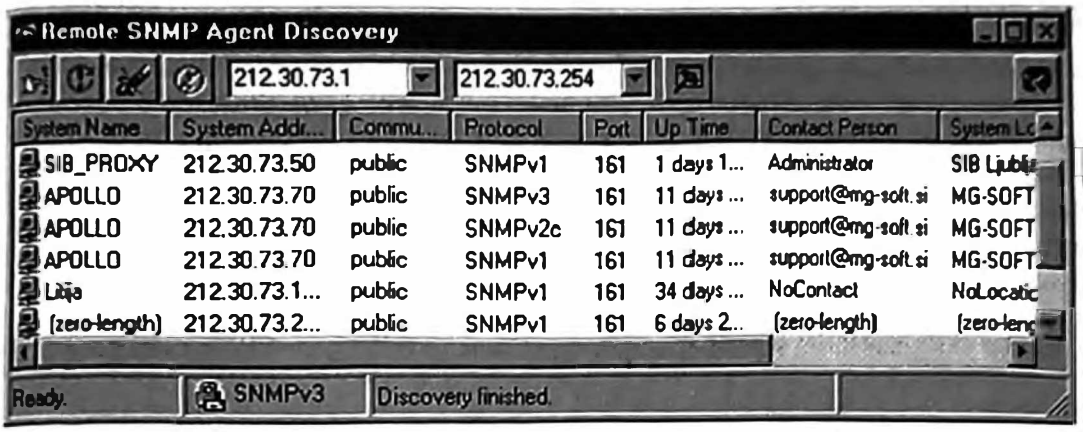
NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
```

yetenekleri dahil olacak şekilde, ağ aygıtı bilgilerini toplamak için kullanılabilecek pek çok yardımcı program vardır. Zayıf yapılandırılmış ağ yönetim olanakları, orta derecede yetenekli saldırganların önemli saldırı profili bilgileri toplamasına izin verecektir. **ŞEKİL 11-17** Remote SNMP Agent Discovery aracını göstermektedir.

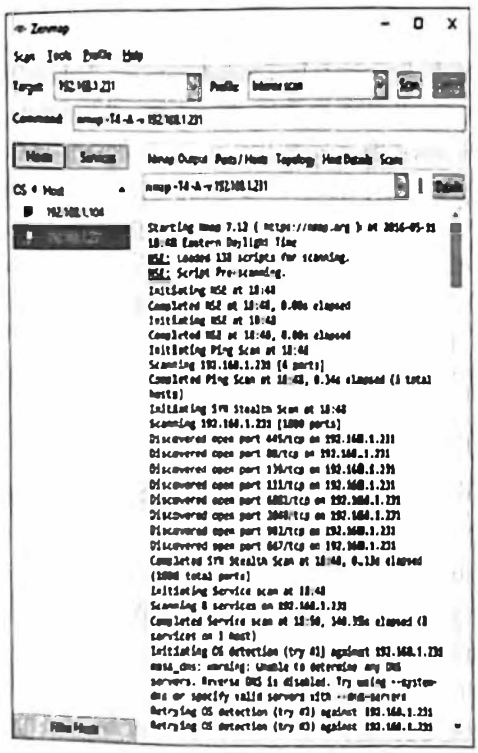
Bağlantı Noktası Tarama ve Bağlantı Noktası Eşleme Araçları: Bir saldırgan bir hedef ağı belirledikten sonra, bir sonraki adım hangi sistemlerin ve servislerin erişilebilir olduğunu kontrol etmek olabilir. Bu hedefe ulaşmak için, bir saldırgan birtakım popüler bağlantı noktası tarama uygulamalarını kullanabilir. En popüler yazılımlardan biri UNIX, Linux ve Windows için hazır olan Nmap Security Scanner® aracıdır. Angry IP Scanner, Windows, Linux ve OS X için kullanılan bir başka ağ keşif aracıdır. Tasarımı sayesinde, hızlı ve kullanımı kolaydır. ŞEKİL 11-18, Nmap bağlantı noktası tarama aracı için bir Windows GUI ön ucu (*front end*) olan Zenmap®'i göstermektedir.

Bu araçlar, bir saldırganın, ping taramaları gerçekleştirerek bilgisayarları keşfetmesine ve tanımlamasına, açık TCP ve UDP servis bağlantı noktalarını yoklamasına ve çalışan işletim sistemlerini ve uygulamalarını belirlemesine olanak sağlar.



ŞEKİL 11-17

Remote SNMP Agent Discovery ağda tepkisel SNMP ajanlarını keşfetmenizi sağlar.



ŞEKİL 11-18

Zenmap, Nmap bağlantı noktası eşleme aracı için bir Windows GUI ön ucu

Güvenlik Yoklayıcıları: Nessus veya onun açık kaynak eş değeri olan OpenVAS, güvenlik yöneticilerinin çok sayıda güvenlik zafiyetini değerlendirmesine yardımcı olur. Ağ, işletim sistemi ve uygulama ile ilgili bir takım ortak güvenlik problemlerini tespit eder. Problemleri istismar etmeden rapor edebilir. Nessus ve OpenVAS ağa erişimi olan herkes için mevcut olan bilgileri toplar. Düzgün bir şekilde yapılandırılmış bir güvenlik duvarı (*firewall*) kullanımı ile, bilgileri yetkisiz erişime karşı koruyacak politikaları doğru şekilde uygulayabilirsiniz. Ancak, bu araçların her biri iki ucu keskin bir kılıç gibidir. Pek çok araçta olduğu gibi, saldırganlar da bu araçları güvenlik uzmanları kadar kolay bir şekilde kullanabilir. Ağınızın Nessus® veya OpenVAS ile keşfedilip keşfedilmediği ile ilgili kanıtlar için tarama yapmak iyi bir fikirdir.

Erişim ve Ayrıcalık Yükseltmesi

Bir saldırgan potansiyel güvenlik zafiyetleri için bir hedef ağı tanımladığı ve yokladığı zaman, hedef sistem(ler)e erişmesi gerekir. Birincil erişim hedefi, bir hedef bilgisayara (genellikle bir sunucu platformuna) ilk bağlantıyı kurmaktır. Bilgisayar korsanlığı araç takımlarının (*hacking toolkits*) gizlice kurulması gibi ek keşif faaliyetleri yürütmek için, saldırganın sistemde yönetici hakları kazanması gerekir.

Erişim yöntemi, hedef ağa ulaşmak için gerekli olan bağlantı teknolojisine dayanmaktadır. Birçok kuruluş web merkezli iş modellerine evrildikçe, ikincil uzak ağ geçidi (*gateway*) olarak veya gözetim nedeniyle genellikle eski çevirmeli erişim altyapılarını korurlar. Bazı durumlarda, kuruluşlar dış telefon hatlarına ya da özel birim santrallerine (*Private Branch Exchanges* - PBX'ler) bağlı olarak

Parola Yakalama ve Kod Kırma

Erişim kazanmanın bir yöntemi, parolaları yakalamak (*password capturing*) veya kırmaktır (*cracking*). Bir saldırgan bir hedef makineye bir arka kapı Truva atı *(backdoor Trojan)* olarak bir parola kaydedici *(logger)* yükleyebilir ve uzak oturum açma işlemleriyle ilişkili belirli protokol ve program etkinliklerini izleyebilir. Alternatif olarak, eğer saldırgan oturum açma metinlerini uzaktan yakalarsa, LophtCrack *(www.l0phtcrack.com)* gibi bir program, yönetici ve kullanıcı parolalarını hızlı bir şekilde çözebilir ve ele geçirebilir. Aslında, parolaları ele geçirmek o kadar çekicidir ki, birçok saldırgan bu konuda oldukça becerikli hale gelmiştir. Parola kırmada iyi çalışan mevcut bilgisayar donanımlarını belirlemişlerdir. Yeni kişisel bilgisayarların çoğu, ekran kartlarında güçlü grafik işlem birimlerine (*Graphics Procesing Units* - GPU'lar) sahiptir. Bu GPU'lar, grafik görüntülerin oluşturulması (*rendering*) için gereken ileri düzey matematik hesaplamalarını yürütmek için tasarlanmıştır. Saldırganlar GPU'ların parolaları kırmak için de iyi iş çıkardığını bulmuşlardır. Pek çok yeni parola kırma aracı, tüm süreci hızlandırmak için matematiğin büyük bölümünü ekran kartı GPU'larına devreder.

Bir Uzaktan Yönetim Aracı Kullanarak Erişim Sağlama

Uzaktan Erişim Aracı *(Remote Access Tool* - RAT) çalıştırıldığı zaman, bir saldırganın ele geçirilen bir bilgisayarı uzaktan kontrol etmesini ve bilgisayara erişimini sürdürmesini sağlayan bir Truva atıdır. Bu, aşağıdakilerden biri ile yapılır:

- **Mağdurun makinesindeki bir sunucu-** Bu sunucu mağdura gelen bağlantıları dinler. Bir bağlantı aldığında, bağlanan istemci için uzaktan erişim sağlar. Kullanıcı arayüzü olmadan, görünmez şekilde çalışır.
- **Saldırganın makinesindeki bir istemci-** Bu, mağdur makinelerdeki sunuculara bağlanmak ve bunları yönetmek için saldırganın kullandığı bir GUI ön ucudur.

Mağdurun makinesine bir sunucu kurulduğunda ne olacağı, Truva atının yeteneklerine, saldırganın çıkarlarına ve tamamen farklı çıkarları olabilecek başka bir saldırganın sunucunun kontrolünü ele geçirmeyi başarıp başaramayacağına bağlıdır.

Sunucular, masaüstü bilgisayarlar, dizüstü bilgisayarlar ve mobil cihazlar dahil olmak üzere tüm cihaz türlerinde uzaktan yönetim ile bulaşma, virüsler kadar sık görülür hale gelmektedir. Ortak kaynaklardan biri dosya ve yazıcı paylaşımıdır. Saldırganlar bir sabit sürücüye erişmek için dosya ve yazıcı paylaşımını kullanabilirler. Saldırgan daha sonra Truva atını başlangıç klasörüne yerleştirebilir. Truva atı yasal bir kullanıcı bir sonraki sefer oturum açtığında çalışacaktır. Diğer bir yaygın saldırı yöntemi, Truva atını kullanıcıya e-postayla göndermektir. Saldırgan kullanıcıyı Truva atını çalıştırmaya ikna etmek için sosyal mühendislik kullanmaktadır.

Bu programların yazarları çoğu zaman onların izinsiz giriş aracı olmadıklarını iddia eder. Aksine, bunlar sadece uzaktan kontrol araçları ya da bir işletim sistemindeki zayıflıkları ortaya çıkarmak için kullanılan araçlardır. Bununla birlikte, geçmiş faaliyetlere dayanarak, asıl amaçlarının yetkisiz kullanım için bilgisayarlara erişim sağlamak olduğu açıktır.

bırakılan modem olanaklarından haberdar bile olmayabilir. Alternatif olarak, genellikle mevcut ağ çevre savunmasını tehlikeye atan kullanılmayan modem bağlantılarını öylece bırakmanın doğuracağı güvenlik risklerini göz önünde bulundurmayabilirler. Bu bağlantılar, kötü amaçlı kod saldırıları için başka bir giriş noktası sağlar.

Saldırı İzlerini Gizleme

Tespit edilmekten kaçınan bir saldırgan için en önemli aşamalardan biri, bir saldırının tüm izlerini ortadan kaldırmaktır. Bir saldırganın yaptığı belirli eylemler bir saldırıdan diğerine farklılık gösterse de, temel adımlar aynıdır. Tecrübeli saldırganlar ilk olarak oluşturmuş olabilecekleri tüm dosyaları kaldırmaya ve mümkün olan en fazla sayıda dosyayı saldırı öncesi durumlarına geri yüklemeye çalışırlar. İkinci olarak, muhtemelen saldırgan saldırının kanıtı olabilecek herhangi bir günlük dosyası (*log file*) girdisini kaldırmaya çalışacaktır. İkinci adım genellikle ilk adımdan çok daha zordur. Çoğu sistem, günlük dosyalarını değişikliklerden koruyan denetim yöntemleri kullanır. Bu, saldırganların izlerini silmek için günlük dosyalarına veya denetim sistemine saldırması gerekebileceği anlamına gelir. Çabadan bağımsız olarak, geride bıraktıkları izleri temizlemek, bir saldırının farkedilmemesi olasılığını büyük ölçüde arttırır. Güvenlik kontrollerinizi ve diğer değerli varlıkları koruduğunuzdan emin olun. Bu sayede, bir saldırıyı durdurmasanız bile, bunun gerçekleştiğini (veya şu anda gerçekleşmekte olduğunu) tespit edebilirsiniz.

Saldırı Önleme Araçları ve Teknikleri

BT güvenlik uygulayıcıları kötü niyetli kod saldırılarına karşı savunma amacıyla etkili karşı önlemlerin nasıl uygulanacağını anlamalıdır. Ayrıca, bu karşı önlemleri sürekli izlemeli, test etmeli ve geliştirmelidirler.

Derinlemesine savunma (*Defense in depth*) genel koruma seviyesini arttırmak ve olaylara müdahale etmek için daha fazla tepki süresi sağlamak için, savunmaların bölgelere katmanlı olarak yerleştirilmesi uygulamasıdır. Derinlemesine savunma, birden fazla koruma katmanı oluşturmak, tekli savunma hattını ortadan kaldırmak ve bir saldırının maliyetini etkin bir şekilde arttırmak için insanların, işlemlerin ve güvenlik teknolojilerinin yeteneklerini birleştirir. Bireysel karşı önlemleri bütünleşik bir koruyucu tedbirler grubunun bir parçası olarak ele alarak, tüm güvenlik zafiyetlerini ele aldığınızdan emin olabilirsiniz. Yöneticiler bu savunmaları kritik konumlarda güçlendirmelidir. Daha sonra saldırıları izlemeli ve bunlara hızla tepki vermelidirler.

Zararlı kod tehditleriyle ilgili olarak, bu koruma katmanları belirli kritik savunma bölgelerine uzanır:

- Uygulama savunmaları
- İşletim sistemi savunmaları
- Ağ altyapısı savunmaları

Derinlemesine savunmanın hedefleri aşağıdaki gibidir:

- Tek sistemlerde bile, güvenlik ve tespit katmanları bulunmalıdır.
- Saldırganlar her katmanı tespit edilmeden geçmeli veya atlamalıdır.
- Diğer katmanlar bir katmandaki bir kusuru örtebilir.
- Genel sistem güvenliği, genel ağ güvenliği içinde bir dizi katman haline gelir.
- Güvenlik, saldırganın cahil iken mükemmel olmasını zorunlu kılarak iyileştirilir.

Uygulama Savunmaları

Yazılım uygulamaları son kullanıcıların paylaşılan verilere erişimini sağlar. Bu verilerden bazıları hassas ya da gizlidir ve tüm kullanıcılar tarafından kullanılamaz. Saldırganlar, hassas verilere erişmeye veya bunlara zarar vermeye çalışmak için genellikle uygulama yazılımlarına saldırılar başlatır. Tüm bilgisayarlarda çalışan bütün uygulama yazılımlarını güvence altına almak için uygun kontroller konuşlandırmalısınız. Bazı yaygın kontroller aşağıdakileri içerir:

- Tüm bilgisayar sistemlerinde düzenli antivirüs taraması gerçekleştirmek
- Virüs tanımı dosyalarının güncel olmasını sağlamak
- Tüm çıkarılabilir ortamların taranmasını gerekli kılmak
- Güvenlik duvarı ve IDS yazılımını bilgisayarlara ek bir güvenlik katmanı olarak yüklemek
- Değişiklik tespiti yazılımı ve bütünlük kontrolü yazılımı konuşlandırmak ve günlük dosyaları tutmak
- E-posta kullanım kontrolleri uygulamak ve e-posta eklerinin taranmasını sağlamak
- Saldırganların açılır (*pop-up*) pencereleri göstermesini engellemek ve yanlışlıkla kötü amaçlı yazılımların çalıştırılmasına maruz kalma riskini azaltmak için, tüm kullanıcıların web tarayıcılarındaki açılır pencere engelleyicilerinin etkinleştirilmesini sağlamak
- Yazılım kurulumları ve yükseltmeleriyle ilgili net bir politika oluşturmak
- Dijital imzalar ve diğer onaylar yoluyla yazılımları tedarik ederken, kurarken ve yükseltirken yalnızca güvenilir kaynakların kullanıldığından emin olunmasını sağlamak

İşletim Sistemi Savunmaları

İşletim sistemi, uygulama yazılımları ve donanım kaynakları arasında bir arayüz hizmeti sağlar. İşletim sistemini ele geçiren herhangi bir saldırı, hassas verileri depolayan sistem kaynaklarına

Saldırganların İlerisinde Olmak

Çoğu kötü amaçlı yazılımlardan koruma yazılımı (***anti-malware***), güncel bir kötü amaçlı yazılım imza veritabanına dayanmaktadır. Bu en yaygın kötü amaçlı yazılım önleme çözümleri, yalnızca bilinen kötüye kullanımları tespit edebilir. Peki ama kimsenin bilmediği yeni kötüye kullanımlara dayanan saldırılarda ne olacak? Bunlara sıfırıncı gün (***zero day***) saldırıları denir, çünkü saldırılar başlangıçta kötü amaçlı yazılım imza veritabanları kullanılarak tespit edilemez. Bir saldırı bildirildiğinde, kötü amaçlı yazılımdan koruma yazılımı tedarikçilerinin imza veritabanlarını güncellemeleri ve bir güncelleme yayınlamaları gerekir. Daha sonra kullanıcılar güncellenen yazılımı veya veritabanını indirmek ve kurmak zorundadır. Bu gecikme, saldırganlara az dirençle karşılaşacakları saldırılar yapmak için bir zaman penceresi sunar.

Sıfır gün saldırıları dahil kötü amaçlı yazılımla mücadele etmenin bir yolu, kara liste (***blacklisting***) veya beyaz liste (***whitelisting***) kullanmaktır. **Kara liste (blacklisting),** bilinen tüm tehlikeli sitelerin bir listesini tutmaktır. Kara listedeki bir siteden gelen mesajlar işlenmeden bırakılır. Kara liste yönteminin temel sorunu, kara listeyi güncel tutmaktır. Ayrıca, pek çok potansiyel müşterinin bağlantıları ve ağ mesajlarını görmezden gelmesi ile birlikte, bir kara listeye yanlışlıkla giren herhangi bir siteye olan erişim önemli ölçüde azalacaktır. Sorunları daha kötü hale getiren bir diğer faktör, saldırganların bilgisayar veya site adreslerini sık sık değiştirmekte çok iyi olması nedeniyle, kara liste güncellemelerinin sürekli yapılması gerekliliğidir.

Beyaz liste (whitelisting), güvenilen sitelerin bir listesini tutmaktır. Beyaz listede olmayan sitelerin tüm mesajları ve bağlantı istekleri dikkate alınmaz. Beyaz liste kara listelemeye göre daha güvenlidir ancak daha kısıtlayıcıdır. Kullanmak istediğiniz tüm sitelerin bağlantılara izin verilmeden önce beyaz listenize eklenmesi gerekir. Kötü amaçlı yazılım saldırılarını önlemek için hem kara liste hem de beyaz liste ek bir koruma katmanı olarak kullanılabilir.

neredeyse sınırsız erişim sağlayabilir. İşletim sistemine yapılan başarılı saldırılar, saldırganın bir bilgisayara sahip olmasına ve onu çok amaçlı kullanmasına imkan verebilir. İşletim sistemini korumak için yapılacak kontroller önemlidir. Bunlar aşağıdakileri içerir:

- Değişiklik tespiti (*change-detection*) ve bütünlük kontrolü (*integrity-control*) yazılımı konuşlandırılması ve günlük dosyaların tutulması
- Bütün sunuculara değişiklik tespiti ve bütünlük kontrolü yazılımı konuşlandırılması veya etkinleştirilmesi
- Tüm işletim sistemlerinin tutarlı olmasının ve tedarikçilerden gelen en son güncellemelerle yama yapılmasının sağlanması
- İşletim sistemi kodunu yüklerken ve yükseltirken yalnızca güvenilir kaynakların kullanıldığından emin olunması
- Güvenlik zafiyeti oluşturabilecek gereksiz işletim sistemi servislerinin ve süreçlerinin devre dışı bırakılması

Ağ Altyapısı Savunması

Neredeyse tüm bilgisayarlar ve günümüzdeki kuruluşlarda giderek daha fazla sayıda cihaz bir noktada bir ağa bağlanmaktadır. Bilgisayarlara ve cihazlara yapılan çoğu saldırı, ağlar hedeflere uzaktan erişmeyi kolaylaştırdığı için mümkün olmaktadır. Zararlı yazılımlar genellikle yayılmak için ağları kullanır. Ağlar son kullanıcı erişimi için gerekli olduğundan, ağların kendileri hedef olabilmektedir. Aşağıdakiler dahil olmak üzere, ağınızı korumak için denetimler konuşlandırmalısınız:

- Ağda tıkanma noktaları (*chokepoints*) oluşturulması
- Kritik servisleri korumak için vekil sunucu (*proxy*) servisleri ve savunma kalesi bilgisayarları (*bastion hosts*) kullanılması
- Tıkanma noktalarında trafiği taramak için içerik filtreleme kullanılması
- İşletim sistemi kodunu yüklerken ve yükseltirken yalnızca güvenilir kaynakların kullanıldığından emin olunması
- Güvenlik zafiyetine neden olabilecek gereksiz ağ servislerinin ve süreçlerinin devre dışı bırakılması
- Güncel IDS imza veritabanlarının sağlanması
- Yeni tehditlere karşı koruma sağlamak ve güvenlik zafiyetlerini azaltmak için ağ aygıtlarına güvenlik yamaları uygulanması

En basit önleme tekniklerinden biri, gereksiz ağ servislerini, özellikle de belirli TCP ve UDP dinleme bağlantı noktalarını devre dışı bırakmaktır. Bu sayede, bu servisleri istismar etmeye odaklanan herhangi bir saldırı önlenecektir. Bununla birlikte, bu servisler yasal kullanıcılar için gerekliyse, bu yöntem etkili olmayabilir.

Ağ kaynaklarına zararlı kod saldırılarını önlemek için çok çeşitli karşı önlemler ve uygulamalar kullanabilirsiniz. Bunlar aşağıdakileri içerir:

- Ağ segmentlerine veya belirli servislere giden ve gelen trafiği engelleyen filtreleme yazılımı kullanma
- Hasarı önlemek veya azaltmak için yeterince hızlı tepki veren aktif sensörler (izinsiz giriş tespiti, antivirüs tespiti) kullanma
- Trafiği koruma bölgeleri boyunca akmaya zorlamak için ağda tıkanma noktalarının kullanılması
- Sensörlerin ve filtrelerin, korunan ağa geçmesine izin vermeden önce trafiği denetlemesine izin verme

- Tarayıcılardaki güvenlik özelliklerini, komut dosyalarının ve aktif kodun işlenmesinden önce kullanıcıdan onay isteyecek veya bunların çalışmasını engelleyecek şekilde ayarlamak
- Ağa gereksiz uzak bağlantıların ortadan kaldırılması ve kullanılabilir durumda kalması gerekenlerin korunması için etkin erişim kontrol önlemlerinin alınması
- Mevcut kontrol sistemlerinin ve karşı önlemlerin atlatılmasından kaçınılması

Her ne kadar bu öneriler geçerli olsa da, tüm ağ cihazları için bunları uygulamak gittikçe daha da zorlaşmaktadır. Ağlara bağlı olan cihazların sayısının ve çeşitlerinin arttığını daha önce öğrenmiştiniz. Bu yeni tür cihazlara aletler *(appliance)*, araçlar, çevresel sensörler ve kontroller ve hatta giyilebilir aksesuarlar dahildir. Ağlara bağlı birçok cihazın bu büyüyen topluluğuna genellikle Nesnelerin İnternet'i (*Internet of Things* - IoT) denir. Tüm bu cihazların (ve bağlı oldukları ağın) güvenli tutulması, ağa bağlı cihazların sayısındaki artış hızı nedeniyle daha da zorlaşmaktadır.

Güvenli Kurtarma Teknikleri ve Uygulamaları

Karşı önlemlerinizin ne kadar etkili olduğuna bakılmaksızın, sonunda kötü amaçlı yazılım nedeniyle bir tür veri kaybıyla karşılaşmanız olasıdır. Veri kaybını iyileştirme yeteneğiniz bu duruma ne kadar iyi hazırladığınıza bağlıdır. Tamamen kötü amaçlı yazılım içermeyen bir kurtarma süreci sağlamadığınız sürece, tam anlamıyla kurtarılma gerçekleşmez. Kurtarma ortamlarınızın ve yordamlarınızın herhangi bir kötü amaçlı yazılımı yeniden oluşturmayacağından emin olmanıza yardımcı olacak birkaç ilke aşağıdadır:

- Potansiyel kötü amaçlı yazılım enfeksiyonlarından kurtulmayı kolaylaştırmak için işletim sistemi ve veri dosyası yedekleme imgelerini dış ortamda saklamayı göz önünde bulundurun.
- Yazılımı yeniden yüklemeden önce yeni ve yedek ortamı kötü amaçlı yazılımlara karşı tarayın.
- Geri yükleme prosedürleri veya yükseltmeleri sırasında, koruma yazılımını veya servislerini yeniden etkinleştirene ya da yükleyene kadar sistemlere olan ağ erişimini devre dışı bırakın.

Etkili Yazılım En İyi Uygulamalarının Gerçekleştirilmesi

Tüm kuruluşlar ağ servisleri ve kaynakları için bir kabul edilebilir kullanım politikası (*Acceptable Use Policy* - AUP) benimsemelidir. İyi bir AUP, belirli ağ etkinlikleri için kısıtlamaları ve yazılım lisanslama ve kurulum ile ilgili bilgisayar kullanıcı alışkanlıklarını ve bunların yanı sıra dosya ve medya iletimi için prosedürleri içermelidir. Güvenlik zafiyetlerini gidermek adına yamaları ve yükseltmeleri kontrol edebilmeniz için standartlaştırılmış yazılımları benimsemeniz önerilmektedir.

ISO/IEC 27002 uyumlu bir güvenlik politikası uygulamayı göz önünde bulundurun. ISO/IEC 27002 en çok tanınan güvenlik standardıdır. ISO/IEC 27002'ye veya ayrıntılı herhangi bir güvenlik standardına uygunluk, bu nedenle, kuruluşların güvenlik bilinci en fazla olanları için bile önemsizden çok uzak bir girişimdir. Sertifikalandırma daha da göz korkutucu olabilir. Daha fazla bilgiyi *www.iso27001security.com/html/27002.html* adresinde bulabilirsiniz.

Saldırı Tespit Araçları ve Teknikleri

Saldırı tespit araçları (*intrusion detection tools*), derinlemesine savunmanın ayrılmaz bir parçasıdır. Her kuruluş, bir erken uyarı sistemi olarak ağın kritik alanlarında bir derinlemesine savunma yaklaşımı konuşlandırmalıdır. Bu konuda çeşitli uygulamalar bulunmaktadır. Her uygulama, ağları ve bilgisayarları zararlı aktivitelerden korumak için özgün yetenekler sağlayan özelliklere sahiptir.

Katmanlı bir derinlemesine savunma yaklaşımı hem ağ tabanlı hem de bilgisayar tabanlı saldırı tespitinin etkin kullanımını önerir. Bu yaklaşım hem imza temelli hem de anomali temelli tespit planlarına izin veren ürünlerin konuşlandırılmasını da kapsayabilir.

Antivirüs Tarama Yazılımı

Günümüzde çoğu bilgisayar kullanıcısı enfeksiyon tespit etmek ve önlemek için bir çeşit virüs koruması kullanmaktadır. Birçok mobil cihaz kullanıcısı o kadar dikkatli değildir. Bazı anketler, tüm kullanıcıların yarısından azının mobil cihazlarında temel güvenlik ve antivirüs yazılımlarına sahip olduğunu göstermektedir. İzinsiz giriş tespitini bilgisayar ve ağ seviyelerinde katmanlaştırabileceğiniz gibi, antivirüs korumasını destekleyen tüm cihazlara konuşlandırmalısınız.

> **NOT**
>
> Anomali tespiti, servisler veya trafik kalıpları gibi normal veya kabul edilebilir aktivitelerin bir ağ dayanak (baseline) profilinin oluşturulmasını ve ardından gerçek ağ trafiğinin bu dayanağa göre ölçülmesini içerir. Bu teknik, hizmeti engelleme veya sürekli oturum açma girişimleri gibi saldırıları tespit etmek için yararlı olabilir ancak bir öğrenme veya ön yapılandırma süresi gerektirmektedir.

Bilgisayar tabanlı antivirüs yazılımları için önemli güvenlik zafiyetleri aşağıdaki gibidir:

- Her bilgisayar sistemini en güncel virüs tanımı dosyalarıyla güncel tutmak için sürekli gereksinim duyulması
- Lisanssız veya yetkisiz yazılımların yüklenmesi ya da virüslü e-posta veya belge dosyalarının gelişigüzel alınıp verilmesi gibi güvenli olmayan kullanıcı uygulamaları aracılığıyla korumadan olası taviz verilmesi durumları

Ağ tabanlı antivirüs yazılımları, sunuculardaki dosyaların ve e-posta trafiğinin taranmasına olanak veren ve istemcilerin tutarlı bir şekilde uzaktan taranmasını ve güncel tehlikelere karşı aşılanmasını *(inoculation)* sağlayan bir seçenektir.

Birçok kuruluş hem ağ hem de bilgisayar tabanlı koruma kullanmaktadır; bazıları tespit yeteneklerini en üst düzeye çıkarmak için birden fazla ürün konuşlandırmaktadır. Virüs tanımı dosyalarını güncel tutmanız zorunludur. Artık çoğu tedarikçi, yeni virüs tanımları yayınladıklarında yazılımın otomatik olarak güncellenmesi hizmetini sağlamaktadır.

Ağ İzleyicileri ve Çözümleyicileri

Güvenlik uygulamalarının etkin kalmasını sağlamak için, ağ yazılımlarını ve aletlerini düzenli olarak izlemenin yanı sıra, ağ trafiğini düzenli olarak analiz etmelisiniz. İşletim sisteminize bağlı olarak, Nessus veya Microsoft Baseline Security Analyzer gibi bir güvenlik zafiyeti tarayıcısını ya da bu ikisinin bir kombinasyonunu arada bir çalıştırın. Saldırganların da bu araçları kullandığını unutmayın. Gereksiz açık servis bağlantı noktaları için ağı düzenli aralıklarla taramalısınız; yazılım yükseltmeleri genellikle sistemleri varsayılan ayarlarına geri döndürür.

İçerik/Bağlam Filtreleme ve Kaydedici Yazılımlar

İçeriği filtreleyen karşı önlemleri uygularken mahremiyeti ve güvenliği dengelemelisiniz. Bununla birlikte, kabul edilebilir kullanım üzerine net bir şirket politikası ile birleştirildiğinde, bu yapı zararlı kodlara karşı ek bir savunma katmanı haline gelmektedir. E-posta eklerini ve içeriğini taramak için kullanılan eklentilerin yanı sıra, ağ yönlendiricilerindeki bağlam tabanlı filtreleme (erişim kontrol listeleri) de ek bir güvenlik koruma katmanı sağlamaktadır.

Bir Bal Ağı Nedir?

Bal ağı (honeynet), gerçek, canlı bir ağı simüle etmek için yapılmış bir ***bal küpü (honeypot)*** grubudur. Bal ağları faydalıdır çünkü daha fazla veri sağlarlar ve saldırganlara daha çekici gelirler. Bununla birlikte, bir bal ağının kurulum ve bakım gereksinimleri biraz daha ileri düzeydedir. Bir bal ağı birçok sunucu, bir yönlendirici ve bir güvenlik duvarı içerebilir. Bir bal ağı, ***üretim ağıyla (production network)*** özdeş olabilir veya bir araştırma laboratuvarı olabilir. Her iki durumda da bal ağları bir saldırganın saldırması için daha gerçek bir ortam sağlamaktadır.

İçerik tabanlı filtreleme, aktif kod (Java, ActiveX vb.) bileşenleri için ağ trafiğini analiz etmeyi ve web tarayıcı yazılımlarında komut dosyası işlenmesini devre dışı bırakmayı içermektedir. Bağlam tabanlı filtreleme, aktivite kalıplarının dayanak oluşturan standartlarla karşılaştırılmasını kapsamaktadır, böylece ağ davranışlarındaki olağandışı değişiklikleri olası zararlı aktiviteler için değerlendirebilirsiniz.

Bal Küpleri ve Bal Ağları

Bal küpleri (*honeypot*), potansiyel bilgisayar korsanlığı saldırıları için yem olarak hareket etmek üzere bir ağın kenarlarında konuşlandırılan kurban edilmiş bilgisayarlar ve servislerdir. Genelde, bu sistemleri gerçek görünmeleri için yapılandırırsınız. Aslında, gerçek ağdan izole edilmiş, **bal ağı (*honeynet*)** adı verilen ayrı bir ağa yerleştirilmiş bir sunucu grubunun parçası olabilirler. Bal küpünün amacı, saldırılar için kontrollü bir ortam sağlamaktır. Bu, ağın gücünü test etmek için saldırıyı kolayca tespit ve analiz etmenizi mümkün kılar. Aktivileri kaydetmek için bilgisayar tabanlı izinsiz giriş tespiti ve izleme yazılımı yüklersiniz.

Bal küpüne giden ve bal küpünden gelen tüm trafik şüphelidir çünkü bal küpü üretim uygulamaları içermez. Bal küpü ağır saldırı altında olmadıkça, bal küpü üzerinde az sayıda kayıt üretmelisiniz. Günlük kayıtlarını (log) okumak ve anlamak kolay olmalıdır. Bir saldırgan bir bal küpünü yokladığında, bir yönetici kendi gerçek üretim ağına önleyici kontroller yerleştirebilir.

Bir bal küpü en azından aşağıdaki unsurları içermelidir:

- Gerçek bir bilgisayar gibi görünmeli ve davranmalıdır.
- Hiçbir zaman kendi varlığını ifşa etmemelidir.
- Ele geçirilmesi durumunda tüm giden trafiği önleyen bir adanmış (*dedicated*) güvenlik duvarına sahiptir.
- Normal trafikten etkilenmeyen bir arındırılmış bölgede (demilitarized zone - DMZ) yaşar.
- Gelen veya giden herhangi bir trafik olduğu zaman sessiz alarmlar çalmaktadır.
- Bir izinsiz girişi ilk algıladığında, tüm izinsiz giriş aktivitelerini kaydetmeye başlar.

Düşük katılımlı bir bal kübü, Hipermetin Aktarım Protokolü (*Hypertext Transfer Protocol* - HTTP) veya Basit Posta Transfer Protokolü (*Simple Mail Transfer Protocol* - SMTP) gibi bir dizi sahte servisler sağlar. Düşük katılımlı bal küpleri saldırganların servislere bağlanmalarını ama başka bir şey yapmamalarını mümkün kılar. Bu bal küpü türü ile, bir saldırgan genellikle işletim sistemi erişimi sağlayamaz. Bu nedenle, saldırgan tehdit oluşturmaz.

Yüksek katılımlı bir bal küpü, saldırgan için gerçek bir işletim sistemi sağlayarak orijinal servisler ve güvenlik zafiyetleri üretir. Bu bal küpü sınıfının amacı saldırganların onu ele geçirmesini sağlamaktır, böylece gerçekçi veriler toplayabilirsiniz. Yüksek katılımlı bal küpleriyle ilgili sorun, çevreyi sıkı bir şekilde kontrol etmeniz gerekmesidir. Ele geçirilen bir sistem başka bir sisteme saldırı başlatmak için bir kaynağa dönüşebilir.

BÖLÜM ÖZETİ

Bu bölümde, farklı kötü amaçlı yazılım türlerini ve her bir türün nasıl çalıştığını öğrendiniz. İstenmeyen elektronik posta, casus yazılım ve fidye yazılımı ile bunların bugünün kuruluşları üzerindeki etkilerini öğrendiniz. Farklı ağ saldırıları türlerini ve ağlarınızı saldırılardan korumanın yöntemlerini öğrendiniz. Ayrıca, tuş vuruşu kaydedicileri aldatmacalarının tehlikelerini ve web sayfası içeriklerinin bozulmalarını da öğrendiniz. Kötü amaçlı yazılımların tarihçesini ve günümüzdeki kuruluşlar için tehditlerin nasıl ortaya çıktıklarını öğrendiniz. Son olarak, farklı saldırı türlerini ve saldırganların bunları gerçekleştirmek için araçları nasıl kullandıklarını öğrendiniz.

ANAHTAR KAVRAMLAR VE TERİMLER

Active content - Aktif içerik
Adware – Reklam yazılımı
Arbitrary code execution – İsteğe bağlı kod çalıştırma
Armored Virus - Zırhlı Virüs
Backdoor – Arka kapı
Blacklisting - Kara liste
Bot-herder – Bot-çobanı
Botnet – Robot ağ
Browser add-ons - Tarayıcı eklentileri
Cookie - Çerez
Cross-platform virus - Platformlar arası virüs
Data infector – Veri virüsü
Defense in depth - Derinlemesine savunma
File infector - Dosya virüsü
Hactivist - Politik amaçlı bilgisayar korsanı
Header manipulation – Başlık manipülasyonu
Honeynet – Bal ağı
Honeypot – Bal küpü
Injection techniques - Enjeksiyon teknikleri
Keystroke logger - Tuş vuruşu kaydedici
Logic bomb – Mantık bombası
Macro virus – Makro virüs
Malware – Kötü amaçlı yazılım
Multipartite virus - Çok bölümlü virüs
Pharming - Site trafiğini yönlendirme
Phishing - Oltalama
Polymorphic virus - Çok biçimli virüs
Ransomware - Fidye yazılımı
Remote code execution - Uzaktan kod yürütme
Retro virus – Retro virüs
Rootkit - Korsanlık amaçlı program
Session hijacking – Oturum ele geçirme
Slow virus – Yavaş virüs
Smurf attack – Smurf saldırısı
Spam - İstenmeyen elektronik posta
Spyware – Casus yazılım
Stealth virus - Gizli virüs
SYN flood – SYN taşkını
SYN-ACK – SYN-ACK
System infector - Sistem başlatma virüsü
Trojan - Truva
Virus - Virüs
Web applications – Web uygulamaları
Web defacement - Web sayfası içeriğinin bozulması
Web graffiti - Web grafiti
Whitelisting – Beyaz liste
Worm - Solucan

BÖLÜM 11 DEĞERLENDİRME

1. Hangi kötü amaçlı yazılım türü diğer programlara eklenir veya bunları enfekte eder?
   A. Casus yazılım
   B. Virüs
   C. Solucan
   D. Korsanlık amaçlı program

2. _____ herhangi bir istenmeyen mesajdır.

3. Hangi zararlı yazılım türü, bir bilgisayardan diğerine yayılan bağımsız bir programdır?
   A. Casus yazılım
   B. Virüs
   C. Solucan
   D. Yılan

4. Kötü amaçlı yazılım bağlamında, aşağıdakilerden hangisi *mobil kod* terimini en iyi tanımlar?
   A. Web sitesi aktif içeriği
   B. PDA'ları ve akıllı telefonları hedef alan kötü amaçlı yazılım
   C. Birden fazla işletim sisteminde çalışan yazılımlar
   D. Yayılmak için ağları kullanan kötü amaçlı yazılım

5. Bir _____ saldırganların saldırıları başlatmak ve kötü amaçlı yazılım yaymak için kullandıkları, ele geçirilmiş bilgisayarlardan oluşan bir ağdır.
   A. Siyah ağ (Black network)
   B. Robot ağ
   C. Saldırı ağı (Attacknet)
   D. Truva atı mağazası

6. TCP SYN taşkını saldırısı (*SYN flood attack*) bir DDoS'a neden olmak için ne yapar?
   A. Ağ arka plan programının (*deamon*) çökmesine neden olur
   B. Bilgisayarı çökertir
   C. Mevcut ağ bant genişliğini sömürür
   D. Bekleyen bağlantılar tablosunu doldurur

7. Hangi saldırı türü, yasal bir web sitesi olarak maskelenerek bir kullanıcıyı kişisel bilgiler sağlaması için kandırır?
   A. Şebekeye izinsiz girme *(Phreaking)*
   B. Oltalama *(Phishing)*
   C. Trollemek *(Trolling)*
   D. Tuş vuruşu kaydetme

8. Tuş vuruşu kaydedicilerden en iyi savunma şekli, bir bilgisayarı kullanmadan önce klavye kablosunu dikkatlice incelemektir çünkü kaydedici klavyenin kablosuna bağlanmalıdır.
   A. Doğru
   B. Yanlış

9. Kötü amaçlı yazılımların ilk günlerinde virüsler nasıl yayıldı?
   A. Kablolu ağ bağlantıları
   B. Delikli kartlar *(Punch cards)*
   C. Disketler
   D. Programın hataları gibi

10. Bir saldırının en yaygın ilk aşaması hangisidir?
    A. Güvenlik zafiyeti belirlenmesi
    B. Keşif ve yoklama
    C. Hedef seçimi
    D. Kanıt tutma

11. Hangi yazılım aracı kapsamlı bağlantı noktası tarama yetenekleri sağlamaktadır?
    A. Ping
    B. Whois
    C. Rpcinfo
    D. Nmap

12. _____ stratejisi, korunan herhangi bir kaynağa ulaşmak için, bir saldırganın birden fazla kontrolü ele geçirmesi gerektiğini garanti eder.

13. Bir bal küpü, potansiyel bilgisayar korsanlığı saldırıları için yem olarak hareket etmek üzere bir ağın kenarlarına konuşlandırılmış, kasıtlı olarak güvenli olmayan servislere sahip olan kurban edilmiş bir bilgisayardır.
    A. Doğru
    B. Yanlış



KISIM III

Bilgi Güvenliği Standartları, Eğitim, Sertifikasyonlar ve Kanunlar

BÖLÜM 12 Bilgi Güvenliği Standartları 396

BÖLÜM 13 Bilgi Sistemleri Güvenliği Öğretimi ve Eğitimi 412

BÖLÜM 14 Bilgi Güvenliği Mesleki Sertifikasyonlar 433

BÖLÜM 15 ABD Uygunluk Kanunları 452

BÖLÜM

12

Bilgi Güvenliği Standartları

Yazılım ve donanım ile ilgili her şeyi tek bir üreticiden satın almak neredeyse imkânsız bir şeydir. Günümüz kuruluşları, kendi BT (Bilgi Teknolojileri – *Information Technologies* - IT) altyapılarını farklı üreticilerden almaktadırlar ve bu ürünlerin birlikte çalışmalarını beklemektedirler.

Farklı üreticilerden gelen bu kadar çok ürün nasıl birlikte çalışabilir? **Standartlar** sayesinde birlikte çalışabilirler. Standartlar, donanım ve yazılım üreticileri için rekabetçi bir pazar yaratmak ve bu pazarı sürdürmek için gereklidir. Günümüzün bilgi işlem ortamlarındaki ürünlerin birlikte çalışmasını sağlamak için yönergeler (*guideline*) sağlamaktadırlar.

Birçok kuruluş bilgisayarlar için standartlar geliştirmekte ve bunları sürdürmektedirler. Bu bölümde, bilgisayar ve ağ ürünleri ve servisleri için en yaygın standartları öğreneceksiniz. Özellikle, bu standartlardan güvenlik ile ilgili olanlar hakkında bilgiler öğreneceksiniz.

12. Bölüm Konular

Bu bölüm aşağıda verilen konuları ve kavramları içermektedir:

- Kuruluşların bilgi güvenliğine uyguladıkları standartların neler olduğu
- ISO 17799'un ne olduğu
- ISO/IEC 27002'nin ne olduğu
- PCI DSS'nin ne olduğu

12. Bölüm Hedefler

Bu bölümü tamamladığınız zaman, yapabilecekleriniz:

- Bilgi güvenliği standartlarını belirleyen önemli kuruluşları tanımlayabilme
- ISO 17799'un içeriğini özetleyebilme
- ISO/IEC 27002'nin bilgi güvenliği ile nasıl örtüştüğünü açıklayabilme
- PCI DSS gereksinimlerini tanımlayabilme

Standart Kuruluşları

İlk bilgisayarlar özel amaçlar için özel olarak geliştirilmiştir. Tasarımcılar, özel olarak geliştirilen bilgisayarın gereksinimlerine dayanarak, bileşenlerini nasıl birleştirileceğine ve bunların nasıl iletişim kuracağına karar vermişlerdir. Ancak, kısa bir süre içinde, tasarımcılar; iletişim standartlarını uygulayarak, farklı üreticilerin bileşenlerinin birlikte çalışmasını sağlayabileceklerini fark ettiler. Bu standartlaşma müşterinin bilgisayarlara olan güvenini arttırdı. Müşteriler, standartlara dayanan ürünleri satın alırken kendilerini daha rahat hissettiler. Buna rağmen, bazı tescilli sistemler standartları desteklememektedir.

Standartlara uymak pazardaki ilgiyi arttırmak ve çoğu zamanda yönetmeliklere uymak için gereklidir. Bilgi işlem ve ağ iletişimini birçok farklı açıdan yöneten standartları geliştiren ve sürdüren en etkili kuruluşları bilmeniz sizler için önemlidir.

Ulusal Standartlar ve Teknoloji Enstitüsü

Ulusal Standartlar ve Teknoloji Enstitüsü (*National Institute of Standards and Technology* - NIST), ABD Ticaret Bakanlığı bünyesinde faaliyet gösteren bir devlet kuruluşudur. 1901'de Ulusal Standartlar Bürosu (*National Bureau of Standards* - NBS) olarak kurulan NIST, ABD'nin ilk resmi fizik bilimleri araştırma laboratuvarıdır. NIST'in görevi, "ekonomik güvenliği yükseltecek ve yaşam kalitesini arttıracak şekilde ölçme bilimlerini, standartları ve teknolojiyi geliştirerek ABD yenilikçiliğini ve endüstriyel rekabeti ilerletmek" olarak belirtilmektedir. NIST, neredeyse tüm bilgi işlem cihazlarının dayandığı ölçüm ve teknoloji standartlarını sağlamaktadır. Buna ek olarak, NIST, ABD'nin resmi zamanını koruyan atom saatini korumaktadır. NIST, düzenleyici bir kuruluş olmamasına rağmen, pek çok kuruluş yayınlarına saygı duymakta ve bu yayınları kabul etmektedir.

NIST, temel görevini dört iş birliği programı aracılığıyla yürütmektedir:

- **NIST Laboratuvarları:**—ABD teknoloji altyapısını geliştirmek için araştırma yapan laboratuvarlardır. Ulusal endüstri, ürünlerin ve hizmetlerin kalitesini arttırmak için bu altyapıyı kullanmaktadır.
- **Baldridge Ulusal Kalite Programı (*Baldridge National Quality Program*)**—Üreticileri, servis kurumlarını, eğitim kurumlarını, sağlık hizmeti sağlayıcılarını ve kar gütmeyen kuruluşları içeren ABD kuruluşları arasında mükemmelliği güçlendiren ve destekleyen ulusal bir programdır. Aynı zamanda, kaliteyi arttırmaya çalışmakta ve kalite hedeflerine ulaşan kurumları onaylamaktadır.
- **Hollings Üretim Genişletme Ortaklığı (*Hollings Manufacturing Extension Partnership*)**—Küçük ve orta büyüklükteki üreticilere teknik ve ticari yardım sunan ulusal çapta bir merkezler ağıdır.
- **Teknoloji Yenilik Programı (*Technology Innovation Program*)**—Ulusal çıkarların kritik ihtiyaçlarını uygulayacak potansiyel yenilikçi teknolojileri desteklemek için kuruluşlara ve üniversitelere ödüller sunan başka bir ulusal programdır.

NIST, bilgisayar güvenliği topluluğuna genel ilgi duyan standartların ve yayınların bir listesini tutmaktadır. NIST, Bilgi Teknolojileri güvenlik yayınları için ayrı bir kimlik sağlamak amacıyla 1990 yılında Özel Yayınlar 800 (*Special Publications 800*) serisi adı verilen bir belgeler topluluğu oluşturmuştur. Bu serideki yayınlar; hükümet, sanayi ve akademik kuruluşlardaki bilgisayar güvenliği ile ilgili araştırma ve yönerge çalışmalarını raporlamaktadır.

NOT

NIST hakkında daha fazla bilgiyi internet sayfasında *www.nist.gov* bulabilirsiniz. NIST'in özel yayınları hakkında daha fazla bilgi için *http://csrc.nist.gov/publications/PubsSPs.html* adresine bakınız.

Bu alandaki pek çok kişi, 800 serisindeki NIST SP adlı yayınlara atıf yapmaktadır. Örneğin, birçok kişi, "NIST Özel Yayın 800-66" başlıklı belgeye NIST SP 800-66 olarak atıf yapmaktadır. (NIST SP 800-66, HIPAA'ya uymak için başlangıç kılavuzunu içermektedir.)

NIST Özel Yayınlar 800 serisi, bilgi sistemlerinin güvenlik faaliyetleri için rehberlik sağlayan pek çok standart içermektedir. **TABLO 12-1**'de, NIST Özel Yayınlar 800 serisinde bulabileceğiniz kaynakların bazıları listelenmektedir.

NIST, 2015'ten itibaren SP 1800, NIST Siber Güvenlik Uygulamaları Kılavuzları (*NIST Cybersecurity Practice Guides*) adında özel bir alt bölüm yayınları başlatmıştır. SP 1800; SP 800'ü genişletmekte, kamu ve özel sektörlerdeki siber güvenlik uygulamaları ile ilgili belirli konuları hedeflemektedir. **TABLO 12-2**, SP 1800 içindeki yayınları listelemektedir.

Uluslararası Standartlar Teşkilatı

Uluslararası Standartlar Teşkilatı (*International Organization for Standardization* - ISO), 1946 yılında kurulmuştur. Uluslararası bir sivil toplum kuruluşudur. Amacı, uluslararası standartları geliştirmek ve yayınlamaktır. ISO, merkezi Cenevre, İsviçre'de olmak üzere, 161 ulusal standart

TABLO 12-1 NIST Özel Yayınları 800 serisi örnek belgeleri.

SAYI	BAŞLIK
800-61 Rev. 2	*Bilgisayar Güvenliği Ayrıcalıklı Olay (incident) - İşleme Kılavuzu*
800-73-4	*Kişisel Kimlik Doğrulaması (Personal Idendity Verification - PIV) için Arayüzler (3 Bölüm)* *Bölüm 1: PIV Kart Uygulama Ad Alanı, Veri Modeli & Gösterimi* *Bölüm 2: PIV Kartı Uygulama Kartı Komut Arayüzü* *Bölüm 3: PIV İstemci Uygulama Programlama Arayüzü*
800-83 Rev. 1	*Masaüstü Bilgisayarlar ve Dizüstü Bilgisayarlar için Kötücül Yazılım Ayrıcalıklı Olayının Önlenmesi ve İşlenmesi Kılavuzu*
800-88 Rev. 1	*Medya Temizleme (sanitization) için Yönergeler*
800-94 Rev. 1	*TASLAK Saldırı Tespit ve Önleme Sistemleri için Kılavuz (Intrusion Detection and Prevention Systems - IDPS)*
800-107 Rev. 1	*Onaylanmış Özet (Hash) Algoritmalarını Kullanan Uygulamalar İçin Öneriler*
800-121 Rev. 1	*Bluetooth Güvenliği için Kılavuz*
800-124 Rev. 1	*Kurumdaki Mobil Cihazları Yönetmek ve Güvenliğini Sağlamak için Kılavuz*
800-133	*Şifreleme Anahtar Üretimi için Öneri*
800-146	*Bulut Hesaplamaya Genel Bakış ve Öneriler*
800-153	*Kablosuz Yerel Alan Ağlarının (WLAN'ların) Güvenliğini Sağlama Rehberi*
800-162	*Öznitelik Tabanlı Erişim Denetimi (Attribute Based Access Control - ABAC) Tanımı ve Dikkate Alınacak Konular için Kılavuz*
800-164	*Mobil Cihazlarda Donanım Kökenli Güvenlikle İlgili Yönergeler*
800-177	*TASLAK Güvenilir E-posta (İkinci taslak)*

TABLO 12-2 NIST Özel Yayınları 1800 serisi belgeleri.

SAYI	BAŞLIK
1800-1	TASLAK *Mobil Cihazlar üzerindeki Elektronik Sağlık Kayıtlarının Güvenliğini Sağlama*
1800-2	TASLAK *Elektrik Hizmet Uygulamaları için Kimlik ve Erişim Yönetimi*
1800-3	TASLAK *Öznitelik Tabanlı Erişim Denetimi*
1800-4	TASLAK *Mobil Cihaz Güvenliği: Bulut ve Hibrit Yapılar*
1800-5	TASLAK *BT Varlık Yönetimi*

enstitüsünden oluşan bir ağdır. ISO, kamu ve özel sektör arasında bir köprü görevi yapmaktadır. Bazı üyeleri devlet kurumlarıdır; bazıları ise özel sektördedir. ISO'nun hedefleri, her iki gruba da hitap etmeyen ancak fikir birliğine ulaşan standartları geliştirmektir.

Kuruluşun kısa ismi olan ISO, bir kısaltma gibi görünse de aslında öyle değildir. ISO, uluslararası bir organizasyon olduğu için, tam adı dile bağlı olarak değişmektedir. ISO üyeleri, *eşitlik* anlamına gelen, Yunanca *isos* sözcüğünden türetilen ISO kısa adı üzerinde anlaşmışlardır. ISO, ad seçiminde de fikir birliğine varmaya çalışmaktadır. Fikir birliği üzerine odaklanma, ISO'nun pek çok alanda standartları geliştirme ve teşvik etme konusunda başarılı bir otorite haline getirmektedir.

ISO, nerdeyse tüm sektör için birçok standart yayınlamaktadır. Örneğin, Uluslararası Standart Kitap Numarası (*International Standard Book Number* - ISBN) bir ISO standardıdır. Bilgi teknolojileri alanı için belki de en iyi bilinen ISO standardı, **ŞEKİL 12-1**'de gösterilmekte olan Açık Sistemler Ara Bağlantısı Referans Modeli (*Open Systems Interconnection* - OSI)'dir. Uluslararası olarak kabul gören bu standartlar çatısı farklı bilgisayar sistemlerinin ağları kullanarak nasıl iletişim kuracağını belirlemektedir. Referans modeli, ağ iletişimi ile ilgili yedi farklı konuyu ele alan yedi farklı katmanı içermektedir. Referans modeli, farklı üreticilerden gelen bilgisayar ve cihazların iletişim kurmasını sağlayan standartları tanımlamaktadır.

Modeldeki her katman ilgili işlevlerin bir koleksiyonunu sunmaktadır. Her fonksiyon hemen üstündeki katmana hizmet sunmakta ve hemen altındaki katmandan hizmetler almaktadır.



ŞEKİL 12-1
OSI Referans Modeli

Örneğin, Taşıma Katmanı (Katman 4) bir ağ boyunca hatasız iletişim sağlamaktadır. Oturum Katmanı'ndaki (Katman 5) yazılım işlevleri tarafından ihtiyaç duyulan bağlantıları da sağlamaktadır. Buna ek olarak, ağ iletişiminin içeriğini oluşturan paketleri göndermek ve almak için bir sonraki katmandaki Ağ Katmanı'ndaki (Katman 3) işlevleri çağırmaktadır.

Birçok yeni ağ çözümü yedi farklı katmanın yapısına tam olarak uymasa da, OSI Referans Modeli hala ağ kavramlarını öğretmek için kullanılan etkin bir araçtır. OSI Referans Modeli, ağların standart bir ortamda genel hizmetleri nasıl sağladığını anlamanın temelini oluşturmaktadır.

Güncel yazılımlara diğer modeller daha doğrudan eşleşebilse bile, OSI Referans Modeli ağ temellerini öğretmek için hala önemli bir araçtır.

NOT

www.iso.org/iso/home.html web sayfasından ISO standartlarına göz atabilir ve kuruluş hakkında daha fazla bilgi edinebilirsiniz.

ISO birçok standardını, her bir standarda atadığı hem Uluslararası Standartlar Sınıflaması (*International Classification for Standards* - ICS) hem de Teknik Komite (*Technical Committee* - TC) tarafından organize etmektedir. 200'den fazla TC'den birine atanmış 40 farklı Seviye 1 ICS arasında yayılmış standartları bulabilirsiniz. Bu standartların genişliği için size bir fikir vermektedir.

Uluslararası Elektroteknik Komisyonu

Uluslararası Elektroteknik Komisyonu (*International Electrotechnical Commision* - IEC), çoğunlukla ISO ile çalışan bir standart kuruluşudur. IEC, elektrikli ve elektronik cihazlar ve süreçlerle ilgili teknolojiler için uluslararası standartların geliştirilmesi ve yayınlanmasında en önde gelen kuruluştur. İnsanlar IEC tarafından **elektroteknoloji** olarak belirtilen ortak bilgi yığınına atıfta bulunurlar.

IEC, 1906 yılında elektrikli cihazlarla ilgili büyüyen teknolojilere ilişkin sorunları çözmek için kurulmuştur. Günümüzde IEC standartları aşağıdakileri de içeren çok çeşitli alana hitap etmektedir:

- Güç üretimi
- Enerji iletimi ve dağıtımı
- Ticari ve tüketici elektrikli ev aletleri
- Yarı iletkenler
- Elektromanyetik
- Aküler
- Güneş enerjisi
- Telekomünikasyon

NOT

Gauss manyetik alan için bir ölçümdür, hertz saniyedeki döngülerin bir gösterimidir ve weber manyetik akışın bir ölçümüdür.

IEC; gauss, hertz ve weber de dahil olmak üzere elektrik ölçümleri için standartların geliştirilmesini sağlamıştır. IEC, çabalardan sinerji oluşturmak için ISO ve ITU-T (bu bölümde daha sonra anlatılacaktır) ile yakından çalışmaktadır. Standartların uluslararası kabulünü ve en iyi şekilde kullanımını sağlamak için IEC, mümkün olduğunca çok ülkeden katılımı teşvik etmektedir. Bu yazı hazırlanırken, Ulusal Komiteler

(National Committees - NC) olarak da bilinen 60 tam IEC üyesi ve yardımcı 23 IEC üyesi bulunmaktadır. 2001'de IEC, üyeliğini daha çok gelişmekte olan ülkeleri de içerecek şekilde genişletmiştir. Ortaklık Ülke Programı (*Affiliate Country Programme*) daha küçük 84 ülkeyi içermektedir.

Bir BT uzmanı olarak, fiziksel bilgisayar ve ağ donanımı ile ilgili IEC standartları ile büyük olasılıkla karşılaşacaksınız. IEC'nin odağı, kurulduğunu günden bu yana elektrik ve elektronik sektörleri değiştikçe genişlemiştir. Günümüzde, IEC'nin odak noktasında, ortaya çıkan güç ihtiyaçları ve bunların diğer işlevsel alanları nasıl etkilediğini ele alan standartlar bulunmaktadır. IEC; güvenlik, performans, çevre sorumluluğu, enerji verimliliği ve yenilenebilir enerji kaynaklarını ve kullanımını destekleyen standartların geliştirilmesinde aktif olarak yer almaktadır.

NOT

IEC kuruluşu ve standartları hakkında daha fazla bilgiyi IEC'nin internet sayfasından alabilirsiniz: www.iec.ch

World Wide Web Konsorsiyumu

1990'da World Wide Web'in oluşturulması, kullanıcıların internetteki kaynaklara erişiminde bir dönüm noktası olmuştur. İnternetin ilk günlerinde rakip satıcılar, Web'in ilk dili olan Hiper Metin İşaretleme Dili (*HyperText Markup Language* - HTML)'nin kendi sürümlerini yayınladılar. Bu sürümler diğer satıcıların sürümleri ile uyumsuzdular. Bu uyumsuzluklar web tarayıcılarında sorunlara neden olmuş ve Web'in işlevselliğini sınırlamışlardır. Web'e ilgi arttıkça, temel bir dili standartlaştırma ihtiyacı belirginleşti. World Wide Web'in sonunda geleceği durum için orijinal öneriyi yazan bilgisayar bilimcisi Sir Tim Berners-Lee, standart eksikliklerini gidermek için 1994'te **World Wide Web Konsorsiyum (*World Wide Web Consortium* - W3C)**'unu kurmuştur.

W3C, anında World Wide Web için temel uluslararası standart bir kuruluş haline gelmiştir. W3C'nin belirtilmiş olan amacı, World Wide Web'i birleştirmek ve uzun vadeli büyümesini sağlamak için protokoller ve yönergeler geliştirmektir. W3C'nin günümüzde iş kurumları, kar amacı gütmeyen kuruluşlar, üniversiteler ve çeşitli devlet kurumlarını temsil eden 419 üyesi bulunmaktadır.

W3C, web geliştirme ve işlemlerinin birçok yönünü yöneten ve düzenleyen web ile ilgili birçok standart geliştirmiştir. W3C tarafından geliştirilen veya onaylanan standartlar aşağıdaki gibidir:

- Basamaklı Stil Şablonları (*Cascading Style Sheets* – CSS)
- Ortak Ağ Geçidi Arayüzü (*Common Gateway Interface* - CGI)
- Hiper Metin İşaretleme Dili (*HyperText Markup Language* - HTML)
- Basit Nesne Erişim Protokolü (*Simple Object Access Protocol* - SOAP)
- Web Servisleri Tanımlama Dili (*Web Sevices Description Language* - WSDL)
- Genişletilebilir İşaretleme dili (*Extensible Markup Language* - XML)

Bu standartların ve teknik özelliklerin her biri, web uygulamalarının diğer satıcıların web bileşenleri ile etkileşimde bulunmasını sağlamak için gerekmektedir. Herhangi bir World Wide Web bileşeni ile çalışıyorsanız, büyük olasılıkla bir ya da daha fazla W3C standardı ile karşılaşırsınız.

NOT

W3C ile ilgili daha fazla bilgi, standartları, World Wide Web için standartlar ve kılavuzlar sağlama çalışmaları hakkında daha fazla bilgi için www.w3.org adresindeki W3C web sitesine bakınız.

İnternet Mühendisliği Görev Grubu

İnternet Mühendisliği Görev Gücü (*Internet Engineering Task Force* - IETF), İnternet standartları geliştirmekte ve desteklemektedir. IETF web sitesine göre, kuruluşun amacı "İnternetin daha iyi çalışmasını sağlamak"'tır. IETF, internet iletişiminin mühendislik konularına

odaklanmaktadır ve politika ile iş sorunlarından kaçınmaya çalışmaktadır. IETF, öncelikle TCP/IP veya internet protokol paketinin standartları üzerine odaklanarak W3C ve ISO/IEC ile yakın bir şekilde çalışmaktadır. IETF açık bir organizasyondur. Üyelik şartı yoktur. Katkıda bulunanlar ve liderler de dahil olmak üzere tüm iştirakçiler gönüllüdür. İşverenleri genellikle kendi çalışmalarını finanse etmektedir.

NOT

IETF ve etkinlikleri hakkında daha fazla bilgi için, IETF'nin *www.ietf.org* adresindeki web sayfasını ziyaret ediniz.

IETF ilk kez 1986'da temel internet iletişim protokollerini resmileştirmek isteyen 21 araştırmacıdan oluşan bir grup olarak bir araya gelmiştir. Bugün IETF, her grup belirli bir konuyu ele alan, çalışma gruplarından (*working group* - WG) oluşmaktadır. Günümüzde 100'den fazla WG bulunmaktadır. WG'ler bağımsız olarak çalışmaya eğilimli oldukları için, IETF her grup için asgari standartları belirlemektedir. Her WG'nin, grubun hedeflerini ve beklenen çıktılarını belgeleyen tüzüğü ve belirlenmiş bir başkanı veya eşbaşkanları bulunmaktadır.

Her WG, herkesin abone olabileceği özel bir posta listesine sahiptir. Bu WG posta listeleri, katılımcılar için birincil iletişim ortamı olarak görev yapmaktadır. Çoğu katılımcı, ilgisini çeken bir veya daha fazla WG posta listesine abone olarak başlamaktadır. WG'ler ayrıca, tüm katılımcılara açık olan periyodik toplantılar düzenlemektedir. Genel olarak toplantılara katılmak yararlı olmasına rağmen, sadece posta listesiyle etkileşim kurarak da bir WG'ye katılmak mümkündür.

Yorumlar için İstekler

IETF **yorumlar için istekler** (***requests for comments*** – **RFC**) üretmektedir. RFC, basit notlardan birkaç standart belgeye kadar uzanan bir belgedir. Her RFC'nin tanıtımı kendi durumunu göstermektedir. RFC modeli, birçok kaynağın girdisine izin vermekte ve işbirliği ve hakem denetimini (*peer review*) teşvik etmektedir. IETF, RFC'ler için yönergeler yayımlamaktadır. RFC'ler hakkında aşağıda birkaç nokta bulunmaktadır:

- **Yalnızca bazı RFC'ler standartları belirtmektedir**—"Bu belge ..... belirtmektedir" veya "Bu belge ..... belgelemektedir" gibi ifadeleri içeren RFC'ler standart ya da normatif belge olarak dikkate alınmalıdır.
- **RFC'ler asla değişmez** —RFC'deki herhangi bir değişiklik yeni bir sayı almakta ve böylece yeni bir RFC haline gelmektedir. Geçmiş belgeler güncelliğini yitirmiş olabileceğinden her zaman en yeni RFC aranmalıdır.
- **RFC'ler başka kuruluşlar ile başlatılabilir**—IETF sadece bazı RFC'leri oluşturmaktadır. Diğerleri bağımsız kaynaklardan, IAB'den veya İnternet Araştırma Görev Gücü'nden (*Internet Research Task Force* - IRTF) gelebilmektedir.
- **Resmi standartları tanımlayan RFC'lerin dört aşaması bulunmaktadır**—Bir RFC bir aşamadan diğerine geçerken, daha resmi hale gelir ve daha fazla kuruluş bunu kabul eder. Aşamalar şunlardır:
  - **Önerilen standart (*Proposed Standard* - PS)**—Bir standardın ilk resmi aşamasıdır.
  - **Taslak standart (*Draft Standard* - DS)**—Katılımcılar standardın çalışma ortamlarında uygulandığını gösterdikten sonraki standardın ikinci aşamasıdır.
  - **Standart (*Standard* - STD)**—Yaygın olarak kabul görmüş ve uygulandıktan sonra bir standardın son aşamasıdır.
  - **En İyi Mevcut Uygulama (*Best Current Practice* - BCP)**—Resmi standartlar olmayan işlemsel tanımlamaları (*operational specifications*) belgelemek için kullanılan alternatif bir yöntemdir.

IETF standartlarının bazı örnekleri arasında RFC 5878 ve RFC 5910 bulunmaktadır. RFC 5878, "Aktarım Katmanı Güvenliği (*Transport Layer Security* - TLS) Yetkilendirme Uzantıları", TLS el sıkışma (*handshake*) protokolünün uzantılarına ilişkin belirtimleri içermektedir. RFC 5910, "Genişletilebilir Hazırlama Protokolü (Extensible Provisioning Protocol - EPP) için Alan Adı Sistem Güvenliği Uzantıları Eşlemesi (DNS Security Extensions Mapping)", merkezi bir depoda depolanan DNSSEC alan adları için EPP uzantısı eşlemesini açıklamaktadır. Bu RFC'lerin her ikisi de önemsiz okumalar yapmamaktadır. İnternetin nasıl çalıştığını tanımlayan oldukça teknik ayrıntıları içermektedirler.

İnternet Mimarisi Kurulu

İnternet Mimarisi Kurulu (*Internet Architecture Board* - IAB) IETF'nin bir alt komitesidir. Ayrıca, İnternet Topluluğu (*Internet Society* - ISOC) için bir danışma konseyi olarak hizmet etmektedir. IAB, bağımsız araştırmacılar ve internetin refahı konusunda teknik ilgi duyan profesyonellerden oluşmaktadır.

NOT

www.ietf.org/rfc.html adresinde yer alan IETF'nin RFC web sayfasında, RFC'ler hakkında daha fazla bilgiyi bulabilir ve bir RFC arama motoruna erişebilirsiniz.

IAB birçok IETF etkinliği için bir gözetim komitesi olarak görev yapmaktadır. IAB aşağıdakiler için gözetim yapmaktadır:

- İnternet protokolleri ve süreçleri için mimari
- Standartlar oluşturmak için kullanılan süreçler
- RFC'ler için editör ve yayın süreçleri
- IETF başkan ve teknik bölge müdürlerinin onayı

IAB, IETF ile ilgili işin yürütme süreçlerinin üst düzeyde yönetilmesini ve onaylanmasını sağlar. IAB, interneti etkileyen birçok standart üzerinde önemli bir etkiye sahip olan etkili bir komitedir.

Elektrik ve Elektronik Mühendisleri Enstitüsü

Elektrik ve Elektronik Mühendisleri Enstitüsü (*Institute of Electrical and Electronics Engineers*) web sitesine göre (www.ieee.org/index.html), Elektrik Elektronik Mühendisleri Enstitüsü (IEEE), "teknolojinin ilerlemesi için dünyanın en büyük profesyonel kuruluşu"dur. IEEE, elektrik ve elektronik ile ilgili standartların geliştirmesi ve yaygınlaştırılması üzerine odaklanan uluslararası kar amacı gütmeyen bir kuruluştur. 160 ülkede yaklaşık 420.000'den fazla üyesi ile dünyadaki en fazla üyeye sahip teknik meslek kuruluşudur. IEEE, 1963 yılında iki eski kuruluşun, 1912'de kurulan Radyo Mühendisleri Enstitüsü'nün (*Institute of Radio Engineers*) ve 1884'te kurulan Amerikan Elektrik Mühendisleri Enstitüsü'nün (*American Institute of Electrical Engineers*) birleşmesiyle kurulmuştur.

NOT

ISOC'un web sitesine göre, www.*intersociety.org*, ISOC; internet ile ilgili standartlarda, eğitimlerde ve dünya genelindeki politikalarda önderlik sağlamak için 1992'de kurulmuş olan kar amacı gütmeyen bağımsız bir kuruluştur.

IEEE, belirli teknik alanlardaki faaliyetlere odaklanan 39 topluluğu desteklemektedir. Bu teknik alanlar manyetik, fotonik ve bilgisayarları içermektedir. Her topluluk yayın geliştirir, konferanslar düzenler ve belirli bir alanda daha fazla bilgi ve ilgiye yönelik etkinlikler ve faaliyetler geliştirir. IEEE, çok sayıda mühendislik konularını kapsayan birçok eğitim ve öğretim olanakları da sunmaktadır.

IEEE ayrıca standart üreten en büyük kuruluşlardan biridir. IEEE Standartları Birliği (*IEEE Standards Association* - IEEE-SA) bu standartları yönetmektedir. IEEE standartları, bilgi teknolojisi de dahil olmak üzere birçok endüstriyi kapsamaktadır. IEEE şu anda 1,300'den fazla standart ve

TOBLO 12-3 Ortak IEEE 802 standardı çalışma grupları.

Çalışma Grubu	Adı
802.1	Daha Yüksek Katman LAN Protokolleri
802.3	Ethernet
802.11	Kablosuz LAN (802.11a, 802.11b, 802.11g, 802.11n, 802.11ad vb.)
802.15	Kablosuz Kişisel Alan Ağı (WPAN)
802.16	Genişbant Kablosuz Erişim (WiMAX)
802.18	Radyo Düzenleyici TAG
802.19	Kablosuz Koekzistans
802.20	Mobil Genişbant Kablosuz Erişim

NOT

802 çalışma grubu adını toplandığı ilk tarihten, Şubat (2.ay) 1980, almaktadır.

projeyi yayınlamakta veya sponsorluk yapmaktadır. Bilgi güvenliği ile ilgili en iyi bilinen standart IEEE 802 LAN/MAN standart ailesidir. Bu standart grubu, çeşitli tiplerdeki yerel alan ağının (LAN) ve metropol alan ağının (MAN) protokollerinin çalışma şeklini tanımlamaktadır. **TABLO 12-3**, IEEE 802 LAN/MAN standardında daha fazla tanınan çalışma gruplarının bazılarının bir listesini vermektedir.

IEEE, belirli profesyonel gereksinimleri karşılayan teknik topluluk üyelerine açıktır. Tam üyeler IEEE seçimlerinde oy kullanabilirler. Öğrenciler, IEEE'ye öğrenci üyelikleri edinebilir; oy kullanma hakkı dışındaki tam üyeliğin tüm avantajlarından yararlanabilirler. Öğrenci olmayan ve teknik gereksinimleri karşılamayan ilgili taraflar için IEEE, sınırlı ayrıcalıklara sahip olan yardımcı üyelikler sunmaktadır.

Uluslararası Telekominikosyan Birliği Telekominikasyon Sektörü

Uluslararası Telekomünikasyon Birliği (*International Telecommunication Union* - ITU), bir Birleşmiş Milletler kuruluşudur. Bilgi ve teknoloji konularını yönetmekten ve teşvik etmekten sorumludur. ITU, ağların ve ilgili hizmetlerin hem devlet hem de ticari olarak geliştirilmesi için küresel bir odak noktasıdır. ITU, gelişmekte olan telgraf iletişim endüstrisi için uluslararası standartlar geliştirmek üzere 1865 yılında Uluslararası Telgraf Birliği (*International Telegraph Union*) olarak kurulmuştur. ITU, 1947'de bir BM ajansı haline gelmiştir. 1956'da Uluslararası Telgraf ve Telefon Danışma Komitesi (*International Telegraph and Telephone Consultative Committee*-CCITT) olarak ismi değiştirilmiş ve sonunda 1993 yılında bugünkü adını kabul etmiştir. ITU merkezi İsviçre Cenevre'de bulunmaktadır. Üyeleri arasında 193 üye ülke ve 700'den fazla sektör üyesi ve iştirak bulunmaktadır.

ITU'nun en eski ve en tanınmış etkinliği, iş geliştirme standartlarıdır. **ITU Telekomünikasyon Sektörü (ITU *Telecommunication Sector* – ITU-T)** tüm ITU standartları çalışmalarını yerine getirmektedir. ITU-T, tüm ulusların telekomünikasyon alanlarını kapsayan standartların verimli ve etkili bir şekilde üretilmesinden sorumludur. ITU-T ayrıca, uluslararası telekomünikasyon

hizmetleri için tarife ve muhasebe ilkelerini tanımlamaktadır. Zamanlama, ITU-T standartlarının önemli bir odağı haline gelmiştir. 2001'de organizasyon, eski standartları geliştirme prosedürlerini, standartları oluşturmak için gereken süreyi yüzde 95 azaltmak için revize etmiştir.

ITU-T, **öneriler (*recommendations*)** ürettiği uluslararası standartları çağırmaktadır. Bunlar, bir üye ülkenin ulusal yasalarının bir parçası olarak kabul edildiğinde zorunlu hale gelirler. ITU-T bir BM ajansı olduğu için, standartları uluslararası ağırlık taşımaktadır. ITU-T, standartlarını öneriler olarak isimlendirse de önemli bir otorite olmak eğilimindedir.

ITU-T, önerilerini her biri alfabenin benzersiz bir harfini içeren 26 ayrı seriye bölmektedir. Örneğin, anahtarlama ve sinyal önerileri Q serisindedir. Veri ağları, açık sistem iletişimleri ve güvenlik önerileri X serisindedir. ITU-T, her türlü iletişimin teknik detaylarını ele alan birçok iletişim önerisi geliştirmiş ve yayınlamıştır. X serisi önerilerin birçoğu doğrudan bilgi güvenliği ile ilgilidir. **TABLO 12-4**, bilgi güvenliği ile ilgili ITU-T önerilerinin bazı aralıklarını listelemektedir.

NOT

ITU ve ITU-T hakkında daha fazla bilgiyi www.itu.int adresindeki ITU web sayfasında bulabilirsiniz.

Amerikan Ulusal Standartlar Enstitüsü

Amerika Birleşik Devletleri'nin önde gelen standart ajanslarından birisi **Amerikan Ulusal Standartlar Enstitüsü'dür (*American National Standards Institute* - ANSI)**. ANSI'nin amacı, ABD pazarını küresel ekonomide güçlendirmektir.

Aynı zamanda, tüketicilerin sağlığı ve güvenliği ile çevrenin korunmasını sağlamak için çaba göstermektedir. Bu hedefe gönüllü uzlaşma standartlarını ve uygunluk değerlendirme sistemlerini geliştirerek ulaşmayı amaçlamaktadır.

ANSI, hemen hemen her sektördeki işletmeleri doğrudan etkileyen pek çok standart ve yönergenin oluşturulması, yayınlanması ve yönetilmesini denetlemektedir. ANSI standartları; akustik

TABLO 12-4 Bilgi güvenliği ile ilgili ITU–T önerileri

ITU-T ÖNERİSİ	TANIM
X.800-X.849: Güvenlik	Bu serideki öneriler, güvenlik sorunlarını farklı ağ katmanlarıyla ilişkili olarak ele almaktadır.
X.1000-X.1099: Bilgi ve ağ güvenliği	Genel ağ güvenliği
X.1100-X.1199: Güvenli uygulamalar ve hizmetler	Uygulamaların ve hizmetlerin güvenli bir şekilde geliştirilmesi ve yerleştirilmesinin sağlanması
X.1200-X.1299: Siberuzay güvenliği	Genel olarak siber güvenlik, kimlik yönetimi ve spam karşıtlığı
X.1300-X.1399: Güvenli uygulamalar ve hizmetler	X.1100-X.1199'dan farklı olarak, bu seri acil durum iletişimi ve sensör ağ güvenliği üzerine odaklanmaktadır
X.1500-X.1599: Siber güvenlik bilgi alış verişi	Güvenli bir ortamdaki aktörler arasındaki bilgi alışverişine odaklanmaktadır
X.1600 – X.1699: Bulut hesaplama güvenliği	Özellikle bulut ortamları ile ilgili güvenlik başlıkları

cihazlar, inşaat donanımları, süt ve hayvancılık üretimi ve enerji dağıtımı gibi farklı sektörleri kapsamaktadır.

ANSI, beş mühendislik derneği ve üç devlet kurumunun birleşmesi yoluyla 1918'de kurulmuştur. Bu gruplar Amerikan Mühendislik Standartları Komitesi (*American Engineering Standards Committee* - AESC)'ni oluşturmak üzere birleştiler. 1928'de AESC, Amerikan Standartları Birliği (*American Standards Association* - ASA) haline gelmiştir.

1966'da ASA yeniden düzenlendi ve Amerika Birleşik Devletleri Standartları Enstitüsü (*United States of America Standards Institute* - USASI) adını aldı. Son olarak, 1969'da USASI ANSI haline geldi. Bugün ANSI; devlet kurumları, organizasyonlar, eğitim kurumları ve bireylerden oluşmaktadır. ANSI 125.000'den fazla şirket ve 3.5 milyon profesyoneli temsil etmektedir.

ANSI, BT'nin neredeyse tüm yönlerini etkileyen standartlar üretmektedir. Özellikle, bilgisayarın ve iletişimin mühendislik veya teknik yönlerine odaklanan diğer kuruluşların aksine, ANSI öncelikle yazılım geliştirme ve bilgisayar sistemi işlemlerini destekleyen standartlara hitap etmektedir. **TABLO 12-5**, bilgi güvenliği ve yazılım geliştirme alanlarında karşılaşacağınız bazı ANSI standartlarını listelemektedir.

NOT

ANSI hakkında daha fazla bilgiyi organizasyonun *www.ansi.org* adresindeki web sayfasında bulabilirsiniz.

Avrupa Telekomünikasyon Standartları Enstitüsü Siber Güvenlik Teknik Komitesi

ETSI, Avrupa Telekomünikasyon Standartları Komitesi (*European Telecommunications Standards Institute*), Avrupa Birliği (*European Union* - EU) üye devletleri tarafından ortak olarak kabul edilmiş bilgi ve iletişim teknolojileri (*information and communications technologies* - ICT) için standartlar geliştirmektedir.

ETSI standartları hem kablolu hem de çeşitli kablosuz iletişim teknolojilerini kapsamaktadır. 66 farklı ülkeden 800'den fazla üye kuruluşu bulunmaktadır. ETSI resmi olarak Avrupa Birliği tarafından bir Avrupa Standartlar Organizasyonu (*European Standards Organization*) olarak tanınmaktadır. 2014'te ETSI, TC CYBER adında bir Siber Güvenlik Teknik Komitesi (*Cyber Security Technical Committee*) oluşturmuştur. TC CYBER, ETSI komiteleri içindeki tüm siber güvenlik standartlarını merkezileştirmektedir. TC CYBER standartlarının, başlangıçta üye AB ülkeleri tarafından kabul edilecek uluslararası standartlarla sonuçlanması amaçlanmıştır. Bu standartlar, öncelikle, internetle ve sürmekte olan ticari iletişimler ile ilgili güvenlik konularına odaklanmaktadır. Tüm

TABLO 12-5 Önemli ANSI standartları.

Standard	Description
ANSI Kodu	ANSI kodu, bilgisayarlardaki karakterleri temsil etmek için kullanılan bir dizi değeri tanımlayan bir standarttır. Birden çok bilgisayarın veri paylaşması ve birbirleriyle iletişim kurabilmesi için bir standart gereklidir. ANSI kod seti, daha eski ASCII yedi-bit kod setinin bir uzantısıdır.
American Standart Fortran	American Standart Fortran, ilk standart programlama dilidir ve Fortran 66 olarak da adlandırılmaktadır. ANSI, 1966 Mart'ında bu standart dili yayınlamıştır.
ANSI C	ANSI, 1989'da C programlama dilinin standart bir sürümü olarak ANSI C'yi yayınlamıştır.

organizasyon, Avrupa çapındaki kuruluşlar ve vatandaşlar için gizlilik ve güvenliği uygulamak için standartlar önermektedir. TC CYBER tarafından yayınlanan herhangi bir sonuç Avrupa merkezli olmasına rağmen büyük olasılıkla Avrupa organizasyonlarının çok ötesinde etkilere sahip olacak ve etkileyecektir.

ISO 17799 (Geri çekilmiş)

ISO 17799, eski bir uluslararası güvenlik standardıdır ve geri çekilmiştir. Geri çekilmedi, çünkü bir şey yanlıştı. Aslında çok iyi kabul edildi ve başarılı oldu ve tamamen güncellendi ve yeni bir isimle yeni bir standart haline geldi. Bir sonraki bölümde yeni standart hakkında bilgi edineceksiniz. ISO 17799'un orijinal biçimi çok önemli bir bilgi güvenlik standardı olduğu için onu anlamak önemlidir. Bu standart, bilgi sistemlerinde en iyi uygulamaları temsil eden kapsamlı bir denetimler setini belgelemektedir. Standart aslında iki ayrı bölümden oluşur:

- ISO 17799 uygulama kodu
- Bilgi güvenliği yönetim sistemi için BS 17799-2 spesifikasyonu

Standartın temel amacı, iş ortamlarındaki bilgi sistemleri için gerekli güvenlik kontrollerini belirlemektir. Standart, başlangıçta "DTI Uygulama Kodu (*DTI Code of Practice*)" olarak İngiltere'de ortaya çıktı ve daha sonra BS 7799 olarak yeniden adlandırıldı. Denetim için aşırı basit yaklaşımı ve esnek olmaması nedeniyle uluslararası popülerlik kazanamadı. Geliştiriciler, standardın zayıf yönlerini ele almak için 1999 yılında 2. sürümünü yayımladılar. Geliştiriciler, standardı akreditasyon ve yayınlanması için ISO'ya sundu. ISO, standardı 2000 yılında ISO 17799 olarak yayınladı.

Standarda ilgi hızla arttı. Birçok şirket, ISO 17799'u uygulamaya yardımcı olmak için araçlar ve hizmetler sağlamaya başladılar. Hızlı bir şekilde en etkili bilgi güvenliği standardı haline geldi. ISO 17799, pek çok kuruluşa güvenlik politikalarını oluşturmak için bir çerçeve sundu. Standart ile tam uyum hızlı bir şekilde bir hedef haline geldi. Aynı zamanda, rakipler arasında da bir farklılık haline geldi. Standart, potansiyel müşterilerin kuruluşları verilerin güvenliğini sağlamaya yönelik çabaları konusunda değerlendirmelerine olanak sağladı.

ISO standardı 10 temel bölüme ayırmıştır:

- **Güvenlik Politikaları**—Yönetim yönünün bir açıklaması.
- **Güvenlik Organizasyonu** —Bilgi güvenliği yönetimi veya bilgi güvenliğinin nasıl yürütüleceği.
- **Varlık Sınıflaması ve Denetim**—Bilgi varlıklarını sınıflandırmak ve yönetmek için prosedürler.
- **Personel Güvenliği**—Personeli koruyan ve sınırlayan güvenlik denetimleri için rehberlik
- **Fiziksel ve Çevresel Güvenlik**—Bilgisayar tesislerinin korunması.
- **İletişim ve Operasyon Yönetimi**—Sistemlerdei ve ağlardaki teknik güvenlik denetimlerinin yönetimi.
- **Erişim Denetimi**—Ağ kaynaklarına, uygulamalara, işlevlere ve verilere erişim haklarını sınırlayan denetimler.
- **Sistem Geliştirme ve Bakım**—Uygulamalara güvenlik dahil etmek ve tasarlamak için yönergeler.

- **İş Sürekliliği Yönetimi**—İşle ilgili kritik süreçleri ve sistemleri koruma, bakım ve kurtarma.
- **Uygunluk**—Bilgi güvenliği politikalarına, standartlarına, kanunlarına ve düzenlemelerine uygunluğun sağlanması.

ISO/IEC 27002 adlı daha yeni bir standart, ISO 17799'un yerini almıştır. Büyüklüğe, endüstrisine veya konuma bakmaksızın tüm kuruluşlar tarafından erişilebilir kapsamlı bir bilgi güvenliği standardı sağlamaktadır. ISO/IES 27002, geri çekilen ISO 17799'un yerini almış olsa da, önde gelen bilgi güvenliği standardı olduğundan ISO 17799'a yapılmış olan referansları yine de göreceksiniz.

ISO/IEC 27002

ISO/IEC 27002, ISO 177999 standardının güncellemesi olarak 2005'te ortaya çıkmıştır. 2007'de ISO ismini orijinal ismi olan ISO 17799:2005'ten ISO/IEC 27002:2005'e değiştirmiştir. Bu, diğer 27000 serisi ISO/IEC standartlarında kullanılan isimlendirme kuralına uymak içindir. ISO/IEC 27000 serileri, giderek büyüyen genel bilgi güvenlik standartları ailesidir. ISO/IEC 27002 "Bilgi Güvenliği Yönetimi için Uygulamanın Bilgi Teknolojileri Güvenlik Teknikleri Kodu (*Information Technology Security Techniques Code of Practice for Information Security Management*)"dur.

ISO/IEC 27002, kendisinden öncekiler gibi, kuruluşlara bilgi güvenliği yönetimi konusunda en iyi uygulama önerilerini sunmaktadır. Standart, önerilerini bilgi güvenliği yönetim sistemlerinden sorumlu yönetim ve güvenlik personeline yönlendirmektedir. Bilgi güvenliği, CIA üçlü grubu kapsamında bir standarttır:

- **Gizlilik (*Confidentiality*)**—Veriye sadece yetkili kullanıcıların erişebilmesinin ve diğer hiç kimsenin erişememesinin garantilenmesi.
- **Bütünlük (*Integrity*)**—Veriyi sadece yetkili kullanıcıların değiştirebilmesinin ve diğer hiç kimsenin değiştirememesinin garantilenmesi.
- **Kullanılabilirlik (*Availability*)**—Bilgi talep edildiğinde sadece yetkili kullanıcıların bilgilere erişim sağlandığının garantilenmesi.

ISO/IEC 27002, iki yeni bölüm ekleyerek ve diğerlerini yeniden organize ederek eskisini genişletmektedir. ISO yeni standardı 12 ana bölüme ayırmaktadır:

- **Risk Değerlendirmesi**—Riskleri tanımlama ve sınıflandırma için formel yöntemler.
- **Güvenlik Politikası** —Yönetim yönünün bir açıklaması.
- **Bilgi Güvenliği Organizasyonu**—Bilgi güvenliğinin yönetilmesi veya bilgi güvenliğinin nasıl yürütüleceği.
- **Varlık Yönetimi**—Bilgi varlıklarını elde etmek, sınıflandırmak ve yönetmek için kullanılan prosedürler.
- **İnsan Kaynakları Güvenliği**—Bir organizasyona katılmak, ayrılmak veya bir organizasyon içinde taşınmak için güvenlik yönergeleri.
- **Fiziksel ve Çevresel Güvenlik**—Bilgisayar tesislerinin korunması.
- **İletişim ve Operasyon Yönetimi**—Sistemler ve ağlardaki teknik güvenlik kontrollerini yönetmek.
- **Erişim Denetimi**—Ağ kaynaklarına, uygulamalara, işlevlere ve verilere erişim haklarını sınırlayan denetimler.

- **Bilgi Sistemleri Kazanımı Geliştirme ve Bakım**—Uygulamalara güvenlik tasaralamak ve eklemek için yönergeler.
- **Bilgi Güvenliği Ayrıcalıklı Olay Yönetimi**—Bilgi güvenliği ihlallerini önceden görme ve uygun yanıtı verme.
- **İş Sürekliliği Yönetimi** —İşle ilgili kritik süreçleri ve sistemleri koruma, bakım ve kurtarma.
- **Uygunluk**— Bilgi güvenliği politikalarına, standartlarına, kanunlarına ve düzenlemelerine uygunluğun sağlanması.

Standart, her bölümde önerilen güvenlik kontrollerini belirlemekte ve özetlemektedir. Çoğu kişi, bilgi güvenliği denetimlerini en iyi uygulamalar olarak görmektedir. Bu en iyi uygulamalar, her bir amaca ulaşmak için yöntemler sağlamaktadır. ISO/IEC 27002, önerilen kontrollerin her birinin uygulanması için de rehberlik sağlamaktadır.

NOT

ISO/IEC 27002 hakkında daha fazla bilgiyi ISO'nun resmi web sayfasının yer aldığı *www.iso.org/iso/catalogue_detail?csnumber=50297* adresinde bulabilirsiniz.

Ödeme Kartı Endüstrisi Veri Güvenliği Standardı

Ödeme Kartı Endüstrisi Veri Güvenliği Standardı (*Payment Card Industry Data Security Standard* - PCI DSS), ödeme kartlarını içeren alışverişleri işleme konusunda uluslararası bir standarttır. Ödeme Kartı Endüstrisi Güvenlik Standartları Konseyi (*The Payment Card Industry Security Standards Council* - PCI SSC), standardı geliştirmekte, yayınlamakta ve korumaktadır. PCI DSS şimdiye kadar gördüğünüz diğer standartlardan farklıdır. Dünyanın en büyük ödeme kartı üreticilerinden bazıları PCI DSS'i oluşturmuştur. Bu satıcılar aşağıdaki gibidir:

- Visa
- MasterCard
- Discover
- American Express
- Japan Credit Bureau

Bu kuruluşların her biri, ödeme kartı bilgilerini korumak için kendi standardına sahipti. Bu kuruluşlar çalışmalarını birleştirdiler ve PCI DSS'in ilk sürümünü Aralık 2004'te yayınladılar. En son sürüm olan PCI DSS 3.2 sürümü, Nisan 2016'da piyasaya sürülmüştür. Ödeme kartı kullanıcılarını dolandırıcılıktan korumak ve sektördeki yasal gereksinimlerini önceden belirlemek için PCI DSS oluşturuldu. İşleme, iletilme ve saklanma sürecinde ödeme kartı ile ilgili tüm bilgileri korumak için kontrol katmanları gerekmektedir. Standart, ödeme kartı işleme sürecinin herhangi bir aşamasına katılan tüm kuruluşlar için uygundur.

PCI DSS standartlarına uymak, üye kuruluşlardan herhangi biriyle iş yapmak için bir ön şarttır. Herhangi bir kuruluş PCI DSS standartlarını ihlal ederse, ödeme kartlarını işleme özelliğini kaybedebilir. Çoğu durumda uyumsuzluk, cezalar ve/veya daha sık yapılan denetimler ile sonuçlanmaktadır. Sıradan suçlular işlem ayrıcalıklarının iptal edildiğini görebilirler. Ödeme almaya aracı olarak ödeme kartlarına bağımlı olan çoğu kuruluş için uygunluk bir iş gereksinimidir.

Bir kuruluşun uyması gereken kurallar, kuruluşun işlem yaptığı ödeme kartı işlemlerinin sayısına bağlıdır. Kuruluşlar uygunluğu en az yılda bir kez değerlendirirler. Büyük hacimli işlemleri yapan kuruluşların uygunluğu, bağımsız bir nitelikli güvenlik değerlendiricisi (*qualified security*

TABLO 12-6 PCI DSS kontrol hedefleri ve gereksinimleri.

KONTROL HEDEFİ	GEREKSİNİM
Güvenli bir ağ ve sistemler kurun ve bakımını yapın.	Kart sahibinin verilerini korumak için bir güvenlik duvarı yapılandırması kurun ve bakımını yapın. Sistem şifreleri ve diğer güvenlik parametreleri için sağlayıcı tarafından sağlanan varsayılan değerleri kullanmayın.
Kart sahibinin verilerini koruyun.	Saklanan kart sahibine ait verileri koruyun. Açık, ortak ağlardaki kart sahibi verilerinin iletimini şifreleyin.
Güvenlik açığı yönetim programı sağlayın.	Kötü amaçlı yazılımlardan genellikle etkilenen tüm sistemlerde antivirüs yazılımını kullanın ve düzenli olarak güncelleyin. Güvenli sistemler ve uygulamalar geliştirin ve muhafaza edin.
Güçlü erişim denetim ölçütleri uygulayın.	Kart sahibi verilerine erişimi, iş gereksinimine göre kısıtlayın. Bilgisayar erişimi olan her kişiye benzersiz bir kimlik (ID) atayın. Kart sahibi verilerine fiziksel erişimi kısıtlayın.
Düzenli olarak ağları izleyin ve test edin.	Ağ kaynaklarına ve kart sahibi verilerine olan tüm erişimi takip edin ve izleyin. Güvenlik sistemlerini ve süreçlerini düzenli olarak test edin.
Bir bilgi güvenliği politikası uygulayın.	Bilgi güvenliğini ele alan bir politika sağlayın.

NOT

PCI DSS hakkında daha fazla bilgiyi PCI Güvenlik Standartları Konseyi'nin resmi sayfası olan www.pcisecuritystandards.org adresinde bulabilirsiniz.

assessor - QSA) tarafından değerlendirilmelidir. Daha küçük hacimlerde işlem yapan kuruluşlar, bir PCI DSS özdeğerlendirme anketi (*self-assesment quastionnaire* - SAQ) kullanarak kendi kendini belgelemeyi seçebilirler.

PCI DSS 3.2 sürümü, uygunluk için **kontrol hedefleri** olarak adlandırılan altı gruba ayrılmış 12 gereksinimi tanımlamaktadır. **TABLO 12-6,** 12 PCI DSS kontrol hedeflerini ve gereksinimlerini listelemektedir.

BÖLÜM ÖZETİ

Bazı kuruluşlar, teknik özellikleri veya kurallar, yönergeler veya özelliklerin tanımları olarak kullanılmak üzere diğer spesifik kriterleri belgeleyen standartları tanımlamaktadır. Kuruluşlar ve sektördeki firmalar da ürünlerin ve hizmetlerin tutarlı olmasını sağlamak için standartları kullanmaktadırlar. Farklı kuruluşlardan farklı ürünlerin birlikte çalışabilmesi standartlara bağlıdır. Bilişim teknolojisi endüstrisi ilerledikçe, yeni ve güncellenmiş standartlara olan ihtiyaç da artmaktadır. Bu bölümde bazı standart organizasyonlarını ve bilgi güvenliğini doğrudan etkileyen bazı standartları öğrendiniz. Bu standart organizasyonlarını araştırın ve çalışmalarıyla tanışın. Muhtemelen onları tekrar göreceksiniz.

ANAHTAR KAVRAMLAR VE TERİMLER

American National Standards *American National Standards Institute (ANSI)* - Amerikan Ulusal Standartlar Enstitüsü (ANSI)

Control objectives – Kontrol hedefleri

Electrotechnology – Elektroteknoloji

International Electrotechnical Commission (IEC) - Uluslararası Elektroteknik Komisyonu (IEC)

International Organization for Standardization (ISO) - Uluslararası Standardlar Teşkilâtı (ISO)

International Telecommunication Union (ITU) - Uluslararası Telekomünikasyon Birliği (ITU)

Internet Engineering Task Force (IETF) - İnternet Mühendisliği Görev Gücü (IETF)

ISO 17799 – ISO 17799

ISO/IEC 27002 – ISO/IEC 27002

ITU Telecommunication Sector (ITU-T) - ITU Telekomünikasyon Sektörü (ITU-T)

National Institute of Standards and Technology (NIST) - Ulusal Standartlar ve Teknoloji Enstitüsü (NIST)

Recommendations - Öneriler

Request for comments (RFC) – Yorumlar için istek (RFC)

Standards - Standartlar

World Wide Web Consortium (W3C) – World Wide Web Konsorsiyumu

BÖLÜM 12 DEĞERLENDİRME

1. İlk sayısal bilgisayarlar deneysel standartların bir sonucudur.
   A. Doğru
   B. Yanlış

2. Hangi standart kuruluşunun adı *eşit* kelimesinin Yunanca karşılığından gelmektedir?
   A. IEC
   B. ISO
   C. PCI
   D. W3C

3. Hangi standartlar kuruluşu 1906'da kuruldu ve piller için standartları yönetmektedir?
   A. IEC
   B. ISO
   C. PCI
   D. W3C

4. Hangi standart kuruluşu CGI, HTML ve XML gibi standartları yayınlamaktadır?
   A. IEC
   B. ISO
   C. PCI
   D. W3C

5. IETF öncelikle ..... internet protokol paketinin standartları üzerine odaklanmaktadır.

6. IETF ..... adında belgeler üretmektedir.

7. Aşağıdakilerden hangisi en çok bilinen ISO standardıdır?
   A. OSI Referans Modeli
   B. TCP/IP protokolü
   C. TCP/IP Referans Modeli
   D. OSI protokolü

8. ..... teknolojinin ilerlemesi için dünyanın en büyük meslek derneğidir.

9. Hangi standart kuruluşu 802.11g standardını yayınlamıştır?
   A. ISO
   B. IEC
   C. ITU-T
   D. IEEE

10. American Standard Fortran'ı hangi standart kuruluşu yayınlamıştır?
    A. IEEE
    B. ANSI
    C. ITU-T
    D. NIST

BÖLÜM

13 Bilgi Sistem ve Eğitimi

Bilgi sistemleri güvenliği veya siber güvenlik uzmanı olmak istiyor olabilirsiniz. Birinci iş olarak kurumunuzun altyapısının kullanılabilirliğinden, gizliliğinden ve bütünlüğünden emin olmalısınız. Ayrıca, kurumunuzun hassas verisinin gizliliğinden ve mahremiyetinden de emin olmalısınız. Bu, üst düzeyde bir sorumluluk, yetki ve güven gerektirmektedir. Bilgi teknolojilerini bilmelisiniz. Kuruluşun BT ve BT güvenlik politikalarını, standartlarını ve prosedürlerini de bilmeniz gerekmektedir. Teknoloji her gün değişir. Riskler, tehditler ve güvenlik açıkları da. Eğitim, bu hızlı değişimlerle güncel kalmak için kritik öneme sahiptir. Bu becerilere olan talep artmaya devam etmektedir. İstihdam edilen adayların istikrarlı bir şekilde tedarik edilmesi kritik öneme sahiptir. Adayların doğru eğitim geçmişine sahip olmaları gerekmektedir. Daha da önemlisi, güvenlik önlemlerini ve kontrollerini uygulamak için gerekli olan pratik beceri setlerine sahip olmalıdırlar. Bu bölümde, bilgi sistemleri güvenliği veya siber güvenlik öğretim ve eğitim fırsatları hakkında bilgi edineceksiniz. Buna ek olarak, bir bilgi sistemleri güvenlik uzmanı olarak iş görevlerinizi gerçekleştirmek için gerekli olan pratik beceri setlerini nereden edinebileceğinizi öğreneceksiniz.

13. Bölüm Konular

Bu bölüm aşağıda verilen konuları ve kavramları içermektedir:

- Kendi kendine öğrenme eğitim programlarıyla bilgi sistemleri güvenliği nasıl öğrenilir
- Sürekli eğitim programlarından hangilerinin uygun olduğu
- Hangi lise sonrası eğitim programlarının uygun olduğu
- Hangi bilgi sistemleri güvenlik eğitimi programlarının uygun olduğu
- Güvenlik farkındalığı eğitiminin ne olduğu ve neyi içermesi gerektiği

13. Bölüm Hedefler

Bu bölümü tamamladığınız zaman, yapabilecekleriniz:

- Bilgi sistemleri güvenliğinde kendi kendine öğrenim eğitim programlarını tanımlama
- Bilgi sistemleri güvenliğinde bulunan sürekli eğitim programlarını bulma
- Bilgi sistemleri güvenliği konularındaki lise sonrası eğitim programlarını karşılaştırma
- Hangi kuruluşların bilgi sistemleri güvenlik eğitimi programları sunduğunu tanımlama
- Bir kuruluşun güvenlik farkındalığı programlarını tanımlama

Kendi Kendine Çalışma Programları

Bilgi sistemleri güvenliğini öğrenmenin en kolay ve en hızlı yolu kendinize öğretmektir. Bilgisayarlar, yazılımlar ve internet taramaları ile yüksek bir konfor düzeyine sahip olmak tipik bir ön şarttır. Birçok bilgi sistemleri güvenliği ve siber güvenlik kaynakları hem çevrimiçi hem de kitap şeklinde mevcuttur ancak bunları bulmak konusunda yetenekli olmalısınız. Yerel kitabeviniz muhtemelen bilgi sistemleri güvenliği veya siber güvenlik konularını kapsayan birçok kitap ve dergi bulundurmaktadır. Aslında, seçiminizi sadece birkaç taneye indirgemeyi zor bulabilirsiniz.

Eğitiminizi bilgi sistemleri güvenliği veya siber güvenlik ortamında sürdürmeye başlamadan önce, kendi kendine çalışmanın sizin için en iyi yaklaşım olup olmadığını değerlendirmeniz gerekmektedir. Kendi kendine çalışma çok uygun maliyetli ve uygun bir seçenek olabilir ancak her durumda en iyi çözüm olmayabilir.

İlk olarak, kendi kendine çalışma veya kendi kendine öğrenmenin avantajlarından bazılarını dikkate alın:

- **Kendini motive etme**—Kendini motive eden bir kişiyseniz ve kendi bilgisayarınızın önünde uzun saatler çalışabilirseniz, bilgi sistemleri güvenliği ve siber güvenlik sizin için olabilir. Sonuçta, bilgisayar korsanları ve failleri, bilgisayarlarında saldırı planlama ve seçilen hedefler üzerinde keşif ve port tarama yapmak için sayısız saat harcıyorlar. Saldırılarını önlemeyi öğrenmek için eşit zaman harcanmalıdır.
- **Düşük maliyet**—Açık kaynaklı araçların ve uygulamaların, kamuya açık alanlarda, uygulamalı laboratuvarlar ve beceri hazırlığı için hazır olduğu göz önüne alındığında, kendi kendine çalışma genellikle en ucuz eğitim seçeneğidir. Hedeflerinizi karşılamak için yalnızca gerekli malzemeleri almalısınız. Bütçenize en uygun malzemeleri seçebilirsiniz. Bazı kendi kendine çalışma materyalleri ücretsiz olarak mevcuttur. Kendi bilgi sistemleri güvenliği veya siber güvenlik test laboratuvarınızı kurarsanız, ağ donanımları, bilgisayarlar, RAM, depolama ortamı ve yüksek hızlı internet bağlantısı satın almak da gerekebilir. Laboratuvar sistemlerinizi sanallaştırmanız maliyetlerinizi düşürür.
- **Esnek materyaller**—Kendi kendine çalışma ile en çok sevdiğiniz kaynak materyallerini seçersiniz. Farklı insanlar farklı şekillerde öğrenirler. Bir video dersini tercih edebilirsiniz, oysa bir başkası basılı bir kitabı tercih edebilir. Her iki durumda da, kendi kendine çalışma size öğrenme stilinize en uygun kaynakları bulma seçeneği sunmaktadır.
- **Esnek zaman çizelgesi**—Zaman çizelgeniz için en iyi çalıştığınız zaman çalışabilirsiniz. Bazı insanlar sabahları daha iyi çalışır; diğerleri akşamları daha iyi çalışır. Kendi kendine çalışma seçeneği, hangi çalışma programının sizin için en iyi sonucu verdiğine karar vermenizi sağlamaktadır.
- **Kişisel hız**—Kendiniz yaparken, hızı ayarlamanız gerekmektedir. Kendi kendine çalışma seçeneği, eğitim materyalini ne kadar hızlı tamamlayacağınızı seçmenize izin vermektedir. Bazı konuları yavaş ve bazılarını daha hızlı keşfetmeniz gerekebilir. Bir diğer avantaj ise, gerekiyorsa geri dönüp bir konuya tekrar bakabilmenizdir.
- **Ek materyaller**—Kimse her alanda uzman değildir ve hiçbir alan tek bir uzman tarafından öğretilmemektedir. Herhangi bir konuda öğrencilerin çoğu, bir defa ya da daha fazla ek materyalden yararlanırlar. Kendi kaynaklarınızı seçtiğinizde, ek malzemeleri ne zaman kullanacağınıza karar verebilirsiniz. Birincil materyallere ilişkin ilk arama, ihtiyacınız olduğunda ve gerektiğinde size iyi ek malzemeler için bir fikir verecektir.

Kendi kendine çalışma seçeneğinin seçilmesinde bazı dezavantajlar da vardır. Kişisel çalışmaların sizin için doğru olup olmadığını belirlerken bu endişeleri de dikkatlice göz önünde bulundurun:

- **Erteleme**—Kendi kendine çalışmanın en yaygın tuzaklarından biri erteleme şeklindedir. Zamanınız üzerinde çok fazla talep vardır; incelemek için harcanacak zamanı ayırmanız çoğu kez zordur. Dahası, kendi kendine çalışmanın planladığınızdan daha fazla zaman aldığını görebilirsiniz. Programa devam etmek için disiplin ve kararlılığa ihtiyacınız olacaktır. Kendi zamanınız üzerinde çalıştığınızda, bir çalışma programına ne kadar sadık kalacağınızı ciddi olarak düşünmelisiniz.
- **Kaynak seçimi**—Kendi kaynaklarınızı seçmek bir avantaj olabilmesine rağmen, aynı zamanda bir dezavantaj da olabilir. Kaynağın değerini gerçekten çalışmadan öğrenmek çok zordur. Bazı kaynaklar ilk bakışta harika görünür ancak ihtiyacınız olan derinliğe veya değere sahip değildir. Kullanabileceğiniz çok sayıda seçenek, en iyi ürünleri tanımlama sürecinizi zorlaştırabilir.
- **Etkileşim eksikliği**—Kendi kendine çalışma, tek yönlü bir öğretim tekniğidir. Diğer öğrencilerden veya eğitmenlerden geribildirim alamazsınız. Başkaları ile öğrenmeyi seviyorsanız, kendi kendinize çalışma sizin için en iyi seçenek olmayabilir. Çoğu kişi etkileşimden faydalanmalarına rağmen, diğer seçeneklerin verdiği rahatsızlık ve masraflar sizi kendi kendine çalışmaya zorlayabilir.
- **Kalite**—Çoğu kendi kendine çalışma kaynakları, özellikle düşük maliyetli öğrenci pazarını hedef alır. Diğer bir deyişle, sınırlı bütçeleri karşılamak için düşük maliyetli ürünlerdir. Bu, bu ürünlerin iyi olmadığı anlamına gelmez; sadece yüksek maliyetli ürünlerle aynı görünüşe sahip olmadıkları anlamına gelir. Bazı durumlarda, kalite maliyetle doğrudan ilgilidir. Bununla birlikte, çok iyi ucuz kaynaklar vardır ve sınırlı değeri olan pahalı kaynaklar vardır. Satın aldığınız malzemelere dikkatlice bakın.
- **Onaylanmış sonuç**—Güvenlik konularını öğrenmek için yalnızca kendi kendinize çalışma yapıyorsanız, doğrulama sizin için bir endişe kaynağı olmayabilir. Bununla birlikte, bir çalışma alanını başarıyla tamamladığınıza dair doğrulama almak iyidir. Diğer eğitim yöntemlerinin çoğu, bir çeşit değerlendirme ve doğrulama sürecini içerir. Kendi kendine çalışma böyle bir sürece sahip değildir. Onayınız, öğrendiklerinizi gösterme becerinizdir. Bu bir sertifika sınavını geçmek veya başlamadan önce daha fazla bilgi ve beceriye sahip olmak olabilir.

Kendi kendine çalışmayı sürdürmeye karar vermenin bir başka önemli özelliği, çalışmanızın amacı üzerinde karar vermektir. Bir konuyu incelemek istediğiniz özel nedenler, size en iyi yaklaşımı seçmenize yardımcı olabilir. Çoğu durumda, aşağıdakiler de dahil olmak üzere en az bir nedenden dolayı bir çalışma şeklini izleyeceksiniz:

- **Genel bilgi**—Büyük resmi anlamak için genel güvenlik bilgisi gerekmektedir. Güvenlik, BT altyapısının tüm alanlarını ve BT altyapısının dışındaki bir çok farklı alanı içermektedir. Sonuç olarak, bir güvenlik uzmanının genel güvenlik konularını iyi anlaması gerekmektedir. Uzmanların çoğu, bir veya daha fazla güvenlik alanına odaklanır. Bu uzmanlar, güvenlik işlerinin genel anlayışından daha iyi yararlanabilirler. Buna ek olarak, pek çok güvenlik yöneticisi, belirli güvenlik ayrıntılarının bir komutundan ziyade daha genel bir bilgi setine ihtiyaç duymaktadırlar.
- **Özel bilgi ve beceriler**—Güvenlik görevlerinin çoğu, genel bilgi ve özel alan bilgisi gerektirmektedir. Buna ek olarak, bir görevi yerine getirmek için belirli becerilere ihtiyaç duyabilirsiniz. Örneğin, güvenlik duvarı kurallarını oluşturmak çok karmaşık olabilir. Güvenlik duvarı yapılandırmasının ayrıntılarını ve kuruluşunuzdaki cihazlardaki kuralları nasıl koruyacağınızı bilmeniz gerekmektedir. Genel bilgi, üst düzey bir görünüm için iyidir ancak pratik

uygulayıcılar da özel bilgiye ihtiyaç duymaktadır. Kullandığınız kendi kendine çalışma materyallerinin ihtiyacınız olan konuyu ayrıntılı olarak kapsadığından emin olun.

- **Sertifikasyon hazırlığı**—Kendi kendine çalışma için yaygın olarak kullanılan bir uygulama, bir sertifika sınavına hazırlanmaktır. Bir sertifika sınavına girmek için şartları yerine getirebilir ancak materyali gözden geçirmek ve bilgi eksikliklerinizi gidermek isteyebilirsiniz. Kendi kendine çalışma, bu ihtiyaca tam olarak uyabilir.
- **Beceri seti (*skill-set*) hazırlığı ile uygulamalı laboratuvarlar (*hands-on-labs*)**—İşe alım veya kariyer gelişimi için en önemli ölçütlerden biri, bilgi sistemleri güvenlik uzmanı olarak beceri seti için hazır olduğunu göstermektir. Pek çok kendi kendine çalışma kursu veya eğitim programı, gerçek dünya BT altyapısını taklit eden uygulamalı laboratuvarları gerçekleştirebilecek durumda değillerdir. Bilgi sistemleri güvenliğine ilişkin bilgilerinizi gerçek dünya BT altyapılarına nasıl uygulayacağınızı bilmeniz gerekmektedir. Uygulamalı laboratuvarlarla deneyimsel öğrenmeyi kendi kendine çalışarak öğrenme sürecine dahil ederek, kitap bilgisi sahibi olma ve uygulama yeteneklerinizi netleştirme arasındaki boşluğu doldurabilirsiniz.

BT güvenliği veya bilgi güvenliği eğitimlerinde kendi kendine çalışma için birçok kaynak bulunmaktadır. Bu tam bir liste değildir, ancak başlamanıza yardımcı olabilir. Herkesin kendi kendine alıştırma yapmasının farklı olduğunu unutmayın. Tüm kendi kendine çalışma eğitim programları aynı materyalleri sunmamaktadır.

Kendi kendine öğrenme için en iyi eğitim materyallerini bulmak için aşağıdaki yönergeyi izleyin:

- **Bilinen Kaynaklar**—Herhangi bir web sitesinden kaynak satın almayın. Şirketin iyi bir itibarı olduğundan emin olun. IBM ve Cisco gibi önde gelen ürün şirketleri zaten iyi bir ürün itibarına sahiptirler. Küçük şirketler bu kadar iyi bilinmeyebilir. Hem büyük hem de küçük şirketler ürün eğitimi sunabilirler. Herhangi bir ürün satın almadan önce şirket hakkında yorum ve değerlendirmeler bulmak için biraz araştırma yapın. Sadece çok saygın olumlu müşteri değerlendirmeleri bulunan saygın bir iş yerinden materyal satın almalısınız.
- **Materyal yorumları**—Saygın firmalar bile, ihtiyaçlarınızı karşılamayan eğitim ürünleri satabilir. Her satıcının eleştirilerini kontrol etmenin yanı sıra, ürün yorumlarına da bakın. Satın almak istediğiniz kitap veya kurs için olumlu eleştiriler bulmanız gerekmektedir. Ürün adına basit bir internet araştırması, kalitesiyle ilgili eleştirileri veya yorumları getirmektedir.
- **Birden fazla ürün**—Birden fazla ürün sunan perakendeciler, daha kaliteli eğitim ürünleri üretme eğilimindedir. Bir dizi ilgili ürün geliştirmek ve pazarlamak için önemli bir yatırım gerekmektedir. Ürün yaratıcıları, ilave satışlar üretmek için kalitenin yüksek olmasını istemektedir. Dikkatli olun. Körü körüne miktarın kaliteyle aynı olduğunu varsaymayın. Bazı perakendeciler satabilecekleri her şeyi taşırlar. Şüpheniz olduğunda, ürün ve satıcı değerlendirmeleri için arama yapın.
- **Uygulamalı beceri seti laboratuvarları**—Birçok kendi kendine araştırma eğitim programı, bir laboratuvarda veya sanal laboratuvar olanağı sunmaz; bu nedenle, bu programlar eleştirel bir öğrenme unsuru içermemektedir. Profesyonel bir sertifika sınavı için öğrenmek ve geçmekle ilgileniyorsanız, uygulamalı beceri setlerine ihtiyacınız olmayabilir. Yeni bir beceri seti öğrenmeye ve bilgi sistemleri güvenliği veya bilgi güvencesi görevlerini yerine getirme deneyimine ihtiyaç duyuyorsanız, eğitim programınızın laboratuvar faaliyetlerini içerdiğinden emin olun. Kendi bilgi sistemleri güvenliği veya siber güvenlik test laboratuvarınızı kurmanız gerekecektir. Kendi siber güvenlik laboratuvarınıza sahip olduğunuzda, bilgisayar korsanları ve

nobel

> **NOT**
>
> Bilgisayar korsanlarının kullandığı her araç ve uygulama, bir bilgi sistemleri güvenliği veya siber güvenlik uzmanının kullanmayı öğrenmesi gereken bir araç ve uygulamadır. Etik bir bilgisayar korsanı olarak, bilgisayar korsanlarının hangi araçları ve uygulamaları kullandığını öğrenmek zorundasınız, böylece bu araç ve uygulamalar tarafından üretilen IP paketlerini ve IP trafiğini nasıl önleyeceğinizi öğreneceksiniz. Herhangi bir uygulama laboratuvarının parçası olması gereken açık kaynak veya ücretsiz araçlar ve uygulamalar genellikle Wireshark® (www.wireshark.org), Nmap® (*https://nmap.org*), Meta Sploit™ (*www.metasploit.com*) ve Kali Linux® penetrasyon test araçlarını (https://tools .kali.org) içermektedir.

failleri ile mücadele etmek için gerekli olan uygulamalı becerileri setini edinebilirsiniz.

TABLO 13-1, kendi kendine çalışma kaynaklarının sınırlı bir listesini içermektedir. Bir internet araması birçok ilave kaynak üretecektir. "Bilgi güvenliği eğitimi" veya "siber güvenlik eğitimi" için arama yapmayı deneyin. Çeşitli eğitim kuruluşlarının yanı sıra kendi kendine çalışma materyalleri için genel kullanıma açık içerikten de birçok seçenek bulacaksınız.

Kişisel çalışmanın sizin için iyi bir seçenek olup olmadığı durumunuza bağlıdır. Bir karar vermeden önce bütçenizi, zamanlamanızı, öğrenme stilinizi ve deneyiminizi göz önünde bulundurun. Kendi kendine çalışma, gitmek için tek yol değildir. İlerleyen bölümlerde güvenlik öğretimi ve eğitimleri için diğer seçenekler hakkında bilgi edineceksiniz.

Eğitmen Tarafından Yönlendirilen Programlar

Kendi kendine öğrenmeye bir alternatif, eğitmenlerin yönlendirdiği bir sınıfta eğitimdir. Birçok okul ve üniversite, yerel topluluk işgücünü geliştirme sürecinin bir parçası olarak sürekli eğitim programlarını tanıtmakta ve pazarlamaktadır. Devam eden eğitim grubu, okulun bir parçası olabilir veya yakından ilgili bir eğitim birimi olabilir. Bazı durumlarda, aslında üniversitedeki bölümlerden biridir. Sürekli eğitimin amacı, diploma değil, bir sertifikaya veya mesleki sertifikaya götüren resmi eğitim kursları sağlamaktır. Çoğu durumda, öğrencilerin diplomaları zaten vardır ve becerilerini ve bilgilerini güncellemek istemektedirler. Kurslar, çok genel, çok özel ve teknik olmak üzere çeşitlilik gösterebilir. Bu kurslar, topluluk üyelerinin aşağıdakileri de içeren çeşitli ihtiyaçlarını karşılamaktadır:

- Lisans programlarına hazırlık sınıfları
- Yetişkinler için derslere destek
- Çocuklar ve gençler için yaz stajı kampı tarzı sınıflar
- Mesleki eğitim
- Sertifikasyon hazırlığı

Listelenen son kategori hem güvenlik hem de diğer birçok öğretim alanlarını kapsamaktadır. Sürekli eğitim kursları genellikle yetişkin öğrencilerin ihtiyaçlarını karşılamaya çalışmaktadır. Çoğu erişkin öğrencinin işi olduğundan, devam eden birçok eğitim sınıfının akşamları veya hafta sonları bir araya geldiklerini göreceksiniz.

Sertifika Programları

Sürekli eğitim programları, **bitirme sertifikasına (*certificate of completion*)** ulaşılan genellikle bir akşam eğitim programının bir parçası olarak sunulur. Bitirme sertifikası, programın tamamlanmasının ardından bir öğrenciye verilen ve eğitmen tarafından imzalanmış bir belgedir. Bitirme belgesi, dersi tamamladığınızı ve bir değerlendirmede yeterli puanı aldığınızı belgelemektedir.

TABLO 13-1 BT güvenliği kendi kendine çalışma kaynakları.

KAYNAK	YORUMLAR
Satıcıya özel eğitim	Satıcıya özel kendi kendine eğitim eğitim programları, Cisco Systems veya Microsoft gibi satıcısına veya üreticisine bağlı olarak değişmektedir. Cisco Systems çevrimiçi e-öğrenme özdeğerlendirme programları, *https://learningnetwork.cisco.com/index.jspa* adresindeki Cisco Öğrenme Ağı (*Cisco Learning Network*) aracılığıyla sunulmaktadır. Microsoft çevrimiçi e-öğrenme kendi kendine çalışma programları, internet erişimi olan herhangi bir yerden, her zaman kullanılabilir. Daha fazla bilgiyi *https://www.microsoft.com/en-in/learning/default.aspx* adresinde bulabilirsiniz. Bu kapsamlı kurslar ve klinikler, uygulamalı sanal laboratuvarlar ve ilerlemenizi izleme yeteneği gibi etkileşimli özellikler sunar.
YouTube eğitimi	YouTube'un bilgisayar korsanları, failleri, güvenlik eğitimcileri, eğitim uzmanları ve profesyoneller tarafından yüklenen gerçek eğitim videoları bulunmaktadır. Saldırı topluluğunun paylaştığı şeylerle savaşmak isterseniz, tüm dünyadaki bilgisayar korsanları tarafından yüklenen yüzlerce "How to hack..." videolarını arayın, incelediğiniz her bir "hack" videosu için bir bilgi sistemi güvenlik ve siber güvenlik önlemi oluşturun. YouTube'daki sesli anlatım ile eğitim videolarını izleyerek, "How to hack" ve "How to secure" ile ilgili bilgi edinebilirsiniz.
SANS Enstitüsü kendi kendine çalışma	SANS Enstitüsü (*www.sans.org/selfstudy/*), bağımsız çalışmaktan zevk alan öğrenciler için kendi kendine çalışma eğitim programları sunmaktadır. Kurslar; ders kitabı ve MP3 ses ve video dosyalarıyla ve/veya diğer ders metaryelleri ile takviyeli bir CD-ROM içermektedir. Bazı dersler, uygulamalı laboratuvarları gerçekleştirmeleri için gerekli olan, VMWare® gibi sanal makinelerin kullanımını içermektedir; böylece öğrenciler el becerilerini geliştirmeye yönelik çalışabilirler.
Jones & Bartlett e-öğrenme	Bu metnin yayıncısı olan Jones & Bartlett Learning, *www.issaseries.com* adresindeki çevrimiçi e-öğrenme, Bilgi Sistemleri Güvenlik ve Güvencesi (*Information Systems Security&Assurance* - ISSA), müfredatını sunmaktadır. 12 ISSA kursunun her biri kendi kendine çalışma, çevrimiçi, e-öğrenme kursu olarak satın alınabilir. ISSA kendi kendine çalışma ve canlı sanal öğretim eğitimi çözümleri ayrıca *www.security-evolutions.com* adresindeki Security Evolutions, Inc. aracılığıyla da edinilebilir.
Cybrary	*www.cybrary.it* adresinden bulunabilen Cybrary, canlı bir eğitmen tarafından sesli anlatımlı video kaydı içeriği ile kendi kendine çalışma olanağı sunmaktadır. Temel, orta ve ileri bilgi sistemleri güvenliği, siber güvenlik ve mesleki sertifika hazırlığına yönelik içerik bulunmaktadır. Canlı sanal eğitmenle diyalog veya etkileşim yoktur. İçerik, alanında yeni başlayanlar için iyi bir tanımlama ve başlangıç noktası sağlamaktadır.
(ISC)²® kendi temposu ile e-öğrenme	(ISC)² kişisel tempolu e-öğrenme, CISSP® kendi temposu veya SSCP® kimlik bilgisi için CBK® İnceleme Seminerlerine (*Review Seminars*) dayanmaktadır. Bu e-öğrenme çözümleri, e-öğrenme eğitmeninin önderliğindeki bir etkinlikle birleştiğinde en etkili çözümdür; ancak kendi kendine çalışma olarak alınabilirler. Örneğin, (ISC)² kişisel tempolu e-öğrenme programı, 30, 60 veya 90 günlük abonelik ile kendi kendine çalışma için kullanılabilir. Bu dinamik e-öğrenme kursları anlatımlı dersler ve alıştırmalar içermektedir ve Certification Partners, Inc. tarafından verilmektedir. Tüm e-öğrenme teklifleri, sürekli mesleki eğitim kredileri (CPE'ler) için uygundur.
Kitapevi	Yerel kitabevinizi ziyaret edin veya çevrimiçi (örneğin *www.amazon.com* veya *www.barnesandnoble.com*) kitapevlerine gidin ve "bilgi sistemleri güvenliği" ve "siber güvenlik" başlıklarına göz atın. En son bilgileri ve güncellemeleri içerdiğinden emin olmak için her kitabın yayın tarihini kontrol edin.
Kütüphane	Yerel kütüphaneniz, bilgi sistemleri güvenliği veya siber güvenlik başlıkları veya yayınları olabilir, ancak çoğunlukla güncel olmayan materyaller bulunmaktadır. Kütüphanenizdeki kaynakları arıyorsanız, materyalin en son sürümüne ve en son yayınına sahip olduğunuzdan emin olun.

Bitirme belgesi ile mesleki sertifika arasındaki fark, bitirme belgesinin sadece dersleri aldığınızı ve görevleri ve ödevleri tamamladığınızı ifade ettiğini unutmayın. Profesyonel bir sertifika, bir iş-görev analizi gerektirir ve yasal olarak savunulabilir olması için sertifika sınavından geçme notu alınmasını gerektirmektedir.

Sertifika programları genellikle eğitim kurumuna özgüdür. Farklı okullarda benzer programların farklı gereksinimleri olabilir. Her kurum kendi teslim yöntemini de belirlemektedir. Hem geleneksel sınıfları hem de çevrimiçi teklifleri içeren harmanlanmış programları da oldukça sık görülmektedir. Bir sertifika programı sizi ilgilendiriyorsa, yerel kolejlerinize ve üniversitelerinize başvurarak başlayın. Bir çok sürekli eğitim sağlayıcısı, yerel işverenlerin ve diğer kuruluşların ihtiyaçlarını karşılayan sınıflarından emin olmak için her konudaki uygulayıcılarla yakın işbirliği içinde çalışmaktadırlar. Yerel kuruluşlarda aldığınız sınıfların, yerel kuruluşlar tarafından teşvik edilen belirli içeriği sağladığını görebilirsiniz. Bu, yerel şirketlerin ihtiyaç duyduğu ve istediğiniz belirli bilgi ve becerileri kazanmanıza yardımcı olabilir.

Bir çok sürekli eğitim sağlayıcısı çevrimiçi programlara sahip olduğundan, aramanızı yerel sağlayıcılarla sınırlamanız gerekmemektedir. Bir internet araması size hemen hemen her ilgi alanı için birçok devam eden eğitim teklifi gösterecektir. "bilgi güvenliğinde sürekli eğitim (*continuing education in information security*)" ifadesini arayın. Sertifika programları sağlayan birçok kurum bulacaksınız.

Sürekli Eğitim Programları

Sürekli eğitim programları, bir sertifikaya götürmeyen kursları da içermektedir. Uygulayıcıları güncel ve bilgilendirici tutmak için birçok kurs bulunmaktadır. Bu kurslara genellikle **sürekli mesleki eğitim (*continuing professional education* - CPE) veya sürekli mesleki gelişim (*continuing professional development* - CPD)** kursları denir. Bu kurslar genellikle seçtikleri alanda çalışan uygulayıcıları hedef almaktadır. Sertifikaların birçoğu sertifikasyon sahiplerinin sertifikalarını güncel tutmak için her yıl ilave eğitim almalarını gerektirir. Ek eğitim gerektiren sertifikalar genellikle her sertifikanın gerektirdiği kredilerin sayısını belirtir. Bir sertifika sahibi minimum kredi sayısını kazanamazsa sertifikayı kaybedebilir.

NOTE

Aldığınız her sertifikasyon için CPE gerekliliklerini not edin ve kazandığınız CPE'leri takip edin. Çoğu sertifikayı muhafaza etmek için her yıl CPE'ye ihtiyacınız olacaktır.

Sürekli eğitimin geçerliliğinin onaylama sürecini kolaylaştırmak için çoğu kurum, kurslar için standart bir birimde kredi sunmaktadır. Kurumlar, her kursa CPE değeri atamaktadır. Her bir CPE kredisi 50 dakikalık sınıf eğitimini göstermektedir. Öğrenciler kazanabilecekleri CPE kredilerinin sayısına göre ders seçebilirler. Sertifika alan öğrenciler bir kursun tamamlandığını kanıtlayabilir ve daha sonra CPE'leri sertifikasyon bakım gereksinimlerine göre talep edebilirler.

UYARI

Bir çalışma programını seçmeden önce, programın **akredite edilmiş** olup olmadığını araştırın. Çoğu olası işveren, akredite edilmiş programları, yetersiz olanlardan daha çok değer vermektedir. Akreditasyon, Eyalet Eğitim Müdürlüğü (*State Department of Education*) tarafından okulun bulunduğu eyalette verilmektedir.

Sürekli eğitim programı, yeni bilgileri takip etmek ve sertifikaları güncel tutmak için mükemmel bir yoldur. Hangi dersleri sunduklarını öğrenmek için yerel kolejlerinize veya üniversitelerinize başvurun. Sürekli eğitim kursu tekliflerini ararken, çevrimiçi arama yapmayı da unutmayın. Aradıklarınızı sadece bir çevrimiçi derste de bulabilirsiniz. Sadece çevrimiçi kurslar arıyorsanız, yerel kolejlerinizin ve üniversitelerinizin dışında da bakabilirsiniz.

Lise Sonrası Eğitim Programları

Üniversiteler ve kolejler ayrıca, bilgi sistemleri güvenliği, siber güvenlik veya bilgi güvencesi ile ilgili derece programları da sağlamaktadır. İki yıllık ön lisans, dört yıllık lisans ve iki yıllık yüksek lisans programları sunan kolej ve üniversitelerin sayısı hızla artmaktadır. Buna hem kar amacı gütmeyen okullar hem de akredite edilmiş lisans programları sunan kar amacı gütmeyen okullar dahildir. Bugün iki yıllık ön lisans programlarından doktora düzeyine (PhD) kadar değişen dereceler için örgün eğitim, çevrimiçi eğitim ve ikisini birlikte harmanlayan eğitim programlarını ve ders yazılımlarını bulabilirsiniz. Bilgi sistemleri güvenliği, siber güvenlik veya bilgi güvencesi alanında bir derece düşünüldüğünde, hangi kariyer olanaklarını ve istihdamı öncelikle aradığınızı düşünün.

Herhangi bir üniversite veya kolej, eyaletin eğitim kurulu müfredatı için akreditasyonu aldıktan sonra bilgi sistemi güvenliği veya siber güvenlikle ilgili lisans programı sunabilmektedir. Siber Uzayı Güvenleştirmek için Ulusal Strateji (*National Strategy to Secure Cyberspace*), kaliteli güvenlik eğitimi sunan ve ilgili araştırmaları yapan eğitim ve araştırma kurumlarını tanımak için Şubat 2003'te bir program çağrısında bulunmuştur. Bu stratejiye yanıt olarak, Ulusal Güvenlik Teşkilatı (*National Security Agency* - NSA) ve ABD Ulusal Güvenlik Bakanlığı (*Department of Homeland Security* - DHS) ortaklaşa iki önemli programı desteklemektedir:

- **Bilgi Güvenliği Eğitiminde Ulusal Akademik Mükemmellik Merkezleri (*The National Centers of Academic Excellence in Information Assurance Education* - CAE/IAE) programı** *(https://www.nsa.gov/resources/educators/centers-academicexcellence/cyber-defense/)*—CAE/IAE programı, programın bilgi güvenliği eğitim yönergelerini karşılayan eğitim kurumlarını tanımlamaktadır.
- **Araştırmada Akademik Mükemmellik Ulusal Merkezleri (*The National Centers of Academic Excellence in Research* - CAE/R) programı**—Aynı URL'de bulunan CAE/R programı, araştırma yönergelerine uyan kurumları belirtmektedir.

NSA web sitesine göre "Bu programların amacı, bilgi güvenliğindeki (*information assurance*- IA) yüksek öğrenim ve araştırma envanterini teşvik ederek ve çeşitli disiplinlerdeki IA uzmanlığıyla giderek artan profesyonel üreterek ulusal bilgi altyapımızdaki kırılganlığı azaltmaktır."

NSA, Siber Operasyonlar Programı (*Cyber Operations Program*) için Ulusal Akademik Mükemmellik Merkezlerini (*National Centers of Academic Excellence* - CAE) kurmuştur. Birçok kolej ve üniversite, bilgi güvenliği derecesi programlarını çeşitli NSA standartlarına göre belgelendirmiştir. CAE programı, Siber Güvenlik Eğitimi Ulusal Girişimi (*National Initiative for Cybersecurity Education* - NICE): Dijital Bir Ulus Oluşturma (*Building a Digital Nation*)'yı desteklemektedir.

İstenen Mükemmellik Merkezi (*Center of Excellence*) adını elde eden kolejler ve üniversiteler, ülkenin siber güvenlik alanındaki işgücünü yetiştirme konusundaki kararlılığını göstermektedirler. Bu iki program, birlikte, ülkenin en iyi bilgi güvenliği derecesi programları ve lisans üstü araştırmalarını belirlemektedir. NSA'nın arzulanan CAE/IAE veya CAE/R atamasını elde etmek, müfredat ve araştırma kurumlarının, NSA tarafından tanımlanan standartları karşıladığı veya bunları aştığı anlamına gelmektedir. Onay süreci, müfredat öğrenme hedeflerini NSA'nın siber güvenlik görevleri için çeşitli bilgi sistemleri güvenliği ve bilgi güvenliği standartlarına sıkı bir şekilde eşleştirmeyi gerektirmektedir. Akademi veya Araştırma için Mükemmellik Merkezleri (*Centers of Excellence for*

NOT

Siber güvenlik içeriklerini, NSA CAE içerik eşleme gereksinimlerine uygun şekilde eşleşmiş olan akredite edilmiş lisans programlarının bir listesi *https://www.iad.gov/nietp/reports/current_cae_designated_institutions.cfm* adresinden bulunabilir.

Academia or Research) listesi, NSA programlarına eşdeğer lisans programları sunan üniversitelerin ve kolejlerin tam listesini sunmaktadır. Bilgi sistemleri güvenliği veya bilgi güvencesi derecesi programlarıyla ilgilenen öğrenciler araştırma yapmalıdır.

Ön lisans Derecesi

Birçok kurumun sunduğu derecelerden biri de önlisans derecesidir. Bu derece en erişilebilir olanıdır çünkü genellikle iki yıllık bir programı temsil eder. Bazı kurumlar, öğrencilerin iki yıldan kısa bir sürede mezun olmasına izin veren hızlandırılmış programlar sunmaktadır. Her iki durumda da, ön lisans, dört ya da daha fazla yıl okula harcamadan bilgi güvenliği alanına girmek isteyen insanlar için temel bir eğitim sağlamaktadır. Bu programlar sizi BT ve bilgi güvenliği alanındaki giriş seviyesi pozisyonlar için hazırlayabilir. **TABLO 13-2**, çeşitli kurumlar tarafından sunulan ön lisans programlarını sunmaktadır.

Farklı kurumlar farklı türlerde önlisans dereceleri sunmaktadır. Birkaç isim vermek için, bir fen bilimi ön lisansına (*associate of science* - AS), teknik sanatlar ön lisansına (*associate of technical arts* - ATA) veya uygulamalı bilimler ön lisans (*associate of applied sciences* - AAS) derecesine sahip olabilirsiniz. Hem örgün hem de çevrimiçi derece programlarını her seviye için bulabilirsiniz.

Lisans Derecesi

Lisans derecesi, bir çok kurumun önereceği bir sonraki derece seviyesidir. Standart lisans programı, dört yıllık lisans programıdır. Bununla birlikte, birçok kurum dört yıldan daha kısa bir süre içinde bitecek şekilde derece gereksinimlerini tamamlamak için hızlandırılmış programlar sunmaktadır. Lisans derecesi, giriş seviyesi pozisyonlar dışındaki herhangi bir bilgi güvenliği pozisyonu için genellikle şarttır. Aslında, bazı giriş seviyesi pozisyonlar bile en az bir lisans derecesi gerektirmektedir.

Birçok lisans programı bulunmaktadır. Bazı lisans programları bilgi genişliğine odaklanır; diğerleri ise bilgi derinliğine odaklanır. Genel olarak, liberal sanat enstitüleri ve daha büyük üniversiteler genişliğe odaklanan programlar sunmaktadır. Teknik kurumlar ise genellikle daha çok derinlik üzerine odaklanırlar. Kurumlar tarafından sunulan çeşitli lisans programlarını göz önünde bulundurun ve derece gereksinimlerini karşılamak için alacağınız kursları karşılaştırın. Profesyonel hedeflerinize uyan bir program bulun.

Diğer lisans programlarında olduğu gibi hem örgün hem de çevrimiçi çalışma programları sunan kurumlar bulabilirsiniz. Çevirmiçi çalışma için geçerli olan terim uzaktan öğrenme yöntemidir. Bu türden bir çalışma sizi ilgilendiriyorsa, çevrimiçi olarak "bilgi güvenliği uzaktan öğrenme programları (*information security distance learning degree programs*)"nı araştırmayı deneyin. Birçok seçenek olduğunu göreceksiniz.

Birkaç farklı lisans türünü takip edebilirsiniz. Seçenekler fen bilimleri lisansı (*bachelor of science* - BS veya BSc), bilgi teknolojisi biliminde lisans (*bachelor of science in information technology* - BScIT), uygulamalı bilim lisansı (*bachelor of applied science* - BASc) ve teknolojinin lisansı (*bachelor of technology* - B.Tech) olabilir. Programlar, almanız gereken dersler ve lisans programlarının odaklandığı konu bakımından farklılık göstermektedir. Örneğin, B.Tech derecesi muhtemelen çoğunlukla teknik derslerden oluşacak iken, bir BS derecesi büyük bir olasılıkla daha geniş bir konu yayımına odaklanacaktır. Yine, planlarınıza en uygun çalışma programını seçin. **TABLO 13-3**, çeşitli kurumların sunduğu lisans programlarından bazılarını listelemektedir.

TABLE 13-2 Siber güvenlik ağırlıklı önlisans derece programları.

KURUM	TANIM
ITT Teknik Enstitüsü	ITT, bilgisayar ağı yönetiminde çevrimiçi ve örgün olarak verilen iki yıllık ön lisans derecelerini sunmaktadır. Program, TCP/IP ve bilgisayar ağı konularını kapsamaktadır. Öğrenciler bu konuları sınıf teorisi ve uygulamalı laboratuvarlar aracılığıyla araştırırlar. Daha fazla bilgi için www.itt-tech.edu/programs/ adresini ziyaret edin.
Strayer Üniversitesi	Strayer Üniversitesi, çevrimiçi ve örgün olarak bilgi sistemleri dereceleri sunmaktadır. Daha fazla bilgi için www.strayer.edu/academic-program-finder/associate adresini ziyaret edin.
Herzing Üniversitesi	Herzing Üniversitesi, bilgisayar bilimlerinde çevrimiçi ve örgün olarak önlisans derecelerini sunmaktadır. Daha fazla bilgi için, *www.herzing.edu/career-programs/undergraduate-degrees/technology* sayfasını ziyaret edin.
Northern Virginia Community College (NOVA)	Northern Virginia Community College iki yıllık AAS siber güvenlik derecesi sunmaktadır. "Bu müfredat, siber güvenlik alanında (bilgi güvenliği), şu an BT alanında veya güvenlik alanında da çalışan ve bilgilerini artırmak ve becerilerini yenilemek isteyenler için ve bilgi güvenliği alanındaki bilgi ve becerilerle diğer alanlardaki kişilerin kendilerini geliştirmesi için tasarlanmıştır. Müfredat, NOVA'nın Akademik Mükemmellik Merkezi olarak belirlenmesi için gerekli olan NSA/DHS Bilgi Birimleriyle eşleştirilmektedir. " Daha fazla bilgi için http://www.nvcc.edu/cybersecurity/cae.html adresini ziyaret edin.
Edmonds Community College	Edmonds Community College, bilgisayar bilgi sistemleri, bilgi güvenliği ve adli bilişim (digital forensics) alanında çevrimiçi ve örgün önlisans derecelerini sunmaktadır. Daha fazla bilgi için http://*catalog.edcc.edu/content.php?catoid=14&navoid=*5902 adresini ziyaret edin.

Yüksek Lisans Derecesi

Bir sonraki akademik derece yüksek lisans derecesidir. Yüksek lisans programı, lisans derecesi programının bir ileri seviyesine geçmektedir. Genellikle lisans derecesinden sonra iki yıllık bir çalışmadan oluşur. Bazı kurumlar, öğrencilerin iki yıldan daha kısa bir sürede yüksek lisans derecesini kazanmalarını sağlayan hızlandırılmış programlar sunmaktadır. Yüksek lisans derecesi, sahibinin bilgi güvenliği uygulayıcılarının genel bilgilerinden daha derin bir bilgi düzeyine sahip olduğunu göstermektedir.

Yüksek lisans programları genellikle bir çalışma alanına özgüdür. Bir yüksek lisans programına girdiğinizde, zamanınızın çoğunu belirli bir çalışma alanına odaklanarak harcarsınız. Bu seviyedeki programlar bilgi genişliğine değil, bilgi derinliğine odaklanmaktadır.

Birkaç farklı yüksek lisans derecesi vardır. Bunlar arasında; fen bilimleri yüksek lisansı (*master of science* - MS veya MSc), bilgi teknolojisi yüksek lisansı (*master of science in information technology* - MScIT) ve işletme yüksek lisansı (*master of business administration* - MBA) bulunmaktadır. Bu seviyedeki lisans programlarında kesin bir fark bulunmaktadır. Temel fark, MS ve MBA dereceleri arasındadır. Her birinin farklı bir odağı bulunmakta ve farklı bir öğrenci grubuna hitap etmektedir.

Yüksek lisans derecesi –MS, MSc ve MScIT- bilgi güvenliğinin teknik yönlerine odaklanmaktadır. Başka bir deyişle, bu dereceler güvenlik uygulayacıları için uygundur.

TABLO 13-3 Siber güvenlik ağırlıklı lisans programları.

KURUM	TANIM
ITT Teknik Enstitüsü	ITT Tech, bilgi sistemleri güvenlik ve bilgi sistemleri ile siber güvenlik alanlarında çevrimiçi ve örgün olarak verilen BS dereceleri sunmaktadır. Daha fazla bilgi için *www.itt-tech.edu/programs/* adresini ziyaret edin.
Capella Üniversitesi	Capella Üniversitesi, bilgi güvenliği ve güvenlik uzmanlığı için çevrimiçi BS dereceleri sunmaktadır. Capella Üniversitesi, NSA ve Homeland Security ünvanlarını almıştır. Daha fazla bilgi için, *www.capella.edu/business-technology-degrees/undergragraduate/programs/* adresini ziyaret edin.
George Washington Üniversitesi	George Washington Üniversitesi (GWU), önlisans veya teknik olmayan derecesi olan öğrenciler için siber güvenlik alanında BS derecesi sunmaktadır. Daha fazla bilgi için *https://cps.gwu.edu/cybersecurity-bachelors* adresini ziyaret edin.
Kaplan Üniversitesi	Kaplan Üniversitesi, güvenlik ve adli tıp konularına odaklanma imkânı ile bilgi teknolojisinde çevrimiçi BS dereceleri sunmaktadır. Daha fazla bilgi için *http://www.kaplanuniversity.edu/programs/bachelors-degrees.aspx* adresini ziyaret edin.
Maryland Üniversitesi/Üniversite Koleji	Maryland Üniversitesi/Üniversite Koleji siber güvenlik yönetimi ve politikaları, bilgisayar ağları ve siber güvenlik ve yazılım geliştirme ve güvenlik bölümlerinde BS derece programı sunmaktadır. Her bölüm, kariyer hedeflerinize ulaşmanıza yardımcı olmak için tasarlanmıştır. Daha fazla bilgi için, *www.umuc.edu/cybersecurity/academics/bachelors-degrees.cfm* ziyaret edin.
Southern New Hampshire Üniversitesi	Southern New Hampshire Üniversitesi'nin çevrimiçi BS dereceleri, BT güvenliği, bilgi güvenliği veya adli tıp konularını içermektedir. Bilgi Teknolojileri alanında çevrimiçi BS derecesinde siber güvenlik alanında, siber saldırılara karşı ağları ve bilgi sistemlerini savunmayı ve korumayı kapsamaktadır. Daha fazla bilgi için *http://www.snhu.edu/online-degrees/bachelors/bs-in-information-technologies /cyber-security* adresini ziyaret edin.
Phoenix Üniversitesi	Phoenix Üniversitesi, çevrimiçi ve örgün olarak verileri Bilgi Teknolojileri BS derecelerini sunmaktadır. Bu BT dereceleri; BT güvenliği, bilgi güvenliği veya adli bilişim konularını içermektedir. Daha fazla bilgi için *www.phoenix.edu/programs/degree-programs/technology/bachelors/bsit-iss.html* adresini ziyaret edin.
Strayer Üniversitesi	Bilgi sistemlerinde çevrimiçi ve örgün olarak verilen BS dereceleri, adli bilişim, siber güvenlik ve ulusal güvenlik alanlarında özel konularda sunulmaktadır. Daha fazla bilgi için, *www.strayer.edu/degree/bachelors-degree/bachelor-science-information-systems/* adresini ziyaret edin.

Pratik ortamda çalışmak ve güvenlikle ilgili çalışmalar yapmak istiyorsanız, bu dereceler iyi seçimler olabilir. Bu tür derece programları, BT altyapısının nasıl çalıştığını ve uygun güvenlik kontrollerini nasıl tasarlanacağını ve uygulanacağını ayrıntılı olarak anlatmaktadır. Yüksek lisans programları, sizi bilgi güvenliği alanına girmeye ve sistemleri güvence altına almaya hazırlamaktadır. **TABLO 13-4**, çeşitli kurumlar tarafından sunulan bazı yüksek lisans programlarını listelemektedir.

TABLO 13-4 Siber güvenlik yüksek lisans programları.

KURUM	TANIM
SANS Enstitüsü	SANS Enstitüsü, çevrimiçi, kendi kendine çalışma ve örgün olmak üzere bilgi teknolojisi dereceleri sunmaktadır. SANS, öğrencilerin iletişim, proje yönetimi, öğretim, rehberlik ve ikna becerilerini geliştirmelerini sağlamaktador. Daha fazla bilgi için *www.sans.edu* adresini ziyaret edin. Not: Sahada çok saygı gören SANS, Maryland Eyaleti tarafından yüksek lisans derecesi vermeye yetkilidir.
Capella Üniversitesi	Capella, Ulusal Güvenlik Teşkilatı (*National Security Agency*) tarafından Bilgi Güvenliği Eğitiminde Ulusal Akademik Mükemmellik Merkezi (*National Center of Academic Excellence in Information Assurance Education* - CAE/IAE) olarak seçilen seçkin dört yıllık akademilerden ve yüksek lisans düzeyindeki üniversitelerden biridir. Buna ek olarak Capella, belirli güvenlik konularına sahip benzersiz MS programları sunmaktadır. Daha fazla bilgi için, *http://www.capella.edu/online-information-technology-degrees/masters-programs/* adresini ziyaret edin.
Kaplan Üniversitesi	Kaplan Üniversitesi, bilgi güvenliği ve güvencesi alanında uzmanlaşmak için siber güvenlik alanında çevrimiçi bir MS derecesi sunmaktadır. Daha fazla bilgi için, *www.kaplanuniversity.edu/informationtechnology/cybersecurity-management-master-degree.aspx* adresini ziyaret edin.
Phoenix Üniversitesi	Phoenix Üniversitesi çevrimiçi ve örgün olarak MS yönetim bilgi sistemi (*management information system* - MIS) derecelerini sunmaktadır. Bu program bilgi güvenliği veya siber güvenlik seviyelerini içermektedir. Daha fazla bilgi için *www.phoenix.edu/programs/degreeprograms/technology/masters/mis.html* adresini ziyaret edin.
Southern New Hampshire Üniversitesi	Southern New Hampshire Üniversitesi, bilgi güvenliği konusunda bilgi teknolojisinde çevrimiçi bir MS derecesi sunmaktadır. Öğrenciler, ağ düzeyinde güvenlik politikalarını nasıl uygulayacaklarını ve bir kuruluşun BT altyapısını nasıl düzgün bir şekilde güvence altına alacağını öğrenmektedirler. Daha fazla bilgi için, *www.snhu.edu/campus-majors/graduate/ms-information-technology/information-security/* adresini ziyaret edin.
Strayer Üniversitesi	Strayer Üniversitesi, bilgisayar güvenlik yönetimi veya bilgisayar adli bilişim yönetimi konularında çevrimiçi ve örgün olarak bilgi sistemleri MS derecelerini sunmaktadır. Daha fazla bilgi için, *www.strayer.edu/degree/masters-degree/information-systems/* adresini ziyaret edin.
Liberty Üniversitesi	Liberty Üniversitesi, ağ ve güvenlik konularına sahip bilgi teknolojisi alanında çevrimiçi bir yüksek lisans derecesi sunmaktadır. Daha fazla bilgi için, *www.liberty.edu/online/degree/master/information-technology-network-design-and-security/* adresini ziyaret edin.

İşletme Yüksek Lisansı

İşletme yüksek lisans programı (*master of business administration* - MBA), bilgi sistemleri güvenliği sürecini yönetmeye odaklanmaktadır. Lisans programları öğrencileri bilgi güvenliği çalışmaları yapmaya hazırlarken, MBA programları öğrencileri bilgi güvenliğindeki insanları ve çevreyi yönetmeye ve bakım altına almaya hazırlamaktadır. Bilgi güvenliği alanlarında MBA derecesine sahip olan bir kişi, bilgi güvenliği veya BT gruplarını yönetmeye hazırlanacaktır. Herhangi bir teknik ortamı yönetmek için gerekli beceriler, teknik işi yapmak için gerekli becerilerden farklıdır. Ayrı bir derece programı, öğrencileri kendi seçtikleri alana girmeye hazırlar. **TABLO 13-5**, çeşitli kurumlar tarafından sunulan bazı MBA derecelerini listelemektedir.

TABLO 13-5 Siber güvenlik alanında işletme yüksek lisans programları.

INSTITUTION	DESCRIPTION
George Washington Üniversitesi	George Washington Üniversitesi, siber güvenlik alanında uzmanlaşmış bir global MBA sunmaktadır. Alanın en üst kademelerindeki uzmanlar, sorumluluk ve yasal yönetimlerden bilgi güvencesi teknolojisi ve uygulamalarına kadar kendileri ile en çok ilgili olan siber güvenlik boyutlarına odaklanarak programa kayıtlı öğrencilere eğitim vermektedir. Daha fazla bilgi için, *http://business.gwu.edu/brave-new-world-of-cyber-security/* adresini ziyaret edin.
Ferris State Üniversitesi	Ferris State Üniversitesi'nin Bilgi Güvenliği ve İstihbarat (*Information Security and Intelligence*) Programı Yüksek Lisans Programı iş zekası kariyeri, proaktif ve reaktif olay tepkisi ve güvenli uygulamalar kullanarak proje yönetiminde kariyer için öğrencileri hazırlamaktadır. Daha fazla bilgi için, *www.ferris.edu/business/program/misi/* adresini ziyaret edin.
James Madison Üniversitesi	James Madison Üniversitesi, bilgi güvenliği ile MBA derecesi sunmaktadır. Bu MBA derecesi sadece öğrencilere tüm iş ilkelerinde sağlam bir temel sağlamaz, aynı zamanda bilgi güvenliğinin iş sonuçlarına ilişkin güçlü bir anlayışa sahip olmalarını da sağlamaktadır. Daha fazla bilgi için, *www.jmu.edu/academics/graduate/programs/business-administration.shtml* adresini ziyaret edin.
DeVry / Keller İşletme Okulu	Keller Üniversitesi, bilgi güvenliği konusunda yoğunlaşmış, çevrimiçi ve örgün olarak verilen bir MBA sunmaktadır. MBA Bilgi Güvenliği programında, bilgi koruma, saldırı tespiti, güvenlik prosedürleri ve hukuksal ve etik düşünceler gibi günümüz iş dünyasındaki giderek daha önemli rolünü yerine getirmek için aranan beceri ve bilgileri öğrencilere sunmak üzere tasarlanmıştır. Daha fazla bilgi için, *www.keller.edu/graduate-degree-programs/mba-program/mba-in-information-security.html* adresini ziyaret edin.

Doktora Programı

En yüksek akademik derece doktora derecesidir. Bu derece, en saygın akademik seviyeyi temsil eder ve elde edilmesi en zor olan akademik derecedir. Bir doktora programı, yüksek lisans için gerekli olan çalışma seviyesinden daha da ileri seviyeye gitmektedir. Derecenin türüne bağlı olarak, şartlar normal olarak titiz ders çalışma ve sahaya anlamlı bir katkıda bulunan kapsamlı araştırma içermektedir. Diğer derecelerin aksine, doktora dereceleri belirli bir süreyi içermemektedir. Birçok doktora programı üç ila beş yıl arası sürmektedir ancak derece tamamlamak için standart bir zaman çizelgesi yoktur.

Doktora derecesi, seçilen bir çalışma alanındaki kapsamlı eğitimi değerlendirecek kişiyi tanımlamaktadır. Bu kişi, özel yetenek ve bakış açısı gerektiren düzeyde çalışabilme kabiliyetine sahip olacaktır. Bilgi güvenliği alanında doktora derecesine sahip kişiler çoğunlukla araştırma, büyük kurumsal bilgi güvenliği yönetimi veya akademik roller üstünde çalışırlar.

Akademik, teknik veya yönetim tercihinize bağlı olarak çeşitli doktora programları mevcuttur. Bilgi güvenliği alanlarında mevcut doktora derecelerinin bazıları, bilim doktorası (*doctor of science* - Dsc), bilgi teknolojileri doktorası (*doctor of information technology* - DIT), teknoloji doktorası (*doctor of technology* - DTech) ve en çok tanınan doktora derecesi olan felsefe doktorasıdır (*doctor of philosophy* - PhD) . Bu seviyede bile, kurumlar hem çevrimiçi hem de geleneksel

TABLO 13-6 Doktora derecesi programları.

KURUM	TANIM
Capella Üniversitesi	Capella Üniversitesi, bilgi güvenliği konusunda çevrimiçi bir PhD programı sunmaktadır. Bu PhD programı, bilgi güvenliği uzmanlığınızı kariyerinize uyacak şekilde ilerletmek için tasarlanmıştır. Bilgi gizliliği, bütünlük, denetim, uygunluk ve risk yönetimi gibi konularda ileri seviyede beceri geliştirme ve doktora araştırması için fırsatlar sunmaktadır. Daha fazla bilgi için, *www.capella.edu/online-degrees/phd-information-assurance-security/* adresini ziyaret edin.
Colorado Teknik Üniversitesi	Colorado Teknik Üniversitesi (*Colorado Technical University* - CTU) bilgi güvenliği konusunda bilgisayar bilimlerinde çevrimiçi bir PhD programı sunmaktadır. CTU programı, bu alandaki gelecekteki sorunları ve gelişmeleri yönetmek ve tahmin etmek için gerekli olan teorik, araştırma ve uygulama yeteneklerini geliştirmeye yardımcı olmak için tasarlanmıştır. Öğrencilere, önemli bir sorunun araştırılması ve seçilmesi, daha sonra sonuçların iletilmesi ve yayınlanmaya hazırlanması ile bilgi güvenliği alt disiplininde uzmanlık göstermesi konusunda eğitim vermektedir. Daha fazla bilgi için *www.coloradotech.edu/degrees/doctorates/computer-science/information-assurance/* adresini ziyaret edin.
Dakota State Üniversitesi	Dakota State Üniversitesi, veri toplama, yazılımların kullanılması, kötü amaçlı kod analizi ve tersine mühendislik de dahil olmak üzere siber işlemler faaliyetlerinde uzmanlaşmış bilgi güvencesinde çevrimiçi bir PhD programı sunmaktadır. Bu teknolojiler istihbarat, askeri ve kolluk kuvvetleri ile diğer veri odaklı sanayilerdeki işverenler için kritik öneme sahiptir. Daha fazla bilgi için *http://dsu.edu/graduate-students/dsccs/* adresini ziyaret edin.
Northcentral Üniversitesi	Northcentral Üniversitesi, bilgisayar ve bilgi güvenliğine odaklanarak, işletme yönetimi alanında çevrimiçi bir PhD programı sunmaktadır. Uzmanlık; adli bilişim ve kanıt taşıma, federal ve devlet gizliliği, fikri mülkiyet, arama ve nöbet süreci ve siber suçlarla ilgili en iyi uygulamaları geliştirmeye odaklanmaktadır. Daha fazla bilgi için, *www.ncu.edu/school-of-business-and-technology/doctor-of-business-administration/computer-and-information-security/* adresini ziyaret edin.
Nova Southestern Üniversitesi	Nova Southeastern Üniversitesi, bilgi güvenliği konusunda çevrimiçi ve örgün olarak verilen bir PhD programı sunmaktadır. Bu doktora programı; iş dünyasında ve endüstride olmak üzere, mezunlarını akademik alanda, iş dünyasında ve endüstride olmak üzere, kilit pozisyonlar için hazırlayan kapsamlı, federal, eyalet ve yerel yönetim kurumlarında, çok disiplinli bir araştırma programıdır. Müfredat hem teknik olarak yoğun hem de yönetim odaklı güvenlik kurslarını, bilgi güvenliği/bilgi güvenliği çalışmasına kapsamlı bir yaklaşımla birleştirir. Daha fazla bilgi için, *http://cec.nova.edu/doctoral/dia/index.html* adresini ziyaret edin.

yapılarda programlar sunmaktadır. **TABLO 13-6** farklı kurumlar tarafından sunulan doktora derecesi programlarının bazılarını listelemektedir.

Bilgi Güvenliği Eğitim Programları

Geleneksel eğitim programları normalde çeyrek veya yarıyıl boyunca bir çok bilgiyi öğrenen öğrencilere odaklanmaktadır. Bazı programlar uygulamalı becerileri tanıtırken, eğitim kurumları konuları tam olarak kapsamaya odaklanır. Bunlar, öğrencilerin kararların ve konuların arkasındaki nedenleri

anlamalarını istemektedirler. Bazen tüm öğrenciler beceri kazanmak ya da çok özel bilgi edinmek istemektedirler. Güvenlik eğitim programları bu ihtiyacı birçok farklı seçenekle doldurmaktadır.

Genel olarak, güvenlik eğitim programları (*security training programs*), güvenlik öğretim programlarından (*security education programs*), uygulama becerilerine ve sürelerine odaklanmaları açısından farklıdırlar. Öğretim sınıfları genelde birkaç ay boyunca haftada birkaç saat bir araya gelirken, güvenlik eğitim sınıfları genellikle birkaç saatten birkaç güne kadar yoğun oturumlar için bir araya gelmektedirler. Güvenlik eğitim kurslarının temel amacı, bir veya daha fazla beceride öğrencileri hızla eğitmek veya bir veya daha fazla özel alanda gerekli bilgi sağlamaktır. Tam zamanlı çalışanlar, yoğun bir hafta boyunca ders bulabilir; diğerleri sadece, örneğin akşam sınıflarına birkaç haftaya yayılmış olarak katılabilirler. Birçok güvenlik eğitim kursu öğrencileri özellikle sertifika sınavlarına hazırlamaktadır.

Güvenlik Eğitimi Gereksinimleri

Ulusal Standartlar ve Teknoloji Enstitüsü (*National Institute of Standards and Technology* - NIST) 800 Serisi yayınları, bilgi güvenliğini yönetmek için NIST tarafından önerilen tüm prosedürleri kapsamaktadır. Yayınlar ayrıca güvenlik kurallarının uygulanması için yönergeler sunmaktadır. Bu yayınlar, BT ortamlarını güvence altına almak için gerekli olan birçok prosedürü ortaya koymaktadır. Kullanıcıların güvenlik prosedürlerini anladıklarından ve bunları uygulayabileceklerinden emin olmaları açısından eğitim almaları öncemlidir.

ABD Personel Yönetimi Ofisi (*US Office of Personal Management* - OPM), federal kurumların NIST yönergeleri tarafından önerilen eğitimleri sunmasını şart koşmaktadır. Ajansların tüm çalışanlarını eğitmesini ve her çalışanının işe alınma tarihinden itibaren 60 gün içinde tüm yeni çalışanları eğitmesini gerektirir. OPM şartları uyarınca, acenteler aşağıdaki koşullardan herhangi biri meydana geldiğinde de eğitim sağlamalıdır:

- Ajansın BT güvenlik ortamında önemli bir değişiklik bulunmaktadır.
- Ajansın güvenlik prosedürlerinde önemli bir değişiklik bulunmaktadır.
- Bir çalışan hassas bilgilerle ilgilenen yeni bir pozisyona geçmektedir.

Ajanslar ayrıca, belirli aralıklarla periyodik olarak da eğitim vermelidir. Buna ek olarak, yönetmelikler, tüm BT çalışanlarının veya diğer personelin, güvenli BT uygulamalarına ve sistemlerine erişmeden önce uzmanlaşmış bir güvenlik eğitimi almasını gerektirmektedir.

Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (*Health Insurance Portability and Accountability Act* - HIPAA), güvenlik farkındalığını ve eğitimini gerektiren yönergeler de içermektedir. Uygulama tanımlamaları aşağıdakileri içermektedir:

- Bir güvenlik farkındalığı programı hazırlama
- Kötücül yazılımlar ile ilgili eğitim sağlama
- Oturum açma izleme prosedürleri konusunda eğitim sağlama
- Parola yönetimiyle ilgili eğitim sağlama

1987 Bilgisayar Güvenliği Yasası (*Computer Security Act*), NIST ve OPM'nin bilgisayar güvenliği bilinci ve eğitimi için yönerge oluşturmasını şart koşmaktadır. Bu ajansları, bir ajansın işlevsel örgütsel rollerine özgü eğitim vermeye yöneltmiştir. NIST Özel Yayın 800-16, Bilgi Teknolojisi Güvenliği Eğitim Gereksinimleri: Bir Rol ve Performansa Dayalı Model, (*Information Technology Security Training Requirements: A Role- and Performance-Based Model*) bu yönergeleri içermektedir. Bu yayın,

aynı zamanda, bazı kurumların önemli bilgi güvenliği sorumluluklarına sahip farklı kitlelere yönelik eğitim kursları geliştirmek için kullandığı bir metodoloji de içermektedir. Özel Yayın 800-50, Bir Bilişim Teknolojileri Güvenlik Farkındalığı ve Eğitim Programı Oluşturma, (*Building an Information Technology Security Awareness and Training Program*) bilgi güvenliği farkındalığı ve eğitimi ile ilgili bir başka NIST belgesidir. NIST SP 800-50'deki dört ana alan şunlardır:

- **Farkındalık**—Tüm personelin uyanık kalmasına yardımcı olmak için sürekliliği olan bir süreçtir. Buna, kabul edilebilir kullanım politikası (*acceptable use policy* - AUP), hatırlatıcılar, oturum açma banneri, posterler, e-posta mesajları ve personelin güvenliği düşünmesini sağlamaya yönelik diğer teknikler dahil olabilir.
- **Eğitim**—Bir bütün olarak çalışanlara ve işi BT'de olanlara gerekli güvenlik becerilerini ve yeterliliklerini öğretin.
- **Öğretim**—Güvenlik becerilerini ve yeterliliklerini ortak bir bilgi kümesine entegre edin.
- **Profesyonel Gelişim (kurumlar ve sertifikalar)**—Bir değerlendirme veya ölçme kriterini uygulayarak bir standardı karşılayın.

Özdeğerlendirme Anketi (*self-assessment questionnaire* - SAQ) Gereksinimi 12.6 için PCI DSS v3.2 standardı şunu belirtmektedir: "Tüm personelin kartlı veri güvenliği politikası ve prosedürlerinden haberdar olmasını sağlayacak resmi bir güvenlik farkındalığı programı uygulayın." Bu PCI DSS v3.2 gereksinimi yeni işe alma eğitimi ve en azından yıllık güvenlik farkındalık eğitimi güncellemeleri ile desteklenmelidir. Buna ek olarak, PCI DSS v3.2, personelin en az yılda bir kez güvenlik politikası ve prosedürlerini okuduğunu ve anladığını onaylamayı gerektirmektedir.

Bunlar, devam etmekte olan bir güvenlik eğitimi ve farkındalığı programı gerektiren düzenlemelerin sadece birkaç örneğidir. Birçok kurum güvenlik politikasında güvenlik farkındalığını ve eğitimini de içermektedir. Personelinizin güvenlik politikaları ve prosedürlerinden haberdar edilmesinin sağlanması, kuruluşunuz yönetiminin birincil sorumluluğudur. Güvenlik ve eğitim personeli, güvenlik mesajını geliştirebilir ve iletebilir; ancak yönetim, politikalarını ilettiklerinden emin olmakla yükümlüdür.

Tek başına güvenlik eğitimini sağlamak yeterli değildir. Her organizasyon her iş fonksiyonuna özgü eğitim vermelidir. Veri sahipleri gibi bazı iş fonksiyonlarının, yöneticiler gibi diğer iş fonksiyonlarından farklı eğitime ihtiyaçları bulunmaktadır. Tüm personelin iş işlevlerine özel eğitimi almalarını sağlamalısınız.

Güvenlik Eğitimi Kurumları

Bazı kuruluşlar, personelinin ihtiyaç duyduğu düzeyde güvenlik eğitimini sağlayamazlar. Bu gibi durumlarda, güvenlik personeli için gerekli eğitim ve belgelendirme konusunda ayrı güvenlik eğitim organizasyonları önemli bir rol oynamaktadır. Bazı kuruluşlar belirli güvenlik eğitimi verirken diğerleri sertifikasyon programları sağlamaktadır.

Bir çok güvenlik eğitimi sağlayıcı, güvenlik eğitimi sunmaktadır. Eğitim kurumlarında olduğu gibi örgün, çevrimiçi ve önceden paketlenmiş çalışma seçenekleri sunacak sağlayıcılar bulabilirsiniz. Bütçeniz, öğrenme stiliniz ve zamanlamanız için en iyi sonucu veren kurs seçeneğini belirleyin. Sizin için birçok seçenek var, bu nedenle mevcut ürünleri değerlendirmek için biraz zaman ayırın. **TABLO 13-7**, daha büyük olan güvenlik eğitim satıcılarının bazılarını ve bu satıcıların sunduklarını listelemektedir.

Pek çok kaliteli eğitim organizasyonu arasından seçim yapabilirsiniz. Mevcut ders tekliflerine bakmak için her birinin web sitesini ziyaret edin. Muhtemelen ihtiyaçlarınızı karşılayan bir sınıf ve öğrenme şekli bulacaksınız.

TABLO 13-7 Güvenlik eğitimi sağlayıcıları.

SAĞLAYICI	TANIM
SANS Enstitüsü	SANS, dünyanın bilgi güvenliği eğitiminde en büyük ve en güvenilir kaynaklardan biridir. Geliştirme, uygulama, yönetim ve denetleme rollerini kapsayan birçok güvenlik konularında dersler sunmaktadır. SANS kursları yarım gün ila altı gün arasında değişmektedir, küresel olarak mevcuttur ve pratik eğitime odaklanmıştır. Daha fazla bilgi için *www.sans.org* adresindeki SANS web sitesini ziyaret edin.
IT Professional Group, Inc. (ITPG)	ITPG, $(ISC)^2$ olarak bilinen Uluslararası Bilgi Sistemleri Güvenlik Sertifikasyonu Konsorsiyumu (*International Information Systems Security Certification Consortium*) için küresel ve Kuzey Amerika çapında profesyonel sertifikasyon programları sunmakta ve yerine getirmektedir. Daha fazla bilgi için *http://itpg.org* adresindeki ITPG web sitesini ziyaret edin.
InfoSec Enstitüsü	InfoSec Enstitüsü, ABD genelinde düzenli kurslara sahip olan büyük bir güvenlik eğitim organizasyonudur. Amacı, sertifikasyon hazırlığından çok spesifik teknik güvenlik konularına kadar birçok konuda öğrencilere mümkün olan en iyi eğitimi vermektir. InfoSec Enstitüsü'nün *www.infosecinstitute.com* web sitesinde daha fazla bilgi bulabilirsiniz.
Bilgi Sistemleri Denetim ve Kontrol Birliği (ISACA)	ISACA, "bilgi sistemleri için dünya çapında kabul görmüş, endüstri lideri bilgi ve uygulamaların geliştirilmesi, benimsenmesi ve kullanılması"nı destekleyen kâr amacı gütmeyen global bir organizasyondur. Dünya çapında bilgi sistemleri denetimi ve yönetimi ile ilgili konferanslar ve eğitim etkinlikleri bulunmaktadır. Daha fazla bilgi için ISACA web sitesini ziyaret edin: *www.isaca.org*.
Phoenix TS	Phoenix Technology Solutions (Phoenix TS), Maryland, Virginia ve Washington, DC'deki kamu ve ticari kuruluşlara düşük maliyetli, uygulamalı bilgisayar eğitimi, BT sertifikası ve yönetim kursları sunmaktadır. Daha fazla bilgi için *www.phoenixts.com/* adresini ziyaret edin.
Security Evolutions, Inc. (SEI)	SEI, BT güvenliğinde ve bilgi güvencesinde çeşitli profesyonel sertifikasyon programlarının çevrimiçi, e-öğrenme, kendi kendine çalışma ve canlı öğretmen ile anlatım şeklinde programlar sağlamaktadır. Bunlara Security+®, SSCP®, CISSP®, NSA 4011 ve NSA 4013-Advanced dahildir. Daha fazla bilgi için *www.security-evolutions.com/* adresini ziyaret edin.

Güvenlik Farkındalığı Eğitimi

Her kuruluş, sektördeki dikey veya düzenleyici uygunluk yasası koşullarından bağımsız olarak, yeni bir işe alım ve devam eden veya yıllık güvenlik farkındalığı eğitim programına sahip olmalıdır. Bu **güvenlik farkındalığı eğitimi (*security awareness training*)**, bir kuruluşun **güvenlik farkındalığı kampanyasının** bir parçası olmalıdır. Bir güvenlik farkındalığı kampanyası, eğitim, periyodik bültenler veya notlar, "öğle yemeği ve öğrenme" eğitim oturumları ve bir güvenlik politikası ihlalinin sonucu olarak açılan güvenlik olaylarından oluşur. Bir kuruluşun çalışanlarının politikalara, prosedürlere ve onların uyumlarına nasıl tepki verdiğine bağlı olarak, güvenlik farkındalığı eğitiminin artırılması gerekebilir. Unutmayın, Kullanıcı Etki Alanı (*User Domain*), tüm BT altyapısında en zayıf halkayı barındırmaktadır: İnsanlar.

NOT

Kişisel olarak tanımlanabilir bilgi (*personally identifiable information*, PII), çalışanların veya kuruluşun bireysel müşterilerinin mahrem verisidir. Korunan sağlık bilgileri (*protected healthcare information* - PHI), bir bireyin özgün sağlık verileridir.

Aşağıdaki ilkeler, genellikle bir kuruluşun yeni işe alım güvenlik farkındalığı eğitim kursuna dahildir. Bu konular, gereksinime bağlı olarak kabul edilebilir kullanım politikasında (*acceptable use policy* - AUP) ve kuruluşun yıllık güvenlik farkındalığı eğitiminde güçlendirilebilir:

- **Mevzuat gereklilikleri ve kanunlara uygunluk**—Güvenlik farkındalığı eğitimi, genellikle, kuruluşunuzun mevzuata uygunluğu ve bir çalışan olarak yasal gerekliliklerle ilgili konuları içermektedir. Bu, kişisel olarak tanımlanabilir bilgiler (*personally identifiable information* - PII), korunan sağlık bilgileri (*protected health care information* - PHI) veya kart hamili verileri (kredi kartı numaraları) gibi hassas verilerin mevzuata uygunluğunu ve korunmasını içerebilir.
- **Parola Davranışları**—Kuruluşun parola yönetimi politikası ve karmaşık parola gereksinimleri, genellikle yıllık güvenlik farkındalığı eğitiminde gözden geçirilir.
- **Bilgi/veri sınıflandırması, kullanımı ve etiketlenmesi**—Bu, güvenlik farkındalık eğitiminin önemli bir parçası olup, çalışanlara düzenlenmemiş verilere karşı düzenlenmiş hassas veriler için uygun şekilde davranmalarını hatırlatmaktadır.
- **Temiz masa politikaları**—Güvenlik farkındalığı eğitimi, çalışanlara masalarında hassas bilgi ya da belgeler bırakmadan gizlilik sağlamalarını hatırlatmalıdır.
- **Yakında durmayı önleyin**—Çalışanlar, güvenli giriş kapıları veya giriş yollarının tehlikeye atılmaması için arkalarından yaklaşan kişiler hakkında uyarılmalıdır.
- **Kişisel olarak sahip olunan cihazlar**—Dizüstü bilgisayarlar veya akıllı telefonlar gibi kişisel olarak sahip olunan cihazların kullanılmasına izin veren kuruluşlar, yıllık güvenlik farkındalığı eğitiminde kendi cihazını getir (*bring-your-own-device* - BYOD) politikasına uymalıdır.
- **Yeni tehditler ve yeni güvenlik eğilimleri/uyarıları**—Güvenlik farkındalığı eğitimi, çalışanları yeni saldırı yöntemleri, korsanlara ve faillere yönelik eğilimler konusunda eğitmek için iyi bir araçtır.
- **Yeni virüsler (ör. fidye yazılımı (*ransomware*), dosya şifreleme (*cryptolocker*) vb.)**—Güvenlik farkındalığı eğitimi, çalışanları yeni saldırı virüsleri ile fidye yazılımı ve dosya şifreleme yazılımı gibi kötü amaçlı yazılımlar konusunda eğitmek için iyi bir araçtır.
- **Oltalama saldırıları**—Oltalama (*phishing*) e-postaları ve hedeflenen oltalama e-postaları hakkında hatırlatmalar, genellikle yıllık güvenlik farkındalığı eğitiminde bildirilmektedir.
- **Sıfır gün açıkları**—Korunma çözümüne sahip olmayabilecek malware ve kötücül yazılımlar, kuruluşunuzdaki BT varlıklarının üretilmesine engel olabilecek sıfırıncı gün açığına neden olabilir. Sıfırıncı gün saldırıları ve açıkları, genellikle yıllık güvenlik farkındalığı eğitiminde iletilir.
- **Sosyal paylaşım ve uçtan uca iletişim kullanımı**—Her ikisi de AUP ve diğer politika tanımlarında genellikle yasaklanmıştır; bu nedenle, bu konu genel olarak yıllık güvenlik farkındalığı eğitiminde paylaşılmaktadır.

Periyodik güvenlik farkındalığı eğitimi olmadan, çalışanlar gizlilik ve mahremiyet ile ilgili yeni politikalar ve prosedürlerden haberdar olmayacaktır. Bazı kuruluşlar, güvenlik farkındalığı eğitiminin her çalışanına ve yüklenicilerine (*contractors*) yıllık olarak güncellenmesini ve sağlanmasını sağlamak için bir politika önermektedir. Bu, Kullanıcı Etki Alanı (*User Domain*) ve insanlar tarafından oluşturulan riski gidermek için önemli bir risk azaltma gereksinimidir. İnsan kaynakları personelinden, çalışanların yıllık güvenlik farkındalığı eğitim programını aldıklarını ve bu

programdan geçtiklerini doğrulayan raporlar üretmeleri istenebilir. Bu, denetleyici tarafından mevzuata uygunluk denetimi yapılırken o anda talep edilebilir.

BÖLÜM ÖZETİ

Nitelikli bir güvenlik uzmanı olmak, ilgili bilgi ve becerileri gerektirmektedir. Güvenlik konularını anlamalısınız ve bu anlayış üzerinden hareket edebilmelisiniz. Eğitim ve öğretim kurumları, size gerekli bilgileri sağlayabilir ve gerekli becerileri geliştirmeye yardımcı olabilir. Bilgi sistemleri güvenliği hakkında daha fazla bilgi edinmek için birkaç farklı seçeneği araştırdınız. Bazı durumlarda kendi kendine çalışmanın uygulanabilir bir seçim olduğunu öğrendiniz. Aynı zamanda maliyeti en düşük olandır. Ek bilgi ve becerileri nereden veya nasıl kazandığınıza bakılmaksızın, bu bölümde verilen bilgilerin okunması ve araştırılması, size daha iyi bir kavrama vermiştir.

Öğrenme, bir sertifika veya bir derece ile bitmemektedir. Eğitim için sürekli eğitim teklifleri ve çeşitli örgün eğitim seviyeleri için lisans programları hakkında bilgi edindiniz. Kısa dersler ile odaklanmış eğitim sunan kuruluşlardan bazılarını öğrendiniz. İşyerinde, güvenlik farkındalığı, bir organizasyonun insanlar tarafından oluşturulan riski azaltmak için uygulayabilecekleri bir numaralı güvenlik denetimidir. Birçok organizasyon yıllık güvenlik farkındalığı eğitimine ihtiyaç duyar ve personelin yıllık güvenlik farkındalığı eğitim programını aldıklarını ve bu programdan geçtiklerini doğrulayan raporlar üretmeleri istenebilir. Bu raporlar denetçiler tarafından istenebilir.

ANAHTAR KAVRAMLAR VE TERİMLER

Accredited – Akredite edilmiş

Certificate of completion – Bitirme sertifikası

Continuing education – Sürekli eğitim

Continuing professional development (CPD) – Sürekli mesleki gelişim (CPD)

Continuing professional education (CPE) – Sürekli mesleki eğitim (CPE)

National Centers of Academic Excellence in Information As- surance Education (CAE/IAE) - Bilgi Güvenliği Eğitiminde Ulusal Akademik Mükemmellik Merkezleri (CAE/IAE)

National Centers of Academic Excellence in Research (CAE/R)- Araştırmada Akademik Mükemmellik Ulusal Merkezleri (CAE/R)

Security awareness campaign – Güvenlik farkındalığı kampanyası

Security awareness training – Güvenlik farkındalığı eğitimi

BÖLÜM 13 DEĞERLENDİRME

1. Kendi kendine çalışmanın dezavantajlarından birisi, malzemelerin genellikle pahalı olmasıdır.
   A. Doğru
   B. Yanlış

2. Günümüzde kendi kendine çalışma materyallerine sahip olmak için olası en az kaynak aşağıdakilerden hangisinde olurdu?
   A. Çevrimiçi kitapçı
   B. Yerel kitapevi
   C. Yerel kütüphane.
   D. Çevrimiçi kütüphane
   E. Hiçbiri

3. Kendi kendine çalışma materyalleri seçerken, birçok ürün satan bir tedarikçi her zaman daha kaliteli ürünlere sahiptir.
   A. Doğru
   B. Yanlış

4. Aşağıdakilerden hangisi genellikle bir dereceye götürmeyen ancak bir akademi veya üniversite ile ilişkili dersleri sunmaktadır?
   A. Önlisans programı
   B. Gelişim programı
   C. Sürekli Eğitim
   D. Mesleki eğitim organizasyonu
   E. Hiçbiri

5. Sertifikayı geçerli tutmak için gereken kredi birimini hangi terim ifade etmektedir?
   A. Kredi Saati
   B. Kalite noktası
   C. GPA
   D. CPE

6. Bir _____ sınıf, öğrencilerin ve en az bir öğretmenin aynı odada olduğu bir sınıftır.

7. Hangi iki organizasyon Ulusal Akademik Mükemmellik Merkezlerine sponsor olmaktadır?
   A. NSA ve DHS
   B. HHS ve DOD
   C. DOD ve DHS
   D. NSA ve HHS
   E. Hiçbiri

8. Aşağıaki terimlerden hangisi bir eğitim kurumunun geçerli standartları karşılayıp karşılamadığını belirlemek için harici bir organ tarafından başarıyla değerlendirildiğini gösterir?
   A. Sertifikalı
   B. Akredite edilmiş
   C. Denetlenmiş
   D. Kabul Edilmiş
   E. Hiçbiri

9. Hangi ABD ajansı, tüm federal kurumların çalışanlarına güvenlik eğitimi vermesini istemektedir?
   A. DOD
   B. NIST
   C. OPM
   D. NSA
   E. Hepsi

10. Aşağıdakilerden hangisi NIST Özel Yayın 800-50'deki ana alanlardan biri değildir?
    A. Sorumluluk
    B. Farkındalık
    C. Eğitim
    D. Profesyonel gelişme
    E. Hiçbiri

11. Güvenlik farkındalığı eğitimi hangi durumda yapılmalıdır?
    A. İlk İK uyum sürecinde ve devam ederken
    B. Herhangi bir erişim denetim oturum açma kimlik bilgilerini vermeden önce
    C. En az yılda bir kez
    D. Güvenlik farkındalığını güçlendirmek için bir politika ihlali oluştuğunda
    E. Hepsi

12. Aşağıdakilerden hangisi, genellikle yıllık güvenlik farkındalığı eğitimine dahil edilmez?
    A. Yeni politikalar ve süreçler
    B. Parola davranışlarının yapılması ve yapılmaması gerekenleri
    C. Oltalama e-posta saldırıları
    D. Bilgisayarınızda nasıl oturum açabilirsiniz
    E. Uçtan uca iletişim ile ilgili riskler

13. Kullanıcı Alanında meydana gelen riski azaltmak için periyodik güvenlik farkındalık eğitimine sahip kabul edilebilir bir kullanım politikası (AUP) en iyi güvenlik önlemidir.
    A. Doğru
    B. Yanlış

14. Siber güvenlik uygulamalı laboratuvarınız için aşağıdaki açık kaynak kodlu araçlardan ve uygulamalardan hangisini öneriyorsunuz?
    A. Wireshark
    B. Nmap
    C. Metasploit
    D. Kali Linux
    E. Hepsi

15. Bilgi sistemleri güvenlik veya siber güvenlik uzmanının birincil görevi nedir?
    A. Tüm çalışanlara güvenlik farkındalığı eğitimi vermek
    B. Kuruluşunuzun BT altyapısının kullanılabilirliğini, gizliliğini ve bütünlüğünü sağlamak
    C. Yeni tehditlerin ve yeni güvenlik trendlerinin/uyarılarının farkında olmak
    D. Kuruluşun BT ve BT güvenlik politikalarını, standartlarını ve prosedürlerini geliştirmek
    E. Hiçbiri

BÖLÜM

14

Bilgi Güvenliği Mesleki Sertifikasyonlar

BİLGİ GÜVENLİĞİ konusu sürekli daha karmaşık bir hale gelmektedir. Yeni ve daha yetenekli yazılım ve donanım ürünleri ortaya çıkarken, saldırganlar daha fazla güvenlik açığı bulmaktadırlar. Bu süreçte güvenlik uzmanlarının güncel kalmaları daha zorlaşmaktadır. Ek olarak, firma sahiplerinin sistemlerini güvence altına alacak nitelikli kişileri belirlemesi daha zor olmaktadır.

Günümüzde bir güvenlik uzmanının sahip olduğu becerileri belirlemek için en yaygın yöntemlerden biri **sertifikalandırmadır.** Sertifika, sahibinin ölçülebilir düzeyde bir yetkinliğe, belirli bir seviyede deneyime sahip olduğunu ve ilgili sınavı geçtiğini kanıtlar. Her sertifika, farklı bir beceri seti ile farklı gereksinimlerin karşılandığını onaylar.

Bugün, bilgi sistemleri güvenliği ve siber güvenlik ile ilgili birçok sertifikasyon vardır. Bu sertifikalar, üst düzey güvenlik yönetiminden ayrıntılı pratik uygulayıcılara kadar çeşitli alanlardaki personel içindir.. Bilgi sistemleri güvenliği alanındaki ilgi ve deneyiminiz ne olursa olsun, sizin için olası bir sertifikalandırma vardır. Sertifikalandırma, ilgili sertifikanın bilgi hedefleriyle uyumlu olduğunuzun ve eğitimlerini sürdürdüğünüzün, başkaları tarafından belirlenmesine yardım eder. Bu bölümde, en popüler bilgi sistemleri güvenlik sertifikaları ve gereksinimleri hakkında bilgi edineceksiniz.

14. Bölüm Konular

Bu bölüm aşağıda verilen konuları ve kavramları içermektedir:

- Siber güvenlik kuvvetleri için ABD Savunma Bakanlığı (*Department of Defense* - DoD)/Askeri standartlarının neler olduğu
- Herkes tarafından bilinen satıcı bağımsız mesleki sertifikaların neler olduğu
- Herkes tarafından bilinen satıcıya özel mesleki sertifikaların neler olduğu

14. Bölüm Hedefler

Bu bölümü tamamladığınız zaman, yapabilecekleriniz:

- Bilgi sistemleri güvenliği ve siber güvenlik alanlarında mesleki sertifikaları tanımlanma
- ABD DoD/Askeri Yönerge 8570.01 ve yeni DoDD 8140.01 arasındaki ayrımı yapabilme
- Satıcı bağımsız meslek sertifikalarını tanımlama
- Satıcıya özel meslek sertifikalarını tanımlama

ABD Savunma Bakanlığı/Askeri Yönerge 8570.01

Amerika Savunma Bakanlığı (*Department of Defense* - DoD), günlük operasyonları ve işlemleri neredeyse her yönüyle yönetmek için çok sayıda gereksinim tanımlamış ve standart geliştirmiştir. DoD tarafından geliştirilen standartların bir kısmı doğrudan bilgi güvenliği için geçerlidir. DoD Yönerge 8570.01 "Bilgi Güvenliği Eğitimi, Sertifikasyonu ve İşgücü Yönetimi (*Information Assurance Training, Certification and Workforce Management*)"; bilgi güvenliği açısından DoD personeli ve yüklenicileri için gereksinimleri tanımlar. DoD Yönerge 8570.01, "Bilgi güvencesi fonksiyonları ile ilgili görevlere atanan tüm DoD personelinin ve yüklenicilerinin (*contractors*) çok özel sertifikasyon seviyelerine sahip olmasını gerektirir". Farklı işler, farklı sertifika gereklilikleri taşır. Bu yönergenin ilk sürümü 19 Aralık 2005'te yayınlanmıştır. En son güncellemesi, 20 Kasım 2015'te Değişim 4 (*Change 4*)'ü içerir.

DoD Yönerge 8570.01 hakkında ek bilgiler için "GOV IT Wiki *http://govitwiki.com/wiki/8570.01*" değerli bir kaynaktır. Burada, her iş türü için özel sertifika gereksinimleri hakkında daha fazla bilgi bulabilirsiniz. İhtiyaçların organizasyonunuzu veya işinizi nasıl etkileyebileceği konusunda da açıklamalar bulabilirsiniz. Genel olarak, DoD Yönerge 8570.01, tüm DoD birim veya yüklenici organizasyonlarını etkiler. Bilgi güvenliği ile doğrudan ilgili olan tüm personelin güvenlik sertifikalarına sahip olmasını sağlar. Bu yönergenin amacı, niteliksiz personelin güvenlik gereksinimi olan bilgiye erişebilme olasılığını azaltmaktır. DoD Yönergesi 8570.01, eğitim ve sertifikasyon kuruluşları için yeni bir fırsat alanı yarattı. Çok sayıda güvenlik eğitimi ve sertifikası sağlayıcısı, DoD Yönerge 8570.01'e uyumluluk yollarını önermek için DoD çalışanlarını ve yüklenici firmalarını hedefine aldı. Zorunlu sertifika şartı, sertifika almak isteyen personel sayısını artırmıştır. Ayrıca, sürekli mesleki eğitim (*continuing professional education* - CPE) kredisi kazanarak yeterlilik belgelerini güncel tutmaları için, öğrencilerin güvenlik sınıflarına istikrarlı bir akışını sağlar. Etkinliği sorgulansa da DoD Yönerge 8570.01, yürütülen güvenlik eğitimlerini almak isteyen güvenlik personelinin sayısını artırmıştır.

NOT

DoD Yönerge 8570.01, DoD Yönerge (DoDD) 8140 olarak değiştirilmiştir. DoDD 8140 önceki yönergede olduğu gibi, DoD Bilgi Teknolojileri BT (*Information Technology* – IT) personelinin ve yüklenicilerinin kendi çalışma alanlarında uzmanlık sertifikaları almalarını gerektiriyor. DoDD 8140 bilgiyi, becerileri ve yetenekleri (*knowledge, skills, and abilities* - KSA) adresler. Bu yazının yazıldığı sırada tamamlayıcı bir el kitabı (8140.01-M olarak gösterilmesi beklenen) henüz yazılmamıştır. Bu nedenle, DoDD 8140, 8140.01-M onaylanana kadar 8570.01-M'yi kabul etmiştir.

ABD DoD/Askeri Yönerge 8140

ABD Savunma Bakanlığı'nın bir kolu olarak Savunma Bilgi Sistemleri Ajansı (*Defense Information Systems Agency* - DISA); Beyaz Saray, Savunma Sekreterliği ve Amerika Birleşik Devletleri savunmasına katkıda bulunan tüm askeri sektörlere, bilgi teknolojisi ve iletişimi desteği sağlar. DISA, önceki yönerge 8570.01'in yerini alacak yeni, operasyonel olarak odaklanmış bir siber güvenlik eğitimi çerçevesi geliştirmektedir.

Bu yeni siber güvenlik eğitimi çerçevesinin vizyonu; "giderek artan tehdit temelli bir ortamda ağları daha iyi çalıştırmak ve savunmak için DoD siber savaşçılarını hazırlayacak, sağlam bir işgücü eğitim ve sertifikasyon programı oluşturmaktır".

Ulusal Güvenlik Teşkilatı (*National Security Agency*) eski müdürü ve Amerika Birleşik Devletleri Siber Komutanlığı genel başkanı Keith Alexander, "Bir okulda veya birden fazla okulda siber eğitim yapsak da, eğitim tek bir standartta yürütülmelidir" demiştir. Sanırım yapmamız gereken

budur; sahadaki savaşçı komutanlar ve güçler, bir asker, denizci, havacı veya mürettebat her birey bir standarda uygun eğitilmiştir ve görevlerini beklendiği şekilde başarabileceklerini bilirler.

8140 Sayılı yeni yönergenin, siber güvenlik iş gücü sektörü için temel ilkeleri aşağıdakileri içermektedir:

- Rol tabanlı ve mürettebatın sertifikasyonu için bir "Eğitim Strateji Yol Haritası (*Training Strategy Roadmap*)" sağlanacaktır.
- Savunma Dairesi ihtiyaçlarını daha iyi karşılamak üzere, uzun zamandır güvenilir ve pek çok durumda askeri kullanım için çok geniş kapsamlı olan ticari sertifikasyon uyarlanacak ve daraltılacaktır.
- DISA, Birleşik Devletler siber savaşçılarına odaklı, ilgili nitelikleri ve sertifikaları üretebilir.
- Mürettebat sertifikasyonu; siber uzayda çalışırken ve savunurken istenen etkiyi sağlayacak, nitelikli rol tabanlı operatörlerin gruplanmasıdır.
- "Siber Savunma Akademisi (*Cyber Defense Academy*)", mürettebat ve ekiplerin etkin bir parçası olarak çalışabilecek rol tabanlı bireylere niteliklerini kazandırır.
- Ortak Siber Uzay Eğitim ve Sertifikasyon Standardı (*Joint Cyberspace Training & Certification Standard* - JCT & CS), iş-rol tanımı için geçerli temel standartlardır.
- Siber Güvenlilik Eğitimi Ulusal Girişimi (*National Initiative for Cybersecurity Education* - NICE) merkezi hükümet ile ilgili ve DoD iş-rol tanımları için geçerli temel standartları oluşturacaktır.

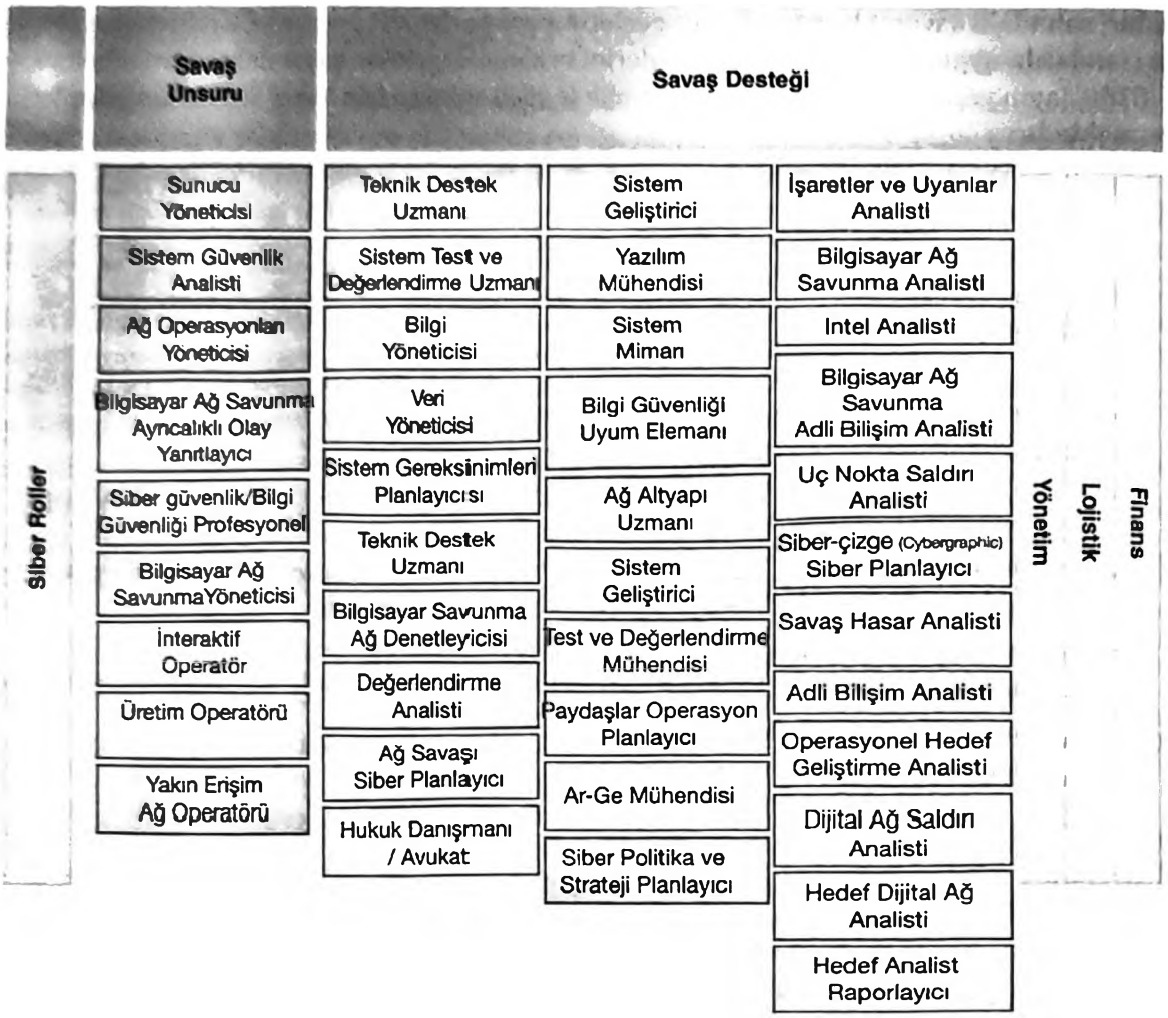
ŞEKİL 14-1, 8140 siber güvenlik alanında işgücü geliştirme girişimi için, belirli rollerin gereksinimlerini sunmaktadır.

Aşağıdaki DoD girişimleri, yeni DoDD 8140 siber güvenlik iş gücü geliştirme standardını destekleyecektir:

- DoDD 8140 işgücü gereksinimleri girişimi (JCT&CS tarafından belirlenen siber güvenlik rolleri için gereksinimleri tanımlayacaktır)
- Savunma Sekreterliği Personel ve Hazırlık Ofisi (*Office of the Under Secretary of Defense for Personnel and Readiness* - OSD-P&R) tarafından Öğrenim Yönetim Sistemi'nin (*Learning Management System*) seçimi
- JCT&CS, (CONOPs) operasyonları kavramı ve Uygulama Planı
- Ulusal Güvenlik Dairesi (*Department of Homeland Security* - DHS) ve Ulusal Güvenlik Teşkilatı (*National Security Agency* - NSA) Akademik Mükemmellik Merkezleri (*Centers of Academic Excellence*)
- DISA Siber İşgücü Gelişmeleri (*Cyber Workforce Developments*)

Önceki 8570.01 yönergesinden, rol-tabanlı DoDD 8140 yönergesine geçiş; savaş desteği için gerekli çeşitli siber güvenlik rollerini yerine getirmek için, daha özlü bir çözüm sunar. Aşağıdaki roller 8140 yönergesiyle tanımlanır:

- Güvenliği sağlamak
- İşletme ve bakım
- Koruma ve savunma
- Analiz
- İşletme ve toplama
- Gözetim ve geliştirme
- Soruşturma



ŞEKİL 14-1

Birleşik siber uzay eğitim ve sertifikalandırma standartları.
Savunma Bilgi Sistemleri Ajansı (Defense Informatiom Systems Agency - DISA), Genel Müdür Yardımcısı, Saha Güvenliği Operasyonları.

ABD DoD / NSA Eğitim Standartları

Bilgi güvenliği, her geçen gün daha karmaşıklaşan, giderek büyüyen bir disiplindir. DoD ve NSA, bilgi güvenliğiyle ilgili ve çok sayıda endişe duyulabilecek alanı tespit etmiştir. DoD ve NSA, 8140 sayılı yönergenin gereklerinin yapılabilmesi için çeşitli eğitim standartlarını benimsemiştir. Bunlar standart olarak isimlendirilmiş olsalar da, kabul edilen anlamda bilgi güvenliği standartları olarak görülmezler. Belirli iş sorumlulukları için, gerçekten gerekli eğitimlerdir. Bu eğitim standartları, belirli iş sorumlulukları ile ilgili konular için öğrenme hedeflerini içeren uzun listelerdir. Ulusal Güvenlik Sistemleri Komitesi (*Committee on National Security Systems* - CNSS) ve Ulusal Güvenlik Telekomünikasyon ve Bilgi Sistemleri Güvenliği (*National Security Telecommunications and Information Systems Security* - NSTISS) Komitesi tarafından geliştirilmişlerdir. DoD/NSA, gereksinimleri karşılayacak eğitim içeriğinin ve materyallerinin geliştirilmesinde kurs ve mesleki sertifika tedarikçileri için rehberlik sağlarlar.

TABLO 14-1 DoD/NSA eğitim standartları.

EĞİTİM STANDARDI	TANIM
NSTISS-4011	Bilgi Sistemleri Güvenliği için Ulusal Eğitim Standardı (InfoSec) Uzmanları
CNSS-4012	Kıdemli Sistem Yöneticileri için Ulusal Bilgi Güvencesi Eğitim Standardı
CNSS-4013	Sistem Yöneticileri (*System Administrator* - SA) için Ulusal Bilgi Güvenliği Eğitim Standardı
CNSS-4014	Bilgi Güvenliği Görevlisi (*Information Assurance Officer* - IAO) Eğitimi
NSTISSC-4015	Sistem Sertifika Sağlayıcıları için Ulusal Eğitim Standardı
CNSS-4016	Risk Analistleri için Ulusal Bilgi Güvenliği Eğitim Standardı

Bazı standartlar giriş, orta ve ileri gibi farklı uzmanlık seviyelerini tanımlar. **TABLO 14-1** bilgi güvenliği ile ilgili güncel CNSS/NSTISS eğitim standartlarını göstermektedir.

Bu eğitim standartları, iş yeterliliklerinin kapsamlı tanımlarını sunar. Potansiyel ve mevcut InfoSec profesyonelleri için rehberlik sağlarlar. InfoSec'te çalışan veya bu alanda çalışmak isteyen herkes, bu standartları gerekli becerilere sahip olduklarından emin olmak için kullanabilirler. Belki de daha önemlisi, yeni nesil InfoSec profesyonellerini farklı iş fonksiyonları için donatmaya ortam hazırlıyor olmalarıdır.

NOT

Bu standartlar, DoD/NSA gereksinimlerini karşılayan materyallerin geliştirilmesinde satıcılara yardım ederler. Aslında, Jones & Bartlett Öğrenme Bilgi Sistemleri Güvenlik & Güvencesi (ISSA) Eğitim Planı, hem NSTISS-4011'i hem de CNSS-4013-İleri Seviye'yi karşılar. Giriş ve Orta seviye olarak iki seviyeyi de içerir. Jones & Bartlett Öğrenme ISSA Eğitim Planı, NSA ve Ulusal Siber Güvenlik Eğitimi Girişimi (NICE) tarafından onaylanmıştır.

Satıcı-Bağımsız Profesyonellik Sertifikaları

Sertifikasyon, bir kişinin belirli iş gereksinimlerini yerine getirdiğini doğrulayan resmi bir bildirimdir. Bu gereksinimler çoğunlukla aşağıdakileri içerir:

- Belirli düzeyde deneyim sahibi olunduğu
- Bir eğitim kursunu tamamlandığı
- Sınavı başarıyla geçildiği

Yetkili bir organizasyon, bir kişinin sertifikalandırma gereksinimlerini karşıladığını bildiren sertifikayı verir.

Sertifikalar mükemmel olmasa da bunlara sahip olunması, güvenlik uzmanları için öğrenme ve eğitimini ilerletmek için standart bir yol sunar. Sertifikalar, bir güvenlik uzmanının güvenlik hakkında daha fazla öğrenmeye zaman, emek ve para yatırdığını göstermektedir. Birçok potansiyel işveren, iş başvurularını tararken güvenlik sertifikalarını dikkate alır. Gerçek güvenlik uzmanlığı, sadece bir sertifikasyona sahip olmaktan fazlasını gerektirir. Bununla birlikte, adayları sertifikasyona hazırlayan organizasyonlar, adayları eğitmek ve sınava hazırlamak için iyi bir eğitim planı geliştirmişlerdir.

NOT

Belgelendirme, bir kişinin belirli bir işte iyi olduğunu garanti etmez. Maalesef, sertifikalı kötü güvenlik uzmanları olduğu gibi, sertifikaya sahip olmayan mükemmel güvenlik uzmanları da vardır. Genellikle, sertifika profesyonel bir endüstri sertifikası ise bir işi gerçekleştirmek için gerekli olan becerileri, bilgiyi ve deneyimi tanımlayan bir **iş görev analizine (*job task analysis*)** tabi tutulmalıdır. Bu iş görev analizi, kapsamlı ve doğru bir şekilde gerçekleştirildiğinde profesyonellik sertifikasyonunun mahkemede savunulabilir olmasını sağlar.

Sertifikalar, belirli bilgi ve uzmanlık alanlarını hedeflemektedir. Güvenlikle ilgili iş fonksiyonları ve uzmanlık düzeylerinin her birisi için en az bir sertifika bulunmaktadır. İlk sertifika türü, **satıcı-bağımsız olan sertifikalardır (*vender-neutral certification*).** Bu tür bir sertifika, doğasında genel olan kavramları ve konuları kapsar. Belli bir ürün veya ürün grubuna odaklanmaz. Birçok kuruluş, güvenlik topluluklarının yüksek değere sahip gördüğü sertifikaları sağlar. İlerleyen bölümlerde, bazı sertifika kuruluşları ve kalite gereklilikleri ele alınmaktadır.

Uluslararası Bilgi Sistemleri Güvenliği Sertifika Konsorsiyumu A.Ş.

Uluslararası Bilgi Sistemleri Güvenliği Sertifikasyon Konsorsiyumu A.Ş. (*International Information Systems Security Certification Consortium, Inc.* – $(ISC)^2$), en saygın küresel sertifikasyon kuruluşlarından biridir. $(ISC)^2$, tüm deneyim seviyelerinde güvenlik uzmanlarını eğitmeye ve sertifikalandırmaya odaklanan, kazanç amacı gütmeyen bir kuruluştur. $(ISC)^2$, her biri farklı güvenlik profesyonelliği rolünü adresleyen yeterlilik belgeleri (*credentials*) sunmaktadır. Yedi temel yeterlilik belgesi şunlardır:

- Sistemler Güvenliği Sertifikalı Uygulayıcısı (*Systems Security Certified Practitioner* - SSCP®)
- Sertifikalı Bilgi Sistemleri Güvenlik Uzmanlığı (*Certified Information Systems Security Professional* - CISSP®)
- Sertifikalı Yetkilendirme Uzmanlığı (*Certified Authorization Professional* - CAP®)
- Sertifikalı Güvenli Yazılım Yaşam Döngüsü Uzmanlığı (*Certified Secure Software Lifecycle Professional* - CSSLP®)
- Sertifikalı Siber Adli Bilişim Uzmanlığı (*Certified Cyber Forensics Professional* - CCFP®)
- Sağlık Hizmetleri Sertifikalı Bilgi Güvenliği Mahremiyet Uygulayıcısı (*HealthCare Certified Information Security Privacy Practitioner* - HCISPP®)
- Sertifikalı Bulut Güvenlik Uzmanlığı (*Certified Cloud Security Professional* - CCSP®)

NOT

$(ISC)^2$ Profesyonellik sertifikası kalite gereksinimleri hakkında daha fazla bilgi için; *www.isc2.org* adresindeki $(ISC)^2$ web sitesini ziyaret ediniz.

SSCP®

Sistemler Güvenliği Sertifikalı Uygulayıcısı (*Systems Security Certified Practitioner* - SSCP) yeterlilik belgesi, güvenlik uygulayıcılarının kendi yetkinlik düzeylerini kanıtlamalarına olanak tanır. SSCP, bilgi güvenliği için en başarılı uygulamalardaki yedi alanı kapsar. $(ISC)^2$, SSCP Ortak Bilgi Tabanı'nda (*Common Body of Knowledge* - CBK) yüksek başarımlı güvenlik uygulamalarını yayınlar. SSCP kalite gereksinim bilgileri; kıdemli ağ güvenlik mühendisleri, kıdemli güvenlik sistemleri analistleri veya kıdemli güvenlik yöneticileri olarak çalışan veya çalışacaklar için uygundur.

CISSP®

$(ISC)^2$'nin en önde gelen yeterlilik belgesi Sertifikalı Bilişim Sistemleri Güvenlik Uzmanlığı (*Certified Information Systems Security Professional* - CISSP)'dır. CISSP, bilgi güvenliği alanında ilk ANSI/ISO onaylı (akrediteli) kalite gereksinim belgesidir. CISSP, bilgi güvenliği uzmanlarına tarafsız bir yeterlilik ölçütü ve küresel olarak kabul edilen bir başarı standardı sağlar. CISSP yeterlilik belgesi, $(ISC)^2$ CISSP, CBK'nın sekiz alanındaki yeterliliğin karşılandığını kanıtlar. CISSP yeterlilik belgesi; güvenlik

bilişim kurulu başkanı (*chief information security officer* - CISO), güvenlik başkanı (*chief security officer* - STK) ya da üst düzey güvenlik mühendisleri gibi görevlerde bulunmuş ya da halen çalışmakta olan orta ve üst düzey yöneticiler için tanımlıdır.

CAP®

Sertifikalı Yetkilendirme Uzmanlığı (*Certified Authorization Professional* - CAP) yeterlilik belgesi, bilgi sistemlerinde yetkilendirme ve bakım sürecinde yer alan profesyoneller için gerekli olan bilgi ve becerileri ölçmek için bir yöntem sunmaktadır. CAP yeterlilik belgesi en çok risk değerlendirme ve güvenlik gereksinimlerini belirleme için kullanılan süreçlerin geliştirilmesi ve uygulanmasından sorumlu personele uygundur. CAP yeterlilik belgesinin arandığı uzmanlar; yetkilendirme görevlilerini, sistemin sahiplerini, bilginin sahiplerini, bilgi güvenliği görevlileri ve sertifika sağlayıcılarını içerebilir. Bu kalite gereksinimleri, hem özel sektör hem de ABD hükümet personeli için uygundur.

NOT

CISSP® CBK'nın, kapsamı 10 etki alanından 8 etki alanına değiştirilmiştir. CISSP CBK'nın kapsamındaki 8 etki alanı şunlardır:

- Güvenlik ve Risk Yönetimi
- Varlık Güvenliği
- Güvenlik Mühendisliği
- İletişim ve Ağ Güvenliği
- Tanımlama ve Erişim Yönetimi
- Güvenlik Değerlendirmesi ve Testi
- Güvenlik Operasyonları
- Yazılım Geliştirme Güvenliği

CSSLP®

Sertifikalı Güvenli Yazılım Yaşam Döngüsü Profesyoneli (*Certified Secure Software Lifecycle Professional* - CSSLP); güvenli yazılım geliştirmeye ait az sayıdaki kalite gereksinim tanımlarından birisidir. CSSLP yeterlilik belgesi, güvenli uygulama geliştirme ve uygulamaya alma için gerekli olan bilgi ve becerileri açısından profesyonelleri değerlendirir. Bu kalite gereksinimleri, yazılım geliştiriciler, yazılım mimarları ve yazılım geliştirme ve uygulamaya alma sürecinde yer alan herkes için uygundur.

CCFP®

Sertifikalı Siber Adli Bilişim Uzmanı (*Certified Cyber Forensics Professional* - CCFP) yeterlilik belgesi, temel bir adli sertifikalandırması değildir. Daha çok var olan bir adli bilişim sertifikalandırmasını ya da "EnCase® Forensic" veya "Forensic Toolkit® (FTK®)" gibi ticari olarak mevcut bir adli bilişim analiz uygulamasını kullanma düzeyinin üzerine kuruludur. CCFP kalite gereksinimi, dijital adli bilişim araştırmalarını gerçekleştirmek ve yürütmek için gerekli bilgi ve beceriler için profesyonelleri test eder ve değerlendirir. Bu yeterlilik belgesi; kolluk görevlileri, siber suçlar ve siber güvenlik uzmanları, adli bilişim mühendisleri ve adli bilişim danışmanları için uygundur.

HCISPP®

Sağlık Hizmetleri Sertifikalı Bilgi Güvenliği Mahremiyet Uygulayıcısı (*HealthCare Certified Information Security Privacy Practitioner* - HCISPP), sağlık hizmetleri sektörüne hitap etmek ve korunan sağlık bilgileri (*protected health care information* - PHI) veya elektronik olarak korunan sağlık bilgilerini (*electronic protected health care information* - ePHI) korumak için geliştirilmiştir. HCISPP yeterlilik belgesi, sağlık kuruluşları için güvenlik ve mahremiyet çalışmalarını gerçekleştirmek ve yürütmek için profesyonellerin gerekli bilgi ve becerilerini test eder ve değerlendirir. Bu yeterlilik belgesi, bir sağlık kuruluşu içinde Bilgi Teknolojileri - BT veya BT güvenlik alanında kariyer yolunu arayan kişiler için uygundur.

CCSP®

Bulut ve sanal bilişim alanındaki hızlı büyüme ile birlikte, Sertifikalı Bulut Güvenlik Profesyoneli (*Certified Cloud Security Professional* - CCSP) sertifikası, $(ISC)^2$ ve Cloud Security Alliance (CSA) birlikteliği tarafından oluşturulmuştur. CCSP yeterlilik belgesi, bulut bilişim ortamlarını güvenli hale getirmek ve yönetmek için uzmanların gerekli olan bilgi ve becerilerini test eder ve değerlendirir. Bu yeterlilik belgesi; bulut altyapılarındaki uygulamaları tasarlayan, uygulayan, barındıran ve yöneten BT, BT güvenliği, sistem yöneticileri ve sistem mimarları için uygundur.

Ek $(ISC)^2$ Meslek Sertifikaları

CISSP'nin özgün anlayışı ve bilgi sistemleri güvenliğinin gelişimindeki süreklilik sonrası, $(ISC)^2$, daha gelişmiş içeriği adresleyen bilgi sistemleri güvenlik mimarisi, mühendisliği ve yönetimi de dahil olmak üzere, bu odak alanları için yeterlilik belgeleri geliştirmeye ihtiyaç duyulduğunu keşfetti. CISSP odak alanlar aşağıdaki fonksiyonel alanlardadır:

- Mimari (CISSP-ISSAP®)
- Mühendislik (CISSP-ISSEP®)
- Yönetim (CISSP-ISSMP®)

NOT

CISSP® odak alan sertifikaları hakkında daha fazla bilgi için *https://www.isc2.org/concentrations/default.aspx* web adresini ziyaret ediniz.

ISSAP®

ISSAP odak alanı; adayın mimarlık alanında iki yıllık uzman deneyimine sahip olduğunu göstermesini gerektirir ve genellikle bağımsız danışmanlar veya benzer kapasitelerde çalışan baş güvenlik mimarları ve analistleri için uygun bir yeterlilik belgesidir.

ISSEP®

ISSEP odak alanı, NSA ile birlikte sistem güvenlik mühendisliği profesyonelliklerinin her birisi için paha biçilemez bir araç olarak geliştirildi. ISSEP'in odak alanı; güvenlik bileşenlerinin projelerle, uygulamalarla, iş süreçleriyle ve tüm bilgi sistemleriyle bütünleştirilmesinde bir yol haritası olmaktır.

ISSMP®

ISSMP odak alanı, adayın bir kurum genelinde güvenlik operasyonları ve yönetimi alanında iki yıllık mesleki deneyim göstermesini gerektirir. Bu odak alanı, proje yönetimi, risk yönetimi, güvenlik farkındalığı programı kurma ve sunma ve iş süreklilik planlama programını yönetmek gibi daha derin yönetim unsurlarını içerir.

Küresel Bilgi Güvenliği Sertifikası / SANS Enstitüsü

Bir sonraki büyük sertifikasyon kuruluşu da ANSI tarafından akredite edilen küresel bir organizasyondur. Küresel Bilgi Güvenliği Sertifikası (*Global Information Assurance Certification* - GIAC) yaklaşık 30 kişisel yeterlilik belgesi sunmaktadır. Bu yeterlilik belgeleri birkaç bilgi güvenliği iş disiplinini kapsamaktadır:

- Denetim (*Audit*)
- Adli Bilişim (*Forensics*)
- Yasal (*Legal*)
- Yönetim (*Management*)
- Güvenlik yönetimi (*Security administration*)
- Yazılım güvenliği (*Software security*)

SANS Enstitüsü tarafından 1999 yılında kurulan GIAC, çeşitli sertifikalar veren yönetim organıdır. SANS Enstitüsü, GIAC yeterlilik belgelerinin her biri için öğrencileri hazırlayan, özel eğitimler sunar. Bireysel bir GIAC yeterlilik belgesini seçebilir veya daha üst düzey yeterlilik belgeleri kazanmak için bir yol izleyebilirsiniz.

GIAC yeterlilik belgesine sahip olan herkes, bilgi güvenliğinin önemli alanlarından birisinde teknik bir yayın sunabilir. Kabul edilen bu teknik yayın Altın Yeterlilik Belgesi (*Gold credential*) olarak temel GIAC yeterlilik belgesine eklenir. Altın yeterlilik belgesi, güvenlik uzmanının, diğer yeterlilik belgesi sağlayanlardan ayrı bir statüde tutulmasını sağlar. GIAC Güvenlik Uzmanı (*GIAC Security Expert* - GSE) yeterlilik belgesi, güvenlik uzmanlarının diğer yeterlilik belgelerini sağlayanlardan ayrı durması için başka bir yöntem sunmaktadır. GSE şartları; üç GIAC yeterlilik belgesini (yeterlilik belgesinin iki tanesi Altın yani teknik yayın yapmış olmaktır), GSE yazılı sınavından geçmeyi ve yoğun iki günlük bir uygulamalı laboratuvarı tamamlamayı içermektedir. GSE, GIAC içindeki en üst seviyedeki yeterlilik belgesini temsil eder.

TABLO 14 - 2 GIAC'e göre varolan GIAC yeterlilik belgelerini ve ilgili düzeylerini listelemektedir.

> **NOT**
>
> GIAC güvenlik sertifikaları hakkında daha fazla bilgi için https://www.giac.org/certifications/categories adresindeki GIAC web sitesini ziyaret ediniz.

Sertifikalı İnternet Web Yöneticisi

Sertifikalı İnternet Web Yöneticisi (*Certified Internet Webmaster* - CIW) hem genel, hem de web ile ilgili güvenlik odaklı çeşitli yeterlilik belgelerini sunmaktadır. CIW'ın ileri seviye bazı yeterlilik belgelerinde, bir sınavdan geçmek ve başka bir satıcıdan en az bir tanınmış sertifika belgesi almış olmak gerekir. CIW, güvenlik bilgi ve becerilerinin genişliğini teşvik etmek için bu harmanlanmış yaklaşımı kullanmaktadır. **TABLO 14 - 3**, CIW güvenlik ile ilgili yeterlilik belgeleri ve bu belgelerin genel gereksinimlerini listelemektedir.

CIW-onaylı yeterlilik belgesi listesi, CIW Web Güvenliği Uzmanı (*Web Security Specialist*) ve CIW Web Güvenliği Profesyoneli (*Web Security Professional*) kalite gereksinimlerini sağlayan diğer tedarikçiler için kalite gereksinimlerini içerir. CIW gereksinimlerini karşılayan diğer yeterlilik belgeleri şunları içerir:

- $(ISC)^2$ SCCP veya CISSP
- GSE, GCFW, GCIH ve benzeri gibi çeşitli GIAC yeterlilik belgeleri
- CompTIA Güvenlik+ (*CompTIA Security +*)
- Satıcıya özel birçok kalite gereksinimi

> **NOT**
>
> CIW yeterlilik belgeleri ve mevcut gereksinimler hakkında daha fazla bilgi için, www.ciwcertified.com adresindeki CIW web sitesine bakınız.

CompTIA

CompTIA'nın Güvenlik+ (*Security+*) sertifikası, ürün bağımsız bir sertifikadır. Güvenlik+, herhangi bir BT veya BT güvenlik uzmanı için küresel olarak kabul gören temel bir sertifikadır. CompTIA'nın Güvenlik+ sertifikası, bu alanda daha fazla iş ve bilgiyi takip etmek isteyen BT uzmanları

TABLO 14-2 GIAC Yeterlilik Belgeleri.

İŞ ALANI	SEVİYE	YETERLİLİK BELGESİ
Denetim	Orta İleri	GIAC Sertifikalı ISO-27000 Uzmanı (G2700) GIAC Sistem ve Ağ Denetçisi (GSNA)
Adli Bilişim	Orta İleri Uzman	GIAC Sertifikalı Adli Bilişim İncelemeci (GCFE) GIAC Sertifikalı Adli Bilişim Analist (GCFA) GIAC Tersine Mühendislik Kötücül Yazılımlar (GREM)
Yasal	İleri	GIAC Yasal Konular (GLEG)
Yönetim	Orta İleri İleri	GIAC Bilgi Güvenliği Uzmanı (GISP) GIAC Güvenlik Liderliği Sertifikası (GSLC) GIAC Sertifikalı Proje Yöneticisi Sertifikasyonu (GCPM)
Güvenlik Yöneticisi	Giriş Orta Orta İleri İleri İleri İleri İleri İleri Uzman Uzman	GIAC Bilgi Güvenliği Esasları (GISF) GIAC Güvenlik Temelleri Sertifikasyonu (GSEC) GIAC Sürekli İzleme (GMON) GIAC Sertifikalı Güvenlik Duvarı Analisti (GCFW) GIAC Sertifikalı Saldırı Analisti (GCIA) GIAC Sertifikalı Ayrıcalıklı Olay İşleyicisi (GCIH) GIAC Sertifikalı UNIX Güvenlik Yöneticisi (GCUX) GIAC Sertifikalı Windows Güvenlik Yöneticisi (GCWN) GIAC Sertifikalı Sızma (Penetrasyon) Testçisi (GPEN) GIAC Web Uygulama Sızma Testçisi (GWAPT) GIAC Kablosuz Ağların Değerlendirilmesi (GAWN) GIAC Saldırı Araştırmacısı ve Gelişmiş Sızma Testçisi (GXPN)
Yazılım Güvenliği	İleri İleri	GIAC Güvenli Yazılım Programcısı-.NET (GSSP-NET) GIAC Güvenli Yazılım Programcısı-Java (GSSP-JAVA)
GSE	Uzman	GIAC Güvenlik Uzmanı (GSE)

TABLO 14-3 CIW Yeterlilik Belgeleri.

SERTİFİKA İÇİN YETERLİLİK BELGESİ	GEREKLİLİK
CIW Web Güvenliğiyle İlgili	CIW Web Güvenliğiyle İlgili Sınavdan Geçmek (1D0-571)
CIW Web Güvenlik Uzmanı	Web Güvenliğiyle ilgili Sınavdan Geçmek (1D0-571) ve ek olarak CIW onaylı yeterlilik belgesi listesinden bir yeterlilik belgesi hak etmek
CIW Web Güvenlik Profesyoneli	Web Güvenliğiyle ilgili Sınavdan Geçmek (1D0-571) ve ek olarak CIW onaylı yeterlilik belgesi listesinden iki yeterlilik belgesi hak etmek

için giriş seviyesi bilgi güvenliği sertifikası haline gelmiştir. CompTIA'nın Güvenlik+ sertifikası, BT içinde hangi kariyer yolunun seçileceğine karar vermeye çalışan yeni üniversite mezunlarına veya giriş seviyesindeki BT uzmanlarına ulaşmak için hazırlanmıştır.

Giriş seviyesi bilgi sistemleri güvenliği veya siber güvenlik sertifikasyon yeterlilik belgesini sağlamayı isteyen profesyoneller için CompTIA Güvenlik+ sertifikasının faydaları şunlardır:

- 147'den fazla ülkede sertifikalı profesyonelleriyle, küresel olarak bilinen bir yeterlilik belgesidir.
- ISO 17024 standardına uygundur ve DoD 8570.01-M gereksinimleri tarafından onaylanır.
- Güvenlik+, endüstri desteklidir, önde gelen BT uzmanları tarafından geliştirilmiştir ve güncellenir.
- Bilgi sistemleri güvenliği ve takip eden ek güvenlik sertifikalarıyla bir kariyer sağlar.

5 yıldan 10 yıla kadar deneyime sahip güvenlik uzmanları için CompTIA, CASP™ veya CompTIA İleri Seviye Güvenlik Uygulayıcısı (*Advanced Security Practitioner*), yeterlilik belgesi sunar. CompTIA'nın sertifikasyon web sitesine göre, CASP "ISO 17024 standardını karşılar ve 8570.01-M yönergesinin gereklerini yerine getirmesi için ABD Savunma Bakanlığı tarafından onaylanır. Federal Bilgi Güvenliği Yönetim Yasası (*Federal Information Security Management Act* - FISMA) hükümet düzenlemeleri ile uyumludur."

ISACA®

Önceden, Bilgi Sistemleri Denetim ve Kontrol Derneği (*Information Systems Audit and Control Association*) olarak bilinen ISACA, "bilgi sistemleri için dünyada kabul görmüş, endüstri lideri bilgi ve uygulamaların geliştirilmesi, benimsenmesi ve kullanılmasını" destekleyen kazanç amacı gütmeyen bir küresel organizasyondur. ISACA, konferans ve eğitim etkinliklerinde güvenlik eğitimleri sağlamaktadır. Kuruluş, BT güvenlik uzmanları için dört sertifika programı sunmaktadır. **TABLO 14 - 4**, ISACA sertifikalarını listelemektedir.

NOT

CompTIA'nın yeterlilik belgeleri ile ilgili daha detaylı bilgi için www.comptia.org/certifications.aspx adresindeki CompTIA'nın web sitesini ziyaret ediniz.

NOT

ISACA sertifikaları ve gereksinimleri ile ilgili daha detaylı bilgi için www.isaca.org adresindeki ISACA web sitesini ziyaret ediniz.

Diğer Bilgi Sistemleri Güvenlik Sertifikaları

Değer taşıyan, sadece önceki satıcılar ve sertifikalar değildir. Disiplindeki niş alanlara yönelik birçok sertifika vardır. Aşağıdaki sertifika tablosu ayrıntılı bir liste değildir, fakat birçok mevcut seçeneğin araştırılması için bir başlangıç noktasıdır. İzlenecek doğru sertifikasyona karar vermeden önce, ilgilendiğiniz alandaki en güncel teklifleri araştırın. Satıcılar sürekli olarak yeni sertifikalar sunmaktadır. Satıcılar ayrıca, mevcut ürünlerini sıklıkla güncellerler. Takip etmek istediğiniz sertifikalarla ilgili en son bilgiler için kendi aramanızı yaptığınızdan emin olun. **TABLO 14-5**, bu bölümde henüz ele alınmamış daha popüler sertifikalardan bazılarını listelemektedir.

Satıcıya-Özel Profesyonellik Sertifikaları

Birçok donanım ve yazılım satıcısı da sertifika programları sunmaktadır. Bu **satıcıya özel sertifikalar (*vendor specific certifications*)** kapsamlı ürün bilgisine sahip profesyonelleri belirlemeye yardımcı olur. Birçok organizasyon, bu sertifikaları, satıcı bağımsız sertifikalarla birlikte,

TABLO 14-4 ISACA Sertifikaları.

SERTİFİKALANDIRMA	TANIMI
Sertifikalı Bilgi Güvenliği Yöneticisi (CISM) *Certified Information Security Manager (CISM)*	CISM, güvenlik yönetimiyle uğraşan deneyimli bilgi güvenliği uzmanları sertifikasyon programıdır. Kurumsal güvenlik programlarını tasarlamak, uygulamak ve yönetmek için gerekli bilgi ve becerileri ölçmek için bir yol sağlar.
Sertifikalı Bilgi Sistemleri Denetçisi (CISA) *Certified Information Systems Auditor (CISA)*	CISA sertifikasyon programı, bilgi sistemleri denetim, kontrol ve güvenlik uzmanlarını adreslemektedir. BT denetim ve kontrol alanındaki başarının temel blokları olan becerileri ve uygulamaları tanımlar ve geliştirir.
Kurumsal BT Yönetiminde Sertifikalı (CGEIT) *Certified in the Governance of Enterprise IT (CGEIT)*	CGEIT yeni bir ISACA sertifikasyon programıdır. Kuruluşlarının BT yönetim gereksinimlerini karşıladığından emin olan güvenlik profesyonellerini hedef alır. CGEIT, gereklerini, küresel konunun uzmanlarından gelen ISACA ve BT Yönetişim Enstitüsünün (*IT Governance Institute* - ITGI) denetim ve kontrol kılavuzlarına dayandırmaktadır.
Risk ve Bilgi Sistemleri Kontrolünde (CRISC) Sertifikalı *Certified in Risk and Information Systems Control (CRISC)*	CRISC sertifikası geniş bir alanı içine alan güvenlik uzmanlıkları için geçerlidir. Bu sertifika, riske yönelik güvenlik kontrollerini tasarlamak, uygulamak, izlemek ve yönetmek için gerekli bilgi ve becerilere odaklanmaktadır. CRISC, tanımlama, değerlendirme, yanıtlama ve izleme dahil tüm risk yönetim alanlarını ele alır.

muhtemel çalışanları ve personeli değerlendirirken kullanmaktadır. Satıcı bağımsız nitelikteki sertifikalardaki gibi, belirli bir satıcı için bir sertifika almak yetkiyi garanti etmez ancak bunu ima eder. Bir başvuru sahibi sertifika şartlarını yerine getirirse, başvuranın belirli bir bilgi ve beceri düzeyine sahip olduğu anlamına gelir. Bu bölümde, satıcıya özel sertifika programlarından bazılarını öğreneceksiniz. Sertifikasyon programları sık sık değişir. BT altyapınızda etkin olan yazılım ve donanım ürünlerinin her biri için satıcı web sitesini ziyaret etmeniz gerekir. Pek çok satıcının sertifika sunduğunu göreceksiniz. Aşağıdaki bölümlerde, güvenlik personeli için birçok satıcıya özel sertifika sunulmaktadır.

Cisco Sistemleri

Cisco Sistemleri, ağ güvenlik aygıtları ve yazılımlarının en büyük üreticilerinden biridir. Cisco, ağ ürünleri için bir dizi sertifika sunmaktadır. Eğitim ve sertifikasyon süreci, Cisco ürünleri ile çalışan güvenlik uzmanlarının, ortamlarını korumak için ihtiyaç duydukları bilgi ve becerilere sahip olmasını sağlamaya yardımcı olur. Cisco farklı alanlarda çok sayıda farklı sertifika seviyeleri sunmaktadır. Bu seçenekler, güvenlik uzmanlarının Cisco ürünlerinden en iyi şekilde yararlanmak için ihtiyaç duydukları özel bilgi ve becerilere odaklanmalarına olanak tanır.

Cisco, farklı deneyim düzeylerine sahip profesyonellerin ihtiyaçlarını karşılamak için beş farklı düzeyde sertifika sunmaktadır. Giriş seviyesindeki profesyoneller ek eğitim ve tecrübe ile hedefledikleri düzeye yükselebilirler. Önemli Cisco ürünlerinde deneyimine sahip olan uzmanlar,

TABLO 14-5 Ek bilgi sistemleri güvenlik sertifikaları.

SATICI	SERTİFİKASYONLAR	DAHA FAZLA BİLGİ İÇİN
Uluslararası E-Ticaret Danışmanları Konseyi (EC-Konseyi)	Sertifikalı Etik Korsan (*Certified Ethical Hacker* - CEH) Bilgisayar Korsanlığı Adli Bilişim Araştırmacısı (*Computer Hacking Forensic Investigator* - CHFI) EC-Konseyi Sertifikalı Güvenlik Analisti (*EC-Council Certified Security Analyst* - ECSA)/Lisanslı Sızma Testçisi (*Licensed Penetration Tester* - LPT)	http://cert.eccouncil.org/
Yazılım Mühendisliği Enstitüsü—Carnegie Mellon Üniversitesi	CERT-Sertifikalı Bilgisayar Güvenliği Ayrıcalıklı Olay İşleyicisi (*Certified Computer Security Incident Handler*) SEI-Yetkili CERT Eğitmeni (*Authorized CERT Instructor*)	https://www.sei.cmu.edu/training/certificates/security/handler.cfm
Mile 2	Çoklu Güvenlik Sertifikasyonu	www.mile2.com/
Sertifikalı Kablosuz Güvenlik Profesyoneli	Çoklu Kablosuz Güvenlik Sertifikasyonu	www.cwnp.com/certifications/cwsp/
Yüksek Teknoloji Suç Ağı	Sertifikalı Bilgisayar Suçları Araştırmacısı (Temel, İleri) Sertifikalı Bilgisayar Adli Bilişim Teknikeri (Temel, İleri)	www.htcn.org
Uluslararası Adli Bilişim Müfettişleri Derneği	Sertifikalı Bilgisayar Müfettişi (*Certified Computer Examiner* - CCE)	www.isfce.com/certification.htm
Siber Güvenlik Enstitüsü	Siber Güvenlik Adli Bilişim Analisti (*CyberSecurity Forensic Analyst* - CSFA)	www.cybersecurityforensican alyst.com/
Saldırgan Güvenlik (*Offensive* Security)	Çoklu Sertifikasyon	www.offensive-security.com/information-security-certifications/

daha yüksek bir seviyeden sertifika almaya başlamak isteyebilirler. Cisco şu seviyelerde sertifikalar sunmaktadır:

- Giriş (*Entry*)
- İlişkili (*Associate*)
- Profesyonel (*Professional*)
- Uzman (*Expert*)
- Mimar (*Architect*)

Cisco, başvuru sahiplerinin sertifikasyon düzeylerine göre farklı zorlukta değerlendirme süreci uygulamaktadır. Giriş seviyesinde sertifikalar, sadece tek bir sınav gerektirir. Daha gelişmiş sertifikalar birden fazla dersi almayı ve sınavları gerektirir. Cisco, konuyla ilişkili olanlar, profesyoneller ve uzmanlar için birden fazla yol da sunmaktadır. Bu yollar, Cisco yeterlilik belgesine sahip kişilerin belirli alanlarda uzmanlaşmasını sağlarlar. Aşağıdaki yollardan birini seçerek Cisco sertifikası alabilirsiniz:

- Tasarım
- Güvenlik

NOT

Cisco'nun sertifikasyon programları hakkında daha fazla bilgi için *www.cisco.com/c/en/us/training-events/training-certifications/certifications.html* adresindeki Cisco web sitesini ziyaret ediniz.

- Ses
- Kablosuz
- Yönlendirme (*Routing*) ve anahtarlama (*switching*)
- Servis sağlayıcı operasyonları

TABLO 14 - 6 Cisco sertifikasyonlarını listelemektedir.

TABLO 14-6 Cisco sertifikasyonları.

Seviye	Sertifika
Giriş	Cisco Sertifikalı Giriş Ağ Teknikeri (*Cisco Certified Entry Networking Technician* - CCENT) Cisco Sertifikalı Tekniker (*Cisco Certified Technician* - CCT)
İlişkili	Cisco Sertifikalı Tasarım Bileşeni (*Cisco Certified Design Associate* - CCDA) Cisco Sertifikalı Ağ Bileşeni (*Cisco Certified Network Associate* - CCNA) Veri Merkezi (*Data Center*) Cisco Sertifikalı Ağ Bileşeni (CCNA) Yönlendirme ve Anahtarlama (*Routing and Switching*) Cisco Sertifikalı Ağ Bileşeni (CCNA) Güvenlik (*Security*) Cisco Sertifikalı Ağ Bileşeni (CCNA) Servis Sağlayıcı (*Service Provider*) Cisco Sertifikalı Ağ Bileşeni (CCNA) Servis Sağlayıcı Operasyonları (*Service Provider Operations*) Cisco Sertifikalı Ağ Bileşeni (CCNA) Video (*Video*) Cisco Sertifikalı Ağ Bileşeni (CCNA) Ses (*Voice*) Cisco Sertifikalı Ağ Bileşeni (CCNA) Kablosuz (*Wireless*)
Profesyonel	Cisco Sertifikalı Tasarım Profesyoneli (*Cisco Certified Design Professional* - CCDP) Cisco Sertifikalı Ağ Profesyoneli (*Cisco Certified Network Professional* - CCNP) Cisco Sertifikalı Ağ Profesyoneli (CCNP) Veri Merkezi Cisco Sertifikalı Ağ Profesyoneli (CCNP) Güvenlik Cisco Sertifikalı Ağ Profesyoneli (CCNP) Servis Sağlayıcı Cisco Sertifikalı Ağ Profesyoneli (CCNP) Servis Sağlayıcı Operasyonları Cisco Sertifikalı Ağ Profesyoneli (CCNP) Ses Cisco Sertifikalı Ağ Profesyoneli (CCNP) Kablosuz
Uzman	Cisco Sertifikalı Tasarım Uzmanı (*Cisco Certified Design Expert* - CCDE) Cisco Sertifikalı İnternet Ağı Uzmanı (*Cisco Certified Internetwork Expert* - CCIE) Veri Merkezi Cisco Sertifikalı İnternet Ağı Uzmanı (CCIE) Yönlendirme ve Anahtarlama Cisco Sertifikalı İnternet Ağı Uzmanı (CCIE) Güvenlik Cisco Sertifikalı İnternet Ağı Uzmanı (CCIE) Servis Sağlayıcı Cisco Sertifikalı İnternet Ağı Uzmanı (CCIE) Servis Sağlayıcı Operasyonları Cisco Sertifikalı İnternet Ağı Uzmanı (CCIE) Ses Cisco Sertifikalı İnternet Ağı Uzmanı (CCIE) Kablosuz
Mimar	Cisco Sertifikalı Mimar (*Cisco Certified Architect* - CCAr)

Juniper Ağ Teknolojisi

Juniper Ağ Teknolojisi, çeşitli ağ güvenliği donanımı ve yazılımı üretmektedir. Juniper, ayrıca ağ ürünleri için çeşitli sertifikalar da sunmaktadır. Cisco gibi, Juniper Ağ Teknolojisi çok sayıda sertifikasyon seviyesi ve farklı sertifikasyon alanı sunmaktadır. Sertifikalandırma, Juniper Ağ Teknolojisi donanımlarını kullanan kurum çalışanlarına ürünlerden en yüksek verimliliği almasında yardım eder.

Sertifika adayları, 11 farklı alandan 4 seviyede sertifika almaya hak kazanmak için dersler alabilir ve sınavlara katılabilirler. Juniper Ağ Teknolojisi her alan için tüm seviyelerde sertifika sunmaz. **TABLO 14 - 7**, Juniper Ağ Teknolojisi'nin sertifikasyon seviyelerini ve hangi seviyelerde hangi alanlarda sertifikalandırma olduğunu göstermektedir.

RSA

RSA, kurumsal ortamlar için güvenlik, risk ve uygunluk çözümleri sunan küresel bir kuruluştur. RSA ürünleri, kimlik güvencesi, veri kaybını önleme, şifreleme ve tokenizasyon cihazlarını içerir. Ayrıca, güvenlik uzmanlarının RSA ürünlerini etkili bir şekilde kullanma bilgi ve becerilerini edinmelerine ve göstermelerine yardımcı olmak için özel eğitim ve sertifikalar da sağlamaktadır. RSA, kuruluşlar bünyelerinde yaygın olarak çeşitli kapasitelerde RSA ürünlerini kullandığı için, çeşitli sertifikasyon seçenekleri sunar. RSA, şu anda RSA Archer ve RSA SecurID sertifikalarını sunmaktadır. Her belgelendirme, başvuranın bir veya daha fazla zorunlu dersi almasını ve ardından gerekli bir sınava girmesini gerektirir.

NOT

Juniper Ağ Teknolojisi sertifikaları hakkında daha fazla bilgi için *www.juniper.net/us/en/training/certification/* adresindeki web sitesini ziyaret ediniz.

NOT

RSA sertifikaları hakkında daha fazla bilgi için *www.emc.com/training/rsa-education-services/certification.htm* adresindeki RSA web sitesini ziyaret ediniz.

Symantec

Symantec Corporation, çok çeşitli güvenlik yazılım ürünleri sunmaktadır ve diğer tedarikçiler gibi kendi ürün grupları için sertifikalar sunar. Sertifikalandırma, belirli ürün eğitimini sağlar ve Symantec ürünleri ile ilgili uygulamacıların bilgi ve becerilerini doğrular. Aşağıda Symantec Sertifikalı Uzman (*Symantec Certified Specialist* - SCS) programındaki sertifikaların bir listesi sunulmaktadır:

NOT

Symantec sertifikaları hakkında daha fazla bilgi için *https://www.symantec.com/products-solutions/training/certification/* adresindeki Symantec web sitesini ziyaret ediniz.

- UNIX için Veritas Storage Foundation 6.0 Yönetimi
- UNIX için Veritas Cluster Server 6.0 Yönetimi
- UNIX için Symantec NetBackup 7.5 Yönetimi
- Symantec Enterprise Vault 10.0 for Exchange Yönetimi
- Symantec Endpoint Protection 12.1 Yönetimi
- Symantec Backup Exec 2012 Yönetimi
- Windows için Veritas Storage Foundation and High Availability Solutions 6.0 Yönetimi
- Windows için Symantec NetBackup 7.5 Yönetimi
- Symantec Client Management Suite 7.1/7.x Yönetimi
- Symantec Management Platform 7.1 Yönetimi

Juniper Ağ Teknolojileri

TABLE 14-7 Juniper Ağ Teknolojileri sertifikasyon düzeyleri ve alanları

ALAN	JUNIPER NETWORKS SERTİFİKALI İNTERNET EKSPERİ (JNCIE)	JUNIPER NETWORKS CERTIFIED INTERNET SPECIALIST (JNCIS)	JUNIPER NETWORKS CERTIFIED INTERNET PROFESSIONAL (JNCIP)	JUNIPER NETWORKS CERTIFIED INTERNET EXPERT (JNCIE)
E Serileri	JNCIA-E	JNCIS-E	JNCIP-E	
Kurumsal Yönlendirme ve Anahtarlama	JNCIA-ENT	JNCIS-ENT	JNCIP-ENT	JNCIE-ENT
Güvenlik Duvarı/VPN		JNCIS-FWV		
SaldırıTespit ve Önleme (IDP)	JNCIA-IDP			
Junos Sinyal (Pulse) Erişim Denetim		JNCIS-AC		
Junos Sinyal (Pulse) Güvenli Erişim		JNCIS-SA		
Junos Güvenlik)	JNCIA-JUNOS	JNCIS-SEC	JNCIP-SEC	JNCIE-SEC
QFabric		JNCIS-QF		
Servis Sağlayıcı Yönlendirici ve Anahtarlama	JNCIA-JUNOS	JNCIS-SP	JNCIP-SP	JNCIE-SP
Wireless LAN		JNCIS-WLAN		
WX	JNCIA-WX			

TABLE 14-8 Check Point sertifikaları.

SEVİYE	AĞ GÜVENLİĞİ	YÖNETİLEN GÜVENLİK	UÇ NOKTA GÜVENLİĞİ
İlişkili	Check Point Sertifikalandırılmış Güvenlik Prensipleri İştiraki (*Certified Security Principles Associate* - CCSPA)		
Yönetici	Check Point Sertifikalandırılmış Güvenlik Yönetimi (*Certified Security Administrator* - CCSA)		Check Point Uç Nokta Yönetimi (*End-point Administrator* - CCEPA)
Uzman	Check Point Sertifikalandırılmış Güvenlik Uzmanı (*Certified Security Expert* - CCSE)	Check Point Sertifikalandırılmış Yönetilen Güvenlik Uzmanı (*Certified Managed Security Expert* - CCMSE)	Check Point Sertifikalandırılmış Uç Nokta Uzmanı (*End-point Expert* - CCEPE)
İleri Seviye Uzman	Check Point Sertifikalandırılmış Yüksek Mimar (*Certified Master Architect* - CCMA)	Check Point Sertifikalandırılmış Yüksek Mimar (*Certified Master Architect* - CCMA)	

- Symantec Clearwell eDiscovery Platform 7.x Yönetimi
- Symantec Veri Kaybı Önleme (*Data Loss Prevention*) 11.5 Yönetimi
- Symantec Ağ Erişim Denetimi (*Network Access Control*) 12.1 Yönetimi

Symantec daha gelişmiş bir sertifikasyon da sunmaktadır. Symantec Sertifikalı Profesyonel (*Symantec Certified Professional* - SCP) sertifikası, SCS sertifikalarından çok daha fazla deneyim ve daha fazla bilgi sunar. Symantec, güncel olarak Bulut Güvenliği için SCP sertifikasını önermektedir.

Check Point

Ağ ve güvenlik aygıtları ve yazılımının bir başka küresel üreticisi Check Point'dir. Güvenlik uzmanları için Check Point ürünlerini kullanmada en üst seviyedeki bilgi ve becerileri teşvik etmek için eğitim ve sertifikasyon yolları sağlar. Güvenlik uzmanları, üç alan ve üç seviye arasından seçim yapabilecekleri çeşitli sertifikasyon seçeneklerine sahiptir. Check Point sertifikaları, başvuru sahiplerinin, %80'i eğitim materyali ve %20'si uygulamalı deneyim içeren bir sınavı geçmesini gerektirir. **TABLO 14 - 8**, her seviye ve alan için Check Point sertifikalarını göstermektedir.

NOT

Check Point sertifikaları hakkında daha fazla bilgi için *www.checkpoint.com/support-services/training-certification/index.html* adresindeki Check Point web sitesini ziyaret ediniz.

BÖLÜM ÖZETİ

Bu bölümde, var olan güvenlik sertifikalarından bazılarını öğrendiniz. Güvenlik sertifikaları yeterliliği garanti etmese de, işverenlere, sertifika sahibinin standart bir bilgi ve beceri düzeyine sahip olduğuna ilişkin güven verebilirler. Çoğu kuruluş, sınırlı bir süre için sertifika verir; bu nedenle sahip olunan niteliklerin var olan bilgi ve becerilerle

ilgili olduğunu da belirleyebilirsiniz. Satıcı bağımsız ve satıcıya özel sertifikaları öğrendiniz. $(ISC)^2$ ve CompTIA gibi organizasyonlardan alınan mesleki sertifikalar, satıcı bağımsız sertifikalardır. Cisco, Juniper ve Check Point gibi satıcıların sertifikaları ise satıcıya özeldir. Ayrıca, DoD/Askeri Yönerge 8570.01'nin bilgi güvencesi eğitimi, sertifikasyonu ve işgücü yönetimi için bir standart tanımladığını öğrendiniz. Bu, siber güvenlik alanındaki işgücü geliştirme için yeni Rol Temelli Standart 8140 ile değiştirildi.

Bilgi sistemlerinizin güvenliği veya bilgi güvencesi kariyeriniz boyunca gelişiminizi yönlendirmek, bilginizi ve deneyiminizi ölçmenize yardımcı olmak için sertifikaları kullanmanız gerekir. Bununla birlikte, değerinizi veya yeteneklerinizi sahip olduğunuz sertifikaların sayısıyla ölçmeyin. İşverenler beklentilerini değerlendirmek için sertifikalar kullanır ancak en iyi değerlendirme, olası adayın gerçek performansıdır.

ANAHTAR KAVRAMLAR VE TERİMLER

Certification – Sertifikasyon/ Sertifikalandırma

Job task analysis – İş görev analizi

Vendor-neutral certification – Satıcı bağımsız sertifikalandırma

Vendor-specific certification – Satıcıya özel sertifikalandırma

BÖLÜM 14 DEĞERLENDİRME

1. Bir sertifikasyon, kişinin belirli şartları yerine getirdiğini doğrulayan resmi bir bildirimdir.
   A. Doğru
   B. Yanlış

2. Hangi $(ISC)^2$ sertifikası uygulayıcılar için yedi güvenlik alanını kapsar?
   A. CISM
   B. CCNA
   C. SSCP
   D. GSEC
   E. Hiçbiri

3. Hangi $(ISC)^2$ sertifikası özellikle güvenli yazılım geliştirmeyi adresler?
   A. CISSP
   B. CSSLP
   C. GSEC
   D. CISA
   E. Hiçbiri

4. Aşağıdakilerden hangi sertifikasyon en üst seviyede GIAC kalite gereksinimini içerir?
   A. CAP
   B. GSEC
   C. GCIH
   D. GSE
   E. Hiçbiri

5. _____ Uzman ve Profesyonel sertifikalar, onaylı bir satıcının bir veya daha fazla sertifikasını bulundurmanızı gerektirir.

6. Hangi CompTIA sertifikası, temel güvenlik konularını hedeflemektedir?
   A. Güvenlik+
   B. TIA uygulayıcısı (*practitioner*)
   C. TIA+
   D. InfoSec uygulayıcısı
   E. Hiçbiri

7. Güvenlik denetçilerine hangi ISACA sertifikası uygulanır?
   A. CISSP
   B. SSCP
   C. GSEC
   D. CCNA
   E. Hiçbiri

8. _____ mesleki sertifikası, bilgi sistemleri denetimi gerçekleştirmeye özeldir.
   A. CISSP
   B. CISA
   C. GSEC
   D. CCNA
   E. Hiçbiri

9. Hangi ağ aygıt üreticisi beş seviyede sertifikasyon sunmaktadır: giriş, ilgili, profesyonel, uzman ve mimar?
   A. Cisco Systems
   B. Check Point
   C. Juniper Networks
   D. Symantec
   E. Hiçbiri

10. 10. Hangi satıcı, UNIX ve Windows ortamlarında kendi ürünleri için ayrı sertifikalar sunar?
   A. Cisco
   B. Check Point
   C. Juniper Networks
   D. Symantec
   E. Hiçbiri

11. DoD Yönergesi 8570'in temel amacı nedir?
   A. Yükleniciler dahil olmak üzere DoD iş gücünün, iş görevlerini yerine getirmek için asgari düzeyde eğitim ve sertifikasyona sahip olmasını şart koşar.
   B. Personelin güvenlik eğitimi almasını gerektirir.
   C. Personelin güvenlik sertifikalarını alması gerekmektedir.
   D. DoD bileşenlerine ve yüklenicilerine güvenlik eğitiminin sağlanması gerekir.
   E. DoD bileşenlerinde ve yüklenicilerinin güvenlik politikalarını uygulaması zorunlu tutulur.

12. Aşağıdakilerden hangisi bir iş görevi analizinin amacıdır?
   A. İlgili becerileri belirleme
   B. Gerekli bilgiyi tanımlama
   C. Gerekli deneyim miktarını belirleme
   D. İş tanımının mahkemede savunulabilir olduğundan emin olmak
   E. Hepsi

13. Satıcı bağımsız sertifika, satıcıya özel sertifikadan daha iyidir.
   A. Doğru
   B. Yanlış

14. Bir sertifikaya sahip olmak, işe ait bir görevi ya da fonksiyonu yerine getirme yetkinlik düzeyinizi garanti etmez.
   A. Doğru
   B. Yanlış

15. CompTIA Güvenlik+ sertifikasyonu için aşağıdakilerin hangisi doğrudur?
   A. Küresel olarak tanınmış olması
   B. Giriş seviyesinde temel sertifikasyonu sağlar
   C. Güvenlik terimlerini ve tanımlarını tam olarak anlamayı gerektirir
   D. Temel, giriş seviyesi bilgi sistemleri güvenlik eğitimi için DoD tarafından onaylanmıştır
   E. Hepsi

BÖLÜM

15

ABD Uyg

Siber uzay ABD vatandaşlarına ve kurumlarına her gün yeni tehditler getirmektedir. İnsanlar her zamankinden daha fazla veri paylaşıyor. İnsanlar internetten hizmet ve ürün almak için veri paylaşıyor. Çalışma arkadaşları ve diğer arkadaşları ile bağlantı kurmak için de veri paylaşıyorlar. Kurumlar işlerini yapmak için veri topluyor ve kullanıyor. Federal hükümet ve eyalet hükümetleri vatandaşlarına sunmak üzere veri topluyor ve kullanıyor.

Daha fazla veri toplanması, verinin yerinde kullanımı ile ilgili soru işaretleri doğuruyor. İnsanlar, hassas verilerini emanet ettikleri kurumların bu verileri korumak için adım atmalarını talep ediyor. Eğer kurumlar gönüllü olarak koruma sağlamazlarsa, insanlar çoğunlukla "Bir kanun bulunmalı" diyor. Birleşik Devletler'de kapsamlı bir veri koruma kanunu bulunmamaktadır. Bunun yerine, belirli veri türlerine odaklanmış federal veri koruma kanunları bulunur. Bu kanunlar kurumların topladıkları çeşitli veri türlerini korumak için güvenlik kontrolleri kullanmalarını gerektirir. Kanunlar tercihi değildir. Eğer bir kanun bir kurumu ilgilendiriyorsa, kurum kanuna uymak zorundadır. Bazen kurumların birden çok kanuna uyması gerekir. Bu bölüm ABD'de son 15 yıl içinde yürürlüğe girmiş uygunluk kanunlarını (*compliance laws*) sunmaktadır. Bu kanunların gizlilik ve mahremiyet gereklerine odaklanmaktadır. Bu bölüm ayrıca, kanun olmamakla birlikte, kart sahibi verisi (*card holder data* - CHD) saklayan, işleyen veya aktaran tüm kurumların takip etmesi gereken uluslararası Ödeme Kartı Endüstrisi Veri Güvenliği Standardı'nı (*Payment Card Industry Data Security Standard* - PCI DSS) tanıtmaktadır.

15. Bölüm Konular

Bu bölüm aşağıda verilen konuları ve kavramları içermektedir:

- Uygunluğun ne olduğu
- Federal Bilgi Güvenliği Modernizasyon Kanunu'nun (*Federal Information Security Modernization Act*)ne olduğu
- Sağlık Sigortası Taşınabilirlik ve Sorumluluk Kanunu'nun (*Health Insurance Portability and Accountability Act*) ne olduğu
- Gramm-Leach-Bliley Kanunu'nun ne olduğu
- Sarbanes-Oxley Kanunu'nun ne olduğu
- Aile Eğitim Hakları ve Mahremiyet Kanunu'nun (*Family Educational Rights and Privact Act*) ne olduğu
- Çocukların İnternetten Korunması Kanunu'nun (*Children's Internet Protection Act*)'nun ne olduğu
- Ödeme Kartı Endüstrisi Veri Güvenliği Standardı'nın (*Payment Card Industry Data Security Standard* - PCI DSS) ne olduğu
- Bilgi güvenliği uygunluk yasalarının nasıl anlaşılması gerektiği

15. Bölüm Hedefler

Bu bölümü tamamladığınız zaman, yapabilecekleriniz:

- Uygunluğun ne olduğunu ve bilgi güvenliği ile ilişkisini açıklamak
- Ana hatları ile Federal Bilgi Güvenliği Modernizasyon Kanunu'nu tanımlamak
- Ana hatları ile Sağlık Sigortası Taşınabilirlik ve Sorumluluk Kanunu'nu tanımlamak
- Ana hatları ile Gramm-Leach-Bliley Kanunu'nu tanımlamak
- Ana hatları ile Sarbanes-Oxley Kanunu'nu tanımlamak
- Ana hatları ile Aile Eğitim Hakları ve Mahremiyet Kanunu'nu tanımlamak
- Çocukları İnternetten Koruma Kanunu'nu tanımlamak
- Ödeme Kartı Endüstrisi Veri Güvenliği Standardı'nı tanımlamak

Uygunluk Kanunen Gereklidir

Kurumlar çok fazla veri kullanır ve depolar. Birçok kurum için, bilgi en önemli varlıklarındandır. Onu işlerini yapmak için kullanırlar. Müşterilerin ürün tercihlerini takip etmek için büyük ve karmaşık veritabanları kullanılır. Aynı bilgi teknolojilerini (BT) müşterilerine sundukları ürün ve hizmetleri yönetmek için de kullanırlar. Çoğunlukla bir çok insanın hassas olarak değerlendirdiği verileri toplarlar. Bunlar kişileri tanımlamak amacıyla kullanabileceğiniz, **kişisel tanımlayıcı bilgiler (*personally identifiable information* - PII)**'dir. PII şunları içermektedir:

- İlk isim, ikinci isim, soyadı
- Ev adresi
- Sosyal güvenlik numarası
- Ehliyet numarası
- Hesap numarası veya kişisel tanımlayıcı numarası (*personal identification number* - PIN) gibi finansal hesap verisi
- Sağlık verisi ve biyometrik veri
- Kullanıcı adı veya giriş adı ve şifreler gibi kimlik doğrulama delilleri

Maalesef, kurumlar bazen PII'ları korumada çok iyi bir iş çıkartmaz. Veriyi kaybedebilirler. Haber başlıklarında bundan *veri ihlali (data breach)* olarak bahsedilir. Aynı zamanda veriyi müşterilerinin uygun karşılamadığı şekilde kullanabilirler. Kurumlar PII'ları gönüllü olarak korumadığında hükümetler onları zorlamak için kanunlar çıkartır. Bu kanunlar yürürlüğe girdiğinde kurumlar onlara uymak zorundadır. Buna **uygunluk (*compliance*)** denir.

Uygunluk önemli bir hukuki kavramdır. Hukuk sistemi içerisinde uygunluk, kurumunuzla ilgili kanun, kural ve uygulamaları takip etme işlemidir. Bir kurum için uygunluk, sadece kanun ve uygulamaları takip etmeyi değil, aynı zamanda onları politika ve prosedürleri tanımlayacak şekilde

yorumlamayı içerir. Bir kurum, politika, prosedür ve ilkelerini uygunluk faaliyetlerinin bir parçası olarak belgelemek zorundadır. Bir kurum, dava açılması veya soruşturma yapılması durumunda uygunluğunu ispat edebilmek zorundadır.

Bir uygunluk kanununa tabi kurumların şunları yapması gerekir:

- Uygunluk kanununu ve gereklerini gözden geçirmek
- Kurumunuzun uygunluğundan sorumlu ve hesap verebilir bir uygunluk memuru veya şahıs atamak
- Kanuni ve düzenleyici gerekleri karşılayacak politikalar, standartlar, prosedürler ve ilkeler belirlemek
- Kurumunuzun uygunluk eksiklerini belirlemek ve bunları örtmek için önceliklendirme yapmak
- BT altyapınızda uygunluk kanununun gereklerini destekleyecek uygun güvenlik kontrolleri ve karşı tedbirleri hayata geçirmek
- Çalışanları kurumun yasal uygunluk gereksinimleri ile ilgili eğitmek için yıllık olarak güvenlik farkındalığı eğitimleri oluşturmak ve vermek

Uygunluk sadece uygun olma halini içermez. Aynı zamanda uygun hale gelmek için atılması gereken adımlar ve takip edilecek süreçleri içerir. Uygunluk çoğu zaman şu soruları sorar: Kurallar nelerdir? Kurallar nasıl takip edilmelidir? Eğer bir kurum yükümlülüklerini yerine getirmezse, cezalar ile karşılaşması mümkündür.

İPUCU

Eğer kurumunuz uygunluk içerisinde değilse, düzgün ileri yönlü gayret gösterilmesi çok önemlidir. Bir kurum kanunlara her gün uyduğunu ispat edebilmek zorundadır. Herhangi bir kurumun uygunluğu için başlangıç noktası politikaları, standartları, prosedürleri ve ilkeleri belirlemek ve belgelendirmektir. Belgelenen politika ve prosedürlerin uygulanması uygulama olgunluğunun kanıtlanması için gereklidir.

İPUCU

Kurumlar tipik olarak rol-tabanlı erişim kontrolü mekanizmaları kullanarak hassas verilerin gizliliğini temin eder. Hassas verinin ilgili harflerini "çarpılamak" için maskeleme kullanılır. Örneğin, 16 basamaklı bir başlıca erişim numarası (primary access number - PAN) şu şekilde maskelenir: XXXX-XXXX-XXXX-1234, 16 basamaklı bir kredi kartı numarasının sadece son 4 hanesi gösterilir. Tüm verinin şifrelenmesi elbette şu örnekte olduğu gibi hassas veriyi "okunamaz" yapacaktır: @#$2 – AAD8 – @#(+ – !@#D.

Birleşik Devletler'de kapsamlı bir veri koruma kanunu bulunmamaktadır. Bunun yerine, farklı işletme düzlemlerinde bulunan farklı veri türlerine odaklanan birden çok kanun vardır. Bu kanunlar mahremiyet ve bilgi güvenliği kavram ve gereklerini içerir. Aynı zamanda verinin nasıl kullanılacağına ve verinin nasıl korunacağına odaklanır. Birden çok federal kurum bu kanunlarla uygunluğu düzenler. Bu bölümde, bu kanunları kısaca öğreneceksiniz. Ancak bu kanunların uzun ve detaylı olduğuna ve burada sağlanandan daha detaylı inceleme gerektirdiğine dikkat etmelisiniz. Gerçekte, kanunların her biri kolaylıkla kendi başına bir kitap bölümü olabilir. Bu bölümün devamında, tüccar ve servis sağlayacıların kart sahibi verisini (CHD) nasıl depolayacağı, işleyeceği ve aktaracağına dair yönetsel bir standart olan ama kanun olmayan Ödeme Kartı Endüstrisi Veri Güvenliği Standardı (PCI DSS) sizlere tanıtılacak. **TABLO 15-1** ilgili kanunları, ilgilendikleri veri türünü ve uygunluğunu düzenleyen federal hükümet otoritesi veya sertifikasyon birimini listelemektedir.

Bilgi güvenliği sistemi uzmanları olarak sizler, kurumunuzu etkileyen uygunluk kanunlarını tanıyor olmalısınız. İşiniz kanunun yasal çıkarımlarını bilmekten ziyade kanunun kurumunuzu nasıl etkilediğini ve BT güvenliği perspektifinden yapmanız gerekenleri bilmektir. Bilgi güvenliği sistemi uzmanı olarak sizler, kurumunuzun hukuk müşaviri, yönetim kurulu ve BT kurumları ile çalışmaktan sorumlu olacaksınız.

TABLO 15-1 Bilgi güvenliğini etkileyen kanunlar.

KANUN ADI	DÜZENLENEN BİLGİ	DÜZENLEYEN KURUM
Çocukları İnternetten Koruma Kanunu (*Children's Internet Protection Act* - CIPA)	Belirli okullar ve kütüphanelerdeki internet erişimi	Federal Ticaret Komisyonu (*Federal Trade Commission* - FTC)
Aile Eğitim Hakları ve Mahremiyet Kanunu (*Family Educational Rights and Privacy Act* - FERPA)	Öğrencilerin eğitim kayıtları	ABD Eğitim Bakanlığı (*U.S. Department of Education* - DOE)
Federal Bilgi Güvenliği Yönetimi Kanunu (*Federal Information Security Management Act* - FISMA 2002)	Federal bilgi sistemleri	Yönetim ve Bütçe Dairesi (*Office of Management and Budget* - OMB)
Federal Bilgi Güvenliği Modernizasyon Kanunu (*Federal Information Security Modernization Act* - FISMA 2014)	Federal bilgi sistemleri	Yönetim ve Bütçe Dairesi (*Office of Management and Budget* - OMB) ve ABD Ulusal Güvenlik Bakanlığı (*U.S. Department of Homeland Security* - DHS)
Gramm-Leach-Bliley Kanunu (*Gramm-Leach-Bliley Act*- GLBA)	Tüketici finansal bilgisi	FTC
Sağlık Sigortası Taşınabilirlik ve Sorumluluk Kanunu (*Health Insurance Portability and Accountability Act* - HIPAA)	Sağlık bilgisi koruması	Sağlık ve İnsani Hizmetler Bakanlığı (*Department of Health and Human Services* - DHHS)
Ödeme Kartı Endüstrisi Veri Güvenliği Standardı (*Payment Card Industry Data Security Standard* - PCI DSS)*	Kart sahibi verisi: Adı ve soyadı, 16 basamaklı başlıca erişim numarası (PAN), üç basamaklı kimlik doğrulama kodu (CVV), son kullanma tarihi (AA/YY)	Ödeme kartı verenler: VISA, MasterCard, Discover, American Express ve JCB
Sarbanes-Oxley Kanunu (SOX)	Kurumsal finansal bilgi	Sermaye Piyasası Kurumu (*Securities and Exchange Commission* - SEC)

* PCI DSS uluslararası bir standarttır, kanun değildir.

Mahremiyet ve Bilgi Güvenliği Hangi Yönden İlgilidir?

Çoğu federal veri koruma kanunu hem mahremiyet (*privacy*) hem bilgi güvenliği (*information security*) gereksinimlerini içerir. Bilgi güvenliği ve mahremiyet yakından ilgilidir. Ancak, aynı olmadıklarını bilmek sizin için önemlidir. *Mahremiyet* bir kişinin kendi şahsi bilgisinin kullanım ve paylaşımını kontrol etme hakkıdır. Bu demektir ki, kişiler bir durumu değerlendirme ve verisinin nasıl kullanıldığını belirleme hakkına sahiptir. *Bilgi güvenliği* veriyi gizli tutmak için kullanılan süreçtir. Güvenlik süreçtir, mahremiyet ise sonuçtur.

Mahremiyet birkaç farklı ancak ilgili kavramı ifade eden bir terimdir. Özünde, mahremiyet bir kişinin kendi kişisel verisini kontrol etmesidir. *Kontrol* kişinin kendi verisinin nasıl toplandığı, kullanıldığı ve üçüncü taraflarla paylaşıldığına karar vermesi demektir. Bu bir kurumun mahremiyet politikası beyanı ile yerine getirilir. Bireylere kurumun mahrem verisini kullanması ile ilgili "kalmayı tercih (*opt-in*)" veya "ayrılmayı tercih (*opt-out*)" seçenekleri sunulur.

Mahremiyet üzerine çoğu geleneksel görüş hükümetin vatandaşların mahremiyetine karışma gücünün sınırlı olduğu inancını da içerir. Bu demektir ki kişiler ve bilgileri hükümetin gerekçesiz erişiminden bağımsız olmalıdır.

Hükümet kişileri veya kişilerin bilgilerini iyi bir gerekçe göstermeksizin incelememelidir. Mahkemeler hükümetlerin vatandaşlarını incelemelerine izin veren sebepleri tanımlamak için çok fazla zaman harcamaktadır. Bir çok Amerikalı için bu mahremiyet kavramının özüdür.

Bilgi sistemleri güvenliği BT altyapılarının ve içerdiği sistemlerin gizliliğini (*confidentiality*), bütünlüğünü (*integrity*) ve kullanılabilirliğini (*availability*) sağlama ile ilgilidir. Veriyi güvene almak bir şeydir veriyi gizli kılmak ise başka bir şeydir. Çoğu kurum kendi çalışanlarının müşterinin mahrem verisine erişimini engeller; örneğin, bazı müşteri ilişkileri yönetimi sistemleri bir bireyin Sosyal Güvenlik numarasının ilk beş basamağını kapatır, sadece son dört basamak ile kimlik doğrulaması yapılmasını gerektirir. Bilginin güvende olması gizli olması anlamına gelmez.

Bilgi güvenliği veri gizliliğini (*confidentiality*) sağlamak ile ilgilidir. Veri iş verisi veya müşterinin mahrem verisi olabilir. Veri şifreleme veriyi güvenli hale getirebilir. Rol tabanlı erişim kontrolleri sadece erişim hakkı verilmiş bireylerin gizli (*private*) veriye erişimini temin edebilir. Sistemler çalışanların rolüne göre veriye erişim imkanı tanır. Güvenlik kontrolleri uygulayarak kurum içerisinde veri mahremiyeti (*privacy*) başarılabilir.

Federal Bilgi Güvenliği

Federal hükümet ABD'deki en büyük veri üreticisi ve kullanıcısıdır[1]. Hükümetin BT sistemleri, hükümet operasyonları için kritik veriler saklamaktadır. Bu sistemler federal hükümetin işlerini yürütebilmesi için önemli olan verileri içerir. Aynı zamanda, hassas askeri verileri bulundurur. Bu sistemler ayrıca ABD vatandaşlarının kişisel verilerini bulundurur. Bütün bu kişisel veriler de çok hassastır.

Federal BT sistemleri ve içerisindeki veri çok çekici kriminal hedeflerdir. 2010 yılında, federal bilişim kurulu başkanı (*chief information officer* - CIO), Vivek Kundra, hükümetin bilgisayarlarının her gün milyonlarca defa saldırıya uğradığını söylemiştir[2]. Bu sürpriz değildir.

2002 Tarihli Federal Bilgi Güvenliği Yönetimi Kanunu

2002 yılında ABD Kongresi Federal Bilgi Güvenliği Yönetimi Kanunu'nu (*Federal Information Security Management Act* - FISMA)[3] oluşturdu. Bu kanun kısmen 11 Eylül 2001 terörist saldırılarına cevaben oluşturulmuştur. Saldırılar federal hükümet içerisinde daha iyi bilgi güvenliğine olan ihtiyacı vurgulamıştır. Saldırılardan sonra, hükümet federal BT sistemlerinin bilgisayar güvenliğinin olması gerektiği gibi olmadığını fark etti. FISMA, hükümetin bilgi güvenliğine yaklaşımını değiştirdi. Federal hükümetin eski bilgisayar güvenliği kanunlarının pek çoğunu hükümsüz kıldı. Şu anda, federal kurumların BT sistemlerini nasıl koruması gerektiğini tanımlayan ana kanun durumundadır.

FISMA federal kurumlar ve onların BT sistemleri için geçerlidir. Federal kurumlar ABD hükümetinin icra kolu altında yer almaktadır. Başkana rapor verirler. FISMA uygunluğundan Yönetim ve Bütçe Dairesi (*Office of Management and Budget* - OMB) sorumludur.

Amaç ve Başlıca Gereksinimler

FISMA *bilgi güvenliğini* federal kurumların BT sistemlerini gizlilik, bütünlük ve kullanılabilirlik[4] sağlamak amacıyla korumak olarak tanımlar. Kurumlar BT sistemlerini (ve içindeki veriyi) yetkisiz kullanım, erişim, bozulma, değiştirme ve yok edilmeye karşı korumalıdır. Başlıca sorumluluğunuz uygunluğu sağlamak amacıyla uygunluk kanununun gereksinimleri ile kurumunuzun güvenlik

kontrolleri arasındaki açığı kapatmaya yardımcı olmaktır. FISMA her federal kurumun aşağıdakileri içeren kurum çapında bir bilgi güvenliği programı oluşturmasını gerektirir:

- **Risk değerlendirmesi**—Kurumlar risk değerlendirmesi yapmalıdır. BT sistemlerinin yetkisiz erişimi veya kullanımından doğacak zararı ölçmelidir. Kurumlar bilgi güvenliği programlarını bu risk değerlendirmesini temel alarak oluşturmalıdır.
- **Yıllık envanter**—Kurumlar BT sistemlerinin envanterini tutmalıdır. Her yıl bu envanteri güncellemelidir.
- **Politikalar ve prosedürler**—Kurumlar riski kabul edilebilir seviyeye çekecek politika ve prosedürler oluşturmalıdır. Politikalar BT sistemlerini yaşam döngüleri boyunca korumalıdır. Kurumlar ayrıca kurulum yönetim politikaları belirlemelidir.
- **Alt planlar**—Kurumlar ağları, tesisleri ve sistemleri veya BT sistem gruplarını koruyacak planlara sahip olduklarından emin olmalıdır. Bu planlar daha büyük bir bilgi güvenliği programının parçası olan teknolojiler ve sistem bileşenleri içindir.
- **Güvenlik farkındalığı eğitimi**—Kurumlar çalışanlarına ve üstlenici firmalar dahil diğer tüm BT sistemi kullanıcılarına eğitim vermelidir. Bu eğitim, insanları kurumun BT sistemine karşı risklere dair bilinçli hale getirmelidir. Bu eğitim ayrıca, çalışanları sistemleri korumak için olan görevlerine dair bilinçli hale getirmelidir.
- **Test etme ve değerlendirme**—Kurumlar güvenlik kontrollerini en az yılda bir test etmelidir. Her BT sistemi için yönetimsel, operasyonel ve teknik kontrolleri yerine getirmelidir.
- **İyileştirici faaliyetler**—Kurumların bilgi güvenliği programlarının zayıflıklarını güçlendirmeye yönelik planları olmalıdır.
- **Ayrıcalıklı olay müdahalesi**—Kurumların ayrıcalıklı bir olaya *(incident)* yanıt prosedürleri olmalıdır. Kurumun ayrıcalıklı olayların nasıl farkına varacağını ve ayrıcalıklı olayları nasıl çözeceğini belirtmesi gerekir. Kurumlar ayrıca ayrıcalıklı olayları Ulusal Güvenlik Bakanlığı'na (*Department of Homeland Security* - DHS) raporlamalıdır.
- **Operasyonların sürekliliği**—Kurumların bilgi güvenliği programlarının bir parçası olarak iş sürekliliği planlarının bulunması gerekir.

Bir kurumun bilgi güvenliği programı kuruma ait BT sistemlerini veya veriyi kullanan diğer tüm kurumları da ilgilendirir. Bir kurum işleyişini destekleyen BT sistemlerini korumalıdır. BT sistemleri bir başka kuruma veya yükleniciye ait olsa dahi korumalıdır. Bu FISMA'nın kapsamını federal bir kurumun ötesine genişletebilir. Bu önemlidir çünkü BT sistemleri ve özellikleri çoğu zaman dışarıdan temin edilir. Sistem güvenliği uzmanları kendi BT sistemleri federal kurumlara ait herhangi bir bilgi kullanıyor veya işliyor mu bilmek durumundadır. Eğer öyleyse, FISMA uygulanabilir.

FISMA bilgi güvenliği programının en önemli kısımlarından biri, kurumlar tarafından test edilmesi ve değerlendirilmesidir. FISMA kurumların kendi BT sistemlerini en az yılda bir test etmesini gerektirir. Kurumlar, daha riskli BT sistemlerini daha sık test etmelidirler. Kurumlar ayrıca bu sistemler üzerindeki bilgi güvenliği kontrollerini gözden geçirmelidir. FISMA kurumların erişim kontrolü ölçütleri gibi belirli türlerde kontroller uygulamalarını gerektirir. Kurumlar kontrollerinin çalışmasından emin olmalıdır. Yıllık testler güvenliğin süregelen bir süreç olduğu kabulüyle yapılır. Kurumlar sürekli olarak güvenlik risklerini gözlemlemelidir. Ayrıca, bu riskleri karşılayacak kontrolleri de gözlemlemelidirler.

NOT

FISMA'ya göre, kurumlar bilgi güvenliğinden sorumlu bir üst düzey yetkili belirlemelidir. Çoğu durumda bu bilgi güvenliği başkanı (*chief information security officer* - CISO) olmaktadır. Bu yetkililer güvenlik konusunda tecrübe sahibi bilgi güvenliği uzmanları olmalıdır[5].

Her kurum OMB'ye yıllık olarak FISMA uygunluk işleri ile ilgili rapor vermelidir. Rapor kurumun bilgi güvenliği programını gözden geçirmelidir. Aynı zamanda, kurumun program veya güvenlik kontrolleri zayıflıklarını güçlendirmeye yönelik ilerlemesini değerlendirmelidir. Bir kuruma ait rapor geniş çaplı paylaşılır. Kurum birer kopyayı belirli kongre komitelerine ve diğer federal kurumlara göndermelidir. OMB kurumların rapor içerisinde BT sistemi faaliyetlerine dair çok detaylı bilgi vermemelerini söyler. Suçluların bu raporları okuyarak federal BT sistemlerinin zayıflıklarına dair bilgi edinmesi mümkündür.

FISMA'nın yıllık raporlama süreci zaman alır. Kurumlar raporlarını oluşturmak için çok fazla zaman harcarlar. OMB bunları değerlendirmek için çok fazla zaman harcar. Raporları değerlendirmek için üç tam zamanlı çalışanın bir aydan fazla çalışması gerekir[6]. Süreç aynı zamanda çok kağıt israf eder. Örneğin, Dışişleri Bakanlığı raporlama gereksinimlerini yerine getirmek için altı yılda 133 milyon dolar harcayarak 95.000 sayfa üretmiştir[7]. 2010 yılında, OMB bütün federal kurumların raporlarını elektronik olarak teslim etmesini gerekli kılmıştır. Yeni elektronik teslim aracı kurumlara ve OMB'ye kurumun bilgi güvenliği duruşunu daha hızlı değerlendirme imkanı sağlayacaktır[8].

NOT

OMB'nin 2010 FISMA raporu talimatlarını *www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy12_fisma.pdf*'den okuyabilirsiniz.

2014 Tarihli Federal Bilgi Güvenliği Modernizasyon Kanunu

2014 tarihli Federal Bilgi Güvenliği Modernizasyon Kanunu (*Federal Information Security Modernization Act*) 2014 yılı Aralık ayında yürürlüğe girmiştir. Kanun DHS'ye resmi olarak FISMA bilgi güvenliği, politika, prosedür ve güvenlik kontrollerini federal hükümetin görev alanında geliştirme, uygulama ve sağlama görevini vermiştir. FISMA 2014 yeni güvenlik gereksinimleri getirmez ancak FISMA güvenlik kontrolleri ve gereksinimlerinin tam anlamıyla uygulanması için gerekli olan rolleri, sorumlulukları, izlenebilirlikleri, gereksinimleri ve uygulamaları net olarak tanımlar.

Aşağıda FISMA 2002 ile FISMA 2014 mevzuatlarının bire bir karşılaştırması sunulmaktadır:

- OMB'ye ek olarak DHS, FISMA 2014 ile uygunluğun sağlanmasından sorumlu olan yönetici kurum olarak atanmıştır.
- ABD federal hükümet kurumlarının raporlama gereksinimleri tanımlanmıştır.
- Güvenlik ayrıcalıklı olayları için yeni rehberler ve raporlama gereksinimleri duyurulmuştur.
- Veri ihlali duyurusu uygunluğu için politika ve rehberler detaylandırılmıştır.

OMB'nin bilgi güvenliği politikaları ve uygulamalarını sağlama ve NIST'in geliştirdiği standart ve rehberleri denetleme sorumluluğu vardır. Tüm ABD federal hükümet kurumlarının bu yeni bilgi güvenliği politikalarına, standartlara, prosedürlere ve yönergelere uyduğunu sağlama çabaları DHS'in liderliğinde yapılır. FISMA 2014'ün getirdiği görev dağılımı OMB'nin DHS ile arasındaki siber güvenlik sorumluluklarını tanımlayan M-10-28 genelgesi ile uyumludur.

Güvenlik ayrıcalıklı olay müdahalesi raporlama ve veri ihlali duyurma FISMA 2014 mevzuatında açık olarak tanımlanmıştır. FISMA 2014 güvenlik olgusunu şöyle tanımlar: "Bir bilginin veya bilgi sisteminin gizlilik, bütünlük ve kullanılabilirliğini, kanuni temeli bulunmaksızın, fiilen veya yakın zamanda tehlikeye atan veya kanun, güvenlik politikası, güvenlik prosedürü veya uygun kullanım politikalarını ihlal eden, ihlalini tesis eden veya bunlara yakın tehdit oluşturan bir olaydır". Ek

olarak, artık her ABD federal hükümet kurumunun önemli ayrıcalıklı olayları yedi gün içinde kongreye ve ek olarak OMB ve/veya DHS'te bulunan ABD federal hükümet yetkililerine raporlama sorumluluğu bulunmaktadır.

NOT

2014 Tarihli Federal Bilgi Güvenliği Modernizasyon Kanunu'nun güncellenmiş halini şuradan okuyabilirsiniz: *www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy_2013_fisma_report_05.01.2014.pdf*.

Ulusal Standartlar ve Teknoloji Enstitüsü'nün Rolü

FISMA'nın her iki versiyonu da bilgi güvenliği standartları ve rehberleri oluşturulmasında ABD Ticaret Bakanlığı (*U.S. Department of Commerce*)'na güvenir. Ticaret Bakanlığı bu görevini kurumlarından biri olan Ulusal Standartlar ve Teknoloji Enstitüsü'ne (*National Institute of Standards and Technology* - NIST) devretmiştir. NIST bütün federal kurumların bilgi güvenliği programlarında kullanması için rehberler oluşturur. NIST kurumların veri ve BT sistemlerini sınıflandırmak için kullanacakları standartları oluşturur. Aynı zamanda, BT sistemleri için minimum bilgi güvenliği kontrollerini ve yönergeleri oluşturur. Kurumlar bu standartları ve yönergeleri takip etmelidir.

NIST iki farklı türde belge oluşturur. Bunlara Federal Bilgi İşleme Standardı (*Federal Information Processing Standards* - FIPS'ler) ve Özel Yayınlar (*Special Publications* - SP'ler) denir. FIPS'ler standartlardır. SP'ler yönergelerdir. FISMA'ya göre, federal kurumlar hem FIPS'leri hem SP'leri takip etmelidir.

NOT

Genel olarak, bir standart (*standard*) bir kurumun BT sistemlerini korumak için yapması gereken mecburi işlemleri belirtir. Bir yönerge (*guideline*), bir kurumun takip etmesi gereken tavsiye niteliğindeki işlemleri belirtir.

NIST, FISMA ile uygunluk için bir risk yönetim çerçevesi (*risk management framework* - RMF) kullanılmasını tavsiye eder[9]. Riski organize eden ve önceliklendiren hükümet kurumları bu riskten kaçınmayı sağlayacak bir bilgi sistemi güvenliği programı benimseyebilir. NIST RMF federal BT sistemlerini korumak için özetle altı basamak belirler:

Birleşik Devletler Bilgisayar Acil Durum Hazırlık Takımı

FISMA'ya göre, hükümetin bir federal ayrıcalıklı olaya yanıt (IR) merkezi olmalıdır. Bu merkezden OMB sorumludur. 2003 yılında, federal bir IR merkezini işletme sorumluluğu DHS'e verilmiştir. Selefini yeni bir IR merkezine dönüştürmüştür. DHS merkezinin adı Birleşik Devletler Bilgisayar Acil Durum Hazırlık Takımı (*United States Computer Emergency Readiness Team*) veya US-CERT'tir.

FISMA'ya göre, bütün federal kurumlar güvenlik ayrıcalıklı olaylarını US-CERT'e rapor etmelidir. Bunlar ulusal güvenlik sistemleri ile ilgili ayrıcalıklı olayları içerir. Bir ayrıcalıklı olay (*incident*), bilgisayar güvenlik politikası veya uygulamasının ihlalidir. Bu, politikalar ve uygulamaların ihlaline yönelik yakın tehditleri de içerir. Hükümetin alt IR kategorisi vardır. Kurumların ayrıcalıklı olayları belirli zaman aralıkları içerisinde raporlamaları gerekir. Raporlama aralığı ayrıcalıklı olay kategorisine göre değişir. Bazı ayrıcalıklı olayların fark edilir edilmez raporlanması gerekir.

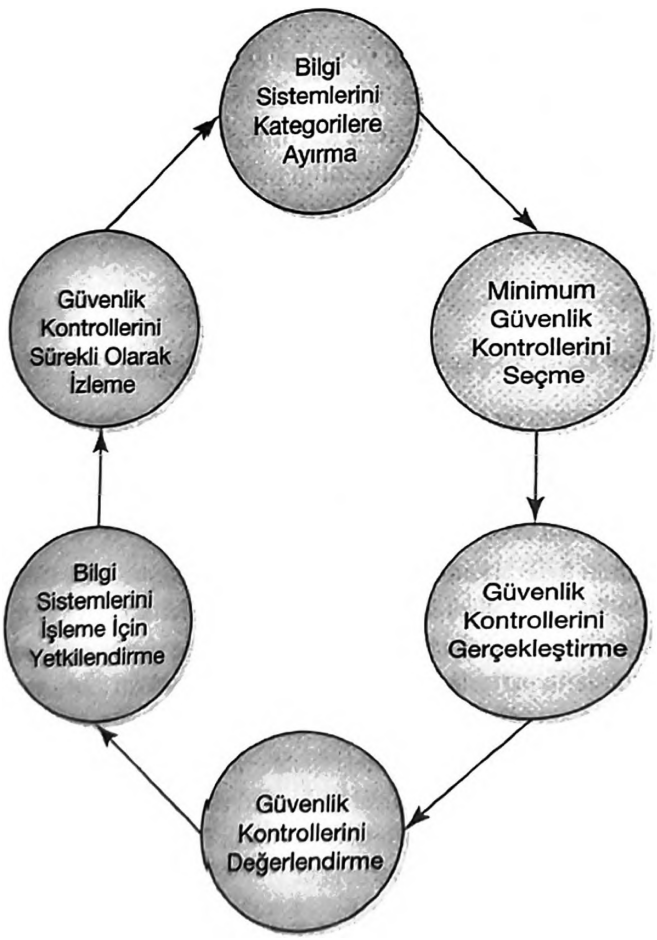
DHS'in desteklediği *www.us-cert.gov* sitesi işletme ve kullanıcılar için faydalı siber farkındalık içeriği sağlar. Daha teknik altyapısı olanlar uyarıları, güncel faaliyetleri veya bültenleri faydalı bulacaktır. Daha genel ilgiye tabi bilgiler arayanlar önerileri okuyabilir. Mutlaka Ulusal Siber Farkındalık Sistemi (*National Cyber Awareness System*) web sayfasını, *www.us-cert.gov/ncas*, ziyaret edin.

- **Bilgi sistemini kategorilere ayırma**—Kurum BT sistemlerini risklerine göre sıralamalıdır.
- **Minimum güvenlik kontrollerini seçme**—Kurum BT sistemleri için kontrolleri risk kategorisine göre seçmelidir.
- **Güvenlik kontrollerini BT sistemleri içinde uygulama**—Kurum kontrolleri NIST tarafından belirlenen alanlarda uygulamalıdır. Bunlar arasında erişim kontrolü, acil durum planlaması ve ayrıcalıklı olay müdahalesi bulunur.
- **Güvenlik kontrollerinin etkinliğini değerlendirme**—Kurum, riski düşürmedeki etkinliklerinden emin olmak için sürekli olarak kontrollerini değerlendirmelidir.
- **BT sistemini işlem için yetkilendirme**—Kurum, kendi BT sistemlerini test etmeli ve işletimlerini onaylamalıdır. Kurum bir sistemin işletilmesine izin vermeden önce işletim risklerini açıkça kabullenmelidir. Bu süreç FISMA terminolojisinde *sertifikasyon ve akreditasyon* olarak bilinir.
- **Güvenlik kontrollerini sürekli izleme**—Kurum, etkinliğinden emin olmak için sürekli olarak güvenlik kontrollerini gözlemlemelidir. Aynı zamanda BT sistemlerindeki değişiklikleri belgelemeleri gerekir. Değişiklikleri yeni risklere karşı değerlendirmelidir.

NIST'in sağladığı RMF sürekli bir kategorilere ayırma ve değerlendirme süreci tavsiye eder. Aynı zamanda sürekli izleme gerektirir. **ŞEKİL 15-1** RMF sürecini göstermektedir.

ŞEKİL 15-1

Risk yönetimi çerçevesi süreci.



Ulusal Güvenlik Sistemleri

FISMA federal kurumların ulusal güvenlik sistemlerini (*national security systems* - NSS'ler) risk tabanlı bir yaklaşımla korumalarını gerektirir. Bu sistemler şunlar için kullanılır:

- İstihbarat faaliyetleri
- Ulusal güvenlik
- Dış politika
- Askeri faaliyetler

Bu sistemlerin ulusal güvenlikteki önemleri sebebiyle özellikle korunmaları gerekir.

Ulusal Güvenlik Sistemleri Komisyonu (*Committee on National Security Systems* - CNSS) FISMA faaliyetlerini denetler. CNSS Birleşik Devletler Başkanı'na rapor verir. 21 oy veren üyesi bulunur. Bunlar arasında Ulusal Güvenlik Yönetimi (*National Security Administration* - NSA), Merkezi Haber alma Teşkilatı (*Central Intelligence Agency* - CIA) ve Savunma Bakanlığı (*Department of Defense* - DoD) yetkilileri bulunur. CNSS ile ilgili daha fazla bilgi edinmek için *www.cnss.gov* adresine bakabilirsiniz.

Ulusal güvenlik sistemi olan federal kurumların NIST RMF sistemlerini korumak için kullanılan ile aynı altı basamaklı süreci takip eden CNSS politikalarına uymaları gerekir. NIST ve CNSS bu politikaları belirlemek için birlikte çalışmıştır.

Sağlık Sigortası Taşınabilirlik ve Sorumluluk Kanunu

Çoğu insan sağlık bilgisinin en hassas kişisel bilgi türleri arasında olduğunu düşünür. Gizli detaylarla dolu olabilir. İnsanlar bu bilgiyi tedavi almak için sağlık hizmeti sağlayıcılarla paylaşırlar. Sağlık kayıtları içerisinde hastalık teşhisleri, laboratuvar sonuçları ve tedavi seçenekleri gibi detaylar bulunur. Bu kayıtlar ayrıca hayat tarzı, kronik rahatsızlıklar veya akıl sağlığı rehberliği gibi detaylar içerir.

İnsanlar sağlık verisinin saklı tutulmamasının kendilerini utandıracağından korkmaktadır. Bazı insanlar sağlık rehberliği alma sebepleri gibi özellikle mahrem gerçeklerin ortaya çıkmasının hayatlarını tehlikeye atacağından dahi endişelidir. Diğer insanlar şirketlerin veya işverenlerin onları sağlık kayıtlarında yer alan bilgilerden dolayı reddetmesinden çekinir.

İnsanlar çoğu zaman sağlık bilgilerinin nasıl paylaşıldığı veya korunduğu üzerinde çok az kontrol sahibi olduklarını düşünürler. Hemen her gün haberlerde bu endişeleri doğrulayan raporlar yer alır. Örneğin, 2009 yılı Kasım ayında, Northeast Inc.'a bağlı Health Net 1.5 milyon hastanın kayıtlarının kaybolan bir harici diskten etkilendiğini bildirmiştir. Disk aynı zamanda sağlık ağına bağlı hizmet veren doktorların kişisel bilgilerini içermektedir. Disk üzerindeki bilgiler şifrelenmemiştir.

Federal hükümet, sağlık bilgisini oldukça hassas olarak tanır. Onu korumak için Sağlık Sigortası Taşınabilirlik ve Sorumluluk Kanunu'nu oluşturmuştur.

Amaç ve Kapsam

Kongre, Sağlık Sigortası Taşınabilirlik ve Sorumluluk Kanunu'nu 1996 yılında geçirmiştir. 2009 yılında Ekonomik ve Klinik Sağlık için Sağlık Bilgisi Teknolojisi Kanunu (*Health Information Technology for Economic and Clinical Health* -HITECH) ile değiştirilmiştir. HIPAA kişisel olarak tanımlayıcı sağlık bilgisinin güvenlik ve mahremiyetine yönelik veri koruma kuralları ile tanınır. Sağlık ve İnsani Hizmetler Bakanlığı (*Department of Health and Human Services* - HSS) bu kuralları yapar ve uygunluğunu denetler.

HIPAA **korunan sağlık bilgisine (*protected health information* - PHI)** uygulanır. PHI bir kişinin sağlığına dair herhangi bir kişisel tanımlayıcı bilgidir. Akıl sağlığı ve fiziksel sağlık verisini ve ayrıca geçmiş, güncel ve geleceğe dair bilgiyi içerir[10]. Aynı zamanda sağlık hizmetinin nasıl ödendiği bilgisini içerir. PHI herhangi bir yapıda olabilir. Genelde bir kişinin sağlık kayıtları arasında olan bütün bilgiler olduğu değerlendirilir.

HIPAA'ya göre, kapsanan varlıklar PHI'yı yalnız belirli şekillerde kullanabilir. **Kapsanan varlıklar (*covered entities*)** kanun tarafından belirlenmiştir. HIPAA'yı takip etmesi gereken çok detaylı varlık türlerine atıfta bulunur. Bu varlıklar şunları içerir:

- Sağlık planları
- Sağlık hizmeti takas merkezleri
- Elektronik halde PHI aktaran herhangi bir sağlık hizmeti sağlayıcı

NOT

PHI sağlık kayıtlarınız doktorunuzun koyduğu notları da içerir. Aynı zamanda aldığınız sağlık hizmeti ile ilgili doktorunuzun herhangi bir başkası ile yaptığı görüşmeleri içerir. PHI içerisinde size sağlanan sağlık ürünleri ve hizmetleri için kesilen fatura bilgileri bulunur. Sağlık sigortası şirketinizin sağlık hizmetlerinize dair sahip olduğu bilgi de PHI olabilir.

Hangi varlıkların HIPAA tarafından kapsandığını tespit etmek karmaşık olabilir. Genel olarak, HIPAA bütün sağlık hizmeti sağlayıcıları kapsar. HHS varlıklara HIPAA tarafından kapsanıp kapsanmadıklarına karar vermek için araçlar sağlamıştır. Bu araçlara *www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html* adresinden erişilebilir.

HIPAA kapsanan varlıkların **iş ortaklarına (*business associates*)** da uygulanır. İş ortağı, kapsanan varlık için bir sağlık hizmeti faaliyetini yerine getiren bir kurumdur. Kapsanan varlıklar hak talebi ve faturalama gibi bazı sağlık hizmeti işlevlerini bu kurumlar üzerinden dışarıdan temin edebilirler. İş ortakları HIPAA'ya uymalıdır. HITECH kanununa göre, HHS iş ortaklarının HIPAA'ya uygunluğunu doğrudan talep edebilir.

2009 tarihli Amerika İyileştirme ve Yeniden Yatırım Yapma Kanunu'nun (*American Recovery and Reinvestment Act of 2009*) bir parçası olarak yürürlüğe giren HITECH kanunu, sağlık bilgisi teknolojisinin yaygın kullanımı ve standartlaştırılmasını teşvik etmek için tasarlanmıştı. Elektronik sağlık kaydı (*electronic health record* - EHR) sistemine geçen sağlayıcılar EHR platformuna geçişin maliyetini karşılamak için anlamlı kullanım teşvikine başvurabilecekler. Anlamlı kullanım programı gibi federal olarak desteklenen programlara katılım, sağlayıcıların HIPAA güvenlik ve mahremiyet kuralına uygunluğunu gerektirir.

HIPAA Mahremiyet Kuralının Temel Gereksinimleri

Mahremiyet Kuralı (*Privacy Rule*) kapsanan varlıkların PHI'nın gizliliğini nasıl koruması gerektiğini kararlaştırır. HHS son Mahremiyet Kuralı'nı Aralık 2000'de yayınladı. Mahremiyet Kuralı ile uygunluğun Nisan 2003'e kadar sağlanması gerekliydi. Mahremiyet Kuralı ile ilk defa ABD hükümeti PHI için federal mahremiyet koruması sağlamıştır.

Mahremiyet Kuralı'na göre, kapsanan varlıklar ilgili kişinin yazılı iznini almadan PHI kullanamaz veya açıklayamaz. *Kullanma (use)* terimi kapsanan varlığın kurum içerisinde PHI paylaşımı ve kullanımını ifade eder. *Açıklama (disclosure)* terimi kapsanan varlığın kendisi ile ilişkisi bulunmayabilecek başka kurumlarla PHI paylaşımını ifade eder.

Mahremiyet Kuralı'nın bazı istisnaları vardır. Bu istisnalar kapsanan teşekkülün kişinin yazılı izni olmaksızın ona ait PHI'ı paylaşmasına izin verir. PHI'ın ana izinli kullanım ve açıklama amacı,

Mahremiyet Kuralı'na göre bir kişinin tedavisi, ödemelerinin yapılması veya sağlık işlemlerinin yapılmasıdır. Bir kapsanan teşekkülün bu amaçlar için bir kişinin PHI'ını paylaşırken yazılı izne ihtiyacı yoktur çünkü çoğu insanın sağlık sağlayıcısının kendi PHI'ını tedavi amaçlı olarak kullanmasını isteyeceği varsayılmaktadır. Tedavi, ödeme ve sağlık işlemleri genel kapsanan varlık faaliyetleridir. Bu işlevleri yerine getirmek için birinin yazılı iznini aramak verimsiz olurdu.

Kapsanan bir işletmenin, çocuk istismarı ve ihmali mağdurlarının rapor edilmesi gibi, PHI'yı izinsiz olarak açıklayacağı başka durumlar da olabilir. İzinsiz PHI paylaşımına dair kurallar karmaşıktır. Kapsanan varlıkların kuralları dikkatle analiz ederek onları takip ettiğine emin olması gerekir.

Yazılı izin gerektirmeksizin PHI kullandığı veya açıkladığı durumlarda dahi kapsanan varlık **minimum ihtiyaç kuralına (*minimum necessary rule*)** uymalıdır.[11] Kapsanan varlık, PHI'nın sadece bilginin kullanma veya açıklama sebebinin gerektirdiği kadarlık kısmını açıklayabilir, daha fazlasını değil. Bir kapsanan varlık uzman değerlendirmesi kullanmalı ve PHI kullanımını veya açıklamasını sınırlamak için makul çaba sarf etmelidir. Eğer bir talebi karşılamak için bir kişinin sağlık kayıtlarının sadece bir kısmına ihtiyaç duyuluyorsa, bir sağlık hizmeti sağlayıcı tamamını açıklamamalıdır.

Kapsanan varlık kişileri nasıl PHI kullandığı ve açıkladığı konusunda bilgilendirmelidir.[12] Bunu bir mahremiyet bildirimi ile yapar. Kapsanan varlık sadece bu bildirimde belirtildiği yollarla PHI kullanabilir ve açıklayabilir. Mahremiyet Kuralı'nın bu bildirimlerin nasıl yazılması gerektiği ile ilgili pek çok gereksinimi vardır. Bu gereksinimlerin en önemlisi kapsanan varlığın bildirimi yalın bir dille yazmasıdır. Ortalama bir insan onu anlayabilmelidir.

Mahremiyet Kuralı kapsanan varlıkların izinsiz PHI kullanımı ve açıklamasını azaltmasını gerektirir.[13] HITECH Kanunu'ndan önce, bir kapsanan varlığın izinsiz şekilde PHI kullanımı veya paylaşımını kişilere bildirmesi şart değildi. HITECH Kanunu şu anda bunu gerektiriyor. Korunmamış PHI'nın ihlal edilmesi durumunda kapsanan varlıkların takip etmesi gereken bildirim gereksinimleri oluşturuyor.[14] Korunmuş sayılması için PHI, HSS onaylı bir süreç ile şifrelenmelidir.

> **NOT**
>
> HIPAA'ya göre bir ihlal *(breach)* korunmamış PHI'nın herhangi bir müsaade edilemez kullanım veya açıklama sonucu güvenliğinin veya mahremiyetinin zarar görmesidir. Kullanım veya açıklama, etkilenen kişinin zarar görmesi için önemli bir risk oluşturmalıdır. Zarar, finansal veya itibari olabilir.[15]

Hem kapsanan varlıklar hem iş ortakları ihlal bildirim kurallarını takip etmelidir. Eğer bir kapsanan varlık bir korunmamış PHI ihlali yaşarsa, bunun olay mağdurlarına olayın tespitinden sonraki 60 gün içerisinde bildirilmesi gerekir. Bir ihlal kapsanan varlığın haberdar olduğu ilk gün "tespit edilmiş" durumdadır. "Sebepsiz gecikme" olmaksızın bireylerin bilgilendirilmesi gerekir. Emniyet görevlilerinin talebi halinde bir kapsanan varlık bildirimi geciktirebilir. HIPAA'nın ihlal bildiriminin nasıl verilmesi gerektiğine dair pek çok kuralı vardır.

İhlal bildirim kurallarına göre, iş ortaklarının da korunmamış PHI ihlali tespit etmeleri halinde kapsanan varlığa bildirimde bulunma gereksinimi vardır. İş ortağı bir ihlal tespit ettiğinde, 60 günü geçmeksizin kapsanan varlığı bilgilendirmelidir. Kapsanan varlığın mağdurları bilgilendirmesine yardım etmelidir.

CMS, Medicare ve Medicaid Hizmetleri Merkezi (www.cms.gov) DHHS tarafından değerlendirilen veri ihlalleri veya HIPAA ihlalleri yaşamış kapsanan varlıkları fiilen takip eder. Buna ek olarak, CMS federal olarak desteklenen programlara katılan kapsanan varlıklar için bir kılavuz olan *Risk Yönetimi El Kitabı: Ayrıcalıklı Olay Yönetme (Risk Management Handbook: Incident Handling)* yayınını yayımlamıştır. Bu belge, *www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VII_7-2_Incident_Handling_Procedure.pdf* adresinde bulunabilir.

HIPAA Güvenlik Kuralının Başlıca Gereksinimleri

HHS'nin Güvenlik Kuralı 2005 yılından beri kapsanan varlıklar tarafından elektronik PHI'nın gizlilik, bütünlük ve kullanılabilirliğinin korunmasını gerektirmektedir. Bu kural kapsanan varlıkların **elektronik korunan sağlık bilgisini (*electronic protected health information* - EPHI)** korumak için tedbirler oluşturmasını gerektirir. EPHI, elektronik ortamda saklanan PHI'dır.

Mahremiyet Kuralı gibi Güvenlik Kuralı (*Security Rule*) da federal hükümetin elektronik PHI için ilk defa güvenlik tedbirleri ele alışıdır. Kural kapsanan varlıkların oluşturdukları, teslim aldıkları veya idare ettikleri bütün EPHI'yı korumasını gerektirir. Aynı zamanda aktardıkları EPHI'yı da korumaları gerekir.[16]

EPHI'yı mantık çerçevesinde öngörülen tehditlere karşı korumalıdırlar. Aynı zamanda Mahremiyet Kuralı tarafından izin verilmemiş kullanım ve açıklamalara karşı da korumalıdırlar.

Güvenlik Kuralı kapsanan varlıkların bilgi güvenliği programı oluşturmalarını gerektirir.[17] Bu programları nasıl oluşturacaklarında esnek davranabilirler. Belirli güvenlik teknolojilerini kullanmak zorunda değildirler. Kendi programını oluşturmak için, bir kapsanan varlık şunları göz önüne alır:

- Boyutu ve karmaşıklığı
- Teknik altyapısı, donanım ve yazılım güvenliği kaynakları
- Güvenlik tedbirlerinin maliyetleri
- EPHI'ya karşı potansiyel tehditler[18]

> **NOT**
>
> Bir bilgi güvenliği tedbirine aynı zamanda bilgi güvenliği kontrolü (*information security control*) denir. Farklı kanunlar ya tedbir (*safeguard*) ya da kontrol (*control*) terimini kullanır. Bazen kanunlar bu iki terimi alternatifli olarak kullanırlar. Aynı anlama gelirler.

Güvenlik Kuralı kapsanan varlıkların EPHI'yı korumak için aynı zamanda bilgi güvenliği prensipleri de kullanmasını gerektirir. İdari, fiziksel ve teknik tedbirler kullanmalıdırlar. Kural her tedbir türü için talimatlar içerir. Bazı tedbirler *gerekli*dir. Kapsanan varlıklar onları uygulamak zorundadır. Diğerleri *adreslenebilir*dir. Adreslenebilir şartları uygulamak kapsanan varlığın takdirindedir. Adreslenebilir şartlar için, varlık kontrolün mantıklı olup olmadığını ve ortama uygunluğunu değerlendirmelidir.[19] Eğer öyleyse, kapsanan varlık onu kullanmalıdır. Değilse, kapsanan varlık onu kullanmak zorunda değildir.

Güvenlik Kuralı'nın gerektirdiği tedbirlerinin yarısı idari kontrollerdir. Bunlar Güvenlik Kuralı'nı takip edecek kapsanan varlığın uygulaması gereken eylemler, politikalar, ve prosedürlerdir. Dokuz farklı idari tedbir vardır. **TABLO 15-2** bunları özetlemektedir.

Fiziksel tedbirleri bir kapsanan varlığın fiziksel kaynaklarını korumak için oluşturulmuş kontrollerdir. Bilgi sistemlerini, ekipmanları ve binaları çevresel tehditlerden korurlar. Güvenlik Kuralı dört fiziksel güvenlik standardı içerir. **TABLO 15-3** Güvenlik Kuralı'nın gerektirdiği gerekli ve değinilebilir fiziksel tedbirleri özetlemektedir.

Teknik tedbirleri bilgi sistemlerinin donanım ve yazılımına uygulanır. Güvenlik Kuralı beş teknik güvenlik standardı içerir. **TABLO 15-4** Güvenlik Kuralı'nın gerektirdiği gerekli ve değinilebilir teknik tedbirleri özetlemektedir.

Gözetim

HIPAA Mahremiyet ve Güvenlik Kuralları'na uygunluğu HSS denetler. Bu işlevini Vatandaşlık Hakları Dairesi'ne (*Office for Civil Rights* - OCR) devretmiştir. OCR, kuralları hem kapsanan varlıklara hem de iş ortaklarına uygular. Bir kapsanan varlığın HIPAA ihlali yaptığına dair iddiaları olan insanların şikayetlerini OCR araştırır ve yanıtlar.

TABLO 15-2 Güvenlik Kuralı yönetimsel tedbirleri.

TEDBİR	GEREKLİ ŞARTLAR	ADRESLENEBİLİR TANIM
Güvenlik Yönetimi Süreci	Risk analizi Risk yönetimi Yaptırım politikası Bilgi sistemi faaliyet değerlendirmesi	
Güvenlik Kuralı Uygunluğu için Yetkili Atanması	Gerekli	
EPHI Korumak için İşgücü Güvenliği Tedbirleri		Yetkilendirme ve/veya teftiş İşgücü erişim yetkilendirmesi İşten çıkarma prosedürleri
EPHI Erişimi Yönetimi	Sağlık hizmeti takas merkezi hizmetlerinin ayrılması	Erişim yetkilendirmesi Erişim oluşturma ve değişikliği
Güvenlik Farkındalığı ve Eğitimi		Güvenlik hatırlatıcıları Zararlı yazılımdan korunma Oturum izleme Parola yönetimi
Güvenlik Ayrıcalıklı Olay Prosedürleri	Müdahale ve raporlama	
Acil Durum Planlaması	Veri yedekleme planı Felaket kurtarma planı Acil durum işletme planı	Test etme ve revizyon prosedürü Uygulama ve veri kritiklik analizi
Güvenlik Tedbirleri Programının Değerlendirmesi	Gerekli	
İş Ortağı Sözleşmeleri ve Diğer Anlaşmalar	Yazılı sözleşmeler ve diğer anlaşmalar	

ABLO 15-3 Güvenlik Kuralı fiziksel tedbirler.

TEDBİR	GEREKLİ ŞARTLAR	ADRESLENEBİLİR TANIM
Tesis Erişim Kontrolleri		Acil durum işlemleri Tesis güvenlik planı Erişim kontrolü ve doğrulama prosedürleri Bakım kayıtları
İş İstasyonu Kullanımı	Gerekli	
İş İstasyonu Güvenliği	Gerekli	
Araç ve Depolama Ortamı Kontrolleri	Elden çıkarma Depolama ortamı yeniden kullanımı	İzlenebilirlik Veri yedekleme ve depolama

TABLO 15-4 Güvenlik Kuralı teknik tedbirler.

TEDBİR	GEREKLİ ŞARTLAR	ADRESLENEBİLİR TANIM
Erişim Kontrolü	Tekil kullanıcı tanıma Acil durum erişim prosedürü	Otomatik oturum sonlandırma Şifreleme ve şifre çözme
Denetim Kontrolleri	Gerekli	
Bütünlük		Elektronik korunan sağlık bilgisinin doğrulanması için düzenek
Kişi veya Varlık için Kimlik Denetleme	Gerekli	
Aktarım Güvenliği		Bütünlük kontrolleri Şifreleme

NOT

OCR ile uygunluğu olan süreç ile ilgili bilgiler *www.hhs.gov/ocr/privacy/hipaa/complaints/index.html* sayfasında bulunmaktadır.

OCR, HIPAA ile uygunluğu uygulayan polis gücü olarak hareket eder. OCR aynı zamanda HIPAA güvenlik veya mahremiyet kuralına uygunluğu ihlal eden bir kapsanan varlığa ceza yazabilir. HITECH Kanunu her HIPAA mahremiyet ihlalinin, dolayısıyla cezasının seviyesini değerlendiren katmanlı bir sistem tanımlamıştır:

- **Katman A**—Bu katman, failin kanunu ihlal ettiğini fark etmediği ve fark ederse ayrıcalıklı olayı daha farklı ele almış olacağı ihlalleri ifade eder. Sonuç, takvim yılı içerisinde aynı ihlaller için toplamı 25.000$'ı geçmeyecek şekilde her ihlal için 100$ cezadır.
- **Katman B**—Geçerli sebebe dayanan ancak "kasti ihmal" ile gerçekleşmiş ihlaller içindir. Sonuç, takvim yılı içerisinde 100.000$'ı geçmeyecek şekilde her ihlal için 1.000$ cezadır.
- **Katman C**—Kuruluşun en sonunda düzelttiği, kasti ihmale dayalı ihlaller içindir. Sonuç, takvim yılı içerisinde 250.000$'ı geçmeyecek şekilde her ihlal için 10.000$ cezadır.
- **Katman D**—Kuruluşun düzeltmediği kati ihmale dayalı ihlaller içindir. Sonuç, takvim yılı içerisinde 1.500.000$'ı geçmeyecek şekilde her ihlal için 50.000$ cezadır.

Geniş Kapsamlı Düzenlemeler

2013 Haziran ayında, HIPAA ve HITECH Kanun hükümlerinin tamamını güncelleyen bir Geniş Kapsamlı Kural (*Omnibus Rule*) yayınlanmıştır. Geniş Kapsamlı Kural kapsanan varlıkların ve iş ortaklarının gereksinimlerini şu yönlerden daraltır:

- Korunmamış PHI ihlallerinin raporlanması standardında değişiklik
- HHS'in yürütme yetkisinin iş ortaklarını kapsayacak şekilde genişletilmesi
- İş ortağı *(business associate)* terimi tanımının sağlık bilgisi kuruluşlarını, elektronik reçete ağ geçitlerini, PHI veri aktarımı hizmetleri sağlayan ve rutin PHI erişimi gerektiren varlıkları ve kişisel sağlık kaydı tedarikçilerini kapsayacak şekilde genişletilmesi

- İş ortaklığı anlaşmalarının gereksinimlerinde değişiklik
- İş ortaklarına iş ortaklığı anlaşmalarını belirtme zorunluluğu getirilmesi
- Kapsanan varlıkların iş ortaklarının davranış ve ihmalleri üzerindeki sorumlulukları ile ilgili sınırlamaların kaldırılması
- Mahremiyet uygulamalarının bildirim gereksinimlerinde değişiklikler
- PHI satışı üzerinde yeni sınırlamalar
- Pazarlama amacıyla PHI kullanımı ve açıklamalarına dair yeni sınırlamalar ve netleştirmeler
- Bağış toplama amacıyla PHI kullanımına dair belirli sınırlamaların kaldırılması
- Araştırma amacıyla PHI kullanımı ve açıklamalarına dair izinlerle ilgili mevzuatın geliştirilmesi

Kapsanan varlıkların ve iş ortaklarının HIPAA politikalarını, prosedürlerini, mahremiyet uygulaması bildirimlerini ve iş ortaklığı anlaşmalarını geniş kapsamlı düzenlemeye uyumlu olacak şekilde 30 Eylül 2013 tarihine kadar güncellemiş olmaları gereklidir.

Gramm-Leach-Bliley Kanunu

Verizon'un *2013 Tarihli Veri İhlalleri Araştırma Raporu (Data Breach Inverstigations Report)*'na göre, 2003-2012 yılları arasında 1.1 milyardan fazla kaydın gizliliğini ihlal eden 2.500'den fazla veri ihlali gerçekleşti.[20] Kurbanlar sürüsünün lideri, 2012'de gerçekleşen tüm veri ihlali mağdurlarının yüzde 37'si ile finansal kurumlardı. Çalışmaya göre, tüm ihlal suçlarının yüzde 92'si kurum dışı aktörlerce işlenmişti. Devlet bağlantılı, Çin Halk Cumhuriyeti ile ilişkili suçlular ABD'ye ait fikri mülkiyet (*intellectual property* - IP) varlığı çalma çabalarında liste başıydı. Bu bulgu tüm IP hırsızlığı ile ilgili ihlallerin yaklaşık beşte birine karşılık gelmektedir.

Tüketici finansal bilgisi kişisel tanımlayıcı bilgidir. Kişinin mal veya hizmet almak için tedarikçiye sağladığı bilgidir. Müşteriler onu bankalar veya diğer finansal kuruluşlardan hizmet almak için sağlayabilirler. Bu kuruluşlar bu veriyi ev veya araba kredisi sağlamak, kredi kartı onaylamak, veya cari hesap açmak için toplar ve kullanır. Müşteriler, finansal kuruluşlarının bu bilgiyi korumasını ister.

NOT

FTC'ye göre, sadece 2012 takvim yılında çalıntı kimlikle yapılmış alışveriş tutarı 21 milyar $'ı aşmıştır. Müşteri, finansal kuruluş ve satıcıların toplam zararı daha da yüksektir.

Gramm-Leach-Bliley Kanunu (*Gramm-Leach-Bliley Act* - GLBA) tüketici finansal bilgisinin mahremiyeti ve güvenliği ile ilgilidir. 1999 tarihli Finansal Hizmetleri Modernleştirme Kanunu (*Financial Services Modernization Act of 1999*) olarak da bilinen GLBA, bankacılık sektöründe büyük değişiklikler yaptı. Ana amacı bankalar, tahviller ve sigorta şirketlerinin birleşmesiydi. GLBA'den önce buna izin verilmiyordu. Finans sektörü müşterilerin tüm finansal hizmet ihtiyaçlarını tek bir firma kullanarak gerçekleştirebilmesi için Kongre'ye GLBA'yı geçirmesi yönünde baskı yaptı.

GLBA'dan sonra bu yeni, daha büyük şirketler daha geniş ölçekli tüketici finansal bilgisine erişebileceklerdi. İnsanlar mahremiyetlerinin zarar görmesinden korktu. Bu korkuyu dindirmek için, Kongre GLBA'ya mahremiyet ve güvenlik koruması ekledi. Bu, HIPAA kuralında olduğu gibi hem mahremiyet hem güvenlik gereksinimlerini şart koşar.

GLBA, ABD bankacılık sektörüne hizmet eden bir düzenleme kuruluşu olan Federal Finansal Kurumlar İnceleme Konseyi (*Federal Financial Institutions Examination Council* - FFIEC) ile uyum içindedir. Konsey, finansal kurumların Federal Rezerv Sistemi Yöneticiler Kurulu (*Board of Governors of the Federal Reserve Board* - FRB), Federal Mevduat Sigorta Fonu (*Federal Deposit Insurance Corporation*

- FDIC), Ulusal Kredi Birliği Yönetimi (*National Credit Union Administration* - NCUA), Para Birimi Kontrolör Dairesi (*Office of the Comptroller of the Currency* - OCC) ve Tüketici Finansal Koruma Bürosu (*Consumer Financial Protection Bureau* - CFPB) tarafından federal incelemesi için tek tip prensipler, standartlar ve rapor formları tanımlamak ve belirtmekle sorumlu olan resmi bir kurumlararası kuruldur. Konseye 2006 yılında eyalet planlı bankalara hitap etmesi için Eyalet İrtibat Komitesi (*State Liaison Committee* - SLC) eklenmiştir. Konsey aynı zamanda Eyalet Bankaları Denetleyicileri Birliği (*Conference of State Bank Supervisors* - CSBS), Amerikan Eyalet Tasarrufları Denetleyicileri Konseyi (*American Council of State Savings Supervisors* - ACSS) ve Ulusal Eyalet Kredi Birliği Denetleyicileri Derneği'nden (*National Association of State Credit Union Supervisors*) üyeleri içerir.

FFIEC Konseyi bankanızın veya finansal kuruluşunuzun siber güvenlik olgunluğunu tanımlamak için özdeğerlendirme aracı olarak kullanılabilecek bir Siber Güvenlik Değerlendirme Aracı (Değerlendirme) (*Cybersecurity* Assessment Tool (Assessment))geliştirmiştir. FFIEC Siber Güvenlik Değerlendirme Aracı iki parçadan oluşur:

- İçsel Risk Profili Durumu Değerlendirmesi (*Inherent Risk Profile Posture Assessment*)
- Siber Güvenlik Olgunluğu Durumu Değerlendirmesi (Cy*bersecurity Maturity Posture Assessment*)

FFIEC içsel risk profili durumu değerlendirmesi aşağıdaki kategorileri kapsar:

- Teknolojiler ve Bağlantı Türleri
- İletim Kanalları
- Çevrimiçi/Mobil Ürünler ve Teknoloji Hizmetleri
- Kuruluşun Karakteristikleri
- Harici Tehditler

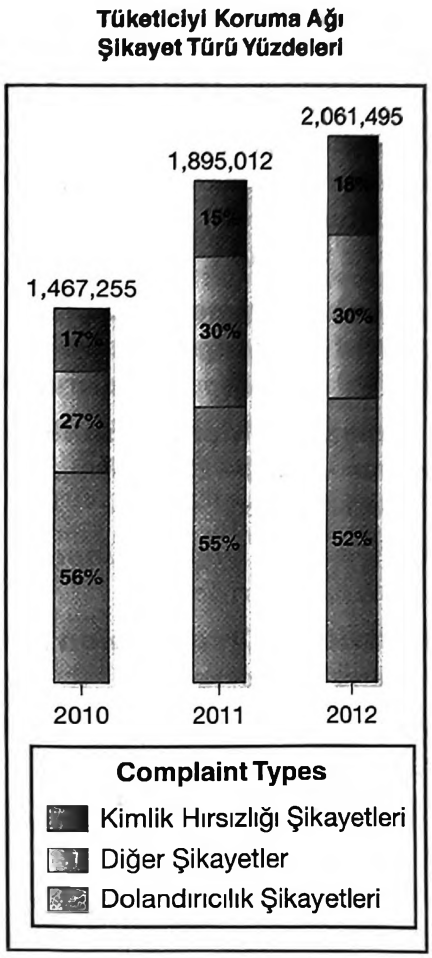
Buna göre yönetici kadronuzun kurumunuzun Siber Güvenlik Olgunluğu seviyesini aşağıdaki her bir alan için ölçmesi gereklidir:

- Siber Risk Yönetimi ve Gözetim
- Tehdit İstihbaratı ve İşbirliği
- Siber Güvenlik Kontrolleri
- Harici Bağımlılık Yönetimi
- Siber Ayrıcalıklı Olay Yönetimi ve Esneklik

Yönetim, kurumunuzun içsel risk profilini ve siber güvenlik olgunluğu durum seviyesini tüm alanlarda inceleyerek, riskleri azaltırken toplam siber güvenlik durumunu da güçlendirmek için açıkları kapatma ve sıkılaştırmaya gerek olup olmadığını değerlendirebilir. FFIEC, bir banka veya finansal kuruluşun süregelen risk yönetimi programını ve siber güvenlik uygulamalarını tamamlamaya alışkındır.

Federal Ticaret Komisyonu (*Federal Trade Commission* - FTC), *Tüketiciyi Koruma Ağı Veri Kitabı (The Consumer Sentinel Network Data Book)* içinde, kimlik hırsızlığı, dolandırıcılık, ve Ponzi şeması/oyunu gibi diğer tüketici ile ilgili sahtekarlıklara karşı tüketici şikayetlerini takip eder. 2012 Ocak-Aralık zaman aralığında, FTC dolandırıcılık şikayetlerinin yarıdan biraz fazlasını teşkil ettiği 2 milyondan fazla tüketici şikayeti kaydetmiştir (bkz. **ŞEKİL 15-2**).

Her yıl FTC dolandırıcılık ve kimlik hırsızlığı ile ilgili şikayetleri Tüketici Koruma Veritabanı (*Consumer Sentinel Database*) ile paylaşan bir rapor düzenler. En son yıllık raporu *www.ftc.gov/enforcement/consumer-sentinel-network/reports* adresinden indirebilirsiniz.



ŞEKİL 15-2
FTC tarafından belgelenen tüketici şikayetleri. Federal Ticaret Komisyonu'ndan çoğaltılmıştır.

Amaç ve Kapsam

Dolandırıcılık zafiyetlerinden dolayı, finansal kuruluşlar veri ihlallerini ve kimlik hırsızlığını azaltmaya yardım etmek için GLBA mahremiyet ve güvenlik kurallarını uygulamalıdır. Ödünç alma, borç verme, kredi danışmanlığı alma, borç toplama ve benzeri aktiviteler gibi herhangi bir finansal hareket, müşteri verisinin mahremiyetini sağlamak için özel özen gerektirir. Bu hareketler para ve yatırım ile ilgilidir. Bu tanım çok geniştir. Bu tür faaliyetlere girişen her kurum GLBA'yı uygulamalıdır. GLBA sadece müşterilerin finansal faaliyetleri için geçerlidir. Bunlar şahsi, ailevi veya hane halkı ile ilgili hizmetlere yönelik gerçekleşen hareketlerdir. GLBA iş hareketlerine uygulanmaz.

GLBA finansal kuruluşların tüketicilere ait kamuya açık olmayan finansal bilgiyi korumasını gerektirir. **Kamuya açık olmayan kişisel bilgi (*nonpublic personal information* - NPI)** bir tüketicinin bir finansal kuruluşa verdiği kişisel tanımlayıcı finansal bilgidir. Tüketicinin finansal bir hareket esnasında paylaştığı bilgidir. NPI ayrıca bir kuruluşun tüketiciden farklı kaynaklar üzerinden elde ettiği PII'yı da içerir. NPI kağıt üzerinde veya elektronik ortamda olabilir. GLBA'ya göre, NPI şunları içerir:

- Sosyal güvenlik numarası
- Finansal hesap numaraları
- Kredi kartı numaraları

- Doğum tarihi
- İsim, adres, ve finansal veri ile birlikte toplanmış telefon numaraları
- Herhangi bir hareketin detayları veya bir bireyin bir finansal kuruluşun müşterisi olduğu gerçeği

GLBA karmaşık bir kanundur. Uygunluğu temin etmek zor olabilir. Sebeplerden biri farklı federal kurumların GLBA denetleme sorumluluğu bulunmasıdır. Sorumluluk, incelenen finansal kuruluşun türüne göredir. GLBA denetleme sorumluluğu bulunan kurumlar şunlardır:

NOT

NPI, tüketicinin halka açık bir bilgisini içermez. Örneğin, bir kişinin telefon rehberindeki adresi halka açıktır.

- **Menkul Kıymetler ve Takas Komisyonu (*Securities and Exchange Commission* - SEC)**—Menkul kıymet aracılarını ve borsa ajanlarını denetler.
- **Amerikan Merkez Bankası (*Federal Reserve System* - FED)**—Eyalet planlı üye bankaları ve banka sahibi şirketleri denetler.
- **Federal Mevduat Sigorta Fonu (*Federal Deposit Insurance Corporation* - FDIC)**—Fed'e üye olmayan eyalet planlı bankaları denetler.
- **Ulusal Kredi Birliği Yönetimi (*National Credit Union Administration* - NCUA)**—Federal olarak sigortalanmış kredi birliklerini denetler.
- **Para Birimi Kontrolör Dairesi (*Office of the Comptroller of the Currency* - OCC)**—Ulusal planlı bankaları denetler.
- **Tasarruf Teftiş Dairesi (*Office of Thrift Supervision* - OTS)**—Bütün ulusal planlı ve bazı eyalet planlı tasarrufları denetler.
- **Federal Ticaret Komisyonu (*Federal Trade Commission* - FTC)**— GLBA'ya göre diğer kurumlardan biri tarafından düzenlenmemiş herhangi bir finansal kuruluşu denetler.

GLBA Mahremiyet Kuralı'nın Başlıca Gereksinimleri

GLBA Mahremiyet Kuralı[21] 1 Temmuz 2001'de yürürlüğe girdi. Tüm GLBA düzenleme kurumları onu yaratmak için bir arada çalıştı. Bu kurala göre, bir finansal kuruluş bir tüketicinin NPI'sını ilintili olmayan üçüncü taraflarla paylaşamaz. Bir finansal kuruluş bu bilgiyi ancak tüketiciye mahremiyet uygulamaları bildirimini ilk gönderişinden sonra paylaşabilir. Bu bildirim tüketiciye kuruluş tarafından toplanan veri türleri hakkında bilgi vermelidir. Aynı zamanda toplanan bilginin kuruluş tarafından nasıl kullanıldığını belirtmelidir. Bildirim ayrıca kuruluşun tüketicinin NPI'sını nasıl koruduğunu açıklamalıdır. Mahremiyet Kuralı tüketicilerin ilintili olmayan üçüncü taraflarla veri paylaşımının belirli türlerinden ayrılmayı tercih etme hakkına sahip olmalarını gerektirir.

GLBA müşteriler ve tüketiciler arasında bildirim gereksinimlerinde bir ayrıma gider. Bir *tüketici* bir finansal kurumdan tüketici finansal ürünü veya hizmeti alan herhangi bir şahıstır. Bir *müşteri* kuruluşla sürekli bir ilişki içinde olan bir tüketicidir. Müşteri ilişkisi olmayan tüketiciye bir örnek, kendi şahsi bankasına ait olmayan bir ATM'den para çeken bir şahıstır. Şahıs bankanın ATM hizmetinin tüketicisidir ancak bankanın müşterisi değildir. Müşteriler finansal kurumun mahremiyet bildirimlerini teslim almalıdır. İlintili olmayan şahıslarla tüketici NPI'sını paylaşmayan finansal kuruluşların tüketicilere mahremiyet bildirimi vermesi gerekmez.

Bir kuruluşun müşteri ilişkileri başlar başlamaz müşteriye mahremiyet uygulamalarını bildirmesi gerekir. Aynı zamanda ilişki sürdüğü sürece müşterilerin her yıl mahremiyet bildiriminin bir kopyasını teslim alması gerekir. Bildirim yazılı olarak sunulmalıdır ve anlaşılır olmalıdır.

İlintili olmayan şahıslarla tüketici NPI'sını paylaşmayı planlayan finansal kuruluşların tüketicilerine mahremiyet bildirimi vermesi gerekir. Mahremiyet bildiriminin tüketiciye finansal kuruluşun ilintili olmayan üçüncü taraflarla tüketici NPI'sını paylaşmasını durdurma imkanı tanıması gerekir. Buna *ayrılmayı tercih koşulu (opt-out provision)* denir. Mahremiyet bildirimi şahıslara nasıl ayrılacaklarını açıklamalıdır. Eğer bir tüketici ayrılmazsa, finansal kuruluş mahremiyet bildiriminde açıklanan yollarla NPI paylaşabilir.

NOT

İlintili olmayan taraf (nonaffiliated party) finansal kuruluş ile yasal bağı bulunmayan bir varlıktır. Bağlı taraflar ile aynı şey değildir. Bağlı taraflar *(affiliated parties)* yasal ilişki içindedir. Aynı kurumsal ailenin üyeleridirler. Bir bağlı şirket bir varlığı kontrol eden, onun tarafından kontrol edilen veya bir başka varlığın ortak kontrolü altında olan taraftır.

GLBA tüketicilere finansal kuruluşun bağlı şirketleri ile NPI paylaşması durumlarından ayrılmayı tercih etme hakkı tanımaz. Bazı örneklerde, tüketicilerin ayrılmayı tercih etme imkanı dahi bulunmaz. Örneğin, tüketiciler kanunen gerekli bir açıklamadan ayrılmayı tercih edemez.

GLBA Tedbirler Kuralı'nın Başlıca Gereksinimleri

GLBA finansal kuruluşları düzenleyen kurumların takip etmesi için güvenlik standartları yayımlamasını gerektirir. Bu gereksinime Tedbirler Kuralı denir. Kanun her kurumun şunları yapan güvenlik standartları oluşturmasını gerektirir:

- Müşteri verisinin güvenliğini ve gizliliğini koruma
- Müşteri verisini güvenliği veya bütünlüğüne karşı tehditlerden koruma
- Müşteri verisini bir müşterinin zarar görmesi ile sonuçlanabilecek yetkilendirilmemiş erişimler veya kullanımlara karşı koruma[22]

Mahremiyet Kuralı'nın aksine, GLBA denetim sorumluluğu bulunan kurumlar bir tedbir kuralını birlikte oluşturmamıştır. SEC kendi kuralını Haziran 2000'de yayımladı. Fed, FDIC, NCUA, OCC, ve OTS ortak bir kuralı birlikte çalışarak 2001'in başlarında yayımladı. FTC kendi Tedbirler Kuralı'nı Mayıs 2002'de yayımladı. Bu kurallar birbirine çok benzer. Kolaylık olsun diye, bu bölümde FTC'nin Tedbirler Kuralı'ndan bahsedilecektir.

FTC Tedbirler Kuralı (FTC Safeguards Rule)[23] bir finansal kuruluşun yazılı olarak *bilgi güvenliği programı* oluşturmasını gerektirir. Program kuruluşun müşteri verisini nasıl topladığını ve kullandığını belirtmelidir. O veriyi korumak için kullanılan kontrolleri de açıklamalıdır. Finansal kuruluşlar idari, teknik veya fiziksel kontroller kullanmalıdır. Program kağıtta ve elektronik ortamda bulunan bilgiyi korumalıdır.

Tedbirler Kuralı finansal kuruluşlara bazı esneklikler tanır. Bütün kuruluşların takip etmesi gereken genel güvenlik programı gereksinimleri içermez. Bunun yerine, finansal kuruluşların kendi boyut ve karmaşıklıklarına uygun programlara sahip olmalarını gerektirir. Programlar ayrıca kuruluşun kullandığı müşteri verisinin hassasiyetine uygun olmalıdır. Daha hassas olan veri daha fazla koruma gerektirir. Kural kuruluşların aynı zamanda şunları yapmasını gerektirir:

- Programı yürütecek bir çalışan atamak
- Müşteri bilgisine yönelik riskleri tanımlamak için risk değerlendirmesi yürütmek

- Güncel tedbirlerin etkin olduğunu değerlendirmek
- Riskleri kontrol edecek tedbirleri tasarlamak ve uygulamak
- Servis sağlayıcılar seçmek ve bunlarla olan sözleşmelerin müşteri bilgisini korumaya yönelik maddeler içerdiğinden emin olmak
- Yapılan işteki değişiklikleri göz önüne alarak bilgi güvenliği programını düzenli olarak gözden geçirmek

Tedbirler Kuralı finansal kuruluşlara müşteri verisini en iyi koruyacak kontrolleri seçme imkanı tanır. Kuruluşlar, programlarını belirtilen üç alanda gözden geçirmelidir:

- Çalışan yönetimi ve eğitimi
- Bilgi sistemleri tasarımı
- Saldırıları ve sistem arızalarını tespit ve bunlara müdahale

Gözetim

GLBA uygunluğunu denetleyen kurumlar, düzenledikleri finansal kuruluşları yasal takibe alabilir. GLBA'yı ihlal eden kuruluşlara ceza verilebilir. Para cezaları azımsanmayacak miktarlarda olabilir.

GLBA finansal kuruluşların mahremiyet ve güvenlik kurallarını takip etmesini gerektirir. Eğer kuruluşunuz finansal bir kuruluşsa veya finansal faaliyetleri varsa, bu kuralları bilmeniz gerekir. Kuruluşunuzun BT sisteminin kanun ile uygunluk içinde işlediğinden emin olmak istersiniz.

Sarbanes-Oxley Kanunu

2000'lerin başlangıcı birçok kurumsal skandalla sarsıldı. Enron, Adelphia ve WorldCom gibi şirketler hatalı ve yanıltıcı finansal raporlama uygulamaları ile haberlere çıktı. Bu uygulamalar şirketleri olduklarından daha başarılı göstererek yatırımcıları aldattı. Kurumsal çalışanlar da dahil birçok yatırımcı, büyük miktarlarda para kaybetti. Herkes gerçekleri öğrendiğinde yatırımcı zararlarının kurtarılması mümkün değildi. Bu skandallar ortaya çıktığında ABD ekonomisinde yatırımcı güveni sarsıldı. Sonuç olarak, 2000 ile 2009 yılları arasındaki on yılda borsa gelmiş geçmiş en kötü performansını yaşadı.[24]

Doğru bilgi, "yatırımcının en iyi aracı"dır.[25] İnsanlar akıllı yatırım yapıp para kazanabilmek için doğru finansal bilgiye ihtiyaç duyar. Yatırımcıların dolandırıcılığı tespit etmesi zordur. Kongre, yatırımcıları korumak için 2002 yılında Halka Açık Şirket Muhasebesi Reformu ve Yatırımcı Koruma Kanunu (*Public Company Accounting Reform and Investor Protection Act*)'nu geçirdi.[26] Bu kanun yaygın olarak **2002 yılı Sarbanes-Oxley Kanunu (*Sarbanes-Oxley Act*)** olarak bilinir. Birçok kaynakta SOX veya Sarbox olarak adlandırılır. Başkan George W. Bush SOX'u 30 Temmuz 2002 günü imzalayarak yasalaştırdı. O zaman SOX için "Franklin Delano Roosevelt'in zamanından beri Amerikan iş uygulamalarındaki en kapsamlı reformlardır." dedi.[27]

Amaç ve Kapsam

SOX'un ana hedefi yatırımcıları finansal dolandırıcılıktan korumaktır. SOX diğer federal güvenlik kanunlarını tamamlar. Sermaye Piyasası Kurumu'na kayıtlı olması gereken **halka açık şirketlere** uygulanır. Yatırımcılar borsada hisseleri satın almak yoluyla bir halka açık şirketin sahibi olurlar. SOX **özel şirketlere** uygulanmaz.

SOX pek çok hüküm içeren detaylı bir kanundur. Yürürlüğe ilk girdiğinde birçok şirket BT bileşenleri bulunmadığını varsaymıştır. Kongre kanunun hiçbir yerinde BT'den bahsetmemiştir. Bu görüş, şirketler SOX'u daha dikkatli incelediğinde değişmiştir. Çoğu SOX hükmü şirketlerin finansal bilgilerinin doğruluğunu teyit etmesini gerektirir. BT sistemleri birçok finansal bilgi türü içerdiği için, şirketler ve denetleyiciler bu sistemlerin SOX ile uygunluğun bir parçası olduğunu hızla fark ettiler. Bu, o sistemlerin kullanım yollarının ve alınması gereken güvenlik tedbiri kontrollerinin SOX ile uygunluk için gözden geçirilmesi gerektiği anlamına geliyordu.

> **NOT**
>
> En popüler iki ABD borsası New York Borsası (*New York Stock Exchange - NYSE*) ve NASDAQ Borsası'dır. Ulusal sermaye takaslarının SEC tarafından kayıt altına alınması gerekir. Daha fazlasını *www.sec.gov/divisions/marketreg/mrexchanges.shtml* adresinden öğrenebilirsiniz.

BT ile SOX uygunluğu arasındaki ilişki evrim geçirmeye devam ediyor. Bu bölüm SOX'un 404. paragrafının (*Section* 404) sertifikalandırma gereksinimlerine odaklanmaktadır. 404. paragraf bir kuruluşun icra yetkililerinin şirketin finansal raporlamaları üzerindeki iç kontrollerinin (*internal controls over financial reporting* - ICFR) etkinliğini oluşturmasını, korumasını, gözden geçirilmesini ve raporlanmasını gerektirir. Bir kuruluşun yöneticileri bu sertifikasyonları alabilmek için şirketin BT sistemlerinin nasıl çalıştığını anlamalıdır. Bu bölüm uygunluk sağlamaya çalışan BT uzmanlarının başını çok ağrıtmıştır.

SOX Kontrol Sertifikasyonu Gereksinimleri

SOX'un 404. paragrafı bir şirketin yönetici kadrosunun şirketin ICFR'ının etkinliğini raporlamasını gerektirir. Yönetim bu sertifikasyonu şirketin finansal raporlarının doğruluğunu temin etmeye yardımcı olmak için alır. Yatırımcıları hileli finansal faaliyetlere karşı korumaya yardımcı olur. Yönetim, bu sertifikasyonu şirketin SEC'e teslim ettiği belgeler üzerine almalıdır.

Bir şirket ICFR'ını oluşturmalı, belgelendirmeli ve test etmelidir. Her yıl ICFR üzerine raporlama yapmalıdır. Şirketin yıllık raporunu yapmasının ardından dış denetçiler onu gözden geçirmelidir. Dış denetçiler raporda belirtilen ICFR'ın doğruluğunu teyit etmelidir.

SEC kurallarına göre, ICFR bir kuruluşun finansal raporlarının güvenilir olduğuna dair mantıklı güvence sağlayan süreçlerdir. ICFR yönetime şu konularda mantıklı güvence sağlar:

- Finansal raporlar, kayıtlar ve veri doğrulukla muhafaza edilmektedir.
- Hareketler muhasebe kurallarına uygun olarak hazırlanmakta ve düzgün bir şekilde kaydedilmektedir.
- Finansal beyanları etkileyebilecek veri veya varlıkları yetkisiz temin etme veya kullanma durumları engellenecektir ve oluşmaları zamanında saptanacaktır.

404. paragraf ile uygunluk sağlamaya çalışan şirketler BT sistemlerini gözden geçirmeleri gerektiğini hemen farkettiler. Özellikle ICFR'ın BT sistemleri ile ilgili kısımlarını gözden geçirmeleri gerekiyordu. Bir Ernst & Young anketine göre, SOX uygunluğu almanın ilk yılında olan şirketler vakitlerinin %70'ini BT kontrollerini irdelemeye harcamaktadır.[28] Şirketler BT kontrollerine

çok zaman harcar çünkü finansal veri BT sistemleri içindedir. Bu sistemlerdeki bir hata finansal beyanların yanılgı ve hatalar içermesine sebep olabilir. 404. paragraf ile uygunluk için, şirketler sistem verisinin doğru olduğundan emin olmalıdır. Tutarsız veriyi tespit etmek için gerekli süreçlerin bulunduğundan emin olmaları gerekir.

SOX'un 404. paragrafı ile uygunluk kolay değildir. 404. paragraf şirketlerin uygulaması gereken ICFR türlerini çok genel olarak ele almaktadır. ICFR için genellikle detaylı bir tanım vermez. BT kontrollerinden bahsetmez. 2007 yılında, SEC şirketlere 404. paragraf denetlemeleri esnasında ICFR değerlendirmesi yapabilmeleri için ek rehberler yayınladı. Bunu 404. paragraf denetlemelerinin geniş kapsamı ile ilgili alınan çok sayıda şikayet sebebiyle yaptı. Bu şikayetlerin çoğu BT kontrollerinin nasıl irdeleneceği üzerineydi.

SEC rehberinde iki genel prensip duyurdu:

- Yönetim dahili kontrollerin finansal raporlardaki eksiklikleri nasıl engellediği ve tespit ettiğini değerlendirmelidir.
- Yönetim bu kontrollerin etkinliğini risk-tabanlı olarak gözden geçirmelidir.

NOT

SOX, şirketlerin uygulaması gereken BT kontrollerini belirtmez. Bunun yerine, şirketler kendi sistemleri için en iyi kontrolleri belirlemelidir.

SEC aynı zamanda yönetimin 404. paragraf denetlemesinin kapsamını kısıtlamak için kendi uzman hükmünü kullanması gerektiğini söyledi. Şirketlere SOX'un BT kontrolleri de dahil olmak üzere sadece finansal raporları etkileyecek dahili kontrollere uygulandığını hatırlattı.[29] Bu demektir ki 404. paragraf denetlemesi kesinlikle finansal veri işleyen BT sistemlerini içerir. Finansal olmayan veri işleyen BT sistemlerini içermeyebilir.

Yönetim genel BT kontrollerini gözden geçirerek BT sistemlerinin düzgün ve tutarlı çalıştığından emin olmalıdır. Kuruluşlar BT kontrollerini değerlendirmek için birçok yaklaşım kullanırlar. Kontroller yönetime BT sistemlerinin finansal raporları korumak üzere düzgün işlediğine dair mantıklı güvence sağlamalıdır. **TABLO 15-5**, ICFR hedeflerinin bilgi güvenliği hedefleri ile nasıl eşleştiğini göstermektedir.

Bir şirket SOX'un 404. paragrafına karşı olan sorumluluğundan finansal görevlerini dışarıya aktararak kaçamaz. SOX şirketlerin ICFR'larının dışarı aktarılmış işlemlerle ilgili kısımlarını da gözlemlemesini gerektirir. Birçok şirket bunu dış kaynak tedarik ettikleri şirketlerden dışarı aktarılmış işlemleriyle ilgili özel bir denetim raporu isteyerek yapar. Bir şirket bu raporu dış kaynak tedarik ettikleri şirketin kontrollerinin yeterliliğine karşı değerlendirmelidir.

TABLO 15-5 İç kontroller ve bilgi güvenliği hedefleri.

DAHİLİ KONTROLLERE YÖNELİK ADIMLAR	BİLGİ GÜVENLİĞİ HEDEFLERİ
Finansal raporlar, kayıtlar ve veri doğru tutulmaktadır.	Bütünlük
Hareketler GAAP kurallarına göre hazırlanmıştır ve düzgün kaydedilmiştir.	Bütünlük, kullanılabilirlik
Finansal beyanları etkileyebilecek, veri veya varlıkları yetkisiz temin etme veya kullanma durumları engellenecektir ve oluşmaları zamanında saptanacaktır.	Gizlilik, bütünlük, kullanılabilirlik

SOX Kayıtları Saklama Gereksinimleri

SOX bazı kayıt saklama hükümleri içerir. Bir sistem güvenliği uzmanı olarak bu gereksinimleri bilmelisiniz. Çünkü birçok şirket kayıtlarını elektronik olarak depolar. Bazı çalışmalar tüm iş belgelerinin %93'ünün elektronik olarak oluşturulduğunu ve depolandığını öngörmektedir.[30] Şirketlerin, SOX saklama gereksinimlerini karşılaması için, BT sistemlerinin nasıl çalıştığını anlaması gereklidir. Elektronik kayıtların nasıl yönetileceği ve korunacağına yardım etmede şirketinize faydalı olacaksınız.

SOX halka açık şirketlerin finansal denetim belgelerini yedi yıl saklamalarını gerektirir.[31] Denetimde kullanılan çoğu belge denetim belgesidir. Bunlar bir denetim raporunun sonuçlarını destekleyici materyallerdir. SOX'un kaydedilmesi gereken belge türleri ile ilgili geniş bir bakış açısı vardır. Bu iş belgeleri, notlar ve yazışmalardır. Aynı zamanda denetimle ilgili olarak oluşturulan, gönderilen ve alınan kayıtları da içerir. SOX elektronik kayıtları da içerir.

SOX halka açık bir şirketin finansal raporlama üzerindeki dahili kontrollerini değerlendirmek için kullandığı kayıtları ve belgeleri saklaması gerekir.[32] SEC tarafından yayımlanan rehber bu belgelerin birden farklı yapıda olduğunu belirtir. Elektronik veriyi de içerir. Şirketler bu bilgiyi kalıcı olarak saklamalıdır.

Kayıtları doğru süre boyunca saklamamanın cezası ağır olabilir. SOX, kayıt saklama hükümlerini bilerek ve isteyerek ihlal etmeyi bir kişi veya şirket için suç sayar. Bu hükmü ihlal eden bir kişi 10 yıla kadar hapis cezası alabilir.

Gözetim

Sermaye Piyasası Kurumu çoğu SOX hükmünü denetler. SEC, 1934 tarihli Sermaye Piyasası Kanunu ile oluşturulmuştur. Görevi yatırımcıları korumak ve sermaye piyasasının bütünlüğünü temin etmektir. SEC, SOX'a uymayan halka açık şirketleri inceleme ve onaylama gücüne sahiptir.

SEC'in ABD başkanı tarafından atanan beş komisyon üyesi vardır. Bu üyeler beş yıl süreyle görevlidir. Üyelerin üçten fazlası aynı siyasi partiye üye olamaz. SEC'in Birleşik Devletler'de 11 bölgesel çalışma yeri vardır.

SOX, SEC'in halka açık bir şirketin yıllık ve üç aylık raporlarını üç yıl içinde en az bir defa gözden geçirmesini gerektirir.[33] Bunu yatırımcı kişilere zarar verebilecek dolandırıcılıkları ve hatalı finansal beyanları tespit etmeye çalışmak için yapmalıdır. SEC'in şirketleri ne sıklıkla gözden geçireceğine takdir yetkisi vardır.

Bilginize

Birçok federal kanun ve eyalet kanunu kayıt saklama gereksinimi içerir. SOX bu listeye eklenen bir başka kanundur. Şirketler farklı mesuliyetlerini takip etmek için belge saklama politikaları geliştirmelidir.

Aile Eğitim Hakları ve Mahremiyet Kanunu

Üniversite, yüksekokul ve ilköğretim okulları öğrencilere dair bir sürü bilgiye erişim sahibidir. Aşağıdaki öğrenci bilgisi türlerini toplayabilir ve depolayabilirler:

- Nüfus bilgisi
- Adres ve iletişim bilgisi
- Ebeveynlerin nüfus bilgisi
- Ebeveynlerin adres ve iletişim bilgisi
- Not bilgisi
- Disiplin durumu bilgisi

Bu veriler öğrencileri eğitmek için öğrenim kurumlarına faydalıdır. Bu bilgiler çok hassas olabilir. Bir eğitim kurumunun bu bilgileri üçüncü taraflarla uygunsuz şekilde paylaşması ihtimali gizlilikle ilgili kaygıya sebep olur. Öğrenci veya ailesi için utandırıcı bir durum gelişebilir. Aile Eğitim Hakları ve Mahremiyet Kanunu (*Family Educational Rights and Privacy Act* - FERPA) öğrenci bilgisinin mahremiyetini koruyan başlıca federal yasadır.

Amaç ve Kapsam

Kongre FERPA'yı 1974 yılında oluşturdu.[34] Federal kaynak kullanan herhangi bir eğitsel kuruluşa uygulanır. Eğitsel kuruluşlar şunları kapsar:

- Halk üniversiteleri
- Yüksekokullar ve üniversiteler
- İlk ve ortaöğretim okulları (anasınıfından 12 yaşa kadar)
- Eyalete ait veya yerel eğitim kurumları (bir okul yönetim kurulu gibi)
- Okul öncesi eğitim veren okullar veya kurumları
- Federal kaynak kullanan herhangi başka bir eğitim kuruluşu

Bu bölüm bu eğitim kuruluşlarının hepsinden *okul* olarak bahseder. Çoğu eğitim kuruluşu ABD Eğitim Bakanlığı'ndan bir şekilde kaynak alır. Eğer bir okul FERPA ile uygun olmayı seçmezse, hiçbir federal kaynak alamaz. Federal kaynaklar okullar için önemlidir. Sonuç olarak hemen hemen okulların tümü FERPA ile uygundur. Bazı küçük özel okulların federal kaynak almıyor olması mümkündür. Eğer federal kaynak almıyorlarsa, FERPA ile uygun olmaları gerekmez.

FERPA birçok hükmü olan detaylı bir kanundur. Başlıca amacı öğrenci kayıtlarının mahremiyetini korumaktır. Bir öğrenci kaydı, okulun öğrenci ile ilgili tuttuğu her veriyi içerir. Bu kayıtlar yazılı belgeleri, bilgisayar ortamlarını, videoları, filmleri ve fotoğrafları içerir. Aynı zamanda okul adına hareket eden dış taraflarca tutulan kayıtları da içerir. Bu kayıtlar kağıtta veya elektronik ortamda olabilir.

FERPA öğrenci kayıtlarını korumak için özel bilgi güvenliği kontrollerinin uygulanmasını gerektirmez. Ancak, sistem güvenliği uzmanlarının FERPA'nın gereksinimlerinden haberdar olmaları gerekir. Eğer bir kuruluş eğitim kuruluşu ise veya bir okul için kayıt tutuyorsa FERPA

Bilginize

Bu bölüm boyunca kullanılmış olan soyut kişisel tanımlayıcı bilgi tanımının aksine, FERPA kişisel tanımlayıcı bilgiyi somut olarak tanımlar. Herhangi bir kanunu okuduğunuzda, o kanunun belirli terimleri nasıl tanımladığını mutlaka kontrol etmelisiniz. Bazen bir kelimenin kanuni tanımı jenerik tanımından çok farklı olabilir.

kullandığı veriyi ilgilendiriyor olabilir. O zaman, kuruluş elektronik öğrenci kayıtlarının mahremiyetini korumak için BT sisteminde güvenlik kontrolleri uygulamalıdır.

Başlıca Gereksinimler

FERPA'ya göre öğrenciler (veya 18 yaşını doldurmamışlarsa ebeveynleri) aşağıdaki haklara sahiptir:

- Öğrencinin öğrenci kaydında hangi verilerin olduğunu bilme hakkı, kaydı inceleme ve gözden geçirme hakkı
- Bir okuldan öğrenci kaydındaki yanlışları düzeltmesini talep etme hakkı
- Belirli öğrenci verisinin açıklanmasına onay verme hakkı

Bir okul öğrencilerinin kayıtlarını korumalıdır. Özel olarak, kayıtlarında yer alan kişisel tanımlayıcı bilgiyi korumalıdır. FERPA'ya göre, kişisel tanımlayıcı bilgi öğrencinin adı, Sosyal Güvenlik numarası ve öğrenci numarası gibi doğrudan tanımlayıcı bilgileri kapsar. Aynı zamanda öğrenci adıyla eşleştirilebilecek dolaylı tanımlayıcıları kapsayabilir. *Dolaylı tanımlayıcılar (indirect identifiers)* öğrencinin belirlenmesi için kolaylıkla kullanılabilecek kişisel özelliklerdir. Genelde bir okul, öğrencinin yazılı izni olmaksızın üçüncü taraflara öğrenci kaydı veremez.

Okulun öğrencinin izni olmaksızın öğrenci kaydı açıklayabileceği bazı istisnalar vardır. Örneğin, bazı okul yetkilileri iş görevleri gerektirdiğinde öğrenci kayıtlarını inceleyebilir. Ek olarak, bir okul, öğrencinin izni olmaksızın bir öğrencinin kaydını eski okulundan yeni okuluna aktarabilir. Okullar öğrenci kayıtlarını finansal yardım veya denklik almak amacıyla aktarabilir. Okullar hakim kararı veya mahkeme çağrısına uymak için bazı öğrenci bilgilerini açıklayabilir.

FERPA özel bir kişisel tanımlayıcı bilgi kategorisinin öğrenci onayı olmaksızın açıklanmasına izin verir. Bir okul, öğrenciye bu bilgiyi açıklayacağına dair bildirim verdiği sürece bunu yapabilir. Bu bilgi kategorisine **dizin bilgisi (*directory information*)** denir. Dizin bilgisi tüm öğrenciler için kamuya açık olan bilgidir. Dizin bilgisi öğrencinin adı, adresi veya telefon numarası gibi bilgiler içerir. Çoğu okul bu bilgiyi açıklar. Yüksekokul ve üniversiteler çoğunlukla bu tür bilgiyi çevrimiçi dizine yerleştirir.

Bir okul dizin bilgisini öğrencinin izni olmaksızın açıklayabilir. Ancak, bir öğrenci kendisine dair bu tür bilginin açıklanmasını yasaklamayı tercih edebilir. Öğrenci bu tür bilgiyi açıklamamasını okula söylemelidir. Eğer bir öğrenci okula dizin bilgisini açıklamamasını söylerse, okul bu bilginin açıklanmamasını sağlayacak önlemleri almalıdır.

FERPA okulların öğrenci ve ailelere okulun FERPA faaliyetleri ile ilgili yıllık bildirimler yapmasını gerektirir. Bu bildirim, öğrencilere ve ailelerine FERPA hakları konusunda bilgi verir. Öğrencilere, izinleri olmaksızın kayıtlarına erişebilen okul yetkililerini söyler. Örneğin, FERPA okul kayıtlarına erişmek için yasal eğitsel menfaati olanların öğrencinin onayı olmaksızın ona erişmesine izin verir.

Okul bu yetkilileri tanımlamalıdır. Öğretmenler, eğitim elemanları, öğretim üyeleri olabilirler. Müdürler veya dekanlar gibi idari yetkililer de olabilirler.

Yüksek öğretim kurumları için çalışan BT ve bilgi sistemi güvenliği uzmanları da FERPA ile uygun olmalıdır. Öğrenicinin mahremiyet verisi PII ve transkript notlarını içerir. Tipik olarak, okullar gizli öğrenci verisini kayıt taşıma ve yüksek lisansa geçişte paylaşırlar. Yüksek öğretim kurumlarının BT bölümleri öğrencinin mahremiyet verisinin gizliliğini sağlamakla yükümlüdür.

NOT

Öğrenci veya ebeveyn olarak sahip olduğunuz FERPA mahremiyet haklarınızla ilgili daha fazla bilgi için *www.ed.gov/policy/gen/guid/fpco/ferpa/index.html* adresini ziyaret ediniz.

Gözetim

FERPA ile uygunluğu Aile Politikası Uygunluk Dairesi (*Family Policy Compliance Office* - FPCO) denetler. FPCO'nun FERPA şikayetlerini gözlemleme ve araştırma yetkisi vardır. FERPA'yı ihlal eden okullar federal kaynaklarını kaybedebilirler. FERPA hakları ihlal edilen öğrencilerin okulu bu sebeple dava etme hakkı yoktur. FERPA'yı ihlal eden okullara karşı sadece FPCO yaptırım yetkisine sahiptir.

Çocukları İnternetten Koruma Kanunu

Çocukların İnternetten Korunması Kanunu'nun (*Children's Internet Protection Act* - CIPA) amacı çocukların internetteki rahatsız edici içeriğe maruz kalmasını engellemektir. CIPA kamusal okul sistemlerinin ve E-Rate federal kaynağı kullanan kamu kütüphanelerinin CIPA ile uygun olmalarını gerektirir. CIPA ebeveynlere ve ücretsiz, kamuya açık kablosuz internet erişimi sağlayıcılarına çocuklarımızı rahatsız edici içerikten korumak için en iyi yöntemi temin eder.

Amaç ve Kapsam

Kongre CIPA'yı 2000 yılında geçirdi.[35] Bazı okulların ve kütüphanelerin, rahatsız edici İnternet içeriğini filtrelemelerini, böylece çocukların bu içeriğe erişememelerini gerektirir. CIPA, 17 yaşın altındaki herkesi çocuk olarak tanımlar. Rahatsız edici içerik, müstehcen, çocuk pornosu veya çocuklara zarar verebilecek görsel tasvirler içerir (eğer bilgisayarlar çocuklar tarafından erişiliyorsa). CIPA "küçüklere zararlı" ifadesini şu özelliklerdeki herhangi bir görsel resim olarak tanımlar:

- Küçüklere uygun olmayacak şekilde; çıplaklık, cinsellik veya dışkılamaya şehvetli bir ilgi içeren
- Küçüklere uygun olmayacak şekilde; cinsel ilişki, temas veya organı açıkça, rahatsız edici biçimde resmeden, tarif eden veya yansıtan
- Küçüklere uygun olmayacak şekilde; bütün olarak ele alındığında, ciddi bir edebi, sanatsal, politik veya bilimsel değerden yoksun olan

Bütün okul ve kütüphanelerin CIPA ile uygun olması gerekmez. Ama E-Rate programından federal kaynak alan herhangi bir okul veya kütüphane olmalıdır. E-Rate programı çoğu ilkokul, ortaokul ve kütüphane için internet erişiminde indirim sağlar.

İndirimler gerçek maliyetlerin %20 ile %90'ı arasındadır. Okul ve kütüphanelerin bu kaynakları kabul etmesi zorunlu değildir. İnternet erişimine özel bütçelerinden ödeme yapabilirler veya internet kullanmamayı tercih edebilirler. E-Rate programını Federal İletişim Komisyonu (*Federal Communication Commission* - FCC) yönetir.

CIPA'ya hızla karşı çıkıldı. Amerikan Kütüphaneler Birliği (*American Library Association*) ve Amerikan İnsan Hakları Birliği (*American Civil Liberties Union*) CIPA'nın yetişkinlerin serbest konuşma özgürlüğünü ihlal ettiğini iddia etti. Aynı zamanda, kanunun küçüklerin göğüs kanseri gibi belirli konularda bilgi almasına engel olacağını iddia ettiler. Bir federal mahkeme CIPA'nın özgür konuşma haklarını ihlal ettiğine hükmetti. Bu mahkeme, 2002 yılında CIPA'yı geçici olarak bozdu.

NOT

Kanun, yasal yetişkinlik yaşına erişmemiş herkesi küçük kabul eder. Bir küçük, bir çocuktur. Farklı yasalar bir kişinin küçük olup olmadığını belirlemek için farklı yaşlar tayin edebilirler.

Hükümet federal mahkemenin kararını ABD Yargıtayı'nda temyize götürdü. Davanın adı *ABD'ye karşı Amerikan Kütüphaneciler Birliği (United States et al. v. American Library Association, Inc. et al.)* şeklindedir. 2003 yılında yargıtay alt seviye mahkemenin kararını bozdu ve kanunu tekrar yürürlüğe soktu. Yargıtay sadece internet erişimi için E-Rate kaynaklarından faydalanan okul ve kütüphanelerin CIPA ile uygun olması gerektiğini belirtti. Eğer isterse, bir okul veya kütüphane kaynağı kabul etmemeyi tercih edebilirdi. Dava aynı zamanda CIPA'nın sadece küçüklere uygulanabileceğini gösterdi. Okullar ve kütüphaneler yetişkinlere filtresiz internet erişimi sağlamaya izin verecek bir yöntem sahibi olmalıydı. Aksi takdirde, sansür uygulamaktan ve yetişkinlerin Birinci Yasa Değişikliği (*First Amendment*) haklarını ihlal etmekten inceleme geçirebilirlerdi.

NOT

ABD Anayasası'nın Birinci Yasa Değişikliği (*First Amendment of the U.S. Constitution*) din, dil, basın ve toplantı özgürlüğü haklarını ortaya koyar. Bu haklar arasında dolaylı olarak, mahremiyet bileşeni olan, düşünce özgürlüğü hakkı da yer alır. Sansürleme faaliyetleri Birinci Yasa Değişikliği'ne aykırıdır.

Başlıca Gereksinimler

CIPA, kapsanan okul ve kütüphaneler tarafından rahatsız edici internet içeriğinin çocukların erişemeyeceği şekilde filtrelenmesini gerektirir. Okul ve kütüphaneler, bu gereksinimi yerine getirmek için teknolojik araçlar kullanırlar. CIPA bu araçları **teknoloji koruma önlemi (*technology protection measure* - TPM)** olarak tanımlar. Bir TPM, sakıncalı içeriği filtreleyen veya engelleyen herhangi bir teknolojidir. İçerik filtrelemek için kullanılan bir vekil sunucu (*proxy server*) bir TPM örneğidir.

Müstehcen ve Sakıncalı İçeriğin Tanımlanması

Pek çok insan çocukların müstehcen içerikten korunması gerektiğinde anlaşır. Ancak, *müstehcen içerik* teriminin tanımı karmaşıktır. 1973 tarihli ABD Yargıtayı davası *Miller'a karşı California*, müstehcenin tanımlanmasına yardım eder. Yargıtay bir içeriğin *müstehcen* olarak belirlenebilmesi için üç şartı sağlaması gerektiğini söyler. Şartlar güncel toplum standartlarını uygulayan ortalama bir kişiye göre tanımlanmıştır. Bu teste göre, bir içerik eğer şu şartları sağlıyorsa müstehcendir:

- Büyük çoğunlukla şehvetli arzuları cezbeder; şehvetli olma hastalıklı, alçaltıcı ve sağlıksız bir cinsel ilgi belirtir
- Cinsel ilişkiyi açıkça ve rahatsız edici biçimde yansıtır veya tarif eder
- Ciddi bir edebi, sanatsal, politik veya bilimsel değerden mahrumdur

Bu test yaygın olarak **Miller testi** diye bilinir. Mahkemeler bir içeriğin müstehcen olup olmadığına karar verirken onu kullanır.

FCC bir TPM'nin %100 etkin olamayabileceğini kabul eder. Ancak, ne CIPA ne de FCC hangi seviyenin kabul edilebilir olduğunu tanımlamaz. Bir üçüncü taraf şirket, filtresinin CIPA ile uygun olduğunu iddia edebilir. Ancak, bir filtrenin gerçekten CIPA ile uygun olduğunu doğrulayacak bir sertifikasyon süreci bulunmamaktadır. FCC her yerel yetkilinin kendi topluluğu için hangi ölçütlerin en etkin olacağına karar vermesi gerektiğini belirtmiştir.

CIPA neyin filtrelenmesi gerektiğini belirtir ama nasıl filtreleneceğini belirtmez. TPM'lere ek olarak, bir okul veya kütüphane bir internet güvenliği politikası oluşturmalı ve filtreleme istisnalarını ele alacak bir yöntem tespit etmelidir.

NOT

Birçok şirket çeşitli amaçlarla vekil sunucular (*proxy servers*) kullanır. Kullanımları sadece CIPA uygunluğu ile sınırlı değildir. Örneğin, çalışanların belirli internet sitelerine erişimini kısıtlama amacıyla kullanılabilirler.

Okul ve kütüphaneler CIPA ile uygun bir internet güvenliği politikası benimsemeli ve uygulamalıdır. Bu politikadaki hükümler çocukların çevrimiçi faaliyetlerini gözlemleyebilmelidir. Politika aynı zamanda okul veya kütüphanenin sakıncalı çevrimiçi içeriğe erişimi nasıl engelleyeceğini belirtmelidir. Çocukların e-posta kullanırken ki, sohbet odalarındaki veya elektronik iletişimdeki güvenliğine ve korumasına değinmelidir. Çocuğun interneti kanundışı faaliyetler için kullanması durumuna ve bir çocuğun kişisel bilgisinin yetkisiz kullanımına değinmelidir.

CIPA'ya göre, bir kütüphane veya okul bilgisayar kullanması gereken bir yetişkin için TPM'yi devre dışı bırakacak bir yöntem kullanmalıdır. Bu önemli bir noktadır. Eğer bir yetişkin için TPM'yi devre dışı bırakamazsanız, bu yetişkinin Birinci Yasa Değişikliği haklarını ihlal etme riski alırsınız. Yetişkinlerin sistemi hiçbir filtreleme olmaksızın kullanabilmesi gerekir.

Kütüphaneler TPM'yi devre dışı bırakmak için kendi konumlarında en iyi çalışan yöntemi kullanabilirler. Örneğin, kütüphane çalışanları bazı bilgisayarları "sadece yetişkinler için" şeklinde işaretleyebilir. Kütüphaneciler küçüklerin bu bilgisayarları kullanmasını engelleyecektir. Kütüphaneciler TPM'yi devre dışı bırakmak üzere tasarlanmış bir programla giriş yapabilirler. Sadece uygun yetkilere sahip çalışanlar TPM'yi devre dışı bırakabilir. Bir başka yöntem ise bir yöneticinin TPM'yi devre dışı bırakmasını gerektirmektir. Kullanıcının isteği üzerine, kütüphaneci bu kullanıcı için TPM'nin devre dışı bırakılmasını istemek üzere yönetici ile temasa geçebilir.

Gözetim

CIPA denetimi FCC'ye aittir. Ancak, çok az denetim faaliyeti gereklidir. Bir devlet okulu veya kütüphane E-Rate kaynağı talep ettiğinde, CIPA ile uygun olduklarını belgelendirmeleri gerekir. Bu sertifikasyon genelde gereken tek şeydir.

Eğer bir TPM arızalanırsa, okul veya kütüphanenin arızayı gidermek için gerekli adımları atması beklenir. Eğer kütüphane bunu gidermezse, kullanıcı FCC'ye şikayette bulunabilir. Eğer FCC çok fazla sakıncalı resmin filtrelenmediğine dair şikayetler alırsa, inceleme başlatabilir.

FCC, Kongre'nin CIPA ile uygunluğu olmayan kütüphanelere ceza verilmesini tasarlamadığını varsayar. FCC, en fazla, bir kütüphaneden uygun olmadığı zaman aralığı için sağlanan E-Rate indirimini iade etmesini isteyebilir.

Ödeme Kartı Endüstrisi Veri Güvenliği Standardı

Kredi kartı veri ihlalleri bugünün haber başlıklarından ilk akla gelenlerdendir. Birisi veya bir şirket tam şu anda ihlal ediliyor ya kimlik hırsızlığı ya gerçek veri ihlali ya da verinin açığa çıkması sebebiyle. Beş büyük kredi kartı markası (American Express, Discover, JCB, MasterCard ve Visa) 2006

yılında, kart sahibi verisi ve hareket işleme görevlerinin gizlilik, bütünlük ve kullanılabilirliğini sağlayacak standartların yönetimi ve uygulamasını birlikte tanımlamak için PCI Konseyi'ni kurdu.

Amaç ve Kapsam

PCI Konseyi'nin iki temel önceliği vardır. Birinci öncelik tüccarlar ve finansal kuruluşların ödeme sistemlerini kart sahibi verisinin çalınması ve ihlaline karşı korumalarını sağlayacak güvenlik politikalarını, teknolojileri ve süregelen süreçleri anlamalarına ve uygulamalarına yardımcı olmaktır. İkinci öncelik, tedarikçilerin güvenli ödeme çözümlerinin düzgün olarak uygulandığını temin edecek PCI standartlarını ve gereksinimlerini anlamalarına ve uygulamalarına yardımcı olmaktır.

PCI Veri Güvenliği Standardı (*PCI Data Security Standard* - PCI DSS) v3.2 standardı[36] PCI standardının en son tanımlanan versiyonudur. Bu standart şunlara değinir: Güvenlik konuları, PCI uygunluğu gereksinimleri, BT altyapınızın korunması ve süregelen güvenlik risk değerlendirmeleri, güvenlik testleri, ve çalışanlar için yıllık güvenlik farkındalığı eğitimi gibi belirli risk yönetimi görevlerinin yerine getirildiğini doğrulayan yıllık çalışmaların yapılması.

NOT

PCI güvenlik standartları konseyi giriş sayfası *https://www.pcisecuritystandards.org* adresindedir. PCI DSS v3.2 standardı tanımı ile ilgili detaylı bilgi için *https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf* adresindeki standardı inceleyiniz. v3.1 ile v3.2 arasındaki farkların özetini görmek için, *https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2_Summary_of_Changes.pdf* belgesini gözden geçiriniz.

TABLO 15-6 PCI Veri Güvenliği Standardı'nın uygunluk gereksinimlerini sunmaktadır. Bu gereksinimler **kontrol hedefleri** denilen gruplar halinde düzenlenmiştir.

Uygunluğu doğrulamak için, kredi kartı hareket hacmi ve kabul kanalından bağımsız olarak tüm tüccar ve servis sağlayıcılar, iki doğrulama gereksinimini karşılamalıdır. Bazı tüccar ve servis sağlayıcılar, sertifika sınavından geçmiş sertifikalı bir uzman olan **nitelikli güvenlik denetçisi (*qualified security assessor* - QSA)** tarafından yıllık olarak yerinde yapılan PCI denetiminden geçerek uygunluklarını doğrularlar. Buna ek olarak, **onaylı tarama sağlayıcısı (*approved scanning vendor* - ASV)** tarafından üç aylık dönemlerde zafiyet değerlendirme taraması yapılmalıdır. Bu, şirketin geçer not alabilmek için yeniden tarama öncesinde bir yama iyileştirmesi gerçekleştirmesini gerektirir. Diğer kuruluşların yıllık olarak öz-değerlendirme anketi (***self-assessment questionnaire* - SAQ)** ve üç aylık dönemlerde onaylı bir ASV tarama şirketince yapılmış güvenlik açığı değerlendirme taraması doldurması gerekir.

TABLO 15-7 farklı katman seviyelerindeki tüccarlar için PCI uygunluk gereksinimlerini belirtir. Katman seviye ataması yıllık kredi kartı hareketlerinin toplam hacminin birleştirilmesi ile kararlaştırılır. Bu belirlendikten sonra, tüccarın katman seviyesi tanımlanabilir.

TABLO 15-8 farklı katman seviyelerindeki servis sağlayıcılar için PCI uygunluk gereksinimlerini belirtir. Katman seviye ataması yıllık kredi kartı hareketlerinin toplam hacminin birleştirilmesi ile kararlaştırılır. Bu rakam kararlaştırılınca, servis sağlayıcının katman seviyesi tanımlanabilir.

NOT

Yıllık yerinde güvenlik denetimi bir **uygunluk raporu (*report of compliance* - *ROC*)** tamamlanmasını gerektirir. ***Uygunluk onayının (attestation of compliance* - *AOC*)** tamamlanıp CEO ve QSA tarafından imzalanması için ROC gereklidir. QSA, PCI uygunluk denetimini (ör. ROC) gerçekleştiren ve AOC'yi dolduran esas kişidir. CEO'yu kuruluşunun PCI uygunluğundan sorumlu tutan AOC'dir.

Öz Değerlendirme Anketi

Öz değerlendirme anketi (*self-assessment questionnaire* - SAQ) farklı SAQ seviyeleri için gerekli olan güvenlik kontrolü gereksinimlerini listeler. Kuruluşunuzun kullanması gereken SAQ türü

TABLO 15-6 PCI Veri Güvenliği Standardı gereksinimleri.

KONTROL HEDEFLERİ	PCI DSS GEREKSİNİMLERİ
Güvenli bir ağ kurmak ve yürütmek	1. Kart sahibi verisini koruyacak bir güvenlik duvarı kurmak ve yürütmek 2. Sistem parolaları ve diğer güvenlik parametreleri için tedarikçi tarafından sağlanan varsayılan değerleri kullanmamak
Kart sahibi verisini korumak	3. Saklanmış olan kart sahibi verisini korumak 4. Açık, kamusal ağlar üzerinden aktarılan kart sahibi verisini şifrelemek
Bir güvenlik açığı yönetimi programı yürütmek	5. Zararlı yazılımlardan yaygın olarak etkilenen tüm sistemlerde antivirüs yazılımı kullanmak ve bunu düzenli olarak güncellemek 6. Güvenli sistemler ve uygulamalar geliştirmek ve yürütmek
Güçlü erişim denetim önlemleri gerçekleştirmek	7. Kart sahibi verisine erişimi iş ihtiyaçları ile kısıtlamak 8. Bilgisayar erişimi olan her kişiye kendisine özgü ID atamak 9. Kart sahibi verisine fiziksel erişimi kısıtlamak
Düzenli olarak ağları izlemek ve test etmek	10. Ağ kaynaklarına ve kart sahibi verisine her türlü erişimi takip etmek ve izlemek 11. Güvenlik sistemlerini ve süreçlerini düzenli olarak test etmek
Bir bilgi güvenliği politikası yürütmek	12. Bilgi güvenliğine değinen bir politika yürütmek

kuruluşunuz tarafından gerçekleştirilen kredi kartı hareketlerinin yöntemi ve türüne göre belirlenir. **TABLO 15-9** SAQ uygunluğu açısından her bir kredi kartı hareketi yöntemi ve türünün gerektirdiklerini belirtir.

Başlıca Gereksinimler

PCI DSS v3.2 standardı 2016 Nisan ayında açıklanmıştır. Bu standart bazı konulara açıklık kazandırmış ve şimdi güncellenmiş SAQ'larda yer alan uygunluk doğrulaması ile ilgili bazı ek gereksinimler getirmiştir. Bu ek gereksinimler SAQ'ın 12 gereksinim kategorisine dağıtılmıştır. Bu yeni v3.2 güvenlik kontrolü gereksinimleri şöyledir[37]:

- **Gereksinim 3.3** – Başlıca erişim numarasının (yani 16-basamaklı kredi kartı numarası) ilk-altı/son-dört hanesinden fazlasının gösterimi geçerli bir iş gerekçesine bağlanacak şekilde gereksinim güncellenmiştir. Başlıca maskeleme senaryolarına yönelik rehber eklenmiştir.
- **Gereksinim 8.3**— Gereksinim 8.3 alt gereksinimlere genişletilerek CDE'ye konsol harici yönetici erişimi olan tüm personel ve uzaktan erişimi olan tüm personel için çok faktörlü kimlik denetimi (*multifactor authentication*) gereksinimi getirilmiştir.
  - **Gereksinim 8.3.1** (*1 Şubat 2018'den itibaren geçerli*)—CDE'ye konsol harici yönetici erişimi olan tüm personel için çok faktörlü kimlik denetlemesine yönelik yeni bir gereksinim.

TABLO 15-7 PCI Veri Güvenliği Standardı'nın tüccar katman seviyeleri.

KATMAN	ÖLÇÜTLER	YERİNDE GÜVENLİK İNCELEMESİ	ÖZ DEĞERLENDİRME ANKETİ	AĞ TARAMASI	ONAYLI ÜÇÜNCÜ TARAFA AİT ÖDEME UYGULAMASI
1	Kabul kanalından bağımsız olarak, yılda 6 milyondan fazla hareket işleyen tüm tüccarlar Hesap ifşası ile sonuçlanmış bir güvenlik açığından zarar görmüş tüm tüccarlar	Yılda bir gerekli (bir QSA, ROC, ve AOC gerektirir)		Üç ayda bir gerekli	Gerekli
2	Her yıl 1 ile 6 milyon arası hareket işleyen tüm tüccarlar	Yılda bir gerekli (bir ROC ve AOC gerektirir)		Üç ayda bir gerekli	Gerekli
3	Her yıl 20.000 ile 1 milyon arası hareket işleyen tüm tüccarlar		Yılda bir gerekli	Üç ayda bir gerekli	Gerekli
4	Kabul kanalından bağımsız olarak, 1., 2., ve 3. seviyede olmayan tüm diğer tüccarlar		Yılda bir gerekli	Üç ayda bir gerekli	Gerekli

TABLE 15-8 PCI Veri Güvenliği Standardı servis sağlayıcı katman düzeyleri.

KATMAN	ÖLÇÜTLER	YERİNDE GÜVENLİK İNCELEMESİ	ÖZ-DEĞERLENDİRME ANKETİ	AĞ TARAMASI	ONAYLI ÜÇÜNCÜ TARAFA AİT ÖDEME UYGULAMASI
1	Tüm işlemciler ve tüm ödeme ağ geçitleri	Yılda bir gerekli (bir QSA, ROC, ve AOC gerektirir)		Üç ayda bir gerekli	Gerekli
2	Seviye 1'de olmayan ve yılda 1 milyondan fazla hesap/hareket depolayan, işleyen veya aktaran herhangi bir servis sağlayıcı	Yılda bir gerekli (bir ROC ve AOC gerektirir)		Üç ayda bir gerekli	Gerekli
3	Katman 1'de olmayan ve yılda 1 milyondan fazla hesap/hareket depolayan, işleyen veya aktaran herhangi bir servis sağlayıcı		Yılda bir gerekli	Üç ayda bir gerekli	Gerekli

TABLO 15-9 SAQ, kredi kartı hareketinin işlenme türüne göre belirlenir.

SAQ	AÇIKLAMA
A	Kartsız işlem yapan, kart sahibi ile ilgili tüm veri işlevlerini PCI DSS tarafından onaylanmış üçüncü taraf hizmet sağlayıcılara aktarmış, sisteminde veya yerleşkesinde kart sahibi bilgisini elektronik olarak depolamayan, işlemeyen veya buradan aktarmayan tüccarlar (e-ticaret veya posta/telefon siparişleri). *Yüz yüze kanallar için geçerli değildir*
A-EP	Tüm ödeme işlemlerini PCI DSS tarafından onaylanmış üçüncü taraflara aktarmış ve kart sahibi verisini doğrudan almayan ancak ödeme hareketinin güvenliğini etkileyebilecek bir internet sitesi(leri) olan e-ticaret tüccarları. Tüccarın sisteminde veya yerleşkesinde kart sahibi verisi depolanmaz, işlenmez veya buradan aktarılmaz. *Sadece e-ticaret kanalları için geçerlidir*
B	Sadece şunları kullanan tüccarlar için: • Elektronik kart sahibi verisi depolanmayan etiketleme makineleri; ve/veya • Elektronik kart sahibi verisi depolanmayan bağımsız, dışarı arama terminalleri. E-ticaret kanalları için geçerli değildir.
B-IP	PCI DSS onaylı bir üçüncü taraf servis sağlayıcı tarafından temin edilen ve barındırılan bir internet tabanlı sanal terminal çözümüne, her defasında tek bir hareketi klavye üzerinden elle giren tüccarlar. Elektronik kart sahibi verisi depolanmaz. *E-ticaret kanalları için geçerli değildir.*
C-VT	Sadece onaylı, PCI SSC listesinde yer alan bir P2PE çözümüne dahil olan veya böyle bir çözüm ile yönetilen donanımsal ödeme terminallerini kullanan, elektronik kart sahibi verisi depolamayan tüccarlar. *E-ticaret kanalları için geçerli değildir.*
C	internete bağlı ödeme uygulaması sistemleri olan, elektronik kart sahibi verisi depolamayan tüccarlar. *E-ticaret kanalları için geçerli değildir.*
P2PE-HW	Sadece onaylı, PCI SSC listesinde yer alan bir P2PE çözümüne dahil olan veya böyle bir çözüm ile yönetilen donanımsal ödeme terminallerini kullanan, elektronik kart sahibi verisi depolamayan tüccarlar. *E-ticaret kanalları için geçerli değildir.*
D	*Tüccarlar için SAQ D:* Yukarıdaki SAQ türleri için yapılan açıklamalara dahil olmayan tüm tüccarlar. *Servis sağlayıcılar için SAQ D:* Bir ödeme markası tarafından bir SAQ tamamlama niteliklerine sahip görülen tüm servis sağlayıcılar.

- **Gereksinim 8.3.2**—Eski Gereksinim 8.3'ü bünyesinde toplayan ve CDE'ye uzaktan erişimi olan tüm personel için çok faktörlü kimlik denetlemesine yönelik yeni bir gereksinim.

- **Gereksinim 10.8.1** (*1 Şubat 2018'den itibaren geçerli*)—Servis sağlayıcıların kritik güvenlik kontrolü sistemlerinin hatalarını tespit etmesi ve raporlamasına yönelik yeni bir gereksinim.
- **Gereksinim 11.3.4.1** (*1 Şubat 2018'den itibaren geçerli*)—Servis sağlayıcıların en az her altı ayda bir bölümleme (*segmentation*) kontrolleri üzerinde sızma testi (*penetration testing*) uygulamasına yönelik yeni bir gereksinim.
- **Gereksinim 12.4** (*1 Şubat 2018'den itibaren geçerli*) —Servis sağlayıcıların yönetici kadrosunun kart sahibi verisinin korunması ve PCI DSS uygunluğu programı için sorumlulukları saptamasına yönelik yeni bir gereksinim.

- **Gereksinim 12.11.1** (*1 Şubat 2018'den itibaren geçerli*)— Servis sağlayıcıların, çalışanlarının güvenlik politikalarını ve işletme prosedürlerini takip ettiğinden emin olmak için en fazla üç ay aralıklarla teftişte bulunmasına yönelik yeni bir gereksinim.

Bilgi Güvenliği Uygunluğu Kanunlarını Anlamlandırmak

Birleşik Devletler'in sadece tek bir veri koruma kanunu yoktur. Bunun sonucu olarak, birçok kanun farklı veri türlerine odaklanır. Bu bölüm özellikle federal veri koruma kanunlarına odaklandı. Eyaletlerin de veri koruma kanunları olabileceğini unutmamalısınız. Pek çok farklı eyaletin veri koruma kanunu çeşitleri üzerine bir tartışma, kendi içinde bir kitap olabilir. Önemli olan kuruluşların federal kanunlara *ve* yerleşik oldukları eyaletin kanunlarına uygun olmaları gerektiğini hatırlamaktır. Sistem güvenliği uzmanları uygunluk projelerinde çalışırken her iki kanun türünün de farkında olmalıdır.

Kuruluşun takip etmesi gereken her kanun için ayrı bilgi güvenliği programı oluşturmak pratik değildir. BT sistemleri çok farklı veri türleri içerebilir. Bir kuruluşun sistemlerinin birden fazla kanun ile uygunluğunu sağlaması gerekebilir. Sonuç olarak, bir kuruluşun bilgi güvenliği programı kapsayıcı olmalıdır. Birçok kanuna ortak karşılık verip onları bağdaştırmalıdır. Bunu yapmak için, sistem güvenliği uzmanlarının bilgi güvenliği itibariyle hangi kanunların ortak noktaları olduğunu anlaması gerekir.

Örneğin, bu bölümde tartışılan kanunların çoğu bir kuruluşun kendi BT sistemlerinin güvenliğini değerlendirmesini gerektirir. Bunu yapmak için, kuruluş bir risk değerlendirmesi yürütmelidir. Bu pek çok kanunun belirtilmiş bir gereksinimidir. FISMA, GLBA, HIPAA ve SOX'un hepsi bu gereksinimi içerir. Çoğu zaman bu risk değerlendirmesini gerçekleştirmekten sistem güvenliği uzmanları sorumlu olur. BT sistemlerinin nerelerde korunmasız olduğunu belirlemeye yardımcı olurlar. Kuruluşa olası riskleri azaltmak için adımlar atılmasında yardımcı olurlar. Risk değerlendirmesi gerçekleştirme ve riskleri azaltma adımları atma süreci **risk yönetimi** (***risk management***) olarak bilinir.

Sistem güvenliği uzmanları eşsiz bir pozisyondadır. Bu kanun ve düzenlemelerin BT sistemlerinin nasıl çalışacağı üzerindeki etkilerini anlamalıdırlar. Aynı zamanda bilgi güvenliğinin temel ilkelerinin bu kanunları nasıl etkilediğini anlamalıdırlar. Burada tartışılan hemen tüm kanunlar belirli veri türlerinin gizliliğini korumaya odaklıdır. FISMA, HIPAA, GLBA ve FERPA'nın hepsi gizlilik gereksinimleri içerir. Bilgi güvenliği sadece iyi bir fikir değildir; kanundur.

Bu kanunların bazılarının bütünlük gereksinimleri vardır. Hem FERPA hem de HIPAA kuruluşların tutarsız veriyi tespit etmek için bir yolu olmasını gerektirir. Aynı zamanda bunları düzeltebilmelidirler. SOX kuruluşların BT sistemlerinde kullandıkları dahili kontrolleri test etmelerini ve doğruluğunu temin etmelerini gerektirir. Bu kontroller finansal veriyi düzgün yetkilendirme olmaksızın gerçekleşecek değişikliklerden korumalıdır.

Diğer kanunların kullanılabilirlik gereksinimleri vardır. CIPA belirli çevrimiçi içerik türlerinin bir kitle için kullanılır olmasını (yetişkinler), ama bir başka kitlenin (çocuklar) aynı içerikten mahrum bırakılmasını gerektirir. Bu bir kullanılabilirlik kavramıdır. CIPA ile uygun olmak isteyen bir kuruluşun erişim kontrolü önlemleri kullanması gerekecektir. FISMA federal kurumların BT sistemleri için acil durum planları oluşturmalarını gerektirir. HIPAA'nın benzer bir gereksinimi vardır. Bu planlar BT sistemlerinin bir ayrıcalıklı olay veya felaket sonrası kullanılır olmalarını temin eder. Bir kanun kullanılabilirlikten doğrudan bahsetmese dahi, kullanılabilirlik hemen tüm kuruluşlar için önemli bir gereksinimdir. Kuruluşlar, iş yürütebilmek için, verileri ve BT sistemlerinin kullanılır olmasına ihtiyaç duyar.

TABLO 15-10 Kanunlar ve bilgi güvenliği kavramları.

GİZLİLİK	BÜTÜNLÜK	KULLANILABİLİRLİK
FISMA	FISMA	FISMA
HIPAA	HIPAA	HIPAA
GLBA	SOX	GLBA
FERPA	FERPA	SOX CIPA
PCI DSS v3.2*	PCI DSS v3.2*	PCI DSS v3.2*

* PCI DSS uluslararası bir standarttır, kanun değildir.

TABLO 15-10 bu bölümde tartışılan kanunlarla ilgili bilgi güvenliği kavramları bakımından nasıl düşünmeniz gerektiğini göstermektedir. Bu çizelge kanunları bu bölümde tartışıldıkları şekilde gösterir.

Sistem güvenliği uzmanları olarak bu uygunluk kanunlarını anlamlandırmak için gerekli olan yeteneklere sahip olmanız gerekecek. BT sistemlerinin kuruluşunuzun uygunluk gereksinimlerini karşılayacak şekilde nasıl yapılandırılacağını anlayacaksınız. Bu kanunların BT sistemlerini nasıl etkilediğini açıklayabiliyor olmalısınız. Aynı zamanda bu kanunlarla uygun olmak için kuruluşunuzun attığı adımları açıklayabiliyor olmalısınız.

NOT

Acil durum planları ayrıcalıklı olay müdahalesi ve felaket kurtarma planlarını içerir.

BÖLÜM ÖZETİ

Bu bölüm farklı işletme düzlemlerindeki ABD uygunluk kanunlarını sundu. Bu kanunlar ya bir güvenlik bileşeni, ya bir mahremiyet bileşeni veya her ikisini birden içerir. Bu işletme düzlemlerinin herhangi birinde çalışan kuruluşlar uygunluk içinde olmalıdır. Bu tercihe bağlı değildir; federal kanun olduğu için zorunludur. Bir kuruluş bu kanunlarla uygunluğunu belgelemelidir ve denetlenmeleri halinde bunu yaptıklarını ispat edebilmelidir.

Bilgi sistemi güvenliği uzmanları bu uygunluk kanunlarından dolayı meşguldür. Kanuni gereksinimleri taktik güvenlik uygulamalarına çevirebilmeleri gerekir. BT altyapısını baştan başa kapsayacak güvenlik kontrolleri uygulayabilmeleri gerekir. Kişisel mahremiyet verisi gibi bilgilerin mahremiyetini korumak uygun güvenlik kontrolleri gerektirir.

Kanun olmasına rağmen, PCI DSS standardının kart sahibi verisi depolayan, işleyen veya aktaran PCI tüccarları ve servis sağlayıcıları tarafından takip edilmesi gerekir. PCI'ın kredi kartı hareketi işlemleri gerçekleşirken kullanılan kart sahibi verisinin gizliliğini, bütünlüğünü ve kullanılabilirliğini temin etmek için detaylı gereksinimler vardır. Kredi kartı hareketlerini nasıl işlediğiniz, kuruluşunuzun uyması gereken SAQ'ı belirler. Yıllık kredi kartı hareketlerinin sayısı kuruluşun tüccar veya servis sağlayıcı katman seviyesini belirleyecektir. 2016 Nisan ayında yeni PCI DSS v3.2 standardına ve SAQ kontrol listeleri ne yeni gereksinimler eklenmiştir.

ANAHTAR KAVRAMLAR VE TERİMLER

Approved scanning vendor (ASV) - Onaylı tarama sağlayıcısı (ASV)
Attestation of compliance (AOC) - Uygunluk onayı (AOC)
Business associates - İş ortakları
Compliance - Uygunluk
Control objectives - Kontrol hedefleri
Covered entity - Kapsanan varlık
Directory information - Dizin bilgisi
Electronic protected health information (EPHI) - Elektronik korunan sağlık bilgisi (EPHI)
Miller test - Miller testi
Minimum necessary rule - Minimum ihtiyaç kuralı
Nonpublic personal information (NPI) - Kamuya açık olmayan kişisel bilgi (NPI)
Personally identifiable Information - Kişisel tanımlayıcı bilgi
Privately held companies - Özel şirketler
Protected health information (PHI) - Korunan sağlık bilgisi (PHI)
Publicly traded companies - Halka açık şirketler
Qualified security assessor (QSA) - Nitelikli güvenlik denetçisi (QSA)
Report of compliance (ROC) - Uygunluk raporu (ROC)
Risk management - Risk yönetimi
Sarbanes-Oxley Act of 2002 - 2002 tarihli Sarbanes-Oxley Kanunu
Self-assessment questionnaire (SAQ) - Öz değerlendirme anketi (SAQ)
Technology protection measure (TPM) - Teknoloji koruma önlemi (TPM)

BÖLÜM 15 DEĞERLENDİRME

1. Adreslenebilir bir HIPAA güvenlik kuralının tebligat gereksinimi eğer sizin ortamınıza _____ ise uygulanmalıdır.

2. Yazılı bir GLBA bilgi güvenliği programı hangilerini içermelidir?
   A. Teknik tedbirleri
   B. Fiziksel tedbirleri
   C. İdari tedbirleri
   D. Programı yürütmesi için atanmış bir çalışan
   E. Hepsi

3. Hangi tür şirketlerin Sarbanes-Oxley Kanunu hükümlerinin hepsini takip etmesi gerekir?
   A. Halka açık
   B. Özel
   C. Kar amacı gütmeyen
   D. Kamu işletmeleri
   E. Hiçbiri

4. CIPA bir kütüphanenin TPM'yi belirli durumlarda devre dışı bırakabilmesini gerektirir.
   A. Doğru
   B. Yanlış

5. Hangi kanun öğrenci bilgilerinin açıklanmasını düzenler?
   A. HIPAA
   B. SOX
   C. FERPA
   D. CIPA
   E. Hiçbiri

6. HIPAA Mahremiyet veya Güvenlik Kuralı'nı ihlal etmenin yıllık cezası en fazla ne kadardır?
   A. 100$
   B. 1.500$
   C. 1 milyon $
   D. 1.5 milyon $
   E. Sınırsızdır.

7. Birleşik Devletler'in kapsamlı bir veri koruma kanunu vardır.
   A. Doğru
   B. Yanlış

8. Bir eğitim kuruluşun üçüncü taraflarla kişisel öğrenci bilgisi paylaşmadan önce edinmesi gereken nedir?
   A. Sözlü onay
   B. Noter onayı
   C. İmzalı yeminli belge
   D. Yazılı onay
   E. Hiçbiri

9. CIPA'ya göre kim "küçük"tür?
   A. 13 yaşın altındaki herhangi biri
   B. 17 yaşın altındaki herhangi biri
   C. 20 yaşın altındaki herhangi biri
   D. 21 yaşın altındaki herhangi biri
   E. Hiçbiri

10. Hangisi kişisel tanımlayıcı bilgidir?
    A. İsim ve soyadı
    B. Doğum tarihi
    C. Sosyal Güvenlik numarası
    D. Ev adresi
    E. Hepsi

11. FISMA federal kurumların bilgi güvenliği kontrollerini en az yılda bir test etmelerini gerektirir.
    A. Doğru
    B. Yanlış

12. PCI Güvenlik Konseyi'nin ana amacı nedir?
    A. Kart sahibi verisinin korunması için standartlaştırılmış bir yaklaşım tanımlamak
    B. Güvenlik duvarı çözümleri tavsiye etmek
    C. Kredi kartlarının nasıl işleneceğini tanımlamak
    D. Kart sahibi verisini korumak üzere kuruluşlara bir standart zorlamak
    E. Hiçbiri

13. Hangi PCI DSS tüccar katman seviyesi(leri) onaylı QSA uzmanı tarafından gerçekleştirilmesi gereken yıllık, yerinde denetim gerektirir?
    A. 1
    B. 2
    C. 3
    D. 4
    E. Hem A hem B

14. PCI DSS'e göre, bir servis sağlayıcının hangi SAQ'ta tanımlı güvenlik kontrolü gereksinimleri ile uygun olması gerekir?
    A. A
    B. B-IP
    C. C-VT
    D. D
    E. AB

15. PCI DSS v3.2 standardı ve SAQ-D içinde kaç tane gereksinim bölümü vardır?
    A. 6
    B. 7
    C. 8
    D. 10
    E. 12

DİPNOTLAR

1. U.S. Office of Management and Budget, Circular No. A-130, "Management of Federal Information Resources," December 2000, www.whitehouse.gov/omb/circulars_a130_a130trans4/ (accessed April 21, 2010).

2. Committee on Oversight and Government Reform, "Federal Information Security: Current Challenges and Future Policy Considerations," March 24, 2010, https://oversight.house.gov/hearing/federal-information-security-current-challenges-and-future-policy-considerations/ (accessed April 21, 2010). See prepared testimony of Mr. Vivek Kundra.

3. Federal Information Security Management Act, Title III of the E-Government Act of 2002, P.L. 107-347; U.S. Code Vol. 44, sec. 3541 et seq.

4. U.S. Code Vol. 44, sec. 3542(b)(1).

5. U.S. Code Vol. 44, sec. 3544(a)(3)(A)(ii).

6. GovInfoSecurity.com, "Automated FISMA Reporting Tool Unveiled," October 30, 2009, www.govinfosecurity.com/articles.php?art_id=1894 (accessed April 24, 2010).

7. Committee on Oversight and Reform, "Federal Information Security: Current Challenges and Future Policy Considerations," March 24, 2010. See prepared testimony of Mr. Vivek Kundra.

8. The White House Blog, Vivek Kundra, "Faster, Smarter Cybersecurity," April 21, 2010, www.whitehouse.gov/blog/2010/04/21/faster-smarter-cybersecurity (accessed April 23, 2010).

9. National Institute of Standards and Technology, SP 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life-Cycle Approach," February 2010, http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf (accessed May 21, 2010).

10. Code of Federal Regulations, Title 45, sec. 160.103.

11. Code of Federal Regulations, Title 45, sec. 165.502(b).

12. Code of Federal Regulations, Title 45, sec. 164.520.

13. Code of Federal Regulations, Title 45, sec. 164.530(f).

14. Health Information Technology for Economic and Clinical Health Act (2009), Pub. L. No. 111-5, sec. 13402.

15. Ibid.

16. Code of Federal Regulations, Title 45, sec. 164.306.

17. Code of Federal Regulations, Title 45, sec. 164.316.

18. Code of Federal Regulations, Title 45, sec. 164.306.

19. Ibid.

20. Verizon Business, 2009 *Data Breach Investigations Report*, April 15, 2009, www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf (accessed March 1, 2010).

21. U.S. Code Vol. 15, sec. 6801-6803.

22. U.S. Code Vol. 15, sec. 6801(b).

23. Standards for Insuring the Security Confidentiality, Integrity and Protection of Customer Records and Information ("Safeguards Rule"), Code of Federal Regulations, Title 16, sec. 314.

24. *The Wall Street Journal*, "Investors Hope the '10s Beat the '00s," December 20, 2009, http://online.wsj.com/article/SB10001424052748704786204574607993448916718.html (accessed April 16, 2010).

25. U.S. Securities and Exchange Commission, "Information Matters," February 22, 2006, www.sec.gov/answers/infomatters.htm (accessed April 16, 2010).

26. Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (codified as amended in scattered sections of U.S. Code Vol. 15).

27. *The New York Times*, "Bush Signs Bill Aimed at Fraud in Corporations," July 30, 2002, www.nytimes.com/2002/07/31/business/corporate-conduct-the-president-bush-signs-bill-aimed-at-fraud-in-corporations.html?pagewanted=1 (accessed April 16, 2010).

28. Ernst & Young, "Emerging Trends in Internal Controls: Fourth Survey and Industry Insights," September 2005, www.sarbanes-oxley.be/aabs_emerging_trends_survey4.pdf (accessed April 16, 2010).

29. Commission Guidance Regarding Management's Report on Internal Controls Over Financial Reporting, Code of Federal Regulations, Title 17, sec. 241.

30. Marcella, Albert J., "Electronically Stored Information and Cyberforensics," *Information Systems Control Journal*, Vol. 5 (2008).

31. U.S. Code Vol. 15, sec. 7213m.

32. Commission Guidance Regarding Management's Report on Internal Controls Over Financial Reporting, Code of Federal Regulations, Title 17, sec. 241.

33. U.S. Code Vol. 15, sec. 7266.

34. U.S. Code Vol. 20, sec. 1232g.

35. The Children's Internet Protection Act, Pub. L. No. 106-554, 114 Stat. 2763A-335 (codified in scattered sections of U.S. Code).

36. PCISecurityStandards.org, "Summary of Changes from PCI DSS Version 3.1 to 3.2 Payment Card Industry (PCI) Data Security Standard," April 2016, https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2_Summary_of_Changes.pdf (accessed May 13, 2016).

37. PCISecurityStandards.org, "Payment Card Industry (PCI) Data Security Standard," April 2016, https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf (accessed May 13, 2016).



EK

A

ahtarı

BÖLÜM 1 Bilgi Sistemleri Güvenliği

1. A 2. A 3. C 4. A 5. B 6. E 7. E 8. D 9. A 10. A 11. A
12. A 13. E 14. D 15. B

BÖLÜM 2 Nesnelerin İnterneti Yaşantımızı Değiştiriyor

1. A 2. E 3. D 4. E 5. E 6. E 7. B 8. A 9. B 10. E 11. B 12. C

BÖLÜM 3 Kötücül Saldırılar, Tehditler ve Zafiyetler

1. A 2. E 3. B 4. Paket koklayıcı (*packet sniffer*) 5. A 6. A 7. D 8. E 9. A
10. C 11. C 12. Tehdit (*Threat*) 13. Zafiyet (*Vulnerability*) 14. B 15. D

BÖLÜM 4 Bilgi Güvenliği Sektörünün Sürücüleri

1. A 2. A 3. B 4. E 5. B 6. D 7. E 8. A 9. A 10. D 11. C
12. E 13. HIPAA 14. A 15. E

BÖLÜM 5 Erişim Denetimleri

1. A 2. D 3. B 4. A 5. C 6. A 7. B 8. B 9. D 10. B 11. E
12. B 13. D 14. A 15. D

BÖLÜM 6 Güvenlik Operasyonları ve Yönetimi

1. A 2. D 3. B 4. C 5. B 6. B 7. D 8. E 9. A 10. B 11. B
12. A 13. E 14. A 15. D 16. A 17. E 18. B

BÖLÜM 7 Denetleme, Sınama ve İzleme

1. A 2. E 3. B 4. C 5. E 6. A 7. C 8. B 9. A 10. B
11. B 12. D

BÖLÜM 8 Risk, Yanıt ve Kurtarma

1. C 2. A 3. A 4. A 5. C 6. E 7. A 8. D 9. B 10. C

BÖLÜM 9 Kriptografi

1. C 2. A 3. B 4. D 5. A 6. A 7. A 8. E 9. A 10. B 11. D 12. A

BÖLÜM 10 Ağlar ve Telekomünikasyon

1. C 2. A 3. B 4. A 5. D 6. Yönlendirici (*Router*) 7. B 8. A
9. C 10. B 11. A 12. B 13. B 14. D 15. D

BÖLÜM 11 Kötücül Kod ve Etkinlik

1. B 2. Spam 3. C 4. A 5. B 6. D 7. B 8. A 9. C 10. B
11. D 12. Derinlemesine savunma (*Defense in depth*) 13. A

BÖLÜM 12 Bilgi Güvenliği Standartları

1. A 2. B 3. A 4. D 5. TCP/IP 6. Yorumlar için istek (*Request for Comments - RFC*) 7. A 8. IEEE 9. D 10. B

BÖLÜM 13 Bilgi Sistemleri Güvenliği Öğretimi ve Eğitimi

1. B 2. C 3. B 4. C 5. D 6. Eğitmen tarafından yönetilen
7. A 8. B 9. C 10. D 11. E 12. D 13. A 14. E 15. B

BÖLÜM 14 Bilgi Güvenliği Mesleki Sertifikasyonlar

1. A 2. C 3. B 4. D 5. CIW 6. A 7. E 8. B 9. A 10. D
11. A 12. E 13. B 14. A 15. E

BÖLÜM 15 ABD Uygunluk Kanunları

1. Kabul edilebilir ve uygun (Reasonable and appropriate)
2. E 3. A 4. B 5. C 6. E 7. B 8. D 9. B 10. E 11. A
12. A 13. A 14. D 15. E

EK

B

Standart Kısaltmalar

ACK	acknowledgment
ACL	access control list
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AP	access point
API	application program interface
B2B	business-to-business
B2C	business-to-consumer
BBB	Better Business Bureau
BCP	business continuity plan
CA	certificate authority
CCC	CERT Coordination Center
CCNA	Cisco Certified Network Associate
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CISSP	Certified Information System Security Professional
COPPA	Children's Online Privacy Protection Act
DBMS	database management system
DDoS	distributed denial of service
DES	Data Encryption Standard
DMZ	demilitarized zone
DoS	denial of service
DPI	deep packet inspection
DRP	disaster recovery plan
DSL	digital subscriber line
DSS	Digital Signature Standard
DSU	data service unit
EDI	Electronic Data Interchange
EIDE	Enhanced IDE
FACTA	Fair and Accurate Credit Transactions Act
FAR	false acceptance rate
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FEP	front-end processor
FRCP	Federal Rules of Civil Procedure
FRR	false rejection rate
FTC	Federal Trade Commission
FTP	file transfer protocol
GIAC	Global Information Assurance Certification
GLBA	Gramm-Leach-Bliley Act
HIDS	host-based intrusion detection system
HIPAA	Health Insurance Portability and Accountability Act
HIPS	host-based intrusion prevention system
HTML	hypertext markup language
HTTP	hypertext transfer protocol
IAB	Internet Architecture Board
ICMP	Internet Control Message Protocol
IDEA	International Data Encryption Algorithm
IDPS	intrusion detection and prevention system
IDS	intrusion detection system
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
InfoSec	information security

IPS	intrusion prevention system
IPSec	IP security
IPv4	Internet protocol version 4
IPv6	Internet protocol version 6
IRS	Internal Revenue Service
(ISC)²	International Information System Security Certification Consortium
ISO	International Organization for Standardization
ISP	Internet service provider
ISS	Internet security systems
ITRC	Identity Theft Resource Center
ITU	International Telecommunication Union
IVR	interactive voice response
LAN	local area network
MAN	metropolitan area network
MD5	Message Digest 5
modem	modulator demodulator
NAT	Network Address Translation
NFIC	National Fraud Information Center
NIDS	network intrusion detection system
NIPS	network intrusion prevention system
NIST	National Institute of Standards and Technology
NMS	network management system
OS	operating system
OSI	open system interconnection
PBX	private branch exchange
PCI	Payment Card Industry
PGP	Pretty Good Privacy
PKI	public key infrastructure
RAID	redundant array of independent disks
RFC	Request for Comments
RSA	Rivest, Shamir, and Adleman (algorithm)
SAN	storage area network
SANCP	Security Analyst Network Connection Profiler
SANS	SysAdmin, Audit, Network, Security
SAP	service access point
SCSI	small computer system interface
SET	secure electronic transaction
SGC	server-gated cryptography
SHA	Secure Hash Algorithm
S-HTTP	secure HTTP
SLA	service level agreement
SMFA	specific management functional area
SNMP	Simple Network Management Protocol
SOX	Sarbanes-Oxley Act of 2002 (also Sarbox)
SSA	Social Security Administration
SSCP	Systems Security Certified Practitioner
SSL	Secure Sockets Layer
SSO	single system sign-on
STP	shielded twisted cable
TCP/IP	Transmission Control Protocol/Internet Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TFTP	Trivial File Transfer Protocol
TNI	trusted network infrastructure
UDP	User Datagram Protocol
UPS	uninterruptible power supply
USB	universal serial bus
UTP	unshielded twisted pair cable
VLAN	virtual local area network
VoIP	Voice over Internet Protocol
VPN	virtual private network
W3C	World Wide Web Consortium
WAN	wide area network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	wireless local area network
WNIC	wireless network interface card
WPA	Wi-Fi Protected Access
WWW	World Wide Web

EK

C

CompTIA Security + Sertifikası Almak

Neden InfoSec'i (Bilgi Güvenliğini) Kariyer Olarak Seçmelisiniz

CIO 2016 Durum Raporu'na göre, güvenlik yönetimi ankete katılan CIO'lar için üçüncü en önemli faaliyet alanı haline geldi. Siber güvenliğin arttırılması çoğu zaman diğer faaliyet alanlarının gerisinde kalan bir işletme yönergesi olmuştur ancak bu durum değişmektedir. Siber güvenliğin iyileştirilmesi gittikçe daha fazla önem kazanırken, eğitimli güvenlik personeli havuzunun ihtiyacı karşılamakta yetersiz kaldığı açıkça ortaya çıkıyor.

2015 $(ISC)^2$ Küresel Bilgi Güvenliği İşgücü Çalışması, 2020 yılına kadar 1,5 milyon eğitimli güvenlik personeli eksikliği olacağını öngörüyor. Şimdi InfoSec alanına girmek ve çözümün bir parçası olmak için harika bir zaman.

NOT

2016 CIO Durum Raporu'nun tamamını http://www.cio.com/article/3022833/cio-role/state-of-the-cio-2016-its-complicated.html adresinden indirebilir ve okuyabilirsiniz. 2015 (ISC)2 Küresel Bilgi Güvenliği İşgücü Çalışması'nı https://www.isc2cares.org/uploadedFiles/ wwwisc2cares-org/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf adresinde bulabilirsiniz.

InfoSec uzmanları, güvenlik uygulayıcısından bilişim kurulu başkanına kadar çeşitli pozisyonlara sahiptir ve deneyimli, sertifikalı bir bilgi güvenliği uzmanı için ortalama maaş yılda yaklaşık 100.000$'dır. Ayrıca, bilgi güvenliği uluslararası bir problem olduğundan bu yetenekler dünya çapında talep görmektedir. Aşağıdaki bölümler başlamanız için size birkaç ipucu vermektedir.

Bilgi Güvenliği Alanına Girmek

Eğitimli Olun - Bilgi güvenliğinde bir kariyer seçerseniz, bilgi sistemlerine yönelik gelişen tehditleri ele almak için uzmanlık eğitimi almanız gerekecektir. Uzun yıllar boyunca görülen zayıflıklar ve tehditler - hackleme, solucanlar, virüsler, veri hırsızlığı ve verinin bozulması - bugün hala geçerlidir, ancak yeni tehditler - mobil güvenlik, bulut bilişim, yazılım/uygulama ve sosyal medya açıkları gelişmeye devam ediyor.

Sertifika alın - Elbette çoğu öğrenci ve yeni mezun, en seçkin sertifikaları almak için gerekli deneyime sahip olmayacaktır. Ancak bazı pratik deneyimler kazandıktan sonra, daha fazla sertifika elde edilebilir. Başlangıç için en uygun olan, CompTIA Security+ sertifikası gibi, giriş düzeyinde bir güvenlik sertifikası almaktır. Security+ sertifikası üreticiden bağımsızdır ve genellikle sertifika sahibini, işe alım fırsatları için değerlendirilen diğer giriş seviyesi adaylardan ayırır. Bilgi güvenliği alanında faaliyet göstermek için gerekli olan bilgi genişliğini elde etmek için zaman ayırdığınızı gösterir.

Tecrübe Kazanın—Doğru eğitim ve sertifikasyon önemlidir ancak deneyim herşeyden önemlidir. Tecrübe, pratik bilginizi birçok alanda derinleştirir ve ayrıca sizi daha seçkin sertifikalar için yeterli hale getirir. Global olarak tanınan bir veya daha fazla seçkin sertifika alarak, rekabetinizde üstünlük sağlayarak bilgi sistemleri güvenliğindeki bilgi, beceri ve yeteneklerinizi kanıtlamış olacaksınız.

Kariyerinizi Başlatmada Yardımcı Olmak İçin CompTIA Security+'ı Değerlendirin

CompTIA Security+ sertifikası, herhangi bir düzeyde deneyim gerektirmeyen teknik bir sertifikadır. Bununla birlikte, CompTIA, adayların en az 2 yıl ilgili BT yönetimi deneyimine sahip olmasını ve Network+ sertifikasını almış olmalarını önermektedir. Security+ sertifikası, güvenlik olaylarına karşı tepki vermek için güvenlik kavramları, araçları ve prosedürlerini uygulama bilgisine sahip olurken, güvenlik tehditlerine karşı koruma sağlamak için bilgi sistemlerini sürekli izleyen uygulayıcılar içindir. Bu belgelendirme, teknik ve mühendislikle ilgili bilgi güvenliği pozisyonlarının yanı sıra özel olarak güvenlikle ilgili olmayan bilgi teknolojisi pozisyonlarına sahip olan veya yönelik çalışan bireylere uygundur. Örneğin, bir ağ güvenliği mühendisi, sistem güvenliği analisti veya güvenlik yöneticisi olarak çalışıyor olabilirsiniz. Bu sertifika, güvenlik kavramları ve en iyi uygulamaların anlaşılmasını gerektiren bir bilgi teknolojisi pozisyonunda çalışanlar için de iyi bir seçenek olabilir. Bu tür güvenlikle ilgili olmayan pozisyonlar sistem yöneticileri, uygulama programcıları, veritabanı yöneticileri ve sistem analistlerini içerebilir. Sertifikanın odağı, bilgi güvenliğinin teknik yönleri ve belirtilen politikalara uygun olarak bilgi sistemlerinin tasarımı, uygulanması ve yönetimidir. Security+ sertifikasyonunun değerini arttırmak için, sertifikasyon 8570.1 Direktifini karşılamak için ABD Savunma Bakanlığı tarafından da onaylandı. Eğer bilgi güvenliğinde devlet konumunda bir pozisyonda işe girmek istiyorsanız, 8570.1 Direktifini sağlayan bir sertifika almak çok yardımcı olacaktır.

Hızla gelişen teknolojiler nedeniyle, Security+ sertifikasyonunun sınav hedefleri gelişmeye devam edecektir, bu nedenle CompTIA sınavlarını periyodik olarak güncellemektedir. Bu sertifikasyon sınavı, günümüzün mobil bilişim, bulut bilişim, risk yönetimi, yazılım güvenliği, iş sürekliliği planlaması ve bir felaketten nasıl kurtarılacağı gibi bilgi güvenliği sorunlarını ele almaktadır.

CompTIA Security+ sınavının bu ders kitabı kapsamındaki altı alanı şunlardır:

- 1.0 Ağ Güvenliği
- 2.0 Uyum ve Operasyonel Güvenlik
- 3.0 Tehditler ve Güvenlik Açıkları
- 4.0 Uygulama, Veri ve Ana Bilgisayar Güvenliği
- 5.0 Erişim Kontrolü ve Kimlik Yönetimi
- 6.0 Şifreleme

Sertifika Neden Önemli

Dünyada ve Amerika Birleşik Devletleri'ndeki işe alım yöneticilerinin yüzde 90'ından fazlası, en büyük işe alım zorluklarının doğru beceri ve deneyim seviyesine sahip adaylar bulmak olduğunu belirtmektedir. İşverenler, Security+ gibi bir sertifikaya sahip olan adayların bilgi güvenliği alanındaki bilgilerini kanıtladığını anlamaktadır. Bilgiyi açığa çıkarmak için özgeçmişlerini incelemek zorunda kalmazlar. Elbette, sertifikasyona eşlik eden deneyimi ararlar ancak ilk işinize başvururken bazen bunu sunmak zor olabilir. Ayrıca, belirli sertifika sahiplerinin, sertifika sahibi olmayan bilgi güvenliği uygulayıcılarından/profesyonellerinden yaklaşık olarak yüzde 20 daha fazla kazandıkları bilinmektedir.

Hangi sertifikanın/sertifikaların alınacağına karar verirken, önceden plan yapmak önemlidir. Aşağıda göz önünde bulundurmanız gerekenler yer almaktadır:

- Sertifika, teknolojiye veya satıcıya özel midir? Test edilen beceriler herhangi bir ortama uygulanabilir mi?
- Sertifika global olarak tanınmakta mıdır? Uluslararası iş başvurusunda bulunmak istiyorsanız, bir işverenin yeteneklerinizi takdir ettiğinden nasıl emin olabilirsiniz?
- Birçok kuruluş ve devlet kurumu adaylarının sertifikalandırılmasını talep etmektedir; almayı düşündüğünüz sertifika onların ihtiyaçlarını karşılıyor mu?
- İlk sertifikanızı kazandıktan sonra ve kariyer yolunda ilerlemek istediğinizde, yolculuğunuzda size yardımcı olacak başka sertifikalar var mı?
- Sertifika sahibi olmak becerilerinizin her zaman güncel kalmasını sağlamak için size daha fazla eğitim fırsatı sunuyor mu?
- Sertifika onaylayan kuruluş, üyelerine ücretsiz ya da düşük maliyetli küresel etkinlikler ve ağ oluşturma fırsatları sağlıyor mu?

CompTIA Hakkında

Bilişim Teknolojileri Endüstrisi Birliği (Computing Technology Industry Association - CompTIA), 1982 yılında, bilgi teknolojisi endüstrisi için eğitim ve satıcıya yönelik profesyonel sertifikalar sunmak üzere kurulmuş kar amacı gütmeyen bir ticaret birliğidir. CompTIA, Security+ sertifikasına ek olarak çok çeşitli sertifikalar sunmaktadır. Diğer popüler CompTIA sertifikaları: A+ (bilgisayar teknisyeni), Network+, CompTIA Gelişmiş Güvenlik Uygulayıcısı (CompTIA Advanced Security Practitioner - CASP), Server+, Sertifikalı Teknik Eğitimci (Certified Technical Trainer - CTT+), Sertifikalı Belge Görüntüleme Mimarı (Certified Document Imaging Architect - CDIA+), Linux+, Project+, Yakınsama Teknolojileri Profesyoneli (Convergence Technologies Professional - CTP+), Cloud+ ve Network+. CompTIA hakkında daha fazla bilgi için *https://www.comptia.org/* adresini ziyaret edin.

CIO 2016 Durum raporunun tamamını *http://www.cio.com/article/3022833/cio-role/state-of-the-cio-2016-its-complicated.html* adresinden indirebilir ve okuyabilirsiniz.

2015 (ISC)2 Küresel Bilgi Güvenliği İşgücü Çalışması *https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf* adresinde mevcuttur.

Anahtar Terimler Sözlüğü

(ISC)² | Uluslararası Bilgi Sistemleri Güvenlik Sertifikasyon Konsorsiyumu. Bilgi sistemleri güvenlik uzmanlarını sertifikalandırmaya adanmış kâr amacı gütmeyen bir organizasyondur.

A

ABD Vatanseverlik Kanunu (USA Patriot Act) | 11 Eylül 2001'deki terörist saldırılara yanıt olarak yürürlüğe giren ve kanun uygulayıcı kurumların ABD'de istihbarat toplama konusundaki kısıtlamalarını önemli ölçüde azaltan bir yasadır; Hazine Bakanı'nın, özellikle yabancı şahısları ve kurumları içeren finansal işlemleri düzenleme yetkisini ve terör ve ilgili eylemlerden şüpheli göçmenleri gözaltına alma ve/veya sınır dışı etmede kolluk kuvvetleri ve göçmenlik makamlarının takdir yetkisini genişletmiştir.

Acil durum operasyon grubu (Emergency operations group) | Diğer olası acil durumlar arasında, doğal afet veya ekipman arızası durumunda hassas verilerin korunmasından sorumlu olan bir gruptur.

Acil durum operasyon merkezi (Emergency operations center - EOC) | Bir felaket sırasında kurtarma ekibinin buluştuğu ve çalıştığı yerdir.

Aciliyet/Öncelik (Urgency) | Birinin bir şeyler yapmasını veya bilgi paylaşmasını sağlamak için öncelik veya acil stres durumunu kullanan bir sosyal mühendislik saldırısıdır.

Açık anahtar altyapısı (Public key infrastructure-PKI) | Güvenilir varlıklar ve dijital sertifikalar kullanarak şifreleme anahtarlarını idare etme konusunda genel bir yaklaşımdır; dijital sertifikaların tüm yönlerini yönetmeye yönelik donanım, yazılım, politikalar ve prosedürlerdir.

Açık eylem (Overt act) | Açıkta gerçekleştirilen veya başkaları tarafından kolayca izlenebilen bir eylemdir.

Açık Kimlik Denetleme için Girişim (Initiative for Open Authentication - OATH) | Kimlik denetleme için açık standartları ve şifreleme kullanımını destekleyen ortak bir organizasyondur.

Açık metin (Cleartext) | Şifrelenmemiş veriler, şifreli metnin tersidir. Açık metin olarak gönderilen veriler okunabilir ve anlaşılabilir.

Açık Sistemler Ara Bağlantısı (Open Systems Interconnection - OSI) Referans Modeli (Reference Model) | Ayrı bilgisayar sistemlerinin, ağları kullanarak nasıl iletişim kurduğunu belirleyen uluslararası kabul görmüş bir standartlar çerçevesidir.

Açık şifreleme (Open ciphers) | Kaynak kodunun kolaylıkla bulanabildiği şifrelemelerdir, bu da dünya çapındaki uzmanların şifrelemeleri zayıf yönleriyle incelemelerini mümkün kılar.

Açık/kamusal/asimetrik anahtar kriptografisi (Asymmetric key cryptography) | Matematiksel olarak ilişkili iki anahtar kullanan - verileri şifrelemek için bir anahtar ve verilerin şifresini çözmek için bir anahtar - bir şifreleme tekniğidir.

Açıklama (Disclosure) | 1. korunan bilgilere erişen yetkilendirilmemiş bir kullanıcının herhangi bir örneğidir. 2. HIPAA kapsamında, kapsanan bir varlığın (*covered entity*) korunan bilgileri diğer organizasyonlarla nasıl paylaştığına dair bir referanstır.

Açılır pencere (Popup) | Tarayıcı penceresinin üstünde görünen bir pencere türüdür. Açılır pencereler genellikle reklam içerir. Açılır pencereler kesinlikle reklam yazılımı (*adware*) olmasa da birçok reklam yazılımı programı bunları kullanıcılarla etkileşimde bulunmak için kullanır.

Açılır pencere engelleyici (Pop-up blocker) | Tarayıcının açılır pencereleri görüntülemesini yasaklayan bir web tarayıcı seçeneğidir. Bu, yanlışlıkla kötücül yazılımların yürütülmesine maruz kalma riskini azaltabilir.

Adres Çözümleme Protokolü (Address Resolution Protocol - ARP) | ARP, bir İnternet Protokolü (IP) adresini fiziksel bir adrese veya MAC adresine eşlemek için kullanılır.

Ağ adresi çevirisi (Network address translation - NAT) | Bir sistemin gerçek, dahili IP adresini gizlemek için alternatif, genel bir IP adresi kullanan bir IP adresi atama yöntemidir.

Ağ anahtarları (Network keys) | Anahtarları şifrelemek ve şifresini çözmek için kullanılan yazılım şifreleme anahtarlarıdır.

Ağ arayüz kartı (Network interface card - NIC) | Bu, bir bilgisayar ve Ethernet LAN arasındaki fiziksel arayüzdür. Özgün bir 6 byte'lık MAC-katmanı adresi içerir.

Ağ ayrımı (Network separation) | Trafiği bir ağdan diğerine taşımayı engelleyen, ağlar arasındaki bölünmeleri yürüten güvenlik duvarı filtreleme kurallarıdır.

Ağ bağlantı noktası (Network port) | Bir ağ kablosunun takılı olduğu bir ağ cihazındaki bir donanım jakı veya belirli bir ağ hizmeti türü için belirlenmiş bir tür ağ mesajı (veya sınıfı) tanımlayan bir yazılım yapısıdır.

Ağ erişim denetimi (Network access control - NAC) | Bir ağa erişim kimliği veya diğer kuralları temel alarak kısıtlayan bir yöntemdir.

Ağ haritalama (Network mapping) | Bir kuruluşun sistemlerinde ve ağlarında çalışan hizmetleri ve yerleşim planını belirlemek için araçların kullanılmasıdır.

Ağ keşfi (Network reconnaissance) | Gelecekteki bir saldırıda kullanılmak üzere bir ağ veya sistem hakkında bilgi toplamadır.

Ağ operasyon merkezi (Network operations center - NOC) | Bir telekomünikasyon servis sağlayıcısının omurga ağı ve müşteri ağları için kumanda denetim merkezidir. Müşteri arıza aramaları, yönetilen hizmetleri ve SLA'ları desteklemek için NOC tarafından cevaplandırılmaktadır.

Aile Eğitim Hakları ve Mahremiyet Kanunu (Family Educational Rights and Privacy Act - FERPA) | K-12 ve yükseköğretim kurumlarının uyması gereken, transkriptleri ve notları da dahil olmak üzere, öğrencilerin özel verilerini koruyan bir ABD federal yasasıdır.

Akıllı kart (Smart card) | Kart üzerindeki mikroçip veya manyetik bir şeride gömülü kimlik denetleme bilgilerine sahip plastik bir karttır.

Akıllı telefon (Smartphone) | Mobil iletişim yazılımını çalıştıran ve ses, İnternet taraması, e-posta ve metin mesajlaşmasını destekleyen bir cep telefonudur.

Akreditasyon (Accreditation) | Yetkilendirme görevlisinin sistemi uygulama riskinin resmi olarak kabulüdür.

Akredite/Onaylanmış (Accredited) | Kurumun uygulanabilir standartları karşılayıp karşılamadığını belirlemek için dış bir kuruluş tarafından değerlendirmeden başarıyla geçmiş olan bir eğitim kurumunu ifade eder.

Aksama (Disruption) | Ani bir planlanmamış olaydır.

Aktarım şifrelemesi (Transport encryption) | Aktarım sırasında iletişim güvenliğini sağlama sürecidir, genellikle yazılım tarafından yapılır.

Aktif içerik (Active content) | Kullanıcılarla etkileşimde bulunmak için işlevsellik sağlayan, özellikle web sitelerinde bulunan bileşenleri ifade eder.

Alan Adı Sistemi (Domain Name System - DNS) | Tam etki alanı adlarını (*fully qualified domain names* - FQDN) karşılık gelen IP adreslerine çözümleyen bir ağ servisidir. DNS, çoğu ağın ve bunların dizin hizmetlerinin temel bir servisidir.

Aldatma (Spoofing) | Bir kaynağa erişmek için bir kişinin, programın veya bilgisayarın kendisini başka bir kişi, program veya bilgisayar olarak gizlediği bir saldırı türüdür.

Aldatmaca (Hoax) | Alıcıyı aldatmaya veya kandırmaya yönelik bir eylemdir. Bu bağlamda, aldatmacalar normalde e-posta mesajları ile dolaşır. Genellikle, bu mesajlar tahrip edici yeni virüslerle ilgili uyarılar içerir.

Algılayıcı denetim (Detective control) | Bir eylem gerçekleştiğinde algılayan bir denetimdir. Algılayıcı denetimler duman dedektörlerini, log monitörlerini ve sistem denetimlerini (*audit*) içerir.

Algoritma (Algorithm) | Bir çeşit matematik fonksiyonu gerçekleştirmek için kullanılan matematiksel bir işlem veya formüldür.

Alt ağ (Subnet) | IP adresinin aynı ağ adresi bölümünü paylaşan cihazlar tarafından tanımlanan bir ağ bölümüdür.

Alt ağ maskesi (Subnet mask) | IPv4 adresleri için ağ ile ana bilgisayar adresleri arasındaki ayırma çizgisini tanımlayan bir ağ yapılandırma parametresidir. Maske, ağ bitleri için tüm "1"ler ve ana bilgisayar bitleri için "0"ların tümü olarak ayarlanmış bir 32 bitlik sayıdır.

Alt ağ maskesi adresi (Subnet mask address) | IP ağ numarasını ve IP ana bilgisayar adresini tanımlayan bir IP adresinin tamamlayıcısıdır.

Amerikan Ulusal Standartlar Enstitüsü (American National Standards Institute - ANSI) | Amacı, tüketicilerin güvenliğini, sağlığını, ve çevreyi korumaya yardımcı olurken, küresel ekonomideki ABD pazarının konumunu güçlendirmek için üyelerine ve kurucularına yetki vermek olan bir ABD standartlar organizasyonudur.

Anahtar (Key) | Bir şifrelemenin, bilgileri şifrelemek veya şifresini çözmek için kullandığı gizli bir değerdir.

Anahtar (Switch) | Gönderen ve alan bir port arasında doğrudan bir bağlantı oluşturan, ağ bölümlerini birbirine bağlayan bir ağ cihazıdır.

Anahtar dağıtım merkezi (Key distribution center) | Bir kriptosistemin geçerli kullanıcılarına iletişim kurabilmeleri için anahtar verme işlemidir.

Anahtar dağıtımı (Key distribution) | Bir şifreleme anahtarının, anahtar üreticisinden anahtar kullanıcısına, herhangi bir yetkilendirilmemiş kullanıcıya bildirilmeden güvenli bir şekilde taşınması işlemidir.

Anahtar dizini (Key directory) | Tüm ortak anahtarların güvenilir bir deposudur.

Anahtar emaneti (Key escrow) | Belirli şartlar altında yetkilendirilmiş bazı üçüncü şahısların bir anahtara erişimine izin veren harici bir anahtar saklama yöntemidir.

Anahtar kelime karıştırılmış alfabe şifrelemesi (Keyword mixed alphabet cipher) | Bir anahtar kelimeden oluşan, bir şifreleme alfabesi kullanan, tekrar eden harflerin çıkarılmasının ardından alfabenin kalan harflerini içeren bir şifrelemedir.

Anahtar şifreleme anahtarı (Key-encrypting key) | İletmeden önce diğer anahtarları şifrelemek için kullanılan bir şifreleme anahtarıdır.

Anahtar uzatma (Key stretching) | Girdi olarak bir anahtar (genellikle zayıf bir anahtar) alan ve daha kararlı bir saldırıya dayanabilen gelişmiş bir anahtar üreten bir fonksiyondur.

Anahtar uzayı (Keyspace) | Tüm olası şifreleme anahtarlarının kümesidir.

Anahtar yönetimi (Key management) | Şifreleme anahtarlarını yönetme ve koruma işlemidir.

Anahtarın iptal edilmesi (Key revocation) | Birinin artık güvenilmez olduğu veya bir kriptosistemi kullanmasına izin verilmediği bir durumdur. Herkesin aynı anahtarı paylaştığı simetrik bir anahtar sisteminde, anahtarın bir kopyasını riske atmak tüm kopyaları riske atar.

Anlık mesajlaşma (IM) sohbeti (Instant messaging (IM) chat) | Bire-bir veya bire-çok gerçek zamanlı sohbeti destekleyen bir oturum başlatma protokolü (*session initiation protocol* - SIP) uygulamasıdır. Örnekler, AOL IM, Yahoo! Messenger ve Google Talk'u içermektedir.

Anlık mesajlaşma sohbeti (IM chat) | Bkz. Anlık mesajlaşma (Instant messaging - IM) sohbeti.

Anomali tabanlı IDS (Anomaly-based IDS) | Mevcut aktiviteyi, normal (beklenen) aktivitenin kayıtlı profilleri ile karşılaştıran bir saldırı tespit sistemidir.

Antivirüs (Antivirus) | Başta virüs, solucan ve Truva atı dahil olmak üzere bazı kötü amaçlı yazılım türlerini tespit etmek ve azaltmak için tasarlanmış yazılımdır.

Arabellek taşması (Buffer overflow) | Bir bellek arabelleğinin kapasitesini aştığı ve içeriğini bitişik belleğe genişlettiği bir durumdur. Genellikle zayıf programlama tekniklerine veya zayıf yazılım kalite kontrolüne karşı bir saldırı olarak kullanılır. Bilgisayar korsanları, bellekte tutabildiklerinden daha fazla veri enjekte edebilir ve bu da bir sonraki bellek alanına ek verilerin taşmasına neden olabilir. Eğer taşma, kod yürütme için belirlenen bir sonraki bellek bölümüne genişlerse, yetenekli bir saldırgan, mevcut programla aynı ayrıcalıklarla yürütülecek isteğe bağlı kod ekleyebilir. Yanlış biçimlendirilmiş taşma verileri aynı zamanda sistemin çökmesi ile sonuçlanabilir.

Arama motoru optimizasyonu (Search engine optimization - SEO) | Bir siteyi daha tarayıcı dostu yapmak için kullanılan stratejileri ifade eder.

Araştırmada Akademik Mükemmellik Ulusal Merkezleri (National Centers of Academic Excellence in Research - CAE/R) | Özel federal bilgi güvenliği araştırma yönergelerine uyan kurumlardır.

Arındırılmış bölge (Demilitarized zone - DMZ) | Kamusal İnternet ve bir organizasyonun BT altyapısı arasında (örneğin, LAN-dan-WAN'a Etki Alanı) tampon bir bölge görevi gören bir dış ağdır.

Arıza için ortalama süre (Mean time to failure - MTTF) | Bir cihazın bir arızayla karşılaşmadan önce çalışması beklenen ortalama süredir.

Arızalar arasındaki ortalama süre (Mean time between failures - MTBF) | MTBF, bir IT sisteminin üretim işlemi sırasındaki başarısızlıkları arasındaki öngörülen süredir.

Arka kapı (Backdoor) | Normal erişim denetimlerini atlayan bir bilgisayar kaynağına belgelenmemiş ve çoğunlukla yetkilendirilmemiş bir erişim yöntemidir.

Artakalan risk (Residual risk) | Önlem ve denetimleri kurduktan sonra kalan risktir.

Asenkron belirteç (Asynchronous token) | Bir sunucu ile kimlik sorma-cevap kimlik denetlemesini işlemek için kullanılan bir kimlik denetleme belirtecidir. Belirteç, sunucunun kimlik sorma değerini alır ve bir cevap hesaplar. Kullanıcı, bir bağlantıyı doğrulamak için cevabı girer.

Azaltıcı faaliyetler (Mitigation activities) | Bir güvenlik açığının zararını azaltmak veya tamamen ortadan kaldırmak için tasarlanmış faaliyetlerdir.

B

Bağlantı noktası güvenliği (Port security) | Bağlantı noktalarına göre trafiği filtreleyen güvenlik duvarı filtreleme kurallarıdır.

Bağlantı şifreleme (Connection encryption) | İletişimin uçtan uca güvenliğinin sağlandığından emin olunmasıdır, örneğin bir HTTPS web sitesi ve bir masaüstü veya mobil cihazın güvenli tarayıcı bağlantısı arasındaki iletişim.

Bal ağı (Honeynet) | Gerçek bir canlı ağı simüle etmek için yapılmış, ancak ondan izole edilmiş bir grup bal küpüdür.

Bal küpü (Honeypot) | Potansiyel bilgisayar korsanlığı saldırılarına karşı yem görevi görmek için bir ağın kenarında konuşlandırılmış bir ana bilgisayar veya servistir. Bal küpünün amacı, saldırılar için kontrollü bir ortam sağlamaktır. Bu, ağın gücünü test etmek için saldırıyı kolayca tespit ve analiz etmenizi sağlar.

Balina avcı (Whaling) | Yönetici kullanıcısını veya en değerli çalışanları hedef alan bir oltalama (*phishing*) saldırısıdır, aksi takdirde "balina" veya "büyük balık" olarak kabul edilir. Aynı zamanda, genellikle yüksek oranda odaklanılan bir oltalama saldırısında olduğu gibi "hedef odaklı oltalama (*spear phishing*)" olarak da adlandırılır.

Bant dışı anahtar değişimi (Out-of-band key exchange) | Veri için kullandığınız anahtardan farklı olarak anahtar alışverişi yapabileceğiniz farklı bir iletişim kanalıdır.

Bant içi anahtar değişimi (In-band key exchange) | Anahtar değişimi yapmak için kişinin kendi IP veri ağının kullanılmasıdır.

Basit Ağ Yönetimi Protokolü (Simple Network Management Protocol - SNMP) | IP cihazları ile SNMP veri toplama sunucusu arasında ağ yönetimi verilerini iletmek için kullanılan, güvenli olmayan, bağlantısız UDP tabanlı bir protokoldür.

Başlık manipülasyonu (Header manipulation) | Güvenli olmayan bir iletişim veya eylem yaratmak için geçersiz veya yanlış komutlarla başlığı değiştirme, çerezleri ve tarayıcı URL bilgilerini çalma eylemidir.

Belirteç (Token) | Kullanıcının kimliğini denetlemek için kullanıcıya gizli bir kod ileten fiziksel bir cihazdır. Bir donanım cihazı belirteci veya yazılım tarafından üretilen bir belirteç olabilir.

Bell-La Padula modeli (Bell-La Padula model) | Hiyerarşi tabanlı sistemlere, uygulamalara ve verilere erişim için çok katmanlı güvenlik sağlayan bir erişim denetim modelidir.

Beyaz kutu testi (White-box testing) | Uygulamanın tasarım ve kaynak kod bilgisini temel alan bir güvenlik testidir.

Beyaz Liste (Whitelisting) | Güvenilir web sitelerinin listesini tutma eylemidir. Beyaz listede olmayan sitelerin tüm mesajları ve bağlantı istekleri yok sayılır.

Beyaz şapka korsanı (White-hat hacker) | Güvenlik açıklarını gidermek veya düzeltmek için çeşitli penetrasyon test araçlarını kullanan bir bilgi güvenliği veya ağ uzmanıdır. *Ayrıca bkz. etik bilgisayar korsanı (ethic hacker).*

Biba bütünlük modeli (Biba integrity model) Veri bütünlüğünü sağlamak için tasarlanmış erişim denetim kurallarıdır. Veriler ve özneler, sıralanmış bütünlük seviyelerinde gruplandırılmıştır; bu, kullanıcıların erişebileceklerinden daha yüksek seviyedeki verileri bozmasını önler ve veri bütünlüğünü sağlamaya yardımcı olur.

Bilgi (Knowledge) | Kimlik denetlemede, parola, uzun parola (*passphrase*) veya PIN gibi bildiğiniz bir şeydir.

Bilgi Güvenliği Eğitiminde Ulusal Akademik Mükemmellik Merkezleri (National Centers of Academic Excellence in Information Assurance Education - CAE/IAE) | Özel federal bilgi güvenliği eğitim yönergelerine uyan eğitim kurumlarıdır.

Bilgi güvenliği (Information security) | Verilerin kendisinin korunmasıdır.

Bilgi sistemleri (Information systems) | Bilgi ve verinin bulunduğu sunucular ve uygulama yazılımıdır.

Bilgi sistemleri güvenliği (Information systems security) | Bilgi sistemlerinin, uygulamaların ve verilerin korunmasıdır.

Bilgi Teknolojileri Güvenlik Değerlendirmesi için Ortak Kriterler (Common Criteria for Information Technology Security Evaluation) | Bilgisayar güvenliği için ISO/IEC 15408 standardıdır.

Bilgisayar korsanı (Hacker) | Bilgi edinmek için bilgisayar ortamlarını araştıran bir bilgisayar uzmanıdır.

Bilinmesi gereken (Need to know) | Belirli bir nesneye erişmesi gerektiğini belirten belirli bir özneyi belirten bir özelliktir., Bu, nesnenin sınıflandırması için uygun izne sahip olmasının yanı sıra, nesneye erişmek için de gereklidir.

Birbirine bağlı güvenlik sözleşmesi (Interconnection Security Agreement - ISA) | Bağlantılı varlıkların teknik gereksinimlerini belgeleyen, çoğu zaman bir MOU'nun bir uzantısı olan birlikte çalışabilirlik anlaşmasıdır.

Birleşik iletişim (Unified communications) | Tek bir ağ üzerinde, anlık mesajlaşma, ses, görüntü ve veri gibi kurumsal iletişim çoklu türlerinin entegrasyonudur.

Birleşik mesajlaşma (Unified messaging - UM) | Faks, e-posta ve sesli iletişimin tek bir yerde saklanmasıdır.

Birleşik şifreleme (Product cipher) | Birden çok şifrenin birleşimi olan şifreleme kodudur. Her biri yer değiştirme (*transposition*) veya yerine koyma (*substitution*) olabilir.

Birleşik tehdit yönetimi (Unified threat management - UTM) | Filtreleme sağlamak için kullanılan cihazlar ve bunlara ek birçok güvenlik servisi.

Birlik (Federation) | Kimlik denetleme bilgilerini paylaşan sunucular topluluğudur.

Birlikte çalışabilirlik (Interoperability) | Birlikte çalışmak üzere yapılandırılabilecek bilgisayarları, cihazları veya uygulamaları tanımlamak için kullanılan bir terimdir.

Bitirme sertifikası (Certificate of completion) | Bir öğrencinin dersleri tamamladığını ve sınavda yeterli bir puan aldığını doğrulayan bir belgedir.

Biyometrik (Biometrics) Fizyolojik veya davranışsal bir insan tanıma sistemidir (örneğin, parmak izi okuyucu, retina tarayıcı, ses tanıma okuyucusu, vb.).

BlackBerry (BlackBerry) Akıllı telefonlar ve elde taşınan mobil cihazlar için bir marka adıdır.

Blok şifreleme (Block cipher) Bir kerede bir girdi bloğun tamamını şifreleyen kriptografik şifrelemedir.

Bluejacking (Bluejacking) | İstenmeyen mesajları Bluetooth kullanarak, alıcının mesajları açmasını ve potansiyel olarak alıcının cihazına bulaşmasını sağlamak için başka bir cihaza göndermektir.

Bluesnarfing (Bluesnarfing) | Veri çalmak amacıyla Bluetooth özellikli bir cihaza erişmektir.

Bot-herder (Bot-herder) Bir botnet işleten bilgisayar korsanıdır.

Bölge aktarımı (Zone transfer) | Bölgesinin içeriğini soran bir DNS sunucusunun özgün bir sorgusudur.

Brewer ve Nash bütünlük modeli (Brewer and Nash integrity model) | Adil rekabeti sağlamak için 1989 yılında yayınlanan matematiksel bir teoriyi temel almaktadır.

Brute-force/Kaba kuvvet parola saldırısı (Brute-force password attack) | Her giriş kombinasyonunu deneyerek oturum açma ve parola erişim denetimlerini ihlal etmek için kullanılan bir yöntemdir. Brute-force parola saldırıları, genellikle kullanıcı bilgisini elde etmek için sosyal mühendislik kullanımı da dahil olmak üzere belirli bir saldırı planını takip eder.

BT güvenlik politikası çerçevesi (IT security policy framework) | Güvenlik için birtakım kurallardır. Çerçeve hiyerarşiktir ve politikaları, standartları, prosedürleri ve yönergeleri içerir.

Bulut bilişim (Cloud computing) | Uygulamaya ve verilere uzaktan erişime sahip sanallaştırılmış bir veri merkezinde barındırılan hesaplama servislerinin kullanım uygulamasıdır (örneğin, Hizmet Olarak Yazılım [Software as a Service - SaaS] bulut bilişim kullanır).

Bulut Güvenliği Birliği (Cloud Security Alliance - CSA) | Bulut bilişim kullanımı için en iyi güvenlik uygulamalarını teşvik etme misyonuyla kar amacı gütmeyen bir organizasyon.

Bulut servis sağlayıcısı (Cloud service provider - CSP) | Her biri birden fazla sanal makine çalıştıran sunucu bilgisayarlarının raflarıyla veri merkezlerini barındıran ve aynı anda birçok müşteriye hizmet sağlayabilen bir şirkettir. Her tür kuruluş, kendi veri merkezlerini barındırmak zorunda kalmamak için CSP'lere başvurmaktadır.

Bütünlük (Integrity) | Bilginin veya verilerin geçerliliğidir. Bütünlüğü yüksek olan veriler değiştirilmemiş veya tahrif edilmemiştir.

C - Ç

California Veritabanı Güvenlik İhlali Kanunu (California Database Security Breach Act - SB 1386) | Kendi türünün ilk yasasıdır, bir güvenlik ihlali olduğunda müşterilerini bilgilendirmek için müşteri verilerini elektronik olarak saklayan herhangi bir şirketi gerektirir.

Casus Yazılım (Spyware) | Kullanıcı bilgilerini, kullanıcının bilgisi olmadan kullanıcının İnternet bağlantısı üzerinden toplayan yazılımdır.

Caydırıcı denetim (Deterrent control) | İstenen bir işlemi tamamlamanın bir ihlal veya tehdit ile sonuçlanabileceği konusunda kullanıcıyı uyaran bir denetimdir.

Christmas/Noel saldırısı (Xmas attack) | Kasıtlı olarak hatalı biçimlendirilmiş bir ağ paketini alıcı ağ cihazının beklenmedik şekilde yanıt vermesini, örneğin yeniden başlatılmasını veya çökmesini umarak gönderen eski bir saldırıdır. Hatalı biçimlendirilmiş paket, bir Noel ağacının ışıkları gibi, "1" olarak ayarlanmış veya etkinleştirilmiş birkaç TCP başlık bitini içerir.

Clark ve Wilson bütünlük modeli (Clark and Wilson integrity model) | 1987'de David Clark ve David Wilson tarafından yayınlanan bu model, kullanıcıların yapmalarına izin verilmeyenleri yapmak için bir sisteme girmelerine izin verildiğinde ne olduğuna odaklanmaktadır.

Çalışma Süresi (Uptime) | BT sisteminin, uygulamanın ve verinin erişilebilir olduğu toplam süredir.

Çapraz hata oranı (Crossover error rate) Biyometrik bir cihazın hassasiyetinin yanlış reddetmeleri (false rejections) ve yanlış kabulü (false acceptance) eşit olarak döndürdüğü noktadır.

Çapraz site betiği/Çapraz site komut dosyası çalıştırma (Cross-site scripting - XSS) | Bir saldırganın istemci tarafı komut dosyası kodunu/betiğini bir web uygulamasına girdiği bir saldırıdır. Kod daha sonra diğer kullanıcılar tarafından görüntülenebilir ve kullanıcıların istemci yazılımı komut dosyası talimatlarını uygulayacaktır. XSS saldırısı, kullanıcıların bir sunucu için sahip oldukları güvenden yararlanır. Bir XSS saldırısının sonuçları, web sitesindeki verilerin bozulmasını veya sitenin ziyaretçilerinin kimlik hırsızlığını içerebilir.

Çapraz-site İstek Sahtekarlığı (Cross-site Request Forgery - XSRF) | XSS saldırısına benzer şekilde, saldırgan, giriş betik/komut dosyasını (*script*) görüntüleyen güvenilir bir kullanıcının bir web sunucusuna kötü amaçlı komutlar göndermesine neden olan betik kodu sağlar. XSRF saldırısı, sunucunun kullanıcıya olan güveninden yararlanır.

Çerez (Cookie) | Bir web sitesinden bir web tarayıcısına daha sonra kullanılmak için saklanmak üzere gönderilen bir metin dosyasıdır. Çerezler, bir web sitesine yapılan ziyaretlerden toplanan detayları içerir.

Çevik geliştirme (Agile development) | Uzun proje döngüleri yerine küçük proje tekrarlamalarına veya sprintlerine dayanan bir yazılım geliştirme yöntemidir.

Çıkarılabilir depolama (Removable storage) | Nispeten kolaylıkla ve zarar vermeden çıkarılabilen ve/veya değiştirilebilen depolama ortamıdır.

Çift taraflı merkezler (Reciprocal centers) | Aynı işi yapan ancak doğrudan rakip olmayan işletmelerin veri merkezleri bir felaket durumunda alternatif işlem alanları olarak kullanılabilir.

Çocukların Çevrimiçi Mahremiyetini Koruma Yasası (Children's Online Privacy Protection Act - COPPA) | 2000 yılında yürürlüğe giren COPPA Kuralı, 13 yaşın altındaki çocuklardan çevrimiçi bilgilerin nasıl toplandığını kısıtlamaktadır.

Çocukların İnternet Koruması Yasası (Children's Internet Protection Act - CIPA) | İnternet üzerinden rahatsız edici içeriğe küçüklerin ve çocukların erişebileceği okul ve kütüphane bilgisayarlarından erişim hakkındaki endişeleri gidermek için Kongre tarafından onaylanmış federal bir yasadır.

Çok biçimli virüs (Polymorphic virus) | Virüsün ana gövdesini çoğaltırken virüs gövdesini şifreli biçimde depolayan ayrı bir şifreleme motoru içeren bir tür kötücül yazılımdır.

Çok bölümlü virüs (Multipartite virus) | Diğer dosyalara bulaşan ve çeşitli şekillerde yayılan bir virüs türüdür.

Çok kiracılı (Multitenancy) | Farklı kullanıcı gruplarının, birbirlerinin verilerine erişmeden veritabanına erişmelerini sağlayan bir veritabanı özelliğidir.

Çoklu Protokol Etiket Anahtarlama (Multiprotocol Label Switching - MPLS) | Bir WAN altyapısında uç noktalar arasında sanal yollar oluşturmak için paket başlığına etiketler (*label* ya da *tag*) ekleyerek Katman 2'de çalışan bir geniş alan ağı teknolojisidir. Bu, IP paketlerinin yönlendirilmesine ve anahtarlanmasına gerek kalmadan IP paketlerinin WAN üzerinden taşınmasının daha hızlı bir yöntemidir.

Çok-Sağlayıcılı Bir Ortamdaki Uygulamalar için Güvenli Avrupa Sistemi (Secure European System for Applications in a Multi-Vendor Environment - SESAME) | Tek Oturum Açma (Single Sign-On) yeteneğini sağlamak için Avrupa Komisyonu tarafından finanse edilen bir araştırma ve geliştirme projesidir. SESAME, Kerberos'taki zayıflıkları gidermek için geliştirilmiştir.

Çöp karıştırma (Dumpster diving) | Bir saldırganın bir kurumun çöpünü veya atılan diğer öğelerini dahili veya özel bilgileri öğrenmek için incelediği bir keşif türüdür. Çöp karıştırmanın sonuçları genellikle sosyal mühendislik saldırılarını sürdürmek için kullanılır.

D

Dağıtık hizmet reddi (Distributed denial of service - DDoS) | Bir sunucunun veya sistemin kullanılabilirliğini engellemek için ping veya ICMP yankı-isteği (*echo-request*) yankı-yanıtlama (*echo-reply*) mesajları kullanan bir saldırıdır. DDoS saldırıları birden fazla ana cihazdan başlatılır.

Dağıtık/Merkezi olmayan erişim denetimi (Decentralized access control) | Erişim denetimini, sistem kullanıcılarına en yakın olan departman yöneticileri gibi kişilere veren bir sistem; bu sistemde erişim isteklerini işleyecek tek bir merkezi varlık yoktur.

Datagram (Datagram) | Başlık (*header*) ve yük (*payload*) veya veriyi de içeren İnternet Protokolü (Internet Protocol - IP) paketinin genel adıdır.

Dayanak (Baseline) | Bir sistemin birden çok uygulama ve farklı ürünler karşısında minimum güvenlik düzeyini sağladığından emin olmak için kullanılan bir karşılaştırmalı değerlendirmedir (*benchmark*).

Değişiklik denetimi (Change control) | Bilgisayar/cihaz konfigürasyonundaki veya uygulama yazılımındaki değişikliklerin yönetilmesi işlemidir.

Değişiklik denetimi komitesi (Change control committee) | BT sistemlerinde, uygulamalarında ve üretim varlıklarında önerilen tüm değişiklikleri denetleyen bir gruptur.

Delphi yöntemi (Delphi method) | Birden fazla turda resmi anonim anketler kullanan bir bilgi ve görüş toplama yöntemidir.

Denetim (Audit) | Bir kuruluşun mevcut finansal durumunun, BT gerçekleştiriminin ve/veya BT güvenlik gerçekleştiriminin bağımsız bir üçüncü parti tarafından incelenmesidir.

Denetim (Control) | Bir saldırıyı önleyen, tespit eden veya ele alan herhangi bir mekanizma veya eylemdir.

Denetim hedefleri (Control objectives) | Bir denetim veya gereksinimin doğru bir şekilde uygulandığında gerçekleştirmesi gereken amaç veya nihai sonuçtur.

Denetimli alt ağ (Screened subnet) | Üç NIC'e sahip bir güvenlik duvarı cihazıdır. Bir NIC İnternete, ikinci NIC iç ağa ve üçüncü NIC bir DMZ'ye bağlanır.

Derinlemesine savunma (Defense in depth) | Kale Yaklaşımı (*Castle Approach*) olarak da adlandırılmaktadır, BT altyapısı (derinlik) boyunca çoklu güvenlik katmanlarının (savunma) gerçekleştirimidir.

Devlet Bilgi Güvenliği Reformu Kanunu (Güvenlik Reformu Kanunu) (Government Information Security Reform Act (Security Reform Act)) | Federal Bilgi Güvenliği Yönetim Kanunu'nun (Federal Information Security Management Act - FISMA) öncüsü olan Güvenlik Reform Kanunu, ABD devlet kurumlarının bilgi güvenliği programına sahip olmasını, periyodik risk değerlendirmeleri yapmasını ve ABD devlet çalışanları için zorunlu güvenlik bilinci eğitimi almasını zorunlu tutmuştur.

DIAMETER (DIAMETER) | RADIUS'u başarıyla geçen, kararlı ve statik iş gücü için erişim denetimi sağlayan popüler bir merkezi erişim denetim protokolüdür.

Diferansiyel kriptanaliz (Differential cryptanalysis) | Çok miktarda şifreli metin için örüntü arama eylemidir.

Diffie-Hellman algoritması (Diffie-Hellman algorithm) | Bir gönderici ve alıcının, simetrik anahtarları güvenli bir şekilde değiştirmek için asimetrik şifreleme kullandığı bir algoritmadır.

Dijital imza (Digital signature) | Bir mesajı veya verileri belirli bir varlığa bağlamak için asimetrik şifreleme kullanan bir nesnedir.

Dijital İmza Algoritması (Digital Signature Algorithm - DSA) | Dijital imzalar için NIST standardıdır. İlk olarak 1993'te Federal Bilgi İşleme Standardı (Federal Information Processing Standard - FIPS) olarak yayınlandı.

Dijital media (Digital media) | Dijital olarak kaydedilen veya yakalanan ses, video veya görüntü dosyalarıdır.

Dijitalleştirilmiş imza (Digitized signature) | Elektronik olarak üretilen imzanın bir görüntüsüdür.

Dinamik Ana Bilgisayar Yapılandırma Protokolü (Dynamic Host Configuration Protocol - DHCP) | İstemci bilgisayarlara otomatik olarak yapılandırma ayrıntıları sağlamak için IP ağlarında kullanılan bir protokoldür.

Dizin bilgisi (Directory information) | Bir okuldaki tüm öğrenciler gibi, bir bilgisayar sisteminin kullanıcıları hakkında kamuya açık olan bilgilerdir.

Dizin gezme (Directory traversal) | Yetkilendirilmemiş bir dizinden komut yürütmeyi de içeren, bir web sunucusunun kök dizini dışındaki bir dosya dizinine erişme eylemidir.

DNS zehirlenmesi (DNS poisoning) | Bir DNS (bkz. Alan Adı Sistemi - Domain Name System) sunucusundaki verilerin sahte olduğu bir kullanım şeklidir, böylece DNS çözümleme sorgularına daha sonra gelen yanıtlar yanlıştır. DNS zehirlenmesi, ortadaki adam saldırılarına neden olabilir.

Doğum günü saldırıları (Birthday attacks) | Aynı sınıftaki iki öğrencinin (veya bir gruptaki herhangi kişilerin) şaşırtıcı derecede yüksek olasılıkla aynı doğum gününü

paylaşmalarından adını alan özet çarpışmalarla (*hash collisions*) (aynı anahtarla farklı metin) ilgili bir kriptografik saldırıdır.

Dosya Aktarım Protokolü (File Transfer Protocol - FTP) | Alındı bildirimli (*acknowledgement*) bağlantılı (*connection-oriented*) TCP iletimlerini kullanan güvenli olmayan bir dosya aktarımı uygulamasıdır.

Dosya virüsleri (File infector) | Öncelikle, çalıştırılabilir programları etkileyen bir virüs türüdür.

Döngü koruması (Loop protection) | Güvenlik duvarı kuralları, mesaj adreslerine bakmak ve sonsuz bir döngüye gönderilen mesajları reddetmek için yapılandırılmıştır.

Durağan ortamlar (Static environments) | Geliştirimden sonra çok fazla ya da hiç değişmeyen sistemlerdir.

Durum (State) | Ağ paketlerinin geçip geçmemesi konusunda karar vermek için güvenlik duvarları tarafından kullanılan bir ağ bağlantısının mevcut durumunu açıklayan bilgidir.

Durum denetimi güvenlik duvarı (Stateful inspection firewall) | Bir paketin nasıl işleneceğini belirlemek için bağlantının durumunu ve basit adres, port ve protokol kurallarını inceleyen bir güvenlik duvarıdır.

Duruma dayalı eşleme (Stateful matching) | Ağ trafiğini, trafiğin görünümüne ve diğer paketlerle olan ilişkisine dayanan kurallar veya imzalarla eşleme tekniğidir.

Dünya Çapında Ağ/World Wide Web (World Wide Web - WWW) | Birbirleriyle aralarında köprü olan ve İnternet kullanarak erişilen bir belgeler topluluğudur.

Dünya Çapında Ağ/World Wide Web Konsorsiyumu (World Wide Web Consortium - W3C) | 1994 yılında World Wide Web için standartlar geliştirmek ve yayınlamak için kurulmuş bir organizasyondur.

Düz metin (Plaintext) | Şifrelenmemiş bilgidir.

Düzeltici denetim (Corrective control) | Tehdidin etkisini azaltan veya hafifleten bir denetimdir.

E

Ele geçirme (Hijacking) | Saldırganın, iki makine arasındaki oturumun denetimini ele geçirdiği ve bunlardan biriymiş gibi davrandığı bir saldırı türüdür.

Elektrik ve Elektronik Mühendisleri Enstitüsü (Institute of Electrical and Electronics Engineers - IEEE) | Elektronik teknolojisi ile ilgili özellikleri ve standartları tanımlayan standartlar birimidir.

Elektronik olarak korunan sağlık bilgisi (Electronic protected health information - ePHI) | Bilgisayar tabanlı hasta sağlığı bilgisidir. Elektronik olarak depolanan PHI'dır.

Elektroteknoloji(Electrotechnology) | Uluslararası Elektroteknik Komisyonu (International Electrotechnical Commission - IEC) tarafından ele alınan ortak bilgi tabanıdır.

Eliptik Eğri DHE (Elliptic Curve DHE - ECDHE) | Anahtar üretmek için cebirsel eğriler kullanan bir asimetrik kriptografik anahtar değişim algoritmasıdır.

Eliptik eğri kriptografisi (Elliptic curve cryptography - ECC) | Eliptik eğrilerin yapısına dayanan bir açık anahtar kriptografik algoritmasıdır.

EMI kalkanı (EMI shielding) | Dış elektromanyetik parazitin (EMI) hassas elektronik ekipman üzerindeki etkisini azaltmak için manyetik veya iletken malzeme kullanma uygulamasıdır.

En düşük erişim hakkı/En az ayrıcalık (Least privilege) | Bir öznenin (bir kullanıcı, uygulama veya başka bir varlık olsun), geçerli fonksiyonları yerine getirmek için gereken en düşük hak seviyesine sahip olması gerektiği prensibidir.

Enjeksiyon tekniği (Injection technique) | Yazılım denetimlerini bozmak veya atlatmak için kasıtlı olarak geçersiz veriler girerek saldırılar yapmak için kullanılan bir tekniktir.

Ephemeral modunda Diffie-Hellman (Diffie-Hellman in ephemeral mode - DHE) | Anahtar üretmek için modüler aritmetik kullanan asimetrik kriptografik anahtar değişim algoritmasıdır.

Erişim denetim/kontrol (Access control) | Bir kaynağın, sadece onu kullanmasına izin verilenler tarafından kullanılması için korunması süreci; kaynaklara erişimi kısıtlamak veya izin vermek için kullanılan belirli bir yöntemdir.

Erişim denetim/kontrol listesi (Access control list - ACL) | Yetkilendirilmiş kullanıcı kimlikleri (ID) tablosu tutarak bir kaynağa erişimi kontrol etmek için bir uygulama tekniği; ayrıca yönlendiriciye/anahtar arabirimlerine (*router/switch interfaces*) gelen ya da yönlendiriciden/anahtar arabirimlerinden iletilen IP paketlerinin yönetilen IP trafik akışına geçişine izin vermek veya yasaklamak için de kullanılmaktadır.

Erişim denetim/kontrol politikası (Access control policy) | Yetkilendirilmiş kullanıcıların rollerine ve iş işlevlerine ve görevlerine göre kaynaklara nasıl erişebileceklerini tanımlayan bir organizasyon politikası tanımı. Bu politika, çalışanların ve yetkilendirilmiş yüklenicilerin erişimine nasıl izin verildiği ve erişimlerinin nasıl kaldırıldığı ile ilgili kuralları tanımlamaktadır.

Eşik (Threshold) | Normalden anormal davranışa doğru değişiklik gösteren bir değerdir. Başarısız oturum açma denemeleri durumunda, beş değerinde bir eşik, bir kullanıcı beş kez oturum açamadığında, eylemin olağan dışı olarak kabul edilmesi gerektiği anlamına gelir.

Ethernet (Ethernet) | Ethernet ağı için 10 Mbps'den 10 Gbps'ye kadar hızları destekleyen bir IEEE 802.3 CSMA/CD standardıdır.

Ethernet Üzerinden Fiber Kanal (Fibre Channel over Ethernet - FCoE) | Fiber kanal özellikli cihazları bir Ethernet ağına bağlamak için kullanılan bir protokoldür.

E-ticaret (E-commerce) | Güvenli bir web sitesi üzerinden çevrimiçi olarak kredi kartıyla ödeme veya çek hesabından otomatik ödeme ile mal ve hizmet alımı ve satımıdır.

Etik bilgisayar korsanı (Ethical hacker) | Güvenlik açıklarını ortaya çıkarmak veya gidermek için çeşitli penetrasyon test araçlarını kullanan bir bilgi güvenliği veya ağ uzmanıdır. Aynı zamanda beyaz şapka bilgisayar korsanı olarak da adlandırılır.

Etki (Impact) | Güvenlik zayıflığını kullanan bir tehdidin neden olabileceği zararın büyüklüğüdür.

Etkinlik (Event) | Bir bilgisayar veya ağ içinde gözlemlenebilir herhangi bir olaydır.

Eylemler (Actions) | Yetkilendirilmiş kullanıcıların BT varlıklarını, sistemlerini, uygulamalarını ve verilerini kullanarak gerçekleştirebilecekleri işlemlerdir.

F

Faaliyet aşaması denetimleri (Activity phase controls) | Teknik veya idari olabilen ve aşağıdaki gibi sınıflandırılmış olan güvenlik kontrolleri:

Tehdidin zayıflıkla buluşmasını önlemek için önleyici denetimler (*preventive controls*) mevcuttur.

Tehdidin sistemimize girdiğini tespit etmek için algılayıcı denetimler (*detective controls*) mevcuttur.

Ortaya çıkan tehdidin etkilerini hafifletmek veya azaltmak için düzeltici denetimler (*corrective controls*) mevcuttur.

Fark Analizi (Gap Analysis) | Mevcut güvenlik denetimlerinin ve tespit edilen tüm tehditlerin ele alınması için gereken denetimlerin karşılaştırılmasıdır.

Federal Bilgi Güvenliği Modernizasyon Kanunu 2014 (Federal Information Security Modernization Act 2014 - FISMA) | 2002 Federal Bilgi Güvenliği Yönetimi Kanunu'nun gereksinimlerini modern tehditler ve güvenlik uygulamaları ile güncel hale getirmek için onaylanan bir ABD federal yasasıdır.

Federal Bilgi Güvenliği Yönetim Kanunu 2002 (Federal Information Security Management Act 2002 - FISMA) | ABD devlet kurumlarının vatandaşların özel verilerini korumalarını ve uygun güvenlik kontrollerini yapmasını gerektiren bir ABD federal yasasıdır.

Federal Finansal Kuruluşlar İnceleme Konseyi (Federal Financial Institutions Examination Council - FFIEC) | "Finansal kurumların denetiminde tek biçimliliği ve tutarlılığı teşvik etmek için" var olan beş ABD düzenleyici kurumundan oluşan bir birlikteliktir. *Bkz. https://www.ffiec.gov/.*

Felaket kurtarma planı (Disaster recovery plan - DRP) | Büyük felaketlerin veya kesintilerin nasıl ele alınacağını ve kritik sistemlerin, uygulamaların ve verilerin nasıl kurtarılacağına yönelik yazılı bir plandır.

FICO (FICO) | Equifax, Experian ve TransUnion tüketici kredisi raporlama kuruluşları tarafından kullanılan, bilgi sağlayan halka açık bir şirkettir.

Fırsat maliyeti (Opportunity cost) | Bir şirketin, kasıtlı veya kasıtsız olarak, aksama süresi (*downtime*) nedeniyle kaybedeceği para miktarıdır. Aynı zamanda, bkz gerçek kesinti maliyeti (*true downtime cost*).

Fiber kanal (Fibre channel) | İlk olarak süper bilgisayarlarda depolama cihazlarını bağlamak için kullanılan bir depolama ağı protokolüdür.

Fidye Yazılımı (Ransomware) | Bir sistemi ele geçiren, dosyaları gizli anahtarla şifreleyen, fidye ödeyene kadar meşru kullanıcılar tarafından erişilemez hale getiren kötücül bilgisayar yazılımıdır.

Fikri mülkiyet (Intellectual property) | Bir işletmeye benzer sektörlerdeki benzer şirketlere kıyasla rekabet avantajı sağlayan özgün bilgidir.

Fiziksel erişim denetimi (Physical access control) | Binalar veya odalar gibi fiziksel kaynaklara erişimi düzenleyen bir mekanizmadır.

Fiziksel olarak kısıtlanmış kullanıcı arayüzü (Physically constrained user interface) | Yetkilendirilmemiş bilgi girmenin fiziksel bir yolunu sağlamayan bir kullanıcı arayüzüdür.

Flash çerezleri (Flash cookies) | Kullanıcı, çereze-benzer nesnelerden bilgisayarını temizlediğini düşündüğü halde, kullanıcının sistemine bu nesneleri yerleştirmek için Flash kullanan bir tür web uygulaması saldırısıdır. Yaygın olmayan kullanımda, yerel olarak paylaşılan nesne (*local shared object* - LSO) olarak da adlandırılmaktadır.

Frekans bozumu (Jamming) | Yasal kablosuz iletişimi bozmak ve engellemek için telsiz frekanslarını, kablosuz ağ erişim noktalarıyla aynı frekansta gönderme eylemidir.

Fuzzing (Fuzzing) | Beklenmeyen verileri nasıl işlediğini görmek için yazılıma rasgele girdi sağlamaktan oluşan bir yazılım test yöntemidir.

G

Geçici Anahtar Bütünlüğü Protokolü (Temporal Key Integrity Protocol - TKIP) | WPA'da ,WEP'in yerini almak için kullanılan bir şifreleme yöntemidir.

Geçici ayırma (Temporal isolation) | Kaynak erişimini belirli zaman aralıklarında kısıtlama yöntemidir. Geçici ayırmanın daha yaygın olarak günün belirli saati kısıtlamaları (*time of day restrictions*) olarak tanımlandığını görebilirsiniz.

Geçiş fonksiyonları (Transition functions) | Bir durumdan diğer duruma geçiştir.

Geçişli erişim (Transitive access) | İstenen hedef sisteme veya servise, ilk önce hedef tarafından güvenilen bir sistemin gizliliği ihlal edilerek, dolaylı olarak saldırmaktır.

Geçişli güven (Transitive trust) | Başlangıç oturum açma kimlik bilgilerinin, istek üzerine diğer güvenilir sunuculara iletildiği bir kimlik denetleme yöntemidir.

Genişletilebilir Kimlik Denetleme Protokolü (Extensible Authentication Protocol - EAP) | Anahtarların taşınmasını ve kimlik denetleme bilgilerini tanımlayan bir kimlik denetleme çerçevesidir. EAP, kablosuz ağ kimlik denetlemesinde yaygın olarak kullanılmaktadır.

Gerçek kesinti maliyeti (True downtime cost) | *Bkz. Fırsat maliyeti (opportunity cost).*

Gerçek zamanlı iletişimler (Real-time communications) | Mesajların doğrudan alıcıya hemen (gerçek zamanlı olarak) gönderildiği bir iletişim yöntemidir.

Gerçek zamanlı izleme (Real-time monitoring) | Faaliyetin gerçekleşirken analizidir.

Gizli anlaşma (Collusion) | Bir güvenlik politikasını ihlal etmek için birlikte çalışan iki veya daha fazla kişidir.

Gizli engelleme (Implicit deny) | Açıkça izin verdiğiniz durumlar dışındaki tüm mesajları reddedecek güvenlik duvarı yapılandırmasıdır.

Gizli eylem (Covert act) | Gizlilik içinde yürütülen bir eylemdir.

Gizli kanallar (Covert channels) | Bunlar kurumsal politikaya karşı bilgi aktarmanın gizli yollarıdır.

Gizli virüs (Stealth virus) | Kullanıcıdan veya tespit etme yazılımından kendisini gizlemek için bazı teknikler kullanan bir virüs türüdür.

Gizlice anlaşmak (Colluding) | Siber saldırı planlayan birden çok saldırganın eylemidir; diğerleri ise özellikle yasa dışı veya yetkilendirilmemiş bir şey yapmak için gizlice çalışırlar.

Gizlilik (Confidentiality) Bilgilerin mahrem ya da gizli tutulması gereksinimidir.

Görevlerin ayrılığı (Separation of duties) | Bir görevi, her birini genel görevin sadece bir bölümünü yürütmesine izin verilen farklı insanlar tarafından gerçekleştirilen bir dizi özgün faaliyete bölme işlemidir.

Görünüm tabanlı erişim denetim (View-based access control - VBAC) | Kullanıcıların doğrudan veritabanı tablolarındaki verilere erişmesine izin vermek yerine, kullanıcıların veritabanı görünümlerine (*view*) erişimi kısıtlamaktır.

Gramm-Leach-Bliley Kanunu (Gramm-Leach-Bliley Act - GLBA) | Bankacılık ve finans kurumlarının müşterilerinin özel verilerini koruması ve uygun güvenlik denetimlerine sahip olmasını gerektiren bir ABD federal kanunudur.

Gri kutu testi (Gray-box testing) | Bir uygulamanın tasarımının sınırlı bilgisini temel alan güvenlik testidir.

Gri şapka bilgisayar korsanı (Gray-hat hacker) | Bir gün siyah şapkalı bir bilgisayar korsanı haline gelebilecek ortalama yeteneklere sahip bir bilgisayar saldırganıdır. Aynı zamanda özenti (*wannabe*) olarak da adlandırılmaktadır.

Grup Politikası (Group Policy) | Windows'un çalışma şeklini düzenleyen merkezi bir kurallar kümesidir.

Grup Politikası Nesnesi (Group Policy Object - GPO) | Grup Politikası ayarları topluluğunu içeren adlandırılmış bir nesnedir.

Grup üyelik politikası (Group membership policy) | Kaynaklara erişimin hangi grupta/gruplarda olduğunuza göre belirlendiği bir yetkilendirme yöntemidir.

Günün belirli saati kısıtlamaları (Time of day restrictions) | *Bkz. Geçici ayırma (Temporal isolation).*

Güvenli Soketler Katmanı Sanal Özel Ağ (Secure Sockets Layer virtual private network - SSLVPN) | Güvenli bir web sitesine uzaktan erişim sağlamanın bir yoludur. Başka bir deyişle, Güvenli Soketler Katmanı (Secure Sockets Layer) üzerinde çalışan ve güvenli bir tarayıcı bağlantısı üzerinden iletişimi güvenli bir web sunucusuna şifreleyen bir VPN'dir.

Güçlendirilmiş yapılandırma (Hardened configuration) | Gereksiz servislerini kapattığınız veya devre dışı bıraktığınız, hala çalışmakta olanlarını ise koruduğunuz bir bilgisayarın veya cihazın durumudur.

Güçlendirme (Hardening) | Bilgisayarları ve cihazları mümkün olduğu kadar güvenli hale getirmek için donanım ve yazılım yapılandırmalarını değiştirme işlemidir.

Günlük dosyaları (Log files) | Sisteme kimin giriş yaptığı, ne zaman giriş yaptığı ve hangi bilgilere veya kaynaklara erişildiği gibi ayrıntıları sağlayan günlük kayıtlarıdır.

Günlük kaydı analizi (Log analysis) | Keşif eylemini ve hatta daha önce gerçekleşmiş olan saldırıları tanımlamak için güvenlik duvarı ve diğer ağ cihazı günlük dosyalarını inceleme işlemidir.

Güven (Trust) | Başkalarının sizin yararınıza davranacağı ya da bir kaynağın gerçek olduğu beklentisine olan güvendir. Bilgisayar ağlarında güven, diğer kullanıcıların kuruluşun güvenlik kurallarına göre hareket edeceği ve ağın ve kaynaklarının kararlılığını, gizliliğini veya bütünlüğünü ihlal etme girişiminde bulunmadığına olan güvendir.

Güvenilir işletim sistemleri (Trusted operating systems - TOS) | Son derece hassas bilgileri işleyen sistemlerin ek güvenlik gereksinimlerini karşılamak için ek denetimler içeren bir işletim sistemi türüdür.

Güvenli Hiper Metin Aktarım Protokolü (HTTPS) | Çevrimiçi bankacılık web siteleri gibi güvenli web sayfalarına bilgi giren kullanıcıların veri girişinde güvenliği sağlayan HTTP ve SSL/TLS şifreleme kombinasyonudur.

Güvenli Kabuk (Secure Shell - SSH) | Uzak sunuculara güvenli oturum açma başlatmak için yaygın olarak kullanılan protokoldür.

Güvenli LDAP (Secure LDAP) | Ağda paylaşılan tüm mesajlar için SSL/TLS kullanan bir LDAP sürümüdür.

Güvenli Özet Algoritması (Secure Hash Algorithm - SHA) | ABD Ulusal Güvenlik Ajansı tarafından geliştirilen bir dizi kriptografik özet fonksiyonudur.

Güvenli yönlendirici yapılandırması (Secure router configuration) | Yönlendiricinizin sadece geçerli düğümlerden (*nodes*) ve geçerli düğümlere akan geçerli ağ trafiğine izin verdiğini garantileyen ayarların bir topluluğudur.

Güvenlik (Security) | Bir şeyi risklerden, tehditlerden veya güvenlik açıklarından korumak için kullanılan, politika, prosedür ve kapı gibi fiziksel bir denetimdir.

Güvenlik açığı (Security gap) | Yürürlükteki güvenlik denetimleri ile tüm güvenlik açıklarını gidermek için gereken denetimler arasındaki farktır.

Güvenlik açığı tarayıcısı (Vulnerability scanner) | Hedef bilgisayarda veya ağda var olan bilinen tüm zayıflıklar hakkında bilgi toplayan bir yazılım aracıdır.

Güvenlik açığı/Zafiyet (Vulnerability) | Bir tehdidin gerçekleşmesine veya bir varlık üzerinde bir etkiye sahip olmasına izin veren bir zayıflıktır.

Güvenlik açığı/Zafiyet testi (Vulnerability testing) | Bir sistemdeki zayıflıkları bulma ve hangi yerlerin saldırı noktası olabileceğini belirleme sürecidir.

Güvenlik Bildirim Biçimlendirme Dili (Security Assertion Markup Language - SAML) | Hem kimlik denetleme hem de yetkilendirme verilerinin değiş-tokuşu için kullanılan açık bir XML standardıdır.

Güvenlik Bilgi ve Olay Yönetim (SIEM) Sistemi (Security Information and Event Management (SIEM) system - SIEM) | Günlük dosyalarının içeriğinin toplanmasına, saklanmasına ve analiz edilmesine yardımcı olan yazılım ve cihazlardır.

Güvenlik birliği (Security association - SA) | ISAKMP anahtar yönetiminin temel unsurudur. SA, çeşitli ağ güvenliği hizmetlerini gerçekleştirmek için gereken tüm bilgileri içerir.

Güvenlik çekirdeği (Security kernel) | Bilgisayar sistemlerinin erişim denetimini uygulayan bir bilgisayar ortamının donanım, yazılım ve belleniminin (*firmware*) merkezi kısmıdır.

Güvenlik çekirdeği veritabanı (Security kernel database) | Bireysel kullanıcıların erişim haklarını belirleyen kurallardan oluşan bir veritabanıdır.

Güvenlik Duvarı (Firewall) | Üzerinden geçen ağ trafiğini denetleyen ve yapılandırmada belirlediğiniz bir dizi kurala dayanarak bu trafiğe izin veren veya izin vermeyen bir program veya özel donanım cihazıdır.

Güvenlik duvarı kuralları (Firewall rules) | Güvenlik uzmanının güvenlik gereksinimlerini gerçekleştirmesini sağlamak için güvenlik duvarının yapılandırmasında tanımlanan filtrelerdir.

Güvenlik farkındalığı eğitimi (Security awareness training) | Güvenlik politikaları, tehditler ve dijital varlıkların yönetilmesi ile ilgili eğitimdir.

Güvenlik farkındalığı kampanyası (Security awareness campaign) | Kullanıcıların bilgi güvenliği konusundaki anlayışını ve kaygılarını arttırmayı hedefleyen özel eğitimdir.

Güvenlik ihlali (Security breach) | CIA güvenlik ilkelerinin ihlal edilmesine neden olan herhangi bir olaydır.

Güvenlik kontrolü (Security control) | Bir kuruluşun riski azaltmasına yardımcı olmak için gerçekleştirdiği eylemdir.

Güvenlik olay müdahale ekibi (Security incident response team - SIRT) | Güvenlik olaylarını tanımlamak ve bunlara müdahale etmek için örgütlenmiş insan ekipleridir. SIRT, olayların etkisini en aza indirmek ve olayı analiz etmek için gerekli kanıtları toplamaktan sorumludur.

Güvenlik politikası (Security policy) | Bir kuruluşun tesislerini ve BT altyapısını nasıl koruduğunu belirleyen bir dizi politikadır. Aynı zamanda, kuruluşun mevzuat gereksinimlerini nasıl karşıladığını da ele alabilir.

Güvenlik yönetimi (Security administration) | Bir kuruluşun güvenlik planını planlamaktan, tasarlamaktan, uygulamaktan ve izlemekten sorumlu bireyler grubudur.

H

Hafif Genişletilebilir Kimlik Denetleme Protokolü (Lightweight Extensible Authentication Protocol - LEAP) | Kablosuz anahtarları ve kimlik denetlemesini yönetmeye yardımcı olmak için Cisco sistemleri tarafından geliştirilmiş olan kablosuz kimlik denetleme çerçevesidir. LEAP, güvenli bağlantılar kurmak için WEP veya TKIP kullanabilir.

Hafifletilmiş Dizin Erişim Protokolü (Lightweight Directory Access Protocol - LDAP) | Ağ tabanlı kimlik denetleme için bir dizin servisidir. LDAP iletişimi şifrelenebilir.

Halka açık şirketler (Publicly traded companies) | Bir dizi farklı yatırımcının sahibi olduğu, hisselerinin paylaşıldığı şirketler.

Hata toleransı (Fault tolerance) | Bir tür hataya veya yanlışlıkla karşılaşma ve yine de kritik işlemleri destekleyebilmektir.

Hedef odaklı oltalama (Spear phishing) | Gizli verilere yetkilendirilmemiş erişim arayan, belirli bir organizasyonu hedef alan bir e-posta veya anlık mesaj aldatma sahtekarlığı girişimidir.

Hiper Metin Aktarım Protokolü (Hypertext Transfer Protocol - HTTP) | Kullanıcıların web sayfaları ve tarayıcılar aracılığıyla içeriğe erişmelerini ve iletişimlerini sağlayan bir uygulama katmanı protokolüdür.

Hizmet bürosu (Service bureau) | Küçük müşterilere dış kaynaklı toptan satış hizmeti sunmak için yeterli kapasiteye sahip bir servis sağlayıcıdır.

Hizmet dışı kalma/Aksama Süresi (Downtime) | Bir BT sisteminin, uygulamanın veya verinin kullanıcılar tarafından kullanılamadığı süredir.

Hizmet olarak Her Şey (Anything as a Service - AaaS) | Genellikle bulut altyapısı içinde üçüncü taraf bir sağlayıcı tarafından barındırılan bir çözüm sunan yeni bir teknolojidir. Bir bulut altyapısı içinde barındırılarak, birden-çoğa (*one-to-many*) bir dağıtım çözümü desteklenebilmektedir. Bu tür bir dağıtım çözümü, müşterinin teknoloji, donanım veya yazılım çözümünün kullanımı için aylık bir ücret ödediği yinelenen bir gelir modeline izin vermektedir.

Hizmet Olarak Yazılım (Software as a Service - SaaS) | Müşterilerin talep üzerine uygulama kullandığı bir yazılım dağıtım veya servis modelidir.

Hizmet reddi (Denial of service - DoS) | Ping veya ICMP yankı-isteği (*echo-request*), bir sunucunun veya sistemin kullanılabilirliğini azaltmak için yankı-yanıtlama (*echo-reply*) mesajları kullanan bir saldırıdır. DoS saldırıları genellikle tek bir ana cihazdan kaynaklanır.

HMAC tabanlı tek kullanımlık parola (HMAC-based one-time password - HOTP) | Bir kimlik denetleme sunucusu kullanarak bir mobil cihaz kullanıcısının kimliğini denetlemek için çok güvenli bir yöntem sağlayan bir algoritmadır.

Hub (Hub) | Gelen tüm trafiği diğer tüm bağlantı noktalarına göndererek ağ bölümlerini bağlayan bir ağ cihazıdır.

I - İ

ICMP yankı isteği (ICMP echo request) | Ping yanıtı bekleyen bir ping isteği gönderen bir Internet Protokolü (IP) iletişim mekanizmasıdır.

IEEE 802.3 CSMA/CD (IEEE 802.3 CSMA/CD) | Birden çok bilgisayarın aynı kablolamayı kullanarak iletişim kurmasına olanak veren yerel alan ağı için bir IEEE standardıdır. Bu aynı zamanda Ethernet olarak da bilinmektedir.

IP adresi (IP address) | Bir ağdaki bir bilgisayar gibi bir cihazı benzersiz şekilde tanımlayan 32 bit (IPv4) veya 128 bit (IPv6) bir numaradır.

IP durum denetlemeli güvenlik duvarı (IP stateful firewall) | Engelleme veya iletme kararları almak için paket içindeki IP, TCP ve UDP katmanlarını inceleyen bir cihazdır. Güvenlik duvarları, ağların birbirine bağlandığı giriş/çıkış noktalarına yerleştirilir.

IP Üzerinden Ses (Voice over IP - VoIP) | IP ağları üzerinden sesli iletişim ve oturumlar sunmak için bir iletişim protokolleri ve teknolojileri topluluğudur.

IP varsayılan ağ geçidi yönlendiricisi (IP default gateway router) | LAN'ınızın giriş/çıkış cihazı olarak işlev gören yönlendirici arayüzünün IP adresidir.

IPv4 adresleri (IPv4 addresses) | Ağdaki her cihazı benzersiz şekilde tanımlayan dört byte'lık (32 bit) adreslerdir.

ISO / IEC 27002 | ISO 17799 standardına yapılan bir güncellemedir.

ISO 17799 | Bilgi sisteminin en iyi uygulamalarını temsil eden kapsamlı bir denetim setini belgeleyen uluslararası bir güvenlik standardıdır.

ITU Telekomünikasyon Sektörü (ITU Telecommunication Sector - ITU-T) | ITU komitesi, tüm uluslar için telekomünikasyon alanlarını kapsayan standartların verimli ve etkili bir şekilde üretilmesini sağlamaktan sorumludur.

IV saldırı (IV attack) | İletimdeki şifreli bir IP paketinin başlangıç vektörünü (*initialization vector*), zaman içinde ortak bir şifreleme anahtarının şifresini çözme umuduyla değiştiren bir kablosuz ağ saldırısıdır.

İçerideki tehdit (Insider threat) | Kuruluş içinde güvenilen bir çalışan, yüklenici veya kişiden kaynaklanan tehlikedir.

İçerik denetimi (Content inspection) | Paketin, IP durum denetlemeli güvenlik duvarından (*IP stateful firewall*) geçmesine izin verilip verilmeyeceğini belirlemek için bir IP paketinin içine bakmaktır.

İçerik filtreleme (Content filtering) | Etki alanı (*domain*) adı ve URL aramalarındaki belirli anahtar kelimelerin veya kelime öbeklerinin engellenmesidir. Web içerik filtreleme etkin durumdayken belirli URL'lere ve etki alanı adlarına erişilemez.

İki adımlı kimlik denetleme (Two-step authentication) | Bkz. İki faktörlü kimlik denetleme (*Two-factor authentication*)

İki faktörlü kimlik denetleme (Two-factor authentication) | İki tür kimlik denetleme bilgisi kullanan bir kimlik denetleme yöntemidir. Ayrıca bkz. İki *adımlı kimlik denetleme (two-step authentication)*.

İletim Denetimi Protokolü/İnternet Protokolü (Transmission Control Protocol/Internet Protocol - TCP/IP) | OSI Referans Modelinin hem Ağ hem de Aktarım Katmanında çalışan popüler bir protokol takımıdır. TCP/IP, Internet üzerindeki, çoğu şirket ve ev ağındaki tüm etkinlikleri yönetir.

İlişkiler (Relationships) | Kullanıcılar ve kaynaklar arasında mevcut olan isteğe bağlı koşullardır. Bunlar okuma, yazma ve yürütme gibi yetkilendirilmiş bir kullanıcıya verilen izinlerdir.

İnce istemci (Thin client) | Sadece kullanıcı G/Ç (I/O) işlevselliğini işleyen ve çoğu iş mantığı (veri işleme), veri depolama ve veri erişimi işlemlerini gerçekleştirmek için sunuculara bağlı olan istemci yazılımıdır.

İnkâr edememe (Nonrepudiation) | Bir partinin önceki bir ifadeyi veya eylemi reddetmesini önler.

İnternet (Internet) | Yaklaşık 2 milyar kullanıcıyı birbirine bağlamak için TCP/IP protokol ailesini ve uygulamalarını kullanan küresel bir bilgisayar ağları ağıdır.

İnternet Kontrol Mesajı Protokolü (Internet Control Message Protocol - ICMP) | IP ağları için bir yönetim protokolüdür.

İnternet Küçük Bilgisayar Sistem Arayüzü (Internet Small Computer System Interface - iSCSI) | Veri

depolama cihazlarını IP ağlarına bağlamak için kullanılan bir depolama ağı protokolüdür.

İnternet Mimarisi Kurulu (Internet Architecture Board - IAB) IETF'in, İnternet'in genel iyiliği konusunda teknik ilgisi olan bağımsız araştırmacılardan ve uzmanlardan oluşan bir alt komitesidir.

İnternet Mühendisliği Görev Gücü (Internet Engineering Task Force - IETF) | İnternet standartlarını geliştiren ve destekleyen bir standartlar organizasyonudur.

İnternet Protokol Güvenliği (Internet Protocol Security - IPsec) | IP ağları kullanarak siteleri güvenli bir şekilde bağlamak için tasarlanmış bir protokol setidir.

İptal etme (Revocation) | Verilere erişim için yetkilendirmenin durdurulmasıdır.

İsteğe bağlı erişim denetim (Discretionary access control - DAC) | Nesnelere erişimi, nesnelerin ve/veya ait oldukları grupların kimliğini temel alarak kısıtlamanın bir yoludur.

İsteğe bağlı kod yürütme (Arbitrary code execution) | Bir bilgisayar korsanının gizliliği ihlal edilmiş bir sistemde yetkilendirilmemiş komut satırı fonksiyonları çalıştırmasına izin veren bir istismardır. Arabellek taşması saldırıları ve SQL enjeksiyon saldırıları genellikle isteğe bağlı kod yürütülmesine izin verebilir.

İstemci-tarafı saldırısı (Client-side attack) | Kötü niyetli bir sunucuya veya uygulamaya bağlanan kullanıcının iş istasyonundan yapılan saldırılardır.

İstismar yazılımı (Exploit software) | Bir bilgisayar sistemindeki veya IP ana bilgisayar cihazındaki bir zayıflığı "istismar" etmek için bilinen yazılım güvenlik açıklarını, verileri ve betik dosyası komutlarını içeren bir uygulamadır.

İş etki analizi (Business impact analysis - BIA) | İş operasyonlarını ve işlevlerini ve bunlarla ilişkili olan BT sistemlerini, uygulamalarını ve verilerini ve bir hizmet kesintisi veya hizmet dışı kalma süresinin etkisini önceliklendiren bir iş sürekliliği planı için bir ön koşul analizidir.

İş görevi analizi (Job task analysis) | İş görevlerinin ve sorumluluklarının belirli bir rolle nasıl uyumlu olduğu araştırmasıdır.

İş İstasyonu (Workstation) | Bir masaüstü bilgisayar, bir dizüstü bilgisayar, özel amaçlı bir terminal veya ağınıza bağlanan başka bir cihazdır.

İş ortakları (Business associates) | HIPAA kapsamında, kapsanan bir varlık adına PHI'ya veya ePHI'ya erişim gerekli olduğunda bir sağlık hizmeti faaliyeti gerçekleştiren kuruluşlardır.

İş rotasyonu (Job rotation) | Çalışanları farklı sistemler veya görevler arasında döndürerek riski en aza indiren bir stratejidir.

İş sürekliliği planı (Business continuity plan - BCP) | İş operasyonlarını sürdürmek için BT sistemlerine, uygulamalarına ve veri erişimine yönelik hizmet kesintilerini nasıl ele alacağınızla ilgili bir plandır.

İş sürücüleri (Business drivers) | İş hedeflerini destekleyen insanları, bilgiyi, finansları ve performans hedeflerini içermektedir.

İşbirliği (Collaboration) | WebEx gibi ekip üyeleri veya meslektaşları ile gerçek zamanlı tartışmalar için sesli konferans ve belgelerin (metin, elektronik tablolar, sunumlar, vb.) paylaşılmasını destekleyen yazılım tabanlı bir uygulamadır.

İşe alım (Onboarding) | Birlikte çalışabilirlik ilişkilerini kurarken, tüm tarafların hedeflerini ve beklentilerini net bir şekilde sağlayan bir süreçtir.

İşletim sistemi (Operating system - OS) parmak izi tarayıcısı (fingerprint scanner) | TCP/UDP paket cevaplarındaki küçük değişiklikleri temel alan işletim sistemlerini ayırt etmek için tasarlanmış bir yazılım programıdır.

İşletim sistemi parmak izi (Operating system fingerprinting) | Bir saldırganın, bilgisayarda hangi işletim sisteminin ve sürümünün çalıştığını öğrenmek için bağlantı noktası eşlemesini kullanmasını sağlayan keşif tekniğidir.

İşletmeden-işletmeye (Business-to-business - B2B) | Genellikle entegre tedarik zinciri alımları ve teslimatları için, işletmeden-işletmeye işlemler yapmak için bağlantıları olan çevrimiçi sistemler oluşturan bir işletmeyi tanımlamak için kullanılan bir terimdir.

İşletmeden-müşteriye (Business-to-consumer - B2C) | Müşterilerin doğrudan mal ve hizmet satın almaları için çevrimiçi bir mağaza tanımlamada kullanılan bir terimdir. *http://www.amazon.com* B2C sitesine bir örnektir.

İşlevsel denetim (Operational control) | Operasyonel personelin, fiziksel güvenlik ve olaya müdahale gibi uygulayabileceği ve yönetebileceği bir denetimdir.

İşlevsel politika (Functional policy) | Bir kuruluşun e-posta, uzaktan erişim ve İnternet'te gezinme gibi belirli işlevsel alanlardaki güvenliği için kuruluşun yönetim yönergesini belirten bir açıklamadır.

İşten çıkarma (Offboarding) | Verilerin ve diğer varlıkların denetiminin nasıl aktarılacağını, iletişimlerin nasıl sonlandırılacağını ve açık işlemlerin nasıl tamamlanacağını tanımlayan birlikte çalışabilirlik ilişkilerini sonlandırırken bir işlemdir.

İyileştirme (Remediation) | Bir BT altyapısında tanımlanmış veya bulunan bilinen bir riski, tehdidi veya güvenlik açığını düzeltme eylemidir.

İzinsiz sızma testi (Intrusive penetration testing) | Bir bilgisayar korsanının bir bilgisayar sistemine veya IP ana bilgisayar cihazına girmek için yaptığı test; izinsiz test kötü niyetli ağ trafiği oluşturur.

İzleme (Accounting) | Bilgi sistemlerine ve uygulamalarına erişim kontrollerini izlerken denetleme geçmişlerinin (*audit trails*) ve log dosyalarındaki olayların kayıt işlemidir.

İzlenebilirlik (Accountability) | Rolleri, sorumlulukları ve kilit BT güvenlik çalışanlarının ve olay müdahale ekibi üyelerinin yapmaları gerekenleri tanımlamaktır.

K

Kablolu Eş değer Mahremiyet (Wired Equivalent Privacy - WEP) | Kablosuz ağlar için eski şifrelemedir. WEP zayıftır ve çoğu trafik için yeterli koruma sağlamaz.

Kablosuz Bağlantı (Wireless Fidelity - Wi-Fi) | Kablosuz üreticiler arasında kablosuz LAN standartlarıyla uyumlu, sertifikalı ürünleri markalamak için bir anlaşmadır. Bir Wi-Fi bağlantı noktası (*hotspot*) kablosuz bir LAN erişim konumudur.

Kablosuz erişim noktası (Wireless access point - WAP) | Kablosuz LAN teknolojisi üzerinden IP iletişimini alan ve ileten bir radyo alıcı-verici aygıtıdır.

Kablosuz LAN (Wireless LAN - WLAN) | Bilgisayarları ve cihazları bağlamak için kablolar veya teller yerine telsiz iletimlerini kullanan bir LAN'dır.

Kabul edilebilir kullanım politikası (Acceptable use policy - AUP) | BT varlıklarının çalışanlar ve yetkilendirilmiş yükleniciler (*contractor*) tarafından kullanılmasına ilişkin neye izin verildiğini ve neyin yasaklandığını tanımlayan kurum çapında bir politikadır.

Kalın istemci (Thick client) | Kullanıcı G/Ç (I/O) ve çoğu iş mantığını (veri işleme) yöneten, yalnızca veri depolama ve veri erişimi için sunucuyu kullanan istemci yazılımıdır.

Kamusal (asimetrik) anahtar (Public (asymmetric) key) | Paylaşılabilen ve gizli tutulması gerekmeyen bir şifreleme anahtarıdır.

Kamusal anahtar kriptgrafisi (Public key cryptography) | Matematiksel olarak ilişkili iki anahtar kullanan kriptografik algoritmadır - verileri şifrelemek için bir anahtar ve verilerin şifresini çözmek için bir anahtar.

Kamuya açık olmayan kişisel bilgi (Nonpublic personal information - NPI) | Bir tüketicinin bir finansal kuruma sağladığı kişisel olarak tanımlanabilir herhangi bir finansal bilgidir. Bu terim, Gram-Leach-Bliley Yasası ile tanımlanır.

Kapsanan varlık (Covered entity) | Sağlık planları, sağlık kurumları ve belirli türden sağlık bilgilerini elektronik biçimde aktaran herhangi bir sağlık kuruluşu.dur Bu kuruluşlar HIPAA Güvenlik ve Gizlilik Kurallarına uymak zorundadır.

Karakteristik (Characteristic) | Kimlik denetlemede, parmak izi veya imza gibi benzersiz bir fiziksel özellik veya yüz ifadesi biçimidir. Bu niteliklere genellikle "olduğunuz şey" denir.

Kara-kutu testi (Black-box testing) Bir programın mimari bilgisine doğrudan temel almayan bir güvenlik testi yöntemidir.

Karaliste (Blacklisting) Bilinen tüm tehlikeli web sitelerinin veya hedef IP adreslerinin bir listesini tutma eylemidir. Kara listedeki bir siteden veya bu hedef IP adresinden gelen herhangi bir mesaj silinir.

Karışık mod (Promiscuous mode) | Yoklayıcıların (*sniffer*) çalıştığı mod'dur; kesintisizdir ve ağ trafiği oluşturmaz. Bu, her veri paketinin yakalandığı ve yoklayıcı tarafından görülebileceği anlamına gelir.

Karşılaştırmalı değerlendirme (Benchmark) | Bilgisayarınızın veya cihazınızın güvenli bir şekilde yapılandırılıp yapılandırılmadığını belirlemek için karşılaştırıldığı standarttır.

Karşılıklı yardım (Mutual aid) | Felaket ihtiyaç anında BT işlemlerini yeniden konumlandırarak birbirlerine yardım edebilecek kuruluşlar arasında bir anlaşmadır.

Kart sahibi verileri (Cardholder data) | Bir kredi kartında, 16 haneli kredi kartı numarası, kart sahibinin adı, son kullanma tarihi ve kredi kartının arkasındaki 3 basamaklı güvenlik kodudur.

Katman 2 anahtarı (Layer 2 switch) | Nereye gönderileceğini belirlemek için bir IP paketinin MAC katman adresini inceleyen bir ağ anahtarıdır. Katman 2 anahtarı, genellikle 10/100/1000 veya 10 Gbps Ethernet hızlarında korumasız bükümlü çift kablolama (*unshielded twisted pair*) üzerinden LAN bağlantısını destekler.

Katman 3 anahtarı (Layer 3 switch) | Nereye yönlendirileceğini belirlemek için Ethernet çerçevesinin ağ katmanı adresini inceleyen bir ağ anahtarıdır. Katman 3 anahtarı, genellikle 10/100/1000 veya 10 Gbps Ethernet hızlarında korumasız bükümlü çift kablolama (*unshielded twisted pair*) üzerinden LAN bağlantısını destekler ve yönlendirici ile aynıdır.

Kayıp beklentisi (Loss expectancy) | Bir BT varlık hatası nedeniyle kaybedilen para miktarıdır.

Kaynaklar (Resources) | Bilgisayar sistemindeki dosyalar, bilgisayarlar veya yazıcılar gibi korunan nesnelerdir.

Kendi Cihazını Getir (Bring Your Own Device - BYOD) | Çalışanların, yüklenicilerin (*contractors*) ve diğerlerinin kendi kişisel ekipmanlarını şirket ağına bağlamasına izin veren veya hatta teşvik eden bir organizasyon politikasıdır; bu, maliyet tasarrufu sağlar ancak uygun güvenlik kontrolleri, politikaları ve prosedürleri gerektirmektedir.

Kesintisiz şifreleme (Stream cipher) | Bir seferde tek bir byte (veya bit) şifreleyen kriptografik şifrelemedir.

Keşif (Reconnaissance) | Bilgi toplama sürecidir.

Kılavuz (Guideline) | Bir ürün veya sistemi nasıl kullanacağınız veya nasıl satın alacağınızla ilgili bir öneridir.

Kırpma seviyesi (Clipping level) | Güvenlik izlemesinde kullanılan, güvenlik operasyon personeline belirtilen bir değerin altına düşen faaliyetleri görmezden gelmesini belirten bir değerdir.

Kısıtlandırılmış kullanıcı arayüzü (Constrained user interface) | Kullanıcıların yalnızca belirli bilgileri girmesini ve yalnızca belirli eylemleri gerçekleştirmesini sağlayan yazılımdır.

Kimlik bilgisi yönetimi (Credential management) | Sisteme giriş kimlikleri (ID) ve parolalar gibi erişim denetimleriyle ilgili bilgileri toplamak, yönetmek ve kullanmak için bir sistemdir.

Kimlik denetleme (Authentication) | İddia ettiğiniz kişi ya da varlık olduğunuzu kanıtlama işlemidir.

Kimlik denetleme, yetkilendirme, ve izleme (Authentication, authorization, and accounting – AAA) | Ağ kaynakları için erişim denetimini standartlaştırmaya yardımcı olmak için bir veya daha fazla merkezi sunucu tarafından sağlanan temel hizmetlerdir.

Kimlik hırsızlığı (Identity theft) | Yeni hesaplar açmak, alışveriş yapmak veya sahtekarlık yapmak amacıyla kişisel olarak tanımlanabilir bilgileri çalma eylemidir.

Kimlik tabanlı şifreleme (Identity-based encryption - IBE) | Anahtar türetmek için gönderenin kimliğini kullanmaktadır.

Kimlik tanımlama (Identification) | Belirli bir kişi veya varlık olduğunu iddia etmek için kimlik bilgileri sağlama sürecidir.

Kimliksizleştirilmiş veri (De-identified data) | Bir birey hakkında, belirli bir bireyin kimliğiyle (örneğin, ad, adres, doğum tarihi vb.) ilişkilendirilebilecek hiçbir bilgi içermeyen verilerdir.

Kişisel dijital yardımcı (Personal digital assistant - PDA) | Cep telefonunu, İnternet taramasını ve e-postayı destekleyen bir mobil bilgisayar cihazı olarak işlev gören elle taşınabilir bir cihazdır.

Kişisel kimlik numarası (Personal identification number - PIN) | Bir kullanıcının kimliğini denetlemek için kullanılan, genellikle iki faktörlü kimlik denetleme şemasının bir parçası olarak kullanılan sayısal bir paroladır.

Kişisel tanımlayıcı bilgiler (Personally identifiable information - PII) | Bir kişiyi şahsen tanımlamak için kullanılabilecek verilerdir. Örnekler, Sosyal Güvenlik numaralarını, ehliyet numaralarını, finansal hesap verilerini ve sağlık verilerini içermektedir.

Kod kırıcılar (Cracker) | Çok yönlü becerilere sahip ve finansal kazançla ilgilenebilen düşman niyeti olan bir bilgisayar saldırganıdır.

Koklama (Sniffing) | Veri iletişimlerinin fiziksel olarak engellenmesidir; ortam dinleme (*eavesdropping*).

Koklayıcı (Sniffer) | Bkz. Paket yoklayıcı (*packet sniffer*).

Komut dosyası çocuğu (Script kiddie) | Bir saldırı yapmak için gerçekleştirilen adımların anlamını tam olarak anlamadan talimatları izleyen az veya hiçbir becerisi olmayan bir kişidir.

Komut enjeksiyonu (Command injection) | Dizin gezmeye (*directory traversal*) bakınız.

Konsorsiyum anlaşması (Consortium agreement) | Bir grubun üyelerinin birbirleriyle nasıl etkileşim içinde olacağının yasal tanımıdır.

Kontrol listesi testi (Checklist test) | Belirtilen numaraların güncel olduğundan ve planın şirketin önceliklerini ve yapısını yansıttığından emin olmak için planın yöneticiler ve iş sürekliliği ekibi tarafından yapılan basit bir incelemesidir.

Korumalı Genişletilebilir Kimlik Denetleme Protokolü (Protected Extensible Authentication Protocol - PEAP) | Bir TLS tünelinde çalışan bir kimlik denetleme çerçevesisir. PEAP, kimlik denetleme değişimleri için EAP'tan daha fazla güvenlik sağlar.

Korunan sağlık bilgisi (Protected health information - PHI) | Bir kişinin geçmişi, bugünü veya geleceğiyle sağlığı hakkında bireysel olarak tanımlanabilir bilgilerdir. Zihinsel ve fiziksel sağlık verilerini içerir.

Korunma (Safeguard) | Bir sistemde yapısal (*built-in*) olarak bulunan veya istismara yol açabilecek açıklıkları ya da zayıflıkları denetimlerde adreslemek için kullanılan bir şeydir.

Kötü amaçlı yazılım (Malware) | *Bkz. Kötücül yazılım.*

Kötü ikiz (Evil twin) | Bir saldırgan, bir kullanıcı kendisine bağlandığında tüm IP paketlerini dinlemek ve yakalamak için sahte bir açık veya genel kablosuz ağ oluşturduğu kablosuz ağ saldırısının bir biçimidir.

Kötücül eklentiler (Malicious add-ons) | Yasal programlar veya yazılım uygulamalarında, ek kötücül yazılımlar çalıştıran yazılım takılabilir (*plug-in*) veya eklentileri yazılımlarıdır.

Kötücül kod (Malicious code) | Kötücül niyetle yazılmış yazılımdır, örneğin bir bilgisayar virüsü.

Kötücül yazılım (Malicious software) | Bir veya daha fazla hedef bilgisayara sızmak ve bir saldırganın talimatlarını takip etmek için tasarlanmış yazılımdır. Aynı zamanda, kötü amaçlı yazılım (*malware*) olarak da bilinmektedir.

Kriptanaliz (Cryptanalysis) | Anahtar bilgisi olmadan kodları kırma işlemidir.

Kriptografi (Cryptography) | Bilgiyi gizleme çalışması veya pratiğidir.

Kriptografik özet (Cryptographic hash) | Büyük miktarda veriyi tek bir sayıya dönüştüren bir algoritmadır.

Kriptogram (Cryptogram) | Küçük bir şifreli mesajdır.

Kriptokilitleyici (Cryptolocker) | Mağdur şifre çözme anahtarlarını almak için bir fidye ödeyene kadar kritik dosyaları veya verileri, şifreleyen özel bir fidye yazılımıdır.

Kriptosistem (Cryptosystem) | Verileri şifrelemek ve şifresini çözmek için kullanılan algoritmalar veya şifrelemelerdir.

Kuantum kriptografi (Quantum cryptography) | Veri şifreleme ve şifre çözme veya güvenli anahtar değişimi sağlama gibi kriptografik görevleri gerçekleştirmek için kuantum mekaniğini kullanan kriptografidir.

Kullanıcı adı (Username) | Bir kullanıcıyı bir sisteme tanımlamanın en yaygın yöntemidir. Genellikle bir bilgisayar

sistemine erişen bir kişiyi veya grubu temsil eden bir karakter dizisidir.

Kullanıcı kabulü (User acceptance) | Yazılım geliştirmenin son aşamasıdır. kullanıcılar yazılımla çalışırken gerçek dünya kullanımını simüle eder.

Kullanıcı Veri Bloğu İletişim Kuralı (User Datagram Protocol - UDP) | Bağlantısız ve az miktarda veri veya mesaj alışverişi yapmak için popüler olan bir iletişim protokolüdür.

Kullanıcıya atanmış ayrıcalıklar (User assigned privileges) | En ayrıntılı yetkilendirme politikasıdır, bireysel kullanıcıya özel ayrıcalıklar atar.

Kullanılabilirlik (Availability) | Bir sistem için çalışma süresi (*uptime*) miktarını, hizmet dışı kalma/aksama (downtime) süresine göre ölçen matematiksel bir formüldür. Genellikle, belirli bir takvim ayı içindeki bir oran veya yüzde olarak gösterilmektedir.

Kum havuzu (Sandbox) | Programları ayırmak ve bunları kendi sanal uzaylarında çalıştırmak için bir stratejidir.

Kural tabanlı yönetim (Rule-based management) | Neyin kabul edilebilir neyin kabul edilemeyeceği hakkındaki ağ cihazı kurallarını tanımlayarak bir ağın güvenliğini yönetmektir.

Kurtarma noktası hedefi (Recovery point objective - RPO) | Bir felaketten sonra kabul edilebilir maksimum veri kaybı seviyesidir.

Kurtarma süresi hedefi (Recovery time objective - RTO) | Bir BT sistemini, uygulamayı ve veri erişimini kurtarmanın ne kadar sürmesi gerektiğine dair tanımlanmış bir ölçümdür.

Kümeleme (Clustering) | Sabit sürücüdeki bir veya daha fazla sektörden oluşan mantıksal bir veri bölümüdür. Bir küme, mantıksal hacim boyutuna bağlı olarak genellikle 512, 1.024, 2.048 veya 4.096 byte'lık adreslenebilir en küçük sürücü depolama birimidir.

L

LDAP enjeksiyonu (LDAP injection) | Kullanıcı girdisine dayalı olarak LDAP'i oluşturan web sitelerini kullanan bir saldırıdır. Girdiyi temizlemeyen web uygulamaları, saldırganların LDAP deyimlerinin nasıl oluşturulduğunu değiştirmesine olanak verir. Saldırgan tarafından değiştirilen LDAP ifadeleri, komutu uygulayan bileşenle aynı izinlere sahip olarak çalışır, böylece sahte veya taklit bir kimlik ve kimlik denetleme LDAP komutları ve paketleri, kimlik denetlemesi için bir web uygulamasına gönderilebilir.

M

MAC adres filtresi (MAC address filter) | MAC adresiyle kablosuz ağ trafiğini filtreleyen güvenlik duvarı filtreleme kurallarıdır.

Mahremiyet (Privacy) | Kişisel hakların ifşa edilmemesi için korunmasıdır.

Mahremiyet politikası (Privacy policy) | Kuruluşunuzun bireyler hakkındaki bilgileri nasıl topladığını, kullandığını ve ortadan kaldırdığını belirten bir politikadır.

Makro virüs (Macro virus) | Genellikle bir veri dosyasını etkileyen ve zararlı makro komutları enjekte eden bir virüs türüdür.

Maksimum tolere edilebilen aksama süresi (Maximum tolerable downtime - MTD) | Kritik iş süreçlerinin ve kaynaklarının, bir kuruluşun onarılamayacak ticari zararlar yaşamaya başlamadan önce çevrimdışı olma süresidir.

Mantık bombası (Logic bomb) | Önceden belirlenmiş bazı tetikleyiciler tarafından aktive edilmek üzere, kasıtlı olarak bir yazılım sistemine yerleştirilmiş, zarar vermek için tasarlanmış bir kod parçasıdır.

Mantıksal erişim denetimi (Logical access control) | Bilgisayar sistemlerine ve ağ kaynaklarına erişimi kısıtlayan bir mekanizmadır.

Maskeleme (Masking) | Kredi kartı numarası veya Sosyal Güvenlik numarası gibi hassas bir veri öğesinin bazı karakterlerini gizlemek için özel bir karakterin (örneğin, X veya *) kullanılmasıdır.

Mesaj özeti algoritması (Message digest algorithm - MD5) | 128 bitlik özet değerine sahip kriptografik bir özet fonksiyonudur.

Meydan Okuma-El Sıkışma Kimlik Denetleme Protokolü (Challenge-Handshake Authentication Protocol - CHAP) | Gizlice dinleme ve yeniden gönderme saldırılarını engellemek için parolaları tek kullanımlık numara ile özetleyen (*hash*) dağıtık kimlik denetleme protokolüdür.

Mıknatıslık giderme bobini (Degausser) | Manyetik depolama ortamından verileri silen bir manyetik alan oluşturan bir cihazdır.

Miller testi (Miller test) | Bir şeyi müstehcen olarak etiketleyip etiketlememeye karar vermek için ABD Yüksek Mahkemesi tarafından tanımlanan üç aşamalı yaklaşımdır.

Minimum ihtiyaç kuralı (Minimum necessary rule) | Kapsanan işletmelerin belirli bir fonksiyonu yerine getirmek için sadece kesinlikle gerekli olan korunan sağlık bilgisi miktarını ifşa edebileceği ile ilgili bir kuraldır.

Mobil cihaz yönetimi (Mobile device management - MDM) | Çalışanların mobil cihazları için güvenlik yönetimi uygulamasıdır.

Mobil IP | Mobil cihazların LAN bölümlerini şeffaf bir şekilde değiştirmesine izin veren bir protokoldür.

Mobilite (Mobility) | Fiziksel olarak tek bir ofise veya konuma sınırlandırılmak zorunda kalmadan iş yapabilme yeteneğidir.

Mutabakat bildirisi/İyi niyet sözleşmesi (Memorandum of Understanding - MOU) | Ortak eylemlere neden olan

ortak çıkar alanlarını ifade eden iki veya daha fazla taraf arasındaki bir anlaşmadır.

Mükemmel iletme gizliliği (Perfect forward secrecy) | Her iletişim oturumu kurulum işleminin benzersiz olduğu bir yaklaşımdır. Eğer bir saldırgan, mevcut bir oturumun anahtarlarını tehlikeye atarsa, önceki herhangi bir oturum anahtarını riske atmaz.

N

Nesnelerin İnterneti (Internet of Things - IoT) | Artık İnternete bağlanabilen çok sayıda ağ tabanlı cihaza (örneğin kişisel eşyalar, ev aletleri, bulut hizmetleri, araçlar vb.) atıfta bulunmak için kullanılan bir terimdir.

Netcat (Netcat) | Ağ bağlantılarını okuyan ve ağ bağlantılarına yazan yardımcı bir ağ programıdır.

Nicel risk değerlendirmesi (Quantitative risk assessment) | Her bir riske sayısal bir değer, genellikle maliyet değeri atayan ve risk etki karşılaştırmalarını daha objektif yapan bir tür risk değerlendirmesidir.

Nitel risk değerlendirmesi (Qualitative risk assessment) | Riskleri tanımlayan ve daha sonra iş operasyonları üzerindeki göreceli potansiyel etkilerini sıralayan bir tür risk değerlendirmesidir.

Nitelikli güvenlik denetçileri (Qualified Security Assessor - QSA) | PCI uygunluk değerlendirmesi yapmak için nitelikli ve yetkilendirilmiş sertifikalı bir bireydir.

Noel saldırısı (Christmas attack) | Xmas saldırısına bakın.

Noktadan Noktaya Tünel Protokolü (Point-to-Point Tunneling Protocol - PPTP) | İki bilgisayar arasında bir VPN bağlantısı kurmak için bir protokolüdür.

O - Ö

Olasılık (Likelihood) | İlişkili bir tehdit ortamı oluştururken potansiyel bir güvenlik açığı oluşma olasılığıdır.

Olay (Incident) | Güvenlik politikanızı ihlal eden veya güvenlik politikanıza olası bir tehdit teşkil eden bir olaydır.

Olay günlükleri (Event logs) | Bir yazılım veya uygulama tarafından oluşturulan, bazı eylemlerin gerçekleştiğini belirten kayıttır.

Olay müdahale ekibi (Incident response team) | Kuruluşun, olay ekibi liderini, iletişim ekibi liderini ve BT ve BT güvenlik personelini içeren güvenlik olayı müdahale ekibi üyeleridir.

Olay tabanlı senkronizasyon sistemi (Event-based synchronization system) | Her erişim isteği için, bir belirtecin (*token*) değerinin bir sunucu ile senkronize edildiği bir kimlik denetleme yöntemidir. Belirtecin sayacı, her yeni değer istendiğinde artırılır.

Oltalama (Phishing) | Bir saldırganın kurbanı özel bilgi sağlaması için kandırmaya çalıştığı bir tür dolandırıcılıktır.

Omuz sörfü (Shoulder surfing) | İnsanların omuzları üzerinden, insanlar bankaların bankamatik cihazına veya benzin pompası gibi güvenli cihazlara kod girerken hakmalıtır.

Onarım için ortalama süre (Mean time to repair - MTTR) | Bir cihazı onarmak için gereken ortalama süredir.

Onaylı Tarama Sağlayıcısı (Approved Scanning Vendor - ASV) | güvenlik açığı değerlendirmesi taramalarını yapabilen nitelikli ve onaylı bir şirkettir.

Ortadaki adam saldırısı (Man-in-the-middle attack) | Saldırganın, iki taraf arasına girdiği ve mesajları amaçlanan hedeflerine aktarmadan önce engellediği bir saldırıdır.

Otomatik numara çevirici (Wardialer) | Bilgisayar modemi ile başarılı bir şekilde bağlantı kurabilen telefon numaralarını belirlemek için kullanılan bir bilgisayar programıdır.

Oturum anahtarı (Session key) | Her yeni iletişim oturumu için benzersiz bir anahtardır.

Oturum ele geçirme (Session hijacking) | Saldırganın iki ağ bilgisayarı arasındaki mevcut bağlantıyı ele geçirmeye çalıştığı bir ağ saldırısıdır.

Ödeme Kartları Endüstrisi Veri Güvenliği Standardı (Payment Card Industry Data Security Standard - PCI DSS) | Kart sahibi verilerinin işlenmesinin, saklanmasının ve iletiminin korunmasına ilişkin satıcılar ve hizmet sağlayıcılar için bir uyum kanunu değil bir standarttır.

Öndeki kişinin yakınından gitmek (Tailgating) | Güvenli bir kapı veya erişim alanından gizlice geçmek için bir bireyi yakından takip etme eylemidir.

Önemsiz Dosya Aktarım Protokolü (Trivial File Transfer Protocol - TFTP) | İki IP cihazı arasında hızlı ve küçük dosya aktarımı için kullanılan bağlantısız, UDP tabanlı bir dosya aktarım protokolüdür.

Öneriler (Recommendations) | ITU-T uluslararası standartları için resmi terimdir.

Önlem (Countermeasure) | Belirli bir tehdide karşı koymak veya ele almak için yüklenmiş olan bir önlemdir.

Önleyici denetim (Preventive control) | Bir eylemi gerçekleşmeden önce durduran bir denetimdir. Önleyici denetimler, kilitli kapılar, güvenlik duvarı kuralları ve kullanıcı parolalarını içerir.

Örüntü veya imza-tabanlı IDS (Pattern- or signature-based IDS) | Mevcut trafiği, bilinen ağa izinsiz giren kişilerin etkinlik örüntüleriyle (imzalarıyla) karşılaştırmak için örüntü eşleştirme ve durum bilgisi eşleştirme kullanan bir saldırı tespit sistemidir.

Öz-değerlendirme anketi (Self-assessment questionnaire - SAQ) | PCI Veri Güvenliği Standardı tarafından tanımlanmıştır, standardın gereksinimleri ile kuruluşun kendi uygunluğunu belirlemeye yönelik olarak kuruluşa kılavuzluk etmek çin kullanılan bir dizi evet ya da hayır sorusudur.

Özel (simetrik) anahtar (Private (symmetric) key) | Bilgileri şifrelemek ve şifresini çözmek için aynı anahtarı kullanan bir şifreleme kodudur.

Özel şirketler (Privately held companies) | Küçük bir grup özel yatırımcı tarafından sahip olunan bir şirkettir.

Özenti (Wannabe) | *Bkz. Gri şapka bilgisayar korsanı.*

Özet (Hash) | Büyük miktardaki veriyi tek (uzun) bir sayıya dönüştüren bir algoritmadır. Matematiksel olarak bir kez özetlendikten sonra, ilgili verinin bütünlüğünü doğrulamak için özet değeri kullanılabilir.

Özetleme fonksiyonu (Hashing function) | Girdiyi alan ve bu girdiden benzerini üretmesi zor ve tersine çevirmesi aşırı zor olan bir çıktı üreten tek yönlü bir fonksiyondur (*one-way function*).

Öznitelik tabanlı şifreleme (Attribute-based encryption - ABE) | Kullanıcının gizli anahtarının ve şifreli metnin, gönderenin ülke veya eyalet gibi özelliklerine bağlı olduğu bir tür açık anahtarlı şifrelemedir.

P

Paket filtrelemeli güvenlik duvarı (Packet-filtering firewall) | Aldığı her paketi inceleyen ve bu paketi ağ yöneticisi tarafından yapılandırılan bir kurallar listesiyle karşılaştıran bir güvenlik duvarıdır.

Paket koklayıcı (Packet sniffer) | Bir ağ bölümü boyunca gönderilen tüm ağ paketlerini yakalamak için karışık modda (*promiscuous mode*) bir donanım adaptör kartı kullanan bir yazılım uygulamasıdır.

Paralel testler (Parallel tests) | Tam kesinti testi (*full-interruption test*) ile aynıdır, ancak işlem birincil alanda durmaz.

Parola Doğrulama Protokolü (Password Authentication Protocol - PAP) | Açık metin kullanıcı adlarını ve parolalarını kullanan merkezi olmayan/dağıtık kimlik denetleme protokolüdür.

Parola kırıcı (Password cracker) | İki fonksiyondan birini gerçekleştiren bir yazılım programıdır: Bir sisteme yetkilendirilmemiş erişim sağlamak veya bir bilgisayar sisteminde depolanan parolaların kurtarılması için brute-force/kaba kuvvet parola saldırısı.

Penetrasyon/Sızma testi (Penetration testing) | Bir saldırganın, sisteme başarılı bir şekilde sızabileceğini kanıtlamak için sistemdeki bir zayıflığı kullanmaya çalışan bir test yöntemidir.

Ping (Ping) | "Paket internet yoklayıcısı (*packet Internet groper*)" anlamına gelir. Ping, uçtan uca IP bağlantısını doğrulamak için İnternet Kontrol Mesajı Protokolü'nün (Internet Control Message Protocol - ICMP) yankı-isteği (*echo-request*) ve yankı-yanıtlama (*echo-reply*) iletişimlerini kullanır.

Platformlar arası/Çapraz platform virüsü (Cross-platform virus) | Hem Linux hem de Windows'ta etkili bir virüs gibi, birden fazla platformda veya işletim sisteminde zararlı olan virüslerdir.

Politik amaçlı bilgisayar korsanları (Hactivist) | Siyasi ya da sosyal adalet endişeleri ile motive olan ve seçtiği pozisyonunu güçlendirmek için bilgisayar korsanlığı becerilerini kullanan kendisinin bilgisayar korsanı olduğunu iddia eden ya da bilgisayar korsanı olan kişidir.

Port tarayıcı (Port scanner) | Etkinleştirilmiş açık portlar için IP ana bilgisayar cihazlarını taramada kullanılan bir araçtır.

Proaktif değişiklik yönetimi (Proactive change management) | Beklenen sorunları önlemek için değişiklikleri başlatma eylemidir.

Proje Yönetimi Bilgi Tabanı (Project Management Body of Knowledge - PMBOK) | Proje yönetimi mesleğinin bilgi birikiminin ve en iyi uygulamalarının bir topluluğudur.

Proje Yönetimi Enstitüsü (Project Management Institute - PMI) | Proje yönetimi alanını teşvik eden, proje yöneticilerinin kar amacı gütmeyen uluslararası bir organizasyonudur.

Prosedür (Procedure) | Bir güvenlik gereksinimini, işlemini veya hedefini gerçekleştirmek için yürütülecek bir dizi adım adım eylem kümesidir.

Protokol (Protocol) | İletişim kurmak için kuralların ve yöntemlerin listesidir

Protokol çözümleyici (Protocol analyzer) | Bir bilgisayarın, açık metin olarak parolaları ve verileri de içermek üzere ağ trafiğini izlemesini ve yakalamasını sağlayan bir yazılım programıdır.

Proxy güvenlik duvarı (Proxy firewall) | Güvenlik duvarı ve İnternet'teki dahili bilgisayarlar ile bilgisayarlar arasında bir aracı olarak hizmet veren bir ağ cihazı veya bilgisayardır.

Proxy sunucusu (Proxy server) | Dış dünya ile kullanıcı arasında veri paylaşımı için aracı olarak davranan bir DMZ LAN üzerine yerleştirilmiş bir sunucudur. Proxy sunucuları, bağlı oldukları iş istasyonlarının mecbur kalmaması için riskleri, tehditleri ve güvenlik açıklarını üstlenir.

R

Radyo frekansı ile tanımlama (Radio frequency identification - RFID) | Ürünün hareketini izlemek için bir okuyucu ile bir ürüne bağlı bir etiket arasındaki kablosuz bağlantı yoluyla veri alışverişinde bulunan bir teknolojidir.

Rainbow tabloları (Rainbow tables) | Belirli bir karakter alanında mevcut olan tüm parolaların önceden hesaplanmış özetleri ile çalışan parola kırıcı türüdür.

Reaktif değişiklik yönetimi (Reactive change management) | Rapor edilen sorunlara cevap olarak değişiklikleri yürütme eylemidir.

Referans monitörü (Reference monitor) | Tüm kaynak erişim talepleri için merkezi bir işlem noktası sağlayan yazılımdır.

Reklam yazılımı (Adware) | İnternet kullanımı hakkında bilgi toplayan ve kullanıcılara hedeflenmiş reklamlar sunmak için kullanan bir yazılım programıdır.

Retro virüsü (Retro virus) | Virüsten koruma yazılımı imza dosyaları veya bütünlük veritabanları gibi karşı önlemlere saldıran bir virüstür.

RFC 1087: Etik ve İnternet ((RFC 1087: Ethics and the Internet) | Etik ve İnternet'i tanımlayan ABD hükümeti ve İnternet Danışma Kurulu (*Internet Advisory Board*) tarafından yayınlanan bir kabul edilebilir kullanım politika (*acceptable-use policy*) bildirimidir.

Risk (Risk) | Genelde kötü bir şey olan bir şeyin bir varlığın başına gelme olasılığıdır.

Risk kaydı (Risk register) | Risk belirleme sürecinden kaynaklanan tanımlanmış risklerin bir listesidir.

Risk metodolojisi (Risk methodology) | Genel riski nasıl yöneteceğinizin bir tanımlamasıdır. Her bir riski ele alan yaklaşımı, gerekli bilgileri ve teknikleri içerir.

Risk yönetimi (Risk management) | Riskleri belirleme, değerlendirme, önceliklendirme ve ele alma sürecidir.

Rivest-Shamir-Adelman (Rivest-Shamir-Adelman - RSA) | Büyük sayıları çarpanlarına ayırma zorluğuna dayanan bir dijital imza algoritmasıdır.

Robot Ağlar (Botnets) Robotik olarak kontrol edilen ağ. Bir botnet, saldırganların saldırıları başlatmak ve kötü amaçlı yazılımları yaymak için kullandıkları gizliliği ihlal edilmiş bilgisayarlardan oluşan bir ağdan oluşur.

Rol tabanlı erişim denetimi (Role-based access control - RBAC) | Kullanıcının atandığı işlere erişim denetim onaylarını temel alan bir erişim denetimi yöntemidir.

Rootkit (Rootkit) | Bir bilgisayarın ele geçirildiği gerçeğini gizlemek için bir veya daha fazla programı değiştiren veya yerini alan bir kötücül yazılım türü.

S - Ş

Sağlama toplamı (Checksum) | Tek yönlü bir algoritmanın çıktısıdır. Bazı girdilerin matematiksel olarak türetilmiş sayısal gösterimidir.

Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (HIPAA) | Sağlık kurumlarının ve sigorta sağlayıcılarının hastaların özel verilerini korumaları ve uygun güvenlik denetimlerine sahip olmalarını gerektiren bir ABD federal kanunudur.

Sahiplik (Ownership) | Kimlik denetlemede, akıllı kart, anahtar, rozet veya belirteç gibi sahip olduğunuz bir şeydir.

Sahte erişim noktaları (Rogue access points) | Kullanıcıları bağlantı kurmaları için kandırmak için bir bilgisayar korsanı tarafından kurulan ve yapılandırılan bir kablosuz LAN erişim noktasıdır. Bilgisayar korsanı daha sonra, ortadaki adam saldırısı gibi bir saldırı gerçekleştirmek için bağlantıyı kullanabilir.

Sahte URL (Typo squatting) | Bir kullanıcının amaçlanan URL'yi yanlış yazma umuduyla az oranda hatalı bir URL'yi tescil ettirmesi ve "squatting" eylemidir. Ayrıca bkz. URL kaçırma (*URL hijacking*).

Sakla ve ilet iletişimler (Store-and-forward communications) | İki veya daha fazla kullanıcı arasındaki iletişimi ara depolamayla iletme tekniğidir. Göndericiden merkezi depolamaya gönderim hemen yapılır, ancak alıcıya yapılan son aktarım uygunluk durumuna ve saklanan bilgi için yapılan isteğe bağlıdır.

Saldırı (Attack) | Bir BT donanım varlığı veya uygulamasında bir güvenlik açığından yararlanma girişimidir.

Saldırı tespit sistemi/Saldırı engelleme sistemi (Intrusion detection system/intrusion prevention system - IDS/IPS) | İstenmeyen IP trafiğini izlemek ve engellemek için genellikle İnternet'ten giriş/çıkış noktasında LAN-dan-WAN-a Etki Alanı'na kurulan ağ güvenlik cihazlarıdır.

Sanal LAN (Virtual LAN - VLAN) | Tüm iş istasyonlarının aynı mantıksal LAN'da olduğu Ethernet'teki yayınlama etki alanıdır (*broadcast domain*).

Sanal özel ağ (Virtual private network - VPN) | IP paketlerini, bir tünelde olduğu gibi, bir uçtan diğerine şifreleme yöntemidir.

Sarbanes-Oxley Kanunu (Sarbanes-Oxley Act - SOX) | Halka açık şirketlerin memurlarının doğru ve denetlenmiş mali tablolara sahip olmalarını gerektiren bir ABD federal kanunudur. SOX ayrıca finansal kayıtları ve içeriden edinilen bilgileri korumak için uygun güvenlik kontrollerini gerektirir.

Satıcı-bağımsız sertifikalandırma (Vendor-neutral certification) | Bu tür bir sertifikasyon, doğası gereği genel olan ve belirli bir ürün veya ürün hattına odaklanmayan kavramları ve konuları kapsar.

Satıcıya özel sertifikalandırma (Vendor-specific certification) | Bu tür bir sertifikasyon, derinlemesine ürün bilgisine sahip profesyonelleri tanımlamaya yardımcı olur. Birçok kuruluş, işe alınacak çalışanları ve personeli değerlendirirken, satıcı-bağımsız sertifikalarla birlikte bu sertifikaları kullanır.

Sayaç Modu Şifreleme Bloğu Zincirleme Mesaj Doğrulama Kodu Protokolü (Counter Mode Cipher Block Chaining Message Authentication Code Protocol - CCMP) | 802.11i standardını uygulayan bir şifreleme protokolüdür. CCMP, AES standardının Sayaç Modunu (*Counter Mode*) kullanarak daha fazla güvenlik sağlar.

Senkronize belirteç (Synchronous token) | Bir ağın uzak kullanıcıları için oturum açma denetleyicisi olarak kullanılan bir cihazdır.

Sertifika yetkilisi (Certificate authority - CA) | Verisign veya Computer Associates gibi doğrulanmış dijital sertifikaları saklayan ve dağıtan güvenilir bir varlıktır.

Sertifikalandıran/Sertifika Verici (Certifier) | Sistem için güvenlik testi ve değerlendirmesini (ST + E) yapmaktan sorumlu kişi veya ekiptir. Sertifika verici ayrıca, yetkilendirme görevlisi için sistemin işletilmesi riski hakkında bir rapor hazırlar.

Sertifikalı Bilgi Sistemleri Güvenlik Profesyoneli (Certified Information Systems Security Professional - CISSP®) | (ISC)² tarafından sunulan, dünya çapında tanınan bir bilgi sistemleri güvenlik profesyoneli sertifikasıdır.

Sertifikasyon (Certification) | Bir sistemi doğru bir şekilde gerçekleştirdiğinizden emin olmak için sistemin teknik değerlendirmesidir. Ayrıca, bir kişinin belirli gereksinimleri yerine getirdiğini gösteren resmi bir açıklamadır. Gereksinimler genellikle belli bir deneyime sahip olmayı, bir çalışma kursunu tamamlamayı ve bir sınavı geçmeyi içerir.

Servis seviyesi anlaşması (Service-level agreement - SLA) | Bir servis sağlayıcı veya destek kurumu tarafından müşterilerine veya kullanıcılarına yapılan, sözleşmeye bağlı bir taahhüttür.

Sesli konferans (Audio conferencing) | İki veya daha fazla konuşmacının telefon kullanmak yerine bilgisayarları üzerinden sohbet etmesini sağlayan IP üzerinden ses (voice over IP - VoIP) kullanan bir yazılım uygulamasıdır.

Sıfırıncı gün (Zero day) | Mevcut özel savunmaların olmadığı yeni ve daha önce bilinmeyen bir saldırıdır. "Sıfırıncı gün", bilgisayar korsanları topluluğunda günler veya haftalarca bilinen bir istismarın yeniliğini ifade eder. Böyle bir saldırı ilk kez gerçekleştiğinde, savunuculara sıfır gün öncesinden bildirim verilir (bu nedenle böyle isimlendirilmiştir).

Sınır güvenlik duvarı (Border firewall) | Kapalı veya güvenli ağı, İnternet gibi dış veya genel ağlardan ayıran bir güvenlik duvarıdır.

Siber Güvenlik (Cybersecurity) | İnternete ve Web'e bağlı olan bireyleri, işletmeleri, organizasyonları ve hükümetleri güvence altına alma ve koruma eylemidir.

Siber Uzay (Cyberspace) | Bireylerin, işletmelerin, organizasyonların ve hükümetlerin birbirine bağlandığı İnternet tarafından oluşturulan küresel çevrimiçi sanal dünya.

Simetrik anahtar kriptografisi (Symmetric key cryptography) | İki taraf anahtar değişimi yapana kadar, yazışmaları güvence altına alamayacak bir kriptografi türüdür.

Simülasyon testi (Simulation test) | Bir iş kesintisinin simüle edildiği bir BCP veya DRP'yi test etme yöntemidir ve müdahale ekibi durum gerçekmiş gibi yanıt verir.

Sistem başlatma virüsü (System infector) | Bir bilgisayardaki temel donanım ve sistem yazılımı bileşenlerini hedefleyen ve genellikle sistem başlatma işlemleriyle ilişkili bir virüs türüdür.

Sistem sahibi (System owner) | Bir sistemin günlük işletilmesinden ve sistemin yetkilendirme görevlisi tarafından belirtilen koşullara uygun olarak çalışmaya devam etmesini sağlamaktan sorumlu kişidir.

Sistem yaşam döngüsü (System life cycle - SLC) | Sistem mühendisliğinde, tasarım, geliştirme, dağıtım, işlem ve yok etme dahil olmak üzere sistemin varlığının aşamalarını tanımlamak için kullanılan bir yöntemdir.

Siyah-şapka bilgisayar korsanı (Black-hat hacker) | BT güvenliği, meydan okumak ve teknik maharetlerini kanıtlamak için kırmaya çalışan bir bilgisayar saldırganıdır.

Smurf saldırısı (Smurf attack) | DoS saldırıları oluşturmak için sahte İnternet Kontrol Mesaj Protokolü'nün (Internet Control Message Protocol - ICMP) yankı-isteği (*echo-request*) paketlerinin uzak konumlardaki IP yayımlama (*broadcasting*) adreslerine gönderildiği bir ağ saldırısıdır.

Smurfing (Smurfing) | Kurban bilgisayarı için ağ trafiği taşkını (*flood*) oluşturmak için yönlendirilmiş yayın kullanan bir DoS saldırısıdır.

Solucan (Worm) | Cihazdan cihaza yayılabilen, kendini kopyalayan, kötücül bir yazılımdır.

Son Kullanıcı Lisans Sözleşmesi (End-User License Agreement - EULA) | Yazılım üreticisi ve kullanıcıları arasında, yazılım hataları, bug'lar veya güvenlik açıkları ile ilgili sorumluluğu sınırlayan bir lisans sözleşmesidir.

Sonu Açık Sipariş Sözleşmesi (Blanket Purchase Agreement - BPA) | Düzenli bir sarf malzemesi veya hizmet satın alma yöntemi tanımlayan bir anlaşmadır.

Sosyal medya (Social media) | Forumlar, mesaj panoları, bloglar, wiki'ler ve podcast'leri içeren, sosyal uygulamaları tanımlayan bir terimdir. Sosyal medya uygulamaları Google+, Facebook, Instagram ve YouTube'u içerir.

Sosyal mühendislik (Social engineering) | Bir kişiyi bilgiyi açıklamaya ikna etmeye dayanan bir tür saldırıdır.

Sözlük parola saldırısı (Dictionary password attack) | Tüm kelimeleri bir sözlük dosyasından alan ve her sözlük girişini bir parola olarak girerek sisteme giriş yapmaya çalışan bir saldırı yöntemidir.

Spam (Spam) | İstenmeyen e-posta veya istenmeyen mesajlardır.

Spim (Spim) | İstenmeyen mesajların spamına benzer, ancak e-posta yerine anlık mesajlaşma servisi aracılığıyla gerçekleşmektedir.

Sprint (Sprint) | Yazılım geliştirmenin diğer yöntemlerinin klasik uzun proje programlarının aksine, yazılım geliştirmenin "çevik (*agile*)" yönteminde kullanılan küçük proje yinelemelerinden biridir.

SQL enjeksiyonu (SQL injection) | Bir bilgisayar korsanının, kimlik denetlemesini atlamasına, verilerin çıkarılmasına, bilginin eklenmesine veya bir komut kabuğuna erişime neden olmak için SQL (yapılandırılmış sorgu dili) ifadeleri gönderdiği bir web uygulaması saldırısı biçimidir.

SSL el sıkışma protokolü (SSL handshake protocol) | İstemci ve sunucu arasında ilk güvenli iletişim oturumunu oluşturan bir işlemdir.

Standart (Standard) | Kurum genelinde güvenlik riskiyle mücadele etmek için kullanılan bir donanım veya yazılım çözümü için zorunlu bir gerekliliktir.

Steganografi (Steganography) | Gizli mesaj yazma sanatı ve bilimidir.

Suyun başı saldırısı (Watering hole attack) | Hedef kullanıcı ya da şirket tarafından ziyaret edildiği bilinen üçüncü taraf bir web sitesine kötücül bir kod yerleştirmektir. Saldırgan daha sonra hedefin kurban siteyi ziyaret etmesini ve yerleştirilen kodun hedef sistemlere saldırmaya yardımcı olmasını beklemelidir.

Sürekli eğitim (Continuing education) | Herhangi bir lisans programını beraberinde getirmeyen, ancak sürekli eğitim kredilerine katkıda bulunan resmi kurslar sunan, genellikle bir kolej veya üniversite ile ilişkili olan bir eğitim programıdır.

Sürekli kimlik denetleme (Continuous authentication) | Bir kullanıcının, birçok defa veya olay aralıklarında kimliğinin doğrulandığı bir kimlik denetleme yöntemidir.

Sürekli mesleki eğitim (Continuing professional education - CPE) | 50 dakikalık eğitime eşdeğer standart bir kredi birimidir.

Sürekli mesleki gelişim (Continuing professional development - CPD) | Profesyonel bir iş ortamında, kişinin neyi öğrendiği, eğittiği ve uyguladığı ile ilgili bir ölçümdür.

SYN taşkını (SYN flood) | Alındı onayı olmayan (*unacknowledged*) bağlantı isteklerinin bir taşkınını göndererek bilgisayarın bağlantı tablosunu dolduran bir DoS saldırısıdır. Bağlantı tablosu dolduğunda, bilgisayar herhangi bir yeni geçerli bağlantı isteğine yanıt veremez.

SYN-ACK (SYN-ACK) | Bir ağ bağlantısı kurma isteğine (SYN) yanıt vermek (ACK) için kullanılan belirli bir TCP ağ mesajıdır. Bu tür bir mesaj, üç aşamalı bağlantı tokalaşma (*handshake*) anlaşmasının ikinci aşamasındadır.

Şelale modeli (Waterfall model) | Geliştirme faaliyetlerinin bir aşamadan diğerine nasıl ilerleyeceğini tanımlayan bir yazılım geliştirme modelidir.

Şifre Çözme (Decryption) | Şifreli metini çözerek düz metin haline getirme eylemidir.

Şifreleme (Cipher) | Bilgiyi şifrelemek veya bilginin şifresini çözmek için bir algoritmadır.

Şifreleme (Encryption) | Açık metin verisini çözülemeyen şifreli metin haline dönüştürme işlemidir.

Şifreli Metin (Ciphertext) | Şifreli veriler, açık metnin tersidir. Şifreli metin olarak gönderilen veriler anlaşılmaz veya deşifre edilemez.

T

Taklit etme (Impersonation) | Bir web sitesi veya web uygulaması açısından, saldırganın geçerli bir kullanıcının oturum kimlik bilgilerini kullanmaya çalışmasıdır.

Tamsayı taşması (Integer overflow) | İzin verilen maksimum boyutu aşan matematiksel bir taşma oluşturma eylemidir. Bu, finansal veya matematiksel bir uygulamanın donmasına veya bir güvenlik açığı oluşturmasına ve saldırıya açık olmasına neden olabilir.

Tarayıcı eklentileri (Browser add-ons) | Web tarayıcınızla birlikte çalışan yardımcı programlardır.

Taşıyıcı Duyarlı Çoklu Erişim / Çarpışma Tespiti (Carrier Sense Multiple Access/Collision Detection - CSMA/CD) | Ethernet Yerel Alan Ağı segmentinde erişim ve çarpışma tespiti için IEEE 802.3 Yerel Alan Ağı standardıdır.

Tehdit (Threat) | Bir varlığa zarar verebilecek herhangi bir işlemdir.

Tek arıza noktası (Single point of failure - SPOF) | Ağın çalışması için veya daha büyük sistem için çalışması gereken tek bir donanım veya yazılım parçasıdır.

Tek faktörlü kimlik doğrulama (Single-factor authentication) | Yalnızca tek bir kimlik denetleme bilgisi türü kullanan bir kimlik denetleme yöntemidir.

Tek kullanımlık şifreleme (One-time pad cipher) | Bkz. *Vernam şifrelemesi.*

Tek oturum açma (Single sign-on - SSO) | Bir kullanıcının bir sistemde oturum açmasını ve ilk oturum açmayla ağ içindeki diğer kaynaklara erişmesini sağlayan bir erişim denetimi yöntemidir. SSO, bir kullanıcının birden çok kez oturum açmasından ve çeşitli sistemler için birden çok parolayı hatırlamasından kaçınmasına yardımcı olur.

Tek yönlü algoritma (One-way algorithm) | Karşılık gelen şifre çözme algoritmasına sahip olmayan bir şifreleme algoritmasıdır.

Teknik denetim (Technical control) | Bir bilgisayar sistemi tarafından gerçekleştirilen veya yönetilen bir denetimdir.

Teknoloji koruma önlemi (Technology protection measure - TPM) | Bazı kaynaklara erişimi kısıtlamak için kullanılan teknolojidir.

Telafi edici denetim (Compensating control) | Gerçekleştirim maliyeti yüksek ya da gerçekleştirimi zor olan tercih edilen bir denetim yerine tehdidi ele almak için tasarlanmış bir denetimdir.

Telefon dinleme (Wiretapping) | Kablolu bağlantı üzerinden gönderilen iletişimi engellemedir.

Telefon hizmet engelleme (Telephony denial of service - TDoS) | Hizmet reddi (DoS) saldırılarının bir çeşidir, ancak geleneksel ve VoIP telefon sistemlerine karşı yapılmaktadır. Bir TDoS saldırısı, çeşitli yöntemlerle bir kuruluşun telefon sistemini kullanmasını engeller.

Telefon hizmeti (Telephony) | Sesli iletişim çözümlerinin geliştirilmesi ve dağıtılmasını içeren teknoloji alanıdır.

Telefon şebekelerine yasadışı girme (Phreaking) | Telefon sisteminde var olan hataları ve zayıflıkları kullanma sanatıdır.

Telefonla kişisel bilgilerin ele geçirilmesi (Vishing) | Kişisel bilgileri açığa çıkarmak için telefonla oltalama saldırısı (*phishing*) gerçekleştirme eylemidir.

Telnet (Telnet) | Açık metin iletimi sırasında uzaktan terminal erişimini destekleyen güvenli olmayan bir uygulamadır.

Temiz masa/temiz ekran politikası (Clean desk/clear screen policy) | Kullanıcıların sahipsiz bir masa veya iş istasyonunda hiçbir zaman hassas bilgileri açık bir görünümde bırakmaması gerektiğini belirten bir politikadır.

Terminal Erişim Denetleyici Erişim Sistemi (Terminal Access Controller Access System - TACACS) | Ağa uzaktan erişen kullanıcılara kimlik denetleme ve yetkilendirme özellikleri sağlayan bir uzaktan erişim istemci/sunucu protokolüdür. Güvenli bir protokol değildir.

Terminal Erişim Denetleyicisi Erişim Sistemi + (Terminal Access Controller Access System Plus - TACACS +) | Kimlik denetleme, yetkilendirme ve izleme sağlayan Cisco tescilli bir uzaktan erişim istemci/sunucu protokolüdür.

Toplam risk (Total risk) | Tüm işletme varlıkları için birleşik risktir.

Trafiğe boğma koruması (Flood guard) | Ana bilgisayarlardan trafik bant genişliğini sınırlandırabilen ve herhangi bir ana makinenin bir ağı trafiğe boğma yeteneğini azaltan güvenlik duvarı kurallarıdır.

Truva (Trojan) | Kullanıcıya zararsız görünen, ancak aslında kötücül niyetli bir kişi adına bir görev gerçekleştiren kötücül bir yazılım kodudur.

Truva atları (Trojan horses) | *Bkz. Truva (Trojan).*

Tuş vurucu kaydedicileri (Keystroke logger) | Bir kullanıcının kaydettiği her tuş vuruşu için bir günlük dosyasına kayıt yapan gözetim yazılımı veya donanımıdır; aynı zamanda tuş kaydedici (*keylogger*) olarak da bilinmektedir.

Tuz değeri (Salt value) | Şifreleme anahtarını oluşturmak için gerçek bir girdi anahtarıyla birleştirebileceğiniz rastgele karakterlerdir.

Tuzak (Mantrap) | Korunan bir alana girişi kontrol eden bir fiziksel güvenlik önlemidir. Bu giriş yöntemi, küçük bir odanın her iki ucunda iki kapıya sahiptir.

U - Ü

Ucuz Diskler Yedek Dizisi (Redundant Array of Inexpensive Disks - RAID) | Hız ve hata toleransı kazanan bir disk seti yönetim teknolojisidir. RAID, sabit sürücü arızasına karşı bir miktar koruma sağlayabilir, ancak virüs bulaşma gibi yazılım veya veri gizliliği ihlallerine karşı koruma sağlamaz.

Ulusal Güvenlik Açıkları Veritabanı (National Vulnerability Database - NVD) | Daha önce Yaygın Güvenlik Açıkları ve Etkilenme (Common Vulnerability & Exposures) listesi olarak bilinmektedir.

Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology - NIST) | Misyonu "ölçüm güvenliğini, standartları ve teknolojiyi ekonomik güvenliği artırarak ve yaşam kalitemizi geliştirerek ABD inovasyonunu ve endüstriyel rekabetçiliği teşvik etmek" olan ABD Ticaret Bakanlığı bünyesindeki federal bir ajanstır.

Uluslararası Bilgi Sistemleri Güvenlik Sertifika Konsorsiyumu (International Information Systems Security Certification Consortium) | *Bkz.* $(ISC)^2$.

Uluslararası Elektroteknik Komisyonu (International Electrotechnical Commission - IEC) | Elektrik ve elektronik cihaz ve işlemlerle ilgili teknolojiler için uluslararası standartlar geliştirmek ve yayınlamak için etkili bir organizasyondur.

Uluslararası Standartlar Teşkilatı (International Organization for Standardization - ISO) | Amacı, uluslararası standartları geliştirmek ve yayınlamak olan uluslararası bir sivil toplum kuruluşudur.

Uluslararası Telekomünikasyon Birliği (International Telecommunication Union - ITU) | Bilgi ve teknoloji konularının yönetimi ve tanıtımından sorumlu olan başlıca Birleşmiş Milletler ajansıdır.

URL filtrelemesi (URL filter) | IP adresinin aksine, web trafiğini URL'ye göre filtreleyen güvenlik duvarı filtreleme kurallarıdır.

URL kaçırma | *Bkz. Sahte URL (Typo squatting).*

USB belirteci (USB token) | Bilgisayarınızın USB bağlantı noktasına taktığınız kimlik denetlemesi için kullanılan bir donanım cihazıdır. Bu cihaz, kullanıcının herhangi bir şey yazması gerekmeden kimlik denetleme bilgilerini sağlar.

Uygulama ağ geçidi (Application gateway) | Güvenlik duvarı ve İnternet'teki dahili (*internal*) bilgisayarlar ile bilgisayarlar arasında bir aracı olarak hizmet veren bir ağ cihazı veya bilgisayardır.

Uygulama saldırıları (Application attacks) | Genellikle halka açık web sunucularına, uygulamalara ve arka-uç veritabanlarına yönelik izinsiz sızma (penetrasyon) testleri şeklindeki saldırılardır.

Uygulama servis sağlayıcısı (Application service provider - ASP) | Bulutta ve İnternette barındırılan uygulamaları geliştiren ve ticari olarak bu uygulamayı birden çoğa bir dağıtım modelinde satan bir yazılım şirketidir.

Uygulama vekil sunucusu güvenlik duvarı (Application proxy firewall) | İki sistem arasındaki tüm trafiği işleyen gelişmiş bir güvenlik duvarıdır. Proxy, iki sistem arasında doğrudan bir bağlantıya izin vermek yerine, her sisteme ayrı olarak bağlanır ve filtreleme kurallarını temel alarak filtrelenmiş trafiği hedefe iletir.

Uygunluk (Compliance) | Kuruluşunuza ve kuruluşunuzdaki BT sistemlerinin, uygulamalarının ve verilerinin kullanımına uygulanacak kanunları, kuralları ve yönetmelikleri takip etmektir.

Uygunluk irtibatı (Compliance liaison) | Sorumluluğu, çalışanların bir kuruluşun güvenlik politikalarının farkında olmasını ve bunlara uymasını sağlamak olan bir kişidir.

Uygunluk Onayı (Attestation of Compliance - AOC) | PCI Veri Güvenliği Standardı tarafından tanımlanan, Genel Müdür tarafından imzalanan, herhangi bir boşluk veya telafi edici güvenlik kontrolleri ile tanımlanmış ve belgelenmiş, bir kuruluşun uygunluğunu belirten yıllık yazılı bir beyandır.

Uygunluk raporu (Report of compliance - ROC) | PCI Veri Güvenliği Standardı tarafından tanımlanan, bir denetim sırasında gerçekleştirilen değerlendirme faaliyetlerinin bir özetidir. Uygunluk Onayı'nın (*Attestation of Compliance*) bir parçası olarak dahil edilmiştir.

Uzak günlük kaydı (Remote journaling) | Gerçek zamanlı olarak uzak bir sunucuya işlem kaydetme yöntemidir.

Uzaktan Kimlik Denetleme Çevirmeli Giriş Kullanıcı Hizmeti (Remote Authentication Dial-In User Service - RADIUS) | İlk olarak 1990'ların başında tanıtılan, merkezi sunuculara bağlanmak isteyen çok sayıda kullanıcı için uzaktan kullanıcı kimlik denetlemesini destekleyen popüler protokoldür.

Uzaktan kod yürütme (Remote code execution) | Bkz. İsteğe bağlı kod yürütülme (*arbitrary code execution*).

Uzaktan silme/temizleme (Remote wiping) | Bir aygıttaki veya depolama ortamındaki verileri uzaktan silme veya temizleme özelliğidir.

Uzun Parola (Passphrase) | Genellikle bir paroladan daha uzun ve daha karmaşık olan bir kimlik denetleme bilgisidir. Uzun parola cümleleri birden fazla kelime içerebilir.

Üst veri (Meta data) | Veriler hakkındaki verilere atıfta bulunmak için kullanılan bir terimdir (örneğin, veritabanı tablosunda 100 giriş var, 100 girişin, 99'u manuel ve 1'i otomatik olarak girildi, vb.).

Üzerine Yazma (Overwriting) | Fiziksel depolama ortamındaki belirli alanlara, bu alanlarda depolanmış önceki verileri etkin bir şekilde değiştirmek için, tekrar tekrar veri yazma işlemidir.

V

Varlık (Asset) | Bir kuruluş veya bir kişi için değeri olan herhangi bir öğedir.

Veri ihlali (Data breach) | Hassas verilere erişildiği ve çalındığı bir olaydır.

Veri sınıflandırma standardı (Data classification standard) | Güvenlik hassasiyeti açışından farklı veri tiplerinin bir tanımıdır.

Veri Şifreleme Standardı (Data Encryption Standard - DES) | Yerine koyma ve değiştirmenin 16 yinelemesinden oluşan 56 bit anahtarlı bir birleşik şifreleme (product cipher) şifrelemesidir. İlk olarak 1977'de Federal Bilgi İşleme Standardı (Federal Information Processing Standard - FIPS) olarak yayınlandı.

Veri virüsü (Data infector) | Gömülü makro programlama yeteneklerini içeren belge dosyalarına saldıran bir virüs türüdür.

Vernam şifreleme (Vernam cipher) | Tek kullanımlık kriptografik şifrelemedir. Aynı zamanda, tek kullanımlık şifreleme de (one-time pad) denir.

Video konferans (Video conferencing) | Arayanlar arasında bağlantı kurmayı ve onların web kameraları görüntülerini destekleyen ortak bir video konferans uygulamasıdır.

Vigenère şifreleme (Vigenère cipher) | Birbirini izleyen/ardışık birden çok şifreleme şeması kullanan bir şifreleme kodudur. Örneğin, her beşinci harfi kendi yerine koyma şifrelemesiyle (*substitution cipher*) şifreleyebilirsiniz.

Virüs (Virus) | Bilgisayarın, özgün program geliştiricisi tarafından tasarlanan komutları izlemesini sağlamak amacıyla kendisini başka bir programa ekleyen veya kopyalayan bir yazılım programıdır.

VPN yoğunlaştırıcı (VPN concentrator) | VPN bağlantılarında uzmanlaşmış bir tür yönlendirici gibi davranan ağ cihazıdır.

W

War chalking (War chalking) | Herhangi bir kablosuz erişim noktasının ve ağın fiziksel ve coğrafi konumunun bir haritasını yaratma eylemidir.

War driving (War driving) | Bir tespit etme cihazıyla coğrafi bir alan etrafında hareket ederek kablosuz ağları keşfetme yöntemidir.

Web graffiti (Web graffiti) | Aynı zamanda, web sayfası içeriğinin bozulması (*web defacement*) olarak da adlandırılmaktadır, bir web sunucusuna yetkilendirilmemiş erişime sahip olan ve sunucudaki bir web sitesinin bir veya daha fazla sayfasını değiştiren bir kişiyi ifade eder.

Web güvenlik ağ geçidi (Web security gateway) | URL filtreleme yapan ancak paketin içeriğini incelemeyen bir cihazdır.

Web sayfası içeriğinin bozulması (Web defacement) | Aynı zamanda, web grafiti (*web graffiti*) olarak da adlandırılmaktadır, bir web sunucusuna yetkilendirilmemiş erişime sahip olan ve sunucudaki bir web sitesinin bir veya daha fazla sayfasını değiştiren birini ifade eder.

Web sitesi trafiğinin yönlendirilmesi (Pharming) | Etki alanı yanıltması (*domain spoofing*) yoluyla kişisel veya özel finansal bilgilerini ele geçirmeyi amaçlayan bir saldırıdır.

Web uygulama saldırıları (Web application attacks) | *Bkz. Uygulama saldırıları.*

Web uygulamaları (Web applications) | Kullanıcıların bir web tarayıcısı kullanarak bir ağ üzerinden, genellikle İnternet üzerinden, erişebildiği uygulamalardır.

Wi-Fi Korumalı Erişim (Wi-Fi Protected Access - WPA) | Kablosuz ağlar için mevcut şifrelemedir. WEP'ten

çok daha güçlü olan WPA, kablosuz kullanım için önerilen şifrelemedir.

X

XML enjeksiyonu (XML injection) | Saldırganın veri almak için XML etiketlerini ve verilerini bir veritabanına enjekte ettiği bir web uygulaması saldırısıdır.

XTACACS (Genişletilmiş Terminal Erişim Denetleyici Erişim Sistemi - Extended Terminal Access Controller Access System) | Ağa uzaktan erişen kullanıcılara kimlik denetleme ve yetkilendirme olanakları sağlayan TACACS uzaktan erişim istemcisi/sunucusu protokolünün bir uzantısıdır. Güvenli bir protokol değildir.

Y

Y Kuşağı (Generation Y) | Amerika Birleşik Devletleri'nde 1980-2000 doğumlu olanlardan oluşan kuşaktır. Y kuşağı üyeleri, "baby boomers"ın (2. Dünya savaşını izleyen yıllarda doğanlar) sahip olmadığı teknolojilerle (örneğin, cep telefonları, kablolu TV, İnternet, iPod'lar vb.) büyüdü.

Yakın alan iletişim saldırısı (Near field communication attack) | İki mobil işletim sistemi cihazı arasındaki yakın mesafeden (birkaç inç) iletişimi engelleme eylemidir.

Yakınlık (Familiarity) | Bilgi çıkarımı için bir kişiye yardım ederek (veya yakınlık ve hoşlanma), kişilerle sürekli ve sık etkileşime dayanan bir tür sosyal mühendislik saldırısıdır.

Yakınlık okuyucusu (Proximity reader) | Fiziksel temas gerektirmeden bir kişinin yakındaki belirtecini veya erişim kartını algılayabilen bir cihazdır.

Yama (Patch) | Bir programın güvenlik açıklarını gideren bir yazılım veya kod parçasıdır. İşletim sistemleri dahil olmak üzere birçok yazılım türü için yamalar bulunur.

Yanlış negatif (False negative) | Anormal aktiviteyi yanlışlıkla normal olarak tanımlamaktır.

Yanlış pozitif (False positive) | Normal aktiviteyi yanlışlıkla anormal olarak tanımlamaktır.

Yapılandırma kontrolü (Configuration control) | Bir sistemin veya cihazın temel ayarlarını yönetme işlemidir.

Yavaş virüs (Slow virus) | Virüsten koruma programlarının virüslü dosyalardaki değişiklikleri tespit etmesini engelleyen ve virüsün tespit edilmesini yavaşlatan bir virüs.

Yazılım geliştirme yaşam döngüsü (Software development life cycle - SDLC) | Yazılım uygulamalarını planlama, geliştirme, test etme ve dağıtma sürecini tanımlamak için kullanılan popüler bir yöntemdir.

Yazılım güvenlik açığı/zafiyeti (Software vulnerability) | İstismar için kullanılabilecek, yazılım kodunda bir hata veya yanlışlıktır.

Yedek (Redundancy) | Çoklu iletişim yollarının varlığını garantileyen ağ tasarım özelliğidir. Amaç, tek arıza noktasını (*single point of failure*) önlemek veya bundan kaçınmaktır.

Yedekleme planlaması (Succession planning) | Kilit personel yetersiz veya uygun olmadığında devreye girecek olan planlama eylemidir.

Yeniden gönderme saldırısı (Replay attack) | Bir bilgisayar korsanının ağ trafiğini yakalamak için bir ağ koklayıcısı (*network sniffer*) kullandığı ve daha sonra bu trafiği tekrar ağa aktardığı bir saldırı türüdür. Yeniden gönderme saldırıları, gerçek kullanıcının bir sisteme giriş yapmasına izin veren aynı paketlerin yeniden iletilmesinin bilgisayar korsanına aynı erişimi sağlayacağı umuduyla genellikle kimlik denetleme trafiğine odaklanır.

Yer değiştirme şifrelemesi (Transposition cipher) | Karakterleri veya veri bitlerini yeniden düzenleyen bir şifreleme kodudur.

Yerel alan ağı (Local area network - LAN) | Birbirine veya ortak bir ortama bağlı olan bilgisayarlar topluluğudur. LAN üzerindeki bilgisayarlar genellikle bir binadan daha büyük olmayan bir alan içindedir.

Yerel paylaşılan nesneler (Local shared objects - LSO) | *Bkz. Flash çerezleri.*

Yerine geçme saldırısı (Masquerade attack) | Bir kullanıcının veya bilgisayarın başka bir kullanıcı veya bilgisayar gibi davrandığı bir saldırıdır.

Yerine koyma şifrelemesi (Substitution cipher) | Bit, karakter veya bilgi bloklarını diğer bit, karakter veya bloklarla değiştiren bir şifreleme kodudur.

Yetersizlik (Scarcity) | Bilgi aktarması için mağduru baskı altına almak için erişimin bir biçimi ya da mağdurun bir şeyin eksik (yetersizlik) olduğu duygusuna dayanan bir sosyal mühendislik saldırısıdır.

Yetkilendiren görevli (Authorizing official - AO) | Bir sertifikasyon raporunu inceleyen ve gerçekleştirim için sistemi onaylama kararını veren, atanmış bir üst düzey yöneticidir.

Yetkilendirme (Authorization) | Belirli kaynaklara erişim için kimin onaylandığına karar verme sürecidir.

Yetki seviyesi politikası (Authority-level policy) | Erişim kaynaklarına, kullanıcının yetki seviyesi tarafından karar verilen bir yetkilendirme yöntemidir.

Yıllık gerçekleşme oranı (Annualized rate of occurrence - ARO) | Olasılık olarak da adlandırılan, her yıl bir kaybın ne sıklıkta ortaya çıkacağıdır. Yıllık kayıp beklentisi (*annualized loss expectancy* - ALE), bu oranın ve tekil kayıp beklentisinin (*single loss expectancy* - SLE) çarpımıdır. Matematiksel olarak şöyle ifade edilmektedir: $ALE=ARO \times SLE$

Yolun Sonu (End of life - EOL) | Satıcının veya üreticinin, bir ürün veya yazılım uygulamasına yönelik yazılım güncellemelerini ve yamaları desteklemeye ve sağlamaya son vereceği tarihi tanımlamak için kullanılan bir terimdir.

Yorumlar için İstek (Request for comments - RFC) | IETF tarafından üretilen bir belgedir, RFC'ler standartların yanı sıra diğer spesifikasyonları veya tanımlayıcı içerikleri kapsar.

Yönetim denetimi (Management control) | Risk sürecini yönetmek için tasarlanmış bir denetimdir.

Yönetimsel denetim (Administrative control) | Politikayla ve prosedürlerle uyumu geliştirme ve sağlama sürecinde yer alan bir denetimdir.

Yönlendirici (Router) | İki veya daha fazla ağı birbirine bağlayan ve önceden belirlenmiş rotalara veya yol tespitlerine dayanarak veri paketlerini seçime bağlı olarak değiştiren bir cihazdır.

Yük dengeleme (Load balancing) | Mesaj trafiğini iki veya daha fazla bağlantı üzerine bölen yönlendirme protokolleridir.

Yük dengeleyici (Load balancer) | Tıkanıklığı önlemek için ağ trafiğini farklı ağ bölümlerine dinamik olarak yönlendirebilen bir ağ cihazıdır (genellikle bir güvenlik duvarı).

Z

Zafiyet değerlendirme (Vulnerability assessment) | Yazılımdaki hataları veya yanlışlıkları tanımlayan bir yazılım incelemesidir.

Zafiyet penceresi (Vulnerability window) | Bir yazılım satıcısının, güvenlik yamasını serbest bırakmasıyla sizin onu uygulamanız arasındaki süredir.

Zaman damgası (Timestamping) | Bir üreticinin bilgiyi oluşturduğu veya gönderdiği zamanın tam olarak sağlanmasıdır.

Zaman tabanlı senkronizasyon sistemi (Time-based synchronization system) | Eşleşen değerler oluşturmak için bir belirtecin iç saatinin bir sunucunun saatiyle senkronize edildiği bir kimlik denetleme yöntemidir.

Zaman tabanlı tek kullanımlık parola (Time-based one-time password - TOTP) | Bir HOTP örneği olarak, bu algoritma, yeniden gönderme saldırılarına (*replay attack*) yönelik güvenlik açığını azaltmak için bir zaman damgasını özetlenmiş bir değerle birleştirir.

Zararlı yazılım denetimi (Malware inspection) | Kötü amaçlı yazılım belirtileri için paket içeriğine bakan içerik denetlemenin özel bir biçimidir.

Zırhlı virüs (Armored virüs) | Kendini, keşfedilme, tersine mühendislik veya silme işlemlerinden gizlemeye çalışan bir virüstür.

Zorunlu erişim denetimi (Mandatory access control - MAC) | Nesnenin sınıflandırmasını ve kullanıcının güvenlik iznini temel alarak bir nesneye erişimi kısıtlamanın bir yoludur.

Kaynakça

Andress, Jason and Steve Winterfeld. *Cyber Warfare*. Burlington, MA: Syngress Press, 2011.

Altholz, Nancy, and Larry Stevenson. *Rootkits for Dummies*. New York: John Wiley and Sons Ltd., 2007.

Amoroso, Edward. *Cyber Security*. Summit, NJ: Silicon Press, 2006.

Aquilina, James M., Eoghan Casey, and Cameron H. Malin. *Malware Forensics: Investigating and Analyzing Malicious Code*. Burlington, MA: Syngress, 2008.

Bacik, Sandy. *Building an Effective Information Security Policy Architecture*. Boca Raton, FL: CRC Press, 2008.

Bailey, Mike et al. *Client-Side Attacks and Defense*. Woburn, MA: Newnes, 2012.

Bellovin, Steven M. *Thinking Security*. New York: Addison-Wesley Professional, 2015.

Benantar, Messaoud. *Access Control Systems: Security, Identity Management and Trust Models*. New York: Spring, 2010.

Bhaiji, Yusuf. *Network Security Technologies and Solutions (CCIE Professional Development Series)*. Indianapolis: Cisco Press, 2008.

Biegelman, Martin T., and Daniel R. Biegelman. *Building a World-Class Compliance Program: Best Practices and Strategies for Success*. New York: Wiley, 2008.

Brotby, W. Krag. *Information Security Metrics: A Definitive Guide to Effective Security Monitoring and Measurement*. Chicago: Auerbach, 2008.

Bumiller, Elisabeth. "Bush Signs Bill Aimed at Fraud in Corporations," *The New York Times*, July 30, 2002. http://www.nytimes.com/2002/07/31/business/corporate-conduct-the-president-bush-signs-bill-aimed-at-fraud-in-corporations.html?pagewanted=1 (accessed April 16, 2010).

Calder, Alan, and Steve Watkins. *IT Governance: A Manager's Guide to Data Security and ISO 27001/ISO 27002*, 4th ed. London: Kogan Page, 2013.

Carpenter, Tom. *CWNA Certified Wireless Network Administrator & CWSP Certified Wireless Security Professional All-in-One Exam Guide (PW0-104 & PW0-204)*. New York: McGraw-Hill Osborne Media, 2010.

Chabrow, Eric. "Automated FISMA Reporting Tool Unveiled," GovInfoSecurity.com, October 30, 2009. http://www.govinfosecurity.com/articles.php?art_id=1894 (accessed April 24, 2010).

Children's Internet Protection Act, The, Pub. L. No. 106-554, 114 Stat. 2763A-335 (codified in scattered sections of U.S. Code).

CISM Review Manual 2009. Chicago: Isaca Books, 2008.

Code of Federal Regulations, Title 45, sec. 160.103.

Code of Federal Regulations, Title 45, sec. 164.306.

Code of Federal Regulations, Title 45, sec. 164.316.

Code of Federal Regulations, Title 45, sec. 164.520.

Code of Federal Regulations, Title 45, sec. 164.530(f).

Code of Federal Regulations, Title 45, sec. 164.502(b).

Commission Guidance Regarding Management's Report on Internal Controls Over Financial Reporting. Code of Federal Regulations, Title 17, sec. 241.

Committee on Oversight and Government Reform, "Federal Information Security: Current Challenges and Future Policy Considerations," March 24, 2010. https://oversight.house.gov/wp-content/uploads/2012/01/20100324Fountain.pdf (accessed April 21, 2010). *See* prepared testimony of Mr. Vivek Kundra.

Consumer Sentinel Network Data Book for January–December 2012. Washington: Federal Trade Commission, 2013. http://ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012. pdf (accessed June 13, 2013).

Davis, Chris, Mike Schiller, and Kevin Wheeler. *IT Auditing: Using Controls to Protect Information Assets.* New York: McGraw-Hill Osborne Media, 2011.

Doherty, Jim. *SDN and NFV Simplified.* New York: Addison-Wesley Professional, 2016.

Douligeris, Christos, and Dimitrios N. Serpanos. *Network Security: Current Status and Future Directions.* New York: Wiley-IEEE Press, 2007.

Elisan, Christopher. *Malware, Rootkits & Botnets: A Beginner's Guide.* New York: McGraw Hill Professional, 2012.

Ernst & Young, "Emerging Trends in Internal Controls: Fourth Survey and Industry Insights," September 2005. http://www.sarbanes-oxley.be/aabs_emerging_trends_survey4.pdf (accessed April 16, 2010).

Ethics and the Internet (Request for Comments 1087). Internet Activities Board, January 1989. http://tools.ietf.org/html/rfc1087 (accessed May 22, 2013).

Faircloth, Jeremy, and Paul Piccard. *Combating Spyware in the Enterprise.* Burlington, MA: Syngress, 2006.

Federal Information Security Management Act, Title III of the E-Government Act of 2002, Pub. L. 107-347; U.S. Code Vol. 44, sec. 3541 et seq.

Ferraiolo, David et el, 2007, *Role-based Access Control.* Norwood, MA: Artech House Publishers, 2007.

Free Software Foundation. http://www.fsf.org (accessed September 17, 2010).

Freund, Jack and Jack Jones. *Measuring and Managing Information Risk.* Waltham, MA: Butterworth-Heinemann, 2014.

GNU public license agreement. http://www.gnu.org (accessed September 17, 2010).

Hampton, John J. *Fundamentals of Enterprise Risk Management: How Top Companies Assess Risk, Manage Exposure, and Seize Opportunity.* New York: AMACOM, 2014.

"Hazard Identification and Business Impact Analysis." Continuity Central (Portal Publishing Ltd.). http://www.continuitycentral.com/HazardIdentificationBusinessImpactAnalysis.pdf (accessed October 2, 2010).

Health Information Technology for Economic and Clinical Health Act (2009), Pub. L. No. 111-5, sec. 13402.

Hernandez, Steven and Corey Schou. *Information Assurance Handbook: Effective Computer Security and Risk Management Strategies.* New York: McGraw-Hill Education, 2014.

Hill, David G. *Data Protection: Governance, Risk Management, and Compliance.* Boca Raton, FL: CRC Press, 2009.

Hillson, David. *The Risk Management Handbook: A Practical Guide to Managing Multiple Dimensions of Risk*. Philadelphia: Kogan Page, 2016.

Hoopes, John. *Virtualization for Security: Including Sandboxing, Disaster Recovery, High Availability, Forensic Analysis, and Honeypotting*. Burlington, MA: Syngress, 2008.

Howard, Rick. *Cyber Fraud: Tactics, Techniques and Procedures*. Chicago: Auerbach, 2009. Institute of Electrical and Electronics Engineers (IEEE). http://www.ieee.org (accessed September 17, 2010).

Hubbard, Douglas W. and Richard Seiersen. *How to Measure Anything in Cybersecurity Risk*. New York: John Wiley & Sons, 2016.

International Information Systems Security Certification Consortium (ISC)². http://www.isc2.org (accessed September 17, 2010).

Isaca. *CISM Review Manual*, 14th ed. Rolling Meadows, IL: Author, 2016.

Krause, Micki, and Harold F. Tipton. *Information Security Management Handbook*, 6th ed. (ISC)² Press. Chicago: Auerbach, 2007.

Kundra, Vivek. "Faster, Smarter Cybersecurity," The White House Blog, April 21, 2010. http://www.whitehouse.gov/blog/2010/04/21/faster-smarter-cybersecurity (accessed April 23, 2010).

Lauricella, Tom. "Investors Hope the '10s Beat the '00s," *The Wall Street Journal*, December 20, 2009. http://online.wsj.com/article/SB10001424052748704786204574607993448916718 (accessed April 16, 2010).

Loo, Jonathan et al. *Mobile Ad Hoc Networks*. Boca Raton, FL: CRC Press, 2011.

Mandia, Kevin et al. *Incident Response & Computer Forensics*, 3rd ed. New York: McGraw-Hill Education, 2014.

Marcella, Albert J., "Electronically Stored Information and Cyberforensics," *Information Systems Control Journal*, Vol. 5 (2008). http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=52106&TEMPLATE=/ContentManagement/ContentDisplay.cfm (accessed April 16, 2010).

Mason, Alex et al. *Sensing Technology: Current Status and Future Trends IV*. New York: Springer, 2014.

Meeuwisse, Raef. *Cybersecurity for Beginners*. Canterbury, UK: Author, 2015.

Mogollon, Manuel. *Cryptography and Security Services: Mechanisms and Applications*. London: Cybertech Publishing, 2008.

Moldovyan, Alex, and Nick Moldovyan. *Innovative Cryptography (Programming Series)*, 2nd ed. Rockland, MA: Charles River Media, 2006.

National Institute of Standards and Technology, SP 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," February 2010. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf (accessed May 21, 2010).

O'Toole, Darren. *Incident Management for IT Departments*. St. Albans, UK: Author, 2015.

Oriyano, Sean-Philip and Jim Doherty. *Wireless and Mobile Device Security*. Burlington, MA: Jones & Bartlett Learning, 2014.

Pearson, Brock and Tyler Wrightson. *Wireless Network Security A Beginner's Guide*. New York: McGraw Hill Professional, 2012.

"Risk Management Framework." EPCB Risk Management Consulting Services (n.d.). http:// www.emergencyriskmanagement.com/site/711336/page/248974 (accessed October 2, 2010).

Rose, Adam, and Linda S. Spedding. *Business Risk Management Handbook: A Sustainable Approach*. Oxford: Cima Publishing, 2007.

Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (codified as amended in scattered sections of U.S. Code Vol. 15).

Schneier, Bruce. *Applied Cryptography*. New York: John Wiley & Sons, 2015.

Senft, Sandra et al. *Information Technology Control and Audit*, 4th ed. Boca Raton, FL: CRC Press, 2012.

Shackleford, Dave. *Virtualization Security*. New York: John Wiley & Sons, 2012.

Sikorski, Michael and Andrew Honig. *Practical Malware Analysis*. San Francisco: No Starch Press, 2012.

Stallings, William. *Cryptography and Network Security*. Upper Saddle River, NJ: Prentice Hall, 2011.

Stallings, William. *Network Security Essentials*. Upper Saddle River, NJ: Prentice Hall, 2013.

Standards for Insuring the Security Confidentiality, Integrity and Protection of Customer Records and Information ("Safeguards Rule"), Code of Federal Regulations, Title 16, sec. 314.

Stoneburner, Gary, Alice Goguen, and Alexis Feringa. *Risk Management Guide for Information Technology Systems* (NIST SP 800-30). National Institute for Standards and Technology, 2002. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (accessed October 2, 2010).

Swenson, Christopher. *Modern Cryptanalysis: Techniques for Advanced Code Breaking*. New York: Wiley, 2008.

Tipton, Hal, Kevin Henry, and Steve Kalman, e-mail conversation with author, June 2008.

Tipton, Harold F. and Micki Krause Nozaki. *Information Security Management Handbook*, 6th ed. Boca Raton, FL: CRC Press, 2012.

Total Disaster Risk Management Good Practice. Asian Disaster Reduction Center, 2009. http:// www.adrc.asia/publications/TDRM2005/TDRM_Good_Practices/Index.html (accessed October 2, 2010).

U.S. Code Vol. 15, sec. 6801-6803.

U.S. Code Vol. 15, sec. 6801(b).

U.S. Code Vol. 15, sec. 7213m.

U.S. Code Vol. 15, sec. 7266.

U.S. Code Vol. 20, sec. 1232g.

U.S. Code Vol. 44, sec. 3542(b)(1).

U.S. Code Vol. 44, sec. 3544(a)(3)(A)(ii).

U.S. Government Accountability Office. *Federal Information System Controls Audit Manual*, 1999. http://www.gao.gov/special.pubs/ai12.19.6.pdf (accessed October 2, 2010).

U.S. Office of Management and Budget, Circular No. A-130, "Management of Federal Information Resources," December 2000. http://www.whitehouse.gov/omb/circulars_a130_a130trans4/ (accessed April 21, 2010).

U.S. Securities and Exchange Commission, "Information Matters," February 22, 2006, http://www.sec.gov/answers/infomatters.htm (accessed April 16, 2010).

Vacca, John R. *Computer and Information Security Handbook*. San Francisco: Morgan Kaufmann, 2013.

Valeriano, Brandon and Ryan C. Maness. *Cyber War Versus Cyber Realities*. New York: Oxford University Press, 2015.

Verizon Business, *2009 Data Breach Investigations Report*, April 15, 2009. http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf (accessed March 1, 2010).

VoIP Security Alliance. http://www.voipsa.org (accessed September 17, 2010).

Weiss, Martin and Michael G. Solomon. *Auditing IT Infrastructures for Compliance*. Burlington, MA: Jones & Bartlett Learning, 2015.

Wheeler, Evan. Security Risk Management. Burlington, MA: Syngress Press, 2011.

Whitman, M. E., and H. J. Matford *Principles of Incident Response and Disaster Recovery*. Boston: Course Technology, 2006, p. 492.

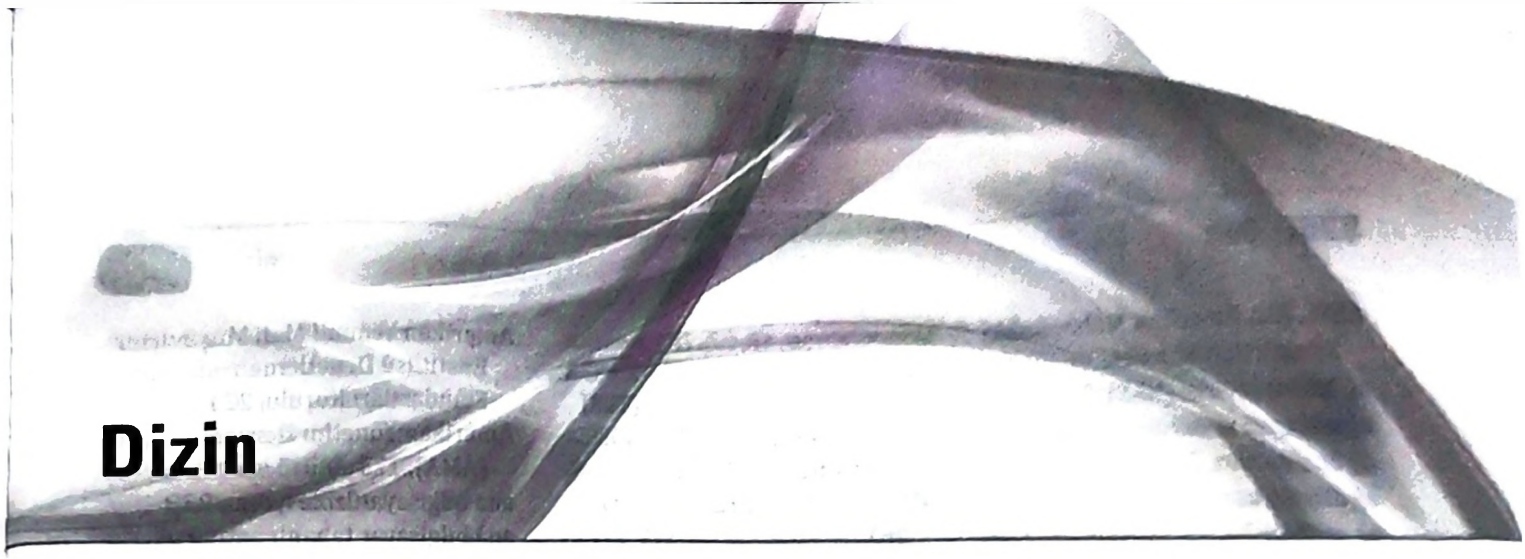
Williams, Barry L. *Information Security Policy Development for Compliance*. Boca Raton, FL: CRC Press, 2013.

Williams, Branden R. and Anton Chuvakin. *PCI Compliance*. Burlington, MA: Syngress Press, 2014.

Wood, Charles Cresson. *Information Security Policies Made Easy*. Baseline Software, Incorporated, 1997.

Wright, Craig S. *The IT Regulatory and Standards Compliance Handbook: How to Survive Information Systems Audit and Assessments*. Burlington, MA: Syngress, 2008.

Wright, Steve. PCI DSS: *A Practical Guide to Implementation*, 2nd ed. Rolling Meadows, IL: IT Governance Ltd, 2009.



Dizin

Not: f ve *t* ile gösterilen sayfa numaraları sırası ile şekil ve tabloları göstermektedir.

(ISC)² kendi temposu ile öğrenme, 417*t*
(ISC)². Bkz. Uluslararası Bilgi Sistemleri Güvenlik Sertifikasyon Konsorsiyumu
(KDC) sunucusu, 152
"abonelikten çık" linki, 86
"Binanın Kaybı" etki senaryoları, 119
"Binanın Kaybı" etki senaryoları, 119
"güvenilir yol" problemi, 148
"telefon-ev" yama yönetimi, 240
"telefon-ev" yama yönetimi, 240
1950 yılının Mühimmat Kontrol Yasası, 291
1987 Bilgisayar Güvenliği Yasası, 127, 426
1999 tarihli Finansal Hizmetleri Modernleştirme Kanunu, 467
20. yüzyıl kriptografisi,291–292
2000 yılı Devlet Bilgi Güvenliği Reformu Kanunu (Güvenlik Reform Kanunu), 127
2002 yılı Halka Açık Şirket Muhasebesi Reformu ve Yatırımcı Koruma Kanunu, 472
2003 yılının California Veritabanı Güvenlik İhlali Kanunu, 127
802.11 Kablosuz Güvenlik (Wi-Fi), 315–316

A

AAA sunucuları. *Bkz.* kimlik denetleme, yetkilendirme, ve izleme sunucuları
AaaS. *Bkz.* Hizmet olarak Herşey
ABD Anayasası'nın Birinci Yasa Değişikliği, 479
ABD askeri istihbarat ve taktikleri, 37
ABD Eğitim Bakanlığı, 476
ABD federal hükümeti veri sınıflandırma standartı, 43
ABD Gümrük ve Sınır Koruma (CBP), 141
ABD hükümeti sınıflandırması, 197
ABD NSA eğitim standartları, 436–437
ABD Personel Yönetimi Ofisi (OPM), 426
ABD Sağlık ve İnsani Hizmetler Bakanlığı (HHS), 461, 464
ABD Savunma Bakanlığı (DoD), 434–437, 443
ABD Savunma Bakanlığı Yönerge 8140, 434–435
ABD Savunma Bakanlığı Yönerge 8570.01, 434–437
ABD Ulusal Güvenlik Bakanlığı (DHS), 419
ABD Ulusal Güvenlik Bakanlığı (DHS), 435
ABD Ulusal Güvenlik Ajansı (NSA), 440
ABD uygunluk kanunları, 12–14, 14*f*, 452–487
ABD Vatanseverlik Kanunu 2001, 126
ABD'ye karşı Amerikan Kütüphaneciler Birliği, 479
ABE. Bkz. öznitelik tabanlı şifreleme
ACH. Bkz. otomatik takas merkezi
acil durum operasyon merkezi (EOC), 271
acil operasyonlar grubu, 183
aciliyet, 103
ACK mesajı, 370
ACLs. Bkz. erişim denetim listeleri
açık ağ, 329, 330
açık anahtar altyapısı (PKI), 148, 313
açık eylemler, 229
Açık Kimlik Denetleme için Girişim (OATH), 172
açık metin, 9, 9*f*, 17, 17*f*, 289
Açık Sistemler Ara Bağlantısı (OSI) Referans Modeli, 327–328, 399–400, 399f
Açık Sistemler Ara Bağlantısı'nın fiziksel katmanı, 328, 328f
Açık Sistemler Ara Bağlantısı'nın oturum katmanı, 327, 328f
Açık Sistemler Ara Bağlantısının Aktarım Katmanı, 328, 328f, 400
açık şifrelemeler, 290
açık yazılım programları, 371
açık/kamusal (asimetrik) anaktar şifreleme, 290
açık/kamusal anaktar, 290
açıklama/ifşa, 90–91, 462
açılır pencere, 102
açılır pencere, 102
adanmış internet erişimi, 29
Adil ve Doğru Kredi İşlem Kanunu (FACTA), 154–155
adli bilişim, 130
adres bağımlı (COA), 61
adres çözümleme protokolü (ARP), 94
adres yanıltması, 94
AES anahtar sarmalama özelliği, 322
AES. Bkz. Gelişmiş Şifreleme Standardı

AESC. Bkz. Amerikan Mühendislik Standartları Komitesi
ağ adresi çevirisi (NAT), 332
ağ altyapısı savunmaları, 389–390
ağ anahtarları, 26t
ağ arayüz kartı (NIC), 24
ağ ayırma, 342
ağ bağlantı noktası, 336
ağ erişim denetimi (NAC), 237, 347
ağ erişim sunucusu (NAS), 170
ağ güvenliği riskleri, 338–341
ağ güvenliği savunma araçları, 341–347
ağ güvenliği, 299t, 322, 326
ağ haritalama, 242, 244–247
ağ hizmet reddi, 340–341
ağ izleyicileri ve çözümleyicileri, 391
Ağ Katmanı şifreleme, 231
Ağ Katmanı, 328, 328f, 400
ağ keşfi, 339
ağ operasyon merkezi (NOC), 31
ağ protokolü, 333, 334
ağ saldırı tespit sistemi (NIDS), 234, 238
  güvenlik duvarı tamamlayıcısı olarak, 235f
ağ servisleri, 389
ağ ve ağ cihazları, 231
ağ yönetim yazılım paketleri, 383
Ağ Zaman Protokolü (NTP), 232
ağı gizlice dinleme, 339–340
ağı trafiğe boğma, 340
ağlar, 329–334
ağ-tabanlı antivirüs yazılımı, 391
AH. Bkz. kimlik denetleme başlığı
ahlaklı/etik bilgisayar korsanı, 79
A-I-C üçlüsü, 14
Aile Eğitim Hakları ve Mahremiyet Kanunu (FERPA), 14, 126, 455t, 476–478
Aile Politikası Uygunluk Dairesi (FPCO), 478
akıllı kartlar, 35, 36t, 138, 141, 148, 153
akıllı telefon, 10, 33, 34
akıllı uygulamalar, 377
akreditasyon, 207, 208
akredite edilmiş lisans programları, 418
aksama süresi, 18, 77–78
aksama, 270
Aktarım Katmanı Güvenliği (TLS) Yetkilendirme Uzantıları, 403
aktarım şifrelemesi, 293
aktarma, olumsuz risk yanıtları, 263
aktif içerik zafiyetleri, 367
aktif içerik, 367
aktif izinsiz dinleme yöntemleri, 85
aktif saldırı, 93, 96
aktif tehditler, 93–98
aktivite aşaması denetimi, 266
Alan Adı Sistemi (DNS) Güvenliği Uzantıları, 403
Alan Adı Sistemi (DNS) sunucu yazılımı, 372
alan adı, 98, 372–373
alan teorisi, 302
alan, 302
alarmlar ve uyarılar, 229–230
aldatmacalar, 87, 103, 373
ALE. Bkz. yıllık kayıp beklentisi
algılayıcı denetim, 234, 266
algoritmalar, 289
alındı, 296, 297t, 299t
alt ağ maskesi adresi, 24, 335
alt ağ, 335
alt küme toplamı problemi, 307
alt planlar, 457
alternatif işlem stratejileri, 283–285
altyapı değerlendirmeleri, 130
AMA. Bkz. Amerikan Yönetim Derneği
Amerika Birleşik Devletleri Standartları Enstitüsü (USASI), 406
Amerikan İnsan Hakları Birliği, 479
Amerikan Kütüphaneler Birliği, 479
Amerikan Merkez Bankası, 470
Amerikan Mühendislik Standartları Komitesi (AESC), 406
Amerikan Standartları Birliği (ASA), 406
Amerikan Ulusal Standartlar Enstitüsü (ANSI), 405, 406 t
Amerikan Yeminli Mali Müşavirler Enstitüsü Denetleme Standartları Kurulu, 221
Amerikan Yönetim Derneği (AMA), 173
ana bilgisayar izolasyonu, 238
ana bilgisayar tabanlı antivirus yazılımı, 391
ana bilgisayar tabanlı etkinlik, 231
ana bilgisayar tabanlı saldırı tespit sistemi (HIDS), 230, 234–235, 237, 238
ana bilgisayar, 258
ana önyükleme kayıt virüsleri, 357–358
ana önyükleme kayıt/önyükleme sektörü virüsleri, 362
anahtar çiftleri, 304, 305
anahtar dağıtım merkezleri (KDC), 310–311
anahtar dağıtımı, 310
anahtar dizini, 317
anahtar emaneti, 317
anahtar kelime karıştırılmış alfabe şifrelemesi, 301
anahtar uzayı, 290, 308–311
anahtar yönetimi, 309, 321–323
anahtarın iptal edilmesi, 317
anahtarlamalı ağlar, 231, 333–334
anahtarlar, 288, 308–311
anahtarlar, 333–334
anahtarları bölme, 310
anahtarların kağıt olarak dağıtımı, 310
anahtar-şifreleme anahtarı, 303, 310
analiz yöntemleri, 236
analog telefon hatları, 34
anasayfa ele geçirme, 374
Android işletim sistemi, 59, 258
Angry IP Scanner, 384
Animal (Trojan), 100
anketler, 226
anlaşmaların işlenmesi, 284
anlık mesajlaşma (IM) sohbeti, 33
anomali tespiti, 391
anomali-tabanlı saldırı tespit sistemleri, 236
anonimlik, 296, 297t, 299, 299t
ANSI X9.17, 310, 323

ANSI. Bkz. Amerikan Ulusal Standartlar Enstitüsü
anten, türleri ve yerleşimi, 350
anti-malware pragramları, 97, 107
anti-malware ürünleri, 107
anti-spam üreticisi, 364
antivirüs program değerlendirmesi, 241
antivirüs taraması, 21*t*, 23*t*, 391
antivirüs yönetimi, 129
AO. Bkz yetkilendiren makam
AOC. Bkz. uygunluk onayı
Apple, 59
APWG. Bkz. Oltalama Dolandırıcılığını Önleme Çalışma Grubu
ara bellek taşması, 81, 100, 105, 168, 363
ara bellek taşması, 81, 100, 105, 168, 363
arabulucu program, 163
aracı, 369–370
araç setleri, 313
arama motoru optimizasyonu (SEO), 50, 56
Araştırmada Akademik Mükemmellik Ulusal Merkezleri (CAE/R) programı, 419
araya girme, 104
Arındırılmış bölge (DMZ), 27, 238, 344, 392
arıza için ortalama süre (MTTF), 18
arızalar arasındaki ortalama süre (MTBF), 18
arka kapı programları, 375
arka kapılar, 85
ARO. Bkz. yıllık gerçekleşme oranı
ARP. Bkz. adres çözümleme protokolü
artakalan risk, 264–265, 265f
artan yedekleme, 276
AS. Bkz. kimlik denetleme sunucusu
ASA. Bkz. Amerikan Standartları Birliği
asenkron belirteçler, 146–148
asenkronize kimlik sorma-karşılık verme oturumu, 147
asimetrik anahtar, 291, 304–305, 307–308, 316–318
asimetrik kriptosistem, 320
ASPs. Bkz. uygulama servis sağlayıcıları
ASV. Bkz. onaylı tarama sağlayıcısı
Atama Görevleri Standartlarına İlişkin Açıklamalar No.16 (SSAE 16), 222
Denetleme Standartları No.70 (SAS 70), 221–222
denetlemeler, 222
AUP. Bkz. kabul edilebilir kullanım politikası
AV. Bkz. varlık değeri
AVG Anti-Virüs, 107
Avira AntiVirüs, 107
Avrupa Telekomünikasyon Standartları Komitesi (ETSI), 406–407
avuç içi izi, 149
ayrıcalıklı olay günlükleri, 224
ayrıcalıklı olay işleme, 280
ayrıcalıklı olay yönetme, 277–280
ayrıcalıklı olay, 253, 459
ayrıcalıklı olaya yanıt, 457
ayrım gözetmeyen izin seviyesi, 219
azaltma, olumsuz risk yanıtları, 130, 263

B

B2B. Bkz. işletmeden işletmeye
B2C. Bkz. işletmeden müşteriye
bağımsız disklerin yedek dizisi (RAID), 122, 272
bağlam filtreleme, 391–392
bağlama, 165
bağlam-tabanlı sistem, 159
bağlantı noktası eşleme araçları, 384, 385f
bağlantı noktası eşleme araçları, 384, 385f
bağlantı noktası güvenliği, 342
bağlantı noktası güvenliği, 342
bağlantı noktası tarama uygulamaları, 384, 385f
Bağlantı noktası, 33
bağlantı noktası/port tarayıcıları, 80
bağlantı seçenekleri, 330–331
bağlantı şifreleme, 293
bakım, 204, 210f
bakımı, 31
bal ağı, 392
bal küpü, 392
Baldridge Ulusal Kalite Programı, 397
balina avı, 103
bant dışı anahtar değişimi, 294
bant içi anahtar değişimi, 294
basit ağ yönetim protokolü (SNMP), 31, 383–384, 385f
basit bütünlük aksiyomu, 164
Basit Posta Transfer Protokolü (SMTP), 392
basit yerine koyma şifrelemesi, 301
başarısızlıkları denetleme, 145, 146
başlangıç noktası, 380
başlıca erişim numarası (PAN), 464
başlık manipülasyonu, 105, 374
BCM. Bkz. iş sürekliliği yönetimi
BCP. Bkz. En İyi Mevcut Uygulama: iş sürekliliği planı
beceri seti uygulamalı laboratuvarları, 415
beklenmedik durum/olay planları, 227t, 272, 460, 465t, 486, 487
beklenmedik olay taşıyıcıları, 284–285
belirteç, 35, 36t
bellek bölümleme, 131
Bell-La Padula Modeli, 164
Berners-Lee, T., 401
betik/komut dosyası çocuğu, 79
beyaz kutu testi, 248
beyaz liste, 388
beyaz şapkalı bilgisayar korsanı, 79
beyin fırtınası tekniği, 256
BHO Trojan/Truva atı programı. Bkz. tarayıcı yardımcı nesnesi Trojan/Truva atı programı
BIA. Bkz. iş etki analizi
Biba Bütünlük Modeli, 164–165
bildirim, 278
bilet-onaylama sunucusu (TGS), 152

Bilgi Güvenliği Eğitiminde Ulusal Akademik Mükemmellik Merkezleri (CAE/IAE) programı, 419
bilgi güvenliği açığı, 123–124, 254
bilgi güvenliği ayrıcalıklı olay yönetimi, 409
bilgi güvenliği başkanı (CISO), 457
bilgi güvenliği eğitim programları, 425–430
bilgi güvenliği hedefleri, 296, 297*t*, 298
bilgi güvenliği ilkeleri, 127, 128*f*
bilgi güvenliği kontrolü, 464
bilgi güvenliği mesleki sertifikasyonlar, 433–449
bilgi güvenliği organizasyonu, 408
bilgi güvenliği risk yönetimi, 123*t*, 252–255
bilgi güvenliği savaşı, 10
bilgi güvenliği uygunluğu, 486–487, 487*t*
bilgi güvenliği, 292–295, 456
bilgi sınıflandırma amaçları, 197
Bilgi Sistemleri Denetim ve Kontrol Birliği (ISACA), 225, 443, 444*t*
bilgi sistemleri güvenliği, 3–14, 456
Bilgi Sistemleri Güvenlik Mimarisi Uzmanı (ISSAP), 440
Bilgi Sistemleri Güvenlik Mühendisliği Uzmanı (ISSEP), 440
Bilgi Sistemleri Güvenlik Yönetimi Uzmanı (ISSMP), 440
bilgi sistemleri kazanımı geliştirme ve bakım, 409
bilgi sistemleri, 11
bilgi sistemlerini kategorilere ayırma, 460
Bilgi Teknolojisi Altyapı Kütüphanesi (ITIL), 225
Bilgi Teknolojisi Sistemleri için Risk Yönetimi Rehberi, 123
Bilgi ve İlgili Teknolojiler için Denetim Amaçları (COBIT), 225
bilgi, 142
bilginin değeri, 196
bilginin hassasiyeti, 196
bilginin kritikliği, 196
bilgisayar korsanları, 78–79, 143
bilgisayar sistemleri için güvenlik izleme, 230–231
günlük tutma anomalileri, 232
günlük yönetimi, 232–233
sorunlar, 231–232
bilgisayar uygulamaları, 379
bilgisayar virüsleri, 99, 356–363, 357*f*
bilinen düz metin saldırısı (KPA), 306, 306f
bilinen kaynaklar, 415
bilinmesi gereken, 158, 189, 204
birden fazla ürün, 415
Birinci Yasa Değişikliği hakları, 479, 480
birincil güvenlik kontrolü, 234
Birleşik Devletler Bilgisayar Acil Hazırlık Takımı (US-CERT), 107, 459
birleşik iletişim (UC), 10
birleşik mesajlaşma (UM), 52
birleşik şifreleme, 302
birleşik tehdit yönetimi (UTM), 345
birleştirilmiş erişim, 152
BitDefender, 107
bitirme sertifikası, 416, 418
biyometrik cihazların doğruluğu, 148
biyometrik cihazların tepki süresi, 149
biyometrik ölçümlerin kabul edilebilirliği, 149
biyometrik parmak izi okuyucu, 35
biyometrik teknolojilerin mahremiyet sorunları, 151
biyometrikler, 141, 148, 150
BlackBerry cihazları, 33, 34
Blaster solucanı, 365–366
Blok şifreleme, 297
Blowfish şifreleme, 314
bluejacking, 104
bot-çobanı/bot-herder, 369
boyut gizliliği, 360, 361
bölge aktarımı, 244
bölümlere ayrılmış bilgi, 197
BPA. Bkz. sonu açık sipariş sözleşmesi
BPA. Bkz. sonu açık sipariş sözleşmesi
brain virüsü, 376
Brewer ve Nash bütünlük modeli, 165–166, 166*f*
Brewer ve Nash bütünlük modeli, 165–166, 166*f*
brute-force/kaba kuvvet saldırıları, 93, 143, 290
BT altyapısı, 19–38, 20*f*, 33, 38–40, 75–76, 75*f*
BT fiziksel güvenlik, 267–268
BT güvenlik politika altyapısı, 192–196, 192*f*, 193*f*
BT güvenlik politika çerçevesi, 16, 40–42, 41*f*
BT sistemleri, 460
BT ve ağ altyapısı, 75–76, 75*f*
BT Yönetim Enstitüsü (ITGI), 225
bulaşma, 386
bulguların sunumu, 229
bulut bilişim, 174–176
Bulut Güvenliği Birliği (CSA), 176, 440
bulut servis sağlayıcısı (CSP), 175
bütünlük, 14, 17, 18f, 127, 293, 295, 354, 378, 408, 486, 487*t*

C - Ç

CA. Bkz. Sertifika yetkilisi
CAP. Bkz. Sertifikalı Yetkilendirme Uzmanlığı
CAST algoritması, 314
casus yazılım çerezleri, 372
casus yazılım, 101–102, 371–372
casusluk, 91
caydırıcı denetim, 266
CBF. Bkz. Kritik iş fonksiyonu
CBK. Bkz. Ortak Bilgi Tabanı
CCFP. Bkz. Sertifikalı Siber Adli Bilişim Uzmanlığı
CCSP. Bkz. Sertifikalı Bulut Güvenlik Uzmanlığı
CCTA Risk Analizi ve Yönetimi Metodu (CRAMM), 123, 123*t*
cep telefonları, 34
cep telefonu hizmeti, 33
CER. Bkz. Çapraz hata oranı
CERT Koordinasyon Merkezi, 94
CGEIT. Bkz. Kurumsal BT Yönetiminde Sertifikalı

CHAP. Bkz. Meydan Okuma-El Sıkışma Kimlik Denetleme Protokolü
CHD. Bkz. kart sahibi verisi
Check Point sertifikaları, 449, 449*t*
Christmas (Xmas) saldırısı, 94
CIA üçlüsü, 408–409
CIA. Bkz. gizlilik, bütünlük, ve kullanılabilirlik
CIPA. Bkz. Çocukların İnternetten Korunması Kanunu
CISA. Bkz. Sertifikalı Bilgi Sistemleri Denetçisi
CISM. Bkz. Sertifikalı Bilgi Güvenliği Yöneticisi
CISO. Bkz. bilgi güvenliği başkanı
CISSP. Bkz. Sertifikalı Bilgi Sistemleri Güvenlik Profesyoneli
CIW. Bkz. Sertifikalı İnternet Web Yöneticisi
cihaz erişm denetim, 131
cihaz güvenliği, 130–131
Cisco Sistemleri sertifikaları, 108, 446*t*
Clark–Wilson bütünlük modeli, 165
CMS. Bkz. İletişim Güvenliği Malzeme Sistemi
CNSS. Bkz. Ulusal Güvenlik Sistemleri Komitesi
COA. Bkz. adres bağımlı
COBIT. Bkz. Bilgi ve İlgili Teknolojiler için Denetim Amaçları
Code Red solucanı, 374, 377
Cohen, Fred, 376
CompTIA, 441, 443
control hedefleri, 410, 481
COPPA. Bkz. Çocukların Çevrimiçi Mahremiyetini Koruma Kanunu
COSO. Bkz. Sponsor Kuruluşları Komitesi
CPD. Bkz. sürekli mesleki gelişim
CPE değeri. Bkz. sürekli mesleki eğitim değeri
CRAMM. Bkz. CCTA Risk Analizi ve Yönetimi Metodu
creeper virüsü, 99
CRISC. Bkz. Risk ve Bilgi Sistemleri Kontrolünde Sertifikalı
CRM. Bkz. müşteri ilişkileri yönetimi
CSA. Bkz. Bulut Güvenliği Birliği
CSMA/CD. Bkz. taşıyıcı duyarlı çoklu erişim/çarpışma tespiti
CSP. Bkz. bulut servis sağlayıcısı
CSSLP. Bkz. Sertifikalı Güvenli Yazılım Yaşam Döngüsü Uzmanlığı
Cybrary, 417*t*
çakışmalar, 275
çalışanlar, 379
çalışma süresi, 18
çapraz hata oranı (CER), 149
çapraz site betikleme (XSS), 105, 368
çerezler, 87–88, 105, 371–372
Çevik Yazılım Geliştirme için Manifesto, 211–212, 212f
çevik yazılım geliştirme yöntemi, 211–212, 212*f*
çevirmeli erişim altyapısı, 386
çevresel masraf, 269
çıkar çatışması, 166
çıkarılabilir depolama, 131
çıkış mülakatı, 228
çift taraflı merkez, alternatif
Çin Seddi güvenlik politikası, 165
Çocukların Çevrimiçi Mahremiyetini Koruma Kanunu (COPPA), 126–127
Çocukların İnternetten Korunması Kanunu (CIPA), 13, 455*t*, 478–480
çoğal ve ekle davranışı, 358
çok biçimli kötücül yazılım, 76
çok biçimli kötücül yazılım, 76
çok biçimli virüs, 360, 360f
çok biçimli virüs, 360, 360f
çok bölgeli WAN bulut servisleri, 29
çok bölümlü virüs, 362, 362f
çok gizli kategorisi, 197
çok gizli veri, 43
çok katmanlı güvenlik duvarı firewall, 344–345
çoklu kiracılı, 164
çoklu protokol etiket anahtarlama (MPLS), 29, 30
Çok-Sağlayıcılı Bir Ortamdaki Uygulamalar için Güvenli Avrupa Sistemi (SESAME), 153

D

DAC. Bkz. isteğe bağlı erişim denetim
dağıtık hizmet reddi (DDoS) saldırıları, 84, 340
dağıtım kutuları, 333–334
daha geniş strateji, 119
daha geniş strateji, 119
Danışmalı Kontrol ve Veri Toplama Sistemi (SCADA), 258
Dark Avenger virüsü, 376
davranışsal biyometrikler, 148
dayanak noktası yapılandırması, 240
dayanaklar, 195–196, 195*f*, 229, 240
DDoS saldırıları. Bkz. dağıtık hizmet redid saldırıları
Deep Crack, 302
değerlendirme güvence seviyeleri (EAL), 206
değişiklik denetim komiteleri, 201–202
değişiklik denetim problemleri, 203
değişiklik denetim prosedürleri, 202, 202*f*
değişiklik denetimi, 200, 200*f*
değişiklik yönetim süreci, 200–203
değişiklikler, 93
değişikliklerin gözden geçirilmesi, 201
değiştirme tehdidi, 91–92
Delphi metodu, 115, 256
denetçi, 223–224, 227
denetim günlükleri, 233
denetim raporuna yönetim yanıtı, 228–229
denetimler, 254
denetimli alt ağ, 344, 344f
denetimli sınıflandırılmamış bilgi, 43
denetleme kapsamı, 223–224, 224f
denetleme karşılaştırmalı değerlendirme, 224–225

denetleme planı, 223–224, 227*t*
denetleme raporu, 228–229, 474
denetleme raporunun, 228
denetleme sıklığı, 221
denetleme sonrası faaliyetler veri analizi, 228
bulguların sunulması, 229
çıkış mülakatı, 228
denetleme raporunun oluşturulması, 228–229
denetleme süreci, 226
denetleme veri toplama yöntemleri, 226–227
denetlemeler, 183, 197, 216, 218, 220, 221, 475
depolama alan ağı (SAN), 122
depolama, 37
derinlemesine savunma (DiD), 155
derinlemesine savunma, 22, 387, 390
DES. Bkz. Veri Şifreleme Standardı
destek mülkiyeti, 129
DHCP. Bkz. Dinamik Ana Bilgisayar Yapılandırma Protokolü
DHE. Bkz. Ephemeral modunda Diffie-Hellman
DHS. Bkz. ABD Ulusal Güvenlik Bakanlığı
DIAMETER, 170–171
DISA. Bkz. Savunma Bilgi Sistemleri Ajansı
dışarıda gerçekleştirilen analiz, 228
dışlamalı VEYA fonksiyonu, 302, 309
DiD. Bkz. derinliğine savunma
diferansiyel kriptanaliz, 302
diferansiyel yedekleme, 276
Diffie-Hellman algoritması, 292
digavsing/mıknatıslanmanın giderilmesi, 206
dijital abone hattı (DSL) hizmeti, 330
dijital anahtar dağıtımı, 310
dijital imza algoritması (DSA), 312, 319*f*
dijital imzalar, 311–312, 312*f*
dijital medya, 47, 310
dijitalleştirilmiş imza, 311–312, 312*f*
Dinamik Ana Bilgisayar Yapılandırma Protokolü (DHCP), 335, 336*f*
dizin bilgisi, 477
dizüstü VPN istemci yazılımı, 34
DLP. Bkz. veri kaybını önleme
DMZ. Bkz. arındırılmış bölge
DNS Güvenliği Uzantıları. Bkz. Alan Adı Sistem Güvenliği Uzantıları
DNS sunucu yazılımı. Bkz. Alan Adı Sistemi sunucu yazılımı
DNS sunucuları, 98, 372
DNS zehirlenmesi, 98
DoD eğitim standartları, 436–437, 437*t*
DoD. Bkz. ABD Savunma Bakanlığı
doğru biçimlendirilmiş işlem, 165
doğrudan maliyetler, 117, 284
doğrudan saldırılar, 381–382, 381*f*
doğum günü saldırısı, 93
doktora derecesi, 424–425, 425*t*
dokümantasyon, 183, 203, 223, 226, 280
dokümantasyonu, 119–120, 280
dolaylı maliyetler, 117
dolaylı saldırılar, 382
domains of IT infrastructure, 19–38, 20*f*, 75–76, 75*f*, 90*t*
donanım anahtar dağıtımı, 310
donanım denetimleri, 156*t*
donanım envanteri, 199–200
donanım konfigürasyon çizelgesi, 199
DoS saldırıları. Bkz. hizmet redid saldırıları
DoS tehditleri, 92
DoS. Bkz. Hizmet Reddi
dosya (program) virüsleri, 358–359, 359*f*
Dosya Aktarım Protokolü (FTP), 26–27
dosya sunucusu ve yazdırma sunucusu, 24
dosya virüsleri, 357–359, 376
DRP. Bkz. felaket kurtarma planı
DRP'nin önleyici bileşenleri, 122
DS. Bkz. Taslak Standart
DSA. Bkz. dijital imza algoritması
DSL hizmeti. Bkz. dijital abone hattı hizmeti
durağan ortam, 258–259
durum denetimi güvenlik duvarı, 342
durum kontrolü, 347
durum, 164
duruma dayalı eşleme, 236
düşük-katılımlı bal küpleri, 392
düz metin, 288, 289
düzeltici denetimler, 266
düzensiz davranışı yakalama, 230

E

EAL. Bkz. değerlendirme güvence seviyeleri
EAP. Bkz. Genişletilebilir Kimlik Denetleme Protokolü
ECDHE. Bkz. Eliptik Eğri DHE
Eddie6 virüsü, 376
EDI. Bkz. elektronik veri değişimi (EDI)
Edmonds Community College, 421*t*
EF. Bkz. maruz kalma faktörü
efsaneler, 373
Egghead Yazılım, 168
eğilimler, 229–230
eğitim, 415, 427
eğitim, NIST SP 800-50, 427
eğitmen tarafından yönlendirilen programlar, 416–418
e-işletme stratejisi, 56–57, 57*f*
ek materyaller, 413
eke geçirme, 94–95
Ekonomik Kalkınma ve İşbirliği Örgütü (OECD), 188
Ekonomik ve Klinik Sağlık için Sağlık Bilgisi Teknolojisi Kanunu (HITECH) Act, 461, 463, 466
ekran kilitleri, 131
el geometrisi, 149
Elektrik ve Elektronik Mühendisleri Enstitüsü (IEEE), 24, 403–404, 404*t*
elektronik izleme, 173
elektronik korunan sağlık bilgisi (EPHI), 464
elektronik olarak gizlice dinleme, 167

elektronik posta bombası, 359
elektronik veri değişimi (EDI), 76
elektroteknoloji, 400
Eliptik Eğri DHE (ECDHE), 292
Eliptik eğri kriptografisi (ECC), 297
Elk Cloner virüsü, 376
elle yapılan/manuel testler, 216
en düşük erişim hakkı prensibi, 189
en düşük erişim hakkı, 158
En İyi Mevcut Uygulama (BCP), 402
engellemeler, 92
Enigma (Alman şifreleme makinesi), 291
enjeksiyon teknikleri, 368–369
envanter kontrolü, 131
envanter, 131, 457
EOC. Bkz. acil durum operasyon merkezi
Ephemeral modunda Diffie-Hellman (DHE), 292
EPHI. Bkz. elektronik korunan sağlık bilgisi
e-posta içerik filtresi ve karantina sistemi, 28
e-posta solucanları, 377
e-posta, 32–34
EPP. Bkz. Genişletilebilir Hazırlama Protokolü
E-Rate programı, 479
erişim denetim ihlalleri, 166–167
erişim denetim listeleri (ACL), 139, 160–161, 162f, 342
erişim denetimler, 23 t, 24, 25, 137–140, 157, 184, 298, 407, 408
erişim günlükleri, 233
erişim kontrol merkezileştirme, 168–169
erişim kontrolü ihlalleri, 166–167
erişim ve ayrıcalık yükseltmesi, 386–387
erişimn denetlenmesi, 182
erteleme, 414
ESET Nod32 Antivirüs, 107
ESP. Bkz. kapsüllenen güvenlik yükü
eşik, 145
eşlik eden virüs, 359
Ethernet ağları, 332–333
Ethernet üzerinden Fiber Kanal (FCoE), 333
Ethernet, 24
e-ticaret, 2, 14, 55–57, 68–69
e-ticaret, fiziksel işletmeler, 55–57
etik kurallar, 188
etik, 40, 188
etki değerlendirmesi, 202
etki, 119, 253, 262–263, 262f
etkileşim eksikliği, 414
etkin risk yönetim süreci, 122, 123t, 255–270, 255f
EULA. Bkz. son kullanıcı lisans sözleşmesi
ev etmeni (HA), 61
evrak çantası anahtar uzayı, 308
eylemler, 140, 141

F

faaliyetleri azaltma, 243
FACTA. Bkz. Adil ve Doğru Kredi İşlem Kanunu
Fair Isaac Corp. (FICO) kişisel kredi notu, 15
FAR. Bkz. yanlış kabul oranı
fark analizi, 123, 275, 276
farkındalık, 191, 427
farklar, 275
FCC. Bkz. Federal İletişim Komisyonu
FCoE. Bkz. Ethernet üzerinden Fiber Kanal
FDIC. Bkz. Federal Deposit Insurance Corporation
federal ayrıcalıklı olaya yanıt merkezi, 459
Federal Bilgi Güvenliği Modernizasyon Yasası (FISMA), 13, 125–126, 458–459
Federal Bilgi Güvenliği Yönetim Yasası (FISMA), 12, 125, 456
Federal Bilgi İşleme Standartları (FIP), 290, 302, 319, 459
Federal Finansal Kurumlar İnceleme Konseyi (FFIEC), 67, 125
Federal İletişim Komisyonu (FCC), 479, 480
Federal kanunlar, 221
Federal Mevduat Sigorta Fonu (FDIC), 470
Federal Ticaret Komisyonu (FTC), 98, 468, 469f, 470
felaket değerlendirmesi, 183
felaket kurtarma ekibi, 120, 280
felaket kurtarma için veri merkezi seçenekleri, 121
felaket kurtarma için veri merkezi, 121t, 284t
felaket kurtarma planı (DRP), 11, 38, 39t, 118–122, 253, 270, 280, 281
felaket kurtarma, 120–122, 121t, 183, 280–285, 284t
felaketten kurtarma, 282
fen bilimleri yüksek lisansı, 421–422, 423t
FERPA. Bkz. Aile Eğitim Hakları ve Mahremiyet Kanunu
FFIEC. Bkz. Federal Finansal Kurumlar İnceleme Konseyi
FIP. Bkz. Federal Bilgi İşleme Standartları
fırsat maliyeti, 78
FISMA. Bkz. Federal Bilgi Güvenliği Modernizasyon Yasası
fiber kanal, 333
fidye yazılımı, 75, 363
fikri mülkiyet (IT), 74, 76
finans ve finansal veri, 36, 74, 76–77
finansal kuruluşlar, 471
finansal raporlamalar üzerindeki iç kontroller (ICFR), 222t, 473
finger aracı, 383
fiziksel anahtarlar, 308
fiziksel biyometrikler, 148
fiziksel denetimler, 156t
fiziksel erişim denetimler, 138
fiziksel erişim, 37, 167
fiziksel imha, 206
fiziksel iş modelleri, 55–58
fiziksel olarak kısıtlanmış kullanıcı ara yüzleri, 164
fiziksel tedbirler, 464, 465t
fiziksel ve çevresel güvenlik, 407, 408
fiziksel güvenlik, 227t, 267–268
flash çerezleri, 105, 372
Forensic Toolkit (FTK), 143

Form5 yükleme sektörü virüsü, 376
FPCO. Bkz. Aile Politikası Uygunluk Dairesi
FRR. Bkz. yanlış reddetme oranı
FTC Tedbirler Kuralı, 471
FTC. Bkz. Federal Ticaret Komisyonu
FTP. Bkz. Dosya Aktarım Protokolü
fuzzing, 205

G

G DATA Antivirüs, 107
garanti koşulları, 12
gauss, 400
Geçici Anahtar Bütünlüğü Protokolü (TKIP), 349
geçici ayırma, 159–160
geçici işlem stratejileri, 283–285
geçiş fonksiyonları, 164
geçişli güven, 152
geleneksel eğitim programları, 425
geleneksel sınıflar, 418
Gelişmiş Şifreleme Standardı (AES), 315
genel bulut, 174
genel güvenlik bilgisi, 414
geniş alan ağları (WAN), 19, 329–332, 329*f*
bağlantı seçenekleri, 330–331
yönlendiriciler, 331–332
geniş bant Wi-Fi İnternet erişimi, 33
geniş bant Wi-Fi İnternet erişimi, 33
geniş bant, 29–31
geniş bant, 29–31
geniş kapsamlı kural, 466–467
Genişletilebilir Hazırlama Protokolü (EPP), 403
genişletilebilir işaretleme dili (XML), 323
Genişletilebilir Kimlik Denetleme Protokolü (EAP), 347
Genişletilmiş Terminal Erişim Denetleyici Erişim Denetim Sistemi (XTACACS), 170
gerçek kesinti maliyeti, 78
gerçek zamanlı erişim, 33
gerçek zamanlı iletişimler, 10, 52
gerçek zamanlı izleme, 244
gerçek zamanlı olmayan izleme, 230
gerçekleştirim, 204, 204*f*, 207, 269
gereken özen, 270
gerekli olmayan hizmetler, 240, 389
gerekli olmayan servisleri etkisiz hale getirme, 240
gereksinimler, 482–486
gereksinimleri, 475
gerilim koruyucular, 122
GIAC Güvenlik Uzmanı (GSE), 441
GIAC. Bkz. Küresel Bilgi Güvenliği Sertifikası
giriş seviyesi, Cisco sertifikaları, 446*t*
gizli anlaşma, 158
gizli engelleme, 342
gizli eylemler, 244–247
gizli kanallar, 158
gizli olmayan test uzmanları, 244–247
gizli testler, 244–247
gizli veri, 42, 43, 127–128
gizli veri, 43
gizli virüs, 360, 361f
gizli, 127–128
gizlice dinleme, 96, 167, 339–340
gizlilik, 14, 16–17, 127, 293, 295, 354, 378, 408, 478, 481, 486, 487*t*
gizlilik, bütünlük, ve kullanılabilirlik (CIA), 56, 62
GLBA Privacy Rule, 470–471
GLBA Safeguards Rule, 471–472
GLBA. Bkz. Gramm-Leach-Bliley Kanunu
gömülü sistem, 258
görev tabanlı erişim denetimi, 159
görev tabanlı izinler, 159
görevler ayrılığı, 158, 189
görevler ayrılığı, 158, 189
görünüm tabanlı erişim denetim (VBAC), 164
gözlem, denetleme için veri toplama yöntemleri, 226–227
GPO. Bkz. Grup Politikası Nesnesi
GPS. Bkz. küresel konumlama sistemi
Gramm-Leach-Bliley Kanunu (GLBA), 13, 126, 455t, 467–472, 469f
gri kutu testi, 248
gri şapka bilgisayar korsanları, 79
Grup Politikası Nesnesi (GPO), 169
Grup Politikası, 169
grup üyelik politikası, 140
Grup-tabanlı izinler, 159
GSE. Bkz. GIAC Güvenlik Uzmanı
günün belirli saati kısıtlamaları, 160
Güvenli Bilgisayar Sistem Değerlendirme Kriterleri (TCSEC), 158
Güvenli Hiper Metin Aktarım Protokolü (HTTPS), 17, 34, 317
Güvenli Soket Katmanı (SSL), 35, 293, 317, 346
tokalaşma, 317
güvenli soketler katmanı sanal özel ağ (SSLVPN), 30
Güvenlik Bildirim Biçimlendirme Dili (SAML), 171
güvenlik bilgi ve olay yönetim (SIEM) sistemi, 28, 233–234
güvenlik parametresi endeksi (SPI), 322
güvenlik testi ipuçları ve teknikleri, 248
güç seviyesi kontrolleri, 350
güçlendirilmiş yapılandırma, 239
güçlü parolalar, 144
günlük bilgisi, 233–234
günlük dosyaları, 154, 232, 233
günlük kaydı analizi, 342
günlük kayıtları, 224, 233, 233
günlük tutma anomalileri, 232
günlük tutma yazılımı, 391–392
günlük yönetimi, 232–233
güven, 103
güvence, 198
güvenilir işletim sistemleri (TOS), 140
güvenilirlik, 330, 335
güvenli kablosuz ağ, 347–348
Güvenli Kabuk (SSH), 27, 293
Güvenli Özet Algoritması (SHA), 312

Güvenli Özet Algoritması (SHA-1), 319
güvenli tarayıcı yazılımı, 34
güvenli yönlendirici yapılandırması, 332
güvenliği atlama, 167
güvenliğin dış kaynaklardan edinilmesi, 184–185
ilgili hususlar, 184–185
olumlu yanları ve olumsuz yanları, 184
güvenlik açığı tarayıcısı, 80–81
güvenlik birliği (SA), 322
güvenlik çekirdeği veritabanı, 139
güvenlik çekirdeği, 139–140
güvenlik denetleme/analiz, 216, 220
denetlemelerin amacı, 220–221
güvenlik denetimlerinin adresledikleri
güvenlik denetleme alanı, 220
izin seviyeleri, 219–220
kabul edilebilirin belirlenmesi, 219
müşteri güveni, 221–222
risk, 218
güvenlik duruşu, 229
güvenlik duvarı kuralları, 342
güvenlik duvarı yerleştirme teknikleri, 343–345
güvenlik duvarları, 97, 108, 313, 341–345
güvenlik eğitimi, 190, 425–430, 428t
personel güvenliği prensipleri, 190
güvenlik farkı, 123, 275, 276
güvenlik farkındalığı eğitimi, 21t, 23t, 32t, 428–430, 457
güvenlik farkındalığı kampanyası, 428
güvenlik farkındalığı politika, 42
güvenlik farkındalığı programı, 190–191
güvenlik gözden geçirme döngüsü, 219f
güvenlik günlük dosyaları, 233
güvenlik hedefleri, 295, 296, 299t
güvenlik ihlali, 83–88, 379
ek güvenlik zorlukları, 86–88
arka kapılar, 85
dağıtık hizmet reddi
hizmet reddi saldırısı, 83–84
saldırısı, 84
telefon dinleme, 85
veri değişiklikleri, 86
web'de uygunsuz gezinme davranışları, 84–85
güvenlik incelemesi, 218
güvenlik izinleri, 161
güvenlik kontrolleri, 16, 35, 36, 155, 156t, 460
doğrulama
ana bilgisayar izolasyonu, 238
analiz yöntemleri, 236
antivirüs yazılımları değerlendirme, 241
HIDS, 237
katmanlı savunma, 237
kontrol denetlemeleri, 238
saldırı tespit sistemi (IDS), 234–236
sistem güçlendirme, 238–240
risk, 218–219
güvenlik kontrollerinin uygulanması, 460
güvenlik kuruluşları, 408
güvenlik olay müdahale ekipleri (SIRT), 106
güvenlik önlemi, 296
güvenlik politikaları, 123, 192–194, 192f, 193f, 219, 229, 407, 408
güvenlik politikası hiyerarşisi, 193f
güvenlik politikası ortamı, 192
güvenlik programı, 229
güvenlik testi için yol haritası road map for security testing, 242–243
güvenlik testi, 242f, 243f
güvenlik testinin yapılması, 226
güvenlik yönetim firması, 184
güvenlik yönetimi, 182–185
belgeleme, prosedürler, erişimin denetlenmesi, 182
felaket değerlendirmesi ve genel bakış, 181
kurtarma, 183
mesleki etik, 187–191
güvenliğin dış kaynaklardan edinilmesi, 184
dış kaynak kullanımı ile ilgili hususlar, 184
ve klavuzlar, 183
güvenlik zorlukları, 86–88
aldatma, 87
çerez, 87–88
spam ve spim, 86–87
güvenlik, 208–212, 210f, 212f
iş ilişkilerinde, 295–296
güvenlikteki en zayıf halka, 38–40
güvenlik yoklayıcıları, 385

H

HA. Bkz. ev etmeni
hacktivist, 340, 370
hafıza kartları, 148
Hafif Genişletilebilir Kimlik Denetleme Protokolü (LEAP), 349
Hafifletilmiş Dizin Erişim Protokolü (LDAP), 105, 153
Halka Açık Şirketler Muhasebe Gözetim Kurulu (PCAOB), 125
halka açık şirketler, 473
hasarlı sistemlerin geri yüklenmesi,
hassas varlıklar listesi, 183
hassasiyet/systemin kritikliği, 196, 241
hassasiyet/systemin kritikliği, 196, 241
hata toleransı, 272
Hatlar arasında dinleme, 85
hattı değiştirerek dinleme, 85
hazırlık, ayrıcalıklı olayın ele alınması, 278
HCISPP. Bkz. Sağlık Hizmetleri Sertifikalı Bilgi Güvenliği Mahremiyet Uygulayıcısı
herkese açık etki alanı verileri, 42
hertz, 400
Herzing Üniversitesi, 421t
hesap kilitleme politikası, 145–146
HHS. Bkz. Sağlık ve İnsani Hizmetler Bakanlığı
HIDS. Bkz. ana bilgisayar tabanlı saldırı tespit sistemi

HIPAA Güvenlik Kuralı, 464, 465t, 466t
HIPAA Mahremiyet Kuralı, 462–463
HIPAA. Bkz. Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası
HITECH Act. Bkz. Ekonomik ve Klinik Sağlık için Sağlık Bilgisi Teknolojisi Kanunu
hibrit bulut, 174
Hipermetin Aktarım Protokolü (HTTP), 26, 392
hiyerarşik BT güvenlik politikası çerçevesi, 41, 41*f*
hizmet bürosu, 285
Hizmet olarak Altyapı (IaaS), 175
Hizmet olarak Herşey (AaaS), 55
Hizmet olarak Platform (PaaS), 175
Hizmet olarak Platform (PaaS), 175
Hizmet olarak Yazılım (SaaS), 50, 50f, 175
Hizmet Organizasyonu Kontrolü (SOC), 222t
hizmet reddi (DoS) saldırıları, 83–84, 145, 167, 340–341,369–370, 376–377
HMAC-tabanlı tek kullanımlık parola (HOTP), 172
Hollings Üretim Genişletme Ortaklığı, 397
HOTP. Bkz. HMAC-tabanlı tek kullanımlık parola
HTTP. Bkz. Hipermetin Aktarım Protokolü
HTTPS. Bkz. Güvenli Hiper Metin Aktarım Protokolü
hukuki endişeler, 130
hücresel ağlar, 330

I

IaaS. Bkz. Hizmet olarak Altyapı
IAB. Bkz. İnternet Mimarisi Kurulu
IANA. Bkz. İnternet Atanan Numaralar Yetkilisi
ICFR. Bkz. finansal raporlama üzerindeki iç denetimler
ICMP (ping), 246*f*, 383
ICMP yankı istek, 338
ICMP. Bkz. İnternet Kontrol Yönetimi Protokolü; İnternet Kontrol Mesaj Protokolü
IDEA. Bkz. Uluslararası Veri Şifreleme Algoritması
IDS. Bkz. saldırı tespit sistemi
IEC. Bkz. Uluslararası Elektroteknik Komisyonu
IEEE 802.1x standardı, 347
IEEE 802.3 CSMA/CD standardı, 24
IEEE. Bkz. Elektrik ve Elektronik Mühendisleri Enstitüsü
IETF. Bkz. İnternet Mühendisliği Görev Gücü
IIA. Bkz. İç Denetçiler Enstitüsü
ılık bölge, 121*t*, 283, 284*t*
InfoSec Enstitüsü, 428*t*
IoT. Bkz. Nesnelerin İnterneti
IP adres yanıltması, 94
IP adresleri, 332, 335–336, 336*f*, 372
IP ağ tasarımı, 30
IP durum denetlemeli güvenlik duvarı, 27
IP mobil iletişimler, 60–62, 61*f*
IP mobil, 58–59
IP üzerinden Ses (VoIP), 47, 81
IP yanıltması, 370
IP yönlendiriciler, 27
IP. Bkz. İnternet Protokolü
IPS. Bkz. saldırı önleme sistemi
IPSec. Bkz. İnternet Protokol Güvenliği
IPv4, 335–336
IPv6, 335
IRC kanalları. Bkz. İnternet Aktarmalı Sohbet
ISACA. Bkz. Bilgi Sistemleri Denetim ve Kontrol Birliği
ISAKMP. Bkz. İnternet Güvenlik Birliği ve Anahtar Yönetimi Protokolü
ISBN. Bkz. Uluslararası Standart Kitap Numarası
ISO 17799 standardı, 407–408
ISO 27002, 224–225
ISO. Bkz. Uluslararası Standartlar Teşkilâtı
ISO/IEC 27002 standardı, 390, 408–409
ISO/IEC 27005, 123, 123*t*
ISOC. Bkz. İnternet Topluluğu
ISPs. Bkz. İnternet Servis Sağlayıcısı
ISSAP. Bkz. Bilgi Sistemleri Güvenlik Mimarisi Uzmanı
ISSEP. Bkz. Bilgi Sistemleri Güvenlik Mühendisliği Uzmanı
ISSMP. Bkz. Bilgi Sistemleri Güvenlik Yönetimi Uzmanı
ITGI. Bkz. BT Yönetim Enstitüsü
ITIL. Bkz. Bilgi Teknolojisi Altyapı Kütüphanesi
ITT Teknik Enstitüsü, 421*t*, 422*t*
ITU Telekomünikasyon Sektörü (ITU-T), 404–405, 405*t*
ITU. Bkz. Uluslararası Telekomünikasyon Birliği
ITU-T. Bkz. ITU Telekomünikasyon Sektörü
IV saldırısı, 104
İç Denetçiler Enstitüsü (IIA), 225
iç güvenlik, 295
iç kontroller ve bilgi güvenliği hedefleri, 474*t*
iç tehditler, 379
iç yönlendiriciler, 332
içeriğe bağlı erişim denetim, 163, 163*f*
içeriğe bağlı sistem, 159
içerik denetimi, 345
içerik filtreleme, 21, 391–392
içerik-tabanlı filtreleme, 392
içsel tutarlılık, 165
ifşa tehditleri, 90–91
iki adımlı kimlik denetleme, 23t
iki faktörlü kimlik denetleme (TFA), 142
ikinci seviye kimlik denetimi, 35, 36
ileri seviye uzman, Check Point sertifikaları, 449t
İletim Denetimi Protokolü (TCP), 8, 26
İletim Denetimi Protokolü/İnternet Protokolü (TCP/IP), 8–9, 9f, 334–338
  genel bakış, 334–335, 335t
  IP adresleme, 335–336, 336t
  İnternet Kontrol Mesajı Protokolü, 336–338

ortak bağlantı noktaları, 336, 337t
ortak protokoller, 336, 337t
İletişim Güvenliği Malzeme Sistemi (CMS), 316
iletişimler, 407, 408
ilgili düğüm (CN), 61
ilişkiler, 140
ilişkili algoritmalar, 304
imza dinamikleri, 150
imzalar, 296, 297t, 298, 299t, 311–312, 312f
ince istemci, 22
indirect identifiers, 477
inkar edememe, 294–296, 299t, 320–321
insan hatası, 322
insan kaynakları güvenliği, 408
insan kaynakları ve bordro, 36
İnternet Aktarmalı Sohbet (IRC) kanalları, 369
İnternet Atanan Numaralar Yetkilisi (IANA), 27
İnternet Güvenliği Tehdit Raporu, 358
İnternet Güvenlik Birliği ve Anahtar Yönetimi Protokolü (ISAKMP), 322
İnternet güvenliği politikası, 480
İnternet Kontrol Mesaj Protokolü (ICMP), 336–338, 370
İnternet Kontrol Yönetimi Protokolü (ICMP), 383
İnternet Küçük Bilgisayar Sistem Arayüzü (iSCSI), 333
İnternet Mimarisi Kurulu (IAB), 40, 188, 403
İnternet Mühendisliği Görev Gücü (IETF), 65, 401–403
İnternet pazarlama stratejisi, 56–57
İnternet Protokol Güvenliği (IPSec), 322, 346–347
İnternet Protokolü (IP), 8–9
İnternet Servis Sağlayıcısı (ISP), 29t, 49, 330
İnternet solucanlarının kendini kopyalama hızı, 377
İnternet Topluluğu (ISOC), 54, 403
İnternet, 3, 40, 329–331, 376–378
iOS ürünleri, 59
iptal etme, 296, 297t, 299t
ipuçları ve teknikler, 248
iris taraması, 149
istatistiksel tabanlı yöntemler, 236
isteğe bağlı erişim denetim (DAC), 156
isteğe bağlı olmayan erişim denetim, 160
istemci/sunucu modu, 171, 172f
istemci-tarafı saldırısı, 105
istismar yazılımı, 81
iş etki analizi (BIA), 38, 42, 116, 271, 273–274
iş etki analizi (BIA), 38, 42, 116, 271, 273–274
iş güvenliği business security, 298–299, 299t
iş güvenliği business security, 298–299, 299t
iş istasyonları, 22, 23t, 24, 88t, 240
İş İstasyonu Etki Alanı, 20f, 22, 23t, 88t, 90t
iş istasyonu etkisi, 262–263, 262f
iş kurtarma gereksinimleri, 116, 272–273, 273f
iş kurtarma gereksinimleri, 116, 272–273, 273f
iş ortakları, 462
iş ortamları, 121
iş rotasyonu, 189
iş sürekliliği yönetimi (BCM), 270–276, 408, 409
iş sürekliliği yönetimi (BCM), 270–276, 408, 409
iş süreklilik planı (BCP), 11, 18, 38, 39t, 116–118, 253, 270
iş süreklilik planı (BCP), 11, 18, 38, 39t, 116–118, 253, 270
iş sürücüleri, 112
iş sürücüleri, 112
iş yerinde izleme, 173–174
işbirliği anlaşmaları, 120
işbirliği, 47
işe alım/işten çıkarma, 130
işe uyum süreci, 185
işlem stratejileri, 284
işletim sistemi parmak izi tarayıcı, 80
işletim sistemi parmak izi, 244
işletim sistemi savunmaları, 388–389
işletim sistemleri, 8
işletim sistemleri-tabanlı DAC, 157–159
işletme yüksek lisansı (MBA), 423, 424t
işletmeden işletmeye (B2B), 56
işletmeden işletmeye (B2B), 56
işletmeden müşteriye (B2C), 55, 56
işletmeden müşteriye (B2C), 55, 56
işletmeler arası güvenlik, 295–296, 298–299
işlevsel gereksinimler, 204
işlevsel politika, 193–194
işlevsel tanım, 204
işten ayrılma uyum süreci, 185
itibar zedeleme, 379
itibar, 74, 78
iyileştirici faaliyetler, 457
iyileştirme, 186
izin seviyeleri, 159, 219–220
izin/erişim yetkisi, 189, 196
izinler, 138, 161, 182
izinlerin periyodik incelemesi, 157
izinli izin seviyesi, 219
izinsiz dinleme, 85
izinsiz sızma testi, 81
izleme güvenlik sistemleri, 218, 241–248
izleme, 173–174
izleme, 36, 127, 142
izlenebilirlik, 20, 22, 25, 28, 31, 35, 36, 38, 137, 154–156, 182

J

James Madison Üniversitesi, 424t
Japon Mor Şifresi, 291, 307
JCT&CS. Bkz. Ortak Siber Uzay Eğitim ve Sertifikasyon Standardı
Jerusalem virüsü, 376
Jones & Bartlett e-öğrenme, 417t
Juniper Ağ Teknolojileri, 108, 447–449, 448t

K

kablo modem, 330

Kablolu Eşdeğer Mahremiyet (WEP), 231, 316, 348–349
kablosız LANlar (WLAN), 24, 316
kablosuz ağ güvenlik denetimleri, 348–351
Kablosuz ağ saldırısı, 104
kablosuz ağlar, 348–351
Kablosuz Bağlantı (Wi-Fi)
kablosuz erişim noktaları (WAP), 24, 316, 348
kablosuz güvenlik, 315–316
kablosuz şifreleme, 348–349
kabul edilebilir artakalan risk, 264–265, 265*f*
kabul edilebilir eylemler, 219
kabul edilebilir kullanım politikası (AUP), 20, 41, 84, 173, 390
kabul edilmez eylemler, 219
kabul testleri, 204
kalın istemci, 22
Kaliforniya zorunlu açıklama yasası, 168
kalite güvencesi, 37
kamusal anajtar kriptografisi, 304
kamusal ve özel anahtar, 305–308
kamusal-özel anahtar çifti, 304, 305
kamuya açık olmayan kişisel bilgi (NPI), 469
Kanada yasası, 221
kanunlar/yasalar, 124–127, 279, 452–487
kapalı-devre TV, 230
Kaplan Üniversitesi, 422*t*, 423*t*
kapsanan varlık, 462–464
kapsüllenen güvenlik yükü (ESP), 322
kara kutu testi, 248
kara liste, 388
karakteristikler, 142, 148–151
karışık mod, 80, 96
karşılaştırmalı değerlendirmeler, 224–225
karşılıklı kimlik denetleme, 95, 153
karşılıklı yardım, 121, 284
kart sahibi verisi (CHD), 464
Kaspersky Anti-Virüs, 107
katmanlı ağ cihazları, 237
katmanlı savunma, 234, 237
kayıp beklentisi, 260
kayıtları saklama
kaynak seçimi, 414
kaynaklar, 140
KDC. Bkz. anahtar dağıtım merkezleri
Keller Üniversitesi, 424*t*
Kendi Cihazını Getir (BYOD), 58–59, 129–130
Kendi Cihazını Getir (BYOD), 58–59, 129–130
kendi kendine çalışma esnekliği, 413
kendi kendine çalışma kaynakları, 413, 415–416, 417t
kendi kendine çalışma kaynakları, 413, 415–416, 417t
kendi kendine çalışma kaynaklarının kalitesi, 414
kendi kendine çalışma yöntemi, 413–416
kendi kendine çalışma yöntemi, 413–416
kendini motive etme, 413
kendini motive etme, 413
Kerberos key distribution center
Kerberos süreci, 153
kesintiler, 93
kesintisiz güç kaynağı (UPS), 122
kesintisiz şifreleme, 297
keşif, 242, 243–244, 339, 382–385, 382f, 384f–385f
kırıcı, 79
kırma araçları, 144
Kırmızı Kitap, 206
kırpma seviyeleri, 232
kısa sürelilik, 278–279
kısıtlandırılmış kullanıcı ara yüzü, 163–164
kısıtlanmış ana giriş sayfası, 351
kimlik bilgisi yönetimi, 169
kimlik denetleme başlığı (AH), 322
kimlik denetleme sunucusu (AS), 35, 152
kimlik denet eme, 35, 127, 137, 142–154, 82, 292, 293–294, 298, 299t, 313, 347
kimlik denetleme, yetkilendirme ve izleme (AAA) sunucuları, 169–172
kimlik hırsızlığı, 2, 15, 74, 467, 468, 469*f*
kimlik tabanlı şifreleme (IBE), 290
kimlik yönetim sistemi, 227
kimliksizleştirilmiş veri, 64
Kişisel Bilgi Koruma ve Elektronik Belgeler Yasası (PIPEDA), 221
kişisel bilgisayar (PC)
kişisel dijital yardımcı (PDA), 22, 33, 34, 58
kişisel iletişim, 10
kişisel kimlik numarası (PIN), 142
kişisel tanımlama bilgisi (PII), 102, 168, 453, 477
kişisel veri mahremiyeti, 173
kitapevleri, 413, 417*t*
kitapevleri, 413, 417*t*
koklama, 85, 96, 167–168
koklayıcılar, 80
komut enjekte etme, 105, 368
konferans odası testi. Bkz. yapılandırılmış gözden geçirme
konfigürasyon çizelgesi, 199–200
konfigürasyon denetimi, 200, 200*f*
konfigürasyon yönetimi, 199–200
konfigürasyonlar, 226
kontrol listeleri, 226
kontrol listesi testi, 122, 275
kontrol sertifikasyonu gereksinimleri, 473–474, 474*t*
konum araştırma, 351
korkutma, 103, 191
Korumalı Genişletilebilir Kimlik Denetleme Protokolü (PEAP), 347
korumasız bükümlü-çift kablolama, 24
korunan sağlık bilgisi (PHI), 462
korunmalar, 254
kötücül yazılım, 99–102, 355–356
kötü amaçlı yazılım içermeyen kurtarma süreci, 390
kötü ikiz, 104
kötücül eklentiler, 105, 367–368
kötücül faaliyet, 73–74, 74t
kötücül kod, 11, 23t, 375–378
kötücül kripto kilitleyici, 75
kötücül saldırılar, 92–98
kötücül yazılım 11, 72, 99–102, 106–108, 354, 356–375, 393
kredi kartları, 311, 485*t*

kriptanaliz, 288, 305–308
kripto sistem, 288
kriptografi, 17, 288–323
kriptografik anahtarlar, 292, 308
kriptografik fonksiyonlar, 296–299, 297t, 299t
kriptografik özet, 82
kriptografik şifrelemeler, 296–299, 297t, 299t
kriptografik uygulamalar ve kullanım alanları, 312–321, 319*f*
kriptogram, 301
kritik altyapı, 69
kritik iş fonksiyonu (CBF), 271
kuantum kriptografi, 297
Kullanıcı Datagram Protokolü (UDP), 26, 171
Kullanıcı Etki Alanı, 19–20, 21*t*, 86*t*, 88*t*, 90*t*
kullanıcı kabulü, 130
kullanıcı kimliği ve parola, 36, 85, 152, 171, 294
kullanıcı parola kombinasyonu, 142
kullanıcılar, 3, 36–38, 140
kullanıcıların erişimini kısıtlama, 189
kullanıcı-tabanlı izinler, 159
kullanılabilirliğin reddi, 380
kullanılabilirlik, 14, 17–19, 127, 354, 378, 408, 486, 487, 487*t*
kullanılmayan bağlantı noktaları, 168
kullanılmayan özellikleri devre dışı bırakma, 131
kum havuzları, 285
kural tabanlı erişim denetim, 156, 160
kural tabanlı yönetim, 342
kurban, 370
Küresel Bilgi Güvenliği Sertifikası (GIAC), 440–441, 442t
kurtarma alternatifleri, felaket kurtarma gereksinimi
kurtarma noktası hedefi (RPO), 116
kurtarma planları, 121, 280–285, 284t
kurtarma süresi hedefi (RTO), 18, 116, 271
kurtarma teknikleri ve kurtarma, 282–283
kurtarma, 37
Kurumsal BT Yönetiminde Sertifikalı (CGEIT), 444*t*
kurumsal politikalar, 130
kurumsal uygunluk, 183
küresel konumlama sistemi (GPS), 131

L

LAN anahtarı, 24
LAN cihazları, 333–334
LAN Etki Alanı, 20f, 22–25, 26t, 90t
LAN. Bkz. yerel alan ağları
LAN-dan-WAN-a Etki Alanı, 20f, 25–28, 88t, 90t
Layer 2 anahtar, 24
Layer 3 anahtar, 24
LDAP enjeksiyonu, 368
LDAP. Bkz. Hafifletilmiş Dizin Erişim Protokolü
LEAP. Bkz. Hafif Genişletilebilir Kimlik Denetleme Protokolü
Lehigh virüsü, 376
Linux solucanları, 365
Lion solucanı, 365
lisans derecesi programları, 420, 422*t*
lise sonrası eğitim programları, 419–425
loop koruması, 342
LophtCrack program, 386
Loveletter e-posta solucanı, 377
LSO. Bkz. Yerel paylaşılan nesneler
Lucifer algoritması, 314
LUHN formülü, 311

M

MAC adres filtreleme, 348, 350
MAC. Bkz. zorunlu erişim denetim; Ortam Erişim Denetimi
mahrem veri, 16, 36t, 39t, 42
mahremiyet beklentisi, 172–176
mahremiyet politikası, 127, 194
mahremiyet, 130, 184, 295, 297t, 298, 299t, 378, 455
makro virüsler, 359–360, 360f, 377
maksimum tolere edilebilen aksama süresi (MTD), 271, 272–273, 273f
MAN. Bkz. metropol alan ağı
mantık bombaları, 367
mantık saldırıları, 83
mantıksal erişim denetimler, 138–140
mantıksal/teknik denetimler, 156t
manyetik şeritli kart, 148
maruz kalma faktörü (EF), 260
masaüstü egzersizi, 122
maskeleme, 43
material yorumları, 415
MBA. Bkz. işletme yüksek lisansı
MD5 mesaj özeti algoritması, 318–319, 319f
MDM. Bkz. mobil cihaz yönetimi
mekansal dağılım, 231
mektup zinciri biçimi, 373
Melissa e-posta solucanı, 377
menüler, 164
merkezi erişim denetim, 168–169
merkezi olmayan/dağıtık erişim denetim, 169–176
mesaj doğrulama, 295, 298, 299t
mesaj özeti algoritması, 318
mesleki etik, 187–191
  kurallar, 188
    İnternet Mimarisi Kurulu (IAB), 188
    mesleki gereksinimler, 188
  personel güvenlik prensipleri. Bkz. personel güvenliği
  yaygın yanlış düşünceler, 187
mesleki gereksinimler, 188
meslektaş denetimi, 203
metropol alan ağı (MAN), 404
Metropol Ethernet LAN bağlantısı, 29
mevzuat gereklilikleri, 429
mevzuata uygunluk, 183, 429
Meydan Okuma–El Sıkışma Kimlik Denetleme Protokolü (CHAP), 172
mıknatıslık giderme bobini, 155
MITM saldırıları. Bkz. ortadaki adam saldırıları

Microsoft Security Essentials, 107
Miller testi, 479
Miller'a karşı California, 479
mimar seviyesi, Cisco sertifikasyonları, 446*t*
mimari değerlendirmeler, 130
minimum güvenlik kontrolleri, 460
minimum ihtiyaç kuralı, 463
MN. Bkz. mobile düğüm
mobil cihaz yönetimi (MDM), 131
mobil cihazlar, 258
mobil çalışanlar, 129–131
mobil site, 121t, 258, 283
mobil telefonlar, 58
mobil uygulamalar, 59–62
mobile düğüm (MN), 61
mobilite, 129, 130
modemler, 34
modern anahtar yönetim teknikleri, 321–323
Morris solucanı, 100, 365, 376
MOU. Bkz. Mutabakat bildirisi/İyi niyet sözleşmesi
MPLS. Bkz. çoklu protokol etiket anahtarlama
MTBF. Bkz. arızalar arasındaki ortalama süre
MTD. Bkz. maksimum tolere edilebilen aksama süresi
MTTF. Bkz. arıza için ortalama süre
MTTR. Bkz. onarım için ortalama süre
mükemmel iletme gizliliği, 292
MultiTech Systems, 108
Mutabakat bildirisi/İyi niyet sözleşmesi (MOU), 185
müstehcen içerik, 479
müşteri güveni, 221–222
müşteri ilişkileri yönetimi (CRM), 36
müşteri verisi, 74–75
müşteriler, 470

N

NAC. Bkz. ağ erişim denetimi
NAS. Bkz. ağ erişim sunucusu
NASDAQ Borsası, 473
NAT. Bkz. ağ adresi çevirisi
NBS. Bkz. Ulusal Standartlar Bürosu
NC. Bkz. Ulusal Komiteler
NCSA. Bkz. Ulusal Siber Güvenlik İttifakı
NCUA. Bkz. Ulusal Kredi Birliği Yönetimi
negatif riskin kabulü, 113, 263, 264, 265*f*
Nesnelerin İnterneri (IoT) (*devamı*)
  birlikte çalışabilirlik ve standartlar, 48, 62, 65–67
  e-ticaret ve ekonomik kalkınma sorunları, 62, 68–69
  etkileri, 51–55
  gelişimi, 49–50, 50*f*
  güvenlik, 48, 62–63
  mahremiyet, 48, 62–65
  sosyal ve ekonomik sorunlar, 48
  yasal ve mevzuat sorunları, 48, 62, 67–68
Nesnelerin İnterneti (IoT), 2, 10*f*, 390
Nessus, 385
netcat yardımcı yazılımı, 85
NetStumbler, 316
new user registration, 157
New York Borsası (NYSE), 473
New York Times web sayfası, 374, 375f
NIC. Bkz. ağ arayüz kartı
NICE. Bkz. Siber Güvenlik Eğitimi Ulusal Girişimi
NIDS. Bkz. ağ saldırı tespit sistemi
NIST CSF. Bkz. NIST Siber Güvenlik Çerçevesi
NIST laboratuvarları, 397
NIST Özel Yayınlar, 253, 266, 398, 398t–399t, 426–427
NIST Siber Güvenlik Çerçevesi (NIST CSF), 225
NIST. Bkz. Ulusal Standartlar ve Teknoloji Enstitüsü
nicel analiz, 259–260, 260f
nicel risk analizi/değerlendirmesi, 259–263, 260f, 261t, 262f
nicelin hesaplanması, 260–262, 261t
Nimda solucanı, 366, 377
nitel analiz, 259–260, 260f, 262–263, 262f
nitel risk analizi/değerlendirmesi, 259–263, 260f, 262–263, 262f
nitelikli güvenlik denetçisi (QSA), 410, 481
Nmap bağlantı noktası tarama aracı, 384, 385f
NOC. Bkz. ağ operasyon merkezi
Noktadan Noktaya Tünel Protokolü (PPTP), 346
Noktadan Noktaya Tünel Protokolü (PPTP), 346
Northcentral Üniversitesi, 425t
Norton Antivirüs, 107
NPI. Bkz. kamuya açık olmayan kişisel bilgi
NSA eğitim standartları, 436–437, 437t
NSA. Bkz. Ulusal Güvenlik Ajansı
nslookup, 383
NSS. Bkz. ulusal güvenlik sistemleri
NTP. Bkz. Ağ Zaman Protokolü
NYSE. Bkz. New York Borsası

O - Ö

OATH. Bkz. Açık Kimlik Denetleme için Girişim
OCC. Bkz. Para Birimi Kontrolör Dairesi
OCR. Bkz. Vatandaşlık Hakları Dairesi
OCTAVE. Bkz. Operasyonel Kritik Tehdit, Varlık ve Güvenlik Açıkları Değerlendirmesi
OECD. Bkz. Ekonomik Kalkınma ve İşbirliği Örgütü
okuma gizliliği, 360
olasılık, 260
olasılık, 262
olay günlükleri, 186, 233
olay tabanlı senkronizasyon sistemi, 146
olay, 253
Oltalama Dolandırıcılığını Önleme Çalışma Grubu (APWG), 98
oltalama dolandırıcılığı, 97, 98
oltalama saldırıları, 429
oltalama, 87, 97–98, 191, 372–373

olumlu risk yanıtları, 113, 263–264
olumsuz risk yanıtı, 253
olumsuz risk yanıtları, 113
OMB. Bkz. Yönetim ve Bütçe Dairesi
omuz sörfü, 103
onarım için ortalama süre (MTTR), 18
onay, 296, 297*t*, 299*t*
onay, 297*t*, 299*t*
onaylanmış sonuç, 414
onaylı tarama sağlayıcısı (ASV), 481
OpenVAS, 385
operasyon yönetimi, 407, 408
Operasyonel Kritik Tehdit, Varlık ve Güvenlik Açıkları Değerlendirmesi (OCTAVE), 123t
operasyonların sürekliliği, 457
optic omurgalar, 28
ortadaki adam (MITM) saldırıları, 95–96, 168
ortadaki adam ele geçirmesi, 94
Ortak Bilgi Tabanı (CBK), 438
Ortak Ölçütler, 148, 157, 205–206
ortak seviye, 446*t*, 449t
Ortak Siber Uzay Eğitim ve Sertifikasyon Standardı (JCT&CS), 435
ortak siber uzay eğitimi, 436*f*
ortak siber uzay sertifika standartları, 436*f*
ortalama olasılık, 113, 114
ortam araçlarının imha edilmesi gereksinimi, 154–156
Ortam Erişim Denetimi (MAC), 328
ortamları araştırma, denetçinin rolü, 223
OSI Referans Modeli. Bkz. Açık Sistemler Ara Bağlantısı Referans Modeli
OSI'nin sunum katmanı, 327, 328f
OSI'nin Veri Bağlantı Katmanı, 328, 328*f*
otomatik numara çevirici, 81–82
otomatik takas merkezi (ACH), 76
otomatize edilmiş testler, 216
OTS. Bkz. Tasarruf Teftiş Dairesi
oturum açma denemeleri, 145
oturum açma denemeleri, 36t
oturum açma eylemlerini denetleme, 145, 146
oturum açma olayları, 145, 146
oturum anahtarı, 292
Oturum Başlatma Protokolü (SIP), 10
oturum ele geçirme, 95, 374
oyun konsolları, 258
Ödeme Kartı Endüstrisi Güvenlik Standartları Konseyi (PCI SSC), 409, 481
Ödeme Kartı Endüstrisi Veri Güvenliği Standardı (PCI DSS), 14f, 56, 126, 174, 233, 409–410, 480–486
öğrenci kayıtları, 476
öğrenci mahremiyet verisi, 478
öndeki kişinin yakınından gitmek, 103
Önemsiz Dosya Aktarım Protokolü (TFTP), 27
Önerilen Standart (PS), 402
öneriler, 405
önlemek, olumsuz risk yanıtları, 122, 263–264, 265*f*
önlemler, 106–108, 254, 266–270, 387, 389–391
önleyici denetim, 234, 266
önlisans derecesi programları, 420, 421*t*
önyükleme kayıt virüsleri, 357
önyükleme kayıt virüsleri, 357
önyükleme sektörü virüsleri, 376
önyükleme virüsleri, 361
örüntü eşleştirme sistemleri, 236
örüntü veya imza tabanlı saldırı tespit sistemleri, 236
özdeğerlendirme anketi (SAQ), 410, 481–482, 485t
özdeğerlendirme anketi (SAQ), 410, 481–482, 485t
özel (simetrik) anahtar, 290
özel bilgi ve beceriler, 414–415
özel bulut, 174
özel şirketler, 473
Özel Yayınlar (SP), 459
Özel Yayınlar 800 serileri, 398, 398t, 399t, 427
özenti, 79
özet değeri, 318
özet fonksiyonlar, 311–312, 312*f*, 318–320, 319*f*
özet, 289
öznitelik-tabanlı şifreleme (ABE), 290

P

P2P modu, 171, 171f
PaaS. Bkz. Hizmet olarak Platform
paket filtreleme, 332, 342
paket filtrelemeli güvenlik duvarı, 342
paket koklayıcı, 80, 104
Palo Alto Networks, 108
PAN. Bkz. başlıca erişim numarası
PAP. Bkz. Parola Doğrulama Protokolü
Para Birimi Kontrolör Dairesi (OCC), 470
paralel test, 122, 276
paranoyak izin seviyesi, 219
parmak izi, 149
parola değiştirme politikası, 143
Parola Doğrulama Protokolü (PAP), 172
parola hesap politikaları, 143
parola kırma, 386
parola kırma, 82
parola prosedürleri, 226
parola sıfırlama ve saklama, 145
parola standardı, 226, 239
parola yakalama ve kırma, 386
parolalar, 36t, 143–145, 386
pasif saldırı, 93
paylaşma izinleri, 161
paylaşma, pozitif risk
PC virüsü. Bkz. kişisel bilgisayar virüsü
PCAOB. Bkz. Halka Açık Şirketler Muhasebe Gözetim Kurulu
PCI DSS Özdeğerlendirme Anketi (SAQ), 410
PCI DSS. Bkz. Ödeme Kartı Endüstrisi Veri Güvenliği Standardı
PCI SSC. Bkz. Ödeme Kartı Endüstrisi Güvenlik Standartları Konseyi
PDA. Bkz. kişisel dijital yardımcı

PEAP. Bkz. Korumalı Genişletilebilir Kimlik Denetleme Protokolü
penetrasyon testi, 226
  gözden geçirme, denetçinin rolü, 224
  sonuç, 242, 243, 243f
personel güvenliği, 407
personel güvenlik prensipleri, 189–191
  erişimin kısıtlanması, 189
  görevler ayrılığı, 189
  güvenlik eğitimi, 190
  güvenlik farkındalığı, 190–191
  iş rotasyonu, 189
  sosyal mühendislik, 191
  zorunlu izinler, 190
PHI. Bkz. korunmuş sağlık bilgisi
PII. Bkz. kişisel tanımlama bilgisi
PIN. Bkz. kişisel kimlik numarası
PIPEDA. Bkz. Kişisel Bilgi Koruma ve Elektronik Belgeler Yasası
PIPEDA. Bkz. Kişisel Bilgi Koruma ve Elektronik Belgeler Yasası
ping aracı, 338, 339
ping aracı, 338, 339
ping, 29t, 383
ping, 29t, 383
PKI. Bkz. açık anahtar altyapısı
PKI. Bkz. açık anahtar altyapısı
plan değerlendirmesi, 274
plan değerlendirmesi, 274
platformlar arası virüs, 362
PMBOK. Bkz. Proje Yönetimi Bilgi Tabanı
PMBOK. Bkz. Proje Yönetimi Bilgi Tabanı
PMI. Bkz. Proje Yönetim Enstitüsü
PMI. Bkz. Proje Yönetim Enstitüsü
politika tanımla aşaması, 137
politika yürütme aşaması, 137
politikalar, 41, 192–194, 192f, 193f, 216, 227t, 457
politikalar, 41, 192–194, 192f, 193f, 216, 227t, 457
Ponzi şemaları/oyunu, 468
Ponzi şemaları/oyunu, 468
potansiyel güvenlik etkisi, 201
pozitif riskin kabulü, 113, 264
PPTP. Bkz. Noktadan Noktaya Tünel Protokolü
proaktif değişiklik yönetimi, 201
profesyonel gelişim, 427
profesyonel seviye, Cisco sertifikasyonları, 446t
profil-tabanlı sistemler, 236
proje başlatma, 204
proje planlama, 204
proje tabanlı erişim denetim, 159
Proje Yönetim Enstitüsü (PMI), 113, 114, 255
Proje Yönetimi Bilgi Tabanı (PMBOK), 113
prosedürler, 41, 183, 194–195, 195f, 457
protokol çözümleyici, 80
protokol örüntüleri, 236
protokol, 9
protokoller, 333, 334
PS. Bkz. Önerilen Standart

Q

QSA. Bkz. nitelikli güvenlik denetçisi

R

RADIUS. Bkz. Uzaktan Aramalı Kullanıcı Kimlik Denetleme Hizmeti
radyo frekansı ile tanımlama (RFID), 49
RAID. Bkz. bağımsız disklerin yedek dizisi
Rainbow Serileri, 158, 205–206
rainbow tabloları, 143
rapor değerlendirme, denetleyicinin rolü, 224
raporlama, ayrıcalıklı olay işleme, 280
rastgele kod yürütme, 105, 369
RAT. Bkz. Uzaktan Erişim Aracı; Uzaktan Yönetim Aracı
RBAC. Bkz. rol tabanlı erişim denetim
RC2 blok şifreleme, 315
RC4 kesintisiz şifreleme, 315, 316
reaktif değişiklik yönetimi, 201
referans monitörü, 139
reklam yazılımı, 102, 372
Remote SNMP Agent Discovery aracı, 384, 385f
retina taraması, 149
retro virüs, 361, 362f
RFC 1087: Etik ve İnternet, 32t, 40, 188
RFC. Bkz. yorumlar için istekler
RFID. Bkz. radyo frekansı ile tanımlama
Rijndael, 315
risk analizi, 114, 115, 224, 259–263, 260f, 261t, 262f
risk değerlendirmeleri, 122, 123t, 256, 259–263, 260f, 261t, 262f, 408, 457, 486
risk etkisi, 122, 264–265, 265f
risk izleme ve kontrol, 256, 269–270
risk kayıtçısı, 114, 257
risk metodolojisi, 114
risk olasılığı, güvenlik denetimlerinde, 218
risk tanımlama, 114, 115
  anket, 256
  beyin fırtınası, 256
  çalışma grupları, 256
  durağan ortamlar, 258–259
  geçmişe ait bilgiler, 256–257
  gelişmekte olan tehditler, 257–258
  kontrol listeleri, 256
  mülakatlar, 256
Risk ve Bilgi Sistemleri Kontrolünde Sertifikalı (CRISC), 444t
risk yanıt planlaması, 115, 256, 263–265
  artakalan risk, 264–265, 265f
  geliştirme, 264
  kabul edilebilir risk miktarı/kaçınma, 263
  yararlanma, 263
risk yönetim çerçevesi (RMF) yaklaşımı, 459, 460f, 461
risk yönetimi, 113–115, 114f, 252–255, 486
  amaç, 254–255
  bileşenleri, 254
  izleme ve risk yanıtını denetleme, 269–270
  risk yanıt planı, uygulanması, 265–266
  süreç, 255–270
  terminolojisi, 253–254

riskler, 11, 20, 21t, 22, 23t, 25, 26t, 28, 29t, 31, 32t–33t, 34, 35, 36t, 38, 39t, 88–92, 88t, 113, 114f, 122, 123t, 218, 253, 255–270, 255f, 338–341
Rivest-Shamir-Adelman (RSA), 302, 312, 447
robot ağlar/botnet, 364, 369
robot ağlar/botnet, 364, 369
ROC. Bkz. uygunluk raporu
rol mühendisliği, 161
rol tabanlı erişim denetim (RBAC), 159, 161–163
rollerin genelleştirilmesi, 162–163
rootkitler, 85, 101, 362–363
röportajlar, 226
RPC servisi. Bkz. uzak yordam çağrısı
RPO. Bkz. kurtarma noktası hedefi
RSA. Bkz. Rivest-Shamir-Adelman
RTO. Bkz. kurtarma süresi hedefi

S - Ş

SA. Bkz. güvenlik birliği
SaaS. Bkz. Hizmet olarak Yazılım
sabotaj, 91
sadece şifreli metin saldırısı (COA), 306, 306*f*
sağlama toplamları, 293, 298, 318
Sağlık Hizmetleri Sertifikalı Bilgi Güvenliği Mahremiyet Uygulayıcısı (HCISPP), 439
Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (HIPAA), 13, 125, 154, 221, 426, 455*t*, 456, 461–467
sahiplik, 142, 146–148, 184, 296, 297t, 298, 299t
sahte erişim noktası, 104
sakıncalı içerik, 479
sakla ve ilet iletişimler, 52
saldırganın amacı, 102
saldırganlar, 168
saldırganlar, 360, 363, 368–370, 372, 375, 377–383, 391–392
saldırı aracı, 79–82
saldırı aşamaları, 382–387, 382*f*
saldırı önleme sistemi (IPS), 21t, 28, 83, 241, 266
saldırı önleme, 387–390
saldırı tespit sistemi (IDS), 21*t*, 27, 234–236, 238
saldırı tespit, 145, 146, 390–392
saldırılar, 102–105, 379–387, 391–393
saldırılar, 370
SAML. Bkz. Güvenlik Bildirim Biçimlendirme Dili
sanal özel ağlar (VPN), 30, 345–347, 346f
  güvenlik duvarları, 35
  toplayıcı, 346
  tunnels, 30, 32–33t, 33–35
  web sunucusu, 35
  yoğunlaştırıcılar, 35
  yönlendiriciler, 35
sanal yerel alan ağı (VLAN), 25, 334
sanallaştırma sunucuları, 37
SANS Enstitüsü, 417t, 440–441
SAQ. Bkz. özdeğerlendirme anketi
Sarbanes-Oxley Yasası (SOX), 13, 125, 222t, 455t, 472–475
SAS 70. Bkz. Denetleme Standartları No.70
satıcı satnadartları, 221
satıcı-bağımsız profesyonellik sertifikaları, 437–443
satıcı-bağımsız sertifika, 438
satıcıya-özel kendi kendine çalışma eğitim programları, 417*t*
satıcıya-özel profesyonellik sertifikaları, 443–449
satış siparişi girişi, 37
Savunma Bilişim Sistemleri Ajansı (DISA), 434–435
savunma bölgeleri, 387
Sayaç Modu Şifreleme Bloğu Zincirleme Mesaj Doğrulama Kodu Protokolü, 349
SCADA. Bkz. Danışmalı Kontrol ve Veri Toplama Sistemi
SDLC. Bkz. yazılım geliştirme yaşam döngüsü
SEC. Bkz. Sermaye Piyasası Kurumu
seçilmiş düz metin saldırısı, 306
seçilmiş şifreli metin saldırısı, 307
senkronize belirteçler, 146
SEO. Bkz. arama motoru optimizasyonu
SEO. Bkz. arama motoru optimizasyonu
Sermaye Piyasası Kurumu (SEC), 470, 475
sertifika programları, 416, 418
sertifika yetkilisi (CA), 317
sertifika, prensipleri, 321–323
sertifikalandıran, 207
Sertifikalı Bilgi Güvenliği Yöneticisi (CISM), 444*t*
Sertifikalı Bilgi Sistemleri Denetçisi (CISA), 444*t*
Sertifikalı Bilgi Sistemleri Güvenlik Uzmanlığı (CISSP), 44, 438–439
Sertifikalı Bulut Güvenlik Profesyoneli (CCSP), 440
Sertifikalı Güvenli Yazılım Yaşam Döngüsü Profesyoneli (CSSLP), 439
Sertifikalı İnternet Web Yöneticisi (CIW), 441, 442*t*
Sertifikalı Siber Adli Bilişim Uzmanı (CCFP), 439
Sertifikalı Yetkilendirme Uzmanlığı (CAP), 439
sertifikasyonlar, 207, 297t, 298, 415, 418, 427, 433, 437
servis kullanılabilirliği ve verimlilik, 74, 77–78
servis kullanılabilirliği ve verimlilik, 74, 77–78
servis paketi yönetimi, 199–200
servis sağlayıcı katman seviyeleri, 484t
servis seti tanımlayıcısı (SSID), 350
servis seviyesi anlaşmalar (SLA), 19, 30, 184–185
ses deseni, 150
SESAME. Bkz. Çok-Sağlayıcılı Bir Ortamdaki Uygulamalar için Güvenli Avrupa Sistemi
sesli konferans, 47
Sezar şifreleme, 300
sezgisel analiz, 107
SHA. Bkz. Güvenli Özet Algoritması

SHA-1. Bkz. Güvenli Özet Algoritması
sıcak bölge, 121*t*, 283–285
SIEM sistemi. Bkz. güvenlik bilgi ve olay yönetimi sistemi
sıfırıncı gün, 105, 388
sınıflandırılmamış bilgi, 43
sınıflandırılmamış kategori, 197
sınıflandırma, 197–198
sınır güvenlik duvarları, 343–344, 344*f*
sınır güvenlik duvarları, 343–344, 344*f*
sınır yönlendiricileri, 331, 331*f*
sınır yönlendiricileri, 331, 331*f*
SIRT. Bkz. güvenlik olay müdahale ekipleri
Siber Güvenlik Eğitimi Ulusal Girişimi (NICE), 435
Siber Güvenlik Teknik Komitesi (TC CYBER), 406–407
siber güvenlik, 8, 10, 225
siber saldırılar, 73
siber uzay, 3, 8, 8*f*, 40
Siber Uzayı Güvenleştirmek için Ulusal Strateji, 419
simetrik anahtar algoritmaları (ya da standartları), 314–316
simetrik anahtar kriptografisi, 291
simetrik anahtar şifrelemele, 303–304
simülasyon testi, 122, 275–276
sistem bütünlüğünü izleme, 230
sistem geliştirme ve bakım, 407
Sistem Güvenliği Sertifikalı Uygulayıcısı (SSCP), 438
sistem güçlendirme, 22, 238–240
sistem güçlendirme, 238–240
sistem günlüğü, 231
sistem sahibi, 207
sistem tasarım spesifikasyonu, 204
sistem ve hizmetin yama ihtiyacı var, 242f
sistem virüsleri, 357–358, 358f
sistem yaşam döngüsü (SLC), 203
  gerçekleştirme, 204
  işlevsel gereksinimler ve tanım, 204
  kabul testi, 204
  oluştur (geliştir) ve belgele, 204
  operasyonlar ve bakım, 204
  proje başlatma ve planlama, 204
  system tasarım spesifikasyonu, 204
  yok etme, 204
sistem yönetimi, 24
Sistem/Uygulama Etki Alanı, 13f, 20f, 36–38, 39t, 88t, 90t
sistematik eylemler systematic actions, 194–195, 195f
sistemlerin temin edilmesi, 205
siyah şapka bilgisayar korsanı, 79
SLA. Bkz. servis seviyesi anlaşmalar
SLC. Bkz. sistem yaşam döngüsü
SMTP. Bkz. Basit Posta Transfer Protokolü
smurf saldırıları, 338, 370, 371f
smurfing, 84
sneakernet, 375
SNMP. See simple network management protocol
Snopes Web sitesi, 86
SOC. Bkz. Hizmet Organizasyonu Kontrolü
soğuk bölge, 121*t*, 283–284, 284*t*
solucanlar, 32*t*, 100, 364–366, 365*f*, 377
son kullanıcı lisans sözleşmesi (EULA), 11, 12
SonicWALL, 108
sonu açık sipariş sözleşmesi (BPA), 185
sonu açık sipariş sözleşmesi (BPA), 185
sosyal medya, 47
sosyal mühendislik, 96–97, 103, 191, 244
SOX. Bkz. Sarbanes-Oxley Yasası
sözlük parola saldırısı, 82, 94
sözlük saldırısı, 82, 143
spam, 86–87, 363–364
SPI. Bkz. güvenlik parametresi endeksi
spim, 86
SPOF. Bkz. tek arıza noktası
Sponsor Kuruluşları Komitesi (COSO), 225
sprintler, 211
SSAE 16. Bkz. Atama Görevleri Standartlarına İlişkin Açıklamalar No.16
SSCP. Bkz. Sistemler Güvenliği Sertifikalı Uygulayıcısı
SSH. Bkz. Güvenli Kabuk
SSID yayını, 350
SSID. Bkz. servis seti tanımlayıcısı
SSL. Bkz. Güvenli Soket Katmanı
SSO stratejisi. Bkz. tek oturum açma stratejisi
standartlar (STD), 41, 194, 396, 402, 403, 459
standartlar kuruluşları, 397–407
STD. Bkz. standartlar
steganografi, 291
StrangeBrew virüsü, 377
sunucu işletim sistemler ve çekirdek ortamlar, 37
sunucu işletim sistemler ve çekirdek ortamlar, 37
sunucu mimarisi, 37
sunucu mimarisi, 37
sunucu/uygulama günlükleri inceleme, denetçinin rolü, 224
sunucu/uygulama günlükleri inceleme, denetçinin rolü, 224
suyun başı saldırısı, 105
sürekli eğitim programları, 416
sürekli kimlik denetimi, 146
sürekli mesleki eğitim (CPE) değeri, 418
sürekli mesleki gelişim (CPD), 418
Symantec Corporation, 447–449
Symantec Sertifikalı Uzman (SCS) programı, 447–449
SYN taşkını, 84, 370, 371f
SYN-ACK mesajı, 370
şebekeye girme, 97, 103, 372
şebekeye izinsiz girme, 97
şebekeye izinsiz girme, 97
şelale modeli, 210–211, 210*f*
şifre çözme, 289
şifreleme, 17, 17*f*, 26*t*, 32*t*, 164, 231, 289, 348–349
şifreleme, 289, 299–302
şifrelenmemiş bilgi, 289
şifrelenmiş bilgi, 289–290
şifreli metin, 17, 17*f*, 288
şirket standardı yazılım, 240

T

TACACS. Bkz. Terminal Erişim Denetleyici Erişim Denetim Sistemi
TACACS+. Bkz. Terminal Erişim Denetleyici Erişim Denetim Sistemi +
tahribat tehditleri, 92
tam cihaz şifrelemesi, 130
tam kesinti testi, 122, 276
tam yedekleme, 276
tamsayı taşması, 105
tanıklık, 297*t*, 298, 299*t*
tanımlama, 35, 137, 141–142, 182, 297*t*, 298, 299*t*
tanıyor havasına girmek, 191
tarayıcı eklentileri, 368
tarayıcı ele geçirmesi, 94–95
tarayıcı yardımcı nesnesi (BHO) Trojan/Truva atı programı, 374
tarayıcı yardımcı nesnesi (BHO) Trojan/Truva atı programı, 374
tarayıcı zafiyeti, 374
tarayıcı zafiyeti, 374
Tasarruf Teftiş Dairesi (OTS), 470
Taslak Standart (DS), 402
taşıt sistemi, 258–259
taşıyıcı Duyarlı Çoklu Erişim/Çarpışma Tespiti (CSMA/CD), 24
taşkın saldırıları, 83
TCP. Bkz. İletim Denetimi Protokolü
TCP/IP dünyasına dönüşüm, 50–51, 51*f*
TCP/IP. Bkz. İletim Denetimi Protokolü/İnternet Protokolü
TCP/SYN scans, 244, 246f
TCSEC. Bkz. Güvenli Bilgisayar Sistem Değerlendirme Kriterleri
TDoS saldırısı. Bkz. telefon hizmet reddi saldırısı
tedbirli izin seviyesi, 219
tehdit analizi, 118–119,253–254
tehdit değerlendirme ve izleme, 42
tehdit türleri, 90–92
  değiştirme tehditi, 91–92
  ifşa tehditleri, 90–91, 90t
  red veya tahribat tehditi, 92
  tehditler, 11, 20, 21t, 22, 23t, 25, 26t, 28, 29t, 31, 32t–33t, 35, 36t, 38, 39t, 88–92, 88t, 90t, 114, 114f, 122, 123t, 167–168, 253, 375–379
tehditlerin hedefleri, 89–90, 90t
tek arıza noktası (SPOF), 272
tek faktörlü kimlik denetleme, 142
tek kullanımlık şifreleme, 305
tek oturum açma (SSO) stratejisi, 151–154
tek yönlü algortima, 289
tek yönlü öğretim tekniği, 414
tekil kayıp beklentisi (SLE), 260
teknik denetim, 266
teknik kurtarma gereksinimleri, 116, 274–276
teknik tedbirler, 464, 466t
teknoloji koruma önlemi (TPM), 479–480
Teknoloji Yenilik Programı, 397
tekrarlı yazma, 155
telafi edici denetim, 266
telefon hizmet reddi (TDoS) saldırısı, 340–341
telefon hizmeti, 326
telefon şebekesine girme, 97
telefon şebekesine girme, 97
Telefonla kişisel bilgilerin ele geçirilmesi, 103
telekomünikasyon servis sağlayıcıları, 121, 274, 282, 283
Telnet. Bkz. terminal ağı
temassız akıllı kart, 148
temel protokol, 170
temiz masa/temiz ekran politikası, 198, 429
terminal ağı (Telnet), 27
Terminal Erişim Denetleyici Erişim Denetim Sistemi (TACACS), 170
Terminal Erişim Denetleyici Erişim Denetim Sistemi + (TACACS+), 170
ters DNS araması, 383
test, 37, 457
  güvenlik sistemleri
    ağ haritalama yöntemleri, 244
    gizli ve gizli olmayan test uzmanları, 244–247
    güvenlik testi ipuçları ve teknikleri, 248
    keşif yöntemleri, 243–244
    test hedeflerinin oluşturulması, 243
    yol haritası, 242–243
    yöntemler, 248
  maliyet, 269
  ve kalite güvencesi, 37
TFA. Bkz. iki faktörlü kimlik denetleme
TFTP. Bkz. Önemsiz Dosya Aktarım Protokolü
TGS. Bkz. bilet-onaylama sunucusu
Thomas, B., 99
tıbbi uygulamalar, 60
tıkanma noktaları, 389
ticari işletmeler, 378–379
ticari işletmeler, 378–379
TJX Şirketleri, 73, 77
TKIP. Bkz. Geçici Anahtar Bütünlüğü Protokolü
TLS Yetkilendirme Uzantıları. Bkz. Aktarım Katmanı Güvenliği Yetkilendirme Uzantıları
toplam risk, 264
topluluk bulutu, 174
TOS. Bkz. güvenilir işletim sistemleri
TOTP. Bkz. zaman tabanlı tek kullanımlık parola
TPM. Bkz. teknoloji koruma önlemi
traceroute aracı, 338, 339
trafiğe boğma koruması, 342
trafik tabanlı yöntemler, 236
transposition ciphers, 299, 300, 300f
Trend Micro, 107
Trojanlar, 32t, 374
Truva atı kötücül yazılım programı, 82
Truva atları, 100–101, 167, 366–367, 375
Tüketici Koruma Veritabanı, 468, 469*f*
Tüketiciyi Koruma Ağı Veri Kitabı, 468
Turuncu Kitap, 158, 206
tuş darbesi dinamikleri, 150

tuş vurucu kaydedicileri, 82, 373
tuz değeri, 315
tüccar katman seviyeleri, 483t
tüketici finansal bilgisi, 467
tüketiciler, 469, 470

U

uç nokta güvenliği, 130–131
uçtan uca iletişimler, 429
uçtan-uca IP aktarımı, 28
UDP. Bkz. Kullanıcı Veri Bloğu İletişim Kuralı
Ulusal Güvenlik Ajansı (NSA), 419–420, 436–437, 437t
Ulusal Güvenlik Sistemleri (NSS), 461
Ulusal Güvenlik Sistemleri Komitesi (CNSS), 436, 461
Ulusal Komiteler (NC), 400–401
Ulusal Kredi Birliği Yönetimi (NCUA), 470
ulusal optic omurgalar, 28
Ulusal Siber Güvenlik İttifakı (NCSA), 107
Ulusal Standartlar Bürosu (NBS), 397
Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), 225, 397–398, 398t, 426–427, 459–460, 460f
Uluslararası Bilgi Sistemleri Güvenlik Sertifikasyon Konsorsiyumu, $(ISC)^2$, 44, 438
Uluslararası Elektroteknik Komisyonu (IEC), 400–401
Uluslararası Standart Kitap Numarası (ISBN), 399
Uluslararası Standartlar Teşkilâtı (ISO), 398–400
Uluslararası Telekomünikasyon Birliği (ITU), 404–405
Uluslararası Veri Şifreleme Algoritması (IDEA), 314
UNIX-tabanlı solucan, 376
UPS. Bkz. kesintisiz güç kaynağı
URL ele geçirmesi, 94–95
URL filtresi, 345
USASI. Bkz. Amerika Birleşik Devletleri Standartları Enstitüsü
USB belirteci, 148
US-CERT. Bkz. Birleşik Devletler Bilgisayar Acil Hazırlık Takımı
UTM. Bkz. birleşik tehdit yönetimi
uydurmalar, 92
uygulama ağ geçidi güvenlik duvarları, 28
uygulama günlüğü, 230–231
Uygulama Katmanı, 231, 327, 328*f*
uygulama kontrolü, 131
uygulama savunmaları, 388
uygulama servis sağlayıcıları (ASP), 50
uygulama sunucularının, 37
uygulama vekil sunucusu güvenlik duvarı, 343
uygulama yazılım güvenliği, 203–208
uygulama yazılımının test edilmesi, 205–208
uygulamalar, 36–38, 168
uygulamalar, 390
uygulama-tabanlı DAC, 158–159
uygunluk irtibatı, 186
uygunluk kanunları, 12–14, 14*f*, 124–127
uygunluk masrafı, 269
uygunluk onayı (AOC), 481
uygunluk raporu (ROC), 481
uygunluk, 154–156, 185–186, 408, 409, 453–456
uzak yordam çağrısı (RPC) servisi, 383
Uzaktan Aramalı Kullanıcı Kimlik Denetleme Hizmeti (RADIUS), 170, 349
Uzaktan Erişim Aracı (RAT), 386
Uzaktan Erişim Etki Alanı, 20f, 32–36, 36t, 88t, 90t
uzaktan erişim sistemleri, 224f
uzaktan erişim, 345–347
uzaktan kod yürütme, 369
uzaktan öğrenme, 420
uzaktan slime, 150
uzaktan yönetim
Uzaktan Yönetim Aracı (RAT), 386
uzantılar, 170
uzman seviye, 446*t*, 449*t*
uzun parola, 145
üçlü DES protokolü, 314
üçüncü parti yama yönetimi yazılımı, 240
üç-yönlü yaklaşım, 127, 128
ürün maliyeti, 269
üssel şifreleme, 302
üst veri, 64
üzerine yazma, 155

V

varlık değeri (AV), 260
varlık kimlik denetleme, 297*t*, 298, 299*t*, 466*t*
varlık koruma
  BT ve ağ altyapısı, 75–76
  fikri mülkiyet, 76
  hizmet kullanılabilirliği ve verimlilik, 77–78
  itibar, 78
  mali durum ve mali veriler, 76–77
  müşteri verisi, 74–75
varlık koruma politikası, 42
varlık sınıflama politikası, 42
varlık takibi, 131
varlık yönetim politikası, 42
varlıklar, 41–42, 91, 182, 407, 408
varsayılan kullanıcı adı ve parola, 85, 240
varsayılan parolalar, 240
Vatandaşlık Hakları Dairesi (OCR), 464
vazgeçilen planlar, 203
VBAC. Bkz. görünüm tabanlı erişim denetim
vekil sunucu güvenlik duvarları, 28
vekil sunucu, 27, 28
vekil sunucular, 480
Venona projesi, 309
veri analizi, 228
veri arşivleme ve saklama, 38
Veri Bağlantısı Katmanı şifrelemesi, 231
veri blokları, 171
veri bütünlüğü, 378
veri değişiklikleri, 86, 380
veri dışa aktarımı, 380
veri gizliliği, 127, 128
veri ihlalleri, 4–11, 4*t*–7*t*, 467, 469, 480
veri kaybını önleme (DLP), 230
veri koruma kanunları, 486
veri mahremiyeti, 172–176

veri politikaları, 206
veri sahipliği, 129
veri sınıflandırma standartları, 16, 36*t*, 37, 39*t*, 42–43, 118, 196–198
Veri Şifreleme Standardı (DES), 290, 302, 314
veri toplama yöntemleri, denetleme, 226–227
veri virüsleri, 357
verilerin tutulması, 154–156
verimlilik etkisi, 269
verimlilik, 378–379
verinin bozulması, 166
verinin yalnızca dahili kullanımı, 42
veritabanı görünümleri, 164
veritabanı yönetim sistemleri, 120
Vernam şifreleme, 301, 305
video konferans, 47
Vigenere, 301
viral kod, 376
virüs kod aktiviteleri, 356
virüs, 356–363, 357f, 375–377
virüs, 376
virüsler, 11, 87, 99–100
VLAN. Bkz. sanal yerel alan ağı
VoIP. Bkz. IP üzerinden Ses
VPN. Bkz. sanal özel ağlar

W

W32/Nimda solucanı, 377
W3C. Bkz. World Wide Web Konsorsiyumu
WAN Etki Alanı, 20*f*, 28–31, 32*t*–33*t*, 88*t*, 90*t*
WAN iletişim hatları, 30
WAN. Bkz. geniş alan ağları
WAPs. Bkz. kablosuz erişim noktaları
War chalking, 104
War driving, 104
WatchGuard Technologies, 108
web grafiti, 374
web güvenlik ağ geçidi, 345
web içerik filtresi, 28
web sayfası içeriğinin bozulması, 374–375, 375*f*
web sitesi trafiğinin yönlendirilmesi, 98, 372–373
web sunucuları, 35, 238, 272
web uygulamaları, 104–105, 374
web yanıltması, 95
web'de uygunsuz gezinme, 84–85
Webroot Antivirüs, 107
WEP. Bkz. Kablolu Eşdeğer Mahremiyet
WHOIS aracı, 383, 384*f*
WHOIS hizmeti, 245*f*
Wi-Fi Korumalı Erişim (WPA) standardı, 231, 316, 349
Windows izinleri, 161
WLANlar. Bkz. kablosuz LANlar
World Wide Web (WWW), 3
World Wide Web Konsorsiyumu (W3C), 401
WPA standardı. Bkz. Wi-Fi Korumalı Erişim standardı

X

X9.17, 323
XKMS. Bkz. XML anahtar yönetimi özelliği
XML anahtar yönetimi özelliği (XKMS), 323
XML enjeksiyonu, 105, 368
XML. Bkz. genişletilebilir işaretleme dili
XSRF. Bkz. çapraz site istek sahtekarlığı
XSS. Bkz. çapraz site betiği/komut dosyası çalıştırma
XTACACS. Bkz. Genişletilmiş Terminal Erişim Denetleyici Erişim Denetim Sistemi

Y

Y Kuşağı, 10
yabancı etmen (FA), 61
yakın alan iletişim saldırısı, 104
yama ve servis paketi yönetimi, 199–200
yamalar, 129
yanıltma, 94
yanıt, ayrıcalıklı olay işleme, 279
yanıtları, 264
yanlış kabul oranı (FAR), 149
yanlış negatifler, 232
yanlış pozitifler, 232, 236
yanlış reddetme oranı (FRR), 148–149
yansıtılmış site, 283
yapılandırılmış gözden geçirme, 122, 275
yapısal olmayan saldırılar, 380–381
yapısal saldırılar, 381
Yapısal Sorgulama Dili (SQL) enjeksiyonu, 105, 368
yardım için başvuru, 191
yasal sorumluluk, 11, 379
yavaş virüs, 361, 361*f*
yazılım denetimleri, 156*t*
yazılım en iyi uygulamaları, 390
yazılım geliştirme yaşam döngüsü (SDLC), 37
yazılım geliştirme, 208–212, 210*f*, 212*f*
  çapraz site betikleme (XSS), 209
  çapraz site istek sahtekarlığı (XSRF), 209
  çevik, 211–212, 212*f*
  model, 209–212
  şelale modeli, 210–211, 210*f*
  Yapısal Sorgulama Dili (SQL) enjeksiyonu, 209
yazılım güvenliği, 208–212
yazılım zafiyet penceresi politikası, 23*t*, 26*t*
yazım hatası, 95
yedek, 272
yedekleme uygulaması, 276–277
yedekleme verisi, 276–277
yedekleme, 37
yeniden gönderme saldırıları, 95, 104
yerel alan ağları (LAN), 24, 332–334, 333*f*, 376, 404
Yerel paylaşılan nesneler (LSO), 105, 372
yerine geçme saldırıları, 96
yerine koyma şifrelemesi, 299, 300–302
yetersizlik, 103
yetkilendiren görevli (AO), 207
yetkilendirilmemiş erişim, 10
yetkilendirme kuralları, 140
yetkilendirme politikası, 140–141
yetkilendirme, 35, 127, 128, 137, 182, 196, 295, 297*t*, 299*t*
yetki-seviyesi politikası, 141
yıllık gerçekleşme oranı (ARO), 260

yıllık kayıp beklentisi (ALE), 261–262
yok etme, SLC, 203, 205
yoklama, 382–385, 382*f*, 384–385*f*
yolun sonu (EOL), 63
yorumlar için istekler (RFC), 80, 402–403
YouTube eğitimi, 417*t*
yönergeler, 41, 183, 196, 415, 459
yönetici seviyesi, Check Point sertifikaları, 449*t*
Yönetilen PKI, 323
yönetilen servisler, 30
Yönetim ve Bütçe Dairesi (OMB), 125, 126
Yönetim ve Bütçe Dairesi (OMB), 456, 458, 459
yönetimsel denetimler, 156*t*, 266
yönetimsel tedbirler, 464, 465*t*
yönlendirici ve ekipman yönlendiriciler, 331–332
yöntemler, 243–244
yük dengeleyici, 345
yüksek değerli müşteriler, 56
yüksek lisans derecesi, 421–423, 423*t*, 424*t*
yüksek olasılık, 262
yüksek-seviye güvenlik politikası denetleme, 220
yüz tanıma, 150

Z

zafiyet değerlendirme, 23*t*, 26*t*, 42
zafiyet değerlendirme, 23*t*, 26*t*, 42
zafiyet penceresi, 23*t*
zafiyet/güvenlik açığı testi, 242, 243, 243*f*
zafiyetler/güvenlik açıkları, 11, 20, 21*t*, 22,23*t*, 26*t*, 28, 29*t*, 31, 32*t*–33*t*, 35, 36*t*, 38, 39*t*, 88–92, 88*t*, 90*t*, 114, 114*f*, 122, 123*t*, 242, 243, 243*f*, 253
tehdit hedefleri, 89–90, 90*t*
tehdit türleri, 90–92
zaman damgası, 295, 296, 297t,298, 299t
zaman tabanlı senkronizasyon sistemi, 146
zaman tabanlı tek kullanımlık parola (TOTP), 172
zararlı yazılım denetimi, 345
zayıf parolalar, 143
Zengin Ol ya da Uğrunda Öl Operasyonu, 77–78
zırhlı virüs, 75, 360
zorunlu erişim denetim (MAC), 159–160, 196
zorunlu izinler, 190
ZyXEL, 108



David Kim | Michael G. Solomon

Bilgi Sistemleri Güvenliğinin Temelleri

Çeviri Editörü | Dr. Öğr. Üyesi Özgü Can

Fundamentals of Information Systems Security

Alandaki en son veri ile gözden geçirilmiş ve güncellenmiş olan ***Bilgi Sistemleri Güvenliğinin Temelleri, 3. Basım***, bilgi sistemleri güvenliğinde kariyer sahibi olmak isteyen okuyuculara bilmeleri gereken temel kavramları kapsamlı bir genel bakış ile sunmaktadır. Kitap, dijital dünyaya geçişle ilgili yeni risklerin, tehditlerin ve güvenlik açıklarının tartışılmasıyla başlamaktadır. II. Bölüm, Security+ sınavı için genel bir bakış açısı sunmaktadır ve öğrencilere bu sertifikasyona yönelik bilgi vermektedir. Bu kitap, bilgi güvenliği standartları, eğitim, mesleki sertifikalar ve uyumluluk yasaları hakkındaki bilgiler ile sonlanmaktadır. Pratik, konuşma dilinde yazılmış ve adım adım örnekler içeren bu kitap, bilgi sistemleri güvenliği dünyasına girenlerin sahip olması gereken bir kaynaktır.

TEMEL ÖZELLİKLER

- CompTIA Security+ SY0-401 Sertifikasyon Sınavının temel altı etki alanıyla tamamen eşleşme,
- FISMA, NIST SP800-171 ve PCI DSS v3.2'yi de içeren en son uyumluluk yasaları ve standartları içerecek şekilde güncellenmiş,
- Kötücül kripto kilitleyici ve fidye yazılımları gibi uç noktalara yapılan ileri kötücül yazılımlar ve APT saldırıları ile ilgili yeni içerik,
- Veri ihlaline ve veri ihlali olay yanıt planlamasına yönelik içerik,
- En son "Nesnelerin İnterneti" risk tehditlerini ve mahremiyet konularını sunma,
- Öğrencilerin gerçe[illegible]yebilecekleri uygulamalı, etkile[illegible]venlik Bulut Laboratuvarları [illegible]

DİJİTAL DEĞİL BASILI OKU

JONES & BARTLETT LEARNING
An Ascend Learning Company
www.jblearning.com

Okuyucu İnceleme Kopyaları için okuyucu@nobelyayin.com
facebook.com/nobelyayin
twitter.com/nobelyayin
twitter.com/nobelkitap

ISBN 978-605-133-000-7

nobel

NOBEL AKADEMİK YAYINCILIK EĞİTİM DANIŞMANLIK TİC. LTD ŞTİ.
Ankara Büro: Mithatpaşa Cad. No.: 74/4 Kızılay ANKARA
Tel: +90312 418 20 10 Faks: +90312 418 20 20
Kazımpaşa Mah. Rıhtım Cad. Nemlizade Sok. Güleryüz Apt. No:9 Daire:3 Kadıköy / İSTANBUL Tel-Faks: +90216 418 20 10
nobel@nobelyayin.com - www.nobelyayin.com

YERLİ ÜRETİM

www.nobelkitap.com