BGD Siber Güvenlik ve Savunma Kitap Serisi 1

Siber Güvenlik ve Savunma

FARKINDALIK ve CAYDIRICILIK



Editörler
Prof. Dr. Şeref Sağıroğlu
Prof. Dr. Mustafa Alkan

Grafiker Yayınları

Siber Güvenlik ve Savunma

FARKINDALIK ve CAYDIRICILIK

Editörler
Prof. Dr. Şeref SAĞIROĞLU
Prof. Dr. Mustafa ALKAN

Ankara 2018

Siber Güvenlik ve Savunma
Farkındalık ve Caydırıcılık

Editörler
Prof. Dr. Şeref SAĞIROĞLU
Prof. Dr. Mustafa ALKAN

Yazarlar
Prof. Dr. Şeref SAĞIROĞLU
Prof. Dr. Mustafa ALKAN
Prof. Dr. Refik SAMET
Doç. Dr. Güzin ULUTAŞ
Doç. Dr. Yıldıray YALMAN
Dr. Öğretim Üyesi Gökhan ŞENGÜL
Dr. Cengiz PAŞAOĞLU
Dr. Öğretim Üyesi Atila BOSTAN
Dr. İbrahim Alper DOĞRU
Dr. Murat DÖRTERLER
Dr. Ahmet EFE
Dr. Yılmaz VURAL
Mustafa ŞENOL
Duygu Sinanç TERZİ
Ömer ASLAN
Salih Erdem EROL
Çağrı SÜMER
Rami URFALIOĞLU

ISBN: 978-605-2233-22-1

1. Baskı
Aralık, 2018 / Ankara
1000 Adet

Grafiker®
Yayınları
Yayın No: 287
Web: grafikeryayin.com

Kapak, Sayfa Tasarımı Baskı ve Cilt
Grafiker®
Grafik-Ofset Matbaacılık Reklamcılık
Sanayi ve Ticaret Ltd. Şti.
1. Cadde 1396. Sokak No: 6
06520 (Oğuzlar Mahallesi) Balgat-ANKARA
Tel : 0 312. 284 16 39 Pbx
Faks : 0 312. 284 37 27
E-mail : grafiker@grafiker.com.tr
Web : grafiker.com.tr

HAVELSAN Bu kitap HAVELSAN'ın katkılarıyla basılmıştır.

İÇİNDEKİLER

EDİTÖRLERDEN **9**
BİLGİ GÜVENLİĞİ DERNEĞİNDEN **13**
ÖN SÖZ **17**

1. BÖLÜM
SİBER GÜVENLİK VE SAVUNMA:
ÖNEM, TANIMLAR, UNSURLAR VE ÖNLEMLER

1.1. Tanımlar 21
1.2. Siber Saldırılar ve Türleri 34
1.3. Siber Güvenlik ve Savunmanın Önemi 35
1.4. Karşılaşılabilecek Saldırılar ve Tehditler 38
1.5. Siber Güvenlik Unsurları 41
1.6. Saldırılara Karşı Koyma Adımları 42
1.7. Nasıl Bir Siber Güvenlik ve Savunma 42
1.8. Değerlendirmeler 45

2. BÖLÜM
SİBER GÜVENLİĞİN TEMELLERİ

2.1. Şifre Bilim Tarihçesi 49
2.2. Şifre Bilim 51
2.3. Şifre Bilimde Kullanılan Teknikler ve Algoritmalar 52
Asimetrik Algoritmalar 54
Simetrik Algoritmalar 55
Hibrit Yaklaşımlar 55
2.4. Anahtarlar 56
2.5. Şifreleme Algoritmaları 59
Sezar Şifreleme Yaklaşımı 62
Sezar Açık Anahtar Şifreleme Yaklaşımı 63
Polialfabetik Şifreleme Yaklaşımı 64

Vernam (One-time Pad) Şifreleme Yaklaşımı 65
DES (Data Encryption Standard) Algoritması 66
RSA (Rivest, Shamir ve Adleman) Algoritması 66
AES Algoritması 68
2.6. Özetleme (Hashing) Algoritmaları 69
2.7. Şifre Bilim Standartları 73
2.8. Steganografi 74
2.9. Kuantum Şifreleme 75
2.10. Güvenlik Protokolleri 76
PGP 76
SSL/TSL 76
SSH 77
S/MIME 77
IPSec 77
Kerberos 78
2.11. Elektronik İmza (E-İmza) 78
2.12. Değerlendirmeler 83

3. BÖLÜM
SİBER GÜVENLİK

3.1. Siber Uzay 87
3.2. Siber Savaş 89
3.3. Siber Güvenlik ve Güvenliğe Duyulan İhtiyaç 90
3.4. Siber Güvenlik ve Bilgi Güvenliği Arasındaki Fark 91
3.5. Siber Ortamda Tehditler 93
3.6. Güncel Siber Saldırılar 95
3.7. Siber Güvenlik İstatistikleri 98
3.8. Değerlendirmeler 100

4. BÖLÜM
SİBER GÜVENLİK FARKINDALIĞI,
ÖNEMİ VE YAPILMASI GEREKENLER

4.1. Giriş 105
4.2. Bilgi Güvenliği Farkındalığı ve Bileşenleri 110
4.2.1. Tehdit 113
4.2.1.1. Siber Saldırı Yaşam Döngüsü 114

4.2.1.2. Siber Saldırı Yaşam Döngüsü Örnek Olay Değerlendirmesi ... 116
4.2.2. Algı ... 118
4.2.3. Farkındalık ... 119
4.2.4. Davranış ... 120
4.3. Farkındalık ve Davranış İlişkisi ... 120
4.4. Farkındalık Ölçüm Yöntem ve Modelleri ... 124
4.4.1. Farkındalık Yeterlilik Seviyesi Ölçüm Yöntemleri ... 125
4.4.2. Farkındalık Yeterlilik Seviyesi Ölçüm Modelleri ... 127
4.4.3. Farkındalık Modelleri ... 130
4.5. Değerlendirmeler ... 134

5. BÖLÜM
SİBER GÜVENLİK FARKINDALIĞI OLUŞTURMA
5.1. Giriş ... 145
5.2. En Zayıf Bileşen İnsan ... 146
5.3. Siber Güvenlik Farkındalığında Zeviyeler ve Sorumluluklar ... 148
5.4. Farkındalık, bilgi ve Davranış İlişkisi ... 153
5.5. Farkındalık Eğitimleri ... 154
5.5.1. Bilgilendirme ... 156
5.5.2. Örnek Problem Çözümleri ve Alınan Dersler ... 156
5.5.3. Uygun Sıklıkla Tekrar ve Güncellemeler ... 157
5.5.4. Güvenli Davranış Biçimlerini Otomatikleştirme (Refleks Gelişimi) ... 157
5.5.5. Etkin Takip ... 157
5.5.6. Teşvik ve Ödüllendirme ... 158
5.6. Değerlendirmeler ... 158

6. BÖLÜM
SİBER GÜVENLİKTE BÜYÜK VERİ VE AÇIK VERİ KULLANIMI
6.1. Giriş ... 165
6.2. Açık Veri ve Açık Kaynağın Önemi ... 165
6.3. Değerlendirmeler ... 173

7. BÖLÜM
HİBRİT SAVAŞ KAPSAMINDA SİBER SAVAŞ VE SİBER CAYDIRICILIK

7.1. Giriş 181
7.2. Savaşın Tanımlanması ve Çeşitleri 183
7.3. Hibrit Savaş 187
7.4. Siber Savaş 192
7.5. Siber Caydırıcılık 207
7.6. Değerlendirmeler 214

8. BÖLÜM
KÖTÜ AMAÇLI YAZILIMLAR VE ANALİZİ

8.1. Giriş 225
8.2. Siber Saldırı Türleri ve Saldırılarda Kullanılan Kötü Amaçlı Yazılım Çeşitleri 227
8.2.1. Virüsler (Viruses) 228
8.2.2. Solucanlar (Worms) 229
8.2.3. Truva Atları (Trojan Horses) 229
8.2.4. Arka Kapılar (Backdoors) 230
8.2.5. Fidye Yazılımları (Ransomware) 230
8.2.6. Korsan Amaçlı Kullanılan Yazılımlar (Rootkits) 230
8.2.7. Robotlar (Bots) 231
8.2.8. Casus Yazılımlar (Spywane) 231
8.3. Yeni Nesil Kötü Amaçlı Yazılımlar 232
8.4. Kötü Amaçlı Yazılım Analizi 234
8.4.1. Statik Analiz 236
8.4.1.1. Statik Yazılım Analizinde Bilgi Çıkarma Yolları 240
8.4.2. Dinamik Analiz 243
8.4.3. Statik ve Dinamik Analizin Karşılaştırılması 249
8.5. Değerlendirmeler 251

9. BÖLÜM
SİBER TERÖR, TERÖRİZM VE MÜCADELE

9.1. Giriş 259
9.2. Siber Terörizmde Saldırganların Kullandıkları Yöntemler 261

9.3. Tarihsel Süreçte Siber Terörizm Örnekleri 265
9.3. Gelecek ve Siber Terörizm 269
9.4. Siber Terörizmle Mücadele 271
9.5. Değerlendirmeler 277

10. BÖLÜM
DÜNYADA VE TÜRKİYE'DE KİŞİSEL VERİLERİN KORUNMASI

10.1. Giriş 283
10.2. Temel Kavramlar 285
10.2.1. Kişisel Veri 286
10.2.2. Kişisel Verilerin İşlenmesi 286
10.2.3. Açık Rıza 286
10.2.4. İlgili Kişi 287
10.2.5. Veri Sorumlusu 287
10.2.6. Veri İşleyen 287
10.3. Dünyada Kişisel Verilerin Korunması 288
10.3.1. Kapsamlı Model 291
10.3.2. Sektörel Model 291
10.3.3. Öz Düzenleme Modeli 292
10.3.4. Birleşmiş Milletler Kararları 294
10.3.5. OECD Rehber İlkeler 296
10.3.6. Avrupa Konseyi 108 Sayılı Sözleşme 297
10.3.7. Avrupa Birliği (AB) Düzenlemeleri 298
10.4. Türkiye'de Kişisel Verilerin Korunması 299
10.4.1. Kanun Yapım Çalışmaları 300
10.4.2. Anayasal Hak Olarak Kişisel Verilerin Korunması 301
10.4.3. 6698 Sayılı Verilerin Korunması Kanunu 302
10.5. Değerlendirmeler 307

11. BÖLÜM
MOBİL CİHAZLARDA SİBER GÜVENLİK

11.1. Giriş 311
11.2. Mobil Kötücül Yazılımlar 315
11.3. Mobil Cihazlara Yönelik Saldırılar 320

11.4. Mobil Cihazlara Güvenlik Analizi 323
11.4.1. Statik Analiz Yaklaşımı 326
11.4.2. Dinamik Analiz Yaklaşımı 328
11.4.3. Hibrit Analiz Yaklaşımı 328
11.4.4. Makine Öğrenmesi Teknikleri 329
11.5. Mobil Cihaz Yönetimi 331
11.6. Güvenli Mobil Cihaz Kullanımı 335
11.7. Değerlendirmeler 341

12. BÖLÜM
SİBER GÜVENLİK DENETİMİ

12.1. Giriş 349
12.2. Siber Güvenlik Denetiminde Amaçlar 351
12.3. İç ve Dış Denetim 363
12.4. Dış Denetim 366
12.5. Siber Güvenlik Olgunluk Modelleri 367
12.6. Denetleyici Eylem Planları 369
12.7. Değerlendirmeler 370

13. BÖLÜM
SİBER GÜVENLİK İÇİN BÜYÜK VERİ YAKLAŞIMLARI

13.1. Giriş 375
13.2. Siber Güvenlik İçin Büyük Veri 379
13.3. Siber Tehdit Olarak Büyük Veri 382
13.4. Büyük Verinin Güvenliği 383
13.5. Değerlendirmeler 384

Yazarların Özgeçmişleri 389

EDİTÖRLERDEN

Bilgi Güvenliği Derneği (BGD), kuruluşundan bugüne kadar ülkemizin Bilgi ve Siber Güvenliği ile Savunmasının gelişimine katkı sağlamakta, birikimini çevreye aktarmakta, bilgi güvenliği alanında açık kaynak yaklaşımını benimseyen ve bu kapsamda içerik üretilmesine ve geliştirilmesine destek vermekte, bunları yaymakta, paylaşmakta ve kamuoyunun kullanımına sunmaktadır. Düzenlediği ulusal ve uluslararası etkinliklere ait "Konferans Bildiriler Kitapları" serisi, hazırladığı raporlar, taslak strateji dokümanları ve eylem planları vb. bunların başında gelmektedir. "Siber Güvenlik ve Savunma Kitapları Serisi" ise BGD'nin ülkemize sunduğu önemli bir diğer katkıdır.

Tehditlerin artması, boyut ve yön değiştirmesi, çeşitlerinin artması, siber tehdit ekosisteminin büyümesi, kritik altyapıların hedef haline gelmesi, bilgi hırsızlıklarının çoğalması, yeraltında çalışan konsanların etkinleşmesi, siber tehditlerin artık savaşa dönüşmesi, siber suçların ve suçluların çoğalması, siber terörün artması, siber saldırılarla, suçlarla, terörizimle, zafiyetlerle mücadeleye her zamankinden daha fazla ihtiyaç duyulmaktadır. Kapsamlı bir mücadele için; ulusal stratejileri ve eylem planlarının hayata geçirilmesi, etkili araştırma merkezlerinin açılması, yeni altyapılar kurulması, yeni programların açılması ve son zamanlarda ise "siber ordular", "mükemmelliyet merkezleri", "ulusal siber olaylara müdahale", "siber savunma ajansı" gibi yapıların kurulması, bizleri bu kitap serisini hazırlamaya yöneltmiştir. Tehditlerin boyutunu ve geleceğini anlamak ancak ve ancak bu alanın kapsamını iyi anlamak, gelecekte karşılaşılacak olan tehditleri öngörmek, buna hazır olmak için konunun etkileşim içerisinde olduğu tüm alanları iyi bilmek, etkileşim içerisinde olunan alanları iyi tanımak, yeni alanları öğrenmek gerekmektedir. Bu kitap serisinde 100'e yakın konu başlığı farklı bölümlerde sunulmuş, konunun tehlike boyutu verilmiş, alınması

gereken önlemlerden bahsedilmiş ve konuyla ilgili önemli hususlar da bölümlerde tartışılmıştır. Kitap serisi içerisinde yer alacak konu başlıkları öncelikle belirlenmiş, ülkemizde bu alanda çalışan akademisyenler ve uzmanlar ile paylaşılmış, ilgili bölümleri yazmak isteyen yazarlardan bölümleri belirli zamana kadar tamamlamaları istenilmiştir. Belirlenen süre içerisinde bölümleri tamamlayan yazarlarımızın eserleri ise bu ilk cilte alınmıştır. Bundan sonraki süreçte, belirlenen diğer konular belirli sürelerde tamamlanıp sırasıyla yayımlanacaktır.

Siber güvenlik ve savunmaya kapsamlı bir bakış sunmayı amaçlayan bu eser serisinin, ülke siber güvenliğimiz ve savunmasına katkı sağlaması beklenmektedir.

13 farklı bölümün sunulduğu ve siber güvenliğin farklı açılardan irdelendiği bu ciltte; temel konular, siber terminoloji ve tanımlar, siber güvenliğin kapsamı ve boyutu, yapılan saldırıların türleri, alınabilecek önlemler, karşılaşılan yeni riskler ve problemlere yer verilmiş ve sonuçta alınması gereken önlemler ve yapılması gerekenler özetlenmiştir.

Her bir bölüm; ülkemizde bu alana katkı sağlayan, bu alanda eğitim almış, tez hazırlamış, çalışmalar yapmış değerli akademisyen, kamu çalışanı ve üst düzey yöneticiler tarafından hazırlanmıştır. Her bir bölüm, birbirinden bağımsız olarak hazırlansa da konu bütünlüğü ve devamlılığının sağlanmasına mümkün olduğunca dikkat edilmiştir. Her bölüm, editörler olarak tarafımızdan değerlendirilmiş, yazarlara bazı konularda uyarılarda bulunulmuş, düzeltmeler yapılması istenilmiş, tavsiyelerde bulunulmuş ve sonuçta yapılan değişiklikler dikkate alınarak bu kitap hazırlanmıştır. Kitapta yazılan bölümler intihal taramasından geçirilmiş, tekrar tekrar kontrol edilmiş ve sonuçta yayımlanmıştır.

Bu kitabın, siber güvenlik ve savunma konusunda yapılacak çalışmalara ışık tutması, yeni çalışmaların yapılmasına katkı sağlaması, bu konuda yapılacak olan işbirliklerini geliştirmesi, konunun boyutunun ve kapsamının daha iyi anlaşılmasına katkı sağlaması ve en önemlisi bilgi güvenliği ve siber güvenlik alanında duyulan ihtiyacı karşılaması, açık kaynak olarak sunulması ile de kaynaklara erişimi kolaylaştırıcı bir başvuru kitabı serisi olması beklenmektedir. Başvuru kitabı olarak hazırlanan bu eser, açık kaynak olarak Bilgi

Güvenliği Derneği web sayfasında (www.bilgiguvenligi.org.tr) kitap serisi olarak yayımlanacaktır. Bu kitapta yer alan tüm hususlar, kaynak gösterilmek kaydıyla kullanılabilir.

Bu kitap ile ilgili en önemli hususlardan birisi; yazarlarımızın açık kaynak olarak bu kitabın yayımlanmasını kabul etmeleri, hazırladıkları bölümler ile ilgili olarak "açık kaynak felsefesini" desteklemeleri, kitap bölümünün basımı ve dağıtımı ile ilgili olarak herhangi bir telif hakkı talep etmemeleridir. Tüm yazarlarımıza bu ulvi davranışlarından dolayı, editörler olarak çok özel teşekkürlerimizi ve şükranlarımızı sunarız.

Kitabın titizlikle hazırlanmasında, kontrolünde ve basılmasında başta yazarlarımız olmak üzere emeği geçen tüm paydaşlarımıza, bu fikri destekleyen Bilgi Güvenliği Derneği YK üyelerimize ve bu kitabın basılmasına verdiği destekten dolayı Havelsan Yönetimine teşekkürlerimizi sunarız.

Faydalı olması ve ülke siber güvenliğinin sağlanmasına katkı sağlaması temennilerimizle...

Prof. Dr. Şeref SAĞIROĞLU
BGD Kurucu Üyesi
Gazi Üniversitesi MF Bilgisayar Mühendisliği Bölümü
Öğretim Üyesi

Prof. Dr. Mustafa ALKAN
BGD Kurucu Başkanı
Gazü Üniversitesi TF EE Mühendisliği Bölümü Öğretim Üyesi

BİLGİ GÜVENLİĞİ DERNEĞİ'NDEN

Bilgi Güvenliği Derneği (BGD); 22.07.2007 tarihinde, Bilgi Güvenliği ve Siber Güvenlik alanında toplumun her kesiminde bilgi ve bilinç düzeyini arttırmak, bu konu ile ilgili teknolojik gelişmeleri izlemek, yerli ve milli teknolojilerin geliştirilmesine katkı sağlamak; bireysel, kurumsal ve ulusal düzeydeki riskler konusunda farkındalık oluşturmak ve kamu-sektör-üniversite işbirliklerini geliştirmek amacı ile kurulmuştur.

BGD'nin vizyonu; "bilgi güvenliği alanında ulusal ve uluslararası düzeyde tarafsız, güvenilir ve etkin bir ulusal sivil toplum kuruluşu olmaktır." BGD amacı doğrultusunda; tüm paydaşlarla işbirliği yaparak mevzuatın oluşturulmasında ve geliştirilmesinde aktif rol almakta, gerçekleştirdiği konferans, sempozyum, çalıştay ve eğitimler ile, yayımladığı rapor ve yazılar ile farkındalığın oluşmasına ve bunun davranışa dönüştürülmesine katkı sağlamaktadır.

Derneğimiz bu kapsamda; "Ulusal Siber Güvenlik Strateji Belgesi" ve "Ulusal Siber Güvenlik Eylem Planı" hazırlanmasına öncülük etmiş, hazırladığı taslak metin kabul görmüş ve sonuçta ülkemizin siber güvenlik sratejisi ve eylem planlarının gecikmeden yayımlanasına katkı sağlamıştır. Aynı zamanda; bu alanda nitelikli insan kaynağı yetiştirilmesi, mesleki yeterliliklerin belirlenmesi, kamu-endüstri-üniversite işbirliklerinin geliştirilmesi, önemli politika ve stratejilerin oluşturulması gibi konularda etkin rol üstlenmektedir.

BGD, "Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı", "Ulusal Siber Güvenlik Stratejisi Çalıştayı", "Veri Merkezleri ve Siber Güvenlik Çalıştayı", "Siber Güvenlik Hukuku Çalıştayı", "Mobil Dünyada Çocuk ve Gençlerin Güvenliği Sempozyumu", "IPv6 Konferansı", "Kritik Enerji Altyapılarının Korunması Sempozyumu", "Ulusal Siber Terör Konferansı", "Siber Güvenlik Yaz Kampı" gibi etkinlikleri düzenleyerek ve destekleyerek bilgi güvenliğinin

dokunduğu her alanda paydaşlar oluşturmuş ve Cumhurbaşkanlığı, BTK, UAB, MEB gibi farklı paydaşlar ile çalışmaktadır.

BGD, yayın hayatında da CyberMag Dergisi ile toplumun tüm kesimlerine ulaşmaya çalışmaktadır. BGD, 2018 yılında 11. sini düzenlediği "Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı" kısaca ISCTurkey Konferansı olarak bilinen uluslararası etkinlik ile kurulduğu günden bu yana kamu kurumları, özel sektör ve üniversiteleri bir araya getirmeyi başarmıştır. Bu konferansın sonuç bildirgelerinde yer alan husular Siber Güvenlik alanında çalışan akademisyenlere, şirketlere ve kamu kurumlarına ve ilgili paydaşlara yol gösterici olmuştur.

Bununla birlikte, Bilgi Güvenliği alanında ulusal ve uluslararası düzeyde tarafsız, güvenilir ve etkin bir ulusal, sivil toplum kuruluşu olan Bilgi Güvenliği Derneği'nin bünyesinde bir gençlik platformu olarak oluşturulan BGD Genç; Bilgi Güvenliği Derneğimiz ile birlikte; bireysel, kurumsal, ulusal ve evrensel boyutlarda bilgi ve iletişim güvenliği alanında teknik, bilimsel, sosyal ve kültürel faaliyetler yürütmek, orta ve yüksek öğrenim gören genç üyelerimizin mesleki gelişimini artırmak, Siber Güvenlik alanında farkındalık oluşturmak, ülkemizin Siber Güvenlik Uzmanı insan kaynağını oluşturmak için gençlerimizin bu alana ilgilisni artırmak için kurulmuştur. Yapılan çalışmalar ile Siber Güvenlik alanında ülke yeteneklerini artırmaya hizmet etmektedir.

ISCTurkey etkinlikleri, BGD tarafından Gazi Üniversitesi, İstanbul Teknik Üniversitesi ve ODTÜ işbirliği ile düzenlenmekte ve Ulaştırma ve Altyapı Bakanlığı ile Bilgi Teknolojileri ve İletişim Kurumu tarafından desteklenmektedir. Bu etkinlik, Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) tarafından "Avrupa Siber Güvenlik Ayı" platformu etkinliklerine dâhil edilen ilk ve tek etkinliktir. Ayrıca, düzenlendiği ilk yıldan beri ülkemizin Siber Güvenlik alanındaki bilimsel ve sektörel çalışmaların paylaşıldığı, üniversite-kamu-endüstri işbirliğinin geliştirildiği, kamunun bilgilendirildiği, paydaşların eğitildiği, tüm bilim insanları, araştırmacılar ve sektörel uygulayıcılar arasında bilgi alışverişini sağlayan ülkemizde bu alandaki en önemli etkinliktir.

Bu etkinliklere ilave olarak, ülkemizde siber güvenliğe bakış açımızı geliştirmek, ülkemizde bu alanda başvuru kitabı olmak, bu alanda

yapılan çalışmalara yenilerini eklemek ve en önemlisi, açık kaynak olarak paylaşılacak olan bu kitap serisi çalışmasının ülkemizin siber güvenliğine katkı sağlamasını dileriz.

Bu kitabın hazırlanmasında katkı sağlayan, başta editörlerimiz olmak üzere yazarlarımıza, sponsorlarımıza ve bugüne kadar ülke bilgi güvenliği ve siber güvenliğine ve bu alanın gelişimine katkı sağlayan BGD yöneticilerimize ve üyelerimize şükranlarımı sunarız.

Bu kitap serisinin, ülkemiz siber güvenlik ve savunma çalışmalarına katkılar sağlamasını gönülden dileriz.

Bilgi Güvenliği Derneği Yönetim Kurulu

ÖN SÖZ

Günümüzde siber güvenlik, beşinci savaş ortamı olarak kabul edilmenin ötesinde tüm ülkeler için ulusal güvenliğin ayrılmaz ve en önemli bileşeni olarak değerlendirilmektedir.

Yerli, güvenilir, yenilikçi ve yüksek kaliteli Siber Güvenlik çözümleri geliştirerek ülkemizin siber güvenliğinin sağlanmasında ana unsur; uluslararası pazarlarda güçlü ve güvenilir Siber Güvenlik teknoloji ve hizmet sağlayıcısı olmak vizyonu ile çalışmalarını yürüten HAVELSAN, ülkemizin siber uzayda güvenliğini sağlayacak bir mükemmeliyet merkezi olmak, ülkemizin yetenek ve kaynaklarının etkin kullanılmasına öncülük etmek adına var gücüyle çalışmalarını sürdürmektedir.

Bir Türk Silahlı Kuvvetlerini Güçlendirme Vakfı şirketi olan HAVELSAN tarafından hayata geçirilen Siber Savunma Teknoloji Merkezi çatısı altında siber güvenlik operasyon merkezi hizmetleri, kurumsal siber güvenlik danışmanlık ve destek hizmetleri, güvenlik analiz ve test hizmetleri, siber güvenlik eğitimleri ve yerli siber güvenlik ürünleri geliştirme faaliyetleri yürütülmektedir.

Siber güvenlik alanında ülkemizin nitelikli insan kaynağını artırmak için Türkçe kaynak ihtiyacının en az bu alanda verilen eğitimler kadar değerli olduğunun bilincinde olan HAVELSAN, bu ihtiyacı karşılayacak değerli bir yayın olarak gördüğü bu kitabı desteklemektedir.

Ahmet Hamdi ATALAY
HAVELSAN Genel Müdürü

Siber Güvenlik ve Savunma: Önem, Tanımlar, Unsurlar ve Önlemler

BÖLÜM 1

Prof. Dr. Şeref SAĞIROĞLU

SİBER GÜVENLİK VE SAVUNMA: ÖNEM, TANIMLAR, UNSURLAR VE ÖNLEMLER

"Siber Güvenlik ve Savunma Kitapları Serisi" çalışmalarında anlatılan hususları ve sunulan konuların önemini daha iyi anlamak, anlatılanları kavramak, işin felsefesini öğrenmek ve kısaca konulara hızlı bir giriş yapmak için bu bölüm hazırlanmıştır. Bu kapsamda; siber dünyada kullanılan terimler ve kavramlara yer verilmiş, mümkün olduğunca kullanılan terimler açıklanmış, tanımlar yapılmış, siber güvenlik ve savunma bakış açısı tanımlanmaya çalışılmış, konunun önemi üzerinde durulmuş ve son olarak ta karşılaşılabilecek tehdit boyutları, en önemlisi çok basit olarak alınması gereken önemler açıklanmıştır.

Bu bölümde sunulan terimler mevcut sözlükler, TDK sitesi, internet siteleri ve kişisel deneyimlerim ve bilgi birikimim temel alınarak hazırlanmış ve bu bölümde sunulmuştur.

1.1. Tanımlar

Siber güvenliğin ve savunmanın daha iyi anlaşılması ve yüksek seviyede bir koruma sağlanması için tanım ve terminolojilerin iyi bilinmesi ve bu kavramının doğru anlaşılması gereklidir. Siber dünyamıza baktığımızda karşımıza pekçok terim çıkmaktadır. Her geçen gün de bu tanımlara yenileri eklenmektedir. Bu terimlerden bazıları sıralanırsa; siber savaş, siber varlık, siber olay, siber zorbalık, siber casusluk, siber silah, siber polis, siber suç, siber suçlarla mücadele, siber terörizm, siber terörist, siber saldırı, siber tehdit, siber güvenlik, siber savunma, siber psikoloji, siber sağlık vb. gibi kelimeler olduğu görülmektedir. Dikkat edilebileceği gibi kullanılan pekçok kelimenin başına siber kelimesi eklenmiş ve yeni kelimeler, terimler ve ifadeler oluşmuştur. Temel terimler; elektronik ortamları daha iyi anlamak, bu ortamlarda işlenen, saklanan, aktarılan,

değiştirilen, üretilen, yok edilen veya analiz edilen verileri daha iyi anlamak ve kavramak, işin mantığını öğrenmek, konuyu daha hızlı kavramak açısından önemlidir.

Kişisel gözlemim; en temel terimimiz olan "veri" veya "bilgi" gibi terimleri bile tam tanımlayamadığımız veya eksik tanımladığımızdır. Hatta, herşeye bilgi dediğimiz, veri, bilgi ve özbilgi gibi kavramları birbirinden ayrıştıramadığımızdır. Dolayısıyla; korunulacak olan varlıkların farkında olmak, "veri", "bilgi", "özbilgi", "güvenlik", "bilgi güvenliği", "siber güvenlik" veya buna benzer temel kavramları bilmek, anlamak ve kavramaktan geçmektedir. Onun için bu kitap serisinde kullanılacak olan terimler, mümkün olduğunca bu bölümde aşağıda tanımlanmış ve temel kavramlar kısaca farklı başlıklar altında açıklanmıştır.

Veri, bir durum hakkında, birbiriyle bağlantısı henüz kurulmamış bilinenler veya kısaca sayısal ortamlarda bulunan ve taşınan sinyaller ve/veya bitler olarak tanımlanabilir. TDK web sitesinde verinin tanımını, aşağıda verilen şekilde yapmaktadır.

1. Bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge, muta, done: *"İstatistik veriler."*- .
2. Bir sanat eserine veya bir edebî esere temel olan ana ilkeler: *"Bir romanın verileri."*- .
3. Bilgi, data.
4. *matematik* Bir problemde bilinen, belirtilmiş anlatımlardan bilinmeyeni bulmaya yarayan şey.
5. *bilişim* Olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi.

Bilgi, verinin bir üst formu olup, verinin değerlendirilmiş, analiz edilmiş, düzenlenmiş ve verinin belirli bir anlam ifade edecek forma dönüştürülmüş halidir. Claude Elwood Shannon bilginin; "belirsizliği giderdiğini" ve "bir konu hakkında var olan belirsizliği azaltan bir kaynak" olduğunu belirtmektedir. Bu terim, Türk Dil Kurumu web sitesinde aşağıda verildiği şekilde tanımlandığı görülmştür.

1. İnsan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bili, malumat.
2. Öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek, malumat, vukuf.

3. İnsan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü, malumat, vukuf.
4. *felsefe* Genel olarak ve ilk sezi durumunda zihnin kavradığı temel düşünceler, malumat.
5. Bilim: *"Doğa bilgisi."*- .
6. *bilişim* Kurallardan yararlanarak kişinin veriye yönelttiği anlam.

Bazı sözlüklerde ise bilgi; "öğrenme, araştırma ve gözlem yoluyla elde edilen her türlü gerçek, malumat ve kavrayışın tümü" olarak ifade edilmektedir. Farklı kaynaklarda, bilginin tanımının da farklı şekilde yapıldığı, sahip olunan bilgi birikimi ve alan uzmanlıklarının bu tanımları yaparken etkili olduğu belirtilmektedir. Sahip olunan bilgi birikimi, alınan eğitim, yaşanılan kültür, bulunulan ortam, sahip olunan yetenek gibi unsurlarda bu tanımları etkilemektedir. Bilginin literatürde farklı tanımları mevcut olsa da bilgisayar mühendisliği bakış açısıyla bilgiyi en iyi tanımlayan ifadelerin; "işlemiş veri", "üzerinde analiz edilmiş veri", "belirsizliği azaltan varlık" veya "anlamlı ifadeler bütünü" olduğudur. Bilginin "değerli" veya "değersiz", "güncel" veya "değil", "doğrulanabilir" veya "doğrulanamaz" "faydalı" veya "faydasız", "erişilebilir" veya "değil" oluşu, bilginin kendisi kadar önemlidir. Sahip olunan bilgilerin değerinin bilinmesi; imaj, itibar, saygı, değer gibi insani, ahlaki, stratejik veya maddi kayıpların önlenmesi veya azaltılması için önemlidir.

Özbilgi (knowledge), tecrübe veya öğrenme şeklinde veya iç gözlem şeklinde elde edilen gerçeklerin, doğruların veya bilginin, farkında olunması ve anlaşılmasıdır. Diğer bir ifadeyle, ne, niçin, nasıl ve kim olduğunu bilmektir. Kısaca; olayı bilme, olayın altında yatan ilke ve yasaların farkında olma, bu olayı çözebilme becerisi, neyin nasıl yapılacağını kavramadır.

Siber, hepimizin artık kullanmaya alıştığı bir kelime olsa da henüz TDK web sitesinde bulunmamaktadır. Bu kelime aranıldığında "siber sözü bulunamadı. 26 Eylül 2006 tarihinden itibaren 650.608.052 kez söz arandı." gibi bir açıklama web sitesinde yer almaktadır. 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planında, TDK'ya bu alanda terminolojileri geliştirme görevi verilse de bugüne kadar bu konuda herhangi bir geliştirme maalesef sağlanamamıştır. Siber, tanım itibarıyla "elektronik ortamları" ifade etse de içerisinde çok

farklı unsurları barındırmaktadır. Bu unsurların bulunduğu, işletildiği, yönetildiği ve geliştirildiği ortamlarda bulunan veriler; "bilgisayar, sunucu, cihaz, donanım, yazılım, protokol, algoritma, işlem, politika, süreç, laboratuvar ve sistem" gibi unsurları içermektedir. İnsanda, artık siber dünyanın önemli unsurlarından birisidir.

Siber güvenlik, veri, işlem, süreç, politika, deneyim, kapasite, insan ve sistemlerin güvenliğinin siber ortamda sağlanmasıdır. Ulusal stratejide siber güvenlik; *"siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilgi/verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesi"* olarak tanımlanmıştır. Uluslararası Telekomünikasyon Birliği (ITU) siber güvenliği; *"kurum, kuruluş ve kullanıcıların bilgi varlıklarını korumak amacıyla kullanılan yöntemler, politikalar, kavramlar, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulama deneyimleri ve kullanılan teknolojiler bütünü"* olarak tanımlamaktadır.

Siber varlık, siber ortamlarda bulunan, araçlar, işlemler, dokümanlar, planlar, dokümante edilmiş düşünceler, veriler veya bilgilerdir. Bu bir bilgisayar, sunucu veya bir ağ cihazı olabileceği gibi kişisel, kurumsal veya ulusal veriler de olabilir. İnternete bağlı televizyon, cihaz, sistem veya araç olabileceği gibi veri tabanı, veri merkezi, veri kayıt sistemi veya kullanılan yazılımlar, donanımlar ve süreçler siber ortamdaki varlıklardır.

Siber olay, siber varlıkların bir şekilde etkilendiği, zarar gördüğü, ihlal edildiği veya çeşitli şekilde oluşan ve üzerinde işlem yapılan durumdur. Elektronik ortamlarda, işlenen verilerin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesi, verilere zarar verilmesi, verilerin ele geçirilmesi veya buna teşebbüs edilmesi gibi konular buna verilebilecek örneklerdir. Bir siber saldırı sonucu elektriklerin kesilmesi, haberleşme sistemlerinde oluşan bir ihlal veya buna benzer bir durum, "siber olay" olarak ifade edilmektedir. ABD'de bir güvenlik enstitüsü bir siber olayı, "sistematik yapılar veya fonksiyonlar üzerinde etkiye sahip değişikler" olarak tanımlanmaktadır. Sosyal mühendislik saldırılarının da bu kapsamda değerlendirildiğini belirtmekte fayda vardır.

Siber uzay, "siber alan" veya "siber dünya" olarak ta bilinmektedir. Siber uzay; ulusal strateji dokümanında "tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan veya bağımsız bilgi sistemlerinden oluşan sayısal ortam" olarak tanımlanmaktadır.

Siber savaş, sahip olunan siber varlıkların; ulusal çıkarlar ve menfaatler çerçevesinde korumak için karşı tarafın bilişim sistemlerine zarar vermek, hizmetlerini durdurmak veya bozmak için bir başka ülkenin BT sistemlerini yavaşlatmak, bozmak, hizmetini aksatmak veya ele geçirmek amacıyla yapılan saldırılardır. Aynı zamanda, yapılacak saldıra karşı koymak için başvurdukları bir durumdur. Kendine has dünyası veya kuralları olan, kuralsız bir şekilde topluluklar, saldırganlar, sistemler ve hatta devletler arasında siber silahlar kullanılarak yürütülen simetrik, asimetrik veya hibrit yaklaşımların kullandığı savaş şeklidir.

Siber casusluk, çoğunlukla elektronik ortamları kullanarak yapılan casusluğa verilen isimdir. Ülkelerin sahip olduğu internet, bilgisayar, cihaz, yazılım veya bunların bağlı olduğu ve hizmet verdiği ağlar ve sistemler üzerinde bulunan bilgi varlıklarının; elektronik ortamda oluşan açıklıklar, bulunan zafiyetler, sahip olunan tehditler, yapılan saldırılar, bilerek bırakılan açık kapılar ve kullanılan yazılım ve donanımlar üzerinden bilgi varlıklarını belirli bir çıkar için ele geçirme, bilgi sızdırma, amaca uygun faaliyetler yürütmekdir.

Siber silah, elektronik ortamda saldırı ve savunma amaçlı olarak kullanılabilecek her türlü araçtır. *"Kötücül amaçlı yazılım veya kod parçaları"* olarak ifade edilmektedir. NATO'ya göre siber silah, *"saldırı yeteneğine sahip olan ve karşıya zarar veren yazılım veya kod parçasıdır".*

Siber terör, terörizm ve **terörist,** Siber Terörle Mücadele: Tehditler ve Önlemler Ulusal Konferansı Sonuç Bildirgesinde (www.siberteror.org), siber terör ve terörizmle ilgili olarak terimlerin ve kavramların tekrar tartışılmasına ve tanımlanmasına katkı sağlamıştır. **Siber Terörizm**, *"terör örgütlerinin faaliyetlerinde siber ortamın sunduğu kolaylıkları, uygulamaları, araçları, altyapıları, teknik ve teknolojileri, boşlukları, zararlı yazılım ve içerikleri bulup kullanarak, tuzak kurarak veya yeni yöntemler geliştirerek hedefi doğrultusunda kişileri, toplumları veya ulusları yönlendirme, yıldırma, bezdirme, sindirme, zarar verme ve çıkar elde etme amacıyla yapılan faaliyetler"* şeklinde tanımlanmıştır.

FBI **Siber Terörizmi**, *"planlı ve politik amaçlara hizmet etmek amacıyla planlı olarak kimliği belirsiz kişiler tarafından gerçekleştirilen, barışçıl kişileri hedef alan, verilere, bilgisayar sistemlerine, bilgisayar programlarına ve platformlara yap*ılan *saldırılar"* olarak tanımlamaktadır. **Siber Terör**, *"siber ortamda bulunan her türlü hizmeti, açıklığı, altyapıyı, uygulamayı, zararlı yazılımları ve/veya içerikleri, her türlü boşluğu veya fırsatı kullanarak kişileri, toplumları, kurumları veya ulusları yönlendirme, yıldırma, bezdirme, sindirme veya zarar verme amacıyla doğrudan veya dolaylı olarak yapılan faaliyet"* olarak tanımlanmıştır. **Siber Terörist**, *"siber ortamda bulunan her türlü hizmeti, açıklığı, altyapıyı, uygulamayı, zararlı yazılımları, boşluğu veya fırsatı kullanarak hedefi doğrultusunda kişileri, toplumları, kurumları veya ulusları doğrudan veya dolaylı olarak amacı doğrultusunda yönlendiren, yıldıran, bezdiren, sindiren veya zarar veren, çıkar elde eden, bu tür faaliyetlere yardım yapan veya destek veren kişi"* olarak tanımlanmıştır.

Siber caydırıcılık, *"sanal ortamlarda karşılaşılabilecek tehdit ve tehlikelere maruz kalmamak için saldırganlığı önleme, engelleme ve önlem alma girişimleri"* olarak ifade edilebilir. Diğer bir ifade ile *"saldırıları veya saldırganları amacından vazgeçirmek", "korkutarak cesaret kırmak ve vazgeçirmek için temel üstünlüklere sahip olma girişimlerinin tümü"* olarak ta tanımlanabilir. Bu konu, Bölüm 7'de detaylı açıklanmıştır.

Siber güvenlik, *"siber ortamlarda karşılaşılabilecek tehdit ve tehlikeler ile oluşabilecek riskleri önceden öngörüp bunlara karşı önceden önlem alma girişimi", "siber varlıkların tehdit ve tehlikelerden korunması için doğru teknolojiler, yöntemler, çözümler, önlemler, politikalar, standartlar, testler gibi girişimlerin doğru amaç, hedef veya* şekilde kullanılarak *siber varlıkların veya sistemlerin istenilmeyen kişiler/sistemler tarafından elde edilmesini önleme girişimi"* veya *"siber ortamlarda oluşacak riskleri minimize etmek ve yönetmek"* olarak ta tanımlanabilir.

Bilgi güvenliği, *"bilginin bir varlık olarak tehditlerden veya tehlikelerden korunması için doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak, bilgi varlıklarının her türlü ortamda istenmeyen kişiler tarafından elde edilmesini önleme girişimi"* olarak tanımlanır. Diğer bir ifadeyle, *"kişi ve kurumların BT kullanırken karşılaşabilecekleri tehdit ve tehlikelerin daha önceden analizlerinin yapılarak gerekli önlemlerin önceden alınmasını sağlama"* işlemleridir. Kısaca, "öneme sahip veya değerli bilginin korunmasına yönelik çabaların tümü" olarak tanımlanabilir.

Parola/Şifre, bilgisayarlar ve bilgisayar sistemlere erişim güvenliğini sağlamak için kullanılan karakter dizileridir. Parolalar, bilgilere, bilgisayarlara ve sistemlere doğrudan erişim sağladığından dolayı önemlidir ve korunması gereklidir. Bu terimler sıkça karıştırılmaktadır. İkisinin de farklı tanımlar olduğu ifade eden kaynaklar vardır. Bu kelimeler, Fransızca chiffre (şifre) ve parole (parola) sözcüklerinden Türkçemize geçmiş olup sırasıyla rakam (chiffre) ve söz (parole) anlamına gelmektedir. İngilizce sözlüklere bakıldığında ise hem şifre hem de parola anlamına gelen "password" kelimesi karşılığı olarak ifade edilmektedir. Çevirisi yapıldığında "geçiş veya erişim kelimesi" olarak ifade edilebilir. **Şifreler**, geri dönüştürülebilir veya dönüştürülemez metinlerden oluşur, aksi gerekmediği sürece ASCII karakterleri şeklinde olurlar. **Parola** ise, herhangi bir okunabilir, seçilmiş ve gizli tutulması gereken kelimedir. "Parola" kelimesinin kullanımının daha doğru olduğunu düşünüyorum.

Parola güvenliği, başkaları tarafından tahmin edilmesi zor bir karakter dizisi seçilerek sağlanabilir. Yeterli zaman ve kaynak olduğu sürece her parolanın kırılabileceği düşünülse de zor bir karakter dizisinin bu süreyi uzattığı bilinmektedir. Seçilen parolanın kısa, sözlükte bulunabilecek kelimelerden oluşması, tahmin edilebilmesi, kendi ismi veya soyadı olması veya çok basit kelimelerden oluşması karşılaşılan güvenlik zafiyetlerindendir. Parola seçiminde; karakter uzunluğu seçimi, seçim içerisinde rakam bulunması, büyük ve küçük karakter içermesi, @, $, %, ^, !, & gibi özel karakterlere yer verilmesi ve sonuçta bu karakterleri bir arada kullanma, şifrenin kırılmasına karşı koyma açısından çok önemlidir. Belirtilen hususlara dikkat edilerek seçilen ve farklı yazım biçiminden oluşan parolaya "@TaTüRk!9!9" gibi bir örnek verebilir.

Reklam yazılımı (adware), BT kullanıcı alışkanlıklarını izleyerek bunları merkezi bir noktaya aktaran, kullanıcıyı hedef üye sitelere yönlendirerek o sitelerin yüksek ziyaret oranlarına sahip olmalarını sağlamak gibi korsan işlemleri yerine getiren yazılımdır.

Virüs, işletim sistemleri de dahil olmak üzere kendini bir taşıyıcıya yerleştirerek yayılan kötücül kod parçasıdır. Tek başına çalışamadıkları için, aktif hale gelebilmeleri için taşıyıcı bir programa ihtiyaç vardır. Bilgisayar sistemlerini en çok tehdit eden yaklaşımları bünyelerinde barındırırlar. Günümüz virülerinin, zekileştiği, otomatik-

leştiği, farklı forma ve formata kolaylıkla dönüşebildikleri bilindiğinden, farklı yöntemleri bünyelerinde barındırmaktadırlar.

Kurtçuk (worm), taşıyıcı kaynaklarını kullanarak tek başına ve farklı bilgisayarlar üzerinde de çalışabilen ve tam bir kopyasını oluşturabilen programlardır. Zararsız gibi görünürler, bulaştığı program veya bilgisayarın normal çalışmasını bozmadan işlerini veya görevlerini arka planda kullanıcının dikkatinden uzak bir şekilde yaparlar.

Casus yazılım, casusluk faaliyetlerini yapmak üzere geliştirilen kötücül amaçlı yazılımlardır. Bunlar, sadece bir fonksiyonu yerine getirmenin yanında tüm bilgisayar etkinliklerini takip edebilirler, saklayabilirler, raporlayabilirler, eposta ile 3. taraflara gönderebilirler veya sms atabilirler, ftp'ler ile topluca gönderebilirler, vb. pekçok işlemi yapabilirler.

Saldırı, en basit tanımlama ile siber ortamlar**ın za**fiyete uğratılması veya suistimal edilmesi için yapılan girişimlerdir.

Güvenlik modelleri; siber güvenlikte farklı amaçlar için kullanılmaktadır. Bunlar, şifrelemelerde kullanılan teknikler veya algoritmalar olabileceği gibi protokoller, Bell-LaPadula, Harrison-Ruzzo-Ullman, Çin Duvarı, Biba, Clark-Wilson vb. güvenlik modelleri olabilir.

APT (Advanced Persistent Threat), "gelişmiş sürekli tehdit", "hedef odaklı saldırı", "ileri düzey sürekli tehdit", "ileri düzey kalıcı tehdit", "ileri düzey saldırı" veya "ileri düzey tehdit" olarak literatürde bilinmekte ve bu isimler altında tanımlanmaktadır. Tanımlamalardan da anlaşılacağı üzere; ileri düzey, özel ve kapsamlı saldırıları içerisinde barındıran bir saldırıya verilen isimdir. Geliştirilmeleri, bulaştırılması ve operasyonel olarak kullanımı, çok amaçlı kullanım maksatlı değil belirli bir hedefe yönelik olarak yapılırlar. Dikkatli ve sistematik bir çalışmanın ürünü olup, kapsamlı bilgi birikimine, deneyime ve uzmanlığa ihtiyaç vardır. Geliştirilmesi veya keşfedilmesi zor ve uzun zaman alır. İleri düzey ve seviyede motivasyon içerirler. Bu saldırı türüne bakıldığında; içerisinde sıfır gün saldırıları bulunan, işletim sistemi ve mimarilerinin zafiyetlerini kullanan, sinsice saklanan ve geleneksel metotlar ile bulunamayan, içerisinde casus yazılımlar olabilen, anti viral yazılımların tespit etmesinin mümkün olmadığı, ileri düzey teknik ve teknolo-

jileri kapsayan, ileri düzey uzman olmayan kişilerin fark etmesinin mümkün olmadığı, son dönemde de yapay zeka yaklaşımlarını da içinde barındıran kapsamlı saldırılardır. Bu saldırılara en iyi örnek Stuxnet olarak verilebilir. Buna ilave olarak; Flame, DuQu, Wiper, Aurora, Nitro, ShadyRAT, Lurid, Night Dragon verilebilecek diğer örneklerdir. Bugün için 100'e yakın bu saldırı türüne örnek saldırılar bulunmaktadır.

Fidye yazılımı (ransomware), son dönemde gündemde olan en önemli zararlı yazılım türü olup, oldukça geniş kitleleri etkilemiştir. Bu yaklaşım içerisinde; büyük oranda oltalama veya sazan avlama gibi zararlı yazılımlar barındıran web siteleri aracılığı ile dağıtılırlar. BT sistemlerine ise gönderilen bir e-posta ekine sıkıştırılmış (ZIP) bir dosya, PDF veya Word dokümanı olarak sistemlere bulaştırılırlar. Bu sistemin çalışma mekanizması incelendiğinde; BT sistemine giriş yapılması ile başladığı, bu erişim ile bir şifreleme yaklaşımı kullanılarak girilen veya erişilen sistemde bulunan dokümanlar şifrelenir. Şifreli doküman veya verilerin tekrar deşifre edilmesi için, fidyeci, kullanıcıya bir e-posta gönderir veya irtibat kurar. Gönderilen e-postada durumdan kullanıcı haberdar edilir. Bu durumdan kurtulmak için belirlenen tutardaki fidyeyi belirtilen hesaba, verilen zaman kısıtı içerisinde transfer edilmesi istenilir. Transfer teyidi yapıldığında ise fidyeci, şifreli dokümanı açmak için ihtiyaç duyulacak parolayı, ilgili kullanıcıya gönderir ve veriler deşifre edilir. Fidyecilerin kullandığı yöntem burada çok basit olarak veya en basit haliyle anlatılmıştır. Bunların farklı versiyonlarıda bulunmaktadır. WannaCry, Petya buna verilebilecek güncel örneklerdir.

Sızma (penetration) testi, BT sisteminin mevcut durumunu analiz etmek, varsa üzerinde barındırdığı zafiyetleri, tehditleri, açıklıkları veya zayıflıkları tespit etmek için yapılan ve son dönemlerde ise yapılması rutin haline gelen güvenlik testlerini içeren yaklaşımlarını ifade eder. Diğer bir ifade ile saldırganların sistem zafiyetlerini ve açıklıklarını öğrenmeden, BT sistemine sahip olan kişi veya kurumların, sahip oldukları bilgi varlıklarının ne kadar güvende olduğunu öğrenmeleri ve alınması gereken önlemleri önceden tespit etmek için yapılan testlere verilen isimdir. Son dönemde, kamu kurumlarının bu testleri yaptırmaya başlamaları, ulusal strateji ve eylem planı kapsamında bunun zorunlu hale getirilmesinin amacı ise güvenlik politikalarına ve standartlara uyumluluğu test etmek,

varsa zafiyet ve açıklıkları belirlemek ve önceden gidermek, riskleri ve maliyetleri düşürmek, sistem performansını ve verimliliğini değerlendirmek, gelecekte karşılaşılabilecek olası saldırı, sızma ve istismar girişimlerini belirlemek ve önlemek, ve gelecek planları yaparak güvenliği daha etkin sağlamaktır.

Zafiyet, bir yazılım, donanım, sistem, süreç, tasarım ve üretim aşamalarında kaynaklanan algoritmik, mantık, tasarım, bakım veya test aşamalarında yapılan hatalardan kaynaklanabilecek ve istismara açık olan hususlara verilen addır. Zafiyetlerin, donanım, yazılım, tasarım ve işletimden kaynaklı olabileceği gibi insan faktöründen de kaynaklanabileceği de her zaman hatırda bulundurulmalıdır.

Ulusal Siber Olaylara Müdahale (USOM), 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı kapsamında, ulusal ve uluslararası koordinasyonun sağlanması için kurulmuştur. USOM, hem ulusal ve uluslararası koordinasyon görevini yürütmekte hem de internet aktörleri, kolluk güçleri, uluslararası kuruluşlar, araştırma merkezleri ve özel sektör arasındaki iletişimi gerçekleştirmektedir. Aynı zamanda, ülkemize karşı yapılan saldırıları yakınen takip etmekte, önlemler almakta ve 2000'e yakın Kurumsal SOME ile bu görevi başarıyla yürütmektedir.

Siber Olaylara Müdahale Ekibi (SOME), ülkemizde USOM ile işbirliği içersinde çalışan, kurum ve kuruluşların sorumluluğunu yürüten birim veya ekibe verilen isimdir. Bir siber saldırının tespit edilmesi, tespitin USOM'a bildirilmesi, USOM'dan gelen uyarıların veya bildirimlerin yerine getirilmesi, giderilmesi için atılması gereken adımları bilen ve bunu yerine getiren yetişmiş uzmanları tanımlar. Ulusal Siber Güvenlik Stratejisi ve Eylem Planında SOME'ler, "kurumlarına doğrudan ya da dolaylı olarak yapılan veya yapılması muhtemel siber saldırılara karşı gerekli önlemleri alma veya aldırma, bu tür olaylara karşı müdahale edebilecek mekanizmayı ve olay kayıt sistemlerini kurma veya kurdurma ve kurumlarının bilgi güvenliğini sağlamaya yönelik çalışmaları yapma veya yaptırmakla yükümlü" ekiplerdir. Ayrıca, ulusal strateji dokümanı kapsamında meydana gelen siber olayların önlenmesi, zararlarının azaltılması, kurum BT sistemlerinin kurulması, işletilmesi veya geliştirilmesi ile ilgili çalışmalarda teknik ve idari tedbirler konusunda da ilgili birimlere öneriler sunabilmektedirler.

Truva atı, Çanakkale'de bulunan ve tarihteki örneğinden esinlenerek geliştirilmiş bir casus yazılım türüdür. Genellikle başka bir dosyanın içerisinde saklanarak sisteme sızan ve sistemi ele geçiren bir saldırı türüdür. Mesela, bir resim olduğu düşünülen bir dosyaya tıklandığında, Truva atı yazılımı da devreye girmekte ve hedeflenen görevi yerine getirmektedir.

Dağıtık Hizmet Engelleme (DoS, DDoS) saldırısı, belirli bir internet sitesini erişilmez veya hizmet veremez hale getirme işlemidir. Bu saldırıda köle bilgisayarlar (botnetler) kullanılarak, sahip olunan çok sayıda köle bilgisayarın veya sistemin aynı anda hedeflenen bir hizmet için talep yoğunluğu oluşturarak, sistem erişilemez hale getirilir.

Oltalama, Yemleme veya Sazan Avlama saldırısı (phishing), günümüzde yapılan saldırılar doğrudan veya dolaylı olarak yapılmaktadır. Bu saldırının temel amacı; kullanıcıyı bir şekilde kandırarak bilgilerini, parolasını, kredi kart numarasını veya bunları alabileceği dolaylı bilgileri bir şekilde elde etmektir. Oltalama saldırısı, kullanıcıyı başka bir şey oluyormuş gibi kandıran ve sonuçta saldırganın belirlediği gizli amaca ulaşmada kullandığı bir saldırı türüdür. Mesela; kullanıcıya kendisini bir banka, bir kurum, bir şirket veya bir sosyal medya hesabından gelen bir e posta gibi göstererek; kredi kartı ekstresini tıklatma, parola yenileme mesajı gibi gösterme ve kişisel verileri elde etme, bir dokümanı indirmeni isteyerek bir kötücül yazılım indirtme, önemli bir hususu öne çıkararak bir linke tıklatma şeklinde gösterebilmektedir.

Güvenlik duvarı, bir ağ içerisinde izin verilmeyen içten veya dıştan gelebilecek istekleri veya işlemleri, belirlenen kurallar çerçevesinden önleyen veya bloklayan, sistemleri kendi dışındaki işlemlerden korumak üzere kullanılan yazılım, donanım ya da her ikisinin birleşiminden oluşan çözümleri içeren güvenlik sistemidir.

Bilgisayar korsanı (Hacker), günümüzde sistemlerin yapısını, çatısını veya işleyişini ihlal eden, zafiyetleri kullanarak çıkar elde eden, amacı veya işlevi dışında sistemleri kullanan, kullanıma açan veya zarar veren, genellikle yıkıcı, kötü amaçlı bilgisayar kullanıcılarına verilen isimdir. İlk yıllarda korsanların, bilgisayar biliminin ve teknolojisinin gelişimine katkı veren üstadlar olduğu, bu alanın gelişimine büyük katkılar sağladıkları, saygın araştırmacılar oldukları,

öncül görevler üstlendikleri bilinmektedir. Bunlara örnek olarak; Linux'un geliştiricisi Linus Torvalds, GNU projesinin lideri Richard Stallman, Microsoft'un patronu Bill Gates aslında bilinen ünlü bilgisayar korsanlarıdır. Eric Steven Raymond ise bilgisayar korsanını "çoğu BT kullanıcının aksine yazılım, donanım ve sistemlerin ayrıntılarını bilmekten, incelemekten ve öğrenmekten hoşlanan ve sistem yeteneklerini geliştiren uzman" olarak tanımlamaktadır.

Saldırı tespit/Koruma sistemi (IDS/IPS); bir bilgisayar, sunucu veya ağ sistemine yapılan saldırıları, izinsiz erişimleri veya sızmaları tespit ederek, bunu bir uyarıya (alert) dönüştüren ve sistemleri saldırılardan koruyan sistemlerdir.

Sosyal mühendislik ve saldırıları; günümüzde bilinen dört önemli saldırı türünden birisidir. Bu saldırıların temel amacı; sistemlerin, bilgisayarların veya ağların suistimal edilmesi yerine, insanları yani kurbanları kandırmaya, duyguları istismar etmeye, zafiyetleri veya zayıflıkları kullanmaya dayanmaktadır. Bu saldırganlar; kurbanlarını başka birisi olduklarına ikna edenler, yakınlık kurarak sırlarını alanlar, güvenlik uzmanı olarak sistemlerini koruyacaklarını söyleyenler, kendilerini yardımsever olarak gösterenler, kişilere beklemedikleri samimiyeti ve desteği sunanlar, kişilerin zafiyetlerini iyi anlayanlar, bunlara verilebilecek örneklerden bir kaçıdır.

İki adımlı kimlik doğrulama; adından da anlaşılabileceği gibi kimlik doğrulama işlemini iki basamakta tamamlama işlemlerini kapsar. Bu doğrulama, kullanıcıların parola yanında ikinci bir erişim kontrol adımını sisteme ekleyerek, kullanıcının farklı bir şekilde sisteme giriş yapmasını sağlar. Örneğin, internet bankacılığında telefonlara gelen bir SMS, buna örnek verilebilir. Böylece sadece kullanıcı adı ve parola ile sisteme giriş yapılabileceğinden ve telefona yani diğer bir ortama gönderilen kısa onay kodu ile güvenlik kademeli hale getirilir ve güvenlik artar. Bu kimlik doğrulama, oluşabilecek ihlalleri büyük oranlarda düşüren bir çözümdür.

Sıfırıncı gün saldırıları; henüz siber güvenlik dünyası tarafından bilinmeyen, uzmanların keşfedemediği, yayımlanmamış açıklıklara sıfırıncı gün (zero day) açığı adı verilmektedir.

Kayıtediciler (activity monitoring system); sistem etkinliklerini takip etmek için geliştirilmiş yazılımlardır. Bir zararlı yazılıma dönüş-

türülebilirler. Hedef sisteme bağlı giriş ve çıkış cihazlarını (klavye, fare, monitör, yazıcı) takip ederler ve her hareketi kaydederek, sisteme izinsiz erişen kişi veya kişilere iletirler. Bu sayede, yazılan her şey karşı tarafa (3. tarafa) gittiği için kullanıcı adı ve parolalar, kredi kartı bilgileri ya da özel yazışmalar, 3. tarafların eline geçer.

Yığın e-posta (spam mail); istenmeyen e-postalara verilen isimdir. Genelde yasa dışı (ilaç, fidye, reklam, porno site vb.) ürünlerin reklamı yapmak için kullanılır. Son zamanlarda kimlik hırsızlığı sebebiyle oltalama saldırıları yapılmaktadır.

Anti-virüs; üzerinde işletim sistemi bulunan her bilgisayar veya telefon başta olmak üzere işletim sistemi olan neredeyse her sistemde kullanılabilen bir güvenlik çözümüdür. Bu yazılımlar, virüsleri ve zararlı yazılımları, imza adı verilen küçük kod parçalarına bakarak tanır ve bunlara karşı sistemin zarar görmesini önler

Şifrebilim veya Şifreleme Bilimi (Kriptoloji); veri, bilgi veya özbilginin şifrelenmesi, saklanması veya istenilmeyen kişilerin anlamasını zorlaştırma veya şifrelenmiş veri, bilgi veya özbilgilerin çözülmesi üzerine *çalışılan bilim dalıdır.* Kriptoloji kelimesinin, Yunanca "kryptos logos" yani "gizli kelime veya dünya" kelimesinden geldiği literatürde belirtilmiş olsa da dilimize Fransızca "cryptologie" kelimesinden girmiştir. Kriptoloji, Türk Dil Kurumu sözlüğünde *"gizli yazılar, şifreli belgeler bilimi veya incelemesi"* olarak tanımlanmaktadır. Kriptolojiyi kısaca "güvenli ve genellikle gizli haberleşmeyi ele alan bilim dalı" olarak tanımlamak mümkündür. Kısaca, matematiksel tabana dayanan uygulamalar ve teknikler üzerinde çalışılan bilim dalı olarak özetlenebilir. Kriptoloji, kriptografi ve kriptoanaliz olarak ikiye ayrılmaktadır. **Kriptografi**, geleneksel olarak, bilginin anlaşılabilir (normal olan) bir formdan/formattan anlaşılamaz bir forma/formata (okunamaz veya anlaşılamaz) hale dönüştürme yöntemlerini içermektedir. **Kriptoanaliz,** kriptografik sistem mekanizmalarını ve yaklaşımlarını inceleme ve çözme bilimidir. Şifrelenmiş verileri çözmek veya onları anlamlı hale getirme yaklaşımlarını içerir. Bu bilim dalı, bir *şifreleme sistemini inceleyerek* zayıf ve kuvvetli yönlerini ortaya çıkarmak, *şifreleri* doğrudan *çözmek, düzmetni şifrelenmiş metinden elde etmek* gibi farklı şekillerde kullanılabilir. Bu işlemler çoğunlukla şifreleme anahtarına sahip olmadan yapılır. Bu bilim dalında, farklı bilgi birikimlerine, deneyim-

lerine, tekniklerine, altyapılara ve yaklaşımlara ihtiyaç duyulabilir. İşlemler sırasında, yoğun istatistik, matematik ve bilgisayar gücüne ihtiyaç duyulmaktadır. **Kriptoanaliz** *yöntemleri, kaba kuvvet ve diferansiyel kriptoanaliz olmak üzere ikiye ayrılır.* **Kaba kuvvet**, bir şifreleme algoritması tarafından kullanılabilecek tüm anahtarları tek tek veya belirli bir mantık çerçevesinde deneyerek kullanılmış olan şifreleme anahtarını bulma yaklaşımı iken, bilinen açık şifreli mesaj çiftleri arasındaki farkların hesaplanması **diferansiyel kriptoanaliz** olarak ifade edilebilir.

Şifreleme algoritması; şifreleme ve şifre çözme işlemlerinde kullanılan algoritmaya verilen isimdir. Genel olarak değerlendirildiğinde şifreleme yaklaşımları, gizli anahtarlı ve açık anahtarlı olmak üzere ikiye ayrılır.

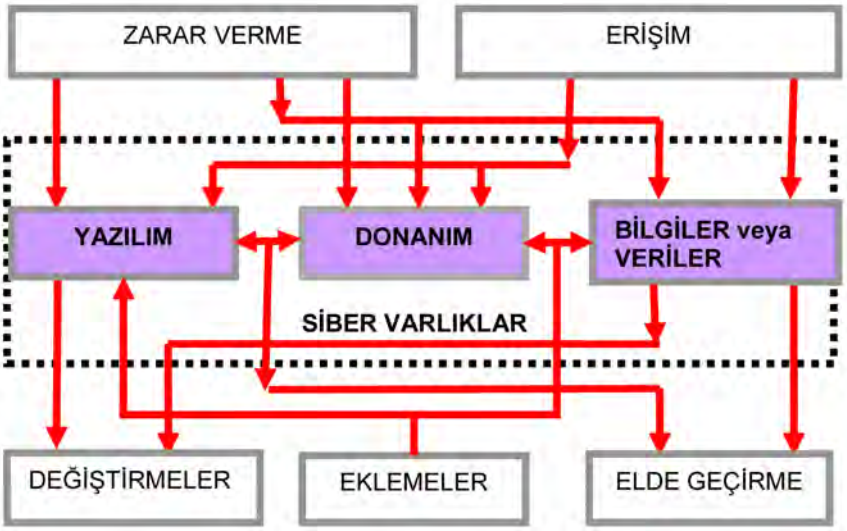
- Simetrik yaklaşım olarakta bilinen gizli anahtarlı yaklaşımda, şifreleme ve şifre çözme için tek bir anahtar kullanılır. En popüler gizli anahtarlı şifreleme yaklaşımı veri şifreleme standardı olarak isimlendirilen DES (Data Encryption Standard)'dir.

- Asimetrik olarakta bilinen açık anahtarlı yaklaşımda, kullanıcı bir çift anahtara yani hem açık bir anahtara hem de gizli bir anahtara sahiptir. Bu anahtarlar, özel (private) veya gizli ve genel (public) veya açık olarak ta isimlendirilir. Açık (genel) anahtar herkese açıkken, gizli (özel) anahtar ise sadece kişiye özeldir. Şifreleme açık anahtarla yapılırken, şifre çözme işlemi gizli anahtarla yapılmaktadır. Bunun terside mümkündür. Açık anahtarlı şifreleme yaklaşımlarında en popüler yaklaşım RSA (Rivest, Shamir ve Adleman)'dır.

1.2. Siber Saldırılar ve Türleri

Siber alanlarda karşılaşılan açıklıkların, tehditlerin, saldırıların veya zafiyetlerin sayısı her geçen gün artmaktadır. Karşılaşılan bu güvenlik açıkları genel olarak değerlendirildiğinde, oluşabilecek açıklar Şekil 1.1'de özet olarak verilmiştir. Şekilden de görülebileceği gibi bir BT sisteminin veya siber varlığın mevcudiyeti, kullanılması veya işletilmesi esnasında, normal kullanımına ilave olarak kötü niyetli davetsiz misafirler, BT sistemlerin sahip olduğu yazılım, donanım ve/veya veri/bilgi varlıklarına; erişilebilir, zarar verilebilir, sisteme

yeni eklemeler yapalabilir, veriler veya yazılımlar kopyalanabilir, veriler veya yazılımlar silinebilir veya yok edilebilir, yeni veriler ve yazılımlar eklenilebilir, siber varlıklar ele geçirilebilir, siber varlıklara zarar verilebilir, veriler değiştirebilir, bilgi veya yazılım verileri çalınabilir, veriler veya bilgiler üzerinde hiç bir işlem yapılmadan sadece okunabilir, çok az bir ihtimal de olsa başka amaçlar için kullanılabilir.



Şekil 1.1. BT Sistemlerine Yapılabilecek Saldırılar ve Türleri

1.3. Siber Güvenlik ve Savunmanın Önemi

Yukarıda verilen tanımlardan ve sunulan şekildende görülebileceği gibi siber güvenlik ve savunmanın kapsamı geniştir. Siber varlıkların başına gelebilecek tehditler incelendiğinde ise bu konunun önemi de daha iyi anlaşılacaktır. Siber varlıkların mecazi anlamda ise dijital toprakların önemi ve değeri de yüksektir. Topraklarımızı nasıl koruyorsak dijital topraklarımızı da aynı hassasiyetle korumak zorundayız.

Siber güvenlik ve savunmanın önemi; aşağıda verilen maddelerde özetlenmiştir.

- Ülkelerin mevcut bilgi ve siber varlıkları, o ülkelerin dijital topraklarıdır. Dijital topraklarımızı veya tüm siber varlıklarımızı korumak zorundayız.

- Kişisel, kurumsal veya ulusal bilgi varlıkları, ülkelerin en önemli değerleridir. Kişisel olarak önemli olduğu kadar, toplumların, kurum veya kuruluşların ve ulusların bilgi varlıklarının korunması için gereklidir. Bunun hukuki ve insani pekçok sebebi olmakla birlikle, kurumsal ve ulusal olarakta önemi yüksektir. Gerek kamunun gerekse özel sektörün siber güvenliğine gereken önemi vermek, ülkenin geleceğine önem vermektir.
- Bilişim toplumu olma yolundaki gayretlerin hızla arttığı ülkemizde, bilişim teknolojisini kullanan her seviyedeki personel, kurum ve kuruluş, bilişim güvenliği kavramını bilmek ve bunu uygulamak zorundadır. Bu malımızı, itibarımızı, sağlığımızı, saygınlığımızı ve belki de canımızı korumak için önemli ve gereklidir. Buna dikkat edilmez ise, kurumsal veya kişisel imajların zedelenmesi, kurumlara veya kişilere olan güvenin sarsılması, iş gücü ve zaman kaybı oluşması, sistemi eski durumuna getirmenin yüksek maliyetlere yol açması, bilgi veya veri kaybı bazen de kaybedilenlerin hiç geri alınamaması gibi ciddi problemleri ortaya çıkaracaktır.

- Siber ortamlar, farklı verilerin, ortamların, sistemlerin, belge ve bilgilerin, süreçlerin, standartların, politikaların ve en önemlisi kritik yapıların bulunduğu ortamlardır. Bu ortamlardaki verilerin boyutu, kapsamı, çeşitliliği artmakta ve bu verilerden değer elde etme ise yaygınlaşmaktadır. Bununla beraber, bu verilerin ihlali, kötüye kullanımı, istismar edilmesi de arttığından, verilerin korunması da gereklidir.
- Veri koruma artık hukuki sonuçlar da doğurmaktadır. Kanun ve yönetmeliklerin uygulanması, yasal yükümlülüklerin yerine getirilmesi için önemlidir ve bir zorunluluktur.
- Siber ortam verilerinin; gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanması hem rekabet gücünü artırma hem de ticari imajı korumak ve sürdürmek için bir zorunluluktur.
- Mevcut varlıkları korumak için; sahtekarlık, casusluk, sabotaj, yıkıcılık, yangın ve sel gibi çok farklı kaynaklardan gelen tehdit ve tehlikelere karşı koymanın yanında virüslere, casus ve kötücül yazılımlara, APT saldırılarına, siber saldırılara, bilgisayar korsanlarına, hizmet saldırılarına karşı koyma, artık kurumlar

kadar her kullanıcı için de önemlidir. Bu tehlikeleri ortadan kaldırmak açısından da siber güvenliği sağlama önemlidir.

- Bilgi sistemlerine ve hizmetlerine bağımlılık, işletmelerin güvenlik tehditlerine karşı daha savunmasız olduğu anlamına gelmektedir. Genel ve özel ağların birbiriyle bağlantısı ve bilgi kaynaklarının paylaşımı, erişim denetimini oluşturmadaki zorlukları artırmaktadır. Ayrıca, yeni teknolojiler, altyapılar, kullanılan algoritmalar, uygulamalar ve hizmetler sürekli değişmekte ve gelişmekte, beraberinde yeni saldırılarıda getirmektedir. Bunlardan dolayı, oluşabilecek tehdit ve tehlikeleri gidermek, güven tesis etmek ve siber güvenliği üst seviyelerde tutmak için de önemlidir.
- Mevcut siber varlıkların korunması, yüksek seviyede bir güvenlik sağlanması, kayıpların en aza indirilmesi, risklerin minimize edilmesi, yeni teknolojilerin geliştirilmesi, yeni bilgilerin üretilmesi, fırsatların yatırımlara dönüşmesi, ülkemizin kalkınması ve uluslararası pazarlarda söz sahibi olması, ve sonuçta sağlıklı bir siber güvenlik ekosistemi ve ekonomisinin oluşturulması için önemlidir.
- Siber ortamlarda; online alışveriş sistemleri, bankacılık sistemleri, elektrik-üretim ve dağıtım tesisleri, akıllı şebekeler, cep telefonu opretatörleri, SCADA sistemleri, haberleşme sistemleri, doğal gaz kontrol ve aktarma sistemleri, hava trafik kontrol merkezleri, bilgisayar ve iletişim sistemleri, buna benzer kritik altyapılar ve ağlar, kritik yazılımlar ve buna benzer pekçok alanda yer alan uygulamalar ve sistemler bulunmaktadır. Bu ortamlara yapılacak saldırılar, ulusal hizmetlerin aksamasına, karmaşa, karışıklık veya kaosa sebebiyet verebileceğinden, siber güvenliğin sağlanması olmazsa olmalar arasındadır.
- Yapay Zeka, Nesnelerin İnterneti, Büyük Veri, Derin Öğrenme, Kuantum Hesaplama gibi yeni yaklaşımların, teknolojilerin, bakış açılarının ve uygulamalarının hızla artış gösterdiği günümüzde yeni tehdit ve tehlikelerin oluşacağı dikkate alındığında, siber güvenliğe ve savunmaya daha fazla ihtiyaç duyulacağı için önemlidir.
- Kullanıcılar ve sistemler için siber güvenliğin sınırları; tarafların verilerini, kendilerini ve sistemlerini güven içinde hissetmeleri

için gerekli ve düzenleyici politikalar doğrultusunda ve hukuki zorunluluklar çerçevesinde belirlenir. Güvenliğin bir kurum veya kuruluşun faaliyete geçmesiyle başladığı, varlığını sürdürdüğü zaman içerisinde süreklilik arz ettiğini belirtmekte fayda vardır. Bu sürekliliğin sağlıklı bir şekilde yürütülmesi, kurum veya kuruluşun büyümesinin veya küçülmesinin kullanıcılar veya sorumlular tarafından dikkatli olarak izlenmesi ve gerekli adımların zamanında atılmasına bağlıdır. Dolayısıyla, bu işlemlerin zamanında yapılması, kaynak israfını önleyeceği gibi, verimliliği ve hizmet kalitesini arttıracak, ve sonuçta daha güvenli siber güvenlik sistemi kurulmuş olacaktır.

Son olarak;

- bilişim sistemlerinin yaygınlaşmasıyla özellikle ülkelerin ve organizasyonların siber varlıklarının temeli olan stratejik bilgilerin üretilmesi, işlenmesi, saklanması ve iletilmesi esnasında, Şekil 1.1'de de özetlendiği gibi, oluşabilecek tehditler potansiyel hedefler olmaya devam edecektir.

- Günümüz rekabet koşulları, çıkar, rant, ekonomik avantaj ve rekabet gücü sağlayacak kişi, kurum ve hatta ülkelerini korumak için siber güvenliğe çok önem vermek zorundadırlar.
- Bilişim toplumu olma yolunda emin adımlarla ilerleyen ülkemizde, bilişim teknolojilerini kullanan her seviyedeki personel, kurum ve kuruluş, *"siber güvenlik kavramını bilmek, farklılığını oluşturmak ve politikalarını belirlemek, siber varlıklarını, itibarlarını ve saygınlıklarını korumak"* zorundadır. Bunun için, siber güvenlk ve savunma önemli bir ulusal meseledir.

1.4. Karşılaşılabilecek Saldırılar ve Tehditler

Günümüzde teknolojiler geliştikçe karşılaşılabilecek tehdit türlerinde azalma beklenirken, maalesef saldırılarda artışlar görülmektedir. Bugün için, yüzbinlerce saldırı türü, milyarın üzerinde kötücül yazılım, onbinlerce siber silah aracı, her yıl yüz binin üzerinde yeni saldırı ve yüze yakın ileri düzey kalıcı saldırı yaklaşımları, vb. bulunmaktadır. APT, casus program sızmaları, açık portları kullanma, TCP/IP korsanlığı, virüsler, casus yazılımlar, kötücül yazılımlar, yığın e-postalar, solucanlar, oltalama veya sazan avlama (phishing),

botnetler, sosyal mühendislik saldırıları, yapay zeka saldırı araçları, vb. bunlardan bazılarıdır.

Literatür incelendiğinde; bunların farklı şekillerde **sınıflandırıldığı** bilinmektedir. Bu sınıflandırmalar aktif ve pasif olarak yapılmaktadır. Bunlar;

- Pasif : Dinleme
- Aktif : Engelleme, değiştirme, üretim

olabileceği gibi

- iç ortamlardan (iç ağdan) veya
- dış ortamlardan (dış ağdan)

yapılan saldırılar olarakta sınıflandırılmaktadır.

Son zamanlarda yapılan saldırılar değerlendirildiğinde, yapılan çalışmalar gözden geçirildiğinde, ve içinde bulunan durum araştırıldığında, saldırıların;

- otomatik yapılan saldırılar
- manuel olarak yapılan saldırılar ve
- hibrit saldırılar

ve/veya

- zeki saldırılar ve
- zeki olmayan saldırılar

ve/veya

- düşük riskli saldırılar,
- orta riskli saldırılar,
- yüksek riskli saldırılar
- kritik veya riskli saldırılar

ve/veya

- ileri düzey kalıcı saldırılar
- geçici olan saldırılar

ve/veya

- kablolu sistemlere yapılan saldırılar
- kablosuz ortamlara yapılan saldırılar

ve/veya

- bilinen yöntemlerle yapılan saldırılar
- bilinmeyen yöntemlerle yapılan saldırılar (sıfır gün saldırıları

ve/veya kullanılan işletim sistemlerine göre yapılan saldırılar

- Linux
- Unix
- Microsoft
- iOS

ve/veya kullanılan yaklaşımlara göre yapılan saldırılar

- Kriptografi,
- Steganografi,
- Kuantum

ve/veya

- otomatik araçlar kullanılarak yapılan saldırılar,
- yeni geliştirilen araçlarla yapılan saldırılar

ve/veya

- profesyonel saldırganlar tarafından yapılan saldırılar veya
- uzman olmayanların yaptıkları saldırılar

ve/veya

- delillendirilebilen (cezalandırılan) saldırılar
- delillendirilemeyen (cezalandırılamayan) saldırılar

olarak ta sınıflandırmalar mevcuttur. Bu sınıflandırmaların temelinde dikkate alınan kriterler incelendiğinde ise;

- saldırganlar
- hedefler,
- risk seviyeleri,
- kullanıcılar,
- bilim dalı,
- sistemler,
- ortamlar,
- verilen zararlar,
- cihazlar,
- yazılımlar,
- altyapılar,
- işletim sistemleri,

- hedef ülkeler ve ortamlar,
- verilen veya alınan hizmetler,
- faydalanılan araçlar, teknikler ve teknolojiler,
- kritiklik seviyeleri, ve
- ihtiyaç duyulan yetenekler

vb. belirlenen hedeflere göre değişiklikler gösterebilir.

Genel olarak değerlendirdiğimizde ve literatür incelendiğinde ise bilgisayar sistemlerinde karşılaşılabilecek tehditler;

- sistemlere izinsiz erişim,
- sistemlere ve verilere zarar verme,
- verilerde değişiklik yapma ve
- veri üretimi

olmak üzere dört farklı başlık altında gruplanmıştır.

1.5. Siber Güvenlik Unsurları

Yüksek seviyede bir siber güvenliğin sağlanması ancak ve ancak aşağıdaki hususlara dikkat edilmesi ve bu unsurların yerine getirilmesiyle sağlanır. Bunlar; gizlilik, bütünlük, kimlik doğrulama, erişilebilirlik, inkar edememe gibi unsurlardır. Bu unsurlar aşağıda kısaca açıklanmıştır.

Gizlilik, "verilerin sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğunu garanti etmektir". Diğer bir ifade ile "verilerin erişim yetkisi olmayan kişilerce elde edilmesini önleme girişimleridir". Bu unsur, şifreleme algoritmaları kullanılarak sağlanmaktadır.

Bütünlük, siber güvenlik unsurlarından bir diğeridir. "Verilerin ve işleme yöntemlerinin doğruluğunu ve içeriğin değişmezliğini sağlamak" veya "verinin bir ortamdan diğerine değişmeden gönderildiğini doğrulamak" olarak tanımlanabilir. Özetleme (parmakizi) fonksiyonları kullanılarak veya farklı fonksiyonlar kullanılarak sağlanır.

Kimlik doğrulama, "yetkilendirilmiş kullanıcıların kimliğinin doğrulanması ve o kişi olduğunun garanti edilmesi" veya "kullanıcı kimliğinin belirlenmesi veya doğrulanması işlemi" olarak tanımlanabilir. Bu unsur, elektronik imza ile sağlanır.

İnkar edememe, aslında adından da anlaşılacağı gibi mesaj veya bilgi kaynağının gönderdiği mesajı veya gönderdiğini yalanlaya-

mamasıdır. Diğer bir ifade ile "yetkilendirilmiş kullanıcının mesaj gönderim veya alım işlemlerinin ispatlanması veya gönderim veya alım işleminin inkar edilememesinin sağlanmasıdır". Bu unsur, açık anahtar altyapısı ve zaman damgası ile sağlanır.

Erişilebilirlik, "yetkilendirilmiş kullanıcıların bilgiye ve ilişkili kaynaklara erişim hakkına sahip olmalarının garanti edilmesi", "yetkilendirilmiş kullanıcıların sistemlere güvenli ve sürekli olarak erişmelerinin garanti edilmesi" veya "hizmetin sürekliliğinin sağlanması için gereken önlemleri alma girişimi" olarak tanımlanmaktadır.

1.6. Saldırılara Karşı Koyma Adımları

Siber saldırılara karşı koyabilmek için belirli bir sistematik içerisinde siber olaylara müdahale etmek, belirli bir adımları takip ederek bu adımları gerçekleştirmek gereklidir. Koruma adımları aşağıda verilmiştir.

(1) Yapılan saldırıları önlemek için bir saldırı tespit ve koruma sistemi yaklaşımı gereklidir. Bu kurulmalıdır.

(2) Tehdidi saptama için bir sistem gereklidir. Bu sistem kurulmalıdır.

(3) Yapılan saldırıların ne zaman, nasıl, kim veya kimler tarafından yapıldığı saptanır. Bunun için kayıtları analiz edecek bir sistem kurulur veya uzmanlıklardan faydalanılır.

(4) Saldırılara karşı koyma (reaksiyon gösterme) işin önemli ve son adımıdır. Saptanan ve tespit edilen tehditler bu adımda giderilir. Karşılaşılan tehditler ortadan kaldırılır ve verilen zararlar giderilir. Sistem kayıplardan arındırılarak, önceki haline dönüştürülür.

1.7. Nasıl Bir Siber Güvenlik ve Savunma

İyi ve yüksek seviyede bir koruma için; siber ortamları, siber varlıkları, saldırıları, saldırganları, saldırı araçlarını, saldırılara karşı koyma tekniklerini, saldırıları önleme teknik ve teknolojilerini, geliştirilen çözümleri, kullanılan uygulamaları, sistemlerin çalışma ve koruma mekanizmalarını, kullanılan algoritmaları, vb pekçok unsuru bilmek, takip etmek, mevcut standartları takip etmek, uygulamak ve denetlemek gereklidir.

Siber sistemlerine yapılan saldırıların birçok sebepleri bulunmaktadır. Bunlar, çok küçük şeyler olabileceği gibi çok büyük gerekçelere de dayanabilmektedir. Saldırıları kısaca değerlendirdiğimizde, bunların gerekçelerinin kişisel, kurumsal veya ulusal olduğu, arkasında artık gelişmiş ülkelerin bulunduğu, ülkeler arası soğuk savaşın bu ortamlarda yapıldığı, siber varlıkları, dijital toprakları ve kişisel, kurumsal ve ulusal çıkarları koruma, çıkarlarına zarar verecek unsurlarla bu ortamlarda doğrudan veya dolaylı olarak savaşma, saldırganlarla mücadele etme, saldırıları yok etme, saldırganları pasifize etme, hızlı bir takip sistemi kurma, suçluları yakalama ve cezalandırma bu ortamlarda yapılan çalışmalardır.

Saldırılar ve saldırganlara baktığımızda; merak, kendini tatmin etme, zarar verme, etkisiz hale getirme, para ve itibar kazanma, itibar azaltma veya yok etme, kişisel kurumsal ve ulusal mahremiyeti öğrenme veya bunlara zarar verme, politik veya dini çıkar elde etme, terörist faaliyetler yürütme, ulusal çıkarlara hizmet etme veya ulusal çıkarları koruma gibi sebeplerin, ana motivasyonlarını oluşturduğu bilinmektedir. Siber sistemlere saldırmak veya sızmak için, saldırganların en kolay yolları bulmaya çalışacakları, en belirgin, en çok beklenilen veya saldırılara karşı en çok önlem alınmış yollar haricinde bunların olabileceğinden dolayı, saldırıların tüm yönleriyle ve kapsamlı olarak değerlendirilmesi gereklidir.

Siber ortamların her zaman güvenlik açıklarının olabileceği veya saldırılara veya sızmalara maruz kalınabileceği hiçbir zaman unutulmamalıdır. BT sistemlerinin; fiziksel güvenlikten haberleşme güvenliğine, yayınım güvenliğinden bilgisayar güvenliğine, ağ güvenliğinden bilgi güvenliğine, cihaz güvenliğinden sistem güvenliğine, yazılım güvenliğinden donanım güvenliğine, bulut ortamlarının güvenliğinden siber güvenliğe kadar birçok tedbirin alınması gerektiği bilinmeli ve korunacak olan siber varlıkların sınıfına, ortamına veya değerlerine göre gerekli güvenlik seviyeleri belirlenmeli ve koruma sağlanmalıdır.

Siber güvenlikte temel hedef; güvenliği **mükemmele yakın sağlama** olmalı, riskler iyi belirlenmeli, giderilmeye çalışılmalı ve iyi bir risk yönetimi yapılmalı, mevcut teknikler, teknolojiler, politikalar, standartlar ve çözümler uygulanarak, belirlenen **siber güvenlik felsefesi** kapsamında çalışmalar yürütülmelidir. Bu felsefede aşağıdaki unsurlar yer almalıdır. Bunlar;

- Bir güvenlik politikası oluşturulmalı ve uygulanmalıdır.
- Gereği kadar koruma prensibi uygulanmalıdır.
- İyi bir risk analizi ve yönetimi yapılmalıdır.
- Sistemlerde oluşabilecek hataları, eksiklikleri ve açıklıkları gidermek için zaman zaman testler (sızma testleri) yapmak ve tüm zafiyetleri gidermek gerekmektedir.
- Sistemleri kullanan her kullanıcıya en az hak verme yaklaşımı benimsenmelidir. Bir kullanıcıya ihtiyaç duyacağı hakları vermenin karşılaşılabilecek problemleri azaltacağı unutulmamalıdır.
- Siber güvenlik standartları (ISO 270XX Serisi Standartlar) yakınen takip edilmeli ve uygulanmalıdır. Bunlara ilave olarak, yakın olan diğer standartlardan da mutlaka faydalanılmalıdır.
- Elektronik ortamların her zaman güvensiz ortamlar olabileceği unutulmadan, sahip olunan bilgi varlıklarının yedeklenmesi veya kurtarılmasına yönelik sistemler (Felaket Kurtarma Merkezi) kurulmalı ve işletilmelidir.
- Güncel tehdit ve tehlikeleri yakınen takip etmek ve varsa da gidermek gereklidir. Ayrıca, gelecek tehdit ve tehlikeleri de önceden öngörmek ve önlem almak ta gereklidir. Buna hazır olacak, mekanizmalar ve yapılar kurmalı ve işletmelidir.
- Güvenli sistem bileşenlerini tanımlama ve güvenlik gerektiren bileşenlerin sayılarını en aza indirgeme temel amaç olmalıdır.
- Siber güvenlik sistemlerini kuran, işleten, yöneten ve güncelleyenlerin güvenlik uzmanları olduğu unutulmadan, siber güvenlik uzmanlarının kendilerini geliştirmelerine fırsatlar verilmeli, bu birimlere daha fazla insan kaynağı ayırılmalıdır. Güvenliği teknik ve teknolojilerin yardımıyla insanların sağladığı veya ihlal edildiği de unutulmadan gerekli tedbirler alınmalıdır.

Sonuç olarak, "yüzde yüz bir güvenliğin" hiçbir zaman sağlanamayacağı yaklaşımıyla, varlıklar (yazılım, donanım, veri, süreç, uzmanlık, vb.) değerleri oranında ve sadece değerleri geçerli olduğu sürece korunmalıdır. Korumak için harcanan süre, çaba, emek ve maliyet, korunacak olan siber varlıkların değerleriyle orantılı olma-

lıdır. Karşılaşılacak riskler, ortak akıl ve bilimsel yaklaşımlar kullanılarak giderilmelidir.

1.8. Değerlendirmeler

İnsanlık tarihi kadar eski olan şifreleme bilimi ve günümüze ışık tutan şifreleme tarihçesi, muasır medeniyet seviyesine ulaşmak isteyen toplumlar için ibret alınması gereken birçok hususu içerisinde barındırmaktadır. Veri, bilgi ve özbilginin barındırıldığı ve iletildiği ortamların güvenliği, gelişmek ve ilerlemek isteyen bütün toplumların üzerinde sürekli durması; yenilikleri takip etmesi ve kendi yöntemlerini geliştirmesi gerekmektedir.

Siber ortam ve sistemlerin güvenliğinin önemini anlamak ve güvenliğini sağlamak için;

- tehditlerin, saldırıların, açıklıkların, teknolojilerin ve çözümlerin boyutunu ve kapsamını görmek ve anlamak,
- kullanılan terminolojileri kavramak,
- mevcut teknik ve teknolojileri bilmek ve yakınen takip etmek,
- standartları bilmek ve uygulamak,
- politikalar oluşturmak ve denetlemek, ve
- siber güvenlik ve savunmada karşılaşilabilecek riskleri minimize etmek ciddiye almak

gerekmektedir. Bu hususlara dikkat edilmesi, karşılaşılabilecek tehdit ve tehlikelerin yüzdesini azaltacaktır. Bu hususların tam bir güvenlik için gerekli fakat yeterli olmadığını burada hatırlatmakta fayda vardır.

Siber Güvenliğin Temelleri

BÖLÜM 2

Prof. Dr. Şeref SAĞIROĞLU
Prof. Dr. Mustafa ALKAN

SİBER GÜVENLİĞİN TEMELLERİ

Bu bölümde, siber güvenlik ve savunma bilimi veya bilgi güvenliği bilimi içerisinde yer alan kriptoloji, steganografi, kuantum şifreleme yaklaşımları ile bunun temelini oluşturan matematiksel fonksiyonlar, şifreleme ve şifre çözme algoritmaları, şifreleme tarihçesi, bilimi, önemi, kullanılan standartlar, özetleme algoritmaları, steganografi bilimi, kuantum şifreleme, elektronik imza gibi hususlara yer verilmiş, siber güvenliğin temelleri kısaca açıklanmıştır.

Hazırlanan bu kapsamlı kitap serisinin bilimsel ve matematiksel altyapısını oluşturan kriptoloji bilimi, literatürde pekçok kaynakta gayet kapsamlı olarak açıklanmış olsa da bu kitap serisi çalışmasında kapsam geniş tutulduğundan, bölümlerde anlatılan konulara bir altlık oluşturulması, konunun daha iyi anlaşılmasına katkı sağlama, temel bilgilerin kapsamlı olarak aktarılması ve bölüm yazarlarının 2005 yılında yayımlanan "Her Yönüyle E-İmza" isimli kitabından alıntılanmış, yayınevinden izin alınarak ve güncellenerek burada sunulmuştur.

2.1. Şifre Bilim Tarihçesi

İlk şifreleme yaklaşımlarının M.Ö. 1900'lerde Mısırlılar tarafından kullanıldığı tespit edilmiş olsa da şifrebilimi tarihçesinin insanla başladığını ifade etmek pek de yanlış bir ifade olmayacaktır. Yapılan araştırmalarda Mısırlıların, hiyeroglif yazılarını değiştirerek, şifreleme yaptığı tespit edilmiştir. M.Ö. 100-44 yılları arasında sunulan Sezar yaklaşımı, birçok bilim insanının da teyit ettiği gibi kullanılan ilk şifreleme yaklaşımlarındandır.

1623'de Francis Bacon'un, 5-bit ikili kodlamayla karakter tipi değişikliğine dayanan bir yaklaşım geliştirmesi, 1790'da Thomas Jefferson tarafından "strip cipher" makinası icat edilmesi bu konuda

yapılan önemli çalışmalardır. Jefferson'ın M-138-A makinasının II. Dünya Savaşında kullanılması ise diğer bir önemli adımdır. 1917'de Joseph Mauborgne ve Gilbert Vernam'ın "One Time Pad-OTP" algoritmasını geliştirmesi diğer bir önemli buluş olarak kabul edilmektedir.

II. Dünya Savaşında şifreleme yaklaşımlarının çok önemli rol oynaması ve yaşanmış acı tecrübeler, şifre bilimine olan ilgiyi ve önemi arttırmış ve yeni şifreleme yaklaşımları geliştirmek için büyük çabalar harcanmıştır. O yıllarda, ABD, ilk kriptoanaliz laboratuarından birisini kurmuştur. Purple Machine ile askeri haberleşmelerde kullanılan şifreleme sisteminin, Alan Turing ve ekibi tarafından da Enigma'nın çözülmesi konuya olan ilgiyi ve önemi daha da arttırmıştır.

Savaş sonrasında, hem askeri ve devlet güvenliğini sağlamak hem de diğer ülkelerin haberleşme bilgilerini ele geçirmek ve kriptografik standartların gelişmesini sağlamak amacıyla Amerika'da *Ulusal Güvenlik Merkezi* kurulmuştur. 1960'larda, bilgisayarların gelişmesi ve iletişim sistemlerinin kullanımının yaygınlaşmasıyla, konuya özel sektörün ilgisi artmıştır. 1970'lerde IBM ile başlayan çalışmalar, ABD Federal Bilgi İşleme Standardının (USA Federal Information Processing Standard) benimsenmesiyle, DES (Data Encryption Standard) veri şifrelemede bir standart olarak kabul edilmiştir. Bu standart, bugün için çok güvenli olmasa da bankacılık, e-imza ve e-ticaret alanlarında hala kullanılan bir şifreleme tekniğidir.

1976 yılında Diffie-Hellman tarafından geliştirilen açık anahtarlı şifreleme yaklaşımı, bundan iki yıl sonra Rivest, Shamir ve Adleman isimli üç bilim insanı, ilk açık anahtarlı şifreleme yaklaşımını pratik olarak gerçekleştirmişlerdir. Geliştirenlerin adlarının ilk harflerinden oluşan bu yaklaşıma **RSA** (**R**ivest, **S**hamir ve **A**dleman) şifreleme metodu adı verilmiştir. Bu yaklaşım, büyük asal tamsayı çarpanlarının etkileşmesi gibi zor bir matematiksel temele dayanmaktadır. Bugün için hala güvenle kullanılmaktadır.

1990'da Lai ve Massey tarafından geliştirilen IDEA ve 1991 yılında Zimmerman tarafından geliştirilen PGP (Pretty Good Privacy) ile şifreleme biliminde büyük gelişmeler kaydedilmiştir. Açık anahtarlı şifrebilimi, bugün için sayısal ortamda bilgi güvenliğinin sağlan-

masında büyük kolaylık sağlayacak olan e-imza ortamının ve altyapısının geliştirilmesine büyük katkı sağlamıştır.

1991'de sayısal imza konusunda ilk uluslararası standart olan ISO/IEC 9796 hayata geçirilmiş olup, RSA açık anahtar yaklaşımı kullanılmıştır. 1994'de ise ABD hükümeti El-Gamal açık anahtar sistem temeline dayalı Sayısal İmza Standardını kabul etmiştir.

DES'in güvenlik ihtiyaçlarını tam olarak karşılayamaması üzerine yeni standartların aranmasına girişilmiş ve yapılan bir yarışma sonucunda Rijndael algoritmasının bu beklentilere cevap verebileceği tespit edilmiştir. Bu algoritma daha sonra AES (Advanced Encryption Standard) adını almış ve 21. YY'da kullanılabilecek bir güvenlik standardı olarak kabul edilmiştir.

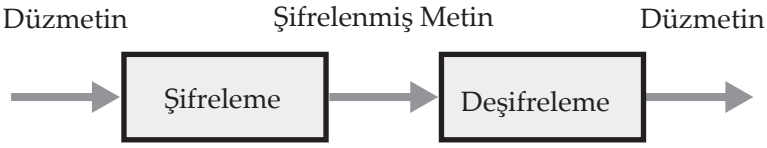
Bilgisayar teknolojilerindeki hızlı gelişmeler ile bilişim teknolojileri kullanımı artmış, bilgi sistemlerini yoğun bir şekilde kullanan toplumun güvenlik ihtiyaçlarını karşılamak için açık anahtar tabanlı yeni araştırmalar, gelişmeler, yaklaşımlar, algoritmalar ile yeni güvenlik yazılım ve donanım ürünleri geliştirilmektedir.

2.2. Şifre Bilim

Siber güvenlik bilimi, günümüzde sadece internet üzerinde değil, mobil ve sabit telefonlarda, bilgisayarlarda, televizyonlarda, ileri teknoloji içeren uydularda, uçak ve füzelerde, ev aletlerinde, beyaz eşyalarda, arabalarda, gemilerde vb birçok alanda kullanılmaktadır. Nedeni ise, saldırganların, korsanların, casusların, meraklıların, iyi niyetli olan veya olmayan kişilerin haberleşme sistemlerini dinlemeleri ve elektronik depolama ünitelerine girip mevcut bilgileri elde etme veya onlara ulaşabilme istekleridir.

Verilerin güvenli olarak bir ortamdan diğerine aktarılmasında veya saklanmasında matematiksel yaklaşımlar sıkça kullanılmaktadır. Şifreleme bilimi **(kriptoloji)**, kriptografi ve kripto analiz olmak üzere iki alanı kapsayan bilim dalıdır. **Kriptografi;** matematik, elektronik, optik, bilgisayar bilimleri gibi birçok disiplini içeren özelleşmiş bir bilim dalıdır. Kabaca, belgelerin veya bilgilerin şifrelenmesi ve şifrelerinin çözülmesi için kullanılan yöntemlere verilen genel addır. Bir başka ifadeyle, üçüncü şahıslar tarafından algılanamayacak veya öğrenilemeyecek farklı bir forma veriyi işleyerek dönüştürme işlemidir. Bu işlemler veri kaybı olmadan gerçekleştirilir. Güvenlik

için kullanılan yaygın bir yaklaşımdır. Matematiksel temele dayanan bu bilimde, matematiksel fonksiyonlar, şifreleme (encryption) ve şifre çözme (deşifre) için kullanılır. *Şifreleme,* düzmetni anlaşılamayacak bir forma dönüştürme işlemidir. Bu işlem, matematiksel bir fonksiyon ve bir anahtar veya anahtar çiftinin biri kullanılarak yapılır. **Deşifreleme** ise, şifrelenmiş mesajı, şifrelemede kullanılan fonksiyonun tersini ve bir anahtar veya anahtar çiftinin diğerini kullanarak düzmetine dönüştürme işlemi olarak tarif edilebilir. Bu işlemleri gösteren akış şeması Şekil 2.1'de gösterilmiştir.



Şekil 2.1. Şifreleme ve Deşifreleme (Şifre Çözme) İşlemleri

Kriptoanaliz ise; kriptografik sistem mekanizmalarını ve yaklaşımlarını inceleme ve çözme bilimidir. Şifrelenmiş verileri çözmek veya onları anlamlı hale getirme yaklaşımlarını içerirler. Kriptoloji içindeki önemi ise çok büyüktür. Ortaya konan bir şifreleme sistemini inceleyerek, zayıf ve kuvvetli yönlerini ortaya çıkarmak için kullanılabileceği gibi, şifrelerin çözülmesi için de kullanılabilir. Şifreleme anahtarı olmadan, düzmetni şifrelenmiş metinden elde etme işlemi olarak bilinir ve bu işlem çoğunlukla şifreleme anahtarına sahip olmadan yapılır. Bu bilim dalında, farklı bilgi birikimlerine, deneyimlerine, tekniklere ve yaklaşımlara ihtiyaç duyulabilir. İşlemler sırasında, yoğun istatistik, matematik ve bilgisayar gücüne ihtiyaç vardır. Bundan dolayı da uygulama alanı sınırsızdır.

Kriptoanaliz yöntemleri, **kaba kuvvet** ve **diferansiyel kriptoanaliz** olmak üzere ikiye ayrılır. *Kaba kuvvet*, bir şifreleme algoritması tarafından kullanılan bir anahtarı veya anahtar çiftini, tüm anahtarları tek tek veya belirli bir mantık çerçevesinde deneyerek, kullanılmış olan şifreleme anahtarını bulma yaklaşımı iken, *diferansiyel kriptoanaliz*; bilinen açık şifreli mesaj çiftleri arasındaki farkların hesaplanması temeline dayanır.

2.3. Şifre Bilimde Kullanılan Teknikler ve Algoritmalar

Şifreleme ve şifre çözme işlemlerinde kullanılan birçok algoritma, teknik ve yaklaşım mevcuttur. Genel olarak değerlendirildiğinde, şifreleme yaklaşımları, kapalı anahtarlı ve açık anahtarlı olmak

üzere ikiye ayrılır. *Kapalı anahtarlı* yaklaşımlar, *simetrik* yaklaşımlar olarak da bilinmektedir. Bu yaklaşımda, hem şifreleme hem de şifre çözme işlemi için **tek bir anahtar** kullanılır. En popüler kapalı anahtarlı şifreleme yaklaşımı veri şifreleme standardı olarak isimlendirilen DES (Data Encryption Standard)'dir. *Açık anahtarlı* yaklaşımlar, *asimetrik* yaklaşımlar olarak da bilinmektedir. Kullanıcı **bir çift anahtara** yani hem **açık** bir anahtara hem de **gizli** bir anahtara sahiptir. Bu anahtarlar, **özel** (private) veya **gizli**, ve **genel** (public) veya **açık** olarak da isimlendirilir. Açık (genel) anahtar, herkese açıkken, gizli (özel) anahtar ise, sadece kişiye özeldir. Şifreleme açık anahtarla yapılırken, şifre çözme işlemi gizli anahtarla yapılmaktadır. Bunun tersi de mümkündür. Açık anahtarlı şifreleme yaklaşımlarında en popüler yaklaşım, RSA (Rivest, Shamir ve Adleman'in baş harflerinden oluşmuştur)'dır.

Simetrik ve asimetrik yaklaşımlar, genel güvenlik unsurları açısından değerlendirildiğinde, ortaya çıkabilecek hususlar Tablo 2.1'de verilmiştir. Tablo 2.1'den de görülebileceği gibi, simetrik algoritmalar hızlı mesaj şifrelemede, asimetrik şifreleme yaklaşımları da yavaş oldukları için anahtar şifrelemede yüksek performans gösteren yaklaşımlardır. Genel olarak ise, asimetrik yaklaşımlar, hesaplama hızları düşük olsa da güvenlik unsurlarının tamamını desteklemeleri açısından çok önemlidir.

Anahtar temelli şifreleme yaklaşımları veya algoritmalar, genel olarak simetrik ve asimetrik olmak üzere ikiye ayrılır. Bu algoritmalar aşağıda detaylı açıklanmıştır.

Güvenlik Unsurları	Simetrik yaklaşımlar	Asimetrik yaklaşımlar
Gizlilik	Sağlar	Sağlar
Bütünlük	Sağlar	Sağlar
Kimlik doğrulama	-	Sağlar
İnkar edemezlik	-	Sağlar
Hesaplama hızı	Yüksek	Düşük
Güvenlik	Anahtar uzunluğuna bağlı	Anahtar uzunluğuna bağlı
Genel değerlendirme	Şifrelemede iyi sonuç veriyor.	Anahtar şifrelemede iyi sonuç veriyor.

Tablo 2.1. Şifreleme Yaklaşımlarının Karşılaştırılması

Asimetrik Algoritmalar

Daha önce de vurgulandığı gibi bu algoritmalar, açık anahtarlı algoritmalar olarak bilinmektedirler. Bu algoritmalarda, şifreleme ve şifre çözme için farklı anahtar çiftleri kullanılmaktadır. Bu anahtarlar çift olarak üretilirler, tek yönlü çalışırlar, fakat birbirlerini tamamlarlar. Bu anahtar çiftinde, şifreleme anahtarı **açık anahtar** veya **genel anahtar** (public key), şifre çözme anahtarı ise **gizli anahtar** (secret key) veya **özel anahtar** (private key) olarak adlandırılır. Simetrik algoritmalardaki gizli anahtarlar ile karıştırılmaması için, gizli anahtar yerine açık anahtar teriminin kullanımı daha yaygındır.

Açık anahtar şifreleme işleminde, açık anahtarlarla şifrelenen düz metinler veya mesajlar, yalnız gizli anahtar kullanılarak deşifre edilebilir. Bu işlemi gösteren yaklaşım Şekil 2.2'de verilmiştir. Gizli anahtar sadece ait olduğu kişide bulunurken, açık anahtar çeşitli şekillerde insanlara iletilebilmektedir, yani açık olarak dağıtılmaktadır. Bu algoritmalara açık anahtarlı algoritmalar denmesinin sebebi, açık anahtarın herkese, yani genel kullanıma açık olmasıdır.



Şekil 2.2. Açık Anahtarlı Şifreleme ve Şifre Çözme İşlemi

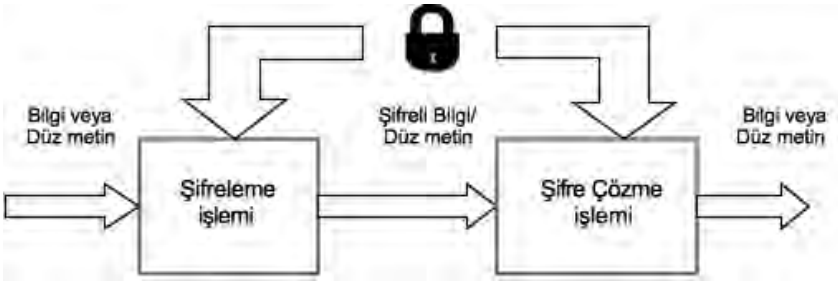
Farklı biri, bir bilgiyi şifrelemek için birinin genel anahtarını kullanırsa, sadece o ilgili birinin özel anahtarına sahip bir kişi, bu bilginin şifresini çözebilir. Bilgiler, genel anahtar ile şifrelenip özel anahtar ile çözülebileceği gibi, özel anahtarla şifrelenip genel anahtarla çözülebilirler. RSA, açık anahtarlı şifreleme tekniğidir ve çoğunlukla tercih edilen bir yaklaşımdır.

Diğer bir açık anahtarlı şifreleme tekniği, *Sayısal İmza Algoritması* (Digital Signature Algorithm-DSA)'dır ve bu teknik imzalama için kullanılır. Eliptik Eğri Şifreleme Sistemi (Elliptic curve crypto

systems) ise eliptik eğriler olarak bilinen matematiksel nesneler üzerine oluşturulmuş, şifrelemede kullanılan yaklaşımlardandır. Diffie-Hellman Anahtar Anlaşması Protokolu (Diffie-Hellman Key Agreement Protocol), güvensiz bir kanalda gizli anahtar oluşturmada kullanılan diğer bir popüler açık anahtar şifreleme tekniğidir.

Simetrik Algoritmalar

Bu algoritmalar, özel, tek veya gizli anahtarlı geleneksel algoritmalardır ve çoğunda şifreleme anahtarı ile şifre çözme anahtarı aynıdır. Güvenli bir iletişim için gönderici ile alıcı, bir gizli anahtar üzerinde uzlaşırlar. Seçilen gizli anahtar ile, mesajlar veya düz metinler şifrelenir veya şifrelenmiş mesajların, düz metinlerin şifreleri çözülebilir. Birbiri ile şifreli haberleşmek isteyen taraflar, seçilen gizli anahtarı paylaşmak zorundadırlar. Simetrik algoritma yaklaşımının daha açık anlaşılması için şifreleme ve şifre çözme yaklaşımını detaylı gösteren blok çizim Şekil 2.3'de verilmiştir.



Şekil 2.3. Tek Anahtarlı (Gizli) Şifreleme ve Şifre Çözme İşlemi

Anahtarın genel kullanıma sunulması, isteyen herkesin şifrelenmiş mesajları çözebileceği anlamına geldiği için, bu yaklaşımda anahtarlar gizli tutulmak zorundadır. Modern bilgisayarlar ile kullanılan anahtarın bulunabilmesi mümkün olduğundan, simetrik algoritmalarda güvenlik anahtar uzunluğuyla doğru orantılıdır. Günümüzde kabul edilebilir anahtar büyüklüğü en az 128 bit olup iletişimin gizli kalması için anahtarın da gizli tutulması şarttır. DES ve 3DES en çok kullanılan yaklaşımlardandır.

Hibrit Yaklaşımlar

Simetrik algoritmaların hızlı olması, asimetrik algoritmaların güvenilir fakat yavaş olması *Hibrid Kriptosistem* adı verilen bir yapının ortaya çıkmasına sebep olmuştur. Simetrik algoritmalarda en bü-

yük problem anahtarın karşı tarafa iletimindedir. Bu yapı temelde bilginin simetrik bir algoritma ile şifrelenmesini, bu algoritmada kullanılan anahtarın da asimetrik bir algoritma ile şifrelenip gönderilecek bilgi ile birlikte iletilmesinde temel teşkil eder. Böylelikle bilginin şifrelenmesi, simetrik algoritmadan dolayı hızlı olup, anahtarın iletimi de, asimetrik algoritmadan dolayı güvenli olacaktır. Bu yapıların ortak kullanılması ile hız ve güvenirlik bir arada sağlanabileceğinden, verimlilik artmaktadır. Bundan dolayı birçok işlemde, bu ve buna benzer yaklaşımlar tercih edilmekte ve geliştirilmektedir.

2.4. Anahtarlar

Modern kriptolama yaklaşımları, anahtar tabanlı olduğundan, algoritmanın detayları ile ilgilenilmez. Anahtarın güvenliğinin sağlanması, sistemin genel güvenliğinin sağlanması ile eş anlamlıdır. Dolayısıyla anahtarlar, kriptografik yaklaşımların temel yapı taşlarıdır ve güvenlik, anahtarın güvenliğine veya bit katarlarının uzunluğuna bağlıdır.

Anahtar uzunlukları farklılıklar gösterse de, anahtarlar, büyük bir sayı kümesinden seçilmiş değerlerdir. Mesela; 48 bitlik bir anahtara örnek Şekil 2.4'de verilmiştir. Burada anahtarlar bit olarak ifade edilebildiği gibi farklı bir formada da sunulabilir. Base64 buna bir örnek olarak verilebilir. Anahtarların farklı uzunluklarda olabileceğini belirtmiştik. Eğer 1024 bit uzunluğunda bir anahtar kullanılıyorsa, 2^{1024} farklı değer içerisinden seçilen bir sayının veya bu değerlerden birisinin anahtarınız olabileceğini hatırlatmakta fayda vardır.

Simetrik algoritmalarda, yetkilendirilmiş kişilerin değişiminde veya işten ayrılmasında yeni bir anahtar değişikliğine ihtiyaç duyulabilir.

Anahtarları ve anahtarın önemini anlamak için, anahtarlara farklı açılardan bakılmasında ve farklı değerlerle mukayese etmemizde fayda vardır. Mesela; $2^{64}=10^{19}$ değerinde bir büyüklüğü ifade eder. 64 bitlik bir anahtar, 64 farklı 1100111111111111 1111110000000000 1110001110000001 1000000011001101 oluşmaktadır. Bu bitleri, ikili taban yerine 16'lık veya farklı tabanlara göre ifade etmek de mümkündür.



= 11001111111111111111110000000000**1110001110000001**

(a) Şifrelemede Kullanılan 48 Bitlik Bir Anahtar



= 2489349e894859f45489450dab45454ca0908d8809

(b) Farklı Formda Bir anahtar Örneği

Şekil 2.4. Şifrelemede Kullanılan Anahtar Örnekleri

Bunun yanında, verilen bu sayıların onluk tabanda gerçek değerlerle ifade edilmesi, bu sayıların büyüklüğü hakkında bize fikir verecektir. Evrenin yaşının 10^{10} yıl olduğu, dünyadaki atomların sayısının yaklaşık 2^{170} veya 10^{51} tane olduğu, genetik olarak bir kişinin var olma ihtimalinin 300 milyarda 1 veya 2^{40} olduğu, bir gün içinde yıldırım sonucu ölme ihtimalinin 9 milyarda 1 veya 2^{33} olduğu düşünülürse, anahtarların boyutları hakkında daha anlaşılabilir bir değerlendirme yapmak mümkün olabilecektir.

"128-bit" veya "40-bit" kodlama ifadesi anahtarın boyutunu gösterir. 128-bit kodlamanın 40-bit kodlamadan yaklaşık olarak $3x10^{26}$ kez daha güvenli olduğu bildirilmiştir. Moore kanununa göre her 18 ayda ikiye katlanan PC hızı, 256-bit kodlamanın yakın bir gelecekte kolaylıkla kırılamayacağını göstermektedir. 40-bit kodlamanın ise artık kolaylıkla kırılabildiğini belirtmekte fayda vardır.

Anahtarları temel alarak, algoritmaları değerlendirdiğimizde, simetrik yaklaşımlarda tek bir anahtar üretimi yapılırken, asimetrik algoritmalarda, anahtarlar bir çift olarak üretilirler.

Simetrik bir algoritma için, anahtarın alıcıya iletilmesi, mutlaka gizli bir yoldan yapılması gerekmektedir. Burada iki kişi arasında yapılacak olan haberleşmelerde pek sıkıntı yoktur, fakat ikiden fazla kişi ile güvenli haberleşileceği zaman sıkıntılar oluşmaktadır. Bunun aşılması için bu yaklaşımda anahtar yönetimi gereklidir ve bu konu dikkat edilmesi gereken önemli bir husustur. Bu yaklaşımda, her bir bilgisayar bir başka bilgisayarla, diğer bilgisayarlardan bağımsız bir iletim hattı oluşturmaktadır. N elemanlı bir ağda N'in 2'li kombinasyonu kadar iletim hattı oluşacağı dikkate alınırsa bu işin zorluğu da ortaya çıkar. Küçük bir ağ üzerinde bunun bir problem

teşkil etmeyeceği düşünülebilir, fakat büyük veya dünya çapında bir ağ üzerinde düşünüldüğünde fiziksel olarak bu sayıda bir iletim hattı oluşturmak imkansızdır. Ayrıca, her bir eleman diğer bütün elemanların anahtarlarını depolamak zorundadır.

Simetrik algoritma anahtarlarının iletiminde, TTP (*trusted third party*), kullanan yöntemlerden birisidir. Bu yöntemde, bütün kişi ve kurumlarca doğruluğu ve güvenirliği kabul edilen üçüncü bir ara yapı kullanılmaktadır. Gönderici herhangi bir alıcıya bilgi göndermek istediği zaman, bu ara yapıdan anahtar talebinde bulunur. TTP adı verilen bu yapı ise, göndericiye anahtar temin ederken, göndericinin bildirdiği alıcıya da aynı anahtarı ulaştırır. Ağa bağlı kullanıcılar anahtar teminini TTP yapısından elde ederler. Ancak bu yapının üstünlükleri olduğu kadar, dezavantajları da bulunmaktadır. Herhangi bir eleman ağdan atıldığında veya ağa eleman eklendiğinde bu yapının bundan etkilenmemesi, her bir elemanın sadece TTP'nin verdiği bir anahtarı depolamak zorunda olması, bilinen üstünlükleri iken, her bir bilgi iletiminde öncelikle, TTP ile iletişim kurulmak zorunda olması, TTP'de n adet anahtar depolanma zorunluluğu, TTP'nin tüm mesajları okuması ve TTP'nin anahtar iletiminde güvenliği sağlayamaması bilinen sakıncalarıdır.

Asimetrik algoritma anahtarlarının iletiminde kullanılan diğer yöntemlerden biri Genel Anahtar Tekniği'dir. Bu yapıda mevcut iki anahtar bulunduğu için, genel anahtarlar her kullanıcının erişebileceği bir ortamda tutulurlar. Kişi_A kullanıcısı Kişi_B kullanıcısına bilgi göndereceği zaman, önce merkezden veya bilinen bir yerden Kişi_B kullanıcısının genel anahtarını temin eder. Daha sonra göndermek istediği bilgiyi bu anahtarla şifreleyip, Kişi_B'ye gönderir. Bu yapıda üçüncü bir ara yapıya gerek olmaması önemli bir üstünlüktür. Bu sayede, iletilecek bilginin üçüncü bir kişi tarafından okunma riski ortadan kaldırılmış ve çok sayıda anahtar depolama sıkıntısı giderilmiştir.

Kriptografik yaklaşımların temel taşları olan anahtarlar, aynı zamanda açık anahtar altyapısının da temel taşlarıdır. Tablo 2.2'de, desteklenen unsurlar ve ihtiyaç duyulan anahtarlar verilmiştir. Güvenlik unsurlarının tamamını destekleyebilecek bir yapıda olan açık anahtarlama sistemleri ile, tam bir güvenlik sağlanabilir.

Anahtar uzunluğunun güvenliğe etkisini gösterme açısından literatürde verilen bir değerlendirme yaklaşımını burada sunmakta fay-

da vardır. Tablo 2.2'de görülebileceği gibi, bit sayısı (anahtar uzunluğu) arttıkça anahtarların kırılma sürelerinde müthiş bir artış göze çarpmaktadır. Bu sürelerin fazlalığı, anahtarların güvenli olduğunu göstermektedir.

Desteklenen Unsur	Gizlilik	Bütünlük	Kimlik doğrulama	İnkar edemezlik
birey	Özel anahtar	Özel anahtar	Özel anahtar	Özel anahtar
herkes	Açık anahtar			

Tablo 2.2. AAA Yapılandırılmasında Özel ve Genel Anahtarlar

Anahtar Uzunluğu (bit)	Sayı Değeri	10^6 şifre/s	10^9 şifre/s	10^{12} şifre/s
32	~$4x10^9$	36 dk	2.16 s	2.16 ms
40	~10^{12}	6 gün	9 dk	1 s
56	~$7.2x10^{16}$	1142 yıl	1 yıl 2 ay	10 saat
64	$1.8x10^{19}$	292 000 yıl	292 yıl	3.5 ay
128	$1.7x10^{38}$	$5.4x10^{24}$ yıl	$5.4x10^{21}$ yıl	$5.4x10^{18}$ yıl

Tablo 2.3. Farklı Anahtar Uzunluklarına Göre Şifre Kırma Zamanları

Şekil 2.5'de anahtarların elektronik ortamda tutulduğu donanımlara örnekler verilmiştir. Bu iki donanım en çok kullanılan ortamlardandır.



(a) akıllı çubuk



(b) akıllı kart

Şekil 2.5. E-imza Taşıma Ortamları

2.5. Şifreleme Algoritmaları

Algoritmalar, şifreleme ve şifre çözmede kullanılan matematiksel işlemleri içerirler. Güvenlikleri ise, çalışma biçimlerine ve daha önce de vurgulandığı gibi seçilen anahtar uzunluklarına bağlıdır. Çalışma biçimi veya kullanılan matematiksel yaklaşım gizleniyorsa,

bu bir *sınırlandırılmış algoritma* yaklaşımıdır. Bu algoritmalar, kullanıcı sayısının artması, gruptan bir kullanıcının ayrılması veya gizlenen algoritmanın yanlışlıkla ortaya çıkması durumlarında, geri kalan herkesin başka bir algoritmayı kullanması gerektirdiği için, pek tercih edilmemektedir. Bu algoritmaların başarısı gizlilik esasına dayalı olduğundan, algoritmanın açıkları kolaylıkla belirlenemez veya bilinemez, kalite kontrolü yapılamaz ve standartlara ne derece uyulduğu detaylıca gözden geçirilemez. Bu algoritma; geneli kapsamadığı, üçüncü şahıslar tarafından öğrenilebilme olasılığının ve maliyetinin yüksek olması, ve fazlaca işgücüne ihtiyaç duyduğu için tercih edilmemektedir. Daha çok, az sayıda kullanıcısı olan ve alt seviyede güvenlik gerektiren uygulamalarda kullanılırlar.

Şifreleme algoritmaların kullanıcılar tarafından kolaylıkla kullanılabilmesi için, yukarıda belirtilen olumsuzluklardan ve sınırlamalardan mümkün olduğunca kaçınılmalıdır. Bugün, literatürde bu ihtiyaçlara cevap verebilecek herkese açık algoritmalar mevcuttur.

Bir algoritmanın güvenilirliği o algoritmanın herkese açık olmasından, bir başka ifadeyle, teorik yapısının herkes tarafından biliniyor olmasından geçmektedir. Daha önce de belirtildiği gibi, sistem veya bilgi güvenliği, kullanılan anahtara veya anahtar çiftlerine bağlıdır. Bu yaklaşımlarda, üçüncü şahısların algoritmayı bilmesi ve teorisini kavraması önemli değildir. Burada asıl önemli olan, gizli veya özel anahtarın başkaları tarafından bilinmemesidir. Bu sağlandığı takdirde, şifrelenmiş olan bilgiler, mesajlar, düzmetinler veya dokümanlar, başkaları tarafından deşifre edilemez, anlaşılamaz veya okunamazlar.

Günümüzde, verilerin güvenli olarak bir ortamdan diğerine aktarılmasında çok farklı algoritmalar kullanılmaktadır. Modern şifreleme ve anahtarlama teknikleri, hibrit sistemler, steganografik yaklaşımlar en çok kullanılan yaklaşımlardır.

Algoritmalarda; şifreleme işlemleri, özel matematiksel fonksiyonlar yardımıyla yapılır. Bu tür fonksiyonlarda, X tanım kümesinden Y aktarım veya dönüşüm kümesine bir *f* fonksiyonu tanımlanmıştır. X kümesinin her bir elemanına *f* fonksiyonu uygulandığında, Y kümesi çıkışları elde edilir. Tek yön fonksiyonu olarakta bilinen bu yaklaşımda, çıkışlardan hareket ederek girişler elde edilemezler. Yani Y kümesinden X kümesine bir f^{-1} fonksiyonu elde edilemez.

Sebebi ise her Y kümesi elemanıyla bir X kümesi elemanı eşleştirilememektedir.

Algoritmalarda, eşleşme (bijeksiyon) fonksiyonu, diğer bir yaklaşım olup, X tanım kümesinden Y aktarım kümesine bir *f* fonksiyonu olarak tanımlanır. Tek yön fonksiyonunun aksine, bu fonksiyonun çıkışlarından girişler elde edilebilmektedir. Sebebi ise, X kümesinin her bir elemanına *f* fonksiyonu uygulandığında, Y kümesinin tüm elemanları çıkış olarak elde edilmesidir. Bunun sonucu olarak, Y kümesinden X kümesine f^{-1} fonksiyonu elde edilebilir.

Daha önce de belirtildiği gibi, şifreleme algoritmaları, simetrik ve asimetrik fonksiyonlar olarak ikiye ayrılırlar. Temelde her iki tür fonksiyonun da yaptığı aynıdır. Her iki fonksiyon türünde, girdi olarak alınan veriler, parametreler dahilinde işlenir ve çıktı olarak, şifrelenmiş veri elde edilir. Bu veri artık güvenli, yani gizli olarak alıcısına gönderilmeye hazırdır. İletim esnasında herhangi bir saldırganın bu verilerden bilgi edinebilmesi, fonksiyonun içeriğine bağlı olarak zordur. Fonksiyon, sabit ve parametresiz ise güvenilirlik ve esneklik çok daha az olacaktır. Üçüncü şahıslardan veriyi gizlemek veya saklamak, sabit bir yöntem ile pek de mümkün olmayacaktır. Daha çok, parametrik bir fonksiyon tercih edilmektedir. Bu tür fonksiyonların güvenilirlik derecesini parametre ve bunlara karşılık gelen çıktı kombinasyonlarının belirleyeceği unutulmamalıdır.

Şifreleme algoritmalarında aranan bir takım özellikler vardır ve bu özellikler aşağıda sıralanmıştır. Bunlar;

- Şifrelenmiş mesajın deşifre edilmesi esnasında bilgi kaybı olmaması,
- İhtiyaç duyulan güvenlik seviyesine göre şifreleme işleminin zorluk seviyesinin seçilebilmesi,
- Önemli olmayan bilgilerin düşük seviyeli şifreleme yaklaşımları ile, yüksek seviyeli bilgi içeren dokümanlarının ise yüksek seviyeli şifreleme yaklaşımlarıyla şifrelenebilmeleri,
- Verimi düşürecek, maliyeti ve işgücü kaybını arttıracak yaklaşımları içermemesi,
- Şifreleme işlemlerinde güvenlik seviyesinin mümkün olduğunca yüksek olması,

- Basitlik ve kolaylıkla gerçekleştirilebilme özelliğinin ön planda olması,
- Kullanılan algoritmaların karıştırıcı özelliği olması,
- Şifrelenmiş mesaj ile düz metin arasındaki ilişkilerin zor kurulabilmesi,
- Şifreleme yaklaşımlarının herkese açık olması ve
- Açıklarının ortaya çıkarılabilmesi için, başkaları tarafından test edilebilmesinin sağlanması

olarak verilebilir.

Sezar, MD2, MD4, MD5, RSA, Lucifer, Blowfish, AES, CAST 128, DES, 3DES, IDEA, Skipjack, Gost, El-Gamal, Schnorr, Elliptic Curve, Needham-Schroeder, Diffie-Hellman, PGP, S/MIME, IPSec, Kerberos, RIPEMD, HMAC, SHA-1 ve SHA-2, güvenli bir iletişimde kullanılan şifreleme algoritmaları, yaklaşımları, protokolları ve fonksiyonlarından bazılarıdır. Şifrelemede kullanılan yaygın yaklaşımlardan bazıları basitten karmaşığa aşağıda kısaca tanıtılmıştır.

Sezar Şifreleme Yaklaşımı

Verilerin güvenli olarak bir ortamdan diğerine aktarılmasında kullanılan en eski şifreleme metotlarından birisidir. Bir mesajın bu yaklaşımla şifrelenmesi aşağıdaki matematiksel fonksiyonla ifade edilebilir.

$$E(M) = M+3 \bmod 29 = C \qquad (2.1)$$

Fonksiyondaki; 'M' mesajı, 'E' şifreleme işlemini (encryption), 'C' ise şifrelenmiş mesajı ifade etmektedir. '29' ise, şifreleme yapılacak olan dildeki karakter (harf) sayısıdır. Türkçemizde 29 alfabetik karakter olduğu için burada 29 rakamı kullanılmıştır. Şifrelenmiş mesajın deşifre edilmesi;

$$D(C) = C- 3 \bmod 29 = M \qquad (2.2)$$

formülü ile sağlanır. Bu formülde, 'D', deşifreleme (decryption) işlemini ifade etmektedir. Burada dikkat edilmesi gereken husus ise, harflerin sayıya dönüştürülmesidir. Mesela, İngiliz alfabesi için

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

0 1 2 3 4 5 ... 23 24 25 *(2.3)*

harfler 0'dan 25'e kadar etiketlenir. Bu etiketleme sonucunda elde edilen sayılar formüllerde yerine konularak, her bir harfin farklı bir sayıya dönüşmesi sağlanır. Mesela; "e imza" kelimesini ele alalım ve bunu Sezar'a göre şifreleyelim. Burada İngiliz alfabesini kullandığımızı varsayarsak;

e i m z a

4 8 12 25 0 ***(2.4)***

karakter karşılıklarını bulabiliriz. Burada elde edilen değerleri E(M)=M+3 mod 26 şifreleme fonksiyonundan geçirdiğimizde,

7 11 15 3 ***(2.5)***

sayılarını elde ederiz. Bu sayılara karşılık gelen harfler ise

h l p c d ***(2.6)***

şeklindedir.

Yukarıdaki açıklamalardan da görülebileceği gibi, "e" harfi "h" ye "i" harfi "l" ye, "m" harfi "p" ye, "z" harfi "c" ye ve "a" harfi ise "d" ye dönüşmüştür.

Sezar şifreleme metodu, simetrik, aynı zamanda da eşleşme (bijeksiyon) özelliği gösteren bir şifreleme metodudur. Şifreleme ve şifre çözme anahtarları aynıdır. Bu anahtarın alıcıya gizli bir yolla iletilmesi şarttır. Alıcıya anahtarın gönderilmesinde güvenilir bir yol bulunması veya seçilmesi unutulmamalıdır. Bu sağlansa bile her alıcıya farklı bir anahtar temin etmek gerekebilir. Bu ise, hem zahmetli hem de oldukça zor olup ihlal oluşturabilecek bir yapıdadır.

Sezar Açık Anahtar Şifreleme Yaklaşımı

Bu yaklaşım, Sezar metodunun genelleştirilmiş bir formudur. Bu yaklaşım da Sezar metodunda olduğu gibi kaydırma temellidir. Bu yaklaşımda şifreleme;

$$E(M) = (M+N) \bmod 29 = C \qquad (2.7)$$

ile yapılırken deşifreleme işlemi;

$$D(C) = (C- N) \bmod 29 = M \qquad (2.8)$$

formülüyle gerçekleştirilmektedir. Burada 0<=N<29 olduğunu hatırlatmakta fayda vardır.

Mesela;

(M+1) mod 29 ***(2.9)***

fonksiyonuyla "BİLİM" kelimesi şifrelenirse, çıktı olarak "CJOJK" kelimeleri elde edilir. Artık iletim işlemi, yeni veriyle gerçekleştirilir. Üçüncü bir şahsın bu veriyi kolaylıkla algılaması bir derece daha zorlaşacaktır. Bu fonksiyonun ters işlemi ile mesaj ***(C-1) mod 29*** ile deşifre edilmektedir. Bu sayede şifrelenmiş mesaj kolaylıkla geri elde edilebilir.

Polialfabetik Şifreleme Yaklaşımı

Bu tip şifrelemede, mono alfabetik yöntemlerden farklı olarak bir harf değiştirilince her seferinde aynı harfe dönülmez. Bu işlem, "Vigenere Tablosu" olarak bilinen bir tablo ile gerçekleştirilir. Tablo 2.4'de bu tabloyu görebilirsiniz.

	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
A	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
B	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A
C	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B
Ç	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C
D	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç
E	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D
F	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E
G	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F
Ğ	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G
H	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ
I	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H
İ	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I
J	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ
K	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J
L	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K
M	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L
N	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M
O	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N
Ö	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O
P	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö
Q	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P
R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R
S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S
Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş
T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T
U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U
Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü
V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V
W	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y
X	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
Y	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A
Z	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B

Tablo 2.4. Vigenere Tablosu

Bu yaklaşımla bir mesajın şifrelenebilmesi için, bir anahtar kelimeye ihtiyaç vardır. Mesajın her bir karakteri sütun üzerinde, anahtar kelimede bulunan harf ise, satırdan bulunur. Satır ve sütunun kesiştiği noktadaki harf, şifrelenmiş mesajın harfi olarak belirlenir.

Buna bir örnek verelim. "EİMZA KULLANMALIYIZ" cümlesi şifrelenecek mesajımız olsun. "HEMEN" kelimesini ise, anahtar olarak kullanalım. Bu harflere karşılık olarak, anahtar kelimenin yardımıyla Tablo 2.4'den aşağıdaki yeni harfler elde edilebilir.

Mesaj	EİMZA	KULLA	NMALI	YIZ
Anahtar	HEMEN	HEMEN	HEMEN	HEM
Şifreli mesaj	LNBDN	ŞİAPN	ÜRMPV	GML

Elde edilen şifrelenmiş mesajın şifrelerinin çözümü için, aynı anahtar "HEMEN" kullanılmalıdır. Deşifreleme işlemi ise, aşağıda verilen adımlarda gerçekleştirilir ve bu işlemler sonucunda şifrelenmiş olan karakterler tekrar geri elde edilebilir.

Şifreli mesaj	LNBDN	ŞİAPN	ÜRMPV	GML
Anahtar kelime	HEMEN	HEMEN	HEMEN	HEM
Açık mesaj	EİMZA	KULLA	NMALI	YIZ

Böylece, başlangıçta şifrelenen düz metin yukarıda verildiği gibi tekrar geri elde edilebilir.

Vernam (One-Time Pad) Şifreleme Yaklaşımı

Bu yaklaşımda, rasgele üretilen tek bir kullanımlık karakter dizisiyle şifreleme işlemi gerçekleştirilir. Açık mesaj içinde yer alan her karakter, üretilen dizide karşısına gelen karakterlerle işleme sokularak, şifreli mesaj elde edilir. Mesajı çözmek için rasgele dizinin bilinmesi gereklidir.

Mesajımızın bir önceki bölümde verilen mesajla aynı olduğunu farz edelim. Bu durumda üretilen rasgele diziye göre şifreli mesaj elde edilir. Örnek olarak "EİMZA KULLANMALIYIZ" cümlesinin mesajının şifreli hali aşağıdaki gibidir.

Mesaj	EİMZA	KULLANMALIYIZ
Rasgele dizi	HNMET	KSYROQAZWPGLU
Şifreli mesaj	LYBDT	VNJ..…….

Bu yöntemde güvenlik rasgele üretilen diziye bağlı olduğundan bu şifreleme sistemi, "mükemmel bir şifreleme yöntemi" olarak da bili-

nir. Burada mükemmeliği sağlayan husus, rasgele dizinin gerçekten rasgele olarak seçilmesi ve anahtar uzunluğu ile aynı olmasıdır.

DES (Data Encryption Standard) Algoritması

Bu algoritma, 1977'de IBM tarafından geliştirilmiş ve daha sonra da standart olarak kabul edilmiştir. Bu algoritmanın anahtar uzunluğu 56 bittir. Günümüzde bu algoritmanın anahtar uzunluğu yeterli gibi görünse de, kısa sürede çözülebilmektedir. Aslında sorun sadece anahtar uzunluklarında olmayıp, fonksiyonların simetrik olmasının güvenliği önemli ölçüde tehdit etmesinden kaynaklanmaktadır.

Bu şifreleme yaklaşımında, X verisi K anahtarıyla şifrelenerek, Y verisine dönüştürülür. Şifrelenmiş Y verisi, daha sonra alıcıya gönderilir. Y verisi, alıcı tarafından göndericiye gizli bir kanaldan gönderilmiş olan K anahtarı ile, ancak deşifre edilir. Tek yönlü fonksiyon özelliği gösteren algoritmalara, DES, bir örnek olarak verilebilir.

64 bit blok şifreleme de yapılabilen bu algoritma da, şifreleme esnasında 16 farklı döngü kullanılır. Bu işlemlerde veri, anahtar ve önceki döngü ile karıştırılır ve bir permütasyon işlemine tabi tutularak anlaşılamayacak bir forma getirilmeye çalışılır. Bir önceki döngünün çıkışı, bir sonraki döngüye giriş olarak uygulanır. Her bir döngüde, en sağdaki girişin 32 biti, çıkışın solundaki 32 bite kaydırılır. Sonra, sağ ve sol bitler ve anahtar, bir fonksiyondan geçirilerek çalıştırılır. Her bir döngüde anahtar kaydırılır ve son bir permütasyon ile işlem tamamlanır.

Bu yaklaşım, 1997 yılında İsrailli araştırmacılar tarafından kırılmıştır. Bu şifreleme yaklaşımının anahtar güvenliğini ve şifreleme güvenliğini arttırmak için 3 DES (Triple DES) geliştirilmiştir. 168 bit anahtar uzunluğuna sahip olan bu yaklaşım, günümüzde hala güvenli olarak kullananlar vardır.

Bu algoritmanın hızlı olması ve lisanssız kullanımının serbest olması önemli özelliklerindendir. Daha çok bankacılık uygulamalarında ve AAA'da halen kullanılmakta olan şifreleme algoritmasıdır.

RSA (Rivest, Shamir ve Adleman) Algoritması

AAA'da birçok unsuru desteklemek ve güvenli bir ortam oluşturmak için asimetrik fonksiyonlar geliştirilmiştir. Bu gruba dahil fonksiyonlar, şifreleme ve deşifreleme yaparken, biri özel biri ge-

nel olmak üzere iki anahtar parametrelerini kullanırlar. Tasarımcılarının isimlerinin baş harflerinden oluşan RSA (**R**ivest, **S**hamir, **A**dleman) algoritması, asimetrik fonksiyonlara verilebilecek en iyi örnektir.

RSA algoritması, bijeksiyon fonksiyon özelliği gösterir. Bu algoritmada bir özel ve birde açık olmak üzere bir anahtar çifti vardır. Açık (genel) anahtar herkese dağıtılır, özel anahtar ise, sadece kişiye özeldir ve o kişiden başka kimsede bulunmaz.

X verisi alıcının genel anahtarıyla şifrelenerek Y verisine dönüştürülüp, alıcıya gönderilir. Y verisi, ancak alıcının özel (gizli) anahtarı kullanılarak X verisine dönüştürülür. Burada gönderici bile, mesajı şifreledikten sonra açamaz. Şifrelenmiş veriyi anlamlı bir bilgiye çevirebilecek tek parametrenin alıcının gizli anahtarı olması, bu algoritmanın güvenilirliğini arttırmaktadır. Bu yaklaşımı kabaca gösteren blok Şekil 2.6'da verilmiştir.

Bu şifreleme yaklaşımında, N = p.q olduğunu kabul edelim. Burada p ve q yüksek basamaklı asal sayılar olsun. Bu durumda şifreleme işlemi için;

$$C = M^e \bmod N \qquad (2.10)$$

formülü, şifrelenmiş mesajı çözmek için ise;

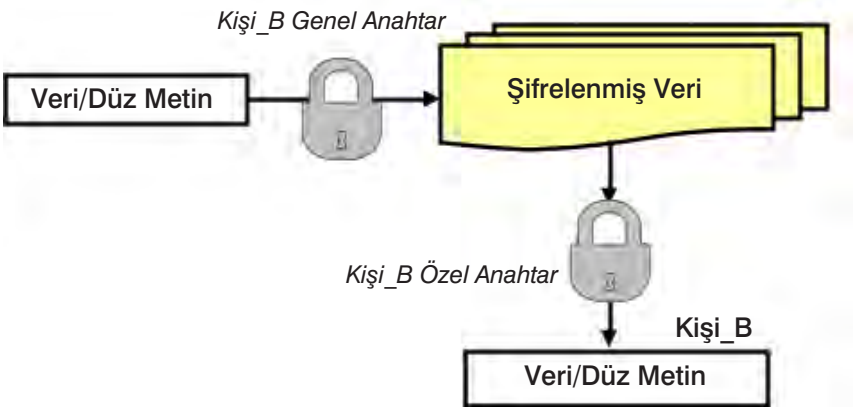
$$M = C^d \bmod N \qquad (2.11)$$

formülü kullanılır. Bu formüllerde, (n,e) açık anahtarı, (d) ise özel anahtarı ifade etmektedir.

Şekil 2.6'da verilen bloklardan da görülebileceği gibi, bu iki tarafın birbirleriyle haberleşebilmesi için Kişi_A ve Kişi_B'nin açık anahtarları herkese dağıtılır. Kişi_A, Kişi_B'ye bir mesaj göndereceği zaman, Kişi_B'nin açık anahtarı ile göndereceği bilgileri şifreler ve Kişi_B'ye gönderir. Şifrelenmiş veriyi alan Kişi_B ise, şifrelenmiş mesajı anlamlı bilgiye çevirebilecek tek parametre olan özel anahtara sahip olduğu için, bu anahtarını kullanarak veri veya düzmetini şifrelenmiş veriden ayrıştırabilir.

Açık anahtar algoritmalarının tümü, çok büyük sayılarla yapılan bazı işlemlerin bir yönde kolay, aksi yönde ise, zor olduğu gerçeğini kullanmaktadırlar. RSA'da çok büyük asal sayıları üretmenin kolaylığına karşın, büyük sayıların asal bileşenlerinin bulunmasının zor

olması prensibine göre işlemler yapılır. Matematikçilerin tamsayıları asal bileşenlerine ayırmanın hızlı bir yolunu henüz bulamamış olmaları, bu prensibin hala geçerli olduğunu göstermektedir. RSA ve benzeri algoritmalar, asal sayılarla yüksek çarpanlı matematik işlemleriyle gerçekleştirildiklerinden, bilgisayar uygulamalarında problemlerle karşılaşılması olasıdır. Bu işlemler gerçekleştirilirken, üretilen veriler karakter katarları şeklinde bilgisayar hafızasının elverdiği kadar saklanabilmektedir. Bunun için aritmetiksel işlemleri yeniden tanımlamak, yeniden yapılandırmak gerekebilir. Tüm bu zorluklara rağmen, RSA, açık algoritma mantığıyla çalıştığı, ve yüksek güvenlik sunduğu için, en çok tercih edilen asimetrik algoritmadır.



Şekil 2.6. RSA Algoritmasıyla Şifreleme ve Şifre Çözme

AES Algoritması

Gelişen teknik ve teknolojiler, saldırıların boyut değiştirmesi, şifreleme algoritmalarına yapılan saldırıların artması, kullanılan algoritmaların saldırılara karşı dayanıklığının zayıflaması, araştırmacıları yeni algoritmalar geliştirmeye yöneltmiştir. AES ise son yıllarda kullanılan en önemli algoritmadır. AES'in geliştirilmesinin temelinde ise DES şifreleme algoritmasının saldırılara karşı dayanıksız olması vardır. 1997'de Joan Daemen ve Vincent Rijmen tarafından geliştirilmiş 128, 192, 256-bitlik anahtar uzunluğu seçeneklerine sahip olan Rijndael algoritması, daha önceki sayfalarda da vurgulandığı gibi Gelişmiş Şifreleme Standardı (AES) ismiyle veri şifreleme standardı olarak belirlenmiştir. 1997'den beri ise farklı anahtar

uzunlukları tercih edilen AES, günümüzde hala güvenilirliğini korumakta ve bilişim dünyasında güvenlik için kullanılmaktadır.

AES algoritmasında, sahip olduğu anahtarlara göre farklı sayıda döngüsel işlem yapılır. AES 128-bitlik düz metni şifrelerken veya şifrelenmiş metni çözerken de aynı anahtarı kullanır. Bu döngüsel işlemin artmasıyla veri daha çok güvenilir hale gelir. Fakat, aynı zamanda yapılacak olan döngüsel işlemlerin de artmasıyla hem işlem sayısı hem de bellek alanı artar.

Bu algoritmada; AES-128 AES-192 AES-256 gibi veri blokları, 4,6,8 gibi kelime uzunluğu, 10,12,14 gibi tur sayısı uygulanabilmektedir.

2.6. Özetleme (Hashing) Algoritmaları

Farklı uzunluklarda mesaj, doküman veya yazıyı işleyerek, sabit uzunlukta veri oluşturma işlemine, özet veya özetleme denir. Elde edilen özet bilginin, mesaj, doküman veya yazıyı temsil edebilecek bir formda olması beklenir. Bundan dolayı, elde edilen özet değeri mümkün olduğunca tekil olması veya benzerinin olmaması istenilir. Bu işlemde, bir özetleme (hash) fonksiyonu kullanılır ve bir grup veriden veya mesajdan sabit uzunlukta bir dizi üretilir. Üretilen bu dizi, o mesajın, dokümanın veya yazının bütünlüğünün test edilebilmesi için kullanılan bir imza niteliğindedir. Bu işlemleri gerçekleştiren algoritmalara, özetleme algoritmaları veya fonksiyonları denir. Bir özetleme fonksiyonunun temel özellikleri aşağıda verilmiştir.

- Uzunlukları farklı olan verileri, sabit uzunluklu bir çıktıya dönüştürmelidir.
- özet değeri kolay hesaplanabilmelidir.
- özet değerinden mesajı elde etmek zor olmalıdır.
- farklı mesaj veya dokümanlardan aynı özet değerinin üretilmemesi gereklidir.
- Elde edilecek özet değeri tekil (unique) olmalıdır.
- Aynı özet değerini üretecek iki farklı mesajı bulmak ise oldukça zor olmalıdır.

Pratikte özetleme fonksiyonları, şifre doğrulama, bütünlük kontrolü, e-imza ve güvenli e-posta uygulamalarında kullanılmaktadır. Genellikle veri bütünlüğünü garanti etmesi, hızlı olması, sabit

uzunlukta çıktı vermesi, açık anahtar algoritmalarından daha iyi olması, dosya boyutunun alınan özeti etkilememesi ve yüksek performanslı bir haberleşme sağlaması bu yaklaşımın üstünlükleridir.

Farklı güvenlik seviyelerinde kullanılan birçok özetleme algoritmaları bulunmaktadır. MD serisi, SHA serisi veya RIPE-MD-160 algortimaları bunlardan bazılarıdır. En çok kullanılan algoritmalar, aşağıda kısaca açıklanmıştır.

MD serisi mesaj özetleme algoritmaları, Ron Rivest tarafından geliştirilmiştir. Son yıllara en çok kullanılan özetleme algoritmalarındandır. Bu algoritmaların tamamı, 128-bit özetleme sağlar. Bu seride MD2 en yavaşı iken, MD4 ise en hızlılarıdır. MD5, MD4'e göre daha kapsamlı geliştirildiğinden, hızı nispeten düşüktür. Tüm bu algoritmaların herkese açık olması önemli üstünlükleridir.

MD5'in çarpışma saldırılarına karşı zayıf olduğunun keşfedilmesinden sonra bilimadamları, MD5 yerine SHA-1 veya RIPEMD-160 gibi alternatiflerin kullanılmasını tavsiye etmektedirler.

SHA-1 (Güvenli Özetleme algoritması-Secure Hashing Algorithm) ilk olarak NSA (Ulusal Güvenlik Ajansı-*National Security Agency*) tarafından geliştirilmiş ve NIST'in desteğiyle, 1993 yılında ABD'de standart olarak kabul edilmiştir. Bu algoritma, MD serisi algoritmalardan daha uzun özet bit üretebilmektedir. 160-bit uzunluğunda üretilen bir dizi için gerekli süre MD5 algoritmasından yaklaşık olarak %25 oranında daha yavaş olsa da, kullanılması tavsiye edilen bir algoritmadır.

Günümüzde karışıklığı önlemek amacıyla, ilk sürüm, SHA-0 olarak adlandırılır. SHA-0 ve SHA-1, en fazla 2^{64} uzunlukta mesajlardan 160-bitlik özet değeri üretir. NIST, 2001 yılında SHA'nın 256, 384 ve 512 bit versiyonlarıyla SHA-256, SHA-384 ve SHA-512 yapılabildiğini duyurmuştur. Bunun güncel bir versiyonu olan SHA-2 ise en çok kullanılan versiyonudur.

Özetleme algoritmalarının ürettiği değerlere örnekler vermek ve anlatılan algoritmaları karşılaştırmak için burada bir çalışma yapılmıştır. Bu çalışmada, MD4, MD5 ve SHA-1 özetleme algoritmaları, "Şeref Sağıroğlu" kelimeleriyle test edilmiştir. Burada kısa bir yazı seçilmiş olsa da, bunun sadece örnek vermek için seçildiğini belirtmek isteriz. "Şeref Sağıroğlu" ifadesinin bir karakterin (E veya R)

değişmesi, Tablo 2.5'den de görülebileceği gibi özetleme sonuçlarını tamamen değiştirmektedir.

RIPE-MD-160 (RACE Integrity Primitives Evaluation Message Digest) algoritması, Avrupa Birliğinde kullanılan bir algoritmadır. Farklı uzunluktaki dosya veya veriler için 160 bitlik sabit uzunlukta dizi üretmesi ve diğer şifreleme yaklaşımlarından daha hızlı olması, bilinen üstünlükleridir. Sadece bütünlüğü sağlaması ise, en önemli dezavantajı olarak bilinmektedir.

RIPE-MD-160'ın gelecek yıllarda güvenilir olacağı öngürülmekte ise de, bu algoritmanın bazı ataklara karşı zayıf olduğu birkaç farklı çalışmada vurgulanmıştır. Algoritmanın tasarımı MD4, MD5 ve RIPEMD'nin zayıf yönlerinin değerlendirilmesi prensibine dayanmaktadır. İki farklı ve paralel hesaplama işleminin sonucunun, her bir sıkıştırma işlemi sonunda birleştirilmesi, bu fonksiyonun ayırt edici özelliğidir. Diğer özetleme algoritmaları gibi, 32 bit işlemcilerde en iyi performansı verecek şekilde ayarlanmıştır. Bununla beraber, RIPE-MD'nin 258 bitlik ve 320 bitlik sürümleri de mevcuttur.

Tablo 2.5. Özetleme Algoritmalarının Karşılaştırılması

Algortima	Algoritma Çıktısı
MD4	8452D193D25A0EA1EA11C5C687178E95
MD5	83579DE9B0A8B960420233BF880E09F4
SHA-1	A89896DB99C5CB906E5334800466016C3A013210

(a) "Şeref Sağıroğlu" için Çıktılar

Algortima	Algoritma Çıktısı
MD4	441D160540F64625FF9C425802693528
MD5	8F47416E93145A82AD2160AA73D57B5D
SHA-1	D99EE77E96D12C2353C37599BC6F0C4F3458C8EA

(b) "Şeref Sağıroğlu" için Çıktılar

Algortima	Algoritma Çıktısı
MD4	FEB84240E469732CB119EEF1C98C4AFE
MD5	BEBC96CEF00B858733697EA82DA3AB40
SHA-1	460BDA1231717DFDE002925F96120508EFB65352

(c) "Şeref Sağıroğlu" için Çıktılar

MAC (Mesaj Onaylama Kodları-Message Authentication Codes) ise bilinen diğer bir ilginç özetleme algoritmasıdır. Diğerlerinden farkı, bir MAC oluşturma veya doğrulama için, yalnız bir anahtara ihtiyaç duyulmasıdır. Bu özelliğin, özetlerin iletişim anında ele geçirilemeyeceğini doğrulama için önemli bir yaklaşım olduğunu savunanlar vardır. HMAC (RFC 2104) ve SHA-1 temelli NMAC bunlara örnek olarak verilebilir.

Anahtarlı özetlemeli mesaj doğrulama kodları (HMAC), bir anahtara dayalı ve tek yönlü çalışan bir özetleme yöntemidir ve hem veri bütünlüğünü hem de veri kaynağının doğrulanmasını sağlar. HMAC'lar incelenen özetleme fonksiyonları ile aynı özellikleri taşır. Bu özetleme fonksiyonlarından birini kullanır, ancak ilave olarak, bir gizli anahtar kullanılır. HMAC'lar, veri alışverişinde kullanıldığı gibi, herhangi bir şahsa alt dosyalarının değiştirilip değiştirilmediğini kontrol etmek amacıyla da kullanılabilir.

Bosselaers, özetleme algoritmalarını hesaplama hızı bakımından karşılaştırmıştır. Tablo 2.6'da verilen bu karşılaştırma, 90 MHz Pentium işlemcili bilgisayarlar ile çalıştırılarak, Assembler dilinde gerçekleştirilmiştir.

Tablo 2.6. Özetleme Algoritmalarının Karşılaştırması

Algoritma	Döngü no	Mbit/s	MB/s
MD4	241	191,2	23,90
MD5	337	136,7	17,09
RIPEMD	480	96,0	12,00
RIPEMD-128	592	77,8	9,73
SHA-1	837	55,1	6,88
RIPEMD-160	1013	45,5	5,68

Bu algoritmalar, güvenilirlik açısından karşılaştırıldığında, en güvenli olanının RIPEMD-160 olduğu ve sıralamayı SHA-1 algoritmasının takip ettiği belirtilmiştir.Daha önce de belirtildiği gibi MD5, zayıflıklarından dolayı güvenilirliği şüpheli bulunmuştur.

2.7. Şifre Bilim Standartları

Bilgisayar sistemlerinin ülke içi ve ülkeler arası haberleşmelerinde, bir uyum içerisinde problemsiz çalışmalarını sağlamak için ortak

belirlenmiş olan kural ve politikalara ihtiyaç duyulmaktadır. Bu politikalar ve kurallar bütününe standart denilmektedir. Başka bir ifadeyle, kaliteyi tutturmak, verimliliği arttırmak, zaman kaybını azaltmak ve birlikte çalışabilirliği sağlamak için ortak kurallar, yani standartlar gereklidir.

Şifre biliminde bunun sağlanması için, devlet, özel sektör ve diğer organizasyonlar ortak standartlar belirlenmesine katkıda bulunmaktadırlar. ISO, ANSI, IEEE, NIST, ITU ve IETF bunlardan bazılarıdır. Açılımları aşağıda verilmiştir.

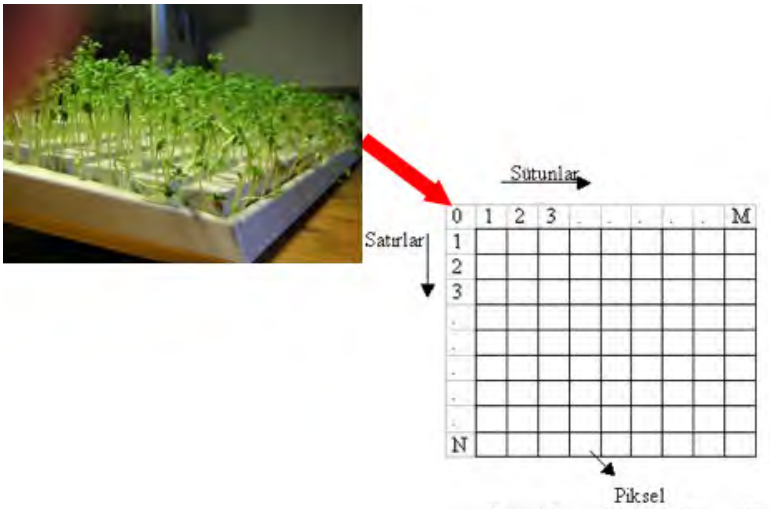
ISO	:	Uluslararası Standarlar Organizasyonu (International Standards Organization)
ANSI	:	Amerikan Ulusal standartlar enstitüsü (American National Standards Institute)
IEEE	:	Elektrik ve Elektronik Mühendisleri Odası (Institute of Electrical and Electronics Engineers)
NIST	:	Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology)
IETF	:	İnternet Mühendisliği Çalışma Grubu (Internet Engineering Task Force)
EU	:	Avrupa Birliği (European Union)
WTO	:	Dünya Ticaret Örgütü (World Trade Organisation)
ICC	:	Uluslar arası Ticaret Odası (International Commerce Chamber)
ITU	:	Uluslararası Telekomünikasyon Birliği (International Telecommunications Union)
CEN	:	Avrupa Standartlaşma Örgütü (European Committe for Standardization)
ETSI	:	Avrupa Telekomünikasyon Standartları Enstitüsü (European Telecommunication Standards Institute)
UNCITRAL	:	Uluslararası Ticaret Kanunu üzerine Birleşmiş Milletler Konferansı (United Nations Conference on International Trade Law)

2.8. Steganografi

Bilişim teknolojilerinin gelişmesi ve yaygınlaşmasıyla birlikte, bilgi güvenliği ve bilginin iletişim güvenliğinin önemi daha da artmış ve kullanılan yaklaşım ve metodolojilerde de farklılıklar gözlemlenmiştir. Steganografik yaklaşımlar da bunlardan birisidir.

Bu yaklaşım, kısaca, bir nesnenin içerisine bir verinin gizlenmesi olarak ifade edilebilir. Ses, sayısal resim, video görüntüleri üzerine veri saklanabilir. Bu veriler metin dosyası olabileceği gibi, görüntü veya ses dosyaları da olabilir. Veri gizleme ile ilgili olarak literatürde yapılmış birçok çalışma bulunmaktadır.

Literatürde vektör kuantalama, k-n eşikleme yöntemi ve çeşitli dönüşümler kullanarak (Ayrık Kosinüs Dönüşümü gibi) gerçekleştirilen, steganografik uygulamalar bulunmaktadır. Steganografik işlemleri daha iyi anlamak için, temel yöntem olan en az öneme sahip bit (LSB: Least Significant Bit) kavramının bilinmesi gereklidir. Bir resmin piksellerinin son bitlerinin mesaj bitleriyle yer değiştirmesiyle bu işlem gerçekleştirilir. Mesela, Şekil 2.7'de verilen resimde bulunan piksellerin LSB'leri ile mesaj bitleri sırasıyla değiştirilebilir. Bu sayede bir resim içerisine bir mesaj veya doküman kolaylıkla saklanabilir. Daha sonra yerleştirilen bu bitlerin tekrar sırasıyla geri elde edilmesiyle, deşifreleme işlemleri gerçekleştirilerek, verilerin tekrar elde edilmesi sağlanmaktadır.



Şekil 2.7. Sayısal Resim Yapısı

İçerisine doküman gizlenmiş bir resim e-posta veya başka bir elektronik iletişim yoluyla karşı tarafa gönderildiğinde arada giden mesajımızı izleyen veya elde eden herhangi bir kişi sadece resmi görebilecektir. Bu resim içine doküman gizlendikten sonra, beklendiği gibi, boyutlarda bir değişim gözlenmemektedir. Boyut değişikliğinin olmaması, şifreleme işleminin başarısının ayrı bir göstergesidir. Gizlenen dokümanın tekrar elde edilmesi için yine geliştirilen programda yapılan bir ters işlem ile gizlenen doküman otomatik olarak geri elde edilir. Bu yaklaşımda ses içerisine ses, resim ve doküman gizlenebileceğini burada belirtmekte fayda vardır.

2.9. Kuantum Şifreleme

Yukarıda anlatılmış olan metotların yanında, üzerinde çalışılan diğer bir şifreleme yaklaşımı da kuantum şifrelemedir. Bu şifreleme yaklaşımına ilginin yüksek olmasının sebebi, haberleşmenin gizli veya açıktan dinlenme tehdidini tamamen ortadan kaldırmasıdır.

Bu yaklaşım, optik haberleşmede fotonların kuantum özelliklerini temel almalarından dolayı mutlak güvenliği garanti etmektedir.

Önceki bölümlerde de vurgulandığı gibi, şifreleme ve şifre çözme yöntemlerinin etkinliği, kriptolama algoritması ile birlikte kullanılan anahtarın uzunluğuna bağlıdır. Eğer amaç, iletilen mesajların gizliliği ise algoritmaların tersine çevrilebilir olması gereklidir. Kuantum anahtar dağıtımında, tek fotonluk alıcılar ve vericiler kullanılarak, kırılamayan anahtarlar iki taraf arasında güvenli ve hızlı bir şekilde değiş tokuş edilir.

Kuantum yaklaşımıyla şifrelenen bir verinin, iki taraf arasındaki iletim sırasında, bir saldırgan tarafından, araya girilerek okunmaya çalışılması halinde, kuantum fizik yasalarına göre, ortaya çıkan "kuantum gürültüsü" saldırganın veriyi çözebilmesini imkansız kılmaktadır. Buna karşın gerçek alıcı, elindeki anahtar sayesinde, kuantum gürültüsünü ortadan kaldırarak orijinal veriye ulaşır.

Sayısal veri içindeki her bitin değeri, fotonlara polarizasyon uygulanarak belirlenir ve polarizasyon, elektrik alanının osilasyon yönüdür. Düşey ve yatay fotonları birbirinden ayırt etmek için, bir filtre ve diyagonal fotonlar için de, ikinci bir filtre kullanılabilir. Foton, doğru filtreden geçirilirse, polarizasyonu değişmez, aksi durumda polarizasyon rasgele bir değişime uğrar. İşte bu nedenle, iletim yolu

üzerinde, istenmeyen üçüncü bir şahıs veya saldırgan fotonları gözetlemeye çalışırsa, yüksek bir olasılıkla, fotonların polarizasyonunu değişikliğe uğratacaktır. Bu girişim, alıcı tarafından kolaylıkla öğrenilebilecek ve sonuç olarak verici ve alıcı taraflar gerekli önlemleri alabilecekltir.

Kuantum kriptolama kullanılarak gerçekleştirilen iletişimde, fiber optik ortam kullanılmasının yanında, uydu haberleşmelerinde de, bu yaklaşım kullanılmaya başlanacaktır. Bu sayede, gelecek yıllarda saniyede Gigabit mertebesinde akan trafiği de şifreleyebilmek mümkün olabilecektir.

2.10. Güvenlik Protokolleri

Açık anahtar tabanlı şifreleme kullanan başarılı protokoller arasında PGP (Pretty Good Privacy), SSL (Secure Socket Layer) ve çoğunlukla sertifika gerektirmeden kullanılabilse de SSH (Secure SHell) yer almaktadır. Bu yaklaşımlar aşağıda kısaca açıklanmıştır.

PGP

Güvenli bir e-posta yazılımı olan PGP'nin, ücretsiz ve açık kodlu olması ve güçlü şifreleme algoritmaları içermesi en önemli üstünlükleridir. Kullanımı çok da kolay olmayan bu yazılımın, kendine has ve oldukça karmaşık bir güven ve sertifika modeli bulunmaktadır. Bu sayede, güvenlik konularında az da olsa bilgi sahibi olan birisi, kendi güven sistemini istediği şekilde oluşturabilmektedir.

SSL/TSL

SSL, genel amaçlı kullanım için geliştirilmiş bir endüstri standardıdır. Güvenli HTTP bağlantısı sağlaması ve yaygın olarak tarayıcı (browser) programlar tarafından desteklenmesiyle, büyük bir kullanıcı kitlesine sahiptir. SSL ve TSL protokolleri, genel olarak TCP/IP protokollerine güvenlik katmak amacıyla geliştirilmiştir.

SSL, kendi başına çok karışık bir protokol olmamasına rağmen, bir kaç farklı opsiyon ve varyasyon sunmaktadır. SSL'in en basit hali, iletişim hattının şifrelenmesi durumudur. Bu protokol, bağlantı kuran iki uç arasındaki kimlik doğrulamayı, doğrulama işlemini şifrelemeden ayırmayı ve daha önceki bağlantının kaldığı yerden devam etmesini sağlamayı içeren daha karmaşık seçenekler sunmaktadır. SSL protokolü, bir birlerine gönderilen ya da gönderilmeyen bir dizi mesaj kümesinden oluşur.

SSL protokolü, Netscape tarafından geliştirilmiş olmasına rağmen, bu protokolün internette yaygın kullanımından dolayı, IETF için çok kritik bir hale gelmiştir. SSL protokolünün IPSec araştırmalarından ayrılmasını da içeren çeşitli nedenlerden dolayı, IETF bu protokolü biraz daha geliştirerek TSL (Ulaşım Güvenlik Katı-Transport Security Layer) olarak değiştirmiştir. TSL protokolü SSL'e göre çok az değiştirilmiş, güvenliği daha da arttırılmıştır.

SSH

Daha çok telnet ve ftp gibi uzaktan erişim protokolleri yerine kullanılan ve sunucu ile istemci arasındaki iletişimi şifrelemeye yarayan bir protokoldür. İstemci, sunucuya ilk bağlantı sırasında sunucunun gönderdigi açık anahtarı çevrim dışı yollarla doğrulayıp listesine ekleyebilir. Böylelikle, sertifika gerektirmeden, sunucunun açık anahtarı istemci tarafından öğrenilmiş olur. Bu işlem bir seferlik olup, SSH sisteminin kullanım amacı; sunucuda hesabı bulunan kısıtlı sayıdaki kullanıcıya hizmet vermektir.

S/MIME

Bu protokol, güvenli e-posta ortamı oluşturmak için kullanılan bir standarttır. Bu yapı PKCS#7 yapısı üzerine kurulmuştur ve RSA-DSA ve MIME standartlarını içerir. Bu protokolde mesaj içeriği açıktır, fakat tüm yapı şifrelenmiştir. Mesaj alındı teyidi, güvenlik etiketleri, posta listeleri, anahtar belirleme gibi işlemleri destekler. MD2, MD4, DES, 3DES, SHA-1, MD5, RSA, DSA, Diffie-Hellman gibi özetleme, imzalama, şifreleme ve anahtar şifreleme algoritmaları bu yapı içerisinde kullanılır.

IPSec

IP adresini taklit etme, veri trafiğini izleme ve veri paketlerini değiştirme gibi işlemlerin, internet ortamında kolaylıkla yapılabildiği bilinmektedir. Bu protokol iki bilgisayar arasındaki haberleşmeden, IP paketlerinin şifrelenmesi, online anahtar dağıtımı, sanal özel ağ (VPN) haberleşmesi, bilgisayar ile şifreleme cihazlarının haberleşmesine kadar, internet tabanlı tüm haberleşmelerde güvenliği sağlamak veya güvenli bir ortam oluşturabilmek için kullanılır.

Bu protokolun, IPv4 ve v6'ya uygulandığını burada belirtmekte fayda vardır. IPSec işlemi, IP doğrulama başlığı ve IP zarflama modları olmak üzere iki türde gerçekleştirilebilir. Değiştirilmiş veriyi ve tak-

lit edilen IP adreslerini anlama ve tüm paketlerin bütünlüğünün ve kimlik doğrulamasının yapılması, birinci türde gerçekleştirilmektedir. İzlemeyi önleme için, şifreleme ve paketteki verinin bütünlüğü ve kimlik doğrulama işlemi ise, ikinci türde gerçekleştirilir.

Bu protokolde şifreleme ve kimlik doğrulama, işlemlerini hızlandırmak, simetrik algoritmalarla yapılır. Bu işlemler yapılırken, SKIP veya IKE gibi protokoller de kullanılmaktadır.

Kerberos

Bu protokol, Needham ve Shroeder tarafından 1978 geliştirilmiştir. Simetrik anahtarların, bir anahtar sunucusu tarafından dağıtılması için kullanılır. Bu işleme, anahtar dağıtım merkezinden bir bilet almayla başlanır. Anahtar dağıtımı için önemli olan bu merkezin, her zaman aktif tutulması gereklidir. AAA ve sertifika kullanılması halinde bu protokole gerek kalmaz.

2.11. Elektronik İmza (e-imza)

Yasal açıdan imza, kişinin en değerli varlığıdır. Geleneksel imzalar gözden geçirildiğinde; kullanılan en eski yöntemlerin mühürleme ve parmakizi basma olduğu bilinmektedir. Günümüzde ıslak imza çok yaygın olarak kullanılmakta olup, *geleneksel imza* veya *ıslak imza*; "**elle atılan, çoğu zaman atan kişiye özgü olan, çoğu zaman imzalayanın adı ve soyadının farklı bir estetikle ortaya konduğu, değişmeyen bir şekle sahip, imzalayan kişinin imzalanan evrakları veya dokümanların içeriğini anladığını ve onayladığını gösteren ve hukuken anlam taşıyan düzenli veya anlamlı şekil veya karakterleri içerirler**" olarak tanımlanmaktadır.

Hayatımızın birçok alanında kullanılan ıslak imzalar; inkar edememe, taklit edememe, yeniden kullanamama, içerik değiştirememe, imzalayanın tanınması, belge ve belge içeriklerinin onaylanması, onaylayanın adı ve soyadı, onaylama tarihi ve buna benzer diğer hususların tespit edilmesinde kullanılmaktadır. Fakat, gerçekte bu hususlar değerlendirildiğinde, bunlardan bir çoğu doğru değildir. İmzalar taklit edilebilir, belgeler üzerinde değişiklikler yapılabilir, başka ortamlara taşınabilir.

Türk Hukukunda, 22 Nisan 1926 tarih ve 818 sayılı Borçlar Kanununun 14. Maddesinde ıslak imza; "***İmza*, üzerine borç alan kimsenin**

el yazısı olmak lazımdır. Bir alet vasıtasıyla vazolunan imza, ancak örf ve adetçe kabul olunan hallerde ve hususiyle çok miktarda tedavüle çıkarılan kıymetli evrakın imzası lazım geldiği takdirde kafi olunur." şeklinde tanımlanmaktadır.

Elektronik ortamda da ıslak imza benzeri bir imzanın yani e-imzanın kullanılması için, bir önceki paragrafta belirtilen özelliklerin bu ortamda da bulunması veya bu ortama aktarılması gereklidir. 5070 sayılı Yasanın 3. Maddesinde Tanımlar kısmında "***elektronik veri*: elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtları**", "***elektronik imza*: başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri**" şeklinde tanımlanmaktadır.

Ülkemizde "e-imza", "dijital imza", "sayısal imza" veya "elektronik imza" olarak da isimlendirilen bu yaklaşım, artık sadece elektronik ticaret yapanları, bankacıları, özel ve kamu hukukçularını değil herkesi ilgilendirmektedir. E-imza ile e-devlet yapısının yaygınlaşmasıyla, devletin vatandaşıyla, vatandaşın devletle, vatandaşın vatandaşla ve devletin devletle olan ilişkileri, elektronik ortama taşınarak, güvenli bir iletişim kanalı oluşturabilecektir. Devletin birim ve kurumlarının, özel sektörün ve bireylerin elektronik ortamda kimliklendirilmesiyle, hayatımız kolaylaşacak ve belki de daha yaşanılır bir hale gelebilecektir.

E-imza ve açık anahtar altyapısı; gelişmiş teknolojiler kullanarak, elektronik ortamda gönderilen veya alınan bilgilerin, bunları gönderen kişi veya kuruma ait olduğunun *doğrulanmasını*, iletilen veya alınan verilerin bilinmeyen kişiler (başkaları) tarafından gönderilmediğini veya bildiğimiz kişiler tarafından gönderildiğinin *belirlenmesini*, verileri gönderenlerin gönderdiğini ve alanların aldığını *inkar edememesini,* gönderilen veya alınan bilgilerin *içeriğinin değiştirilmemesini*, başkaları tarafından elde edilse bile, içeriğin başkaları tarafından *anlaşılamamasını* sağlamayı garanti eden, elektronik ortamda bit katarlarından oluşturulmuş **güvenli haberleşme ortamı**na verilen addır.

Diğer bir ifadeyle, **e-imza** veya **sayısal imza**, "bir elektronik mesaj veya iletiye eklenen ve göndereni emsalsiz şekilde tanımlayan veya taklit edilmesi çok zor olan bir sayısal kod" olarakta tanımlanmak-

tadır. Göndereni tanımlamanın yanısıra, mesajın içeriğinin onaylandığı, yapılan onaylamanın inkar edilemediği ve gereken durumlarda da gizliliğin sağlanması için kullanılmaktadır. Bir e-imzada bulunması gereken önemli özellikler;

- güvenilirlik,
- taklit edilemezlik,
- yeniden kullanılamazlık,
- inkar edilemezlik,
- içerik değiştirilemezlik ve
- yardıma gerek duyulmadan kullanılabilirlik

olarak sıralanabilir.

Amerikan "Electronic Signatures in Global and National Commerce Act (E-Sign)", e-imza'yı; "*elektronik bir ses, sembol veya veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan verileri değiştirmek veya işlemek için kişinin verileri imzalama (işaretleme) girişimi*" olarak ifade etmektedir.

Normal (ıslak) imzalarda olduğu gibi, e-imza tiplerinde de farklılıklar mevcuttur. İnkar edilemeyen imza, tuzak imza, sahte imza, vekalet imza, ve kör imza bunlardan bazılarıdır.

İnkar edilemez imza, imzayı atanın bilgisi olmadan doğruluğu kanıtlanamayan veya e-imzaların kopyalanmasını engellemek için kullanılır.

Bir kimsenin, içeriğini görmeden veya bilmeden bir belgeyi imzalamasına imkan veren e-imza tipi ise *kör imza* olarak bilinir.

Atılan bir e-imzanın sahte olduğunu kanıtlamaya çalışan e-imza yaklaşımı ise *tuzak imza* olarak isimlendirilir.

Bir diğer imza şekli de *vekalet imza*'dır. E-imza kullanacak kişiye, kendi gizli anahtarını açmadan bir başkasına imzasını kullandırma hakkı tanıyabilmesine imkan veren imza şeklidir.

Her ne kadar bu imzaların sayısını arttırmak mümkün olsa da, elektronik ortamda mümkün olduğunca tek bir imza kullanılması, her zaman güvenliği ve kullanılabilirliği arttıracaktır. Bu nedenle, farklı farklı imzalar kullanma yerine, tek bir imza kullanılmalıdır.

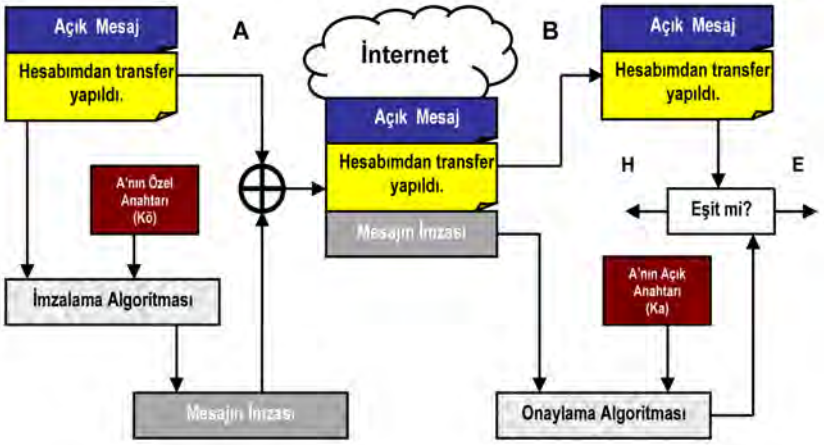
Bu sayede gizli anahtarların güvenliği artacak ve karşılaşılabilecek güçlükler ve tehlikeler azaltılmış olacaktır. Bu, günümüzde kullandığımız kredi kartlarına benzetilebilir. Kredi kartının sayısı arttıkça, kontrolünün de zorlaştığını çoğumuz gözlemlemişizdir. Bu bağlamda, birden fazla e-imza kullanımının, benzer zorluğu yaşatabileceği söylenebilir.

E-imza; farklı formatlarda ve formlarda bulunabilmektedir. Gelecek nesilde, e-imzaların veya m-imzaların yerini, kişilerin veya kullanıcıların parmak izi, retina, ses ve yüz gibi biometrik özelliklerden oluşturulacak imzaların alacağı açıktır.

İnternet ortamı bizlere birçok konuda kolaylıklar sağlasa da, bu ortamda işlem yaparken, bilgilerin başkaları tarafından her zaman elde edilme, dinlenme veya çalınma riski olduğu kesinlikle unutulmamalıdır. Şekil 2.8'de gösterildiği gibi, göndericiden (A) alıcıya (B), internet üzerinden bir mesaj gönderilirken, bu mesajın sardırgan veya üçüncü şahıslar tarafından dinlenme veya değiştirilmesi her zaman mümkündür.

İnternet/intranet ortamında gönderilen mesajlar, iletiler veya dokümanlar, çoğu zaman "düz metin" veya "açık metin" olarak isimlendirilirler. İnternet/intranet uzayında yapılan haberleşmelerin aktif veya pasif olarak dinlenilmesini önlemek için, mesaj içeriklerinin gizlenmesi veya kolaylıkla algılanamayacak bir formata dönüştürülmesi gerekir. Bu metinlerin saklanması, başka bir forma dönüştürülmesi işlemine, daha önceki bölümde de vurgulandığı gibi *şifreleme* denir. Bu işlem ile, mesaj güvenli olarak iletilebilir ama tam bir güvenlik için, yalnız şifreleme yeterli değildir. Bunlara ilave olarak, kimlik doğrulama, belirlenen kişi olduğunu ispatlama, bütünlük ve aldığını veya gönderdiğini reddetmeme gibi işlemlerin de haberleşme sırasında sağlanması gereklidir.

Bir e-imzalama sürecinde, imzalı bir mesaj gönderilmesi için, mesaj ile, mesajı imzalayacak kişiye ait özel anahtar bir imzalama algoritmasından geçirilir. Bu sayede mesajın imzası elde edilir. Elde edilen mesaj imzası açık mesaja eklenerek karşı tarafa gönderilir. E-imzalı haberleşme süreçleri Şekil 2.8'de verilmiştir.



Şekil 2.8. E-imzalama Süreci

Şekil 2.8'de verilen e-imzalama süreci aşağıda sırasıyla verilmiştir. Bunlar:

(1) Mesajı göndermek isteyen A, mesajını oluşturduktan sonra bu mesajı kendi özel anahtarı (Kö) ile imzalama algoritmasından geçirerek şifreler.

(2) Bu işlem sonucu oluşan şifreli mesaj, orjinal mesajın sonuna mesaj imzası olarak eklenir.

(3) Mesaja, imzayı ekleyerek B'ye (karşı tarafa) gönderir.

(4) B mesajı aldığında, imzayı onaylamak için mesajın imzasını A'nın açık anahtarı (Ka) ve onaylama algoritmasını kullanarak çözer. Eğer şifreli mesaj imzasını A'nın açık anahtarı ile çözebilirse, bu mesajın, gerçekten A'dan geldiğinden emin olur. A'nın açık anahtarı ile sadece, A'nın özel anahtarı ile şifrelenmiş mesajların çözebileceğini hatırlatmakta fayda vardır. A'nın özel anahtarı da, yalnız kendisindedir.

(5) Bu işlem sonucunda, orjinal mesajın elde edilip edilmediği karşılaştırılır. Eğer onaylama işlemi sonucu elde edilen imza mesajı ile, açık olarak gelen orjinal mesaj aynı ise, mesajın A'dan geldiği garanti edilmiştir.

(6) Şekilde gösterildiği gibi mesajın değiştirilip değiştirilmediğinin (bütünlüğü), burada kontrol edildiğini belirtmekte fayda vardır. Kimlik doğrulamaya ek olarak, bütünlüğün de kontrol edilmesi

beraberinde bir problemi açığa çıkarmaktadır. Doğal olarak bu problem, e-imza mesaj uzunluğunu iki katına çıkarmaktadır. Bu sorunu çözmek için ise özetleme fonksiyonları kullanılır.

2.12. Değerlendirmeler

Siber güvenliğin ve savunmanın iyi bir şekilde yapılabilmesi, şifre bilim, protokoller, algoritmalar, kuantum şifreleme yaklaşımları, matematiksel fonksiyonlar, simetrik ve asimetrik şifreleme ve şifre çözme, özetleme algoritmaları, steganografi bilimi, elektronik imza gibi hususların bilinmesi ve uygulanması kadar, büyük veri analitiği, derin öğrenme, 5G, SDN, NFV, yapay zeka, nesnelerin interneti, IPv6, yeni nesil internet, mahremiyet koruma vb. yeni geliştirilen teknik ve teknolojilerin de bilinmesi ve uygulanmasıyla sağlanabilecektir. Dolayısıyla; bu bölümde kısaca tanıtıldığı ve önemli hususlara kısaca parmak basıldığı unutulmamalı, bu teknolojiler ve algoritmalar ile yeni geliştirilen teknolojiler, yaklaşımlar, algoritmalar ve çözümler yakınen takip edilmeli, yeni konular üzerinde daha detaylı olarak çalışılmalı ve bunlar yeni çözümlerin geliştirilmesinde kullanılarak siber güvenliğin ve savunmanın iyileştirilmesi ve güncellenmesi için kullanılmalıdır.

Siber Güvenlik

BÖLÜM 3

Doç. Dr. Güzin ULUTAŞ

SİBER GÜVENLİK

Siber güvenliğin tanımından bahsedilecek olan bu bölümde, öncelikle siber güvenliğin uygulama ortamı olan siber uzay hakkında bilgi verilecek; siber uzayda meydana gelen siber savaşlar ve böyle bir ortamda bizler için siber güvenlik neden önemli gibi sorulara cevap aranmaya çalışılacaktır. Siber güvenlik ile Bilgi güvenliğinin beraber irdelemesi gerçekleştirilecek ve ardından siber güvenliğin ilgilendiği tehditler üzerine detaylı bir analiz yapılacaktır. Özellikle son yıllarda gerçekleştirilen siber saldırılar ise gelecekteki siber güvenlik politikalarına olan bakışımızı genişletebilmek amacı ile ayrıntılı olarak irdelenecektir.

3.1. Siber Uzay

İlk kez Amerikalı yazar William Gibson tarafından yazılan kısa bir hikayede tanımlanan siber uzay, 1984 yılında aynı yazarın "Neuromancer" isimli kitabında görüldü. 1984 yılını takip eden birkaç yıl içerisinde, siber uzay ifadesi bilgisayar sistemleri ile doğrudan ilişkilendirildi [1]. Siber uzayın internetten fazlası olduğu; yalnızca donanım, yazılım ve bilgiden değil aynı zamanda ağ içerisindeki sosyal etkileşimlerden de oluştuğu muhakkaktır. Sanal bir bilgisayar dünyası olarak da düşünülebilen siber uzay, günlük hayatı devam ettirecek hizmetleri sunabilen global bilgisayar ağını oluşturabilmek amacı ile kurulan elektronik bir ortamdır.

Çok katmanlı bir model olarak da ifade edilebilen siber uzay dört ana unsurdan oluşur: Fiziksel altyapı, Mantıksal yapılar, Bilgi ve İnsan [2]. İlk unsur, sistemleri oluşturan fiziksel birimleri temsil etmektedir. Havadan ve karadan geçen kablolar, yol boyunca haberleşmeyi sağlayan uydular, yönlendiriciler, anahtarlar vb. yapılar siber uzayın fiziksel temellerini oluşturmaktadır. Mantıksal yapılar ise yazılımı ifade eder. İşletim sistemleri, tarayıcılar, cep telefonu

yazılımları mantıksal yapılara verilebilecek örnekler arasında yer almaktadır. Yazılım, fiziksel birimlerin haberleşebilmesini ve görev yapabilmesini olanaklı kılacaktır. Üçüncü unsur olan bilgi siber uzay içerisinde var olur. Sosyal medya ortamındaki yazışmalar, postalar, resimler, videolar vb. siber uzayda akıp giden veriye örnek olarak gösterilebilir. Bilginin oluşturduğu, fiziksel temeller üzerine kurulu mantıksal yapılar yolu ile hareket eden Siber uzaydaki kuşkusuz en önemli unsur insandır. Uzaydaki bilgiyi kullanan, değiştiren, ileten, fiziksel ve mantıksal yapıları tasarlayan kişi insandır.

Zaman, Uzay, Bilinmezlik, Denksizlik ve Verimlilik olarak sıralayabileceğimiz beş parametre ise; siber uzayda oluşabilecek tehlikeleri anlayabilmek, yorumlayabilmek ve siber güvenliğin önemini görebilmek adına önemlidir [3]. Zaman, insan hayatının vazgeçilemez unsurudur. Bir olayın hazırlanması ve gerçekleşmesi belirli bir zaman alır. Siber uzayda ise bir olayın gerçekleşmesi anlıktır, önceden herhangi bir uyarı yoktur. Dünyada iki ülke arasında savaşın olabilmesi bir zaman gerektirir. Zaman süresince gerçekleşen politik olaylar aslında kötüye gidişin habercisi olabilir. Fakat siber uzayda gerçekleşecek siber savaşlar için durum farklıdır. Fiziksel olarak en yakındaki veya en uzaktaki bir yerden yapılabilecek saldırı anidir ve siber uzaydaki zamanda anlık bir olaydır. Uzay, aslında zaman ile beraber siber uzayı oluşturmaktadır. Siber uzayda, sınırlar önceden kestirilemez. Zaman içerisinde farklı bölgelere doğru genişleyebilir veya daralabilir. Teknolojik tabanlı veya ağ tabanlı güncellemeler gibi durumlar, uzayın değişimine sebep olur ve uzay bilinmezdir. Denksizlik, siber uzayda oluşabilecek tehlikeleri anlayabilmek ve güvenliği sağlayabilmek için uygulanacak adımları belirleyebilmek adına ilk öğrenilmesi gereken parametredir. Siber uzayda saldırıyı yapan kişinin yerini belirleyebilmek ve kimlik tespiti yapabilmek, bilinmezliği ortadan kaldırır. Fakat belirleme ve tespiti siber uzayda yapabilmek zordur. Siber uzayda gerçekleşen siber saldırıları bazen politik bilgisayar korsanı grupları üstlenirken bazen de saldırı sahibi kişi sadece meraklı bir üniversite öğrencisidir. Asimetrik savaşlarda, kişi, karşı tarafın zaaflarını kullanarak onu yenmeye çalışır. Bu dünyada gerçekleşen mücadelelerde, taraflar sayısal olarak denk olmasa bile, savaş kazanılabilir. Siber uzay asimetrik savaşların yeridir ve siber uzaydaki tarafların denksizliği, ülkeler açısın-

dan siber tehditleri oluşturur [4]. Bir siber saldırının verimliliğinden bahsederken internetteki kesintilerden ziyade, bir ülkenin veya bir kurumun güvenilirliğinin sarsılması temel alınabilir. Siber uzaydaki verimlilik farklı boyutlarda aynı anda birden fazla işi yapabilme ile ölçülür.

Siber uzayın tanımını yaptıktan ve onu etkileyen parametreler hakkında fikir sahibi olduktan sonra, aynı uzayda tanımlı rolleri ve durumları da sınıflayabilmek mümkün olacaktır.

3.2. Siber Savaş

İnsanlık tarihinde bilinebilen en eski savaşlar karada ve denizde gerçekleşiyordu. 1900'lü yıllardan sonra havacılık alanındaki gelişmeler, ülkelerin kendilerine ait hava kuvvetleri ordularını kurmasına olanak tanımıştır. 1950'lerden itibaren dünyadaki süper güçler arasındaki yeni savaş yeri ise uzay oldu. Bahsi geçen bu dört temel savaş alanı arasına, 21. yy'den itibaren yeni bir alan daha eklendi. Siber uzayda gerçekleşen ve farklı taraflara sahip olan bu savaşlar siber savaş olarak adlandırılmaktadır. Hangi zararlı teknolojik işlemin siber savaş sınıfına dahil olacağı henüz net olarak tanımlanmasa da genel olarak aşağıda ifade edildiği şekilde genel hatları çizilebilir.

Siber Savaş: Bir ülkeye karşı, işleyen kamu hizmetlerini aksatmak, itibarını zedelemek ve güvenilirliğini azaltmak adına başka bir ülke tarafından düzenlenen dijital saldırıdır.

Her ne kadar tanım ifadesinde sadece ülkelerden bahsedilmiş olsa da siber savaştaki taraflar değişebilir. Bazen işletmeler arasında bazense sadece bilgisayar korsanı grupları arasında siber savaşlar mümkün olabilir. Tablo 1'de son yıllarda ilgi çekmiş belli başlı siber savaşlar ve kimler arasında gerçekleştiğine dair bilgiler mevcuttur.

3.3. Siber Güvenlik ve Güvenliğe Duyulan İhtiyaç

Siber güvenlik; Bilgisayarları, sunucuları, elektronik sistemleri, ağları ve veriyi kötü niyetli siber tehditlerden koruma için uygulanan yöntemleri barındıran bir disiplindir. Kronolojik sıraya uygun olarak "Siber güvenlik nedir" sorusunun akademik çevrelerdeki karşılığı alt başlıklarda listelenmiştir [7].

Tablo 3.1. Son yıllarda adı duyulan siber savaş vakaları [5]

Yıl	Atak Adı	Etkisi
2010	Aurora	Çin ve Amerika arasında gerçekleşti, Dünyada ilk kez bir devlet diğerini siber atak yönetmek ile suçladı.
2010	Stuxnet	Endüstriyel SCADA sistemleri hedef alındı, Amerika ve İsrail tarafından İran'a karşı düzenlendiği düşünülmekte
2012	Red October	Sovyet Federasyonu Devletleri ve Doğu Avrupa etkilendi, Rusya ve İsrail ataktan sorumlu tutuldu
2014	Darkhotel	Bu saldırı daha çok yüksek profilli özel sektör yöneticilerini hedef aldı [6]
2015	Ukrain power grid	İlk kez bir siber saldırı güç şebekelerini hedef aldı. Geçici elektrik kesintileri yaşandı. Rusya tarafından düzenlendiği düşünülmekte.

1. Siber güvenlik: Yazılımlara, bilgisayarlara ve ağlara gerçekleştirilecek olan siber saldırıların riskini azaltmayı hedefler. Bu amaçla sızmaları tespit eden, virüsleri ve kötü niyetli erişimleri durduran, doğrulamayı zorunlu kılan, şifreli haberleşmeyi sağlayan vb. araçlar içerir [8].
2. Siber güvenlik: Araçların, kararların, güvenlik konseptlerinin, güvenlik önlemlerinin, kılavuzların, risk yönetim yaklaşımlarının, öğrenmenin, en iyi pratiklerin bir koleksiyonudur ve amaç siber ortamı ve kurum/tüzel kişilerin çıkarlarını korumaktır [9].
3. Siber güvenlik: Siber uzayın, siber saldırılardan korunmasıdır [10].
4. Siber güvenlik: Ağları, bilgisayarları, programları ve veriyi saldırıdan, tahripten veya yetkisiz erişimden koruyabilmek için tasarlanmış teknolojiler, süreçler, karşı hareketler ve yapılması gereken eylemler bütünüdür. Bu sayede gizliliği, bütünlüğü ve erişilebilirliği sağlar [11].
5. Siber güvenlik: Elektronik verinin izinsiz veya yasa dışı kullanımına karşı korunma durumudur veya bunu sağlayabilmek için tedbir alma yöntemidir [12].

Yukarıda verilen tanımlamalara genel olarak bakıldığında siber güvenliğin esas hedefinin; siber uzayda var olabilecek tehditlere karşı korunmak olduğunu anlıyoruz.

Siber uzayın genişlemesi, hükümetlerin, işletmelerin ve tüzel kişilerin daha çok servisi siber uzay üzerinden kullanıma açması, onları siber saldırılara ve siber savaşlara karşı daha aciz hale getirmektedir. Sadece hükümet veya kamu kuruluşları değil aynı zamanda son kullanıcılara ait bilgisayarlar, tabletler ve cep telefonları da bu uzayda yer almaktadır. Bilişime ait tüm donanımların birbirine böylesine bağlı olduğu bir uzayda, güvenliğin sağlanması muhakkak ki gerek devletler nezdinde gerekse kişiler nezdinde önem taşımaktadır.

3.4. Siber Güvenlik ve Bilgi Güvenliği Arasındaki Fark

Bilgisayar ağlarının kullanımının giderek artışı ve hayatımızın birçok alanına dahil oluşu, bilgi güvenliğinin sağlanması problemini beraberinde getirmiştir. Bu durumda siber güvenliğin tanımı ile beraber cevaplanması gereken bir soru da "Bilgi Güvenliği"ni "Siber Güvenlik"ten ayıran unsurların ve ortak yanlarının ne olduğudur.

Bilgi güvenliği; sağlanan servislerin, sistemlerin ve verinin korunmasını sağlar. Kişiler bilgi güvenliğini kendi bakış açısı ile değerlendirdiğinde, günlük hayatta kullandıkları bilgisayarların veya her gün kullandıkları sosyal paylaşım platformlarına girişin vb. güvenliğinin sağlanması olarak düşünebilir. Her kullanıcı için bilişim sisteminin farklı olanaklar sunduğu düşünülürse, bu durumda "bilgi güvenliği" ifadesinin kişilere özgü olarak farklı anlamlar taşıyabileceği söylenebilir. Son yıllarda günlük hayatımıza giren bir diğer ifade ise "siber güvenlik"tir. Özellikle kurumlar tarafından güvenlik uzmanı arayışında, iş ilanına yazılması gereken ifadenin "bilgi güvenliği uzmanı" mı yoksa "siber güvenlik uzmanı" mı olması gerektiği kafa karıştırıcı soru olarak kalmaktadır. Her ne kadar "bilgi güvenliği" ve "siber güvenlik" ifadeleri birbirlerinin yerine kullanılsa da aslında farklı anlamlar içermektedir. Her ikisinin örtüşen tarafları olduğu gibi ayrışan tarafları da mevcuttur.

Bilgi güvenliği, fiziksel ve sayısal olarak tutulan verinin, yetkisiz erişimlerden, kullanımlardan, bozulmalardan veya değiştirilmelerden korunmasıdır.

Siber güvenlik, bilgisayarların, verinin ve ağların yetkisiz sayısal ataklardan, erişimden veya tahripten, çeşitli yöntem ve teknolojilerin kullanımı ile korunmasıdır [13, 14].

Her iki terimin ortak değerlendirilmesi gerekirse:

1. Her ikisi de verinin güvenliğinin fiziksel olarak sağlanmasını gerektirir. Veriye olan fiziksel erişimin, sayısal veya fiziksel formların herhangi birinde tutulması durumunda dahi, yerinde olması gerekir. Her iki mekanizma için de verinin güvenliği ön plandadır.
2. Bilgi güvenliği açısından değerlendirildiğinde firmaya ait verinin yasa dışı herhangi bir erişimden uzak tutulması gerekirken, siber güvenlik açısından veriye yasa dışı sayısal erişimin engellenebilmesi temel problemdir. Siber güvenlik, siber uzayı yetkisiz sayısal erişimlerden korurken, bilgi güvenliği bilgi varlıklarının yetkisiz erişimlerden korunmasıdır.
3. Siber güvenlik, siber uzayda var olan veya var olmayan tehditlere karşı (sosyal medya hesaplarının, kişisel bilgilerin vb. korunması) koruma sağlarken, bilgi güvenliği bilgiye karşı olan tehditlerle ilgilenir. Bilgi güvenliğinin sağlamaya çalıştığı üç temel amaç: Bütünlük, gizlilik ve erişilebilirliktir.

Tablo 3.2'de siber güvenlik ve bilgi güvenliği tanımları karşılaştırmalı olarak sunulmuştur.

Tablo 3.2. Siber Güvenlik ve Bilgi Güvenliği Arasındaki Temel Farklılıklar

Siber Güvenlik ile Bilgi Güvenliğinin Kıyaslanması	
Siber güvenlik sayısal veya elektronik formdaki bilginizin korunması ile uğraşır.	Bilgi güvenliği, gerek fiziksel ve gerek sayısal biçimdeki bilgi varlıklarınızın korunması ile uğraşır.
Siber alemde var olan veriyi yetkisiz erişimlerden korur.	Bilgiyi korumakla ilgilenir ve bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlar.
APT (Advanced persistant threat) ler ile uğraşır.	Veri güvenliğinin temelidir.
Siber tehditlerle ilgilenir.	Tüm tehditlerle, uygun güvenlik protokollerinin olması gerektiği yerde olduğunu garantileyerek, ilgilenir.

Sonuç olarak, her ne kadar iki terim birbirleri ile değişmeli olarak kullanılabilir diye düşünülse de, "Siber Güvenlik" ağların, bilgisayarların ve verinin izinsiz elektronik erişiminden korunması ile ilgilenirken, "Bilgi Güvenliği" verinin sayısal veya fiziksel biçim-

de tutulmasına bakılmaksızın tüm veri varlıklarının korunmasını hedefler. Her iki alandaki uzmanlar için de, güvenlik tehditlerini özümseyebilmek temel hedeftir.

3.5. Siber Ortamda Tehditler

Siber ortamı tehlikeye atan, zarar veren veya bilinmez bir duruma sürükleyen hareketler, tehdit olarak algılanmaktadır. Siber ortam üzerinde oluşabilecek tehditleri tanımlamak, bu tehditler karşısında alınabilecek önlemleri belirleyebilmek adına önem taşımaktadır. Tehditler zararlı veya kasti hareketlerin sonucunda oluşabileceği gibi, bazen de kişilerin bilmeden gerçekleştirdiği bir olaydan da kaynaklanabilir. Örneğin sistemde yeni kullanıcı oluşturulması esnasında verilen izinlerin yanlış yapılandırılması istenmeden yapılmış bir hareket olmakla birlikte, siber ortam üzerinde istenmeyen etkiler oluşturabilmektedir.

Siber güvenliğin ilgilendiği tehditler beş başlıkta incelenebilir: Hacktivism, Siber Suç, Siber Sabotaj, Siber Terörizm, Siber Savaş. Her tehdit türünün bir motivasyonu, aktörleri ve hedefleri mevcuttur. Şekil 3.1'de tehdit türlerinin genel bir değerlendirmesi görülmektedir. Şekilde yukarıdan aşağıya doğru indikçe, siber tehdidin yaygın etkisi artmaktadır.

	Motivasyon	Aktör	Hedef
Hacktivism	Politik değişim, Egoizm	Aktivist, hacktivist ve bireyler	Ülkeler, işletmeler ve bireyler
Siber Suç	Ekonomik, finansal	Suçlular	İşletmeler, kişiler ve çeşitli kazançlar
Siber Sabotaj	Bilgi çalma	Milletler ve organizasyonlar	Devletler, organizasyonlar ve bireyler
Siber Terörizm	Politik değişim, korku, politik, dini veya ideolojik amaçlar	Teröristler, milletler	Altyapılar, genel hedefler, organizasyonlar ve bireyler
Siber Savaş	Politik veya sosyal değişimler	Milletler, bireysel bilgisayar korsanları, terörist gruplar	Kritik altyapılar, ülkeler, askeri güçler, kritik hedefler

Şekil 3.1. Siber tehditlerin motivasyon, aktör ve hedef bakımından değerlendirilmesi [3]

Hacktivizm, bir bilgisayar sisteminin veya ağın, sosyal veya politik açıdan teşvik eden bir sebep için amacı dışında kullanımıdır. Hacktivism, genel ilgiyi hareketi gerçekleştiren ve hacktivist olarak adlandırılan kişinin empoze etmeye çalıştığı konuya çeker. Çoğunlukla bireylerden oluşmakla birlikte bazı koordineli hareket eden hacktivist grupları da mevcuttur (Anonymous, LulzSec vb.).

Siber Suç, siber uzaydaki cinayet gibi tanımlanır. Bu olayda cinayetin zanlısı bir bilgisayardır. Siber suçlular bilgisayar teknolojisini kişisel bilgileri ele geçirmek, ticari sırları öğrenmek veya kötü amaçlı internet araştırmasını gerçekleştirebilmek için kullanırlar.

Siber Sabotaj: Gerçek dünyada, farklı milletlere ait planlar veya aktiviteler hakkında bilgi edinebilmek için ajanların kullanılması anlamına gelmektedir. Siber uzay açısından değerlendirildiğinde ise, bilgisayar korsanlarının bir ülke veya organizasyon tarafından tutulan sunuculara izinsiz erişerek gizli bilgiyi elde etmek amacı ile bilgisayar ağlarını kullanmasıdır. Gerçek dünyadaki ajanların, siber uzaydaki karşılığı ise bu tanımla beraber bilgisayar korsanları olmuştur.

Siber Terörizm: Desteklenen ve politik açıdan bir alt yapıya dayanan, bilgisayar sistemlerine, bilgisayar programlarına, önemli veriye karşı olan ve olayda seyirci kalan karşı tarafın zararı ile sonuçlanan ataktır [21].

Siber Savaş: Bir ülkeye karşı, işleyen kamu hizmetlerini aksatmak, itibarını zedelemek ve güvenilirliğini azaltmak adına başka bir ülke tarafından düzenlenen dijital saldırıdır.

3.6. Güncel Siber Saldırılar

Bu bölümde, özellikle son iki yılda gerçekleştirilmiş olan ve siber uzay üzerinde önemli etkilere sebep olmuş olan saldırılara ilişkin detaylar verilecektir. Çünkü; karşılaşılan siber saldırılar hakkında fikir edinilmesi ve sızmaların nasıl ve nerden kaynaklandığı sorularına cevap aranması, gelecekte izlenecek olan siber güvenlik politikalarının oluşturulması adına önem taşımaktadır.

Shadow Brokers: Shadow Broker isimli korsan grubu, Ekim 2016'da NSA tarafından kullanılan Hacking araçlarını çaldığını iddia etti [15]. Aynı ayın sonlarına doğru, bilgisayar korsanları NSA bağlantı-

lı grup olan Equation tarafından sızıldığını iddia ettiği sunucuların listesini içeren bir dosya yayınladı. Equation isimli bilgisayar korsanları grubu listedeki bu sunuculara, INTONATION ve PITCHIMPAIR kod isimleri ile anılan hacking araçlarını kullanarak sızmıştı. Shadow Broker grubu iki ayrı PGP şifreli arşive bağlantıyı yayınladı. Arşivlerden ilki saldırıların (hack'lerin) kanıtını içerirken (ve tamamen açıkken), grup diğer arşiv için 1 milyon BTC istedi. Yaklaşık 300 MB veri içeren ilk arşivde güvenlik duvarı zararlı yazılımları, hacking araçları, vb. içerik mevcuttu. Dosyaların çoğu en az üç yıllıktı ve en yeni zaman damgası Ekim 2013'dü. Nisan 2017'de grup satış modelini değiştirerek, NSA'nın hacking araçlarının bulunduğu ambarı, yeraltı bir sitede doğrudan satışa çıkardı.

Günümüze geldiğimizde, Shadow Broker grubu, Equation grubuna ait birçok hacking aracını ve zararlı yazılımını yayınladı. Ve en sonunda ise kendi şifreli dosyalarına erişimi sağlayacak olan parola, "Don't forget your base" başlıklı bir blog yazısında grup tarafından açık olarak yayınladı.

***WannaCry*:** 12 Mayıs 2017'de WannaCry isimli bir fidye yazılımı tüm dünyaya yayıldı (150 den fazla ülkede 200.000 den fazla sistem bu durumdan etkilendi) [16, 17]. Genel kuruluşlardan büyük işletmelere kadar birçok birim bu zararlı yazılımın etkisinde kaldı. İngiltere'deki National Health Service hastaneleri ve tesisleri geçici olarak işlem dışı kaldı ve bu durum İngiliz sağlık sistemi için o anda önemli bir kaos oluşmasına sebep oldu. Rusya'da ilgili fidye yazılımından en çok etkilenen ülkeler arasında yer aldı. Kamuya bağlı demiryolu şirketleri, Rusya'nın en büyük ikinci Telekom ağı fidye yazılımından etkilenen önemli kurumlar arasında yerini aldı. İspanya, Almanya, Fransa, İsveç ve Amerika'da ilgili yazılımın etkisinde kalan ülkeler arasındaydı.

WannaCry isimli bu kötü amaçlı yazılım iki ana parçadan oluşmaktadır: Trojan ve fidye yazılımı. Trojan yazılımı eski ve yamalanmamış Windows sistemlerdeki SMB güvenlik zafiyetini araştırarak sızma gerçekleştiriyorken, diğer kısım ise sızılan sistemdeki bütün dosyaları şifreleyerek WNCRY uzantısı ile yeniden kaydediyordu. Ardından yazılım her dizinde bir fidye mesajı oluşturuyor ve arka plan resmini ise kullanıcının ödemesi gereken miktarı ifade eden yazı ile değiştiriyordu. WannaCry yazılımı aslında EternalBlue isimli bir Windows zafiyetinden faydalanıyordu. Microsoft Mart

ayında bir yama yayınlamış olmasına rağmen, birçok işletmenin bu yamayı uygulamamış olması onları bu yazılıma karşı aciz hale getirdi. Sonuç olarak WannaCry toplamda yaklaşık 130,000 dolar elde etti, bu miktar böyle bir fidye yazılımı için aslında çok da fazla değildi.

Wikileaks CIA Vault 7: Mart 7'de, WikiLeaks CIA'den çalınmış 8761 adet dökümanın bulunduğu bir veri ambarı yayınladı. Bu ambarda birçok hacking aracı ve spying işlemlerinin dökümantasyonu mevcuttu. IOS ve Android zafiyetleri, Windows'daki böcekler, bazı akıllı TV'leri dinleme cihazına dönüştürebilme yöntemleri ile alakalı dökümanlar bu ambarda mevcuttu. Wikileaks bu ambarı "Vault 7" olarak adlandırdı [17].

198 Million voter Record Exposed: 19 Haziranda Chris Vickery isimli bir araştırmacı, 198 milyon Amerikalı seçmene ait kişisel bilginin bulunduğu bir veri tabanına genel erişimin olduğunu fark etti. Deep Root Analytics isimli bir veri firması ilgili veri tabanını Amazon S3 sunucusu üzerinde tutuyordu. Sunucu üzerindeki verilerin bazıları korunurken bir Terabyte'dan daha fazla seçmen bilgisi web üzerinden herkesin erişimine açıktı. Böyle bir yanlış yapılandırma siber güvenlik açısından önemli bir durumken, gerek kişisel gerekse tüzel açıdan siber risk oluşturmaktadır [17].

***Macron Campaign Hack*:** Fransa'nın son etap cumhurbaşkanlığı seçiminden iki gün önce, bilgisayar korsanları, sol eğilimli yarışı önde götüren Fransız Emmanuel'in partisinden olan 9GB büyüklüğündeki postaları sızdırdı [17]. Macron'un böyle bir karşı saldırıya karşı cevap verebilmesi, sızmanın zamanına bakıldığında çok zordu. Fakat yine de Macron kampanyası, sunulan verilerdeki her şeyin doğru olmadığına dair beyanlarda bulundu. Bu atak Amerika'daki seçimde Hillary Clinton'ın maruz kaldığı siber saldırıdan daha az stratejikti ve Macron'un kendisinden önceki örneğe bakarak karşılık verme yöntemini belirleyebilme şansı vardı. Araştırmacılar bu saldırının arkasında Rusya hükümeti bağlantılı bir korsan grubu olan FancyBear'ın varlığına dair bulgulara erişti.

2018'in ilk yarısına bakıldığında, devlet düzeyinde sızmalar veya global fidye yazılım atakları 2017'ye kıyasla daha az miktarda gerçekleşti.

***Russian Grid Hacking*:** 2017 yılında, güvenlik araştırmacıları Rus korsanların Amerika'daki firmalara sızdığı ve inceleme yaptığına yönelik bilgi verdi. 2017'den itibaren gerçekleşen Rus kökenli saldırılar da göz önüne alındığına, böyle bir sızma testi hükümet düzeyinde açıklamaları beraberinde getirdi. NotPetya zararlı yazılımı ve şebeke saldırısı olayları, Amerikan hükümeti tarafından yapılan bir açıklama ile doğrudan Rusya ile ilişkilendirildi. Her ne kadar olayların bağlantısı güvenlik çevrelerince biliniyor olsa da ilk kez devlet düzeyinde bir açıklama geldi [18].

US Universities: Mart ayında, Amerikan Adalet bakanlığı dokuz İranlı korsanı ülke çapındaki 300'den fazla üniversitede düzenlenen ataklardan sorumlu tuttu [18]. Şüpheliler, 144 Amerikan üniversitesine, diğer 21 ülkedeki 176 üniversiteye, 47 özel şirkete ve diğer bazı hedeflere saldırıdan suçlandı. DOJ korsanların 31 Terabyte'lık veri çaldığını rapor etti. Saldırılar, üniversitedeki öğretim üyelerinin zararlı bağlantılara tıklamasını ve kendi ağlarında kullandıkları kullanıcı isimlerini ve parolalarını girmelerini sağlayan özel oluşturulmuş postalar ile gerçekleştirildi. 100,000 hesap hedeflenen saldırıda 8000 tanesi ele geçirildi. DOJ'un raporunda göre, Mabna Enstitüsü olarak adlandırılan Tahran tabanlı korsanların yer aldığı kuruma kadar saldırı izlerinin devam ettiğini rapor etti.

Rampant Veri Sızıntısı: Veri sızıntıları 2018 yılında da devam etti. Fakat 2017 yılından farklı olarak, 2018'in ilk yarısında veri teşhiri atakları ağırlıklıydı [18]. Veri teşhiri, isminden de anlaşılacağı üzere, verinin internet üzerinden herkese açık hale gelmesi anlamını taşımaktadır. Bu çoğunlukla bulut kullanıcılarının yanlış yapılandırdığı veri tabanlarından kaynaklanmaktadır. Böylelikle veriye herhangi ek bir doğrulama prosedürüne ihtiyaç duyulmadan erişilebilmektedir. Exactis isimli firma neredeyse 340 milyon kaydı genele açık bir sunucu üzerinde korunaksız bıraktı. Verinin içerisinde güvenlik numaraları veya kredi kartı numaraları gibi bilgiler içermese de, yüzlerce Amerikalı gence ait kişisel 2 Terabyte'lık bilgi mevcuttu. Bu problem güvenlik araştırmacısı Vinny Troia tarafından tespit edildi ve Haziran'da WIRED tarafından rapor edildi.

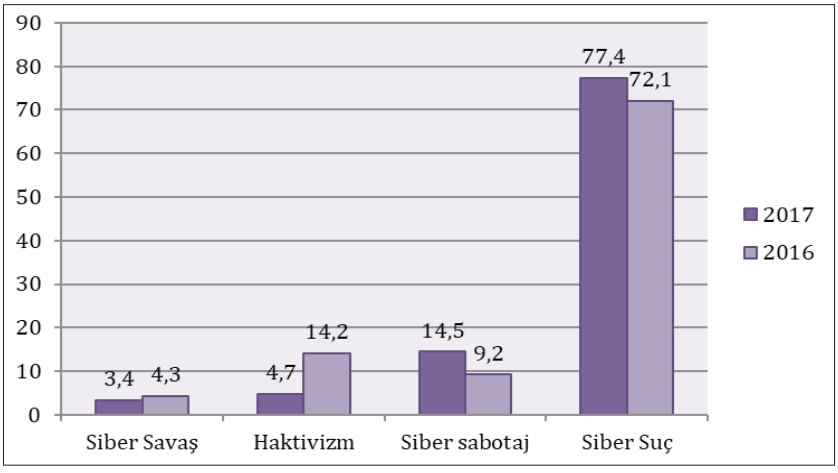
3.7. Siber Güvenlik İstatistikleri

Siber güvenliğin önemini anlayabilmek adına bazı istatistiklere bakmak yeterli olmaktadır [19]. Verilen istatistiki bilgiler, dünya

üzerinde her gün gerçekleşen siber atakların sayısındaki artışı ve bunların acı bilançolarını net olarak ortaya koymaktadır. 1 Ocak 2005'den, 18 Nisan 2018'e kadar kaydedilen 8854 sızıntı mevcuttur. 2017 yılında dünya genelinde kuruluşların %31'i işletme teknoloji altyapılarında siber ataklara maruz kaldı. Siber atakların böylesine yoğun olduğu ve bizlerin de içerisinde bulunduğu siber uzayda, 2016 yılından itibaren rapor edilmiş önemli sızıntılar Tablo 3.3'de listelenmiştir.

Tablo 3.3. 2016 yılından itibaren olan önemli sızıntılar [19]

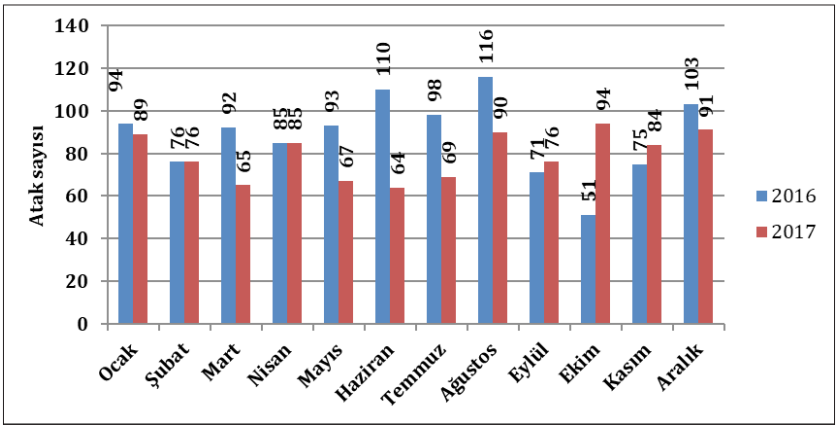
Yıl	Etkisi
2016	3 milyar Yahoo hesabı ele geçirildi.
2016	ÜBER firması korsanların 57 milyonun üzerinde sürücü bilgisinin çalındığını açıkladı.
2017	412 milyon kullanıcı hesabı Friendfinder sitesinden çalındı.
2017	147.9 milyon tüketici Equifax açığından etkilendi.
2017	150 ülkedeki 100.000 grup ve 400.000'den fazla makine Wanncry isimli virüse maruz kaldı.
2017	Symantec'in raporlarına göre neredeyse her gün 24000 kötü amaçlı mobil yazılım bloklandı.
2018	Under Armor, kendilerine ait olan "My Fitness Pal"'ın kırıldığını ve 150 milyon kullanıcının bundan etkilendiğini açıkladı.



Şekil 3.2. 2016-2017 yıllarındaki siber tehditler açısından dağılım [20]

Siber tehditler açısından değerlendirildiğinde son iki yıl içerisindeki istatistikler Şekil 3.2'de verilmiştir [20]. 2017 yılında siber suçlar açısından %5'lik bir artış gözükmektedir.

Diğer bir istatistikte 2016 ve 2017 yıllarında ay bazında gerçekleşen siber saldırılar hakkında bilgi verilmektedir [20]. Şekil 3.3'de görüldüğü gibi 2017 yılı 2016'ya göre daha az siber saldırı sayısı gözükmektedir. Fakat 2017 yılında gerçekleşen WannaCry veya NotPetya gibi ataklar yaygın bir etkiye ve tahribe sebep olmuştur.



Şekil 3.3. 2016 ve 2017 yıllarının ay bazında siber saldırılar cinsinden değerlendirmesi [20]

3.8. Değerlendirmeler

Devlet düzeyindeki hizmetlerin, işletmelere ait süreçlerin, bireysel işlemlerin gün geçtikçe daha çok siber uzaya transfer edildiği düşünüldüğünde muhakkak ki bu uzaydaki güvenliğin sağlanması kaçınılmaz olacaktır. Özellikle son yıllarda devletler düzeyinde siber güvenliğe önem verilmekte ve siber uzay yeni bir savunulması gereken alan olarak görülmektedir. Siber saldırıların bırakmış olduğu tahrip gerek devlet gerekse kurumsal düzeyde sıkıntılara yol açmaktadır. Tüm dünya genelinde devlet politikalarında siber güvenliğin önemi vurgulanmakta ve devletler kendi siber uzaylarını savunabilecek siber ordular kurmaya çalışmaktadır. İlerleyen yılların siber savaşlara gebe olduğu düşünüldüğünde, her ülkenin kendini savunacak gerekli bilgi ve donanıma sahip siber ordular oluşturmasının önemi net olarak anlaşılmaktadır.

Kaynaklar

[1] K. N. Sevis, E. Seker, "Cyber warfare: terms, issues, laws and controversies," 2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security), London, 2016, pp. 1-9. doi: 10.1109/CyberSecPODS.2016.7502348

[2] Dave Clemente, "Fundamentals of Cyber Security", A biennial collection of analysis on international agreements for security and development, Vertic (Verification, Research, Training and Information Centre), Chapter 10.

[3] Jenna Ahokas, Tuomas Kiiski, Cybersecurity in ports, Publications of the hazard project, vol 3., 2017.

[4] The threat, defense, and control of cyber warfare, http://cimsec.org/threat-defense-control-cyber-warfare/32106

[5] The world's 10 most dangerous cyberwarfare attacks, https://www.techworld.com/security/worlds-10-most-dangerous-cyberwarfare-attacks-3601660/

[6] DarkHotel malware attacks target poorly secured networks, especially in hotels https://www.pcworld.com/article/2846238/darkhotel-malware-attacks-target-poorly-secured-networks-especially-in-hotels.html

[7] Dan Craigen, Nadia Diakun-Thibault, Randy Purse, "Defining Cybersecurity", Technology Innovation Management Review, pp. 13-21, Ekim 2014.

[8] Amoroso, E. 2006. Cyber Security. New Jersey: Silicon Press.

[9] ITU. 2009. Overview of Cybersecurity. Recommendation ITU-T X.1205. Geneva: International Telecommunication Union (ITU). http://www.itu.int/rec/T-REC-X.1205-200804-I/en

[10] CNSS. 2010. National Information Assurance Glossary. Committee on National Security Systems (CNSS) Instruction No. 4009.

[11] Public Safety Canada. 2014. Terminology Bulletin 281: Emergency Management Vocabulary. Ottawa: Translation Bureau, Government of Canada.

[12] Oxford University Press. 2014. Oxford Online Dictionary. Oxford: Oxford University Press. October 1, 2014: http://www.oxforddictionaries.com/definition/english/Cybersecurity

[13] Cyber Security Vs Information Security, https://www.hack2secure.com/blogs/cyber-security-vs-information-security

[14] Difference Between Cyber Security and Information Security, http://www.differencebetween.net/technology/difference-between-cyber-security-and-information-security/

[15] The Shadow Brokers release more alleged NSA hacking tools and exploits https://securityaffairs.co/wordpress/57859/intelligence/shadow-brokers-nsa-hacking-tools.html

[16] WannaCry, https://www.webopedia.com/TERM/W/wannacry.html

[17] The biggest cybersecurity disasters of 2017 so far, https://www.wired.com/story/2017-biggest-hacks-so-far/

[18] The worst cybersecurity breaches of 2018 so far, https://www.wired.com/story/2018-worst-hacks-so-far/)

[19] 60 Must-Know Cybersecurity Statistics for 2018, https://blog.varonis.com/cybersecurity-statistics/

[20] 2017 Cyber Attacks Statistics, https://www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/).

[21] Cyber Security Focusing on Hackers and Intrusions, https://www.fbi.gov/news/stories/cyber-security

Siber Güvenlik Farkındalığı, Farkındalık Ölçüm Yöntem ve Modelleri

BÖLÜM 4

Y. Müh. Salih ERDEM EROL
Prof. Dr. Şeref SAĞIROĞLU

SİBER GÜVENLİK FARKINDALIĞI, FARKINDALIK ÖLÇÜM YÖNTEM VE MODELLERİ

Bu bölümde öncelikle geçmiş yıllarda yaşanan siber saldırılar ışığında siber güvenlik kavramının önemine değinilmiş, bilgisayar ve internet kullanıcı sayılarındaki artış ile birlikte saldırganların hedeflerindeki değişimler ve sistematik yaklaşımları ortaya konulmuştur. Farkındalık bakış açısıyla siber saldırı yaşam döngüsü ortaya konulmuş ve örnek bir olay ile açıklanmıştır. İnsan faktörünün saldırılarda öneminin giderek artmasından dolayı, farkındalığın bilgi güvenliğinin sağlanmasında etkin bir unsur olarak kullanılabilmesi için öncelikle kavramsal değerlendirmesi yapılarak bileşenleri belirlenmiş ve bileşenlerin birbiri ile olan ilişkileri açıklanmıştır. Son olarak, farkındalık seviyesinin belirlenmesi ve arttırılmasına yönelik olarak literatürde yapılan çalışmalar incelenerek değerlendirmeler sunulmuştur.

4.1. Giriş

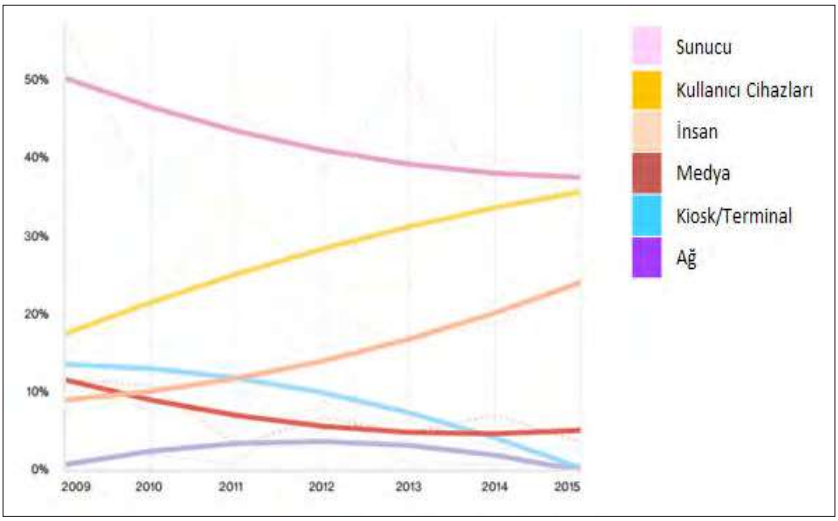
Bilgi teknoloji sistemlerinin bilgiye her yerden ve merkezi olarak erişimi mümkün kılmasından dolayı bilgi sistemleri hayatın tüm alanlarında etkin olarak kullanılmaktadır. Günümüzde e-devlet uygulamalarının da kullanıma sunulması ile resmi işlemlerden yasal işlemlere, eğlenceden eğitime kadar birçok alanda bilgi teknolojileri gündelik hayat içerisinde kendisine yer edinmiştir. Bu denli hızlı gelişen bilgi teknoloji sistemlerine göz atıldığında öneminin hızla arttığı görülmektedir. Özellikle sistemlerin birbirine bağımlılığının artmasıyla iş dünyası ve kamu hayatı hızla artan sayılarda ve çok çeşitli saldırılara maruz kalmaktadır. Bilginin basılı, elektronik ortamda, tabelalarda, konuşmalarda vb. birçok şekilde bulunması, bilgi paylaşımlarının yaygınlaşması ve farklı birçok yöntem ile

gerçekleştirilmesi saldırıların yöntem ve çeşitliliğinin artmasına da imkân sağlamaktadır. Verinin paylaşımı ve sürekli erişime açık olması nedeniyle bilginin gönderen kaynaktan alıcıya kadar gizlilik içerisinde, bozulmadan, yok edilmeden, değiştirilmeden, başkaları tarafından ele geçirilmeden ve bütünlüğü sağlanmış bir şekilde iletilmesi bilgi güvenliğinin sağlanması için temel kriterlerdir [1]. Kamu hayatını düzenleyen sistemler açısından bakıldığında bu kriterlerin önemi çok daha açık bir biçimde açığa çıkmaktadır.

Kamu hayatını düzenleyen sistemlere kişisel, kurumsal ve ulusal bilgi güvenliği açısından bakıldığında bilgi güvenliğinin günümüzde hangi noktalara ulaşabildiğini görmek mümkündür. Estonya'nın 26 Nisan 2007'de Bronz Asker heykelini kaldırmasıyla dünyada siber savaş kavramı bir gerçekliğe dönüşmüş ve Rusya yanlısı gruplar tarafından gerçekleştirilen DOS saldırılarıyla Estonya Hükümeti, kamu kurumları ve bankacılık hizmetlerine ait birçok internet sitesi hizmet dışı kalmıştır. Estonya konuyu NATO'nun gündemine taşımış, dünya bir savaşın eşiğine gelmiştir. Benzer olarak Rusya, Gürcistan ile savaşırken eş zamanlı olarak siber saldırıları da başlatarak Gürcistan devlet kurumlarının bilgi sistemlerini uzun süre erişilemez hale getirmiş ve zarara uğratmıştır [2].

Günümüzde kişisel kayıplardan, uluslararası anlaşmazlıklara kadar çok geniş bir etki alanı bulunan bilgi güvenliği kavramı endişelerin yanı sıra ilgiyi de bu alana çekmiştir. Ancak bilgi güvenliğine yönelik akademik ve endüstriyel çalışmaların uygulama ve teknolojik çözümlere yoğunlaştığı görülmektedir. Bilgi güvenliğin aslında başlangıç noktası olan ve son yıllarda saldırganların teknolojik önlemleri aşmak için emek ve zaman harcamak yerine daha maliyetsiz olan insan üzerinden kapıları açma eğiliminin artması ve daha yüksek başarım elde etmeleri farkındalık kavramının önemini bir kez daha ortaya koymuştur.

Şekil 4.1'de 2009-2015 yılları arasında varlık kategorilerine göre yaşanan veri sızıntılarına ilişkin grafik yer almaktadır [3]. Bu grafikte saldırganların insan ve kullanıcı cihazlarına yönelik başarılı saldırıları ciddi oranlarda artarken diğer alanların tamamında 2009 yılı verilerine göre azalma olduğu görülmektedir. Bu yükselişe kullanıcıların farkındalık düzeylerinin düşük olmasının büyük etkisi bulunduğu değerlendirilmektedir.



Şekil 4.1. Varlık kategorilerine göre veri sızıntısı gerçekleşme oranları [3]

Türkiye'deki genel durum değerlendirildiğinde, kullanıcıların farkındalık düzeylerinin incelenmesine yönelik yapılan bir çalışmada [4], 501 kullanıcının %96,3'lük çok büyük bir kısmı bilgi güvenliği benim için önemlidir derken, aynı kullanıcıların %51,5'i cihazlarına yönelik tehditlerden haberdar olmadığı cevabını vermiştir. Dolayısıyla kişisel ya da kurumsal olarak bilgi güvenliğinden bahsedebilmek için ilk şart kullanıcıların farkındalık sahibi olmasıdır ve insan günümüzün en büyük hedefi haline dönüşmüştür.

2015 yılında IBM tarafından sunulan bir raporda veri sızıntılarının %95'inin insan hataları sonucunda gerçekleştiği ortaya konulmuştur [5]. Bu denli yüksek oranda bilgi sızıntılarına kaynak teşkil eden insan faktörü gelişen teknoloji ve maliyetlerdeki düşüşle beraber her geçen gün daha etkin bir şekilde bilişim dünyası içerisinde rol almaktadır. TÜİK'in [6] 16-74 yaş arası bireyleri kapsayan, girişimlerde ve hanelerde bilişim teknolojileri kullanımına yönelik yapılan istatistiki çalışmaları doğrultusunda elde edilen sonuçlar Tablo 4.1'de görülmektedir. Bu çizelgede artık girişimlerin neredeyse tamamının işlemlerini bilgisayarlar vasıtasıyla dijital ortamda gerçekleştirdiğini, birçoğunun kullanıcılara yönelik web sayfası da işlettiğini, hane kullanıcılarının ise 2005 yılına göre yaklaşık %800'lük bir artışla %69.5'lik bir oranda internet erişimine sahip olduğunu, bir diğer istatistiki veride hanelerin %96,8'inde cep telefonu ya da

akıllı telefon bulunduğu, %20,9'unda internete bağlanabilen akıllı televizyon bulunduğu tespit edilmiştir.

Bu veriler ışığında kişisel ve kurumsal bilgi varlıklarının eskiye oranla çok daha fazla dijital ortamda işlem gördüğünü, internet ortamına açık olduğunu ve siber saldırganların erişim alanına girmesi nedeniyle tehdit altında olduğu ve bu sistem ve varlıklara erişimi bulunan insan faktörüne karşı tehdidin her geçen gün daha da arttığı açıkça görülmektedir.

Tablo 4.1. TÜİK Bilgi Toplumu istatistikleri [6]

		2005	2010	2011	2012	2013	2014	2015
Kurumlarda	Bilgisayar Kullanımı	87,8	92,3	94,0	93,5	92,0	94,4	95,2
	İnternet Erişimi	80,4	90,9	92,4	92,5	90,8	89,9	92,5
	Web Sitesi Sahipliği	48,2	52,5	55,4	58,0	53,8	56,6	65,5
Hanelerde	Bilgisayar Kullanımı	22,9	43,2	46,4	48,7	49,9	53,5	54,8
	İnternet Kullanımı	17,6	41,6	45,0	47,4	48,9	53,8	55,9
	İnternet Erişimi	8,7	41,6	42,9	47,2	49,1	60,2	69,5

Dünya genelinde de benzer şekilde artan bilişim teknoloji ürünlerinin kullanım ve internete açık olma oranları siber saldırıların oranlarında da artışlara sebep olmaktadır. Symantec'in hazırladığı İnternet Güvenlik Tehdit Raporunda (ISTR) [7], kullanıcıların ve kurumların maruz kaldığı tehditler aşağıdaki maddelerde verilmiştir.

- 500 milyondan fazla kişisel verinin çalındığı,
- 0-gün açıklık sayısının %125 artarak neredeyse her hafta bir 0-gün açıklığının bulunduğu (54 Adet),
- Kullanıcılara karşı her gün 1 milyondan fazla web saldırısı gerçekleştiği,
- Kurum çalışanlarını hedef alan hedefli sazan avlama saldırılarının önceki yıllara göre artış gösterdiği,
- Fidye yazılımların verdiği zararın geçmiş yıllara oranla artış gösterdiği,

- 100 milyon sahte teknik destek aramasının engellendiği,
- Zararlı yazılım türlerinin sayısında artışın devam edildiği,
- Ortalama 1/220 epostanın zararlı yazılım içerdiği,
- Yeni bulunan mobil açıklık sayısında artış olduğu,
- Açıklık tespit edilen web sayfası ortalamasının %2 artarak %78'e çıktığı ve
- Türkiye'nin botnet barındıran ülkeler sıralamasında %4,5 ile dünyada 4. sırada olduğu raporlanmıştır.

Verizon'un 70 kuruluşun katkısı ile yaptığı araştırma sonucunda yayımladığı "Veri Sızıntı Araştırmaları Raporu", karşılaşılan maddi kayıbın boyutunun dünya genelinde 400 milyon $ olduğunu bildirmektedir [8]. Tüm dünyadaki kuruluşlar ve kişiler de hesaba katıldığında ortaya çıkan maddi kaybın çok daha büyük olacağı görülmektedir. Gartner Inc. tarafından yapılan bir çalışmada, veri sızıntısı durumunda oluşan zararın koruyucu önlemlere yapılan harcamalara göre 15 kat daha fazla olduğu ortaya konulmuştur. Günümüzde sayısal ortama geçen kurum ve kuruluşların sayısı ve sahip olunan bilgi varlıklarının boyutları düşünüldüğünde bu değerin çok daha artacağı açıktır.

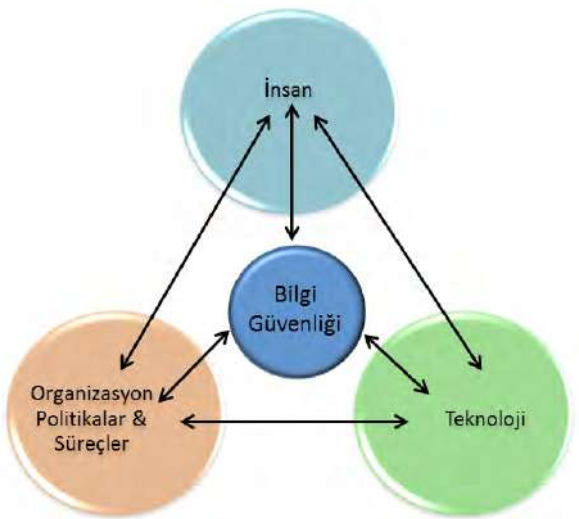
Bahse konu istatistikî veriler ve incelenen ISTR doğrultusunda, siber güvenlik farkındalığının son kullanıcı, kurum çalışanı, statü, yaş gibi etmenleri gözetmeksizin çok önemli bir hale geldiği görülmektedir. Teknolojik önlemlerin günümüzde bilgi güvenliğinin sağlanması için tek başına yeterli olması imkânsız hale gelmiştir. Farkındalık eğitimleri ise etkili, ancak günümüzde siber saldırıların iki eğitim arasında geçen süreden çok daha kısa sürelerde gelişmesi ve farklılaşması sebebiyle yetersiz kalmaktadır. Bu hızlı değişime ancak siber güvenlik farkındalığının etkin yönetimi ile ayak uydurulabileceği açıktır. Etkin yönetimin temeli ise farkındalık seviyesinin doğru yöntem ve uygulamalarla ölçülmesi, takiben dinamik bir süreç içerisinde modellenerek insanlar tarafından davranışa dönüştürülmesine dayanmaktadır. Bu nedenle bilgi güvenliğinden bahsedebilmek için farkındalık kavramının öncelikli olarak gündeme alınması zorunluluk haline gelmiştir.

Bu denli büyük hareket alanı olan siber saldırılar ve yarattığı etkiler; kişisel, kurumsal ve ulusal anlamda yapılan güvenlik yatırımları,

ihtiyaçların giderilmesinde yönetim desteğinin arttırılmasına ortam sağlamaktadır. Ancak içerisinde farkındalık konusunda planlama yapılmayan güvenlik yatırımlarının yeterli olmayacağı da açıkça görülmektedir.

4.2. Bilgi Güvenliği Farkındalığı ve Bileşenleri

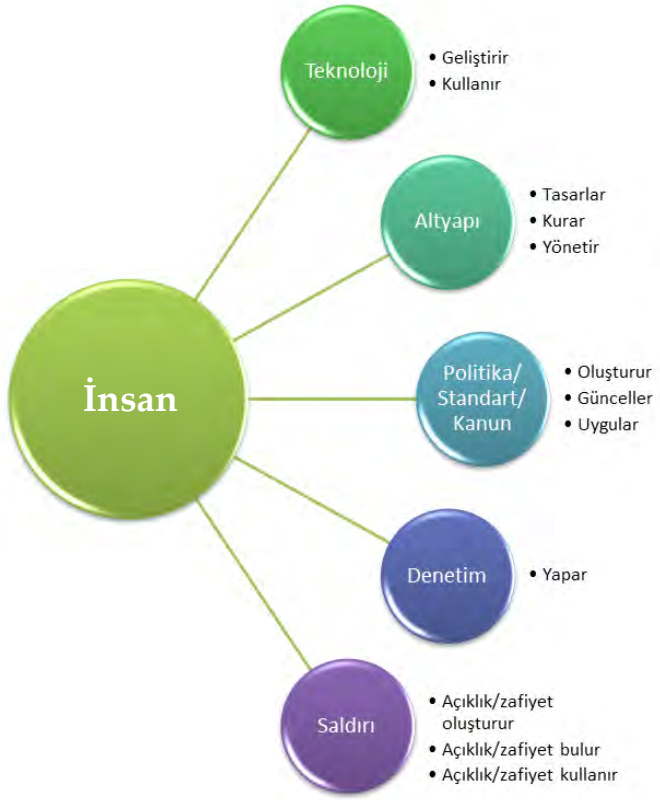
Bilgi güvenliği ile ilgili çalışmalarda genelde 3 sacayağı olduğu değerlendirilmektedir [9]. Roa ve Nayak'ın ortaya koyduğu bilgi güvenliği bileşenleri Şekil 4.2'de görülen insan, teknoloji ve organizasyondan oluşmaktadır [9].



Şekil 4.2. Bilgi güvenliği katmanları [9]

Cherdantseva ve Hilton [10] ise yaptıkları çalışmada, bilgi güvenliği mekanizmalarını 4 ana başlıkta toplamıştır. Bunlar organizasyonel (politika, denetim, strateji vb.), teknolojik (biyometri, güvenlik duvarı, dijital imza vb.), insan merkezli (eğitim, kültür, farkındalık vb.) ve yasal (mevzuat, servis seviyesi anlaşmalar vb.) mekanizmalardan oluşmaktadır. Gerek bileşenler gerekse bu bileşenlere yönelik alınabilecek tedbirler üzerine yapılan sınıflandırmalarda insan en önemli bileşendir. Günümüzde teknolojik, yasal ve organizasyonel alanlara yönelik birçok çalışma yapılırken insan üzerine çalışmalar ikinci planda tutulmaktadır. Ancak bu katmanlı yapının bilgi güvenliğine yönelik bilgi birikimi ve farkındalıkta yaşanan gelişimle

beraber farklılaştığı değerlendirilmektedir. İnsan bilgi güvenliğinin bir katmanı ya da bileşeni olmaktan çıkarak bilgi güvenliğinin sağlanması için organizasyonun oluşturulması, yasal düzenlemelerin yapılması ve teknolojinin yönetilmesinde son derece etkin bir konuma gelmiş ve özetle diğer tüm katmanlara platform sağlar hale gelmiştir. Dolayısıyla insan katmanında oluşacak herhangi bir eksikliğin diğer tüm katmanları da etkisiz hale getireceği değerlendirilmektedir. Yaşanılan dönüşüm sonrası öngörülen bilgi güvenliği katmanları Şekil 4.3'de görülmektedir.



Şekil 4.3. Bilgi güvenliği unsurları ile insan faktörünün ilişkisi

Bilgi ve farkındalık eksikliği olması durumunda insanın bulunduğu konum ve etki alanı doğrultusunda bilgi güvenliği zafiyetleri doğuracağı açıktır. Tüm teknoloji, altyapı, politik/standart/kanun ve denetim alanlarının başarısı insan tarafından gerçekleştirilmektedir. Dolayısıyla günümüzde insan bilgi güvenliğinin bir bileşeni olmak-

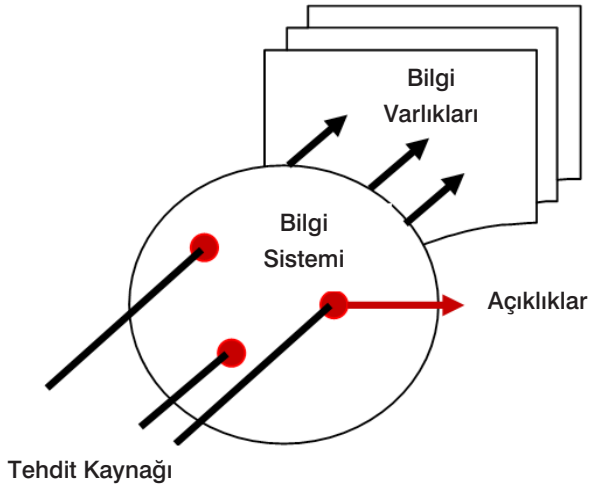
tan çıkmış güvenliğin ana unsuru ve tüm bileşenlerini etkiler hale gelmiştir. Saldırganların günümüzde teknolojik önlemleri aşmaya çalışmak yerine daha kolay ve maliyetsiz olduğu değerlendirilen sosyal mühendislik yöntemlerini sıklıkla kullanır hale gelmesi ve en önemli etken olan insan bileşenini zafiyete uğratması da bu tezi doğrulamaktadır.

Temelde insanın yer aldığı bir yapıda sosyo-politik faktörlerin üzerinde durulması kaçınılmazdır. Hambrick ve Chen'in yeni akademik alanlarda başarının yönlendiricileri konulu çalışmasında sosyo-politik faktörlerin (davranışsal düşünceler) yeni akademik alanların yükselişinde entelektüel gelişmeler (teknik düşünceler) kadar önemli olduğu vurgulanmıştır [11]. Günümüzde bilgi güvenliğinin teknolojik bir çözümden ziyade teknolojik bir problem olduğunun ispatlandığı çalışmaların da bulunması [12] farkındalık kavramının öneminin daha da arttığını açıkça göstermektedir. Özellikle kurumsal anlamda teknik alanlardan ziyade yönetimsel alanlara yoğunlaşılması ve çalışanların farkındalık seviyesinin arttırılması kurumsal güvenlik anlamında daha iyi sonuçlar vermektedir. Bu nedenle bilgi güvenliği problemine yönelik davranışsal düşüncelere yönelik katkıların en az teknolojik çözümlere yapılan katkılar kadar önemli olduğu değerlendirilmektedir.

Sosyal mühendislik kavramının zararlı yazılımlarla bütünleşik saldırılara ortam hazırlamasıyla beraber insan faktörü yönetilmesi gereken en önemli bileşen haline dönüşmüştür. Bilgi güvenliği farkındalığını kavramsal olarak açıklayabilmek için öncelikle bileşenlerinin anlaşılması gerekmektedir. NIST 800-16'ya [13] göre farkındalık bir eğitim değildir ve farkındalık sunumlarının amacı dikkatin güvenlik üzerine yoğunlaştırılmasıdır. Farkındalık sunumları kişilerin BT güvenlik tehditlerinin tanıması ve uygun şekilde davranmasını hedefler. Özetle kişilerin sadece tehditlerin farkında olmasını değil uygun davranışları sergilemesi gerektiğini belirtmektedir. Kişinin tehditler doğrultusunda uygun davranışları seçmesi ise bilgi güvenliği algısı ile mümkün olmaktadır [14]. Bu tanımlamalar doğrultusunda tehdit, algı, farkındalık ve davranış olarak 4 ana unsur bilgi güvenliği farkındalığının temel bileşenleri olup bu bileşenler aşağıda kısaca tanıtılmıştır.

4.2.1. Tehdit

Bilgi güvenliğinden bahsedebilmek için ilk olarak tehdidin kavramsal olarak anlaşılması gerekmektedir. Literatürde varlıklara açıklıkları kullanarak zarar verme potansiyeli [15], bir sistem ya da öznenin maruz kaldığı gizli tehlike ya da dış kaynaklı risk faktörleri [16], bir açıklığa karşı bir tehdit kaynağının başarılı işlem gerçekleştirme potansiyeli [17] gibi farklı tanımlamalar bulunmaktadır. Ortak noktalar değerlendirilerek bir tanımlama yapmak gerekirse; Şekil 4.4'te görüldüğü üzere bir sistemdeki açıklıkların kullanılarak bilgi varlıklarının bir kısmının sızdırılması ya da zarara uğratılması potansiyeli/ihtimali tehdit olarak tanımlanmaktadır. Tehdit kaynakları ise deprem, sel, toprak kayması gibi tehditleri içeren "doğal", uzun süreli elektrik kesintileri, yıldırım gibi tehditleri içeren "çevresel" ve yanlış veri girişi, zararlı yazılımların yüklenmesi gibi "insan kaynaklı" tehditler olarak 3 ana başlıkta toplanmaktadır [15].



Şekil 4.4. Tehdit tanımı

Kişisel, kurumsal ve ulusal bilgi güvenliği açısından değerlendirildiğinde saldırganlar ve kötü niyetli kullanıcılar dışında bilinçsiz ve dikkatsiz çalışanlar ya da kullanıcılar farkında olmadan birer tehdit kaynağı haline dönüşebilmektedir.

Tehdidin tanınması farkındalığa temel teşkil etmektedir. Siber güvenlik tehditleri farklı kaynaklara sahip olsa da çok büyük bir bölümünü siber saldırılar oluşturmaktadır. Bu nedenle siber güvenlik

tehditlerinin kavramsal olarak daha iyi anlaşılabilmesi için farkındalık bakış açısıyla siber saldırı yaşam döngüsüne de kısaca değinilecek ve örnek bir olay ile açıklanacaktır.

4.2.1.1. Siber Saldırı Yaşam Döngüsü

Günümüzde siber saldırılar sistemlerin sahip olduğu bilgi varlıklarının öneminin ve miktarının artmasıyla kabuk değiştirmiştir. Yabancı devletler, terörist gruplar, endüstriyel siber casuslar ve organize siber suçlular, siber eylemciler (hacktivist), bilgisayar korsanları (hackers) saldırılara kaynak teşkil etmektedir [18].

Saldırı ve tehditlerin artması ve çeşitlenmesine paralel olarak güvenlik önlemleri de artmakta, sistemlere erişim eskiye nazaran takım çalışması ve karmaşık bilgilerin çözülmesine yönelik işlemlerle gerçekleştirilmektedir. Sisteme erişimin zorlaşması saldırganların sistematik bir yöntem izlemesini de gerektirmektedir. Tehditleri anlamak ancak siber saldırılar gerçekleştirilirken kullanılan metotların ve adımların anlaşılması ile mümkün olabilir. Bu kapsamda 6 adımlı siber saldırı yaşam süreci [19] ortaya konulmuştur. Ancak iç içe geçen süreçler ve süreç sonucunda saldırganlar tarafından stratejik bir plan doğrultusunda elde edilen kazanç kavramının da siber saldırı yaşam döngüsü kapsamında değerlendirilmesi ile Şekil 4.5'de görülen yaşam döngüsü ortaya çıkmaktadır [20]. Verizon 2016 Veri Sızıntı Araştırma Raporu'nda [3] saldırıların %89'unun kazanç ve casusluk amaçlı gerçekleştirildiği tespit edilmiştir. Casusluğun da rekabette öne geçmek adına elde edilen bir kazanım olduğu değerlendirildiğinde kazanç adımının süreci dinamik hale getirerek saldırganların ve dolayısı ile saldırıların sürekli olarak kendini yenilemesini ve geliştirmesini sağlamaktadır.

Günümüzde Şekil 4.5'de belirtilen saldırı adımlarının gerçekleştirilebilmesine olanak sağlayan birçok araç bulunmaktadır. Dolayısıyla artık çok yüksek bilgi seviyesinde olmayan kişiler bile rahatlıkla hedef sistemlere saldırı gerçekleştirebilmektedir.

Siber saldırı yaşam sürecinin ilk iki adımını, çoğu zaman iç içe geçen bilgi toplama ve keşif oluşturmaktadır. Saldırganlar, sistemlere sızabilmek için sunucu tarama ve port tarama yöntemlerini kullanırlar. TCP Echo, UDP Echo, ICMP tarama ile bir ağda bulunan sunucuları belirlenirken; port tarama atakları ise, açık portların belirlenerek servisler üzerinden saldırı yapılmasına imkân tanır [21].



Şekil 4.5. Siber saldırı yaşam döngüsü

Açık kaynak kodlu araçlarla kolaylıkla port taraması yapılabilmektedir. NMAP birçok farklı port tarama tekniğini tek komutla yapmaya imkân tanımaktadır. Port tarama dışında sosyal mühendislik, whois sorguları, pasif saldırılar (ağa yerleşerek trafiğin izlenmesi, ağ topolojisinin çıkarılması vb.), ping okuma, google hacking, Shodan gibi arama motorları bilgi toplama ve keşif için etkin olarak kullanılmaktadır.

Zafiyetlerin taranması adımında ise sistemin açıklıklarının bulunmasına yönelik uygulamalar yapılmaktadır. Açıklık; istemeden/kazayla başlatılabilen ya da bilerek suistimal edilebilen zaaflar [17] ya da "bir varlığı tehditlere karşı korumasız hale getiren her türlü unsur (sistem bileşenlerinden, güvenlik politika ve prosedürlerinin yokluğundan, yetersizliğinden veya uygulanmayışından, eksik veya hatalı sistem tasarım ve uygulamalarından, organizasyon yapısı, yönetici ve çalışanların bilgi birikimi ve tutumundan kaynaklı nedenler)" olarak tanımlanmaktadır [22].

Açıklıkların tespitinden sonra saldırgan hedefin durumuna göre uygun stratejiyi belirler ve bu strateji doğrultusunda kullanacağı araçlara ve yöntemlere karar verir. Daha önceden tespit ettiği açıklıkları uygun araç ve yöntemlerle kullanarak sistemi ele geçirir ve istismar ederek istediği verileri elde eder. Bazen sistemin devre dışı

bırakılması da istismarın bir çeşidi olabilmektedir. Burada önemli olan saldırganın elde etmek istediği kazanç/faydadır.

Bir saldırının son adımı ise, sistemde yer alan saldırıya ilişkin izlerinin silinmesidir. Bir ağa ya da hedefe sızmayı başaran saldırgan, elde ettiği bilgiler ya da sisteme verdiği zararlar anlaşıldığında kendisine ulaşılmasını engellemek için sisteme bıraktığı izleri silmek isteyecektir.

Genel olarak bir saldırının yaşam döngüsünün anlaşılmasının tehdidin tanınması açısından önemli olduğu değerlendirilmektedir. Tehdidin tanınması kişilerin bir saldırı gerçekleşirken tespit edebilmesi ve farkındalığa ilişkin eylemlerinde daha bilinçli bir tutum sergilemesini sağlayacaktır.

4.2.1.2. Siber Saldırı Yaşam Döngüsü Örnek Olay Değerlendirmesi

Siber saldırı yaşam döngüsü doğrultusunda 2015 yılında da dünya da ve ülkemizde gündemdeki yerini koruyan fidye yazılımları içerisinde yer alan "cryptolocker" örnek olay olarak değerlendirilecektir. Genel işleyiş olarak ülkemizde hizmet veren bir telekom operatöründen gönderildiği izlenimi verilen bir e-posta aracılığı ile kullanıcılara ulaştırılmaktadır. Kullanıcılar da bu e-postayı açarak zararlı yazılımı çalıştırmakta ve kullanıdğı bilgisayarda bulunan tüm dosyalar şifrelenmektedir. Kullanıcının dosyalarına erişebilmek için dünyanın yeni para birimleri arasında yer edinen Bitcoin ile ödeme yapması gerekmektedir.

Cryptolocker'ın en son dalgada dünya çapında 40.000 sistemi etkisi altına aldığı ve 280 milyondan fazla belgeyi şifrelediği tespit edilmiştir. Yayılma ağırlıklı olarak Avrupa ülkelerinde görülmekle birlikte Kanada, Avustralya ve Yeni Zelanda'yı da yoğun olarak etkilemiştir. ESET Kanada Araştırma Ekibi bu fidye yazılımının arkasındaki siber suçluların bu dalgada 600 bin dolar değerinde Bitcoin elde ettiklerini tahmin etmektedir [23].

ESET Kanada Araştırma Ekibi'nden M. M. Léveillé öncülüğünde yapılan bir çalışmada, dünyada Cryptolocker'ın son dalgasından etkilenen 40.000 sistemden 11.700 adedinin Türkiye'de olduğu belirtilmiştir. Türkiye'yi 9.400'ün üzerinde sistem ile Avustralya, 4.600'e yakın sistemle de İtalya'nın takip ettiği belirtilmektedir.

Türkiye'de 100 milyonu aşkın şifrelenmiş dosya olduğu tahmin edilmektedir. Siber suçluların, şifrelenmiş dosyaları açmak için 1000 ile 1500 Avro arasında değişen fidye ödemeleri talep ettiği bu raporda belirtilmiştir [23].



Şekil 4.6. Cryptolocker virüsü için kullanılan bir e-posta örneği [24]

Tüm dünyada çok büyük başarı elde eden Cyrptolocker virüsünü Türkiye açısından siber saldırı yaşam döngüsü (Bkz. Şekil 4.5) doğrultusunda ele aldığımız takdirde saldırganlar tarafından gerçekleştirilen ilk adımın "hedef tespiti" olduğu görülmektedir. Cryptolocker virüsünü geliştirenler hedef olarak Türkiye'de yaygın olarak kullanılan telekomünikasyon abonelerini belirlemiştir. Türk Telekom, Turkcell ve TTNET'in Türkiye'de sahip olduğu müşteri sayıları göz önüne alındığında hedefin çok sayıda ve bilgi güvenliği konusunda hata yapma ihtimali yüksek olan standart kullanıcılara ulaşabilmek olduğu görülmektedir. Benzer şekilde kurumsal e-posta hesapları üzerinden de kurumların sunucu ve çalışan bilgisayarlarında yer alan kurumsal bilgi varlıkları hedef alınmıştır.

Hedef tespitini takiben virüsün geliştiricileri tarafından bilgi toplama işlemleri yapıldığı değerlendirilmektedir. Bilgi toplama adımında bahse konu kurumlar tarafından kullanıcılara atılan Şekil 4.6'da örneği sunulan e-posta formatları ve görünümlerinin belirlendiği, kullanıcılara ortalama gelen fatura meblağlarının tespit edilerek e-postalarda insanlarda şaşkınlık ve merak uyandıracak yüksek meblağların kullanıldığı değerlendirilmektedir.

Sistemin istismar edilmesine yönelik adımda oluşturulan e-posta içerisine eklenen zararlı yazılım kullanılmıştır. Kullanıcıların hazırlanan zararlı yazılımı fark edememesi amacıyla oluşturulan .exe dosyasına PDF dosyası ikonu yerleştirilmiştir. Dolayısıyla faturayı görüntülemek için dosyaya tıklayan kullanıcılar PDF dosyası yerine zararlı yazılımı bilgisayarlarına indirerek çalıştırmaktadır. Bu sayede zararlı yazılım aktif duruma geçerek bilgisayardaki tüm dokümanları şifrelemektedir.

Bahse konu siber saldırıda izlerin temizlenmesi adımına ihtiyaç duyulmamaktadır. Ancak ödemeleri Bitcoin sistemi üzerinden alarak saldırıyı gerçekleştirenlerin kendilerini güvende tutmayı amaçladıkları değerlendirilmektedir.

Siber saldırı yaşam döngüsünün son adımı olan kazancın elde edilebilmesi için şifrelenerek kullanılamaz hale getirilen dosyaların açılabilmesine imkân sağlayan anahtar karşılığında kullanıcıdan veya kurumdan (kurumsal saldırılarda verinin önemi ve boyutu da değerlendirilerek) ciddi miktarda para talep edilmektedir. Bu saldırıda ticari bir kazanç hedeflendiği görülmektedir.

Örnekte de görüldüğü gibi siber saldırganlar çok sistematik ve tüm detayları değerlendirerek saldırılar gerçekleştirmektedir. Bu nedenle siber saldırıların sistematiğinin, karakteristik yapısının ve hedeflerinin çok iyi öğrenilmesi tehditlerin tespiti ve önlenmesi için çok büyük öneme sahiptir.

4.2.2. Algı

Bilgi güvenliği kavramının içselleştirilerek davranışa dönüştürülmesinde bir diğer önemli bileşen algıdır. İnsan beyni, algıladığı ölçüde düşünür, düşündüğü ölçüde uygular [25]. Algı, insan beyninin ana bölümlerinden biri ve insan davranışlarını anlamak için anahtar bileşen olarak değerlendirilmektedir [26]. Bilgi güvenliği algısı ise kişinin bilgi güvenliğine yönelik tehditleri değerlendirerek davranışlarına karar vermesi olarak tanımlanmaktadır [14]. Kişilerin bilgi güvenliği algısını modelleyebilmek için; bilgi, etki, şiddet, kontrol edilebilirlik, farkındalık ve mümkünlük olarak 6 faktörlü bir yapı önerilmiştir [14]. Dolayısı ile algı ve farkındalık kavramları arasında sıkı bir ilişki bulunmaktadır.

Algı yönetiminin çok daha fazla içeriğin daha fazla fayda ve daha az belirsizlik ile dış dünyadan edinilmesi ve kontrolünün geliştirilmesini işaret eden durumlar için uygun bir konsept olduğu belirtilmiştir [27]. Bilgi güvenliğine ilişkin ortaya çıkan tehditlerin çeşitliliği, bilgi varlıklarının büyüklüğü gibi hususlar göz önüne alındığında algı yönetiminin bu alanda büyük katkı sağlayacağı görülmektedir. Etkin bir bilgi güvenliği farkındalık sürecinden bahsedebilmek için tehditlere uygun davranışların tespit edilebilmesi çok önemlidir. Bu da ancak bilgi güvenliği algısı ile gerçekleştirilebilmektedir.

4.2.3. Farkındalık

Bilgi güvenliği farkındalığı, bilgi güvenliğini riske atan faktörler ve söz konusu faktörlere karşı ne tür önlemler alınabileceğini kapsayan güvenlik politikalarından haberdar olunması şeklinde tanımlanmıştır [28]. Bir başka deyişle kişisel, kurumsal ya da ulusal bilgi güvenliğinin sağlanabilmesi için bilgi güvenliğine yönelik tehditlerin ve sonucunda oluşabilecek durumların kavranmasıdır. Kurumsal anlamda ise organizasyonlar tarafından kullanıcıların uyması gereken güvenlik görevlerini belirten tanımlar olarak karşımıza çıkmaktadır (genellikle güvenlik kılavuzları, yönergeler gibi dokümanlarda açıklanır) [29]. Bilgi Güvenliği Forumu (ISF) ise bilgi güvenliği farkındalığını tüm çalışanların bilgi güvenliğinin önemini, kuruluşa uygun bilgi güvenliği seviyelerini ve kişisel bilgi güvenliği sorumluluklarını anlama ve bu doğrultuda hareket etme dereceleri olarak tanımlamaktadır [30]. Literatürde yer alan tanımlar genel olarak değerlendirildiğinde, farkındalık özetle, kişinin tespit ettiği tehdit ve belirlediği karşı davranışların bileşkesi olarak tanımlanabilir. Kişi eğer kurumsal bir görevde ise tespit edilen tehdit kurum varlıkları ve yönetilen sistemleri, kişisel seviyede ise kişisel bilgi varlıklarının ve kullandığı cihazların maruz kalabileceği saldırıları kapsamaktadır.

Bilgi güvenliği farkındalığı tehditlerinin algılanmasını takiben uygulanabilecek davranışların ve bu davranışların doğurabileceği sonuçların bir başka deyişle risklerin değerlendirilmesini kapsar. Bu değerlendirmeler, bilgi ya da deneyimlerle elde edilmiş birikimler doğrultusunda gerçekleştirilmektedir. Kişinin farkındalığı ne kadar yüksek ise karşılaştığı tehditlere ilişkin vereceği kararlar sonucun-

da kişisel, kurumsal ya da ulusal seviyede karşılaşılabilecek bilgi kayıpları azalacaktır.

4.2.4. Davranış

Bilgi güvenliği farkındalığının temel amacı, kullanıcıların bilgi teknolojilerinin kullanımı ile ilgili risklerin farkında olması ve bu riskleri gidermek için gerekli politika ve prosedürleri bilerek uygulamasıdır [31]. Bu farkındalık sayesinde kullanıcılar karşısına çıkan kötücül uygulamalara, bağlantılara ve yazılımlara karşı davranışlarında bilinçli bir tutum sergileyerek saldırganların bilgi sızıntısı yapmasına ya da kullanıcının kendini zorda bırakabileceği, veri, itibar kaybedebileceği durumlara karşı kendini koruyabilir. Bir başka deyişle bireylerin bilgi güvenliğinin ne olduğunu ve neden önemli olduğunu bilmeleri teknolojik tüm önlemlere rağmen insanın bilgi güvenliğinin en uç noktasında bulunduğunun kavranması açısından önemlidir.

Bilgi güvenliği politika ve prosedürlerinin uygulanması ise ancak kullanıcıların bu konuda göstereceği istek ile mümkün olmaktadır. Bu isteğin kullanıcılarda oluşturulmasına yönelik Fishbein ve Azjen çalışmalarında ikna edici iletişimin insan tutum, eğilim ve davranışlarını değiştirmede çok önemli olduğunu belirtmişlerdir [32]. Bilgi teknolojileri güvenliği ve farkındalık eğitimlerinde kullanılan materyallerde bu mesajların verilmesinin önemli olduğunu ortaya koymuşlardır [32].

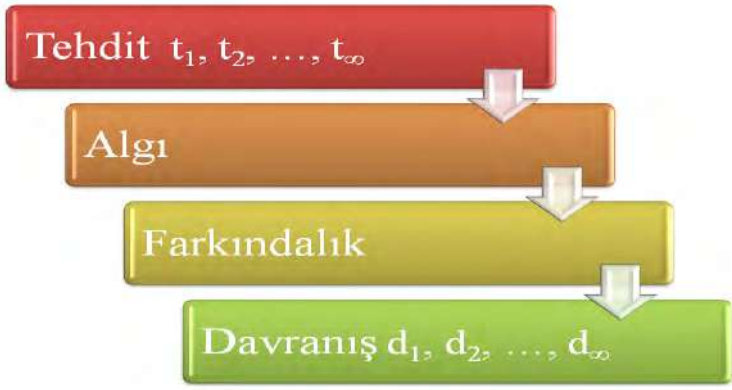
4.3. Farkındalık ve Davranış İlişkisi

Günümüzde kişisel, kurumsal ve ulusal olarak maddi, manevi kayıplara sebep olan bilgi güvenliği sızıntılarına çok büyük oranda farkındalık eksikliğinin sebep olduğu insan hataları temel teşkil etmektedir. Swain ve Guttman bu hataları; ihmal, yetki (işlemleri uygulamada gerçekleştirilen hatalar), sıralama ve zamanlama hataları olarak 4 gruba ayırmıştır [33]. Bu hatalara ilişkin genel gözlem ise insanların sıklıkla davranışsal amaçlarına uygun olarak hareket etmedikleridir [34]. Emniyet kemeri takma, sağlıklı beslenme gibi korumacı davranışlar söz konusu olduğunda insanlar güvenli olanı uygulamaya eğilimlidir, ancak sadece bazıları bu şekilde davranır. Bu da kullanıcı eğilimleri ile davranışları arasında bağlantının düşük olduğunu ortaya koymaktadır [35].

Benzer olarak Dijle'nin Türkiye'de eğitimli insanların bilişim suçlarına yaklaşımına ilişkin yaptığı bir çalışmada [36], yazılımlar aracılığıyla verilerinin çalındığını düşünen kullanıcı sayısı %51,7 iken, açıklıklara ilişkin firmalar tarafından yapılan güncellemelerin kullanılamadığı ve savunmasız bir ortamı meydana getiren lisanssız yazılım kullanım oranı %75 olarak ortaya konulmuştur [36]. Farkındalık seviyesi ile davranışın ayrı yönlerde hareket edebildiği göz önüne alındığında farkındalık üzerine yapılan eğitim ve çalışmalarda davranış değişikliği hedeflenmelidir. Davranış değişikliği ise ancak tekrarlayan ve dinamik bir döngü ile güvenlik kültürü olarak kullanıcılar tarafından içselleştirilebilir.

Kişisel, kurumsal ve ulusal düzeyde siber saldırılara karşı sistemin en zayıf halkası olan insanın eğitilerek ve yetenekleri geliştirilerek hata payının en aza indirgenmesi için bazı tedbirler alınabilir. Bu tedbirlerin alınmasında amaç insan unsurunun [37];

- Bilgisini (insanlar ne biliyor),
- Tavırlarını (insanlar ne düşünüyor),
- Davranışlarını (insanlar ne yapıyor) değiştirebilmek ve geliştirebilmek olmalıdır.



Şekil 4.7. Tehdidin davranışa dönüşmesi

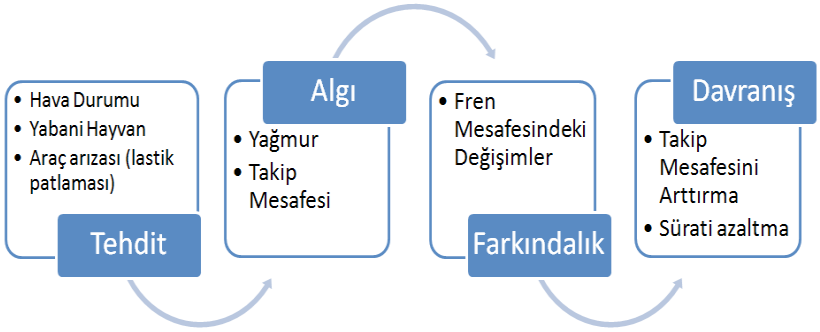
Bilgi güvenliğinde davranışsal sonuçlara ulaşılabilmesi için ise Şekil 4.7'de gösterilen basamaklı bir yapının kişilerin zihninde oluşturul-

ması gerekmektedir. Söz konusu basamaklı yapıda siber ortamda yer alan tehditler t ile sembolize edilmiş olup her geçen gün farklılaşan ve sayı olarak artan siber saldırıları kapsadığından sonsuz sayıda bulunmaktadır. Tehditlere karşı üretilecek davranışlar ise d ile sembolize edilmiş olup bir tehdide karşı uygulanabilecek davranışlar içinde bulunulan durum, algı ve farkındalık gibi parametrelere göre değişkenlik göstereceğinden sonsuz sayıdadır.

Öncelikle kişinin korumakla sorumlu olduğu bilgi varlıkları ve sistemleri belirleyerek maruz kalabileceği değerlendirilen tehdit kaynaklarınca oluşturulabilecek tehditlerin belirlenmesi gerekmektedir. Tehdidin algılanması ise ikinci adımı oluşturmaktadır. Bilgi varlıklarına yönelik saldırı evreninde yer alan tehditlerden kendi varlıklarına yönelik olanları seçebilmesi gerekmektedir. Bu şekilde tehdidin algılanması sonrasında kişi sahip olduğu farkındalık derecesine göre tehdidin ortaya çıkarabileceği riskleri ve sonuçlarını ve bu riskin giderilmesine yönelik gerçekleştirmesi gereken davranışa karar verir. Son olarak bu davranışın gerçekleştirilmesi ile süreç tamamlanır. Kişisel, kurumsal ve ulusal düzeyde bilgi güvenliğinden bahsedebilmek için tüm bireylerin algıladığı tehditlere uygun davranışlarla cevap vermesi gerekmektedir. Uygun davranış gerçekleştirilmediği takdirde kişinin tehditleri tespit etmesi, riskleri ve bu riskleri gidermek için yapması gerekenleri bilmesinin hiçbir anlamı olmayacak, saldırı gerçekleşecektir. Şekil 4.8'den görülebileceği üzere trafikteki tehditleri düşündüğümüzde diğer araçlar, hava durumu, yabani hayvanlar, aracımızda meydana gelebilecek arızalar gibi birçok tehdit belirleyebiliriz. Aracın kullanıldığı gün havanın yağışlı olması, öndeki araç ile olan takip mesafesinin olması gerekenden kısa olduğunun algılanması sonrasında kişi farkındalık sahibi ise algıladığı tehditlere yönelik yapması gerekenlere karar verebilir. Örnek olarak yağışlı havanın takip mesafesinde meydana getireceği değişimlerin farkında olan bir kullanıcı takip mesafesini arttırma, sürati azaltma, şerit değiştirme gibi aynı tehdidi ortadan kaldırabilecek birçok farklı davranıştan birini seçerek uyguladığı takdirde oluşabilecek kazaların önüne geçecektir. Burada kişinin bilgisi, algısı ve farkındalığı ne kadar yüksek olursa olsun davranışa çevirmediği takdirde sonuç olumsuz olacaktır.

Benzer şekilde bilgisayarına virüs bulaşması durumunda veri kaybı yaşayabileceğini, virüslerden nasıl korunabileceğini bilen bir kişi

gerekli önlemleri uygulamadığı takdirde veri kaybını yaşayacaktır. Dolayısıyla etkin bir bilgi güvenliğinden bahsedebilmek için Şekil 4.8'deki adımlarda olduğu gibi sürecin davranış ile son bulması gerekmektedir.



Şekil 4.8. Tehdidin davranışa dönüşmesine örnek gösterim

Genel kabul olarak benzer tehditler için benzer davranışlar sergilenmesi gerekirken her bir tehdit için kişinin çalışma ortamı, kurumun öncelikleri, hedef sistemin değeri gibi durumlar göz önüne alındığında tamamen farklı davranışların da çıktı olması mümkündür. Trafikte araç takip mesafesini düşündüğümüzde aracın özellikleri, hava durumu gibi koşullar doğrultusunda takip mesafesinin arttırılması gerektiği durumlar ortaya çıkabilir. Bunun yanı sıra kişisel tecrübe, bilgi seviyesi ve diğer birçok faktör tehditlerin algılanmasında farklılıklar yaratabilecektir. Çoğu zaman bir siber saldırının birçok farklı önleme yöntemi bulunmaktadır. Bu nedenle kişiler farklı tehditler için kendi farkındalık ve algı seviyelerine göre farklı davranışlar geliştirmelidir. Bunun için de tehdidi doğru algılamak, farkında olmak en önemli noktadır. Farkındalığın sadece bir seviyede ve şekilde olmayacağı açıktır. Örneğin, bir profesör ile bir öğrencinin, ya da bir güvenlik uzmanı ile son kullanıcının benzer tehditler karşısında göstereceği davranışlar tamamen farklı olmalıdır. Burada önemli olan çalışanların ve bireylerin kendi seviye ve sorumluluk sahaları kapsamında uygun davranışları seçebilmesi ve bu davranışları gerçekleştirebilmesidir. Aksi takdirde farkındalık uygun davranışlara dönüşmezse bilgi güvenliği ihlalleri mutlaka ortaya çıkacak, bilgi varlıklarında kayıplara sebep olacaktır.

Henüz literatürde çok net bir tanıma sahip olmasa da bilgi güvenliği kültürü kurumun güvenliği üzerinde potansiyel etkiye sahip

olan ve bu etkiyle bağlantılı olabilecek şekilde kurum çalışanları tarafından ortaya konulan varsayımlar, değerler, tutum ve inançlar ve gerçekleştirdikleri davranışlar olarak tanımlanmaktadır [38]. Şekil 4.9'da görülen davranışsal süreç doğrultusunda farklı kullanıcıların farklı tehditlere karşı ortaya koyduğu davranışların benzer sonuçlara ulaşması durumunda o kurum ya da grupta bir güvenlik kültüründen söz edilebilir. Özetle kişinin davranışı kişisel güvenlik kültürünü, kullanıcıların davranışlarının bileşkesi ise kurumun güvenlik kültürünü oluşturmaktadır.

4.4. Farkındalık Ölçüm Yöntem ve Modelleri

Önceki başlıklarda farkındalığın önemi, bileşenleri ve davranış ile olan ilişkisi ortaya konulmuştur. Farkındalığının siber güvenliğin etkin bir unsuru olarak davranışa dönüşebilmesi için farkındalığın yönetilmesi gerekmektedir. Etkin bir farkındalık yönetiminden bahsedebilmek ancak, farkındalık seviyesinin periyodik ölçümlerle tespit edilmesi, elde edilen sonuçların analiz edilerek tespit edilen eksikliklerin giderilmesine yönelik farklı yöntemlerden faydalanılarak Şekil 4.9 doğrultusunda gelişim sağlanması ile mümkündür.



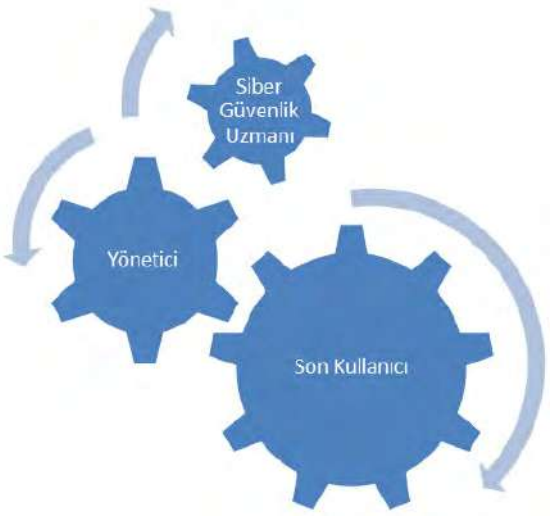
Şekil 4.9. Farkındalık gelişim döngüsü

Farkındalığın ölçülmesi ve kavramsal olarak modellenmesi ile bilgi güvenliği farkındalık seviyesinin dolayısıyla da güvenlik seviyesinin etkin bir şekilde arttırılabileceği değerlendirilmektedir. Bu kapsamda, farkındalık seviyesinin ölçülmesi ve arttırılmasına yönelik

literatürde yer alan yöntem, model ve değerlendirmeler alt başlıklar halinde sunulacaktır.

4.4.1. Farkındalık Yeterlilik Seviyesi Ölçüm Yöntemleri

Bilgi sistemleri ve teknolojideki gelişmeler kullanıcı profilinde de köklü değişikliklere sebep olmuştur. İlk yıllarda bilgisayar kullanıcılarının neredeyse tamamı uzmanlardan oluşmaktayken günümüzde toplam kullanıcı içindeki uzman oranı çok düşük kalmaktadır. Tüm kullanıcıların artık cihazları rahatlıkla edinip kullanabilmesi bilgi güvenliği probleminin de çözümü için dikkatin yoğunlaştırılması gereken kümenin genişletilmesini gerektirmektedir. Kişisel, kurumsal ve ulusal anlamda değerlendirilerek genel bir kullanıcı sınıflandırması yapılırsa son kullanıcı, siber güvenlik uzmanı ve yönetici olarak 3 temel gruptan bahsedilebilir. Sayısal anlamda en büyük kümeyi son kullanıcılar oluşturmakta olup siber güvenlik uzmanına doğru kullanıcı sayısı azalmaktadır. Şekil 4.10'da görüldüğü gibi bilgi güvenliğini bir sistem ve kullanıcı gruplarını da bu sistem içerisindeki çarklar olarak düşünürsek sistemin sağlıklı çalışması için bu 3 grubun da bilgi güvenliğine ilişkin gereklilikleri tam olarak yerine getirmesi gerekmektedir. Herhangi birinde ortaya çıkabilecek bir aksaklık bilgi varlıklarının zarara uğramasına sebep olacaktır.



Şekil 4.10. Bilgi güvenliği kullanıcı grupları

Tüm kullanıcı gruplarını kapsayacak etkin bir bilgi güvenliğinden bahsedebilmek ve kullanıcıların dijital ortamda güvenle hareket edebilmesinin en temel ve öncelikli unsuru farkındalık seviyesinin ölçülmesi ve arttırılması olduğu değerlendirilmektedir. "**Ölçemediğinizi yönetemezsiniz!**" anlayışı siber güvenlik farkındalığı açısından da doğru bir tespit olarak karşımıza çıkmaktadır. Günümüzün en önemli problemlerinden biri haline gelen farkındalığın yönetilebilmesi için öncelikle kişiler ve kurumlar kendi seviyelerini ölçüp tespitlerini ortaya koymalı ve bu doğrultuda kendine bir yol haritası belirlemelidir.

Farkındalık kavramı kişinin ne bildiği, ne tecrübe ettiği, ne uyguladığı gibi farklı tür konuları kapsadığı için ölçümü oldukça zordur. Bu nedenle de farkındalık seviyelerinin ölçülmesi gri alan olarak günümüzde konumunu korumaktadır. Saldırganların yoğunlukla hedeflerine insanlar üzerinden ulaşan bir yöntemi benimsemesi günümüzde farkındalık kavramının önemini arttırmış ve farkındalık yeteneklerinin ölçülerek yetenek seviyelerinin arttırılması neredeyse bir zorunluluk haline gelmiştir.

Bilgi güvenliği farkındalığının ölçülmesinde kullanılan yöntemler genel olarak [39,40];

- **Uzman Geri Beslemeleri**

Kullanıcıların güvenlik bakış açılarının nasıl değiştiği ya da bilgi güvenliği ile alakalı davranışlarına ilişkin durumların doğrudan geri besleme olarak bildirildiği ölçüm yöntemidir. Güvenlik olaylarına ilişkin tartışmaları da içerebilir.

- **Kişisel Değerlendirme**

Kişilerin kendi kendini güvenliği anlama ve gelecek planları ile ilgili değerlendirmelerdir.

- **Bilgi Testleri**

Anket vb. yazılı ya da elektronik ortamda bilgi güvenliği soruları ve verilen cevapların değerlendirilmesidir.

- **Seçici Görüşme**

Genellikle on ya da daha az kişiden oluşan önceden belirlenmiş kriterlere göre seçilmiş homojen bir grup ile belirli bir konu üzerinde geri besleme almak için yapılır.

- **Güvenlik Programı Kıyaslaması**

Benzer durumda olan kurumların genel ortalaması ile bahse konu kurumun durumunun uzmanlar tarafından kıyaslanmasıdır.

- **Kullanıcı Gözlemleri**

Ağ trafiğinin incelenmesi, çalışma ofislerinin ziyareti, parola veri tabanının analiz edilmesi vb. konularda 6 başlık altında gruplandırılmıştır.

4.4.2. Farkındalık Yeterlilik Seviyesi Ölçüm Modelleri

Kişisel anlamda farkındalık yetenek seviyesinin ülke genelinde ölçümlenerek mevcut durumunun ortaya konulması, sonrasında da bu seviyeler doğrultusunda uygun programlar ve modeller ile geliştirilmesinin kişisel, kurumsal ve ulusal bilgi güvenliğe en az teknolojik gelişmeler kadar katkı sağlayacağı değerlendirilmektedir.

Farkındalığın ölçülmesine yönelik olarak, tüketicilerin de bilgi güvenliği farkındalık programlarında göz önüne alınması gerektiği ortaya konulan çalışmada [41], telekomünikasyon alanında özellikle akıllı telefon kullanıcıları temel alınarak "güvenlik politikalarına uyumluluk, kişisel verilerin korunması, sahte/istenmeyen mesajlar, mobil uygulamalar, güvenlik olay bildirimi" olmak üzere 5 odak konuya (focus area) ilişkin bilgi ve davranışları üzerinden bilgi güvenliği farkındalıkları ölçülmeye çalışılmıştır. Bilgi davranış boyutları arasında davranışsal anlamda tutarsızlıklar olduğu ortaya konulmuştur.

NIST 800-16 Bilgi Teknolojileri Güvenlik Eğitim Gereksinimleri [13] dokümanında performans ve rol tabanlı bilgi güvenliği farkındalık eğitimlerinin etkinliğinin ölçülmesine yönelik dört seviyeli bir değerlendirme oluşturulmuştur. Karmaşıklık sırasına göre;

- Öğrencilerin memnuniyetini kapsayan **Kurs Sonu Değerlendirmesi** (1. seviye),
- Öğrenilenlerin etkinliğini kapsayan **Davranış Hedef Testleri** (2. seviye),
- Performans etkinliğini kapsayan **İş Aktarma Yetenekleri** (3. seviye) ve
- Kurumsal faydaları kapsayan **Eğitim Program Etkinliği** (4. seviye) seviyeleri bulunmaktadır.

Kullanıcıların farkındalık seviyelerinin dünya genelinde ölçülmesi amacıyla, güvenlik kılavuzları ve daha önce yapılan çalışmalardan toplanan; bilgisayar kullanıcılarının potansiyel riskli davranışlarının içeren 20 soru, kullanıcılarının farkındalık seviyelerini ölçen 6 soru, kullanıcıların ön yargılarını ölçen 5 soru ve parola kalitesi ve parolaların güvenliğine yönelik 6 soruyu içeren toplam 4 bölüm 37 adet anket sorusundan oluşan Kullanıcı Bilgi Güvenliği Farkındalık Anketinin (UISAQ-Users' Information Security Awareness Questionniare) hazırlanmasına yönelik bir çalışma yapılmıştır [42].

Uluslararası madencilik hizmeti veren bir firmanın bilgi güvenliği farkındalık seviyesinin ölçülebilmesi amacıyla bir prototip model geliştirilmiştir [31]. Bu model; tutum, bilgi ve davranış boyutlarından ve bu boyutlar altında yer alan (her zaman şirketin politikalarına uyar, parola ve kişisel tanıtıcı numaralarını gizli tutar, internet ve e-postaları güvenli kullanır, mobil ekipmanları kullanırken dikkatli olur, virüs gibi olayları bildirir ve tüm işlemlerin sonuçları olabileceğinin farkındadır olarak belirlenmiş) 6 odak konu ve bu konular altında belirlenmiş alt konulardan oluşmaktadır. Belirtilen boyutlar ve odak konulardaki seviyeleri ölçmek için yapılan çalışmalar ile bölgesel ve dünya genelindeki farkındalık seviyesinin ölçülebilmesi amaçlanmıştır.

İnternet kullanımında kullanıcıların karşılaştığı risk ve sonuç farkındalığına yönelik araştırma yapılarak elde edilen bulguların mevcut güvenlik ölçütlerinin eksikliklerinin giderilmesine nasıl etkileri olacağı analiz edilmiş ve bu durumun nasıl azaltılabileceğine yönelik tavsiyelerde bulunulmuştur [43]. Senaryo tabanlı değerlendirmeler sonucunda kullanıcılar tarafından algılanan risklerin genel olarak çok çeşitli olduğu ve bu risklerin çoğu zaman teknolojik önlemlerle ortadan kaldırılmasının mümkün olmadığı ortaya konulmuştur.

Bilgi güvenliği farkındalık programının etkinliğinin ölçülmesine yönelik olarak yapılan çalışmada [44] "İzlenen ve ölçülen şeyler yapılır" cümlesi ana düşünce olarak ortaya konulmuştur. Yıllık olarak parolalar, virüsler, kişisel bilgisayar güvenliği, bilgi güvenliği standartları, veri sınıflandırması ve uzaktan erişim, sosyal mühendislik, sosyal medya gibi konuları kapsayan diğer olarak belirlenen başlıkları kapsayan soruları kapsayan anketler oluşturulmakta ve bu anketler şirketin CEO'su dâhil tüm seviye kullanıcılara uygulanmaktadır. Yıllara göre elde edilen sonuçlar doğrultusunda geli-

şimin izlenebileceği ve yapılan ölçümler doğrultusunda farkındalık programının etkinliğinin belirlenebileceği değerlendirilmektedir.

Çalışanların bilgi güvenliği farkındalığını İnsan Yönüyle Bilgi Güvenliği Anketi (HAIS-Q) [45] ile belirlemek üzerine yapılan çalışmada McGuire'nin çalışması temel alınmıştır. Politika ve prosedür bilgisine yoğunlaşılan çalışmada politika ve kılavuzlar, üst yönetim ile yapılan röportajlar ve odak alanları üzerine yapılan araştırmalar doğrultusunda üzerinde çalışılacak odak alanları belirlenmiştir. İnternet kullanımı, e-posta kullanımı, sosyal ağ kullanımı, parola yönetimi, olay raporlama, bilgi işleme ve mobil hesaplamadan oluşmak üzere 7 odak alanı ve insan hatalarını temel alacak şekilde bu alanlarla ilişkili alt odak alanları belirlenmiştir. Her odak alanı için İyi Davranışlar, Nötr Davranışlar ve Kötü Davranışlar belirlenmiştir. Çalışma sonucunda çalışanların politika ve prosedür bilgilerinin arttırılmasının davranışlarını olumlu etkilediği, model ve anket sorularının doğruluğu ortaya konulmuştur.

Bilgi sistem kullanıcılarının bilgi güvenliği riske sokabilecek davranışlarını belirlemek amacıyla yapılan çalışmada [46], kullanıcılar tarafından kullanılan önleyici uygulamalar, maruz kalabilecekleri tehditler ve riski hangi genişlikte algıladıkları konuları da araştırılmıştır. Öğrenci, akademisyen ve üniversitelerin yönetim kademesinde bulunan kişilere yapılan anketlerin değerlendirilmesi ile bilgi güvenliği farkındalığı ve güvenlik davranışının değerlendirilmesinde kullanılabileceği değerlendirilen;

- Riskli Davranış Ölçeği,
- Korumacı Davranış Ölçeği,
- Saldırıya Maruz Kalma Ölçeği ve
- Risk Algı Ölçeği

olmak üzere 4 ölçek ortaya konulmuştur.

Literatürde yer alan çalışmalar genel olarak değerlendirildiğinde;

1. Anket ve odak alanı temelli yaklaşımların kullanıldığı,
2. Skor tabanlı seviyelendirme yapıldığı (Üretilen puan yüksek olabilir ancak kör noktaların ve eksiklik bulunan yeteneklerin tespitinde zorluklar yaratmaktadır),

3. Soru tabanlı yaklaşım kullanıldığı (Sorular hazırlayan kişinin yetenek ve bilgisine bağlı, tüm yetenekler karşılanmayabilir),
4. Belirli seviyelere yönelik hazırlanmış olduğu (Kişisel, Kurumsal, Ulusal),
5. Ölçüm modellerinde standardizasyon olmadığı,
6. Seviyelendirme standardizasyonu olmadığı (Benzer seviyede bulunan kişi, kurum ya da ulusların birbirleri ile kıyaslama yapmasına imkân bulunmamaktadır) görülmektedir.

4.4.3. Farkındalık Modelleri

Kavramsal modeller gerçek dünyada karşılaşılan olay ve durumların basit ve sadeleştirilmiş, bilimsel bilgilerle tutarlı, kesin ve tamamlanmış gösterimleridir. Kavramsal model bir başka deyişle gerçek nesne, durum ya da olayların basitleştirilmiş gösterimleridir [47]. Genellikle kavramsal model araştırmacılar, öğretmenler, mühendisler gibi gruplar tarafından anlamayı kolaylaştırma veya dünyadaki sistemleri ya da olayların durumlarını öğretmeyi amaçlar. Kavramsal modelleme çalışmalarının çıktısı genelde rasyonel ya da diğer mantıksal modellere dönüştürülebilen diyagramlardır [48]. Kavramsal modelin doğruluk ve yeterliliği insanların ortak anlayışını ne kadar iyi arttırabildiğine bağlıdır [49]. Kavramsal modellerin oluşturulması ve kişiler tarafından kavranabilmesi için bilgi birikimi belirleyici faktördür. Picasso'nun Guernica adlı eserini ilk kez gören kişiler tablo üzerinde bıçaklar, gözler, kafalar görecektir ancak tablo herhangi bir anlam ifade etmeyecektir. Ancak tablonun İspanya Sivil Savaşı'nı anlattığını bilen kişiler için bu imgeler çok daha anlamlı gelecektir [47]. Benzer şekilde kavramsal modellerin ortaya konulması ve anlaşılması için modeli oluşturan adımlara, nesnelere ilişkin bilgi sahibi olunması gerekmektedir.

Bilgi güvenliği farkındalığının kavramsal olarak modellenmesine yönelik literatürde teknolojik önlemlere kıyasla çok daha az sayıda çalışma bulunmaktadır. Bu çalışmalar incelendiğinde Kritzinger ve Smith [50] kurum çalışanlarının bilgi güvenliği seviyelerini geliştirebilmek amacıyla çok boyutlu ISRA (Information Security Retrieval and Awareness) modelini ortaya koymuştur. ISRA modeli teknik olmayan bilgi güvenliği konuları, BT yetki seviyeleri ve bilgi güvenliği dokümanları olarak 3 boyuttan oluşmaktadır. Model özellikle

öne sürülen bilgi gövdesini şekillendiren teknolojik olmayan güvenlik üzerine odaklanmaktadır. Çünkü bu konular teknolojik bilgi güvenliği konularına kıyasla hep ihmal edilmektedir. Model en iyi uygulamalar ve üretilmiş bilgi güvenliği dokümanlarını da bütünleştiren bir yaklaşım sergilemektedir.

Kritzinger ve Solms [51] özellikle ev kullanıcılarının farkındalığını arttırmayı amaçlamış, ev kullanıcılarının internete çıkmadan önce bilgi birikimlerini arttırmaya zorlayan E-Farkındalık Modelini (E-FM) önermiştir. Model kullanıcıların güvenlik olayları, tehditler ve bu tehditlerden nasıl sakınılabileceğini daha iyi anlayarak güvende kalmalarını amaçlamaktadır. E-FM bilgi güvenliğine ilişkin içeriğin sunulduğu E-FM portalı ve zorlayıcı bileşen olarak belirtilen bilgilerin içselleştirilmesini içeren iki bileşenden oluşur. Bu modeli mevcut modellerden ayıran husus farkındalık içeriğinin anlaşılmasının zorunluluk olmasıdır.

NIST 800-50'de ortaya konulan bilgi güvenliği öğretim modeli son kullanıcı ve kurum çalışanlarının dikkatinin güvenliğe yoğunlaştırıldığı farkındalık ile başlar, ilgili ve gerekli güvenlik yeteneklerinin oluşturulmaya çalışıldığı uygulama aracılığıyla ilk iki adımda kazanılan bilgi ve yeteneklerin bütünleştirilerek tek bir ana bilgiye ulaşmayı amaçlayan öğretim adımına ulaşmayı amaçlar. Öğretim adımı güvenlik uzmanlarının vizyonlarına yön vermeyi ve proaktif önlemler almalarını sağlamaya çalışır. Tüm kullanıcıları kapsayan farkındalık eğitimi ile başlamaktadır, ancak seviye arttıkça kullanıcı profili de değişmektedir [52].

Shaw ve arkadaşları [53] tarafından bilgi zenginliğinin, bilgi güvenliği farkındalığı üzerinde etkilerini araştırmak üzere yapılan çalışmada ortaya konulan araştırma modeli algılama, anlama ve tahmin etme olarak adlandırılan 3 farklı farkındalık seviyesi bulunmaktadır. Yapılan araştırma sonucunda algılama ve anlama seviyelerinde başarılı olan kullanıcıların tahmin etme seviyesinde daha başarılı oldukları ortaya konulmuştur. Çalışmada metin içerikle karşılaşan kullanıcıların algılama, çoklu ortam içerikleri ile karşılaşan kullanıcıların ise anlama ve tahmin etme seviyelerinde daha başarılı oldukları tespit edilmiştir.

Kritik altyapıların korunmasında işbirliğine yönelik bir farkındalık modeli geliştirmiştir. Bu model, Shaw ve Arkadaşlarının [54] ça-

lışmasından uyarlanmış olup, farkındalık merdiveni önerilmiştir. Benzer şekilde algılama, anlama ve tahmin etme seviyelerinden oluşmaktadır.

Bir diğer çalışmada [55]; **Nedenli Eylem Teorisi** (Reasoned Action), **Davranış Kuramı** ve **Koruma Motivasyon Teorisi** (Protection Motivation) teorilerini temel alan **Davranışsal Eğilim Modeli** kullanılarak güvenliğe ilişkin olumlu davranışların elde edilebilmesini sağlayacak bir farkındalık süreci olarak modellenmiş, Güney Afrika'da bulunan küçük ve orta ölçekli firmalarda test edilmiştir.

Kullanıcıların eğitilmesinin farkındalığı arttırmada en iyi yöntem olduğu kabul edilerek oluşturulan Bilgi Güvenliği Farkındalık Programı Modeli (ISAPM) [56], 7 temel adımdan oluşmaktadır. Tüm kuruluşların kendi güvenlik hedeflerinin tespit edilmesi ile başlayan modelde, bu hedefler kullanılarak program tasarlanmakta, geliştirilmekte ve uygulanmaktadır. Güncel veriler doğrultusunda programın sürdürülmesi en kritik adım olarak kabul edilmektedir. Model kapsamında düzenli olarak programın bilgi güvenliği farkındalığını arttırmaya yönelik etkisi ölçülür. Bu ölçümler sonucunda elde edilen bulguların ve kurumun değişen hedeflerinin değerlendirilmesini takiben model güncellemeler için tasarım adımına tekrar dönmektedir.

Stewart ve Lacey [57] çalışmalarında; bilgi sistem personeli tarafından kullanıcıların bilmesi gerektiği belirlenen bilgilerle bilgi güvenliği farkındalığını sağlamanın mümkün olmadığını, psikolojik kavramlarında kurumlarda farkındalığın arttırılması için göz önüne alınması gerektiğini öne sürmüşlerdir. Bu kapsamda kurumlarda bilgi güvenliği farkındalık eğitimleri planlanırken sınırlanmış mantık, zihinsel model ve genişletilmiş paralel işleme çerçevelerinin kullanımının daha resmi ve tutarlı yaklaşım fırsatları sunduğunu ortaya koymuşlardır.

Hastanelerde bilgi güvenliği farkındalığının arttırılmasına yönelik yapılan bir çalışmada, NIST 800-50'de ortaya konulan bilgi güvenliği öğretim modeli doğrultusunda rol temelli bilgi güvenliği farkındalık modeli önerilmiştir [58]. Bu model, yönetim, sağlıkçılar ve hastalar olarak üç ana rol belirlenmiştir.

Güvenliğin katmanlı bir yapıda sağlanabileceğinin öne sürüldüğü **Katmanlı Güvenlik Paradigma Modeli** (3-LSP) [59], makina öğ-

renmesi yaklaşımları ile anormallik tespiti, anormallik zekâsı ile anormallik önleme ve çok katmanlı elektronik güvenlik farkındalık modeli katmanı (MEAM) olmak üzere 3 katmandan oluşmaktadır. MEAM yapılacak işlemlere göre uygulamaların kişisel ya da kurumsal, çevrimiçi ya da çevrimdışı olmasına, kaynakların harici ya da paylaşımlı olmasına, kişilerin teknik personel ya da sıradan kullanıcı olmasına, servislerin bağımsız ya da destekleyici olmasına göre, yıllık ortalama farkındalık, yıllık ortalama gerçekleşen saldırı ağırlığı gibi parametreler ile sezgisel kavramları içeren 7 kural ile kullanıcıların önemli verilerle işlem yaparken güvenli davranmasını amaçlamaktadır.

ENISA bilgi güvenliği farkındalığı programlarında;

- **Planlama** (bilgi güvenliği politikaları, risk değerlendirmesi, uyumluluk riski, bütçe gibi parametreleri kapsar),
- **Uygulama** (yüz yüze ve bilgisayar tabanlı eğitimler, Intranet siteleri, test ve küçük sınavlar parametreleri kapsar) ve
- **Gözden geçirme** (Güvenlik olayları kök sebepleri, denetim sonuçları, eğitimi tamamlayan kullanıcı sayıları gibi parametreleri kapsar)

adımlarından oluşan iteratif bir modeli benimsemiştir [60].

ISO/IEC 27001 [61] Bilgi Güvenliği Yönetim Sistemi (BGYS); bu sistemi kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek, denetlemek ve iyileştirmek için izlenmesi gereken adımları belirlemiştir. Bilgi güvenliği sisteminin yönetimi için BGYS politikası, amaçlar, hedefler, süreçler ve prosedürlerin geliştirilmesini kapsayan planlama, BGYS politikası, kontroller, süreçler ve prosedürlerin gerçekleştirilip işletilmesini kapsayan uygulama, BGYS politikası, amaçlar ve süreç performansının değerlendirilmesi, uygulanabilen yerlerde ölçülmesi ve sonuçların rapor edilmesini kapsayan kontrol et ve yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve önleyici faaliyetlerin gerçekleştirilmesini kapsayan önlem al adımlarından oluşan **PUKÖ Döngüsü Modelini** önermiştir. PUKÖ (Planla-Uygula-Kontrol Et-Önlem Al) döngüsünün girdisi güvenlik gereksinimleri, çıktısı ise güvenliktir.

Valentine [62] çalışmasında; geleneksel farkındalık programlarının çalışılan pozisyon ya da görevlerden bağımsız olarak tüm çalışanlar

için tek tip eğitim yaklaşımını benimsediğini belirtmiştir. Daha verimli ve maliyet etkin yaklaşım olarak çok fazlı modelin kurumların ihtiyaçlarını daha iyi karşılayacağı değerlendirilmiş, hangi varlıkların korunması gerektiğinin belirlendiği **değerlendirme**, bu varlıklarla hangi çalışanların ilişkili olduğunun belirlendiği **tanımlama** ve sonrasında senaryo bazlı eğitimleri de kapsayan **eğitim** adında 3 fazdan oluşan bir model önermiştir.

4.5. Değerlendirmeler

Kitabın bu bölümünde öncelikle geçmiş yıllarda yaşanan siber saldırılar ışığında siber güvenlik kavramı değerlendirilmiş, farkındalık bakış açısıyla siber saldırı yaşam döngüsü ortaya konulmuş, kavramsal değerlendirmeler yapılmış, bileşenlerin birbiri ile olan ilişkileri açıklanmış, farkındalık seviyesinin belirlenmesi ve arttırılmasına yönelik olarak literatürde yapılan çalışmalar incelenerek değerlendirmeler sunulmuştur.

Farkındalık çok farklı bilgi birikimi, yetenek, bakış açısı ve yüksek bilinç sahibi olmayı, sahip olunan bilgi varlıklarının değerini bilmeyi, değeri ölçüsünde ise korumayı gerektirmektedir. Literatürde yapılan çalışmalar değerlendirildiğinde, kişilerin farkındalık seviyeleri ile davranışları arasında her zaman tutarlı bir ilişki bulunmadığı, farkındalığı yüksek olan bir kişinin bunu davranışa dönüştürmediği takdirde alınan tüm teknolojik tedbirlere rağmen bilgi güvenliği ihlallerinin gerçekleştiği görülmektedir. Farkındalığın farkında olmak, yapılanları veya yapılması gerekenlerin davranışa dönüştürülmesi ve kurallaştırılması ile sağlanabilmektedir. Bunun sağlanabilmesi için ise bir konuyu bilmek yetmemektedir. Bilineni kurallaştırmak ve o kuralları da uygulamak gerekmektedir.

Farkındalığın etkin bir şekilde davranışa dönüştürülmesi, farkındalık seviyesinin doğru bir şekilde ölçülmesi, kavramsal bir model doğrultusunda dinamik olarak farkındalık seviyesinin arttırılması ve bilgi işlenen tüm alanlarda uygulanması ile mümkün olabilecektir. Günümüzde ağırlıklı olarak teknolojik önlemlere yönelik çalışmalar yapıldığı, farkındalığa yönelik akademik çalışmaların ise son derece kısıtlı olduğu görülmektedir. Bu alanda yeni çalışmaların yapılması, farklı seviyelerde modellerin geliştirilmesi ve bu modellerin uygulaması ve iyileştirilmesi gerektiği görülmüştür. Yüksek seviyede bir siber güvenliğin veya korumanın sağlanması açısından

bu çalışmalar son derece faydalı olacaktır. Ayrıca, kavramsal olgunluğun oluşması ve sonrasında ortaya konulan modellerin, kullanıcının günlük yaşantısında kullandığı akıllı sistemlerle entegre edilmesine yönelik çalışmalar yapılmalıdır.

Farkındalık yöntemleri ve modelleri genel olarak değerlendirildiğinde;

- Başarılı bir farkındalık modelinin ancak tüm seviyelerde (kişisel, kurumsal ve ulusal) uygulanabilecek bir model olması,
- Bilgi güvenliğinin doğası gereği dinamik (döngü) bir model olması gerektiği,
- Model adımlarının içeriklerinin net bir şekilde ortaya konulması,
- Bilgi varlıkları ile doğru orantılı bir farkındalık seviyesine ulaşmayı amaçlaması gibi unsurları içerisinde barındırması

gerektiği değerlendirilmektedir.

Ülkemizdeki genel durum değerlendirildiğinde;

- Siber güvenlik farkındalığımızın düşük olduğu,
- Farklı seviyelerde güvenlik farkındalığı gibi bir konunun farkında olunmadığı,
- Farkındalık modellerinin bilinmediği, anket haricinde bir modelin kullanılmadığı veya uygulanmadığı
- Farkındalığın henüz davranışa dönüştürülemediği ve dönüştürmek içinde çok çaba harcanılmadığı,
- Akademik olarak konunun kapsamlı olarak araştırılmadığı, bu konuda yeteri kadar akademik çalışmanın bulunmadığı,
- Yapılan araştırmalarda ise konunun önemi ve kapsamı dikkate alındığında gereken önemin verilmediği

değerlendirilmektedir.

Günümüzde en önemli unsurlardan biri haline gelen farkındalığın ölçülmesi, değerlendirilmesi ve arttırılabilmesi için dinamik bir farkındalık modeline ve farkındalığın yönetilmesine ihtiyaç vardır. Böyle bir model, [63] nolu kaynakta verilmiştir. Bu bölümün yazarlarından Sn. Salih Erdem Erol'un GÜ Bilgi Güvenliği Mühendisliği ABD'da tamamladığı yüksek lisans eğitimi kapsamında hazırladığı

"Siber Güvenlik Farkındalığı İçin Yetenek Tabanlı Dinamik Model" konulu tez çalışmasında [63], bu konu kapsamlı olarak incelenmiş ve somut çözüm önerileri verilmiştir. Okuyucularımızın, bu tezi incelemelerinde fayda vardır.

Kaynaklar

[1] Vural, Y. (2007). *Kurumsal Bilgi Güvenliği ve Sızma Testleri,* Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

[2] İnternet: *NATO Dergisi*. Yeni Tehditler: Siber Boyut. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.nato.int%2Fdocu%2Freview%2F2011%2F11-september%2FCyber-Threads%2FTR%2F&date=2016-11-16, Son Erişim Tarihi: 16.11.2016.

[3] İnternet: Verizon Enterprise. Data Breach Investigations Report 2016. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.verizonenterprise.com%2Fresources%2Freports%2Frp_DBIR_2016_Report_en_xg.pdf&date=2016-11-16, Son Erişim Tarihi: 16.11.2016.

[4] Çetin, H. (2014). Kişisel Veri Güvenliği ve Kullanıcıların Farkındalık Düzeylerinin İncelenmesi. *Akdeniz İ.İ.B.F. Dergisi*, 14(29), 86-105.

[5] İnternet: IBM. Cyber Security Intelligence Index 2015. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww-01.ibm.com%2Fcommon%2Fssi%2Fcgi-bin%2Fssialias%3Fhtmlfid%3DSEW03073USEN&date=2016-11-16, Son Erişim Tarihi: 16.11.2016.

[6] Internet: Türkiye İstatistik Kurumu. Hane Halkı Bilişim Teknolojileri Kullanım Araştırması. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.tuik.gov.tr%2FPreHaberBultenleri.do%3Fid%3D18660&date=2016-11-16, Son Erişim Tarihi: 16.11.2016.

[7] İnternet: Symantec Corporation. Internet Security Threat Report 2016. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.symantec.com%2Fcontent%2Fdam%2Fsymantec%2Fdocs%2Freports%2Fistr-21-2016-en.pdf&date=2016-11-16, Son Erişim Tarihi: 16.11.2016.

[8] İnternet: Verizon Enterprise. Data Breach Investigations Report 2015. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.verizonenterprise.com%2Fresources%2Freports%2Frp_data-breach-investigation-report_2015_en_xg.pdf&date=2016-11-16, Son Erişim Tarihi: 16.11.2016.

[9] Felix, H. (2015). *Studies on Employees' Information Security Awareness*, Yüksek Lisans Tezi, Göttingen Üniversitesi, Göttingen.

[10] Cherdantseva, Y., Hilton, J. (2013). A reference model of information assurance and security. *2013 International Conference on Availability, Reliability and Security*, Regensburg, 546-555.

[11] Hambrick, D. C., Chen, M. J. (2008). New academic fields as admittance-seeking social movements: The case of strategic management. *Academy of Management Review*, 33(1), 32-54.

[12] Chiprianov, V., Kermarrec, Y., Rouvrais, S., ve Simonin, J. (2012). Extending enterprise architecture modelling languages for domain specificity and collaboration: application to telecommunication service design. *Software & Systems Modelling*, 1-12.

[13] İnternet: NIST. Information Technology Security Training Requirements: A Role- and Performance-Based Model, Special Publication 800-16. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fnvlpubs.nist.gov%2Fnistpubs%2FLegacy%2FSP%2Fnistspecialpublication800-16.pdf&date=2016-11-16, Son Erişim Tarihi: 16.11.2016.

[14] Huang, D. L., Rau, P. P. ve Salvendy, G. (2010). Perception of information security. *Behaviour & Information Technology*, 29(3), 221-232.

[15] İnternet: TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü. (2007). Bilgi Güvenliği Yönetim Sistemi Risk Yönetim Süreci Kılavuzu. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.bilgiguvenligi.gov.tr%2Fdokuman-yukle%2Fbgys%2Fuekae-bgys0004-bgys-risk-yonetim-sureci-kilavuzu%2Fdownload.html&date=2016-11-21, Son Erişim Tarihi: 16.11.2016.

[16] Cardona, O. D. (2003). The need for rethinking the consepts of vulnerability and risk from a holistic perspective: A necessary review and criticism for effective risk management. In G. Bankoff, G. Frerks ve D. Hilhorst (Eds.), *Mapping vulnerability: Disasters, development and people.* (Chapter 3). London: Earthscan.

[17] İnternet: NIST. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology, Special Publication 800-30. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fnvlpubs.nist.gov%2Fnistpubs%2FLegacy%2FSP%2Fnistspecialpublication800-30r1.pdf&date=2016-11-16, Son Erişim Tarihi: 16.11.2016.

[18] İnternet: United States Computer Emergency Readiness Team (2011). Control Systems Security Program(CSSP). URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.us-cert.gov%2Fcontrol_systems%2Fcsthreats.html&date=2016-11-16, Son Erişim Tarihi: 16.11.2016.

[19] Yiğit, T., Akyıldız, M., A. (2014). Sızma Testleri İçin Bir Model Ağ Üzerinde Siber Saldırı Senaryolarının Değerlendirilmesi. *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitü Dergisi,* 18(21), 14-21.

[20] Erol, S., E., Sağıroğlu, Ş., (2015), Kişisel, Kurumsal ve Ulusal Bilgi Güvenliği Farkındalığı Üzerine Bir İnceleme, *8th International Conference on Information Security and Cryptology (ISCTurkey)*.

[21] Al-Jarrah, O., Arafat, A. (2014). Network intrusion detection system using attack behavior classification. *5th International Conference on Information and Communication Systems (ICICS),* 1-6, Jordan.

[22] Özbilen, A. (2012). *TCP / IP Tabanlı Dağıtık Endüstriyel Denetim Sistemlerinde Güvenlik ve Çözüm Önerileri*, Doktora Tezi, Gazi Üniversitersi Fen Bilimleri Enstitüsü, Ankara.

[23] İnternet: Sahte E-fatura Dalgasından En Çok Türkiye Etkilendi. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.eset.com%2Ftr%2Fabout%2Fpress%2Farticles%2Farticle%2Fsahte-e-fatura-dalgasindan-en-cok-turkiye-etkilendi%2F&date=2016-11-16, Son Erişim Tarihi: 16.11.2016.

[24] İnternet: Cryptolocker Virüsü Bu Sefer de Türk Telekom Faturası ile Geliyor. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.hwp.com.tr%2F2014%2F12%2F17%2Fdikkat-cryptolocker-virusu-bu-sefer-de-turk-telekom-faturasi-ile-geliyor%2F&date=2016-11-16, Son Erişim Tarihi: 16.11.2016.

[25] İnternet: Akgül, M. A. (2014). İnsan Beyni Algıladığı Ölçüde Düşünür, Düşündüğü Ölçüde Uygular. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.biltekhaber.net%2F2198.html&date=2016-11-16, Son Erişim Tarihi: 16.11.2016.

[26] Salvendy, G. (Eds.). (2006). *Handbook of Human Factors and Ergonomics*. Üçüncü baskı. New York: John Wiley&Sons.

[27] Ronnie, L., Johansson, M. ve Xiong, N. (2003). Perception management: An emerging concept for information fusion. *Information Fusion*, 4(3), 231-234.

[28] İnternet: Şahinaslan, E., Kandemir, R. ve Şahinaslan, Ö. Bilgi Güvenliği Farkındalık Eğitim Örneği. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fab.org.tr%2Fab09%2Fbildiri%2F117.pdf&date=2016-11-16, Son Erişim Tarihi: 16.11.2016.

[29] Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(l), 31–41.

[30] ISF (2003). The standard of good practice for information security. Version 4.0. *Information Security Forum.*

[31] Kruger, H., A., Kearney, W., D. (2006). A prototype for assessing information security awareness. *Computers & Security*, 25(4), 289-296.

[32] Johnston, A., C., Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3), 549-566.

[33] Swain, A., Guttman, H. (1983). Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. Final Report. *Nuclear Regulatory Commission*, Washington.

[34] Azjen, I., Brown, T. C. ve Carvajal, F. (2004). Explaining the discrepancy between intentions and actions: The case of hypothetical bias in contingent valuation. *Intentions and Actions*, 30(9), 1108-1121.

[35] Bagozzi, R., P. (2007). The legacy of the technology acceptance model and a proposal for a paradigm shift. *Journal of the Association for Information Systems*, 8(4),244-254.

[36] Öğütçü, G. (2010*). E-Dönüşüm Sürecinde Kişisel Bilişim Güvenliği Davranışı ve Farkındalığının Analizi,* Yüksek Lisans Tezi, Başkent Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

[37] Allam, S., Flowerday, S., V. ve Flowerday, E. (2014). Smartphone information security awareness:A victim of operational pressures. *Computers & Security, 42*, 56 -65.

[38] Malcolmson, J. (2009). What is security culture? Does it differ in content from general organisational culture?. *43rd Annual 2009 International Carnahan Conference on Security Technology*, 361-366, San Jose.

[39] İnternet: NIST. Building an Information Technology Security Awareness and Training Program, Special Publication 800-50. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fnvlpubs.nist.gov%2Fnistpubs%2FLegacy%2FSP%2Fnistspecialpublication800-50.pdf&date=2016-11-16, Son Erişim Tarihi: 16.11.2016.

[40] Hansch, N., Benenson, Z. (2014). Specifying IT security awareness. *25th International Workshop on Database and Expert Systems Applications,* 326-330.

[41] Sari, P. K., Candiwan ve Trianasari, N. (2014). Information security awareness measurement with confirmatory factor analysis. *International Symposium on Technology Management and Emerging Technologies (ISTMET 2014),* 218-223, Indonesia.

[42] Velki, T., Solic, K. ve Ocevcic, H. (2014). Development of users' information security awareness questionnaire (UISAQ) – ongoing work. *Information and Communication Technology, Electronics and Microe-*

lectronics (MIPRO), 2014 37th International Convention on, 1417-1421, Croatia.

[43] Harbach, M., Fahl, S. ve Smith, M. (2014). Who's afraid of which bad wolf? A survey of IT security risk awareness. *IEEE 27th Computer Security Foundations Symposium*, 97-110, Vienna.

[44] Wiles, J., Gudaitis, T., Jabbusch, J., Roggers, R. ve Lowther, S. (2012). Information security awareness training: Your most valuable to countermeasure to employee risk. *Low Tech Hacking, Street Smarts for Security Professionals*, 193-225.

[45] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. ve Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers&Security*, 42, 165-176.

[46] Öğütçü, G., Testik, Ö., M. ve Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, 56, 83-93.

[47] Greca, I. M., Moreira, M. A. (2000). Mental models, conceptual models, and modelling. *INT. J. SCI. EDUC.*, 22(1), 1- 11.

[48] Teorey, T., Yang, D. ve Fry, J. (1986). A logical design methodology for relational databases using the extended entity-relationship model. *ACM Comput. Surv.*, 18 (2), 197–222.

[49] Mylopoulos, J. (1992). Conceptual modeling and telos. In P. Loucopoulos, R. Zicari (Eds.), *Conceptual modeling, databases and case: An integrated view of information systems development*. New York: John Wiley&Sons, 50-68.

[50] Kritzingera, E., Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers & Security*, 27(5-6), 224-231.

[51] Kritzinger, E., von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, 29(8), 840-847.

[52] İnternet: NIST. Building an Information Technology Security Awareness and Training Program, Special Publication 800-50. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fnvlpubs.nist.gov%2Fnistpubs%2FLegacy%2FSP%2Fnistspecialpublication800-50.pdf&date=2016-11-16, Son Erişim Tarihi: 16.11.2016.

[53] Shaw, R. S., Charlie, C. C., Albert, L. H. ve Hui-Jou, H. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, 52(1), 92-100.

[54] Hernantes, J., Laugé1, A., Labaka, L., Rich, E., Olav, F., Sarriegi, J. M., Martinez-Moyano, I. J. ve Gonzalez, J. J. (2011). Collaborative mode-

ling of awareness in critical infrastructure protection. *System Sciences (HICSS), 44th Hawaii International Conference on*, Kauai, 1-10.

[55] Gundu, T., Flowerday, S. V. (2013). Ignorance to awareness: towards an information security awareness process. *South African Institute of Electrical Engineers,* 104(2), 69-79.

[56] Maqousi, A., Balikhina, T. ve Mackay, M. (2013). An effective method for information security awareness raising initiatives. *International Journal of Computer Science & Information Technology (IJCSIT),* 5(2), 63-72.

[57] Stewart, G., Lacey, D. (2012). Death by a thousand facts: Criticising the technocratic approach to information security awareness. *Information Management & Computer Security*, 20(1), 29-38.

[58] İnternet: Masetia, O., Pottas, D. (2006). A Role-Based Security Awareness Model For South African Hospitals. URL: http://www.webcitation.org/query?url=http%3A%2F%2Ficsa.cs.up.ac.za%2Fissa%2F2006%2FProceedings%2FResearch%2F76_Paper.pdf&date=2016-11-16, Son Erişim Tarihi: 16.11.2016.

[59] Jidiga, G. R., Sammulal, P. (2013). The need of awareness in cyber security with a case study. *Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, 1-7, Tiruchengode.

[60] İnternet: ENISA. Information Security Awareness Initiatives: Current Practice and The Measurement of Success. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.itu.int%2Fosg%2Fcsd%2Fcybersecurity%2FWSIS%2F3rd_meeting_docs%2Fcontributions%2FENISA_Measuring_Awareness_Final.pdf&date=2016-11-16, Son Erişim Tarihi: 16.11.2016.

[61] TS ISO/IEC 27001 (2006). Bilgi teknolojisi-güvenlik teknikleri-bilgi güvenliği yönetim sistemleri-gereksinimler. *Türk Standartları Enstitüsü*.

[62] Valentine, J., A. (2006). Enhancing the employee security awareness model. *Computer Fraud&Security*, 2006(6), 17-19.

[63] Erol, S., E. (2016). *Siber Güvenlik Farkındalığı İçin Yetenek Tabanlı Dinamik Model*, Yüksek Lisans Tezi, Gazi Üniversitesi FBE Bilgi Güvenliği Mühendisliği ABD. Danışman: Prof. Dr. Şeref SAĞIROĞLU.

Siber Güvenlik Farkındalığı Oluşturma

BÖLÜM 5

Dr. Atila BOSTAN
Dr. Gökhan ŞENGÜL

SİBER GÜVENLİK FARKINDALIĞI OLUŞTURMA

Bu bölümde, siber sistemlerde uygun güvenlik seviyesine ulaşmak ve bu seviyenin devamlılığın sağlamak için, insan bileşeninde güvenlik farkındalığı oluşturmak ve güvenli davranış biçimi alışkanlığı kazandırmak için yapılması gerekli olan uygulamalar ile bu amaca ulaşmak için yol gösterici olabilecek prensipler açıklanmıştır.

5.1. Giriş

Siber güvenlik sistemleri, siber ortamlarının bilinçli veya bilinçsiz olarak kötüye kullanılması ve bu ortamlarda veya bunlar aracılığı ile hasar, kayıp, bozuma gibi istenmeyen sonuçların ortaya çıkmasını engellemeyi amaçlamaktadır. Her geçen gün büyüyen ve yaygınlaşan siber ortamlar, yapıları gereği birden fazla bileşenden oluşmaktadır. Dolayısı ile bu sistemler üzerinde güvenlik sağlamak ve işlemleri takip ederek uygun tedbirleri devreye sokmak amacı ile kurulup çalıştırılan siber güvenlik sistemleri de çok sayıda bileşen içermektedir [1]. Ayrıca derinlemesine güvenlik prensibi ile farklı işlem aşamalarında benzer ürünlerin ve güvenlik çeşitliliği prensibi ile aynı aşamada farklı ürün ve uygulamaların beraber çalıştırılması da bileşen sayısının artmasına neden olmaktadır [2],[3].

Siber güvenlik sistemlerinin hepsinde bir insan bileşeni bulunur [1]. Bu insan bileşeni sistem içerisinde kullanıcı, yönetici, işletmen, tasarımcı ve geliştirici gibi rolleri üstlenmektedir ve doğal olarak güvenlik süreçlerine genellikle doğrudan müdahildir [4]. Ancak, siber güvenlik sistemlerinde aktif etkileri olan bu rollerinden "kullanıcı" rolü özel bir hassasiyet içermektedir ve dolayısı ile özel ilgiye tabi olmuştur. Zira "kullanıcı" rolü ile sistemde yer alan insanlar; hem diğer rollerdekilere göre sayıca daha fazla olmakta ve hem de ilgi

odakları güvenlik haricindeki iş süreçlerinde olduğu için güvenliğin tesis, idame ve kontrolüne yeterince önem ve öncelik vermemektedirler [5]. Siber sistemlerde yer alan tüm insan bileşenlerinin gerçekleştirdikleri eylemlerde güvenlik yansımalarının neler olabileceğini ve bu etkileşimlerin sistem bekası için ne derece önemli olduğu bilinci siber güvenlik farkındalığını tanımlar. Literatürdeki bilimsel çalışmalar bu farkındalık seviyesinin insan bileşeninden kaynaklanan güvenlik ihlal ve yanlış uygulamaları ile doğrudan ilgili olduğuna işaret etmektedir [6]. Başka bir ifade ile, güvenlik farkındalığı yüksek olan kullanıcılar, yöneticiler ve işletmenler, tasarımcı ve geliştiriciler daha az uygulama hatası ve güvenlik prensip ihlali yapmaktadırlar.

Bu bölümde siber güvenlik farkındalığının, siber güvenlik sistemlerinin ayrılmaz bileşeni olan insan davranışları üzerindeki etkisi ve bu davranışları olumlu yönde geliştirmek için siber güvenlik farkındalığı alanında yapılabilecekler anlatılmıştır. Takip eden bölümlerde sırası ile, siber sistemlerde güvenliğin sağlanması için insan bileşenini önemi, güvenlik farkındalığı-bilgi-davranış ilişkisi, farkındalık eğitimleri ve güvenlik farkındalığı oluşturmada, geliştirmede uygun tedbir ve prensipler anlatılmıştır.

5.2. En Zayıf Bileşen İnsan

Siber sistemlerin kaçınılmaz entegre yapısı, birden çok sistemin beraber çalışmasını gerektirmekte ve dolayısı ile sistemler birbirleri ile veri ve hizmet paylaşırken karşılıklı güvenlik risklerinin de artmasına sebep olmaktadırlar. Mevcut tüm otomatik hesaplama, kontrol ve iletişim sistemleri insan hayatını kolaylaştırmak için tasarlanmış ve işletilmektedir. Doğal olarak insan, siber ortamların dolaylı veya doğrudan bir bileşeni olarak sistem içerisinde her zaman yer almaktadır. Siber sistemlerin, doğrudan öznesi veya nesnesi olmasalar bile, dolaylı olarak sistem hizmetlerinden faydalanan, sistemi tasarlayan veya işleten rolleri ile insanlar siber sitemlerle sürekli etkileşim halindedir.

Siber ortamlarda güvelik çok katmalı bir dizi tedbir ve sistemle sağlanmaktadır. Bu çoklu katmanlarda dikey olarak, sistem, ağ, kullanıcı gibi, farklı parametreler üzerinde güvenlik kontrolleri yapılırken, yatay olarak aynı veya benzer parametrelerin farklı sistem veya uygulamalarla çapraz kontrolleri yapılabilmektedir. Güvenlik

sistemlerinde bu tür hiyerarşik ve çok katmanlı yapı genellikle güvenlik zinciri olarak adlandırılır ve bu zinciri oluşturan bileşenlerin beraber çalıştırılması ile güvenlik seviyesinde önemli kazanımların elde edilmesi hedeflenmektedir. Güvenlik zincirindeki her bir bileşenin tek başına güçlü/aşılamaz olması ise kümülatif bakış açısından anlamsızdır, çünkü güvenlik açısından önemli olan en zayıf bileşendir. Zincirdeki bir bileşenden kaynaklanan zafiyet diğer bileşenlerin ve dolayısı ile zincirin görevini yerine getirememesi anlamına gelmektedir. Bu anlayış "*Bir zincir en zayıf halkası kadar kuvvetlidir*" söylemi ile çok öz olarak ifade dilmektedir. İşte bu güvenlik zincirinin bir veya birden fazla noktasında insan bileşenin yer alması kaçınılmazdır. Siber güvenlik olaylarının incelemeleri neticesinde ihlal nedeni olarak, hatalı insan davranışları olduğu sıklıkla belirtilmektedir. Ayrıca alanda yapılan bilimsel araştırma ve taramalarda insan kaynaklı güvenlik olay ve ihlallerinin toplam olaylar içerisinde en büyük yüzdeyi oluşturduğu çarpıcı bir şekilde raporlanmaktadır [7],[8]. İnsandan kaynaklanan güvenlik açıklarının çeşitliliği ve oransal olarak daha çok gerçekleşiyor olması, alanda genel kabul gören "*güvenlik zincirinde en zayıf halka insandır*" söylemini kuvvetlendirmektir.

Farklı bir bakış açısından bakıldığında ise, tüm güvenlik ihlallerini veya açıklarını bir insan rolü ile ilişkilendirmek her zaman mümkündür. Zira, sistemde tespit edilen her türlü güvenlik açığı yeterince derine gidildiğinde bir insan tercihi veya ihmali ile ilişkilendirilebilir. Örneğin, bir kütüphane veya hazır sınıfta (class) ortaya çıkan güvenlik açığı, kullanıcı hatasından ziyade, o kütüphaneyi tasarlayan ve/veya geliştiren insanların tasarım ve geliştirmedeki güvenlik farkındalık eksikliği olarak yorumlanabilir. Bu tür bir geniş açıdan bakıldığında tüm güvenlik ihlal ve açıklarını bir insan rolü ile, kullanıcı, yönetici, işletmen, tasarımcı veya geliştirici ile ilişkilendirmek her zaman mümkündür. Ayrıca, sistem tasarımında kod ve araçların yetersiz kaldığı, yeterli seviyede güvenlik kontrolünü gerçekleştiremediği, durumlarda genellikle sorumluluğu insan bileşenine atfeden mühendislik çözümleri oldukça yaygındır. Örneğin web adres aldatmalarına karşı kullanıcıların adres çubuğundaki karakterleri kontrol etmesi gerekliliği, SSL uygulamalarında geçersiz/hatalı sertifika uyarısında uyarıyı kontrol ederek iletişime devem etme keyfiyetinin/sorumluluğunun kullanıcıya bırakılması veya za-

rarlı olabilecek e-posta ve eklerinin anlamsal olarak kullanıcı tarafından kontrol edilmesi gibi prensiplere dayanan güvenlik yapılanmaları da güvenlik ihlal ve hatalarının insan kaynaklı olmasına yol açmaktadır. Özetle, sistem içerisinde formülize ve otomotize edemediğimiz güvenlik fonksiyonlarını insanlardan beklemek normal karşılanmalıdır, ancak bu fonksiyonları yerine getirmesi beklenen kişilerin bu işlemler için ehil olmaları da vazgeçilemez bir gerekliliktir. Sistemleri oluşturan donanım ve yazılım bileşenlerinin aksine, insan bileşeninin davranış ve tercihlerini kesin olarak öngörmek mümkün değildir. İnsan tercihlerinde ve davranış-alışkanlıklarında olumlu yönde bir değişiklik yapabilmek için insanların eğitilmesine, yapmış oldukları tercihlerin ve davranışların sonuçlarının neler olabileceğinin öğretilmesine ihtiyaç vardır. Sistem güvenliği açısından bakıldığında, tüm rollerde fonksiyon gerçekleştiren insanların ilgili eylemlerinde, tercih ve davranışlarının sistem güvenliği açısından yansımalarını doğru tahmin edebilmeleri ve eylemlerini bu çekinceler ile gerçekleştirmeleri güvenlik farkındalığı olarak adlandırılmaktadır. Güvenlik açığı olmayan, yüzde yüz güvenli, bir sistem geliştirmenin mümkün olamadığı gibi bu farkındalığın tam olması, teorik olarak mümkün değildir. Çünkü yeterince zaman ve kaynak aktarılırsa, her sistemde bir güvenlik açığı bulmak veya alınan güvenlik tedbirlerini atlatmak mümkündür. Ancak güvenlik farkındalığının yüksek olması, sistemlerin daha güvenli olarak tasarlanması, geliştirilmesi, işletilmesi ve kullanılması sonucunu doğurmaktadır. Başka bir ifade ile, sistemlerin güvelik seviyesini yükseltmek ve güvenlik açıklarını en aza indirmek için, kullanıcı, yönetici, işletmen, tasarımcı ve geliştirici rollerindeki insanların güvenlik farkındalığının ve hassasiyetinin artırılması kilit unsurdur [9].

5.3. Siber Güvenlik Farkındalığında Seviyeler ve Sorumluluklar

Siber sistemleri kullanan, tasarlayan, geliştiren ve çalıştıran tüm insan rollerinin fonksiyonlarını yerine getirirken, güvenlik gerekliliklerini göz önünde bulundurmaları ve eylemlerinin sistem ve bilgi güvenliği açısından sonuçlarını doğru ve etkin şekilde değerlendirebiliyor olmaları gerekir. Aksi halde, sistemde güvenlik açıklarını en az seviyeye indirmek mümkün olmayacaktır. Takdir edileceği gibi, kullanıcı, tasarımcı, geliştiren ve çalıştıran kişilerin sistem gü-

venliği ve yerine getirdikleri fonksiyonlardaki güvenlik ihtiyaçları açısından bilmeleri gereken konular ve detayları farklılık göstermektedir. Bir kullanıcının bilmesi ve dikkat etmesi gerekenlerle, bir tasarımcı veya sistem işletmenininkiler oldukça farklıdır. Dolayısı ile, her kullanıcı rolünde, rollerin alt sorumlulukları bazında, güvenlik farkındalık içerik ve seviyesinin özelleşmesine ihtiyaç vardır.

Yukarıdaki paragrafta ifade edileni görselleştirmesi açısından aşağıda örnek durumlar verilmiştir.

Örnek Durum 1[1]*;*

ABD Dış İşleri Bakanlığı yapmakta olan bayan Hillary Clinton, kişisel güvenlik ve mahremiyet çekinceleri ile elektronik posta iletişimi için kendi ev ortamında kurulan bir posta sunucusu üzerinden tüm resmi ve özel elektronik posta iletişimini gerçekleştirmiştir.

Gerçek hayatta yaşanmış olan örnek durum 1 için, bayan Hillary Clinton devlet sırrı niteliği taşıyan bilgileri kontrollü alan dışına çıkarmak ve bir seri güvenlik tedbirini ihlal etmek suçlaması ile karşı karşıya kalmıştır [10]. Ancak bu örnek durumun bir genellemesi ile, üst seviye bir yöneticinin elektronik posta iletişimi üzerinde güvenlik ve mahremiyet çekincelerine sahip olması ve bu çekinceleri gidermek için bir arayış içerisine girmesi oldukça normal ve bu kullanıcı rolü için yeterli bulunması gereken bir durumdur. Yaşanmış olan bu durum için ne derece geçerli olduğu tartışılıyor olmasına rağmen, muhtemelen bayan Clinton'u bu tür bir çözüme yönlendiren teknik danışman(lar)ın varlığından ve bir yanlış yönlendirmeden bahsetmek kuvvetli bir ihtimaldir. Eğitimi, tecrübesi ve dikkati siber güvenlikten tamamen farklı olan ve siber sistemlere sadece bir kullanıcı olarak müdahil olan şahsın bu tür bir kullanımın güvenlik yansımalarının farkında olması ve sonuçlarından sorumlu tutulması oldukça mantıksız görünmektedir. Bu değerlendirmeyi yaparken teknik danışmanlar tarafından bu tür bir kullanımın güvenlik risk ve sorumluluklarının bayan Clinton'a açıklanarak tercihi onun yapmadığı varsayılmıştır. Zira, özel ilgi durumları hariç, bu seviyede

1 *Bu örnek olay 2015 yılında medya tarafından dünya kamuoyu ile paylaşılmıştır. Olayın siyasi, politik ve uluslararası ilişkiler boyutları da mevcut olmasına rağmen, örnek durum bu örnek kapsamında sadece insan rolleri ve bu rollerin siber güvenlik farkındalığı açısından ele alınmıştır.*

ve pozisyonda bulunan şahsın güvenli elektronik posta kullanımı dışında, sunucu hizmetlerinin güvenliği ve güvenlik gerekleri konusunda bilgi sahibi olması, farkındalık geliştirmiş olması, riskleri uygun şekilde değerlendirerek doğru karar vermesi beklenmemelidir.

Örnek Durum 2;

Bir kurumunda, kurum çalışanları tarafından kullanılacak ve gizli bilgi işleyecek olan otomasyon sistemi, güvenlik ihtiyaçları doğrultusunda, SSL/TLS (HTTPS) protokolünü kullanan bir web hizmeti olarak tasarlanmıştır. Ancak, sistem işletmeni tarafından SSL/TLS hizmetinde güvenilen otoriteden alınan sayısal sertifika yerine, kendisi tarafından üretilen bir sertifika kullanılmaktadır. Bu durumda doğabilecek güvenlik risklerine karşı, kullanıcılara site erişimlerinde sertifika detaylarını ve hata mesajını kontrol etmeleri gerektiği bildirilmiştir.

Bu veya benzer sayısal sertifika yanlış kullanımları ile gerçek hayat uygulamalarında sıklıkla karşılaşılmaktadır. Örnek olarak verilen senaryo ve benzeri durumlarda, genellikle maliyet ve prosedürlerden kaçınmak için, olması gereken güvenlik yapılanması sistem işletmenleri tarafından ihlal edilmektedir [11][12]. Bu ve benzeri birçok durumda, sistem işletmeni tarafından yapılan güvenlik tercihleri ve alınan güvenlik riskleri çoğunlukla sistemin diğer paydaşları ile paylaşılmamaktadır. Kaldı ki sistem işletmenlerinin yaptıkları tercihlerin güvenlik yansımaları konusundaki farkındalıkları da tartışmalıdır. Ancak, ikinci örnek durumda vurgulanması gereken bir diğer konu ise, güvenlik tasarımında genellikle kullanıcı rolündeki insan bileşenine atfedilen sorumluluk detayında saklıdır. Verilen örnek durumda kullanıcının SSL sayısal sertifika uyarısını kontrol etmesi beklenmektedir. Takdir edilebileceği gibi bu işlem alanda temel bilgiye ve pratiğe sahip olan şahıslar için bile oldukça karmaşık ve zaman alıcı bir işlemken, bu tür bir fonksiyonun sıradan kullanıcılar tarafından web servisine her yeni ulaşımda tekrarlanan şekilde yerine getirilmesini beklemek gerçek dışıdır. Sıradan kullanıcıların çoğunun tarayıcılar tarafından üretilen sertifika uyarı mesajlarındaki içeriği anlamadıkları ve bu durum ile aldıkları güvenlik risklerinin farkında olmadıkları bilimsel araştırmalarla kanıtlanmıştır [13][14]. İlave olarak, sürekli maruz kalınan uyarı mesajlarının ise kullanıcılarda, duyarsızlık oluşturduğu da bilinmektedir. Sonuç olarak; ikinci örnek durumda verilen senaryo kapsamında, kulla-

nıcının sahte ve taklit bir web hizmetine yönlendirmesini müteakip bir güvenlik ihlalinin oluşması (burada kasıt yönlendirme eylemi değil, bu yönlendirme sonrasında sahte hizmet tarafından yapılan güvenlik ihlalidir. Örn. Kullanıcı parolasının çalınması v.b.), kullanıcının yapması gereken kontrollerde gösterdiği zafiyetten dolayı, kullanıcı hatası olarak nitelenebilir. Ancak bu değerlendirme ne derece gerçekçidir? Kullanıcıların, gerek teknik yeterlilik ve gerekse insan psikolojisi gereği bu tür bir kontrolü etkin olarak yerine getirmesini beklemek, mevcut bilimsel sonuçlar ile, büyük bir hatadır. Güvenlik sisteminin bu bilgiler ve gerçekçi bir değerlendirme ile yapılandırılması, gözlenen olayların bu açıdan da değerlendirilmesi önemlidir.

Örnek Durum 3;

Müşterileri için yazılım geliştirmekte olan bir ticari firmanın ürününde, gerek ürün tasarımında güvenliğin ele alınmamış olması ve gerekse geliştirmede kullanılan yazılım kütüphanelerinin eksiklerinden dolayı, kullanıcıların bilgilerini ve sistem güvenliğini tehlikeye sokan güvenlik açıkları tespit edilmiştir.

Yukarıda belirtilen örnek durum benzeri gerçek olaylar son yirmi yıl içerisinde çok sayıda yaşanmıştır. Bu tür tespitlerin genellikle yaşanan güvenlik ihlalleri neticesinde yapılmasına karşılık, az sayıda durum ise bir güvenlik ihlali yaratmadan önce kullanıcılar veya geliştiriciler tarafından tespit edilmiştir [15][16][17]. Örnek durumda belirtildiği gibi, bu tür güvenlik açıklarının oluşmasındaki en temel neden, güvenliğin sistem tasarımı esnasında bir ihtiyaç olarak göz önüne alınmaması ve sistem geliştirirken kullanılan araç ve bileşenlerin güvenlik boyutunda bir incelemeye tabi tutulmamasından kaynaklanmaktadır. Özellikle günümüzde yazılım sistemlerinde hazır bileşen kullanımının yaygınlaşması ile bu tür riskler oldukça önem kazanmıştır. Zira bir yazılım araç veya kütüphanesinin herhangi bir ara ürün geliştirilmesinde kullanılmasını takiben bu ara ürün daha büyük bir sistemin parçası olarak işlev yapabilmektedir. Bu aşamalardan birinde oluşan güvenlik ihlali tüm sistemin güvenliği için bir risk oluşturmaktadır. Ayrıca, her bir bileşen ve aracın kendi başına değerlendirilmesinde güvenliğinin yeterli seviyede olmasına karşılık, bu bileşenlerin bir arada kullanılmasından yeni veya ilave riskler ortaya çıkabilmektedir.

Örnek Durum 4;

Güvenlik ihtiyaçları doğrultusunda, kullanıcı adı ve parola ile giriş yapılan bir sistemin kullanıcısı bazı kullanım kolaylıkları ve/veya idari/sosyal etkileşimler gereği, bu bilgileri başka şahıslarla paylaşmış ve sistemde kendi bilgisi dışında ancak kendi adına yapılan işlemlerden dolayı mağdur olmuştur.

Bu örnekte bahsedilen benzer durumlarla, özellikle kurum sistemlerinde ve ticari firma işlemlerinde sıklıkla karşılaşılmaktadır. Güvenlik sistem ve mekanizmalarının kullanılabilirlik açsından bir engel gibi görülmesi, süreç ve işlemleri yavaşlattığının düşünülmesi bu tür olaylarda temel motivasyonu oluşturmaktadır [18]. Ancak, bu tür tedbir ve uygulamalarının bilgi, işlem ve şahıs güvenliğinin sağlanması amacı ile kullanılması gerektiği kullanıcılar tarafından kesin olarak bilinmeli ve bu süreç ve işlemler atlanmadan takip edilmelidir.

Belirtilen dört adet örnek durumun, gerek kapsam ve olay içeriği ve gerekse uygulama türü olarak çoğaltılması ve genişletilmesi mümkündür. Bu örnekler farkındalık türleri ve seviyelerine dikkat çekmek, her tür ve seviyede gerekliliklerin farklı olduğunu vurgulamak amacı ile verilmiştir. Örnek durumlardan da çıkarılabileceği gibi siber sistemlerin güvenliğinin sağlanması konusunda sadece bir tür insan rolünün güvenlik farkındalığı yeterli olmamaktadır. Tüm insan rollerinin fonksiyonlarını yerine getirirken güvenlik kaygısını bir ihtiyaç olarak sürekli göz önünde bulundurmaları halinde sistem güvenliğini yüksek seviyede tutmak mümkün olabilecektir. Bu amaçla siber sistemlerde ihtiyacın belirlenmesinden, sistemin tasarlanması, geliştirilmesi, işletilmesi ve kullanılmasına kadar tüm aşamalarda yer alan insan bileşenlerinin icra ettikleri işlemin gereği olan güvenlik risk ve tedbirlerinin farkında olması ve bu süreç ve işlemleri kendi rolleri içerisinde uygun şekilde yerine getirmesi önemlidir.

Özellikle farkındalık eğitimleri bölümünde bahsedileceği gibi, farkındalık kendiliğinden gelişen bir olgu değildir. Farkındalık geliştirmek, bu amaçla eğitim ve uygulamaların yapılmasına, insanlar tarafından süreç ve işlevlerin içselleştirilmesine ihtiyaç duyar [19]. Teknolojinin çok hızlı bir şekilde yaygınlaşarak çeşitlenmesi ve uygulamaların sayı ve tür olarak çoğalmasına paralel olarak, siber

sistemlerde yer alan tüm insan bileşenlerinin rolleri kapsamında güvenlik farkındalığı geliştirmesi sistem güvenliği açısından bir gerekliliktir. Takdir edilebileceği gibi her rol tipi için, farkındalık geliştirici eğitim ve uygulamalar farklı olmak zorundadır.

Siber sistemlerin doğası gereği birden fazla insan bileşeni ürün ve hizmetin ortaya çıkmasında rol almaktadır. Bu kişilerin, sistem güvenlik gereklerinin farkında olmalarının yanında, yerine getirdikleri işlev bazında güvenlik sorumluluklarının da tanımlanmış olmasına ihtiyaç vardır. Böylece, her bir rolün fonksiyonunu yerine getirirken ilgili sorumluğu hissetmesi ve muhtemel ihlallerden, yerine getirdiği işlem bazında, sorumlu olacağını bilmesi, farkındalık oluşturulması ve sürdürülmesinde önemli bir gerekliliktir. Bu amaçla hukuki, idari düzenlemelerin yapılması ve bunların ilgili kişilere bildirilmesine ihtiyaç vardır. Gerekli olan durumlarda sertifika ve ehliyet gibi belgeler ile bu sorumluluk ve yeterliliklerin belirlenmesi önemli fayda sağlayacaktır.

5.4. Farkındalık, Bilgi ve Davranış İlişkisi

Farkındalık terimi çok farklı şekillerde tanımlanmasına karşılık, genel olarak kişinin yapmış olduğu işlerde bilinçli olma hali olarak ifade edilebilir. Bilinçli olmak ise yapılan işin gereklerini ve sonuçlarını bilmek, bu sonuçları isteyerek işlemi yapmaktır. Bu tanımı siber sistemlerde güvenlik farkındalığına taşıdığımızda tanım, siber sistemler üzerindeki eylemlerde, kişinin güvenlik gereklerini bilmesi ve eylemin güvenlik açısından sonuçlarının bilincinde olması hali olarak ifade edilebilir.

Yukarıdaki paragrafta çıkarımını yaptığımız tanım gereği, kişinin farkında olması için eylemin gereklilikleri ve sonuçlarını bilmesine ihtiyaç vardır. Bir başka ifade ile bilgi, farkında olabilmek için kaçınılmaz bir ihtiyaçtır. Ancak tek başına bilginin güvenlik farkındalığı oluşturmada yeterli olmadığı çok sayıda bilimsel çalışma ile ortaya konmuştur. Zira eylemlere ve davranışlara yansımayan teorik bilginin özellikle güvenlik alanında farkındalık için yeterli kabul edilmesi imkansızdır [20]. Bu durumu kırmızı trafik ışığı yanıyorken araçla geçiş yapmanın tehlikeli olduğunu bilmek fakat bu işlemi refleks olarak geliştirmemekle izah edebiliriz. Zira bu örnekte olduğu gibi, bilgi kaza veya ihlalin gerçekleşmesini veya bu yönde ortam oluşturulmasına engel olmamıştır. Kişide bir güvenlik farkındalığı

oluştuğunun tespiti için, güvenli davranış biçimlerinin kazanılmış, sürekli hale getirilmiş ve içselleştirilmiş olmasına ihtiyaç vardır.

Siber sistemler, bilgiyi çok yüksek süratlerde işlemekte, çok sayıda bileşenin beraber çalışması nedeni ile karmaşık yapılara sahip olmakta ve günlük insan yaşantısı içerisinde çok sıklıkla kullanılmaktadır. Bütün bu özellikler, siber sistemlerde farklı rollerde işlev yerine getiren kişilerin dikkatlerini sistem ve bilgi güvenliğine odaklamasını zorlaştırmaktadır. İnsanlar faaliyetlerini yerine getirirken, eylemlerinin güvenlik yansımalarını değerlendirmeyi genellikle ihmal etmektedir. Doğal olarak, işlemin tamamlanması öncelik kazanmakta ve daha önceden geliştirilmiş ve sık kullanım nedeni ile genellikle refleks haline gelmiş davranış şekillerini takip etmektedir [20]. İnsanların işlemleri yaparken güvenli davranış şekillerini benimsemeleri, bu davranışları refleks haline getirmeleri, siber sistemlerde güveliğin sağlanması açısından çok önemlidir. Zira bir anlık bir güvensiz işlemin sonuçlarını geri çevirmek veya doğan zararı telafi etmek genellikle mümkün olamamaktadır. Bu açıdan bakıldığında, sadece bilgi düzeyinde bir güvenlik farkındalığının sistem güvenliği açısından çok bir şey ifade etmeyeceği açıktır. Bu bilginin davranışlara yansıması ve güvenli davranış biçimlerinin refleks olarak geliştirilmesi gereklidir. Güvenli davranış biçimlerinin geliştirilmesi ve refleks kazanımı konusundaki önerileri takip eden farkındalık eğitimleri bölümünde bulabilirsiniz.

5.5. Farkındalık Eğitimleri

Siber sistemlerde güvenliğin sağlanabilmesi için insan bileşenlerinde etkili bir güvenlik farkındalığı oluşturmak gerektiği uzun yıllar öncesinde yapılan bir tespittir. Geçmiş 20-30 yıl içerisinde, kurum ve kuruluşlarda bu amaçla çok sayıda ve farklı kurgular ile eğitim ve davranış geliştirici faaliyetler gerçekleştirilmiştir [21][22]. Bütün bu uygulamalar analiz edildiğinde, ortak noktanın siber sistemlerde güvenliğin önemi, güvenlik gereklerinin neler olduğunun bilinmesi, güvenlik sistem, araç ve teknolojisinin tanıtımı ve kullanımına odaklandıkları görülmektedir. Bazı kısıtlı örnekler hariç tutulduğunda, bu uygulamaların güvenli davranış biçimleri geliştirilmesini amaçlamadıkları, bu yönde bir tasarım içermedikleri görülmektedir. Oysa, bilginin güvenli davranış biçimleri geliştirmede önemli ölçüde kolaylaştırıcı bir gereklilik olduğu,

ancak tek başına yeterli olmadığı bilimsel olarak kanıtlanmış ve tartışmasız olarak kabul görmektedir. Yeterli, güncel bilgiye dayalı ve mantıksal sebep-sonuç ilişkisi içerisinde güvenli davranış biçimlerinin geliştirilmesi, etkin bir güvenlik farkındalığı için bir zorunluktur. Bu açıdan ele alındığında, güvenlik farkındalığı konusunda geçmişte yapılan uygulamaların çok önemli bir bölümünün bilgilendirme aşamasında kaldığı, uygun davranışın geliştirilmesi ve ediniminde yetersiz kaldığı görülmektedir.

Eğitimin her alanında olduğu gibi, etkin bir siber güvenlik farkındalığı için, kişilerin edindikleri bilgilerin onlarda olumlu ve arzu edilen yönde davranış değişikliğine neden olması gerekmektedir [23]. Bu nedenle siber ortamlar ve sistemlerde güvenlik farkındalık eğitimlerinin bilgilendirme aşamasını takiben uygun davranışın içselleştirilmesi faaliyetlerini de kapsaması bir mecburiyettir. Aksi takdirde, gereklilik ve neden-sonuç ilişkilerini teknik olarak bilen, ancak gerçekleşme olasılığının çok düşük olduğu veya işlem ve süreçleri yavaşlattığı gibi gerekçeler ile uygun davranış biçimlerini takip etmekten geri duran kişiler sistemde çoğunlukta olacaktır.

"*Siber Güvenlik Farkındalığında Seviyeler ve Sorumluluklar*" başlığı altında anlatılanlara paralel olarak insan rollerine göre belirlenecek seviye ve sorumluklar çerçevesinde, güvenlik gerek ve teknikleri konusunda yeterli bilgilendirmeyi takiben, ama mutlaka, uygun davranış geliştirmesi ve bu davranışların sürdürülmesini temin edecek uygulamalar yapılmalıdır. Bu uygulamalarda özellikle bilgilendirme ve örnek çözümlerin verilmesini takip eden davranış içselleştirmesi ve otomatik tepki gelişimi aşamalarında haberli ve habersiz kontrollü güvenlik saldırılarının yapılması öne çıkmaktadır. Siber sistemlerde etkin bir güvenlik farkındalık seviyesi elde etmek ve insan bileşenlerinde uygun davranış biçimleri geliştirmek amacı ile takip edilmesi gerekli faaliyetler aşağıda listelenmiş ve takiben bu faaliyetler hakkında kısa içerik bilgileri verilmiştir.

Siber sistemlerde etkin güvenlik farkındalığı oluşturmak için eğitim faaliyetlerinin;

- Bilgilendirme
- Örnek problem çözümleri ve alınan dersler
- Uygun sıklıkla tekrar ve güncellemeler

- Güvenli davranış biçimlerini otomatikleştirme (refleks gelişimi)
- Etkin takip ve
- Teşvik ve ödüllendirme

başlıkları altında desteklenmesi faydalı olacaktır. Bunlar aşağıda kısaca açıklanmıştır.

5.5.1. Bilgilendirme

Siber sistemlerdeki tüm insan bileşenleri rolleri kapsamında ve sorumlulukları gereği güvenlik sistemin gereklilikleri, zafiyetleri, uygun davranış biçimlerinin nedenleri ve sonuçları konusunda yeterli seviyede bilgilendirilmelidir. Bu bilgilendirmenin şahısların rolleri ve sorumlulukları bazında özelleştirilmesi çok önemlidir. Geçmişte, insan rolleri ve sorumlulukları göz önüne alınmadan, genel ve toplu olarak yapılan bilgilendirme faaliyetlerinin, doğal olarak uygun davranışın edinilmesinde etkin olmadığı gözlenmiştir. Bilgilendirmenin kişilerin sorumlulukları çerçevesinde, sistemdeki rolü gereği ve uygulanabilirlik prensibine uygun olarak bilmesi gereken detayda tasarlanması gereklidir. Bu tasarımın başarısı, müteakip aşamalar ve uygun davranış gelişimi için hayati öneme haizdir.

Bilgilendirme faaliyetiyle kişiler kazandıkları edinimlerle neyi, ne zaman, nasıl ve neden kapmaları gerektiği konusunda mantıklı çıkarımlar yapabilecek ve mevcut imkan ve yetenekleri kullanan çözümler üretebilecek seviyede bilgiye sahip olmalıdırlar.

5.5.2. Örnek Problem Çözümleri ve Alınan Dersler

Bu faaliyeti bir önceki "Bilgilendirme" başlığı ile birleştirmek mümkün olsa da, icra sıralamasının önemli olduğuna inandığımız için birbirini takip eden uygulamalar olarak verilmesini daha uygun buluyoruz. Yeterli ve etkin bilgi seviyesine ulaşan kişilerin bu bilgileri ile pratik yapmaları, uygun ve mantıksal çıkarımlarda bulunmaları (ney, ne zaman, nasıl ve neden) örnek durumlar çerçevesinde tecrübe edilmelidir. Seçilen örnek durumların, çoğunlukla izlenen güvenlik olaylarından oluşması ve kişilerin rol ve sorumlulukları ile uyumlu olmasına dikkat edilmelidir. Faaliyete katılan kişilerin, eğitimcilerle ve kendi aralarında neden ve sonuçları tartışmaları, gerekçeleri ve uygun davranış biçimlerini yeterli detayda açıklamaları edindikleri bilginin etkin kullanımına önemli katkılar sağlaya-

cak faaliyetlerdir.

5.5.3. Uygun Sıklıkla Tekrar ve Güncellemeler

Etkin ve uzun süreli öğrenmenin sağlanması için yeterli miktarda ve sıklıkta tekrar çok önemlidir. Özellikle siber sistemlerdeki tekniklerin ve teknolojik gelişmelerin sürati de göz önüne alındığında, bilgilendirme ve pratiğin ihtiyaca göre tekrar edilmesi, güncellenmesi ve yeni uygulama ve bilgileri de kapsaması kaçınılmaz bir gerekliliktir. Sisteme eklenen her yeni uygulama ve/veya kullanıma giren her yeni teknoloji için güvenlik gereklilikleri ve güvenli davranış biçimleri konusunda bilgilendirmenin güncellenmesine ihtiyaç vardır. Bu konuda, sisteme yeni katılan kişiler ile sadece değişiklikler konusunda güncelleme yapılacak kişilerin ayırımı, dikkatin ve ilginin sürekliliğini sağlamak için önemli bir husustur.

5.5.4. Güvenli Davranış Biçimlerini Otomatikleştirme (Refleks Gelişimi)

Siber sitemlerde güvenlik farkındalığı konusunda belki de en önemli aşama güvenli davranış biçimlerinin içselleştirilip otomatik tepkiler haline getirilmesi aşamasıdır. Bu aşamanın başarısı kişilerin bilinçsiz olarak güvenlik ihlali yapma oranını doğrudan etkileyecektir. Sistem tasarımcısının güvenlik ihtiyaçlarını tasarıma otomatik olarak dahil etmesi, geliştiricinin güvenlik için etkin uygulama şekillerini ürün gelişimi esnasında takip etmesi ve kullanması, işletmenin güvenli, fonksiyonel sistem parametrelerini ve yapılanmasını kullanması, kullanıcıların iş yapma süreçlerinde güvenli davranışları takip ederek, tüm bunların her rol bazında otomatikleştirilmesi hata ve ihlal olasılığını önemli ölçüde azaltmaktadır. Güvenli davranış biçimlerinin otomatikleşmesi ise, yeterli sayıda ve frekansta tekrar ile sağlanabilmektedir. Kazanılan bu güvenli davranış şekillerinin otomatikleştirilmesi ve sürekliliğinin sağlanması konusunda bu başlığı takip eden "Etkin takip" ve "Teşvik ve ödüllendirme" uygulamalarının da katkısı ve önemi büyüktür.

5.5.5. Etkin Takip

Güvenli davranış gerekliliklerini ve biçimlerini öğrenen kişilerin bu davranışları otomatikleştirmesi ve sistemde güvenlik ihlallerinin azaltılması açısından, kişi davranışlarının sürekli ve etkin olarak ta-

kip edilmesi, olumlu veya olumsuz davranışlar için kişilere uygun geri bildirimin yapılması önemlidir. Böylelikle kişiler, sergiledikleri davranışların sistem güvenliği konusunda ne derece uygun olduğu konusunda bilgilenecekler ve varsa yarattıkları güvenlik risk ve ihlallerini giderici tedbir ve uygulamaları öğreneceklerdir. Davranışlarının sistem güvenliği açısından takip edildiği ve incelendiğinin bilinmesi kişilerde ilave duyarlılık ve motivasyon yaratacaktır. Ancak burada takip neticesinin cezalandırıcı olmaması, öğretici, düzeltici ve ödüllendirici bir yapıda olması çok önemlidir. Kişi davranışlarını takip eden ve inceleyen şahıs ve mekanizmanın kişi hatalarını bulup onu cezalandırma veya aşağılama yaklaşımında olmaması, bilakis kişilere yardımcı olma ve beraberce daha güvenli bir sistemin oluşturulması, güvenlikte sürekliliğin sağlanması konusunda çaba göstermesi gereklidir. Siber sistemlerde haberli ve/veya habersiz kontrollü güvenlik saldırı ve tatbikatlarının yapılmasının etkin takip için uygun ortam ve verinin edilmesine önemli katkı sağlayacağı unutulmamalıdır.

5.5.6. Teşvik ve Ödüllendirme

Siber sitemlerde kişi davranışlarının güveli kullanım ve güvenlik farkındalığı konusunda takip edilmesi ve incelenmesi neticesinde tespit edilen olumsuzluklar ön plana çıkarılmamalı, daha çok olumlu, uygun ve süreklilik arz eden davranış biçimleri teşvik edilerek, mümkünse ödüllendirilmelidir. Teşvik ve ödülün alandan daha çok diğer kişilerde olumlu etki yaratmak için verildiği unutulmamalıdır. Teşvik, ödüllendirmenin miktarı ve şekli sistemdeki diğer kişilerde özenme, takdir duygusu yaratacak oranda olmalı ve hiç şüphesiz, tartışmaya meydan vermeyecek şekilde açık, saydam ve mutlaka adil olmalıdır.

5.6. Değerlendirmeler

Gerek çok sayıda olmaları ve gerekse güvenlik hiyerarşisinin en zayıf bileşeni olmaları nedeni ile kullanıcılar siber ortamlarda en çok hedeflenen bileşenler olmuştur. Kullanıcıların en zayıf bileşeni oluşturmasında temel etmen ise insan davranışlarının çeşitliliği, tutarsızlığı ve ön görülememesidir. Kullanıcı davranışlarını izleyerek tüm kullanıcı eylemlerinin güvenli sınırlar içinde kalmasını temin edebilecek bir otomatik denetleme sisteminin oluşturulması teorik

olarak imkansızdır. Yaşanmış tecrübeler ve alandaki bilimsel çalışmalar, kullanıcıların kendi davranışlarının güvenlik gereklikleri ve sonuçları konusunda bilinçlendirilmesi ve güvenli kullanım alışkanlıkları oluşturulmasının en etkin çözüm olacağını belirtmektedirler.

Güvenlik farkındalığı olarak adlandırılan kullanıcılardaki bu bilinçlilik durumu özellikleri, doğal olarak, değişik kullanıcı tiplerine uyumlu olarak farklılık göstermektedir. Bunun yanında, insanlarda farkındalık oluşturmak ve kalıcı davranış değişikliği yaratabilmek için, onların planlı bir eğitime tabi tutulmalarına ihtiyaç vardır. Bu tespitler ışığında, kullanıcılarda siber güvenlik farkındalığı oluşturmanın en etkin yolunun kullanıcı fonksiyonlarına ve görevlerine uygun farkındalık eğitimleri olduğu ortaya çıkmaktadır. Zira tüm kullanıcı türlerine uygun genel bir siber güvenlik eğitimi etkin ve uygulanabilir değildir.

Siber güvenlik farkındalık eğitimlerinin bu amaç için özel tasarlanmış ve hedeflenen kullanıcı türüne göre özelleştirilmiş olması kaçınılmaz bir gerçektir. Siber güvenlik farkındalık eğitimleri, bu bölüm beşinci maddesinde belirtilen eğitim hedef ve prensiplerine uygun olarak geliştirilmesi koşuluyla, kullanıcılarda etkin güvenlik farkındalığı oluşturacaktır.

Kaynaklar

[1] Green, Jeremy Swinfen. Cyber Security: An Introduction for Non-Technical Managers. Routledge, 2016.

[2] Jaeger, Trent. "Configuring Software and Systems for Defense-in-Depth." Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense. ACM, 2016.

[3] Levillain, Olivier, Baptiste Gourdin, and Hervé Debar. "TLS record protocol: Security analysis and defense-in-depth countermeasures for HTTPS." Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security. ACM, 2015.

[4] Joinson, Adam, and Tommy van Steen. "Human aspects of cyber security: Behaviour or culture change?." Cyber Security: A Peer-Reviewed Journal 1.4 (2018): 351-360.

[5] Banfield, James Michael. A Study of Information Security Awareness

Program Effectiveness in Predicting End-User Security Behavior. Eastern Michigan University, 2016.

[6] Arachchilage, Nalin Asanka Gamagedara, and Steve Love. "Security awareness of computer users: A phishing threat avoidance perspective." Computers in Human Behavior 38 (2014): 304-312.

[7] Cisco, *Cisco 2018 Annual Cybersecurity Report*, 20.07.2018 tarihinde "https://www.cisco.com/c/en/us/products/security/security-reports.html#~download-the-report" internet adresinden erişilmiştir.

[8] Symantec, 2018 Internet Security Threat Report, 20.07.2018 tarihinde"https://www.symantec.com/security-center/threat-report?inid= globalnav_scflyout_istr" internet adresinden erişilmiştir.

[9] McIlwraith, Angus. Information security and employee behaviour: how to reduce risk through employee education, training and awareness. Routledge, 2016.

[10] Anthony Zurcher, Hillary Clinton emails - what's it all about?, 20.07.2018 tarihinde "https://www.bbc.com/news/world-us-canada-31806907" internet adresinden erişilmiştir.

[11] Bostan, Atila. "Implicit learning with certificate warning messages on SSL web pages: what are they teaching?." Security and Communication Networks 9.17 (2016): 4295-4300.

[12] Tarazan, Şafak, and Atila Bostan. "Customizing SSL Certificate Extensions to Reduce False-Positive Certificate Error/Warning Messages." International Journal of Information Security Science 5.2 (2016): 21-28.

[13] Reeder, Robert W., et al. "An Experience Sampling Study of User Reactions to Browser Warnings in the Field." Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. ACM, 2018.

[14] Felt, Adrienne Porter, et al. "Improving SSL warnings: Comprehension and adherence." Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. ACM, 2015.

[15] Carvalho, Marco, et al. "Heartbleed 101." IEEE Security & Privacy 12.4 (2014): 63-67.

[16] Sinn, Richard. Software security technologies. Cengage Learning, 2015.

[17] Aljawarneh, Shadi A., and Muneer O. Bani Yassein. "A conceptual security framework for cloud computing issues." International

Journal of Intelligent Information Technologies (IJIIT) 12.2 (2016): 12-24.

[18] Stobert, Elizabeth, and Robert Biddle. "The password life cycle: user behaviour in managing passwords." Proc. SOUPS. 2014.

[19] McIlwraith, Angus. Information security and employee behaviour: how to reduce risk through employee education, training and awareness. Routledge, 2016.

[20] Bostan, Atila, and İbrahim Akman. "Bilişim Güvenliği: Kullanıcı Açısından bir Durum Tespiti." Bildiriler Kitabı: 51.

[21] Alotaibi, Fayez, Nathan Clarke, and Steven Furnell. "An analysis of home user security awareness & education." Internet Technology and Secured Transactions (ICITST), 2017 12th International Conference for. IEEE, 2017.

[22] McIlwraith, Angus. Information security and employee behaviour: how to reduce risk through employee education, training and awareness. Routledge, 2016.

[23] Abawajy, Jemal. "User preference of cyber security awareness delivery methods." Behaviour & Information Technology 33.3 (2014): 237-248.

Siber Güvenlikta Büyük Veri ve Açık Veri Kullanımı

BÖLÜM 6

Prof. Dr. Şeref SAĞIROĞLU

SİBER GÜVENLİKTE BÜYÜK VERİ VE AÇIK VERİ KULLANIMI

6.1. Giriş

Siber ortamlar verilerin taşındığı, veriler üzerinde işlemlerin yapıldığı, verilerden değer elde edildiği, veriler ile saldırıların yapıldığı belki de en önemlisi yine bu verilerin analizi sonucunda saldırıların önlendiği ortamlardır. Dolayısıyla, veriye sahip olanlar ve bunları analiz edenler, elektronik dünyada var olabilir, saldırılara karşı koyabilir veya olası saldırıları anlayabilir, karşılaşılabilecek olumsuzluklardan, zararlardan, tehlikelerden daha az etkilenir, yeni araştırmalar yaparak koruma teknikleri ve teknolojileri geliştirebilir ve sonuçta hem bunu bir fırsata dönüştürebilir hem de kişisel, kurumsal ve ulusal bilgi varlıklarını koruyabilirler.

Bu konunun önemini anlayan toplumlar bu konuda çözümler geliştirmişler, verilerini araştırmacılara açımışlar, yüksek seviyede bir koruma sağlamanın yanında bundan hem ekonomik hem de stratejik olarak faydalanmışlardır.

Bu bölümde bu konu kapsamlı olarak incelenmiştir.

6.2. Açık Veri ve Açık Kaynağın Önemi

Açık Kaynak, Açık Toplum, Açık Bilim, Açık Veri, Açık Veri Türkiye son dönemde üzerinde konuşulan konuların başında geliyor.

Açık veya açıklık, kişiler, toplumlar veya ülkeler için önemlidir. Gelişim ve değişim için şarttır. Bunların Konuşulması, paylaşılması, okunulması veya anlatılması bile pozitif bir etki bırakıyor insanın üzerinde. Toplumda güven duygusunu artıran önemli bir etkisi vardır. Güven veriyor.

Açık Bilgi Vakfı (Open Knowledge Foundation) açık veriyi, "herhangi bir telif hakkı, patent ya da herhangi bir kontrol mekanizması-

na tabi olmaksızın herkes tarafından ücretsiz ve özgürce kullanılan veri" olarak tanımlamaktadır. Diğer bir ifadeyle "herkes tarafından ücretsiz olarak erişilebilen, tekrar kullanılabilen ve paylaşılabilen araştırma veya gözlem sonuçları" açık veri olarak ifade edilmektedir. Aynı zamanda, Açık Bilgi Vakfı "açık devlet verisini" ise "devlet ya da devlet kontrolündeki birimler tarafından üretilen, herkes tarafından kullanabilen ve paylaşılabilen veriler" olarak tanımlamaktadır.

Dünyaya baktığımızda; bu kelimeleri konuşan, bunları hayatın içerisine alan, bu konuda çalışmalar yapan, verilerini, dokümanlarını, yaptıklarını ve bunların değerlerini bilen ve koruyan, paylaşılması gereken bilgilerini ise topluma açan veya bunları geniş kitlelerle paylaşanlar gelişmiş toplumlardır. Açık verileri işleyip bunları değere dönüştürenler, ekonomiye katanlar, bunun ekonomisini oluşturanlar ise gelişmiş beyinlere sahip ülkelerdir.

Sümerlerden günümüze kadar geçen uygarlıkları incelediğimizde, bu açıklık ile hareket eden toplumların büyüdükleri, felsefelerini yaygınlaştırdıkları ve sonuçta geliştiklerini tarih bize söylemektedir. Osmanlı imparatorluğunun büyüme felsefesinin arkasında da bu olduğu gibi büyük dünya devletlerinin büyüklüğünün arkasında da bu vardır. Doğal olarak; bu büyüklük, şeffaflıkla ve açıklıkla sağlanabilmektedir. Bu sayede güven artmaktadır. Destekler çoğalmaktadır. Toplumların veya ülkelerin ortak hedeflere koşması veya kilitlenmesi de artmaktadır. Google, Wikipedia, Scholarpedia, GoogleScholar, Facebook, Twitter, Über, TEDTalks, vb ürünler veya ortamlar bunlara verilebilecek iyi örneklerdir. Bu açıklığın ekonomik sonuçları ise Milyar dolarlık şirketler, zengin ve gelişmiş ekonomiler, bilgi toplumları, sosyal projeler, milyarları etkileyen olaylar, değişimler ve sonuçlardır.

Dünya üzerinde büyük etki yaratan uygulamaların sayısını artırmak için; büyük etkiler oluşturabilecek büyük fikirleri geliştirmek, projeleri hayata geçirmek, açık ortamları oluşturmak, paylaşmak, yenilerini düşünmek ve özellikle de bunda ısrar etmek gereklidir.

Ülke olarak açık veriye baktığımızda; bu yönde geliştirdiğimiz büyük projelerin sayısı maalesef azdır. Bunu artırmanın yolu; gelişimin önündeki engellerin kaldırılması, açık bilgiye erişimin yeterli düzeye getirilmesi, üretilen bilginin niteliğinin ve kapsamının ge-

nişletilmesi, teknoloji ve inovasyon kültürünün gelişmesi, yerli ve milli ürünlerin sayılarının artırılması, toplumun hızla gelişip kalkınması, bilgi toplumu ve ekonomisine geçişin hızlandırılmasından geçmektedir. Bundan dolayı, gelişmiş, toplumlar veya ülkeler açık kaynak ve veri yaklaşımlarını desteklemekte, kamu kaynaklarıyla desteklenen projeleri, yayınları, araştırmaları, raporları, araştırma verilerini herkese açmakta, bunun için yasal düzenlemeler yapmakta, bu tür projeleri teşvik etmekte ve bunların hayata geçirilmesinde kolaylıklar göstermektedir.

Büyük ve açık verilerin önemli bir kısmı kamu hizmetlerinden elde edilen verilerdir. Bu verilerin işlenmesi ve elde edilen değerlerin toplumun yararına kullanılması için sahip olunan bazı verilerin kullanıma veya analize açık olması, farklı kurumlar ve birimler tarafından kullanılabilmesi, farklı ve yeni fikirlerin ve çıktıların elde edilebilmesinin yanında girişimciliği ve inovasyonu teşvik etmesi, kurumların verimliliğini artırması, kurumlar arası işbirliğini güçlendirmesi, oluşabilecek ihlallerin tespit edilmesini kolaylaştırması, kayıpları en aza indirgemeye katkı sağlaması, açık verilerden farklı kazanımların elde edilmesi ve bunların vatandaşlara ve yöneticilere aktarılması işlemlerini sağlayacak ve işleri kolaylaştıracaktır.

Akademik ortamlarda "Açık Erişim"; yaklaşık 10 yıldır yoğun olarak ülkemizde tartışılmakta ve bugün dünyada pek çok bilim insanı, araştırmacı, yayınevi, kurum ve kuruluşlar tarafından desteklenmektedir.

Budapeşte Açık Erişim Girişimi Bildirgesinde; Açık Erişim "verilerin okunabilir, kaydedilebilir, erişilebilir, kopyalanabilir, yazdırılabilir, taranabilir, dizinlenebilir, bağlantı verilebilir, başka bir ortama veri olarak aktarılabilir ve her türlü amaç için yasal çerçevede kullanılabilir olması ve ekonomik, hukuki ve teknik engellemeler olmaksızın kamuya ücretsiz olarak açık bulunması" olarak tanımlanmaktadır.

Büyük veri, günümüzde gerek akademik ortamlarda gerekse sektörlerde ve kurumlarda önemli ve popüler konularından biridir. Büyük veri; depolama, yönetim ve analiz için sıradan veri tabanı yazılım araçlarının yeteneklerinin gerisinde kaldığı veri kümesi, yüksek hızda toplama, keşif ve analiz sayesinde çok çeşitli verinin çok büyük hacminden ekonomik olarak değer elde etmek için ta-

sarlanan yeni nesil teknolojiler ve mimariler, geleneksel veri işleme uygulamaları veya genel veri tabanı yönetim araçları kullanılarak yönetilmesi zor olan büyük ve karmaşık veri koleksiyonu, farklı formatlarda ve farklı kaynaklardan çok yüksek hızlarda üretilen büyük miktardaki veriler, gibi tanımlamaları olsa da aslında güncel teknolojiler ile çözülemeyen problemlerin çözümünde kullanılabilecek yeni nesil çözümlerdir. Bu verilere, hız, hacim, çeşitlilik, güvenilirlik ve değer olmak üzere beş temel karakteristiğe (5V Özelliği) sahip olsa da buna yeni özelliklerde eklenmektedir (11V Özelliği). Bu temel karakteristikler, verilere ve veri işleme yaklaşımlarımıza bakış açımızı değiştirmekte, pekçok şeyi tekrar sorgulamamıza, yeni yaklaşımlar geliştirmemize ve en önemlisi bir verinin ne kadar hacimli olduğuna, ne kadar hızlı değiştiğine, ne kadar çeşitli olduğuna, ne denli güvenilir olmasına daha çok dikkat etmemize ve en önemlisi de bu verilerden yeni değer nasıl elde edilebilir odaklanmamızı sağlamaktadır.

Verilerin mahremiyetinin sağlanmasına yönelik, çeşitli anonimleştirme teknikleri ve çözümleri mevcuttur. Bu teknikler, en temelde kayıt bağlama, özellik bağlama, tablo bağlama ve olasılık saldırılarına karşı koruma sağlamaktadır. Burada verilere yapılabilecek olası saldırıların veya oluşabilecek açıkların önceden fark edilmesi veya belirlenmesi, ve sonuçta bu oluşabilecek ihlallerin engellenmesi için anonimleştirme tekniklerinin önemi büyüktür. İstenilen anonimleştirme seviyesi sağlanmadan paylaşılan veri kümelerinin saldırıya ve ihlale açık olduğu bilinmektedir. Buna en iyi örnek, 2006 yılında AOL firması tarafından çeşitli araştırma faaliyetleri için, kullanıcı kimliği ve IP numarası silinerek 650 kullanıcıya ait 20 milyon arama sorgu verisi paylaşılmış, ancak birkaç gün içerisinde bu sorguların kimlere ait olduğu araştırmacılar tarafından tespit edilmiştir. Buna benzer başka örneklerde literatürde mevcuttur. Karşılaşılan bu ihlaller araştırmacılara yol göstermiş olup, bu tür ihlallerin önlenmesine yönelik yeni ve farklı çözümler geliştirilmesine öncü olmuştur.

2016 yılında yayımlanan Kişisel Verileri Koruma Kanununda anonimleştirme, "kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi", kişisel veri ise "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" olarak tanımlanmıştır. Bu tanımlara dayanarak, kişisel veri sınıfına giren büyük

verilerin mahremiyeti belirtilen kanun çerçevesinde gerek işlenmesi ve saklanması gerekse aktarılması veya ifşa edilmesi konularında çalışmalar vardır.

Avrupa Birliği;

- "kamu bilgilerinin Avrupa'daki en büyük veri kaynağı olduğunu ve bunların ise sayısal haritalar, meteorolojik, yasal, trafik, mali, ekonomik ve diğer verilerden oluştuğunu belirtmiş, bu verilerin çoğunun yeniden kullanılabilir olduğunu, hava, finans ve sigorta kuruluşları gibi kurumların yeni ürün ve hizmetlerine entegre edilebileceğini", "verilerin altın olduğunu ve bunun keşfedilmesi, işlenmesi ve değere dönüştürülmesini", açık verileri "petrole benzetmiş" ve "dijital çağda verilere önem verilmesi gerektiğini" raporlamış,
- kendi büyük verisini oluşturmak ve "Açık Erişim Arşivlerini" kurmak için H2020 çerçeve programı kapsamında "OpenAIREplus" projesini destekleyerek, 10 milyonun üzerinde doküman, yayın ve verileri bu sisteme aktarılmasını sağlamış, ve
- CERN ev sahipliğinde oluşturulan açık veri arşivi ZENODO (http://zenodo.org/) ile ülkelerin kullanımı için arşivlenmektedir.

Bunun gerekçeleri ise büyük verilerden farklı ve yeni değerlerin elde edilebilme ve Avrupa toplumlarının bu gelişmelerden daha çok faydalanmasını sağlamak ve kendi ekosistemini kurmaktır.

Nicol, Caruso ve Archambault tarafından 2013'de hazırlanan "Avrupa Araştırma Alanları ve Ötesi: Açık Veri Erişim Politikaları ve Stratejileri" dokümanında sunulan verilere göre;

- ABD'nin bu alana yılda 60 milyar dolar harcadığı,
- AB'nin FP7 projeleri kapsamında bu konunun gelişmesi için 50 milyar avroluk harcama planladığı,
- AB'de H2020 için 70 milyar avro araştırma bütçesi kullanılacağı,
- Yıllık veri artışının ise %30 civarında gerçekleştiği ve
- Büyük verilerin, açık veri haline getirilmesiyle AB ülkelerinin bundan yılda 150-300 milyar avro tasarruf sağlanabileceği

belirtilmiştir.

ABD, İspanya, Almanya, Kanada, Japonya, Yunanistan, İtalya vb. ülkeler kamu kaynaklarıyla desteklenen araştırma çıktılarının açık erişim olarak paylaşılmasını zorunlu hale getirmişlerdir. Günümüzde pekçok uluslararası üniversite açık erişimi, araştırmacıların destek alabilmelerinde ve akademik yükseltmelerde ön koşul olarak sunmaktadır.

Ülkemizdeki durumları incelediğimizde ise;

- Ülkemizde açık erişim çalışmaları 2006 yılında başlamış, ülkemizde açık erişim arşivi ve kültürünün oluşturulmasına katkı sağlamak ve kazanılan tecrübeleri paylaşmak amacıyla ANKOS (Anadolu Üniversite Kütüphaneleri Konsorsiyumu) çatısı altında Açık Erişim ve Kurumsal Arşivler (AEKA) adıyla bir çalışma grubu kurulmuştur. Bu grup çalışmalarını sürdürmektedir.
- Ülkemizde 120'nin üzerinde üniversitenin açık erişim yaklaşımlarını destekledikleri, bazılarının ise bunu senato kararı alarak daha da somutlaştırmışlardır.
- World Wide Web Foundation tarafından yıllık olarak yapılan bir araştırma sonucunu incelediğimizde, ülkelerdeki açık verileri sınayan Open Data Barometer listesinde ülkemiz bu yıl 40. sıradadır. Bu sıralamanın ise hazır olma (readiness), uygulama (implementation) ve etki (impact) kriterleri dikkate alınarak belirlendiği, ülkemizin ise 100 üzerinden 3 kriter için sırasıyla 35, 53 ve 15 puan aldığı görülmüştür.
- Ülkemiz için internette açık veri ile ilgili küçük bir araştırma yapıldığında, bazı belediyelerin bu tür platformları açtığı fakat içerisinde herhangi bir bilginin bulunmadığı, devletin bu konudaki alan isimlerini (www.data.gov.tr) aldığını fakat bunların içeriğinin olmadığı görülebilir.
- Ülkemizde, iyi örneklerimizin de olduğunu belirtmekte fayda vardır. Açık kaynak ve açık veri konusunda YÖK, TÜBİTAK ve Üniversitelerimiz örneklerimizdendir.
- Kurumsal Akademik Arşiv ve Ulusal Akademik Arşiv sistemlerinin kurulması için 2014 yılında kamu kaynaklarıyla yapılan projeler ve araştırmalar sonucunda üretilen yayınların açık erişim olarak sunulması, açık erişim politikalarının oluşturulması için bir proje hayata geçirilmiş ve şu an için Yüksek Öğretim Bilgi Yö-

netim Sistemi (https://istatistik.yok.gov.tr) ile tüm öğretim elemanlarının yaptığı çalışmaların neler olduğunu ve ilgi alanlarını genelde ve özelde görebilmek için geliştirilen "Yükseköğretim Akademik Arşiv Projesi" (http://akademik.yok.gov.tr) portalları üzerinden açık bilgiye erişim kanallarını açılmıştır.

- Üniversitelerimizin bu konuya en çok desteği veren kurumlar olduğu ve son on yıldır bu konuya çok önem verildiği, 100'ün üzerinde üniversite web siteleri altında, açık arşivler oluşturmuşlar ve bu portallarda Açık Erişim ve Açık Ders Arşivleri ile bugün için hizmet vermektedir. Örnek olarak; Gazi Üniversitesinin http://www.acikarsiv.gazi.edu.tr ve **acikders.gazi.edu.tr** adreslerinde, Ankara Üniversitesinin ise acikarsiv.ankara.edu.tr ve açık ders için **acikders.ankara.edu.tr** portallarından kamuya açık kaynak ve ders materyallerini sunduğu, diğer üniversitelerde de buna benzer açık arşiv portalları bulunmaktadır.
- Ülkemizde bu alanda yapılan AB destekli projeler olduğu, açık erişim politikalarıyla ilgili olan MedOANet (Mediterranean Open Access Network), ortak altyapı oluşturmak için OpenAIREplus (Open Archives Infrastructure for Research in Europe) ve MedOANet'in devamı niteliğinde olan ve açık erişim politikalarının ve stratejilerinin geliştirilmesine katkı sağlamak amacıyla PASTEUR4OA (Open Access Policy Alignment Strategies for European Union Research) ile ülke bilgi birikimine katkılar sağlanmıştır.
- Ülkemizde 2012 yılında Açık Yönetim Ortaklığı Girişimini (Open Government Partnership) destekleyen ülkelerden birisi olduğunu belirtmiş ve 23 Ağustos 2013'te 352013/9 sayılı ve "Açık Yönetim Ortaklığı Girişimi" konulu Başbakanlık Genelgesi (http://www.resmigazete.gov.tr/eskiler/ 2013/08/20130823-8.htm) yayımlayarak buna taraf olduğunu ve kurumların bu konuda gereğini yapmasını bildirmiştir. Gelinen noktaya bakıldığında ise ülkemizde yeni yeni kurumların bu konuya ağırlık verdikleri ve gerekli adımları, 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı gereği yerine getirmeye çalıştıkları bilinmektedir. Strateji dokümanında, 22 yerde "açık veri" 24 yerde ise "büyük veri" kelimesi geçmektedir. Eylem planında Hedef 4.2'de "Açık Verinin Kullanım Alanları Yaygınlaştırma" başlığı altında;

- ülkemizde açık veri konusunda kamu kurum / kuruluşlarının yanında özel sektör, sivil toplum kuruluşları gibi diğer paydaşları da içine alacak şekilde yapılacak çalışmaların çerçevesinin çizilmesi, kriterlerin belirlenmesi ve kullanımının yaygınlaştırılması,
- açık veri anonimleştirilmiş kamu verisi, özel sektör, üniversiteler, sivil toplum kuruluşları gibi tüm paydaşların verileri de açık veri olarak belirlenip burada tüm paydaşların dahil edildiği,
- paydaşlar tarafından üretilen verilerin açık veri olarak paylaşıldığı ve
- katma değer sağlanan bir modelin oluşturulması

gerektiği vurgulanmıştır. Ayrıca, açık veri konusunda gerekli mevzuat düzenlemelerinin yapılarak açık verinin üretilmesinin ve kullanımının önündeki engellerin kaldırılmasına ihtiyaç duyulduğu, açık veri ortamlarının ve platformlarının oluşturulması görevinin ise Başbakanlığa verildiği, ve eylem maddelerinin ise E4.2.1 : Açık Veri Paylaşım Portalının Oluşturulması ve E4.2.2 : Kamu Verilerinin Açık Veriye Dönüştürülmesi ve Paylaşılması olduğu strateji dokümanında belirtilmektedir.

- TÜBİTAK ULAKBİM'in geliştirdiği DergiPark Projesi son dönemde en önemli projelerden birisidir. Bu açık dergi platformunda bugün için Türkçe ve İngilizce 1.446 dergi, 239.675 Makale, 133.050 kullanıcının kaydı vardır. Bu platform, daha çok ülkemizde üretilen makalelerin açık olarak yayımlandığı bir projedir. Gazi Üniversitesinde ilk örneği yapılan bu projenin bugün için ülkeye yayılması ve 2013 yılından ULAKBİM altında toplanarak bu hizmetin bilimsel dergilere ücretsiz olarak sunulması ve bunu tüm akademisyenlere açmak çok önemli bir projedir. Bunun etkileri gelecekte daha net olarak görülecektir. Bunun konferanslar, seminerler ve çalıştaylar içinde geliştirilmesi çok faydalı olacaktır. Ülkede üretilen bilimi, bu platform üzerinden sunmak ve gelecekte bu verileri farklı amaçlar için analiz etmek, ona göre planlamalar yapmak, yapılan çalışmaların etkisini görmek kolaylaşacaktır.
- Bilgi Güvenliği Derneğinin her yıl Gazi Üniversitesi, ODTÜ ve İTÜ ile düzenlediği Uluslararası Bilgi Güvenliği ve Kriptoloji konferansında sunulan bildirilerin ve yapılan sunumların www.

iscturkey.org adresinden tamamının ücretsiz yayımlanması ise bir diğer güzel örnektir. Bu tür örneklerin ve paylaşımların hızla artması, verilerin boyutlarının büyümesine ve toplanan verilerden yeni çıkarımların ve değerlerin elde edilmesini kolaylaştıracaktır.

6.3. Değerlendirmeler

Açık veri kavramının temelinde, açık ve şeffaf toplumların ve ülkelerin benimsedikleri yaklaşımlar olduğu, gelişmiş ülkelerin bu konuya önem verdikleri, yapılan işlemleri, hükümet harcamalarını, gelecek planlarını elektronik ortamlarda paylaştıkları, bu verilerin analiz edilmesiyle de bunlardan farklı değerler elde edilebileceği ve en önemlisi yeni bakış açıları, kazanımlar ve gelişmeler sağlanabileceğine inandıklarından bu verileri açtıkları, bunun için uluslararası çalışmaları da yürüttükleri bilinmektedir.

Yukarıda farklı bakış açılarıyla açık ve büyük veri ele alınmıştır. Bu konudaki önerilerim, yapılabilecekler, elde edilebilecek kazanımlar ve alınması gereken önlemlere ilişkin görüşlerim aşağıda maddeler halinde sunulmuştur.

- Sayısallaşmayı gerçekleştiremeyen, tüm süreçlerini elektronik ortamlara aktaramayan kurumlar ve ülkeler açık birim, açık kurum veya açık devlet olamayacaklardır.
- Ülkemizde e-dönüşüm projesi çerçevesinde elektronik altyapıların kurulması, birlikte çalışabilirliğin artırılması, doküman paylaşım standartlarının belirlenmesi, üst veri şemalarının oluşturulması, dosya formatlarının belirlenmesi vb. gibi konularda epey yol alınmış olsa da açık veri konusunda maalesef yapılan çalışmalar çok azdır.
- Kamu kaynaklarının kullanıldığı çalışmalar, projeler, desteklenen çalışmalar, yapılan araştırmalar ve bunlardan elde edilen yayınlar kamuoyuna daha çok açılmalıdır.
- Açıklık bir devlet politikası olmalıdır. Bunun özendirici ve yönlendirici olacağı ve süreci hızlandıracağı değerlendirilmektedir.
- Üniversitelerde olduğu gibi tüm devlet kurumları bu tür portallar oluşturmalı ve bu portallarda raporlarını, yayınlarını, is-

tatistiklerini, çalışmalarını, bütçelerini ve en önemlisi verdiği ve vereceği hizmetleri kamuoyuna açmalıdır.

- TÜBİTAK, açık erişim ve açık veri konusunda aktif ve örnek bir kurum olup aynı zamanda yönlendirici ve teşvik edici bir kurumdur. Bu konuda da verdiği teşvikleri artırmalıdır. "Açık büyük verilerin kamuya açılması, mahremiyetinin sağlanması", gibi konuları desteklemeli ve bunları öncelikli alanlar içerisinde almalı ve teşvik etmelidir.
- Dünyada ve özellikle AB'de yapılan çalışmalar, yayımlanan raporlar, ilgili standartlar, iyi örnekler ve elde edilen tecrübelerden mutlaka faydalanılmalı, yapılan çalışmalar yakından izlenmeli, ve son yıllarda yayımlanan ülke stratejilerimiz ve eylem planlarımızda dikkate alınarak, çalışmalar titizlikle yürütülmeli ve açık veri paylaşım portalları hizmete açılmalıdır.
- Ülkemizde UDHB sorumluluğunda olan 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planında Açık ve Büyük Veri ile ilgili olarak yer alan hususlar kısa sürede hayata geçirilmeli ve sorumlu kurumlar, kısa sürede açık veri portallarını oluşturarak kamuoyuna verilerini açmalıdır.

- Açık verinin ülkede bir dönüşüm ve değişim oluşturacağı, ülkenin geleceği ve toplumun gelişimi için bunun mutlaka yapılmasının gerekli olduğu, özellikle ülkemizin yaşadığı talihsiz darbe girişiminin olumsuz etkilerinin kısa sürede atılmasına ve güven duygusunun artmasına da katkılar sağlayacağı değerlendirilmektedir.
- Bu yazının başında da tanımlandığı gibi açık veri felsefesini anlamaya, ülke olarak bunun getirilerinin farkında olarak bu fırsattan faydalanılmaya çalışılmalıdır. Devletlerin şeffaflaşması, işbirliklerinin artması, güven duygusunun gelişmesi ve en önemlisi bu verilerden yeni çıktılar ve değerler üretilmesi, gelecek için önemli adımların başındadır. Ülke bilgi toplumu ve ekonomisinin oluşturulması ve bu ekosistemin kurulması artık bir zorunluluktur. Bunun farkında olunmalı, tehditlerin fırsata dönüştürülmesi için önlemler alınmalı ve çözümler geliştirilmelidir.
- Ülkemizde açık verilerin paylaşımı konusunda daha işin başında olduğumuz bilinse de, e-devlet strateji ve eylem planına sahip

olmamız, eylem planında belirli takvimlerin bulunması, belirtilen hususların bu belgelerde yer almasının önemli olduğu, bu strateji kapsamında çalışmaların 2019 yılına kadar tamamlanacak olması önemli olup bunun fırsata dönüştürülmesi de şarttır.

- Ülkemizde kişisel verilerin korunması konusunda kanunumuzun yayımlanması önemlidir. Bu hassasiyet dikkate alınarak, ülkenin gelişimine katkı sağlayacak ve yapılacak olan arge çalışmalarının önünü tıkamayacak akılcı çözümlerin geliştirilmesi yönünde yönetmeliklerin çıkarılması faydalı olacaktır.
- Dünya ülkeleri değerlendirildiğinde, gelişmiş ülkelerin kamu verilerini anonimleştirdiği ve kamuoyuna açtığı, üniversitelerin ve araştırma kurumlarının bu verilerden değer elde etme, yeni fikirler ortaya çıkarma, ve çıktıların ekonomik değere dönüştürülmesinde önemli adımlar attıkları, bunun ekonomisini oluşturdukları, dolayısıyla bundan beklenen kazançları elde ettikleri, ama en önemlisi tüm bu işleri kişisel verilerin korunmasına saygı göstererek yaptıkları görülmüştür. Mutlaka bu örneklerden faydalanılmalıdır. Dünya çözümleri dikkate alındığında ise, anonimleştirme için yeteri kadar metot ve metodolojilerin bulunduğu, oluşabilecek ihlaller konusunda çalışmaların yapıldığı, bu alanda yöneticileri ikna edecek gerek akademik çalışmaların gerekse ticari ürünlerin mevcut olduğu, bu birikimlerden de faydalanılması ve gerekli adımların vakit geçirmeden atılması gerektiği değerlendirilmektedir.
- Ülkemizde kamu ve özel sektör verilerinden değer elde etmek için, kurum ve kuruluşların ortak veri platformları oluşturmak için buna zaman, emek ve kaynak ayırmaları gerektiği, kurumsal verilerin kamunun ortak değeri olduğunun bilinciyle, ülke ve kişisel verilerin mahremiyetinin de ihlal edilmeden, gerekli protokoller çerçevesinde büyük verilerin hem işlenip hem de paylaşılabileceği, bu verilerden değer elde edilerek kamu zararlarının önüne geçilebileceği, yeni fırsatların oluşturulabileceği, yeni fikirlerin geliştirilebileceği bilinmeli ve bu konuda gerekli adımlar atılmalıdır.
- Ülkemiz mevzuatlarında belirtildiği gibi açık veri konusunda gerekli adımlar atılmış olsa da bunun mevzuatının da oluşturulması için gerekli düzenlemelerinin yapılarak açık verilerin üretilme-

si ve kullanımının önündeki engellerin kaldırılması gerekmektedir. Açık veri ortamlarının ve platformlarının oluşturulmasında Başbakanlığın "Açık Veri Paylaşım Portalının Oluşturulması" ve "Kamu Verilerinin Açık Veriye Dönüştürülmesi ve Paylaşılması" adımlarının kısa sürede tamamlanması ve üniversite ve araştırma kurumlarının, yurtdışı açık veri portallarından aldıkları verilerle analiz yapmalarının önüne geçilerek insan kaynaklarımızın verimli ve ülke için kullanılmasının önünü açmaları, ülkemizin verilerinden değer elde edilerek ülkenin kalkınmasına ve sektörün gelişiminin ve önündeki engellerin kaldırılması beklenmektedir.

- Büyük veri ile ilgili olarak ülkemizde çalışmaların 2013 yılında başladığı, ticari şirketlerin desteğiyle bu konuda seminerler düzenlendiği fakat daha sonra üniversitelerin bu konuya önem vererek, yeni programlar açmaya başladıkları, büyük veri analiz merkezleri kurdukları, bu konuyu tartışmaya açtıkları bilinmektedir. Bu konuda ülkemizde Büyük Veri Analitiği, Güvenliği ve Mahremiyeti Kamu Çalıştayı ve bu çalıştay sonucunda yayımlanan Çalıştay Sonuç Bildirgesi bu konudaki en önemli dokümandır. Bu dokümana www.bigdatacenter.gazi.edu.tr adresinden erişilebilir. Son yıllarda yapılan konferansların, çalıştayların artması, bu konudaki hem bilgi birikiminin arttığını hem de bu konunun ciddiyetle ele alınıp gerekli çözümlerin sağlanacağını göstermektedir. Bu etkinliklere örnek olarak www.acikveriturkiye.org, www.ubmk.org verilebilir. Ülkemizde büyük veri alanında son yıllarda yapılan akademik çalışmaların belirli bir olgunluğa geldiği görülse de açık veri konusunda ise yapılan çalışmaların, içerik ve derinlik olarak yeterli seviyede olmadığı değerlendirilmektedir. Bu konuya daha çok önem verilmeli ve akademik çalışmalar yapılmalıdır.
- Ülkemizde de verilerin gelecekte değerlendirilmesi için bu verilerin şimdiden depolanmaya başlanması gerekmektedir. Bunlar için devlet uygun veri merkezleri kurmalı ve desteklemelidir. Bu verilerin kamu verileri olabileceği gibi özel şirketlerin de verileri olabileceği unutulmamalıdır. TÜİK'in tuttuğu istatistikler, bakanlıkların, ilgili birimlerin ve belediyelerin gözlem verileri, ulaşım verileri, uçuş verileri, eğitim verileri, finans ve sözleşme verileri, savunma sanayi verileri, yer/mekan verileri, uzay ve

uydu verileri, sigortalama verileri, küresel kalkınma verileri, akıllı ev verileri, kamu planlama verileri, inşaat sektör verileri, su ve orman verileri, hesap verebilirlik ve demokrasi ile ilgili veriler, akademik dergi yayınları, sağlık verileri, bilim ve araştırma verileri, toplumsal hareketlilik ve kalkınma verileri, altyapı verileri, trafik verilerinin açık olarak kullanılabileceği düşünülmeli ve buna göre hareket edilmelidir.

- Verileri açık erişime açmak, bunlardan değerler elde etmek, bu verileri bilgiye veya özbilgiye dönüştürebilmek önemli adımlar olsa da, bu verilerin kamu malı olması sebebiyle, hem güvenliğinin sağlanması hem de mahremiyetine helal gelmemesi için de gerekli önlemlerin alınmasının çok önemli olduğu hiç unutulmamalı, gereken önlemler alınarak verilerin ihlal edilmesinin de önüne geçilmesinin hem bir yasal sorumluluk hem de ülke için çok stratejik olduğu da asla unutulmadan işlemler yapılmalı ve yürütülmelidir. Bunun için verilerin oluşturma, belgeleme, erişim, kulanım, paylaşım, depolama ve yedekleme, mülkiyet hakkı, güvenlik ve mahremiyeti gibi hususlar dikkate alınarak bir strateji ve politika kapsamında yönetilmesi, bunun içinde ulusal ve uluslararası standartlarından faydalanılması gereklidir.

- Devletlerin şeffaflaşması, işbirliklerinin artması, güven duygusunun gelişmesi ve en önemlisi açık verilerden yeni çıktılar ve değerler üretilmesi, gelecek için önemli adımların başındadır. Ülke bilgi toplumu ve bilgi ekonomisinin oluşturulmasında açık veri yaklaşımı önemli olup, bu ekosistemin kurulması artık bir zorunluluktur. Açık veri yaklaşımlarının bir tehdit olarak görülerek hayata geçirilmemesi veya bunun geciktirilmesi engellenmelidir. Mevcut tehditlerin giderilmesine yönelik üniversite-kurum işbirlikleri yapılmalı, bu tehditler azaltılmaya çalışılmalı, tehditler fırsata dönüştürülmeli ve bu yazıda belirtilen hususlarda dikkate alınarak yeni çözümler geliştirilmelidir. Diğer bir ifadeyle, felsefenin anlaşılması, ülke olarak bunun getirilerininde farkında olunması, bu yeni yaklaşımlardan faydalanılması gereklidir.
- Açık veri yaklaşımlarının özellikle inovasyonu teşvik edeceği, kurum ve birimlerin etkinliğini artıracağı, yeni ve farklı görüş-

leri ortaya çıkaracağı ve ekonomik kalkınmayı da teşvik edeceği unutulmamalıdır.

- Prof. Fisk, "büyük etkinin ancak ve ancak büyük fikirler ve büyük veri ile sağlanabileceğini" belirtmektedir. Ülkemizde de bu fırsatlar görülmeli ve vakit geçirmeden gereken adımlar atılmalıdır. Verilerin "ülkelerin sayısal toprakları olduğu ve bu verilerin işlenerek değere dönüştürülmesi" gerektiği unutulmadan, ulusal verilerimizin boyutunu büyütmek, yeni değerler elde etmek içinde verilerin içeriğini geliştirmek ve zenginleştirmek zorundadır.
- Bu çalışmalarda önemli adımlardan birisi, bir sonraki adımı kamu kaynakları ile üretilen araştırma verilerinin açık erişim standartlarına uygun biçimde paylaşımı veya kamuya açılması olacaktır. Konulan uzun dönemli hedef ise bu ulusal akademik arşivde bilimsel çalışmalarını paylaşmak isteyen ülkedeki tüm kamu ve özel sektör kuruluşlarını, kurulacak olan ortak paylaşım platformlarına almak ve kamuya açmaktır.

Son olarak, ülkemiz bilim insanlarının ülke problemlerine odaklanması için büyük açık verilerin akademisyenlere ve araştırmacılara açılması gereklidir. Bu sayede sadece siber güvenlik alanında değil diğer alanlarda da gerçek problemlerin çözümüne daha çok ve doğrudan katkılar sağlanabileceği değerlendirilmektedir.

Kaynaklar

Ş. Sağıroğlu, Büyük ve Açık Veri Türkiye, BTHaber, Nisan 2017.

Hibrit Savaş Kapsamında Siber Savaş ve Siber Caydırıcılık

BÖLÜM 7

Mustafa ŞENOL

HİBRİT SAVAŞ KAPSAMINDA SİBER SAVAŞ VE SİBER CAYDIRICILIK

Bu bölümde; savaşın tanımlanması, çeşitleri ve evrimi kısaca incelenmiş, hibrit savaşın tanımı, süreç ve uygulamaları üzerinde durulmuş, hibrit savaşın uygulama yöntemlerinden birisi olan siber savaşın hibrit savaş içerisindeki yeri ve bu konuda gelişmeler gözden geçirilmiş, özellikle siber saldırılara karşı koymak maksatlı siber uzayda saldırganların istek ve amaçlarından vazgeçirilmesine yönelik siber caydırıcılığın önemi açıklanarak yapılan bazı çalışmalar ile uygulamalar özetlenmiş, son olarak da konularla ilgili görüş ve önerilerde bulunulmuştur.

7.1. Giriş

Arapça "Harp" sözcüğünün Türkçe karşılığı olan "Savaş", Türk Dil Kurumu (TDK) Sözlüğünde "Devletlerin diplomatik ilişkilerini keserek giriştikleri silahlı mücadele" [1] şeklinde tanımlanmaktadır. Diğer sözlüklerde de benzer ifadelerle tanımlanan ve insanlık tarihiyle yaşıt olduğu düşünülen savaş kavramı, özü aynı kalmak üzere, günümüze çok farklı boyut ve evrelerden geçerek gelmiş, günümüzde devam etmekte ve gelecekte de farklı şekil ve boyutlarda yaşanmaya devam edecektir.

Yapılan hesaplamalara göre, MÖ 3600 yıllarından MS 2000'li yıllara 1500'den fazla savaş olduğu, geçen süre içerisinde yaklaşık ise sadece 300 yılın savaşsız ve barış içerisinde geçtiği iddia edilmektedir [2]. Bu iddia bir hesaplamaya dayanmadığı veya elde bir belgeye dayalı kanıt bulunmadığı için, barış içerisinde geçen süre toplamının, yapılan savaşlar dikkate alındığında belki daha da kısa olabileceği değerlendirilmektedir.

Kişilerin yaşamları mücadeleler içerisinde geçerken, toplumların ve devletlerin yaşamı da savaşlar içerisinde geçmekte, ulusların tarihi

savaşlarla başlamakta, devletler savaşlarla kurulmakta ve yine savaşlarla da son bulmaktadır. Bu açıdan bakıldığında yaşadığımız dünyada insanlık tarihi bir savaş tarihidir. Bu nedenle savaşlar anlaşılmadan geçmişi, insanlığı ve dünyayı anlamak zor olduğu gibi, geleceğe yönelik tanımlamalarda ve öngörülerde bulunmak da zor olmaktadır. Bunu kolaylaştırmak ve gelecekle ilgili sağlıklı öngörülerde bulunabilmek, geçmişe ait verilerin incelenerek değerlendirilmesine ve belli sonuçların çıkarılmasına bağlıdır.

Tarihte İlk Çağ döneminde kabileler arası çatışmalardan oluşan savaşların, Orta Çağ döneminde şehir devletleri özel orduları arasında yapılan silahlı bir mücadeleye dönüştüğü, Yeni Çağdan başlayarak ise savaşların ulusal devletlerin ordularıyla hükümdarların mücadelesinden ulusların bütüncül savaşına dönüştüğü, kesin sonuçlu ve yıkıcı bir özellik kazandığı görülmektedir. Çağlar içerisinde teknolojinin de gelişmesine paralel olarak silahlar açısından bakıldığında, başlangıçta kılıç ve yay gibi kas gücünün kullanılmasını takiben yelkenli araçlarla rüzgâr gücünün kullanımına dayanan savaşların yerini daha sonra ateşli silahlarla buhar gücüne dayanan savaşlar almış, Yakın Çağdan başlayarak araçların daha da gelişmesiyle zırhlı araçların ve uçakların kullanıldığı savaşlara dönüşmüş, son yarım yüzyılda yaşanan savaşlar ise nükleer güce ve bilişim teknolojilerine dayanan, simetrik ve asimetrik araçlarla tekniklerin birlikte kullanıldığı hibrit (karma) özellikler kazanmıştır [3].

Tarihsel süreç içerisinde insanlığın yaşam şartları ve seviyesi teknolojinin gelişmesiyle değişip gelişirken, savaşlar ve savaşlarla ilgili kavramlar da değişmekte ve savaşlar da gelişip çeşitlenmektedir. Bu konuda bir görüş de "Savaşlar sayesinde teknolojinin, teknoloji sayesinde de savaşların geliştiği" [2] şeklindedir. Geçmişe ve günümüze bakıldığında bu görüşü gerçekleyen çok sayıda örnek kolayca görülebilmektedir. Ancak temelde büyük bir değişiklik olmadığı halde, isimlendirme ve kavramlarda değişiklikler olduğu, yeni düşünce ve isimlendirmelerin ise bazen yanlış kullanımlara ve karışıklıklara sebebiyet verdiği görülmektedir.

Tarihte çeşitli büyüklükteki savaşlardan iki büyük dünya savaşı ve soğuk savaş dönemleri ile günümüzde yaşanan çok değişik özellikteki savaşlara, savaş ve barış kavramları arasında değişik düşünceler ortaya çıkmaktadır. Güç kazanma/geliştirme ve çıkar sağlama yarışları arasında belli şartların ürünü olarak ortaya çıkan bu dü-

şüncelerle hibrit savaş, siber savaş ve siber caydırıcılık kavramları ortaya çıkmıştır.

Ortaya konulan düşüncelerden hareketle bu bölümde; öncelikle savaşın tanımlaması ve evrimi üzerinde bazı açıklamalarda bulunulmuş, hibrit savaşın tanımı, süreç ve uygulamaları üzerinde durulmuş, hibrit savaşın uygulama yöntemlerinden birisi olan siber savaşın hibrit savaş içerisindeki yeri ve bu konuda gelişmeler gözden geçirilmiş, daha sonra özellikle siber uzayda saldırganların istek ve amaçlarından vazgeçirilerek saldırılara karşı koymak maksatlı olmak üzere siber caydırıcılığın önemi açıklanarak yapılan bazı çalışmalar ile uygulamalar özetlenmiş, son bölümde de konuyla ilgili görüş, öneri ve değerlendirmelerde bulunulmuştur.

7.2. Savaşın Tanımlanması ve Çeşitleri

İnsanlık tarihinin başlangıcından bu güne, kas gücü ile taş ve ağaçtan silahlardan günümüzün güdümlü ve akıllı mühimmatlarına kadar tarihi şekillendiren yaygın bir eylem olarak gelecekte de devam edecek olan savaşın, uluslararası kabul gören bir tanımı olmamakla birlikte, sözlüklerin dışında temel dokümanlarda, askeri ve stratejik yayınlarda pekçok tanımı bulunmaktadır.

Ünlü stratejist General Clausewitz "Harp (Savaş) Üzerine" adlı eserinde savaşı; "Savaş, düşmanı irademizi kabule zorlamak için bir kuvvet kullanma eylemi ve politikanın başka araçlarla devamıdır." şeklinde tanımlamaktadır [4]. Bu tanımda, politik amaç doğrultusunda aynı zamanda caydırıcılık için güç kullanma ve egemenlik sağlama yanında, devletlerin kalıcılığı ve ulusların gelecekteki güvenliğinin sağlanması düşüncesi de bulunmaktadır.

Birleşmiş Milletler (BM) Antlaşmasına göre devletlerin birbirine karşı BM amaçları ile bağdaşmayacak kuvvet kullanması veya kuvvet kullanma tehdidinde bulunması yasaklanmıştır. Herhangi bir kuvvet kullanma veya silahlı çatışma eyleminin savaş sayılıp sayılmayacağı hususundaki temel ölçüt ilgili devletlerin amacı olarak değerlendirilmektedir. Bu nedenle, savaşan taraflardan herhangi birisinin savaş amacıyla hareket etmesi durumunda, söz konusu silahlı çatışmaların savaş olarak değerlendirilmesi gerekmektedir [5]. Herkes tarafından kabul görmemekle birlikte Devletler Hukukuna

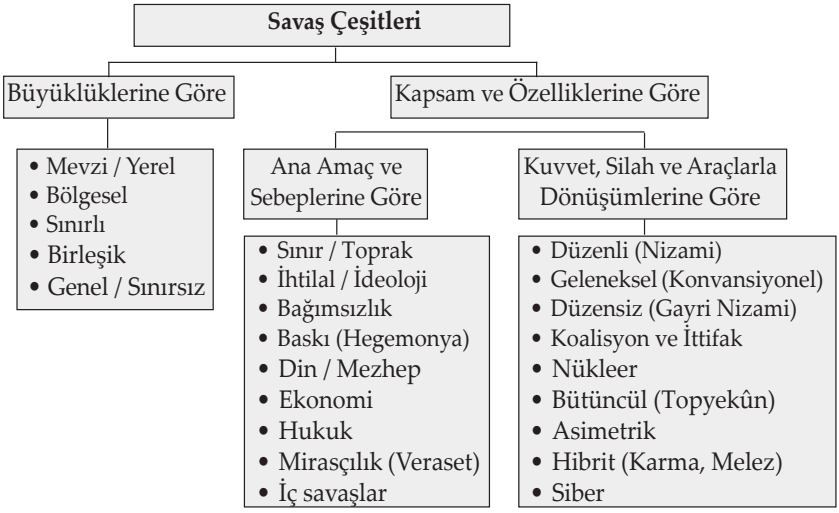
göre savaş; "Bir toplumun, bir ulusun veya devletler topluluğunun isteklerini diğer bir ulus ve devletler topluluğuna zorla kabul ettirmek amacıyla giriştikleri bir mücadele, uluslararası hukuk kurallarına uygun şekilde devletlerarasında yürütülen silahlı bir çatışma, bir çekişme" [6] şeklinde tanımlanmaktadır.

Türk hukukunda, 2941 sayılı Seferberlik ve Savaş Hali Kanunu'nda savaşın tanımı ise; "Devletin bekasını temin etmek, milli menfaatleri sağlamak ve milli hedefleri elde etmek amacıyla, başta askeri güç olmak üzere Devletin maddi ve manevi tüm güç ve kaynaklarının hiçbir sınırlamaya tabi tutulmadan kullanılmasını gerektiren silahlı mücadeledir." [7] şeklinde yapılmıştır.

Savaşın tanımlarında da görüleceği üzere savaşların amaçları, hedefleri, icrası için kullanılan güçler vb. özellikleri değişebilmekte, genellikle ekonomi, politika, teknoloji ve toplumlardaki ortaya çıkan değişimlerin bir araya gelmesi sonucunda da savaşlarda gelişmeler olmaktadır. Geçmişten günümüze yaşanan savaşlar değişen özelliklerine ve gelişmelerine göre de farklı isimler ve terimlerle adlandırılmakta ve sınıflandırılmaktadır.

Bu kapsamda Bilgin Varlık tarafından savaşın tanımlanması konusunda yapılan bir çalışmada savaşlar; büyüklüklerine ve kapsam/özelliklerine göre iki gruba ayrılmaktadır. Birinci grupta; mevzi/yerel, sınırlı, birleşik bölgesel ve genel/sınırsız savaşlar, ikinci grupta ise; "Savaşın Ana Amaç ve Sebepleri" ile "Kuvvet, Silah ve Araçlarla Dönüşümlerine Göre" yapılan savaşlar yer almaktadır [3]. "Hibrit (Karma) Savaş" ikinci grubun, ikinci kısmı içerisindedir. Teknolojinin gelişmesi ve bilgisayarların icadı sonrasında, özellikle internetin de yaygınlaşmasıyla bilgi ve iletişim sistemlerinin insan yaşamının vazgeçilmezleri arasına girmesiyle ortaya çıkan "Siber Savaş" da hibrit savaşla aynı grup içerisinde sınıflandırılabilir. Savaşın çeşitleriyle ilgili olarak, söz konusu çalışmadan da yararlanılarak oluşturulan sınıflandırma Şekil 7.1'de sunulmuştur.

Bazı askeri yazarlar ve stratejistler tarafından savaşların önceki yaşananlar ile kendi içerisindeki değişim ve gelişimlerine göre nesil ya da kuşakları olduğu belirtilmekte, geçmişte yaşananlar ve günümüzde yaşanmakta olanlar bu nesillere göre incelenerek gelecek savaşlara yönelik öngörülerde bulunulmaya çalışılmaktadır.



Şekil 7.1. Savaşların Sınıflandırılması [3].

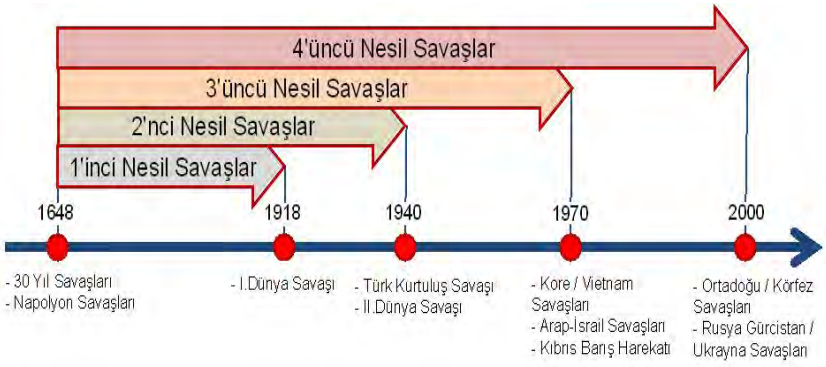
Savaşların nesilleri konusunda bu güne kadar yapılan çalışmalarda 3'lü, 4'lü, 5'li ve 6'lı nesiller şeklinde çözümler ortaya konduysa da, birinden diğerine kökten değişimler içeren dört nesil veya kuşak olarak da adlandırılan sınıflandırma daha yaygın kabul görmüş (Şekil 7.2), ancak savaşın nesilleri ve geleceği ile ilgili öngörüler konusunda tartışmalar devam etmektedir [8]. İki bilim insanı, William S. Lind [9] ve Thomas X. Hammes'in [10] modern savaşları dört nesilde inceledikleri çalışmalarında ortaya koydukları yaklaşımlarında pekçok benzerlikler olmakla birlikte, Dördüncü Nesil Savaşların geleceği konusunda aynı fikirde olmadıkları görülmektedir.

Birinci nesil savaşlar; Birinci Dünya Savaşı öncesinde, tek namlulu yivsiz silahların teknolojide etkin ve yaya unsurlar ağırlıklı kitlesel insan gücünün savaş alanlarında bulundurulmasının ön planda olduğu ve düşmanın yakın gücünün doğrudan yıkılmasına odaklanmış düzenli savaşlardır.

İkinci nesil savaşlar; topçunun savaş alanında ağırlıklı olarak yerini aldığı, ateşin ve ateş destek sistemlerinin yoğun olarak kullanıldığı, kitlesel ateş gücünün etkin olarak kullanılmaya başlandığı, merkezi kontrollü ateş gücü ile piyade, tank ve topçu birliklerinin birlikte kullanıldığı yıpratma stratejisinin benimsendiği, gerilla ve yıkıcı savaş hareketlerinin gelişme oranının kuvvetlendiği Birinci Dünya Savaşı dönemini tanımlamaktadır.

Üçüncü nesil savaşlar; tanklarla mekanize piyade unsurlarının baskın sağlayan hızlarından yararlanmanın topçunun kitlesel ateş gücünün önüne geçtiği, düşmana yaklaşarak onu yok etmek yerine merkezi olmayan kararlarla onu atlama ve mücadele güçlerini çökertme taktiklerinin öne çıktığı, teknolojinin ve özellikle hava gücünün yıkıcı etkisinin kendisini gösterdiği ve nükleer silahların kullanıldığı, düzensiz (gayri nizami) savaş tasarım, teknik ve uygulamalarının yaygınlaştığı ve işgal edilen ülkelerde evrenselleştiği İkinci Dünya Savaşı dönemini tanımlamaktadır.

Dördüncü nesil savaşlar; temel özelliği soğuk savaş döneminden beri uygulanmakta olan ve bugün de hala geçerli bulunan, klasik mücadele anlayışının rafa kaldırıldığı, siyaset ve savaş, sivil ve asker, savaş alanı ve güvenlik alanı, savaş ve barış arasındaki sınırların bulanıklaştığı savaşlardır. Bu dönem geleneksel savaşın yerini devlet ve devlet dışı unsurların birlikte veya devlet dışı unsurların yalnız yürüttükleri düzensiz savaş taktik ve uygulamalarının etkin kullanılmaya başlandığı dönemdir. Savaşlar teknoloji yoğun olarak planlanarak uygulanmaktadır. Bilgi ve iletişim sistemlerinin etkin kullanımı ve ağlar yoluyla karar vericileri etkileme, hedef ülke yöneticilerinin siyasi iradelerini yok etmeye odaklanan siber savaş teknik ve yöntemleriyle propaganda ve psikolojik harekât uygulamaları önem kazanmıştır.



Şekil 7.2. Savaşların Dört Nesil Olarak Tarihi Süreci.

Savaşlar ve eylemlerin alanı genişlemiş, savaş her yerde ve her alanda kendini göstermeye başlamış, beklenmedik durumlarda ortaya çıkan krizlerin yönetimi ve kontrolü zorlaşmıştır. Güçlerin çeşitlili-

ği ve kullanım yöntemleri hibrit savaşların belirgin olarak uygulanmaya başlandığını açıkça göstermektedir. Bu noktada 4'üncü Nesil savaş için bundan sonra nelerin ön planda olacağı konusunda; Lind geleceği asimetrik savaş olarak, Hammes ise bilgi savaşı olarak görmektedir [8]. Ayrıldıkları noktada birleştikleri husus ise; baş döndürücü hızda ilerleyen teknolojinin etkisi ile doktrin değişiklikleri ve belirsizlikleriyle savaşların asimetrik özelliği artarken, geleceğin yapay zekâ, nanoteknoloji ve biyoteknoloji özellikli silah ve araçlarının kullanılmaya başlanmasıyla hem asimetrik etkiler, hem de bilgi savaşlarının etkinliği daha da artacaktır.

7.3. Hibrit Savaş

Dünyada çeşitli askeri ve güvenlik çevrelerinde 2000'li yılların başından itibaren konuşulmaya ve tartışılmaya başlanan hibrit tehditler ve hibrit savaş kavramı, 2014 yılında Rusya - Ukrayna çatışmalarında daha çok ilgi çekmiş, üzerinde daha çok konuşulmaya ve yazılmaya başlanmıştır.

Türkçe karşılığı olarak "Karma", "Birleşik" ve "Melez" sözcükleri de kullanılan, Latince kökenli "Hybrid" sözcüğünden gelmekte olan "Hibrit" kelimesi, TDK Sözlüğüne göre "Melez" ve "İki farklı güç kaynağının bir arada bulunması" [1] şeklinde, İngilizce sözlüklerde ise "İki farklı unsuru birleştirerek yapılan bir şey" [11] olarak açıklanmaktadır. Sözlüklerde açıklanan bu anlamlardan hareket edilerek "Hibrit Savaş" teriminden, düzenli orduyla beraber düzensiz silahlı grupların, askerle beraber sivil halkın, askerî güçle beraber askerî olmayan (ekonomik, sosyal, politik, vb.) imkânların, sıcak çatışmayla beraber şiddet içermeyen yöntemlerin kullanılması amaçlanmaktadır [12].

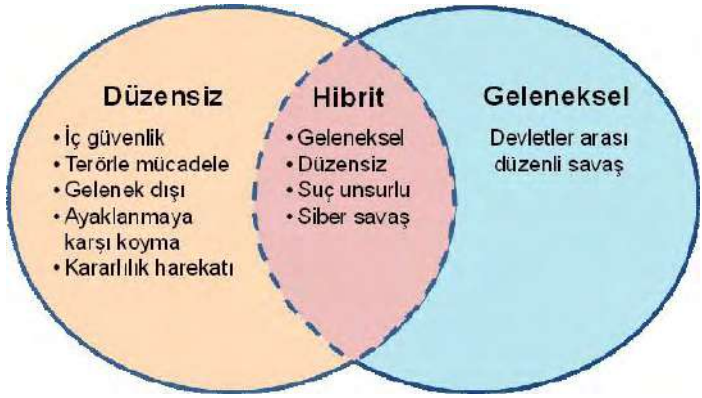
Savaşların kapsam ve niteliklerine göre sınıflandırmasında kullanılan kuvvetler ile silah ve araçların dönüşümü grubunda yer alan, 4'üncü nesil bir savaş olan ve daha da gelişerek 5'nci Nesil Savaş olarak davam edeceği geniş kabul gören "Hibrit Savaş"ın açık tanımı ilk olarak 2007 yılında Frank Hoffman tarafından [13] yapılmıştır. Ancak geçmişten günümüze pekçok farklı tanımı yapılmış olmakla birlikte, ortak bir tanımı ve kullanılmasında henüz genel bir düşünce birliği sağlanamadığı görülmektedir.

Hoffman'a göre; hem devletler hem de devlet dışı çeşitli aktörler tarafından yürütülebilen Hibrit Savaş; içerisinde geleneksel yetenekler, düzensiz taktikler ve oluşumlar, ayrım gözetmeyen şiddet ve zorlama dâhil olmak üzere terör eylemleri ve suç oluşturan düzensizlikler gibi bir dizi farklı faaliyetleri barındıran bir savaş biçimidir. Bu çok yönlü farklı faaliyetler, ayrı birimler veya etkin güç yaratabilmek için harekât alanında taktik veya operasyonel olarak yönetilen ve koordine edilen aynı birim tarafından da gerçekleştirilebilir.

ABD Savunma Bakanlığınca 2010 yılında yapılan inceleme ve değerlendirme sonucunda; kapsadığı çatışmaların artan karmaşıklığını tanımlamak için "Hibrit (hybrid)" teriminin kullanılması uygun bulunmuş, hibrit savaşın bir savaşın bütün özelliklerini taşıdığını ancak yeni bir savaş çeşidi sayılamayacağı, ABD Silahlı Kuvvetleri tarafından son derece uyarlanabilir, esnek ve kullanılabilir olduğu kabul edilmiştir [14]. Aynı değerlendirmede hibrit tehditler ve hibrit savaş tanımları konusunda faklı görüş ve tartışmaların devam ettiği vurgulanarak, resmi bir tanım yapılmamış, Kuzey Atlantik Antlaşması Örgütü (NATO)'nün hibrit savaş ve tehditlerle ilgili kabul ettiği tanıma atıfta bulunulmuştur.

NATO'nun Stratejik Planlama ve Kavramlar Çalışma Grubu'nca Şubat 2010'da "Hibrit tehditler; devlet, devlet dışı ve teröristler de dâhil olmak üzere mevcut veya potansiyel rakiplerin, hedefleri doğrultusunda geleneksel ve geleneksel olmayan araçların eşzamanlı olarak kullanılmasının mümkün olup olmadığı ile bağlantılıdır." şeklinde tanımlanmıştır. ABD Savunma Bakanlığı yetkililerince yapılan incelemelerin ve akademik belgelerin analizi sonucunda, hibrit savaşın, geleneksel - düzenli ve geleneksel olmayan - düzensiz savaşlarla ilgili tüm çatışmaların unsurlarını kapsadığı vurgulanan ve Şekil 7.3'te belirtilen yaklaşım benimsenmiştir.

Bu kapsamda hibrit tehditler devlet ve devlet dışı güçleri de içeren, çok yönlü ve düşük yoğunluklu uluslararası barış ve güvenlikle ilgili tehditler arasında yer alan siber savaş, asimetrik çatışma senaryoları, küresel terörizm, göç, yolsuzluk, etnik çatışmalar, korsanlık, uluslararası organize suçlar, kaynakların güvenliği, küreselleşmeden ve kitle imha silahlarının çoğalmasından kaynaklanan geri dönüşler gibi çok çeşitli mevcut olumsuz koşul ve eylemleri kapsayan şemsiye bir terimdir [15]. Bu tür tehditlerle ilgili çalışmalar, rastlantısal olarak ortaya çıkan olayların aksine, uzun vadeli hedefler şeklinde planlanıp uygulamaya konularak sabırla icra edilirler.



Şekil 7.3. Hibrit Savaşın Temel Oluşumu.

Devletlerden veya devlet dışı çeşitli oluşumlardan gelen hibrit tehditlerle uygulanan hibrit savaşın unsurları; devlet özelinde bulunan geleneksel, yasal, sivil ve askeri güçler (düzenli askeri birlikler, özel kuvvetler, ekonomik, diplomatik vb. milli güç unsurları) ile devlet dışı oluşumlardan (geleneksel olmayan ve düzensiz askeri güçler, siber savaş, bilgi savaşı, psikolojik savaş, isyancılar, teröristler, organize suç örgütleri, özel askeri güvenlik unsurları vb.) meydana gelmektedir. Şekil 7.4'te hibrit savaşta kullanılabilecek güçler ve oluşumlar görülmektedir.



Şekil 7.4. Hibrit Savaşın Güçleri ve Destekleyen Oluşumları.

Hibrit savaşta asıl amaç ya da hedef; bir bölgeyi ele geçirmek veya kontrol etmek olmayıp, uygulayan tarafın elindeki bütün olanaklarını kullanarak istenilen etkileri oluşturmak, karşı tarafın siyasi yönetimini ve devlet kurumlarını kararsız ve dengesiz hale getirmek, yönetim boşluğu oluşturmak ve kargaşa yaratmaktır. Bu amaç içinse hedef ülkenin ulusal güç unsurlarından özellikle zayıf olanlar seçilerek daha da zayıflatılmaya ve yok edilmeye çalışılır.

Hibrit savaşın en belirgin özelliğinin düzensiz savaş taktikleriyle yüksek teknolojinin birleşimi olduğunu belirten Frank Hoffman'ın, Sınırsız Savaş, Birleşik Savaş ve 4'üncü Nesil Savaş kavramlarının hibrit savaşın temelini oluşturduğunu ve ona yön verdiğini vurgulaması [13] bazı sivil/asker yazarlar ve akademisyenler tarafından eleştirilmekle birlikte, konuyla ilgili çalışmalar, yapılan tespit ve değerlendirmeler ile yakın geçmişte ve günümüzde yaşanan savaşlar onu doğrulamaktadır. Başlangıçta, 2006 yılında Lübnan savaşında Hizbullah'ın İsrail'e karşı uyguladığı ve başarılı olduğu geleneksel ve düzensiz taktiklerin karışımı stratejiyi tanımlamak amacıyla kullanılan [16], 2014 yılında Rusya'ın Ukrayna'nın doğusunu ve Kırım'ı işgal etmesiyle daha da önemsenerek tartışılmaya başlanan [17] "Hibrit Savaş"ın tarihte pekçok örnek uygulamasının olduğu görülmektedir.

1806 yılında İngiliz ve Portekiz ordusu ile düzensiz İspanyol güçlerinin Napolyon liderliğindeki Fransız ordusuna yönelik gerçekleştirdikleri etkili eylemleri, Birinci Dünya Savaşında İngilizlerin Osmanlı Devletine karşı yürüttükleri savaşın bir parçası olarak 1914 yılında Arapların Türklere karşı ayaklanması ve Osmanlı için felaket olarak nitelenebilen girişimler, İkinci Dünya Savaşında doğu cephesindeki Sovyet Ordusunun düzensiz halk güçleri ile birlikte Alman ordu birliklerine karşı başarılı muharebeleri, 1965-1973 yılları arasında Kuzey Vietnam'ın düzenli Halk Ordusu ile Vietnam Ulusal Kurtuluş Cephesinin düzensiz güçlerinin müşterek olarak Fransa ve ABD'ye karşı başarılı çatışmaları hibrit savaşın belirgin örnekleridir. Ayrıca 1979-1990 yıllarında Sovyet düzenli ordularının işgaline karşı direniş hareketi ve sonrası yıllarda Afganistan'da, 1994-1996 yıllarında Çeçenistan'da, 1990 sonrası Irak'ta, 1999-2001 yıllarında Bosna-Hersek ve Kosova'da, 2007'de Estonya'da ve 2008'de Gürcistan'da yaşananlar ile 2010 ve 2011 yıllarında Tunus, Yemen, Mısır ve Libya'da yaşanan "Arap Baharı" olayları ve

2011'den beri Suriye'de yaşananlar Hibrit Savaş uygulamalarıyla doludur. Özellikle Suriye'de yaşanan olaylar nedeniyle göçe zorlanan ve Türkiye'de günümüz rakamlarıyla 4 milyona yaklaşan Suriyeli göçmenlerin planlı bir hibrit savaş sonucu olduğu unutulmamalıdır. Ayrıca; 40 yıla yakın süredir PKK Bölücü Terör Örgütü'nün Türkiye'deki faaliyetleri ile Irak ve Suriye'de DAEŞ ve PYD/YPG/PKK gibi radikal terör örgütlerinin kullanılması ve onlara gizli ya da açık lojistik ve istihbarat ile psikolojik destek verilmesi olayları hibrit savaş uygulamalarının açık örnekleridir.

Tarihsel süreç içerisinde, özellikle son yıllarda yaşanan hibrit savaş örnekleri incelendiğinde, hedefleri üzerinde asimetrik etkiler yaratabilmek için terörizm dâhil her türlü insanlık dışı eylemleri de içeren ve "örtülü" ya da "kirli" olarak da adlandırılan bu uygulamalara, genellikle bölgesel veya uluslararası alanda gücü ve etkinliği azalan ve yeniden güç kazanmak isteyen devletler ile gücünün zirvesinde olan devletler tarafından başvurulduğu görülmektedir. Yapılan istatistiklere göre, son yıllarda dünyada yer alan savaşların sadece yüzde 10'unun devlete bağlı düzenli ordular arasında gerçekleştiği, geri kalanının terör unsurları, ne olduğu belirsiz devamlı isim değiştiren silahlı gruplar ve sanal askerlerin işleri olduğu anlaşılmaktadır [18].

Bu tür devletlerin hibrit savaşı tercih etmelerinde ise başlıca iki temel neden gözlenmektedir [19]. Bunlardan ilki ve ana nedeni, BM şatları (güç kullanma yasakları ve zorunluluklar) ve uluslararası anlaşmalar nedeniyle yaptırım ve kısıtlamalardan kaçarak amaçlarına gizli ve dolaylı yollardan ulaşmaktır. İkinci neden ise hedef ülkeye müdahale veya amaçlarını gerçekleştirmek için yasal gerekçesi olmayan devletler tarafından asimetrik etki sağlamak ve bölge halkının direnç oluşturmasının da önüne geçerek her bakımdan daha ekonomik ve maliyeti düşük yolların sağlanmasıdır.

Bu düşünceler çerçevesinde, hibrit savaşın en somut örneklerinden birisi olarak geniş kabul gören, Rusya ve Ukrayna arasında 2014 yılı içerisinde yaşanan olayları kısaca özetlemekte yarar bulunmaktadır.

Rusya'nın 2010 Askeri Doktrini'nde modern savaş; "askeri gücün ve askeri olmayan bir karakterin güçlerinin ve kaynağının bütünleşik olarak kullanılması" ve dünya toplumunun daha sonra askeri gücün kullanılmasına yönelik olumlu bir cevabını şekillendirmek

amacıyla. "askeri güç kullanılmadan politik hedeflere ulaşmak için bilgi harekâtı yöntemlerinin uygulanması" olarak tanımlanmıştır. 2014 yılında askerî harekâtlara düzensiz silahlı güçler ile özel askerî şirketlerin katılımı, harekâtlarda dolaylı ve asimetrik çatışma yöntemlerin kullanılması şeklinde güncellemeler yapılmıştır. Rusya Genelkurmay Başkanı General Valery Gerasimov tarafından yazılan ve "Gerasimov Doktrini" olarak adlandırılan askerî doktrine göre, savaşın kuralları önemli ölçüde değişmiş, stratejik ve politik hedeflere ulaşma yolunda askerî olmayan unsurların etkinliği daha da artmıştır. Rusya, Şubat 2014'ten itibaren Ukrayna'da iki farklı harekât yürütmüştür. Bunlardan birisi Kırım'ın işgali ve ilhakı, diğeri ise Doğu Ukrayna'nın Donbas Sanayi Bölgesinin işgalidir. Kırım'ın işgali elektronik savaş, sabotaj ve yıkıcı faaliyetler, psikolojik harekât, bilgi savaşı ve baskın sağlayan gizli askerî harekât ile başlamış; hava, kara ve deniz güçlerinden oluşan düzenli unsurların harekâtı ile ilhak tamamlanmıştır [20].

Janis Berzins'e göre; Rus modern savaş doktrininde de belirtildiği gibi, yeni nesil savaş olan hibrit savaşın esas harekât alanı insan aklı, temel araçları ise bilgi savaşı ve psikolojik harekâttır [21]. Bu tespiti doğrularcasına, Rusların Ukrayna'ya karşı Doğu Ukrayna ve Kırım bölgelerinde yürüttüğü harekâtın başarısında en temel etkenler, hibrit savaşın özellikle siber savaş - bilgi savaşı ile bilgi ve iletişim sistemleri üzerinden propaganda ve psikolojik harekât uygulamaları olmuştur.

7.4. Siber Savaş

Bilgisayarların keşfi sonrasında, her geçen gün gelişen bilgi sistemleri ve iletişim teknolojileriyle, özellikle haberleşme, finans, enerji ve güvenlik faaliyetlerinin bilgi sistemleri üzerinden yürütülmesi sonucu bilişim sistemleri günlük yaşamın vazgeçilmez bir parçası olmuştur. Bilginin, elektronik ve bilişim sistemlerinin sağladığı imkânlarla üretildiği, daha etkin işlendiği, iletildiği, muhafaza edildiği ve kullanıldığı "Siber Uzay" ya da "Siber Ortam" konuşulmaya başlamış ve bu ortamın öneminin her geçen gün daha da arttığı görülmüştür [22].

Siber ortamda bilgilere ve bilişim sistemlerine yönelik başlayan kötü niyetli hareketlere ve saldırılara karşı bilginin ve bilgi sistemlerinin korunması, karşı tarafın bilgilerine ve bilgi sistemlerine zarar verilmesi veya olumsuz etkilenmesi olayları ile birlikte "siber

güvenlik" ve "siber savaş" kavramları ortaya çıkmıştır [22]. Siber ortamda sahip olunan imkân ve kabiliyetlerin, sadece siber alanda değil, özellikle diplomasi ve askeri alanlarda "caydırıcılık" sağlamak maksadıyla da kullanıldığı görülmüştür.

Siber ortam, sanal ortam, sayısal ortam, bilgi ortamı vb. terimlerle de adlandırılmakta olan ve geçen yıllar süresince pekçok tanımının yapıldığı görülen "siber uzay"; kısaca "bilgisayar ağları üzerinde sayısallaştırılmış bilginin iletildiği düşünsel ortam", geniş kapsamlı olarak da "bilgisayar ve füzelerden, güneşten gelen ışınlara kadar elektronik ve elektromanyetik görüngenin kullanımı ile karakterize edilen alan" [23] şeklinde tanımlanmaktadır.

Türkiye 2016-19 Ulusal Siber Güvenlik Stratejisi Belgesinde siber uzay; "tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan veya bağımsız bilgi sistemlerinden oluşan sayısal ortam" [24] olarak tanımlanmıştır.

Tanımlar incelendiğinde siber uzayın fiziksel ve sanal olarak iki birleşik yapıdan oluştuğu görülmektedir. Fiziksel yapı, sayısal elektronik cihazları, bilgisayarları, akıllı telefonları, akıllı nesneleri, algılayıcıları ve duyargaları, uydu sistemlerini ve internet dâhil bütün bilgisayar ağlarını içeren her türlü bilgi ve iletişim sistemlerini ve kullanıcılarını kapsamaktadır. Sanal anlamda ise, fiziksel ortamdaki işletim sistemleri başta olmak üzere yazılım ve kodlar ile üretilen, depolanan, iletilen ve çeşitli maksatlarla kullanılan her türlü verileri ve bilgileri kapsamaktadır.

Teknolojik gelişmeler sonrası içinde yaşadığımız bilgi çağında, elektronik, bilgi ve iletişim sistemleri ile hayatımızın, beynimizle sinir sistemimizin vücudumuzda olduğu gibi, en önemli parçalarından birisi haline gelen siber uzay; saldırılar, suçlar, terör olayları ve savaş gibi pekçok tehlikeyi de üzerinde barındırmakta, bu tehlikeler de her geçen gün çeşitlenerek artmaktadır.

Kazanç sağlamak veya zarar vermek maksatlarıyla siber uzayda belirlenecek hedef ya da hedeflere yönelik gerçekleştirilecek faaliyetler siber saldırıları oluşturmaktadır. ABD Ulusal Araştırma Konseyi tarafından, 2009 yılında yapılan bir çalışmada siber saldırılar "bilgisayar sistemleri, ağlar veya bilgiyi ve/veya bunlarda yerleşik olan ya da bunları taşıyan programları bozmak, aldatmak, küçük

düşürmek veya yok etmek için yapılan kasıtlı hareketler" [23] olarak tanımlanmıştır.

Siber saldırılar, siber ortamdaki fiziksel veya sanal yapıyı, yazılım, donanım ve alt yapı sistemlerini, genellikle de bu sistemler üzerindeki bilgiyi ve kullanıcıları hedef almaktadır. Saldırganlar bilgiyi ve kullanıcıları hedef alarak eylemlerini gerçekleştirirken temel olarak üç prensibe göre hareket etmektedirler. Bunlar, gizli bilgilerin elde edilmesi veya bilginin gizliliğinin açık edilmesi, bilgiye zarar verilerek değiştirilmesi yani bütünlüğünün bozulması ve bilgiye kullanıcıların erişiminin engellenmesi yani kullanılabilirliğinin önlenmesidir. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı belgesinde bu üç prensipten hareketle siber saldırıların tanımı, "ulusal siber uzayda bulunan bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın her hangi bir yerindeki kişi ve/veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemler" [24] şeklinde yapılmıştır.

Başlangıçta klasik suç tanımına uymayan ve bilgisayar veya bilişim suçları olarak ifade edilmeye başlanan suçlar, bilgisayarın iş hayatında ve internetin yaygınlaşarak sosyal hayatta da kullanılmasıyla birlikte siber suçlar kavramı ile ifade edilmeye başlanmıştır. Genel olarak, "bilgisayarların kötüye kullanılması, bilgileri otomatik işleme tabi tutulmuş ve verilerin nakline ilişkin kanuna ve meslek hayatına aykırı davranışlar" [26] şeklinde ifade edilen ve uluslararası bir konu olan siber suçlar, BM 10'uncu Kongresinde (2000) bilişim sistemi güvenliğini/veri işlemini hedef alan, bilişim sistemi/ağı marifetiyle gerçekleşen kanun dışı eylemler" [27] şeklinde açıklanmıştır.

Avrupa Konseyi Siber Suçlar Sözleşmesinde (2004) ise; yetkisiz erişim, sisteme ve veriye müdahale, bilişim sistemi aracılığıyla sahtekârlık ya da dolandırıcılık suçları yanında, bilgisayar ve veriye yönelik fiillere ilave olarak, bilişim sistemlerinin kullanılmasıyla ve özellikle internetin yaygınlaşması ile birlikte niceliksel olarak ortaya çıkan çocuk pornografisi, telif haklarına ilişkin ihlaller, yabancı düşmanlığının ve ırkçılığın önlenmesine ilişkin hükümler de siber suç kapsamına alınmıştır [28].

Teknolojinin gelişmesine paralel olarak, teknolojik araçlar ve bilişim sistemleri terör unsurlarınca her geçen gün daha yaygın kullanılır

olmuştur. Siber uzay ile terörizm sözcüklerinin birleşiminden oluşan siber terörizm, en basit şekilde, terör gruplarının siber ortamı kullanarak terör faaliyetlerini gerçekleştirmeleri şeklinde açıklanabilir.

Günümüzde özellikle modern terör örgütlerinin, örgütlerini yapılandırmak, eleman temin etmek, amaçları doğrultusunda organizasyon ve eylemlerini planlayarak gerçekleştirmek maksadıyla bilişim teknolojilerini yaygın olarak kullandıkları, kamu ve özel kurumların bilişim sistemlerine yönelik siber saldırı faaliyetleri gerçekleştirdikleri görülmektedir.

Ancak uluslararası ortamda, terörizmin tanımı olmadığı gibi, siber terörizmin de kabul görmüş ortak bir tanımı bulunmamaktadır. Siber terörizmin genel bir tanımı; politik veya sosyal hedefleri gerçekleştirmek, devleti ve vatandaşlarını korkutarak, aşağılayarak, baskı oluşturarak etkilemek ve hükümet politikalarını değiştirtmek maksadıyla, bilgisayarlara, ağ sistemlerine, veri tabanlarına bilişim teknolojisi kabiliyetlerini kullanarak yapılan yasadışı tehdit ve zarar verici saldırılar [28] şeklinde yapılmaktadır. Tanımdan da anlaşılacağı üzere, siber terör olaylarında, silah olarak bilişim sistemleri kullanılarak, hedef olarak kişilere, kurumlara veya devlete ait bilgisayar ve iletişim sistemleri alınarak yapılan siber saldırılar, korku ve şiddet içermesi yanında, can ve mal kaybına da sebep olabilmektedir.

Günlük yaşamda saldırılara, hassas ve değerli varlıklara gelecek her türlü kötülüğe, hasar veya zarara karşı korunma veya karşı koyma derecesi anlamında kullanılan "güvenlik" kavramı TDK sözlüğünde "Toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet" [1] şeklinde açıklanmaktadır. Güvenlik kavramı halk arasında saldırılara karşı koyma anlamına gelen "savunma" kavramı yerine de kullanılmaktadır.

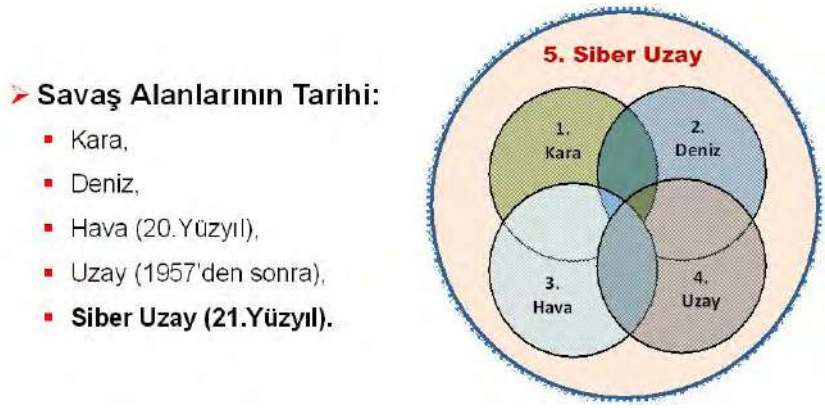
Saldırılarda hedefin merkezinde bilginin olması nedeniyle, başlangıçta "Bilgi Güvenliği" olarak kullanılan kavramın siber güvenliği de kapsadığına dair yaklaşımların olmasına karşın, günümüzde siber ortamın hızlı değişimi dolayısıyla yaşanan olayların da etkisiyle bunun tersinin yaygınlaştığı, siber güvenliğin bilgi güvenliğini de

içerir şekilde kullanılmaya başlandığı görülmektedir. Bu durum, "konuyla ilgili farklı terimlerin ve tanımların ortak temalarından hareketle, siber güvenliğin devlet sırlarının korunması ve ulusal savunmanın sağlaması için temel esas olduğu…" şeklinde NATO Siber Güvenlik Çerçeve Kılavuzu'nda da açıkça vurgulanmıştır [29].

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı belgesinde ise siber güvenliğin; "siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilgi/verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesini" [24] ifade ettiği belirtilmiştir.

Strateji belgesindeki bu tanımlamada görüldüğü üzere, temel amaç bilgiyi korumak ve sistemlerin devamlılığını sağlamak olup, bilgiyi, bilişim sistemlerini ve kullanıcılarını hedef alarak gerçekleştirilen siber saldırılarda kullanılan üç prensip (bilginin gizliliğinin ve bütünlüğünün korunması ve erişilebilirliğinin sağlanması) siber güvenliğin de temelini teşkil etmektedir. Siber saldırı ve olayların tespit edilerek engel olunması ve bilişim sistemlerinin saldırı/olay öncesi duruma döndürülmesi siber güvenliğin temel amaç ve hedefleri arasında yer almaktadır.

Siber ortamın tehlikelerinin farkında olan ülkeler siber güvenliği önemsemekte, siber tehditleri ulusal güvenliğe karşı en önemli tehdit unsurlarından biri olarak kabul etmekte ve başta ülkenin elektronik haberleşme, enerji, su yönetimi, kritik kamu hizmetleri, ulaştırma, bankacılık ve finans sektörleri vb. kritik altyapıları olmak üzere bireylerinin, kurum ve kuruluşlarının varlıklarını siber risklere, tehditlere ve saldırılara karşı korumak için çözümler üreterek uygulamaya koymaktadırlar. Bu konuda gerekli adımları atmayan ülkeler ise geç kalmış demektir. Çünkü başlangıçta küçük çapta ve bir kısmı zararsız denebilecek seviyedeki riskler, tehditler ve saldırılar, teknolojinin gelişmesi ve internetin yaygınlaşmasıyla birlikte, insanoğlunun varoluşundan başlayarak zaman içerisinde kara, deniz, hava ve uzay gibi kendine has özellikleri ve gereklilikleri bulunan dört savaş alanına, 21'inci yüzyıla gelindiğinde, beşinci savaş alanı olarak "siber uzay" (Şekil 7.5) eklenmiştir.



Şekil 7.5. Beşinci Savaş Alanı "Siber Uzay".

Dünya kamuoyu, siber saldırı ve siber suç terimlerine alışırken, özellikle son on-onbeş yıllık zaman süresince siber savaş terimi ile daha fazla meşgul olmaya başlamıştır. İlk yıllarda basit tekniklerle organize olmayan test saldırıları, kısa süre sonra ekonomik güdülerin de öne çıktığı ve komuta kontrol merkezleri aracılığıyla daha gelişmiş teknik ve taktiklerle gerçekleştirilen siber saldırılara dönüşerek, siber savaşa doğru gelişim göstermiştir.

"Bilgi Güvenliği" ile "Siber Güvenlik" kavramlarının iç içe olma durumunda açıklanmaya çalışıldığı gibi, önceleri bilgi savaşının bir alt bölümü olarak görülen siber savaşın, günümüzde bilgi savaşı ile aynı anlamda ve daha yaygın olarak kullanılmaya başlandığı görülmektedir. Nitekim bazı İngilizce sözlüklerde olduğu gibi, BM Terimler Sözlüğünde de "Siber Savaş", "Bilgi Savaşı"nın eş anlamlısı olarak gösterilmekte ve "Bilgisayar sistemlerinin düşman sistemlerine zarar vermek veya yok etme maksadıyla kullanıldığı bir savaş tipi" şeklinde tanımlanmaktadır. Yapılan tanıma ek olarak, "Düşmanın politik, askeri veya ekonomik bilgilerine ve bilgi sistemlerine zarar vermek veya kendi bilgilerini ve bilgi sistemlerini korumak için bilgi üstünlüğü sağlamaya yönelik faaliyetleri kapsayabileceği" [30] belirtilmektedir. Bu tanımlamada dikkat edilmesi gereken husus, "düşman" sözcüğüyle, birbiriyle savaş durumunda olan toplum, ulus veya devlet ya da devletler grubunun ifade edilmesi ve siber savaş kapsamına giren faaliyetlerin de bunlar tarafından icra edilen faaliyetler olmasıdır.

Bu kapsamda siber savaş, "devletler veya devlet benzeri aktörler tarafından gerçekleştirilen, kritik ulusal altyapıları, askeri sistemleri veya ülke için önemli endüstriyel yapıyı tehdit eden, simetrik veya asimetrik, saldırı veya savunma maksatlı dijital ağ faaliyetleri" [31] şeklinde tanımlanırken, hedef, içerik ve özellikleri de ortaya konmaya çalışılmıştır.

Yapılan pekçok tanımdan hareketle siber savaş, siber ortamda bilişim sistemleri kullanılarak bilişim sistemlerine yönelik yapılan saldırılar ile bu saldırılara karşı alınan güvenlik tedbirlerinden oluşan faaliyet ve mücadeleler bütünüdür. Geleneksel (klasik) savaşla kıyaslandığında siber ortamda yapılan saldırılar taarruz, güvenlik tedbirleri ise savunma harekâtına karşılık gelmekte ve her iki harekât türü birlikte siber harekâtı oluşturmaktadır. Siber harekât/savaş sırasında icra edilen siber saldırılar ya da taarruzlar, her ne kadar siber ortamda yapılsa da etkileri ve sonuçları fiziksel ortamda da görülebilmekte, geleneksel savaşta olduğu gibi can ve mal kaybına da sebep olabilmektedir.

ABD'li siber savaş araştırmalarıyla ünlü bilim insanı Martin C. Libicki, siber savaşları amaçlarına, hedeflerine, kapsam ve uygulama seviyelerine göre "Stratejik ve Operasyonel Siber Savaş" olarak ikiye ayırmaktadır. Stratejik Siber Savaş; bir devletin ve topluluğunun, bir devlete ve toplumuna karşı başlattığı, özellikle olmasa da öncelikle hedef devletin tutum ve davranışlarını etkilemek amacıyla başlattığı siber saldırı seferberliğidir. Saldıran taraf devlet veya devlet dışı oluşumlar olabilir. Operasyonel siber savaş, savaş döneminde askeri hedeflere ve askeri bağlantılı sivil hedeflere karşı siber saldırılardan oluşmaktadır. Savaş döneminde siber güç tek başına kullanılmasa da, dikkatli, seçici ve doğru zamanda kullanıldığı takdirde belirleyici bir kuvvet çarpanı olabilir [32].

ABD Savunma Bakanı Leon Panetta'nın 2012 yılında yaptığı konuşmasında, "ABD'nin Siber-Pearl Harbor ihtimali ile karşı karşıya olduğu" sözüyle, benzer hususları belirtmiş ve siber savaşın ulusal güvenlik için büyük bir tehdit olduğunu vurgulamıştır [31]. İnternet ile zaman ve mekân kavramı ortadan kalkmış, kıtalararası iletişim ve bilgi aktarımı herhangi bir zaman ve yerde bir tuşa basmaktan ibaret hale gelmiştir. İnternet aracılığıyla saldırı için küçük bir ağ bağlantısı yeterli olmakta, siber silahları elde etmek de çok

kolay olup, klasik bombalı saldırılardaki gibi "olay yerinde" olma zorunluluğu da bulunmamaktadır.

Bilgisayar ve iletişim sistemlerinde, insanların internetinden nesnelerin internetine, akıllı cihazlardan akıllı evlere/şehirlere, siber uzayda sınır tanımayan ve insanın hayalinde canlandırma sınırlarını zorlayan gelişmeler yaşanmaktadır. İşte böyle bir ortamda, siber saldırı risk ve tehditleri gerçeği ve tehlike boyutu ortadayken, çoğu ülke siber savaşın hem taarruz ve hem de savunma boyutu ile ilgili yasa, politika ve stratejiler üreterek uygulamaya koyarken, siber savaşı küçümseyip bu konuda ciddi çalışmalar içerisinde olmayan ülkeleri çok zor bir gelecek beklemektedir. Çünkü siber savaş gerçektir ve saldırganlar şimdiye kadar gerçek yeteneklerinin ortaya çıkmaması için en gelişmiş siber silahlarını, yani bu konudaki gerçek yeteneklerini, kullanmamışlardır. Tam ölçekli bir siber savaşın yani gerçek yeteneklerin kullanıldığı saldırıların yapıldığı bir savaşın sonuçlarının tahmin edilemeyeceği ve olabileceklerin modern bir ülkeyi mahvedebileceği yorumları yapılmaktadır [25].

Hangi alanda olursa olsun savaşın vazgeçilmezi olan konu istihbarattır. Sun Tzu'nun, "zaferin önceden görülebileceğini, düşmanı ve kendini iyi bilenin hiçbir savaşta tehlikeye düşmeyeceğini, karşısındakini bilmeyen, sadece kendini bilenin bir kazanıp bir kaybedeceğini, karşısındakini de kendini de bilmeyenin her savaşta mutlaka tehlikeye düşeceğini" [33] belirterek önemini vurguladığı İstihbarat; TDK Sözlüğünde "Yeni öğrenilen bilgiler, haberler, duyumlar" [1] şeklinde tanımlanmaktadır.

Zamanla ve günün şartlarına göre değişen, İngilizcede "intelligence" olarak ifade edilen istihbarat aynı zamanda "zeka" anlamına da gelmekte, pekçok sözlükte, kaynak ve dokümanda da faklı şekillerde tanımlanmaktadır. İstihbarat sözcüğünün özünde aklın yanında, "bilgi" bulunmaktadır. İstihbaratın temel hedefi de, ihtiyaç duyulan bilginin akılcı yöntemlerle toplanması, analiz ve değerlendirmesinin yapılması ve zamanında kullanıma sunulmasıdır. Bu ifadelerden hareketle istihbarat; kişi, toplum, kurum, kuruluş, devlet veya devletler topluluğu, her seviyede oluşum açısından, başta güvenlik ve refahın sağlaması için olmak üzere, her maksatla önemlidir.

Ulusal güvenliğin sağlanması, ulusal çıkarların elde edilmesi ve diğer tanımların ortak yönleri de dikkate alınarak genel anlamda istihbarat; "ulusal güvenliği tehdit edecek unsurlara karşı koruma

sağlamak amaçlı yahut politika yapıcıların, ulus menfaatini olumlu şekilde etkileyecek kararların alınması hususunda ihtiyaç duyduğu bilgilerin açık, yarı açık ve gizli kaynaklardan elde edilip doğruluğuna göre sınıflandırılması, karşılaştırılması ve analiz edilmesi süreci sonunda ulaşılan bilgidir." [34] şeklinde tanımlanmaktadır.

Bu tanımlamadan da hareketle, siber saldırı ve olaylara karşı savunma yani siber güvenlik için, ulusal çıkarların korunması maksadıyla siber saldırıların/taarruzların yapılması veya siber caydırıcılık sağlanması, kısaca siber savaşın kazanılması için siber ortamda ihtiyaç duyulan bilgilere ulaşmak maksadıyla yapılan istihbarata siber istihbarat denir.

Siber istihbarat faaliyetleri ile elde edilen bilgiler sadece siber savaş için değil her türlü savaşta, kişi, toplum veya devletlerin ülke içi ya da dışı her alanında kullanılabilmektedir. Teknolojinin ve siber ortamın sağladığı imkânların teknik ve insan istihbaratı ile birlikte kullanılmasıyla siyasi, askeri, ekonomik, sosyal vb. alanlarda kişi, grup, toplum, örgüt, firma ya da ülkeler tarafından icra edilen siber casusluk faaliyetleri ile kısa sürede çok az maliyetle çok yüksek üstünlükler ve kazanımlar elde edilebilmektedir.

Tarihin başlangıcından günümüze her alanda var olan "Güç" kavramının sözlüklerde eş anlamı "Kuvvet" sözcüğü gösterilmekte ve kısaca "etki yapabilme veya etkiye direnebilme kapasitesi/yeteneği" ortak tanımlamasında bulunulmaktadır. Genel anlamda, "hedeflere ya da amaçlara erişme becerisi, daha belirgin olarak da arzulanan sonuçları elde etmek için başkalarını etkileme becerisi" [35] olarak da tanımlanan gücün ölçülmesi için çok çeşitli hesaplamalar ve ölçüm yöntemleri geliştirildiyse de mutlak olmadığı açıktır. Çünkü uluslararası ortamda bir devlet diğer devlete karşı güçlü iken başka bir devlete karşı güçsüz olabilmektedir.

Stratejik yaklaşımlarda "bir ulusun maddi ve manevi değerleriyle toplam potansiyel gücü" olarak tanımlanan "ulusal güç"; bir devletin ulusal çıkarlarını sağlamak ve ulusal hedeflerini elde etmek için kullanabileceği insan gücü, coğrafi güç, ekonomik güç, politik ve idari güç, psiko sosyal güç, bilimsel ve teknolojik güç, askeri güç şeklinde 7 ayrı güç unsurundan [36] oluşmaktadır. "Siber ortamda sahip olunan bilişim sistemleri ve alt yapıları ile bunların etkin olarak kullanılması yeteneği" [22] olarak tanımlanan ve kısaca "siber ortama hâkimiyet" demek olan siber gücü, ulusal güç unsurların-

dan bilimsel ve teknolojik güç unsuru altında değerlendirilir. Ancak siber gücü, 8'inci güç unsuru olarak kabul etmek daha doğru olabilir. Çünkü siber güç oluşumu incelendiğinde, diğer bütün ulusal güç unsurlarını etkilediği, onların etkilerini daha da artırılabildiği ve tek başına da etkin olarak kullanılabildiği görülmektedir. Ülkelerin sahip oldukları siber güçlerinin, hem saldırı aracı ve hem de saldırı hedefi olabileceği kararsızlığa meydan bırakmayacak şekilde ortadadır.

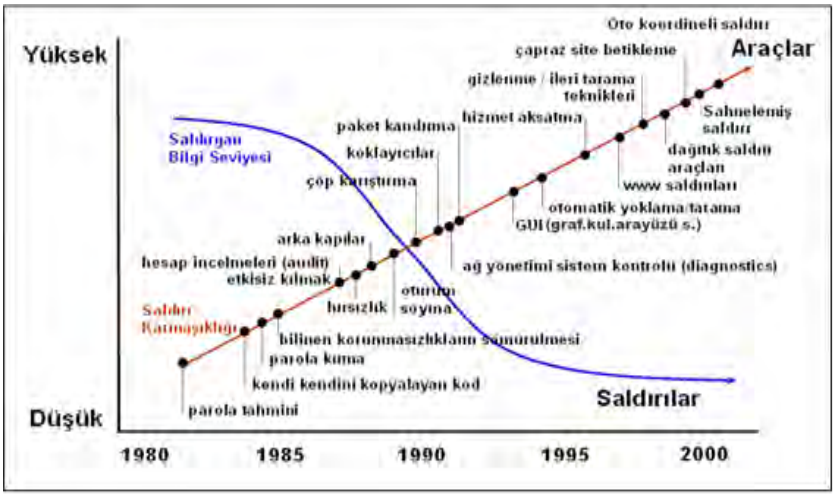
Bir ülkenin savaş alanında gücünün büyüklüğünü ölçerken, taarruz ve savunma açısından değerlendirmek yeterli olurken, siber güç söz konusu olduğunda bu iki faktöre üçüncü bir faktör olarak "Bağımlılık" faktörünün eklendiği görülmektedir. Siber bağımlılık bir ülkenin siber saldırılara açık sistemlere ve ağlara yani siber uzaya ne kadar gereksinim duyduğunun ölçüsü [25] olarak açıklanmaktadır. Bu konuda işlevsel olarak hazırlanan Tablo 7.1'de görüleceği üzere, Kuzey Kore siber gücü en yüksek ve siber saldırılardan en az zarar görecek ülke durumundadır.

Tablo 7.1. Bazı Ülkelerin Siber Savaş Güç Değerlendirmesi [25].

Devlet	Siber saldırı	Siber Savunma	Siber Bağımlılık	Toplam
ABD	8	1	2	11
Rusya	7	4	5	16
Çin	5	6	4	15
İran	4	3	5	12
Kuzey Kore	2	7	9	18

Askeri silah, araç ve gereçlerin nitelik ve miktar olarak artırılması gücü artırırken, bilişim sistemlerinin yaşamın her alanına girmesi ve özellikle kritik altyapıların bilişim sistemlerine ve ağlarına bağımlılığının artmasıyla, bunların güvenliğinin sağlanması daha zorlaşacağı (siber saldırılarda verilebilecek hasar ve zarar miktarı daha yüksek olabileceği) için siber gücü azaltacağı, bağımlılık azaltılamaz ise, zor olsa da savunmanın artırılmasının gerektiği değerlendirilmektedir.

Günümüzde saldırganların bilgi ve yetkinlik seviyeleri ise düşmekle birlikte, işlenen siber suçların ve siber saldırıların çeşitliliği, miktarı ve şiddeti de her geçen gün daha da artarken (Şekil 7.6) [38], siber savaş sadece konuşulmakla kalmayıp, başlamış devam etmektedir.



Şekil 7.6. Tarihi Süreç İçerisinde Siber Saldırganların Bilgi Seviyesi ve Saldırıların Durumu [38]

Dünyada siber savaşın başlayıp devam ettiği değerlendirmesinin doğruluğunu ve siber gücün etkisini ortaya koyan, yazılı ve görsel basın gibi açık kaynaklara da yansıyan önemli siber olaylar ve siber saldırıların bazıları aşağıda sunulmuştur. Bu saldırılar konuyla ilgilenenlerce bilindiği için ayrıntılarına girilmemiş, ancak bir savaş durumunda ya da siber savaşta, siber güçle neler yapılabileceğine dikkat çekmek amacıyla geçmişten günümüze yaşanan bazı siber olaylar ve saldırıların kısaca açıklanmasında yarar görülmüştür [22].

2000'de Avustralya'da arıtma tesisi bilgi sistemlerine saldırı ve kanalizasyon sularının şehre bırakılması: 28 Şubat - 23 Nisan 2000 tarihleri arasında, Avustralya'nın Moroochy eyaletinde, arıtma tesisi bilgi sistemlerine müdahale sonrasında pis kanalizasyon suları, en az 40 defa, parklara, nehirlere hatta turistik bir otelin zeminine bırakılmıştır.

2003'te ABD'nin sekiz eyaletinde 2 gün süren, ölümlere ve zarara yol açan elektrik kesintisi: 14 Ağustos 2003'te ABD'nin sekiz eyaletinde 50 milyon kişiyi etkileyen, bazı şehirlerde 2 gün süren, 11 kişinin ölümüne ve 6 milyar dolar zarara yol açan ve tarihe 'Kuzey Doğu Kesintisi' olarak geçen ABD tarihinin en önemli elektrik kesintisinin nedenlerinden birisinin enerji yönetim sisteminde kullanılan bir yazılımdan kaynaklandığı saptanmıştır.

2007'de Rus bilgisayar korsanlarının Estonya bilgi sistemlerine saldırısı ve ülke çapında faaliyetlerini durma noktasına getirmesi: 2007 yılı Nisan ve Mayıs aylarında, Rus bilgisayar korsanlarının Estonya bilgi sistemlerine sızması, özellikle internet ve bankacılık hizmetlerini durma noktasına getirmiş, ülke çapında ciddi ekonomik ve toplumsal zararlar yaşanmıştır.

Eylül 2007'de İsrail savaş uçaklarının Suriye topraklarına girmesi ve nükleer tesisini imha ederek zayiatsız dönmesi, bu sırada Suriye hava savunmasının hiçbir hedef görememesi: 6 Eylül 2007'de İsrail savaş uçakları Türkiye-Suriye sınırını takip ederek hiçbir engelle karşılaşmadan Suriye topraklarına girmiş, nükleer tesisin yerle bir edilmiş harabesini bırakarak, en ufak bir zayiat vermeden evlerine dönmüşlerdir. İsrail uçaklarının saldırıları sırasında Suriye hava savunması siber saldırılar nedeniyle hiçbir hedef görememişlerdir.

2008'de Rusya-Gürcistan savaşında Gürcistan'a yapılan siber saldırılar sonucu ciddi sıkıntılar yaşanması: 2008 yılı Ağustos ayında, Rusya-Gürcistan savaşında, başta devlet başkanlığı internet sitesi olmak üzere Gürcistan'ın neredeyse tüm internet sayfaları bloke edilmiştir. Finans merkezleri, haberleşme sistemleri ve elektrik santralleri ciddi sıkıntılar yaşamıştır.

2010'da İran nükleer zenginleştirme programını hedefleyen ve ciddi sorunlara sebep olan 'Stuxnet' yazılımı saldırısı: 2010 yılı Temmuz ayında keşfedilen, endüstriyel kontrol sistemlerini hedefleyen ve bilinen en tehlikeli zararlı yazılım olduğu düşünülen 'Stuxnet' yazılımı ile İran nükleer zenginleştirme programına saldırıldığı ve ciddi zararlar verildiği ortaya çıkmıştır. Bu saldırı, yazılım sistemlerine fiziksel zarar veriyor olması ile de bir ilk olmuştur.

Kasım 2010'da WikiLeaks'in yayınladığı belgeler ile diplomaside sanal bomba etkisi yaratması: İsveç merkezli uluslararası bir oluşum olan WikiLeaks, yayınladığı diplomatik belgeler ile dünya çapında ses getirmiş ve şimdiye kadar açıkladığı toplam bir milyon civarında gizli yazışma ile diplomaside depreme yol açmıştır.

Aralık 2011'de İran Silahlı Kuvvetlerinin ABD'ye ait insansız hava aracının kontrolünü ele geçirerek yere indirmesi: 2011 yılı Aralık ayında, İran Silahlı Kuvvetlerinin İran'ın doğusunda, ABD'ye ait insansız casus uçağının kontrolünü ele geçirip sapasağlam yere in-

direrek el koyması, bütün dünyanın ilgisini çeken ve siber harekât açısından incelenmeye değer bir olay olmuştur.

Aralık 2014'te Sony şirketinin yoğun siber saldırılar sonucu Kuzey Kore lideriyle ilgili filmi gösterimden kaldırması: Aralık 2014'te, Kuzey Kore liderine suikast girişimini konu alan komedi filmi Kuzey Kore tarafından tepkiyle karşılanmış, yapımcı Sony Pictures Firması yoğun siber saldırılara maruz kalmış, şirket bilgisayarlarından çekimine başlanmamış film senaryoları ve personel bilgileri dâhil pekçok gizli bilgi/belge sızdırılmış, tehditler ve siber saldırılar sonucu film gösterimden kaldırılmıştır. Saldırılardan Kuzey Kore Cumhuriyeti sorumlu tutulmuş ancak kanıtlanamamıştır.

Ekim 2016'da ABD'de yapılan saldırılar sonucu internet bağlantısının yüzde 90'ının engellenmesi: 21 Ekim 2016'da, ABD'nin doğu yakasına hizmet sunan DNS altyapılarına yönelik olarak başlayan saldırılar ülke geneline yayılarak internet bağlantısının yüzde 90'ını engellemiş ve Türkiye'nin de aralarında bulunduğu birçok ülkede etkisini göstermiştir. Özellikle sanal ticarete darbe vuran saldırıların, ABD ekonomisine maliyetinin 7 milyar doları bulduğu belirtilmiştir.

Yukarıda açıklanan ve dünyada yaşanan bu siber olayların benzerleri Türkiye'de de yaşanmış olup, yaşanan bu önemli siber saldırıların ve olayların bazıları aşağıda sıralanmıştır [22].

Ağustos 2008'de Bakü-Tiflis-Ceyhan boru hattına saldırı sonrası patlama meydana gelmesi: 5 Ağustos 2008'de Bakü-Tiflis-Ceyhan boru hattındaki 1,768 kilometrelik hat üzerinde Erzincan'ın Refahiye ilçesi yakınlarında bir patlama meydana gelmiş, Türk makamların sabotajdan şüphelenmesi ile PKK terör örgütü saldırıyı üstlenmişti. Araştırma sonucunda ise patlamanın nedenin teknik arızadan kaynaklandığı belirtilmişti. Ancak sonradan elde edilen bilgilere göre, bu patlamanın bir siber saldırı sonucunda gerçekleştiği anlaşılmıştır.

Ocak 2009'da zararlı bir yazılımın Atatürk Havalimanı bilgisayarlarını etkilemesi: 30 Ocak 2009 tarihinde birçok ülkenin bilgisayar sistemine yayılan ve önemli zararlar veren 'Conficker' virüsü İstanbul'da Atatürk Havalimanı'nın dış hatlar terminalinde çalışan bilgisayarları ciddi şekilde etkilemiştir.

Haziran 2011'de saldırılar sonrasında TİB'in sitesinin devre dışı kalması: 9 Haziran 2011'de "İnternete Filtre Uygulamasının karşısında temel hak ve özgürlüklerin ihlal edileceğini" savunan 'Anonymous' adlı Uluslararası Bilgisayar Korsanları Topluluğu akşam saatlerinde BTK Telekomünikasyon İletişim Başkanlığının internet sitesine saldırmış, devre dışı kalan site çalışmaya gece yarısından sonra ancak başlayabilmiştir.

Mart 2015'te 79 ili etkileyen elektrik kesintisi: 31 Mart 2015 günü ülkemizde elektriğini İran'dan alan Van ve Hakkâri hariç 79 ilde elektrik kesintisi yaşanmıştır. Nedeniyle ilgili uzmanların görüşü; "Yüklü bir hattın devre dışı kalmasının tüm sistem dinamiğini bozması, ardından diğer hatların bir arıza olduğunu düşünerek kademeli olarak kendilerini kapatması…" şeklinde olmuştur. Kısa süre sonrasında ise, "TEİAŞ Siber Saldırıları Engellemek için Bilgisayar Ağları İhalesine Çıkıyor" haberleri basında yer almıştır.

Aralık 2015'te, 10 gün süreli saldırılar sonucu birçok internet sitesine ve mobil uygulamalara erişim sağlanamaması: 14 Aralık 2015 tarihinde başlayan ve yaklaşık 10 gün süreli, özellikle 'tr' uzantılı alan adlarının yönetildiği sunucuları hedef alan saldırılar sonucu birçok banka, noter ve devlet kurumunun internet sitesine ve mobil uygulamalarına erişim sağlanamamıştır. İnternet trafiğini büyük ölçüde etkileyen bu toplu saldırıların, bugüne değin dünya üzerinde yaşanmış en yoğun siber saldırılardan biri olduğu ifade edilmiştir.

Mayıs 2016'da Sağlık Bakanlığı hastanelerine yönelik siber saldırılar ile veri tabanındaki bilgilerin çalınması ve silinmesi: 18 Mayıs 2016 günü sabah saatlerinde, 33 devlet hastanesinin veri tabanlarında bulunan bilgilerin kopyalandıktan sonra silindiği, saldırıları 'Anonymous' adlı grubun üstlendiği belirtilmiştir. Sağlık Bakanlığı sistemin kısmen etkilendiğini ve yedekleme mekanizması sayesinde olası veri kayıplarının önüne geçildiğini duyurmuştur.

Tüm bu yaşanan olaylar ve siber saldırılar; siber gücün tek başına veya başka güç unsurlarıyla birlikte kullanılmasının sonucudur. Bu sonuçlardan, siber gücün çeşitli strateji, taktik, teknik ve usullerle kullanılmasıyla gerçekleştirilecek siber saldırılarla; askeri haberleşme dâhil girilip yanıltıcı bilgilerin sistemlere bırakılabileceği, hava kontrol sistemlerine sızılabileceği, stratejik sistemlerin devre dışı bırakılabileceği, kritik altyapıların her zaman tehdit altında ka-

labileceği, iletişim ağlarının devre dışı bırakılarak haberleşmenin sekteye uğratılabileceği, ulaşım ve su sistemlerinin bozulabileceği, bankacılık ve finans sektörünün çökertilebileceği, elektrik ve doğalgaz sisteminin kapatılabileceği ve doğalgaz boruları basıncının artırılarak tahrip edilebileceği, baraj kapaklarının açılarak şehirlerin sular altında bırakılabileceği, enerji santrallerin kontrolünün ele geçirilerek potansiyel birer atom bombasına dönüştürülebileceği, toplumsal olayların çıkarılabileceği veya yönlendirilebileceği, halka verilen haberleşme, elektrik, doğalgaz, e-devlet, ulaşım, vb. hizmetler engellenerek ülkede kargaşa ve karışıklık yaratılabileceği, kişi, toplum, devlet ve ülke güvenliği için çok büyük endişeler yaratılabileceği gibi önemli sonuçlara ulaşmak yanlış olmayacaktır [22].

Tek başına siber güç ile gerçekleştirilecek siber saldırılardan oluşan bir siber savaş ile belki zafer kazanılamaz. Ancak, geçmişten bu güne yaşanan siber olayların ve saldırıların sonuçları, siber gücün daha gelişmiş ve etkin şekilde tek başına veya diğer güç unsurlarıyla birlikte kullanılması durumunda, gelecekte yaşanacak hasar, zarar ve olumsuzlukların ne kadar büyük olabileceğini açıkça ortaya koymaktadır. Siber gücün, asıl amacı karşı tarafın siyasi yönetimini ve devlet kurumlarını kararsız ve dengesiz hale getirmek, yönetim boşluğu oluşturmak ve kargaşa yaratmaktır. En belirgin özelliği düzensiz savaş taktikleriyle yüksek teknolojinin birleşimi olan hibrit savaş kapsamında siber savaş maksatlı olarak geçmişteki kullanım ve uygulamalarla da bu durum doğrulanmıştır.

Dünya'da yaşanan siber olay ve saldırılardan; resmen doğrulanmasa da Ruslar tarafından 2007 yılında Estonya bilgi sistemlerine saldırılar ve ülke çapında faaliyetlerin durma noktasına getirilmesi, 2008 yılında Rusya - Gürcistan savaşında Gürcistan'a yapılan siber saldırılar sonucu ciddi sıkıntılar yaşatılması, Eylül 2007'de İsrail savaş uçaklarının görünmeden Suriye topraklarına girmesi ve Suriye nükleer tesisini imha ederek zayiatsız dönmeleri, 2010 yılında İran nükleer zenginleştirme programını hedefleyen ve ciddi sorunlara sebep olan 'Stuxnet' yazılımı saldırısı [39], hibrit savaş kapsamında bütün dünya tarafından geniş kabul gören başarılı siber savaş uygulaması örneklerindendir. Türkiye'de yaşanan siber olay ve saldırılardan ise; Ağustos 2008'de Bakü-Tiflis-Ceyhan boru hattına saldırı sonrası patlama meydana gelmesi, Mart 2015'te 79 ili etkileyen elektrik kesintisi, Aralık 2015'te, 10 gün süreli saldırılar sonucu

birçok internet sitesine ve mobil uygulamalara erişim sağlanamaması ve Mayıs 2016'da Sağlık Bakanlığı hastanelerine yönelik siber saldırılar ile veri tabanındaki bilgilerin çalınması ve silinmesi [39] ayrıntılı incelemeye ihtiyaç duyan ve gelecekte benzerlerinin yaşanmaması için tedbirlerin alınması gereken hibrit savaş kapsamlı siber savaş uygulamalarıdır. Ayrıca; 2000'li yılların başlarında eski Sovyet ülkelerinde ve Balkanlarda gerçekleşen, "Renkli Devrim" olarak adlandırılan ve çoğu ülkede başarılı olan toplumsal hareketler ile 2010 - 2011 yıllarında Tunus, Yemen, Mısır ve Libya'da yaşanan ve "Arap Baharı" olaylarında, özellikle internet ve sosyal ağlar başta olmak üzere bilgi ve iletişim sistemlerinin yoğun şekilde kullanılarak toplumların eğitilmesi ve yönlendirilmesi uygulamaları da hibrit savaş kapsamında gerçekleştirilen propaganda ve psikolojik harekât tekniklerinin etkinlikle kullanıldığı siber savaş uygulamalarıdır.

Hibrit savaşlar kapsamında gerçekleştirilecek siber savaşlarda başarılı olmak için gerekli tedbirlerin gecikmesizin alınarak her zaman hazır olunması kaçınılmaz zorunluluktur. Şüphesiz saldırganların zamanında belirlenme zorlukları dâhil siber savaşın asimetrik özellikleri dolayısıyla öncelikle siber savunma (güvenlik) tedbirlerinin alınması, müteakiben caydırıcılık da sağlayacak seviyede saldırı yani siber taarruz gücüne ve yeteneklerine sahip olunması gerekir. Siber güç imkânları kullanılarak siber savaşları (savunma ve taarruz) başarıyla icra etmek, siber saldırıları veya savaşı düşünenleri bu düşüncelerinden ve eylemlerinden vazgeçirmek, kısaca siber saldırganları caydırmak (siber caydırıcılık) için siber güç imkânları tek başına kullanılabileceği gibi, yeterli olmadığında başka güçlerle birlikte kullanılmasına yönelik stratejiler geliştirilerek uygulamaya konulması, siber alanda günümüzün en önemli ihtiyaçlarından birisi haline gelmiştir.

7.5. Siber Caydırıcılık

Savaşları kazanmak için her zaman ve her bakımdan hazırlıklı olunmalıdır. Ancak savaşta her zaman en mükemmeli hep kazanmak olmayabilir. M.Ö. 500'lü yıllarda yaşamış olan ünlü Çinli filozof ve savaş stratejisti Sun Tzu "En iyisi savaşmadan baş eğdirmektir" [33] derken, ondan yaklaşık bin yıl sonra Ünlü Doğu Romalı Komutan Belisarius da "En mükemmel ve mutlu zafer şudur: Kendiniz bir

zarar görmeden, düşmanı amacından vazgeçmek zorunda bırakmaktır" [40] demiştir. Yani bir anlamda saldırganı isteğinden, amacından, saldırıdan veya savaştan caydırmak, söz konusu siber savaş olduğuna göre "Siber caydırıcılık" en mükemmeli ve en mutlu edeni olabilir.

Türkçede genellikle "korkutarak cesaret kırmak ve vazgeçirmek" anlamlarında kullanılan "caydırmak" sözcüğünden türetilen "Caydırıcılık" kavramı, TDK Sözlüğünde "Bir saldırganlığı önlemek ve engellemek için önlem alma işi" [1] olarak açıklanmaktadır.

"Caydırıcılık"; hukuksal alanda "ceza veya hapis korkusuyla suç işlemekten alıkoyma" [41], uluslararası ilişkilerde yani diplomasi alanında "karşıdaki devleti emellerinden vazgeçirme davranışı veya belirli davranışlara yönlendirme" [42], askeri alanda ise "düşmanı çok yüksek bedel ödeyeceğine inandırarak bir hareketten vazgeçirmek için askeri güç, yaptırım ve tehditlerin kullanımı" [43] olarak tanımlanmaktadır.

Geçmişe ve günümüze bakarak, hukuk alanında bireylerin çeşitli cezalar ile suç işlemelerinin önlenmesine, diplomasi alanında devletlerin çeşitli yaptırımlarla ilişkilerinin yönlendirilmesine ve askeri alanda savaşmadan karşı tarafın farklı davranmasının sağlanmasına, yani bu alanlarda caydırıcılık uygulamasına yönelik, pekçok örnek sıralanabilir [39]; Adli olaylarda para ya da mahkûmiyet cezaları, uluslararası ortamda devletlere çeşitli yaptırımların uygulanması, klasik savaşta güçlü ordularla karşı tarafa güç gösterisi, tatbikatlar vb.

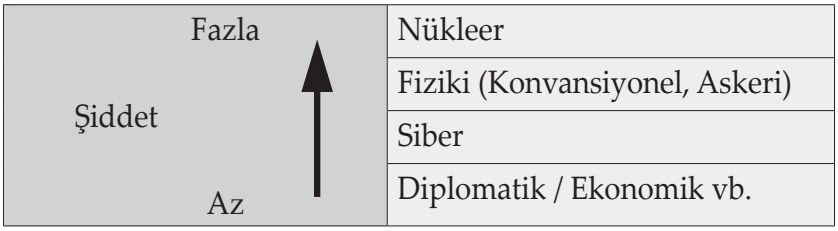
Caydırıcılığın yaygın olarak kullanılan genel tanımı ise, bir düşmanın, belirli bir eylemi gerçekleştirmek için maliyet/fayda hesaplamasına yönelik tahmini üzerinde yönlendirilmesidir [44]. Diğer bir ifadeyle de, potansiyel faydaları azaltarak ya da olası masrafları arttırarak (ya da her ikisini de birden), düşmanı eylemi yapmaktan kaçınmaya ikna etmektir. Bu maksatla caydırıcılığın sağlanması için "Saldırganın eylemini boşa çıkarma" ve "Cezalandırma (misilleme tehdidi)" yoluyla saldırıdan vazgeçirilmesine dayanan iki yöntem uygulanır. Bu yöntemlerden özellikle soğuk savaş döneminde ön planda kullanılan ve nükleer caydırıcılığın esasını teşkil eden cezalandırma yoluyla caydırıcılığın başarıyla sağlanması için üç temel

koşul bulunmaktadır [45]. Bunlar caydırıcının yetenekleri, misilleme tehdidinin güvenilirliği ve tehdidin saldırgana iletilmesidir.

Saygınlık kaybı, gizlilik, kamu yararı, ulusal ve uluslararası güvenlik vb. nedenlerle açıklanmayanlar yanında, yazılı ve görsel basın, medya gibi açık kaynaklarda da yer alan siber saldırı olaylarına ve bunların olumsuz sonuçlarına rağmen, siber savaşın bir savaş olup olmadığı tartışmalarının devam ettiği gibi, siber alanda siber güçle bir caydırıcılığın mümkün olup olmadığı konusunda da tartışmaların başlamış ve devam etmekte olduğu görülmektedir [22].

Caydırıcılık ile ilgili yukarıdaki açıklamalardan doğrultusunda "Siber caydırıcılık" nasıl tanımlanabilir? Sun Tzu'nun "En iyisi savaşmadan baş eğdirmektir" [33] özdeyişinden de hareketle siber caydırıcılık; kısaca "siber ortamda bilişim sistem ve altyapılarına saldırı başlatacak saldırganı saldırıdan vazgeçirmektir" şeklinde tanımlanabilir.

Caydırıcılığı genel anlamda "karşı tarafa düşmanca eylemleri yapmama konusunda gözdağı verme" şeklinde açıklayan Libicki, siber caydırıcılığı; "siber ortamda saldırganın eylemini boşa çıkarma veya cezalandırma (misilleme tehdidi) yoluyla saldırıdan vazgeçirme" olarak tanımlamaktadır [22]. Bu konuda, siber güç ve siber savaş kapsamında misillemenin etkisinin de, Şekil 7.7'de belirtildiği gibi, nükleer ve geleneksel (konvansiyonel) savaş kapsamında caydırıcılıktan sonra, diplomatik ve ekonomik yaptırımlarla sağlanan caydırıcılıktan ise önce geldiğinin kabul edilebileceğini belirtmektedir [32].



Şekil 7.7. Caydırıcılıkta Misillemenin Etki Seviyeleri.

ABD eski Genelkurmay Başkan Yardımcılarından (2007-2011) olan Orgeneral James Cartwright siber caydırıcılığı, "siber ortamda başkalarının bize yapmak istediklerinin aynısını onlara yapma yeteneği" [32] olarak tanımlamıştır. Bu tanımlamanın nükleer veya

konvansiyonel caydırıcılık için karşılık bulduğu kabul edilmekle birlikte, siber gücün ve kullanılmasının özellikleri dolayısıyla, siber caydırıcılık için yeterli olup olmayacağı tartışılmaktadır.

Siber saldırılara ve savaşa karşı caydırıcılık stratejisini analiz eden çalışmaların çoğu soğuk savaş teorilerine dayanmaktadır. Bu kapsamda başarılı bir caydırıcılık için yerine getirilmesi gereken tarafların yetenekleri, misilleme tehdidinin güvenilirliği ve tehdidin saldırgana iletilmesi koşullarının, siber saldırıların yarattığı tehditlere uygulandığında, saldırının başarısız olunmasının beklendiği iddia edilmektedir [45].

İstihbarat yetenekleri bu sorunun çözümünü kolaylaştırsa da, genelde saldırıya karşılık verileceği zaman daha geniş bir potansiyel tehdidi kapsayacak şekilde değerlendirilmelidir. Soğuk savaş döneminde her iki tarafın da yetenekleri açıkça bilinirken, bilgi çağında olası saldırganların sayısının artması ve güçlerinin de belirsizliği, caydırıcılık mesajının kime ve nasıl ileteceğinin zorlukları istikrarlı ve inanılır caydırıcılık sunma olasılığını düşürmüştür.

Siber saldırılara karşı caydırıcılığın zorlukları nedeniyle; nükleer savaşı önlemenin olmazsa olmazı olan caydırıcılık kuramının, günümüzde siber savaşı durdurmakta önemli bir rol oynayamadığı ve ABD'nin nükleer ve konvansiyonel anlamda sağladığı caydırıcılığı, tüm çabasına rağmen siber alanda sağlayamayacağı ileri sürülmektedir [32]. Bu tez, 2011 yılında ABD Savunma Bakanlığınca hazırlanan raporlardan sızan bilgilerden, "siber saldırıların savaş sebebi sayılacağının ve askeri operasyonlarla karşılık verilebileceğinin açıklanması" [46] ile desteklenmektedir.

Ancak, siber silahlar nükleer silahlara benzemez ve bireyler, küçük gruplar ve devletler tarafından kolayca geliştirilip konuşlandırılırlar. Kolayca çoğaltılır ve ağlar arasında dağıtılır [47]. Siber alanda bilgisayar ve iletişim teknolojileri kullanarak elde edilen imkân ve kolaylıkların bir güç (siber güç) olduğu, bu gücün hem saldırı aracı, hem de saldırı hedefi olabileceği, tarafların birbirine zarar vermek, siber güçlerini zayıflatmak veya bazı unsurlarını devre dışı bırakmak maksadıyla karşılıklı siber güçlerini kullanabilecekleri tereddüde meydan bırakmayacak şekilde ortadadır. Bu arada, güçlü ülkelerin en gelişmiş siber silahlarını kullandığı türden bir siber

savaşın henüz gerçekleşmediği [25] öne sürülmektedir. Bu nedenle gelişmiş ve kullanılmayı bekleyen siber silahların kullanılacağı bir savaşı kimin kazanacağı, bu savaşın sonuçlarının ne olacağı şu anda tahmin edilse de tam olarak bilinmemektedir.

Libicki'ye göre ise, siber caydırıcılık işe yarayabilir. Ancak bunun için, siber caydırıcılığı nükleer ve klasik askeri caydırıcılıktan ayıran, siber caydırıcılığın aleyhinde olan ve problemli yanlarını ortaya koyan üçü asıl, altısı yardımcı olmak üzere dokuz soruyu cevaplamak gerekmektedir [32].

Asıl sorular:

- Kimin yaptığı biliniyor mu?
- Onların değerli varlıkları risk altında tutulabilir mi?
- Aynı şey art arda tekrarlanabilir mi?

Yardımcı sorular:

- Eğer misilleme caydırıcılığı sağlamazsa, en azından silahsızlandırmayı sağlayabilir mi?
- Üçüncü gruplar mücadeleye katılır mı?
- Misilleme kendi tarafımıza doğru mesajı verir mi?
- Saldırıya karşılık vermek için bir eşik var mıdır?
- Tırmanmadan kaçınılabilir mi?
- Saldırgan tarafa vurmaya değmediği durumda ne olur?

Nükleer caydırıcılıkta cevaplanması kolay olan bu soruların, siber caydırıcılık söz konusu olduğunda cevaplanması zorlaşmakta ve bazen de imkânsızlaştığı görülmektedir. Ancak siber ortamda siber güç kullanılarak siber güvenlik ve caydırıcılık sağlanması düşünülüyorsa bu soruların cevaplanması ve bu cevaplar doğrultusunda stratejilerin oluşturulması, planlamaların yapılması ve eyleme dönüştürülmesi gerekmektedir.

Will Goodman "Siber Caydırıcılık Pratikte Teoriden Daha Zor" konulu çalışmasında [48], siber caydırıcılık üzerine geliştirilen teorik yaklaşımların işlevselliğini sorgulamış ve siber caydırıcılığın teoride kolay, pratikte ise daha zor olduğunu vurgulamıştır. Tespitlerini de 2007 yılında Estonya'da 2008 yılında da Gürcistan'da yaşa-

nan siber saldırı olaylarını inceleyerek somutlaştırmaya çalışmıştır. Goodman'ın, caydırıcılığın sağlanabilmesi için belirlediği esaslar Libicki'nin belirlediği esaslara benzer şekildedir. Siber caydırıcılığın sağlanması, "Çıkar, Duyurma, Engelleme, Cezalandırma, İnandırma, Güven verme, Korku, Kar-zarar durumu" başlıklarıyla sıralanan sekiz temel esasa göre hareket edilmesine bağlıdır.

Christopher Hale ise [49], caydırıcılık teorisinde amacın, maliyetleri ve sonuçları avantajlardan ağır basarak saldırıları gidermek olduğunu belirtmekte ve bu stratejiyi uygulamak için öncelikle güçlü bir savunmaya sahip olmanın gerektiğini (saldırganı durmaya zorlamak için) vurgulamakta, ikinci yöntem olarak da, misilleme üzerine odaklanmakta ve bazı başarılı saldırganların eylemlerini takiben ağır cezalandırma ile karşı karşıya kalındığında, diğer istekli saldırganların hiç saldırmamayı seçebileceği üzerinde durmaktadır. Üçüncü bileşen olarak da, zorluğuna rağmen saldırının saldırgan tarafa dayandırılması (saldırgana isnat) yaklaşımlarının önemi üzerinde durmaktadır.

Eric T. Jensen "Siber Caydırıcılık" konulu çalışmasında [50] Hale'ın vurguladığı cezalandırma konusunda siber saldırganlara karşı yasal işlemlerin önemine işaret ederken, ulusların ağlarını ve altyapılarını savunmak için mücadelede, caydırıcılık ilkelerini siyasal etkinliklere uygulayabilme becerilerinin daha da önem kazanmakta olduğunu ve siber ortamda caydırıcılığın, geleneksel misillemeye ek olarak, soğuk savaşın nükleer çağında geliştirilen geleneksel caydırma metotlarından daha fazla yasal işlemleri yapma ve ağları görünmez, esnek ve birbirine bağlı hale getirme gibi seçenekleri de sunduğunu belirtmiştir. Siber yetenekler ulusal hedefleri gerçekleştirmek için benzersiz ve yenilikçi araçlar sağlarken, aynı şekilde "misilleme gibi geleneksel caydırma metotları ve yenilmezlik, görünmezlik, esneklik ve karşılıklı bağımlılık gibi" yeni ve yenilikçi bazı caydırıcılık yöntemleri de sunmaktadır.

Konula ilgili olarak askeri ve akademisyen araştırmacı, yazar ve düşünürlerin görüş birliği sağladığı husus; saldırıların bir kısmının devlet destekli olduğu bilinse de bazılarının küçük saldırı gruplarınca gerçekleştirildiği siber saldırıların ve olayların, daha önce açıklandığı üzere, sadece bilinen sonuçlarına bakmanın bile, "siber alanda siber güç kullanılarak caydırıcılık (siber caydırıcılık) sağlanabilir" sonucuna ulaşmak için yeterli olduğudur [22].

Siber caydırıcılıkta, askeri yeteneklerin ve güç gösterilerinin aksine, bir ülkenin büyüklüğü pek önemli değildir. Bir siber savaşın savaş alanı tüm dünya dâhil siber uzay olup, nitelik, girişim ve konum özellikleri genellikle nicelikten daha önemlidir [51]. Bunun daha iyi anlaşılması için, siber saldırılarla caydırıcılığın nasıl sağlandığı ve hedeflenen sonuçlara nasıl ulaşıldığı açıkça görülen ve açık kaynaklarda da geniş yer bulan, "Aralık 2014'te Kuzey Kore lideriyle ilgili film nedeniyle Sony şirketinin yoğun siber saldırılara maruz kalması ve filmin gösterimden kaldırılması" olayı [22] ayrıntılı olarak incelenerek analiz edilmelidir. Sony şirketine saldırı olayı, iki devlet arasında olamamakla birlikte, saldırıların hedefinin, arkasında ABD olan ve dünyanın sayılı küresel şirketlerinden birisi, saldıran tarafın ise açık kanıt ve kabul durumu olmasa da Kuzey Kore destekli saldırganlardan oluşması nedeniyle iki tarafın devlet özelliğinde oluşumlar olarak değerlendirilmesi yanlış olmayacaktır.

Söz konusu Sony saldırısı olayında, saldıran tarafın başarılı olması buna karşılık saldırılan tarafın ise misilleme ve cezalandırma konusunda yeterli olamamasının nedenleri ise Amir Lupovici'nin çalışmasında kısmen de olsa açıklanmaktadır. Yaptığı "Siber Savaş ve Caydırıcılık" konulu çalışmada, siber uzayda devletler tarafından caydırıcılığın sağlanıp sağlanamayacağını sorgulayan Lupovici'nin de belirttiği [45] gibi, siber saldırganın eylemini boşa çıkarma ve cezalandırma (misilleme) yöntemlerinden cezalandırma yoluyla caydırıcılığın başarılı olabilmesi için caydırıcının yetenekleri (kapasitesi), misilleme tehdidinin güvenilirliği ve misilleme tehdidin saldırgana başarılı bir şekilde duyurulması şartlarının sağlanması gerekmektedir. Bu şartlardan yetenek veya kapasite konusunun asimetrik bir etki doğurmasından dolayı göreli olarak küçük olan devletler, klasik savaş maliyetlerinin çok azıyla siber uzayda önemli bir saldırı kapasitesi oluşturabilmektedir. Buna karşın büyük ve gelişmiş devletler saldırı yeteneklerini geliştirmelerine rağmen, siber ortama bağımlı yapılarından dolayı savunma kapasitelerini aynı oranda geliştiremediklerinden ve caydırıcılıklarını sağlamak için yapacakları siber misilleme tehditleri saldırganın bilgi ve iletişim sistemleri altyapıları yetersizlikleri ile ağsız yapısı nedeniyle etkisiz kalmaktadır.

7.6. Değerlendirmeler

"Savaş zorunlu ve hayati olmalıdır. … Ancak, ulusun yaşamı tehlikeye girmedikçe, savaş bir cinayettir." [52] sözüyle "savaş"ın gerçek yüzünü göstererek en anlamlı tanımını yapan büyük savaşçı ve lider Mustafa Kemal Atatürk; "Yurtta Barış Dünyada Barış" [53] sözüyle de "Barış"ın önemini vurgulamış, yurtta ve dünyada barış ve güvenlik içerisinde yaşamak için bu ilkeyi Türkiye Cumhuriyeti'nin iç ve dış politikalarının temel dayanağı yapmıştır. Ancak, insanlığın varoluşundan beri savaşlar değişerek ve gelişerek devam etmektedir. Ulusun huzuru ve güvenliği yani barış içerisinde yaşamak, ülkenin ve devletin kalıcılığını sağlamak için savaşa hazır olmak ve karşı karşıya kalındığında kazanmak gerekir. Bu çerçevede savaşı kazanacak kadar kuvvetli, ondan kaçınacak kadar da akıllı olunmalıdır [54].

Hem akıllı hem de kuvvetli olmak için, öncelikle geçmişi bilmek, geçmişten günümüze yaşanan olaylardan çıkarılan derslerle geleceğin ihtiyaç ve hedeflerine yönelik öngörülerde bulunularak, aynı zamanda caydırıcılık da sağlayacak strateji ve politikalarının bilimsel yaklaşım ve yöntemlerle oluşturulması ve uygulanmasına yönelik esas ve prensiplerin belirlenmesi gerekir. Konuyla ilgili sivil, asker, düşünür, araştırmacı ve akademisyenlerin ortak görüşünün de bu yönde olduğu görülmekte, savaşın geçmişini anlamadan, gelecekte savaşın kontrol edilemeyeceği savunulmaktadır [55].

Geçmişten günümüze teknolojinin gelişmesinin de etkisiyle savaşlar değişmiş ve gelişmiş, "4'üncü Nesil" ya da yaygın kullanılan ismiyle "Hibrit Savaşlar" uygulanmaya başlanmıştır.

Hibrit savaşlar; asıl amacı karşı tarafın siyasi yönetimini ve devlet kurumlarını dengesiz hale getirmek, yönetim boşluğu oluşturmak ve kargaşa yaratmak olan, hedef ülkenin güçlü yanlarını bir kenara atarak, çatışma koşullarını onun zayıf taraflarına odaklamaya çalışılan, en belirgin özelliği düzensiz savaş taktikleri ve yüksek teknolojinin birleşimi olan, en tehlikeli unsurları devlet dışı aktörlerin büyük güçlerin vekilleri olarak ve onlar tarafından güçlendirilerek onların yerine savaşıyor oldukları çağımızın yeni yeni anlamaya ve alışmaya çalıştığımız savaşlarıdır. Artık aynı harekât bölgesinde ve aynı zamanda geleneksel güçler, düzensiz savaş ve terör örgütleri ile suç örgütleri birlikte savaşmaktadırlar. Bütün bunlarla birlikte

de, teknolojinin ve bilişim sistemlerinin gelişmesiyle, kara, deniz, hava ve uzay harekât alanlarından sonra yerini alan 5'inci harekât alanı "Siber Uzay"ın getirdiği "siber savaş (savunma, taarruz ve caydırıcılık)" uygulamaları yaşanmaktadır. Ayrıca siyasi, diplomasi ve ekonomi alanlarını içine alan propaganda ve psikolojik harekât uygulamalarıyla bütün sivil halkın da dâhil edildiği teknoloji yoğun bir savaş alanı bulunmaktadır.

Hibrit savaşın tanımlanması dâhil, hibrit tehditlerle baş etmenin yolları ve hibrit savaşa başarıyla karşı koymanın yolları araştırılmaya, incelenmeye ve tartışılmaya devam ediyor. Çoğu devlet konuyu anlamış, strateji ve politikalarını belirlemiş, uygulamaya koymuş ya da koymakta, konuyla ilgili ön aldıkları için de sonuçta genelde başarılı olmaktalar.

Tartışmalar sürerken ABD'li Akademisyen Puyvelde konuya farklı bir yaklaşım getirerek, hibrit savaşı, "geleneksel olan ve olmayan, düzenli ve düzensiz, bilgi ve siber savaşın birleşiminden oluşan geniş çaplı bir savaş türü" şeklinde tanımlamakta ve pratikte, herhangi bir tehdidin, tek bir savaş yöntemi ve boyutuyla sınırlı olmadığı sürece hibrit olabileceğini belirtmektedir. Herhangi bir tehdit veya güç kullanımı hibrit olarak tanımlandığında, bu durumun kendi değerini yitireceğini ve modern savaşın gerçekliğini açıklığa kavuşturmak yerine kafa karışıklığına neden olacağını belirtmektedir. "Bu nedenle karar alıcıların "hibrit" olan her şeyi unutması ve karşılaştıkları tehditlerin özgüllüğüne ve birbirine bağlılığına odaklanması gerekir. İster eski ister modern olsun, ister hibrit olsun ister olmasın, savaş daima karmaşıktır ve tek bir terimde birleştirilemez. Etkili bir strateji, bu karmaşık ortamı dikkate almalı ve aşırı basitleştirmeden, onun gereğini yapmanın yollarını bulmalıdır." [56]

Puvyelde bu bakış açısıyla, bir taraftan olayı karmaşıklıktan sadeliğe indirgerken, bir taraftan da hibrit savaşlarla ilgili biraz da doğru anlamamaktan veya doğru yorumlamamaktan kaynaklanan korkuları azaltarak hibrit savaşlara daha açık bir tanımlama getirmektedir. Bu tanımlamadan yola çıkılarak hibrit savaşlarla her seviyede mücadele için strateji ve politikaların belirlenmesi daha da kolaylaşacaktır. Aynı şekilde hibrit savaşların gerçekleştirilmesi için de benzer bakış açısı uygulanabilir.

Çağımızın güçlü ve teknolojide çok ileri seviyelerde olan büyük devletler tarafından, karmaşıklığı yanında teknoloji yoğun hibrit savaşların gerçekleştirilmesi ve bu yolla hedeflerine ulaşmaları kolay görünse de, teknolojik üstünlük, kendi başına, stratejik hedeflerin başarılı bir şekilde elde edilmesi için her zaman yeterli olmaz. İngiliz askeri tarih ve strateji yazarı B.H. Liddell Hart'ın da ifade ettiği gibi "Savaşta, hesaplanamayan, baş edilemez olan insan iradesidir [40]." Tarih, insanoğlunun sürekliliğinin ve ustalığının, teknolojik olarak üstün bir düşmana karşı başarılı olduğu sayısız örneklerle doludur [57]. Çanakkale Savaşı (1915-1916) ve Türk Kurtuluş Savaşı (1919 -1923) bu konuda en etkili ve güzel örneklerdendir.

Hangi savaş olursa olsun öncelikle insan gücü ve iradesi bağlamında harekete geçilerek siyasi, askeri, ekonomik, coğrafik, demografik, bilimsel, teknolojik, sosyal ve kültürel güçten oluşan Milli Güç unsurlarının her zaman ve her alanda eksiksiz savunma için birlikte ele alınması, bütün kurum ve kuruluşların geleceğin tehlikelerine yönelik olarak ayrıntılı ve planlı işbirliği içerisinde hareketini sağlayacak strateji ve politikalar geliştirilmeli ve gecikmesizin uygulamaya konulmalıdır.

Hibrit savaşların gerek teknoloji boyutu ve gerekse bilgi ve iletişim sistemlerinin propaganda ve psikolojik harekât için ağırlıklı olarak birlikte kullanımı açılarından en önemli aracı olan siber savaşların hedefi ülkelerin haberleşme, enerji, su yönetimi, kritik kamu hizmetleri, ulaştırma, bankacılık ve finans gibi kritik altyapı sektörleri oluşturulacak stratejilerde öncelikli olarak ele alınmalıdır. Ülkenin kritik altyapılarının bilişim sistemlerinin siber saldırılara karşı savunulması ve güvenliğinin sağlanması ulusal gücün korunması için de temel şartlardan birisi olduğu her zaman ön planda tutulmalıdır.

Her türlü saldırıya ve dolayısıyla savaşa karşı öncelikle güçlü ve eksiksiz bir savunma gerekmekte, anca tarihte sadece savunmayla hiçbir zafer kazanılmamış, karşı saldırı ve taarruz yeteneğinin de kazanılmasının ve kullanılmasının gerekli ve kaçınılmaz bir zorunluluk olduğu anlaşılmıştır [22]. Özellikle siber ortamda savunma veya taarruz şeklinde icra edilecek mücadele ve savaşlarda, maksat istek veya istekleri karşı tarafa zorla kabul ettirmek ve temel amaç kazanmak olsa da, saldırganları saldırılarından veya savaştan vazgeçirmek için siber caydırıcılık konusu hiçbir zaman unutulmamalıdır.

Siber savaşlarda başarı, siber savaşın doğası gereği siber gücün yeterince güçlü olmasına ve etkin kullanımına bağlıdır. Siber saldırılara karşı konulacağını ve bir saldırı durumunda bunun saldırgana misliyle ödetileceğini göstererek onu saldırıdan caydırmak, bütün bunlar için de etkin bir siber istihbarat yeteneğine sahip olmak, etkili bir siber istihbarata dayanan siber savunma, taarruz ve caydırıcılık yetenekleri toplamı siber güçle bunu desteklemek şarttır. Etkili bir siber güç için özellikle bilgi, bilgisayar ve iletişim konularında milli teknolojilere sahip olmak, milli teknolojilere sahip olunamayan alanlarda sahip olunan teknolojilere hâkim olmak gerekmektedir [22].

Siber gücün geliştirilerek artırılması ve etkin şekilde kullanılması için kullanıcıların yetiştirilmesi ve farkındalıklarını artıracak eğitimler verilmesi çok önemlidir. Kullanıcıların eğitimleri, siber güvenlik ve savunma için önemli olduğu kadar, gerektiğinde saldırı ve taarruz için de bazı görevlerin etkinlikle yerine getirilmesi [22], dolayısıyla siber caydırıcılık sağlamak için de önemlidir.

Siber caydırıcılıkta temel esas ve önemli olan siber saldırıların/savaşın doğru zamanda, doğru hedefe yönelik, doğru teknik ve yöntemlerle yapılmasıdır. Uygulanması zor olmakla birlikte, ülkenin siber güvenliği ve savunmasına daha fazla katkı sağlaması yanında, maliyet ve kullanım kolaylıkları yanında asimetrik saldırı/savaş imkânı da sağlaması nedeniyle "Siber Güçle Caydırıcılık"; üzerinde düşünülmesi, daha fazla önem verilmesi, diğer alanlardaki caydırıcı gücün bu alanda da oluşturulması için ciddi ve ayrıntılı olarak çalışılması, konuyla ilgili doktrinler üretilmesi, stratejiler geliştirilmesi ve geleceğe dönük planlamalar yapılarak uygulanması gereken çok önemli bir konudur [39].

Sonuç olarak; bugünün savaşları olarak gündemde olan ve gelecekte de geliştirilerek uygulanmaya devam edilecek olan 4'üncü Nesil veya Hibrit savaşlar ile bu kapsamda siber savaş ve siber caydırıcılık konularında yeni çalışmalar yapılması, konunun farklı boyutlarıyla ele alınması, bu konuda tezler üretilmesi, ulusal özgün ürün ve teknolojilerin geliştirilmesi, gerekli yatırımların yapılması ve en önemlisi insan kaynağı olarak siber alanda caydırıcı güçlerin oluşturularak geliştirilmesinin ülke siber savunması ve güvenliğine çok büyük katkılar sağlayacağı değerlendirilmektedir.

Kaynaklar

[1] TDK Sözlüğü, Savaş, Hibrit, Güvenlik, İstihbarat caydırıcılık http://www.tdk.gov.tr/index.php?option=com_bts (Erişim: 15 Mayıs 2018).

[2] Güray Alpar, Uluslararası İlişkilerde Strateji ve Savaş Kültürünün Gelişimi, Palet Yay., Konya, 2015.

[3] Ali Bilgin Varlık, Savaşı Tanımlamak: Terminolojik Bir Yaklaşım. Avrasya Terim Dergisi, Sayı 1 (2), Eurasscience Journals, 2013.

[4] Carl von Clausewitz, Harp Üzerine, Gnkur. Basımevi, Ankara, 1991.

[5] Yasin Aslan, "Savaş Hukukunun Temel Prensipleri", Türkiye Barolar Birliği Dergisi, Sayı 79, Ankara, 2008.

[6] Mehmet Yayla, Hukuki Bir Terim Olarak Siber Savaş, Türkiye Barolar Birliği Dergisi, Sayı 104, Ankara, 2013.

[7] Resmi Gazete, Seferberlik ve Savaş Hali Kanunu, http://www.resmi gazete. gov.tr/arsiv/18215.pdf, (Erişim:17 Haziran 2018).

[8] Albertas Kondrotas, Private Armies Throughout The Generations Of Warfare; Pitfalls And Prospects, National Defence Academy, Estonia, 2010.

[9] William S. Lind, Understanding Fourth Generetion War, https://original.antiwar.com/lind/2004/01/15/understanding-fourth-generation-war/, (Erişim:20 Haziran 2018).

[10] Thomas X. Hammes, The Sling and the Stone: On War in the 21st Century, Zenith Press, ABD, 2006.

[11] Oxford English Dictionary, Hybrid, https://en.oxforddictionaries.com/ definition/hybrid, [Erişim: 21 Haziran 2018).

[12] Ali N. Karabulut, Eski Savaş, Yeni Strateji: Rusya'nın Yirmibirinci Yüzyıldaki Hibrit Savaş Doktrini ve Ukrayna Krizi'ndeki Uygulaması", Uluslararası İlişkiler Dergisi, Cilt 13, Sayı 49, İstanbul, 2016.

[13] F.G. Hoffman, Conflict in the 21 Century, Potomac lnstitute for Policy Studies, ABD, 2007.

[14] Loretta Sanchez vd., Hybrid Warfare, Briefing to the Subcommittee on Terrorism, Unconventional Threats and Capabilities, Committee on Armed Services, House of Representatives, GAO, ABD, 2010.

[15] S.D. Bachmann, Hybrid Wars - The 21st Century's New Threats To Global Peace And Security, Scientia Militaria, South African Journal of Military Studies, Vol 43, No. 1, Güney Afrika, 2015.

[16] Lawrence Freedman, Ukraine and the Art of Limited War, survival global politics and strategy journal, 56:6, ABD, 2014.

[17] T.X. Hammes, The Future of Conflict, Charting a Course: Strategic Choices for a New Administration, NDU Press, ABD, 2016.

[18] Banu Avar, Zemberek, Remzi Kitabevi, İstanbul, 2012.

[19] Nihat Dumlupınar, Hibrit Savaş: İran Silahlı Kuvvetleri, Uluslararası Kriz ve Siyaset Araştırmaları Dergisi, Sayı 1(2), Ankara, 2007.

[20] M. Kofman, ve M. Rojansky, A closer look at Russia's "Hybrid War". Kennan Cable - Kennan Institute, No:7, ABD, 2015.

[21] Janis Berziņs "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy", National Defense Academy of Latvia Center for Security and Strategic Research Policy Paper No:02, Letonya, 2014.

[22] Mustafa Şenol, Siber Güçle Caydırıcılık Ama Nasıl?, Gazi Üniv. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:2, No:2, Ankara, 2016.

[23] P.W. Singer ve Allan Friedman, Siber Güvenlik ve Savaş, Buzdağı Yayınları, Ankara, 2015.

[24] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016-2019 Ulusal Siber Güvenlik Stratejisi, UDHB Gn.Md.lüğü Yay.Ankara, 2016.

[25] Richard A Clarke ve Robert, K.Knake, Siber Savaş, İKÜ Yayınları, İstanbul, 2010.

[26] Mehmet Akif Ocak vd., Güncel Tehdit Siber Suçlar, Seçkin Yayınları, Ankara, 2014.

[27] Oğuz Turhan, Bilgisayar Ağları İle İlgili Suçlar, Başbakanlık DPT Müsteşarlığı Yay. Ankara, 2006.

[28] Mehmet Yayla, Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı, Hacettepe HFD, Cilt:4/2, Ankara, 2014.

[29] Alexander Klimburg, National Cyber Security Framework Manual, NATO Yayını, Estonya, 2012.

[30] BM Terimler Sözlüğü, https://unterm.un.org/UNTERM/display/Record/UNHQ/NA?OriginalId=e996b25ea7d3b36e85256b090056d806, (Erişim: 25 Haziran 2018).

[31] Mehmet Yayla, Hukuki Bir Terim Olarak Siber Savaş, Türkiye Barolar Birliği Dergisi, Sayı 104, Ankara, 2013.

[32] M.C. Libicki, Cyberdeterrence and Cyberwar, RAND Corporation, ABD, 2009.

[33] Sun Tzu, Savaş Sanatı, Türkiye İş Bankası Kültür Yayınları, İstanbul, 2014.

[34] Atalay Keleştemur, Siber İstihbarat, Level Kitap-Umuttepe Yayınları, İstanbul, 2015.

[35] Joseph S. Nye. ve David A. Welch, Küresel Çatışmayı ve İşbirliğini Anlamak, T.İşbankası Kültür Yay., İstanbul, 2010.

[36] Erol Mütercimler, Geleceği Yönetmek ve Düşünmek İçin Stratejik Düşünme, Alfa Yayınları, İstanbul, 2006.

[37] Joseph S. Nye, Cyber Power, http://belfercenter.ksg.harvard.edu/ files/ cyber-power.pdf, (Erişim:30 Haziran 2018),

[38] G. Canbek ve Ş. Sağıroğlu, Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme, Politeknik Dergisi, Cilt: 9 Sayı: 3, Ankara, 2006.

[39] Mustafa Şenol, Türkiye'de Siber Saldırılara Karşı Caydırıcılık, Gazi Üniv. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:3, No:2, Ankara, 2017.

[40] B.H. Liddell Hart, Strateji Dolaylı Tutum B.H., Gnkur. ATASE Bşk.lığı Yay., Ankara, 1973.

[41] Zahir Kızmaz, Ceza veya Kriminal Yaptırımın Suç Oranları Üzerindeki Caydırıcı Etkisi, Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi, Cilt:7, Afyonkarahisar, 2005.

[42] Haluk Özdemir, Uluslararası İlişkilerde Güç-Çok Boyutlu Bir Değerlendirme, Cilt:63, Sayı:3, Ankara Üniversitesi SBF Dergisi, Ankara, 2008.

[43] M.T. Akad, Modern savaşın Temel Kavramları, Kitap Yayınevi, Ankara, 2011.

[44] Austin Long, Deterrence From Cold War to Long War, RAND Corporation, ABD, 2008.

[45] Amir Lupovici, Cyber Warfare and Deterrence. Military and Strategic Affairs, Volume:3, No:3, İsrail, 2011.

[46] S. Gorman, ve J.E. Barnes, Cyber Combat: Act of War, http://www. wsj. com/articles/SB10001424052702304563104576355623135782718, (Erişim: 25 Haziran 2018).

[47] Dorothy Denning, Cybersecurity's Next Phase: Cyber-deterrence, https://theconversation.com/cybersecuritys-next-phase-cyber-deterrence-67090, (Erişim: 15 Temmuz 2018).

[48] Will Goodman, Cyber Deterrence Tougher in Theory than in Practice?, http://www.au.af.mil/au/ssq/2010/fall/goodman.pdf, (Erişim: 17 Temmuz 2018).

[49] Chrıstopher Hale, A Theory Of Cyber Deterrence, https://www.georgetownjournalofinternationalaffairs.org/online-edition/a-theory-of-cyber-deterrence-christopher-haley, (Erişim: 17 Temmuz 2018).

[50] Eric Talbot Jensen, Cyber Deterrence, Emory International Law Review 773 (2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2070438, (Erişim: 18 Temmuz 2018).

[51] Viljar Veebel, Baltic States and Cyber Deterrence: Taking or Losing Initiative against Russia?, http://www.fpri.org/article/2017/01/baltic-states- cyber-deterrence-taking-losing-initiative-russia/, (Erişim: 20 Temmuz 2018).

[52] Atatürk'ün Söylev ve Demeçleri, Türk İnkılap Enstitüsü Yay.-1, Cilt:2, Ankara, 2006.

[53] Mehmet Gönlübol, Atatürk'ün Dış Politikası; Amaçlar ve ilkeler, Atatürk Yolu Dergisi, Ankara, 1981.

[54] Güray Alpar, Uluslararası İlişkilerde Strateji ve Savaş Kültürünün Gelişimi, Palet Yay., Konya, 2015.

[55] Peter Paret, Modern Strateji Machiavelli'den Nükleer Çağa, Doruk Yay., İstanbul, 2015.

[56] Damien Van Puyvelde, Hybrid war-does it even exist?, NATO Review Magazine, https://www.nato.int/docu/review/2015/also-in-2015/ hybrid-modern-future-warfare-russia-ukraine/en/index.htm, (Erişim: 25 Temmuz 2018).

[57] Richard Lim, Innovation and Invention: Equipping the Army for Current and Future Conflict. The Institute of Land Warfare - National Security Watch, ABD, 2015.

Kötü Amaçlı Yazılımlar ve Analizi

BÖLÜM 8

Prof. Dr. Refik SAMET
Ömer ASLAN

KÖTÜ AMAÇLI YAZILIMLAR VE ANALİZİ

Kötü amaçlı yazılımlar dinamik olup zaman zaman saldırı biçimini ve hedefini değiştirerek sürekli gelişme gösteren yazılımlardır. Bu yazılımları tespit etmek ve bulaştıkları sistemlerle olan etkileşimlerini anlamak için analiz edilmeleri gerekmektedir. Kötü amaçlı yazılım analizi bu yazılımların nasıl çalıştığını anlamak, tespit etmek ve yayılmasını engellemek amacıyla yapılan çalışmaları kapsamaktadır. Bu bölümde bu yazılımların nasıl analiz ve tespit edileceğiyle ilgili güncel bilgiler bulunmaktadır. Her ne kadar yeni teknik ve yöntemler kullanılsa da bütün kötü amaçlı yazılımları %100 başarı oranıyla analiz ve tespit etmek mümkün görünmemektedir.

8.1. Giriş

Son yıllarda sosyal ve modern kültürün bir zorunluluğu olarak bilgisayar, mobil ve İnternet teknolojilerinin kullanımı tüm dünyada hızla artmıştır. Bu teknolojilerin aşırı yaygınlaşması aynı zamanda birçok siber güvenlik sorununu da beraberinde getirmiştir. Daha önce basit ve amaçsızca yapılan siber saldırılar, yerini daha geniş çaplı ve hedef odaklı saldırılara bırakmıştır. Yapılan araştırmalar siber kaynaklı güvenlik saldırılarının büyük bölümünün kötü amaçlı yazılımlar (Malicious Software - Malware) kullanılarak yapıldığını göstermektedir. Kötü amaçlı yazılımlar kullanıcı bilgisi dışında sistem üzerinde istenmeyen değişiklikler yapan yazılımlar olarak tanımlanabilir. Truva atları, virüsler, solucanlar, yazılım bombaları, fidye yazılımları, robotlar ve casus yazılımlar kötü amaçlı yazılımlara örnek olarak gösterilebilir. Daha önce basit amaçlarla yazılan bu yazılımlar yerini geniş çaplı büyük şirketlerin ve devletlerin olduğu bir sektöre bırakmıştır.

Kötü amaçlı yazılımlar var olan sistem ve uygulama programlarındaki açıklardan ve zafiyetlerden (arabellek taşması, hassas verilerin şifrelenmemesi, kritik işlemler için kimlik doğrulanmaması, vb.) faydalanarak saldırı başlatmaktadırlar. Yapılan akademik araştırmalar ve yazılan bilimsel raporlar, kötü amaçlı yazılım kaynaklı saldırıların her geçen gün artan oranda devam ettiğini ve dünya ekonomisine verdiği zararın da aynı ölçüde arttığını göstermektedir. 2000 yılında "I love you" virüsünün dünya ekonomisine verdiği toplam zarar yaklaşık 15 milyar dolar, "MyDoom" solucanının 2004 yılında verdiği toplam zarar ise yaklaşık 38 milyar dolar olduğu tahmin edilmektedir [Anonymous1, Anonymous2]. Siber güvenlik raporuna göre siber kaynaklı saldırıların dünya ekonomisine verdiği toplam zarar 2015 yılında 3 trilyon dolar olduğu, 2021 yılında bu zararın yaklaşık 6 trilyon dolar olacağı tahmin edilmektedir [Steve Morgan, 2016]. Bahsedilen örneklerden de anlaşıldığı üzere bu yazılımlar hem dünya ekonomisine büyük zararlar vermekte, hem de birçok kişisel ve kurumsal veri risk altında bulunmaktadır. Bu sebepler kötü amaçlı yazılımlara karşı geniş çaplı önlem almanın gerekliliğini ortaya koymaktadır.

Kötü amaçlı yazılımların sürekli şekil ve yöntem değiştirmesi ile uzun yıllardır koruma ve tespit amaçlı kullanılan güvenlik duvarı, saldırı tespit ve koruma sistemleri, anti virüs yazılımları, vb. yöntemler bu yazılımları tespit etmede yetersiz kalmıştır. Bundan dolayı davranış ve kural tabanlı çalışan yeni nesil kötü amaçlı yazılımları da tespit eden sistemler geliştirilmeye başlanmıştır. Bu yöntemlerde kötü amaçlı yazılımlar öncelikle detaylı olarak analiz edilerek (elle veya otomatik) belirli özellikler çıkartılmakta ve bu özelliklere veri madenciliği ve makine öğrenmesi teknikleri uygulanarak tespit işlemi gerçekleştirilmektedir. Bu bölümün amacı kötü amaçlı yazılımların analizini yaparak bu yazılımların çalışma mantığını ve davranışlarını anlamak, bu yazılımları tespit etmek için kullanılabilecek yöntemleri açıklamak ve yayılmasını engellemek amacıyla alınması gereken önlemleri sıralamaktır. Diğer bir ifadeyle, hangi makine ve programların etkilendiğini, sistemdeki hangi güvenlik zafiyetleri kullanılarak saldırının başlatıldığını, hangi verilerin zarar gördüğünü veya çalındığını ve yapılabilecek potansiyel saldırıları önceden belirlemek amaçlanmaktadır. Bu bölümün kalan kısmı şu şekilde organize edilmiştir. Bölüm 8.2'de siber saldırı türleri ve

saldırılarda kullanılan kötü amaçlı yazılım çeşitleri kısaca anlatılmaktadır. Bölüm 8.3'te, yeni nesil kötü amaçlı yazılımlardan bahsedilmektedir. Bölüm 8.4'te, kötü amaçlı yazılım analiz yöntemleri anlatılmaktadır.

8.2. Siber Saldırı Türleri ve Saldırılarda Kullanılan Kötü Amaçlı Yazılım Çeşitleri

Birçok siber saldırının kökeninde kötü amaçlı yazılımlar bulunmaktadır. Son yıllarda kötü amaçlı yazılımlar kullanılarak hedef odaklı siber saldırılar yapılmaktadır. Bu saldırılar şöyle sıralanabilir: 1) Küresel tehditler (Global threats); 2) Gelişmiş kalıcı tehditler (APT) ve 3) Hizmeti engelleme saldırıları (DOS) [Pilling, 2013]. İleri düzey tehditler olarak bilinen küresel tehditler, APT ve DOS saldırıları genelde birden fazla kötü amaçlı yazılım türü (örneğin, virüs, Truva atı, arka kapı, vb.) kullanılarak yapılmaktadır.

1) Küresel Tehditler

Küresel boyuttaki tehditler genelde elektronik e-posta ve İnternet tarayıcılarındaki savunmasızlıklardan yararlanarak tüm Dünya'yı etkilemektedir. Bu tip saldırılarda çok sayıda bilgisayar kullanılarak bir sisteme saldırı yapılır (örneğin, BOTNET). Bu durumda hem saldırının asıl kaynağını belirlemek zorlaşır hem de birçok farklı sistem saldırıya katıldığı için saldırının başarılı olma ihtimali artar.

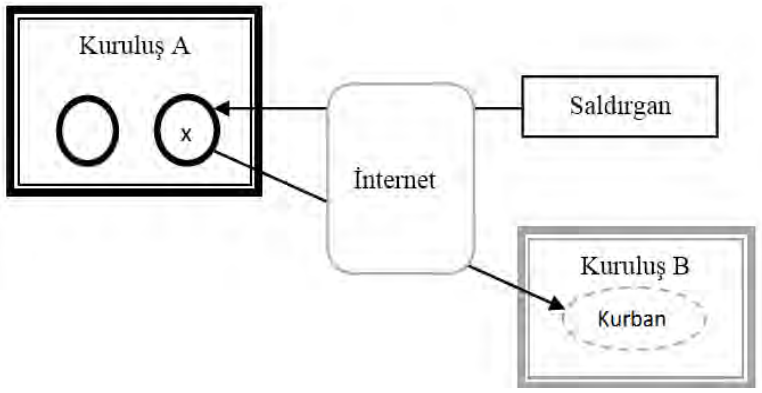
2) Gelişmiş Kalıcı Tehditler

Gelişmiş kalıcı tehditler son dönemlerde öne çıkan saldırıların başında gelmektedir. Bu tehditler hedef odaklı saldırılar olup belli kurum ve kuruşlara yönelik yapılmaktadır. Bu saldırılar sonucunda saldırılan sistem hem büyük zarar görmekte hem de sistemi eski haline getirmek zorlaşmaktadır. Saldırıların hedefinde genelde kurumların finansal kaynakları ve popülerliklerine zarar vermek yatmaktadır.

3) Hizmeti Engelleme Saldırıları

Hizmeti engelleme saldırıları, saldırı yapılan sisteme aşırı miktarda büyük boyutlu veriler göndererek veya çok farklı kaynaktan sürekli benzer veriler göndererek, sistemin cevap veremez hale getirilmesidir. Bu saldırılar farklı şekillerde başlatılabilmekte ve genelde sa-

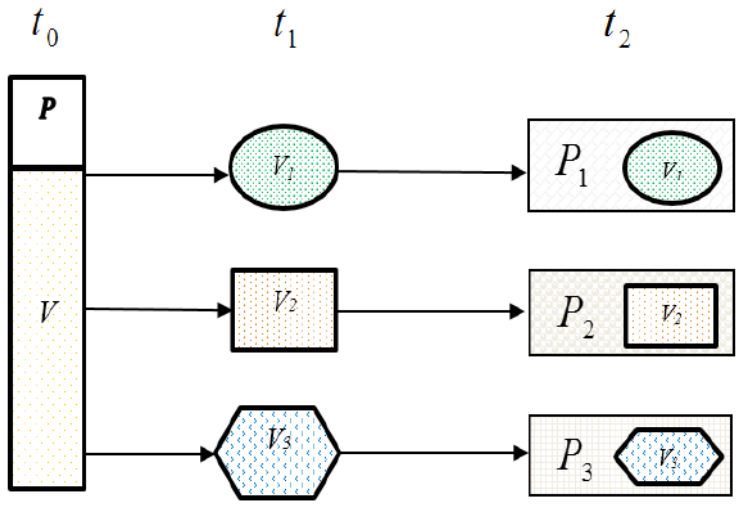
vunmasız bilgisayarlar (Zombi) kullanılarak yapılmaktadır. Saldırı esnasında zombi bilgisayarların kullanılması [Lachow, 2013] ya da başka bir kullanıcının IP adresinden geliyor gibi gösterilmesi, bu saldırıyı başlatan ana kaynağı bulmayı imkansız hale getirmektedir (Şekil 8.1).



Şekil 8.1. Saldırganın siber saldırı sırasında kaynağını gizlemesi

Virüsler, solucanlar, Truva atları, arka kapılar, fidye yazılımları, korsan amaçlı kullanılan yazılımlar, robotlar ve casus yazılımlar yukarıda bahsedilen tehdit ve siber saldırılarda yaygın olarak kullanılan kötü amaçlı yazılımlardır. Aşağıda bu yazılımların kısa tanımları verilmektedir.

8.2.1. Virüsler (Viruses): Çoğalmaları için başka programlara ihtiyaç duyan ve içinde kötü amaçlı kod parçacıkları barındıran programlardır. Bu programlar girdiği sistemlerde sistem dosyalarında değişiklik yaparak çalışmaz hale getirebilir; istenmeyen görüntülerin ekranda görünmesine neden olabilir ya da veriler üzerinde değişiklikler yapabilirler. Virüsler diğer programlara kendilerini enjekte ederek bu programların da virüs haline gelmelerine neden olmaktadırlar. Basit anlamda virüs 3 ana evreden oluşmaktadır: çoğalma, programın tetiklenmesi ve önceden amaçlanan zararın verilmesi. Gelişmiş virüsler varlıklarını gizlemek için bazı gizlenme teknikleri kullanmaktadırlar (Örneğin, obfuscation, packed, encryption). Varlıkları anti-virüs yazılımları ve kötü amaçlı yazılım algılama sistemleri kullanılarak belirlenebilir. "Creeper", "Chernobly (CIH)" "Melissa" ve "ILOVEYOU" yaygın olarak bilinen virüslerdir. Şekil 8.2, virüsün şekil değiştirerek yayılmasını göstermektedir.



Şekil 8.2. Virüsün şekil değiştirerek yayılması

t, P,V, V_1,V_2,V_3 ve P_1,P_2,P_3 sırasıyla zaman dilimi, program, payload (viral set- zararlı kod kısmı), payload'un farklı formları ve diğer programları göstermektedir. t_0 zamanında P programına virüs (V) bulaşmıştır. t_1 zamanında virüs mutasyona uğrayarak 3 farklı formunu V_1,V_2,V_3 oluşturmuştur. t_2 zamanında bu farklı formda bulunan zararlı kod parçaları P_1,P_2,P_3 programlarına kopyalanmıştır. Her V'nin virüs imzası farklı olduğu için normal antivirüs tarayıcılarıyla tespit edilmeleri zordur.

8.2.2. Solucanlar (Worms): Bilgisayar ağlarını kullanarak bir sistemden diğerine bulaşan ve bulaştığı sistemlerde genelde izinsiz girişlere neden olan programlardır. Virüslerin aksine çoğalmaları için başka programlara ihtiyaç duymazlar. Bulaştığı sistemde kendilerini gizleyebilmek için kendi dosyalarını silerler. Solucanlar genelde sistemlerde arka kapı açarak bu sistemleri başka saldırılarda kullanırlar. Son dönemlerde virüs-solucan karışımı programlar görülmeye başlanmıştır. Solucanlar genel olarak 4 farklı bölümden oluşmaktadır: 1)Hedef keşfi, 2)Yayılma ve dağıtım mekanizması, 3) Aktivasyon ve 4)Payload [Nazario, 2004; Christoffersen, 2006; Pratama, 2012]. "Code Red", "Nimda", "MyDoom", "Conficker" ve "Stuxnet" yaygın olarak bilinen bilgisayar solucanlarıdır.

8.2.3. Truva Atları (Trojan Horses): Truva atları normal bir program gibi görünen gerçekte ise kötü amaçlı kodlar barındıran prog-

ramlardır. Sistemleri etkileyebilmeleri için iliştirilen programın çalıştırılması gerekmektedir. Bu tür yazılımlar sistemde arka kapılar açabilmekte, girdiği sisteme izinsiz olarak uzaktan erişime neden olabilmekte ya da bilgisayarda depolanan kritik bilgileri karşı tarafa gönderebilmektedir. Bulaştığı sistemlerde fark edilmeleri zordur, fakat bulaştığı sistemleri genelde yavaşlattıkları için varlıkları ancak uzun uğraşlar sonucunda öğrenilebilir. Truva atları, virüsler ve solucanlar gibi başka dosyaları enfekte ederek çoğalmazlar ve kendi kendini kopyalamazlar [Siddiqui, 2008]. Truva atları oluşturulma amaçlarına ve vereceği zarara göre çeşitli gruplara ayrılmaktadır: "Trojan-Banker", "Trojan-DdoS", "Trojan-Downloader", "Trojan-GameThief", vb. "Zeus" ailesi yaygın olarak bilinen Truva atlarolarak ına örnek gösterilebilir.

8.2.4. Arka Kapılar (Backdoors): Geleneksel güvenlik mekanizmalarını atlatarak kullanıcı bilgisi dışında sistemi uzaktan erişime açan programlardır. Arka kapılar genelde Truva atları kullanılarak kurban sistemlere yüklenir ve sadece arka kapıyı oluşturan kişiler tarafından bilinir. Ayrıca, oluşturulan arka kapılar daha sonra yapılacak karmaşık saldırılar için virüs ve solucanlar tarafından kullanılırlar [Davis vd. 2009]. "FinFisher (FinSpy)", "Tixanbot" ve "Briba" iyi bilinen arka kapılara örnek gösterilebilir.

8.2.5. Fidye Yazılımları (Ransomware): Kötü amaçlı yazılımlardan biri olup, bulaştığı sistemde sistemin bir kısmını veya tamamını şifreleyerek, verilerin kullanıcı tarafından görüntülenmesini engelleyen programlardır. Kullanıcı, verilerini görüntüleyebilmek için saldırganın talep ettiği parayı ödemesi gerekmektedir. Ayrıca, paranın ödenmesi sistem verilerine erişimi garanti etmez. "Wannacry" (2017), "NotPetya" (2016), "SimpleLocker" (2015-2016), "CryptoLocker" (2013-2014), "TB-Locker" (2014), "WinLock" (2010) en iyi bilinen fidye yazılımlarıdır. "Symantec" 2017 raporuna göre son yıllarda fidye yazılımlarında hem sayı olarak hem de dünya ekonomisine verdiği zarar yönünden büyük bir artış görülmüştür [Symantec, 2017].

8.2.6. Korsan Amaçlı Kullanılan Yazılımlar (Rootkits): Bir bilgisayar sistemine yönetici düzeyinde erişim hakkı veren ve dosyalarını ve sistem bilgilerini işletim sisteminden gizlemek suretiyle varlığını

gizlice sürdüren programlar grubudur. En tehlikeli kötü amaçlı yazılımların başında gelen korsan amaçlı kullanılan yazılımların asıl amacı çoğalmak değil, bulunduğu sistemde varlığını gizlemektir. Genellikle tek başlarına pek zararlı görünmeyen bu yazılımlar virüs, solucan ve Truva atlarıyla birleşerek çok yıkıcı saldırılar başlatabilmektedirler. İşletim sistemi seviyesinde işlem ve değişiklik yapabildikleri için hem girdikleri sistem için büyük tehlike oluşturmakta hem de anti virüs yazılımları tarafından tespit edilmeleri zorlaşmaktadır [Davis, 2009]. Oluşturulma amaçlarına göre farklı türlere ayrılmaktadır: "kernel rootkits", "firmware rootkits", "application rootkit", "memory rootkit", "persistent rootkit", vb.

8.2.7. Robotlar (Bots): Botnetler bir dizi robotlardan oluşup zafiyetli bilgisayar ve sistemlere veriler göndererek daha sonra bu bilgisayarları yapacakları saldırılarda kullanılırlar. Robotlar: saldırgan, komuta ve kontrol mekanizması ve zombi bilgisayarlardan oluşur. Saldırgan kontrol mekanizması sayesinde savunmasız bilgisayarları bulur ve bu bilgisayarları kullanarak belirlenen kurbana saldırı yapılır. Botnet kullanılarak sistemler çalışmaz hale getirilebilir, zombi olarak kullanılan bilgisayarlardan önemli bilgiler çalınabilir ya da zombi bilgisayarlar para karşılığı üçüncü kişilere kiraya verilebilirler [Jang-Jaccard ve Nepal, 2014]. Robotlar tarafından yaygın olarak başlatılan saldırılar şöyle sıralanabilir: "DDoS", "spamming", "sniffing traffic", "spreading new malware", vb.

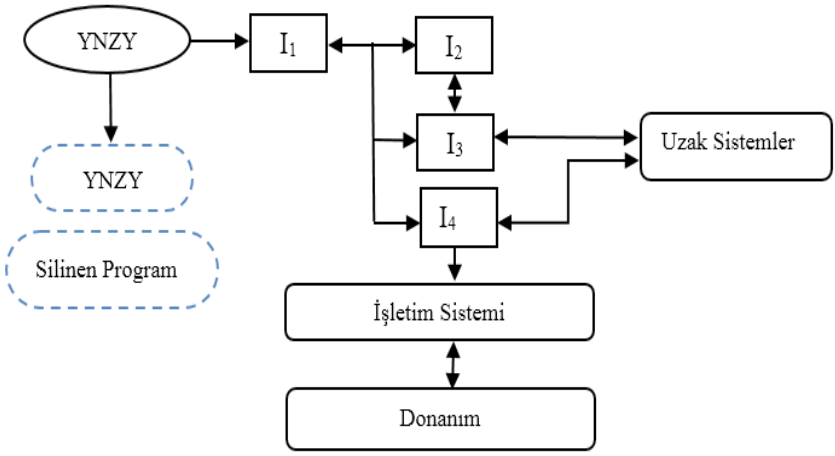
8.2.8. Casus Yazılımlar (Spyware): Kullanıcı ve şirket bilgilerini gizlice toplayıp saldırgan ya da üçüncü kişilere gönderen yazılımlardır. Genellikle kredi kartı bilgilerine erişmek veya kullanıcı alışkanlıklarını saptamak amacıyla yaygın olarak kullanılmaktadırlar. Bu yazılımlara örnek olarak "Keylogger" gösterilebilir. "Keylogger" arka planda çalışıp klavyeden yapılan her vuruşu kaydeden ve bu kayıtları saldırganlara gönderen programlardır. Casus yazılımlar web sitelerine ya da ücretsiz paylaşılan yazılımlara gömülerek yayılmaktadırlar [Stallings vd. 2012]. Bu siteler ziyaret edildiğinde veya bu programlar bilgisayarınıza indirildiğinde sisteminize bulaşmaktadırlar. "CoolWebSearch", "Cydoor" , "BlazeFind" ve "Gator" yaygın olarak bilinen casus yazılımlara örnek gösterilebilir.

Son dönemlerde kötü amaçlı yazılımların hem sayı olarak artması hem de şekil değiştirmesi, siber saldırı miktarı ve şiddeti yönünden

de bir artışa neden olmuştur. "Stuxnet" (2010) ve "Dragonfly" (2014) gibi yeni nesil kötü amaçlı yazılımlar kullanılarak hedef odaklı, kalıcı ve küresel boyutta olan siber saldırılar yapılmaya başlanmıştır. Saldırılarda birden fazla zararlı yazılımın da birlikte kullanılması (örneğin, virüs, solucan, Truva atı, arka kapı, vb.) bu tür siber saldırıları engellemeyi ve tespit sürecini zorlaştırmaktadır. Bundan dolayı yeni nesil kötü amaçlı yazılımlar da göz önünde bulundurularak yeni savunma yazılımlarının geliştirilmesi gerekmektedir.

8.3. Yeni Nesil Kötü Amaçlı Yazılımlar

Kötü amaçlı yazılımların atası olarak kabul edilen virüsler düşünsel olarak kendi kendini kopyalayan "automata" olarak John von Neumann tarafından 1950'li yıllarda ortaya atılmasına karşın, pratik olarak ilk virüs 1971 yılında "the Crepeer" adı altında Bob Thomas tarafından laboratuvar ortamında geliştirilmiştir [Spencer, 2011; Anonymous3]. İlk yıllarda basit amaçlarla yazılan bu yazılımlar zamanla yerini geniş çaplı büyük şirketlerin ve devletlerin olduğu yeni nesil kötü amaçlı yazılımlara bırakmıştır. Çekirdek modunda da çalışabilen ve kullanıcı modunda çalışan geleneksel kötü amaçlı yazılımlara göre çok daha güçlü ve tespit edilmeleri zor olan yazılımlar yeni nesil kötü amaçlı yazılımlar olarak tanımlanabilir. İşletim sistemi denetim özelliklerinin çekirdek modunda uygulanamaması ve üçüncü parti davranış izleme araçlarının tam ve verimli çalışmaması yeni nesil kötü amaçlı yazılımların tespitini zorlaştırmaktadır. Bu kötü amaçlı yazılımlar çekirdek modunda çalışan koruma yazılımlarını (örneğin, virüsten koruma yazılımları, güvenlik duvarları, vb.) rahatça atlatabilmektedirler. Ayrıca, bu yazılımlar kullanılarak daha önce görülmemiş, hedef odaklı, kalıcı ve birden fazla kötü amaçlı yazılım türünün katılarak gerçekleştirildiği ileri düzey siber saldırılar yapılmaktadır. Şekil 8.3, yeni nesil kötü amaçlı yazılım örneğini göstermektedir.



Şekil 8.3. Yeni nesil bir kötü amaçlı yazılımın şekilsel gösterimi

Şekil 8.3'de YNZY, yeni nesil zararlı yazılımı ve (I_1, I_2, I_3, I_4) çalışan işlemleri (işletim sisteminde derlenmiş ve çalışır durumda olan programlar- "işlem") göstermektedir. Kötü amaçlı yazılım öncelikle kendini farklı program ya da işlemlere kopyalamakta (YNZY→I_1), kendi kopyasını oluşturabildiği gibi sistemde arka kapı açarak farklı sistemlere de bağlanabilmekte, daha sonra kendini sistemden silerek görünmez olmaktadır (Şekil 8.3). En son kendini kopyaladığı işlemler yardımıyla (I_1→I_2, I_1→I_3, I_1→I_4) sistem üzerinde daha önce belirtilen değişiklikleri yapmakta ve uzak sistemlerle bağlantı kurmaktadır. Asıl zararlı kodları barındıran kötü amaçlı yazılımın sistemden kendini silmesi ve daha önce belirtilen zararlı davranışları farklı işlemlere (Var olan sistem dosyaları, üçüncü parti yazılımlar ya da kötü amaçlı yazılım tarafından yeni oluşturulmuş işlemler) yaptırması, kötü amaçlı yazılım analiz ve tespitini nerdeyse imkansız hale getirmektedir. Şekil 8.3'te belirtilen kötü amaçlı yazılımın tespit edilebilmesi için hem I_1, I_2, I_3 ve I_4 işlemlerinin ayrı ayrı incelenmesi gerekmektedir hem de bu işlemler arasındaki ilişkiler belirlenmelidir.

İnternet teknolojilerinin hızla gelişimiyle birlikte bilgisayar koruma sistemleri (Örneğin, anti virüs programları; güvenlik duvarları; saldırı tespit, önleme ve koruma sistemleri, vb.) hızlı bir gelişme göstermiştir. Koruma sistemlerinin bu hızlı gelişimi geleneksel kötü amaçlı yazılımların kolayca tespit edilmesini sağlamıştır. Bu durum bilgisayar korsanlarını (Hackers) daha karmaşık ve tespit edilme-

si zor yazılımlar yazmaya sevk etmiştir. Artık bir işlemden oluşan ve basit saldırılar yapabilen yazılımlar yerine çok işlemli, şifreleme teknikleri kullanarak şekil değiştirebilen, hedef odaklı, daha önce görülmemiş siber saldırılar başlatan yazılımlara dönüşmüşlerdir. Sürekli kendilerini yenileyerek farklı şekillere girebilen bu yazılımlar son dönemlerde işletim sistemi seviyesinde de çalışamaya başlamışlardır. Tablo 8.1'de geleneksel ve yeni nesil kötü amaçlı yazılımların karşılaştırılması görülmektedir.

Tablo 8.1. Geleneksel ve yeni nesil kötü amaçlı yazılımlar

Geleneksel Kötü Amaçlı Yazılım Özellikleri	Yeni Nesil Kötü Amaçlı Yazılım Özellikleri
Genelde 1 işlemden oluşmakta	1'den fazla işlemden oluşmakta
Sınırlı sayıda işlemle iletişimde bulunmakta	Var olan işlemleri etkilemekte
Sistemi 1 sefer etkilemekte	Sistemde kalıcı hale gelmekte
Gizlenme ihtiyacı duymamakta	Gizlenme teknikleri kullanmakta
Genel saldırılar başlatmakta	Hedef odaklı saldırılar başlatmakta
Genelde .exe dosyaları yoluyla yayılmakta	Genelde .dll dosyaları yoluyla yayılmakta
Her kopyanın aynı ya da benzer olması	Her kopyanın farklı olması

Kötü amaçlı yazılımların atası olarak kabul edilen virüsler zamanla şekil ve yöntem değiştirerek geleneksel kötü amaçlı yazılımların oluşmasına ve daha da gelişerek yeni nesil kötü amaçlı yazılımları oluşturmuşlardır. Sık sık değişik gizlenme teknikleri kullanan yeni nesil kötü amaçlı yazılımlar hem analiz ve tespit edilmeyi zorlaştırmakta hem de daha ileri düzey siber saldırılar başlatabilmektedirler. Bundan dolayı bu kötü amaçlı yazılımların oluşturduğu ve oluşturacağı olumsuz sonuçları belirlemek adına bu yazılımların daha geniş çaplı olarak analiz edilmesi gerekmektedir.

8.4. Kötü Amaçlı Yazılım Analizi

Kötü amaçlı yazılım analizi bu yazılımların nasıl çalıştığını anlamak, tespit etmek ve yayılmasını engellemek amacıyla yapılan ça-

lışmaları kapsamaktadır. Kötü amaçlı yazılım analizi sadece antivirüs şirket çalışanları tarafından değil, aynı zamanda büyük şirketlerin güvenlikle ilgili acil durumlara müdahale ekibi (Security incidents respond team) tarafından da yapılmaktadır. Bunlar güvenlik uzmanları, sistem mühendisleri veya ağ yöneticileri olabilmektedir [Hahn, 2014]. Bu analistler kötü amaçlı yazılım analizi yaparak aşağıdaki durumları tespit etmeye çalışırlar:

(1) Etkilenen makine ve programları belirlemek;

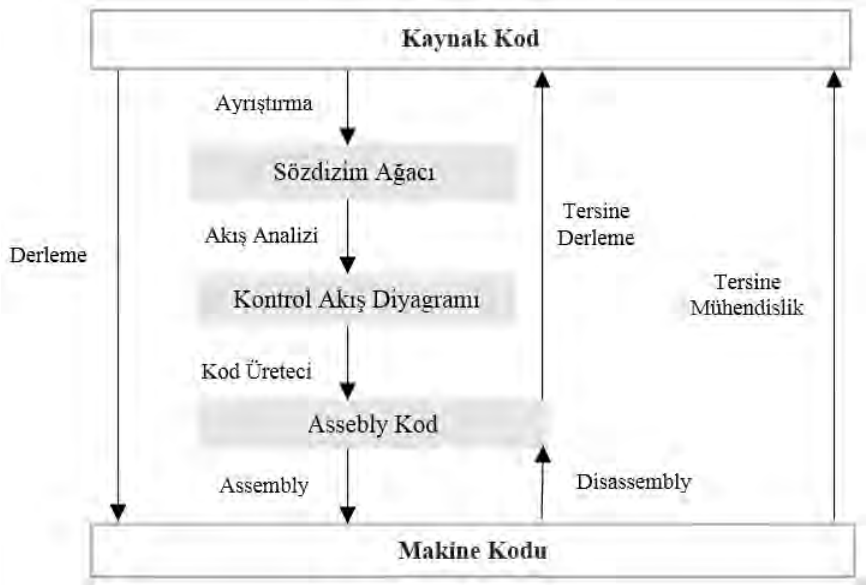
(2) Etkilenen programların eski haline nasıl döndürüleceğini belirlemek;

(3) Sistemdeki hangi güvenlik zafiyeti kullanılarak saldırının başladığını belirlemek;

(4) Zarar gören ve çalınan verileri belirlemek;

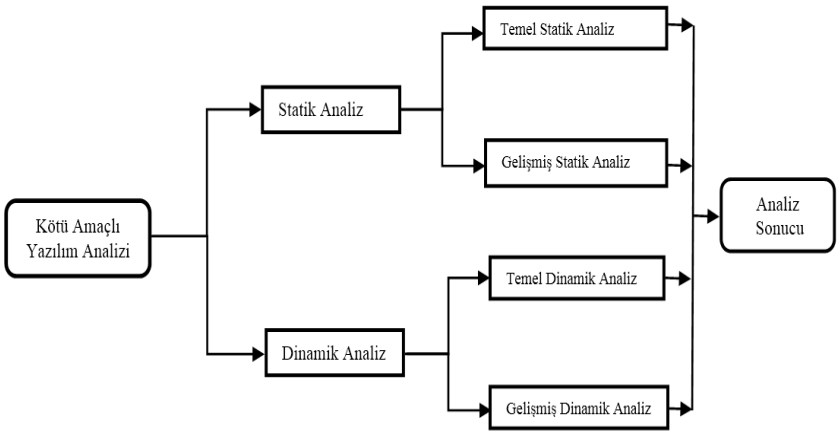
(5) Yapılabilecek potansiyel saldırıları önceden belirlemektir.

Kötü amaçlı yazılım analizi sırasında tersine mühendislik teknikleri (Reverse engineering) kullanılarak program yapısı ve sistemle olan etkileşimi belirlenir (Şekil 8.4).



Şekil 8.4. Derleme ve tersine mühendislik işlemleri

Sistem izleme araçları, paket ayırıcılar (Disassemblers), hata ayıklama araçları (Debuggers), vb. statik ve dinamik araçlar kullanılarak tersine mühendislik yapılmaktadır ve elde edilen sonuçlar kullanılarak program imzası, özellikleri ve davranışları belirlenmektedir. Kötü amaçlı yazılım analizi temel statik analiz, ileri düzey statik analiz, temel dinamik analiz ve ileri düzey dinamik analiz olmak üzere dört gruba ayrılmaktadır (Şekil 8.5).



Şekil 8.5. Kötü amaçlı yazılım analiz yöntemleri

Statik analizde program kodları çalıştırılmadan incelenir. Program kodları çalıştırılmadığı için sistemde herhangi bir zarara neden olmaz. Statik analizde amaç program yapısını ve kod dizilimini anlamaktır. Diğer taraftan dinamik analizde program kodları çalıştırılarak analiz yapılır ve sistemin zarar görmemesi için analiz genelde kapalı ortamlarda (Sandbox ya da sanal makineler kullanılarak) yapılır. Dinamik analizde amaç program kodlarını detaylı olarak incelemeden program davranışlarını anlamaktır. Program kodları değişse bile bir programın göstereceği davranışlar çok değişmeyeceğinden dolayı yeni nesil kötü amaçlı yazılımları yakalamada etkili bir analiz çeşididir.

8.4.1. Statik Analiz

Statik analiz kötü amaçlı yazılım kodlarının çalıştırılmadan işlevselliği hakkında bilgi çıkarma işlemidir. Analiz yapılırken dosya adı, "MD5 checksum", dosya tipi, dosya boyutu, kötü amaçlı yazılım imzası gibi bilgiler elde edilmeye çalışılır. Bu amaçla kullanılan bir-

çok hazır araç vardır: "Md5deep", "Peview", "Resource Hacker", "IDA Pro", "Bintext", vb. (Tablo 8.2).

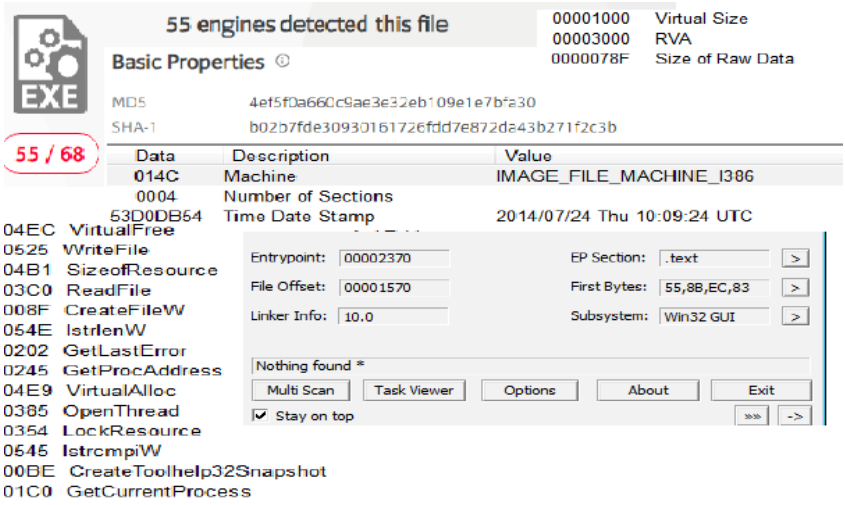
Tablo 8.2. Statik kötü amaçlı yazılım analiz araçları

Araç ismi	Açıklama
PEiD	Paketlenmiş dosyaları saptayan programdır.
PEview	Portable executable (PE) formattaki dosyaların yapı ve içeriklerini görüntüleyen programdır.
PE Explorer	PE'nin yapısını, içeriğini gösteren ve paketlenmiş dosyaları belirleyen programdır.
BinText	İkili dosyalarda gömülü bulunan karakter dizelerini çıkaran bir metin tarayıcısıdır.
UPX	Kötü amaçlı yazılım örneğini sıkıştırmak için kullanılan yürütülebilir bir paketleyicidir.
Md5deep	Dosyalar üzerinde "MD5" (Message digest 5), "SHA-1" (Secure hash algorithm), "SHA-256" hash değeri hesaplayan programdır.
Dependency Walker	Kötü amaçlı yazılım tarafından içe aktarılan DLL'leri ve metotları bulmak amacıyla kullanılan programdır.
Resource Hacker	PE'lere gömülü halde bulunan kaynakları görüntüleme, değiştirme, ekleme ve çıkarma amacıyla kullanılan programdır.
IDA Pro	Kötü amaçlı yazılım analistleri tarafından tersine mühendislik işlemleri için yaygın olarak kullanılan etkileşimli paket ayırıcıdır.
Hex Editors	İkili veri içeren dosyaları görüntülemek ve düzenlemek için kullanılan programdır.
Hex-Rays Decompiler	"Assembly" kodunu okunabilir "C" benzeri kodlara dönüştüren "IDA Pro" eklentisidir.

Örneğin, bir uygulama programının kötü amaçlı yazılım tarafından etkilenip etkilenmediğini anlamak için aynı uygulamanın temiz bir kopyasıyla kod enjekte edilmiş hali karşılaştırılarak zararlı kod ihtiva edip etmediği belirlenmektedir [Cohen, 1987; Levitt vd. 1995]. Bu amaçla "Md5deep" başta olmak üzere "PEiD", "PEview", "PE Explorer", "BinText" ve "Dependency Walker" statik analiz araçları kullanılabilir (Tablo 8.2). Diğer bir yöntem de paket ayırıcı "IDA Pro", "Hex Editors" ve "Hex-Rays Decompiler" kullanılarak kötü amaçlı yazılımdaki desenler belirlenir. Statik analiz, kötü amaçlı yazılım imzaları belirlenirken sıkça kullanılan bir analiz metodudur.

Temel ve ileri düzey statik analizler olmak üzere ikiye ayrılmaktadır.

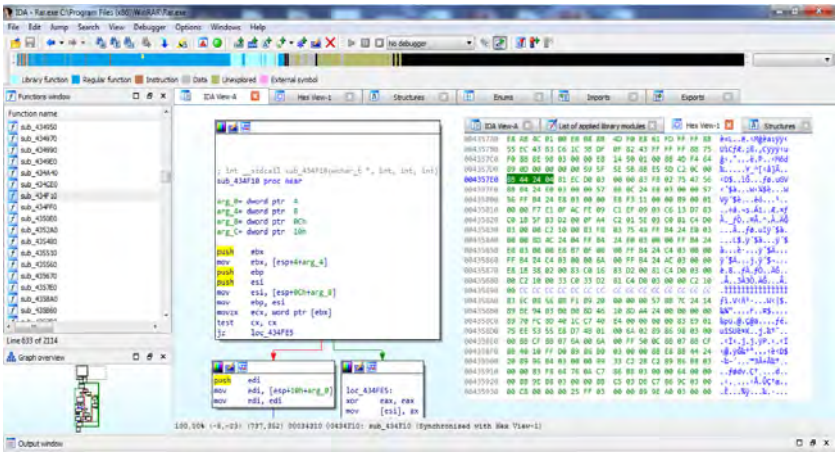
1) Temel (basit) statik analiz: Temel statik analiz kötü amaçlı yazılımın özellikleri ve işlevi hakkında genel bir değerlendirmede bulunmak amacıyla yapılır. Bu analiz türünde kötü amaçlı yazılıma dışardan bakılarak genel bir değerlendirme yapılır ve analiz detaylandırılmaz. Bu analiz sırasında anti virüs yazılımlar (Norton, McAfee, Karspersky, ClamAV, vb.) ve statik analiz araçları (PEiD, PEview, BinText, Md5deep, vb.) kullanılarak hash değerleri ve kullanılan string dizilimler (hata mesajları, export/import metot isimleri, URL'ler ve email adresleri vb.), metotlar ve dosya başlıklarından elde edilen bilgiler kullanılır. Çevrim içi hizmet veren "VirusTotal" websitesi birçok antivirüs yazılımı barındırmaktadır ve temel statik analizin ilk aşaması olarak kullanılabilmektedir. Antivirüs yazılımlar, bazı string dizilimleri ve "MD5", "SHA-256", vb. hashleri kötü amaçlı yazılım imzası olarak görmekte ve bu yazılımları etiketlemek ve tanımlamak için yaygın olarak kullanmaktadır [Aslan ve Samet, 2017]. Statik analizin ikinci aşamasında temel statik analiz araçları kullanılarak başka bilgiler de (Analiz edilen programın kullandığı URL'ler, email adresleri, metotlar, paketlenip paketlenmediği bilgisi, vb.) elde edilmektedir. Şekil 8.6, temel statik analiz kullanılarak "Dyre" kötü amaçlı yazılım analiz sonucunu göstermektedir.



Şekil 8.6. Temel statik analiz kullanılarak "Dyre" kötü amaçlı yazılım analizi (Analiz sonuçları kısaltılarak verilmiştir)

İlgili analiz "VirusTotal", "PEview", "PEiD" ve "Bintext" araçları kullanılarak yapılmıştır. Analiz sonucuna bakılarak antivirüs tarayıcılarının tespit oranı 55/68 (%80.88), kötü amaçlı yazılım imzaları (MD5, SHA-1), yazılımın ne zaman derlendiği, program bölümlerinin diskte ve hafızada ne kadar yer kapladıkları, hangi işletim sistemi API'lerin çağrıldığı ve kötü amaçlı yazılımın paketlenip paketlenmediği gibi sorulara cevap verilebilmektedir. Çoğu antivirüs tarayıcısı "Dyre" kötü amaçlı yazılımını Truva atı olarak işaretlemiştir.

2) İleri düzey (gelişmiş) statik analiz: İleri düzey statik analizde program komutları detaylı incelenerek analiz yapılmaktadır. Bilgisayar komutları bilgisayar işlemcisi tarafından sırasıyla yürütülen adımlar olarak tanımlanabilir ve farklı soyutlama seviyelerinde bulunabilmektedir: Makine kodu (Opcodes), "assembly" dili (en düşük okunabilir soyutlama seviyesi) ve yüksek seviyeli diller "C", "C++", "Java", vb. Program kodlarının çalıştırılabilmesi için yüksek seviyeli dillerden makine seviyesi dillere çevrilmesi gerekmektedir ve derleme olarak adlandırılmaktadır (Şekil 8.4). Diğer taraftan program komutlarının analiz edilebilmesi için makine seviyesi kodlarının daha üst düzey seviye dillere dönüştürülmesi gerekmektedir. Yani tersine derleme yapılmaktadır. Makine kodlarının "assembly" diline çevrilmesi ayırma (Disassembly), daha düşük seviyeli bir koddan yüksek seviyeli dile çevrilmesi ters derleme (Decompilation) olarak adlandırılmaktadır. Tersine derleme sonucu elde edilen kodlar kullanılarak belirli özellikler elde edilmekte ve bu özelikler yorumlanarak ileri düzey statik analiz yapılmaktadır. Tersine derleme sırasında bazı bilgi kayıpları olduğundan (Assembly dilinden C, C++, vb. yüksek dereceli dillere çevrilirken) üst seviye kaynak kodları elde etmek nerdeyse imkansızdır ve bundan dolayı genelde "assembly" seviyesindeki diller ileri düzey statik analiz için kullanılmaktadır. Şekil 8.7, "IDA Pro" kullanarak ileri düzey statik analiz sonucunu göstermektedir.



Şekil 8.7. "IDA Pro" kullanarak program analizi (Analiz sonuçları kısaltılarak verilmiştir)

Program kodları paket ayırıcı (Disassembler) "IDA Pro" kullanarak makine kodundan "assembly" diline dönüştürülmüştür. Şekil 8.7'de görüleceği üzere sırasıyla kullanılan yazmaçlar (register), ara değerler, hafıza adresleri, vb. görülmektedir. Örneğin, "mov ebx, [esp+4+arg_4]" komutu "[esp+4+arg_4]" işlemi sonucunda elde edilen bellek konumundan 4 baytlık bilgiyi "ebx" yazmacına kopyalamaktadır (Şekil 8.7). Burda amaç "assembly" kodları incelenerek analiz edilen kodun ne yapmaya çalıştığını belirlemektir. Örneğin, belirlenen adreste hangi "DNS" istekleri yapılmış, hangi alt yordam da kaç yerel değişken kullanılmış, "DllMain" kaç Windows API metodunu doğrudan çağırmış, "Sleep" metodu kullanıldığında program ne kadar süre uyumuş, vb. bilgiler ileri düzey statik analizle elde edilebilir.

8.4.1.1. Statik Yazılım Analizinde Bilgi Çıkarma Yolları

(1) Antivirüs taraması (Antivirus scanning): Antivirüs tarayıcıları kötü amaçlı yazılım analizinde ilk adım olarak kullanılan yöntemlerin başında gelmektedir. Bu programlar kötü amaçlı yazılım tespiti için şüpheli kod ya da kod bölümlerini tanımlayan dosya imzaları kullanmaktadır [Panley vd. 2014]. Program imzaları, ilgili programdaki belirli kod bölümlerinden program yapısı çıkartılarak oluşturulan ve belirli uzunlukta olan karakter dizilimlerdir. Öncelikle, önceden belirlenmiş kötü amaçlı yazılım imzaları bir veri tabanında

saklanır. Daha sonra, antivirüs tarayıcıları dosyanın imzasını bulur ve veri tabanında saklanan imzalarla karşılaştırır. Eğer imza veri tabanında mevcut ise ilgili dosya kötü amaçlı yazılım olarak işaretlenir, aksi takdirde normal yazılım olarak işaretlenir. Antivirüs tarayıcıları bilinen kötü amaçlı yazılımları (Aynı aileye ait farklı imzalara sahip) tespitte hızlı ve doğru çalışsa da, bilinmeyen kötü amaçlı yazılımları tespit etmede yetersiz kalmaktadır. Şekil 8.8, örnek bir yazılımın antivirüs tarayıcısı olan "ClamAV" tarafından tespit edilen kötü amaçlı yazılım imzasını göstermektedir [Hahn, 2014].

```
Zararlı. exe:1:90FF1683EE0483EB0175F6
```

Şekil 8.8. "ClamAV" bayt imzası

"90FF1683EE0483EB0175F6" ilgili kod bölümünün onaltılık formatta gösterimidir ve "assembly" dilinde Şekil 8.9'daki gibi gösterilmektedir. Aynı bayt imzası "Yara" formatında Şekil 8.10'da gösterilmektedir.


```
Başlama: 0x401A2E length: 0xC
90 nop
FF 16 call dword ptr [esi]
83 EE 04 sub esi, 4
83 EB 01 sub ebx, 1
75 F6 jnz short loc_401A30
```

Şekil 8.9. "90FF1683EE0483EB0175F6" imzasının "assembly" bayt dizilimi

```
Kural örnegi
{
        Bayt dizilim:
        imza = { 66 90 FF 16 83 EE 04 83 EB 01 75 F6 }
        durum:
        imza
}
```

Şekil 8.10. Bayt imzasının "Yara" formatında gösterimi

Bilinmeyen kötü amaçlı yazılımlar (Unknown malware) genellikle, antivirüs tarayıcılarını atlatmak için imzasını ve kod yapısını değiştiren normalde bilinen kötü amaçlı yazılımlardır [You ve Yim, 2010].

"Norton", "McAfee", "Karspersky" ve "ClamAV" yaygın olarak kullanılan antivirüs tarayıcılarıdır. Program imzaları çıkarılırken farklı yöntemler kullanılmaktadır: String analizi, üst ve kuyruk taraması, giriş noktası taraması.

(a) String analizi (String analysis): Belirli dizilimler saldırganın e-posta adresi, zararlı kodla ilişkili "URL'ler", kullanılan metot isimleri, vb. kötü amaçlı yazılımla ilgili uygun bilgiler sunmaktadır ve kötü amaçlı yazılım tespitinde sıkça kullanılmaktadır.

(b) Üst ve kuyruk tarama (Top-and-tail scanning): Bütün dosya yerine sadece dosyanın üst ve bitiş noktalarında belli bölümler alınarak imzalar oluşturulmaktadır [Szor, 2005]. Kendini dosya başlarına ve sonlarına ekleyen virüsleri tespit etmek için oldukça uygun bir imza çıkarma yöntemidir.

(c) Giriş noktası taraması (Entry point scanning): Bir dosyanın giriş noktası o dosya çalıştırılmaya başladığında ilk çalışmanın nerde başlayacağını gösterir. Kötü amaçlı yazılımlar genellikle programların giriş noktalarını zararlı kodların başlangıç noktalarını işaret edecek şekilde değiştirirler ve program kodlarından önce zararlı kodların çalıştırılmasını sağlarlar [Szor, 2005]. Bundan dolayı program giriş noktalarındaki dizilimlerden imza çıkarılarak belli kötü amaçlı yazılımlar tespit edilebilmektedir.

(2) Hashing: Kötü amaçlı yazılımı tespit edebilen bir yöntemdir. Örnek program hash programına girdi olarak verilerek "MD5", "SHA-1" ve "SHA-2" gibi hash değerleri hesaplanır. Daha sonra, hesaplanan hash değerleri önceden hazırlanmış veri tabanlarındaki hash değerleriyle karşılaştırılarak işaretleme yapılır.

(3) Tersine derleme (Reverse compiling): Kötü amaçlı yazılım örneklerinin makine kodu girdi olarak verilip "assembly" seviyesi komutlar elde etme işlemidir [Pandey vd. 2014; Fukushima, 2010]. Tersine derleme sırasında programın yapısı analiz edilebilmektedir: Hangi metotların kullanıldığı, "register" durumları, yığın durumu, vb.

Statik analizde dosya ismi, uzantısı, içeriği, imzası, karakter dizileri, vb. bilgiler ilgili statik analiz araçları kullanılarak çıkartılır ve bu veriler kullanılarak programın yapısı belirlenir. Çıkarılan bu özel-

likler ilgili kötü amaçlı yazılım hakkında bilgi vermekte ve benzer özelliklerin başka kötü amaçlı yazılımlarda olup olmadığına bakılmaktadır. Daha önce bilinen kötü amaçlı yazılımlar bu sayede hızlı ve etkin bir şekilde tespit edilebilmektedir. Fakat bu yazılımlarda yapılan ufak bir değişiklik programın yapısını değiştireceğinden, ayrıca bazı kötü amaçlı yazılımların gerçek program yapısının belirlenmesindeki zorluklar iyi programlanmış kötü amaçlı yazılımları statik analiz kullanarak tespit etmeyi neredeyse imkansız hale getirmektedir. Ayrıca "BinText" ve "PEview" gibi statik analiz araçları kötü amaçlı yazılımlar hakkında çok detaylı bilgi vermemekte ve "IDA Pro" gibi paket ayırıcı programlar kullanmak çok üst düzey işlemci ve işletim sistemi bilgisi gerektirdiğinden dolayı statik analiz kullanarak yeni nesil kötü amaçlı yazılımları analiz ve tespit etmek nerdeyse olanaksızlaşmaktadır.

8.4.2. Dinamik Analiz

Dinamik analiz, program davranışını izleyerek sistemdeki hangi makine ve programların etkilendiğini, etkilenen programların eski haline nasıl döndürüleceğini, sistemdeki hangi güvenlik zafiyetleri kullanılarak saldırının başladığını, hangi verilerin zarar gördüğünü, vb. sorularına yanıt vermek amacıyla yapılır. Ayrıca, dinamik analiz metodu davranışsal kötü amaçlı yazılım tespitinde de sıkça kullanılmaktadır. Dinamik analizde program koduna ve kod dizilişine değil, programın davranışına bakılmaktadır. Program kodları değişse de, programın göstereceği davranışlar büyük oranda değişmeyeceğinden, bu yöntem kullanılarak birçok kötü amaçlı yazılım tespit edilebilmektedir. Dinamik analizin en büyük dezavantajı, kötü amaçlı yazılım korunan bir ortamda (Sanal makine, sandbox ortamında) bütün gerçek davranışlarını göstermeme ihtimalinin bulunmasından dolayı kötü amaçlı yazılımların normal yazılım olarak yanlış işaretlenmesidir. Bu analizler genelde farklı dinamik analiz araçları kullanılarak siber güvenlik uzmanları tarafından elle yapılmaktadır (Tablo 8.3).

Tablo 8.3. Dinamik kötü amaçlı yazılım analiz araçları

Araç İsmi	Açıklama
Process Explorer	Bilgisayar sisteminde çalışan işlemleri ve detaylarını gösteren program
Process Monitor	Gerçek zamanlı olarak bilgisayar sisteminde olan tüm olayları (dosya işlemleri, kayıt defteri işlemleri, bazı ağ işlemleri, vb.) izleyen ve görüntüleyen program
API Monitor	Uygulamalar ve hizmetler tarafından yapılan API çağrılarını izlemeye ve denetlemeye olanak tanıyan program
Regshot	Windows kayıt defterindeki değişimleri gösteren program
ApateDNS	"DNS" yanıtlarını kontrol eden program
Netcat	Gelen ve giden ağ bağlantıları izleyen program
INetSim	Yaygın kullanılan İnternet servislerini simüle eden program
Wireshark	Ağ (Network) protokol analiz programı
Capture BAT	Sistem durumunu izleyen program
WinDbg	Kullanıcı ve kernel modlu hata ayıklama programı
OllyDbg	Hata ayıklama ve tersine mühendislik programı
Burp Suite	Web uygulamalarının güvenlik testleri için geliştirilmiş yazılım platformu
Sandbox (Cuckoo, CWsandbox, Norman, vb.)	Belirli bir zaman dilimi için kötü amaçlı yazılımın çalıştırılarak sistemle olan etkileşimini rapor olarak sunan yalıtılmış ortamlar

Fakat son yıllarda kötü amaçlı yazılım sayısının hızla artmasından dolayı otomatik olarak da yapılabilmektedir. Genel olarak otomatik dinamik analiz üç bölümden oluşmaktadır:

(1) Davranışların Belirlenmesi: Davranışlar belirlenirken sistem çağrıları (API/system calls) veya dosya, kayıt defteri (Registry), bilgisayar ağ olayları vb. incelenerek davranışlar belirlenir. Yani, sistem çağrılarının ya da yapılan dosya, "registry" ve ağ olaylarının sırasına, frekansına, hangi sırada ve ne sıklıkla çağrıldığına bakılarak davranışlar oluşturulur.

(2) Özelliklerin Çıkartılması: Daha önce belirlenen davranışlar gruplanarak dizilimler oluşturulur ve bu dizilimlerden özellikler çıkartılır.

(3) Sınıflandırma: Belirlenen özeliklere makine öğrenmesi algoritmaları (karar ağaçları, logistik regresyon, destek vektör makinesi, vb.) uygulanarak sınıflandırma yapılır.

Genel olarak dinamik analiz temel ve ileri düzey olmak üzere ikiye ayrılır.

1) Temel (basit) dinamik analiz: Kötü amaçlı yazılım davranışlarının izleme programları kullanarak incelenmesidir. Temel dinamik analiz teknikleri sırasıyla şöyle sıralanabilir:

a) Dosya ve "registry" olaylarının izlenmesi;

b) Dosya değişikliklerinin izlenmesi;

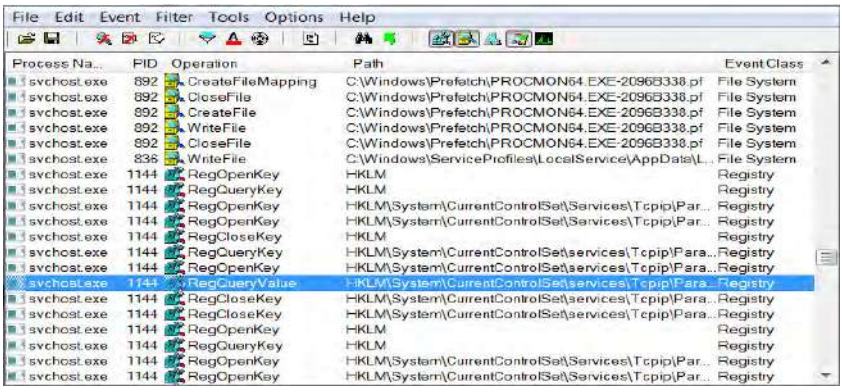
c) "Registry" anlık görüntülerinin karşılaştırılması;

d) Ağ aktivitelerinin izlenmesi;

e) "Sandbox" kullanarak otomatik analiz;

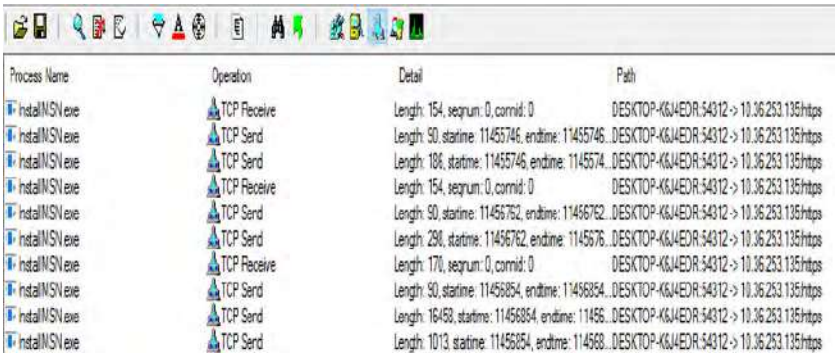
f) Sistem çağrılarının izlenmesi.

Şekil 8.11, Şekil 8.12 ve Şekil 8.13, farklı programlar için basit dinamik analiz sonuçlarını göstermektedir.



Şekil 8.11. "Process Monitor" kullanarak program analizi (Aktivitelerin listesi kısaltılmıştır)

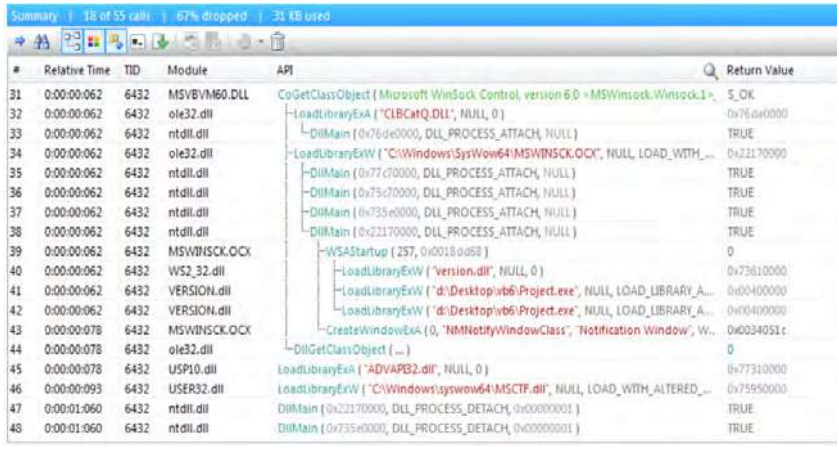
Şekil 8.11, "Process Monitor" kullanarak "svchost.exe" adlı sistem dosyasının çalıştırıldığında göstermiş olduğu dosya, "registry" ve ağ olaylarını göstermektedir. Hangi dizinde hangi dosyaların oluşturulduğu, hangi dizin ya da dosyalarda okuma ve yazma yapıldığı, "registry" değerlerine yapılan atamalar görülmektedir.



Process Name	Operation	Detail	Path
InstallNSN.exe	TCP Receive	Length: 154, seqnum: 0, connid: 0	DESKTOP-K6J4EDR:54312 -> 10.36.253.135:https
InstallNSN.exe	TCP Send	Length: 50, starttime: 11455746, endtime: 11455746	DESKTOP-K6J4EDR:54312 -> 10.36.253.135:https
InstallNSN.exe	TCP Send	Length: 186, starttime: 11455746, endtime: 11455746	DESKTOP-K6J4EDR:54312 -> 10.36.253.135:https
InstallNSN.exe	TCP Receive	Length: 154, seqnum: 0, connid: 0	DESKTOP-K6J4EDR:54312 -> 10.36.253.135:https
InstallNSN.exe	TCP Send	Length: 50, starttime: 11456762, endtime: 11456762	DESKTOP-K6J4EDR:54312 -> 10.36.253.135:https
InstallNSN.exe	TCP Send	Length: 290, starttime: 11456762, endtime: 11456762	DESKTOP-K6J4EDR:54312 -> 10.36.253.135:https
InstallNSN.exe	TCP Receive	Length: 170, seqnum: 0, connid: 0	DESKTOP-K6J4EDR:54312 -> 10.36.253.135:https
InstallNSN.exe	TCP Send	Length: 50, starttime: 11456854, endtime: 11456854	DESKTOP-K6J4EDR:54312 -> 10.36.253.135:https
InstallNSN.exe	TCP Send	Length: 16458, starttime: 11456854, endtime: 11456	DESKTOP-K6J4EDR:54312 -> 10.36.253.135:https
InstallNSN.exe	TCP Send	Length: 1013, starttime: 11456854, endtime: 114568	DESKTOP-K6J4EDR:54312 -> 10.36.253.135:https

Şekil 8.12. Kötü amaçlı yazılımın başka sisteme (10.36.253.135) bağlanırken yaptığı ağ aktivitelerinin "Process Monitor" kullanarak izlenmesi (Aktivitelerin listesi kısaltılmıştır)

Şekil 8.12, kötü amaçlı örnek bir yazılımın başka sisteme (10.36.253.135) bağlanırken yaptığı ağ aktivitelerinin göstermektedir. "Process Monitor" çıktısında gerekli filtrelemeler yapıldıktan sonra hangi "IP" adreslerine ya da web sitelerine bağlanıp kaç bayt gönderip alındığı çıktıda görülebilmektedir.



Summary | 18 of 55 calls | 67% dropped | 31 KB used

#	Relative Time	TID	Module	API	Return Value
31	0:00:00:062	6432	MSVBVM60.DLL	CoGetClassObject (Microsoft WinSock Control, version 6.0 = MSWinsock.Winsock.1 >,	S_OK
32	0:00:00:062	6432	ole32.dll	LoadLibraryExA ("CLBCatQ.DLL", NULL, 0)	0x76da0000
33	0:00:00:062	6432	ntdll.dll	DllMain (0x76da0000, DLL_PROCESS_ATTACH, NULL)	TRUE
34	0:00:00:062	6432	ole32.dll	LoadLibraryExW ("C:\Windows\SysWow64\MSWINSCK.OCX", NULL, LOAD_WITH_...	0x22170000
35	0:00:00:062	6432	ntdll.dll	DllMain (0x77c70000, DLL_PROCESS_ATTACH, NULL)	TRUE
36	0:00:00:062	6432	ntdll.dll	DllMain (0x75c70000, DLL_PROCESS_ATTACH, NULL)	TRUE
37	0:00:00:062	6432	ntdll.dll	DllMain (0x735e0000, DLL_PROCESS_ATTACH, NULL)	TRUE
38	0:00:00:062	6432	ntdll.dll	DllMain (0x22170000, DLL_PROCESS_ATTACH, NULL)	TRUE
39	0:00:00:062	6432	MSWINSCK.OCX	WSAStartup (257, 0x0018dd68)	0
40	0:00:00:062	6432	WS2_32.dll	LoadLibraryExW ("version.dll", NULL, 0)	0x73610000
41	0:00:00:062	6432	VERSION.dll	LoadLibraryExW ("d:\Desktop\vb6\Project.exe", NULL, LOAD_LIBRARY_A...	0x00400000
42	0:00:00:062	6432	VERSION.dll	LoadLibraryExW ("d:\Desktop\vb6\Project.exe", NULL, LOAD_LIBRARY_A...	0x00400000
43	0:00:00:078	6432	MSWINSCK.OCX	CreateWindowExA (0, "NMNotifyWindowClass", "Notification Window", W...	0x0034051c
44	0:00:00:078	6432	ole32.dll	DllGetClassObject (...)	0
45	0:00:00:078	6432	USP10.dll	LoadLibraryExA ("ADVAPI32.dll", NULL, 0)	0x77310000
46	0:00:00:093	6432	USER32.dll	LoadLibraryExW ("C:\Windows\syswow64\MSCTF.dll", NULL, LOAD_WITH_ALTERED_...	0x75950000
47	0:00:01:060	6432	ntdll.dll	DllMain (0x22170000, DLL_PROCESS_DETACH, 0x00000001)	TRUE
48	0:00:01:060	6432	ntdll.dll	DllMain (0x735e0000, DLL_PROCESS_DETACH, 0x00000001)	TRUE

Şekil 8.13. "API Monitor" kullanarak program analizi (API sistem çağrılarının listesi kısaltılmıştır)

Benzer şekilde Şekil 8.13, örnek bir programın "API Monitor" kullanarak yapmış olduğu Windows API sistem çağrılarını göstermektedir. Şekilde hangi .dll ve metodların çağrıldığı görülmektedir. Otomatik çıktı üreten "Process Monitor" ve "API Monitor" gibi araç çıktılarının net olarak yorumlanabilmesi için ya gerekli filtrelemeler

yapıldıktan sonra önemli görülen çıktılar elle yorumlanarak bir sonuca varılmakta ya da özellikler belirlenip ve bu özelliklere makine öğrenmesi uygulanarak analiz edilmektedir. Örnegin, "AdjustTokenPrivileges", "GetWindowsDirectory", "ReadProcessMemory", vb. Windows API'lerinin bir program tarafından çağrılması o programın kötü amaçlı olup olmadığı hakkında önemli bilgiler sunmaktadır. Ayrıca, araç çıktılarında bilgisayar kaynaklarında: dosya, "registry", vb. yapılan değişiklikler görülebilmektedir. Tehlikeli görülen dosyalar ve "registry" girdileri silinerek ya da güncellenerek kötü amaçlı yazılımın yayılması ve zarar vermesi engellenebilmektedir.

2) İleri düzey (gelişmiş) dinamik analiz: Gelişmiş dinamik analizde "debugger" olarak adlandırılan hata ayıklama araçları kullanılır. Hata ayıklayıcılar değişkenlerin, parametrelerin ve hafıza alanlarının hem içeriğini görüntüleme hem de değiştirme amacıyla her komutu tek tek çalıştırmaya olanak vermektedir. "Debugger'lar" hem kullanıcı seviyesinde hem de çekirdek seviyesinde çalışmaktadırlar. İleri düzey dinamik analiz kullanılarak kötü amaçlı yazılımların büyük bir kısmı tespit edilebilmektedir. Ayrıca, "disassembly" kullanarak elde edilmesi zor olan bazı bilgiler de bu yöntemle kolayca elde edilebilmektedir. Fakat "debugger" kullanımı ileri düzey işletim sistemi ve "assembly" seviyesi dil bilgisi gerektirdiği için kullanımı zordur. Şekil 8.14, "OllyDbg" kullanarak yapılmış ileri düzey dinamik analiz soncunu göstermektedir.



Şekil 8.14. "OllyDbg" kullanarak ileri düzey dinamik analiz (Analiz sonuçları kısaltılarak verilmiştir)

Şekil 8.14'te görüleceği üzere "OllyDbg" çıktısı 4 bölümden oluşmaktadır:

1) **Disassembler penceresi**: Analiz edilen program komutlarını sırasıyla göstermektedir. Analizi yapan uzman tarafından herhangi bir zamanda komut ve veriler değiştirilebilmektedir.
2) **Yazmaçlar penceresi**: Yazmaçların mevcut durumlarını göstermektedir. Her komuttan sonra bu değerler değişmektedir. Ayrıca, koda müdahale edilerek yazmaç değerleri her hangi bir zamanda değiştirilebilmektedir.
3) **Bellek dökümü penceresi**: Analiz edilen program komutlarının ve verilerinin anlık olarak bellek dökümlerini göstermektedir. Analizi yapan uzman bellekte bulunan değişkenlere müdahale ederek değiştirebilmektedir.
4) **Yığın (stack) penceresi**: Bu pencere, her iş parçacığı için bellekte bulunan yığının mevcut durumunu göstermektedir. Yığın verilerine müdahale ederek değerler değiştirilebilmektedir.

Örneğin, "PUSH EBP" komutu "EBP" yazmacında bulunan veriyi yığına atmaktadır ve bu anda yığının durumu, bellek dökümü ve yazmaçların durumu Şekil 8.14'te görülmektedir. Burada amaç program kodlarını analiz ederek komutların çalışması sonucu oluşan davranışları belirlemektir. Bu davranışlar şöyle sıralanabilir:

(1) Kod bloğunun ne yapmaya çalıştığı,

(2) Hangi alan adlarının kullanıldığı,

(3) Alan adlarını gizlemek için hangi tekniklerin kullanıldığı,

(4) Yazılımın dışardan alması gereken komutların ne olduğu,

(5) Hangi servislerin oluşturulduğu ve ne amaçla kullanıldığı,

(6) Hangi açıklardan faydalanarak saldırı başlatıldığı ve bu açıklara çalışma zamanında nasıl müdahale edileceği,

(7) Hangi verilerin zarar gördüğü veya çalındığı vb.

Ayrıca, ileri düzey statik analizle elde edilemeyen bilgiler de ileri düzey dinamik analiz yöntemiyle kolayca elde edilebilmektedir.

Dinamik analizde kötü amaçlı yazılımlar çalıştırılarak (program kodlarının) sistemdeki davranışları (dosya olayları, registry olayla-

rı, bilgisayar ağında olan olaylar, vb.) izlenerek analiz edilir. Program kodları değişse de, programın göstereceği davranışlar büyük oranda değişmeyeceğinden dolayı, dinamik analiz kullanılarak oluşturulmuş bir imzayla birçok kötü amaçlı yazılım tespit edilebilmektedir. Ayrıca, daha önce bilinmeyen yeni kötü amaçlı yazılımlar da bu yöntemle başarılı bir şekilde analiz ve tespit edilebilmektedir. Dinamik analizin en büyük dezavantajı, kötü amaçlı yazılımın korunan ortamlarda (Sanal makine, sandbox ortamında) bütün gerçek davranışlarını göstermeme ihtimalinin bulunmasından dolayı kötü amaçlı yazılımın normal yazılım olarak yanlış işaretlenmesidir.

8.4.3. Statik ve Dinamik Analizin Karşılaştırılması

Statik ve dinamik analizin avantaj ve dezavantajlar Tablo 8.4'te ve karşılaştırma tablosu Tablo 8.5'te görülmektedir. Bilinen kötü amaçlı yazılımlar statik analiz kullanılarak kolay ve hızlı bir şekilde analiz edilebilmektedirler. Fakat gizlenme tekniği (Obfuscation, packed, polymorphic, vb.) kullanan kötü amaçlı yazılımları doğru bir şekilde analiz etmek neredeyse imkansızdır (Tablo 8.4).

Tablo 8.4. Statik- dinamik analiz avantaj ve dezavantajları

	Avantajlar	**Dezavantajlar**
Statik Analiz	Genel bir bakış açısı sunar (Multiple path execution)	Tersine mühendislik teknikleri bazı kısıtlamalar içerir
	Zaman ve kaynak tüketimi azdır	"Obfuscation" ve "Polymorphic" tekniklerine karşı savunmasızdır
	Kararlı ve tekrarlanabilir	Zor ve karmaşıktır
	Gerçek makine zarar görmez	Yeni nesil kötü amaçlı yazılımları analizde etkisizdir
Dinamik Analiz	Basit ve kesin sonuçlar üretir	Sınırlı görünüm (Single path execution) sunar
	Gerçek zamanlı davranış bilgileri elde edilir	Çalışma durumuna ve zamanına göre farklı davranışlar gösterir
	Kod obfuscation tekniklerine karşı güçlüdür	Analiz otomatikleştirildiğinde etkileşimli davranış eksik kalır
	Yeni nesil kötü amaçlı yazılımlar tespit edilebilir	Zaman ve kaynak tüketimi fazladır
	-	Sanal ortamlarda bazen bütün davranışlar belirlenemez

Tablo 8.5. Statik- dinamik analiz karşılaştırma tablosu

Karşılaştırma parametresi	Statik Analiz	Dinamik Analiz
Zaman ve kaynak tüketimi	Az	Fazla
Analiz modu	Gerçek zamanlı değil	Gerçek zamanlı
Analizin tekrarlanabilirlik durumu	Aynen tekrarlanabilir	Aynen tekrarlanamaz
Gizlenme tekniklerine karşı	Güçsüz	Güçlü
Bilinen kötü amaçlı yazılımlar için tespit oranı	Yüksek	Düşük
Yeni nesil kötü amaçlı yazılımlar için tespit oranı	Düşük	Yüksek
Yanlış işaretleme oranı	Düşük	Yüksek
Başarı durumu	Düşük	Yüksek

Dinamik analiz sırasında program kodları çalıştırıldığından dolayı gizlenme tekniği kullanan kötü amaçlı yazılımlar tespit edilebilmektedir. Fakat "sandbox" ve sanal makineler üzerinde çalıştırıldığını anlayan bazı kötü amaçlı yazılımlar gerçek davranışlarını gizlemektedirler ve bundan dolayı normal yazılım olarak işaretlenebilmektedirler. Daha önce bilinen kötü amaçlı yazılımlar için statik analiz daha hızlı ve iyi performans göstermesine karşın bilinmeyen (Zero day) kötü amaçlı yazılımlar karşısında dinamik analiz statik analize göre daha iyi bir performans göstermektedir [Aslan ve Samet, 2017] (Tablo 8.6).

Tablo 8.6. Statik ve dinamik analiz performans karşılaştırması

No	İsim	Analiz Tekniği	Tespit oranı (%)	Doğruluk oranı (%)
1	Pandey ve Mehtre, 2014	Statik analiz	80	79
2	Pandey ve Mehtre, 2014	Dinamik analiz	89	83
3	Aslan ve Samet, 2017	Statik analiz	74	77
4	Aslan ve Samet, 2017	Dinamik analiz	80	82,5
5	Aslan 2017	Statik analiz	75	81

Kötü amaçlı yazılım analizi bu yazılımların nasıl çalıştığını anlamak, tespit etmek ve yayılmasını engellemek amacıyla yapılan

çalışmaları kapsamaktadır. Analiz sırasında tersine mühendislik teknikleri kullanılarak program yapısı veya sistemle olan etkileşimi (Program davranışları) belirlenir. Belirlenen çıktılar elle veya otomatik olarak yorumlanarak analiz edilen yazılımın mühtevası hakkında bir karara varılır. Bu analizler temel statik-, ileri düzey statik-, temel dinamik- ve ileri düzey dinamik analiz olmak üzere dört gruba ayrılmaktadır. Statik analizde amaç program yapısını ve kod dizilimini anlamaktır. Program kodları çalıştırılmadığı için sistemde herhangi bir zarara neden olmaz. Bilinen zararlıları tespit etmek hızlı ve etkili olsa da daha önce görülmemiş kötü amaçlı yazılımları tespit etmek neredeyse imkansızdır. Dinamik analizde amaç program kodlarını detaylı olarak incelemeden program davranışlarını anlamaktır. Bu amaçla program kodları çalıştırılarak analiz yapılır ve sistemin zarar görmemesi için analiz genelde kapalı ortamlarda (Sandbox ya da sanal makineler kullanılarak) yapılır. Program kodları değişse de programın göstereceği davranışlar çok değişmeyeceğinden dolayı yeni nesil zararlıları yakalamada etkili bir analiz yöntemidir. Temel analiz yapılarak kötü amaçlı yazılım hakkında bazı temel bilgiler elde edilebilir. Fakat daha net ve detaylı bilgi elde etmek için ileri düzey analize gerek vardır. Örneğin, hangi metotların "import" edildiği temel analizle öğrenilebilir ama bu metotların nerelerde ve niçin kullanıldığı ancak ileri düzey kötü amaçlı yazılım analizi yapılarak anlaşılabilir.

8.5. Değerlendirmeler

Kötü amaçlı yazılımlar dinamik olup zaman zaman saldırı biçimini ve hedefini değiştirerek sürekli gelişme gösteren yazılımlardır. Güncel virüs programları, saldırı tespit sistemleri, güvenlik duvarı ve diğer koruma yazılımları kullanılarak bilgisayar sistemleri büyük ölçüde korunabilse de, yeni bir saldırı yöntemi bütün bu korumaları geçerek sisteme zarar verebilmektedir. Genelde birçok sistem açığı saldırı yapıldıktan sonra tespit edilmekte ve açığı kapatmak zaman almaktadır. Açıklık kapatılana kadar saldırganlar aynı ya da farklı sistemde farklı bir açık tespit edebilmektedirler. Ayrıca, siber saldırılarda birden fazla kötü amaçlı yazılımın birlikte kullanılması bu saldırılara karşı korumayı zorlaştırmaktadır. Bundan dolayı bu yazılımları sadece tespit etmek değil ayrıca, hangi makine ve programların etkilendiğini, etkilenen programların eski haline nasıl döndürüleceği, sistemdeki hangi güvenlik zafiyetinin

kullanılarak saldırının başladığını, hangi verilerin zarar gördüğünü veya çalındığını ve yapılabilecek potonsiyel saldırıları önceden belirlemek amacıyla bu yazılımları analiz etmek gerekmektedir. Kötü amaçlı yazılım analizi genelde basit statik analizle başlamakta ve ileri düzey dinamik analizle sonlanmaktadır. Analiz sırasında birden fazla analiz aracı ve metodu kullanıldığı için kötü amaçlı yazılımlar hakkında birçok bilgi edinilebilmektedir.

Kötü amaçlı yazılımların bulaştığı sistemlerde fark edilmeleri zordur, fakat bulaştığı sistemleri genelde yavaşlattıkları için varlıkları ancak uzun uğraşlar sonucunda öğrenilebilir. Bu yazılımlardan korunmak tam olarak mümkün görünmemekle birlikte bazı önlemler alınarak bu yazılımların sistemlere bulaşması engellenebilir ya da bulaştıktan sonra sisteme vereceği zararlar azaltılabilir. Bu önlemler aşağıda sıralanmıştır:

[1] Sadece güvenirliği test edilmiş yazılımlar kullanmak;

[2] Sistemi zaman zaman kontrol ederek her hangi bir anormallik olup olmadığı test etmek;

[3] Sistem zafiyetlerinin belirlenmesi adına sızma testleri yapmak.

[4] İşletim sistemini ve diğer programları belli aralıklarla güncellemek;

[5] Sık sık sistem yedeği almak;

[6] Zararlı yazılımları tespit eden programlar kullanmak.

Ayrıca, şuan ve yakın gelecekte kötü amaçlı yazılımlar:

[1] Yazılımların güvenilirliğini gösteren sertifikaları çalabilmekte;

[2] Koruma yazılımlarına saldırarak bu yazılımların düzgün çalışmasını engelleyebilmekte;

[3] Sistemleri etkiledikten sonra bu sistemlerin normal hale dönmesini zorlaştırmakta;

[4] Korsan amaçlı kullanılan yazılımlar neticesinde zararlı yazılımlar gizlenebilmekte;

[5] İşletim sistemi ve üçüncü parti yazılımların yapısına müdahale ederek bu yazılımları farklı amaçlar için kullanmakta;

[6] Diğer kötü amaçlı yazılımlarla koordineli çalışarak daha yıkıcı sonuçları olan siber saldırılar başlatmaktadırlar.

Kötü amaçlı yazılımlar dinamikliğinden dolayı zaman zaman saldırı çeşidini ve saldırı hedeflerini değiştirerek gelecekte de var olmaya devam edecektir. Saldırılar artık sadece bilgisayar ağlarına, büyük şirket ve devletlerin veri tabanlarına değil sosyal medya ortamlarından, kritik alt yapı sistemlerine kadar bütün alanlarda saldırı vektörünü genişleterek yayılmaya devam edecekir. Yakın gelecekte yeni gelişen teknolojilerden (örneğin, akıllı telefonlar, sosyal medya ortamları, nesnelerin İnterneti, vb.) dolayı artık siber saldırılar sanal ortamlardan fiziksel ortamlara yayılacak hatta kötü amaçlı yazılımlar kullanılarak fiziksel cisimlere de zarar verilebilecektir. Bu zararlara örnek olarak bir yerde yangın çıkarma veya bir canlıyı öldürmek verilebilir. Bu derecede tehlike arz eden bu yazılımlarla daha etkin bir şekilde mücadele edebilmek için İnternet alt yapısının yeniden yapılandırılması ve ağın denetlenebilmesi gerekmektedir. Çünkü İnternette kullanılan protokollerin günümüz ihtiyaçlarını karşılayamaması ve karmaşık şekilde dağılmış olması, bütün ağın denetimini ve bakımını zorlaştırmaktadır. Ayrıca, yapısı gereği zafiyetlerle dolu bu sisteme her gün yeni cihaz ve yeni yazılımların eklenmesi İnternet ağını daha savunmasız bir hale getirmektedir. Statik ve dinamik analizin birlikte kullanılması, yeni araçların yazılarak analizlerde kullanılması ve analizleri otomatikleştirme adına veri madenciliği ve makine öğrenmesi algoritmalarının daha verimli kullanılması sonucu daha akıllı analiz ve tespit sistemlerinin geliştirilmesi problemi çözme adına büyük başarılar sağlasa da sorunu kökünken çözemeyecektir. Bundan dolayı ilk etapta bütün güvenlik önlemleri de düşünülerek zafiyet barındırmayacak şekilde işletim sisteminden bilgisayar ağına kadar bütün protokoller, programlar yeniden yapılandırılmalıdır. Çünkü yapısı gereği savunmasızlıklarla dolu bir sistemi yeni güncellemeler ve bazı denetlemelerle koruma yerine sorunsuz bir sistem oluşturmak sorun çözme adına daha faydalı olacaktır.

Kaynaklar

[1] Cohen, Fred. "Computer viruses: theory and experiments", Computers & security 6.1 (1987): 22-35.

[2] Lo, Raymond W., Karl N. Levitt, and Ronald A. Olsson. "MCF: A malicious code filter", Computers & Security 14.6 (1995): 541-566.

[3] Nazario, Jose. "Defense and Detection Strategies against Internet Worms", Artech House, (2004).

[4] Szor, Peter. "The art of computer virus research and defense", Pearson Education, (2005).

[5] Dag, Christoffersen. "Worm Detection Using Honeypots", Master thesis, (2006).

[6] Siddiqui, Muazzam Ahmed, "Data mining methods for malware detection", University of Central Florida, (2008).

[7] Lo, David, et al. "Classification of Software Behaviors for Failure Detection: A Discriminative Pattern Mining Approach", Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining. ACM, (2009).

[8] Davis, Michael, Sean Bodmer, and Aaron LeMasters, "Hacking Exposed Malware and Rootkits", McGraw-Hill, Inc., (2009).

[9] Fukushima, Yoshiro, et al. "A behavior based malware detection scheme for avoiding false positive", Secure Network Protocols (NPSec), 2010 6th IEEE Workshop on. IEEE, (2010).

[10] You, Ilsun, and Kangbin Yim. "Malware obfuscation techniques: A brief survey", Broadband, Wireless Computing, Communication and Applications (BWCCA), 2010 International Conference on. IEEE, (2010).

[11] Pratama, Andhika, and Fauzi Adi Rafrastara. "Computer worm classification", International Journal of Computer Science and Information Security 10.4 (2012): 21.

[12] Stallings, William, et al. "Computer security: principles and practice", Pearson Education, (2012).

[13] Lachow, Irving, "Active Cyber Defense A Framework for Policymakers", February (2013).

[14] Pilling, Rafe. "Global threats, cyber-security nightmares and how to protect against them", Computer Fraud & Security 2013.9 (2013): 14-18.

[15] Hahn, Katja. "Robust static analysis of portable executable malware", HTWK Leipzig (2014).

[16] Jang-Jaccard, Julian, and Surya Nepal. "A survey of emerging threats in cybersecurity", Journal of Computer and System Sciences 80.5 (2014): 973-993.

[17] Pandey, Sudhir Kumar, and B. M. Mehtre. "A Lifecycle Based Approach for Malware Analysis", Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on. IEEE, (2014).

[18] Steve Morgan, "Cyber Security Business Report", Aug 22, (2016).

[19] Aslan, Ömer, and Refik Samet. "Investigation of Possibilities to Detect Malware Using Existing Tools", 14th ACS/IEEE International Conference on Computer Systems and Applications AICCSA. (2017).

[20] Aslan, Ömer. "Performance Comparison of Static Malware Analysis Tools Versus Antivirus Scanners To Detect Malware", International Multidisciplinary Studies Congress (IMSC) on. (2017).

[21] Anonymous1 Web sitesi: https://www.webpagefx.com/blog/internet/cost-of-computer-viruses-infographic/

[22] Anonymous2 Web sitesi: https://www.investopedia.com/financial-edge/0512/10-of-the-most-costly-computer-viruses-of-all-time.aspx

[23] Anonymous3 Web Sitesi: https://www.gdatasoftware.com/seccuritylabs/information/history-of-malware

[24] Dick O'Brien, "Internet Security Threat Report on Ransomware", Semantec (2017).

[25] Sean Spencer, "Timeline of Computer Viruses", https://www.mapcon.com/us-en/timeline-of-computer-viruses.

Siber Terör, Terörizm ve Mücadele

BÖLÜM 9

Doç. Dr. Yıldıray YALMAN

SİBER TERÖR, TERÖRİZM VE MÜCADELE

Bu bölümde, teknolojik gelişmelere bağlı olarak internet altyapısının günlük hayatın neredeyse her anında insanlara ve sistemlere (devlet altyapısı, finans, savunma, elektrik/su/doğalgaz şebekeleri, vb.) eşlik ediyor olmasını fırsat bilen saldırganların sayısal/dijital ortamlardaki, özellikle politik amaçlarına ulaşmak için yaptıkları saldırılara, bireyleri ve toplumları en hafif ifade ile huzursuz kılan zararlı eylemlere işaret eden "Siber Terörizm" üzerinde durulmaktadır. Temel kavramların açıklanmasının ardından, siber terör saldırılarının yöntemleri, tarihsel süreçteki örnekler, günümüzde bu ve benzeri faaliyetlere karşı mücadeleye ilişkin detaylar anlatılmaktadır.

9.1. Giriş

Fransızca "terreur" sözcüğünden dilimize geçmiş olan "terör" terimi, Latince kökenli olup "korkudan titreme", "yıldırı" anlamına gelmektedir. Sıklıkla kullanılıyor olmasına rağmen terör teriminin yaygın kabul gören bir tanımı bulunmamaktadır. Terör teriminin sonuna eklenen "-izm" eki terörün sistematik olduğuna vurgu yapmak, terör eylemlerinin siyasi amaçlarına veya terör fikrinin eyleme dönüşmesine atıfta bulunmak için kullanılmaktadır. Bir başka ifade ile terör, hem şiddet yoluyla yaratılan korku ortamını hem de bu ortamı yaratan şiddet eyleminin kendisini ifade ederken; terörizm siyasi amaçlar için örgütlü, sistemli ve sürekli şekilde terörü araç olarak kullanmayı benimseyen bir eylem şekli olarak tanımlanabilir.

Terör bireyler veya toplum üzerinde korku yaratmaya yönelik genel bir kavramı ifade ederken, terörizm korku ortamının oluşturulması için gerekli olan şiddet/korkutma sürecine işaret eder; terörist ise

terörizmi bir yaşam şekli haline getirerek ilgili terör eylem(ler)ini gerçekleştiren saldırganlara verilen bir sıfattır.

Günümüzde en tehlikeli terörizm faaliyetlerinden birisi de teknolojinin bir araç olarak kullanıldığı "Siber Terörizm"dir. Siber terörizm, belirli bir sosyopolitik amaca ulaşabilmek adına bilgisayar veya bilgisayar sistemlerinin bireylere ve ürünlere karşı bir hükümeti veya toplumu yıldırma, baskı altına alma amacıyla kullanılması olarak tanımlanabilir. Kısaca, terör eylemlerinin bilişim araçları kullanılarak gerçekleştirilmesi şeklinde de ifade edilebilir. Bu kapsamdaki eylemlerde her türlü veri ya da bilginin değiştirilmesi, yok edilmesi veya zarar verilmesi söz konusudur. Klasik bilgisayar korsanlığından (hacktivism) farklı olarak doğrudan kişiler/kurumlar hedef alınarak hedeflerin zarar görmesi ve muhataplarda bir korku duygusunun uyandırılması amaçlanır.

Siber suç uzmanlarının Çevrimiçi Terörizm (Online Terrorism) olarak da ifade ettikleri Siber Terörizm, Amerikan Federal Souşturma Bürosu (FBI) tarafından yapılan tanıma göre "art niyetli kişiler tarafından gerçekleştirilen, savaşa/mücadeleye iştirak etmeyen kişileri hedef alan, planlı ve politik amaçlarla bilgilere, bilgi sistemlerine, programlara, platformlara yapılan saldırılar" olarak nitelendirilmektedir. Günümüzde ABD İçişleri Bakanlığı bünyesine katılmış olan ve 2002 yılında kapatılmasından önce ayrı bir birim olarak faaliyet gösteren Ulusal Altyapı Koruma Merkezine göre ise siber terörizm; "bilgisayar ve telekomünikasyon kabiliyetlerinin kullanımı ile hükümeti veya hedeflenen bir topluluğu etkilemek amacıyla karışıklık, belirsizlik ve korku yaratmak; şiddet, tahribat ve/veya hizmetlerin bozulması sonucuna ulaşılan eylemler gerçekleştirmek" şeklinde tanımlanmıştır [1].

Yukarıdaki bilgiler ışığında siber terörizm ile siber suç kavramları arasında bir farklılık olduğunu da belirtmek gerekir. Saldırgan(lar)ın elektronik ortam kullanarak maddi/manevi menfaat sağlamayı temel ilke olarak benimsediği vakalar "Siber Suç" olarak adlandırılırken, saldırının temel motivasyonunun fiziksel/finansal zarar vemek olduğu vakalar ise Siber Terörizm olarak tanımlanmaktadır. Bu kapsamda iki kavramın birbirinden, saldırganların temel motivasyonları açısından ayrıştığı görülmektedir.

9.2. Siber Terörizmde Saldırganların Kullandıkları Yöntemler

Dijital dünyayı temel saldırı platformu olarak kullanan saldırganlar bir takım teknikler kullanarak amaçlarına ulaşmayı hedeflerler. Bu kapsamda kullanılan kimi saldırı yöntemleri-araçları aşağıdaki şekilde sıralanabilir.

Gelişmiş Kalıcı Tehdit (Advanced Persistent Threat, APT): Saldırganların bir ağa sızıp, bu ağ üzerinde farkedilmeden uzun süre boyunca kritik verileri ele geçirmesi olarak tanımlanır. Ağa doğrudan zarar vermek yerine ağdaki güvenlik, üretim ve finansal bilgileri ele geçiren saldırganlar elde ettikleri verileri daha büyük terörizm amaçları için kullanılabilir. Söz konusu olan bir ülkenin kritik bir ağı ise elde edilen bilgiler ilgili ülkenin düşmanlarına satılabilir.

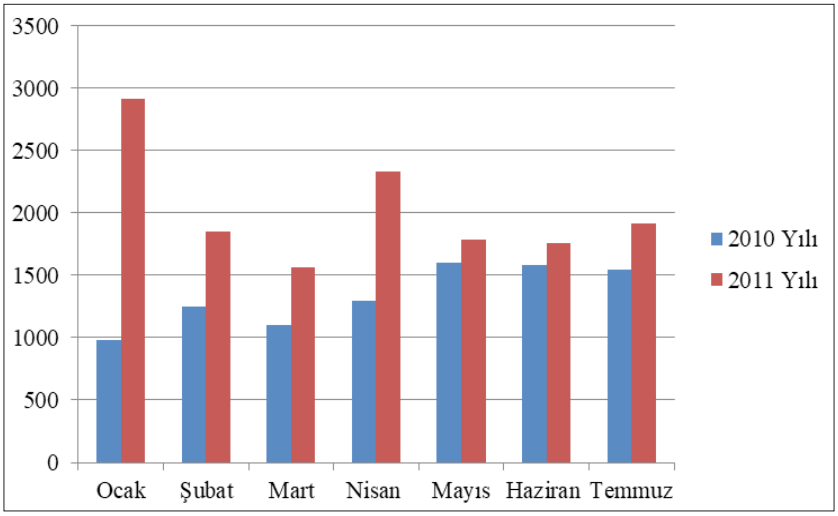
Kötücül Yazılımlar (Malware) - Virüsler, Solucanlar: Virüsler, çalıştığında bilgisayarlara değişik şekillerde zarar verebilen programlardır. Bu programlar (ya da virüs kodları) çalıştırıldıklarında bulundukları sisteme programlanma algoritmalarına göre zarar vermeye başlarlar. Ayrıca, tüm virüs kodları (bilinen adıyla virüsler) bir sistemde aktif hale geldikten sonra çoğalma (enfekte olan bilgisayadaki diğer dosyalara yayılma, ağ üzerinden diğer bilgisayarlara bulaşma, vb.) özelliğine de sahiptir. Solucanlar (worm) ise kullanıcıya gerek duymadan kendini yayabilen, kendi başına çalışan yazılımlardır. Virüslerden farklı olarak diğer dosyalara bulaşmazlar, ancak kendilerini kopyalayarak çoğalma özelliğine sahiptirler. Kendisini ağ üzerinden dağıtan solucanlar, ağ trafiğini yoğunlaştırarak yavaşlatabilirler.

Bu saldırı araçları yardımıyla hedeflenen sistemin kontrol mekanizması ele geçirilebilir. Böylelikle saldırganlar kendi terör-saldırı amaçlarını gerçekleştirmek üzere kullanabilirler ve özellikle mali açıdan ciddi zararlar verebilirler (Tablo 9.1).

Sadece 2010-2011 yılları arasındaki kötücül yazılım kaynaklı sorunlardaki artış Şekil 9.1'de görülmektedir. İlgili yılların ilk 7 ayı kıyaslandığında ay bazında 2011 yılında görülen kötücül yazılım sayısı kayda değer oranda artmıştır.

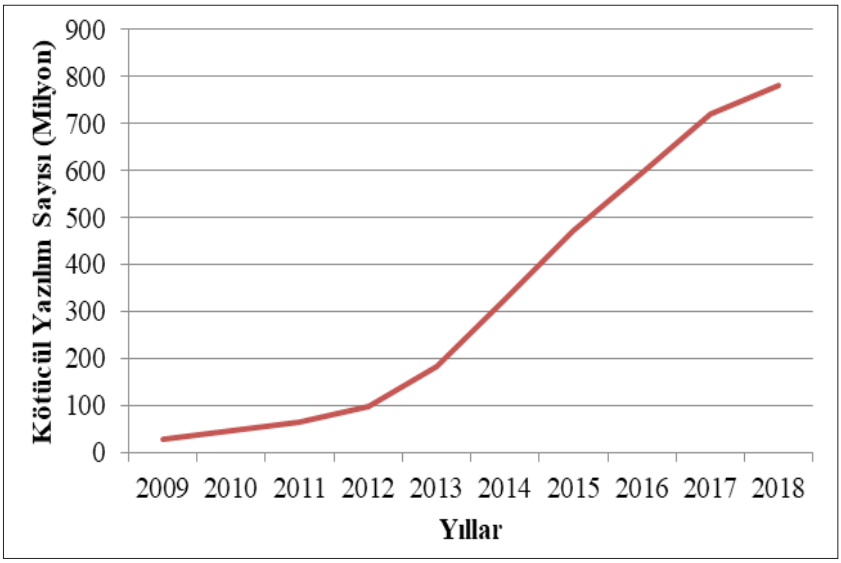
Tablo 9.1. Milenyumun ilk 10 yılında ortaya çıkan en zararlı yazılımlar.

Yıl	Zararlı Yazılımın Adı	Hedefi	Oluşturduğu Tahmini Zarar (Milyar $)
2000	I Love You	Sistem dosyalarını silmek	15
2001	Code Red	Beyaz Saray'da arka kapı oluşturmak	2
2003	Sobig.F	e-posta trafiğini etkilemek	37
2004	MyDoom	e-posta trafiğini etkilemek	38
2008	Conficker	Bilgisayarı açık kapı haline getirmek	9,1



Şekil 9.1. 2010-2011 yıllarının ilk 7 aylık kötücül yazılım vakası karşılaştırması [2].

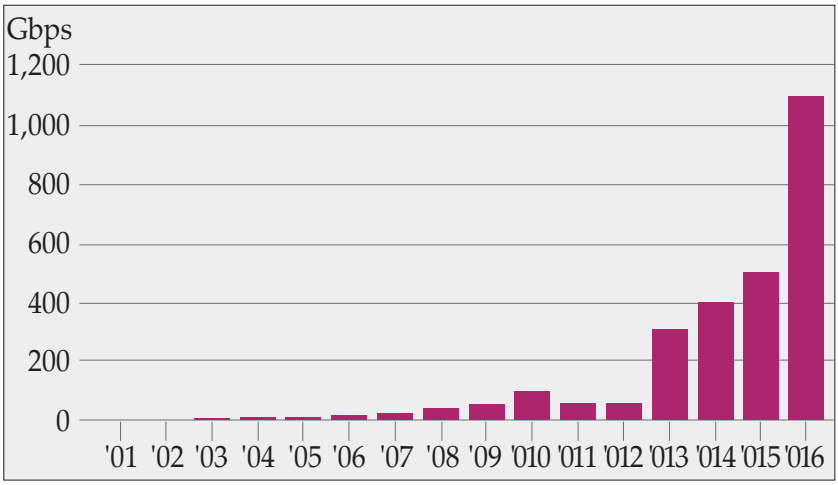
Şekil 9.2'de ise 2009-1018 yılları arasında kötücül yazılım sayısındaki dramatik artış görülmektedir [3]. Bu durum muhtemel tehlikenin boyutunun da hangi oranda arttığına açıkça işaret etmektedir.



Şekil 9.2. 2009-2018 yılları arasında kötücül yazılım sayısındaki artış.

Dağıtık Hizmet Aksattırma Saldırıları (Distributed Denial of Service: DDoS): İnternete bağlı bir sunucunun hizmetlerini geçici veya süresiz olarak aksatarak, bir makineye veya ağ kaynaklarına asıl kullanıcılar tarafından ulaşılamamasını hedefleyen siber saldırı türü hizmet aksattırma (DoS) olarak adlandırılır. Bu tip saldırılarda hedef makine veya kaynağın, gereksiz talepler ile aşırı yüklenmesi ve meşru taleplere doluluk gerekçesi ile cevap verememesi hedeflenir. Bu saldırılar bir grup insanın, bir dükkânın kapılarını tıkayıp, alışveriş yapmak isteyen müşterilerin içeri girişini engelleyerek normal işlemleri aksatmasına benzetilebilir.

DoS saldırıları geniş bir kitle veya zombi olarak kullanılan bilgisayarlar yardımıyla yapıldığında çok tehlikeli bir hal alır ve DDoS adı ile anılır. DDoS saldırıları sonucunda en güçlü sistemler bile ayakta duramayabilir. Her geçen yıl DDoS saldırılarının daha yüksek band genişliğini işgal ederek etkisini arttırdığı düşünüldüğünde, saldırganların giderek daha fazla kullandığı bir saldırı türü olduğu açıkça görülmektedir (Şekil 9.3).



Şekil 9.3. 2001-2016 yılları arasında yayılmış servis reddi atakları arasında en yüksek band genişliğini işgal eden saldırılara ilişkin istatistik.

Fidye Yazılımı (Ransomware): Bir bilgisayarın rehin alınıp sistemin veya dosyaların kontrolünün geri verilmesi için fidye ödenmesinin talep edildiği saldırılardır.

Oltalama (Phishing) Saldırıları: Bu tür saldırılar, günümüzde bireylerin sosyal yaşamında sıklıkla rastlanılan ve kimi otoritelerce bir bağımlılık sorunu (nomo-phobia: no mobile phone anxiety) olarak görülen mobil telefon ile çevrimiçi yaşam içerisinde saldırganların muhtemel kurbanları hakkında veri ele geçirmek ve kimliklerini açığa çıkarmak amacıyla kullanılırlar [4].

Yukarıdaki kısaca özetlenen saldırı araçları-teknikleri kullanılarak etki altına alınabilecek sistemler/platformlardan bazıları aşağıdaki şekilde sıralanabilir:

- Devlet kurumlarına ait elektronik hizmetler,
- Bankacılık ve finans sistemleri,
- Askeri/savunma sistemleri,
- Enerji santralleri,
- Hava kontrol sistemleri,
- Barajlar ve su arıtma sistemleri,
- Yayın organlarının (ajanslar, gazeteler, vb.) web platformları,
- Kent trafik kontrol mekanizması ile raylı sistem sinyalizasyonu.

9.3. Tarihsel Süreçte Siber Terörizm Örnekleri

Dünya Çapında Ağ (World Wide Web) 1989 yılında gündeme gelmiş ve 1991 yılında ilk web sitesi yayınlanmıştır. Günümüzde ise 1,2 milyarın üzerinde web sayfası bulunmaktadır. 1990'lı yılların başında Web 1.0 olarak adlandırılan ilk aşamada bugün kullanılan arama motorları ve etkileşim sayfaları (sosyal medya platformları) bulunmuyordu. Ancak Web 2.0 ve sonrası ile tüm sınırlar zorlanır hale gelmiş olup, bilgisayarların etkileşimi ve günlük hayattaki yeri üst sıralara tırmanmıştır [5]. Dünya genelinde 2017 yılı itibarı ile 3,8 milyar internet kullanıcısı bulunmakta idi. 2015 yılında bu sayının 2 milyar kişi daha az olduğu dikkate alındığında, artış hızı dikkate değer seviyededir [6]. Tablo 9.2'de 2015 ve 2017 yılı gerçekleşmeleri ile birlikte 2022 ve 2030 yıllarına ilişkin tahmini internet kullanıcı projeksiyonları da verilmektedir. İnternet kullanım oranındaki artış, beraberinde siber terör saldırılarına muhatap olacak insanların da büyük oranda artacağına işaret etmektedir.

Teknolojik imkanların artması sayesinde bireylerin ve devletlerin her geçen gün internet ortamındaki faaliyetlerini arttırmalarıyla birlikte saldırganlar saldırı aktivitelerini bu platformlara kaydırmış olup, Siber Terörizm örnekleri de artış göstermiştir. En çok saldırı yapılan platformlar;

- Sağlık hizmetleri,
- İmalat sanayi,
- Finansal servisler,
- Devlet hizmetleri,
- Ulaşım sektörü,

olarak göze çarpmaktadır [6].

Tablo 9.2. Dünyada internet kullanımı [6].

Yıl	Nüfus	İnternet Kullanıcı Sayısı	İnernet Kullanımının Nüfusa Oranı
2015	7,3 milyar	1,8 milyar	% 24
2017	7,6 milyar	3,8 milyar	% 50
2022 (Tahmini)	8 milyar	6 milyar	% 75
2030 (Tahmini)	8,5 milyar	7,5 milyar	% 88

Hangi tip saldırıların siber terörizm olarak değerlendirilmesi gerektiği halen tartışılan bir konudur. Hukukçular, emniyet güçleri, bilişim uzmanları ve teknoloji şirketleri farklı görüşleri savunabilmektedir. Siber Terörizm oldukları yönünde genel kabul gören kimi örnekler aşağıdaki şekilde sıralanabilir:

- 1991: 1. Körfez Savaşı esnasında Hollandalı bir grup saldırgan Pentagon merkezi bilgisayar sistemine sızarak ABD'nin savaş operasyonlarını değiştirmiş ve mevcut planları kopyalamışlardır.
- 1996: CIA'nin internet sayfasına gerçekleştirilen saldırılar sonucunda, sayfadaki bilgiler değiştirilmiştir.
- 2001: California elektrik hizmet sağlayıcısına yapılan saldırı sonucu internet 1 gün süre ile kesilmiştir.
- Mart 2014: Rusya kaynaklı olduğu iddia edilen ve Ukrayna'da internetin kesintiye uğratılması ile Rusya yanlısı isyancıların Kırım'ın kontrolünü ele almasını destekleyen bir DDoS saldırı olmuştur.
- Mayıs 2014: Rusya'da bulunduğu iddia edilen bir grup saldırgan tarafından Ukrayna Cumhurbaşkanlığı seçiminden 3 gün önce seçim komisyonu sistemi hedef alınmış ve sistemin işlevsiz hale getirilmesi için saldırılar yapılmıştır.
- 2014: Bu yılın sonlarında 500 milyon Yahoo kullanıcısının şifreleri çalınmış olup, ilgili şifrelere ek olarak kişisel bilgiler ile gizli soru-yanıtlarının da çalındığı şirket tarafından kabul edilmiştir. Bu skandaldan daha önce de MySpace'in 359 milyon, LinkedIn'in

159 milyon ve Adobe'un 152 milyon kullanıcısına ait bilgiler çalınmıştır.

- 2015: Saldırganlar Alman politikacılar tarafından kullanılan 20 bin bilgisayarı etkileyerek, hassas verileri çalmış ve karşılığında milyonlarca avro istemişlerdir. Bu olayların arkasında Alman hükümetinin Ukrayna'yı desteklemesini protesto eden bir Rus saldırgan grubu olduğu iddia edilmiştir.
- Aralık 2016: Bir grup siber saldırgan tarafından Ukrayna'daki 3 bölgesel elektrik şirketine yapılan DDoS saldırısı sebebiyle 225.000 müşterinin elektrikleri kesintiye uğramıştır. Bu saldırı aynı zamanda telefon hatlarını da kullanılamaz hale getirmiştir.
- Mayıs 2017: Dünya genelinde hastaneler, devlet daireleri WannaCry isimli fidye yazılımı sebebiyle çok zor durumda kalmıştır. Bu virüs fidye karşılığında ele geçirdiği dosyaların iade edilmesini sağlayan bir algoritma ile çalışmaktadır. 99 ülkede 75.000 civarında fidye saldırısı olduğu rapor edilmiştir. Bu vaka saldırganların para temin etme isteği sebebi ile Siber Suç olarak değerlendirilebilmekle birlikte, bilgisayar ve internet kullanıcıları üzerinde oluşturduğu korku, sistemlerin çalışamamasını sağlaması gibi sebeblerle de Siber Terörizm olarakta nitelenebilecek bir olaydır.
- Tüm zamanların en usta bilgisayar korsanlarından biri olarak kabul edilen Yeni Zelandalı Barnaby Jack 2008 yılında satın aldığı 2 ATM cihazını detayları ile inceleyerek 2010 yılına kadar geçen sürede sıkı bir çalışmayla ATM'lerin yazılımında bulunan zayıf noktaları tespit edip, bu zayıflıkların manipüle edilmesi yoluyla internet üzerinden ATM'leri kontrol edip edemeyeceğini araştırmıştır. İki yıl süren çalışmaları süresince Jack, şifre ve seri numarası taleplerini by-pass etmekten, bankomat ve kredi kartlarının üzerindeki manyetik şeritler vasıtasıyla banka hesap bilgilerine ulaşıp ATM kullanıcılarının şifrelerini çalmaya kadar pekçok konuda kendini geliştirmiştir. 2010 yılının Temmuz ayında, Las Vegas'ta düzenlenen Black Hat Briefings adlı konferansa katılan Jack, yalnızca bir telefon modemi vasıtasıyla bir ATM'ye bağlanıp, şifre kullanmadan makinadaki tüm parayı çekmeyi başarır. Bilgisayar teknolojileri literatürüne "Jackpotting" olarak geçen bu olay büyük yankı uyandırır. 2011 yılının Ekim ayında,

Las Vegas'taki bir konferansta yeniden sahne alan Jack, diyabet hastalarının vücutlarındaki insülin dengesini kontrol etmek için vücutlarına küçük bir hortumu yapıştırarak kullandıkları, tıbbi bir cihaz olan "insülin pompası"nı hedef almıştır. Kablosuz internet aracılığıyla diyabetik bir arkadaşının üzerindeki insülin pompasını hacklemeyi başarır. Bunun yanı sıra anten kullanarak, seri numarasını bilmesine bile gerek kalmadan insülin pompasındaki verileri de kontrol eder.

Literatüre Jackpotting olarak geçmiş olan bu saldırı yöntemi 2018 yılı Ağustos ayında FBI tarafından tüm dünyaya "ATM cihazlarına Jackpotting saldırısı yapılması istihbaratı aldıklarına" dair uyarı mesajının iletilmesi ile tekrar gündeme gelmiş ve toplumlarda tedirginliğe sebep olmuştur. Bu tip bir saldırıya maruz kalan bir ATM, saldırganların yönetimine geçmekte ve verilen tek bir komutla kasasında bulunan bütün parayı büyük ikramiye veren slot makinesi gibi teker teker vermeye başlamaktadır.

Yukarıda sadece bir kaçı özetlenen olayların kimi otoritelerce siber suç, kimilerine göre ise siber terörizm faaliyeti olarak değerlendirildiğinden bahsedilmişti. Bu noktada olay bazında değerlendirme yapılması ve bilişim hukuku uzmanlarının ilgili olay özelinde tüm yönleriyle çalışma yaparak nihai kararın verilmesi önem taşımaktadır. Ek olarak şu hususa dikkat çekmek gerekir: her siber suç, siber terörizm faaliyeti olarak değerlendirilemese de; her siber terörizm faaliyetinin bir siber suç olarak değerlendirilmesi gerektiği çok açıktır. Yani siber suç genel bir suç kavramı iken, siber terörizm daha özel/spesifik bir suç faaliyetidir.

Siber terörizmde her ne kadar dijital platformların saldırı için araç olarak kullanılması ve saldırı sonuçlarından çoğunlukla yine dijital platformların etkilenmesi ön plana çıkarılsa da, klasik terör eylemlerinin gerçekleşmesi amacıyla dijital platformların temel haberleşme aracı olarak kullanılması da siber terör başlığı altında değerlendirilebilmektedir [7]. Teröristlerin saldırı planları, ulaşım, karayolu haritaları, uçuş planları, ekonomik veriler, toplu taşıma faaliyetleri (raylı sistem, deniz yolu, vb.) ile ilgili bilgileri aralarında paylaşmaları (e-posta, sohbet odaları, forumlar, Youtube, Google Earth, vb. platformlar ile) birer siber terörizm faaliyeti olarak değerlendirilebilir.

9.3. Gelecek ve Siber Terörizm

Büyük Veri (Big Data) analistlerine göre 2006 yılında özelikle akıllı cihazlar (telefon, tablet bilgisayar, vb.) kullanılarak internete yüklenen veri (ses, video, fotoğraf, vb.) miktarı 2 milyar iken, 2020 yılında bu sayının 200 milyar olması beklenmektedir. 2017 yılında satılan 310 milyon internet bağlantılı giyilebilir cihaz (saat, gözlük, vb.) sayısının 2021 yılında yarım milyara ulaşması hedeflenmektedir. 2020 yılı itibarı ile dünya genelinde kullanıcılar internet ortamında, bir başka deyişle siber uzayda 300 milyar şifreye ihtiyaç duyacaklardır. Ortaya çıkan ve oluşması muhtemel güvenlik açıklarını kapatmak için ise 111 milyar satırdan oluşan yeni bilgisayar kodlarının yazılması öngörülmektedir [6].

Dünya çapındaki sayısal veri miktarının 2016 yılı itibarı ile 4 milyar zetabayttan (1 zetabyte=2^{70} bayt), 2020 yılı itibarı ile 96 milyar zetabayt mertebesine gelmesi beklenmektedir. Yetenekleri arttırılan ve insan vücuduna yerleştirilebilen, kablosuz internet bağlantısı yeteneğine sahip cihazların (insülin pompası, kalp pili, işitme cihazı, vb.) siber terörün hedefi haline gelmesi durumunda oluşacak kaotik yapıyı dikkate almak ve şimdiden gerekli önlemleri alarak çalışmaları yürütmek hayati önem taşımaktadır.

Örneğin oltalama saldırısı yapmayı planlayan saldırganlar sosyal medya aktivitelerinin arttığı zamanları kollayarak daha fazla insanda korku ve endişe yaratmayı hedeflerler. 2014 FIFA Dünya kupası final mücadelesinde dakikada 618.000 mesaj (tweet) atılarak Twitter rekoru kırılmıştır. Benzer şekilde aynı kupa organizasyonunda maçların oynandığı 32 gün boyunca Facebook platformunda 350 milyon kullanıcı 3 milyarın üzerinde mesaj paylaşmış ve yorum yapmıştır [8]. Bu ve benzeri zamanlar masum görünümlü bir mesajın/linkin kullanıcılar tarafından tıklanması yoluyla kaos yaratmak saldırganlar için çok elverişli ve kolaydır. Bu sebepledir ki, kullanıcıları aldatma, oltalama, kötücül/zararlı yazılım vakaları sosyal medya platformlarında giderek artan sıklıkta karşımıza çıkmaktadır [9]. Her ne kadar özellikle sosyal medya platformlarının yetkilileri ve araştırmacılar otomatik olarak bu ve benzeri saldırıları içeren link, mesaj, vb. içeriklerin tespiti için yöntemler geliştirseler de (örneğin Facebook için Web of Trust işlemi), saldırıların tamamının

engellenmesi mümkün olamamaktadır. Bu noktada kullanıcıların bilinçli olmalarının ne denli önemli olduğu bir kez daha karşımıza çıkmaktadır.

Cihazların internete erişerek farklı cihazlar/platformlar ile iletişim halinde olması olarak tanımlanan Nesnelerin İnterneti (Internet of Things:IoT), Cisco şirketine göre 2021 yılında dünya nüfusunun 3 katından fazla sayıda var olacak olan bu nitelikteki dijital nesneler, giderek Sorunların İnterneti (Internet of Trouble: IoT) haline gelmektedir [10]. IoT cihazlarının temel özelliklerinden birisi de bir takım sensörlerden gelen bilgilere göre çalışan otonom sistemler olmasıdır. Önümüzdeki 20 yıl içerisinde 45 trilyon adet sensörün IoT cihazları vasıtasıyla web ortamına veri aktarması, sensörleri bünyesinde barındıran IoT cihazlarının (robot, otomobil, klima, fırın, vb.) dış dünya ile iletişim halinde olması öngörülmektedir. Web ortamından kontrol edilebilen bir fırın modelinin, siber terör saldırısı sonucu bulunduğu evde yangına sebebiyet vermesi, bu modele sahip tüm evlerde aynı istenmeyen olayın oluşması; otonom araçların kontrolden çıkartılarak bir anda binlerce ölümlü kaza vakasının yaşanması kuvvetle muhtemel bir olay olarak insanoğlunun karşısına çıkacaktır.

Karanlık veya Derin Ağ (Dark-Deep Web) olarak adlandırılan ve indekslenemeyen web içeriklerinde klasik web platformlarına kıyasla 5000 kat daha fazla kriminal aktivite olduğu değerlendirilmektedir.

Fidye virüslerinin (ransomware) insanlar üzerinde oluşturduğu psikolojik etki düşünüldüğünde, en tehlikeli siber terör araçlarından biri olduğu aşikardır. Bu sebepledir ki, giderek artan miktarda olay rapor edilmektedir. Günümüzde her 40 saniyede bir fidye yazılımı vakası söz konusu iken, 2019 yılında bu istatistiğin 14 saniyeye düşmesi beklenmektedir. Dünya çapında fidye virüslerinin maliyeti 2017 yılında 5 milyar dolar olurken, bu rakam 2015 yılında gerçekleşen miktarın 15 katına karşılık gelmektedir [6].

Bugünkü ve gelecekte beklenen kabiliyetleri açısından yukarıda kısaca değerlendirilen siber uzay (bir başka ifade ile dijital dünya), insanların yaşamına kolaylık getirmeyi hedeflemekle birlikte, saldırganların önemli bir saldırı aracı olacağını da göz önünde bulundurduğumuzda; güvenlik çalışmaları ve harcamaları yapmak ta ka-

çınılmaz hale gelmektedir. ABD, sadece dijital dünyadaki bilgi güvenliği çalışmaları için 2017 yılında 86 milyar dolar harcarken, 2018 yılında bu miktarın 93 milyar dolara çıkarılması öngörülmektedir. Siber güvenlik girişimcilerine göre önümüzdeki 5 yıl içerisinde siber güvenlik için toplam 1 trilyon dolar seviyesinde bir harcamanın yapılması söz konusudur [6]. Matematik, fizik, bilgisayar bilimi ile uğraşan araştırmacılara ek olarak toplum bilimcilerin de biraraya gelerek oluşan sorunların çözümü ve muhtemel terörizm eylemlerinin önlenmesi için çalışmalar yapması büyük önem taşımaktadır.

9.4. Siber Terörizmle Mücadele

Terörizmin psikolojik sebeplerini ve terör zihniyetini daha iyi anlamak ve analiz etmek adına literatürde bir takım çalışmalar sunulmuştur [11, 12]. Ancak "siber terörizm" üzerine çalışmaların aynı yoğunlukta olduğunu söylemek mümkün değildir [13]. Az da olsa siber teröristlerin psikolojileri [14], toplum üzerinde siber terörizmin etkileri [15] üzerine çalışmalar da yapılmıştır. Bu çalışmalardan en dikkat çekici olanlarından birinde ise siber teröristlerin temel motivasyonları şu şekilde sıralanmıştır [16]:

- Politik amaç,
- Ego tatmini,
- Bir sosyal gruba katılma isteği,
- Para,
- Eğlence,
- Statü.

Birleşmiş Milletler Bölgelerarası Suç ve Adalet Araştırma Enstitüsü (United Nations Interregional Crime and Justice Research Institute) tarafından 2004-2010 yılları arasında siber suçlardan sorumlu olan saldırganların sınıflandırılmasını sağlamak ve mücadele etmek için bir araştırma projesi yapılmıştır. Bu kapsamda saldırganların yetenekleri, bireysel/grup hedefleri, demografik yapıları, tehlike seviyeleri sınıflandırılmaya çalışılmıştır. İlgili çalışmanın ikinci aşamasında ise siber terörizm faaliyetlerinin ortaya çıkmadan önlenmesi için yöntemler geliştirilmesi ve muhtemel siber teröristlerin önceden belirlenmesi için çalışmalar yapılmıştır [17].

ABD Savunma Bakanlığı bünyesinde faaliyet gösteren İleri Savunma Projeleri Ajansı (Defense Advanced Research Projects Agency) tarafından 2010 yılı Ocak ayında "Siber Genom Projesi" başlatılmıştır [18]. Bu proje ile siber atakların genetik yapısı analiz edilmeye ve hangi grup/saldırgan tarafından gerçekleştirildiği, saldırının karakteristiklerine göre savunma/karşı atak stratejileri bulunmaya çalışılmaktadır [19].

Avrupa Birliği bünyesindeki 12 ülkede faaliyet gösteren toplam 17 organizasyonun katılımı ile COURAGE (Cybercrime and Cyberterrorism European Research Agenda) isimli siber suç ve siber terörizm ile ilgili olarak Avrupa araştırma gündemi üzerine 2 yıl boyunca çalışılmış ve 2016 yılında üzerinde daha fazla çalışma yapılması yönünde yasa koyucuların, çözüm ortaklarının, araştırma ve teknoloji organizasyonlarının, politika geliştiricilerin, akreditasyon ve sertifikasyon paydaşları ile eğitim kurumlarının aşağıda belirtilen 12 husus üzerinde daha fazla çalışılması gerektiği sonucu deklare edilmiştir [20]:

- Yasadışı içeriği engellemenin meşruiyeti ve etkinliği,
- Terörizmi destekleyen nefret söylemi ile içerikle ilgili suçların önlenmesi ve mücadele edilmesi,
- Bilgisayarla ilgili dolandırıcılıkların tespiti ve önlenmesi,
- Telif haklarının daha güvenli hale getirilmesi, bu alandaki problemleri önleme yöntemlerinin etkinliğinin arttırılması,
- Siber terörizm olaylarında mağdur ve suçluların tanımı, özellikleri ve davranışları,
- Gizlilik mevzuatı yönetmeliklerine uygun olarak dijital araştırmalar için ileri kabiliyetlere sahip araçların geliştirilmesi,
- Arama linki verilmeyen veya arama motorları tarafından bulunamayan ağlarda (Dark Web: Karanlık Ağ) siber terör faaliyetlerinin tespiti ve önlenmesi,
- Avrupa Birliği genelinde Siber terörizmin net şekilde tanımlanması, üye ve aday ülkelerin tamamında uyumlu hale getirilmesi,
- Siber terörizm ile ilgili önleyici araçların ve strateji geliştirme yöntemlerinin standardizasyonu,

- Yasadışı içerik için yasal çerçeve sorunları: Coğrafi konum ve Yargı yetkisi sorunları,
- Uluslararası ve kamu/özel sektör işbirliği,
- Siber terör tehditlerine karşı toplumsal direncin arttırılması için bilinçlendirme ve eğitim faaliyetleri.

Bugün dünya nüfusunun yaklaşık 8 milyara yaklaştığı ve bu nüfusun neredeyse yarısının aktif olarak internet kullandığı, sosyal paylaşım sitelerinde yaklaşık 2 milyar hesabın bulunduğu bilinmektedir. Detayları Tablo 9.3'te verilen TÜİK verilerine göre, Türkiye'de ise 2018 yılı itibariyle internet kullanan bireylerin oranı %72,9 olarak gerçekleşirken, bu oran her geçen gün artmaktadır. Ayrıca internet üzerinden alışveriş yapanların oranı ise %24.9'dur [21]. Bu oranlardaki artışa paralel olarak siber uzayda oluşan terör faaliyetlerinin sayısı da doğru orantılı olarak artmaktadır.

Tablo 9.3. TÜİK verilerine göre Girişimlerde Bilişim Teknolojileri Kullanımı Araştırması ve Hanelerde Bilişim Teknolojileri Kullanımı Araştırması [21]

	2014	2015	2016	2017	2018
Girişimlerde Bilişim Teknolojileri Kullanımı (%)					
Bilgisayar Kullanımı	94,4	95,2	95,9	97,2	-
İnternet Erişimi	89,9	92,5	93,7	95,9	-
Web Sitesi Sahipliği	56,6	65,5	66,0	72,9	-
Hanelerde Bilişim Teknolojileri Kullanımı (%)					
Bilgisayar Kullanımı (Toplam)	53,5	54,8	54,9	56,6	59,6
Erkek - Male	62,7	64,0	64,1	65,7	68,6
Kadın - Female	44,3	45,6	45,9	47,7	50,6
İnternet Kullanımı (Toplam)	53,8	55,9	61,2	66,8	72,9
Erkek - Male	63,5	65,8	70,5	75,1	80,4
Kadın - Female	44,1	46,1	51,9	58,7	65,5
Hanelerde İnternet Erişimi	60,2	69,5	76,3	80,7	83,8

1990-2011 yıllarını kapsayan bilişim suçları araştırmasına göre çocuk istismarı %3, müstehcenlik %8, telif hakları ihlali %13, bilişim sistemlerine girme, değiştirme ve bozma %17, kişisel verileri değiştirme, bozma, çalma % 2, banka/kredi kartı dolandırıcılığına maruz kalanların oranı ise %57'dir. Gelişmiş Avrupa ülkeleri internet ortamını terörize eden bu tehlikenin farkına vararak bu suçların önüne geçmek ve kişisel bilgilerin korunması amacıyla değişik yönerge ve mevzuat çalışmaları yapma konusunda ciddi ilerleme kaydetmişlerdir. Bu konuda detaylı bilgiye Bölüm 10'da yer verilmiştir.

Siber uzayda oluşması muhtemel terörizm faaliyetlerinin önlenmesi için bir takım güvenlik standartları bulunmaktadır. Güvenlik standartlarının ve bu standartlara ait kılavuzların kullanılmasının temel sebebi, ilgili alanda üretilen yazılım/donanımların veya sistemlerin, bağımsız laboratuarlar tarafından belirli kurallar çerçevesinde test edilmesini ve değerlendirilmesini sağlamak, dolayısıyla kullanıcılara bu konuda garanti verilmesine aracı olmaktır. Bu test ve değerlendirmelerin temel amacı, güvenlik ile ilgili fonksiyonların donanım/yazılım üzerinde eksiksiz olarak gerçekleştirildiğini kontrol etmek ve iddia edilen garanti seviyesinin sağlanıp sağlanmadığını belirlemektir. Yazılım/Donanım güvenliği değerlendirmesi konusundaki ilk çalışmalar, TCSEC (Trusted Computer System Evaluation Criteria) standardının 1983 yılında Amerika Birleşik Devletleri Savunma Bakanlığı tarafından yayınlanması ile başlamıştır [22]. Bilgi güvencesi kapsamında, yazılım ve donanımların TCSEC ve ITSEC (Information Technology Security Evaluation Criteria) gibi standartlara uygunluğunun kontrol edilmesi aksi takdirde kullanılmaması en uygun yaklaşım olacaktır.

Özellikle kurumlar tüm uygulamalarını bilgisayar ortamına taşıyıp gelir-gider, Ar-Ge, ürün, personel, kurum politikaları gibi kurum için hayati öneme sahip olan bilgileri disklerde tutmakta, yedeklerini de yedekleme ünitelerindeki veri saklama ünitelerine almaktadırlar. Aynı şekilde herhangi bir kişinin bilgisayarında kendisine ait gelir-gider, banka işlemleri, sağlık bilgileri, özel resim/video dosyaları gibi kayıtlar bulunabilir. Hatta bu bilgiler kişilerin cep telefonlarında da olabilir. Bu verilerin yedekleri genellikle harici bir disk, bellek, CD, DVD gibi bir saklama ortamında saklanmaktadır. Bu bilgileri kontrol eden yazılımların ve taşıyan/saklayan donanımla-

rın standartlara uygun yapıda olması ve güvenli ortamda bulunması, güvenilir yazılımlar eşliğinde kullanılmaları siber terörizm saldırılarına karşı alınabilecek en temel önlemlerdir.

Ağ güvenliği teknolojileri, ağı siber hırsızlığa, gizli iş bilgilerinin kötü amaçlarla kullanılmasına, internetten kaynaklanan virüs ve solucanların saldırılarına karşı korurlar. Haberleşme güvenliği (COMSEC: Communication Security) ise bilgi ya da haberin iletişim kanallarından güvenli iletimiyle ilgilenir ve bilgisayar sistemlerinin ağ girişleri ile dış dünyaya bağlantı sağlayan noktalardaki güvenlik teknolojilerine odaklanır. Ağ ve haberleşme güvenliğinin sağlanamaması durumunda, yetkisiz sızma, ağın kapanması, hizmet kesintisi riski mevcuttur. Ağın siber terör faaliyetlerine karşı güvenliği söz konusu olduğunda sistemin daima çalışır durumda olması, doğrulama, veri bütünlüğü ve veri gizliliği başlıklarını kapsayan bilgi güvencesinin sağlanması hayati önem taşımaktadır [23].

Ağ ve haberleşme güvenliği tek bir yönteme dayalı olarak gerçekleştirilmez. Bunun yerine, kişisel/kurumsal ağların farklı yöntemlerle savunulması için bir dizi engel kullanılır. Bir çözüm başarısız olsa dahi, diğeri ayakta kalarak ağı ve verileri, siber terör saldırılarına karşı koruyabilir. Ağdaki güvenlik katmanları, işin/iletişimin yürütülmesi için kullanılan değerli bilgilerin yetkili kişilerin kullanımına açık olması ve tehditlere karşı korunmasına imkan sağlar. Temel olarak ideal ağ güvenliği sistemleri (yük dengeleyiciler, güvenlik duvarı, antivirüs yazılımları ve ağ güvenliği için üretilmiş diğer donanım ve yazılım elemanları), dahili ve harici ağ saldırılarına karşı koruma sağlar. Muhtemel siber terör tehdidi, işletmenin ya da odanın dört duvarı içinden veya dışından gelebilir. İdeal bir ağ güvenlik sistemi tüm ağ etkinliğini izleyerek olağandışı davranışı işaretler ve uygun yanıtı verir. Her yerde ve her zaman tüm iletişimin gizliliğini sağlamak için çalışır. Bu noktada önemli olan bireylerin evlerinde veya hareket halindeyken ağ ile iletişimlerinin gizli ve koruma altında olacağı güvencesinin verilebilmesidir.

Ağ güvenlik sistemleri, kullanıcıları ve ağ yapısını doğru bir şekilde tanımlayarak bilgiye erişimi denetleme amacını güderler. Bireyler ya da kurumlar, veri erişimiyle ilgili olarak kendi kurallarını oluşturabilirler. Erişimin reddedilmesi veya onaylanması kullanıcı kimliklerine, iş işlevine veya işle ilgili diğer özel ölçütlere dayanabilir.

Bu sebeple ideal bir ağ güvenlik sisteminin kurulması, güncel gelişmelere adapte edilmesi, log bilgilerinin düzenli analizi ve belirli periyotlarla saldırı yapılarak sistemin dayanıklılığının ölçülmesi (örneğin sızma testleri) siber terör faaliyetlerine karşı güvence oluşturmak adına önemli bir unsurdur.

Siber terörizm ile mücadelede yetişmiş insan kaynağının önemi çok büyüktür. Palo Alto Ağ Araştırmaları Merkezi tarafından 2019 yılında dünya genelinde yetişmiş 6 milyon siber güvenlik uzmanına ihtiyaç duyulacağı rapor edilmektedir. 2014 yılında 1 milyon kişilik yetişmiş insan gücü açığının, 2021 yılında 3,5 milyona çıkacağı öngörülmektedir. Hiç süphesiz yetişmiş insan gücü için eğitim yatırımının yapılması da kaçınılmazdır. 2014 yılında bu kapsamda yapılan yatırımlar dünya genelinde toplam 1 milyar dolar iken, 2017 yılında bu rakam 10 milyar dolar olarak gerçekleşmiştir.

Yukarıda da belirtildiği üzere kişi, kurum ya da kuruluşların siber terör saldırılarına karşı alması gereken önlemler arasında ilgili konularda eğitilmesi ve kritik bilgilerin bulunduğu elektronik ortamların fiziki güvenliğinin sağlanması bulunmaktadır. Pahalı yatırımlarla yazılım, donanım ve emisyon güvenliği önlemlerinin alınmasına karşın, personelin dikkatsiz ve güvenlik açığı oluşturacak eylemler içerisinde olması, bilgilerin depolandığı aygıtların kolaylıkla erişilebilir mekanlarda bulunması tüm önlemlerin etkisiz kalmasına sebep olabilmektedir. Bu sebeple personelin siber terör ve saldırı faaliyetlerine karşı eğitilmesi, depolama aygıtları ve evraklarının gizlilik derecesi aşaması oranında (kimlik kartı, şifre ya da biyometrik giriş sistemine sahip kapılar, kamera ile izlenen depolama ortamları, vb.) uygun ortamlarda tutulması siber terör saldırılarının önlenmesi için hayati önem taşımaktadır [23].

Saldırının muhatabı olan bilgisayar veya ağ sisteminin (dolayısıyla kullanıcıların) bulunduğu tarafa ilişkin alınması gereken bir takım önlemler yukarıda kısaca anlatılmış olmakla beraber, saldırı kaynağının tespiti ve söz konusu durumun tekrarının önlenmesi de son derece önemlidir. Bu kapsamda devletlerin güvenlik güçlerinin Siber Suçlarla Mücadele ve Terörle Mücadele birimlerine büyük görev düşmektedir.

9.5. Değerlendirmeler

Günümüz bilgi ve teknoloji çağının getirdiği yenilikler, toplumların yaşamında varlığını hissedilir derecede arttırmaktadır. Özellikle elektronik ortamların doğasından kaynaklanan güvensizlik unsuru, bilginin güvenliğini tehdit eden en önemli etkenlerden biridir. Bu sebepledir ki, toplumları terörize eden bir takım saldırılar her geçen gün artmakta, insanoğlu bu yeni platformun güvenliğini sağlama amacıyla bir takım önlemler almaktadır. "Siber terör faaliyetlerine karşı etkin bir mücadele bilgi güvencesinin sağlanması ile gerçekleştirilebilir" ilkesinden hareketle, standartlara uygun yazılım/donanımların kullanımı, ağ, haberleşme ve emisyon güvenliğinin sağlanması, personel/kullanıcı eğitimi ve fiziki güvenliğin tesis edilmesi; şifreleme, damgalama ve gizli yazı teknikleri ile bilginin güvenli şekilde iletilmesi veya kaydedilmesi büyük önem arz etmektedir. Şüphesiz, bu önlemlerin tamamı veya bir kısmı günün koşulları ve gelişmeleri dikkate alınarak kullanılabileceği gibi, ihtiyaçlar doğrultusunda ilgili önlemlerin arttırılması da mümkündür.

Bilgisayar ve internet teknolojilerinin yeteneklerinin artmasıyla neredeyse bütün kamu kurumları her türlü iş ve işlemlerini bu ortamda yapabilir durumu gelmiştir. Bir başka ifade ile bilişim araçlarını kullanmak, kurumlar ve bireyler açısından bir zorunluluk halini almıştır. Örneğin bir siber terör saldırısı sonucu elde edilen bir verinin hukuk dışı kullanımı, değiştirilmesi veya bozulması söz konusu olduğunda yeterli incelemenin yapılamaması durumunda, ilgili suç cezasız kalacaktır. Bu sebeple gerek kamu sektöründe ve gerekse özel sektör de vuku bulan ve bulacak olan siber terör vakalarını bilimsel ve hukuki temellerde değerlendirecek en az yüksek lisans düzeyinde eğitim almış Adli Bilişim Uzmanlarının kamu kurumlarınca istihdam edilmesi büyük önem taşımaktadır. Diğer yandan kurumsal bilgi güvenliği politikalarının oluşturulması da Adli Bilişim Uzmanlarınca sağlanarak kişisel verilerin korunması ile kurumlarda bilişim suçlarının önüne geçilebilmesi için önemli bir adım atılmış olacaktır. Adli bilişim uzmanlığı sadece bilişim suçlarını, güvenlik politikalarının kurumda yerleşmesini sağlamakla kalmayacak, adli makamlarla da ortak çalışmaları neticesinde bilişim suçları konusunda bilimsel metotları kullanarak yol gösterici bir kaynak olacaktır. Güvenlik güçleri bünyesinde çalışan Siber Terör uzmanlarının sürekli güncel bilgilerle beslenmesinin sağlanması,

donanım ve yazılım gereksinimlerinin karşılanması da siber terör olaylarının önlenmesi ve takibi, sorumluların tespiti hususlarında büyük önem taşımaktadır.

Siber terör faaliyetlerinin hedefi kurumlar olmakla birlikte, bireyler de olabilmektedir. Bu kapsamda bireylerin erken yaşlardan itibaren teknoloji okur yazarlığı konusunda eğitilmeleri de çok önemlidir. Siber terör, siber güvenlik, siber saldırı, siber zorbalık gibi başlıkları da içerisinde barındıracak şekilde oluşturulacak bir içeriğin örgün ve yaygın eğitim kurumlarında verilmesi yerinde bir adım olacaktır. İlgili ders(ler)in disiplinlerarası içeriğe sahip olduğu [24, 25] gerçeğinden hareketle içerik oluşturulmalı, toplum gelecekte yaşanabilecek çok ağır siber terör saldırılarına karşı da hazırlanmalı, neler yapmaları ve hangi tür önlemler almaları gerektiğine dair bilgilendirilmelidir.

Ülkemizde ilk Ulusal Siber Terör Konferansı Ocak 2017'de yapılmıştır. (www.siberteror.org adresinden erişilebilir.) Bu konferansın başkanlığını Gazi Üniversitesi MF Bilgisayar Mühendisliği Bölümü öğretim üyesi: Prof. Dr. Şeref Sağıroğlu yapmıştır. Bu konferansta ilk kez TDK'da bulunmayan "siber terör" teriminin tanımı yapılmış ve siber terörizmle mücadelede yapılması gerekenler tartışılmış ve elde edilen bulgular bir sonuç bildirgesi hazırlanarak ilgili birimlere gönderilmiş ve web sayfasında yayımlanmıştır. Bu etkinliğin ikincisi ise 3-4 Aralık 2018 tarihinde uluslararası olarak yapılmaktadır. (Detay bilgiye www.ibigdelft.org adresinden erişilebilinir.) Bu ve buna benzer etkinlikler ülkemizde daha çok yapılmalı ve bu konu daha detaylı tartışılmalıdır.

Kaynaklar

[1] Kim, J., Park, S., Hyuni T., "An Inquiry into International Countermeasures against Cyberterrorism", The 7th International Conference on Advance Communication Technology, pp. 432-435, 2005.

[2] Lim, Y.W., Ryu, H.R., Choi, K.S., Park, C.W., Park, W.H., Kook, K.H., "A Study on Malware Detection System Model Based on Correlation Analysis using Live Response Techniques", International Conference on Information Science and Applications, pp. 1-6, 2012.

[3] Av-Test, Malware Statistics, https://www.av-test.org/en/statistics/malware, 2018.

[4] Sadeghi, A.R., "Games without Frontiers: Whither Information Security and Privacy?", IEEE Security & Privacy, vol. 14(1), pp. 3-5, 2016.

[5] Lapayese, M.J.G., "Terrorism and Its Transition to Cyberspace", IEEE European Intelligence and Security Informatics Conference, pp. 178, 2015.

[6] Morgan, S., "2017 Cybercrime Report", Cybersecurity Ventures, Herjavec Group, pp. 1-24, 2017.

[7] Weimann, G., "Terror on the Internet: The New Arena, the New Challenges", United State Institute of Peace, Washington DC, 2006.

[8] Dewan, P., Kumaragru, P., "Towards Automatic Real Time Identification of Malicious Posts on Facebook", 13th Annual Conference on Privacy, Security and Trust (PST), pp. 85-92, 2015.

[9] Zech, M. "17 Spam Scams on Facebook, Twitter", https://nltimes.nl/2014/07/22/flight-17-spam-scams-facebook-twitter/, 2014.

[10] Berghel, A., "Farewall to Air Gaps, Part 2", IEEE Computers & Magazines, vol. 48(7), pp. 59-63, 2015.

[11] Hoffman, B., "Inside Terrorism", New York: Columbia University Press, 2006.

[12] Post, J. "The Mind of Terrorist: The Psychology of Terrorism from IRA to al-Qaeda", New York: Palgrave Macmillian, 2007.

[13] Kilger, M., "Integrating Human Behavior into the Development of Future Cyberterrorism Scenarios", IEEE 10th International Conference on Availability, Reliability and Security, pp. 693-700, 2015.

[14] Silke, A., "Terrorists, Victims and Society: Psychological Perspectives on Terrorism and its Consequences (The Psychology of Cyber-terrorism)", John Wiley & Sons, 2003.

[15] Canetti, D., Gross, M.L., Waismel-Manor, I., "Binary Bullets: The Ethics of Cyberwarfare (Immune from Cyberfire?)", Oxford University Press, 2016.

[16] Cuevas ve Rennison, "The Psychology of Violence (The Psychology of Cyberviolence)", Wiley-Blackwell, 2016.

[17] Bosco, F., "The New Cybercriminals HPP: Hacker Profiling Project", SECURE 2012, Poland, 2012.

[18] DARPA: Defense Advanced Research Projects Agency, "Proposal for R&D Support of DARPA Cyber Genome Program", General

Dynamics Advanced Information Systems, Virgiia, USA, pp. 1-45, 2010.

[19] Cho, H., Lee, S., Kim, B., Shin, Y., Lee, T., "The Study of Prediction of Same Attack Group by Comparing Similarity Domain", International Conference on Information and Communication Technology Convergence (ICTC), pp. 1220-1222, 2015.

[20] Blazic, B.J., Klobucar, T., "Missing Solutions in the Fight against Cybercrime and Cyberterrorism – the New EU Research Agenda", European Intelligence and Security Informatics Conference, pp. 128-131, 2016.

[21] TÜİK, http://www.tuik.gov.tr/HbPrint.do?id=24862, 2017.

[22] Kara, M. "Türkiye'de yazılım/donanım güvenliği değerlendirme çalışmaları", TÜBİTAK-UEKAE, 2009.

[23] Yalman, Y. Yesilyurt, M., "Information Security Threats and Information Assurance", TEM Journal - Technology, Education, Management, Informatics, vol. 2(3), pp. 247–252, 2013.

[24] Kam, H.J., Katerattanakul, P., "Diversifying Cybersecurity Education: A Non-Technical Approach to Technical Studies", IEEE Frontiers on Education Conference, pp. 1-4, 2014.

[25] Page, E.J., Allen, L.A., Gray, J.P., Bateman, S.M., "Development and Description of an Interdisciplinary Course on the Science of Terrorism", IEEE 3rd Integrated STEM Education Conference, pp. 1-4, 2013.

Dünyada ve Türkiye'de Kişisel Verilerin Korunması

BÖLÜM 10

Dr. Cengiz PAŞAOĞLU
Dr. Yılmaz VURAL

DÜNYADA VE TÜRKİYE'DE KİŞİSEL VERİLERİN KORUNMASI

Bu bölümde Türkiye'de ve dünyada kişisel verilerin korunması kapsamında yapılan çalışmalar incelenmiş, kişisel verilerin korunması (KVK) konusundaki temel kavramlar anlatılmış, farklı düzenlemelerde yer alan veri korumanın temel ilkeleri vurgulanmıştır. Dünyadaki temel düzenlemeler detaylı olarak anlatılmıştır. Veri koruma yaklaşımlarının daha iyi anlaşılması için, veri koruma modelleri açıklanmıştır. Ülkemizde 2 yıldır yürürlükte olan Kişisel Verilerin Korunması Kanunu ile söz konusu kanunun getirdiği yükümlülükler ile bu kapsamda kurulmuş olan Kişisel Verileri Koruma Kurulunun yapmış olduğu çalışmalara yer verilmiştir. Avrupada yürürlüğe giren kişisel verileri koruma düzenlemeleri (GDPR) ile ülkemizdeki KVK düzenlemeleri değerlendirilmiştir.

10.1. Giriş

Kişisel veri birçok mevzuatta kimliği belirli veya belirlenebilir bir gerçek kişiyle ilgili her türlü bilgi olarak tanımlanmaktadır. Bu bağlamda kişilerin sadece adı, soyadı, doğum tarihi ve doğum yeri gibi kimliğini ortaya koyan bilgiler değil; kişinin fiziki, ailevi, ekonomik, sosyal ve sair özelliklerine ait bilgiler de kişisel veridir. Ayrıca söz konusu tanımda yer alan, "bir kişinin belirli veya belirlenebilir olması" mevcut verilerin herhangi şekilde bir gerçek kişiyle ilişkilendirilmesiyle, o kişinin tanımlanabilir hale getirilmesini ifade etmektedir [1].

Tüm dünyada yeni iletişim teknolojilerinin sunduğu imkânlar, artan internet kullanımı ve internetin yaşamımızın her alanına hızla girmesi ile kullanıcılar iletişim kurmak, sosyal ağlarda yer almak, alışveriş ve ticaret yapmak, eğlenmek gibi çok çeşitli amaçlarla interneti kullanmaya başlamışlardır. Bunun sonucunda bilginin üretimi, kullanımı, paylaşımı, yayılım ve etkileşimi çok daha kolay hale

gelmiştir [2,22]. Türkiye İstatistik Kurumu araştırmasına göre 2018 yılında Türkiye'de bilgisayar ve internet kullanımı 16-74 yaş arası bireylerde sırasıyla %59.6 ve %72.9 iken, her on hanenin sekizinde internet erişim imkânı mevcut, bireylerin %29.3'ü ise internet üzerinden alışveriş yapmaktadır [3].

Bu kapsamda hem dünyada hem de Türkiye'de artan internet kullanımı ile birlikte içinde bulunduğumuz bilgi ve iletişim çağında hemen hemen her sektörde kişisel veri işleme faaliyetleri yürütülmektedir. Bu faaliyetler kuruluşların hizmet sağladığı müşterileri ve üyeleri olan gerçek kişiler olabileceği gibi kuruluşun kendi çalışanları da olabilmektedir. Bununla birlikte bilgi ve iletişim teknolojileri ekseninde gelişen yeni iş modelleri, ürünler, hizmetler ve çeşitli teknolojiler (büyük veri, nesnelerin interneti, bulut depolama, artırılmış gerçeklik, robotik vb.) ile veri temelli ekonominin kazandığı önem de yadsınamaz boyuta gelmiştir. Söz konusu teknolojilerin temelinde veri olduğu için, her geçen gün işlenen kişisel verilerin çeşidi ve büyüklüğü de gittikçe artmakta, kişisel veri daha kıymetli bir hale gelmektedir. Dolayısıyla kişisel verilerin korunması ve sınır ötesi paylaşımına ilişkin tartışmalar buna bağlı olarak önem kazanmış, yetkisiz ve kötü niyetli olarak verilerin elde edilmesi, bilgisizlik ya da ihmalden kaynaklı veri ihlalleri, kişilerin mahremiyet alanlarının savunmasız hale gelmesi gibi nedenlerle kişisel verilerin işlenmesinin düzenlenmesi gereği ortaya çıkmıştır.

Yukarıda sayılan nedenlerle kişisel verilerin korunması hususunda özellikle 1970'lerden sonra ulusal ve uluslararası birçok düzenleme yapılmaya başlanmış, Birleşmiş Milletler (BM), Avrupa Konseyi (AK), İktisadi İşbirliği ve Kalkınma Teşkilatı (OECD) ve Avrupa Birliği (AB) nezdinde çeşitli mevzuatlar hazırlanmıştır. Günümüzde kişisel verileri koruma kanununa sahip 120'nin üzerinde ülke olduğu bilinmektedir [4].

Kişisel verilerin korunması alanındaki ulusal ve uluslararası düzenlemelerin genel olarak ortak hükümlerini;

- Kişisel verilerin korunması hakkının anayasal güvenceye kavuşturulması,
- Kişisel verilerin belirli ve temel ilkelere uygun olarak işlenmesi,
- İlgili kişilerin (verisi işlenen gerçek kişilerin) haklarının belirlenmesi,

- Verileri hukuka uygun olarak işleyeceklerin görev ve sorumluluklarının belirlenmesi,
- Kişisel verilerin korunması konusunda etkin rol alacak bağımsız, tarafsız ve teknik olarak yeterli bir veri koruma otoritesinin hayata geçirilmesi, ve
- Ceza ve yaptırımlar

oluşturmaktadır.

Bununla birlikte içinde bulunduğumuz bilgi ve iletişim çağında kişisel veriler hukuka uyumlu olarak işlendiğinde ve yönetildiğinde veri temelli ekonomi kapsamında çok önemli bir ekonomik değere dönüştürülebileceğini bilmemiz gerekmektedir. Dolayısıyla kişisel veriler korunurken aynı zamanda dünyadaki veri temelli bir ekonomide iktisadi kuruluşların rekabetçi yapısını koruyacak bir ekosistemin geliştirilmesi büyük önem taşımaktadır.

Bu bağlamda kişisel verilerin korunması hakkı, temel insan hak ve özgürlükleri arasında yer almakta olup, kişinin onur ve şahsiyetinin korunması, hukuk devleti ilkesi ve demokrasinin derinlik kazanması açısından çok önemlidir. Kişisel verilerin korunması özünde verinin kendisinin değil, verinin sahibi olan kişinin temel hak ve özgürlüklerinin, kişilik hakkının ve özel alanının korunmasını amaçlamaktadır [5,6].

Kitabın bu bölümünde öncelikle genel bir altyapı oluşturması maksadıyla kişisel verilerin korunması alanındaki temel kavramlar anlatılmış, daha sonra kişisel verilerin korunması alanında dünyada yapılan önemli düzenlemelerden bahsedilmiştir. Sonrasında ise Türkiye'de kişisel verilerin korunmasının kronolojisi çıkartılarak bu alanda yürürlüğe girmiş olan 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) anlatılmış, Türkiye'de bu hususta yapılan çalışmalar detaylı olarak ele alınmıştır.

10.2. Temel Kavramlar

Kitabın bu bölümünde gelecek bölümlerin daha iyi anlaşılabilmesi için kişisel verilerin korunması hususundaki temel ve önemli kavramlar açıklanmıştır.

10.2.1. Kişisel Veri

Kişisel veri birçok düzenlemede gerçek bir kişiyi belirleyen ya da belirlenebilir kılan bilgiler olarak kullanılmıştır. Bu anlamda kişisel veri kavramının en genel tanımıyla belirli veya kimliği belirlenebilir olmak şartıyla bir kişiye ilişkin bütün bilgileri ifade edeceği, bu bilgilerin; belirli bir kimsenin kimliği, etnik kökeni, fiziksel özellikleri, sağlık, eğitim, istihdam durumu, cinsel yaşamı, aile hayatı, başkaları ile yaptığı haberleşmeler, ikamet adresi, kredi kartı, kişisel düşünce ve inançları, dernek ve sendika üyelikleri, alışveriş alışkanlıkları gibi kişiyle ilgili, kişiyi belirlenebilir hale getiren, doğrudan ya da dolaylı olarak bir gerçek kişiyle ilişkilendirilmesi suretiyle kişiyi tanımlayabilme özelliği bulunan bilgiler olduğu söylenebilir. [6-9] Bununla birlikte yine hâlihazırdaki düzenlemelerde hassas ya da özel nitelikli veri kavramı da karşımıza çıkmaktadır. Söz konusu hassas veriler aslında kişiler arasında ayrımcılığa yol açabilecek veriler olarak düşünülmekte ve veri koruma kanunlarında hassas verilerle ilgili özel hükümler bulunmakta, bu veriler kişisel veriye göre daha sıkı bir biçimde korunmakta ve işlenme şartları kişisel veriye göre daha da kısıtlanmaktadır.

10.2.2. Kişisel Verilerin İşlenmesi

İşlemek kelime anlamıyla bir takım işlemlerden geçirmek demektir. Kişisel verilerin işlenmesi de veriler üzerinde yapılan her türlü işlemi ifade eder. Bu kapsamda kişisel verilerin elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem kişisel verilerin işlenmesi olarak kabul edilmektedir.

10.2.3. Açık Rıza

Açık rıza belirli bir konuya ilişkin, bilgilendirmeye dayanan özgür irade açıklamasıdır [1]. Buradan anlaşılacağı üzere açık rızanın üç unsuru vardır. Açık rızanın öncelikli olarak belirli bir konuya ilişkin ve o konuyla sınırlı olması gerekir. Bu çerçevede, açık rızanın genel nitelikte olmaması, belirli bir konuya ilişkin olarak kaleme alınmış ve o konu ile sınırlı olması gerekir. Açık uçlu ve genel veri işleme faaliyetlerine ilişkin rıza almak doğru olmayacaktır. Ayrıca açık rıza

bir irade beyanı olup, kişinin neye rıza gösterdiğini bilerek özgür bir şekilde onay vermesi gerekir. Cebir, tehdit, hata ve hile gibi iradeyi sakatlayan hallerde kişinin özgür bir şekilde karar vermesi mümkün değildir [7]. Açık rıza kavramı yürürlükten kalkmış bulunan AB 95/46 sayılı veri koruma direktifinde bulunmazken (sadece rıza olarak kullanılmış) yakın zamanda yürürlüğe girmiş olan GDPR'da (General Data Protection Regulation-Genel Veri Koruma Tüzüğü) bulunmakta ve benzer şekilde tanımlanmaktadır.

10.2.4. İlgili Kişi

İlgili kişi kişisel verisi işlenen gerçek kişiyi yani veri süjesini ifade eder. Burada dikkat çekilmesi gereken husus hâlihazırdaki birçok mevzuatta yalnızca yaşamakta olan gerçek kişilerin verilerinin korunması öngörülmüş, tüzel kişilerin ve vefat etmiş kişilerin verileri kanunların kapsamının dışında bırakılmıştır. İlgili kişilere anılan mevzuatlar kapsamında çeşitli haklar verilmiş ve söz konusu hakları ne şekilde kullanacakları hususunda düzenlemeler yapılmıştır.

10.2.5. Veri Sorumlusu

Veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olanlardır. Bu kişiler, gerçek kişiler olabileceği gibi, kamu kurumları, şirketler, dernekler veya vakıflar gibi tüzel kişiler de olabilirler. Veri sorumlusu kişisel verilerin işlenme amacı, işlenecek kişisel verilerin türleri, kişisel verilerin aktarılıp aktarılmayacağı, ne kadar süreyle saklanacağı gibi hususlara karar verir. Bir kurum/kuruluş ya da şirketin kendisi kişisel veri işleme konusunda gerçekleştirdiği faaliyetler kapsamında tüzel kişi veri sorumlusu olarak kabul edilirken (şirketteki herhangi bir bölüm ya da bir kişi veri sorumlusu değil), doktor, avukat gibi hastalarının ya da müvekkillerinin verisini işleyenler gerçek kişi veri sorumlusu olarak kabul edilirler.

10.2.6. Veri İşleyen

Veri işleyen, kişisel verileri veri sorumlusu adına ve onun verdiği talimatlar doğrultusunda işleyen veri sorumlusu organizasyonu dışındaki gerçek veya tüzel kişilerdir. Bu kişiler, kişisel verileri kendisine verilen talimatlar çerçevesinde işleyen, veri sorumlusunun kişi-

sel veri işleme sözleşmesi yapmak suretiyle yetkilendirdiği ayrı bir gerçek ya da tüzel kişidir. Veri işleyenin faaliyetleri veri işlemenin daha çok teknik kısımları ile sınırlıdır [8]. Örneğin bir bulut hizmet sağlayıcı veri sorumlusuyla yaptığı sözleşme kapsamında kişisel verileri anılan veri sorumlusu adına belirli bir bölgede belirli koşullarda barındırıyorsa söz konusu bulut hizmet sağlayıcı veri işleyen olmaktadır.

10.3. Dünyada Kişisel Verilerin Korunması

Uluslararası düzeyde kişisel verilerin korunması ilk olarak 1948 tarihli İnsan Hakları Evrensel Beyannamesi ve 1950 yılında imzalanan Avrupa İnsan Hakları Sözleşmesi (AİHS) ile başlamıştır [10]. Sonrasında 23 Eylül 1980 tarihinde OECD Sözleşmesi kabul edilmiş olmakla birlikte söz konusu sözleşmedeki temel ilkeler bağlayıcı olarak kabul edilmemektedir. Daha sonra Avrupa Konseyi tarafından 1981 tarihinde kişisel verilerin korunması konusundaki ilk geniş kapsamlı sözleşme olan 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi" imzalanmış ve söz konusu sözleşmeyi imzalayan ülkeler tarafından iç hukuka aktarılması yükümlülüğü getirilmiştir. 14 Aralık 1990 tarihine gelindiğinde ise BM Genel Kurulu üye devletlerin kişisel verilerin korunması konusunda asgari bir standart ortaya koyabilmeleri için "Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Denetlenmesine İlişkin Rehber İlkeleri" kabul etmiştir.

Kişisel verilerin korunması konusundaki en büyük gelişme ise 1995 yılında Avrupa Birliği tarafından hazırlanan ve 1998 yılında yürürlüğe giren 95/46/AT sayılı "Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktif" (AB Veri Koruma Direktifi) olmuştur. Söz konusu direktif ile kişisel verilerin korunması konusunda AB'ye üye tüm ülkelerde geçerli olacak temel esaslar belirlenmiş, AB veri koruma standartlarına sahip olmayan ülkelere veri aktarımı yasaklanmıştır [6,9,11]. Söz konusu direktifin yürürlük tarihinden itibaren AB ülkeleri direktifteki kişisel veri koruma standartlarını iç hukuklarına aktarmaya başlamışlardır. Daha sonra geçen süre zarfında AB ülkelerindeki veri koruma kanunlarındaki farklılıkların yarattığı sıkıntılar sebebiyle AB kapsamında yeknesak bir kanuna duyulan ihtiyaç ve teknolo-

jide yaşanan hızlı gelişmeler ile kişisel verilerin korunması hususunda daha katı önlemlerin alınması gerekliliği sonucunda Avrupa Parlamentosu'nda 25 Mayıs 2016 tarihinde bu alandaki son yirmi yılın en büyük düzenlemesi olarak görülen GDPR kabul edilmiş ve 25 Mayıs 2018 tarihinde 95/46/AT sayılı AB Veri Koruma Direktifi yürürlükten kalkarak GDPR yürürlüğe girmiştir. Tablo 10.1'de söz konusu uluslararası düzenlemelerle ilgili kronolojik gösterim mevcuttur.

Tablo 10.1. Kişisel Verilerin Korunmasıyla İlgili Uluslararası Genel Düzenlemeler

Düzenleme	**Tarih**
İnsan Hakları Evrensel Beyannamesi	1948
Avrupa İnsan Hakları Sözleşmesi	1950
OECD Rehber İlkeleri	1980
Avrupa Konseyi 108 sayılı Sözleşme	1981
BM Genel Kurulu Rehber İlkeler	1990
AB Veri Koruma Direktifi	1998
GDPR	2018

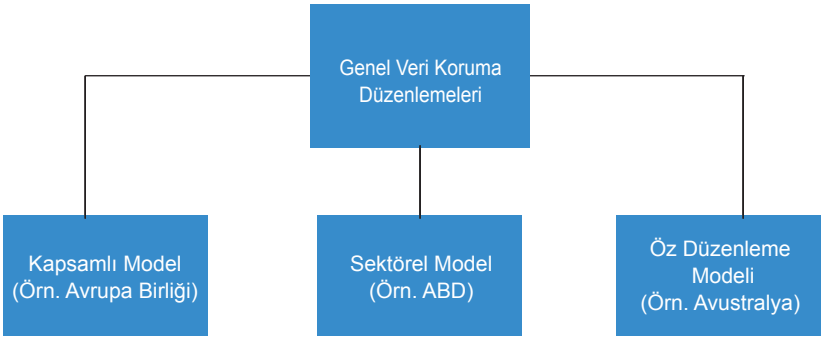
Tüm bu gelişmeler ve artan kamu ilgisinden dolayı, çok sayıda ulusal ve uluslararası çalışmalar yoluyla veri koruma ilkeleri oluşturuldu. Ülkeler bazında inceleme yapıldığında görülmektedir ki Almanya'nın Hessen Eyaleti 1970'de ilk veri koruma kanununu kabul ederken, 1970 tarihli ABD "Adil Kredi Raporlama Kanunu" da bazı veri koruma unsurlarını içeriyordu. Ayrıca ABD 1970'lerin başlarında, bugünkü veri koruma düzenlemelerini şekillendiren Adil Bilgilendirme Pratiklerini de geliştirdi. İngiltere de aynı yıllarda özel şirketlerden gelebilecek veri koruma tehditlerini gözden geçirmek ve benzer sonuçlara ulaşmak için ayrı bir komite kurdu. Kısa bir süre sonra İsveç, ABD, Almanya ve Fransa ile başlayan ulusal kanunlar ortaya çıktı [11].

1973'ten bu yana geçen 45 yıl boyunca yılda ortalama 2.7 ülkede yeni veri koruma kanunu yürürlüğe girdi ve 2017 itibariyle yaklaşık 120 kanun çıkarıldı. Söz konusu kanunların çıkarılma tarihi ve çıkarıldıkları ülkeler tablo 10.2'de sırasıyla gösterilmektedir.

Tablo 10.2. Yıllara göre Veri Koruma Kanunu çıkaran ülkeler [4]

Yıl	Sayı	Ülkeler	Yıl	Sayı	Ülkeler
1973	1	İsveç	1999	2	Arnavutluk, Şili
1974	1	ABD	2000	2	Arjantin, Letonya
1975	0	-	2001	6	CapeVerde, Çad, G.Kıbrıs, Malta, Romanya, Bosna Hersek
1976	0	-	2002	5	Ermenistan, Bulgaristan, Likteştayn, Paraguay, Zimbave
1977	1	Almanya	2003	6	Andora, Bahamalar, Hırvatistan, Estonya, Seyşel Adaları, Vincent Grenadas Adaları
1978	4	Fransa, Avusturya, Danimarka, Norveç	2004	4	Burkino Faso, Cebelitarık, Morityus, Tunus,
1979	2	Grönland, Lüksemburg	2005	2	Makedonya, Katar FC
1980	0	-	2006	2	Makao SAR, Rusya
1981	1	İsrail	2007	3	Dubai IFC, Moldova, Nepal
1982	0	-	2008	6	Kolombiya, Kırgızistan, Karadağ, Senegal, Sıbistan, Uruguay
1983	2	Kanada, San Marino,	2009	2	Benin, Fas
1984	1	İngiltere	2010	8	Bes Adaları, Kurasao Adaları, Faroe Adaları, Kosova, Malezya, Meksika, St Martin, Vietnam
1985	0	-	2011	10	Angola, Aruba, Kosta Rika, Gabon, Hindistan, Lesoto Krallığı, Peru, St Lusya, Trinadad Tobaco, Ukrayna,
1986	2	Guernsey, Man Adası	2012	6	Gürcistan, Gana, Nikaraguay, Filipinler, Singapur, Yemen
1987	2	Finlandiya, Jersey	2013	6	Antigua ve Barbuda, Fildişi Sahili, Dominik Cumhuriyeti, Kazakistan, Mali Güney Afrika
1988	3	Avustralya, İrlanda, Hollanda	2014	0	-
1989	1	İzlanda	2015	2	Abu Dabi GM, Madagaskar
1990	1	Slovenya	2016		Türkiye, Bermuda, Ekvator Ginesi, Katar, Sao Tome ve Principe, Endonezya, Malavi
1991	1	Portekiz	**Toplam**	**120**	**44 yılda ortalama=2.7**
1992	6	Belçika,Çekya,Macaristan, Slovakya, İspanya, İsviçre			
1993	2	Monako, Yeni Zelanda			
1994	1	Güney Kore			
1995	3	Honkong SAR, Tayvan, Japonya			
1996	2	İtalya, Litvanya			
1997	3	Yunanistan, Polonya, Tayland			
1998	1	Azerbaycan			

Bu kapsamda yapılan araştırmalar neticesinde dünyadaki temel veri koruma yaklaşımları genel olarak bakıldığında şekil 10.1'den görüleceği üzere üç ana başlıkta incelenebilir. Bunlar sırasıyla kapsamlı model, sektörel model ve öz düzenleme modelidir.



Şekil 10.1. Genel veri koruma düzenlemeleri

10.3.1. Kapsamlı Model

Kapsamlı model yaklaşımı, uygulanan temel bir çerçeve kanun üzerinden veri işleme faaliyetlerini ve sonuçlarını kapsamlı bir şekilde düzenlemeyi hedefleyen bir yaklaşımdır. Söz konusu veri koruma yaklaşımına örnek olarak Avrupa Birliği düzenlemesi verilebilir. Bu modelde;

- Hem kamu hem de özel sektörde kişisel verinin toplanması, kullanılması ve paylaşılmasına (işlenmesine) ilişkin kurallar öngörülür.
- Veri koruması konusunda yürürlüğe konan kanunları yürüten ve bu çerçevede denetimler yapan bağımsız veri koruma kurumlarının oluşturulması söz konusudur.
- Bu modeli seçen ülkeler genelde, geçmişteki veri koruma ihlallerinin tekrar meydana gelmemesi, AB veri koruma düzenlemeleri ile uyumluluk sağlamak ve e-ticareti desteklemek amacıyla bu modeli tercih etmektedir.

10.3.2. Sektörel Model

Sektörel model yaklaşımı, kişisel verilerin korunması konusunda ilgili sektör özelinde uygulama kabiliyeti olan ve sektörün ihtiyaçlarına uygun ayrı düzenlemeler geliştirme esasına dayalı bir yakla-

şımdır. Bu modele örnek olarak ABD düzenlemeleri verilebilir. Bu modelde;

- Her bir sektör içerisinde farklı bir uyuşmazlık ve bunun çözümü için farklı bir düzenleme gerekeceğinden hareketle sektör bazında veri koruma düzenlemeleri oluşturulmaktadır.
- Veri koruması konusundaki maddelerin yürütülmesi, ilgili maddelerin yer aldığı mevzuatı yürütme konusunda yetkili kurum veya duruma göre Federal Ticaret Komisyonu (FTC) tarafından gerçekleştirilmektedir.

Bu modelin kullanımına örnek olarak gösterilen Amerika Birleşik Devletlerinde 20 ayrı sektöre ya da ortama özgü ulusal mahremiyet veya veri güvenliği yasaları vardır. Bununla birlikte 50 eyaleti ve toprakları arasında da benzer yüzlerce düzenleme vardır. (Sadece Kaliforniya Eyaleti'nde bile eyalete özel 25'ten fazla mahremiyet ve veri güvenliği düzenlemesi vardır). Buna ek olarak şirketler, adil olmayan veya aldatıcı ticaret uygulamaları yaparlarsa FTC tarafından regüle edilen uygulamalara da tabidirler. FTC, bu yetkisini, asgari düzeyde veri güvenliği önlemleri uygulamayan, gizlilik politikalarındaki vaatleri yerine getirmeyen veya kişisel verilerin işlenmesi veya ifşası ile ilgili kişilerin tercihlerini aksatan şirketleri takip etmek için de kullanmaktadır [13].

10.3.3. Öz Düzenleme Modeli

Bu model, kişisel verilerin korunması düzenlemeleriyle ilgili otoritenin çıkardığı düzenlemenin uygulanacağı ilgili sektörün temsilcisi olan kuruma da düzenleme ile yetki verilerek onun da kendi sektörünü öz denetim kuralları ile düzenlemesi/denetlemesi esasına dayanmaktadır. Bu modelle genel veri koruması yaklaşımı kapsamlı model çerçevesi içerisinde belirlenmekte; sektörel detaylar ve uygulamalar o sektörün temsilcisi olan kuruma bırakılarak bu yönüyle sektörel düzenleme modelinin kazanımları elde edilmeye çalışılmaktadır. Bu modele Avustralya'daki düzenlemeler örnek olarak verilebilir. Bu modelde ise;

- Veri koruma konusundaki esasları uygulayan veri koruması kurumu bulunmaktadır. Genel çerçevenin yanında bu çerçevenin uygulandığı sektörün, kendi sektörünün dinamiklerine göre uygulanabilir kurallar oluşturması beklenmektedir.

- Öz düzenleme modelinde aynı zamanda kişisel verinin şirket veya sektör tarafından korunması için uygulama kurallarının şirket ve sektör meclisleri eliyle oluşturulması öngörülmektedir.
- Veri koruması konusunda ilkeleri değiştiren yeni teknolojilerin yarattığı etkilere ve hukuksal değişimlere uyum sağlama konusunda daha etkin bir modeldir.
- Öz düzenleme çerçevesinin yeterli düzeyde koruma sağlayamayacağı ve tüketicinin menfaatini koruyamayacağı endişesi de söz konusudur.

Bu modelin kullanımına örnek olarak gösterilen Avustralya'da veri koruması hâlihazırda Federal ve Eyalet/Bölge mevzuatının birleşiminden oluşmaktadır. Federal Mahremiyet Kanunu 1988 (Cth) ve içerisindeki Avustralya Mahremiyet İlkeleri (APP), yıllık en az 3 milyon Avustralya doları cirosu olan özel sektör kuruluşlarına ve tüm Commonwealth Hükümeti ve Avustralya Başkent Bölgesi devlet kurumlarına uygulanmaktadır.

Mahremiyet Komiseri, mahremiyet kanunu kapsamında soruşturma yürütmek, söz konusu kanuna uyulmasını sağlamak ve ciddi / aleni bir ihlal durumunda veya otorite tarafından bir şirkete herhangi bir düzeltme uyarısı verildiği halde düzeltmelerin gerçekleştirilmediği durumlarda ceza kesmek gibi yetkilere sahiptir.

Avustralya Eyaletleri ve Bölgelerinden her birinin (Batı Avustralya ve Güney Avustralya hariç) kendi yasal düzenlemeleri vardır. Bunlar:

- Bilgi Mahremiyeti Yasası 2014 (Avustralya Başkent Bölgesi)
- 2002 Bilgi Edinme Yasası (Kuzey Bölge)
- Mahremiyet ve Kişisel Bilgi Koruma Yasası 1998 (Yeni Güney Galler)
- Bilgi Mahremiyeti Yasası 2009 (Queensland)
- Kişisel Bilgi Koruma Yasası 2004 (Tasmania)
- Mahremiyet ve Veri Koruma Yasası 2014 (Victoria) [13].

Bununla birlikte dünyadaki ülkelerin yaklaşık %30'unda kişisel verilerin korunması konusunda herhangi bir düzenleme bulunmamaktadır [4,13]. Bu ülkelerde kişisel veri bir hukuksal koruma objesi olarak değil özel hayatın gizliliğinin bir parçası ve/veya neti-

cesi olarak korunmaya çalışılmaktadır. Buna örnek olarak Çin Halk Cumhuriyeti verilebilir.

Günümüzde Çin Halk Cumhuriyeti'nde kapsamlı bir veri koruma yasası bulunmamaktadır. Bunun yerine, kişisel verilerin korunması ile ilgili kurallar çeşitli yasa ve yönetmeliklerde bulunur. Genel anlamda, Medeni Kanunlar ve Asliye Yükümlülük Yasası Genel İlkeleri gibi yasalarda bulunan hükümler, veri koruma haklarını bir itibar veya gizlilik hakkı olarak yorumlamak için kullanılabilir. Ancak, böyle bir yorum da net ve açık değildir. Bununla birlikte, 2017 yılında Ulusal Halk Kongresi Daimi Komitesi tarafından kabul edilen Çin Halk Cumhuriyeti Siber Güvenlik Kanunu (1 Haziran 2017'den itibaren yürürlüğe girmiştir) siber güvenlik ve veri gizliliği korumasını ele alan ilk ulusal düzey yasa haline gelmiştir [13].

Şekil 10.2'de Ocak 2018 itibariyle dünyadaki genel veri koruma kanunlarının ülkeler bazındaki durumu gösterilmektedir.



Şekil 10.2. Dünyada veri koruması düzenlemeleri [14]

Diğer taraftan kişisel verilerin korunması ile ilgili uluslararası kuruluşlarca alınan kararlar ve yapılan düzenlemeler aşağıda kısaca anlatılmaktadır.

10.3.4. Birleşmiş Milletler Kararları

Birleşmiş Milletler ikinci dünya savaşı sonrasında uluslararası barışın devamı ve güvenliğin sağlanması, sürdürülebilir kalkınmanın desteklenmesi ve insan haklarının güvence altına alınması amacıyla

Türkiye dahil 51 ülke tarafından 24 Ekim 1945 tarihinde kurulmuştur. Hâlihazırda 192 üyesi olan bir örgüttür.

Birleşmiş Milletler İnsan Hakları Evrensel Bildirisi, Birleşmiş Milletler Genel Kurulu'nun 10 Aralık 1948 tarih ve 217 A(III) sayılı kararıyla kabul edilmiştir. Hukuki açıdan bağlayıcı bir nitelik taşımasa da uluslararası düzeyde birtakım ideallere hizmet etmesi dolayısı ile uluslararası arenada siyasi ve moral açıdan etkiye sahiptir [15]. Bildirinin 12. Maddesi ile özel hayatın gizliliği düzenlenmektedir ve söz konusu hüküm şu şekildedir:

> "*Hiç kimsenin, özel yaşamına, ailesine, konutuna ya da haberleşmesine keyfi olarak müdahale edilemez, şeref ve adına saldırılamaz. Herkesin, bu gibi karışma ve saldırılara karşı yasa ile korunma hakkı vardır*" [16].

Bununla birlikte BM Genel Kurulu'nun 19 Aralık 1966 tarihli ve 2200 A (XXI) sayılı kararıyla kişisel ve siyasi haklar sözleşmesi kabul edilmiştir. Söz konusu sözleşmenin 17. Maddesi olan mahremiyet hakkı aşağıdaki şekildedir:

> "*Hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemez; onuru veya itibarı hukuka aykırı saldırılara maruz bırakılamaz. Herkes bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahiptir*" [16].

Daha sonra BM, kişisel verilerin korunmasına ilişkin belli bir standart çalışmayı ortaya koymak maksadıyla 14 Aralık 1990 tarihinde 45/95 sayılı "Bilgisayara Geçirilmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeler" isminde kılavuz bir belge yayınlamıştır. On maddeden oluşan ve üye devletlerin kişisel verilerin korunması alanında asgari bir standarda kavuşmasını amaçlayan anılan ilkelerin uygulanması üye ülkelerin inisiyatifine bırakılmıştır. Söz konusu rehber ilkelerde yer alan temel esaslar aşağıdaki gibidir:

- Hukuka uygunluk ve dürüstlük,
- Doğruluk,
- Belirli ve meşru amaç,
- İlgili kişilerin verilere erişim hakkı,
- Ayrımcılıktan kaçınma,

- İstisna getirebilme,
- Güvenlik önlemleri,
- Denetim ve yaptırım,
- Sınır ötesi veri transferi,
- Uygulama alanı.

BM'nin Rehber İlkeleri, kişisel verilerin korunmasına ilişkin ilkelerin uygulamasını denetleyecek yetkili ve bağımsız bir veri koruma organının kurulmasını öngören ilk uluslararası hukuk belgesidir. Ancak bu öncü rolüne karşın metnin, Avrupa Konseyi Sözleşmesi ve OECD İlkelerine göre çok daha sınırlı bir etkisi olmuştur. Bu durumun nedenlerinden biri olarak ilkelerin hukuksal açıdan bağlayıcı olmaması, yalnızca tavsiye niteliğinde bulunması düşünülebilir [15].

10.3.5. OECD Rehber İlkeler

OECD, 14 Aralık 1960 tarihinde imzalanan Paris Sözleşmesi'ne dayanılarak kurulmuş 35 üyesi olan bir kuruluştur. OECD'nin amacı, dünyanın dört bir yanındaki insanların ekonomik ve sosyal refahını arttıracak politikaları geliştirmek ve hükümetlerin benzer sorunlara ortak çözüm bulabilmek için, deneyimlerini paylaşabileceği bir ortam sağlamaktır [17].

OECD bünyesinde kişisel verilerin korunması ile ilgili olarak yürütülen çalışmalar neticesinde 23 Eylül 1980 tarihinde uluslararası bir temel teşkil eden ve bağlayıcı olmayan, "Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler" kabul edilmiştir.

1980 yılında yayınlanmış olan söz konusu rehber ilkelerdeki ikinci bölüm "Ulusal Uygulama Temel İlkeleri" başlığıdır ve bazı temel ilkelerden oluşmaktadır. Bu bölümde yer alan ilkeler, kişisel veri işleme faaliyetlerinde dikkate alınması gereken temel hususları ortaya koymuş ve sonraki düzenlemelere de örnek olmuştur. Anılan ilkeler aşağıdaki gibidir:

- Sınırlı Veri Toplama İlkesi.
- Veri Kalitesi (doğru, tam ve güncel veri) İlkesi.
- Amaca Özgülük İlkesi.
- Sınırlı Kullanım İlkesi.

- Yeterli Güvenlik Önlemlerin Alınması İlkesi.
- Açıklık (Aleniyet) İlkesi.
- İlgili Kişinin Hakları İlkesi.
- Hesap Verebilirlik İlkesi.

10.3.6. Avrupa Konseyi 108 Sayılı Sözleşme

AK, II. Dünya Savaşı sonrasında Avrupa'da meydana gelen bölünmüşlüğün ve savaşın ortaya çıkardığı çatışma atmosferinin yok edilerek barışın tesis edilmesi amacıyla başlatılan çalışmaların neticesinde 5 Mayıs 1949 tarihinde kurulmuştur. Konsey Türkiye'nin de üyelerinin arasında yer aldığı hükümetler arası bir örgüttür.

Kişisel verilerin korunması bağlamında AK tarafından yapılan en önemli çalışma 28 Ocak 1981 tarihinde Strasburg'ta imzaya açılan 108 Sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'dir. Sözleşme 1 Ekim 1985 tarihinde yürürlüğe girmiş ve Türkiye 28 Ocak 1981 tarihinde sözleşmeyi ilk imzalayan ülkelerden birisi olmasına rağmen ancak 17 Mart 2016 tarihinde iç hukuka aktarabilmiştir. Bu sözleşmenim önemi, kişisel verilerin korunması konusunda hukuksal bağlayıcılığı olan ilk uluslararası belge olmasıdır, sözleşme AK üyesi olmayan devletlerin de imzasına açılmış ve taraf olmalarına imkân sağlanmıştır.

Sözleşmenin amacı, her üye ülkede, uyruğu veya ikametgâhı ne olursa olsun gerçek kişilerin temel hak ve özgürlüklerini ve özellikle kendilerini ilgilendiren bilgilerinin otomatik işleme tabi tutulması karşısında özel yaşam haklarını güvence altına almaktır.

AK Sözleşmesi'nin koruma kapsamında hem kamusal hem de özel sektör tarafından işlenen veriler bulunmaktadır. Bununla birlikte yalnızca otomatik yolla işlenen veriler için güvence öngörüldüğünden, elle işlenen veriler kapsam dışında kalmaktadır. Ancak bunu mutlak bir dışlama olarak düşünmemek gerekir. Nitekim Sözleşmeye göre "otomatik işleme" den söz edebilmek için sürecin tamamının otomatik olması gerekmemektedir. Kısmen otomatik işlenen veriler de güvenceden yararlanmaktadır. Bu, sözleşmenin uygulama alanını oldukça genişletmektedir.

Söz konusu sözleşmeye ek olarak 08 Kasım 2001 tarihinde 181 sayılı ek protokol imzaya açılarak kabul edilmiştir. Bu protokolün temel

içeriğini kişisel verilerin korunması alanında denetim ve düzenlemeleri sağlayacak ülkeler nezdinde bağımsız denetleyici makamların kurulması ve görevlerinin belirlenmesi oluşturmaktadır. Ayrıca Avrupa Birliği'nde GDPR'ın kabul edilmesi ile birlikte Avrupa Konseyi tarafından yeni bir ek protokol (108+) daha hazırlanmış ve 18 Mayıs 2018 tarihinde Avrupa Konseyi Bakanlar komitesi tarafından kabul edilmiştir [18]

10.3.7. Avrupa Birliği (AB) Düzenlemeleri

AB'nin bugünkü yapısına kavuşmasını sağlayan süreç,18 Nisan 1951'da 6 ülkenin (Almanya, Fransa, İtalya, Belçika, Hollanda ve Lüksemburg) Paris Antlaşması'nı imzalamasıdır. Daha sonra Avrupa Kömür Çelik Topluluğu'nun (AKÇT) kurulması ile süreç ivme kazanmıştır. 7 Şubat 1992 tarihinde imzalanan Maastricht Anlaşması ile de AB'nin bugünkü yapısının temelleri atılmıştır.

AB, yasama, yürütme ve yargı erkleriyle tam olarak bir devlet yapılanmasına sahip olmamakla birlikte, diğer ulus üstü örgütlere kıyasla, üye devletlerce topluluklara daha geniş yetkiler devredilmiştir. Bu kapsamda, AB'ye dahil olan ülkeler, anayasalarında gerekli düzenlemeler yaparak Topluluk organlarına yetki devri yapmışlardır [15].

Avrupa Birliği'nde kişisel verilerin korunmasına ilişkin 1990'lı yıllarda başlayan çalışmalar neticesinde 1995 yılında Avrupa Parlamentosu ve Avrupa Konseyi AB Veri Koruma Direktifi'ni kabul etmiştir. Söz konusu direktif kişisel verilerin korunması alanında Avrupa ile sınırlı kalmayan ve tüm dünyada kabul gören bir yaklaşım sunmuş, doğrudan hukuki bağlayıcılığı olmaması nedeni ile birlik üyesi her ülke tarafından kendi yerel mevzuatlarını yaratmalarında referans olarak kullanılmıştır. Türkiye'deki 6698 sayılı Kişisel Verilerin Korunması Kanunu da aynı şekilde anılan direktif esas alınarak hazırlanmıştır.

Diğer taraftan günümüzdeki teknolojik gelişmelerin yarattığı etkiyle veri trafiğinin çeşitliliği ve kapasitesi artmış ve veri işlemedeki yeni teknolojik gelişmeler sonucu benimsenen ilkelerin günümüze uyarlanmasına yönelik kapsamlı bir reforma gidilmesi ihtiyacı hasıl olmuştur. Bununla birlikte üye ülkelerin, söz konusu direktifi temel alsa da farklı kanunlarının olması farklı uygulama sonuçları do-

ğurmuş (örneğin bazı ülkede veri ihlallerine hapis cezası verilirken bazı ülkelerde idari para cezası öngörülmüştür) ve tüm AB'yi kapsayacak yeknesak bir kanuna duyulan ihtiyaç gündeme gelmiştir. Bu gelişmeler sonucunda AB, kişisel verilerin korunması alanında ortaya çıkan söz konusu ihtiyaçları karşılamak üzere 2012 yılında yeni bir tüzük çalışması başlatmış, Avrupa Parlamentosu, Avrupa Konseyi ve Avrupa Komisyonu tarafından yapılan çalışmalar neticesinde Genel Veri Koruma Tüzüğü hazırlanmış ve söz konusu tüzük 2016 yılında kabul edilmiş ve 25 Mayıs 2018 tarihinde 95/46 sayılı AB Veri Koruma Direktif'i ilga edilerek tüzük uygulanmaya başlamıştır. Bu kapsamda GDPR'ın direktiften farklı olarak getirdiği birçok yeniliğin mevcut olduğu görülmektedir. Söz konusu yenilikler temel olarak aşağıda belirtilmiştir:

- GDPR'ın uygulanabilirlik kapsamı genişletildi ve daha geniş yetki alanı getirildi. Bu bağlamda AB'de yerleşik olmayan fakat AB'de yaşayan kişilere mal ve hizmet sunan kuruluşlar da GDPR kapsamına alındı.
- Veri işlenmesi için alınacak onay ve açık rızanın şartları ağırlaştırıldı. Onay talebinin veri işleme sebebini içermesi ile verilecek onayın işleme faaliyetlerine özel olması gerekliliği getirildi.
- Veri işlenmesi sırasında göz önünde tutulacak hesap verilebilirlik, şeffaflık ve tasarım aşamasında mahremiyetin göz önünde bulundurulması, veri koruma sorumlusu atanması, ihlal bildirimi gibi yeni ilkeler ve sorumluluklar getirildi.
- Veri sahiplerine unutulma hakkı, veri taşınabilirliği ve veri sınırlandırılması gibi yeni haklar tanındı.
- Veri korumasına ilişkin cezalar ağırlaştırıldı. Veri sorumlularına 20 milyon Avroya kadar para cezası veya şirketin bir önceki mali yılına ait dünya genelindeki cirosunun %4'üne kadar para cezası verilmesi imkanı getirildi.
- Yurt dışına yapılacak veri transferleri için şartlar ağırlaştırıldı ve yeni uygulamalar getirildi.

10.4. Türkiye'de Kişisel Verilerin Korunması

Gerek kamu, gerekse özel kurum ve kuruluşlar, bir görevin yerine getirilmesi veya bir hizmetin sunumuyla bağlantılı olarak, kişisel

veri niteliğindeki bilgileri, öteden beri toplamaktadırlar [21]. Bu durum, bazen kanunlardan kaynaklanmakta bazen kişilerin rızasına veya bir sözleşmeye dayanmakta bazen de yapılan işlemin niteliğine bağlı olarak ortaya çıkmaktadır.

Sosyal ve ekonomik hayatın düzen içinde sürdürülmesi, kamu hizmetlerinin etkin biçimde sunumu, mal ve hizmetlerin ekonomi hayatının gereklerine uygun biçimde geliştirilmesi, dağıtımı ve pazarlanması için kişisel verilerin toplanması kaçınılmazdır. Bu bilgilerin sadece ilgili ve yetkili kişi veya kurumlarca muhafazası ile amaca uygun kullanımı da mutlak bir sosyal ihtiyaçtır.

Avrupa'da birçok devletin mevzuatında kişisel verilerin korunması ile ilgili kanunlar kırk yıldan fazladır yer almaktadır. Çağdaş devletlerin neredeyse tamamı, bu konuda temel kanunlar çıkarmıştır. Henüz bu konuda bir düzenleme yapmamış devletlerin üzerinde ise bazı sebeplerle kişisel verilerin ulusal mevzuatta yer alan temel kanunlarla korunması yönünde artan bir baskı olduğu söylenebilir. Bu yöndeki eğilimin ilk sebebi, daha önce otoriter rejimlerin bulunduğu ülkelerde tekrar bu deneyimlerin yaşanmaması için bireysel temel hak ve özgürlüklerin korunmasına önem verilmesidir. Bir diğer sebep, elektronik ticaret başta olmak üzere teknolojiyle gelişen ticaretin önündeki engelleri kaldırma isteğidir. Üçüncü sebep ise, yürürlükten kalkan AB Veri Koruma Direktifi'nin ve günümüzde de GDPR'ın kişisel verilerin yeterli koruma sağlamayan ülkelere transferini yasaklaması sebebiyle Avrupa ülkeleriyle ticaret yapmak isteyen ülkelerin mevzuatlarında gerekli değişiklikleri yapmasıdır [6,11].

10.4.1. Kanun Yapım Çalışmaları

Yukarıda bahsedilen sebeplerle Türkiye'nin gerek Avrupa Konseyi 108 sayılı sözleşmeyi ilk imzalayan ülkelerden biri olması ve iç hukuka aktarma gerekliliği, gerekse Avrupa Birliği müzakereleri kapsamındaki çalışmalarda ve ilerleme raporlarında Kişisel Verilerin Korunması alanında temel ve çerçeve bir kanuna olan ihtiyacın sürekli vurgulanması neticesinde söz konusu kanun yapım çalışmaları 1989 yılında bir komisyon kurularak başlamıştır. Komisyon çeşitli taslaklar hazırlamış ancak çalışmalarını sonuçlandıramadan dağılmıştır. Ardından 2004 yılında yeni bir komisyon oluşturularak tasarı hazırlık çalışmalarına devam edilmiş, hazırlanan tasarı 2006 yılında Başbakanlığa oradan da 2008 yılında Türkiye Büyük

Millet Meclisi'ne (TBMM) sevk edilmiştir. Ancak araya seçimlerin girmesi nedeniyle tasarı yasalaşamamış ve hükümsüz sayılarak Başbakanlığa iade edilmiştir. Daha sonra 2012 ve 2014 yıllarında Adalet Bakanlığı bünyesinde yeni bir çalışma grubu kurulmuş, önceki tasarı yapılan öneri ve eleştiriler bünyesinde yeniden ele alınmış ve TBMM'ye sunulmuşsa da araya seçimler girmesi sebebiyle hükümsüz sayılmış ve yasalaşamamıştır. Sonrasında tekrar kanun yapım süreçleri çalıştırılmış ve yeni bir tasarı hazırlanmış, söz konusu tasarı 9 Şubat 2016 tarihinde TBMM Adalet Komisyonu'nda, 24 Mart 2016 tarihinde TBMM Genel Kurulu'nda görüşülerek kabul edilmiş ve 6698 sayılı Kişisel Verilerin Korunması Kanunu 7 Nisan 2016 tarihinde Resmi Gazete 'de yayımlanarak yürürlüğe girmiştir.

Söz konusu Kanundan önce de Türk Medeni Kanunu, Türk Borçlar Kanunu, Türk Ceza Kanunu, Türk Ticaret Kanunu ve İş Kanunu gibi temel kanunlar yanında çeşitli mevzuatlarda kişisel verilere koruma sağlayan çeşitli düzenlemeler bulunmaktaydı, ancak anılan mevzuat kişisel verinin ne olduğu gibi temel ve önemli kavramlar ile kişisel verilerin hukuka uygun olarak nasıl işlenmesi gerektiği, veriler işlenirken hangi temel ilkelere uyulması gerektiği gibi sistemin işleyişini sağlayacak temel hususlarda herhangi bir hüküm içermiyordu, dolayısıyla da bu durum sistemin işleyişine engel oluşturmaktaydı.

10.4.2. Anayasal Hak Olarak Kişisel Verilerin Korunması

Türkiye Cumhuriyeti Anayasası'nın ikinci kısmında kişinin temel hak ve ödevleri düzenlenmektedir. Özel hayatın gizliliği de kişinin temel haklarından biridir. Bu hak Anayasa'nın 20. Maddesi ile güvence altına alınmıştır. Teknolojik gelişmelerin temel hak ve hürriyetlere müdahale edebilmeyi kolay hale getirmiş olması ve bu durumun hukuki bir sorun olarak kendinin göstermesi bu konuda yasal düzenlemeler yapmayı gerekli kılmıştır [8].

Bu kapsamda 2010 yılında yapılan referandumdan sonra 5982 sayılı Kanunla Anayasa'nın özel hayatın gizliliğini düzenleyen 20. maddesine "*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas*

ve usuller kanunla düzenlenir" şeklinde bir fıkra eklenerek kişilerin kişisel verilerinin korunması açıkça anayasal güvence altına alınmıştır [8,9,19].

Söz konusu Anayasa değişikliği ile kişisel verilerin korunmasını isteme hakkı Türkiye'de anayasal bir hak haline getirilmiş ve anayasa ile güvence altına alınmıştır. Anılan maddenin sonunda kişisel verilerin nasıl korunacağına ilişkin usul ve esasların bir kanunla düzenleneceği ifade edilmiş ve bu hususta kişisel verilerin korunması kanunu yapımı çalışmaları hızlanmıştır.

10.4.3. 6698 Sayılı Kişisel Verilerin Korunması Kanunu

Türkiye'de 7 Nisan 2016 tarihinde yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu kişisel verilerin korunması konusunda temel ve çerçeve bir kanundur. Söz konusu kanun Türkiye'de kişisel verilerin nasıl işleneceği ve bu kapsamda hangi temel ilkelere uyulacağı, kişisel verilerin yurt içi ve yurt dışına hangi koşullarda aktarılacağı, işlenmesini gerektiren sebepler ortadan kalktığında kişisel verilerin silinmesi, yok edilmesi ya da anonim hale getirilmesi gibi hususları düzenleyen bir kanundur.

Kanunla, kişisel verilerin işlenmesi disiplin altına alınarak sınırsız biçimde ve gelişigüzel toplanması, yetkisiz kişilerin erişimine açılması, ifşası veya amaç dışı ya da kötüye kullanımı sonucu kişilik haklarının ihlal edilmesinin önüne geçilmesi amaçlanmaktadır. Bu amaçla, kişisel verilerin işlenmesine ilişkin denetim mekanizmaları oluşturularak, kişisel verilerin hukuka aykırı olarak işlenmesinin engellenmesi hedeflenmektedir.

Diğer taraftan Kanunda belirlenen ilkelere gerçek ve tüzel kişilerin uyumunu denetlemek, bu konuda yapılacak şikâyetler hakkında karar vermek, veri sorumluları sicilini tutmak ve konuyla ilgili düzenleyici işlemler yapmak üzere Kişisel Verileri Koruma Kurumu kurulmuştur. Kurumun karar organı Kişisel Verileri Koruma Kuruludur. Kurul dokuz üyeden oluşmaktadır ve 12 Ocak 2017 tarihinde Yargıtay Birinci Başkanlık Divanı'nda yemin ederek görevine başlamıştır.

Kanunun genel ilkeleri denilen ve veri işlemenin aslında temelini oluşturan ilkeler yukarıda bahsedilen uluslararası düzenlemelerle de uyumludur. Söz konusu ilkeler;

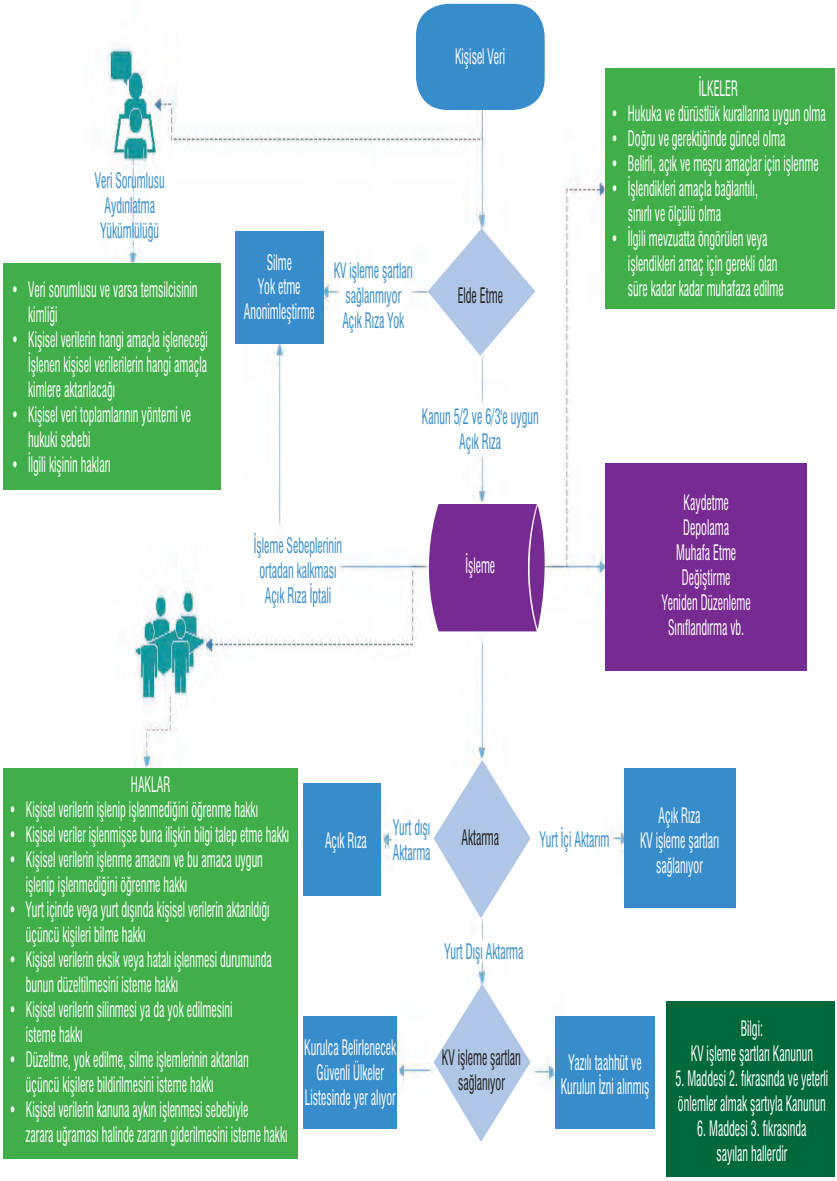
- Hukuka ve dürüstlük kurallarına uygun olma,
- Doğru ve gerektiğinde güncel olma,
- Belirli, açık ve meşru amaçlar için işlenme,
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,
- İlgili mevzuatta ön görülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme,

şeklindedir [1]. Bu ilkelerin veri işlemenin her aşamasında göz önünde bulundurulması gerekir.

Kanunla ayrıca kişisel verilerin ve özel nitelikli kişisel verilerin işlenme şartları, söz konusu verilerin yurt içi/yurt dışı aktarılma koşulları, veri sorumlusunun yükümlülükleri ve ilgili kişilerin hakları da düzenlenmiştir. Şekil 10.3'te kişisel verilerin işlenmesi ve aktarımı ile ilgili akış diyagramı gösterilmektedir. Şekil 10.3'e göre kişisel veriler elde edildiğinde öncelikli olarak kişisel verilerin işlenme şartlarından herhangi biri sağlanmıyorsa (Kanunun 5. Maddesi 2. Fıkrası ya da 6. Maddesi 3. Fıkrası) veya ilgili kişinin verilerinin işlemesiyle ilgili açık rızası yoksa söz konusu verilerin silinmesi, yok edilmesi ya da anonim hale getirilmesi (imha edilmesi) gerekir. Eğer bu şartlar sağlanıyorsa işleme faaliyet gerçekleştirilebilir ama bu kapsamda temel ilkelerin her zaman göz önünde bulundurulması ve ilgili kişilerin de işleme faaliyetlerine başlanmadan önce mutlaka aydınlatılması (Kanunun 10. Maddesi) gerekir. İşleme sebepleri ortadan kalktığında ya da ilgili kişi açık rızasını geri aldığında verilerin imha edilmesi gerekir. Diğer taraftan kişisel veriler işlenirken ilgili kişilerden gelecek kişisel verilerinin durumu ile ilgili sorulara da cevap vermek gerekeceğinin göz önünde bulundurulması gerekir.

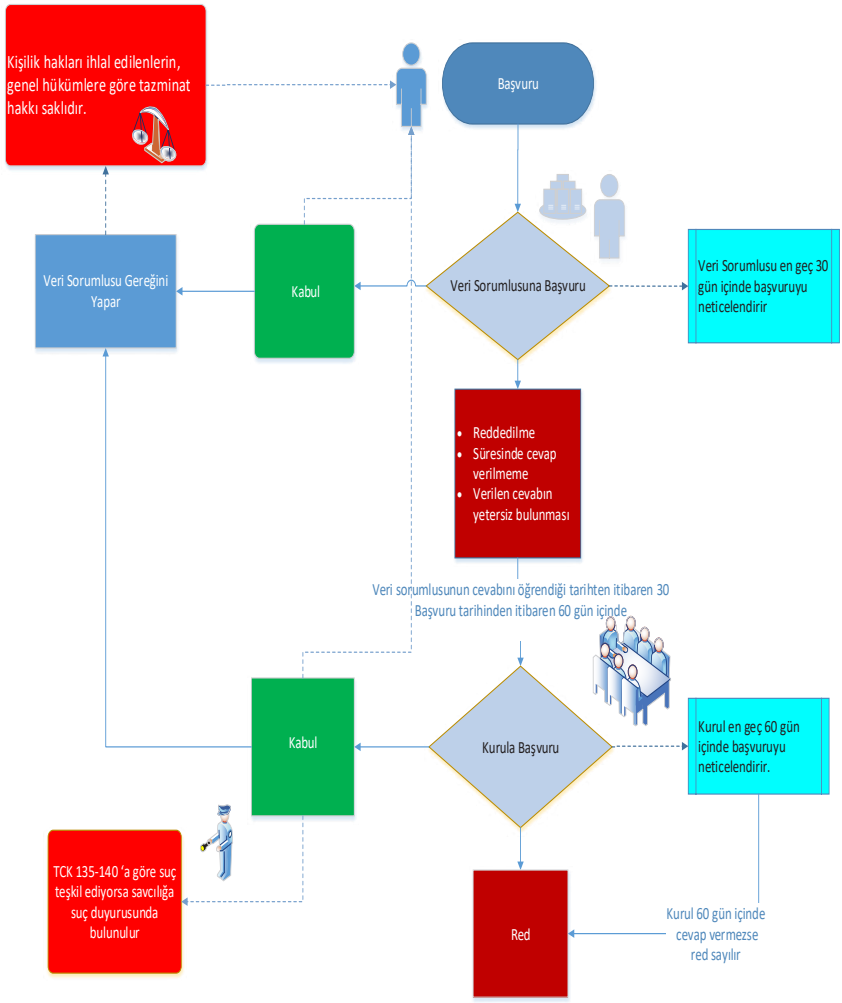
Kişisel verilerin aktarılması ise yurt içi ve yurt dışı aktarım olarak iki başlıkta ele alınmıştır. İlgili kişinin açık rızası varsa ya da kişisel verilerin işlenme şartlarından herhangi biri sağlanıyorsa kişisel veriler yurt içinde üçüncü kişilere aktarılabilir. Bu kapsamda bir şirketin departmanları arasındaki aktarım üçüncü kişilere aktarım olarak kabul edilmemektedir. Yurt dışı aktarım için ise iki farklı durum söz konusudur. İlk olarak ilgili kişinin açık rızası varsa veriler aktarılabilir, ikinci durumda ise kişisel verilerin işlenme şartlarından herhangi biri sağlanıyorsa Kişisel Verileri Koruma Kurulu (Kurul) tarafından yayımlanan güvenli ülke listesine bakılması gerekir.

Eğer aktarım yapılacak ülke söz konusu güvenli ülke listesinde yer alıyorsa aktarım yapılabilir, güvenli ülke listesinde yer almıyorsa yazılı taahhüt ile Kurula başvuru yapılması ve Kurulun izninin alınması ile aktarım yapılabilir.



Şekil 10.3. Kişisel verilerin işlenmesi

Ayrıca Kanun'da ilgili kişilerin kişisel verileriyle ilgili hakları düzenlenmiştir. Bu kapsamda hem bilgi almak hem de haklarının ihlal edildiğini düşünmeleri halinde veri sorumlusuna başvuru ve Kurula şikâyet hakları kanunun 11. Maddesi ile düzenlenmiştir. Söz konusu maddeye göre aslında bir prosedür oluşturulduğu görülmektedir. Buna göre ilgili kişiler, kişisel verileriyle ilgili öncelikle veri sorumlusuna başvuru yapacaklar, daha sonra veri sorumlusundan gelecek cevaba göre de Kurula şikâyette bulunabileceklerdir. Şekil 10.4'te söz konusu prosedür görsel olarak gösterilmiştir.



Şekil 10.4. Veri sorumlusuna başvuru ve Kurula şikayet prosedürü

Bunlarla birlikte Kişisel Verileri Koruma Kurumu çalışmaya başladığı günden bu yana Türkiye'de kişisel verilerin korunması alanından ikincil düzenlemeleri gerçekleştirmiş, bu kapsamda altı adet yönetmelik, iki adet tebliğ ve dört adet ilke kararı yayımlamıştır. Bununla birlikte uygulamada açıklık sağlanması ve söz konusu alanın Türkiye için yeni olması sebebiyle sektörleri yönlendirebilmek için beş adet rehber kitap yayımlamıştır. Söz konusu kararlar ve rehberler Tablo 10.4'te detaylı olarak gösterilmektedir.

Tablo 10.4. Türkiye'de Kişisel Verilerin Korunması alanında çıkarılan ikincil mevzuatlar ve yayınlar [20]

Yönetmelikler	Tebliğler	Kararlar	Rehberler
Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik	Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ	Banko, Gişe, Masa gibi Hizmet Alanlarında Kişisel Verilerin Korunmasına Yönelik Karar	Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular
Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik	Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ	Rehberlik Hizmeti Veren İnternet Sitelerinde/ Uygulamalarda Kişisel Verilerin Korunmasına Yönelik Karar	Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi
Veri Sorumluları Sicili Hakkında Yönetmelik		"Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kararı	Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)
Kişisel Verileri Koruma Uzmanlığı Yönetmeliği		"Veri Sorumluları Siciline Kayıt Yükümlülüğünde İstisna Tutulacak Veri Sorumluları" ile ilgili Karar	Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi
Kişisel Verileri Koruma Kurumu Teşkilat Yönetmeliği			100 Soruda Kişisel Verilerin Korunması Kanunu
Kişisel Verileri Koruma Kurumu Personeli Görevde Yükselme ve Ünvan Değişikliği Yönetmeliği			

10.5. Değerlendirmeler

Bu bölümde Türkiye'de ve dünyada kişisel verilerin korunması kapsamında yapılan çalışmalar incelenmiştir. Öncelikli olarak kişisel verilerin korunması konusundaki temel kavramlar anlatılmış ve birçok düzenlemede yer alan veri korumanın temel ilkeleri vurgulanmıştır. Takip eden bölümlerde genel veri koruma modelleri açıklanmış ve dünyadaki temel düzenlemeler detaylı olarak anlatılmıştır. Türkiye'de 2016 yılından beri yürürlükte olan Kişisel Verilerin Korunması Kanunu ile söz konusu kanunun getirdiği yükümlülükler ile bu kapsamda kurulmuş olan Kişisel Verileri Koruma Kurulu'nun yapmış olduğu çalışmalar da anlatılmıştır. Ayrıca Türkiye gibi birçok ülkede kanun çalışmaları yapılırken, bu alandaki en önemli düzenleme olarak görülen 95/46 sayılı Avrupa Birliği Veri Koruma Direktifi'nin örnek alındığı ve söz konusu direktifin de 2018 yılı itibariyle ilga edildiği vurgulanmıştır. Bu açıdan bakıldığında kişisel verilerin korunması alanındaki son yirmi yılın en önemli düzenlemesi olarak görülen GDPR'ın Avrupa Birliği'nde yürürlüğe girmesiyle birlikte, yaşanacak tecrübeler ve yapılacak çalışmalar neticesinde, Türkiye'nin de Avrupa Birliği ile ilişkileri ve üyelik süreci değerlendirildiğinde 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun revize edilmesinin ve GDPR ile uyumlu hale getirilmesinin ileride gündeme gelebileceği değerlendirilmektedir.

Kaynaklar

[1] Kişisel Verilerin Korunması Kanunu ve Gerekçesi, http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf.

[2] Canbek, G., Sağıroğlu, Ş. (2006). "Bilgi, Bilgi Güvenliği ve Süreçleri üzerine bir inceleme", Politeknik Dergisi, Cilt 9 (3), s.168.

[3] TUİK Haber Bülteni (2018), sayı 27819, http://www.tuik.gov.tr/PreHaberBultenleri.do?id=27819.

[4] Greenleaf, G., (2017), "Privacy Laws & Business International Report", s.14-26. https://privacylaws.com/Documents/PLB_INT_SPL/Intnews145.pdf.

[5] Şimşek, O., (2008) "Anayasa Hukukunda Kişisel Verilerin Korunması", s. 4, Beta yayınları.

[6] Korkmaz, İ., (2016), "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme", TBB Dergisi, vol. 124, s.83-84, s.94-95.

[7] "100 Soruda Kişisel Verilerin Korunması Kanunu", s.26, s.31, Kişisel Verileri Koruma Kurumu (2018).

[8] "Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi", Kişisel Verileri Koruma Kurumu (2018), s.56,57.

[9] Küzeci, E., (2010) "Kişisel Verilerin Korunması", Ankara Üniversitesi Kamu Hukuku Anabilim Dalı, Doktora Tezi s.143, 287.

[10] Gültekin, N. M., (2012) "Kişisel Verilerin Ceza Hukuku Yönünden Korunması", Galatasaray Üniversitesi Kamu Hukuku A.B.D., Yüksek Lisans Tezi, s.22.

[11] Korkmaz, İ., (2017), "Kişisel Verilerin Ceza Hukuku Kapsamında Korunması", s. 74, Seçkin yayınları.

[12] https://privacyinternational.org/explainer/41/101-data-protection,

[13] DLA Piper, (2018), "Data protection laws in the World", s.35, s.110, s.647.

[14] Banisar, D., (2018), "National Data protection/privacy laws and bills", s.1, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416.

[15] Doğan, A.C., (2015) "Kişisel Verilerin Korunması, Muhafazası ve Paylaşımı". , MASAK.

[16] Kaya, M.B., Taştan, F.G., (2016) "Kişisel Veri Koruma Hukuku", s.156-157, Onikilevha yayınları.

[17] https://www.oecd.org/about/ , OECD hakkında.

[18] https://www.coe.int/en/conventions/new-treaties, 108 sayılı sözleşme ek protokol.

[19] Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun, Kanun No: 5982; Resmi Gazete Tarihi: 13.05.2010, Sayı: 27580.

[20] https://kvkk.gov.tr, Mevzuat.

[21] Y. Vural, "ϱ-kazanım: Mahremiyet korumalı fayda temelli veri yayınlama modeli," Doktora Tezi, Bilgisayar Mühendisliği, Hacettepe Üniversitesi, 2017.

[22] Y. Vural ve Ş. Sağıroğlu, "Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme. 508. Gazi Üniv. Müh. Mim. Fak. Der. Cilt 23, No 2".

Mobil Cihazlarda Siber Güvenlik

BÖLÜM 11

Prof. Dr. Mustafa ALKAN
Dr. İbrahim Alper DOĞRU
Dr. Murat DÖRTERLER
Rami URFALIOĞLU
Çağrı SÜMER

MOBİL CİHAZLARDA SİBER GÜVENLİK

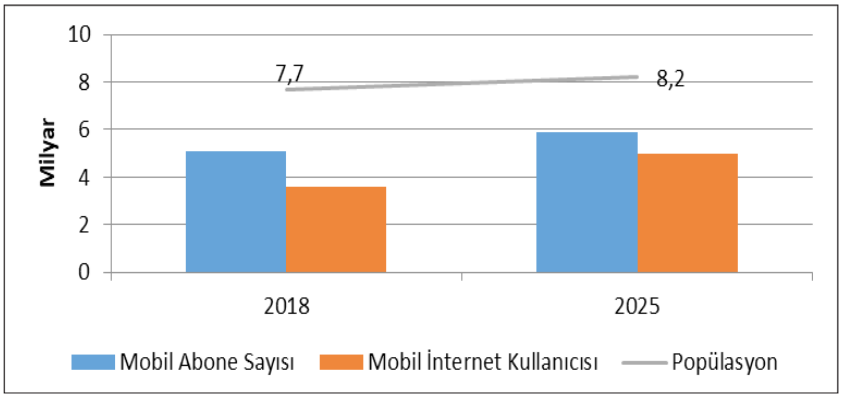
Mobil cihazlar günlük yaşamın vazgeçilmez bir parçası haline gelmiştir. Bu cihazlar ile iletişimden bankacılığa, alış verişten e-ticarete birçok işlem gerçekleştirilebilmektedir. Ülkemizde yer alan mobil abonelerin %75'inin akıllı telefona sahip olduğu ve bunların %60'nın aktif internet kullanıcısı olduğu ifade edilmektedir. Diğer taraftan, 2017 yılında ülkemizde satılan akıllı telefonların %86'sı Android işletim sistemi kullanmaktadır. Akıllı telefonların dünya üzerindeki kullanım yaygınlığı ve akıllı telefon kullanıcılarının güvenlikle ilgili bilinç düzeyinin düşük olması, bu cihazları kötücül yazılım yazarlarının hedefi haline getirmiştir. Yapılan çalışmalar, kullanıcıların büyük bir çoğunluğunun uygulama kurulumu sırasında istenen izinlerden habersiz olduğunu veya bu izinlerin tam olarak ne manaya geldiğini bilmediğini ortaya koymaktadır. Kullanıcı izinler hakkında bilinçlendirilse bile, uygulamalar çalışma zamanında (on run-time) ön görülmemiş başka kötücül eğilimler gösterebilmektedir. Bu nedenle, uygulamaların kötücül özelliğe sahip olup olmadığı konusunda hem yükleme öncesi, hem yükleme esnasında hem de yükleme sonrası çalışma zamanında anti-virüs taramasının yapılmasına ve kullanıcıların bilgilendirilmesine ihtiyaç duyulmaktadır. Bununla birlikte, kötücül yazılımların yaygınlaşması ve gelişmiş türlerinin ortaya çıkması bu tür yazılımların tespitini güçleştirmektedir. Bu çalışmada, mobil cihazlara yönelik siber saldırı tehditleri ve bu tehditlere karşı alınabilecek tedbirler konusunda yapılan araştırmaya yer verilmektedir.

11.1. Giriş

Hazırlanan bir rapora göre ülkemizde yer alan mobil abonelerin %75'inin akıllı telefona sahip olduğu ve bunların %60'nın aktif internet kullanıcısı olduğu ifade edilmektedir [1]. Diğer taraftan,

Gartner tarafından Mayıs 2017'de yayınlanan verilere göre ülkemizde satılan akıllı telefonların %86'sı Android işletim sistemi kullanırken, iOS'un pazardaki payı %13,8'de kalmıştır [2]. Hâlihazırda internet ortamında çok fazla tipte kötücül yazılım bulunmaktadır. Verizon tarafından 170 milyonun üzerinde kötücül yazılımın olduğu ve her saniyede 5 kötücül yazılım ortaya çıktığı rapor edilmektedir. Symantec 317 milyon yeni tür kötücül yazılım olduğunu ve her gün 1 milyon yeni tehdidin ortaya çıktığını raporlamaktadır [3].

Mobil cihazların kullanımı gün geçtikçe artmaktadır. Bu cihazlar ile iletişimden bankacılığa, alış verişten e-ticarete birçok işlem gerçekleştirilebilmektedir. 2025 yılına kadar tüm mobil abonelerin yaklaşık %80'inin akıllı telefon sahibi olması beklenmektedir [4].



Şekil 11.1. Mobil cihaz ve abone eğilimi [4]

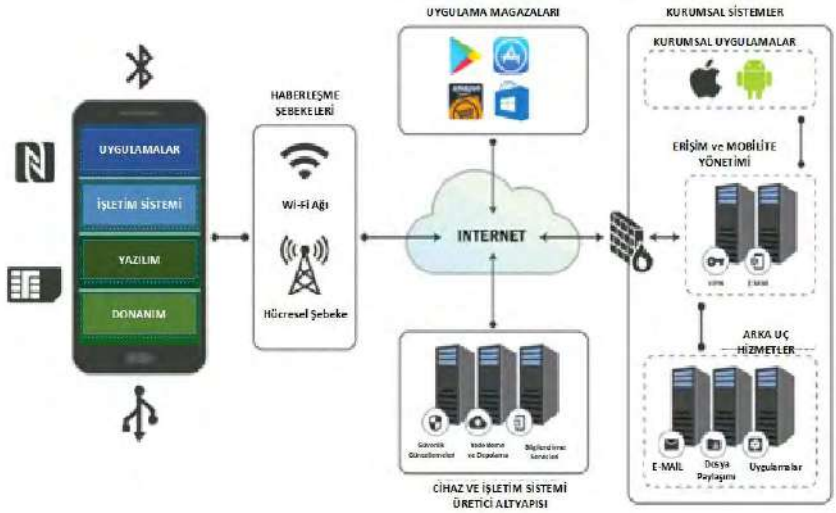
Dünyada kullanılan mobil cihazların %76,88'i android, %20,38'i ise iOS işletim sistemi kullanmaktadır. Geriye kalan %1,23'lük kısımda ise kullanılan işletim sistemi bilinmemektedir [5]. Cihaz üreticileri açısından küresel piyasadaki son duruma bakıldığında, 2018 ikinci çeyrek akıllı cihaz satış rakamlarının %20,9'unu Samsung, %15,8'ini Huawei, %12,1'ini Apple, %9,3'ünü Xiaomi, %8,6'sını OPPO ve geri kalan %33,2'lik kısmını ise diğerleri oluşturmaktadır [6]. Akıllı telefon kullanımında artış ile birlikte, mobil uygulama kullanımı da önemli artışlar göstermiştir. Dünya genelinde uygulama marketlerinde bulunan uygulamaları indirme sayısı 2018 yılı itibariyle 200 milyarı geçmiştir. Uygulama indirme sayısının 2022 yılında 250 milyarı geçmesi beklenmektedir [7].

2016 yılında Apple tarafından, 2 milyondan fazla uygulamanın Apple Store'de bulunduğu ve bunların uygulama marketinin açıldığı 2008 yılından itibaren 130 milyarın üstünde indirildiği ifade edilmiştir. Windows Store, Amazon AppStore ve Blackberry World gibi diğer uygulama mağazalarında yaklaşık 1.5 milyon ilave uygulamanın bulunduğu tahmin edilmektedir [8]. Mobil uygulamaların çok sayıda kullanıcı tarafından indirilmesi, kötücül yazılımların yayılma imkânını ve hızını artırmaktadır.

Mobil güvenlik konusu, kötücül yazılım tespit teknolojileri, mobil güvenlik risk farkındalığı mahremiyet ve izinler gibi farklı konuları içermektedir. Birçok kullanıcı, mobil cihazlara uygulama kurulumunda istenen izinlerin neler olduğu ve ne için istendiği hususlarını ihmal etmektedir.

Bununla birlikte, mobil kullanıcılar antivirüs ve anti kötücül yazılım uygulamalarını kullanmakta tereddüt etmektedirler. Bu durum onları güvenlik zincirinde en zayıf halka yapmaktadır [9]. Mobil cihazların günümüzde artan bağlantı ve işlem kabiliyeti kötücül saldırıların hedefi olmasına neden olmuştur. Akıllı telefonların dünya üzerindeki kullanım yaygınlığı ve akıllı telefon kullanıcılarının güvenlikle ilgili bilinç düzeyinin düşük olması, bu cihazları kötücül yazılım yazarlarının hedefi haline getirmiştir. Diğer taraftan, yeni kötücül yazılımların geliştirilmesi ve saldırı araçlarının modüler bir yapıya kavuşması gibi nedenlerle kötücül yazılım tespitinde kullanılan teknikler yetersiz kalabilmektedir [10].

Mobil cihazlar, uçtan uça birçok sistemi barındıran geniş bir mobil ekosistemin içerisinde çalışmaktadır. Bu ekosistem Şekil 11.2'de görüldüğü üzere, mobil donanımları, yazılımları, mobil uygulamaları, iletişim altyapı ekipmanlarını içermektedir. Böyle bir ekosistemde yer alan her bileşen güvenlik açısından risk oluşturabilmektedir. Ancak, bu çalışmada mobil uygulamaların oluşturduğu riskler, bunların tespit edilmesi ve alınması gereken tedbirler konusu üzerinde durulmuştur.



Şekil 11.2. Mobil ekosistem [8]

Diğer taraftan mobil cihazlar üzerinde dış dünya ile etkileşim halinde olan birçok arayüz bulunmaktadır. Her bir arayüz yapısı itibariyle cihaz üzerinde güvenlik riski oluşturan bir nokta haline gelebilmektedir. Mobil cihazların sahip olduğu arayüzlere ve bunların özelliklerine Şekil 11.3'de yer verilmektedir.



Şekil 11.3. Mobil cihazlarda bulunan arayüzler [8]

Akıllı mobil cihazların yaygınlaşma hızı ve kullanıcıların büyük çoğunluğunun bilinç düzeyinin düşük olması siber saldırganlar açısından bulunmaz bir ortam oluşturmaktadır.

11.2. Mobil Kötücül Yazılımlar

Kötücül yazılımlar, kullanıcının isteği dışında veya izinsiz olarak işlem yapan, önemli bilgileri ele geçiren, değiştiren veya kullanılmaz hale getiren programlar veya kod parçalarıdır. Kötücül yazılımlar genellikle SPAM maillerle veya faydalı uygulamaların içerisine eklenen gizli eklentiler ile hedef sistemlere bulaştırılmaktadır. Kötücül yazılımlar;

- Virüs,
- Solucan,
- Trojan,
- Rootkit,
- Botnet

şeklinde gruplandırılabilir [11]. Söz konusu kötücül yazılımlar kullanılarak mobil cihazlar üzerinde bulunan açıklıklar üzerinden cihazın kontrolü ele geçirilebilmekte veya kişisel bilgiler çalınabilmektedir. Akıllı telefonları ele geçirmek için kullanılan en yaygın kötücül yazılım türlerine ve bunların örneklerine Tablo 11.1'de yer verilmektedir.

Tablo 11.1. Akıllı telefonları hacklemekte kullanılan kötücül yazılımlar [12]

Tür	Tanımlama	Örnekler
Trojan	Yasal uygulamalar gibi davranan programlardır.	Android.Pjapps Trojan, Rogue apps, Hydraq
Virüs	Yerleştiği bilgisayardaki veya mobil cihazdaki dosyalara zarar veren, kendini kopyalama yeteneğine sahip yazılımlardır.	Stuxnet
Botnet	Siber saldırganlar tarafından bilgisayarları kontrol etmek ve gerektiğinde farklı sistemlere saldırı düzenlemek amacıyla kullanılan yazılımlardır. Mobil cihazlardaki sosyal medya uygulamaları botnetler için yeni bir ortam sağlamaktadır.	Opt-in botnet, Aurora botnet, Rustock
Toolkit	Network tabanlı yaygın saldırılar yapmak için kullanılan yazılımlardır.	Phoenix toolkit
Kötücül Reklam (Malvertising)	Sahte internet siteleri ile bağlantılı özgün görünen reklamlardır.	TweetMeme gibi sosyal medya uygulamalarında kullanılan kötücül reklamlar.
Solucan	Mobil şebekelerde havadan yayılabilen ve kendi kendini çoğaltabilen kötücül programlar.	iPhoneOS.Ikee.B, iPhoneOS. Ikee

Mobil kötücül yazılımlar, SMS, MMS, enfekte uygulamalar gibi farklı şekillerde yayılabilmektedir. Kötücül yazılımların ana hedefi, mobil cihazdaki kişisel bilgileri veya kullanıcının hesap bilgilerini ele geçirmektir. Örneğin, SMS.AndroidOS.FakePlayer.b isimli uygulama trojan içermektedir. Bu uygulama kullanıcılar tarafından yetişkin içeriklerin izlenebilmesi için geliştirilmiştir ve manuel olarak kullanıcının bir web sitesinden telefonuna indirerek kurması gerekmektedir. Uygulamanın boyutu çok küçüktür ve kurulum sırasında kullanıcıdan SMS göndermeye ilişkin izin istenmektedir. Kullanıcı tarafından uygulama bir kez çalıştırıldığında kullanıcının bilgisi dışında, program tarafından Premium SMS göndermektedir. Bu mesajlar sonrasında kullanıcının parası, bilgisi dışında siber suçlulara transfer edilmektedir [11].

Akıllı telefonlara yönelik geliştirilen rootkit yazılımları ile GPS, pil, ses ve mesajlaşma gibi telefonlara özel bilgiler ve arayüzler kontrol edilebilmektedir. Bu bilgiler ve arayüzler kötücül yazılım geliştiren korsanlara, kullanıcıların gizliliğini ve güvenliğini tehlikeye sokacak farklı saldırı yöntemleri geliştirme imkanları sunmaktadır. Bu şekilde geliştirilen rootkit yazılımları ile akıllı telefon kullanıcısının telefon görüşmeleri dinlenebilir, mevcut konum bilgisi öğrenilebilir veya telefonun pili bitirilebilir.

Diğer taraftan kötücül yazılımların yapay zekayı kullanması ile birlikte tespit edilmesi ve bunlarla mücadele edilebilmesi güçleşmiştir. Akıllı kötücül yazılımlara, güvenlik araştırmacıları tarafından IOS işletim sistemini kullanan cihazlara yönelik geliştirilen ISAM (iPhone Stealth Airborne Malware) örnek olarak verilebilir [13]. ISAM, kötücül yazılım yayılım mantığı, botnet kontrol mantığı, gizli bilgilerin toplanması ve çalınması, çok sayıda kötücül SMS gönderimi, uygulamaları hizmet dışı bırakma, şebekeyi hizmet dışı bırakma gibi altı farklı kötücül özelliği bünyesinde barındırmaktadır. Ayrıca, senkronize dağıtık saldırıları yerine getirebilmek için programın ve kodların uzaktan güncellenmesi yeteneğine sahiptir.

Bilgisayar korsanları, kullanıcıların kişisel bilgilerini çalmak veya kullanıcıları dolandırmak için mevcut uygulamaların açıklıklarını araştırmaktan ziyade kişisel bilgisayar tabanlı virüs ve kötücül yazılımları akıllı telefonlara hızlıca uyarlamaktadırlar [14]. Google Play'de yaklaşık olarak 3,5 milyon uygulama bulunmaktadır. Bunların %13'lük kısmının düşük kaliteli olduğu ve yüksek güvenlik

riski taşıdığı söylenmektedir. Cambridge Üniversitesi'nin 2015'de yapmış olduğu bir araştırma, Android akıllı telefonlarının %87'sinin bilgisayar korsanları tarafından istismar edilebilecek en az bir savunmasız noktaya sahip olduğunu ortaya koymuştur. Zimperium laboratuvarının araştırması Android cihazların %95'inin SMS vasıtasıyla en az bir kez saldırıya maruz kaldığını göstermektedir [14].

Bununla birlikte araştırmalar kullanıcıların birçoğunun saldırıya maruz kaldığından ve kişisel bilgilerinin çalındığından haberdar olmadığını ortaya koymaktadır. Bu nedenle mobil güvenlik ve mobil güvenlik risklerine karşı alınabilecek tedbirler konusunda kullanıcıların bilinçlendirilmesi gerekmektedir. Ancak, kullanıcıların bilinç düzeyinin artırılması ile mobil cihazlara yönelik güvenlik risklerine karşı mücadele edilebilir.

Mobil cihaz güvenliğinde diğer önemli bir konu mobil cihazlarda kullanılan uygulamaların güvenli olması konusudur. Burada, uygulamayı geliştiren yazılımcılara önemli görevler düşmektedir. Uygulama geliştiricileri, akıllı cihazlarımızda barındırılan telefon defteri, arama kayıtları, internet gezinti kayıtları, resimler ve videolar, finansal bilgiler, mesajlar, GPS konumu, kamera ve mikrofon erişimi gibi kişisel bilgilerimize kolaylıkla erişebilmektedirler. Ayrıca, kişisel iletişimimizi ve hareketlerimizi takip edebilmektedirler. Uygulama geliştiricilerinin genellikle ihtiyaç duyduğu izinlerden daha fazlasını kullanıcıdan alma eğiliminde oldukları görülmektedir. Kullanıcılar ise, uygulama yüklerken nelere izin verdiklerinin ve bunların sonuçlarının neler olabileceği konusunda genellikle fikir sahibi değillerdir.

Mobil kötücül yazılımların %60'ı spesifik olarak mobil cihazlardaki finansal bilgileri hedef almaktadır ve test edilen uygulamaların %95'inde en azından bir savunmasız nokta bulunmaktadır [15]. Gelişmiş güvenliğe rağmen, finansal kurumlar siber suçluların hedefinde kalmaya devam etmektedir. Rootkitler, hibrit tehditler, ortadaki adam/tarayıcı saldırıları ve oltalama gibi tehditler, mobil servisler ve bunları kullananlar için tehlikeli bir ortam oluşturmaktadır [15].

Google Play'de 200'ün üzerinde mobil güvenlik uygulaması bulunmasına rağmen, bunların hiçbirisi kullanıcıların ilgisini tam olarak

çekebilmiş değildir. Akıllı telefon kullanıcıları kişisel bilgisayarlara uyguladıkları antivirüs deneyimlerini akıllı telefonlara aktarmakta başarılı olamamış gibi görünmektedir. Bunun temel sebebi, mobil güvenlik riskleri konusunda kullanıcıların yeterli bilgiye sahip olmamasıdır.

Mobil tehditler, fiziksel, ağ tabanlı, sistem tabanlı ve uygulama tabanlı olmak üzere farklı kategorilere ayrılabilir [16].

- Fiziksel Tehditler: mobil cihazın kaybolması veya çalınması durumunda ortaya çıkmaktadır. Masaüstü bilgisayarlar ile kıyaslandığında mobil cihazlar daha hafif ve taşınabilir olduklarından kaybolma ve çalınma riskleri yüksektir. Bilgisayar korsanı tarafından mobil cihaz fiziksel olarak ele geçirildiğinde, mobil cihazın içerisindeki bilgilerin ele geçirilmesi veya cihaza kötücül yazılım yüklenmesi çok kolay olmaktadır. Bu gibi durumlarla karşılaşmamak için cihazın fiziksel güvenliğin sağlanması ve cihazın yetkisiz erişimlere karşı korunması için şifrelenmesi önemli bir konudur.
- Ağ tabanlı tehditler: Mobil cihazlarda genellikle bağlantı için Wi-Fi veya bluetooth kullanılmaktadır. Bu arayüzlerin her biri kendi kalıtımsal açıklıklarına sahiptir ve Wifite veya Aircrackng Suite gibi araçlar kullanılarak gizli dinleme yapılmaya karşı hassastırlar. Kullanıcılar, WPA2 veya daha iyi ağ güvenlik protokolleri kullanarak sadece güvenilen ağlara bağlanmalıdır.
- Sistem tabanlı tehditler: Cihaz üreticileri bazen istemeden de olsa cihazları zayıf noktaları ile birlikte üretmektedir. Örneğin, Samsung Android cihazlarda kullanılan SwiftKey gizli dinleme girişimlerine karşı korumasız bulunmuştur. Benzer şekilde, Apple cihazlarda kullanılan iOS'da da kritik açıklıklar vardır. No iOS Zone zayıf noktası, kapsama alanında bulunan iOS cihazlara otomatik olarak bağlanmakta ve cihazı kullanım dışı bırakmaktadır [17].
- Uygulama tabanlı tehditler: Sistem açıklıklarına benzer şekilde, cihaz üzerinde yüklü olan üçüncü parti uygulamalar güncelliğini yitirmiş olabilmektedir. Bazı uygulama geliştiricileri zamanında uygulamaların güncel sürümlerini yayınlamazlar. Bazen de kullanıcılar uygulamaları güncellemeyi ihmal etmektedirler. Güncel olmayan uygulamaların kullanımı bu uygulamalardaki

zayıf noktaların siber saldırganlar tarafından istismar edilmesi riskini artırmaktadır.

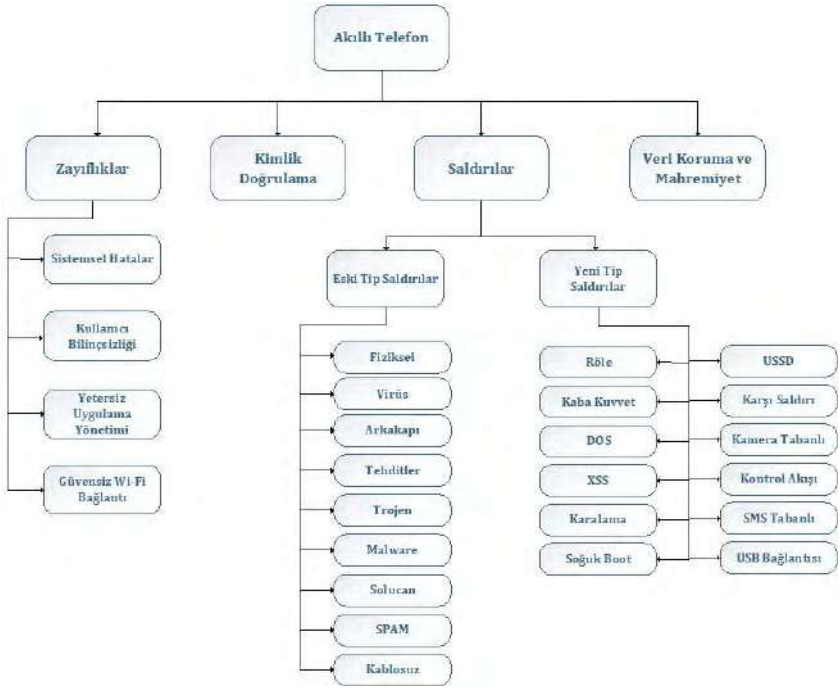
Özellikle mobil cihazların çalınması veya kaybolması durumunda kötü niyetli kişiler tarafında kullanımının engellenmesi amacıyla IMEI bloklama yöntemi kullanılmaktadır. IMEI bloklama yönteminde kaybolan veya çalınan cihaza ait IMEI numarası, hizmet alınan mobil işletmeci tarafından iletişime kapatılmaktadır. Böylece, cihazın kötü amaçlar için kullanılmasının önüne geçilebilmektedir [18]. Ülkemizde de uygulanan IMEI bloklama yöntemi ile mobil cihazların fiziksel olarak güvenlik zafiyeti oluşturma ihtimali azaltılmaya çalışılmaktadır.

Saldırganlar, genellikle kötücül uygulamaları mobil cihazlara yükleyebilmek için kullanıcıları kandırmaya yönelik sosyal mühendislik tekniklerini kullanmaktadır. Bu bir mesaj içerisindeki link, kısaltılmış hiper bağlantı veya yasal bir uygulamanın değiştirildikten sonra yeniden paketlenmesi şeklinde olabilmektedir. Sosyal mühendislik yoluyla yapılan dolandırıcılıkların dünyada en çok kullanılan sahtekarlık yöntemi olduğu INTERPOL tarafından yapılan bir araştırmada ortaya konulmaktadır. Örneğin, İngiltere Ulusal Dolandırıcılıkla Mücadele Bürosu tarafından yapılan bir araştırma Ocak 2014 ile Ocak 2015 tarihleri arasında bu tarz rapor edilen olayların %21 artış gösterdiğini ortaya koymaktadır [18].

Diğer taraftan, mobil cihazlara yönelik tehditler saldırı türlerine göre kötücül yazılım saldırıları, aldatıcı yazılım saldırıları ve casus yazılım saldırıları olmak üzere üç ana kategoride ele alınabilir. Kötücül yazılım saldırıları, mobil cihazlara zarar vermek ve kişisel bilgileri çalmak amacıyla kullanılmaktadır. Aldatıcı yazılım saldırıları genellikle pazarlama amacıyla mobil cihazdan veri toplamak amacıyla kullanılırlar. Bu yazılımların zarar verme amacı olmasa da kullanıcılara rahatsızlık verebilmektedir. Casus yazılımlar ise mahrem kişisel verileri ele geçirmeyi hedeflemektedir [19].

Siber tehdit oluşturan en kritik zafiyetleri sıfırıncı gün açıklıkları oluşturmaktadır. Sıfırıncı gün açıklıkları, henüz üretici tarafından bilinmeyen ve buna ilişkin bir önlemin alınmadığı zayıflıkları ifade etmek için kullanılmaktadır. Eylül 2015'de güvenlik şirketi Zerodium Apple iOS'da bulunacak açıklıklara 1 milyon USD ödül vereceğini açıklamıştır. Belirlenen kriterlere uygun olarak açıklık bulan bir takım bu ödülü kazanmıştır [8].

Akıllı telefon kullanımındaki artış birçok güvenlik riskini de beraberinde getirmektedir. Akıllı telefonlara yönelik güvenlik riskleri Şekil-11.4'deki gibi kategorize edilebilir. Burada görüldüğü üzere akıllı cihazlara yönelik güvenlik risklerini; zayıf noktalar, kimlik doğrulama, veri koruma ve mahremiyet ile saldırılar olmak üzere dört ana kategori oluşturmaktadır.



Şekil 11.4. Akıllı cihaz güvenlik riskleri [20]

11.3. Mobil Cihazlara Yönelik Saldırılar

Kaspersky Lab araştırmacıları tarafından litetatürde Cabir adı verilen ilk mobil kötücül yazılım 2004 yılında tespit edilmiştir. Cabir, dönemin en popüler Symbian işletim sistemine sahip cep telefonlarını hedef almıştır. Cabir bir kez telefona bulaştığında, "Caribe" kelimesi telefon her açıldığında telefon ekranında görüntülenmekteydi. Bu solucan bluetooth iletişimi açıklık olan diğer telefonlara kendini kopyalayabilme özelliğine sahipti. Aslında, Cabir kötücül bir yazılım değildi, ancak sonradan Cabir'in kullanmış olduğu yöntem siber saldırganlar tarafından siber saldırı amacıyla kullanıldığından mobil telefonlara yönelik ilk solucan olarak kabul edilmektedir [21].

2005 yılında, Cabir'in kullandığı yöntemi kullanan Commwarrior adında yeni bir kötücül yazılım ortaya çıkmıştır. Commwarrior, telefona bir kez bulaştığında adres defterindeki tüm kişilere SMS iletebilmekteydi, alıcı mesajı açtığında ise kendini hedef telefona kopyalamaktaydı. Commwarrior, geliştirenler açısından ekonomik bir fayda sağlamamakla birlikte kurbanlar üzerinde finansal etki yapan ilk mobil kötücül yazılımdır [22]. 2006 yılında, RedBrowser Commwarrior'un yapısını geliştirerek java üzerinde çalışabilen çoklu mobil platformlara bulaşabilen ilk trojana dönüştürmüştür. Bu haliyle yazılım, kurbanlarının telefonlarından yüksek ücretli Premium SMS göndererek kullanıcılara ekonomik anlamda zarar vermiştir.

Mobil telefonlar akıllı telefonlara dönüştükçe, kötücül yazılımlar da gelişme göstermiştir. Kötücül yazılımlarla birlikte casus yazılımlarda mobil dünyada yer almaya başlamıştır. Casus yazılımlar, kurbanlarının gizli veya kişisel bilgilerini ele geçirmek amacıyla siber korsanlar tarafından kullanılan bir çeşit kötücül yazılımdır. 2007 yılında ortaya çıkan FlexiSpy, mobil cihazlarda casusluk amacıyla kullanılan ilk kötücül yazılımlardandır. Bu program, mesajların, adres defterinin ve görüşmelerin kaydedilmesinde oldukça başarılı olmuştur ve daha sonra ticarileştirilmiştir.

2007 yılında ilk jenerasyon iPhone telefonlar piyasaya çıktıktan sonra, iOS'a yönelik kötücül yazılımlar da ortaya çıkmaya başlamıştır. 2009'da IKee solucanı jailbreak yapılmış iPhone telefonlara bulaşarak telefonların duvar kağıdını solucanı yazan yazılımcının fotoğrafı ile değiştirmiştir [23].

Kötücül yazılımlar genellikle, yazılımcısına ekonomik kazanç sağlamak amacıyla geliştirilmektedir. Zitmo (Zeus in the mobile), geliştiricisine çok büyük kazanç sağlayan kötücül yazılımlara bir örnektir. Aslında, masaüstü bilgisayarlarda görülen Zeus trojaninin mobil versiyonudur. Bu trojan, Android, Blackberry, Windows Mobile ve Symbian platformlarında çalışan mobil telefonları kullanan kurbanlarının bankacılık işlemleri sırasında kullandıkları hesap ve parola bilgilerini elde etmektedir [24].

Android platformunun yaygınlaşması siber saldırganların bu platforma yönelik kötücül yazılım geliştirme motivasyonunu artırmıştır. 2011 yılında, DroidDream isimli trojan Google Play Store'de yayın-

lanmış, 50'den fazla uygulamaya bulaşmış ve her gün yüz binlerce kez mobil cihazlara indirilmiştir [25]. Bu kötücül yazılım kullanıcıların bilgilerini uzak sunuculara aktarmıştır. Google tarafından fark edilmesi üzerine, trojan bulaşan uygulama marketten kaldırılmıştır. Android cihazları hedef alan Boxer ismindeki diğer bir trojan 2012 yılında geliştirilmiştir. Bu trojan Commwarrior ile benzer özellikler göstermektedir. Boxer trojani 63 ülkede gözlenmiştir.

2013 yılında, Android platformunda ilk fidye yazılımı olan FakeDefender ortaya çıkmıştır. Bu kötücül yazılımın bulaştığı cihazda aslında olmayan bir kötücül yazılımı ortadan kaldırmak için kullanıcılardan para elde edilmesini sağlayan bir sistem kullanılmıştır [26].

2014 sonrasında mobil kötücül yazılım saldırıları üssel olarak artış göstermiştir. 2016 yılında Nokia tarafından yayımlanan bir rapora göre, sadece 2016 Ocak ayından Nisan ayına akıllı telefonlara yönelik mobil kötücül yazılım saldırıları %95 artış göstermiştir [27].

Günümüzde mobil kötücül yazılımlar gittikçe karmaşık bir hal almıştır. 2016 yılında görülen SMS hırsızlığı buna güzel bir örnektir. Bu kötücül yazılım kendisini bir uygulama kaldırma programı olarak tanımlamasına rağmen arka planda kullanıcının kayıtlı mesajlarını çalmaktadır. SMS hırsızlığı yeni bir konu olmasına rağmen, bu uygulamanın kaldırılması oldukça zordur.

2016'da araştırmacılar Xbot adı verilen yeni tip bir trojan içeren 22 Android uygulaması keşfetmişlerdir. Xbot, çoklu kötücül davranışlarını güncelleyen bir fidye yazılımıdır. Öncelikle, Google ödeme arayüzüne benzeyen bir oltalama sayfası kullanarak kullanıcının kredi kartı ve bankacılık bilgilerini çalmaya çalışmaktadır. İkinci olarak, SMS mesajlarını, kontak bilgilerini ve mobil bankacılık onay mesajlarını ele geçirmeye çalışır. Genellikle, kullanıcının cihazını şifreleyerek kullanılmaz hale getirir ve şifreyi kaldırmak için kurbandan fidye ister [28].

Apple IOS'u hedef alan Pegasus adındaki kötücül yazılım ise 2016'da Citizen Lab ve Lookout tarafından keşfedilmiştir. Citizen Lab'ın raporuna göre Birleşik Arab Emirlikleri'nde bulunan insan hakları savunucusu Ahmed Mansoor'un telefonuna iletilen sıfırıncı gün istismarı içeren bir SMS ile telefonuna jailbreak yapılarak casus yazılım yüklenmiştir. Açıklığın tespit edilmesinin akabinde Apple IOS 9.3.5 sürümünü yayınlamıştır [8]. Ağustos 2016 ile Ağustos 2018 arasında, parmak iziyle eşleşen 1.091 IP adresi ve 1.014 alan

adı tespit edilmiştir. Bu bilgilerden geriye doğru Ters DNS sorguları yapılarak Pegasus'tan etkilenmiş olması muhtemel 45 ülke olduğu ortaya konulmuştur. Bu ülkeler; Cezayir, Bahreyn, Bangladeş, Brezilya, Kanada, Fildişi Sahili, Mısır, Fransa, Yunanistan, Hindistan, Irak, İsrail, Ürdün, Kazakistan, Kenya, Kuveyt, Kırgızistan, Letonya, Lübnan, Libya, Meksika, Fas, Hollanda, Umman, Pakistan, Filistin, Polonya, Katar, Ruanda, Suudi Arabistan, Singapur, Güney Afrika, İsviçre, Tacikistan, Tayland, Togo, Tunus, Türkiye, Birleşik Arap Emirlikleri, Uganda, Birleşik Krallık, Amerika Birleşik Devletleri, Özbekistan, Yemen ve Zambiya'dır [29].

Mobil kötücül yazılımların yayılımı zamanla değişim göstermiştir. Uygulama marketlerinde artan güvenlik tedbirleri, kötücül yazılımların markette yer bulmasını güçleştirmiştir. Bunun bir sonucu olarak, masaüstü bilgisayarların kötücül yazılımları mobil cihazlara bulaştırmak için kullanılmasına yol açmıştır. Droidpak, Windows PC'lerde ilk ortaya çıkan kötücül yazılımdır. Android bir cihaz, bilgisayara bağlandığında Droidpak Fakebank adı verilen kötücül yazılımı Android cihaza kurmaya çalışmaktadır. Uygulama bir kez kurulunca, Fakebank cihaz kullanıcısını banka uygulamalarının kötücül versiyonunu mobil cihazına kurmaya ikna etmeye çalışmaktadır.

Mobil cihazların gelişimine paralel olarak, bu cihazları hedef alan kötücül yazılımlarda zaman içerisinde gelişim göstermiştir. Kaspersky Lab'ın en son yayınlamış olduğu rapora göre, 2018 ikinci çeyreği itibariyle yaklaşık 1.7 milyon kötücül yazılım içeren uygulama paketi tespit edilmiştir [30]. Bu kötücül yazılımların genellikle Android platformunun açık kaynak kodlu olmasının ve uygulama geliştiricileri konusunda Apple'de olduğu gibi bir lisanslamanın olmamasının bunun temel nedenini oluşturduğu değerlendirilmektedir.

11.4. Mobil Cihazlarda Güvenlik Analizi

Mobil cihazlara yönelik güvenlik risklerini ortadan kaldırmak amacıyla piyasada kullanılan birçok uygulama bulunmaktadır. Bu uygulamaların güvenlik tehdit türlerine göre hedef aldığı çözümler birbirinden farklılık göstermektedir. Yapılan bir çalışmada, piyasada kullanılan uygulamalar tehditlere karşı savunma mekanizması içerip içermediğine göre analiz edilmiştir.

Tablo 11.2. Mobil güvenlik ürünleri ve sahip olduğu özellikler [14]

Mobil Güvenlik Ürünü	Sahip olduğu özellik																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	Toplam
McAfee Mobil Güvenlik	x	x	x	x	x	x	x	x	x	x		x			x			12
Sophos Mobil Güvenlik	x	x	x	x	x	x	x	x		x	x		x					11
Cheetah Mobil Güvenlik	x	x	x	x	x	x	x	x	x	x								10
Karpersky Lab İnternet Güvenliği	x	x	x	x	x	x	x				x			x		x		10
Quick Heal Mobil Güvenlik	x	x	x	x	x	x		x			x	x	x					10
AVG Free	x	x	x	x		x	x		x	x		x			x			10
G Data İnternet Güvenliği	x	x	x	x	x	x	x				x					x		9
Trend Micro Mobil Güvenlik	x	x	x	x	x	x	x	x			x							9
Alibaba Mobil Güvenlik	x	x	x	x		x	x			x	x							8
Avast Mobil Güvenlik	x	x	x	x	x		x	x	x									8
F-Secure Safe	x	x	x	x	x	x					x			x				8
PSafe DFNDR	x	x	x	x			x	x	x	x								8
Norton Mobil Güvenlik	x	x	x	x	x	x						x	x					8
360 Mobil Güvenlik	x	x	x	x		x	x		x	x								8
Lookout	x	x	x	x	x			x				x					x	8
Ikarus Mobil Güvenlik	x	x	x	x	x	x					x							7
Bitdefender Mobil Güvenlik	x	x	x	x	x		x		x									7
ESET Mobil Güvenlik	x	x	x	x		x				x								6
Webroot	x	x	x	x	x	x												6
Avira	x	x	x	x	x		x											6
AhnLab V3 Mobil Güvenlik	x	x			x		x		x									5
Antiy AVL	x	x						x						x				4
Google Play Protect	x	x	x	x														4
Tencent WeSecure	x	x										x						3
NSHC Droid-X	x																x	2

Tablo 11.2'de yer verilen özellik numaralarının ne anlama geldiğine ilişkin detaylara aşağıda yer verilmektedir.

1. Kötücül yazılımdan korunma: uygulama indirme sırasında kötücül yazılımlara ve virüslere karşı otomatik tarama işlemi yapar.
2. Güvenlik taraması: kötücül kod, dolandırıcılık ve oltalama gibi amaçlarla kullanılan linkleri engeller.
3. Uzaktan silme: kaybolan mobil cihazdaki kişisel bilgilerin yabancıların eline geçmesini engellemek amacıyla uzaktan verileri silmek için kullanılır.
4. Uzaktan kilitleme ve konum belirleme: web arayüzü üzerinden kaybolan akıllı telefonun uzaktan kilitlenmesi ve konumunun belirlenmesi için kullanılır.
5. Mahremiyet koruması: Bir program indirildiğinde veya uygulama kurulurken uygulamanın mobil cihaz üzerinden veri sızıntısı yapıp yapmadığını tespit eder.
6. Arama ve mesaj filtreleme: İstenmeyen mesaj ve aramalara karşı engelleme yapmak için kullanılır.
7. Veri yedekleme: Bulut ortamına veya SD karta önemli verilerin yedeklenmesi için kullanılır.
8. Güvenli uygulama danışmanı: kullanıcılar için güvenilir mobil uygulama tavsiyesinde bulunur.
9. Uygulama kilidi: kişisel verilerin korunması ve mahremiyetin sağlanması için uygulama bazlı PIN koruması sağlar.
10. Wi-Fi güvenliği: güvensiz Wi-Fi bağlantıları üzerinden yapılan bağlantılarda şifreleme ve koruma sağlar.
11. Ebeveyn kontrolü: çocukların internet ortamındaki aktivitelerini kontrol etmek ve gerekli görülen kısıtlamaları yapmak için kullanılır.
12. Çöp dosya temizliği: sistemin sağlıklı çalışması ve disk alanı açmak amacıyla kullanılmayan ve ön bellekte tutulan dosyaları siler.
13. Pil optimize edici: pil ömrünü uzatmak için gereksiz özellikleri kapatır.
14. Güvenli ödeme: online ödeme yapmadan önce ödeme sistemi güvenliğini temin eder.

15. Ağ veri izleyici: akıllı telefonun ağ trafiğini düzenleyerek tarife aşımlarına engel olur.
16. Şifreleme: akıllı telefonu veya telefonun ağ iletişimini şifreler.
17. Kökleme tespiti: telefonun kırılıp kırılmadığını ve bilgisayar korsanları tarafından önemli izinlerin ele geçirilip geçirilmediğini belirlemek için kullanılır.

Birçok antivirüs üreticisi masaüstü bilgisayarlar için üretmiş oldukları antivirüs yazılımlarının mobil versiyonlarını da tüketicilere sunmaktadırlar. Bu mobil çözümlerde genellikle klasik imza tabanlı tespit teknikleri kullanılmaktadır. Bu yaklaşım bilinen kötücül yazılımların tespit edilmesinde kullanılır. Diğer taraftan, bilinmeyen, yeni tipteki veya dönüşüme uğramış kötücül yazılımların tespitinde bu yöntem işe yaramamaktadır. Mobil kötücül yazılımlar dönüşüm ve kod karıştırma teknikleri kullanarak tespit edilmemeye çalışmaktadır. Örneğin, polimorfik ve metamorfik kötücül yazılımlar kendi kodlarını modifiye edebilme yeteneğine sahiptir.

Mobil cihazlarda güvenliği sağlamak önemli konuların başında gelmektedir. Bilindiği üzere, mobil cihazlarda güvenlik riskleri farklı açılardan ele alınabilmektedir. Bununla birlikte, mobil uygulamalar güvenlik riski oluşturma açısından diğer risk parametrelerine göre biraz daha öne çıkmaktadır. Bu nedenle, kötücül yazılımların tespiti kritik bir konu halini almaktadır. Literatürde mobil kötücül yazılım tespitine yönelik birçok çalışmanın yapıldığı görülmektedir. Yapılan çalışmalarda mobil kötücül yazılımların tespitine yönelik farklı yaklaşımlar ele alınmaktadır.

Mobil kötücül yazılımların tespitinde statik, dinamik ve hibrit teknikler başlıca kullanılan tespit yöntemleri olarak karşımıza çıkmaktadır. Bununla birlikte, kötücül yazılımların karmaşık yapılara sahip olması ve çok farklı özellikler sergileyebilmesi bu tür yazılımların tespitinde makine öğrenmesi gibi tekniklerin kullanımını da yaygınlaştırmıştır. Bu bölümde, mobil kötücül yazılım tespitinde kullanılan yöntemlere ilişkin araştırmalara yer verilmektedir.

11.4.1. Statik Analiz Yaklaşımı

Statik analiz yöntemi, uygulama çalıştırılmadan kötücül kodların tespit edilebilmesinde kullanılan tersine mühendislik yöntemidir. Bu yöntemde; çalıştırılabilir modüllere ait büyük veriler (örneğin,

Windows işletim sistemi için taşınabilir çalıştırılabilir içerikler), makine kod komutları, binary veriler (görüntüler, ikonlar, karakter dizinleri vb.) gibi veriler kullanılarak bir analiz gerçekleştirilir [31]. Bu işlem yapılırken kötücül uygulama içerisinde bazı bilgiler çıkarılarak analiz, bu bilgiler üzerinde yapılmaktadır. Uygulamanın süreçleri arasında kullanılan API istekleri bu bilgilere örnek olarak verilebilir [32]. Mevcut statik analiz yöntemleri faklı tiplerdeki kötücül yazılımların tespit edilmesine ve sınıflandırılmasına odaklanmıştır. Literatürde statik analiz yöntemini kullanarak kötücül yazılım tespiti yapılan birçok çalışma bulunmaktadır [33, 34, 35, 36].

Kötücül yazılım tespiti uygulamalarında, çok hızlı bir yöntem olması ve analiz için düşük sistem gereksinimlerine ihtiyaç duyması statik analiz yöntemini araştırmacılar arasında popüler yapmıştır [31]. Çalışma süresi olarak dinamik analiz ile karşılaştırıldığında, statik analiz ile çok daha hızlı sonuçlar elde edilebilmektedir. Ancak, karıştırma yöntemlerinin kullanılması kötücül kodların tespit edilmesi veya sınıflandırılması için tek başına yeterli olmamaktadır [37].

Statik Analiz Türleri;

- **İmza tabanlı analiz** (signature based analysis): İmza tabanlı analizde analiz edilen uygulamalardan elde edilen analizler, imza veri tabanında saklanarak öğrenme sürekli hale getirilmiş olur. Bu analiz yönteminde genelde merkezi bir sunucu ve imza veri tabanı kullanılır. Merkezi sunucu analiz ve koruma süreçlerinde görev alırken, imza veri tabanı elde edilen analizlerin depolanmasını ve sonraki analizlerde tekrar kullanılmasını sağlamaktadır [38].
- **İzin tabanlı analiz** (permission based analysis): Android uygulamalarının analizinde, uygulama yükleme öncesi ve sonrasında istenen izinler önemli rol oynamaktadır. Uygulamaların yüklenmesi esnasında istenen izinler, AndroidManifest.xml dosyasında gösterilmektedir. İstenen bu izinlere erişim verilip verilmemesi kullanıcıya bağlıdır. Ancak bazı uygulamalar bu izinler verilmediğinde işlevini yerine getiremeyeceği için yükleme sürecini sonlandırabilmektedir [39].

11.4.2. Dinamik Analiz Yaklaşımı

Dinamik analiz yöntemi, statik analiz yönteminin tam tersidir. Dinamik analizde uygulama izole bir ortamda çalıştırılır ve çalışırken göstermiş olduğu karakteristiklere göre kötücül mü yoksa iyicil mi olduğu tespit edilmeye çalışılır [10]. Özellikle sıfırıncı gün kötücüllerinin tespit edilebilmesinde statik yöntemler yetersiz kalmaktadır. Çünkü statik yöntemler daha önceden bilinen kötücül özelikler referans alınarak bir analiz gerçekleştirmektedir. Dinamik analiz yöntemleri, imza tabanlı statik analiz yöntemlerinde karşılaşılan söz konusu eksikleri giderebilecek bir özelliğe sahiptir [40]. Bununla birlikte, dinamik analiz yöntemleri statik ve imza tabanlı analizlere göre daha uzun sürmektedir. Kötücül yazılımı yazanlar, kötücül yazılımın sanal ortamlarda çalıştırılarak analiz edilmesi durumunda kötücül taraflarını gizlemeye yönelik yazılım içeriğine daha fazla mantıksal öğeler ekleyerek tespit edilme sürecini daha da uzatabilmektedirler.

Dinamik Analiz Türleri;

- Sistem hizmet çağrıları üzerinden,
- Hizmet çağrıları üzerinden,
- SMS aktivitesi üzerinden,
- Kullanıcının aktivite bilgisi üzerinden,
- Ağ aktivitesi üzerinden,
- Pil kullanım aktivitesi üzerinden,

şeklinde sıralanabilmektedir.

Sandbox konsepti, dinamik analizde yaygın olarak kullanılan bir yöntemdir. Bu yöntemde, analiz edilecek uygulama izole bir ortamda veya bir emülatörde çalıştırılarak davranışları izlenir. Örneğin, DroidScope projesi Android işletim sistemi için açıklık kaynak kodlu bir uygulama sağlamaktadır. Bu uygulama, incelenen mobil uygulamanın farklı katmanlardaki davranışlarını analiz etmek için kullanılır [16].

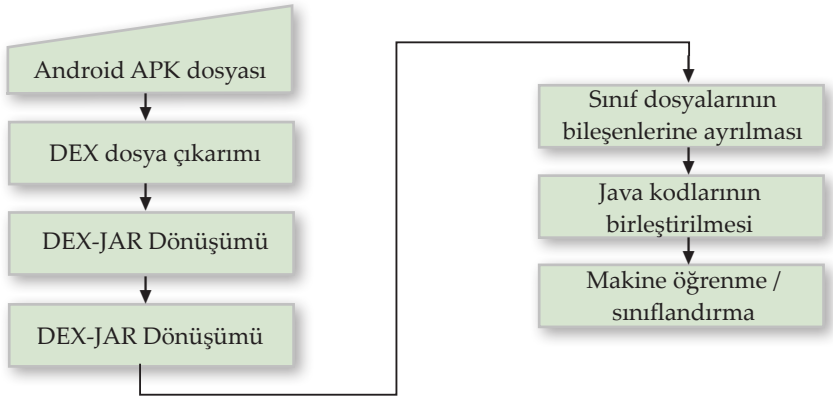
11.4.3. Hibrit Analiz Yaklaşımı

Hibrit analiz yönteminde ise statik ve dinamik analiz yöntemleri birlikte kullanılarak uygulamaların kötücül veya iyicil olup olmadı-

ğı tespit edilmeye çalışılır. Statik ve dinamik analiz yöntemlerinden elde edilen özellikler belirli bir metodolojiye göre birlikte kullanılır [10]. Bu yöntemdeki temel hedef, statik ve dinamik analizde karşılaşılan kısıtların söz konusu iki yöntemi müştereken kullanarak bertaraf edilmesidir.

11.4.4. Makine Öğrenmesi Teknikleri

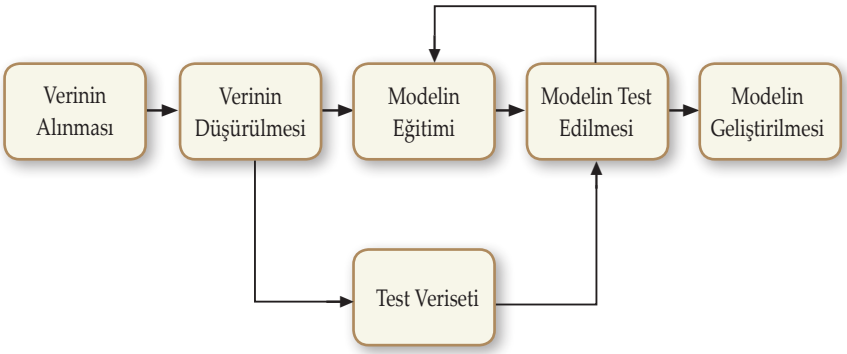
Kötücül kodlar genellikle, kötücül olmayan uygulamaların kullandıkları yolun dışında API araması, yöntemler ve hizmetlerin kombinasyonunu kullanmaktadırlar. Makine öğrenme algoritmaları kötücül servislerin, API ve sistem aramalarının genel kombinasyonunu öğrenerek kötücül olmayan uygulamaları ayırt edebilirler [3]. Şekil 11.5'de genel anlamda, Android tabanlı bir uygulamanın tersine mühendislik ile bileşenlerine ayrılması ve bu bileşenlerin makine öğrenme algoritmaları ile sınıflandırılmasına yönelik akış sırası görülmektedir.



Şekil 11.5. Android bileşenlerine ayırma ve makine öğrenme ile sınıflandırma akış diyagramı [9]

Kötücül yazılımların imza tabanlı yöntemlerde olduğu gibi klasik yaklaşımlar ile tespit edilmesi gün geçtikçe zorlaşmaktadır. Özellikle sahip olduğu imzayı değiştirme yeteneğine sahip çok biçimli kötücül yazılımların tespit edilebilmesi için farklı yöntemler geliştirilmesi gerekmektedir [41]. Kötücül yazılım tespitinde yüksek doğrulukla tespit yapılabilmesi için yazılımlara ilişkin birçok parametrenin ve bunlar arasındaki korelasyonun analiz edilmesi gerekebilmektedir. Bu açıdan, makine öğrenme algoritmaları siber güvelikte

vazgeçilmez araçlardan birisidir. Genel anlamda makine öğrenme sürecine ilişkin akış diyagramı Şekil 11.6'de görülmektedir.



Şekil 11.6. Makine öğrenmesinde genel akış

Analiz edilecek verinin birçok boyutu olabilmektedir. Boyutların yer aldığı özellik vektörü olarak adlandırılan matristen analizde kullanılmayacak olan verilerin süzülmesi gerekmektedir. Bu işlem, özellik çıkarma olarak adlandırılmaktadır. Böylece, geliştirilen modelde analiz edilecek veri setine odaklanılarak hem zamandan hem de işlem maliyetinden tasarruf sağlanmış olacaktır [42].

Makine öğrenme tekniklerinde kullanılan bir diğer önemli yaklaşım ise denetimli ve denetimsiz öğrenme yaklaşımıdır. Denetimli öğrenmede, etiketlenmiş örnek veri setleri kullanılarak model eğitilmekte akabinde, test verileri ile modelin tespit duyarlılığı analiz edilmektedir. Denetimsiz öğrenmede ise, model eğitilirken etiketli örnek veriler kullanılmamaktadır. Burada amaç, belirli bir değeri tahmin etmekten ziyade, işlenmemiş veri içerisinde bir paterni bulmaktır [43]. Kümeleme denetimsiz öğrenme yöntemine örnek olarak verilebilir.

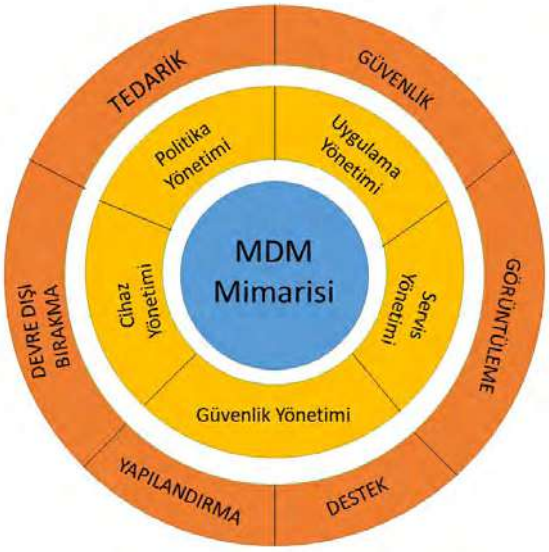
Literatürde yaygın olarak kullanılan makine öğrenme algoritmaları;

- Destek vektör makineleri (Support Vector Machines)
- Karar ağacı (J48 Decision Tree)
- Random Forest
- Naive Bayes
- K en yakın komşu (K Nearest Neighboor)

şeklinde özetlenebilir.

11.5. Mobil Cihaz Yönetimi

Günümüzde mobil cihazlara hem kişisel hem de iş nedeniyle artan bağımlılık sonucu ortaya çıkan güvenlik kaygısı önü alınmadığında, hem kişisel bilgilerin ifşası hem de kurumsal bilgilerin ele geçirilmesi gibi çok önemli sonuçlar doğurmaktadır. Son yıllarda mobil cihaz donanım ve yazılım teknolojinin çok hızlı gelişmesi artık mobil cihazların da özellikle uzaktan olacak şekilde kontrol edilebilmesini sağlayacak fırsatlar doğurmuştur. Kurumlar için çok önemli hale gelen mobil cihaz kontrolünü sağlayacak mobil cihaz yönetim yani mobile device management (MDM) sistemlerinin kullanılması artık kaçınılmaz hale gelmiştir [44].



Şekil 11.7. Mobil cihaz yönetim mimarisi [45]

MDM (Mobile Device Management) Nedir ve Hangi Bileşenlerden Oluşur?

MDM farklı işletim sistemleri ile platfomlar üzerinde çalışan akıllı telefonlar, tablet ile dizüstü bilgisayarları ve pos şeklinde çalışan mobil cihazların genel olarak cihaz, içerik, uygulama ve güvenlik bağlamında uzaktan izlenmesi, güvenliğinin sağlanması, yönetilmesi ve desteklenmesini sağlayan yazılımsal bir mobil cihaz güvenliği sistemidir. Güvenlik sektöründe kurumsal mobilite yönetimi (enterprise mobility management-EMM) olarak da adlandırılabilen

MDM sistemleri ile mobil cihazlardaki veri, işletim sistemi ve kurulum gibi ayarları kontrol edebilir, mobil cihaz ağınızı gerçek zamanlı takip edebilir ve farklı işletim sistemleri ile platformlarına sahip tüm cihazlar üzerinde tutarlı ve benzer politikalar uygulayabilirsiniz. Bir EMM veya MDM sistemi genel olarak alttaki bileşenlerden oluşur [46]:

- Mobil Cihaz Güvenliği (Mobile Device Management, MDM): Cihazın güvenliği, cihazın yönetilmesi, kullanıcı güvenliği.
- Mobil Uygulama Yönetimi (Mobile Application Management, MAM): Mobil cihazdaki in-house ve harici uygulamaların yönetimi ile güvenli uygulama kataloğu.
- Mobil İçerik Güvenliği (Mobile Content Management, MCM): Mobil belge, veri ve içerik güvenliği ile güvenli web tarayıcı uygulaması.
- Mobil E-Posta Yönetimi (Mobile E-Mail Management, MEM): Kurumsal e-postaların güvenliği ve güvenli e-posta uygulaması.
- Kişisel Cihaz Yönetimi (Bring Your Own Device, BYOD): Çalışanların kendi mobil cihazları ile kurumsal kaynaklara ve uygulamalara erişimlerinin güvenliği.

Mobil Cihaz Güvenliği (MDM) Size Neyi Sağlar ve İhtiyaç Nasıl Belirlenir?

MDM, mobil cihaz platformlarının (iOS, Android, Windows Mobile, Blackberry vs) cihaz yönetimi için sunduğu imkanlar ve yönetimi kolaylaştırmak için açtığı API'ler ölçüsünde etkili olabilen bir sistemdir. Bunun yanında örneğin aynı Android işletim sistemine sahip farklı üreticiler (Samsung, Sony, LG, HTC, Huawei vs) arasında bile MDM kapasiteleri ve imkanları arasında ciddi farklar vardır. Hatta daha da ötesi olarak aynı üreticinin Android işletim sistemli farklı ürünleri için bile farklı MDM imkanları söz konusudur.

Bir MDM sistemi almaya karar vermeden önce, bir kurumda MDM'in hangi platformda ve hangi cihaz tipinde kullanılacağı ile MDM'in tam olarak hangi maksatla kullanılacağının çok net bir şekilde belirlenmesi gerekir. Bu tespitlerin yapılmasının ardından bir MDM projesinin başarıya ulaşma ihtimali oldukça yüksektir. Her kurumun farklı bir iş kültürü, işleyişi ve iç dinamikleri

olduğundan her üreticinin MDM sistemi aynı ölçüde yararlı olmayabilir ve verimlilik sağlamayabilir. MDM üreticileri her ne kadar birden çok mobil platform ile işletim sistemine sahip mobil cihazları aynı anda desteklediklerini belirtseler de, aslında MDM sisteminde cihaz karmaşıklığının artmaya başlamasıyla beraber çok ciddi yönetimsel problemler de yaşanmaya başlar. Bu problemlerin en başında, cihazların senkron bir şekilde yönetilememesi ve sürekli tekrarlayan son kullanıcı sorunları gelir. Bu yüzden MDM'i hangi tip cihaz ile işletim sistemlerinde ve hangi maksatla kullanılacağının daha ilk aşamada belirlenmesi gerekir [45].

MDM sistemleri aşağıdaki maksatlar veya ihtiyaçlar için kullanılabilir:

- Kurumsal mobil cihazların coğrafi konumunun takibi.
- Kurumsal mobil cihazların veri (SMS, 3G/4G internet, Wi-Fi) kullanımının takibi.
- Kurumsal e-postaların güvenli ve kontrollü bir şekilde dağıtılması.
- Mobil e-postalar (ActiveSync) için veri sızıntısı önleme tekniklerinin uygulanması.
- Kurumsal e-postaların sadece MDM sistemine dahil olan cihazlar tarafından alınıp gönderilmesi.
- Mobil cihazlardaki yerel e-posta istemcisinin yönetilmesi.
- Mobil cihaz donanım envanterinin takibi.
- Kurumsal mobil uygulama envanterinin takibi. Bu uygulamalar hem kurum içi geliştirilmiş (in-house) hem de uygulama mağazalarından olabilir.
- Mobil işletim sistemi konfigürasyon yönetimi.
- Mobil uygulama kurulumu, güncellenmesi ve kaldırılması.
- Mobil güvenlik politikası uygulanması.
- Mobil cihazlara ortak kablosuz Wi-Fi ayarlarının gönderilmesi.
- Mobil cihazlara ortak Exchange/ActiveSync ayarlarının gönderilmesi.
- Mobil cihazlardaki SMS ve çağrıların izlenmesi (iOS'ta yok ama özellikle Android işletim sistemli bazı ürünler için yapılabiliyor)

- Mobil cihazlardan kurumsal ağa VPN ile erişim sağlanması (hem uygulama tabanlı per-app VPN hem de uzaktan erişim için remote VPN).
- Mobil cihazlara uzaktan komut gönderilmesi (mesela cihaz kaybolduğunda uzaktan silinmesi ve kullanıcılara SMS veya push notification gönderilmesi gibi).
- Kurumsal ortak dosya paylaşım alanlarına mobil cihazlardan erişim.
- Mobil cihazlardaki içeriklerin kontrol altında tutulması (paylaşılmaması, başka bir yere gönderilmemesi veya ekran görüntüsü alınmaması gibi kontrollerin yapılması).
- Mobil cihazlarda işletim sistemi güvenliği ve güvenlik zafiyeti taraması.

Bir Mobil Cihaz Güvenliği (MDM) Sistemi En Azından Hangi Özellikleri Sağlamalıdır?

Bir MDM sistemi almadan önce veya demo çalışmaları safhasında da kurumsal ihtiyaçların da gözetilerek en azından aşağıdaki fonksiyonların yerine getirilmesini beklemek gerekir:

- ActiveSync'i sadece MDM'le yönetilen cihazlara yönlendirebilme. Yani kurumsal e-postalara sadece MDM'e dahil olan cihazlarda kullandırma.
- MDM sisteminin major/minor güncellemelerinde mobil cihaz MDM sistemine yeniden kayıt olmak (register) zorunda olmamalı, profili silinmemeli ve mevcut politikalar çalışmaya devam etmelidir.
- iOS işletim sistemli cihazlardaki yerel e-posta kullanıcılarında mesajlarla gelen eklerin/belgelerin "Open with" ile başka bir uygulamada açılmasını engelleme.
- Kısmi MacOS cihaz kontrolü.
- NAC (network Access control) ürünleriyle entegrasyon.
- AD (Active Directory) gibi LDAP sistemleriyle entegrasyon.
- Kurumsal mobil telefonlarda SIM kart değişikliğini algılama ve bunun tespit edilmesi durumunda cihazı kısıtlama.

- SIEM (syslog) entegrasyonu.
- Kurumsal exchange ayarlarının gönderilebilmesi.
- iOS tabanlı cihazların jailbreak veya Android cihazların rooted edilmesinin kontrolü.
- Mobil cihazlardaki yerel web tarayıcılarını veya MDM'in kendi web tarayıcısını VPN ile tünelleme. Bu sayede kurum içi uygulamalara da mobil cihazdan erişim sağlanması.
- MDM sisteminin harici bir veri tabanına ihtiyaç duymayarak kendi built-in veri tabanını kullanması.
- Mobil cihazın uzaktan tamamen silinmesi (full wipe).
- Mobil cihazın uzaktan sadece kurumsal içeriklerinin silinmesi (enterprise wipe)
- Bir mobil cihazda kullanıcı tarafından MDM uygulamaları ile profillerinin kasti olarak silinmesi yoluyla MDM sisteminden çıkarılması durumunda tüm kurumsal hizmetlerin (e-posta, erişim, uygulama vb) otomatik olarak kesilmesi.
- Mobil cihazlardaki MDM politikalarında önceliklendirme.
- Kurumsal çalışanların esnek bir şekilde etiketlenebilmesi ve etiketlere bağlı olarak politika ve kural verilebilmesi.
- Mobil uygulamalarda kara liste/beyaz liste uygulaması.
- Detaylı raporlama, rapor portalı vb.

11.6. Güvenli Mobil Cihaz Kullanımı

Mobil cihazlarda kötücül yazılımlara karşı alınabilecek önlemleri aşağıdaki gibi sıralamak mümkündür. Söz konusu tedbirlerin alınması ile mobil cihazların kötücül yazılımlara karşı güvenli bir şekilde kullanılabileceği söylenebilir.

1. Mobil cihaza güvenlik yazılımı kurulumu: Güvenilir bir kaynaktan temin edilen güvenlik yazılımı ile mobil cihaz düzenli olarak açıklıklara ve kötücül yazılımlara karşı taranmalıdır.
2. Güvenilir olmayan kaynaklardan veya marketlerden uygulama indirilmemesi.
3. Mobil cihazın işletim sisteminin güncel tutulması. Geliştiriciler genellikle bir güvenlik açıklığı tespit ettiklerinde işletim sistemi-

ni güncelleyerek sorunu ortadan kaldırırlar. Bu nedenle, mobil cihazların işletim sisteminin güncel tutulması güvenlik açısından elzem bir konudur.

Mobil cihazlarda güvenlik açıklıklarına karşı en önemli savunma tekniği, cihazın bilinen açıklıklara karşı yama yazılımlarına sahip olması ve cihazın işletim sisteminin güncel tutulmasıdır. Açıklıklara karşı yama yazılımlarının kullanımı güvenliği büyük ölçüde sağlamakla birlikte, siber korsanların cihaza yönelik saldırı yapabilmesi için daha fazla efor harcamasını gerektirmektedir. Ayrıca, güncel işletim sistemi kullanımı, cihazın en güncel güvenlik tedbirlerine sahip olmasını ve çoğu kişi tarafından bilinmeyen güvenlik açıklıklarına karşı tedbir alınmasını garanti altına almaktadır.

Mobil cihaz güvenliğinde, uygulama güvenliğinin sağlanması güvenlik risklerinin bertaraf edilmesinde önemli bir konu olarak karşımıza çıkmaktadır. Uygulama güvenliğinin garanti edilmesinde ise uygulama geliştiricilere önemli görevler düşmektedir. Uygulama geliştirme sırasında güvenliğe yönelik alınabilecek tedbirlere aşağıda yer verilmektedir.

- Uygulama geliştirme sırasında, uygulamanın geliştirildiği platformun sahip olduğu en son güvenlik tedbirleri bilinerek uygulamalar geliştirilmedir.
- Uygulamanın geliştirildiği platformlardaki güvenlik değerlendirme araçları kullanılarak uygulamanın güvenlik seviyesi test edilmelidir.
- Ağ iletişim açıklıklarından kaynaklanan güvenlik risklerinden korunmak için uygulama geliştirici tarafından uygulamanın geliştirildiği platforma yönelik en son ağ güvenlik konfigürasyonları dikkate alınarak uygulamalar geliştirilmelidir.
- Mobil güvenlik yazılım sağlayan şirketlerin araçları kullanılarak uygulamaların güvenlik seviyeleri analiz edilmelidir.
- Uygulamaların işletim sistemlerinin en son versiyonlarındaki güvenlik mimarisine uygun olması sağlanmalıdır.

Bununla birlikte, uygulama tabanlı tehditlere kaşı gerekli savunma tedbirlerinin alınması gerekmektedir. Uygulama tabanlı tehditleri bertaraf etmek için kullanılan savunma yöntemleri ve bunların fonksiyonlarına Tablo 11.3'de yer verilmektedir.

Tablo 11.3. Savunma yöntemi ve koruma fonksiyonu [8]

Savunma	Tanımlama	Koruma	Tespit	Karşılık Verme
Uygulama geliştirmede en iyi örneklerin takip edilmesi	Android için Google, IOS için Apple tarafından yayınlanan en iyi güvenlik örneklerinin uygulanması konusunda geliştiricilerin eğitilmesi.	x		
Kullanıcı güvenliğinde en iyi örneklerin takip edilmesi	Kullanıcılar, uygulamaların ve işletim sisteminin güncel olduğundan emin olmalıdır. Güvenliğin sağlanmasında güncellemelerin vakit kaybetmeden yapılması önemlidir. Ayrıca, yetkisiz uygulama marketlerinden uygulama indirilmemelidir.	x		
Güvenlik inceleme araçlarının kullanılması	Mobil uygulamaların zayıf noktalarının ve potansiyel zararlı davranışlarının belirlenebilmesine yönelik uygulama güvenliği analiz programlarının kullanılması.	x	x	x
Cihaza entegre izolasyon teknolojisi	Kuruluşlar tarafından zararlı kişisel uygulamalar ve işletmeye yönelik uygulamalar arasında bir ayrım yapılması.	x		
Band dışı kimlik doğrulama	Kötücül yazılımların hassas bilgilere erişimin engellenmesi için güçlü kimlik doğrulama sistemleri kullanılabilir.	x		
Sürekli kimlik doğrulama	Genellikle prototip aşamasında, sürekli kimlik doğrulaması kötücül kullanıcıları veya uygulamaları engeller.	x		
Mobil cihaz yönetimi/ Kurumsal mobilite yönetimi	Zararlı uygulama davranışlarını engellemeye yardımcı olmak amacıyla kullanılan yönetim sistemleri.	x	x	x
Cihaz üzerinde üçüncü parti güvenlik çözümleri	Üçüncü parti güvenlik uygulamaları diğer uygulamaların ağ kullanımı veya bunların hassas kaynaklara erişim durumunu izlemeye yardımcı olur.	x	x	x
Ağ izleme	Bununla yetkisiz veya bilinmeyen noktalara hassas bilgilerin iletimi tespit edilebilir.		x	
Uygulama marketlerinde tehlike azaltma	Apple ve Google uygulama marketlerinde uygulamalara yönelik güvenlik risklerini bertaraf edici tedbirlerin alınması	x	x	x

Saldırı türleri zaman içerisinde değişiklik göstermiştir. Bununla birlikte, her bir saldırı türünün kullandığı zayıflık, saldırının etkisiz hale getirilmesi için uygulanacak çözüm ve saldırının etkisi farklılık göstermektedir. Tablo 11.4 ve Tablo 11.5'de, mobil cihazlara yönelik sırasıyla eski tip ve yeni tip saldırı türleri, zayıf noktaları ve bunlara yönelik uygulanan çözüm yöntemlerine yer verilmektedir.

Tablo 11.4. Eski tip saldırlar ve önlemler [20]

Saldırı İsmi	Zayıf Noktalar	Çözüm	Etkisi
Fiziksel Saldırı	Sistem eksikliği/hatası	Yazılımın veya donanımın yeniden üretimi	Mobil telefonun güvenliğini zayıflatır. Anormal davranışlar.
	Yetersiz API Yönetimi	Güvenilir uygulama form kaynaklarının kullanımı.	Kötücül kodlar, kullanıcının verisini veya dosyalarını etkileyebilir.
Radyo iletişimi saldırıları	Gizle dinleme ve kandırma	Kablosuz bağlantının birdenbire kesilmesi.	Veri kolaylıkla ele geçirilebilir. Bilgisayar güvenliği zayıflatılabilir.
	Güvensiz kablosuz ağ	Sadece güvenilen kablosuz ağların kullanımı. Güvenli iletişim için şifreli kanalların kullanımı.	İletişim sırasında bilgiler ele geçirilebilir.
Arkakapı	Sistem açıklıkları	Cihazın güncellenmesi ve güçlü antivürus programlarının kullanımı.	Akıllı telefonun güvenliği zayıflatılabilir. Virüsler için bir arkakapı oluşturulabilir.
Virus	Hedef bulma, bilinmeyen kaynak ile dosya kopyalama	Sisteme güncel antivirüs programının kurulması	Uygulamaların anormal davranışlar göstermesi. Bilgilerin ve uygulamaların bozulması.
Solucanlar	Bilgi transferi, kötücül programların transferi	Güncel antivirüs programı kullanımı.	Siber saldırganlar için arkakapı oluşturabilir.
Kötücül yazılımlar	İlgilenilen kaynaktan dosya indirilmesi	Güncel antivirüs programı kullanımı, kötücül yazılım engelleme uygulaması kurulumu. Sunucu tabanlı kötücül yazılım tespit sistemi kullanan sistemlerden uygulama indirme.	Cihazın işleyişinin bozulması. Hassas bilgilerin toplanması.
Trojan	Güvenilmeyen kaynaklardan uygulama indirme, gizli kötücül fonksiyonlar.	Akıllı telefonlara özel saldırı tespit sistemi kullanımı. Antivirüs programı kullanmak.	Cihazın işleyişinin bozulması. Hassas bilgilerin toplanması.
SPAM	E-posta veya MMS yoluyla kötücül kodların transfer edilmesi.	Bu türden E-posta veya MMS'lerin açılmaması. Sadece özgün hizmetlerin ve uygulamaların kullanılması.	Posta kutusunun saçma postalar ile dolması. İnternet hızının azalması. Kontak listesindeki bilgilerin çalınması.
Tehdit	Yanıltıcı e-posta, bilgilerin ifşa edilmesi	Siber tehdit yönetim yazılımı kullanımı.	Verilerin bozulması, bilgisayar güvenliğinin zayıflaması. Güvenli ağlarda arka kapıların oluşturulması.

Tablo 11.5. Yeni tip saldırılar ve önlemler [20]

Saldırı Adı	Zayıf noktalar	Çözüm	Etki
Röle saldırısı	Güvensiz ağ ortamı, yetkisiz Proxy servislerinin kullanımı	Güvenli ağların ve Proxy uygulamalarının kullanımı.	İletişim sırasında bilgilerin ele geçirilmesi (hacklenmesi)
Cold Boot saldırısı	RAM ve şifreleme/şifre çözme anahtarlarına yetkisiz erişim.	Anahtar verilerini RAM yerine chip üzerinde tutan sistemlerin kullanımı. Güçlü şifreleme ve şifre çözme yöntemlerinin kullanılması.	Şifreleme anahtarı ele geçirilebilir (hacklenebilir). Bilgi güvenliğini zayıflatır.
Kaba kuvvet saldırısı	Telefon parolasının kırılması için parola kombinasyonlarının ardı ardına denenmesi.	Parola denemesine limit konulması.	Parolanın kırılması, CPU hızının düşmesi
Smudge saldırısı	Dokunmatik ekranın kirli veya yağlı elle tutulması.	Cihazın ekranının temiz tutulması ve temiz elle cihaz dokunulması.	Parola paterninin kolaylıkla tahmin edilmesi.
DoS saldırısı	Diğer cihazların kullanımı ile mobil geniş band bağlantının düşürülmesi. Sahte Wifi bağlantısı ile bağlanma.	İnternet erişim yetkilendirme protokolü kullanımı.	Ağın meşgul olması. Akıllı telefonun meşgul edilmesi ve hizmetlerin bloklanması.
XSS saldırısı	Bir uygulamaya veya yazılıma yerleştirilen HTML 5 tabanlı kötücül kodlar.	Popüler ve özgün uygulamaların kullanımı. Uygulamaların zayıflıklarının tespit edilmesi için tarama araçları kullanımı.	Akıllı telefona kötücül kodların bulaşması Bilgilerin elegeçirilmesine (hacklenmesine) ve arka kapılar açılmasına neden olur.
SMS tabanlı saldırlar	Saldırgan oltalama linklerinin reklamını yapabilir.	Mesaj ayalarında düzenleme yapılarak cihaz korunabilir.	Hassas bilgilerin ele geçirilmesi.
USSD Saldırıları	Bilinmeyen aramalar, mavi ekran korsanlığı	Anomali tabanlı saldırı tespit sistemi kullanımı	Kişisel bilgiler çalınabilir. Akıllı telefon zarar görebilir.
USB bağlantı saldırıları	Root erişimi	Saldırgan olmayan şarj istasyonlarının kullanımı.	Hassas bilgilerin çalınması. Her hangi bir kötücül yazılımın kolaylıkla bulaşabilmesi.
ABD saldırısı	Açıklık komut işlemci aracı	Geriye doğru dilimleme, statik analizör ve dizin analizör kullanımı.	Hassas bilgilerin çalınması.
Kamera tabanlı saldırılar	Kötücül program, yetkisiz kaynaklar.	Casus kamera desteği, etkin erişim kullanımı.	Akıllı telefon güvenliğinin zayıflatılması. Bilgilerin çalınması.
Kontrol akış saldırıları	Kod yerleştirme, hafızada veri taşması	Mobil kontrol akış bütünlük çerçevesi kullanımı.	Kullanıcının SMS veya kontak veri tabanının ele geçirilmesi, hafıza bozulmasının istismar edilmesi.

Kişisel mobil cihazlarda siber tehditlere karşı tedbir almak için yapılabilecekler aşağıdaki gibi sıralanabilir:

- Kesinlikle mobil cihazlar için özel geliştirilmiş ve sürekli güncellenebilen bir anti-virüs programı kullanılmalıdır. (CHOMAR anti-virüs programı hem ücretsiz hem de yerli olması sebebiyle tercih edilebilir.)
- Mobil cihaza erişim için kesinlikle güçlü bir parola oluşturulmalı, cihaz belirli bir süre kullanılmadığı durumlarda otomatik olarak kilitlenecek şekilde ayarlanmalıdır.
- İşletim sisteminin ve yüklenen uygulamalara ait yazılımların güncellemeleri sürekli takip edilmeli ve uygulanmalıdır.
- Uygulama yüklerken uygulamanın talep ettiği izinler dikkatle incelenmeli, uygulamanın çalışmasına fonksiyonel olarak etki etmeyeceğini düşündüğünüz izinler talep ediliyorsa mümkün ise o uygulama tercih edilmemeli ya da o izinler verilmeden yükleme yapılmalıdır.

- Kaynağı bilinmeyen adreslerden ve numaralardan gelen e-posta, SMS veya bunlarla birlikte gelen linkler açılmamalı ve tıklanmamalıdır.
- Web sitelerinde kişisel bilgileriniz istenildiğinde bu bilgileri girerken iki kere düşünülmeli, istenen bilgilerin gerçekten gerekli olup olmadıkları ve web sitesinin güvenilirliği sorgulanmalıdır.
- Güvenirliğinden emin olunmayan uygulamalar yüklenmemelidir. Güvenilirliğinden şüphe edilen uygulamalar muhakkak yüklenmek isteniyorsa öncesinde çeşitli güvenlik uygulamalarında taratılmalı, mümkünse sanal bir telefon üzerinde ilk yükleme yapılarak uygulamanın davranışı dinamik olarak incelenmelidir.
- Telefonun dış dünya ile bağlantısını sağlayan Wi-Fi, bluetooth, kızılötesi gibi işlevler sadece gerekli olduğunda aktif hale getirilmelidir. Gizlilik ayarları sadece istenen kişiye görünecek şekilde ayarlanmalıdır.
- Güvenilmeyen, herkese açıklık kablosuz ağlara bağlanırken iki kere düşünülmelidir.

- Cihazınızın çalınma ve kaybolmalara karşı çeşitli uygulamalar ile takibi yapılacak şekilde ayarlanmalıdır. Böylelikle cihazın harita üzerinde konumu görülebilmektedir.
- Her ne şekilde olursa olsun, mobil cihazların sahibinin rızası dışında elden çıkması durumlarında kullanıcılar telefonla Bilgi Teknolojileri ve İletişim Kurumunun Bilgi ve İhbar Merkezine bilgilendirmede bulunarak cihazlarının şebeke hizmeti almasının engellenmesini sağlamalıdır.

11.7. Değerlendirmeler

Akıllı telefonlar çoklu görevleri yerine getirebilen taşınabilir cihazlardır. Bu cihazlarda fonksiyonelliği artırmak için çok sayıda üçüncü taraf uygulamalar kullanılmaktadır. Bununla birlikte akıllı telefonlar kişisel bilgisayarlardan farklı bir yapıya sahiptir. Benzer şekilde, akıllı telefonların kötücül yazılımlardan korunma çözümleri kişisel bilgisayar veya diğer bilgisayar servislerinden farklılık göstermektedir. Akıllı telefonlar, kişisel bilgisayarlar ile karşılaştırıldığında pil ömrü ve işlemci gücü açısından yetersiz kaynağa sahiptir. Akıllı telefonların kapasitesinin artması ile birlikte, bu özellikler siber korsanlar tarafından kötücül amaçlar için kullanılmaya başlanmıştır.

Mobil cihazların dünyada yaygın kullanımı, beraberinde birçok güvenlik riskini de getirmiştir. Mobil ekosistem içerisinde yer alan mobil cihazlar ve mobil uygulamalar siber güvenlikte en önemli bileşenleri oluşturmaktadır. Genellikle siber saldırganlar tarafından mobil uygulamalar kullanılarak mobil cihazlara karşı saldırılar gerçekleştirilmektedir. Mobil cihazlara yönelik yapılan siber saldırılarda kişisel ve finansal bilgilerin ele geçirilmesi ana hedefi oluşturmaktadır. Yapılan araştırmalarda mobil cihazlara yönelik siber saldırıların %60'ından fazlasının ekonomik fayda sağlamak amacıyla yapıldığını ortaya koymaktadır.

Mobil kötücül yazılımların tespitinin yapılabilmesi ve bunlara karşı önlem alınabilmesi siber güvenlik risklerinin azaltılmasında önemli bir konu olarak karşımıza çıkmaktadır. Literatürde, kötücül yazılım tespitinde statik, dinamik ve hibrit analiz yöntemleri yaygın olarak kullanılmaktadır. Bununla birlikte, yapay zeka uygulamalarının gelişmesi kötücül yazılımların tespitini güçleştirmiştir. Yapay zeka

özellikleri barındıran kötücül yazılımların tespitinde akıllı analiz çözümleri kullanılmaya başlanmıştır. Makine öğrenme teknikleri bu kapsamda ele alınmaktadır. Makine öğrenme tekniklerinin kullanımı ile kompleks yapıya sahip kötücül yazılımların yüksek doğrulukla analiz edilebilmesi mümkün olmuştur.

Diğer taraftan, mobil cihazlarda siber güvenliğin sağlanmasında farklı açılardan alınabilecek tedbirler bulunmaktadır. Bu tedbirlerin mobil cihaz üretimi, uygulama geliştirme ve kullanıcı seviyesi olmak üzere farklı seviyelerde ele alınması gerekmektedir. Her seviyede, ilgili olduğu paydaşlar taraflarından gereken tedbirlerin alınması güvenlik risklerinin bertaraf edilebilmesi açısından büyük önem arz etmektedir.

Güvenliğin her türlüsünde olduğu gibi mobil cihaz güvenliğinde de en zayıf halkanın insan faktörü olduğu unutulmamalıdır. Kullanıcı düzeyinde, mobil cihaz kullanıcılarının güvenlik konusuna gereken hassasiyeti göstermediği görülmektedir. Özellikle mobil uygulamalar yüklenirken kurulum sırasında istenen izinlerin ne için istendiği ve verilen izinler sonucunda ne tür risklerin alındığı kullanıcılar tarafından dikkate alınmalıdır. Mobil cihazlara yönelik siber güvenlik risklerinin azaltılmasında kullanıcıların konuya olan farkındalığının artırılması büyük önem taşımaktadır. Kullanıcı bilinç düzeyinin artırılması ile güvenlik risklerinin azaltılmasında önemli aşamalar kaydedilebileceği değerlendirilmektedir.

Kaynaklar

[1] Anonim,http://www.dijitalajanslar.com/internet-ve-sosyal-medya-kullanici-istatistikleri-2017/, (Son Erişim Tarihi: 16.08.2018).

[2] Anonim, https://webrazzi.com/2017/05/23/akilli-telefon-satislari-2017nin-ilk-ceyreginde-yuzde-9-artti/, (Son Erişim Tarihi: 16.08.2018).

[3] Razak, M.F., Anuar, N.B., Salleh, R., Firdaus, A.,"The rise of malware: bibliometric analysis of malware study", Journal of Network and Computer Applications 75, pp. 58-76, Elsevier, 2016.

[4] GSMA, Global Mobile Trends, Eylül 2018.

[5] Google, Mobile Operating Systems Market Share (Son erişim: 23.09.2018)

[6] Anonim, https://www.statista.com/statistics/271496/global-market-share-held-by-smartphone-vendors-since-4th-quarter-2009/ (Son erişim: 23.09.2018)

[7] Anonim, https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/ , (Son erişim: 23.09.2018)

[8] US Department of Homeland Security, Study on Mobile Device Security Report, Nisan 2017.

[9] Milosevic, N., Dehghantana, A., Choo, K.K.R.,"Machine learning aided android malware classification", Computers and Electrical Engineering Journal, Elsevier, 2017.

[10] Alkhateeb, E.M.,"Dynamic Malware Detection using API Similarity", 2017 IEEE International Conference on Computer and Information Technology.

[11] Polla M.L., Martinelli F., Sgandurra D., A Survey on Security for Mobile Devices, IEEE Communications Surveys&Tutorials, 2012.

[12] Dawson M., Wright J., Omar M., Mobile Devices: The Case for Cyber Security Hardened Systems, Selected Works, Ocak 2016.

[13] Damopoulos D., Kambourakis G., Gritzalis S., iSAM: An iPhone Stealth Airborne Malware, http://www.icsd.aegean.gr/publication_files/conference/462488002.pdf (Son erişim: 22.09.2018)

[14] Yao M.L., Chuang M.C., Hsu C.C., The Kano model analysis of features for mobile security applications, Elsevier, Computer&Security 78, 336-346, 2018.

[15] Vasco J.V., Best Practices in Mobile Security, Biometric Technology Today, Mart 2016.

[16] Pang J.H.J., Chua C.L., Chan G.H., Lim S.L., Challenges in Mobile Security, DSTA Horizon, 2016.

[17] Şenol, S.K., "Mobil Akıllı Cihazlar İçin Zararlı Yazılım Uygulamaları ve Güvenlik Çözümleri" Gazi Üniversitesi Fen Bilimleri Enstitüsü Elektrik-Elektronik Mühendisliği Anabilim Dalı, Doktora Tezi, Ocak 2018.

[18] GSMA, Safety, privacy and security across the mobile ecosystem: key issues and policy implications, 2017.

[19] Dua L., Bansal D., Taxonomy: Mobile Malware Threats and Detection Techniques, CS&IT CSCP 2014, pp. 213-221.

[20] Zaidi, S.F.A., Shah M.A., Kamran M., Javaid Q., Zhang S., A Survey on Security for Smartphone Device, International Journal of Advanced Computer Science and Applivations, Vol. 7, No:4, 2016.

[21] Anonim, https://www.welivesecurity.com/2016/11/01/history-mobile-malware-cabir-sms-thief/ (Son erişim: 22.09.2018)

[22] Niemala J., Symbian Malware What it is and How handle it, F-secure Coorpartion, http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Niemela/BH-Fed-06-Niemela-Symbian.pdf (Son erişim: 22.09.2018)

[23] Anonim, http://malware.wikia.com/wiki/Ikee , (Son erişim: 23.09.2018)

[24] Anonim, https://securelist.com/zeus-in-the-mobile-for-android-10/29258/, (Son erişim: 23.09.2018)

[25] Anonim, https://www.webopedia.com/TERM/D/droiddream.html, (Son erişim: 23.09.2018)

[26] Anonim,https://www.symantec.com/security-center/writeup/2013-060301-4418-99 , (Son erişim: 22.09.2018)

[27] Nokia Security Center Berlin, Nokia Threat Intelligence Report, 2016.

[28] Anonim, https://www.securityweek.com/xbot-android-trojan-steals-banking-info-encrypts-devices , (Son erişim: 23.09.2018)

[29] Anonim, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/, (Son erişim: 24.09.2018)

[30] Anonim,https://securelist.com/it-threat-evolution-q2-2018-statistics/87170/ , (Son erişim: 23.09.2018)

[31] Popov, I.,"Malware detection using machine learning based on word2vec embeddings of machine code instructions", 2017 SSDSE, IEEE, 2017.

[32] Damodaran, A., Troia, F. D.,Corrado,V. A., Austin,T. H., Stamp, M.,"A Comparison of Static, Dynamic, and Hybrid Analysis for Malware Detection", Journal of Computer Virology and Hacking Techniques, pp. doi:10.1007/s11416-015-0261-z, 2015.

[33] Li, Q., Li, X.,"Android malware detection based on static analysis of characteristic tree", Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 84-91, 2015.

[34] Schmith, A., Clausen, J., Camtepe, A.,"Detecting symbian OS malware through static function call analysis", Proceeding 4th International Conference malicious and unwanted software, pp. 15-22, 2009.

[35] Shen, T, Zhongyang Y., Xin, Z., Mao, B., Huang, H.,"Detect android malware variants using component based topology graph", 2014 IEEE 13th International Conference on Trust, Security and Privacy in computing and communications, pp. 406-413, 2014.

[36] Wang, W., Wang, X., Feng, D., Liu, J., Han Z., Zhang, X.,"Exploring permission induced risk in android applications for malicious application detection", IEEE Trans. Inf. Forensic Security, pp. 1869-1882, 2014.

[37] Moser, A.,Kruegel, C., Kirda, E.,"Limits of static analysis formalware detection", IEEE Computer security applications conference, ACSAC 2007. Twenty-third annual,pp. 421–430, 2007.

[38] Kabakuş, A.T., Doğru, İ.A., Çetin, A., "Android kötücül yazılım tespit ve koruma sistemleri" Erciyes, Fen Bilimleri Enstitüsü Dergisi, 31(1):9-16, 2015.

[39] Utku, A., Doğru, İ.A., Android kötücül yazılımlar için izin tabanlı tespit sistemi, Gazi Üniversitesi MMF Dergisi, 2017

[40] Willems, C., Holz, T., Freiling, F.,"Toward automated dynamicmalware analysis using cwsandbox", IEEE Security & Privacy, vol. 5,no. 2, 2007.

[41] Balaji, B., Ralusca, A., "A study of android malware detection techniques and machine learning", Proceedings of the 27th modern artificial intelligence and cognitive science conference, pp. 15-23.

[42] Diri B., Doç. Dr., Yıldız Teknik Üniversitesi Bilgisayar Mühendisliği, Makine Öğrenmeye Giriş, 2014.

[43] Çayıroğlu İ., İleri Algoritma Analizi-5, Yapay Sinir Ağları, Karabük Üniversitesi, Mühendislik Fakültesi.

[44] Anonim, https://en.wikipedia.org/wiki/Mobile_device_management, (Son erişim: 24.09.2018)

[45] Anonim, https://mobilemacsters.com/mdm/ , (Son erişim: 24.09.2018)

[46] Anonim, https://www.gartner.com/doc/2757817/magic-quadrant-enterprise-mobility-management , (Son erişim: 24.09.2018)

Siber Güvenlik Denetimi

BÖLÜM 12

Dr. Ahmet EFE

SİBER GÜVENLİK DENETİMİ

BT kontrollerindeki yatırımlara devam etmek, organizasyonları gittikçe daha karmaşık ve yaygın olarak kullanılan saldırı yöntemlerinden korumak için sürekli olarak gerekli hale gelmiştir. Sadece kurumsal stratejiler kapsamında değil, siber güvenlik ulusal stratejileri giderek daha karmaşık hale geldiği için buralarda konulan hedef ve faaliyetlerin de denetim birimleri tarafından denetlenmesi artık bir ihtiyaç haline gelmiştir. Kasıtlı saldırılar, ihlaller ve olaylar zarar verici sonuçlara neden olabilir. Bu kısım, genel bir çerçeve ve stratejinin bir parçası olarak uygulanan bu kontroller üzerindeki denetim değerlendirmelerine olan ihtiyacın altını çizmekte ve yönetim gözden geçirmesi, risk değerlendirmeleri ile siber güvenlik kontrollerinin BT denetimlerinde ihtiyaç duyulan müteakip güvence ve danışmanlık faaliyetlerine odaklanmaktadır. Siber güvenlik ile ilgili zafiyet, risk ve tehditlerin denetimlerde dikkate alınabilmesi için gerekli olan yaklaşım biçimi ve teknikler hakkında temel bilgiler sağlanmaktadır. Ayrıca COBIT-5 çerçevesi kapsamında siber güvenlik denetimlerinin nasıl yapılması gerektiğine dair de bir altyapı sağlamaktadır.

12.1. Giriş

Siber güvenlik, günümüzde büyük veri ihlallerinden kaynaklanan suiistimaller, tazminat ve yasal cezalar nedeniyle günümüzde birçok kuruluşun yönetim kurullarından büyük ilgi görmektedir. Kamu kurum ve kuruluşları da ulusal stratejiler kapsamında giderek artan bir oranla siber güvenlik yatırımlarına yönlendirilmektedir. Yönetim ve şirket kurullarının üst düzey yöneticileri bazı ihlallere karşı gerekli önlemlerin alınmamış olması nedeniyle pozisyonlarını kaybettiler. Buna benzer durumlardan dolayı organizasyonlar siber güvenlik önlemleri kapsamında değerli kaynaklar harcayıp müş-

terilerini ve paydaşlarını bir bütün olarak memnun etmeye çalıştılar. Organizasyonlar, ihlallerin oluşmasını engellemeye çalıştıkça altyapı harcamaları da arttı. Çünkü önleyici kontroller her zaman çok daha fazla maliyet oluşturmaktadır. Olay tespiti ve müdahale mekanizmalarındaki güvenlik teknolojisi yatırımları, olay meydana geldiğinde hasarı ve yükümlülüğü sınırlamak için tırmanmaktadır. Altyapıyı ve savunma mekanizmalarını geliştirmek için yapılan bu faaliyetler, saldırılardan korunma ve saldırılara karşı sorumlu olanlara yapılan yatırımlarda memnuniyetle karşılanabilmektedir. Bu kapsamda ülkemizin 2016-2019 Ulusal Siber Güvenlik Stratejisinde çok önemli hedefler ve faaliyetler bulunmaktadır. Ancak bunlar herhangi bir siber güvenlik programının sadece bir bileşenini temsil etmektedir.

Sorulması gereken temel sorular şu şekildedir:

- Bir sonraki güvenlik bileşenine yatırım yapmak için en uygun yer neresi ve ne zamandır?
- Doğru miktar ayrılabilmekte midir?
- Ele alınmayan risk alanları var mıdır?
- Mevcut altyapı yeterli midir?
- Bugün kullandığımız yatırımlar akıllıca mı kullanılmakta mıdır?
- Rakipler ve saldırganlar buna nasıl yaklaşmaktadır?
- Siber güvenlik stratejileri ve politikalarında belirtilen hedef ve faaliyetler etkin bir şekilde gerçekleştirilmekte midir?
- Siber güvenlik hedefleri ve faaliyetlerinde ortak çalışması gereken veya bilgi paylaşması gereken birimler arasında etkin koordinasyon yapılabilmekte midir?

Buna benzer soruların sayısı arttırılabilir. Ancak bu sorulara beklenebilecek cevaplar aşağıdaverilmiştir.

1) Mevcut ve ortaya çıkan riskleri, tahsis edilen kaynakları ve sonuçları organizasyona göre değişen yönetim ve yönetişim süreçleriyle birlikte değerlendirmek
2) Bilgi varlıklarını korumak için mevcut veya planlanmış olan güvenlik kontrollerini denetlenmek.

Resmi süreçler olmadan, aracın veya önlemin BT mimarisiyle uygun olduğu yeri anlamadan uygun olmayan program veya araçların satın alınması riski her zaman vardır.

- Önerilen her hangi bir araç veya güvenlik seti, mevcut maliyet setinin ötesinde siber güvenlik yeteneklerini mevcut araç setinin kabiliyetlerinin ötesinde yeterince geliştirebilecek mi?
- Kurumun sahip olduğu risk temelinde, para başka bir yerde daha iyi harcanmış olabilir mi?
- Mevcut araçların kabiliyetleri yeterince uygulandıktan sonra mı yeni araçlar satın alındı yoksa mevcut sistemle uyumu dikkate alınmadan alındı ve şimdi de raf mı?

Bu sorular, denetim ekibi tarafından bir kurum için riskleri değerlendirmek ve siber güvenlik kontrollerini denetlemek için bir miktar rehberlik sağlayacaktır.

12.2. Siber Güvenlik Denetiminde Amaçlar

Her denetimde olduğu gibi siber güvenlik denetimlerinin de bir amacı olmak durumundadır. Siber güvenlik denetiminin amacı, yönetimin siber güvenlik süreçleri, politikaları, prosedürleri, yönetişim ve diğer kontrollerin etkinliğinin değerlendirmesini sağlayarak yönetime sistematik ve bilimsel güvence ve/veya danışmanlık hizmeti sağlamaktır. İnceleme ve denetim siber güvenlik standartlarına, yönergelere ve prosedürlere ve bu kontrollerin uygulanmasına odaklanacaktır.

T.C. Sayıştay Başkanlığı ve Kamu İç Denetim Koordinasyon Kurulu (İDKK) tarafından hazırlanmış olan bilişim denetimlerine dair rehberler kullanılabilir. Bunlar çok sistematik ve detaylı bir yaklaşım uygulanmasına olanak sağlamaktadır. Bu bölümdeki yaklaşımımız, BT denetimlerinde kontrol listesi yaklaşımından öte, olayın felsefesini ve yöntemini anlatmak ve bunun belirlenmesine yardımcı olmaktır.

Denetim/güvence incelemesi, olay yönetim sürecinin diğer operasyonel denetimlerine, ağların ve sunucuların konfigürasyon yönetimi ve güvenliğine, güvenlik yönetimi ve farkındalığına, iş sürekliliği yönetimine, bilgi güvenliği yönetimine, BT ve iş birimlerinin yönetişim ve yönetim uygulamalarına dayanmak ve onları da değerlendirmek durumundadır.

Birincil BT güvenlik ve kontrol konuları genel olarak aşağıda belirtilen kanunları içermektedir. Bunlar;

- Hassas verilerin ve fikri mülkiyetin korunması
- Birden fazla bilgi kaynağının bağlı olduğu ağların korunması
- Cihazda yer alan bilginin varlığı, gizliliği ve sorumluluğunun temin edilmesi

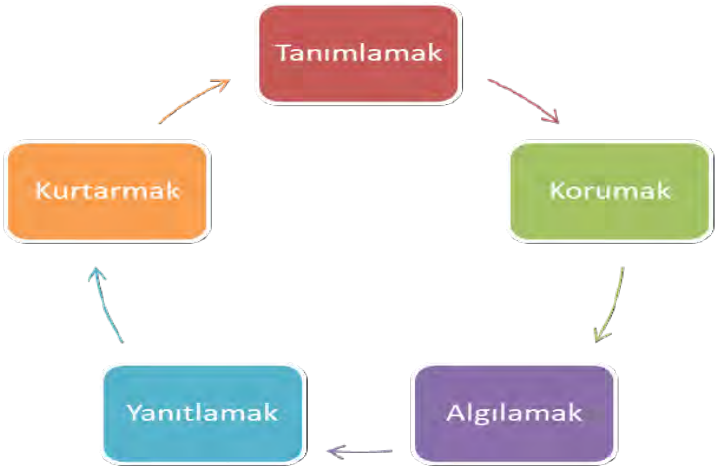
a) Denetim Amaçları

Pekçok denetim amacı tesis edilebilir. Ancak siber güvenlik ile ilgili amaçlar aşağıdaki şekilde sınırlandırılabilir:

- Siber güvenlik politikaları ve prosedürleri ve bunların çalışma etkinliği hakkında bir değerlendirme yaparak yönetime güvence sağlamak.
- Güvenlik kontrollerindeki zayıflıklar nedeniyle kurum verilerinin güvenilirliğini, doğruluğunu ve güvenliğini etkileyebilecek güvenlik kontrolü sorunlarını tespit ederek yönetime rehberlik etmek.
- Yanıt verme ve kurtarma programlarının etkinliğini değerlendirerek kurumsal yaklaşımların içselleştirilmesinde yardımcı olmak.

b) Denetim Kapsamı

BT denetimlerinin kapsamı çok daha geniş tutulabilirken siber güvenlik denetimlerinde daha kısıtlı bir kapsam söz konusu olmaktadır. Siber güvenlik denetim / teftiş / güvence programı, aşağıdaki beş kritik siber güvenlik faaliyeti üzerine kurulmuştur:



Şekil 12.1. Siber Güvenlik Yaşam Döngüsü

Denetimi gerçekleştiren denetçi, gözden geçirilecek kurumsal sistemlerin ve varlıkların kapsamını belirleyecektir. Denetim / güvence programı, farklı güvenlik gerekliliklerine sahip çeşitli iş süreçlerini, uygulamaları veya sistemleri desteklemek üzere uyarlanabilir.

c) İş Etkisi ve Risk Değerlendirmesi

Siber olay, finansal, operasyonel, yasal ve itibar etkisine sahip olabilir. Bir kuruluşun kritik altyapıdaki rolü, bir internet sitesinin potansiyel etkisini de artırabilir. Bir siber ihlalin sonuçları bakımından dikkate alınabilecek olumsuz örnekleri şunları içerebilir:

- İtibar kaybıyla sonuçlanan olumsuz tanıtım, hisse kaybı, değer düşüklüğü, itibarsızlık
- Fikri mülkiyet veya ticari sırların kaybedilmesi
- Uygunsuzluk, gizli veya tüketici kişisel bilgilerinin kaybından veya suiistimalinden kaynaklanan para cezaları, davalar ve yasal ücretler
- Adli soruşturma masrafları
- Kurum veya şirket imajını iyileştirmek için halkla ilişkiler kampanyası maliyetleri
- Siber güvenlik kontrollerini azaltmak ve iyileştirmek için teknoloji geliştirme maliyetleri
- Zaman ve verimlilik kaybı

Dolayısıyla bir siber güvenlik denetiminde siber ihlallerin iş süreçlerine etkileri kapsamında risk değerlendirmesi yapılması büyük önem arz etmektedir.

d) Gerekli Asgari Denetim Becerileri

BT denetim ve güvence uzmanı, güvenlik ve kontrol anlayışına sahip olmalıdır. Özellikle siber güvenlik denetimi yapacak olanların CISA; CRISK, CISM, CSX, CEH veya CISSP gibi temel sertifikasyonlara sahip olmalarında büyük yarar vardır. Bu çok dinamik bir alan olduğu için, bu denetimi gerçekleştiren profesyoneller, siber tehditler ve saldırıları tanımlamak, korumak, tespit etmek ve bunlara cevap vermek için siber güvenlikte kullanılan temel teknolojileri anlamak için gerekli araştırmaları yaptıklarından emin olmalıdır.

Bölüm 1 ve Bölüm 2'yi gözden geçirmenizi öneririz. Ancak, denetçinin iş stratejisi ile uyumu değerlendirmek için yeterli işlevsel ve iş bilgisine sahip da olması önemlidir.

1) Siber Güvenlik Kontrollerinin Özellikleri

Her kuruluş, organizasyonun risk duruşuna özgü kontroller tasarlamalı ve süreçleri ve insanların sürekli olarak kontrolleri yönetecek şekilde olmasını sağlamalıdır. Kontrol sorunları tipik olarak teknolojinin başarısızlığından kaynaklanmaz, ancak daha çok, süreci yürütmeyen veya kötü tanımlanmış bir süreci kullanan bireylerin sonucudur. Yönetimsel, teknik ve operasyonel kontroller, temel olarak Bilgi Güvenliği için COBIT® 5 gibi birçok yerden temin edilebilir [1]. Herhangi bir siber güvenlik programının temel hedeflerinden biri, saldırganın çekiciliğini sınırlamak olmalıdır. Bilgisayar korsanlığı, script kiddie tehdidi sahnesinin çok ötesine geçti ve bir saldırganın bir sisteme nüfuz etmesi için gereken süre, hedefin o kadar az arzu edilir hale gelmesidir.

Siber güvenlik ile ilgili kontrol yatırımları, insanlara, süreçlere, teknolojiye ve güvenlik odaklı bir kültüre yönelik teknik, idari ve operasyonel yatırımlar yoluyla organizasyon genelinde yapılmaktadır. Kurumsal ölçekte yapılan yatırımları değerlendirebilmek için hangi kategorilerde ne tür yatırımlar yapıldığının tespit edilmesi gereklidir. Bu yatırımlar şunları içerebilir:

- Farkındalık yatırımı
- Politika ve düzenleme yatırımı
- Saldırı Tespit Sistemleri
- Olay günlüğü ve loglama
- Olay yanıtı
- Güvenlik açığı taraması
- Bilgi varlık sınıflandırması
- İleri zeka ve analitik
- Mimari ve teknoloji güçlendirme
- Tahkim edilmiş BT sistemleri

a) Farklı Siber Güvenlik Kontrol Çerçevelerinden Yararlanma

Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) Özel Yayını (SP) 800-53 Revizyon 4, Federal Bilgi Sistemleri ve Organizasyonları için

Güvenlik ve Gizlilik Kontrolleri gibi siber güvenlik kontrol ortamlarının belirlenmesi için birçok yaklaşım mevcuttur [2]. NIST 800-53 SP'nin amacı, federal hükümetin yürütme kurumlarını destekleyen bilgi sistemleri için güvenlik kontrollerinin seçilmesi ve belirlenmesi için kılavuz sağlamaktır. Küresel ölçekte NIST modeli genel kabul görmüştür. NIST modeli, COBIT® 5 modelinin aksine, doğası gereği çok belirleyicidir ve birçok kuruluşa karşı çok büyük olabilir. SP 800-53 çok detaylı tanımlar içerir ve en iyi şekilde, kapsamlı siber güvenlik sürecini destekleyen COBIT 5 uygulamalarını gerçekleştirmek için organizasyonlara özgü detaylı etkinlikleri tamamlayıcı ve geliştirmeye yardımcı olabilir.

ABD İnternet Güvenliği Merkezi (CIS), siber saldırıların riskini azaltmak için önceliklendirilmiş bir dizi siber güvenlik uygulaması sağlamak için kritik kontrolleri teşvik etmektedir [3]. Bunlar, teknik tabanlı kontrollerdir - örneğin yetkili ve yetkisiz cihazların doğru stoklarının mevcut olmasını sağlama gibi yapılandırmalar oluşturulur, güvenlik açıkları değerlendirilir ve giderilir ve yönetimsel ayrıcalıklar kontrol edilir - daha yüksek düzeyde kontrol önemi ile önceliklendirilir. Bu kontroller, NIST SP 800-53 kontrollerinde olduğu gibi, ihtiyaç duyulan süreçleri ve uygulamaları desteklemek için detaylı aktivitelerin oluşturulmasında yararlıdır, fakat doğru siber güvenlik faaliyetlerinin verimli ve etkin bir şekilde gerçekleştirilmesini sağlamak için COBIT 5 işlem etkinleştiricileri gereklidir. Bu yapılar sadece CIS Kritik Kontrolleri kullanılarak kolayca anlaşılamaz.

Uluslararası Standardizasyon Örgütü (ISO) Uluslararası Elektroteknik Komisyonu (IEC) 27001, Bilgi teknolojisi — Güvenlik teknikleri — Bilgi güvenliği yönetim sistemleri — Gereksinimler [4] ve Bilgi Güvenliği için İyi Uygulama Standardı Bilgi Güvenliği Forumu Standardı [5] beş temel sürecin tamamlanması için kullanılabilir.

Bilgi Güvenliği çerçevesi için COBIT 5 etki alanları. Bu standartlardaki ilgili rehber, NIST SP 800-53 kontrolleri ile birlikte, Bilgi Güvenliği ekleri için COBIT 5'teki COBIT 5 çerçevesine eşlenmiştir. COBIT 5 çerçevesinin ve ilgili süreçlerin kullanılması, siber güvenlik faaliyetlerinin yönetilmesinden ve planlanmasından programın devam eden operasyonuna ve ölçümüne kadar, siber güvenlik kapsamının yeterli olduğu kapsayıcı yönetişim ve yönetim güvencesini sağlar.

Ülkemizin Siber Güvenlik Ulusal Stratejisinde herhangi bir model kullanılıp kullanılmayacağı ile ilgili olarak herhangi bir hedef, sorumluluk ve faaliyet öngörülmemiştir. Bu nedenle bu kapsamda COBIT-5 çerçevesinin uygulanması iş süreçleri ile entegre olarak uygulanabilir bir siber güvenlik stratejisinin hayata geçirilmesine olanak sağlayabilir.

b) Uygulama Kontrolleri

İşlem ölçeğinde düşük olan kuruluşlar bile, ilk savunma hattı olarak gerekli olan kontrolleri sıklıkla uygulamışlardır, ancak söz konusu çerçevelerin dikkatli bir şekilde tanımlanması ve uygulanmasıyla uygulamayı planlamamış olabilir. Örneğin, bir güvenlik duvarı, antivirüs yazılımı, şifre oluşturma ve yedeklemeler hakkında sınırlı bir kullanıcı eğitimi almış olabilirler. Bu kontrollerin herbiri bilgi varlıklarını korumak için bir amaca hizmet eder. Bununla birlikte, aynı düşük olgunluktaki organizasyon, güvenlik duvarı kurallarının düzenli olarak güncellenmesini, antivirüs yazılımının tüm iş istasyonlarına yüklenmemesini veya en son imzaları içermemesini veya izinli son kullanıcıların güvenliklerini kaçırmasını sağlamaya yeterli dikkat göstermemiş olabilir. Bu nedenle, kontroller yürürlükte gibi görünse bile, bu süreçlerin iyi tasarlandığından ve doğru bir şekilde yürütüldüğünden emin olmak için kuruluş düzenli olarak bağımsız denetimlerde bulunmalıdır.

c) Kontrollerin Raf Ömrü

Kontroller, tehdit ortamını dikkate alarak BT işletim altyapısını korumak için uygulanmaktadır. Genelde bir kontrol tesis edildikten sonra gelişen teknoloji ve yenilikçi ortamda değişkenlik göstererek tehdit ve risk algı ve iştahına göre periyodik olarak gözden geçirilmemektedir. Bu bazı kurumlarda ciddi bir eksiklik olarak dikkate alınabilir.

Bulut, mobil, nesnelerin interneti (IoT), büyük veri, güvenlik analitiği ve bilginin yeni yerini ele almak için yeni kontrol sınıflarına olan ihtiyaç gibi tehdit ortamları değiştikçe, kontroller de değişmelidir. Bu kontroller üzerindeki denetimler de değişmek durumundadır. Çünkü geçmişte gerekli olmayan kontrolleri ele almak için yeni alanların denetlenmesi (yani, bir bulut uygulamasına yönelik yedekleme stratejisinin veya bir mobil cihazdaki şifre kontrollerinin denetlenmesi) gerekir. Önceki denetimlerde yönetim tarafından bir

kez kabul edilen eksiklikler, yeni yasalar ve yönetmelikler veya veri miktarındaki büyümeye müteakip kurum için daha fazla riskin artması nedeniyle artık kabul edilemeyecektir.

2) Siber Savunma ve Değerlendirme Süreçleri Çoklu Hatlar

Denetim ve gözden geçirme evreni, her biri siber güvenlik programının genel güvencesine katkıda bulunan üç savunma adımına sahiptir. Bu adımlar; yönetim, risk yönetimi ve denetim olarak belirlenmektedir.



Şekil 12.2. Siber Savunma Adımları ve Genel Uygulamalar

Bu savunma adımları yönetim, risk yönetimi ve iç denetimdir (bkz. Şekil 12.2). Güvenlik duvarı kurallarının belirlenmesi gibi çok teknik kontroller, bir kontrol değerlendirmesinin (ilk seviye yönetimi), yüksek değerli bir varlığın risk değerlendirmesinin bir parçası olarak gözden geçirilebildiği (ikinci ve üçüncü seviye) gibi, makul güvence sağlanabilir. Bu denetimlerin ve gözden geçirmelerin bağımsız işlevler tarafından gerçekleştirilmesi, kontrol zayıflıklarının tespit edilme olasılığını arttırır ve daha fazla kontrol ve denge sağlar.

a) Yönetimin Gözden Geçirilmesi

Kurumsal düzeyde ilk siber savunma hattı olarak, kurum genelinde yönetimin siber güvenlik kontrollerinin mevcut ve etkin bir şekilde yürütülmesini sağlama konusunda bir çıkar çatışması olmadığını

güvenceye alması gerekir. Sorumluluk ve hesap verebilirlik genellikle kontrol öz değerlendirmeleri (CSA), saldırı ve ihlal sızma testleri, fonksiyonel ve teknik testler, sosyal / davranış testleri ve yönetim değerlendirmeleri gibi çeşitli test faaliyetlerini yürütmek üzere üst yönetimin dahliyle sağlanabilir. Üst yönetimin bu süreçlere önem vermesi gerekir. Bu süreçlerin her biri, tasarımın ya da kontrolün devam eden uygulamasında kontrol zayıflıklarını veya eksikliklerini tanımlamak için tasarlanmış iş süreçlerinin bir parçası olarak düşünülmelidir. Çünkü siber güvenlik süreçleri kendileri için bir değer ifade etmezlerken iş süreçleri ve kurumsal amaçların gerçekleştirilmesine hizmet etmektedir. Bu nedenle de iş süreçleriyle entegre bir şekilde işletilmeli ve iş süreç sahiplerinin öngörü ve ihtiyaçları dikkate alınmalıdır.

Farklı satıcılar tarafından sağlanan hizmetlerin tercih edilip edilmeyeceği veya neden tercih edileceği gibi hususlar yönetim açısından önem arz etmektedir. Bulut hizmetlerinin yaygınlığı ve şirket iş/pazar çevrelerimin ötesindeki verilerin artmasıyla birlikte, pekçok kuruluş, bilgi varlıklarının korunmasıyla ilgili bir miktar rahatlık sağlamak için üçüncü taraf satıcılarına danışmaktadırlar. Satıcılar için teklif isteme (RFP) süreçleri de ISO/IEC 27001, Tasdik Çatışmaları Standartlarına İlişkin Tablolar (SSAE) Hizmet Organizasyonu Denetimi (SOC) tipi raporlar, [6] ve üçüncü taraf standartlaştırılmış satıcı güvenliğine uygunluklarını belirten raporlar talep edilebilmektedir.

b) Siber Güvenlik Risk Değerlendirmesi

Yönetim, nihai olarak organizasyon için yapılan risk kararlarına sahiptir. Bunlar siber güvenlik görevlisi (CSO) ve kurumsal yönetimin risk yönetim süreçleri aracılığıyla alacağı uygun yöne ilişkin rehberlere dayanan kararlar olmalıdır. Risk, şirketin operasyonel alanlarında bulunur ve uygulanan kontroller kurumsal varlıkların korunmasını desteklemelidir. İşletme yöneticisinin, bölümün iş faaliyetlerini sürdürmesi için gerekli olan gizlilik, bütünlük ve erişilebilirlik (CIA) kontrollerinin seviyesinin nasıl belirleneceği konusunda yönlendirilmesi gerekmektedir. Şirketler, ayrıntılı, nicel bir yöntemden daha düşük bir maliyetle yeterli bir risk ölçümü sağlayabilecek niteliksel bir risk değerlendirme sürecinden yararlanabilir. Kantitatif yöntemler, riskle ilgili kesin ölçümlerin veya parasal miktarla-

rının görünümünü sağlayabilir, ancak bu hesaplamalar genellikle çok hassas olmayan sübjektif olasılık ölçütlerine dayanır. Yönetim, yüksek / orta / düşük veya kırmızı / sarı / yeşil gibi hashboard veya heatmap gibi çeşitli isimlerle adlandırılan grafikleri ayrıntılı matematiksel formüllere göre daha kolay anlayabilir ve yorumlayabilir. Bu nedenle birçok kurum uzman, görüşüne dayanan niteliksel bir yaklaşım kullanmaktadır. Herhangi bir risk değerlendirmesindeki amaç, risk değerlendirmesinin daha kolay anlaşılması için riskin durumunu bildirmektir. Risk değerlendirme yaklaşımları tipik olarak aşağıdaki yapıları kullanarak çevreyi incelemeyi içerir.

c) Sistemin Kapsamını Belirlemek

Siber güvenlik sisteminin sınırları ve CIA[1] gereklilikleri bilinmelidir. Risk değerlendirmesinde yer alan sistem ve veriler, halihazırda sistem içerisinde faaliyet gösteren belgelendirilmiş bir ticari amaca, teknik şartnameye ve kontrollere sahip olmalıdır. Bu gereksinimleri anlamak ve bunun CIA gerekliliklerine göre düşük, orta veya yüksek bir sistem olup olmadığını, risk değerlendirmesi için sistemin çerçevelenmesine yardımcı olacaktır. Sistemin doğru şekilde düzenlenememesi, kritik varlıkların güvenlik korumalarından çıkarılmasına neden olabilir.

d) Tehditleri Tanımlamak

Tehditler, hasarı önlemek için yeterli kontroller mevcut değilse, CIA'yı etkileme potansiyeline sahip tehlikelerdir. Bunlar, insan tehditlerinden (örn. Dikkatsizlik, insan hatası, casusluk, hassas veri ifşası, sosyal medya istismarları, sabotaj, dolandırıcılık) çevresel tehditlere (örn. Güç / ısıtma, havalandırma, klima [HVAC] dalgalanması, kablo kesintileri) kadar uzanabilir. teknik tehditlere (hırsızlık, hassas medya bertarafı, sunucu odaları, kırık su boruları, yangın), (örneğin, oturum açma, kötü amaçlı kod, yetkisiz erişim, oturum devralma, mobil medya kaybı, donanım / yazılım hatası, uzaktan erişim).

- Kuruluş kendisine özgü tehditleri tespit etti mi? Örneğin, eğer veri merkezi tehlikeli maddelerin taşındığı bir tren yolunun yakınındaysa, bu muhasebeleştirilmiş midir?

1 Confidentiality, Integrity, Availability ifadelerinin kısaltılmasıdır.

- Ya da hacktivizm ilgisini çekebilecek faaliyetlerde yer alan kuruluş mu? Her kurumun, faaliyet gösterdiği sektöre ve saldırganın güdülerine dayanan tehditleri değerlendirmesi gerekir.

e) Güvenlik Açıklarını Tanımlamak

Güvenlik açıkları risk değerlendirme süreci için son derece önemlidir. Özellikle, güvenlik açıkları bir istismarın gerçekleşmesi için fırsat sağlar; mantıksal olarak, bu nedenle ve tanım gereği, bir güvenlik açığı olmadan, herhangi bir risk yoktur, bir korunmasızlıkla risk potansiyel olarak çok büyük olabilir. Sistem yazılımı, prosedürleri ve dahili kontrollerdeki bu güvenlik açıklarının çoğu uygulanmayan bir kontrolün sonucudur. Birisi bir sanat müzesine gitme ve duvardan değerli bir resim çekmeyi arzulayabilir; ancak, ön kapıdan değerli bir sanat eseriyle çıkma yeteneğinin, bir dizi alarm ve hırsızlığı durduran güvenlik görevlileriyle karşılaşacağından şüphelenirdi. Bunlar uygun kontrollerle hafifletilen güvenlik açıklarıdır. Öyleyse, soru, zayıflıkların dürüst bir şekilde riski değerlendirmek için gözden geçirildiği örgüte sahip mi? Bu güvenlik açıkları yıldan yıla gözden geçirilmeksizin kabul edildi ve kabul edildi mi?

f) Mevcut Kontrolleri Tanımlamak

Tehditler, riskler ve etkileri tespit edildikten sonra mevcut süreçlerde ne tür kontrollerin olduğunu detaylı olarak tespit ederek bunların geçerliliklerini koruyup korumadıkları ve güncellenmeleri gerekip gerekmediği de değerlendirilmelidir. Yeni bir kontrol tasarlarken ve uygularken, amaç bilgi kaynaklarının CIA'sini sağlamak olmalıdır. Kontrol etkinliğini ve sürdürülebilirliği sağlamak genel yönetim sürecinin bir parçası olmalıdır. Kontrol tasarımı, izleme ve test etme, sahiplik dahil olmak üzere bu sürecin temel anahtarıdır. COBIT® 5'i kullanma bu süreçle ilgili özel yetkinlikler ve detaylar sağlar [7]. Ayrıca, Güvenlik için COBIT® 5, ISO/IEC 27001, NIST Siber Güvenlik Çerçevesi gibi kontrol çerçeveleri Yönetişim ve detaylı kontrol seviyelerinde seçim yapmak için mükemmel olanaklar sağlar. Bunlar daha ayrıntılı satıcı rehberliği ile desteklenebilir.

g) Etkileri Belirlemek

Bu adım, güvenlik açığının sömürüldüğünü ve kuruluşun yapılan zararı değerlendirip yanıtlayabileceğini varsayar. Finansal bir sis-

tem kesintisi maliyetine ilişkin bilgi sağlayabilir veya veri ihlalleri konusunda deneyimli / harici kaynaklar, maliyetin kuruluş için yüksek olup olmadığına veya bir zarar yazımı olarak kabul edilip edilmeyeceğine karar verilebilir. Belirli ihlal senaryolarının gerçekleşmesi durumunda ne tür maliyetlerin olabileceği ve bunlara tahammül edilip edilemeyeceği yani risk profili ile risk iştahının belirlenmesi etki analizine dayanır. Etkiler, kurumsal veya kişisel veri veya bilginin yetkisiz bir şekilde ifşa edilmesine, verilerin imhasına, sistem kaybına, itibar kaybına, pazar payının kaybına, hisse değerinin düşmesine ve riskin atfedilen varlığın değerine etki edebilir. Bazen, yeni bir ürün projesi, pazarlama planları veya tasarım özelliklerinin çalışması gibi durumlarda, firmanın masrafları (müşteri gruplarının listesi veya dahili fiyatlandırma listeleri) arttıkça, etki kolayca bilinemeyebilir. Rakip firmaların araştırma ve tasarım maliyetleri olmaksızın çalıntı bilgilerle daha düşük bir maliyetle aynı ürünü inşa etmeleri de dikkate alınmalıdır. İstisnai bir güvenlik açığına cevap verecek düzeltici kontrollerin yapılması önemli olmakla birlikte, önleyici kontrollerin bir saldırının olasılığını azaltmak için etkin ve verimli bir şekilde çalışmasını sağlamak daha önemlidir. Bazen olay bittikten sonra düzeltmek çok zor veya imkânsız olabilir. Etkin bir risk değerlendirmesi, uygun kontrol düzeylerini belirlemede yönetimi yönlendirecektir. Ancak, çoklu değişkenlere bağlı olarak önleyici, dedektif ve düzeltici önlemleri uygulamaktan sorumlu olan yönetimdir. Etki değerlendirme sürecinin ne kadar objektif olduğu, projeksiyonların ne ölçüde makul olduğu konusunda denetim ekibinin değerlendirme yapmasında fayda vardır. Eğer afaki bir şekilde etki değerlendirmelerinin yapıldığı tespit edilirse risk yönetiminin etkin işlemediği kanısına varılabilir.

h) Risk Seviyesini Belirlemek

Risk genellikle, ortaya çıkma olasılığını ve etki değerleriyle birlikte derecelenerek belirlenir ve mevcut tehdit, güvenlik açıkları ve kontrol ortamı durumunu kabul ederek bir risk seviyesinin tespit edilmesine olanak sağlar. Organizasyon ek kontrollerin uygulanması yoluyla riski azaltma fırsatına sahiptir. Bu kontroller uygulandıktan sonra kontrol edilmeyen risk, kalan (residual) risk olarak tanımlanmaktadır. Kuruluş, kalan bakiye risk kabul edilebilir düzeye inene kadar kontrolleri uygulamalı ve yönetim riski resmi olarak kabul

etmeye istekli olmalıdır. Her şeyde risk vardır ve makul olan ise kabul edilebilir maliyetle orantılı bir fayda sağlayan bir risk düzeyi bulmaktadır. Yani kabul edilebilir risk düzeyindeki fırsatları değerlendirmek gerekir. Örneğin, sanal özel ağlar (VPN'ler) ve iki faktörlü kimlik doğrulaması gibi BT kontrollerinin uygulanması, uygulanmayan güvenlik açıklarını kaldırarak, çoğu kuruluş için kabul edilebilir bir düzeye erişebilmeleri için, araya girme (in-themiddle) veya gizlice dinleme (sniffing) saldırıları riskini azaltır. Oldukça gizli ve stratejik bir devlet kurumu için bu kontrol yeterli olmayabilir ve özel ağlara ve artırılmış erişim yetkisine yönelik kısıtlamalar bilgi sisteminin ve varlıkların CIA gereksinimlerine dayanan gerekli bir kontrol olabilir. Denetçiler tarafından risk seviyesi belirleme sürecinin işleyişi değerlendirilmelidir.

i) Siber Güvenlik Risk Tepkisini Anlamak

Risk, dikkatin gerekli olduğu seviyeye yükseldiğinde (örneğin, yüksek veya orta riskli ya da birden fazla düşük riskli bir kombinasyonda), yönetim, hangi yaklaşımı benimseyeceğine karar vermelidir. En belirgin yaklaşım, riski azaltmak için insanlara, teknolojiye veya süreçlere yatırım yapmaktır. Ancak, bu organizasyonun sahip olmadığı kaynak ve para gerektirir. Organizasyon ayrıca bu süreçte birçok risk alanını ortaya çıkarmış olabilir ve birkaç yıl boyunca fonların izin verdiği ölçüde (büyük olasılıkla) öncelikli olarak azaltılması planlanmalıdır. Alternatif olarak, riski çözmek için başka seçenekler de vardır. Risk, şirketin risk iştahına uyuyorsa olduğu gibi kabul edilebilir. Diğer bir deyişle şirket, olayın gerçekleşmeyeceği ihtimalini, muhtemelen etkinin düşük olması ya da tehdit olasılığının önemsiz olması ihtimalini göz önünde bulundurmak istemektedir. Örneğin, bir kuruluş fidye yazılımını hedefleyen yeni bir kötü amaçlı yazılım son nokta koruma ürününe yatırım yapamayabilir çünkü düşük maliyet olarak algılamış olabilir (yedekleme bantlarından geri yükleme, iş istasyonu bölümlere ayrılmış bir ağ üzerindedir) veya diğer tehdit önleme mekanizmaları vardır. Bunlara örnek olarak son kullanıcı kimlik avı eğitimi bilinci ve e-posta taraması teknolojisi olarak kötü amaçlı bağlantılar için yeniden yazma ve test etme gibi kontroller verilebilir. Riskin kabul edildiği durumlarda, etkin bir yöntem, üst düzey yönetim seviyesinde birisinin iş gerekçeleri, gelecekteki etki azaltma planları ve imzanın desteklediği riskleri kabul etmesidir.

Kuruluş, sunucunun artık yamaları almayan veya üretici tarafından desteklenmeyen bir işletim sisteminin hizmetten çıkarılması riskini ortadan kaldırmaya karar verebilir. Riski azaltmak için diğer tespit edici veya önleyici kontrolleri ekleyerek riski sınırlandırmaya karar verebilir. Cihazda veri sızması göründüğünde uyarı vermek için ağ günlüklerinde bulunan süreç alarmlarına eklenebilir. Siber sigorta yaptırmak, riski başka bir tarafa aktarma yoluyla azaltmanın başka bir yoludur. Bu, riski azaltmayacak veya nihai sorumluluğu transfer etmeyecek olsa da, meydana geldiğinde olayın mali etkisini azaltabilir. Yeterli finansmanı sağlamak için, siber güvenlik iyileştirme planlarının tipik olarak bir süre içinde yürütülmesi gerekmektedir. Kuruluşlar, kritik güvenlik açıkları gibi belirli inceleme türlerinin, varlığa ve kuruluşa bağlı olarak yedi, 30 veya 90 gün içinde ele alınmasını beklemelidir. Bu örneklerin, güvenlik açıklarının zaman dilimlerinde ele alındığından emin olmak için denetçiler tarafından gözden geçirilmesi gerekir; Aksi takdirde, tehdidin uygun şekilde ele alınması için süreçlerde veya beklentilerde değişiklikler tespit edilmelidir. Bilgi Güvenliği için COBIT 5, ISO/IEC 27001 ve NIST Siber Güvenlik Çerçevesi gibi çerçeveler, kabul edilebilir bir düzeye indirilmesini sağlamak için siber güvenlik riskinin yönetişimini teşvik eden araçlardır.

12.3. İç ve Dış Denetim

Siber güvenlik süreçleri hem iç denetçiler ve hem de dış denetçiler tarafından denetimin amaç ve kapsamlarına göre dikkate alınmalıdır. Çünkü artık siber risk taşımayan hiçbir iş süreci neredeyse kalmamıştır. Endüstri 4.0, akıllı şehirler, yapay zeka ve büyük verinin her alanı etkilediği göz önüne alınmalıdır. Finansal, teknik, operasyonel veya sistematik her süreçte siber risk bulunmaktadır.

Tanımlanmış süreçlere sahip olmanın önemi, eğitimli ve yetkin siber güvenlik kaynakları ve üst düzey liderlik tarafından uygun eylemlerin gerçekleştirilmesini sağlamakla anlaşılır. Bunun yanı sıra, güncel ortaya çıkan tehditleri ele almak ve günlük olarak etkin bir şekilde yönetilmesini sağlamak için bir yönetişim çerçevesinin işler halde olması gerekir.

Siber güvenlik denetim sürecinin yapılandırılmış olması, denetlenen birim veya kurumda ek olarak hesap verebilirlik oluşturur ve kontrol ortamını daha güçlü da kılar. İç denetim departmanı, ba-

ğımsız bir görüşün işletmenin yönetim kurulu seviyesine iletilmesini sağlamak için denetim komitesine genellikle belirli bir raporlama ilişkisine sahiptir. Tarihsel olarak, bu tartışmalar finansal, operasyonel ve bilgi sistemi denetim alanları üzerinde olmuştur. Bununla birlikte, siber güvenlik gittikçe artan bir şekilde yönetim kurullarının dikkatini çekmektedir ve iç denetim departmanı da bu süreçte hayati bir rol oynayabilmektedir. İç denetim fonksiyonu, iç kontrol testleri, siber güvenlik uyumu, resmi risk kabulü, soruşturma ve adli yardım için sistematik ve objektif destek sağlar.

Siber güvenlik denetimleri, iş çevrimlerinin göz önünde bulundurulması, iş faaliyetlerinde asgari kesintiye yol açması ve bilişim teknolojisinin (BT), yasal, insan kaynaklarının (İK) tam katılım şansının artırılması ve iş çevrelerinin dikkate alınması şeklinde yıllık bir döngüde denetim için gerekli iş alanları planlanmalıdır. Departmanların kanıtlarının toplaması için uygun planlama ve zaman ile (denetimden en az üç ya da dört hafta önce sağlanmalıdır), denetim sorun alanlarını keşfetmeye ve riski değerlendirmek için beklemeye ve tekrar tekrar bilgi talep etmeye odaklanabilir. Denetimler kapsamında giriş, günlük güncelleme ve çıkış toplantıları ile aktiviteler planlanmalı ve her bir aşama için kesin beklentiler açıkça bildirilmelidir. Test faaliyetleri genellikle hesap kurulumu ve faaliyetlerin yürütülmesine erişim gerektirir ve bunları zamanında temin edememek, denetimin uzamasını sağlayabilir.

a) Denetim kapsamı

Kullanıcılar evden çalışırken ev ağlarını kullanıyor olabilirler, uygulamalar bulutta çalışabilir veya bir denetime olanak sağlamak için daha fazla erişim veya yetkiye ihtiyaç duyabilecek özel gizli sistemler (örn. İK bilgileri, yasal belgeler) olabilir [3]. Veriler bu sistemler arasında akabilecek ve bu durum risk oluşturabileceğinden, bu kapsamdaki kısıtlamalar, denetim kapsamının net olması için tanınmalı ve ele alınmalıdır. Kullanıcıların, çevrelerinin denetimine izin veren ev işlerinde çalışan sözleşmeler imzalamaları gerekebilir ya da mobil cihazların kullanımı, cihaz hakkında bilgi ve cihazın yapılandırmaya tabi tutulduğu bir belge tarafından desteklenmelidir. Bilgiyi nasıl ele geçirdiğini göstermek için KVKK kapsamında bilgi işleme süreci - özellikle yüksek duyarlılığa sahip olan veya kişisel

verilerin yer aldığı bilgiler - gerekli olmalıdır. Bu, sözleşmede veya denetim görev emrinde yer alan bir denetim hakkı maddesi, bir güvenlik standardı sertifikası (örn. ISO/IEC 27001, SSAE 16 SOC2 raporu, Cloud Security Alliance (CSA) Kontrol Matrisi raporu ve sözleşme yükümlülüğü yoluyla gerçekleştirilebilir. Bir ihlal meydana geldiğinde, itibar hasarının veriyi işleyen alt birime değil, müşteri veya vatandaş tarafından yetki verilmiş olan kuruluşun hedeflenmesi büyük olasılıktır.

Siber güvenlik denetimleri genellikle genel denetimlerden daha teknik ve karmaşık olduğundan, denetimin yönetişim, risk, yönetim veya güvence alanına bağlı olarak denetimi kolaylaştırmak için farklı yaklaşımlar kullanılabilir.

b) Siber Güvenlik Hedefleri ve İlgili Denetim Amaçları

Denetimler birçok şekil alabilir ve siber güvenliğe genel yönetişim veya teknik test ile ilgili farklı odaklara sahip olabilir. Politika, prosedürler, standartlar ve kılavuz ilkelerin uygun olması, yönetim tarafından onaylanması ve iş değişikliklerine cevap olarak sıklıkla güncellenen ve gözden geçirilmesi sağlanması gerekir. Günümüzde dikkatin tespit ve müdahaleye daha çok kaymasıyla organizasyon, bir ihlal durumunda ne kadar iyi hazırlandığını belirlemek için denetleme yapmak isteyebilir. İşletmenin tüm alanlarını denetlemek imkansız olduğundan, denetlemek için yüksek değerli alanlara ve riskin fazla olduğu süreçlere bakmak şarttır. Örneğin;

- Bir çağrı merkezi ve gerekli sistemler arasındaki telekomünikasyon bağlantısı başarısız olursa ne olur?
- E-ticaret odaklı bir web sitesine yönelik bir hizmet reddi (DDoS) saldırısını önleyecek uygun kontroller var mı?
- Kuruluşun, veri sızdırma ve ihlallerini zaman içinde fark edilmesini veya bu verileri hedeflenen bir saldırıdan korumak için veri ortamlarının ayrılmasını sağlamak için uygun izleme kontrolleri mevcut mu?

Buna benzer sorular denetim hedef ve kapsamının belirlenmesinde sorulması gereken sorulardır.

Tablo 12.1. Planlama ve Kapsam Belirleme

Alan / İnceleme Türü	Yaklaşım	Öneriler
Yönetişim: Siber güvenlik politikası ve ilgili teknik anahtar operasyon prosedürler.	Zamanında nokta atışı, uygulama sonrası güncellenmiş politika	İlgili paydaşlarla birlikte politika ve kuralların güncellemesi dönüşümü destekler. Denetim, iş işlevini / yerel tasarımı ve politikayı destekleyen temel işletim prosedürlerinin uygulanmasını ele alacaktır. Bir sonraki yıl eksiklikler ile ilgili bir takip denetimi yapılmalıdır.
Risk: Siber güvenlikte risk kaydı güncellemesi, tedavi ve risk raporlaması.	Önceki yıl risk denetim sonuçları dahil olmak üzere sonraki yıl sonu değerlendirmeleri	Denetim, risk kaydının doğruluğunu, eksiksizliğini ve uygun güncellemeyi ele alacaktır. Risk raporlaması (zamanlılık, eksiksizlik, doğruluk) dahildir.
Yönetim: Siber güvenlik olayı değerlendirmeleri.	Sürekli, gerçek saldırılara, ihlallere ve olaylara göre öngörü.	Herhangi bir saldırı veya ihlalin (etkilenen varlıklar dahil) ara değerlendirmesidir.
Güvence: Siber güvenlik risklerine karşı makul tedbirlerin mevcudiyeti.	Önceki tespitlerle karşılaştırma, kaynak/ risk/ maliyet optimizasyonuyla makul rehberlik	Denetim, siber güvenlik risk yönetimi sürecinin verimlilik ve etkinliğini bağımsız bir şekilde gözden geçirecektir, yani üçüncü hat, ikinci savunma hattını denetleyecektir.

En iyi iş sonuçlarına ulaşmak için denetim hedefleri siber güvenlik hedefleriyle uyumlu olmalıdır. Siber güvenlik programı hedeflerinin denetim hedefleriyle eşleştirilmesi, siber güvenlik yönetimi içerisinde denetimin desteklenmesini artıracak ve bunun tersi de doğru olacaktır.

12.4. Dış Denetim

Organizasyonlar, denetimlerin tasarımının etkili olmasını sağlamak ve kontrollerin uygulanması gerektiği şekilde işlemek için öncelikle mali ve operasyonel kontrollerin bağımsız bir şekilde güvence altına alınması için dış denetçilerin hizmetlerine yönelik sözleşmeler yaparlar. Bu denetimler tipik olarak bir devlet dairesi veya düzenleyici adına yapılır. Bazen de kurumun üst yönetimi bu şekilde bir

hizmet alımına karar verebilmektedir. Ülkemizde dış denetim, SPK, BDDK ve AB programları mevzuatları kapsamında düzenlenmiştir.

Siber güvenlik denetimlerini denetlemek, bir dış denetçinin uzmanlığından yararlanabilir ve kuruluş içinde bulunmayabilecek beceri kümelerine erişimi koruyabilir. Sızma testi, sunucu veya güvenlik duvarı yapılandırmalarını inceleme veya güvenlik bilgi olay yönetimi (SIEM) kural kümelerini gözden geçirme gibi özel analizler için gerekli teknik beceriler çoğunlukla iç denetim departmanında mevcut olmayabilir ve harici yetenek yeteneklerinden yararlanabilir.

12.5. Siber Güvenlik Olgunluk Modelleri

Diğer siber güvenlik kontrolleri değerlendirildiği ve yeni teknoloji, insan veya süreç kontrolleri uygulandığı için, mevcut durumu analiz etmek için bir siber güvenlik programı olgunluk modeli de uygulanabilir. Olgunluk modelleri COBIT-5 PAM modelinde olduğu gibi ISACA bünyesinde olan CMMI modelinde de mevcuttur. Siber güvenlik sürecinin olgunluk seviyesi bunlarla belirlenebilir. Farklı organizasyonlar ve çerçeveler, artan olgunluk seviyeleri için çeşitli isimlere sahiptir; bununla birlikte, çoğu, olgunluğun kanıtlanması için aşağıdakilerin bazı formlarına bağlıdır: var olmayan (seviye 0), gelişigüzel (seviye 1), tekrar edilebilir (seviye 2), tanımlı (seviye 3), yönetilen (seviye 4) ve optimize edilmiş (seviye 5).

Bazı kurumların süreçleri olmayabilir, bazılarında süreç olsa da yapılandırılmamıştır. Başka yerde sorumluluklar ve hedefler süreçlerle uyumlu olmayabilir. Özellikle siber güvenliğe ve daha geniş bilgi güvenliği programına (örneğin, bilgi güvenliği yetkilisi [CISO]) sorumlu olan bir kişinin görevlendirilmesinden önce birçok programın başlatıldığı bilinen bir durumdur. Bilgi güvenliği başkan yardımcısı, bilgi güvenliği müdürü gibi görevlilerin olması olgunluk ölçeğinin en üst seviyesinde, siber güvenlik kültürün önemli bir parçasıdır. Yönetici puan kartları mali ve operasyonel şirket performansına bağlı olan ölçütleri rapor eder ve siber güvenlik programında sürekli iyileşmeyi sağlamak için endüstri çerçeveleri benimsenir. Raporlama ayrıca organizasyonda gerekli dikkat ve finansmanı elde etmek için yeterince yüksek bir düzeydedir.

Tablo 12.2. Siber Güvenlik Hedefleri ve İlgili Denetim Amaçları

Siber Güvenlik Hedefi	Denetim Amacı	Uyarılar
Siber güvenlik politikaları, standartları ve prosedürleri yeterli ve etkilidir.	• Belgelerin eksiksiz ve güncel olduğunu doğrulayın. • Resmi onay, serbest bırakma ve yaptırımın geçerli olduğunu onaylayın. • Belgelerin tüm siber güvenlik gereksinimlerini karşıladığını doğrulayın. •Bağlı kontrollerin, politikalarda, standartlarda ve prosedürlerde yapılan tüm hükümleri kapsadığını doğrulayın.	Denetim, belgelerin evrenini (yönetişim tarafı) ve bu belgelerin öngördüğü kontrolleri ele almaktadır. "Etkili" bu anlamda uygun onaylama / serbest bırakma / uygulama döngüsünden daha fazlasını denetleyemezken, "yeterli" sadece politikaların, standartların ve prosedürlerin eksiksizliği, yeterliliği ve bütünlüğü ile ilişkili olabilir.
Yükselen risk doğru bir şekilde tanımlanır, uygun şekilde değerlendirilir ve yeterli şekilde yönetilir.	• Risk tanımlama sürecinin güvenilirliğini doğrulayın. • Kullanılan araç, yöntem ve teknikler dahil olmak üzere risk değerlendirme sürecini değerlendirin. • Tüm risklerin sonuçların değerlendirilmesi doğrultusunda ele alındığını onaylayın. • Tedavi edilmemiş risk için tedavinin yeterli olduğunu veya resmi risk kabullerinin bulunduğunu doğrulayın.	Denetim genellikle ilk yıldaki süreçlere, araçlara ve yöntemlere odaklanarak birkaç yıl sürecektir. Takip eden yıllarda, denetçiler büyük olasılıkla risk alanlarının örneklerini alır ve sürece doğru detaylı inceler. Denetim, "ortaya çıkan" riskin tüm kapsamını nitelemek için harici verileri içerebilir.
Siber güvenlik dönüşüm süreçleri tanımlanır, dağıtılır ve ölçülür.	• Dönüşüm sürecinin ve ilgili rehberliğin varlığını ve eksiksizliğini doğrulayın. • Dönüşüm sürecinin, işletmenin tüm bölümleri tarafından uygulandığını ve takip edildiğini doğrulayın. • Dönüşüm hedefleri, risk ve performans ile ilgili kontrolleri, ölçüleri ve ölçümleri onaylayın.	Yıllar boyunca yayılacak olan denetim, siber güvenliğin dönüştürülmesi sürecini kapsayacak şekilde tasarlanmalıdır.
Saldırılar ve ihlaller zamanında ve uygun bir şekilde tanımlanır ve tedavi edilir.	• İzleme ve belirli teknik saldırı tanıma çözümlerini onaylayın. • Güvenlik olay yönetimi ve kriz yönetimi süreçleri ve planları için arayüzleri değerlendirin. • Saldırı yanıtının güncelliğini ve yeterliliğini (geçmiş saldırılara dayanarak) değerlendirin.	Bu, saldırıyı erken tanıma ve tanımlama için teknolojiye bakan, daha sonra olayları tırmandırmak ve yönetmek için sonraki adımlarda görünen derinlemesine bir teknik denetimdir. "Zamanında" ve "uygun", ilgili politikalarda, standartlarda ve prosedürlerde belirtildiği şekilde tanımlanır (öznel denetim kararı yoktur).

Siber güvenlik olgunluk araçları genellikle programın yıldan yıla geliştirilmesini göstermek için siber güvenlik programını yönetmekle sorumlu olan kişiler tarafından kullanılmaktadır. Daha sonra sürdürülebilirlik vade düzeyini arttırmak için yeni araçlar ve yaklaşımlar öneren çok yıllı yol haritaları üretilebilir. Bunlar, satın alma için teklif alma süreçlerini, en iyi fiyatlandırma ve ürüne en son tehdide yanıt verecek şekilde sistematik bir şekilde uygun hale getirmek için satıcıları devreye sokmak için yönlendirebilir. Bu, siber güvenlik projelerinin hemen tamamlanması gerektiği için pahalı bir kaynak tutmaya ihtiyaç duymadan uzun bir süre boyunca yayılabileceğinden, planlı mekanizmalar yoluyla daha düşük maliyetle kontrollerin uygulanmasını sağlayabilir. Bu aynı zamanda, iş alanı, satıcı, danışman, proje yöneticisi ve çabayı yönlendirmeye yardımcı olmak için tahsis edilen teknik kaynak arasında sağlıklı ilişki kurulmasına izin verir. Öncelikli yönetim incelemeleri, risk değerlendirmeleri ve denetim bulguları, siber güvenlik programı olgunluk durumunun bütünsel bir görüntüsünü sağlamak için sürdürülebilir bir modelini oluşturmak ve risk değerlendirmesinde boşlukları dolduracak alanları belirlemek ve daha sonra denetim bulguları iç veya dış bir olasılığın azaltılması için kullanılabilir.

12.6. Düzeltici Eylem Planları

Yönetim kontrolleri, risk yönetimi süreçleri veya iç denetim yoluyla oluşturulan değerlendirmeler, uygulama boşluğunu veya çözümlenme ihtiyacı olan öğeleri belirleyecektir. Bu siber güvenlik açıkları taslak raporlar aracılığıyla bilinir ve kabul edildiğinde, eylemlerin makul bir zaman dilimi içinde (kuruluşa veya ilgili birime bağlı olarak 10-30 gün) ve işletme sahiplerinin kabul ettiği düzeltici eylem planlarında formüle edilmesi gerekir. Eylem planları denetçilerin çözümleme ve önerilerine karşın yönetimin bütçe ve İK olanaklarını göz önünde bulundurarak ortaya koymayı düşündüğü aksiyonları detaylı olarak içermelidir. Yoksa afaki şekilde ölçülmesi zor veya hallederiz gibi bir yaklaşımla ilerleme kaydedilmesi çok zordur. Organizasyon, güvenlik duruşunun boşluk alanlarına dikkatsizlikten dolayı zayıflamadığından emin olmak için üzerinde anlaşılan faaliyetleri, kilometre taşlarını ve teslim tarihlerini izlemelidir. Süreç (veya işletme) sahipleri, belirtilen yeni güvenlik açıklarının düzeltilmesi veya tüm olayların 24 ila 72 saat içinde raporlanması için 90 gün gibi devam eden süreçler için zaman çerçevesi üzerinde anlaş-

malıdır. Denetçiler de sonraki gözden geçirmelerinde bu hususları göz önünde bulundurmalıdırlar.

12.7. Değerlendirmeler

Yaklaşık on yıl kadar önce, çoğu kuruluş mobil, bulut ve sosyal medyaya hitap etmiyordu. Geçtiğimiz on yıl içinde bu platformlardaki bir patlamanın yaşandığı ve şimdi neredeyse herkesin en az bir sosyal medya hesabı ve cebinde bir telefon olduğu kolaylıkla söylenebilmektedir. Nesnelerin İnterneti (IoT), büyük veri analizleri ve yapay zeka satın aldığımız ürünlerde gelişmelere ve değişikliklere neden oluyor. Tehdit istihbaratı kurumlar aracılığıyla paylaşılıyor. Bazen de kişisel veriler ve analizler satılabiliyor. Fidye yazılımları, hedefe yönelik saldırılar, mızrak avcılığı ve artan rekabet olanakları, tehdit ortamını ve savunmamızı düzenli olarak yeniden değerlendirmemize neden oluyor. Bunlarla ilgili kapsamlı risk değerlendirmesi bir amaç değil, bir araçtır [7]. Siber güvenlik olayları yeni saldırı senaryoları için gözden geçirilmeli ve önleme, tespit ve müdahale eylemleri belirlenmeli ve risk değerlendirmesine getirilmelidir. Çünkü yenilikçi teknoloji ve getirdiği kolaylık ve tehditler akıl almaz ölçüde hızla gelişmektedir.

Bir kuruluşun bilgi varlıklarını korumadaki başarısızlık, ticari faaliyetler, finansal durum ve piyasadaki itibar üzerinde yıkıcı bir etkiye sahip olabilir. Saldırganın hedefinin çekiciliğini azaltmak ve saldırı masraflarını artırmak için siber güvenlik kontrollerine uygun yatırım yapılması gerekmektedir. Bilgi Güvenliği için COBIT 5, ISO/IEC 27001 ve NIST Cybersecurity Framework gibi çoklu çerçeveler, NIST SP 800-53 kontrolleri ile birlikte, siber güvenlik kontrollerinin yönetimini sağlamak için birleştirilebilecek süreçler sağlar. Aynı derecede önemli olan, siber güvenlik kontrollerinin bilgi varlıklarını korumak ve etkin bir şekilde çalışmak için iyi bir şekilde tasarlandığından emin olmak için yönetim, risk yönetimi ve iç denetimin çok katmanlı gözden geçirme savunmalarıdır. Bu gözden geçirme süreçleri olmaksızın, kuruluşun kontrol faaliyetlerine bağımlı olması etkinliğin bir alandaki kontrolüne bağlı olduğu için siber güvenlik kontrollerinin yönetimini feda eder. Yönetim gözden geçirmeleri, risk yönetimi süreçleri, iç denetimler ve siber güvenlik kontrollerini yürütmekten sorumlu iş operasyonları birbirini tamamlayıcı niteliktedir. Siber güvenlik kontrollerinin denetlenmesi, iyileştirme fır-

satları için içeriden bir öngörü sağlar ve siber güvenlik programının olgunluğunu artırmak için kuruluş tarafından benimsenmelidir.

Kaynaklar

[1] ISACA, "COBIT 5 for Information Security", USA, 2012, www.isaca.org/COBIT/Pages/info-sec.aspx

[2] National Institute of Standards and Technology (NIST), NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, USA, 2015, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[3] Center for Internet Security (CIS), CIS Controls Library Resources, www.cisecurity.org/critical-controls/Library.cfm

[4] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001, Information technology—Security techniques—Information security management systems— Requirements, 2013, https://webstore.ansi.org/RecordDetail.aspx?sku=ISO%2fIEC+27001%3a2013&source=msn&adgroup=27001&keyword=iso%20iec%2027001&utm_source=bing&utm_medium=cpc&utm_campaign=Campaign%20%231&utm_term=iso%20iec%2027001&utm_content=27001

[5] The Information Security Forum (ISF) Standard of Good Practice for Information Security, 2016, www.securityforum.org/tool/the-isf-standardrmation-security/

[6] American Institute of Certified Public Accountants, Statements on Standards for Attestation Engagements, 2016, www.aicpa.org/Research/Standards/AuditAttest/Pages/SSAE.aspx

[7] Fitzgerald, Todd J. "Auditing Cyber Security: Evaluating Risk and Auditing Controls", ISACA Report, http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/auditing-cyber-security.aspx

Siber Güvenlik İçin Büyük Veri Yaklaşımları

BÖLÜM 13

Duygu SİNANÇ TERZİ
Prof. Dr. Şeref SAĞIROĞLU

SİBER GÜVENLİK İÇİN BÜYÜK VERİ YAKLAŞIMLARI

Büyük veri, her alanda büyük fırsatlar yaratarak daha önce gizli örüntülerin keşfini kolaylaştırmakta ve kararları yönlendirmek için öngörülerin geliştirilmesine olanak sağlamaktadır. Siber uzayın genişlemesiyle, büyük veri ve siber güvenlik ilişkisi de kuvvetlenmeye başlamıştır. Bu bölümde bu ilişki; siber güvenlik için büyük veri, siber tehdit olarak büyük veri ve büyük verinin güvenliği başlıkları altında sınıflandırılarak değerlendirilmiştir.

13.1. Giriş

Günümüzde herhangi bir yerden, herhangi bir zamandan ve herhangi bir cihazdan gelen büyük miktarda karmaşık ve heterojen veriler, büyük veri çağını başlatmıştır.

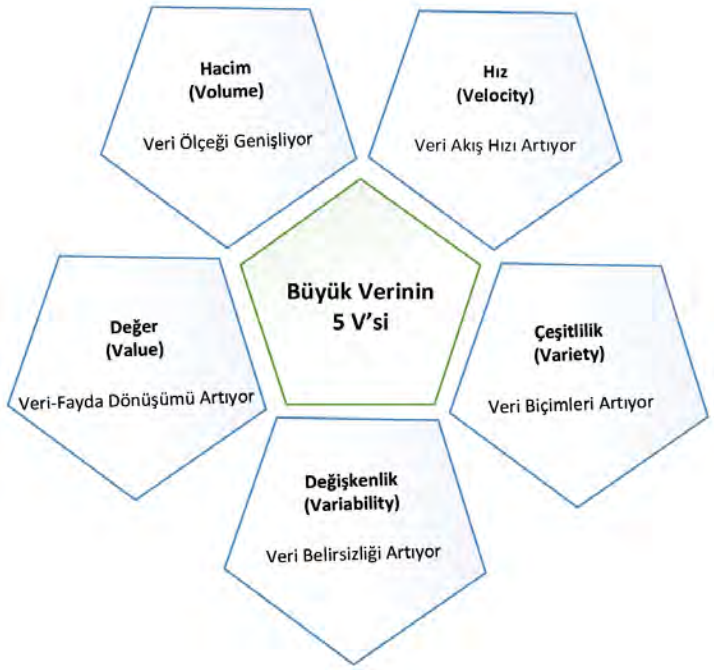
Büyük verinin;

- depolama, yönetim ve analiz için sıradan veritabanı yazılım araçlarının yeteneklerinin gerisinde kaldığı veri kümesi,
- yüksek hızda toplama, keşif ve analiz sayesinde çok çeşitli verinin çok büyük hacminden ekonomik olarak değer elde etmek için tasarlanan yeni nesil teknolojiler ve mimariler,
- geleneksel veri işleme uygulamaları veya genel veri tabanı yönetim araçları kullanılarak yönetilmesi zor olan büyük ve karmaşık veri koleksiyonu, veya
- farklı formatlarda ve farklı kaynaklardan çok yüksek hızlarda üretilen büyük miktardaki veriler

gibi tanımlamaları olsa da aslında güncel teknolojiler ile çözülemeyen problemlerin çözümünde kullanılabilecek yeni nesil çözümlerdir. Genellikle, Şekil 13.1'de 5V olarak özetlenen bileşenlere sahip

olan veri kümeleri, büyük veri olarak sınıflandırılmaktadır [1]. Sadece verinin değişimi değil; veri madenciliği için kolay yöntemler, daha fazla yapay zeka içeren kurumsal uygulama paketleri, bulutta hazır hizmet platformları, otomatize edilmiş makine öğrenimi ve veri yönetimi gibi araç ve tekniklerin gelişimi de kurum ve kuruluşların veri ile ilgili büyük sorularını cevaplamaya yardımcı olmaya başlamıştır [2].

2016 yılında dünyada yaklaşık 8.000'e yakın büyük veri ile ilgili yayın varken bugün için bu sayı 60.000'lere yaklaşmaktadır. Dünya artık büyük veriden büyük değerler elde edildiğini görerek dijital toprak, dijital maden, dijital para, dijital yaşam, dijital dönüşüm gibi terimlerin peşinde koşar hale gelmiştir. Bu değerlerin insan hayatını kolaylaştırdığı, kaliteyi arttırdığı, işleri hızlandırdığı, ihlalleri önlemeye katkı sağladığı, büyük resmin görülmesini kolaylaştırdığı, yeni fikir, çözüm ve değer geliştirilmesine öncülük ettiği artık somutlaşmıştır.



Şekil 13.1. Büyük Verinin 5 Bileşeni

Bu ilerlemelere rağmen, birçok kuruluş standartlaştırılmış, etiketlenmiş ve anormalliklerden arındırılmış büyük miktarda veriye ihtiyaç duyar. Aksi halde "**çöp girerse çöp çıkar**" kuralı doğrultusunda, eksik veya hatalı veri kümeleri ile yapılan analizler doğru olmayan sonuçlara yol açacaktır. Bu noktada devreye giren büyük veri analitiği; veri bilimi, görselleştirme araçları, gelişmiş istatistiksel fonksiyonlar ve algoritmalar kullanarak veri keşfine odaklanır [3]. Büyük veri analitiği operasyonları iyileştirerek, inovasyonu ve uyarlanabilirliği kolaylaştırarak ve kaynak tahsislerini optimize ederek organizasyonları daha verimli hale getirebilir [4]-[5].

Gelişmiş ülkeler, açık kaynak ve açık veri yaklaşımlarını desteklemekte, kamu kaynaklarıyla desteklenen projeleri, yayınları, araştırmaları, raporları, araştırma verilerini herkese açmakta, bunun için yasal düzenlemeler yapmakta, bu tür projeleri teşvik etmekte ve bunların hayata geçirilmesini kolaylaştırmaktadır. Büyük ve açık verilerin önemli bir kısmı kamu hizmetlerinden elde edilen verilerdir. Bu verilerin toplumun yararına dönüştürülmesi için bir kısmının ortak kullanıma açık olması; girişimciliği ve inovasyonu teşvik etmesi, kurumların verimliliğini artırması, kurumlar arası işbirliğini güçlendirmesi, oluşabilecek ihlallerin tespitini kolaylaştırması, kayıpları en aza indirgemeye katkı sağlaması, ve bunların vatandaşlara ve yöneticilere aktarılması işlemlerini sağlayacak süreçleri kolaylaştıracaktır. Bu konu Bölüm b'da detaylı açıklanmıştır.

Büyük düşünenler, büyük verilere sahip olma ve bunlardan değer elde etme peşinde koşarlarken, küçük düşünenler ise verilerini silmeye ve yok etmeye çalışmaktadır. Gelişmiş ülkelerin, verilerini kamuya açma, yarışmalar (codefest, hackfest, teknofest, capture the flag) düzenleme ve projeleri yarıştırma gerekçelerinin arkasında da bu düşünceler vardır.



Şekil 13.2. Siber Güvenliğin 6 Bileşeni

Veri yapısındaki değişikliklerin doğal bir gelişimi olarak, siber saldırıların boyutu ve karmaşıklığı da artış göstermektedir. 2018'in ilk çeyreğinde McAfee Labs, saniyede ortalama beş yeni zararlı yazılım örneği kaydetmiş ve gerçek dünya saldırı düzenlerini görmeyi ve analiz etmeyi sağlayan ürünüyle, her gün ortalama 2.400.000 URL ve 700.000 dosyayı analiz etmiştir [6]. Veri boyutunun ve tehditlerin artmasıyla, bu süreçte büyük veri araçları ve tekniklerinin, siber güvenliğin sağlanması amacıyla kullanılması bir zorunluluk haline gelmiştir.

2017'de 137.9 milyar dolar olan siber güvenlik pazarının, 2022'de 231.9 milyar dolar olacağı tahmin edilmektedir [8]. Bu büyük pazarı oluşturan süreçler temelde, güvenlik açıklarının neden olduğu risklerin belirlenerek azaltılmasına yardımcı olan güvenlik kontrollerinin seçilmesi ve uygulanmasına dayanır.

"Elektronik ortam bilgi varlıklarının, siber uzayı destekleyen BT'nin, toplumsal ve ulusal yeteneklerin ve değerlerin (maddi/manevi) her türlü saldırıya karşı korunma" [7] olarak da tanımlanabilen siber

güvenlik yaklaşımı, içerisinde pekçok bileşeni barındırmaktadır. 6 D olarakta bilinen bu bileşenler ve bunlara ait süreçter [9], Şekil 13.2'de verilmiştir.

Siber uzayın genişlemesiyle kuvvetlenen büyük veri ve siber güvenlik ilişkisi; siber güvenlik için büyük veri, siber tehdit olarak büyük veri ve büyük verinin güvenliği başlıkları altında sınıflandırılarak değerlendirilmiştir.

13.2. Siber Güvenlik İçin Büyük Veri

Kısıtlı veriler ve geleneksel teknolojiler uzun vadeli ve büyük ölçekli analizleri desteklemek için yetersiz kalmaya başlamıştır. Bu yetersizliğin sebepleri, literatürden ve kendi deneyimlerimizden aşağıdaki şekilde özetlenebilir [10]-[12]. Bunlar;

1. Veri kapasitesi hızla artmakta, dinamik olarak değişmekte ve düzensiz yapılarda üretilmektedir.
2. Gürültülü ve yapılandırılmamış veride analitik ve karmaşık sorgular yapmak zorlaşmaktadır.
3. Gizlilik, Bütünlük ve Erişilebilirlik gibi bilgi güvenliği unsurlarını tehdit edebilecek riskler, geleneksel bilgi teknolojisi kaynaklarının ötesinde büyümektedir.
4. İş itibarını, hizmet sunumunu, gizli verileri veya fikri mülkiyetin kaybına yol açan tehditleri izleme ve hafifletme gibi yeni aşamalarla güvenlik yeniden tanımlanmaktadır.
5. Güvenlik uzmanları daha kesin analizler için daha fazla veriye ihtiyaç duymaktadır.
6. Tehditlerin karmaşıklığı, etkinlik süresi ve zarar boyutu giderek artmaktadır.
7. Tek bir tehdit incelemesi için bile bütün veri parçalarının incelenmesi gerekmektedir.
8. Siber saldırıların arttığı sıcak noktaların hızlı bir şekilde belirlenmesi gerekmektedir.
9. Büyük verilerin anlaşılması için doğru bakış açısı sunacak domain uzmanlığına ihtiyaç vardır.
10. Mevcut altyapıların iyileştirilmesi ve yeni teknolojiler, algorit-

malar, analiz ve görselleştirme araçlarının geliştirilmesi gerekmektedir.

11. Büyük veri analitiği için veri ve uzman kadar bu ortamlarda işlem yapabilecek altyapılara ihtiyaç vardır.

Büyük veri analitiği; büyük ölçekli güvenilir kümeler ile içerik analiz aralığının daha da genişlemesini ve analizlerin hızlanmasını sağlayarak daha fazla organizasyonel çeviklik ile siber uzayda risk/ödül dengesinin daha iyi yönetilmesine yardımcı olmaktadır. Ağlarda, sunucularda ve diğer cihazlardaki olayları analiz eden CTI (Cyber Threat Intelligence), IPS (Intruder Prevention System), IDS (Intruder Detection System), SIEM (Security Information and Event Management) ve CSOC (Cyber Security Operations Centre) gibi geleneksel siber güvenlik yöntemlerinin gelişmiş versiyonu olarak adlandırılabilen siber güvenlik için büyük veri çözümleri; Şekil 13.3'de özetlendiği gibi, pekçok kaynaktan elde ettiği veriler üzerinde davranış analizi ve örüntü tespiti yapılarak güvenlik sağlanmaktadır [5].

Siber güvenlik için büyük veriyi kullanma süreç adımları Şekil 13.4'de verilmiştir. Şekilden görülebileceği gibi bu süreç 5 madde de özetlenmiştir [13].

1. Problemin Tanımlanması

   Süreç, hizmet kaybına veya maddi zarara sebep olacak unsurun tanımlanmasıyla başlar. Problem; performansın kötüleşmesi, plansız kesintiler, fikri mülkiyet erişimi ve veri hırsızlığı olarak belirlenebilir.

2. Test Edilecek Hipotezin Belirlenmesi

   Bu adımda çözüm üretilecek problemin sebepleriyle ilgili hipotez kurulur. Verilere nasıl izinsiz erişilir, performans düşüşlerine ne sebep olur, neden hizmet kesintisi oluşur gibi sorulara cevap aranır.

3. Veri Kaynaklarının Seçilmesi

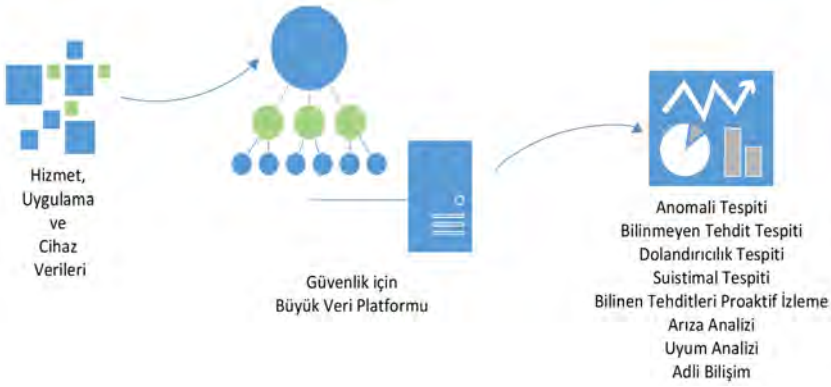
   Surunun tespitini kolaylaştıracak veri kaynaklarının kombinasyonu belirlenir.

4. Gerçekleştirilecek Analizlerin Belirlenmesi

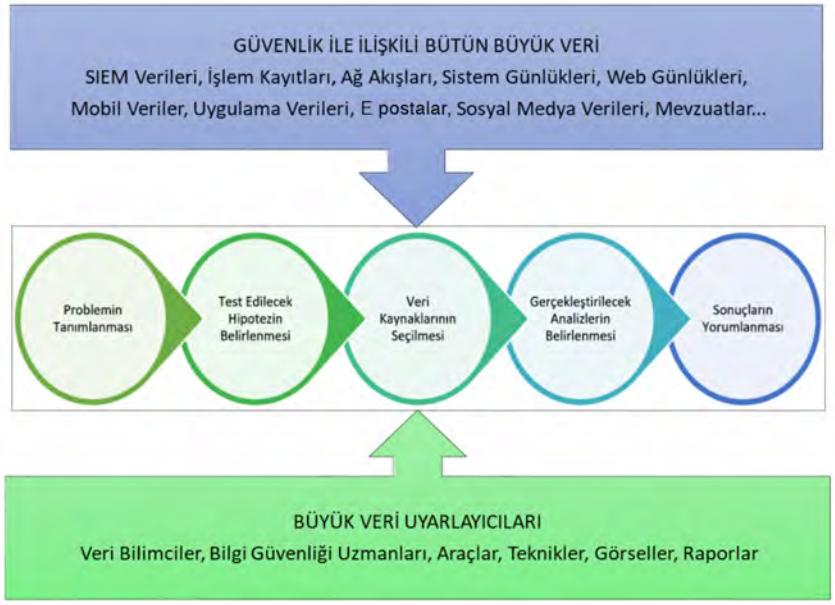
Veri türüne ve yapısına uygun olarak; normal/normal olmayan davranışların tanımlanması, aykırılıkların tespiti ve örüntülerin çıkarılması gibi analizler gerçekleştirilir.

5. Sonuçların Yorumlanması

Son olarak; analizlerin ve elde edilen modellerin performansı, başarısı, parametreleri ve gürbüzlüğü değerlendirilerek uygun aksiyonlar gerçekleştirilir.



Şekil 13.3. Siber Güvenlik için Büyük Veri Kullanımı



Şekil 13.4. Siber Güvenlik için Büyük Veriyi Kullanma Süreç Adımları

Büyük veri analitiğinin, farklı güvenlik boyutlarında nasıl yardımcı olabileceğine dair bazı örnekler aşağıda verilmiştir [3].

1. Ağ Trafiği

   Anormal trafik örüntüleriyle, şüpheli kaynakları ve hedefleri tespit ve tahmin etmek.

2. Web İşlemleri

   Özellikle kritik kaynakların veya faaliyetlerin kullanımında anormal kullanıcı erişim kalıplarını tespit ve tahmin etmek.

3. Ağ Sunucuları

   Sunucu manipülasyonuyla ilgili anormal kalıpları, önceden tanımlanmış politikalara uymama durumlarını tespit ve tahmin etmek.

4. Ağ Kaynağı

   Kaynağın ilettiği, işlediği ve aldığı veri türüne göre herhangi bir makinenin anormal kullanım şekillerini tespit ve tahmin etmek.

5. Kullanıcı Kimlik Bilgileri

   Erişim ve işlem davranışlarının dışına çıkan kullanıcı veya kullanıcı grubuyla ilgili anormallikleri tespit ve tahmin etmek.

13.3. Siber Tehdit Olarak Büyük Veri

Büyük veri destekli yapay zekanın gelişmesiyle siber saldırıların da potansiyeli artmaya başlamıştır. Gelişmiş makine öğrenimi ve derin öğrenme gibi teknikler, büyük veri ve teknolojilerinin aşağıda belirtilen pekçok kötü amaca hizmet etmesine ve tehdit oluşturmasına sebep olabilir [2], [14].

1. Gizli örüntülerin bulmasını ve yorumlamasını sağlayan modeller, güvenlik açıklarının bulunması için de kullanabilir.
2. Yapay zeka modelleri iyi korunmadığı takdirde, kötü niyetli aktörler tarafından hatalı verilerin enjekte edilmesiyle yeni güvenlik açıkları ortaya çıkabilir.
3. APT saldırılarını kolaylaştıracak ortamlar sağlanabilir.
4. Yayıldıkça öğrenen akıllı kötücül yazılımlar ve fidye yazılımları geliştirilebilir.

5. Makine zekası ile kontrol edilebilen küresel siber saldırılar gerçekleştirilebilir.
6. Gelişmiş veri analizi ile davranış takibi doğrultusunda özelleştirilmiş saldırılar gerçekleştirilebilir.

Verinin kullanımının ve yapay zeka modelleri oluşturmanın kalitesi ne kadar fazla olursa siber tehditlere karşı daha iyi savunma ortaya çıkar. Bu yüzden, saldırı için yapay zeka kullanımına karşın savunma için de yapay zeka kullanımı elzem bir hale gelmektedir. Son dönemlerde, gerek zeki saldırıların gerekse karşı zeki savunmanda kullanılan ve başarılı olan çözümlere odaklanan çalışmalar artış göstermektedir.

13.4. Büyük Verinin Güvenliği

Uluslararası avantaj arayan ve üstünlük kurmak isteyen devlet aktörleri, istihbarat elde etmek isteyen rakipler, para kazanmak isteyen suçlular, siyasi/dini/ideolojik amaçlı hacktivistler, hizmet aksattırmayı amaçlayan veya yeteneklerini test eden korsanlar ya da intikam almak isteyen çalışanlar, kurum ve kuruluşların en değerli varlıkları olan büyük verilerine göz dikebilir. Bu sebeple, büyük veri ekosistemi bütüncül bir şekilde ele alınarak her aşamada oluşabilecek riskler çok iyi değerlendirilmelidir. Altyapı güvenliği, veri gizliliği, veri yönetimi ve reaktif güvenlik olarak dört ana grup altında değerlendirilen büyük veri zorlukları [15] ve alınabilecek önlemler kısaca aşağıda özetlenmiştir [12], [14], [16].

1. Mevcut güvenlik çözümleri çoğu zaman NoSQL veritabanları ve dağıtık hesaplama sistemlerini her açıdan garanti altına alamamaktadır.
2. Erişim kontrolü, şifreleme ve bağlantı güvenliği işlemlerinin hızla gerçekleştirilmesi ve güncel olması gerekmektedir.
3. Veri aktarımı süreçleri, ek güvenlik önlemleri gerektirmektedir.
4. BT uzmanlarının, kullanıcıların mahremiyet hakkını göz ardı ederek kişisel verilerini analiz edebilme ihtimali bulunmaktadır.
5. Pekçok farklı kaynaktan beslenen büyük hacimli verilerin kökeninin doğrulanamaması, analiz sonuçlarını da negatif yönde etkilemektedir.

6. Bulutta saklanan veriler, siber casusluk harekatlarında kullanılma riski altındadır.
7. İzinsiz erişim ihtimalleri göz önünde bulundurularak; kod, nesne ve model değişikliklerinin izlenmesi gerekmektedir.
8. Veri toplayan cihazlara özgü güvenlik gereksinimleri karşılanmalıdır.
9. Herhangi bir şekilde sızma gerçekleşse bile veri gizliliğinin sağlanabilmesi için; şifreleme, anonimleştirme ve genelleştirme işlemlerinin uygulanması gerekmektedir.
10. Kuruluşlar, bir bulut sağlayıcısı gibi bir üçüncü tarafın verileri kendi adına işlediğinde bile güvenliğini garanti etmek zorundadır.
11. Uyum yasalarıyla verilerinin ömrü boyunca uyulması gerekmektedir.

13.5. Değerlendirmeler

Geleneksel güvenlik çözümleri artık gerçek zamanlı, büyük hacimli, akan veriler için yetersiz kalmaktadır. Bu noktada büyük veri yaklaşımları en güncel çözümlerin başında gelmektedir. Son dönemde yapılan çalışmalar, büyük veri alanında başarılar sağlandığını gösterse de bu yeni teknolojilerin yeni tehdit ve tehlikeleri de beraberinde getireceği unutulmamalıdır.

Kullanılan büyük veri teknik ve teknolojileri; her ne kadar yüksek seviyede siber güvenlik sağlanmasına destek olsa da mevcut çözümlerden görülen odur ki her sorun için mükemmel çözüm sağlamazlar. Güvenlik uzmanları, karmaşık saldırıları keşfetmenin yeni yollarını aramaya devam edeceklerdir ve etmelidirler de.

Yakın gelecekte, siber güvenliği sağlamada yeni yaklaşımların, metodolojilerin ve stratejilerin üretilmesi için büyük veri teknolojilerinin daha etkin çözümler sunacağından şüphemiz yoktur. Bunu yapanların ise verilere, veri işleme ortamlarına ve veri işleme uzmanlarına ihtiyaç duyacakları muhakkaktır.

Ülkemizde bu konularda çalışan akademisyenlerin olduğu bilinse de bunların sayısının yetersiz olduğu, sahip olunan laboratuvar kapasitelerinin istenilen seviyelerde olmadığı, en önemlisi ise bu ortamlar için çözüm geliştirilecek büyüklükte verilere araştırmacıla-

rın sahip olmadığı bilindiğinden, yakın bir gelecekte bu konularda etkin çözümlerin geliştirilmesi ne yazık ki beklenilmemektedir.

Kaynaklar

[1] Bart Custers, Jaap van den Herik, Cees T. A. M. de Laat, Michel Rademaker, Cor Veenman, "Enabling Big Data Applications for Security - Responsible by Design", The Hague Security Delta, 2017.

[2] Mike Baccala, Chris Curran, Dan Garrett; Scott Likens, Anand Rao, Andy Ruggles, Michael Shehab, "2018 AI predictions 8 insights to shape business strategy", PwC, 2018.

[3] Tariq Mahmood, Uzma Afzal, "Security Analytics: Big Data Analytics for cybersecurity: A review of trends, techniques and tools", 2nd National Conference on Information Assurance (NCIA), 2013.

[4] Nir Kshetri, "Big data's impact on privacy, security and consumer welfare", Telecommunications Policy, vol.38, no.11, pp.1134-1145, 2014.

[5] S. Sandeep Sekharan, Kamalanathan Kandasamy, "Profiling SIEM tools and correlation engines for security analytics", International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 717-721, 2017.

[6] Christiaan Beek, Taylor Dunton, Steve Grobman, Mary Karlton, Niamh Minihane, Chris Palm, Eric Peterson, Raj Samani, Craig Schmugar, ReseAnne Sims, Dan Sommer, Bing Sun, "McAfee Labs Threats Report - June 2018", McAfee, 2018.

[7] Rossouw Von Solms, Johan Van Niekerk, "From information security to cyber security", Computers & Security, vol.38, pp. 97-102, 2013.

[8] Aftab Jamil, Brian Berning, Tim Clackett, Slade Fester, Demetrios Frangiskatos, Hank Galligan, Bryan Lorello, Anthony Reh, David Yasukochi, "8 Tech Predictions for 2018 Scaling Up the Disruption", BDO, 2018.

[9] Joey Cusimano, "The 6 D's of Cyber Security", InfoSec Institute, 2015.

[10] Alvaro A. Cárdenas, Pratyusa K. Manadhata, Sreeranga P. Rajan, "Big Data Analytics for Security", IEEE Security & Privacy, vol.3, no.6, pp.74-76, 2013.

[11] Duygu Sinanc Terzi, Ramazan Terzi, Seref Sagiroglu, "A survey on security and privacy issues in big data", 10th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 202-207, 2015.

[12] Gang Zeng, "Big Data and Information Security", International Journal of Computational Engineering Research, vol.5, no.6, pp.17-21, 2015.

[13] Mark Seward, Fred Wilmot, "Big Data and Security: At the Edge of Prediction", RSA Conference, 2013.

[14] Renu Kesharwani, "Enhancing Information Security in Big Data", International Journal of Advanced Research in Computer and Communication Engineering, vol.5, no.8, pp.323-327, 2016.

[15] Big Data Working Group, "Expanded Top Ten Big Data Security and Privacy Challenges", Cloud Security Alliance, 2013.

[16] Ernesto Damiani, Claudio Agostino Ardagna, Francesco Zavatarelli, Evangelos Rekleitis, Louis Marinos, "Big Data Threat Landscape and Good Practice Guide", European Union Agency For Network And Information Security, 2016.

Yazarların Özgeçmişleri



Prof. Dr. Mustafa ALKAN

- Gazi Üniversitesi Teknoloji Fakültesi Elektrik-Elektronik Mühendisliği Bölümü, Öğretim Üyesi, Ankara

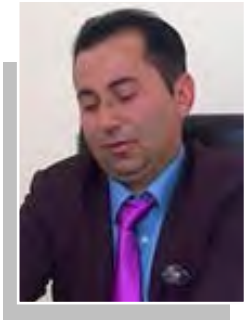
Prof. Dr. Mustafa Alkan Erciyes Üniversitesi Mühendislik Fakültesi Elektronik Mühendisliğinden Mezun olduktan sonra aynı üniversitede Araştırma Görevlisi olarak göreve başladı. Yüksek Lisans ve Doktorasını Elektronik Mühendisliği Anabilim Dalında tamamladı. 1988-1994 Yıllarında Türk Standartları Enstitüsü Kayseri Bölge Müdürlüğünde görev yaptı.

1994-2001 Yıllarında Niğde Üniversitesinde Elektrik-Elektronik Mühendisliği Bölüm Başkanlığı, Bilgi İşlem Merkez Müdürlüğü, Enformatik Bölüm Başkanlığı, Meslek Yüksekokulu Müdürlüğü görevlerinde bulundu. 1998 Yılında Doçent Oldu.

2001-2012 Yıllarında Bilgi Teknolojileri ve İletişim Kurumunda Kurum Başkan Yardımcısı olarak görev yaptı,

2012 Yılında Gazi Üniversitesi Teknoloji Fakültesi Elektrik Elektronik Mühendisliği Bölümüne Prof. olarak atandı aynı bölümde Bölüm Başkanı olarak 2012-2015 yıllarında görev yaptı.

Türkiye Bilişim Konseyi Kurucusu ve Bilgi Güvenliği Derneği Kurucusu ve Başkanlığı görevinde bulundu.



Arş. Gör. Ömer ASLAN

- Siirt Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Araştırma görevlisi, Siirt

- Ankara Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Doktora öğrencisi, Ankara

Kilis doğumlu olan Aslan, yüksek lisansını Teksas Üniversitesinde bilgi güvenliği ve bulut teknolojileri üzerine yapmış olup, ülkemizde bilgi güvenliği, siber güvenlik ve kötü amaçlı yazılım analizi gibi alanlarda çalışmalar yapmaktadır. 7 tane uluslararası yayınlanmış bildirisi bulunmaktadır.

Halen; Ankara Üniversitesi Bilgisayar Mühendisliği Bölümünde Kötü amaçlı yazılım analizi ve tespitiyle ilgili doktora çalışması yapmaktadır ve Siirt üniversitesinde Arş. Gör. olarak çalışmaktadır.

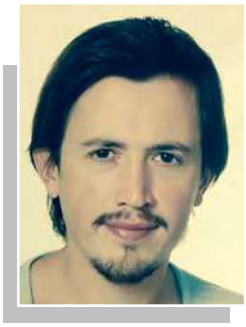


Dr. Öğretim Üyesi Atila BOSTAN

- Atılım Üniversitesi, Bilgisayar Mühendisliği Bölümü, Öğretim Üyesi, Ankara

Bilgisayar güvenliği, sayısal ağlar ve görüntü işleme konularında araştırmalar yapmakta olan Atila Bostan, Türk Silahlı Kuvvetlerinin çeşitli kademelerinde yirmı yıl otomatik bilgi işlem subaylığı yapmıştır. Emekliliğini müteakiben, halen devam etmekte olduğu, Atılım Üniversitesi, Bilgisayar Mühensilği Bölümünde öğretim üyesi olarak göreve başlamıştır. Dr. Bostan'ın "Experiments on Computer Networks" isminde bir yayınlanmış kitabı bulunmaktadır. Ayrıca, gerçek hava boşluğu ile ağlar arasında bilgi aktarma ve temassız kart okuma kontrolü konularında iki adet patent sahibi olan Bostan'ın 15 uluslararası dergi makalesi ve 40 uluslararası konferans bildirisi bulunmaktadır.

TSK ve NATO bilgi sisemleri ve harekat birlikleri bilgisayar ağ desteği konularında birçok proje yöneten Dr. Bostan, NATO ve TSK Üstün Hizmet madalyalarının sahibidir. Ayrıca, Atılım Üniversitesi Bilgisayar Mühendisliği Bölünmünde bilgisayar güvenliği konusunda yürüttüğü projelerle IBM firması tarafından 2009 ve 2011 yıllarında iki kez "IBM Shared University Research Award" ödülünü kazanmıştır. Dr. Atila Bostan, bilgisayar güvenliği, bilgisayar ağları ve görüntü işleme alanlarında uluslarası dergilerde editörlük, makale hakemliği, konferanslarda teknik komite ve bildiri hakemliği yapmaktadır.



Dr. Öğretim Üyesi İbrahim Alper DOĞRU

- Gazi Üniversitesi Teknoloji Fakültesi Bilgisayar Mühendisliği Bölümü, Öğretim Üyesi, Ankara

Tokat ili Erbaa ilçesinde doğan İbrahim Alper Doğru, İlk ve Orta Öğrenimini Tokat'ta tamamladı. Atılım Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliğinden Mezun olduktan sonra Emniyet Genel Müdürlüğü Bilgi İşlem Dairesi başkanlığında Bilgisayar Mühendisi olarak göreve başladı. Yüksek Lisansını Gazi Üniversitesinde Bilgisayar Mühendisliği Anabilim Dalında, doktorasını Gazi Üniversitesinde Elektronik Bilgisayar Eğitimi Anabilim Dalında tamamladı. 2017-2018 Yıllarında Başbakanlık Gümrük Müsteşarlığı Elektronik ve Muhabere Dairesi Başkanlığı çözümleyici; 2018-2011 Sosyal Güvenlik Kurumu Hizmet Sunumu Genel Müdürlüğünde bilişim uzmanı, 2011-2013 yıllarında Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliğinde Araştırma Görevlisi olarak görev yaptı. 2012 Yılında Gazi Üniversitesi Teknoloji Fakültesi Bilgisayar Mühendisliği Bölümüne Dr. Öğretim Üyesi olarak atandı aynı bölümde akademik çalışmalarını sürdürmektedir.



Dr. Murat DÖRTERLER

- Gazi Üniversitesi Teknoloji Fakültesi Bilgisayar Mühendisliği Bölümü Öğretim Görevlisi, Ankara

Kayseri doğumlu olan Dörterler, 2005 yılında Gazi Üniversitesi Bilgisayar Sistemleri Anabilim Dalında Lisans eğitimini tamamladı. Aynı ünivresitenin Elektronik-Bilgisayar Anabilim Dalı'ndan 2008 yılında yüksek lisans, 2013 yılında doktora derecelerini aldı.

2005 yılında Milli Eğitim Bakanlığında çalışma hayatına başlayan Dörterler, 2009 yılına kadar bakanlığın taşra ve merkez teşkilatlarında eğitim-öğretim ve e-dönüşüm süreçlerinde görevler almıştır. 2009 yılından günümüze kadar Gazi üniversitesinin çeşitli birimlerinde akademik çalışmalarını sürdürmektedir.

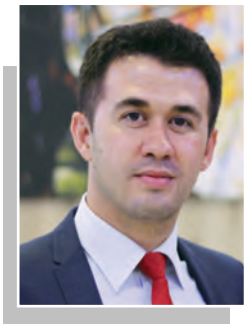
Dörterler'in Yapay Zekâ, Zeki Optimizasyon, Gömülü Sistemler, Yazılım, Dağıtık Sistemler, Bilgi Güvenliği başta olmak üzere çeşitli alanlarda ulusal ve uluslararası mecralarda bildiri, yayın ve projeleri bulunmaktadır. Gazi Mühendislik Bilimleri Dergisi'nin editörlüğünü yapmaktadır. İyi derecede İngilizce bilmektedir. Evli ve İki çocuk babasıdır.



Dr. Ahmet EFE

- Ankara Kalkınma Ajansı İç Denetçisi, CISA, CRISC, PMP

Doğubayazıt doğumlu olan EFE, iktisat, akmu yönetimi, e-devlet ve siber güvenlik alanllarında çoklu disipliner çalışmalar yapmaktadır. Kamu sektöründe müfettişlik, yöneticilik ve iç denetçilik kariyerinde çalışmaya devam etmekte olup, Certified İnformation Systems Auditor(CISA), Certified in Risk and İnformation Control (CRISC) ve Project Management Professional (PMP) gibi uluslararası kabul gören mesleki sertifikaları vardır. Yıldırım Beyazıt Üniversitesi Bilgisayar Mühendisiliği Bölümünde siber güvenlik ile ilgili yüksek lisans ve doktora düzeyinde dersler vermektedir. Yayımlanmış 5 kitabı ve 46 Makalesi ile 2018 yılında ISACA tarafından BT Alanında en iyi yazar ödülüne layık görülmüştür. Evli 4 çocuklu olan EFE; İngilizce ve Arapça bilmektedir.



Salih Erdem EROL

Hava Harp Okulu Bilgisayar Mühendisliği bölümünden 2009 yılında mezun olmuştur. Yüksek Lisans eğitimini Gazi Üniversitesi Fen Bilimleri Enstitüsü Bilgi Güvenliği Mühendisliği bölümünün ilk mezunu olarak 2016 yılında tamamlamıştır. Gazi Üniversitesi Bilişim Enstitüsü Adli Bilişim Anabilim Dalında doktora eğitimine devam etmektedir.

Yazılım proje yöneticiliği, kurumsal bilgi güvenliği denetçiliği gibi alanlarda mesleki tecrübesi, bilgi güvenliği farkındalığına yönelik sosyal sorumluluk projelerine katkıları bulunmaktadır.

Bilgi güvenliği, bilgi güvenliği farkındalığı, yapay sinir ağları ve adli bilişim alanına ilişkin çalışmalar yürütmektedir.



Dr. Cengiz PAŞAOĞLU

- Kişisel Verileri Koruma Kurulu Üyesi, Ankara

Dr. Cengiz Paşaoğlu, 1979 yılında Trabzon'da doğmuştur. Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Elektrik-Elektronik Mühendisliği Bölümünden Lisans, Fen Bilimleri Enstitüsü Elektrik-Elektronik Mühendisliği Anabilim Dalından sırasıyla Yüksek Lisans ve Doktora derecelerini almıştır. 2002- 2016 yılları arasında DHMİ Genel Müdürlüğü'nde çalışmış, birçok ulusal ve uluslararası Ar-Ge projelerinde görev almıştır. DHMİ Genel Müdürlüğü Elektronik Başkan Yardımcı olarak görev yaparken, TBMM Genel Kurulu'nun 05 Ekim 2016 tarihli kararıyla Kişisel Verileri Koruma Kurulu üyeliğine seçilmiştir. İstanbul Teknik Üniversitesi Uçak Mühendisliği Bölümünde Aviyonik Navigasyon Sistemleri konusunda lisansüstü, Gazi Üniversitesi Bilgisayar Mühendisliği Bölümünde Veri Mahremiyetine Giriş konusunda lisans derslerini vermekte ve hava trafik kontrol karar destek sistemleri, hava trafik kontrol sistemlerinde yüksek seviye otomasyon, haberleşme seyrüsefer gözetim sistemleri, hava çarpışma önleme sistemleri, insansız hava araçlarının ulusal hava sahalarına entegrasyonu, kişisel veri mahremiyeti, kişisel veri güvenliği, büyük ve açık veri, kişisel verilerin anonim hale getirilmesi gibi konularda araştırma ve çalışmalarına devam etmektedir. Çeşitli konferans ve dergilerde bilimsel yayınları bulunmaktadır.



Prof. Dr. Refik SAMET

- Ankara Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü Öğretim Üyesi, Ankara

Azerbaycan doğumlu olan Samet, ülkemizde bilgisayar sistemlerinin güvenilirliği, arıza-kaldırılabilirliği, bilgi güvenliği, siber güvenlik, kötü amaçlı yazılım analizi ve adli bilişim konularında çalışmalar yapmaktadır. 6 patenti, 1 kitabı ve 3 kitap bölümü bulunmaktadır. 50'ye yakın ulusal ve uluslararası indeksli dergilerde yayınlanmış makalesi ile 60'ın üzerinde ulusal ve uluslararası yayınlanmış bildirisi bulunmaktadır. 50'in üzerinde TÜBİTAK, NATO, Avrupa Birliği, BAP gibi Bilimsel Araştırma ve Üni-

versite Sanayi İşbirliği Projelerinde görev almış ve projeler yürütmüştür. Birçok Ulusal ve Uluslararası Bilim Konferanslarında ve Dergilerinde Bilim Kurulu üyeliği yapmaktadır.

Halen Ankara Üniversitesi Bilgisayar Mühendisliği Bölümünde Profesör olarak çalışmaktadır.



Prof. Dr. Şeref SAĞIROĞLU

- Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölüm Başkanı, Ankara

Antalya doğumlu olan Sağıroğlu, ülkemizde bilgi güvenliği, siber güvenlik ve büyük veri bilimi, analitiği, güvenliği ve mahremiyeti konularında çalışmalar yapmaktadır. 15 yayınlanmış kitabı bulunmaktadır. Bu kitaplardan sonuncusu "Büyük Veri Analitiği, Güvenliği ve Mahremiyeti" olup ülkemizde bu alanda yayımlanan ilk akademik kitap olup, açık kaynak olarak okuyuculara sunulmaktadır. Biri amerikan patenti olmak üzere 4 patenti, 100'ün üzerinde ulusal ve uluslararası indeksli dergilerde yayınlanmış makalesi ile 300'e yakın ulusal ve uluslararası yayımlanmış bildirisi ve 3000'in üzerinde atıfı bulunmaktadır. Bilgi güvenliği alanında iki akademik derginin de editörlüğünü yapmaktadır.

Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (www.iscturkey.org), IEEE Uluslararası Bilgisayar Bilimleri ve Mühendisliği Konferansı (www. ubmk.org), IEEE Uluslararası Makine Öğrenmesi ve Uygulamaları Konferansı Büyük Veri ve Siber Güvenlik Oturumu (www.icmla-conferences.org/ icmla2017), Büyük Veri Analitiği, Güvenliği ve Mahremiyeti Ulusal Kamu Çalıştayı (bigdatacenter.gazi.edu.tr), Ulusal Siber Terör Konferansı (www.siberteror.org), Açık Veri Türkiye Konferansı (www.acikveriturkiye.org), Siber Güvenlik ve Savunma Çalıştayı (www.iscturkey.org) gibi konferansların başkanlığını veya eşbaşkanlığını yürütmektedir.

Bilgi Güvenliği Derneği (BGD), Türk Bilim Araştırma Vakfı (TÜBAV), Geleceği Önemseyenler Derneği (GÖNDER) Kurucu Üyesidir. İki dönem, BGD Yönetim Kurulu Başkanlığı ve TÜBAV Genel Başkanlığı Gazi Üniversitesi Fen Bilimleri Enstitüsü Müdürlüğü gibi görevleri yürütmüştür.

Gönüllü olarak pekçok sosyal projeyi de yürütmüş olan Sağıroğlu, TÜBİTAK, Avrupa Birliği, BAP gibi Bilimsel Araştırma Projelerde de görev almış ve projeler yürütmüştür.

Ulusal ve uluslararası konferanslarda, Bilgi Güvenliği, Büyük Veri, Siber Güvenlik ve Savunma, Yapay Zeka, Biyometrik Uygulamalar, İnovasyon Kültürü Oluşturma gibi konularda davetli konuşmacı olarak seminer ve konferanslar vermiştir.

Halen; Gazi Üniversitesi Bilgisayar Mühendisliği Bölüm Başkanlığı, BIDISEC Merkez Laboratuvarı Sorumlusu ISACA Ankara Chapter Akademi Koordinatörü, Yüksek Öğretim Kurulu Siber Güvenlik Çalışma Grubu Üyeliği, Bilim Sanayi ve Teknoloji Bakanlığı Yazılım Sektörü Çalışma Grubu Üyeliği, Bilgi Güvenliği Derneği Yönetim Kurulu Üyeliği gibi görevleri yürütmektedir. Havelsan ve Kişisel Verileri Korumu Kurumuna danışmanlık yapmaktadır.



Çağrı SÜMER

İlk, orta ve lise eğitimi sonrasında Türkiye derecesi ile Hacettepe Üniversitesi Tıp Fakültesini kazanıp 5 yıl okumuş olmasına rağmen idealleri doğrultusunda tekrar sınava girip kazanarak gene Hacettepe Üniversitesi Fizik Mühendisliği bölümünden 2014 yılında mezun oldu. Gerek Tıp Fakültesi gerekse Fizik Mühendisliği öğrenciliği sırasında canlı tuttuğu Siber Güvenlik, Bilgi Güvenliği, Kriptoloji ve Yapay Zeka alanlarındaki merak ve heyecanını; Gazi Üniversitesi Bilgi Güvenliği Mühendisliği'nde lisansüstü eğitimi süresince akademik olarak da zenginleştirmektedir. Son 5 yıldır Güney Kore ortaklı bir firmada Uluslararası İş Geliştirme Müdürü olarak görev yapmakta olan Çağrı Sümer evli ve 2 çocuk babasıdır.



Mustafa ŞENOL

- E. Tuğgeneral, Doktor adayı, İTÜ Bilişim Enstitüsü Bilgi Güvenliği Mühendisliği ve Kriptografi Programı, İstanbul.

- HAVELSAN Yönetim Kurulu Başkan Vekili, Ankara.

Kocaeli doğumlu olan Mustafa Şenol; 1977 yılında Kuleli Askeri Lisesi'nden sonra 1981 yılında Kara Harp Okulu (Elektrik-Elektronik Mühendisliği Bölümü)'ndan Muhabere Teğmen olarak mezun olmuştur. 1982 yılında Muhabere (MEBS) Okulu'nu bitirdikten sonra Kara Kuvvetlerine ve Genel Kurmay Başkanlığına bağlı birlik ve karargâhlarda çeşitli görevlerde bulunmuştur.

1991-1992 yıllarında A.B.D.'de Muhabere, Elektronik Bilgi Sistemleri ve Haberleşme Eğitimi görmüş, "IBM Bilgisayarları Oryantasyonu", "Bilgisayar Programlama" ve "İleri Seviye Amerikan İngilizcesi" konularında eğitimler almıştır

Kara Harp ve Silahlı Kuvvetler Akademisi eğitimlerinin ardından tabur / alay komutanlıkları ve karargâh görevleri ile Askerî Ataşelik görevi sonrasında 2009 yılında Tuğgeneralliğe terfi etmiş, iki yıl Tugay Komutanlığı görevinden sonra 2011 yılında Kara Kuvvetleri Muhabere Elektronik ve Bilgi Sistemleri (MEBS) Başkanlığı görevine atanmıştır.

Üç yıl süreli K.K.MEBS Bşk.lığı görevi sırasında Milli Güvenlik Akademisi'ni bitirmiş ve 30 Ağustos 2014 tarihinden itibaren, 40 yıllık askerlik yaşamından sonra kadrosuzluk nedeniyle emekli olmuştur.

2015-2017 yıllarında İstanbul Teknik Üniversitesi Bilişim Enstitüsü'nde "Bilgi Güvenliği Mühendisliği ve Kriptografi" programında Doktora eğitimi görmüş olup sırasıyla; "Siber Savaş (2012)", "Atatürk'ün Askerlik ve Liderlik Anlayışı (2016)", "Siber Güçle Caydırıcılık Ama Nasıl? (2017)", "Ulusal Siber Güvenlik Stratejisi Oluşturma ve Uygulama İçin Bir Yaklaşım" ve "Türkiye'de Siber Saldırılara Karşı Caydırıcılık (2017)" konularında çeşitli dergilerde yayımlanan 5 makalesi ile "Siber Terörizme Karşı Siber Savunma ve Caydırıcılık (2012)" konusunda Milli Güvenlik Akademisi için hazırlanan bir incelemesi bulunmaktadır. Ayrıca, Prof. Dr. Eşref Adalı tarafından yazılan; Bilgisayar ve Bilgi Güvenliği ve Yönetimi (2016) ve Bilişim Etiği ve Hukuku (2017) kitaplarının hazırlanmasında bulunmuş ve katkılar sunmuştur.

2017-2018 yıllarında bir yıl süreli TSK Mehmetçik Vakfı Genel Müdür Yardımcılığı görevinde bulunmuş olan E.Tuğg. Mustafa Şenol, halen 03 Mayıs 2018'de atanmış olduğu HAVELSAN-Hava Elektronik ve Ticaret Sanayi AŞ'nin Yönetim Kurulu Başkan Vekilliği görevini yürütmekte ve "Siber Güvenlik Stratejisi ve Caydırıcılık" konusundaki Doktora tez çalışmalarına devam etmektedir.

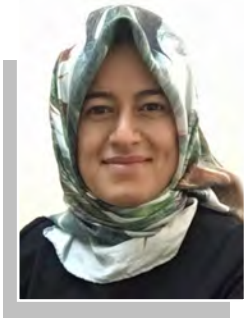


Dr. Öğretim Üyesi Gökhan ŞENGÜL

- Atılım Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, Ankara.

Ankara-Nallıhan doğumlu olan Şengül; görüntü ve sinyal işleme, örüntü tanıma, makine öğrenmesi, biyomedikal mühendisliği, bilgi güvenliği ve siber güvenlik konularında çalışmalar yapmaktadır. Şengül'ün 3 adet patenti, farklı ulusal ve uluslararası indeksli dergilerde yayınlanmış çok sayıda makalesi ve ulusal ve uluslararası yayımlanmış bildirileri bulunmaktadır.

Birçok TUBİTAK ve BAP projelerinde görev almış olan Şengül, halen Atılım Üniversitesi Bilgisayar Mühendisliği bölümünde öğretim üyesi olarak görev yapmaktadır.

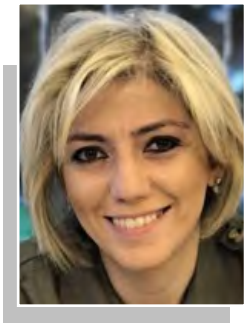


Arş. Gör. Duygu SİNANÇ TERZİ

- Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü Araştırma Görevlisi, Ankara.

Elazığ doğumlu olan Terzi, 2011 yılında Selçuk Üniversitesi Bilgisayar Mühendisliği bölümünde lisans ve 2014 yılında Gazi Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Ana Bilim Dalı'nda yüksek lisans eğitimini tamamlamıştır. 2014 yılından beri Gazi Üniversitesi'nde doktora çalışmalarına devam etmektedir. 2012 yılında Pamukkale Üniversitesi Fen Bilimleri Enstitüsü'nde Araştırma Görevlisi olarak çalışmıştır. Halen, Gazi Üniversitesi Bilgisayar Mühendisliği bölümünde Araştırma Görevlisi olarak ve Gazi Üniversitesi Büyük Veri ve Bilgi Güvenliği Laboratuvarı'nda (BIDISEC) araştırmacı olarak ça-

lışmaktadır. Büyük veri analizi, örüntü tanıma, anomali tespiti ve bilgi güvenliği gibi konular üzerinde akademik çalışmalarını sürdürmektedir.



Doç. Dr. Güzin ULUTAŞ

- Karadeniz Teknik Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü Öğretim Üyesi

Güzin Ulutaş, Trabzon doğumludur. 2002 yılında KTÜ Bilgisayar Mühendisliği Bölümünde Lisans eğitimini tamamlamış ve yine aynı bölümde 2004 yılına kadar araştırma görevlisi olarak görev yapmıştır. 2005-2009 yılları arasında Ondokuz Mayıs Üniversitesi Bilgisayar Mühendisliği Bölümde araştırma görevlisi olarak çalışan Ulutaş, 2012 yılında doktorasını tamamladıktan sonra KTÜ Bilgisayar Mühendisliği Bölümünde Dr. Öğr. Üyesi olarak atanmıştır. Lisans, Yüksek Lisans ve Doktora çalışmaları ağ güvenliği ve çokluortam güvenliği üzerinedir. Doktora sonrası çalışmalarını adli inceleme yöntemleri üzerine yönlendirmiştir. Ülkemizde bilgi güvenliği, siber güvenlik ve ağ güvenliği konularında çalışmalar yapmaktadır. 15 adet yayınlanmış ulusal ve uluslararası indekslerde taranan makalesi bulunmaktadır. 100'e yakın ulusal ve uluslararası yayımlanmış bildirisi vardır. Bilgi güvenliği alanında TÜBİTAK, BAP gibi Bilimsel Araştırma Projelerinde de görev almış ve projeler yürütmüştür. Bölümünde veritabanı, şifreleme ve ağ güvenliği, görüntülerde adli inceleme yöntemleri gibi lisans ve lisansüstü dersler vermektedir.



Rami URFALIOĞLU

1981 yılında Kilis'te dünyaya geldi. İlk, orta ve lise eğitimimi İstanbul'da tamamladı. 1999 yılında girmiş olduğu üniversite yerleştirme sınavı sonucunda Süleyman Demirel Üniversitesi Elektronik ve Haberleşme Mühendisliği bölümüne yerleşti. 2003 yılında bölüm birincisi olarak mezun oldu. 2009 yılında Gazi Üniversitesi Elektrik-Elektronik Mühendisliği anabilim dalında başlamış olduğu yüksek lisans eğiti-

mini 2011 yılında tamamladı. 2016 yılında Gazi Üniversitesi Bilgi Güvenliği Mühendisliği Anabilim Dalında doktora çalışmalarına başladı, halen doktora çalışması devam etmektedir.



Dr. Yılmaz VURAL

Kişisel Verileri Koruma Kurumu, Daire Başkanı, Ankara

Dr. Yılmaz Vural, 1974 yılında Kahramanmaraş'ta doğmuştur. Trakya Üniversitesi Mühendislik Mimarlık Fakültesi Bilgisayar Mühendisliği Bölümünden Lisans, Gazi Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalından Yüksek Lisans ve Hacettepe Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalından Doktora derecelerini almıştır. 20 yılın üzerinde sektör tecrübesine sahip olan Dr. Vural Hacettepe Üniversitesi Bilişim Enstitüsü ve Gazi Üniversitesi Bilgisayar Mühendisliği bölümlerinde Bilgi Güvenliği, Bilgisayar Ağları,Veri Mahremiyeti konularında lisans ve lisansüstü, derslerini vermektedir. Halen Kişisel Verileri Koruma Kurumu Veri Güvenliği ve Bilgi Sistemleri Daire Başkanı olarak görev yapmaktadır.

Dr Vural Veri Mahremiyeti, Siber Güvenlik, Büyük Veri, Nesnelerin İnterneti alanlarında araştırma ve çalışmalarına devam etmektedir. Ulusal ve uluslararası birçok konferans ve dergide bilimsel yayınları bulunmaktadır.



Doç. Dr. Yıldıray YALMAN

- Piri Reis Üniversitesi Mühendislik Fakültesi Elektrik-Elektronik Mühendisliği Bölümü, İstanbul

Doç. Dr. Yıldıray Yalman Kocaeli Üniversitesi Elektronik ve Bilgisayar Eğitimi Bölümünden 2004 yılında sınıf birinciliği ve bölüm üçüncülüğü derecesi ile mezun olmuştur. Aynı üniversitede Yüksek Lisans (2007) eğitimini, TÜBİTAK-2211 Yurtiçi Lisansüstü Burs Programı desteği ile de Doktora Eğitimini (2010) tamamlamıştır.

Temel çalışma alanları Bilgi Güvenliği, Güvenli Haberleşme, Sayısal Görüntü İşleme olup; ilgili alanlar çerçevesinde yayınlanmış çok sayıda ulusal ve uluslararası makale, ulusal ve uluslararası bildiri ve kitapları bulunmakta, Türkiye'de "Veri Gizleme" alanında basılan ilk Türkçe kitabın yazarları arasında yer almaktadır.

TÜBİTAK, KOSGEB ve Üniversiteler tarafından desteklenen Bilimsel Araştırma Projelerinde (BAP) yürütücü, danışman ve araştırmacı olarak görevler almış olan Doç. Dr. Yalman, kırkın üzerinde dergi ve konferansın hakem ve yayın kurulunda görev almakta; "Information Engineering and Applied Computing (http://ojs.whioce.com/index.php/ieac)" isimli derginin Bilgi Güvenliği ve Sayısal Görüntü İşleme başlıklarındaki alan editörlüğünü yürütmektedir.

Halen görev yapmakta olduğu üniversitede C/C++ Programlama, Görsel Programlama, Bilgi Güvenliği, Görüntü İşleme, Bilgisayar Ağları ve Mikroişlemciler derslerini vermektedir.

Bilgi Güvenliği Derneği (BGD), kuruluşundan bugüne kadar ülkemizin "**Siber Güvenlik ve Savunmasının**" gelişimine katkı sağlamakta, birikimini topluma aktarmakta, içerik üretilmesine, yeni çözümler geliştirilmesine ve bilginin yaygınlaştırılmasına destek vermekte, kamuoyunun farkındalığını artırmaya çalışmakta, ve sonuçta siber ve bilgi güvenliğinin kişisel, kurumsal ve ulusal boyutta sağlanmasına katkılar sunmaktadır.

Tehditlerin artması, boyut ve yön değiştirmesi, çeşitlerinin artması, siber tehdit ekosisteminin büyümesi, kritik altyapıların hedef haline gelmesi, bilgi hırsızlıklarının çoğalması, yeraltında çalışan konsanların etkinleşmesi, siber tehditlerin artık savaşa dönüşmesi, siber suçların ve suçluların çoğalması, siber terörün artması nedeniyle, siber saldırılarla, suçlarla, terörizmle, zafiyetlerle mücadeleye her zamankinden daha fazla ihtiyaç duyulmaktadır. Kapsamlı bir mücadele için; ulusal stratejileri ve eylem planlarının hayata geçirilmesi, etkili araştırma merkezlerinin açılması, yeni altyapılar kurulması, yeni programların açılması ve son zamanlarda ise "siber ordular", "mükemmelliyet merkezleri", "ulusal siber olaylara müdahale", "siber savunma ajansı" gibi yapıların kurulması, vb. ihtiyaçlar bizleri bu kitap serisini hazırlamaya yöneltmiştir. Tehditlerin boyutunu ve geleceğini anlamak ancak ve ancak bu alanın kapsamını iyi anlamak, gelecekte karşılaşılacak olan tehditleri öngörmek, buna hazır olmak için konunun etkileşim içerisinde olduğu tüm alanları iyi bilmek, etkileşim içerisinde olunan alanları iyi tanımak, yeni alanları öğrenmek gerekmektedir. Siber güvenlik ve savunmaya kapsamlı bir bakış sunmayı amaçlayan bu eser serisinin, ülke siber güvenliğimiz ve savunmasına katkı sağlaması beklenmektedir.

HAVELSAN Bu kitap HAVELSAN'nın katkılarıyla basılmıştır.

ISBN : 978-605-2233-22-1

9 786052 233221

grafiker.com.tr • 0 312. 284 16 39