T.C.
RADYO VE TELEVİZYON ÜST KURULU

SİBER GÜVENLİK ALANINDA OLUŞABİLECEK TEHDİTLERİN İNCELENMESİ VE ÇÖZÜM ÖNERİLERİ

UZMANLIK TEZİ

PELİN SAYICI GÜLER

ANKARA
ARALIK, 2022


RTÜK
RADYO VE TELEVİZYON ÜST KURULU

T.C.
RADYO VE TELEVİZYON ÜST KURULU

SİBER GÜVENLİK ALANINDA OLUŞABİLECEK TEHDİTLERİN İNCELENMESİ VE ÇÖZÜM ÖNERİLERİ

UZMANLIK TEZİ

PELİN SAYICI GÜLER

DANIŞMAN: ÜST KURUL UZMANI SEYDA MENTEŞ

ANKARA
ARALIK, 2022

Radyo ve Televizyon Üst Kurulu Başkanlığına,

Pelin SAYICI GÜLER adlı Üst Kurul Uzman Yardımcısının hazırladığı "Siber Güvenlik Alanında Oluşabilecek Tehditlerin İncelenmesi ve Çözüm Önerileri" başlıklı bu çalışma Tez Değerlendirme Komisyonu üyelerince oy birliği / oy çokluğu ile **Uzmanlık Tezi** olarak kabul edilmiştir.

	Komisyon Üyeleri	İmza
Başkan	Ebubekir ŞAHİN Üst Kurul Başkanı	……..
Üye	Deniz GÜÇER Üst Kurul Üyesi	……..
Üye	Dr. İbrahim USLU Üst Kurul Başkan Yardımcısı	……..
Üye	Deniz GÜLER Daire Başkanı	……..
Üye	Seyda MENTEŞ Üst Kurul Uzmanı (Tez Danışmanı)	……..

ONAY

Bu tez Radyo ve Televizyon Üst Kurulu Uzmanlığı Yönetmeliği'nin ilgili maddeleri uyarınca …/…/20... tarihinde kabul edilmiştir.

Ebubekir ŞAHİN
Üst Kurul Başkanı

ETİK İLKELERE UYGUNLUK BEYANI

Bu tez çalışmasında;

Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,

Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,

Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,

Kullanılan verilerde ve ortaya çıkan sonuçlarda herhangi bir değişiklik yapmadığımı,

Sunduğum çalışmanın özgün olduğunu bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim. 20/12/2022

Pelin SAYICI GÜLER

Üst Kurul Uzman Yardımcısı

TEŞEKKÜR

"Siber Güvenlik Alaninda Oluşabilecek Tehditlerin İncelenmesi ve Çözüm Önerileri" isimli bu tezin hazırlanması sürecine ilişkin olarak; Sayın Radyo ve Televizyon Üst Kurulu Başkanı Ebubekir ŞAHİN ve Üst Kurul üyelerine, Üst Kurul Başkan Yardımcıları Sayın İbrahim USLU ve Sayın Orhan ÖZDEMİR'e, İzin ve Tahsisler Dairesi Başkanı Sayın Aydın DEMİR'e, Daire Başkan Yardımcıları Sayın Ali SARI ve Sayın Yasin YİĞİT'e, çalışmalarım süresince beni destekleyen tez danışmanım Üst Kurul Uzmanı Sayın Seyda MENTEŞ'e, çalışmalarım esnasında yardımlarını esirgemeyen arkadaşım Hazal ZORAL GEMALMAZOĞLU'na ve İzin ve Tahsisler Dairesi Başkanlığı personellerinden değerli mesai arkadaşlarıma teşekkürlerimi sunarım.

Ayrıca her daim iyi dilek ve temennileriyle yanımda olan, desteklerini her zaman arkamda hissettiğim çok kıymetli ailem Ayşe ve Nedim SAYICI'ya ve sevgili eşim Aykut GÜLER'e teşekkür ederim.

ÖZET

SİBER GÜVENLİK ALANINDA OLUŞABİLECEK TEHDİTLERİN İNCELENMESİ VE ÇÖZÜM ÖNERİLERİ

SAYICI GÜLER, Pelin
Uzmanlık Tezi
Tez Danışmanı: Üst Kurul Uzmanı Seyda MENTEŞ
Aralık, 2022, 107

Günümüz dünyasında dijital teknoloji kullanımı giderek artmaktadır. İnsanlar bilişim sistemlerine her geçen gün daha da bağımlı bir hale gelerek hayatlarının neredeyse her alanında kullanmaya devam etmektedir. Ayrıca bir çok alanda verilerin dijital ortama aktarılarak kullanılmaya başlanmasıyla da birlikte bireyler, kurumlar ve ülkeler kapsamında siber ortamın güvenliği konusunda çeşitli sorunlar ortaya çıkmaya başlamıştır. Bu durum veri ihlalleri ve siber saldırıları daha yaygın bir hale getirmiştir. Böylece siber güvenlik alanı son zamanlarda en çok önem verilen konulardan birisi haline gelmiştir.

Çoğu alanda bilgi ve iletişim teknolojilerinin yaygın olarak kullanımı ile birlikte etkin bir siber güvenlik korunması gerektiği ortaya çıkmıştır. Aksi halde işlerin sekteye uğraması, iş sürekliğinin sağlanamaması, itibar kaybı, bilginin ve gizliliğin korunamaması, verilerin ifşa edilmesi ve korunamaması gibi olumsuz durumlarla karşılaşılmaktadır.

Bu tez çalışmasında, siber kavramı ele alınarak siber unsurlardan bahsedilmiş ve siber ortamdaki tehditler, saldırı çeşitleri, amaçları ve zararlı yazılımlar incelenmiştir. Siber saldırganların izledikleri yol ve yöntemler anlatılmış ve verilen zararlardan bahsedilmiştir. Ülkemizde siber güvenlik alanında faaliyet gösteren kurum ve kuruluşlar incelenmiş ve işleyiş biçimleri gösterilmiştir.

Ülkemiz ve dünyadaki büyük çaptaki siber saldırı örneklerine yer verilerek siber güvenlik kapsamında çıkarılması gereken dersler ele alınmıştır. Bunun yanında bireysel,

kurumsal ve ulusal alanda gereken tedbirler ve önlemler anlatılarak dikkat edilmesi gereken durumlar ve ortaya çıkabilecek olumsuz sonuçlar vurgulanmıştır.

Anahtar Sözcükler: Siber Güvenlik, Siber Saldırı, Siber Tehdit, Siber Farkındalık, Siber Önlem

ABSTRACT

INVESTIGATION OF THREATS THAT MAY OCCUR IN THE FIELD OF CYBER SECURITY AND SUGGESTIONS FOR SOLUTIONS

SAYICI GÜLER, Pelin

Specialization Thesis

Thesis Advisor: Supreme Council Expert Seyda MENTEŞ

December, 2022, 107

In today's world, the use of digital technology is increasing. People become more and more dependent on information systems and continue to use them in almost every aspect of their lives. In addition, with the transfer of data to digital media in many areas, various problems have begun to arise about the security of the cyber environment within the scope of individuals, institutions and countries. This has made data breaches and cyber attacks more common. Thus, the field of cyber security has recently become one of the most important issues.

With the widespread use of information and communication technologies in many areas, it has emerged that an effective cyber security protection is required. Otherwise, negative situations such as disruption of business, failure to ensure business continuity, loss of reputation, failure to protect information and confidentiality, disclosure and failure to protect data are encountered.

In this thesis, the concept of cyber is discussed and cyber elements are mentioned and threats, attack types, purposes and malicious software in the cyber environment are examined. The ways and methods followed by cyber attackers are explained and the damages inflicted are mentioned. Institutions and organizations operating in the field of cyber security in our country have been examined and their functioning has been shown.

By giving examples of large-scale cyber attacks in our country and in the world, lessons to be learned within the scope of cyber security are discussed. In addition, the necessary precautions and precautions in the individual, institutional and national areas are

explained and the situations that need attention and the negative consequences that may arise are emphasized.

Key Words: Cyber Security, Cyber Attack, Cyber Threat, Cyber Awareness, Cyber Precaution

İÇİNDEKİLER

ETİK İLKELERE UYGUNLUK BEYANI iii
TEŞEKKÜR iv
ÖZET v
ABSTRACT vii
İÇİNDEKİLER ix
TABLOLAR DİZİNİ xiii
ŞEKİLLER DİZİNİ xiv
KISALTMALAR/SİMGELER xv
GİRİŞ 1
Problem 1
Amaç 2
Önem 2
Sınırlılıklar 3
Tanımlar 3
Yöntem 3
Verilerin Toplanması 4
Verilerin Çözümlenmesi 4
BÖLÜM 1
SİBER GÜVENLİKLE İLGİLİ KAVRAMLAR 5
1.1. Siber 5
1.2. Siber Uzay 5
1.3. Siber Güvenlik 6
1.4. Siber Güvenlik Unsurları 9
1.4.1. Uygulama Güvenliği 9
1.4.2. Bilgi Güvenliği 10
Bilgi Güvenliğinin Temel İlkesi 10
1.4.2.1. Gizlilik 11
1.4.2.2. Bütünlük 11
1.4.2.3. Erişebilirlik 12
1.4.3. Ağ Güvenliği 15
1.4.4. Olağanüstü Durum Kurtarma/İş Sürekliliği Planlaması 16
1.4.5. Operasyonel Güvenlik 17

1.4.6. Son Kullanıcı Eğitimi 18
1.5. Siber Suç 19
BÖLÜM 2
SİBER SALDIRI TEHDİTLERİ, TÜRLERİ VE ÖRNEKLERİ 22
2.1. Siber Saldırı Tehditleri 22
2.2. Siber Saldırı Türleri 23
2.2.1. Zararlı Yazılımlar 24
2.2.2. Virüsler 26
2.2.3. Solucanlar (Worm) 27
2.2.4. Truva Atları (Trojenler) 29
2.2.5. Fidye Yazılım (Ransomware) 30
2.2.6. Casus Yazılım (Spyware) 31
2.2.7. Klavye Kaydedici (Keylogger) 32
2.2.8. Oltalama Saldırıları (Phishing Attacks) 32
2.2.9. Rootkit 34
2.2.10. DDoS (Hizmet Dışı Bırakma) Saldırıları 35
2.2.11. BOTNET (Bot Networks) 37
2.2.12. Ortadaki Adam (Man in the middle-MITM) 39
2.2.13. SQL Enjeksiyonu (SQL İnjection) Saldırısı 40
2.2.14. IP Sahteciliği (IP Spoofing) 41
2.2.15. Kimlik Bilgileri Doldurma Saldırıları (Credential Stuffing) 42
2.2.16. Siteler Arası Betik Çalıştırma (XSS Zafiyeti (Cross-Site Scripting)) 44
2.2.17. İstem Dışı Alınan E-posta Saldırıları (SPAM) 45
2.2.18. Sosyal Mühendislik Saldırıları 46
2.2.18.1. Sosyal Mühendislik Saldırılarında KullanılanYöntemler 49
2.2.18.1.1. Tersine Sosyal Mühendislik (RSE-Reverse Social Engineering) 50
2.2.18.1.2. Sırtına Binme (Piggyback Rides) Tekniği 51
2.2.18.1.3. Teknik konuşma (Technical Talk) 51
2.2.18.1.4. Balina Avı (Whaling) 51
2.2.18.1.5. Sesle Oltalama (Vishing- Voice Phishing) 52
2.2.18.1.6. Çöp Karıştırma 52
2.2.18.1.7. Nöro-dilbilimsel Programlama (NLP) 53
2.2.18.1.8. Sosyal Medya 54

2.3. Dünya ve Türkiyedeki Büyük Siber Saldırı Olayı Örnekleri 56
2.3.1. Türkiye'deki Siber Saldırı Örnekleri 56
2.3.1.1. Milli İstihbarat Teşkilatı (MİT) Çalışanlarının Kimlik Bilgilerinin İfşa Edilmesi (2001) 56
2.3.1.2. Batman Hidroelektrik Barajı'na yapılan Siber Saldırı (2003) 57
2.3.1.3. Bakü-Tiflis-Ceyhan Petrol Borusu Hattına Siber Sabotaj (2008) 57
2.3.1.4. Atatürk ve Sabiha Gökçen Havalimanlarına Yapılan Siber Saldırılar (2009 ve 2013) 58
2.3.1.5. 10 Gün Süren Siber Saldırı (2015) 59
2.3.1.6. Sağlık Bakanlığına Ait 33 Devlet Hastanelesine Yapılan Siber Saldırı (2016) 59
2.3.2. Dünya Çapinda Gerçekleşen Siber Saldırı Örnekleri 59
2.3.2.1. Estonya Siber Saldırısı (2007) 60
2.3.2.2. Gürcistan Bilgisayar Ağı'na Saldırı (2008) 60
2.3.2.3. İran Nükleer Sistemine Saldırı-Stuxnet Virüsü (2010) 61
2.3.2.4. Sony Playstation Siber Saldırısı (2011) 61
2.3.2.5. Yahoo Siber Saldırısı (2014) 61
2.3.2.6. Rusya-Ukrayna Savaşı Saldırıları (2022) 62
BÖLÜM 3
ÜLKEMİZDE SİBER GÜVENLİK ALANINDAKİ ÇALIŞMALAR VE ALINABİLECEK ÖNLEMLER 63
3.1. Türkiye'nin Siber Güvenlik Çalışmaları 63
3.1.1. Siber Güvenlik Kurulu 64
3.1.2. Ulusal Siber Olaylara Müdahale Merkezi (USOM) 66
3.1.3. Siber Olaylara Müdahale Ekibi (SOME) 67
3.1.4. Bilgi Teknolojileri ve İletişim Kurumu (BTK) 71
3.1.5. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) – Siber Güvenlik Enstitüsü (SGE) 72
3.1.6. TSK Siber Savunma Komutanlığı 74
3.1.7. Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı 75
3.1.8. Milli İstihbarat Teşkilatı (MİT) 75
3.1.9. Türkiye Bilişim Derneği (TBD) 77
3.1.10. Kamu Sanal Ağı (KamuNet) Projesi 78
3.1.11. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Siber Güvenlik Dairesi Başkanlığı 79
3.1.12. On Birinci Kalkınma Planı (2019-2023) 79

3.2. Siber Güvenlik Kapsamında Alınabilecek Önlemler 80
SONUÇLAR VE ÖNERİLER 90
Sonuçlar 90
Öneriler 92
KAYNAKLAR 99
ÖZGEÇMİŞ 107

TABLOLAR DİZİNİ

Tablo **Sayfa**

Tablo 2.1. Web Siteleri ve E-posta Adreslerine Yapılan Oltalama Sayıları. 34
Tablo 3.1. USOM ve SOME'lerin Hizmet Alanları. 68

ŞEKİLLER DİZİNİ

Şekil **Sayfa**

Şekil 1.1 Siber Güvenlik Stratejisi Olan Ülkeler 8
Şekil 1.2 Bilgi Güvenliği Unsurları..... 11
Şekil 1.3 Bilgi Güvenliği Sağlama Yöntemleri..... 12
Şekil 1.4 Güvenlik Duvarı Kullanımı. 16
Şekil 1.5 Dünyada Siber Güvenlik Alanında Girişimcilere Yapılan Yatırım Miktarı 20
Şekil 2.1 Anlık Gerçek Zamanlı Siber Saldırı Haritası..... 22
Şekil 2.2 2020 Yılı Siber Saldırı Türleri Dağılımı..... 24
Şekil 2.3 Zararlı Yazılımların Artışı 25
Şekil 2.4 Solucanların Çalışma Ve Yayılma Şeklini Gösteren Şekil. 28
Şekil 2.5 Ransomware Saldırısı Anlatımı 31
Şekil 2.6 Oltalama Saldırılarının 2021 Yılındaki Artışı..... 33
Şekil 2.7 DDoS Saldırı Şekli..... 36
Şekil 2.8 Köle Bilgisayarların Botnet Saldırısında Çalışma Yapısı..... 38
Şekil 2.9 Ortadaki Adam Saldırısı..... 39
Şekil 2.10 IP Sahteciliği Yapılan Paketin İletimi..... 42
Şekil 2.11 XSS Saldırısı Örneği. 45
Şekil 2.12 Sosyal Mühendislik Döngüsünün Aşamaları..... 48
Şekil 2.13 Tersine Sosyal Mühendislik Aşamaları 50
Şekil 2.14 Dünya Üzerindeki Anlık Siber Saldırı Haritası 60
Şekil 3.1 USOM, Sektörel SOME ve Kurumsal SOME İlişkisi 67
Şekil 3.2 Kurumsal SOME'nin Kurum İçindeki Paydaşları ve Temel Fonksiyonları 69
Şekil 3.3 Siber Olay Esnası Akış Diyagramı 70
Şekil 3.4 SGE Organizasyon Şeması 73
Şekil 3.5 Lisanssız Yazılımların Kötü Amaçlı Yazılımlar İle Karşılaşma Oranı 81

KISALTMALAR / SİMGELER

Kısaltma	Açıklama
APWG	Anti-Phishing Working Group
AR-GE	Araştırma Geliştirme
ARPANET	Gelişmiş Araştırma Projesi Dairesi Ağı
BDDK	Bankacılık Düzenleme ve Denetleme Kurumu
BGE	Bilişim Sistemleri Güvenliği
BİS	Bilgi ve İletişim Sistemleri
BT	Bilgi Teknoloileri
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CBDDO	Cumhurbaşkanlığı Dijital Dönüşüm Ofisi
CD	Compact Disc
CIA	Confidentiality-Integrity-Availability
DDOS	Distributed Denial of Service Attack
DNS	Domain Name System
DRP	Disaster Recovery Plan

DSİ	Devlet Su İşleri
EGM	Emniyet Genel Müdürlüğü
HTML	Hyper Text Markup Language
İP	Internet Protocol
ITU	International Telecomunication Union
LAN	Local Area Network
MİT	Milli İstihbarat Teşkilatı
MITM	Man In The Middle
NAT	Network Address Translation
NATO	North Atlantic Treaty Organization
NLP	Neuro Linguistik Programming
ODTÜ	Orta Doğu Teknik Üniversitesi
OPSEC	Operations Security
Polnet	Polis Bilişim Sistemi
RAM	Random Access Memory
RSE	Reverse Social Engineering

s.	Sayfa
SGE	Siber Güvenlik Enstitüsü
SİSAMER	Siber Savunma Merkezi
SMS	Short Message Service
SOME	Siber Olaylara Müdahale Ekipleri
SQL	Structured Query Language
SSL	Secure Sockets Layer
TBD	Türkiye Bilişim Derneği
TBMM	Türkiye Büyük Millet Meclisi
TCMB	Türkiye Cumhuriyet Merkez Bankası
TİB	Telekomünikasyon İletişim Başkanlığı
TSK	Türk Silahlı Kuvvetleri
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UAB	Ulaştırma Altyapı Bakanlığı
UDHB	Ulaştırma, Denizcilik ve Haberleşme Bakanlığı
UEKAE	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

URL	Uniform Resource Loader
USB	Universal Serial Bus
USENET	User’s Network
USOM	Ulusal Siber Olaylara Müdahale Merkezi
VPN	Virtual Private Network
Wİ-Fİ	Wireless Fidelity
XSS	Cross Site Scripting

GİRİŞ

Bu bölümde, problem, amaç, önem, sınırlılıklar ve çalışmada geçen kavramların tanımları yer almaktadır.

Problem

İçinde bulunduğumuz teknoloji çağında, bilgi ve iletişim teknolojileri ile internetin büyük bir hızla gelişmesiyle teknoloji hayatlarımızda büyük yer edinmektedir. Yaşamımızın neredeyse her alanında teknolojik yapılar kullanılmaktadır. Günümüzde sağlık, iletişim, turizm, ulaşım, eğitim, haberleşme, bankacılık ve neredeyse akla gelen her türlü bireysel ve ulusal bilgi insanlara kolaylık sağlaması amacıyla dijital ortamda saklanmakta, kullanılmakta ve takip edilebilmektedir.

Bilgi ve iletişim teknolojilerinin kullanım alanlarının küresel alanda ilerlemesi ve yaşantılarımızda sağladığı kolaylıklarla birlikte, hayatlarımızın vazgeçilmez bir parçası haline gelmesiyle; verilerin güvenliğinin sağlanabilmesi ciddi bir endişe konusu olarak hayatlarımızda yerini almıştır. Bireysel, kurumsal ve ulusal alanda korunması gereken her türlü verinin, kötü niyetli kişiler ve oluşumlar tarafından ele geçirilebilmesi riskine karşı tedbir alınması gerekliliği üzerinde durulmalıdır.

Küresel çapta hemen hemen her işlemin siber ortamda gerçekleşmesi, bilgilerin gizliliği konusunda endişeye yol açmaktadır. Kişiler, kurumlar ve ülkeler kritik bilgilerinin bir başkasının ele geçirmesini ve ortaya çıkarmasını istemeyeceklerdir. Fakat tüm dünyada aktif bir şekilde siber korsanlar tarafından saldırılar gerçekleşmektedir. Bu durum büyük olumsuzluklara ve maddi manevi zarara yol açmaktadır.

Siber ortamdaki verilerin kolaylık sağlamasının yanısıra tehditlerden gerektiği şekilde korunmaması durumunda zayiatlara sebep olabileceği bilinmektedir. Bu sebeple siber güvenlik bilgi ve iletişim teknolojilerinin hızlı bir şekilde geliştiği kişi, kurum, uluslararası oluşumlar ve devletlerin en önem verdiği ve üzerinde durduğu konular haline gelmiş bulunmaktadır. Günlük hayatta teknolojinin gelişimiyle oldukça önemli bir hale gelen siber güvenlik gelecekte de önemini koruyacaktır. Bilgi ve iletişim teknolojilerinin kullanımı devam ettikçe siber güvenlik tedbirleri, önem ve önceliğini korumaya devam edecektir.

Tüm dünyada bireyler, kurum ve kuruluşlar, ciddi veri kaybı, kritik verilerin açığa çıkarılması veya sızdırılması, sistemlerin sekteye uğraması ve böylece itibar kaybı gibi çeşitli siber güvenlik tehditleri ile yüzyüze gelebilmektedir. Birçok tehditten kaynaklanabilen bu gibi ihlallere karşı zarar görülmemesi için dikkat edilmesi gereken güvenlik önlemleri alınmalıdır.

Günümüzde devletler dahi birbirleriyle siber saldırı yöntemleri ile savaşabilmektedir. Görüldüğü üzere her türlü bilginin güvenliği büyük önem taşımakta ve siber savaşlara kadar uzanabilmektedir. Bu gibi durumların önüne geçilebilmesi amacıyla siber dünyanın parçası olan herkesin kendisini koruması gerekmektedir.

Bireyler, kurumlar ve devletlerin siber güvenliklerini sağlayabilmeleri için, sorumluluk düşen her bir bireye siber tehditlere, siber ortamdan gelebilecek saldırılara, bunlara karşı nasıl önlem alınması gerektiğine, hangi eylemlerin nelere yol açabileceğine karşı farkındalık kazanma sorumluluğu yüklenmesi gerekmektedir. Siber saldırı kavramlarının bilinmesi, siber tehditlerin anlaşılması, siber tehditlerin tespiti ve önlenebilmesi önem oluşturmaktadır.

Amaç

Bu tez çalışmasının kapsamında yapılan araştırmalar, değerlendirmeler ve çalışmalar sonucundaki amaç, siber güvenliğe dair gerekli terimlerin anlaşılması, siber güvenlik alanında yapılan saldırı çeşitleri, güvenlik tehditlerinin araştırılması, dünyada ve ülkemizdeki saldırı örneklerinin incelenerek ders çıkarılması, siber güvenlik ile alakalı kurumların öğrenilmesi ve bu alanda alınabilecek olan tedbirlerin anlaşılmasıdır.

Önem

Verilerin dijital ortama aktarılması ve günümüzde çoğu alanda kullanılmasıyla birlikte siber tehditlerin çoğalması kaçınılmaz olmuştur. Sadece devletler değil aynı zamanda kurumlar ve bireyler de olumsuz ve geri dönüşü olmayan sonuçlarla karşı karşıya kalmaktadırlar. Siber güvenlik tehditlerinin sürekli değişmesi ve yenilenmesi sebebiyle de yapılan çalışmaların güncel olması oldukça önemlidir. Bu çalışma ile siber güvenlik kapsamında güncel çalışmalar ele alınarak bireyler, kurumlar ve ülkemiz açısından

farkındalığın artmasına ve siber ortamda bilinçli hamleler yapılmasına katkı sağlanacağı düşünülmektedir. Olağan riskler için alınması gereken önlemlerin sunulmasıyla olası zararların en aza indirilmesine yardımcı olacağı düşünelerek önem taşımaktadır.

Sınırlılıklar

Bu tez çalışmasında internet ortamındaki her türlü olayın her geçen gün değişmesi ve güncel yeniliklere ev sahipliği yapmasıyla üzerinde durulan siber tehdit ve siber olay örneklerinin mümkün olduğunca en güncel haliyle seçilmesine çalışılsa da her an yeni siber saldırı ve savunma türleri ortaya çıkabilmektedir. Bu sebeple mümkün olduğunca yeni ve farkındalık gerektiren konular üzerinde durulmuş, en çok karşılaşılan türler anlatılmış ve güncel kaynaklardan yararlanılmaya çalışılmıştır.

Tez içerisinde verilen örnekler, siber saldırı örnekleri gibi konular mümkün olduğunca en çok ses getirenler üzerinden anlatılmaya çalışılmıştır. Yer verilen konuların güncel ve en çok karşılaşılan, farkındalık oluşturulması gerektiği düşünülen konular üzerinden aktarılmasına çalışılmıştır.

Tanımlar

Siber güvenlik, bilgisayarların, sistemlerin, sunucuların, mobil cihazların, elektronik sistemlerin, ağların, bilgi ve verilerin kötü amaçlı saldırılardan korunması uygulamasıdır. Kötü amaçlı siber saldırılar genellikle kritik ve hassas bilgileri yetkisiz bir şekilde ele geçirmeyi amaçlamaktadır.

Siber güvenlik önlemleri, bahsedilen kötü amaçlı tehditlerin kurbanlara zarar verebilmesini önlemek amacıyla uygulanması gereken tedbirlerdir. Kurbanların en az ölçüde etkilenmesini amaçlamaktadır.

Yöntem

Bu tez çalışması kapsamında nitel bir çalışma yöntemi olan döküman analizi yöntemi kullanılmıştır. Konu ile alakalı kaynak tarama sonucunda toplanmış olan çeşitli

türlerdeki dokümanların incelenip araştırılarak tez konusu üzerinde hangi amaçlarla katkı sağlayabileceği üzerinde durulmuştur. Araştırmaların neticesinde ilgili olabilecek kaynaklar alt başlıklar ve temalar çerçevesinde sınıflandırılmıştır.

Verilerin Toplanması

Bu tez çalışmasının hazırlanması kapsamında kaynak tarama yöntemi kullanılmıştır. Siber güvenlik alanında derlenmiş olan kitap, dergi, makale, tez, teknik rapor ve araştırmalar, online siber güvenlik eğitimleri, konferanslar ve haber platformaları gibi kaynaklarda çeşitli bilgilere ulaşılarak toplanan veriler üzerinden analiz ve yorumlama yapılarak çeşitli değerlendirmelerde bulunulmuştur.

Verilerin Çözümlenmesi

Tez çalışması kapsamında elde edilen verilerin incelenmesi ve detaylı analizi sonucunda bölümler ve başlıklar kategorize edilmiştir. Toplanmış olan veriler bu sınıflandırma kapsamında değerlendirilerek uygun kısımlara eklenmiştir. İnceleme ve değerlendirme aşamasında bilimsel etik kurallara uygun bir şekilde hareket edilmiştir. Verilerden elde edilen analizlerin sonucunda bütüncül olarak yorumlanmıştır.

BÖLÜM 1

SİBER GÜVENLİKLE İLGİLİ KAVRAMLAR

Bilgi teknolojileri, internet altyapısının gelişmesiyle günümüzde her alanda kullanılmaya başlanmıştır. Bilginin birçok alanda kullanımı ve getirdiği kolaylıklarla beraber bilginin siber ortamda korunması da önemli bir konu haline gelmiştir. Bu bölümde siber güvenliğin anlaşılabilmesi amacıyla bu alandaki temel kavramlara yer verilecektir.

1.1. Siber

Siber kelimesi "sibernetik" kökünden gelmektedir. Sibernetiğin kelime anlamı yönetim demektir (Şahinaslan, 2013). Sibernetik tarihi El-Cezeri'ye dayanmaktadır ve El-Cezeri, "Sibernetiğin Babası" olarak kabul edilmektedir (Korkutata & Toprak, t.y., s.42). Siber kelimesi de aynı şekilde yönetim ve idare anlamıyla bilinmektedir. İnternete ve sanal ortama ait olduğu anlamına çıkarılmaktadır. Bu kelime bir ön ektir ve önüne geldiği kelimelere bilgisayar ve teknolojiyle ilgili olduğu anlamını katmaktadır. Siber uzay, siber saldırı, siber tehdit kavramları bunlardan bazılarıdır.

1.2. Siber Uzay

William Gibson, Neuromancer adlı romanında siber uzay terimini ilk kullanan kişi olarak diğer tüm tanımlara temel oluşturan siber uzayı bilgisayar destekli iletişimin, insan beyni ve bilgisayar ağı ile tanımladığı bölge olarak tanımlamıştır. Gibson'a (1984) göre; "Siberuzay; her ulustan milyonlarca yasal kullanıcının, matematiksel kavramları öğrenen çocukların, her gün yaşadığı bilinç ve duygu ile birlikte giden istem dışı, anlaşmalı halisünasyon ... insan sistemindeki her bir bilgisayarın kayıtlarından yansıtılan verilerin grafiksel sunumu. Kavranamayacak bir karmaşık. Zihnin uzaysızlığında, ışık çizgileri; öbekler ve takımyıldızlar şeklinde düzenlenen veriler. Tıpkı şehrin ışıkları gibi, gitgide uzaklaşan..." (Özdemir ve Şahin, t.y., s. 7) olarak ifade edilmiştir.

2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'na göre ise "doğrudan ya da dolaylı olarak internete, elektronik haberleşme ve bilgisayar ağlarına bağlı olan tüm sistem ve hizmetler" olarak tanımlanmaktadır (Ulusal Siber Güvenlik Stratejisi Eylem Planı 2020-2023, 2020, s. 10).

Benedict'in Cyberspace: First Step kitabına göre "Dünya üzerindeki bilgisayarlar ve iletişim hatları tarafından yaratılan ve sürdürülen paralel bir evren. Bilginin, sırların, ölçülerin, göstergelerin, eğlencenin ve değişen insan faaliyetlerinin global trafiğinin biçim bulduğu bir dünya: Yerin yüzeyinde asla rastlanmayan görüntülerin, seslerin ve varlıkların engin bir elektronik gecede tomurcuklanması." olarak tanımlanmıştır (Kurbak, 2012).

Yapılan tanımlardan yola çıkarak siber uzay, her geçen gün daha da büyümekte olan ve insanların her türlü elektronik bilgiye erişmesine olanak sağlayan donanım, yazılım, ağ ve iletişim altyapıları içeren bilişim sistemlerinden oluşan bir ortam olarak ifade edilebilir.

Siber uzayın kullanımı 21. yüzyılın başlarından itibaren gelişmeye başlamıştır. Bu gelişimle birlikte devletler siber uzayı güvenlik problemi olarak görmeye başlamış ve bazı tedbirler alınması gerektiği sonucuna ulaşmışlardır.

Son yıllarda her alanda hızlı bir şekilde yayılan siber uzay, internet ve mobil iletişim gibi ağ tabanlı araçlardan oluşmaktadır. Bu doğrultuda bireyler küresel ölçekte iletişim kurabilmekte veya örgütlenebilmektedir. Aynı zamanda, belli bir amaçla siber saldırılarda da bulunabilmektedirler. Bu durum devletlerin siber uzayı tehdit olarak görmesine neden olmakta ve hızla güvenlikleştirilmesini isteyip kendi savunma bakanlıklarını, istihbarat örgütlerini kurmuş ve aynı zamanda da güvenlik stratejilerini yayımlamışlardır (Ermiş, 2018).

1.3. Siber Güvenlik

Siber güvenlik, tarihi bir araştırma projesi olarak başlamıştır. 1970'li yıllarda, Cambridge Massachusetts'te BBN Technologies için araştırmacılık yapan Robert Thomas tarafından ilk bilgisayar solucanı geliştirilmiştir. Bu solucan Gelişmiş Araştırma Projesi Dairesi Ağı (ARPANET)'nda ana bilgisayarları etkileyerek, "Ben Creeper, yapabilirsen beni yakala" mesajıyla sistemden sisteme atlayarak bilgisayarlara bulaşmıştır. E-postanın da mucidi olan Ray Tomlinson, Creeper'i takip ederek silebilen ilk antivirüs yazılımı olan The Reaper adında bir çoğaltma programı yazmıştır. Ardından 1988 yılında Robert Morris isimli bir adam internetin boyutunu test etme fikriyle yola çıkarak ağlardan geçen, Unix

terminallerini istila eden ve kendini kopyalayan saldırgan bir program yazmış ve bilgisayarları kullanılamaz hale getirirecek kadar yavaşlatması sebebiyle bu konuda mahkum edilen ilk kişi olmuştur. Bu nokta itibariyle virüsler daha ölümcül, istilacı ve kontrol edilmesi zor hale geldiği için siber güvenliğin ortaya çıkışı kaçınılmaz bir hale gelmiştir (Choudry, 2022).

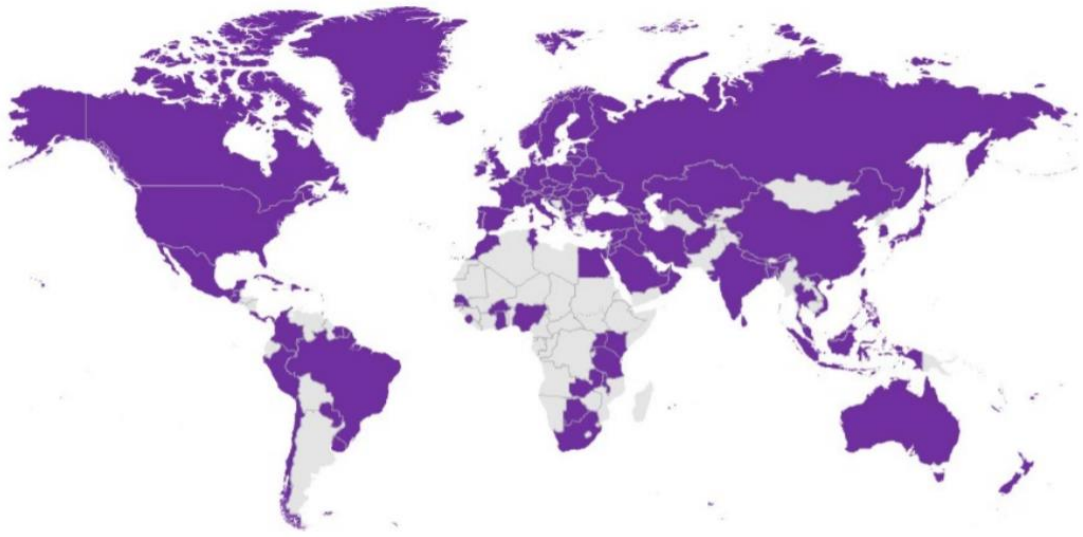
Siber güvenlik, siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin/verinin gizliliği, bütünlüğü ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber olayların tespit edilmesini, bu tespitlere karşı önlem mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber olay öncesi durumlarına geri döndürülebilmesini kapsayan faaliyetler bütünüdür (Ulusal Siber Güvenlik Stratejisi Eylem Planı 2020-2023, 2020, s. 10).

Siber güvenlik, bilgisayarları, sunucuları, mobil cihazları, elektronik sistemleri, ağları ve verileri kötü niyetli saldırılardan koruma uygulamasıdır. Temel işlevi, hepimizin kullandığı cihazları (akıllı telefonlar, dizüstü bilgisayarlar, tabletler ve bilgisayarlar vb.), eriştiğimiz hizmet ve sistemleri hem çevrimiçi hem de hırsızlık veya hasara karşı korumaktır. Modern yaşamın temel parçası haline gelen çevrimiçi bankacılık ve alışverişten e-posta ve sosyal medyaya kadar, siber suçluların hesaplarımızı, verilerimizi ve cihazlarımızı ele geçirmesini engelleyebilecek adımlar atmak önemlidir.

Güçlü bir siber güvenlik stratejisi , resmi veya özel kuruluşların ya da benzer şekilde kullanıcıların sistemlerine ve hassas verilerine erişmek, bunları değiştirmek, silmek, yok etmek veya gasp etmek için tasarlanmış kötü niyetli saldırılara karşı iyi bir güvenlik duruşu sağlayabilmektedir. Siber güvenlik, bir sistemin veya cihazın operasyonlarını devre dışı bırakmayı veya kesintiye uğratmayı amaçlayan saldırıların önlenmesinde de etkilidir.

Şekil 1.1

Siber Güvenlik Stratejisi Olan Ülkeler Global Siber Güvenlik Politikaları ve Türkiye Özelinde Denetim Açısından Önemi, Eren, 2021, s. 4



Son yıllarda, tüm gelişmiş ülkelerde kritik altyapıya yönelik siber saldırılar düzenlenmiş ve sayısız işletmeler büyük kayıplara uğratılmıştır. Birçok kurum ve kullanıcının özel bilgileri siber suçlular tarafından çalınmıştır.

Türkiye'de yer alan 21 kuruluşun katılımı ile elde edilen verilere göre veri ihlali gerçekleştirilen kuruluşların ortalama 1,78 milyon dolarlık zarara uğradığı belirtilmiştir. Dünya geneline bakacak olursak bu maliyet 4,24 milyon dolarlık rakamlara kadar çıkabilmektedir ("Veri İhlali Maliyetleri, Pandemi Sırasında Rekor Düzeye Ulaştı," 2021).

Siber alandaki mevcut güvenlik ihlalleri ve tehditleri, aşağıdakiler de dahil olmak üzere neredeyse her sistemi etkileyebilir. Bazı alanlardaki etkilerine bakacak olursak;

İletişim: Telefon görüşmeleri, e-postalar, kısa mesajlar ve mesajlaşma uygulamalarının tümü siber saldırılar hedefinde olabilmektedir.

Finans: Finansal kurumlar saldırganlar için birincil hedeftir ve banka veya kredi kartı bilgilerini işleyen ya da bunlarla ilgilenen tüm kuruluşlar daima öncelikli olarak risk altındadır.

Hükümetler: Devlet kurumları, vatandaşlara ait özel bilgilerin veya gizli ve kritik kamu verilerinin peşinde olabilecek siber suçlular tarafından yaygın olarak hedeflenir.

Ulaşım: Bağlantılı arabalar, trafik kontrol sistemleri ve akıllı yol altyapısının tümü siber saldırı riski altındadır.

Sağlık hizmetleri: Küçük bir klinikteki tıbbi kayıtlardan ulusal bir hastanedeki kritik bakım sistemlerine kadar her şey saldırılara karşı savunmasızdır.

Eğitim: Eğitim kurumları, gizli araştırma verileri ve öğrenciler veya personel hakkında sahip oldukları bilgiler saldırı riski altındadır.

1.4. Siber Güvenlik Unsurları

- Uygulama Güvenliği
- Bilgi Güvenliği
- Ağ güvenliği
- Olağanüstü durum kurtarma / iş sürekliliği planlaması
- Operasyonel güvenlik
- Son kullanıcı eğitimi

1.4.1. Uygulama Güvenliği

Uygulama güvenliği, siber saldırıların önüne geçebilmek amacıyla, uygulamaları geliştirme aşamasında güvenlik özellikleri de ekleyen aşamadır ve bu siber güvenliğin ilk temel unsurudur. İnternet siteleri ve web tabanlı uygulamalardaki kaynak kodlarına erişilerek buradaki güvenlik açıklıklarından yararlanılan siber saldırılar gerçekleştirilebilmektedir. Uygulama güvenliği aşamasında bu gibi tehdit ve saldırılardan korunmak amaçlanmaktadır.

Cihazların ve yazılım uygulamalarının tehdit oluşturan unsurlardan korunmasını, saldırı durumunda etkilenmemesini sağlamaya çalışmaktadır. İyi bir uygulama güvenliği, yazılım henüz tasarım aşamasındayken veya cihazlar henüz kurulmadan ve kullanılmaya başlamadan önce koruma yapmayı hedeflemektedir ("Siber Güvenlik Nedir?" 2022).

1.4.2. Bilgi Güvenliği

Bilgi güvenliği, bilgilerin yetkisiz erişimini, yayılmasını, kullanılmasını, bozulup değiştirilmesini ya da yok edilmesini önlemeye yönelik bir aşamadır. Bu bilgiler, kişisel bilgiler, cep telefonu, sosyal medya, kişisel bilgisayar veya oturum açma bilgileri gibi kritik bilgiler olabilir.

Bir bilgiye izinsiz bir şekilde erişilmesi, kullanılması, ortaya çıkarılması, yok edilmesi veya değiştirilmesi gibi zararlı eylemlerin önlenmesine yönelik, bilginin aynı zamanda gizliliği, bütünlüğü ve erişilebilirliğinin de korunarak yapılabildiği tüm işlemlere bilgi güvenliği denilebilmektedir.

Bilgi güvenliği, yapılan işlerin devamlılığı, önlenemeyen felaket durumlarındaki tehditlerin en aza indirilebilmesi, verilerin her koşulda gizliliği, ulaşılabilirliği ve korunabilmesini amaçlamaktadır ("Kurumlarda Bilgi Güvenliği Yönetim Sistemi'nin Uygulanması", 2008, s. 511).

Bilgi Güvenliğinin Temel İlkesi

Yaygın olarak CIA olarak bilinen bilgi güvenliğinin üç temel ilkesi vardır. Bunlar gizlilik, bütünlük ve erişebilirlik olarak tanımlanmaktadır. Birbirleriyle ayrılmaz bir etkileşim halindedirler.

Şekil 1.2

Bilgi Güvenliği Unsurları



1.4.2.1. Gizlilik

Gizlilik, yetkisi olan kullanıcılar tarafından hassas bilgilere erişmesine izin veren verilerin korunmasıdır. Hassas olan ve sadece belirli ve sınırılı sayıdaki kişilerle paylaşılması gereken her türlü bilgiyi içerir. İsim, doğum tarihi, yaş, adres, iletişim bilgileri, e-posta hesapları, sosyal medya hesapları, banka hesap bilgisi, aile bilgileri gibi bilgi türleri gizli olarak kabul edilmektedir (Touhid, 2019).

Gizlilik kavramı, verilerin ve bilginin, erişmemesi gereken kişiler tarafından erişimine olanak sağlamadan aynı zamanda bunun yanında yetkili kişilerin ise erişim sağlayabilmesi için gerekli tedbirleri sağlamayı hedefleyen önlemlerden oluşmaktadır. Bilginin yetkisiz kişilerden korunması amaçlanmaktadır.

1.4.2.2. Bütünlük

Bütünlük, verilerin tutarlılığının, doğruluğunun ve eksiksizliğinin korunmasıdır. Bu da verilerin yetkisiz kişiler tarafından düzenlenip değiştirilemeyeceğini garanti etmektedir. Örneğin, bütünlük, verilerin yetkisiz kişilerce yetkisiz bir şekilde ekleme, silme veya herhangi bir değişiklik yapılmamasını temin etmektedir ("Bilgi güvenliği nedir?", 2022).

Verilerin doğru ve güvenilir olmasını ve istemeyerek yani yanlışlıkla ya da kötü niyetle yanlış bir şekilde değişiminin engellenmesini sağlamaktadır ("Bilgi güvenliği nedir | İlke, ilkeler ve tehditler | Imperva", 2022).

1.4.2.3. Erişebilirlik

Kullanılabilirlik, bilgilerin ihtiyaç duyulduğunda veya gerekli, belirli ve arzı edilen zamanlarda tam olarak erişilebilir, değiştirilebilir olacak şekilde yetkili kişiler tarafından kullanılabilecek halde olma yeteneğinin korunmasıdır. Bu sebeple bilgi sadece yetkili kişilerin doğru ve istenilen zamanda erişilebilmesi halinde değer kazanır.

Bu unsurlardan yola çıkarak bilgi güvenliğini sağlamanın yöntemlerinden bahsedecek olursak;

Şekil 1.3

Bilgi Güvenliği Sağlama Yöntemleri



- Kişisel verileri korumak: Sosyal ağlar sebebiyle ad, soyad, doğum tarihi, adres, ilgi alanları, iş hayatı, yapılan işler vb. gibi birçok hassas, kişisel veriler ortaya çıkarak yayılabilmektedir. Bu gibi kişisel bilgileri, sosyal ağlar kullanılırken paylaşmak yerine daha genel bilgileri paylaşmak kişisel verilerin korunmasında etkili olmaktadır.
- Parola yönetimi: İnternet dünyasında yapılan en önemli hatalardan birisi de basit parolalar kullanmak ve aynı parolayı birkaç farklı platformda kullanmaktır. Bu durum siber saldırılar için büyük fırsatlar doğurabilmektedir. Basit parolalara birkaç saniye içinde çok kolayca erişebilmek olabildiğince mümkündür. Bu yüzden parola seçimi yaparken karmaşık yapıları kullanmak gerekmektedir. İyi bir parola politikası, en az sekiz karakter, en az bir büyük harf ile bir özel karakter ve bir sayı kullanılmasını gerektiren bir politikadır. Dahası, şifrelerin düzenli olarak değiştirilmesi de oldukça önemlidir. Kullanıcılar, şifrelerini her 60 ile 90 gün arasında değiştirerek çalınmış veya tahmin edilmiş olabilecek şifrelerin kullanılmasını engelleyebilecektir. Ayrıca kullanıcıları şifre güvenlik politikaları üzerine eğitmek de şifre güvenliği üzerine etkili yöntemlerden birisidir (Bourgeois & Bourgeois, 2014).
- Gizlilik ve güvenlik ayarlarının kontrol edilmesi: Forumlar, haber siteleri ya da çeşitli uygulamalar gibi sosyal ağlara giriş yaparken, üye kaydı esnasında kullanıcılar için gizlilik sözleşmeleri ve uygulama ayarları sunulmaktadır. Kullanıcılar hakkında ne kadar çok bilgi elde edilirse o kadar başarılı siber saldırılar gerçekleştirilebilir. Bu sebeple sosyal ağlar vb. üzerinde gezinirken gizlilik sözleşmelerini dikkatle inceleyip gizlilik ve güvenlik ayarlarını açarak verilere ulaşılması ve kullanılması engellenebilecektir.
- Güvenlik duvarı kullanımı: Güvenlik duvarı, bir ağa herhangi bir zamanda neyin ve kimin erişebileceğini kontrol eden bir güvenlik aygıtıdır (Topalov, 2015, s. 1). Ağlardaki güvenliği artırmak için kullanılır. Ağlarda dış bir kaynaktan akan tüm trafiğin ve erişilen bilgilerin güvende olduğundan emin olmak için veriler güvenlik duvarından geçmelidir. Donanım veya yazılım ya da her ikisi de kullanılabilir. Donanım güvenlik duvarı bilgisayar ağları ile internet sağlayıcıları arasında bulunur ve ağlardaki verileri belli bir kurala göre filtreler. Yazılım güvenlik duvarı ise işletim sistemlerinde ve sunucular üzerinde çalışır. Bu sebeple bilgisayarlara veya ağlara internet ya da diğer ortamlardan gelebilecek saldırılara karşı veri güvenliği sağlanması ve korunması için güvenlik duvarları kullanılmalıdır (Bourgeois & Bourgeois, 2014).
- Güncel işletim sistemi kullanımı: Güncel işletim sistemleri, tespit edilen hatalar ve ortaya çıkabilecek olan güvenlik zafiyetlerine karşı sistemi güvenli ve stabil bir halde

tutabilmek için yayınlanmaktadırlar. Bu sebeple mobil cihaz veya bilgisayarlarda bu güncellemeler yapılarak sistemler güncel tutulmalıdır. Aksi durumda işletim sistemlerindeki zafiyetler ile siber saldırılara açık kapı bırakılarak bu saldırılara maruz kalınması oldukça muhtemeldir.

- Verilerin şifrelenmesi: Veri şifreleme, sadece yetkili kişilerin okuyabilmesi için verinin iletimi veya depolanması sırasında verileri kodlama işlemidir. Bu kodlama iletilecek olan düz metni kodlayan bir bilgisayar programı tarafından gerçekleştirilir. Sonrasında alıcı kodlanmış şifreli metni alarak şifresini çözer. Bunun çalışması için her iki tarafın da kodlama yöntemi üzerinde anlaşması gerekmektedir (Bourgeois & Bourgeois, 2014).
- Verileri yedekleme: Veri yedekleme işlemi, oldukça kritik bir veri güvenliği önlemi türüdür. Verilerin, uygun yöntem seçilerek belirli aralıklarla kopyalanması ve arşivlenmesi ile yapılmaktadır. Yedeklenen veriler deprem, sel, yangın vb. gibi beklenmedik bir olay karşısında farklı tesislerde depolanarak korunmalıdır. Gerekli olması durumunda veriler geri kurtarılabilmektedir.
- E-posta ve web sitelerinin dikkatli kullanımı: E-postalar günümüzde en önemli iletişim araçlarındandır ve internet üzerindeki iletişim açısından önemli rol oynamaktadır. Hal böyle olunca da siber saldırganlar için de en çok kullanılan yollar arasında yer almaktadır. Kullanıcıların sahte e-postalar ve sahte bağlantıları açması çok kısa bir süre içerisinde siber saldırıya maruz kalmalarına neden olacaktır. Bu noktada tanınmayan kişilerden ve şüpheli e-postalardan uzak durmak gerekmektedir. Ayrıca kullanılacak web sitelerinin güvenilir olup olmadığına mutlaka bakılarak, bilgilerinin güvenilirliği bilinmeyen web siteleri ziyaret edilmemelidir.

Sonuç olarak, kişiler veya kuruluşların güvenliğini sağlayabilmesi açısından güvenlik önlemleri alması şarttır. Bahsedilen güvenlik önlemleri bilgi bütünlüğü ve güvenliğini sağlayabilmek için gereklidir. Kuruluşların en önemli varlıkları sahip oldukları kritik bilgilerdir. Kurumun gizliliğini ve yönetilebilirliğini korurken riski en aza indirmek için teknik ve kurumsal güvenlik önlemleri uygulanmalıdır. Güvenlik önlemlerinin, politikalarının ve düzenlemelerinin uygulanması, bir kuruluşun güvenliğini korumasına, uygulamasına, yönetmesine ve denetlemesine olanak tanımaktadır. Kuruluşa karşı herhangi bir tehdit veya saldırı mevcut ise, alınan önlemler riskleri azaltmanın yanı sıra karşı önlemleri hızla uygulamaya da yardımcı olacaktır.

1.4.3. Ağ Güvenliği

Ağ güvenliği, birçok teknolojiyi, cihazı ve süreci kapsayan geniş bir terimdir. Basitçe tanımlamak gerekirse, hem yazılım hem de donanım teknolojilerini birarada içeren, bilgisayar ağlarının ve verilerin bütünlüğünü, gizliliğini ve erişilebilirliğini korumak için tasarlanan kurallar ile etkili bir ağ güvenliğini ve ağa erişimi yöneten yapılandırmalardır ("What is network security?", t.y.).

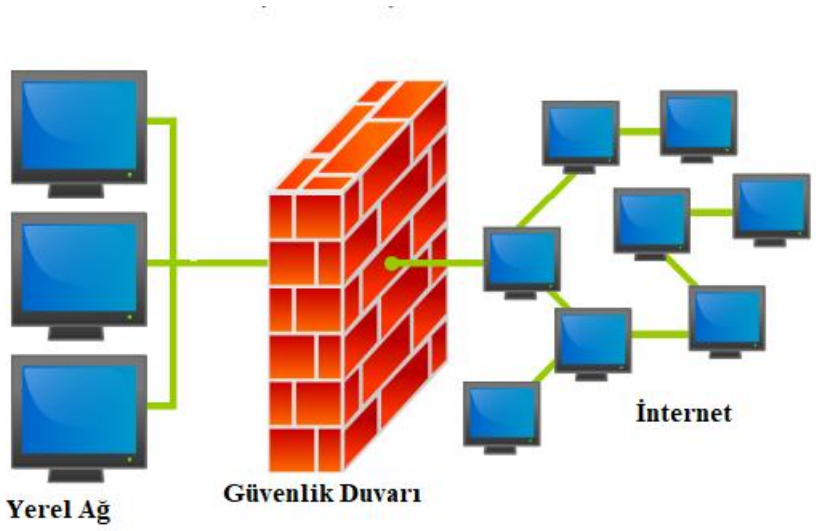
Ağ güvenliği günümüzde gitgide daha da önem kazanmaktadır. Kritik önemlere sahip özel ve kurumsal bilgilerin internet gibi global ve güvensiz bir ortamda dolaşması güvenlik kaygılarının artmasına sebep olmaktadır. Genel olarak, kurumların veri iletişiminde kullandığı tüm kaynakların güvenli olup olmamasını konu edinmiştir ("Ağ Güvenliği Temelleri", 2020).

Ağ güvenliğini sağlamak için ağın mimarisi ve bu mimari üzerinde çalışan uygulamaları incelemek cihazların ve uygulamaların güncelliğini, yönetilebilirliğini ve yasalara uygunluğunu kontrol etmek yapılabilmektedir. Ağ altyapısına gelebilecek siber güvenlik tehditlerine karşı önceden hazırlıklı olabilmek adına firewall cihazları ile kontroller sağlanabilmektedir. Firewall'lar kısaca, yerel ağ ile dış ağ arasındaki güvenlik kontrolünü sağlayan yazılım ya da cihazlardır diye tanımlanabilmektedir. İlk kurulduğunda belirlenen noktadaki tüm geçişleri durdurur, sonrasında belirlenen protokoller dahilinde hangi veri paketlerinin geçip geçmeyeceği ve hangi geçişlerde parola doğrulaması kullanılacağı belirlenir. Böylece sisteme ulaşan kişi ve veri trafiği kontrol altına alınarak gerekli kurallar belirlenir (Bilisim, R. 2020).

Firewall yazılımları, Ağ Adresi Çeviricisi (NAT) sayesinde Yerel Ağ Bağlantısı (LAN)'ndaki yani aynı yerel ağ içerisinde bulunan birçok cihazın aynı İnternet Protokol (İP) adreslerinin gizlenerek tek bir İP ile dış ağlara erişimini sağlar. Bu sayede dış ağlardaki kullanıcılar yerel ağlardaki kritik topoloji ve İP bilgilerini edinemezler (Bilisim, R. 2020).

Şekil 1.4

Güvenlik Duvarı Kullanımı



1.4.4. Olağanüstü Durum Kurtarma/İş Sürekliliği Planlaması

Olağanüstü durum kurtarma planı (DRP), bir felaketin ardından mevcut kaynakların, veri ve bilgi sistemlerinin hızlı ve etkili bir şekilde geri yüklenmesiyle birlikte hızlı bir şekilde sistemin devam ettirilebilmesini sağlayan bir iş sürekliliği planı ve yönetilen prosedürdür. Bu felaketler, bir afet, geniş kapsamlı ve hasar yaratan bir kaza veya doğal afet de dahil olmak üzere ani bir olay olarak sınıflandırılabilir. Ayrıca bu felaket genellikle bir siber güvenlik ihlali içerir. Bir kurum ya da kuruluşu etkileyen potansiyel tehditlere hazırlanmayı, bunları önlemeyi ve bunlardan kurtulmayı amaçlar. Bir kurtarma stratejisi belirlenirken finansal bütçe, kaynaklar, teknoloji, yönetimin tehlikelere ilişkin pozisyonu ve donanım konuları dikkate alınmalıdır (Srinivasan & Simna, 2017, s. 125-130). DRP, bir felaketten sonra normal operasyonlara nasıl hızla devam edilebileceğini açıklayan bir yaklaşımdır. Bir afetin etkilerini en aza indimeye yönelik önlemlerden oluşmaktadır. Tipik olarak, olağanüstü durum kurtarma planlaması, iş süreçlerinin ve süreklilik ihtiyaçlarının bir analizini içerir. Olayları hızlı bir şekilde ele alma yeteneği, aksama süresini azaltabilir ve hem finansal hem de itibar zararını en aza indirebilir.

Olağanüstü durum kurtarma planlaması yapılırken dikkat edilmesi gereken birkaç adıma bakacak olursak,

- Kurum ya da kuruluşlardaki varlıkların kapsamlarını tanımlamak

- Olası tehdit ve güvenlik açıklarını belirlemek
- Verilerin korunmasını sağlamak
- Olağanüstü durum kurtarma ekibini oluşturmak
- Ekibin üyelerine eğitim vermek
- Bir veri kurtarma planı oluşturmak
- Veri kurtarma planını test etmek
- Bu planı düzenli olarak gözden geçirmek
- Düzenli olarak yedek almak
- Planı gerekli durumlarda düzenli olarak güncellemek ve revize etmek

şeklinde sıralayabiliriz (Touhid, 2019).

Olağanüstü durum planları söz konusu iken, yönetimden en alt giriş düzeyine kadar çalışanları dahil etmek planın değerini artırmaya yardımcı olur. Herhangi bir felaket durumunda bu olayı etkili ve verimli bir şekilde halledilebilir olmasını mümkün kılar.

1.4.5. Operasyonel Güvenlik

Operasyonel güvenlik (OPSEC), siber güvenliğin analitik ve risk yönetimi unsurlarını oluşturmaktadır. Kritik veya hassas bilgileri tanımlar ve hassas bilgilerin güvenliğini sağlamak için bir koruma mekanızması geliştirir (Touhid, 2019). OPSEC, hem bir süreç hem de bir stratejidir. Operasyon ve sistemlerin potansiyel bir saldırganın bakış açısından görülmesine teşvik etmektedir. Davranış izleme, sosyal medya takibi ve en iyi güvenlik uygulamaları gibi analitik faaliyet ve süreçleri içerir. Operasyonel güvenlik, kurum ve kuruluşların süreçlerindeki, işleyiş biçimlerindeki ve çalışanlarının kullandığı yazılım ve donanımlardaki potansiyel tehditleri ve güvenlik açıklarını keşfetmek için risk yönetiminin kullanılmasını sağlar ("What is operational security? OPSEC explained", t.y.). Kullanıcıların bir ağa erişirken sahip oldukları izinler ve verilerin nasıl ve nerede depolanabileceğini veya paylaşılabileceğini belirleyen prosedürler bu kapsama girer (Bursa Uludağ Üniversitesi, t.y.).

Etkin bir operasyon güvenliği programı geliştirmek için, operasyonel güvenlik görevlileri öncelikle olası tehditler bulup tanımlar, ardından gerekli önlemleri alırlar. Bu programı gerçekleştirebilmek için aşağıdaki gibi beş adım vardır.

1. İlgili yerin hassas bilgilerini tanımlamak
2. Tehdit oluşturan olası kategorileri tanımlamak
3. Güvenlik açıklarını tespit ve analiz etmek
4. Risklerin incelenip değerlendirilmesi
5. Risklerin azalması için gerekli karşıt önlemlerin alınması (Touhid, 2019)

Bir OPSEC süreç planının anlaşılması basit, uygulanması ve takip edilmesi kolay olmalıdır. Güvenlik tehdidi ortamı geliştikçe güncellenmelidir.

1.4.6. Son Kullanıcı Eğitimi

Sadece devlet, kamu kurum ve kuruluşları değil aynı zamanda son kullanıcılara ait bilgisayar, tablet ve cep telefonları da sibey uzay içerisinde yer almaktadır. Bilişim alanındaki tüm donanımların böylesine birbirine bağlı olduğu bir uzayda, güvenliğin sağlanması gerek devlet gerekse kişiler tarafında oldukça önem taşımaktadır (Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık, 2018, s. 91). Bu sebeple son kullanıcılar herhangi bir zamanda etkisini gösterebileceği için ve öngörülemeyen bir siber güvenlik faktörü olması nedeniyle en önemli güvenlik riski haline gelebileceği görülmektedir.

Siber suç veya siber savaşlarla mücadele bireylerden yani kullanıcılardan başlamaktadır. Son kullanıcı tehditleri aşağıdaki yollar aracılığıyla gelebilmektedir.

- Sosyal medya kullanımları
- Mesajlaşma ve mesajlaşma uygulamaları
- Uygulama indirme
- E-posta kullanımı
- Şifre oluşturma ve kullanımları (Touhid, 2019)

Düzenli olarak siber güvenlik farkındalık eğitim programları düzenlemek etkili olabilmektedir ve aşağıdaki konuları kapsaması gereklidir.

- Siber güvenlik ve önemi
- Farklı siber tehdit türleri
- İnternet nasıl kullanılır
- E-posta kimlik avı ve sosyal mühendislik saldırısı
- Cihaz güvenliği
- Fiziksel güvenlik
- Şifre oluşturma ve kullanımları (Touhid, 2019)

1.5. Siber Suç

Siber suçlar konusunda tamamen kesinleşmiş bir tarif olmasa da en geniş kabul gören tarif Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu'nun Mayıs 1983 tarihinde Paris Toplantısı'nda bahsettiği gibi "Bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış" olarak tanımlanmıştır (Altınok & Vural, 2011, s. 75). Genel anlamıyla bilişim alanındaki yeniliklerle paralellik göstererek çoğunlukla sanal ortamda birey ve kurumlara maddi ve manevi zarar veren davranışlardır (Dijitalleşen Dünyada Bilişim Suçları ve Mücadele Yöntemleri, 2022, s. 3).

Teknolojinin hızlı ilerlemesi ve buna paralel olarak internet kullanımının yaşamımızdaki tüm alanlarda artması ile birlikte bilişim alanında işlenen suçlar da artmaktadır. Siber suç, tüm dünyada yer alan küresel bir meseledir. İnternet üzerinden gerçekleştirilmesi sebebiyle suç dünyasındaki en yeni ve karmaşık suçları kapsamaktadır. Kontrol edilmesinin zorlaşmasının yanında yeni olması sebebiyle bilinmezliklerini koruyarak dünyanın heryerinde hükümet ve kuruluşlar için bilişim alanındaki suçların önüne geçilebilmesini gitgide zorlaştırmaktadır.

Siber hırsızlar son zamanlarda bireylerin sosyal medya gönderilerini incelemekte, konum servislerini kullanmakta ve hatta ebeveynlerin çocuklarını gözlemleyebilmek için yerleştirdiği bebek monitörlerine bile sızabilmektedirler. Bugün sanal ortamları kullanan tüm kişiler bu tehdite maruz kalmaktadır. İnternet ortamında çok hızlı bir şekilde meydana geldiği de düşünülürse bu konuda etkin ve güçlü savunma sistemleri inşa edilmelidir. Ayrıca her geçen gün değişen ve yenilenen bir konu olması sebebiyle daha fazla araştırılması gereken bir alandır. Gerekli hukuki düzenlemelerin yapılmaması durumunda birçok kişi ve kurumun zarar görmesi olasıdır (Küçükçavdar, 2018, s. 1-15).

Uluslararası Telekomünikasyon Birliği (ITU)'ne göre siber suçlar şu şekilde sınıflandırılmıştır.

- Bilgisayardaki veri ve sistemlerin gizliliğine, bütünlüğüne ve kullanılabilirliğine karşı işlenen suçlar (yasadışı erişim, veri çalma, veriye müdahale vb.),
- Bilgisayar ile ilgili suçlar (online kumar, kimlik hırsızlığı, ücret sahteciliği vb.)
- İçerikle ilgili suçlar (ırkçılık, nefret söylemi, şiddeti övme, yanlış bilgi vb.)
- Telif hakkıyla ilgili suçlar (telif ve fikri mülkiyet haklarına saldırı)

Sanal ortamda gerçekleşen bazı siber suç çeşitlerine bakacak olursak;

Dolandırıcılık: Suçluların kendileri için kazanç veya fayda amacıyla bilgileri yetkisiz bir şekilde değiştirmesi, yok etmesi ve kötüye kullanmasıdır.

Hırsızlık: Veri ve yazılım hırsızlıklarını kapsamaktadır.

Lisanssız yazılım kullanımı: Yasal olmayan yazılımların çoğaltılmış hallerini kullanmaktır.

Özel iş: Siber suçlunun özel kazanç ve menfaatleri için kurum veya kuruluşların bilgi işlem bilgisi ve olanaklarının yetkisiz şekilde kullanılmasıdır.

Kişisel bilgilerin kötüye kullanılması: Sanal ortamda resmi olmayan şekilde gezinme ve bireylerin verilerinin yetkisiz şekilde kullanılarak ihlal edilmesidir.

Hacklemek: Bilgisayar sistemlerinde kasıtlı bir şekilde yetkisiz olarak verilere erişim sağlanmasıdır.

Casusluk: Suçluların diğer kişilere gizli verileri satmak suretiyle kişisel bilgisayar veya sistemlere saldırmasıdır.

Sabotaj: İşlem döngüsüne, sisteme veya fiziksel metaryellere kasıtlı zarar verilerek bilgisayarların süreçlerine ve işlemlerine müdahale edilmesidir.

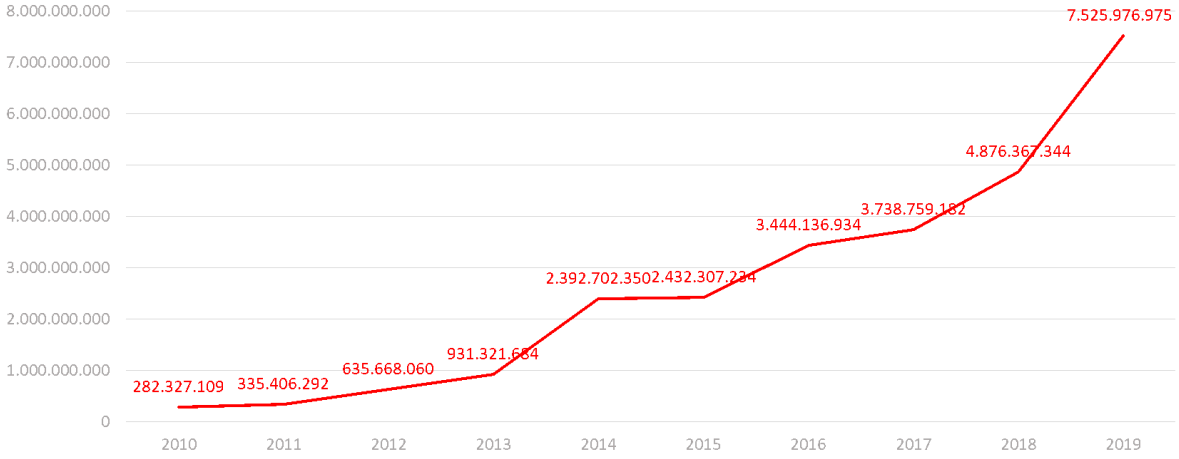
Siber terörizm: Sanal ortamdan terör saldırılarının gerçekleştirilmesidir.

Virüs: Bilgisayarların işleyişlerini bozmak amacıyla zararlı yazılım ve programların dağıtılmasıdır (Cengiz, 2021, s. 412-413).

şeklinde sıralayabiliriz.

Şekil 1.5

Dünyada Siber Güvenlik Alanında Girişimcilere Yapılan Yatırım Miktarı Dünyada Ve Türkiye'de Siber Güvenlik Gerçekleri-1: İstatistikler, Analizler, Öngörüler, Yılmaz, t.y.



Günümüzde küresel çapta siber suçlar yaklaşık 6-7 trilyon dolarlık zarara yol açmaktadır. Gelecek üç yıl içerisinde bu zararın 10 milyon dolara ulaşması beklenmektedir. Şekil 1.5'te de görüldüğü üzere tüm dünyada siber suçlarla mücadele kapsamında büyük yatırımlar yapılmaktadır. Bu oranların büyüklüğü siber güvenliğin önemini bir kez daha gözler önüne sermektedir.

BÖLÜM 2

SİBER SALDIRI TEHDİTLERİ, TÜRLERİ VE ÖRNEKLERİ

Bu bölümde siber saldırı türlerine yer verilecektir. Aynı zamanda ülkemiz ve dünyadaki siber saldırı örnekleri üzerinden yola çıkılarak dikkat edilmesi gereken hususlar ele alınacaktır.

2.1. Siber Saldırı Tehditleri

Giderek daha fazla verinin olduğu bir dünyada, sosyal ağlar, çevrimiçi işlemler, internet üzerinden saklanan ve yönetilen bilgiler ve Bilgi Teknolojileri (BT) sistemleri kullanılarak gerçekleştirilen otomatik işlemler, bilgi güvenliği ve veri gizliliği bakımından sürekli olarak risklerle karşı karşıyadır.

Ağlara, programlara ve verilere yetkisiz erişim elde etmek için sürekli olarak yeni yollar geliştiren saldırganlar, bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini tehlikeye atarak hedeflerini bireyler ya da küçük veya orta ölçekli kurum ve kuruluşlara hatta dev organizasyonlara kadar büyük tutmayı amaçlıyorlar (Bendovschi, 2015, s. 24-25).

Şekil 2.1

Anlık Gerçek Zamanlı Siber Saldırı Haritası Kaspersky cyberthreat gerçek zamanlı harita, 2022



Siber saldırı, saldırganlar tarafından bilgi ve iletişim sistemlerini (BİS) devre dışı bırakma, yetkisiz erişimde bulunma, verileri çalma, değiştirme veya yok etme, verileri ifşa etme, üçüncü kişilerle paylaşma, ek saldırılar başlatma veya tüm verileri yok etme gibi amaçlarla ihlal edilmiş olan bir bilgisayar sistemini kullanmaya çalışma girişimidir. Saldırıda bulunulan oluşumun bilgi sistemlerini ihlal etmeyi amaçlar. Saldırı hedefleri arasında ise kişisel bilgisayarlar, bilgisayar ağları, BT altyapısı ve BT sistemleri yer almaktadır.

Siber saldırıları başlatan kişilere genellikle siber suçlular, tehdit aktörleri, bilgisayar korsanları, siber saldırganlar veya hackerlar denir. Tek başlarına, diğer saldırganlarla işbirliği içerisinde veya organize bir suç grubunun bir parçası olarak da çalışabilirler. Saldıracakları sistemlerdeki güvenlik açıklarını (bilgisayar sistemindeki sorunlar ve zayıflıklar) belirlemeye çalışırlar ve hedeflerini gerçekleştirebilmek için bu açıkları kullanırlar. Ardından tespit edilen zayıflığa göre yöntem belirlenerek siber saldırı gerçekleştirilir.

2.2. Siber Saldırı Türleri

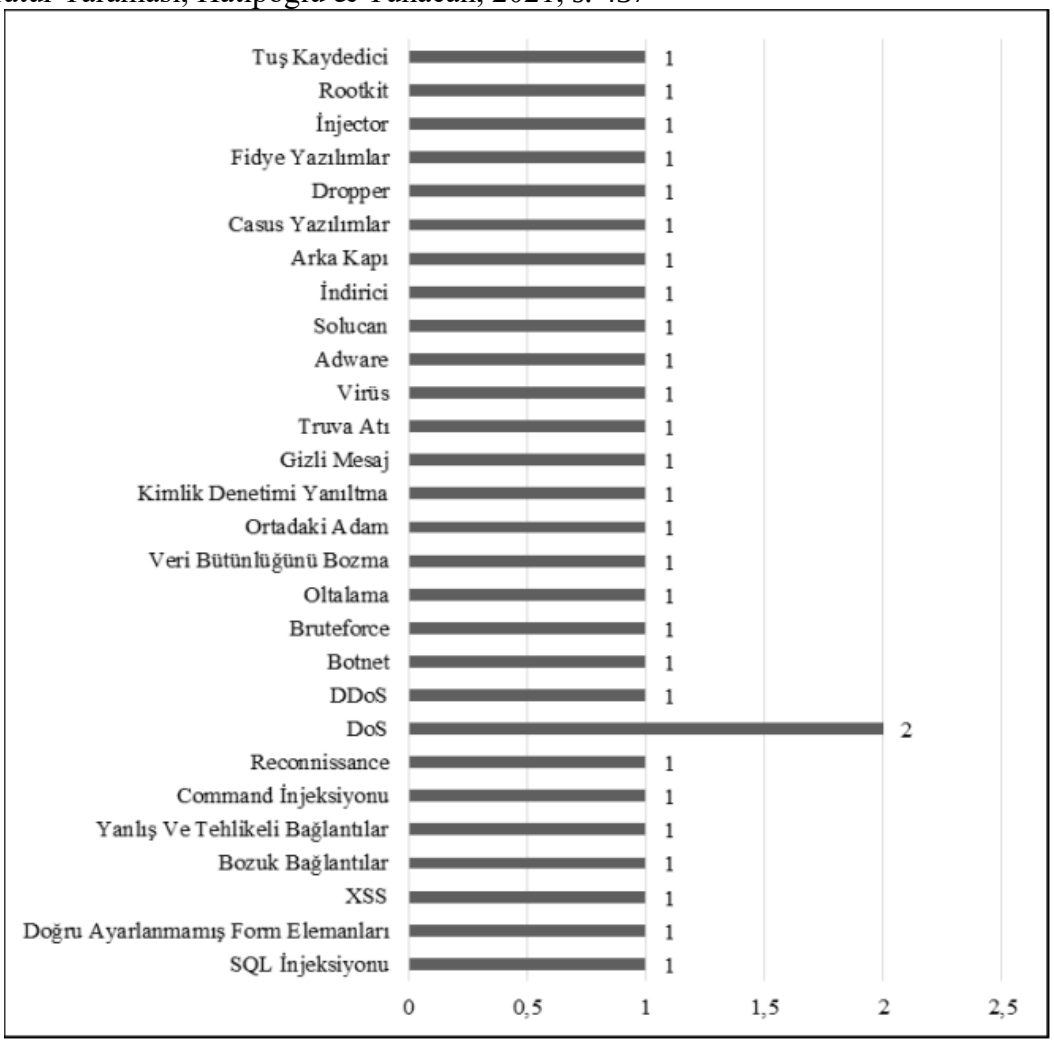
Siber saldırılar, fiziksel altyapılara saldırma ve sosyal mühendislik dışında genel olarak internet üzerinden yapılan saldırılar olarak gerçekleşmektedir. Dünyanın herhangi bir yerinde son derece basit ve maliyetsiz bir şekilde bu saldırılar kolaylıkla yapılabilmektedir (Yılmaz, t.y., s. 29-30).

Siber saldırı çeşitleri artmakta olan saldırı kapasitesi sebebiyle devamlı gelişmekte ve sürekli yenileri eklenmektedir. Böylelikle alınan güvenlik önlemleri de gitgide artmakta her geçen gün güncellenmektedir.

Zararlı yazılımlar, trojenler, virüsler ve solucanlar ile engelleme saldırıları olan Dağıtık Hizmet Reddi Saldırıları (DDOS), sosyal mühendislik girişimleri, oltalama ve yemleme (phishing) saldırıları, klavye dinleyicileri vb. gibi bir çok çeşitli yöntem vardır. Saldırganlar bu yöntemler ile eriştikleri sistemlerde büyük zararlara yol açabilirler. Bu zararlarla kamu veya özel kurum ve kuruluşlarda ciddi maddi zararlara sebep olabileceği gibi itibar kaybı gibi manevi zararlara da sebep olabilirler (Alioğlu, 2019).

Şekil 2.2

2020 Yılı Siber Saldırı Türleri Dağılımı Türkiye'de Siber Saldırı ve Tespit Yöntemleri: Bir Literatür Taraması, Hatipoğlu & Tunacan, 2021, s. 437



Bu bölümde her geçen gün saldırı çeşitlerinin sürekli yenilenen ve değişiklik gösteren daha bir çok çeşidi olması sebebiyle temel saldırı çeşitlerine değinilecek olup bu saldırı çeşitleri ve uygulanış biçimleri incelenmeye çalışılacaktır.

2.2.1. Zararlı Yazılımlar

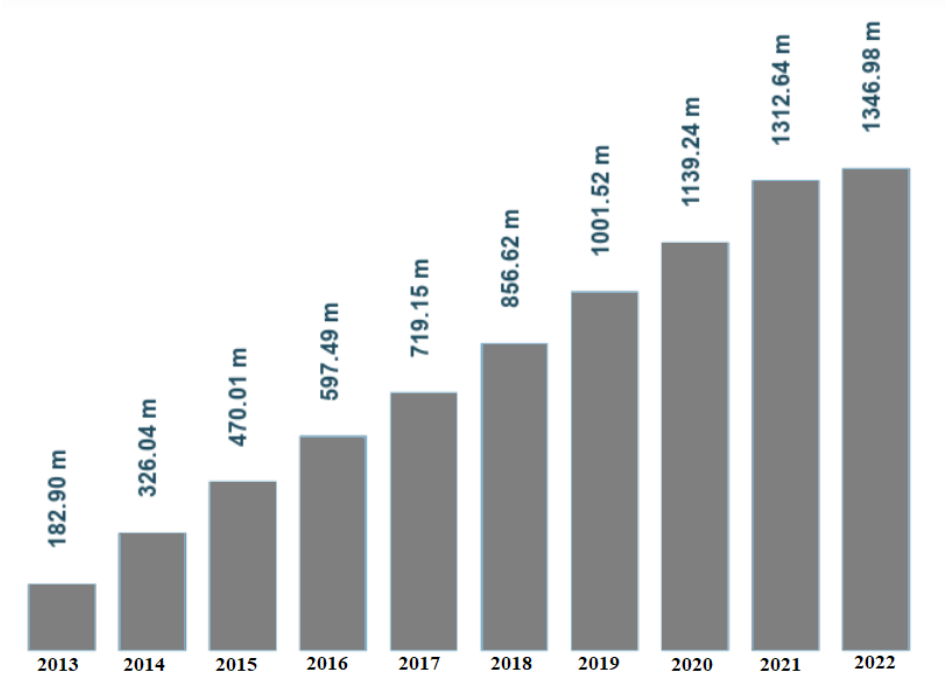
Kötü amaçlı yazılım saldırısı, kullanıcının herhangi bir izni ve yetkisi olmadan bir sisteme bulaşarak zarar veren ve yetkisiz bir şekilde erişerek izleyen siber saldırı sınıfıdır. Bu yazılımlar özel ağlara erişebilir, bilgi işlem süreçlerini kesintiye uğratabilir, hassas

bilgileri veya kullanıcı bilgilerini çalabilir ve bunların sonucunda saldırganlar yasadışı yollarla para kazancı sağlayabilirler (Biju et al., 2019, s. 4851).

Genellikle bir kullanıcı güvenli olmayan bir bağlantıya veya e-posta eki, reklam vb. gibi bir tekdüzen kaynak bulucu (URL)'ya tıkladığında zararlı yazılımlar bilgisayara bulaşarak yüklenir ve bir güvenlik açığı bularak ağı ihlal etmeye başlar. Bu durum sistemin çalışmasını değiştirir, verileri yok eder veya sistemin içinden geçerek kullanıcı veya ağ trafiğini gözetleyebilir. Cihazları işlevlerini kaybettirecek şekilde yavaşlatarak sistemin kullanılamaz bir hale gelmesine sebep olabilir. Ayrıca bu kötücül yazılımlar saldırganlar tarafından uzaktan kontrol ve erişim yetkisi de elde edilmesine yol açabilir. Bir cihazdan diğerlerine yayılabilir veya yalnızca ana cihazı etkileyerek yerinde de kalabilir.

Şekil 2.3

Zararlı Yazılımların Artışı Malware Nedir, Nasıl Temizlenir? - Malware Saldırı Türleri ve Önleme Yöntemleri, t.y.



Şekil 2.3'te zararlı yazılımların yıllar içinde ne kadar çok artış gösterdiğini görüyoruz. Bu durum tehditlerin büyüklüğünü de gözler önüne sermektedir. Bu kapsamda virüsler, solucanlar, truva atı, fidye yazılımı, casus yazılım vb. gibi zararlı yazılımları ele alacağız.

2.2.2. Virüsler

1949'da Illiniois Üniversitesinde "Theory and Organization of Complicated Automata" adlı dersi veren John Von Neumann tarafından virüs hakkındaki ilk akademik çalışma yapılmıştır. Daha sonra 1983'te ise Fred Cohen tarafından bilgisayar virüsleri ilk kez tanımlanarak hayatımıza girmiştir (Sack, 2021).

Bilgisayar virüsleri, kendilerini başka bi programa, bilgisayar ön belleğine veya belgelere kopyalayarak çoğalan ve bilgisayarların çalışma şekillerini bozan/değiştiren kötü amaçlı yazılımlardır. Virüsler kendilerini, kendi kendilerine çoğaltabilirler.

Virüs oluşumunun bir çeşit insan müdahalesi ile başlaması gerekmektedir. Akabinde, sistemler arasında yayılabilmektedirler. Virüsler, virüslerin var olduğu bir sistemde kendi dosyalarını oluşturup belgelere ve sistemlere bulaşarak çoğalırlar ve sistemleri neredeyse kullanılamaz hale getirebilirler.

En basit şekilde örnek verecek olursak, bir kullanıcının internetten indirdiği, bir e-posta iletisinde aldığı veya çıkarılabilir bir depolama aygıtından (Evrensel seri veriyolu (USB) vb.) kopyaladığı yürütülebilir bir dosyada virüs bulunduğunda ortaya çıkar. Kullanıcı bu dosyayı çalıştırır çalıştırmaz virüs harekete geçer ve kullanıcının sistemine bulaşan kötü amaçlı kod çalıştırır. Daha karmaşık mekanizmalı yayılma yöntemlerinde ise, bulaşmış bir sistemde çalışan virüs, kendi yayılmasını başlatmak için harekete geçebilmektedir. Örneğin, bir virüs kendisini sistemdeki tüm medyalara kopyalayabilir ve kendisini bir kullanıcının kişilerine gönderilen e-posta mesajlarına ekleyerek kendisini paylaşılan dosya sunucularına kopyalayabilir (Chapple et al., 2021).

En çok karşılaşılan virüs çeşidi .exe uzantılı dosyalardır. Bu da çalıştırılarak kurulan dosyalar ile bulaşan bir tür olduğunu göstermektedir. .exe uzantılı dosyalar her çalıştığı seferde sisteme bulaşıp yayılmaktadır (Dijitalleşen Dünyada Bilişim Suçları ve Mücadele Yöntemleri, 2022, s. 29).

Bir bilgisayara virüs bulaştığını anlayabilmemize dair birkaç işarete bakacak olursak;

- Bilgisayarın açılması normalden uzun sürüyor ve performası yavaşlamış ise,
- Bilgisayar sık sık kapanma yapıyor ve hata mesajlarıyla karşılaşıyorsa,
- Bilgisayar tıklamalara yanıt vermiyor ve dosyaları açmıyorsa,
- E-postada bozukluk varsa,
- Bilgisayarda depolama alanı azaldıysa,
- Bilgisayardaki dosyalar ve diğer veriler kendiliğinden yok olduysa,

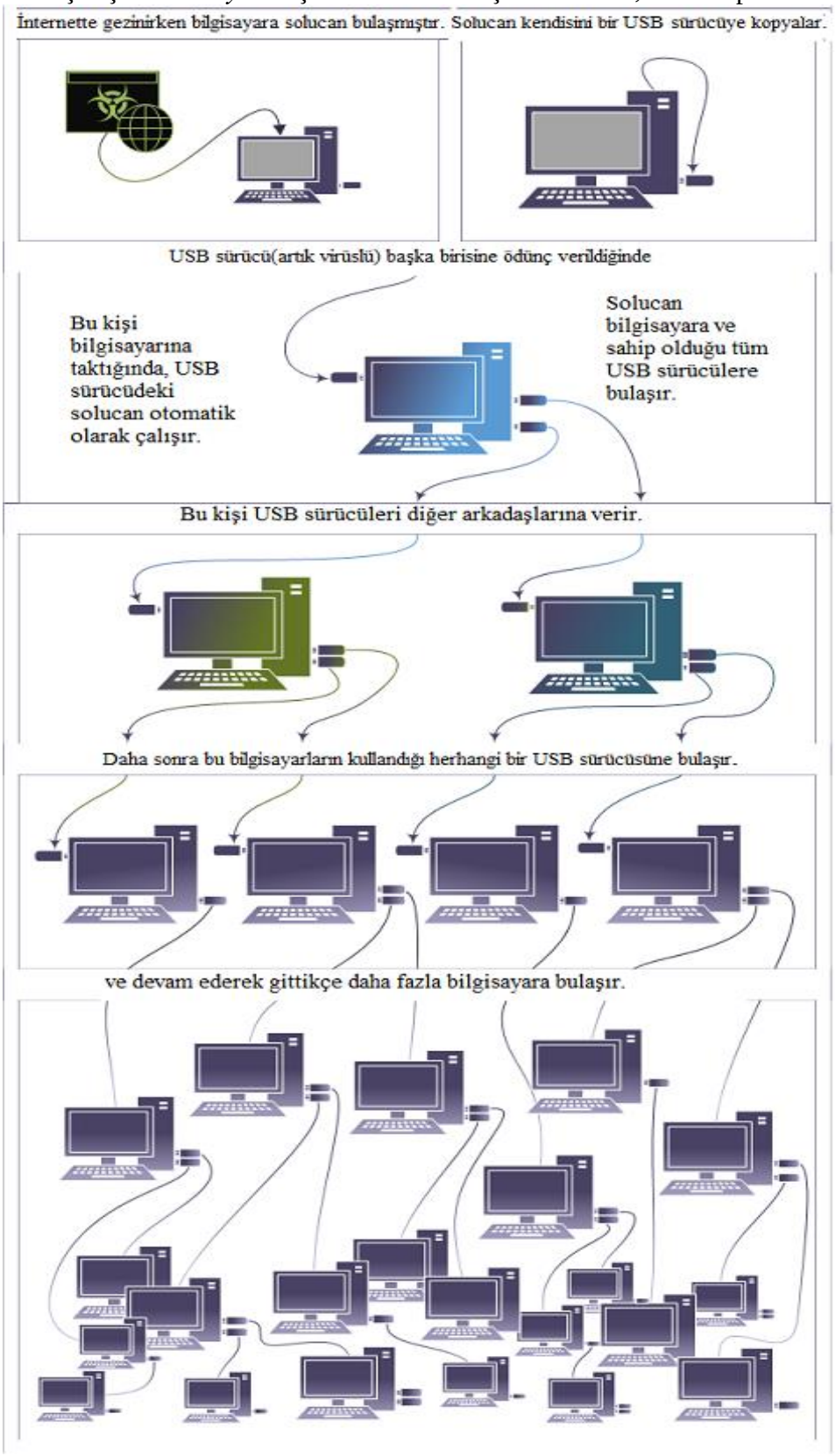
Bu belirtilerden biri ya da birkaçına denk gelinmiş ise bilgisayara çoktan virüs bulaşmış olma ihtimali oldukça yüksektir. Bu durumdan kurtulmak için doğru bir anti-virüs yazılımı kullanmak en iyi hamle olacaktır (Chapple et al., 2021). Fakat kullanılan anti-virüs programları düzenli aralıklarla çalıştırılarak kontrol edilmelidir. Ayrıca güvenli olmayan bağlantılara tıklamamak, güvenliğinden emin olunmadan her gelen e-posta ekine tıklamamak, önemli verilerin sıklıkla yedeklerinin alınması, taşınabilir belleklerin tarama yapmadan ve emin olmadan kullanılmaması gibi basit önlemlerle tedbirler alınabilmektedir.

2.2.3. Solucanlar (Worm)

Solucanlar da yine bir tür virüs çeşididir. Kendi kendisini kopyalayarak bir bilgisayardan diğer bir bilgisayara yayılmayı amaçlamaktadır. Bu işlemi çok hızlı bir şekilde yapmaya çalışarak bilgisayar sistemini ele geçirmek için kendisini çoğaltarak sistem ve sunucuları yavaşlatmayı hatta kullanılamayacak hale getirmeyi hedeflemektedir. Kendisini ve değiştirerek kopyalamış olduğu kopyasını ağ üzerinden geçirerek hızlı ve otomatik bir şekilde yayarak bir çok sisteme bulaştırıp taşıyabilmektedir (Dijitalleşen Dünyada Bilişim Suçları ve Mücadele Yöntemleri, 2022, s. 29).

Şekil 2.4

Solucanların Çalışma Ve Yayılma Şeklini Gösteren Şekil Worms, Dansimp & Christa, t.y.



Virüslerden farklı olarak bu yayılma işlemini ağ üzerinden yapmaktadır. Ayrıca yayılabilmek için bulaşma yoluyla taşınmaları gereken bir dosya türü gerekmemektedir. Yine virüslerin aksine ağa bulaşmak için herhangi bir insan müdahalesi de gerekli değildir.

Solucanlar, işletim sistemlerindeki güvenlik açıklıklarını bulduktan sonra bunları kullanarak veya e-posta yoluyla ağ üzerinden yayılmaktadırlar. Ağ üzerinde kopyalanarak çoğalması ve yayılması sistemdeki alan, güç ve bant genişliği gibi ağ kaynaklarını şişirerek tüketmektedir (Pande, 2017, s. 20).

2.2.4. Truva Atları (Trojenler)

Truva atı saldırıları, normalde faydalı ve zararsız gibi gözükmektedir. Fakat içine kötü amaçlı yazılımlar gizlenmiş, arka planda kullanıcıdan habersiz işlemler yapan zararlı bir yazılım türüdür (Akarslan, 2012, s. 93).

Truva atı virüsü adını geçmişte yaşanıldığına inanılan bir efsaneden almıştır. Bu efsaneye göre Antik Yunan kentinde tahta ile bir at yapılıyor ve bu atın içine Yunan askerleri koyuluyor. Bu şekilde tamamen zararsız ve armağan gibi gözükmekte olan bu at Troy şehrine armağan ediliyor. Gece olduğunda ise atın içinden çıkan askerler Troy şehrinin kapılarını açarak Yunan ordularının kolayca içeriye girmesine ön ayak oluyor. Böylece Yunan askerleri tarafından Troy şehri kolayca ele geçiriliyor.

Tıpkı geçmişteki efsane gibi truva atı virüsü de ilk başta zararsız gibi görünerek kullanıcıların bu dosyaları indirmesini sağlar. İndirildikten sonra ise bu dosyanın çalıştırılması ile Truva atı sisteme giriş yapabilmektedir.

Genellikle kullanıcıların indirdikleri programın içeriği ile ilgili bilgi sahibi olmadan yüklediği programlardan gelmektedirler. Örneğin, bir kullanıcı “Flash Player” programını yüklediğini zannederek “Adobe” veya güvenilir bir program yerine rastgele bir web sitesinden güvenilirliğinden emin olmadan “Flash Player” yüklemesi durumu örnek gösterilebilir. Böyle bir hamleden sonra truva atı içeren programlar, dosyaların sisteme indirilmesi adımından sonra yüklenmesiyle birlikte bilgisayar sistemlerine bulaşmaktadırlar (Siber Güvenliğe İlişkin Temel Bilgiler, 2014, s. 10-11).

Görüldüğü üzere truva atları da tıpkı virüsler gibi bir kullanıcının komut veya hareketine bağlı olarak çalışmaktadır. Kullanıcının truva atı içeren programı çalıştırması ile harekete başladığı görülmektedir.

Bir bilgisayarda aşağıdaki gibi olağandışı belirtilerin gözlemlenmesi ile truva atı bulaştığını tespit edebiliriz.

- Truva atları genellikle çok fazla bilgi işlem kaynağını tüketmesi sebebiyle bilgisayararı yavaşlatabilir.
- Bilgisayarları çok fazla çalıştırması sebebiyle sistemlerde çökmelere sebep olabilir.
- Bilgisayara birçok ek kötü yazılım yüklemesi sebebiyle sistemde tanıdık olmayan kötü amaçlı yazılımlar görülebilir. Masaüstünde ve uygulamalarda da farklı ve yeni simgeler eklenebileceğinden alışıldığın dışında yeni simgeler gözlemlenebilir.
- Bazı truva atları bilgisayarın alan adı sistemi (DNS) ayarlarını değiştirerek kötü amaçlı ve sistemlere zarar verebilecek sitelere yönlendirmeler yapabilir.
- Normalden fazla açılır pencerelere maruz kalınabilir. Truva atları reklam yazılımları yüklemiş olabilirler.
- Truva atları kötü amaçlı yazılımların sistem tarafından farkedilmemesi için bilgisayardaki antivirüs programlarını devre dışı bırakmaya çalışabilirler (Belcic, 2021).

Bu sebeple bir sistem ya da bilgisayara indirilmek istenen dosyaların veya uygulamaların indirilmeden önce antivirüs programı taramasından geçirilmesi oldukça önem arz etmektedir.

2.2.5. Fidye Yazılım (Ransomware)

Fidye yazılımı, bulaştığı sistemlerin bir kısmını veya tamamını şifreleyerek erişilemez hale getiren sonrasında da saldırganlar tarafından şifrenin kırılabilmesi için mağdur kişilerden para talep ettiği zararlı yazılımlardır. Kullanıcıların verileri yeniden görüntüleyebilmesi için talep edilen parayı ödemeleri istenmektedir. Yine de kulanıcılar istenilen parayı ödese bile bu durum verilere kesin bir şekilde yeniden ulaşacağı anlamına gelmemektedir (Sağıroğlu & Alkan, 2018, s. 230). Kurbanın fidyeyi ödeyememesi durumunda saldırgınlar bilgilerin ifşa edileceğine dair tehditlerde bulunurlar.

Genellikle bu yazılımlar kullanıcılara kötü amaçlı yazılım programları içeren ek ile birlikte e-posta gönderilerek veya direkt indirme yoluyla bilgisayarlara yayılabilmektedirler. Saldırganlar verileri şifreledikten sonra kullanıcılara ulaşarak sistemlerinin kilitlenip şifrelendiğini belirterek fidye ücretinin ödenmemesi durumunda tekrar erişimde bulunulamayacağını bildirir. Genel olarak saldırganlar ifşa olmamak için ödemeyi son

zamanlarda oldukça yaygın olan kripto para türlerinden yapılarak anonim bir hesaba gönderilmesini talep etmektedirler.

Şekil 2.5

Ransomware Saldırısı Anlatımı Fidye Yazılımları Nedir? Nasıl Çalışır? (Ransomware), Netpro, 2020



Fidye yazılımlar arasında Wannacry ve Notpetya son zamanlarda bu saldırı türü için ünlüdür. Wannacry mayıs 2017'de Microsoft Windows işletim sistemli bilgisayarlara yayıldı ve mağdurların dosyalarını rehin olarak elinde tuttu. Dosyaların geri verilmesi için Bitcoin cinsinden fidye istendi ("WannaCry fidye yazılımı nedir?," 2021). Notpetya ise çalışma prensibi Wannacry ile aynı olup en maliyetli saldırılar arasında sayılmaktadır.

2.2.6. Casus Yazılım (Spyware)

Casus yazılımlar, kullanıcılara ait bilgiler ile kullanıcıların internet üzerinde yaptığı işlemleri, kullanıcıların bilgisi olmadan tarayıp toplayarak kötü niyetli kişilere göndermeyi sağlayan kötü amaçlı bir yazılım çeşididir. Bu yazılım da diğerleri gibi kullanıcı farketmeden bulaştırılmaktadır. Fakat diğer yazılımlar gibi kendi kopyalarını oluşturarak sistemde yayılmaya ihtiyaç duymamaktadırlar (Canberk & Sağıroğlu, 2007, s. 125-126).

Casus yazılımlar sisteme girdikten sonra bilgisayarlardaki kullanıcılara ait olan özel bilgileri tararlar. Bu bilgileri çerez ve log dosyalarından elde etmeleri mümkündür. Bu kişisel veriler bir dosyada birleştirilir ve sonrasında birleştirilmiş olan dosya kötücül yazılımı

gönderen kişiye bu yazılımlar aracılığıyla açık bırakılan arka kapılar vasıtasıyla internet üzerinden gönderilir. Toplanan veriler genelde reklam amaçlı kullanılır. Saldırgan, toplamış olduğu verilerden ötürü kurbanın internet alışkanlıklarını öğrenmiş olması sebebiyle ilgisini çekebilecek reklam çeşitlerini e-posta yöntemiyle göndererek kullanıcının tıklamasını sağlamaktadır. Bu sayede internet bankacığı, kredi kartı vb. gibi kritik bilgilere erişim sağlanarak kullanıcın banka hesapları vb. boşaltılabilmektedir (Daş et al., t.y., s. 1-2).

Casus yazılımlar en çok kullanıcı zafiyeti ve sosyal mühendislik yöntemleri gibi açıklar sebebiyle bulaşmaktadırlar. Buna ek olarak özellikle orjinal yazılım olmayan indirilen dosyalardaki crackli denilen orjinal lisans numaraları da mevcut olan programların arkasına yerleştirilerek kullanıcının haberi olmadan bu dosyaları bilgisayarlarına indirmeleriyle birlikte bulaşmaktadırlar (Daş et al., t.y., s. 1-2).

2.2.7. Klavye Kaydedici (Keylogger)

Klavye hareketlerini kaydeden yazılımlar kullanıcıların klavye üzerinden yaptığı, tuşladığı her bilgiyi alarak saldırgana gönderen kötü amaçlı casus yazılımlardır. Kötü niyetli saldırganlar bu yazılım sayesinde saldırılan kullanıcının tüm günlük işlerini, kişisel ve finansal bilgilerini, hesap numarası, kredi kartı bilgileri, şifre vb. gibi oldukça kritik olan bir çok bilgiyi edinebilirler. Siber suçlular yazılan herşeyi kaydedebilir ve kullanabilirler.

Sadece yazılım olarak değil aynı zamanda klavye altına bir cihaz yerleştirilerek de gerçekleştirilebilen bu eylem ciddi güvenlik açıklıkları doğurabilmektedirler. Benzer şekilde bankamatiklerin tuşlarına da yerleştirilerek donanımsal olarak da kredi kartı bilgilerini çalma girişimlerinde de bulunulabilmektedirler (Dijitalleşen Dünyada Bilişim Suçları ve Mücadele Yöntemleri, 2022, s. 30).

2.2.8. Oltalama Saldırıları (Phishing Attacks)

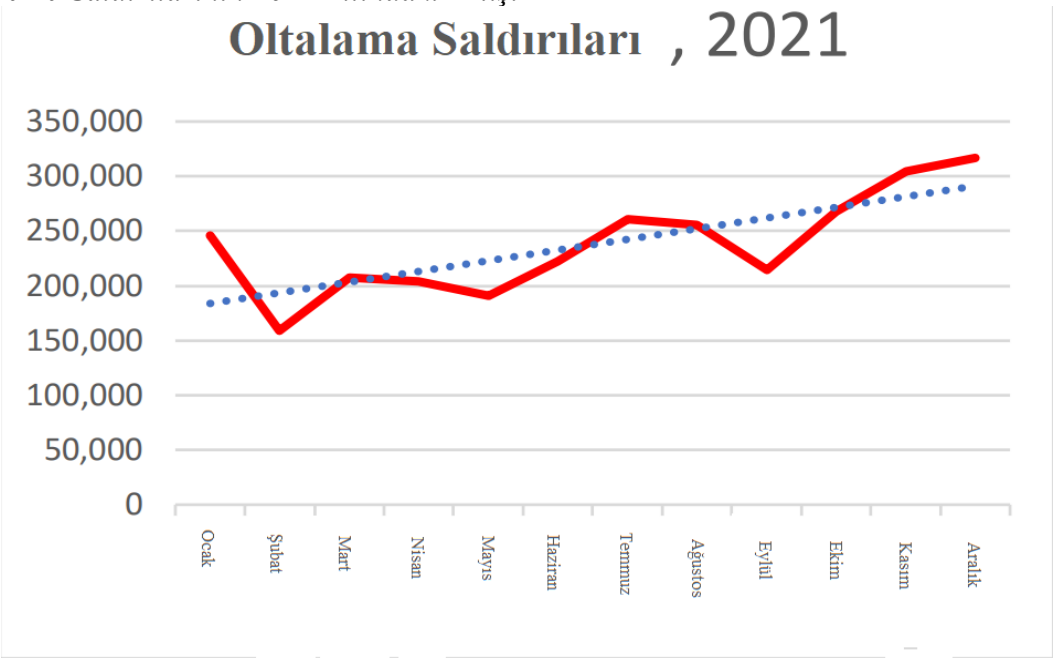
İngilizce Password Harvesting Fishing kelimelerinden türemiş Phishing yönteminde siber suçluların sisteme erişmek için genellikle e-postalar göndererek kullanıcının e-posta içindeki linke tıklamasını sağlayıp bu linkteki sahte internet sitesinde kişisel verilerini gerekli yerlere girmesini sağlamaktır.

Saldırganlar güncel olaylar ve gelişmeleri kendilerine ilham alıp kullanıcıların dikkatini çekebilecek tuzaklar kurarak kullanıcılara genellikle e-posta ekindeki sahte web sitesi linkleriyle mağdurları kandırmaktadırlar (Kara, 2021, s. 450).

Başka bir yöntemde ise resmi kurum ve kuruluşların web sitelerini taklit ederek mağdurların bu sitelere giriş yaparak sahte formları doldurmaları sağlanabilmektedir. Bu tuzak vasıtasıyla kullanıcıların banka hesapları kolayca boşaltılabilmektedir ya da bu bilgiler kötüye kullanılabilmektedir (Kara, 2021, s. 450).

Şekil 2.6

Oltalama Saldırılarının 2021 Yılındaki Artışı



Anti-oltalama saldırıları çalışma grubu (APWG)'nun yayınlamış olduğu rapora göre, 2021'in dördüncü çeyreğinde saptanan oltalama saldırıları için hazırlanmış olan web siteleri sayısı 888.585 ve kişiler veya şirketleri hedef alan oltalama saldırıları için hazırlanmış e-posta sayısının ise 42.748 olduğunu yayınlamışlardır (APWG, 2022).

Tablo 2.1

Web Siteleri ve E-posta Adreslerine Yapılan Oltalama Sayıları

	Ekim	Kasım	Aralık
Web sitelerine yapılan oltalama saldırıları	267,530	304,308	316,747
E-mail hesaplarına yapılan oltalama saldırıları	12,350	13,937	16,461

Phishing Activity Trends Report, 1st Quarter 2022, 2022, s. 3

2.2.9. Rootkit

Unix işletim sistemlerinde yönetici anlamında kullanılan "root" isminden gelen Rootkitler, işletim sistemi çekirdeğine sızarak saldırganlara bilgisayar üzerinde tam yetki verebilen zararlı yazılımlardır. Saldırgan tarafına bu denli büyük ve ciddi bir yetki vermesi sebebiyle en tehlikeli yazılım olduğu bile söylenebilmektedir. Log kayıtlarını silerek veya saldırgan proseslerini silerek saldırının izlerini de yok edebilmektedirler. Bu sayede daha sonraki saldırılara da girişlerini kolaylaştırabilmeleri mümkün olabilmektedir (Canberk & Sağıroğlu, 2007, s. 127).

İşletim sistemi çekirdeği seviyesinde çalışması sebebiyle tespit, analiz ve silme süreçleri oldukça zordur. Bu saldırı çeşidinde rootkit saldırganlarının ileri düzeyde işletim sistemi ve donanım bilgisine sahip olması gerekmektedir. Böylece bu tip saldırıların oldukça akıllı ve bilgili kişiler tarafından yapıldığı görülebilmektedir (Özkaya, 2020, s. 51).

Bu yöntem ile bilgisayara saldıran kişinin yapabileceklerinin sınırı yoktur. Tüm sistemi ele geçirmesi sebebiyle her türlü gizli ve özel veriye erişimi mümkündür. Banka ve kredi kartı bilgileri, kullanıcı hesap bilgileri, mikrofon ve kameraya erişerek mahremiyete de zarar verebilecek olaylar gerçekleştirebilmektedirler.

Her biri farklı platformları etkileyen 8 farklı tipte rootkit türü vardır. Bunlar sırasıyla;

Kernel Rootkit: Çekirdek seviyesinde işletilirler ve tespit edilebilmesi için ileri seviye işletim sistemi ve çekirdek bilgisine sahip olunması gerekmektedir. Bilgisayar üzerinde tam bir yetki sağlamaktadırlar.

Firmware Rootkit: Genellikle donanımsal aygıtlar üzerinde etkilidirler. Cihazın açılmasıyla aktive olup cihaz açık olduğu sürece işlemlerine devam edebilmektedirler. Tespitleri çok zor yapılabilmektedir.

Application Rootkit: Çekirdeği etkilemeden uygulama düzeyinde çalışırlar ve bilgisayarlardaki uygulamaları etkilerler. Uygulama dosyasını rootkit dosyasıyla değiştirerek ya da uygulamaya kod ekleyerek normal çalışmasına engel olarak değiştirirler.

Memory Rootkit: Bu türler rastgele erişilebilir bellek (RAM) üzerinde çalışarak kendilerini gizlerler. Kernel rootkittekine benzer şekilde kaynakları kullanarak RAM performansını düşürürler.

Bootkit Rootkit: Boot Loader Rootkit olarak da bilinen bu türler işletim sistemi her başlatıldığında işletim sistemi ile birlikte otomatik olarak çalışmaya başlarlar. Boot kayıtlarına yerleşmeleri sebebiyle standart dosya sistemlerinde görünmezler ve böylece anti-rootkit yazılımları bu türleri kolayca tespit edemezler. Bu çeşit rootkitler boot kayıtlarını değiştirerek bilgisayarları çalışmaz hale getirebilmektedirler.

Persistent Rootkits: Sistemin başladığı andan kapatıldığı ana kadar aktif olarak kalabilmektedirler. Sistemleri istemsiz şekilde yeniden başlatabilmektedirler.

Library Rootkits: Bilgisayarlardaki kütüphane dosyalarını etkilemektedirler. Örnek olarak Windows.dll gibi dosyalar gösterilebilir.

Hypervisor Rootkits: İşletim sistemlerindeki sanallaştırma teknolojilerini hedef olarak görmektedirler. Hyper-V, VmWare gibi sanal sunucu sistemlerini hedef almaktadırlar (Özkaya, 2020, s. 51-52).

2.2.10. DDoS (Hizmet Dışı Bırakma) Saldırıları

DDoS (Distributed Denial of Service) dağıtık hizmet dışı bırakma saldırısıdır. Bu saldırılar çevrimiçi bir hizmet ya da uygulamanın çalışmasını, bant genişliğinin tamamını kullanarak sistemin cevap vermesine engel olduğu siber saldırı çeşididir (“DDos El Kitabı” Bilgi Teknolojileri ve İletişim Kurumu-Telekomünikasyon İletişim Başkanlığı, 2014, s. 3).

Hizmet aksatma amaçlı bir zararlı yazılım çeşididir. Bir sisteme düzenli bir şekilde ardarda yapılan saldırılar sonucunda sistemi çalışamaz hale getirmek amacıyla hizmet

alınamaz hale getirilir. Bu saldırı türünde hedef sistemin kaynaklarının da tüketilmesi amaçlanmaktadır. DDoS saldırıları sonucunda önemli sunucular çalışamaz hale gelebilir ve bu da büyük sorunlar yaratmaktadır ("Denial of service (Dos) Saldırıları ve Korunma Yöntemleri", 2013).

Şekil 2.7

DDoS Saldırı Şekli



Şekil 2.7'de bahsedilen zombi bilgisayarın ne olduğuna bakacak olursak; kullanılan bilgisayar sahibinin bilgisi olmadan bilgisayarına kötücül bir yazılım bulaştırılarak uzaktan erişim ile kendisinin kullanım ve kontrol yetkisini veren ve bu sebeple tehlikeli olarak nitelendirilen bilgisayarlardır. Ele geçirilmiş olan bu bilgisayar köle bilgisayar ağındakilerden yalnızca biridir. Kötücül görevleri yapması için kullanılmaktadır. Bilgisayar sahibi bilgisayarının ele geçirildiğini bilmeksizin kullanmaya devam ettiği için bu bilgisayarlara köle bilgisayar yani zombi denilmiştir (Ünver et al., 2011, s. 24).

İlk başlarda sadece Dos, yani tek bir kaynaktan tek bir hedefe doğru yapılan bu saldırılar zamanla etkisinin daha da artırılması amacıyla birden fazla kaynaktan tek bir hedefe yapılmaya başlanmıştır. Böylece hem şiddeti hem de etkisi daha fazla olabilmektedir. Bu şekilde Dağıtık Hizmet Dışı Bırakma (DDoS) haline dönüşmüştür.

DDoS saldırılarının amacı, sistemlere kaldırabilecekleri yükten daha fazla anlık istekler ve anlık bağlantılar ile cevap verilemeyecek hale getirebilecek miktarda saldırılar göndermektir. Bu saldırılar vasıtasıyla sistem erişilemez hale getirilmektedir. Ayrıca hedef sistemlerdeki zafiyetler de sistemin erişilebilirliği bakımından risk oluşturmaktadır. İşletim sistemi, uygulama sunucusu veya web sunucusu gibi farklı bileşenlerdeki zafiyetler istismar edilerek sistemin işleyemeyeceği şekilde istekler gönderilir ve sistem erişilemez hale getirilir (Özkaya, 2020, s. 68).

DDoS saldırıları tam olarak bir hackleme faaliyeti olarak görülmeyip genel olarak bu saldırı çeşidinde hedef sistemler durdurularak bu sistemin maddi ve manevi olarak kayıp yaşaması sağlanmaktadır.

DDoS saldırılarına örnek olarak 2011 yılında Suriye'deki rejim yandaşları, hükümete eleştiri amacıyla yapılan yayınlara saldırmak için DDoS saldırı çeşidini kullanmışlardır. 2009 yıllında ise bir sosyal paylaşım sitesi olan Twitter'a DDoS saldırısı yapılarak saatlerce ulaşılmasına engel olunmuştur.

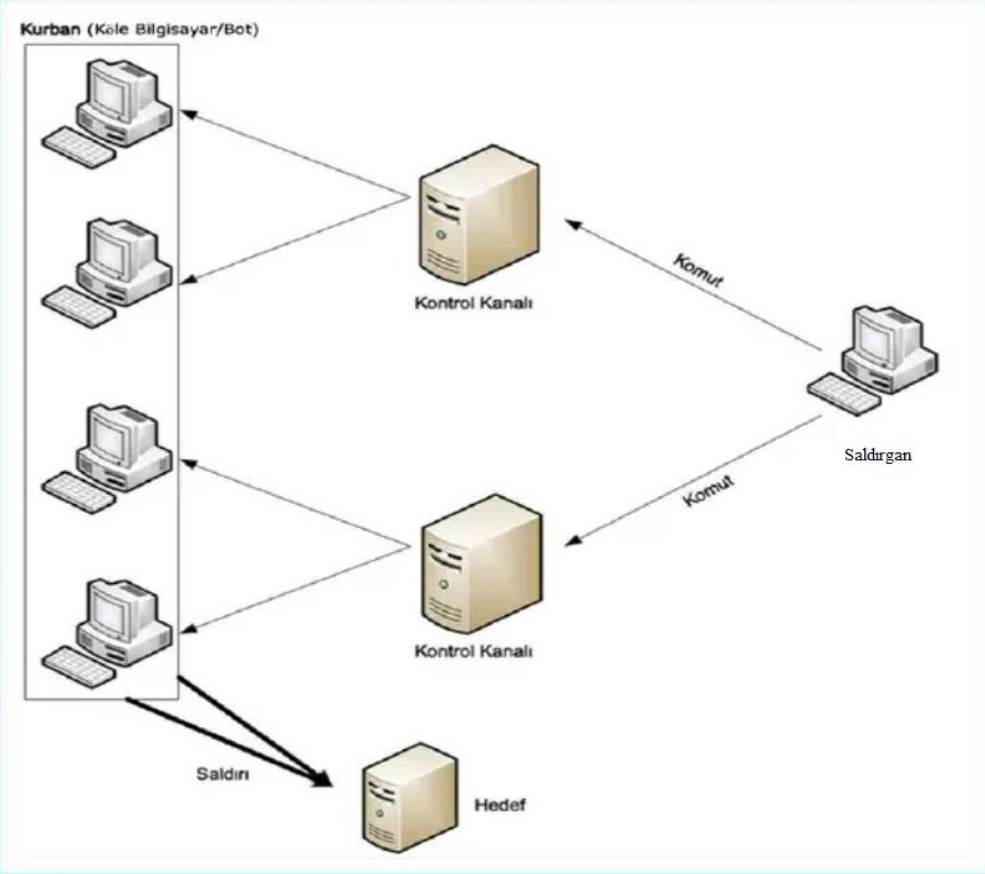
2.2.11. BOTNET (Bot Networks)

Botnet, istenen komutlara uyan ve tasarlandığı amaca uygun şekilde hareket eden anlamında "robot" kelimesinden ve "network" yani ağ anlamıyla birleşerek türetilmiştir. Saldırganlar truva atı veya herhangi bir farklı kötücül yazılım methoduyla kullanıcılara bunları bulaştırarak uzaktan yönetim sağlayabilecekleri bir bilgisayar ağı oluştururlar ve bu da botnet olarak tanımlanır (Özkaya, 2020, s. 69). Bot bilgisayar, köle ya da zombi bilgisayar olarak adlandırılan bilgisayarlardan oluşan bir ağdır.

Botnetler internet üzerinden yani çevrimiçi haldeyken en tehlikeli kötücül yazılımlardandır. İnternet ortamında gezinirken kullanıcıların zararlı e-posta eki veya güvenli olmayan bir linke tıklaması sonucunda kurbanlar Botnet ağlarına dahil olabilmektedirler. Bu kötücül yazılım internet sayfalarından bulaşabileceği gibi aynı zamanda truva atı denilen zararlı yazılım sayesinde de kullanıcılara bulaşabilmektedir.

Şekil 2.8

Köle Bilgisayarların Botnet Saldırısında Çalışma Yapısı Köle Bilgisayar ve Köle Bilgisayar Ağları, Ünver et al., 2011, s. 26



Botnet saldırısının nasıl düzenleneceğini özetleyecek olursak, bilgisayar korsanları saldırıda bulunabilme amacıyla uygulamalarda veya kullanıcı davranışlarında bir güvenlik açığı bulmaya çalışarken kullanıcıların da habersiz olmasını hedeflemektedirler. İnternetten indirme işlemleri, e-postalar, truva atları gibi yollarla web sitelerinin güvenlik sorunlarından yararlanabilmektedirler. Kullanıcıların bilgisayarlarına bulaşma işlemi tamamlandıktan sonra zombi bilgisayarlar oluşturulmaya başlanır. Bunlara bot bilgisayarlar denmektedir. Yeterince bot bilgisayara ulaşım sağlandığında saldırı hareketine geçilebilmektedir. Bot bilgisayarlar uzaktan yönetimle verdiği komutlar ile kötü niyetli faaliyetlerde bulunarak olabildiğince fazla sayıda cihaza bulaşmayı hedeflemektedir.

DDoS saldırı çeşidinde kullanılan Botnetler; spam mailleri, önemli kullanıcı verileri, şifreler gibi kritik verileri zombi bilgisayarlardan çalarak karşı taraflara gönderebilirler. Ek olarak genel işleyişi bozarak kalıcı hasarlara sebep olup sistemleri

kullanım dışı bırakarak önemli ölçüde ekonomik ve prestij kayıplarına sebep olabilirler (Leder et al., t.y.).

Saldırganlar genellikle güvenlik duvarı ve/veya kötücül yazılımlardan koruma programları bulunmayan bilgisayarları hedef almaktadırlar. Makine öğrenmeleri ve yapay zeka sayesinde bot ağlar siber saldırıları oldukça basit bir şekilde otomatik hale getirebilmekte ve hızlıca yayılabilmektedirler.

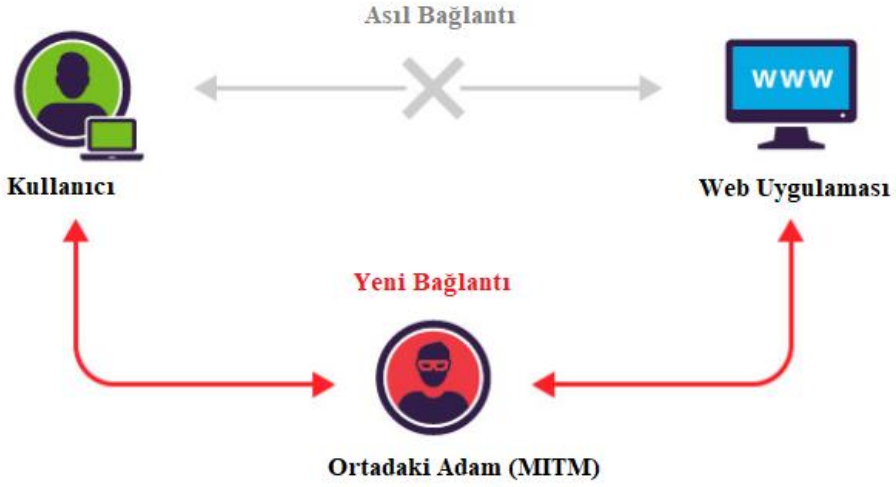
2.2.12. Ortadaki Adam (Man in the middle-MITM)

Ortadaki adam (MITM) saldırısında siber saldırganlar iki farklı cihaz arasında kurulan iletişimin paketlerini ele geçirir ve gizlice izler. Aynı zamanda bununla yetinmeyip bu verileri değiştirme işlemini de yapabilmektedir. Taraflar bu saldırının farkında değillerdir (Güner, 2021).

Bir ağ ortamında hedef ve sunucu, router, switch ve modem gibi ağ unsurları arasında geçen trafiği dinlemek veya değiştirmek amacıyla yapılan bir saldırı çeşididir (Ylli & Fejzajb, 2021). Bağlantı halindeyken saldırgan tarafından, isteği yapan kullanıcı ve yanıt veren kullanıcı arasına girerek istek yapmış olan kullanıcının isteğini yanıtlayıp iletişim kurulacak olan kullanıcı yerine de saldırgan kendisi istekte bulunur (Yüksel & Öztürk, 2017, s. 304).

Şekil 2.9

Ortadaki Adam Saldırısı Mitm - Man in the middle attack Nedir? Bizimyer, 2021



Kablosuz ağlarda en çok da broadcast (Bir mesajın ağdaki tüm cihazlara iletilmesini sağlayan protokol çeşididir.) olarak yayılan paketler siber saldırganlar tarafından oldukça basit bir şekilde yakalanabilmektedir. Bu yönden herkese açık ortamlarda ücretsiz Kablosuz Bağlantı Alanı (Wi-Fi) ağları ortaki adam saldırısı için fazlasıyla elverişli bir ortam sağlamaktadır. Halka açık alanlarda kurbanların ağ trafiği ele geçirilerek bir çok kişinin verilerine ulaşılabilmektedir (Bizimyer, 2021).

2.2.13. SQL Enjeksiyonu (SQL İnjection) Saldırısı

Yapılandırılmış sorgu dili (SQL), veritabanlarında kullanılan ve içindeki bilgileri yönetmek, işlemek, depolamak gibi işlemlerde ortak kullanılan standartlaşmış bir programlama dilidir. Veritabanlarında belirli temel sorgulama işlemlerinin yapılmasını ve tablolar oluşturulmasını sağlamaktadır (Bilen, 2021).

SQL enjeksiyonu saldırısı ise veritabanı içeren uygulamalarda arka tarafta veritabanı üzerinden müdahale etmektedir. Saldırgan veritabanının içeriğine saldırabilmektedir. Uygulama içinde bulunan güvenlik açıklığından yararlanılmaktadır.

Bu saldırı türünün veritabanına müdahale ederek etki gösterebileceği saldırılardan bazıları şu şekildedir.

- Veritabanı üzerinde yetkisiz erişim sağlamak amacıyla kimlik doğrulama işlemlerini atlatarak kullanıcıları ve hatta yöneticileri taklit ederek uygulamalar çalıştırılabilir.
- Veritabanı sorguları ile istenmeyen işlemler (yeni veriler ekleme, veri silme, bilgileri değiştirme) yapılabilir.
- Komutlar işletim sistemi seviyesinde çalıştırılabilir.
- Veritabanı üzerinde yeni ve yetkisiz kullanıcılar oluşturulabilir (Vural & Sağıroğlu, 2010, s. 76).

SQL injection saldırılarını önlemek için yapılabilecek bir takım öneri ve tedbire bakacak olursak;

- Veritabanındaki tablo isimleri kolay tahmin edilebilir seçilmemelidir.
- Web uygulamalarında kullanılan veritabanlarındaki temel özelliklerin (ekleme, silme vb.) sadece bir yönetici tarafından yönetilmesi sağlanmalıdır.
- Kullanılmayan yönetici hesapları kaldırılmalıdır.

- Sistem nesneleri erişimi için genel erişim verilmemeli ve bunlar kullanıcı bazlı olarak verilmelidir.
- Web uygulamaları ve veritabanı sunucularının güvenlik duvarı ile saldırılara karşı korunması gerekmektedir.
- Web uygulamalarındaki veritabanlarının giriş kontollerinde girdilerin uzunluğu kontrol edilmelidir.
- Kayıt satırlarına veri girişi yapılırken sayısal değerlerin formlar arası geçişte de sayısal olup olmadığına dikkat edilmelidir.
- SQL sunucusundaki hataların web formlarında görüntülenmesi engellenmelidir.
- Uygulama üzerinde web formundan sorgu yapmak yerine bu sorgular veri tabanı kısmında saklı yordam olarak yapılmalıdır (Demirol et al., 2013).

2.2.14. IP Sahteciliği (IP Spoofing)

İnternet ortamındaki her bilgisayarın bir IP numarası vardır. Bu numara her bilgisayarda benzersiz olmalıdır. IP adresi, internet üzerinden gönderilen verilerin formatını belirlemektedir.

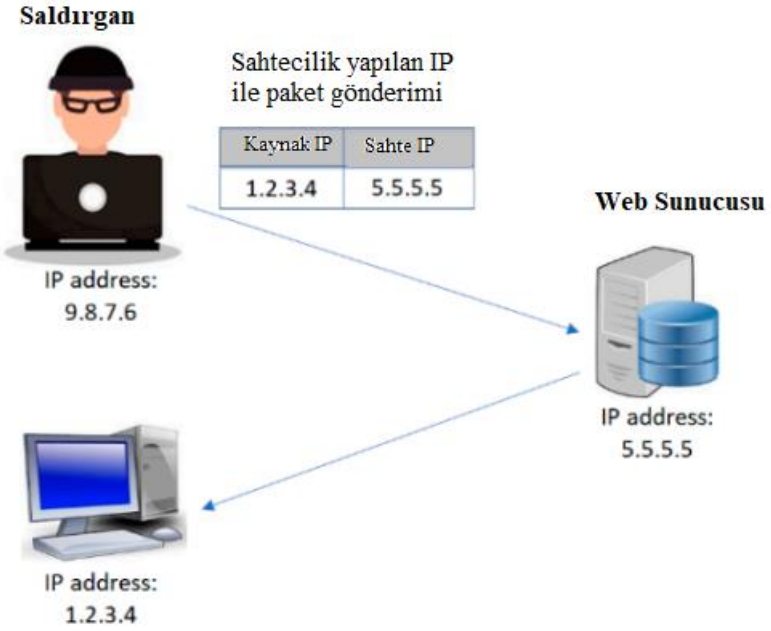
IP sahteciliği, internet ortamındaki IP adreslerinin değiştirilerek farklı şekilde gösterilmesidir. Bu sahtecilikteki amaç iletişim içerisindeki kullanıcıları kandırmaktır.

Sıklıkla karşılaşılan IP sahteciliği saldırısında, özellikle hizmet dışı bırakma (DDoS) saldırıları gibi saldırılarda takip edilmekten kurtulmak için, saldırıyı yapan kişinin IP adresini gizleyebilmesi için, IP adresi tabanlı kimlik doğrulama işlemlerini atlatmak ve güvenilir bir kullanıcı gibi görünmek için ya da ağ trafiğini dinlemek gibi amaçlar için kullanılmaktadır (Karadoğan, 2016).

Siber suçlular IP sahteciliği işlemi esnasında izlerini belli etmemek ve siber soruşturmalara yakalanmamak için Sanal Özel Ağ (VPN) veya Proxy sunucusu kullanmaktadır. Bu sunucular sayesinde IP adresleri bulundukları konumdan başka bir yerdeymiş gibi tamamen farklı bir hale dönüşerek iz belli etmemektedir.

Şekil 2.10

IP Sahteciliği Yapılan Paketin İletimi IP spoofing in and out of the public cloud: From policy to practice, Vlajic et al., 2019, s. 2



IP spoofing esnasında, siber saldırgan paket göndermeden önce kaynak IP adresini değiştirir. Böylece paket alındıktan sonra kaynak IP meşru olarak gözükür. Değiştirilen IP adresleri rastgele bir şekilde oluşturulabilir, otomatik olarak atanabilir ya da başka bir IP adresi kopyalanarak alınabilir (Işık, 2021).

2.2.15. Kimlik Bilgileri Doldurma Saldırıları (Credential Stuffing)

Kimlik bilgileri doldurma saldırısı, siber saldırganın veri sızıntıları sonucunda çalmış olduğu kullanıcı adı ve şifre bilgilerini otomatik olarak numaralandırarak başka bir platformda sistematik bir şekilde deneyerek kullanıcı hesaplarına erişmeye çalıştığı bir siber saldırıdır.

Bu yapıdaki bir saldırının yapılabilmesi için öncelikle kullanıcı adı ve parolaların yer aldığı bir veritabanının çalınması veya satın alınması yoluyla da veriler elde edilebilmektedir. Sonrasında elde edilen oturum açma bilgileri ile güvenlik açıklığı olan web sitelerine bağlanmaya çalışır ve bu kimlik bilgileri basit botnetler ile birlikte bağlanılan web

sitelerinde kullanıcı adı ve şifre kombinasyonlarının geçerliliği test edilerek saldırılar başlatılmaktadır ("Credential stuffing defense FortiGuard security service" t.y.).

Kurbanın bilgileri sızdırıldığında saldırganlar bu elde edilen kullanıcı bilgileri ve parolaları farklı platformlarda denemektedirler. Eğer kurban farklı platformalarda aynı şifreleri kullanırsa bir çok ortamda kolay bir şekilde başarılı bir credential stuffing saldırısı gerçekleştirilmiş olabilmektedir.

Kimlik bilgileri doldurma saldırısından korunabilmek için;

Kullanıcılar için:

- En etkili yollardan biri, kullanıcıların her hesapta farklı parolalar kullanması teşvik edilmelidir.
- Kimlik bilgileri saldırganlar tarafından elde edildiğinde parolalar hızlı bir şekilde değiştirilmelidir.
- https://haveibeenpwned.com/ sitesi üzerinden düzenli olarak e-posta hesaplarına bakılarak sızıntı var ise parolalar değiştirilmelidir.
- Kullanılmayan hesaplar eski parolalar ile şifrelenmiş olması sebebiyle daha kolay saldırıya uğrayabilmektedir. Bu sebeple kullanılmayan/eski hesaplar kaldırılmalı veya silinmelidir.
- Çok faktörlü doğrulama kullanılmalıdır. Böylece kullanıcı bilgilerinin yanında kod bilgisi de eklenerek giriş yapılmaktadır.

Kurum ve kuruluşlar için:

- Çok faktörlü doğrulama kullanılmalıdır.
- Hız sınırlaması kullanılarak önceden belirlenen bir eşikten daha yüksek olan hızları saptayarak otomatik botlar için örneğin saniyede 4-5 kez oturum açma girişiminde bulunan IP adreslerinin engellenmesi sağlanmalıdır.
- Bilinen botlar tarafından ele geçirilmiş olan kötü IP adresleri engellenmelidir.
- Günlük olarak web sitesi trafiğini kontrol ederek bilinen çalıntı kimlik bilgileri listesiyle oturum açma girişimleri kontrol edilerek eşleşen tüm istekler engellenmelidir.
- Oturum açma sayfalarında saldırganlara ipucu verecek geri bildirimlerden kaçınılmalıdır. Örneğin, parola hatalı ya da kullanıcı bilgisi hatalı yerine giriş başarısız uyarısı verilerek saldırganlara bilgi verilmesinin önüne geçilmelidir.
- Güçlü parola politikaları uygulanmalıdır (Sivri, 2021).

2.2.16. Siteler Arası Betik Çalıştırma (XSS Zafiyeti (Cross-Site Scripting))

Siteler Arası Betik Çalıştırma (XSS) saldırısı, siteler arasında komut dosyası çalıştırma saldırısıdır. Siber suçlulardan alınan girdilerin hiç bir denetimden geçirilmeden, kullanıcıların göreceği sayfanın kaynak kodunun içerisine yerleştirilmesi sonucunda kullanıcılar için betik çalıştırılması işlemidir (Özel & Eken, 2014). Basitçe bir saldırganın güvenilir bir uygulama ya da web sitesinin kodlarına kötü amaçlı yürütülebilir komut dosyaları enjekte ettiği bir saldırıdır da denilebilmektedir.

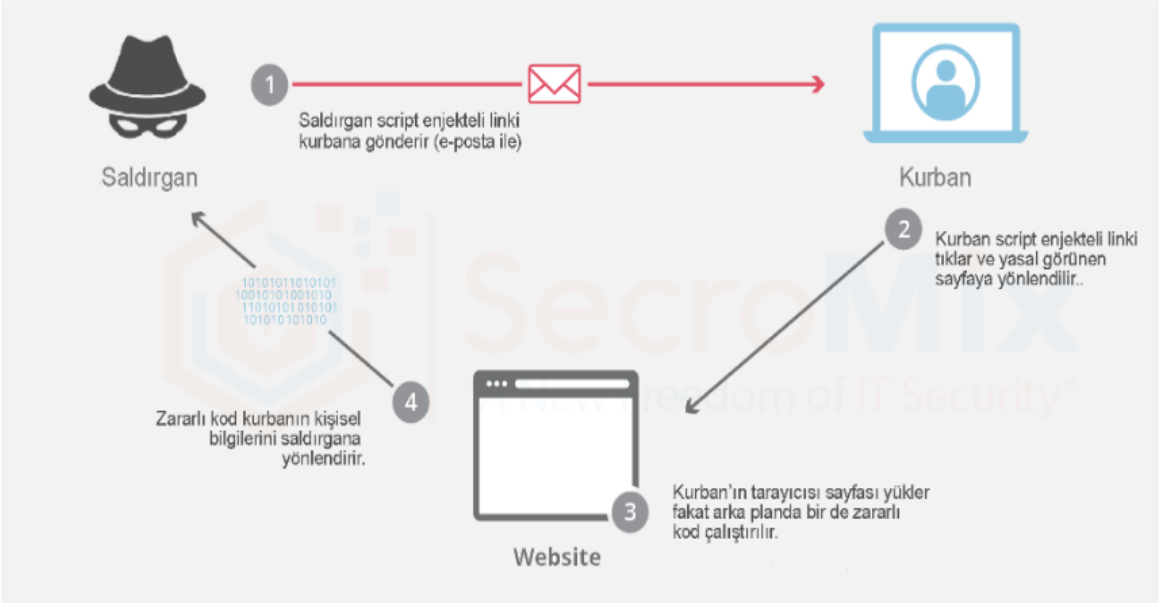
Kötü amaçlı komut dosyalarının, zararsız ve güvenilir ancak güvenlik açığı var olan web sitelerine enjekte edildiği bir enjeksiyondur. Saldırgan, bir kullanıcıya kötü amaçlı komut dosyası göndermek için XSS kullanabilmektedir (Kirsten, t.y.). Saldırı yapılan kullanıcı web sitelerinin geçerli komut dosyası ile gönderilen kötü amaçlı komut dosyası arasında ayrım yapamamaktadır. Bu durumdan yararlanan saldırganlar ciddi sorunlara yol açabilmektedirler.

Güvenlik açığı bulunan bir siteye enjekte edilen kod ciddi veri kayıplarına sebep olabilir, kurbanın bilgisayarına kötü amaçlı yazılımlar yükleyebilir. Ayrıca çerezler vasıtasıyla yetkili kullanıcı gibi davranarak bir çok yetkisiz eylemi gerçekleştirebilmektedir. Kurum ve kuruluşların itibarları zedelenebilmekle birlikte saldırgan web sitelerinin içerikleri ile oynayarak, bozarak imajlarına zarar verebilmektedir.

XSS kodları genellikle Javascript veya Hiper Metin İşaretleme Dili (HTML) dilinde yazılmaktadır. Ancak ActiveX, VBScript, ActiveX, Flash, Java gibi yazılım dilleri ve tarayıcılar tarafından da desteklenen diğer dillerde de yazılabilmektedirler (Vural, 2007).

Şekil 2.11

XSS Saldırısı Örneği XSS güvenlik açığı, t.y.



Siteler arası betik çalıştırma saldırısının olası sonuçları şu şekilde olabilmektedir.

- Kullanıcının klavyedeki tuş vuruşlarını yakalabilme yetisi,
- Kullanıcıyı kötü amaçlı bir web sitesine yönlendirebilmek,
- Web tarayıcısı tabanlı güvenlik açıklığından yararlanabilmek, (örneğin tarayıcıyı bozmak, çökertmek)
- Web sitesine giriş yapan kurbanın çerez bilgilerini ele geçirebilmek (kurbanın hesabını tehlikeye sokabilmek) ("What is cross site scripting (XSS) and how does it work?", 2022).

2.2.17. İstem Dışı Alınan E-posta Saldırıları (SPAM)

İnternet üzerinden bir çok kullanıcıya istekleri dışında gönderilen farklı içeriklerde mesajlar iletilmektedir. Bu mesajların genellikle reklam içerikli olmasıyla birlikte aynı içeriğin birden fazla kişiye kopyalanarak gönderilmesi de ortak özelliğidir. Kullanıcıların isteği dışında zorlayıcı bir nitelikte gönderilmektedir.

Bu istem dışı mesajları gönderen kişilere spammer denmektedir. Tarihteki İlk ciddi spam girişimi 1994'te kendi verdikleri hizmetleri anlatan iki avukatın Kullanıcı Ağı

(USENET)'ndaki 1000'lerce gruba reklam gönderilerini iletmeleri olayı kabul edilmektedir (Ünal & Şahin, 2017, s. 269).

Spam iletiler genellikle aşağıdaki özellikleri içermektedirler.

- İletiyi alan kullanıcı için anlamlı birşey ifade etmezler.
- Gönderilen iletinin içeriği yasadışı, yalan, yanıltıcı olur ya da bu şekilde bir sayfaya yönlendirirler.
- Alıcı olan kullanıcıya, bu mesajları almak istememesi durumunda bunu belirtebilecekleri geçerli bir adres sunulmaz.
- Elde edilmesi ve kullanılması kişilik haklarına tecavüz niteliğinde sayılan içeriklere sahip olurlar ya da bu yollarla toplanan bilgileri içerirler. Gönderilen spam örnekleri olarak ise genellikle bir ürünün reklamı, kolay yoldan para kazanılabileceği söylenen iletiler, sağlık ile ilgili acil olduğu belirtilen mesajlar, pornografik unsurlar vb. gibi içerikler sayılabilmektedir (Ünal & Şahin, 2017, s. 269).

Spamlar gerçek kişilerden gönderilebilir, fakat genellikle kötü amaçlı yazılım bulaşmış olan botnetler tarafından gönderilmektedir. Bu istenmeyen mesajlar düzenli olarak silinmez ve filtrelenmezse e-posta gelen kutularını tıkayabilir ("What is email spam and how to fight it?", 2021). E-posta okuyucuların önemsiz klasörleri konfigüre edilerek tanımlanmalıdır. Doğrudan tanıma veya öğrenme yeteneği ile daha önce belirtilen iletiler bundan sonra SPAM klasörüne düşecektir. Kullanılan anti-virüs programlarının spam tarama özellikleri aktif tutulmalıdır (Ünal & Şahin, 2017, s. 269).

2.2.18. Sosyal Mühendislik Saldırıları

Sosyal mühendislik saldırıları son zamanlarda en çok başvurulan siber saldırı türü örneğidir. Diğer siber saldırı türlerindeki bilgisayar sistemlerinin açıklarından faydalanmanın aksine teknoloji üzerinden ilerleyerek en zayıf halka olan insan faktörünü hedeflemektedir. Bu sebeple bu saldırı türünün sınırları yoktur. Kurbanlara psikolojik baskı uygulama yöntemiyle duygularını sömürerek her türlü bilgiye ulaşmaya çalışılmaktadır.

Saldırganlar her türlü bilgiyi elde etmek isterler ve bu amaç doğrultusunda saldırırlar. En fazla banka bilgileri, çeşitli uygulamalardaki kullanıcı bilgileri, bilgisayar şifreleri gibi verileri ele geçirmeye çalışmaktadırlar. Zayıf halka insandır ve bireylerden her türlü bilgiyi istifade etmeyi amaçlamaktadırlar.

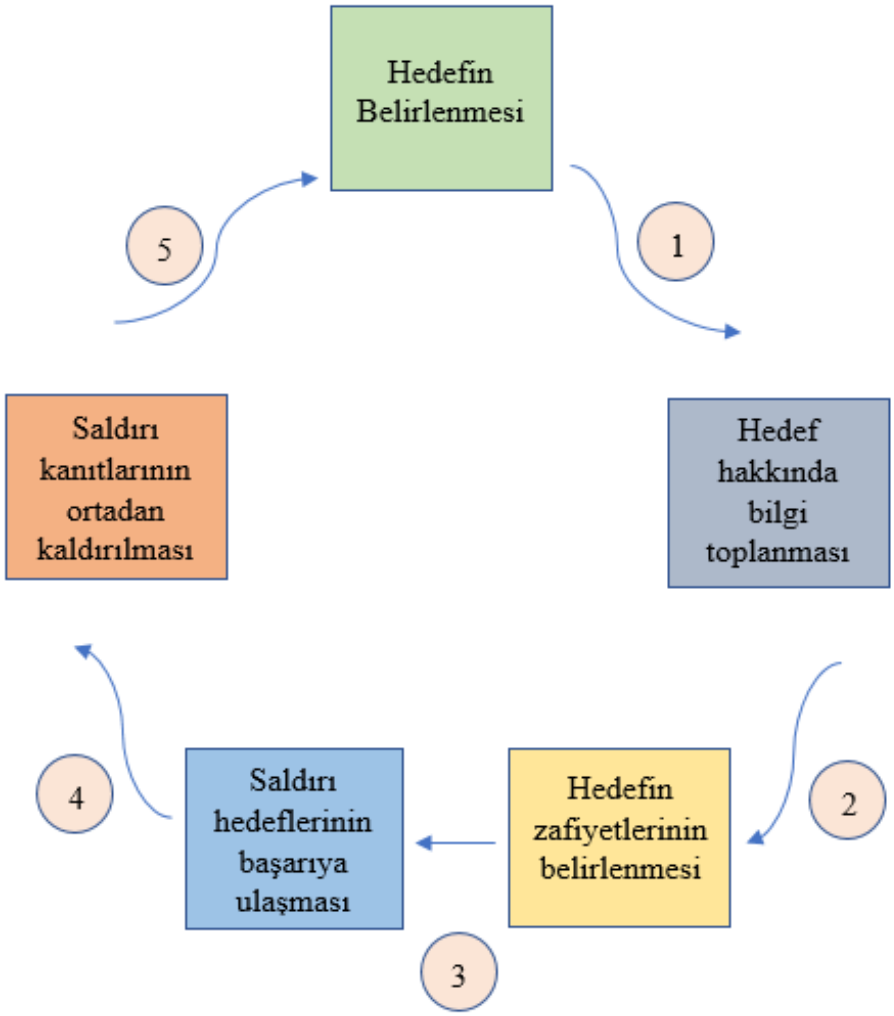
Saldırgan tarafından bilgisayarlara herhangi bir virüs, fidye yazılım vb. gibi kötücül yazılım işlemleri gerektirmediğinden kurbanın güvenini kazanmaya yönelik olması sebebiyle çok daha fazla tercih edilen bir saldırı çeşidi olmaktadır. Önemli olan kurbanların neye ve kime ne şekilde güveneceğini bilmesidir.

İnsanların zafiyetlerinden yararlanarak kurbanları ikna etme ve kandırma yöntemleriyle istedikleri bilgileri almaya çalışırlar. İnsanların karar verme duygularını değiştirmeye çalışmaktadırlar. Saldırganlar insanların duygularını sömürerek kolay yoldan para kazanmaya çalışırlar. Gelişmiş güvenlik önlemleri dahi kişileri bu saldırı yönteminden koruyamayabilir. İnsan faktörü, en iyi güvenlik yöntemlerinin bile atlatılarak kişinin duygusal haline göre farklılık göstermesiyle çok kolay bir şekilde zafiyete sebep olabilmektedir.

En gelişmiş sistemlerin başında dahi insan olması sebebiyle kolay yoldan insanların manipüle edilerek sistemlere sızmak saldırganlar için en etkili yol olabilmektedir. Çoğu bilginin artık dijital ortamda saklanması sebebi ile de özel verilerin güvenliğinin sağlanabilmesi insanoğlunun karşısına ciddi bir mesele olarak çıkmaktadır. Teknik anlamda üst düzey güvenlik önlemleri ile bu sistemlerin aşılması neredeyse mümkün olmasa da bu sistemlerin başındaki en büyük zafiyet olan insan faktörü unutulmamalıdır. Sosyal mühendislik de bu en zayıf halka olan insan faktörünün zafiyetini bilerek çeşitli yöntem ve teknikler kullanmaktadır (Gündüz & Daş, t.y.).

Şekil 2.12

Sosyal Mühendislik Döngüsünün Aşamaları



Şekil 2.12'de görüldüğü gibi sosyal mühendislik saldırıları 5 adımda tamamlanan bir döngü ile gerçekleşmektedir. Öncelikle hedef belirlenerek bu hedefe dair kritik bilgiler toplanmalıdır. Zafiyetler incelenerek belirlenmelidir. Bu zafiyetlere bağlı olarak saldırı işlemi gerçekleştirilmektedir. İşlemlerin başarılı bir şekilde sonlanabilmesi ve saldırganın kendisini ele vermemesi için saldırı kanıtlarının ortadan kaldırılması gerekmektedir.

Sosyal mühendislerin bazı belirgin özelliklerine bakacak olursak;

- Telefon ve internet gibi teknolojik yapıları iyi kullanırlar.
- Yardımsever görünerek güven oluşturmaya çalışırlar.
- Genellikle kılık kıyafetlerine önem vererek iyi bir intiba bırakmaya çalışırlar.
- Kurbanlarının güvenini kazanmaya çalışırlar.

- İkna kabiliyetleri yüksektir.
- Kurbanlarının korku, ahlaki değerler, suçluluk, açgözlülük gibi duygularının zayıf yanlarından yararlanmaya çalışırlar.
- Konuşma ve söz sanatlarında oldukça başarılıdırlar.
- Etkileyici, kibar ve nezaketli bir şekilde davranırlar.
- Yalan söyleme konularında çok iyilerdir ve bunu kurbanlarına belli etmeden ustalıkla yürütürler.
- Önceden hazırlanmış iyi bir plan çerçevesinde çalışırlar.
- Masum sorular arasına özel bilgileri edinmek için ustaca anahtar sorular ekleyebilirler.
- Acındırma, suçluluk hissettirme ve sindirme gibi psikolojik duyguları çokca kullanırlar.
- Bulundukları ortama farkettirmeden uyum sağlayabilirler.
- Sosyal mühendislerin teknik açıdan bilgili olmaları gerekmemektedir.
- Bir siber saldırgan az ya da çok sosyal mühendislik yeteneğine sahiptir (Gündüz & Daş, t.y.).

2.2.18.1. Sosyal Mühendislik Saldırılarında Kullanılan Yöntemler

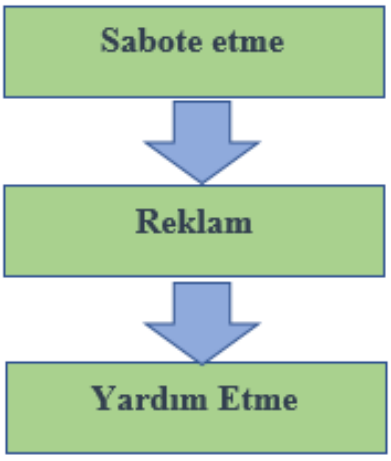
Bir sistemde şifreleme ve yazılım güvenlik önlemleri yeterli derecede alınmış olsa da bu sistemler tüm saldırılara karşı güvenlidir diyebilmek mümkün değildir çünkü en zayıf halka olan insan faktörü asla göz ardı edilmemelidir. Kişiler bilerek ya bilmeyerek saldırganlara erişim verebilir bu durumda hiç bir güvenlik duvarı, antivirüs yazılımı veya şifreleme cihazının bir etkisi kalmayacaktır (Whitaker, 2009). Saldırganın kullandığı silah insan zafiyetidir. Kurbanların saldırının ne şekilde ve nereden geleceğine dair bilgili olabilmesi oldukça önemlidir. Sosyal mühendislik saldırganları kurbanlarına karşı farklı farklı saldırı yöntemleri kullanmaktadırlar. Başlıca sosyal mühendislik saldırı türlerine bakacak olursak;

2.2.18.1.1. Tersine Sosyal Mühendislik (RSE-Reverse Social Engineering)

İlk adımda, bir sosyal mühendis hedef aldığı sisteme karşı teknik bir saldırı yaparak veya bir virüs, kötü amaçlı yazılım vb. bulaştırdığını bildiren bir e-posta yollayarak hedef sistemi sabote etmenin bir yolunu bulmaya çalışır. Kurbana sisteminin bozulmuş olduğu imajını verir. İkinci adım olan pazarlama adımı için sosyal mühendis belirli bir süre bekler ve sonrasında kendisini bir güvenlik danışmanı olarak gösterip kendi hizmetlerini tanıtır veya sistem saldırıları ile mücadele eden bir kurumdanmış gibi davranır. Bu şekilde kendi reklamını verme girişimlerinde bulunur. Kurban, reklam vb. oluşumları gördükten sonra saldırgan ile iletişime geçerek başvuruda bulunur. Bu aşama ise üçüncü adımdır ve sosyal mühendis, kurbana yardım ediyor gibi görünür. Siber korsan, bu adımda sistem içerisinde istediği gibi dolaşabilir. Böylece saldırgan sisteme girdikten sonra sorunu bildiği için yardım ediyor gibi gözüküp aslında gizli verileri çalma, klavye dinleyici yerleştirme ve kendisine yetkili bir oturum açma imkanı bulabilmektedir (Tosun, 2015).

Şekil 2.13

Tersine Sosyal Mühendislik Aşamaları



Kısaca tersine sosyal mühendislikte; sosyal mühendis, saldırganları hedef ağda bir sorun yaratarak bu saldırıda yardımcı olacak kişi gibi gözükmeye çalışır. Bu sorunu kısa sürede çözümleyerek güven kazanır ve yardım ediyor gibi gözükür. Hedef sistemde güvenilir kişi olarak yeni bir üye olarak tanımlanır. Böylece yeni bir teknik üretmesi gerekmeden kolayca sisteme dahil olur (Yalçın & Avşar, 2018, s. 78).

2.2.18.1.2. Sırtına Binme (Piggyback Rides) Tekniği

İngilizcede sırtına alarak ilerleme anlamına gelen piggyback rides, bir sosyal mühendisin resmi olarak bir çalışan gibi gözükerek bir binaya giriş yapabilmesi tekniğidir. O binada çalışan birini takip ederek bu tekniği uygulamaktadır. Sosyal mühendis o binada çalışanlarla bir şekilde arkadaş olarak ya da tanışarak bu tekniği uygulayabilir. Örneğin yangın merdiveninde sigara içen kurum çalışanları ile arkadaş olarak sigaraları bittikten sonra içeri giren kurum çalışanlarının kart okutması ile peşlerinden içeriye girebilirler ya da kurum girişinde elinde ağır bir kutu taşıyor gibi yaparak giriş yapan kişilerden kartına elindeki yük yüzünden ulaşamadığını söyleyerek kart bastırıp giriş yapabilir. Bu ve benzeri örneklerle çok basit bir şekilde fiziki güvenlik kontrollerini aşabilmektedirler. Kurum çalışanlarının zaafları üzerinden ilerlemektedirler. Giriş esnasında hiç bir alarm ya da anormal davranış olmaması sebebiyle bir uyarı işareti de söz konusu olmamaktadır (Yalçın & Avşar, 2018, s. 78).

2.2.18.1.3. Teknik konuşma (Technical Talk)

Bu saldırı çeşidinde sosyal mühendis, saldırmak istediği kurumdaki çalışanları teknik yardım personeli gibi davranarak aramaktadır. Kurum çalışanlarının anlamadığı bir çok teknik terim de kullanarak kullanıcılara istediği işlemi yaptırmayı hedeflemektedir. Bu işlemler parola güncellemesi olabileceği gibi kullanıcıların bilgisayarlarına istediği bir uygulamayı yükletmek de olabilmektedir. Genellikle kurum personellerinin teknik işlemleri çok anlamaması sebebiyle de sosyal mühendislerin işleri oldukça kolaylaşabilmektedir. Bu gibi durumlarda kurum çalışanlarının arayan kişinin bilgi teknolojileri merkezinde çalışıp çalışmadığını teyid etmesi önemli bir tedbir olabilmektedir. Uzaktan bağlantıya izin verdikten sonra bilgisayar başından kalkmayarak işlemleri incelemesi ve parolalarını üçüncü kişilerle paylaşmaması büyük oranda bu saldırıları önleyebilmektedir.

2.2.18.1.4. Balina Avı (Whaling)

Bu saldırı türünde hedef kişiler, pozisyon olarak önemli kişileri içermektedir. Genellikle yüksek pozisyonlu yönetici sınıflarını hedef almaktadırlar. Kritik ve önemli

bilgilere erişimi olan yöneticiler seçilmektedir. Bu yöneticilere kurumun web sitesindeki bilgilerden veya sosyal medyadaki paylaşımlarından bilgi edinerek saldırıda bulunulabilmektedir. Özellikle bu kişi sosyal medyada kendisiyle ilgili bilgileri fazlasıyla paylaşan biriyse sosyal mühendisin işleri daha da kolaylaşacaktır. Saldırgan edindiği bilgilerle bu kişilere ilgilerine göre mail yoluyla davet, etkinlik vb. linkler göndererek ödeme yapması esnasında kredi kartı bilgilerini veya başka türlü hassas bilgilerini edinebilmektedir. Olası balina avı saldırılarından korunabilmek için kritik bilgilere erişimi olan yöneticilerin eğitilmesi büyük oranda önem taşımaktadır. Kurum dışından gelen e-postaların işaretlenerek dikkat edilmesi de iyi bir yol olabilmektedir.

2.2.18.1.5. Sesle Oltalama (Vishing- Voice Phishing)

Vishing, sosyal mühendis tarafından bir kurbanın aranarak bu kişiden özel bilgilerini elde edebilmek için bilinçli olarak sosyal mühendislik taktiklerinin uygulanmasıyla yapılan bir telefon dolandırıcılığıdır.

Genellikle sosyal mühendisler önceden kaydedilen bir mesajı örneğin bankadan aradığını mağdur kişinin kredi kartları ile ilgili bir ihlal olduğunu veya kartının ödeme gününün son günü vb. olduğunu söyleyerek sesli mesajlar bırakabilmektedir. Mağdur kişi bu mesajları aldıktan sonra kendisine bırakılan numarayı arayarak kredi kartı numarasını, şifresini, kişisel bilgilerini ve sosyal mühendisliğin ihtiyaç duyabileceği bir çok bilgiyi verebilmektedir.

Bu şekildeki saldırılardan korunabilmek için;

- Banka çalışanları da dahil olamak üzere telefon üzerinden kimseyle kart ve kişisel bilgiler paylaşılmamalıdır.
- Kendilerini polis, jandarma, savcı vb. kişiler gibi tanıtan kişilere inanmayarak derhal iletişim kesilmeli ve yetkili birimlere şikayet edilmelidir (Yalçın & Avşar, 2018, s. 79-80).

2.2.18.1.6. Çöp Karıştırma

Çöp karıştırma tekniği ile hedeflenen kurum ve kuruluşların bilgilerinin, o kuruma ait çöplerin karıştırılarak elde edilmesi tekniğidir. Genellikle kurum dışında bulunan halka

açık çöpler tercih edilmektedir. Bu şekilde saldırganın yakalanma ihtimali neredeyse yoktur. Halka açık çöplerin karıştırılmasında herhangi bir yasal olmayan durum yoktur (Ahi, 2020).

Bu yöntem ile kurum ile ilgili olarak; alınan kısa notlar, çalışan bilgileri, alınan çıktılar, ihale bilgileri, projeler, planlar, kurum telefon rehberi, hassas bilgiler ve şifreler, cd ve diskler, kurum çalışma düzeni vb. gibi birçok hassas bilgi edinilebilir. Kurum, çöplerini mutlaka kendi sınırları içinde ve erişime kapalı olarak tutmayı ve çalışmayan donanımları atarken içindeki önemli bilgi ve programları sildikten sonra atmayı prensip edinmelidir. Çalışanlar ise çöpe attıkları bilgileri okunmayacak hale getirmelidir. Özel ve hassas verileri apaçık not almamalıdır.

2.2.18.1.7. Nöro-dilbilimsel Programlama (NLP)

Açılımı 'Neuro Linguistik Programming' olan NLP, insanların duygularını nasıl manipüle edileceğini bilen bir tekniktir. Aynı zamanda duygu, düşünce ve hareketlerin istenilen şekilde kontrol edilebilmesidir. Bu teknik ile kişilerin verdiği tepkileri ve davranışları değiştirmek mümkündür. Yine aynı şekilde beynin istemediği davranış, inanış ve düşünceler de değiştirilebilmektedir. Bu tekniğe beyni yeniden programlama da denilebilmektedir (Gençöz & Öncül, 2012, s. 194-216). Hadnagy'nin de 2010 yılında belirttiği gibi, iyi bir sosyal mühendis karşısındaki kişinin beynini nasıl manipüle edeceğini iyi bilmelidir. Bu teknik doğru uygulandığında kurbanı kolay bir şekilde manipüle ederek ele geçirebilmeyi mümkün kılabilmektedir (Gençöz & Öncül, 2012, s. 194-216).

Bu teknik ile sosyal mühendisler, karşılarındaki kişiler için vücut dillerini iyi kullanarak ve kullandıkları kelimeleri özenle seçerek hedefteki kişiye bilinçaltı mesajları vermektedir. Öncelikle saldırgan kişi beden dilini hedefteki kurban ile eşleştirerek işe başlamaktadır. Ayrıca nefes biçimini, ses miktarını, aksanını hedef kişiyle eşleştirmektedir. Böylece bilinçaltı seviyesinde bir ilişki kurmayı amaçlamaktadır. Sonrasında ise gülümseyerek sakince elini omzuna koymak gibi temas içeren hareketler sayesinde olumlu bilinçaltı mesajları vermeye çalışmaktadır. Sosyal mühendis ile kurban arasında bir uyum başlayarak etkileyici bilinçaltı mesajları verilmektedir. Bu aşamadan sonra sosyal mühendis, şirket bilgileri veya kritik özel bilgiler için peşinde olduğu şeyler için iletişime geçebilmektedir (Tosun, 2015).

2.2.18.1.8. Sosyal Medya

Günümüzde oldukça popüler olan ve gitgide her geçen gün daha da popülerleşen hemen hemen herkesin kullandığı internet ortamından yapılan iletişim ve paylaşımlardır (Yalçın & Avşar, 2018, s. 80). Sosyal medya Türkiye'de en çok Twitter, İnstagram, Youtube, Facebook, Tiktok gibi siteleri akla getirmektedir. Bu sitelerin dışında ise çeşitli blog sayfalar, sohbet siteleri, forumlar, sözlükler gibi internet sitelerini de kapsamaktadır diyebiliriz. Sosyal medya ağındaki bu çeşitlilik sayesinde hemen hemen herkesin kullandığı bir sosyal medya hesabı vardır diye düşünülebilmektedir.

Türkiye'de 2022 Ocak ayı verilerine göre 68.90 milyon sosyal medya kullanıcısı mevcuttur (Kemp, 2022). Her geçen gün kullanıcı sayısı ülkemizde ve dünyada hızlı bir şekilde artmaktadır. Bu da demek oluyor ki sosyal medya siber saldırıların gitgide daha fazla hedef noktası olma yolunda ilerliyor. Ayrıca sosyal medya kullanıcıları siber güvenlikteki en zayıf halka olan insanlar tarafından kullanılması sebebiyle de saldırganlar için kolay hedeflerden olduğu düşünülmektedir.

İnsanlar sosyal medya hesaplarında çalıştıkları yer, yaptıkları iş, eğitim durumu, medeni hali gibi bilgilerin de yanısıra neler yapmaktan hoşlandıklarına dair zevk, eğlence, hobi gibi bir çok kişisel bilgilerini paylaşırlar. Bu sebeple sosyal medya hesapları sosyal mühendisler için iyi bir bilgi kaynağı olmaktadır. Özellikle son zamanlarda güncel durum ve zaman güncellemeleri de yapılarak kişilerin nerede ne yaptıkları bile her an sosyal mühendisler tarafından takip edilerek kolaylıkla istedikleri şeyleri alma yolunda kullanılabilmektedir.

Saldırgan sosyal medya üzerinden edindiği bilgilerle kurban ile ilgili yaş, okul, ve eski işyerleri gibi bilgileri edinerek kendisini buradan biri gibi tanıtabilir, kişinin arkadaş listesine erişebilmesi durumunda ortak arkadaş vb. durumlarla ortaklık yakalamaya çalışabilir, mağdurun hobi veya etkinlik gibi verilerini alarak da ortak zevkleri varmış gibi yakınlık kurmaya çalışabilmektedir. Bu gibi ortaklıklar bulmaya çalışarak arkadaş olmayı deneyerek zaaflardan yararlanabilir ve kişilerin hesaplarını ele geçirmeye çalışabilir (Yalçın & Avşar, 2018, s. 80).

Farklı bir şekilde yine inandırıcılık yöntemine başvurarak İnstagram, Twitter, Facebook vb. gibi sosyal medya platformlarından kurbanlar seçilerek mesajlaşma yöntemiyle kandırılmaya çalışılmaktadır. Buradan arkadaşlıklar kurularak güven kazandıktan sonra bilgi edinmeye çalışma, gönderilen linkler sayesinde dolandırıcılık yapabilme gibi kurulan yakınlık durumuna göre saldırı ilerletilebilir. Yine aynı şekilde

sosyal medya üzerinden yardım kampanyaları gibi paylaşımlar yoluyla da insanları kandırarak paralarını almak oldukça popülerdir. Ayrıca sosyal medya kullanıcılarına ilgi çekici mesajlar göndererek gönderilen linklere girilmesi sonucu hesaplarını ele geçirme yöntemine de çok sık başvurulmaktadır. Örneğin kullanıcının tanımadığı bir kişi tarafından mesleği veya herhangi bir ilgisi ile alakalı bir platformda kurban ile ilgili kötü yorumlar yapıldığı ve ilgisini çekerse diye linkini bıraktığını söylediği bir mesaj ile kurbanların o linklere girdikten sonra kullanıcı bilgilerini isteyip bu bilgileri ele geçirmesi son zamanlarda çok fazla karşılaşılmış bir örnektir.

Son yıllarda popülerliği oldukça artan Tiktok uygulaması dahilinde ise kullanıcılar canlı yayınlar açarak izleyen kullanıcılar aracılığıyla bağış adı altında paralar kazanmaktadır. İzleyicilerin emoji göndererek canlı yayındaki kullanıcılara bağış yapması ile gerçekleşmektedir. Bu gibi canlı yayınlar aracılığıyla bir çok kurban bulunarak duygu sömürüleri ile gelir elde edilmektedir. Sosyal mühendisler kendilerini olduklarından farklı göstererek ya da tanıtarak para kazanma yolları bulmaktadırlar. Evlenme vaadleri ile kandırarak para kazanma, belli bir siyasi görüşü savunarak tartışma ortamında kullanıcılardan görüşlerine göre bağış isteme, çocuklara canlı yayınlar esnasında ebeveynlerinin bilgisi olmadan emoji gönderterek para kazanma gibi birçok çeşitli örnekleri mevcut olan kazanç yolları aramaktadırlar.

Bu gibi durumlar için dikkat edilmesi gereken belli başlı hususlara bakacak olursak;

- Hangi sosyal platform olursa olsun özellikle profil resmi olmayan hesaplara itibar edilmemelidir.
- Tanımadık ve bilinmeyen hesaplar üzerinden gelen arkadaşlık istekleri kabul edilmemelidir.
- Hesaplardaki kişisel bilgiler herkese açık şekilde olmamalıdır. Gizlilik ve güvenlik ayarlarının doğru şekilde yapıldığından emin olunmalıdır.
- Doğruluğu bilinmeyen, tanımadık hesaplardan gelen mail, link, paylaşım, oyun isteği, davetiye gibi gönderiler açılmamalı ve direkt silinmelidir.
- Kullanıcılar paylaşılan içerikler konusunda hassas olmalı ve herkese açık şekilde paylaşımda bulunmamalıdır. Ayrıca yapılan paylaşımlar için suç unsuru oluşturup oluşturmadığına dikkat edilerek paylaşım yapılmalıdır.
- Doğum tarihi, telefon numarası, doğum yeri gibi özel ve kişisel bilgiler asla paylaşılmamalıdır.

- Kullanıcı şifreleri ve parolalar konusunda dikkatli olunmalı ve kolay şifreler yerine güçlü farklı harfler, rakamlar ve işaretler içeren tahmini zor şifreler seçilmelidir.
- Sosyal ağlarda gezinirken kaynağı bilinmeyen, güvenilir olduğundan emin olunmayan bağlantılara tıklanılmamalıdır.
- Güncel bir antivirüs programı kullanılmalıdır.

2.3. Dünya ve Türkiyedeki Büyük Siber Saldırı Olayı Örnekleri

Ülkemizde ve dünyada yaşanmış olan siber saldırı olayları, toplumsal olarak ders çıkarılması ve gerekli tedbirlerin alınması açısından oldukça önemlidir. Türkiye ve dünyada yaşanmış olan siber saldırı olayları incelenecektir.

2.3.1. Türkiye'deki Siber Saldırı Örnekleri

Türkiye'de her geçen gün gerçekleştirilen siber saldırıların kişilere, kurumlara, özel sektöre ve kamu kurumlarına maddi ve manevi olarak zararları artmaktadır. Türkiye'de yer alan siber güvenlik şirketlerince gerçekleştirilmiş olan ortak bir çalışmaya göre siber saldırıların 2023 yılına kadar Türkiye'ye maliyetinin 8 ila 28 milyar dolar olacağı tahmin edilmektedir (Milliyet, 2016).

Türkiye'ye yapılan siber saldırılar incelendiğinde siber tehditlerin sürekli olarak arttığı gözlenebilmektedir. Aşağıda siber güvenlik farkındalığı yaratması ve ihtiyaçların farkedilmesi için ders çıkarılması amacıyla bazı siber saldırı örnekleri incelenmiştir.

2.3.1.1. Milli İstihbarat Teşkilatı (MİT) Çalışanlarının Kimlik Bilgilerinin İfşa Edilmesi (2001)

Aksiyon dergisinde yer alan habere göre 2001 yılında kamu bankalarının yazılım ihtiyaçları için kurulmuş olan Fintek şirketi üzerinden yapılan bir casusluk faaliyeti gerçekleştirilmiştir. Ziraat ve Halk Bankasında gizlenen veriler ve kamu bankalarına ait birçok bilgi de özel bir yazılımla ele geçirilmiştir. Yine iddiaya göre maaş ödemesi bu

bankalarca yapılan 5 bin MİT personelinin de bilgileri gizli bir servis tarafından ele geçirilerek açığı çıkartılmıştı (Yeni Şafak, 2007).

Ziraat Bankası, bu haberlerin gerçek olmadığı, MİT personelinin maaşlarının ve özlük bilgilerinin sistemlerinde yer almadığını belirtmesi söz konusu olmuştur. Haberler gerçek olmasa bile bu gibi tehditlerin var olması ihtimali tedbir almak için büyük bir sebeptir (Güven, 2022).

2.3.1.2. Batman Hidroelektrik Barajı'na yapılan Siber Saldırı (2003)

Batman Hidroelektrik Barajının işletim sistemini yapan Alman firması tarafından parasının verilmediği söylenerek şirket bilgisayarları kilitlenmiştir. Hidroelektrik santralinin çalışmaması üzerine Devlet Su İşleri (DSİ) yetkilileri elektrik üretilmediğini belirtmişlerdir. Şifreler, Türkiye Elektromanyetik Sanayi uzmanları tarafından çözülmeye çalışılmıştır. Bu siber saldırı neticesinde elektrik iletimi aksayarak Cizre, Şırnak ve Batman'ın bazı ilçelerine elektrik kesintili bir şekilde verilebilmiştir (Karabacak, 2011, s. 23).

Bu saldırıda görüldüğü gibi en tehlikeli türlerden biri olan içerideki kişiler tarafından saldırı yapılması, kritik yapıların işletiminde kullanılan sistemlerin milli yazılım olmasının önemini ortaya koymaktadır.

2.3.1.3. Bakü-Tiflis-Ceyhan Petrol Borusu Hattına Siber Sabotaj (2008)

Bakü-Tiflis-Ceyhan Petrol Boru Hattında meydana gelen patlamanın siber saldırı olduğu iddia edilmektedir. Dünyanın en güvenli hatlarından biri olduğu söylenen bu hat, sensörlerle görüntülenerek ve birçok önemli verisinin kablosuz erişim ile yapıldığı ve de uzaktan erişim için uydu sistemi kullanılarak inşa edildiği bilinmektedir (Altınsoy & Çobanoğlu, 2020).

Günde yaklaşık olarak 1 milyon varil ham petrolü Hazar Denizi'nden Türkiye'ye taşıyan 1768 kilometrelik Bakü-Tiflis-Ceyhan petrol borusu hattında Erzincan'ın Refahiye ilçesine yakın bir noktasında patlama meydana gelmiştir. İlk başlarda bunun sebebi teknik arıza gibi etkenlere dayandırılsa da aslında bu patlamanın bir siber saldırı olduğu daha sonra anlaşılmıştır (Seren, 2016, s. 21).

Jordan Robertson ve Michael Riley tarafından isimleri belirtilmeyen dört farklı istihbarat kaynağından alınan bilgilerle hazırlanmış bir makaleye göre; bu patlamanın nedeninin aslında hackerlar tarafından hazırlanan bir siber saldırı olduğu öne sürülmüştür. Saldırı silahı olarak ise klavye kullanıldığı belirtilmiştir (Lathrop & Stanisz, t.y., s. 291-309).

Saldırı, boru hattını işleten ağdaki siber açıklıklar kullanılarak ve boru hattının kontrol merkezine sızılarak yapılmıştır. İstihbarat yetkililerince; saldırganlar, boru hattındaki kamera yazılımlarındaki açıklıkları kullanarak işletme ağlarına sızmışlardır. Sızma işlemini gerçekleştirdikten sonra network üzerinden yanlış alarmlar gönderilmesi sağlanarak sistemi kontrol dışı bir hale getirmişlerdir. Böylece kendileri sistem kontrolünü alarak boru hattının petrol basıncının takibini ve bildirimlerini ileten alarm sensörünü devre dışı bırakarak kapatmışlardır. Saldırganlar boru hattına normalin üstünde petrol pompalanmasını sağlamakla basıncı artırmış ve patlamasına neden olmuşlardır (Ring, 2015).

Planlı bir şekilde hazırlanmış olan bu saldırının Türkiye'nin jeopolitik ve siber güvenlik alanlarında birçok sonuç çıkarması gereken yönleri vardır. Türkiye malesef bu saldırıya hazırlıksız bir durumda yakalanmıştır. Türkiye'nin kritik altyapıları arasında olan petrol ve doğalgaz hatlarının saldırılara açık bir halde olduğu ve uygun şekilde korunması gerektiği gözlemlenmiştir.

2.3.1.4. Atatürk ve Sabiha Gökçen Havalimanlarına Yapılan Siber Saldırılar (2009 ve 2013)

Atatürk Havalimanı Dış Hatlar Terminali 30 Ocak 2009 tarihinde siber saldırıya uğramıştır. Terminalde kullanılan harici bellekler vasıtasıyla yayıldığı tespit edilen Confickr isimli bilgisayar solucanı Windows işletim sisteminin açıklarından yararlanarak sistemlere bulaşmıştır. Sistem virüsten etkilenince işlemler manuel şekilde yapılınca çok sayıda yolcu mağdur edilerek zaman kaybına yol açmıştır ve bazı yolcularınsa bagajları havalimanında kalmıştır ("Atatürk Havalimanında Virüs Kabusu," 2009).

Benzer şekilde 26 Temmuz 2013 tarihinde ise yine Atatürk ve Sabiha Gökçen havalimanlarında kullanılan Polis Bilişim Sistemi (Polnet) bilgi sisteminin siber saldırıya uğraması sonucu pasaport kontrolleri imkansız bir hale gelerek insanların saatlerce beklemesine yol açmıştır ("Virus attack strikes at both Istanbul airports", 2013).

2.3.1.5. 10 Gün Süren Siber Saldırı (2015)

Türkiye'de 14 Aralık 2015 tarihinde başlayan yaklaşık 10 gün süren .tr uzantılı internet sitelerinin sunucularını hedef alan saldırılar sebebiyle birçok kurum ve kuruluşun internet adreslerine ve mobil uygulamalarına erişim sağlanamamıştır (Kolcu, 2015). Bu toplu saldırı dönemin Orta Doğu Teknik Üniversitesi (ODTÜ) Rektörü Ahmet Acar tarafından; "uluslararası literatüre geçecek düzeyde, dünya üzerinde yaşanmış en yoğun saldırılardan birisinin gerçekleştiğini"; yurt içinde ve dışında 5 ayrı noktada konuşlanan 6 adet ".tr" alan adı sunucusuna DDoS saldırılarının düzenlendiğini açıklamıştır (Seren, 2016, s. 22).

Saldırının doğurduğu sonuçlar arasında noterler çalışamamış, alım satım işlemleri durmuş, bankalar işlem yapamamıştır. Bankalar bu tehdite karşı koruma amaçlı dışarıya karşı erişimlerini kapatmışlar ve böylece birçok sistem devredışı kalmıştır (Güven, 2022).

2.3.1.6. Sağlık Bakanlığına Ait 33 Devlet Hastanelesine Yapılan Siber Saldırı (2016)

18 Mayıs 2016 günü sabahı Türkiye'deki devlet hastanelerinin veri tabanlarındaki bilgiler siber saldırı ile kopyalanarak silinmiştir (Şenol, 2016, s. 13). 19 Mayıs tarihinde ise ele geçirilen bu bilgiler siber uzayda yayınlanmıştır. Sağlık Bakanlığı sistemde daha önce yedeklenmiş olan veriler sayesinde veri kayıpları bir nebze de olsa aza indirgenmiştir. Bu saldırı sonucu sağlık hizmetleri ciddi anlamda sekteye uğrayarak durma noktasına gelmiştir. Kamuda kayıplara sebep olmasının yanısıra toplum tarafından da huzursuzluklara yol açmıştır (Güven, 2022).

2.3.2. Dünya Çapinda Gerçekleşen Siber Saldırı Örnekleri

Tüm dünyada her geçen gün giderek artan sayıda siber saldırılar gerçekleştirilmektedir. Ülkeler birbirleriyle savaşabilmek için dahi yeni dünyada siber saldırı yöntemlerini kullanmaktadır. Uluslararası düzeyde büyük sonuçlar doğurabilmektedir. Şekil 2.14'te da görüldüğü üzere her an dünya üzerinde saldırılar gerçekleşmektedir. Ses getiren bazı siber saldırıları inceleyelim.

Şekil 2.14

Dünya Üzerindeki Anlık Siber Saldırı Haritası



2.3.2.1. Estonya Siber Saldırısı (2007)

Estonya'daki bronz bir asker heykelinden oluşan savaş anıtının kaldırılmasını isteyen Rusya ile tartışması üzerine Estonya, siber saldırganlar tarafından ulusal bilgi sistemleri, bankacılık işlemlerine yönelik saldırılar, spamlar ve devlete ait internet sitelerine yapılan saldırılar ile karşı karşıya kalmıştır. Estonya'nın birçok servis ve sistemleri günlerce çalışmamıştır. Bu olay siber saldırıların ülkeler arası çatışmalar amacıyla da kullanıldığının ve devletler arası rekabet yarattığının farkedilmesi için bir kırılma noktası olmuştur. Bu olay sonrasında Estonya, Avrupa birliği içerisinde siber güvenlik stratejilerine önem veren ve geliştirmek isteyen ilk ülke olmuştur (Sertçelik, 2015, s. 35).

2.3.2.2. Gürcistan Bilgisayar Ağına Saldırı (2008)

Rusya ile Gürcistan arasında 2008 yıllarındaki anlaşmazlık sebebiyle yabancı korsan siber saldırganlar tarafından Gürcistan'ın bilgisayar ağlarına sızılmıştır. Rusya

geleneksel savaşın yanında siber saldırı da başlatmıştır. Gürcistan'ın resmi web sitelerine graffiti resmi koymuştur. Rusya'nın siber saldırganları, Gürcistan'ın internet trafiğini denetleyen sunucuları ele geçirmiştir. Maddi bir zararı olmayan bu saldırı, Gürcistan devleti üzerinde psikolojik ve politik olarak baskı kurmuştur. Bu savaş gerçek bir hibrit savaş niteliğindedir (Bıçakcı, 2012, s. 205-226).

2.3.2.3. İran Nükleer Sistemine Saldırı-Stuxnet Virüsü (2010)

İran'ın nükleer yakıt zenginleştirme tesislerinin Stuxnet adı verilen kompleks bir bilgisayar virüsü ile saldırıya uğramasıdır. Bu virüsün amacı işleyişteki kontrolü ele geçirerek makineleri yavaşlatmaktı. Ayrıca sistemin anormal bir durum olduğuna dair geri bildirim yapmasını da engelleyerek bu süreci saklayabilmiştir. Bu sebeple de verilen zarar uzun bir süre sonra, haziran 2010'da farkedilmiştir (Bıçakcı, 2012, s. 218).

Altyapı tesislerinin sistemlerini hedef alan ilk kötücül yazılım virüsü olan Stuxnet, baraj, sanayi birimleri, su elektrik kanalizasyon sistemleri ve enerji santrallerini içeren 30 bin sanayi bilgisayar sistemini etkilemiştir. Stuxnet saldırısının tesislerdeki net zararını hesaplamak mevcut teknik aksaklıklar sebebiyle mümkün olmasa da tesisteki 1000 adet santirifüjden 600ünün zarar görerek değiştirildiği bilinmektedir (Çelik, 2013, s. 148).

2.3.2.4. Sony Playstation Siber Saldırısı (2011)

2011 yılında Sony şirketine ait Playstation ağı hacklendi ve bu saldırı sonucu 77 milyon kullanıcıya ait kişisel bilgiler çalındı. Dağıtık hizmet durdurma (DDOS) saldırısıyla yapılmış olan bu saldırı ile kullanıcalara ait kredi kartı verileri ele geçirilmiştir. Playstation konsollarına 23 gün boyunca erişim engellenmiştir (Aydın & Yükçü, 2020, s. 2523). Sony markası yaşanan bu durum üzerine tüm kullanıcılarından özür dilemiştir. Kullanıcıların mağduriyetinin yanında Sony şirketi büyük prestij kaybı yaşamıştır.

2.3.2.5. Yahoo Siber Saldırısı (2014)

Dünyanın en popüler arama motorlarından ve mail hizmeti veren bir internet şirketi olan Yahoo'nun, 3 milyar kullanıcısının hesapları siber saldırganlar tarafından ele

geçirilmişti. İlk başlarda Yahoo bu sayının çok daha az olduğunu söylese de ilerleyen yıllarda tüm kullanıcıların yani 3 milyar hesabın bu saldırıdan etkilendiği ortaya çıkmıştır. Kullanıcılarının kişisel bilgileri saldırganlar tarafından sızdırılmıştır. Çok büyük prestij kaybına uğrayan şirket daha sonra başka bir şirkete satılmış ve ismini değiştirmiştir (Yıldırım, 2018).

2.3.2.6. Rusya-Ukrayna Savaşı Saldırıları (2022)

24 Şubat 2022 tarihinde başlamış olan Rusya-Ukrayna savaşına bağlı olarak, iki devlet arasında siber saldırılar da düzenlenmeye başlamıştır. Daha çok Rus Devleti tarafından askeri harekatla uyum içerisinde devam eden siber saldırılar gerçekleştirilmiştir. Rusya tarafından destekli en az altı ayrı siber korsan grubu tarafından mart 2021'den itibaren Ukrayna'daki birçok kuruluşun sistemlerindeki dosyaları kalıcı olarak yok eden saldırılar yapılmıştır. Bu saldırıların yüzden 40'ından fazlası kritik sektörlere ait altyapılara karşı, yüzde 32'sinin ise doğrudan Ukrayna devlet kuruluşlarına gerçekleştirildiği görülmüştür (TRT Haber, "Microsoft, Rusya'nın Ukrayna'ya siber saldırılarını ortaya çıkardı", 2022). Günümüzde yaşanan yakın tarihli bu örnekle de görüldüğü gibi siber tehditlerin önemi savaş ortamında dahi ciddiyetini korumaktadır.

BÖLÜM 3

ÜLKEMİZDE SİBER GÜVENLİK ALANINDAKİ ÇALIŞMALAR VE ALINABİLECEK ÖNLEMLER

Türkiye de tüm dünyada olduğu gibi yaşamın neredeyse her alanında gerçekleşen dijital ortama dönüşüme uyum sağlayarak teknolojik gelişmelere ayak uydurmuştur. Ülkemizde gerçekleştirilen çoğu işlem dijital ortama aktarılarak yapılmaktadır. Bu durumun doğal sonucu olarak ise kritik belgelerin; sistemlerde ve internet ortamında ya da kişisel bilgisayarlarda korunması gerekmektedir. Ülkemizde bu anlamda ulusal ve uluslararası kapsamda siber güvenliğin sağlanabilmesi amacıyla çeşitli organizasyonlar, kurum ve kuruluşlar çalışmalar gerçekleştirmektedir.

3.1. Türkiye'nin Siber Güvenlik Çalışmaları

Siber güvenlik gitgide tüm dünyada ülkelerin kalkınması için önemli bir unsur olmaya artarak devam etmektedir. Ülkemizde her alanda sürekli olarak gelişen ve karmaşıklaşan yapılar sebebiyle ulusal siber ortam güvenliği oldukça önemlidir. Türkiye'nin ekonomik gelişim sürecinde de payı büyüktür. Ekonomik ve toplumsal alanda büyük değişimlerin olduğu ve teknolojik gelişmelerin de hızlandığı, pandemi sürecinde değişen koşullar sebebiyle gereksinimlerin de artmasıyla siber güvenlik farkındalığı daha fazla artmıştır.

Türkiye'ye karşı ülke içinden ve dışından yapılan saldırıların artması, kurumların hizmetlerinin sekteye uğraması, insanların mağduriyet yaşaması gibi etmenler sebebiyle karşı karşıya kalınan bu olumsuz durumlar karşısında zorunlu olarak siber güvenlik farkındalığı oluşmuştur. Ülkelere yapılan saldırılar, o ülkenin bireysel, kurumsal, ulusal ve hatta küresel çapta ekonomik, siyasi, sosyal gibi birçok alanda uluslararası düzeyde yetersizlik, imaj zedelenmesi gibi sorunlara yol açmaktadır. Söz konusu bu saldırıların karşılığında hem kamu hem de özel sektör alanında tedbirlerin alınması ve gerekli girişimlerin başlatılması zorunlu hale gelmiştir.

Siber saldırılar, bireyleri, kurumları ve ülkeleri hedef alarak dolandırıcılık, kişisel bilgilerin ele geçirilmesi, mali bilgilerin hırsızlığı gibi temelde ekonomik sebeplerle

yapılmasına rağmen son yıllarda devlet destekli organizasyonlara gerçekleştirilmesiyle, devletlerin kritik altyapılarını hedef aldığı gözlemlenmektedir. Bu çerçevede siber güvenlik konusu ülkelerin öncelikli olarak ele alması gerektiği savunma ihtiyaçlarının başında yer almaya başlamıştır (Ünver, t.y.).

Ülkemiz siber saldırılarılarla başa çıkma tedbirlerinin gerekliliğinin günden güne artmasıyla ulusal siber güvenliğin sağlanması amacıyla adımlar atmıştır. Türkiye Global Siber Güvenlik Endeksi Rapor'una göre, siber güvenlik alanında Avrupa'da 6'ncı. Dünyada ise 11'inci sırada yer almaktadır ("Türkiye, Global Siber Güvenlik Endeksi'nde Avrupa'da 6'ncı", 2021).

Ülkedeki kurum ve kuruluşların siber güvenliğinin sağlanabilmesi sadece kurum bünyesinde değil ulusal olarak da gerçekleştirilmesi gereken ayrılamaz bir bütün halindedir. Bu bölümde bu amaçla oluşturulmuş ve bu alanda çalışmalar yapmakta olan kuruluşlar incelenecektir.

3.1.1. Siber Güvenlik Kurulu

Siber Güvenlik Kurulu, Bakanlar Kurulunca, 11 Haziran 2022 tarihinde 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, 20/10/2012 tarihli ve 28447 sayılı Resmi Gazetede yayımlanarak yürürlüğe girmiştir. Bu karar ile Siber Güvenlik Kurulu oluşturularak Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na[1] siber güvenlik alanında görev ve yetkiler verilmiş, siber güvenlik ile ilgili çalışma grupları ve geçici kurulların oluşturulabileceği karara bağlanmıştır (BTK, "Siber Güvenlik Kurulu", 2017).

Siber Güvenlik Kurulu'nun amacı,

- Kurum ve kuruluşlar ile gerçek ve tüzel kişiler bakımından alınacak önlemlerin belirlenmesi, alınacak önlem, plan, program, rapor, usul, esas ve standartların onayı, uygulaması ve koordinasyonunun sağlanması,
- Kamu kurum ve kuruluşlarına ait gizli bilgilerin güvence altına alınması hususundaki usul ve esasları hazırlamak,

[1] Anayasada Yapılan Değişikliklere Uyum Sağlanması Amacıyla Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında 9 Temmuz 2018 tarihli Resmi Gazete'de yayımlanan 703 No'lu Kanun Hükmünde Kararname ile Ulaştırma Denizcilik ve Haberleşme Bakanlığı "Ulaştırma ve Altyapı Bakanlığı" adını almıştır. Bu tez çalışmasında bu tarihten öncesi için "Ulaştırma Denizcilik ve Haberleşme Bakanlığı", sonrası için ise "Ulaştırma ve Altyapı Bakanlığı" ifadesi kullanılmıştır.

- Ulusal siber güvenliğin korunması amacıyla kamu kurum ve kuruluşlarındaki teknik altyapıları takip etmek ve uygulamalarının doğruluğu ile test edilebilmesini sağlamak,
- Ulusal bilgi teknolojilerinin altyapıları, sistem ve veritabanlarının güvenliğini sağlama, kritik altyapıları belirleyerek bunların siber saldırı önleme ve müdahale sistemlerini oluşturma, gerekli merkezlerin kurularak gerekli yapıların güçlendirilmesine yönelik çalışmalar yapmak,
- Ulusal siber güvenliğin sağlanması amacıyla milli çözüm ve siber saldırılara müdahale sistemlerinin gelişimi ve üretimini desteklemek, teşvikte bulunmak ve kullanılmasını sağlamak,
- Ulusal siber güvenlik açısından kritik kurum ve kuruluşlar için gerekli personelin temini, eğitim ve gelişimini planlamak ve yürütmek,
- Diğer ülke ve uluslararası kuruluşlar ile işbirliği sağlamak,
- Ulusal siber güvenlik konusunda bilinçlendirme, farkındalık ve eğitimleri artırmaya yönelik çalışmalar yürütmek,

olarak belirlenmiştir ve yukarıdaki gibi görevleri bulunmaktadır (Bıçakcı et al., t.y., s. 38-39).

Siber Güvenlik Kurulu Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nın başkanlığında,

- Dışişleri Bakanlığı Müsteşarı,
- İçişleri Bakanlığı Müsteşarı,
- Milli Savunma Bakanlığı Müsteşarı,
- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Müsteşarı,
- Kamu Düzeni ve Güvenliği Müsteşarı,
- Milli İstihbarat Teşkilatı Müsteşarı,
- Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı,
- Bilgi Teknolojileri ve İletişim Kurumu Başkanı,
- Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Başkanı,
- Mali Suçları Araştırma Kurulu Başkanı,
- Telekomünikasyon İletişim Başkanı

ile Ulaştırma, Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşmaktadır (BTK, "Siber Güvenlik Kurulu", 2017).

Siber Güvenlik Kurulu görev ve yetkileri 2018 yılı itibariyle Cumhurbaşkanına devredilmiştir.

3.1.2. Ulusal Siber Olaylara Müdahale Merkezi (USOM)

Ulusal Siber Güvenlik Stratejisi 20 Haziran 2013 tarihinde Bakanlar Kurulu Kararı ile yayınlanan 2013-2014 Eylem Planı'nın "Ulusal Siber Olaylara Müdahale Merkezinin (USOM) Kurulması ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) Oluşturulması" başlıklı 4. eylem maddesi uyarınca, Telekomünikasyon İletişim Başkanlığı (TİB) bünyesinde USOM kurulmuştur (BTK, "USOM ve Kurumsal Siber Olaylara Müdahale Ekibi", 2017).

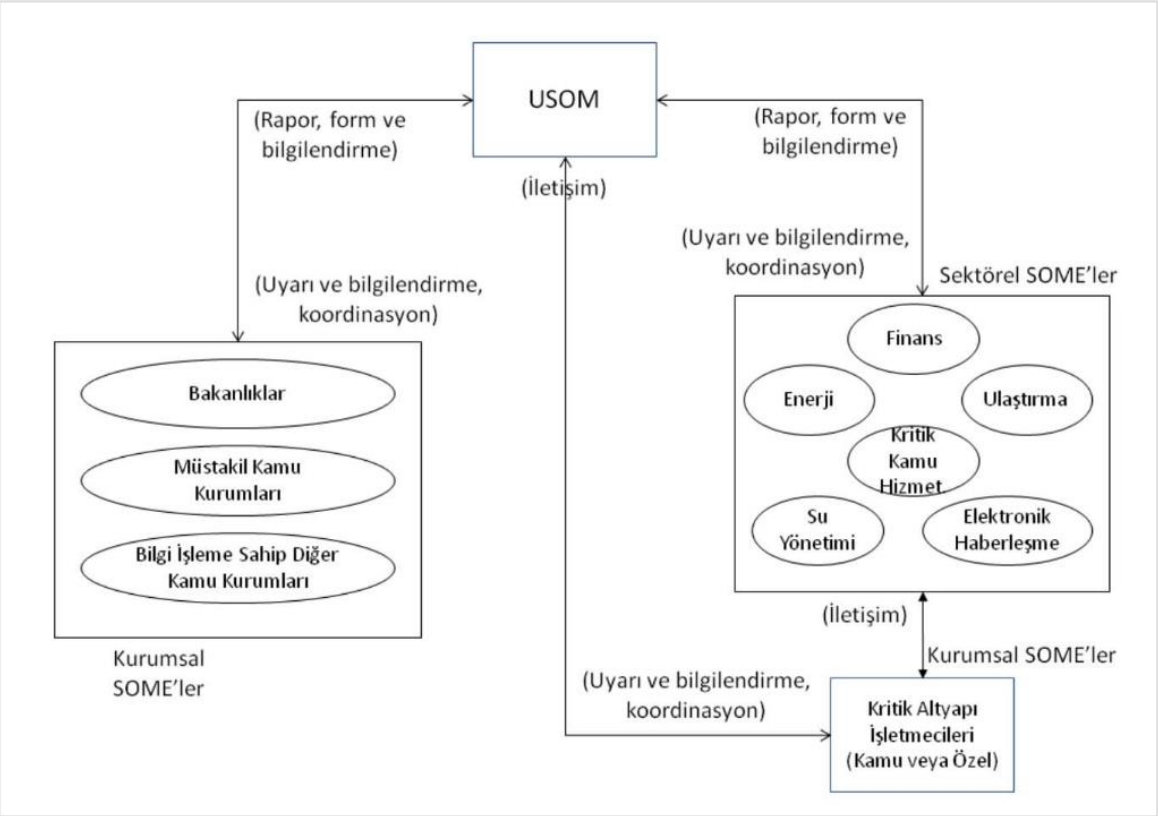
USOM, Türkiye'deki müdahalede ulusal ve uluslararası yapılan tüm işlemlerin koordinasyonu amacıyla kurulmuştur. Tespit edilen siber tehditler konusunda gerekli taraflara ve ülke genelinde alarm, uyarı gibi durumları bildirerek yaşanabilecek olumsuz durumlara karşı önceden uyarıda bulunarak bu gibi durumları önlemeye çalışmaktadır. Siber tehditlere açık olan bilişim sistemleri için koruyucu önlemler alınmasını sağlayan faaliyetler yürütmektedir. Yapılan siber güvenlik çalışmalarında konusu suç teşkil eden bulguların görülmesi durumunda adli makam ve kolluk kuvvetleri ile birlikte hareket etmektedir (USOM, "USOM Hakkında", t.y.).

USOM, gelen ihbarları ilk adımdan itibaren yöneterek özel ekipleri vasıtasıyla çözüm sürecine kadar takip eden ve değerlendiren resmi bir kurumdur. Bunun yanında ulusal ve uluslararası siber güvenlik tatbikatları yaparak kamu kurum ve kuruluşlarının bilincini ve farkındalığını artırmak amacıyla işlemler yürütmektedir (İstanbul Bilgi Üniversitesi, "USOM", t.y.).

Ayrıca, USOM koordinasyonunda çalışacak sektörel "Siber Olaylara Müdahale Ekipleri" (SOME), kurumların bünyesinde ise yine USOM koordinasyonunda çalışacak kurumsal SOME'ler kurulacaktır. Bu kurumlar arasındaki ise ilişki Şekil 3.1'de gösterilmektedir (BTK, "USOM ve Kurumsal Siber Olaylara Müdahale Ekibi", 2017).

Şekil 3.1

USOM, Sektörel SOME ve Kurumsal SOME İlişkisi SOME (Siber Olaylara Müdahale Ekibi) Nedir? Albayrak, 2018



3.1.3. Siber Olaylara Müdahale Ekibi (SOME)

Ulusal ve kurumsal siber güvenliğin sağlanmasındaki en önemli unsurlardan biri olan SOME 11 Kasım 2013 tarihinde ve 28818 sayılı Resmi Gazete'de yayımlanan Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ kapsamında resmi gazetede yayınlanmıştır (Ünver, 2016, s.20). USOM, Sektörel SOME ve Kurumsal SOME'lerin siber güvenlik hizmet alanları Tablo 3.1'de gösterilmektedir.

Tablo 3.1

USOM ve SOME'lerin Hizmet Alanları

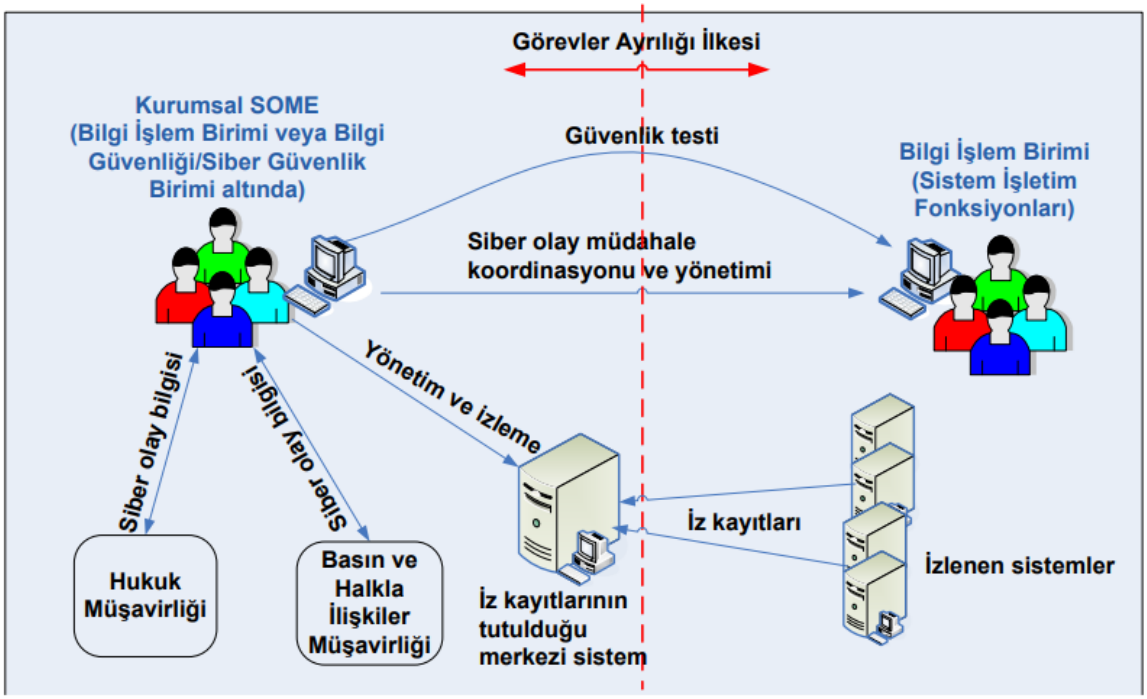
Organizasyon	Kurulduğu Kurum / Kuruluş	Hizmet Alanı
USOM	BTK / Telekomünikasyon İletişim Başkanlığı (TİB)	Ulusal siber ortam
Sektörel SOME	• Kritik Sektörü Düzenleyici ve Denetleyici kurumlar • Düzenleyici ve Denetleyici Kurumlar kuruluncaya kadar ilgili bakanlık	Kritik altyapı sektörü
Kurumsal SOME	Kamu kurum, kuruluşları ve kritik altyapı sektörlerindeki özel kurumlar	Kamu kurum, kuruluşları ve kritik altyapı sektörlerindeki özel kurumların siber ortamları

Kurumsal SOME Kurulum ve Yönetim Rehberi, 2014

Kurumsal SOME'lerin kurulum aşamalarında bilgi işlem biriminin sistem işletimi yapan tarafı ile Kurumsal SOME işlemlerinin farklı personeller tarafından yapılması önem arz etmektedir. Bu durum Şekil 3.2'de anlatılmaktadır.

Şekil 3.2

Kurumsal SOME'nin Kurum İçindeki Paydaşları ve Temel Fonksiyonları Kurumsal SOME Kurulum ve Yönetim Rehberi, 2014



Kurumsal SOME'lerin görev ve sorumlulukları üç aşamada ele alınmaktadır.

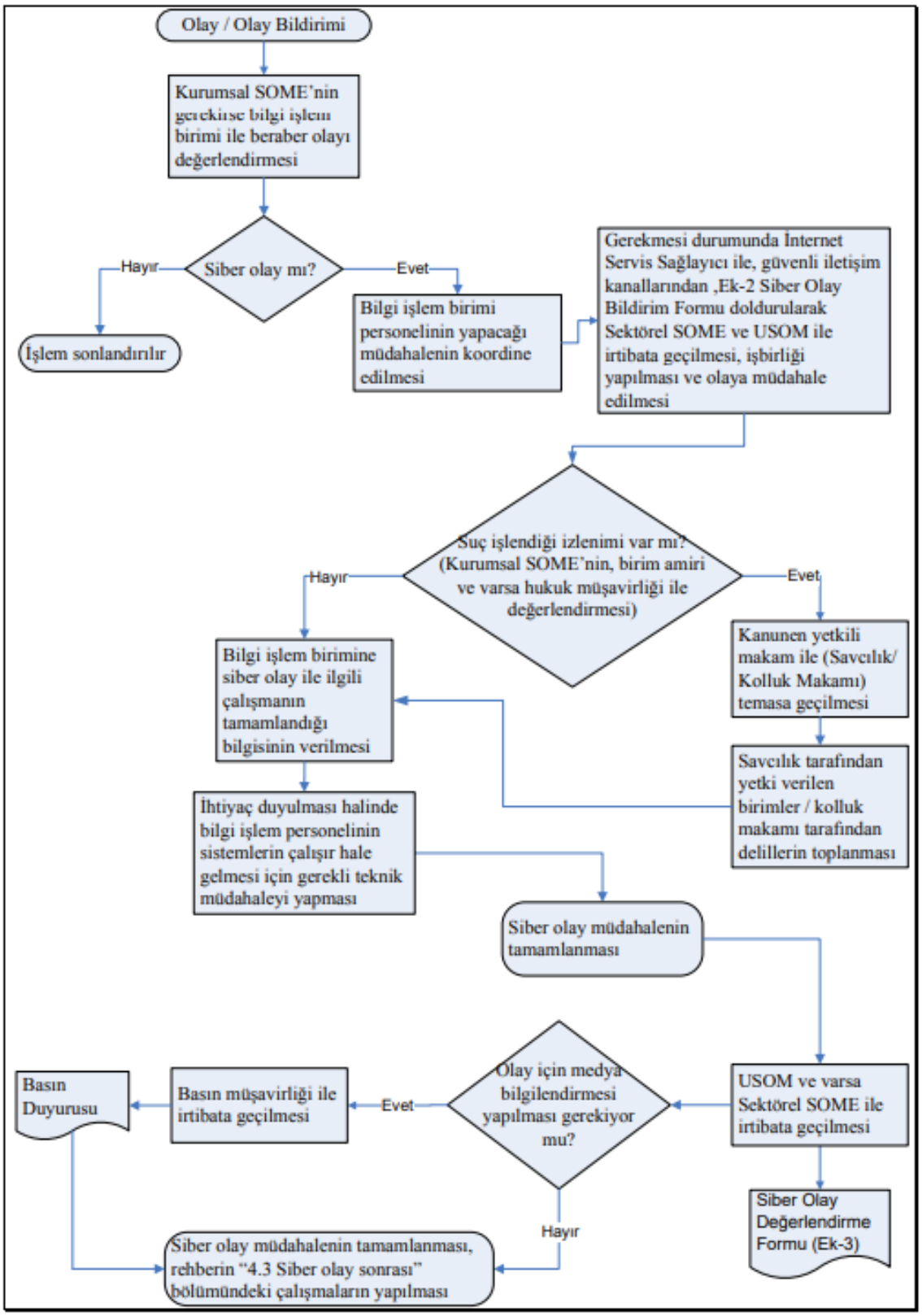
- Siber olay öncesi
- Siber olay esnası
- Siber olay sonrası

Siber olay öncesi: Kurum içinde herhangi bir siber olay olmadığı esnada Kurumsal SOME'ler, kurum içi farkındalık oluşturulması, kurumsal sızma testleri yapılması ve kayıtların düzenli bir şekilde incelenmesi gibi işlemleri yapmaktadırlar. (Kurumsal SOME Kurulum ve Yönetim Rehberi, 2014).

Siber olay esnasında: Bu adımda yapılacak işlemler Şekil 3.3'te özetlenmektedir.

Şekil 3.3

Siber Olay Esnası Akış Diyagramı Kurumsal SOME Kurulum ve Yönetim Rehberi, 2014



Siber olay sonrası: Siber olay gerçekleştikten sonra olaya neden olan açıklık belirlenerek çıkarılan dersler kaydedilir. Yaşanan siber olay vakit kaybetmeden USOM'a veya varsa bağlı olunan Sektörel SOME'ye gönderilir. Yaşanan olay bazında yapılabilecek önlem ve öneriler kurum yönetimine iletilir. Bu siber olaya ilişkin siber olay müdahale raporu hazırlanarak yönetim veya Kurumsal SOME'ye gönderilir (Kurumsal SOME Kurulum ve Yönetim Rehberi, 2014).

3.1.4. Bilgi Teknolojileri ve İletişim Kurumu (BTK)

Türkiye'de Telekomünikasyon sektörünü düzenleme ve denetleme işlemlerinin yürütülmesi adına 2813 sayılı Telsiz Kanununda değişiklik yapan 27 Kasım 2000 tarihli ve 4502 sayılı Kanun ile kurulan Telekomünikasyon Kurumu, 11 Kasım 2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu yeni bir düzenleme ile Bilgi Teknolojileri ve İletişim Kurumu olarak değiştirilmiştir. Böylece 2813 sayılı Telsiz Kanunu da yeni bir düzenleme ile Kanunun adı Bilgi Teknolojileri ve İletişim Kurumunun Kuruluşuna İlişkin Kanunu olarak değiştirilmiştir (BTK, "Kuruluş", 2017).

Bilgi Teknolojileri ve İletişim Kurumu'na 5809 sayılı Elektronik Haberleşme Kanunu'na maddeler eklenerek siber güvenlik ile ilgili yeni görevler verilmiştir. Siber güvenliğe yönelik BTK'ya; "Bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi, İzinsiz erişime karşı şebeke güvenliğinin sağlanması, Kişisel veri ve gizliliğin korunması, Abone, kullanıcı, tüketici ve son kullanıcıların hakları ile kişisel bilgilerin işlenmesi ve gizliliğinin korunmasına ilişkin gerekli düzenlemeleri ve denetlemeleri yapmak. Kurum, elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirlemeye yetkisi, Elektronik haberleşme sektörüne yönelik olarak, millî güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesi amacıyla mevzuatın öngördüğü tedbirlerin alınması" görevleri verilmiştir ("Elektronik Haberleşme Kanunu," 2008). Ayrıca BTK'ya 06/02/2014 tarihinde yayımlanan 6508 sayılı kanundaki "Madde 103" ile 5809 sayılı Kanunun 6 ncı madde birinci fıkra (ü) bendinden sonra gelmek üzere (v) bendi; "Siber güvenlik ve internet alan adları konularında Bakanlar Kurulu, Bakanlık ve/veya Siber Güvenlik Kurulu tarafından verilen görevleri Telekomünikasyon İletişim Başkanlığı veya diğer birimleri marifetiyle yerine getirmek" kısmı eklenerek siber güvenlik ile ilgili görev verilmiştir. (Türkiye Büyük Millet Meclisi (TBMM), "6518 Sayılı Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde

Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun", 2014, Madde 103).

BTK, telekomünikasyon sektöründe düzenleyicilik görevi yapan kurumdur. Görevleri; Denetleme, yetki verme, tüketici haklarını koruma, uzlaştırma, rekabet ortamı koruması, teknik yönergeleri düzenlemek ve yayınlamak, spektrum yönetimi ve izlenmesi gibi işlemlerdir. BTK, bilgi teknoloji işlerini de yöneten bir kurum olarak bu işlemleri Telekomünikasyon İletişim Başkanlığı (TİB) aracılığıyla yürütmektedir (Arslan, 2021).

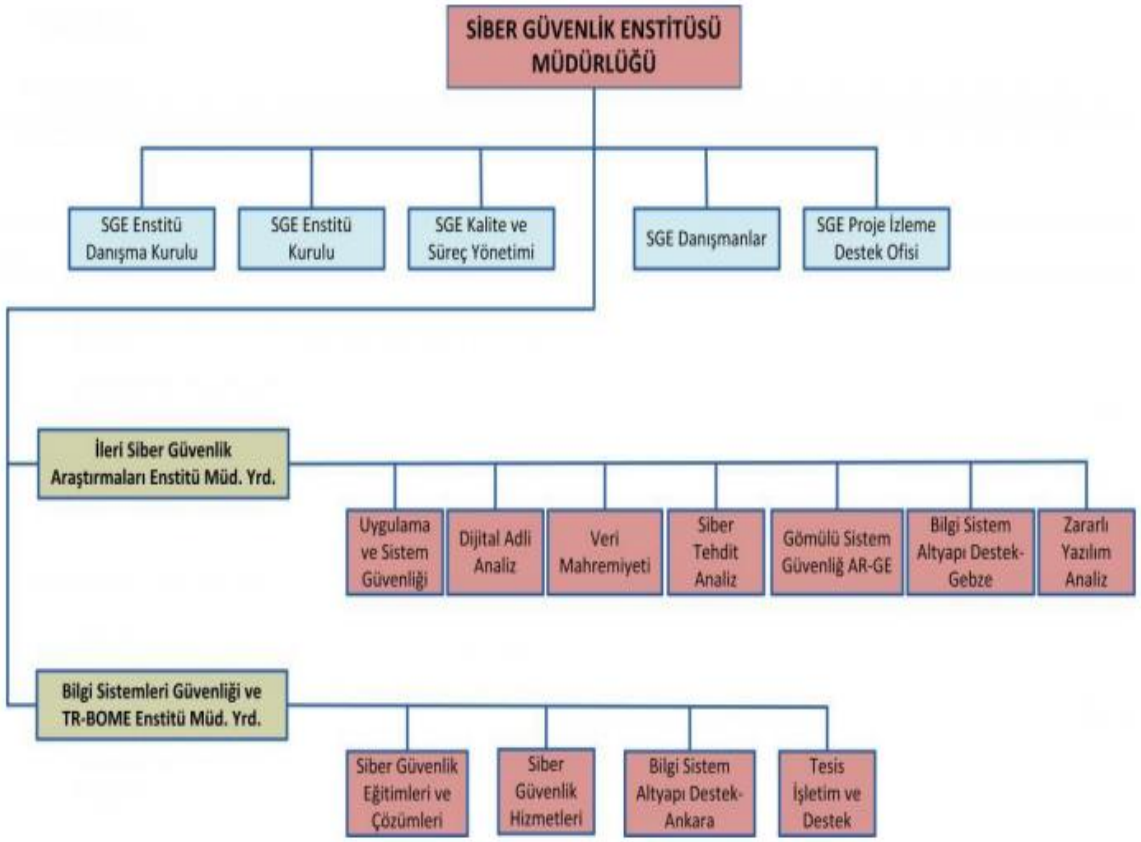
3.1.5. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) – Siber Güvenlik Enstitüsü (SGE)

Ulusal alanda siber güvenlik kapasitesinin artması amacıyla Siber Güvenlik Enstitüsü (SGE), 1997 senesinde Bilişim Sistemleri Güvenliği (BGE) adıyla TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)'de başlamıştır. 2012 yılından itibaren de TÜBİTAK BİLGEM adıyla ayrı bir enstitü olarak faaliyetlerini yürütmüştür (TÜBİTAK BİLGEM, "Siber Güvenlik Enstitüsü", t.y.).

SGE, siber güvenlik konusunda araştırma-geliştirme alanlarında çalışmalar yapmaktadır. Askeri kurumlar, kamu-özel kurum ve kuruluşları için çeşitli projeler yapmaktadır. Şimdiye kadar çok fazla projeye yön vererek ülkemizde siber güvenlik konusunda büyük katkılar sağlamıştır (TÜBİTAK BİLGEM, "Siber Güvenlik Enstitüsü", t.y.).

Şekil 3.4

SGE Organizasyon Şeması Bilgi Güvenliği Uygulamalari ve Çözüm Önerileri, Menteş, 2018



TÜBİTAK, Ekim 2021 yılına kadar siber güvenlikten sorumlu kurum olarak faaliyetlerini yürütmüştür. Bu durum 2012/3842 sayılı Bakanlar Kurulu Kararı ile Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na geçirilmiştir. TÜBİTAK, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (UDHB) ve Ulusal Siber Olaylara Müdahale Merkezi (USOM) ile beraber, 81 ilde 164 farklı noktadan trafik toplayan ülkenin bal küpü (honeypot) siber tehdit tespit sisteminin faaliyetlerini yürütmektedir (Bıçakcı et al., t.y., s. 35). Bal küpleri, bilişim sistemlerindeki yetkisiz erişimleri tespit ederek veri toplamaya çalışan ve yem olarak kullanılan tuzak sunuculardır. TİB'in yetkisi ile kurulmuştur.

2009 yılında, ülkemizdeki siber savunma ve sanal ortam güvenliğinin politikalarını belirleyebilmek adına TÜBİTAK UAKAE (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü) öncülüğünde ilgili kamu kurum ve kuruluşlarının temsilcilerinden oluşan bir çalışma grubu kurularak konu ile alakalı çalışmalarını 30 Ocak 2009 tarihinde bitirmiş ve

"Ulusal Sanal Ortam Güvenlik Politikası" belgesini hazırlamıştır. Çalışma grubunda mevcut olan kamu kurum ve kuruluşları aşağıda yer almaktadır:

- Cumhurbaşkanlığı
- Başbakanlık
- Dışişleri Bakanlığı
- Adalet Bakanlığı
- Milli Savunma Bakanlığı
- Ulaştırma Bakanlığı
- İçişleri Bakanlığı
- Maliye Bakanlığı
- Genelkurmay Başkanlığı
- Devlet Planlama Teşkilatı Müsteşarlığı
- Hazine Müsteşarlığı
- Dış Ticaret Müsteşarlığı
- Türkiye Cumhuriyet Merkez Bankası (TCMB)
- Milli Güvenlik Kurulu Genel Sekreterliği
- Milli İstihbarat Teşkilatı (MİT) Müsteşarlığı
- Bankacılık Düzenleme ve Denetleme Kurumu (BDDK)
- Emniyet Genel Müdürlüğü
- Bilgi Teknolojileri ve İletişim Kurumu (BTK)
- TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

3.1.6. TSK Siber Savunma Komutanlığı

Türk Silahlı Kuvvetleri (TSK), deniz, hava ve kara komutanlığından sonra 2012 yılında TSK Siber Savunma Merkezi Başkanlığı kurulmuştur. Daha sonra kurum "TSK Siber Savunma Komutanlığı"na çevrilmiştir. Bu komutanlığın amacı Türk Silahlı Kuvvetleri'nin ve Genelkurmay Başkanlığının web sayfalarının güvenliğini sağlamak olarak belirlenmiştir. Daha çok savunma işlemleri ile yetkilendirilmiştir (Orak, 2021, s. 214-226). Komutanlık, Ulaştırma Denizcilik ve Haberleşme Bakanlığı (UDHB), TÜBİTAK ve birçok üniversite ile koordine bir şekilde işlerini yürütmektedir. Dahası Kuzey Atlantik Antlaşması Örgütü (NATO) ile de işbirliği içerisinde çalışmaktadır (Menteş, 2018).

TSK bünyesindeki siber güvenlik ve bilgi güvenliği sistemlerinin milli yazılım programları ile geliştirilmesi ve TSK'ya karşı gerçekleştirilen siber saldırılara karşı güvenliği sağlama ve yapılan saldırıların zararının en aza indirilmesini hedefleyen Siber Savunma Merkezi (SİSAMER) Projesi 2017 yılında hayata geçirilmiştir.

3.1.7. Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı

Emniyet Genel Müdürlüğü (EGM), siber suçlar ile mücadele, suçların soruşturulması ve dijital ortamda bırakılan emarelerin araştırılması işlemlerini yapan Daire Başkanlıkları ve illerdeki birimler dağınık halde olması sebebiyle tek bir yapıda toplanması, mükerrer yatırımların önlenmesi ve siber suçlar ile daha başarılı bir şekilde mücadele edilmesi amacıyla 2011/2025 sayılı Bakanlar Kurulu ile Emniyet Genel Müdürlüğü çatısında Bilişim Suçlarıyla Mücadele Daire Başkanlığı kurulmuştur (EGM, "Hakkımızda", t.y.).

Amaçları arasında, siber suçlar ile mücadele, siber suçlar konusunda toplumda bilinç ve farkındalık oluşturma, uluslararası siber ilişkileri geliştirme, ülkemize karşı yapılan siber suçların analizi yapılarak mücadele yöntemlerini geliştirme, bu alanda uzman soruşturmacı ve adli bilişimci personelleri yetiştirmek, teknolojik alandaki yenilikleri takip ederek buna paralel olarak siber suçlarla mücadeleyi geliştirmek gibi konular sayılabilmektedir.

3.1.8. Milli İstihbarat Teşkilatı (MİT)

Milli İstihbarat Teşkilatı, ülkemizde gerçekleşebilecek olan siber saldırıların harekete geçmeden önce belirlenmesi için gerekli işlemlerin yapılabilmesi adına lazım olan istihbarat bilgilerini toplayan kurumlardandır. 6532 sayılı "Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununda Değişiklik Yapılmasına Dair Kanun" 26 Nisan 2014 tarihinde yürürlüğe girmiştir. Aynı kanun 2017 yılında gerçekleşen değişiklikler ile Cumhurbaşkanlığına bağlanmıştır. 6532 sayılı yasa MİT'in görev ve yetkilerini şu şekilde tanımlamıştır: "Dış istihbarat, millî savunma, terörle mücadele ve uluslararası suçlar ile siber güvenlik konularında her türlü teknik istihbarat ve insan istihbaratı usul, araç ve sistemlerini kullanmak suretiyle bilgi, belge, haber ve veri toplamak, kaydetmek, analiz etmek ve üretilen istihbaratı gerekli kuruluşlara ulaştırmak" (Bıçakcı et al., t.y., s.47-48).

MİT'in siber tehditler ve siber suçlulara karşı yetkisi ve gelişimi oldukça önemlidir. Ülkemize karşı yapılabilecek olan devlet destekli veya terör örgütleri ya da uluslararası saldırılar gerçekleştiren gruplara karşı siber tehditlerin önceden analiz edilmesi ve tedbir alınması hususunda ayrıca önemi büyüktür.

3.1.9. Bilgi Güvenliği Derneği (BGD)

Bilgi Güvenliği Derneği, 22 Temmuz 2007 tarihinde, bilgi güvenliği ve siber güvenlik alanında ulusal ve uluslararası alanda tarafsız güvenilir ve etkin bir sivil toplum kuruluşu olmak amacıyla kurulmuştur. Toplumun her kesiminde bilgi güvenliği hakkında bilinç ve farkındalık düzeyini artırmak, güncel teknolojik gelişmeleri takip etmek, milli teknolojilerin gelişimine destek sağlamak; bireysel, kurumsal ve ulusal kapsamdaki risklere karşı farkındalık oluşturmayı hedeflemektedir (Yücel, 2021). Kamu ve özel sektör yöneticileri ile akademisyenlerden oluşan, alanında uzman kişiler tarafından Ankara'da kurulmuştur.

Derneğin kuruluş amaçları:

- Bireysel, kurumsal ve ulusal alanda bilgi güvenliğinin sağlanmasına katkı sağlamak
- Bilgi güvenliği kapsamında politika ve stratejiler üreterek ilgili birimlere sunmak
- Toplumun bilgi güvenliği alanında bilgilendirilmesini sağlamak
- İlgili kurum, kuruluş ve birimlerle işbirlikleri yaparak bilgi güvenliğinin sağlanabilmesi amacıyla ortak aklın oluşturulmasına katkıda bulunmak
- İlgili kurumlarla ulusal ve uluslararası kapsamda işbirlikleri yaparak bilgi güvenliği standartlarına uygun olarak kurum ve kuruluşların yapılandırılmasına katkıda bulunmak
- Bilgi güvenliği alanında konferans, seminer, sempozyum, kurs ve benzeri etkinlikler düzenlemek
- Bilgi güvenliği kapsamında bilgilendirme dokümanları hazırlamak
- Ulusal ve uluslararası kapsamda faaliyet gösteren sivil toplum kuruluşları ve ilgili birimler ile işbirliği yapmak
- Bilgi güvenliği alanında katkı sağlayacak denetlemeler yapma, eğitim ortamı sağlama ve danışmanlık gibi faaliyetleri gerçekleştirmek
- Bilgi güvenliği alanındaki araştırmalara destek vermek

- Bilgi güvenliği kapsamında ulusal ve uluslararası alanda faaliyetler yürütmek
- E-devlet uygulamalarının daha güvenli hale getirilmesinde destek sağlamak ("Bilgi Güvenliği Derneği Tüzüğü", 2007)

BGD, ülkemizde başta kamu ve özel sektör kuruluşları ile üniversiteler ve çeşitli sivil toplum kuruluşları olmak üzere tüm paydaşlarla işbirliği içinde bilgi güvenliği mevzuatının hazırlanması ve geliştirilmesinde aktif olarak çalışmıştır. Ulusal Siber Güvenlik Stratejisinin hazırlanması ve 2012/3842 sayılı Bakanlar Kurulu kararının alınmasında aktif görevlerde bulunarak rol almıştır (Mentes, 2018).

3.1.10. Türkiye Bilişim Derneği (TBD)

Türkiye Bilişim Derneği, 1971 yılında bilişim alanında yetkili ve bilgili kişiler tarafından "Bilişim Kültürünü" toplumun her kısmına yaymak amacıyla kurulan bir sivil toplum örgütüdür. 19 Nisan 1994 tarihinde Resmi Gazete'de 7 Mart 1994 tarih ve 94/5420 sayılı Bakanlar Kurulu kararı gereği Kamu Yararına Çalışan Dernek statüsünü almıştır.

Derneğin kuruluş amaçları:

- Güncel ve gelişen teknolojiler için araştırma yapmak amacıyla çalışma grupları kurar.
- Bilişim alanında gerekli yayınların yapılmasını sağlar.
- Bilişim alanındaki mesleklere ait eğitim programlarının yapılmasını sağlar.
- Bilişim danışmanlığı yapılmasına olanak sağlar, bilgi akışı ve iş birliği gibi yardımlaşmalara öncülük eder.
- Bilişim sektörüne dair ulusal ve uluslararası alanda çalıştay, konferans, seminer gibi toplantılar yapılmasını teşvik eder ve katılımı sağlar.
- Bilişim alanında olabilecek hukuki düzenlemelere görüş bildirir ve gerekli katkıları sağlar.
- Uluslararası alanda bilişim konulu dernek ve kuruluşlara üye olur ayrıca iş birliği ve yardımlaşmalara öncülük eder.
- Bilişim alanındaki küresel gelişmeleri takip ederek ülkemize bununla ilgili katkı sağlanmasına destek olur (TBD, "Tanıtım", t.y.), (TBD, "Tüzük", t.y.).

TBD, prensip edindiği amaçlarını gerçekleştirmek ve hayata geçirmek amacıyla çalışma grupları kurmaktadır. Ulusal ve uluslararası konferans, çalıştay vb. gibi etkinliklere

katılmak, bilişim alanındaki gerekli yayınların yayınlanmasını sağlamak, bu sektördeki gelişmeleri takip ederek ülkemize bu alanda katkılar sağlamak gibi çeşitli faaliyetlerde yer almaktadırlar.

TBD'nin aktif bir şekilde faaliyetlerini gerçekleştiren 7 tane çalışma grubu mevcuttur. Her biri kendi alanlarındaki çalışma faaliyetlerini sürdürmektedir. Bu çalışma grupları şu şekildedir:

- TBD Kamu-BİB (Türkiye Bilişim Derneği Kamu Bilişim Merkezleri Yöneticileri Birliği) Çalışma Grubu
- Hukuk Çalışma Grubu
- Türk Dünyası Ortak Bilişim Terimleri Çalışma Grubu
- Bilişimde Özenli Türkçe Çalışma Grubu
- Türk Dünyası Bilgi Teknolojileri Çalışma Grubu
- Bilişim Kentleri Çalışma Grubu (TBD, "Tanıtım", t.y.).

TBD'nin üye sayısı 12 binin üzerinde olmakla birlikte 10 adet şubesi ve 13 il temsilciliği bulunmaktadır (TBD, "Tanıtım", t.y.).

3.1.11. Kamu Sanal Ağı (KamuNet) Projesi

KamuNet Projesi herkese açık bir şekilde kullanılan kamu kurum ve kuruluşlarındaki veri akışlarının internete kapalı bir ortamda, sanal bir ağ üzerinden gerçekleştirilmesiyle siber tehditlerin en aza indirilmesinin amaçlandığı bir projedir. Kamu kurumlarının KamuNet Projesine dahil edilmesi konulu 2016/28 sayılı Başbakanlık Genelgesi 3 Aralık 2016'da Resmi Gazete'de yayımlanmıştır. KamuNet çalışmaları Ulaştırma ve Altyapı Bakanlığı (UAB) tarafından gerçekleştirilmektedir (UAB, "KamuNet", t.y.).

KamuNet vasıtasıyla paylaşılan verilerin uçtan uca güvenli bir şekilde iletilmesi, iletişimin bir standarta bağlanması, ortak veri iletişim merkezlerinin kurulması gibi işlemleri kolaylaştırması amaçlanmaktadır.

3.1.12. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Siber Güvenlik Dairesi Başkanlığı

İlerleyen teknolojiler, kamu kurumlarındaki yenilikçi hareketler, toplumsal istekler ile paralel olarak farklı kurumlar arasında ayrı bir şekilde yürütülen siber güvenlik, milli teknolojik gelişmeler, yapay zeka gibi çalışmaların tek bir merkezden yürütülmesi maksadıyla 10 Temmuz 2018 tarihli ve 30474 sayılı Resmi Gazete'de yayımlanan T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi kurulmuştur (CBDDO, "Hakkımızda", t.y.).

Siber Güvenlik Dairesi Başkanlığının görevleri ise şu şekildedir:

- Cumhurbaşkanının belirlediği stratejiler doğrultusunda siber tehdit risklerine karşı kamu kurumları ve kritik yapıların siber güvenlik önlemlerinin gelişmesini sağlamak,
- Ülkemizde var olan siber güvenlik ve bilgi güvenliğine dair projeler gerçekleştirmek,
- Siber güvenlik konusunda ülkemizde uygulanan politika ve stratejilerin doğru bir şekilde uygulanmasını sağlamak ve kontrolünü gerçekleştirmek,
- Kritik altyapıların hangileri olduğunun belirlenmesinde gerekli çalışmaları yürütmek,
- Kamu kurumları, özel kuruluş ve üniversiteler arasındaki siber güvenlik kapsamındaki iş birliklerinin geliştirilmesine yardımcı olmak,
- Yerli ve milli siber güvenlik ürünlerinin kamuda kullanılmasına teşvikte bulunmak,
- Kritik altyapı ve teknolojilerin korunmasına dair yapılan çalışma faaliyetlerinde bulunmak,
- Siber güvenlik ve bilgi güvenliği kapsamında standartlar, usuller ve esasların belirlenmesi amacıyla çeşitli çalışmalar yürütmek,
- Siber güvenlik alanındaki hükümlerde istisna tutulacak kurum ve kuruluşların belirlenmesi konusu kapsamında önerilerde bulunmak,
- Özel kuruluşların kapasitesini kritik altyapılara yönlendirmek ve mükerrer işlemlerin önüne geçebilmek amacıyla daha kritik olan siber güvenlik alanlarını belirlemektir (CBDDO, "Siber Güvenlik Dairesi Başkanlığı", t.y.).

3.1.13. On Birinci Kalkınma Planı (2019-2023)

Cumhurbaşkanlığı hükümet sistemine geçilen döneminin ilk kalkınma planı On Birinci Kalkınma Planı 2019 ile 2023 yılları arasını kapsamaktadır. Kalkınma planında

bahsedilen neredeyse her genel başlıkta konuların dijitalleştirilmesi ve dijital sistemlerin diğer konular ile birleştirilmesi düşünülmüşür. Dijital dönüşümler vasıtasıyla da yerli teknolojilerin kullanımının sağlayacağı yararlara değinilmiştir.

On Birinci Kalkınma Planı, işletim sistemlerinin milli yazılımlara çevrilmesi konusundaki çalışmalar için nitelikli kişilerin yetiştirilmesi gerektiği ve bu alanda gerekli olan kaynak ihtiyacının karşılanması meselesinin üzerinde durulması oldukça önemli bir konudur. Ayrıca sadece kamu personeli değil tüm toplumda siber güvenlik farkındalığı oluşturulmasına dair bir yapı tesis edilmesi üzerinde durulmaktadır.

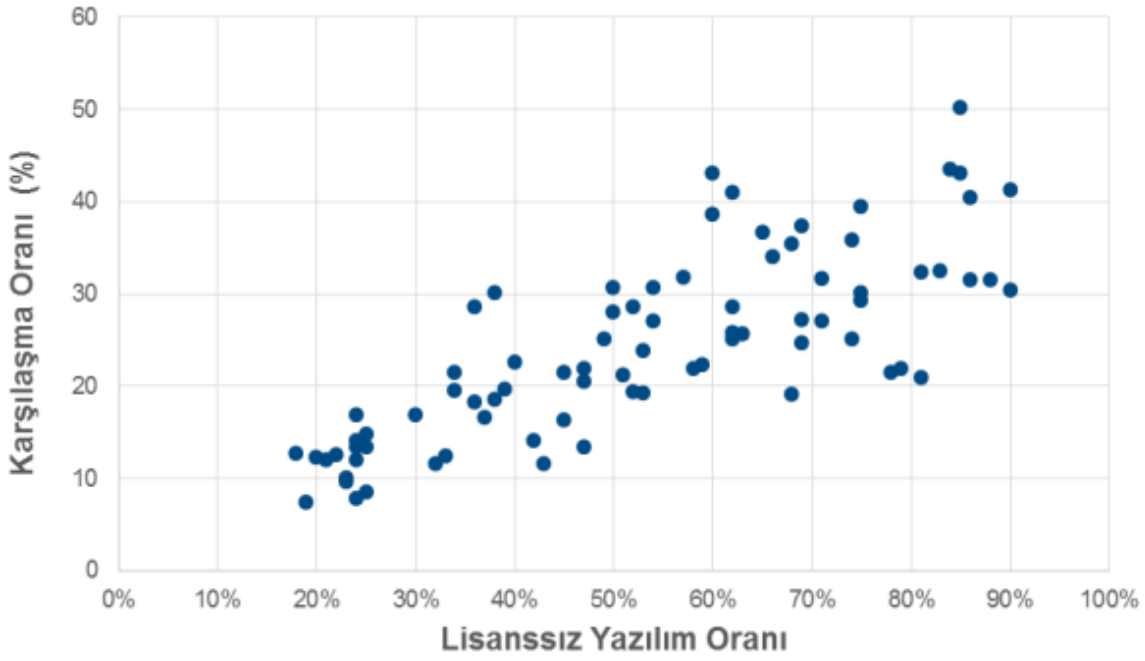
3.2. Siber Güvenlik Kapsamında Alınabilecek Önlemler

Siber güvenlik kapsamında yapılan incelemeler neticesinde alınabilecek önlem ve öneriler sayesinde tamamen risksiz bir ortam oluşturulamasa da meydana gelebilecek olan tehdit ve saldırılar minimuma indirilebilmektedir. Toplum olarak siber alanda hem bireysel hem kurumsal hem de ulusal olarak alınabilecek önlemler incelenecektir.

Lisanssız yazılım kullanılmamalıdır: Bireyler kişisel ve iş bilgisayarlarında lisanssız yazılım kullanmamaya dikkat etmelidir. En basit örnekle herhangi bir lisanssız uygulama veya oyun vb. indirildiğinde kurulum dosyası ile birlikte bir çok kötücül yazılım da bilgisayarlara inebilmekte ve zarar verebilmektedir.

Şekil 3.5

Lisanssız Yazılımların Kötü Amaçlı Yazılımlar İle Karşılaşma Oranı Lisanssız Yazılımlar ve Siber Güvenlik Tehditleri, Gantz et al., 2015, s. 3



Güvenlik paketleri kullanılmalıdır: Kullanıcılar bireysel ve kurumsal bilgisayarlarını güvenlik tehditlerinden koruyabilmek için güvenlik paketleri/antivirüs programları kullanmalıdırlar. Bu yazılımlar sayesinde kullanıcılar güvenli ve kesintisiz olarak internet hizmeti kullanabilirler. Bu yazılımlar kullanıcıların istediği zaman bilgisayarların tamamını tarayarak zararlı ve kötücül yazılımları tespit ederek temizleyebilmektedirler. Aynı şekilde devamlı arka planda da çalışarak yeni gelen saldırılar ve tehditleri de tespit ederek uyarı verip anında kontrol altına alabilirler.

Kötücül yazılımlar her an artabilen, yenileri çıkabilen türlerdir. Güvenlik yazılımları, bu yeni türleri veritabanlarında sürekli tarayarak yenileyebilmektedir. Bu sebeple bu yazılımlar kolay bir şekilde yeni türleri tespit etmekte oldukça iyidirler. Fakat dikkat edilmesi gereken nokta, antivirüs kullanıcıları bilgisayarlarındaki yazılımlarını sıkı bir şekilde güncelleyerek bu yeni türlere karşı tetikte olabilmektedir.

Yazılım güncellemeleri düzenli yapılmalıdır: Kullanıcılar bilgisayarlarındaki yazılım güncellemelerini zamanında yapmadıklarında bilgisayarları siber tehditlere açık bir hale gelmektedir. Dünyada hergün binlerce yeni kötücül yazılım keşfediliyor. Yazılım sahipleri ise bu keşiflere ve yeniliklere ayak uydurarak yazılımlarını bu tehditlerden

korumak için sürekli yeni güncel eklentiler yapıyor. Kullanıcılar, tehditlerden korunabilmek için kullandıkları uygulamaların güncelleme paketleri geldiğinde mutlaka güncelleme yaparak bu gibi siber tehditlere karşı daha güvenlikli kalabilmeleri mümkün oluyor.

Bilgisayarların ilk kuruluşla gelen yetkili kullanıcı isimleri değiştirilmelidir: Bilgisayarların ilk kurulumu esnasında yetkili kullanıcılar belirlenir. Bu genellikle kurulumu yapan destek aldığımız kişiler/firmalar tarafından gerçekleştirilen bir işlemdir. Kurumsal bilgisayarlarda ise BT bölümü çalışanları tarafından yapılmaktadır. Herhangi bir durumda sisteme erişmek isteyen siber saldırganlar giriş yapmaya çalışırken yetkili kullanıcı isimlerini daha önceden biliyor olur iseler işleri kolaylaşacaktır ve sistem daha kolay ele geçirilecektir. Bu sebeple kurulum ile birlikte gelen yetkili kişi isimleri bilgisayarlar alındıktan sonra değiştirilmelidir.

Güçlü bir parola seçilmelidir: Bilgisayarlar, sistemler veya uygulamalar için kullanılan parolalar kolay tahmin edilebilir ve basit olmamalıdır. Parolalar uzun, büyük ve küçük harf ile semboller içeren parolalar olmalıdır. Özel günler ve anlamlar içeren parolalar seçilmemelidir.

Tüm hesaplarda aynı parolalar kullanılmamalıdır: Kullanıcılar parolalarını farklı uygulamalarda farklı şekillerde kullanmalıdırlar. Herhangi bir hesap ele geçirildiğinde diğer hesapların da ele geçirilmesini önlemek için bu tedbir oldukça önemlidir. İşyerlerinde kullanılan şifreler özel kullanım alanlarımızdan farklı olmalıdır. Unutulmamalıdır ki, kişisel hesaplarımız ele geçirilirse aynı şifreyi kullanmamız durumunda, kurumsal alandaki kritik verilerin de ele geçirilmesi mümkün olacaktır.

Parolalar kimseyle paylaşılmamalıdır: Kullanıcılar, parolalarını ne sebeple olursa olsun hiç kimseyle paylaşmamalıdır. Çeşitli sosyal mühendislik yöntemleri ile parolalarını öğrenmeye çalışan kişilere itibar edilmemelidir. Bu gibi konularda kimseye güvenilmemelidir.

Açılan oturumlarda "beni hatırla" seçeneği seçilmemelidir: Kullanıcılar çeşitli uygulamalarda oturum açma sayfasında yer alan "beni hatırla" seçeneğini kullanmamalıdır. Siber saldırganlar veya suçlular tarafından bilgisayarın ele geçirilmesi veya işyeri, topluma açık bir alan vb. bir ortamda sayfanın açık kalması durumunda kullanılabilmesine olanak verilmemelidir.

Belli periyodlarla parolalar değiştirilmelidir: Kullanıcılar parolalarını belirli periyodlarla değişirse şifrelerin ele geçirilmesi durumunda kullanılabilmesinin önüne geçebilmektedir. Güvenlik açısından sürekli değiştirilen parolaların kullanımı daha sağlıklı

olacaktır. Ele geçirilen bir hesap var ise önüne geçilmesi böylelikle daha kolay olabilecektir. Özellikle işyerlerinde kurumsal bilgisayarların şifresi, belirli aralıklarla güncellenmelidir.

Kullanılmayan kullanıcı hesapları kapatılmalıdır: Tek seferlik kullanılacak olan sitelerde açılması gereken hesaplar olabilmektedir. Bu hesaplara tekrar giriş yapılmayacaksa daha sonrasında kişisel bilgilerin ele geçirilmemesi açısından hesaplar kapatılırsa kullanıcılar için daha güvenli bir ortam oluşacaktır.

Önemli ve saldırılara açık olduğu düşünülen veriler düzenli olarak yedeklenmelidir: Kullanıcıların özel ve gizli bilgiler içeren ya da önemli olduğu düşünülen dosyalarının, iş hayatında kritik ve gizli kalması gereken verilerin, düzenli olarak başka ortamlarda yedeklenmesi verilerin kaybını en aza indirgemek açısından oldukça önemlidir. Bazı kritik veriler, doğal afet veya meydana gelebilecek saldırı teşebbüsleri açısından ülkemiz dışında varolan korunaklı veri depolama merkezlerinde yedeklenebilmektedir.

Kullanılmayan anlarda bilgisayarların ekranları kapatılmalıdır: Kullanıcılar herhangi bir ortamda bilgisayarlarını kullanmayacaklarında ve bulundukları yerden ayrılacakları durumlarda ekranlarını kilitlemeyi unutmamalıdır. Kötü niyetli kişiler tarafından bilgisayarın tamamen açık ve güvensiz bir halde bırakılmasına engel olunmalıdır. İş hayatında, erişim yetkisi olmayan kötü niyetli kişiler tarafından da açık kalan bilgisayarlardan veri sızdırılmaya çalışılabilmektedir. Önüne geçebilmek için, ekranlara erişim kapatılmalıdır.

E-posta, Kısa Mesaj Hizmeti (SMS), Twitter, Facebook, İnstagram mesajlarının kaynağından emin olunmalıdır: Bu gibi sanal ortamlarda kullanıcılara herkes tarafından mesaj gelebilmesi mümkündür. Kullanıcılar, tanımadıkları kişiler tarafından veya yardım vb. gibi duygusal zafiyetlerden yararlanmak isteyen kişiler tarafından gönderilen iletilere aldanmamalıdır.

Sosyal mühendislik saldırılarılarına karşı dikkatli olunmalıdır: Kendilerini banka görevlisi, teknik görevli vb. gibi tanıtarak bilgi edinmeye çalışan kişilerle hiç bir bilgi paylaşılmamalıdır. Kişisel ve iş hayatındaki kritik bilgiler konusunda bilgi verilmemelidir. İş ortamında kendisini görevli olarak tanıtan kişilere gerçekliğinden emin olunmadan inanılmamalıdır. Teyit etmeden tanımadığımız kişileri kurum içine almamalı ve bilgi verilmemelidir.

Bilgisayar, tablet, telefon, harici bellek gibi fiziki eşyaların güvenliğine dikkat edilmelidir: Bu gibi fiziki eşyaların güvenliği konusunda gerekli tedbirler alınmalıdır. Başıboş bir şekilde bırakılmamalı ve alınabiliyorsa bu cihazlar sahipleri tarafından

yanlarında taşınmalıdır. Çalınma riskine karşı disk şifreleme yapılmalı ve cihazlara da güçlü parolalar koyulmalıdır.

CD ve USB gibi cihazlar kimseyle paylaşılmamalıdır: Bu gibi harici cihazlar kötücül yazılım taşıyabilmesi riskine karşı kimseyle paylaşılmamalıdır. Kullanması için verilen herhangi bir kişinin cihazına kötücül yazılım bulaşmış olabilmektedir. Cd ve Usb'nin bu cihazlarla kullanılmasıyla beraber bu yazılımlar temiz cihazlara da bulaşacaktır.

Her bağlantıya tıklanmamalıdır: Özellikle oltalama gibi amaçlarla gönderilen iletiler de dahil olmak üzere internet ortamını kullanan kişiler, bağlantılara tıklarken dikkat etmelidir. Bağlantının adres kısmı kopyalanarak (SSL-Secure Sockets Layer Sertifikası) kontrol edilmeli, erişilen sayfalarda kişisel bilgilerin istenmesi durumunda giriş yapılmamalı, iletişim protokolünün çevrimiçi alışveriş sitelerinde https, dosya indirirken "secure ftp" yani güvenli olmasına dikkat edilmelidir.

Kendiliğinden açılan pencereler engellenmelidir: Tarayıcı ayarları yardımıyla zararlı bileşenlere önlem olarak otomatik açılan pencereler engellenmelidir. Çünkü kendiliğinden açılan reklam içeren pencerelerin çoğu potansiyel zararlı yazılım bulundurma riski taşımaktadır.

Herkese açık ücretsiz internet bağlantısı kullanılan ortamlarda dikkatli olunmalıdır: Halka açık alanlarda ücretsiz internet kullanılan ortamlarda siber saldırganlar aynı bağlantı sayesinde çok daha kolay şekilde yetkisiz erişim yapabileceği için çok acil ve önemli olmadıkça bu ağlara bağlanılmamalı ya da çok dikkat edilmelidir.

Evlerdeki modemlerin kullanımında dikkatli olunmalıdır: Kullanıcıların evlerinde kullandıkları kablosuz modemler şifreli iletişim yapacak şekilde ayarlanmalı, parolaları güçlendirilmeli ve belli aralıklarla değiştirilmeli, cihaz adres bilgileri dış dünyadan gizlenmelidir.

Kullanılan sosyal medya hesaplarında iki aşamalı doğrulama yöntemleri seçilmelidir: Bireyler kullandıkları sosyal medya hesaplarında giriş yöntemini iki aşamalı doğrulama olarak kullanırsa meydana gelebilecek olan saldırıların daha fazla önüne geçebilecektir. Bu yöntem ile örneğin şifre ile giriş yapmanın yanısıra telefon vb. Kişisel bir aygıttan da başka bir yöntem vasıtasıyla diğer aşamayı da gerçekleştirerek güvenlik önlemlerini artırabilmektedir.

Sosyal medya hesaplarındaki paylaşımlara dikkat edilmelidir: Sosyal medya hesaplarında paylaşılan bilgiler, resimler ve videolar, dolandırıcılar ve suç örgütleri için çok şey ifade ediyor olabileceğinden dolayı paylaşımlar dikkatle yapılmalı ve minimize olmalıdır. Yapılan paylaşımlar hem kişisel hem de iş hayatı ile ilgili büyük bilgiler

verebileceğinden siber suçlular için önemli bir kaynak olabilmektedir. Özellikle iş hayatı ile bağlantısı olabilecek paylaşımlar sınırlı ve dikkatli yapılmalı, mümkünse saldırganlara yer, mekan ve yapılan iş vb. konularda ipucu verilmemelidir.

Sosyal medya hesaplarının gizliliği kapalı olmalıdır: Bireyler sosyal medya hesaplarını herkese açık bir şekilde tanımlar iseler bir çok konuda siber suçlulara ipucu verebileceğinden ötürü paylaşımları kapalı ve arkadaşlara açık olacak şekilde kontrol edilmeli ve dikkatli tanımlanmalıdır. İş hayatında özellikle yetkili konumdaki kişiler, sosyal medya platformları vasıtasıyla kendileri ile ilgili verileri açık etmeme konusunda özenli davranmayı ihmal etmemelidirler.

Akıllı telefonların konum servisleri kullanılmadığında kapalı olmalıdır: Konum servisi vb. gibi kritik bilgilere erişim sağlayabilmiş olan siber suçlulara karşı bu konuda dikkatli olunmalıdır. Siber korsanlar saldırılarını kurbanların konumuna göre ayarlayarak sosyal mühendislik saldırı türleri yardımıyla gerçekleştirebilmektedir.

Akıllı telefon kullanımda her uygulama indirilmemeli, kişisel bilgilere erişim isteği geldiğinde dikkat edilmelidir: Akıllı telefonlara indirilen uygulamalar, kişilerin çoğu verisine erişmek için izin istemektedir. Bu gibi bildirimleri dikkatli okuyarak seçimler özenle yapılmalıdır. Bu gibi güvenliğinden emin olunmayan uygulamaların da indirilmemesine dikkat edilmelidir. Hem kişisel hem iş hayatı ile ilgili verilerin açık edilmesine sebebiyet verebilmektedir.

Akıllı telefonlar el değiştirirken telefon temizlenmelidir: Akıllı telefonlar satılırken veya el değiştirirken mutlaka içerisindeki tüm veriler temizlenmeli ve telefon fabrika ayarlarına döndürülmelidir.

Kurumlarda çalışan personellere siber güvenlik konusunda eğitimler verilmelidir: Siber tehditlerin farkına varılabilmesi amacıyla kurumlarda düzenli olarak siber güvenlik eğitimleri düzenlenerek çalışan personellere farkındalık yaratılmalıdır. Genellikle çoğu birey, siber güvenliğin öneminin ve alınabilecek önlemlerle risk ve tehditlerin en aza indirebileceğinin farkında değildir. Bu sebeple bilinçlendirici eğitimlerin düzenlenmesi yapılabilecek hataları en aza indirgeyebilmektedir.

İşyerlerinde sorun tespit ve güvenlik analizleri için bilgisayarlarda sistem ve güvenlik kayıtlarının (Log) açık olduğundan emin olunmalıdır: Sistemde tutulan log kayıtları sayesinde hatalar ve analizler geçmişe yönelik işlemler görüntülenebilmektedir. Böylece geriye yönelik yaşanan güvenlik ihlalleri vb. tespit edilerek bunlar için önlem alabilmek daha kolay bir hale gelebilmektedir.

Sistemlerdeki bilgilere erişimler limitlendirilmeli ve erişim yetki sınıfları oluşturulmalıdır: Kurumlarda özellikle önemli ve kritik bilgilerin erişimi sadece yetkili kişilerle sınıflandırılmalı ve ayrı yetki sınıfları tanımlanmalıdır. Herkesin her türlü bilgiye erişebilmesi güvenlik açısından kısıtlanmalıdır.

Kurumsal bilgisayarlar kişisel amaçlarla kullanılmamalıdır: Çalışan bireylerin iş bilgisayarlarını, özel ve kişisel amaçlarla kullanması siber güvenlik açısından tehditlere yol açabilmektedir. Girilen siteler, tıklanan adresler oltalama vb. gibi tehditlerle dolu olabileceğinden iş bilgisayarları kişisel amaçlarla kullanılmamalıdır.

Kurumsal e-posta adresleri, iş dışındaki alanlarda kullanılmamalıdır: Kurumsal e-posta adresleri çevrimiçi alışveriş sitelerinde ya da özel amaçlı iletişim gruplarında paylaşılmamalıdır. E-posta adreslerinin siber korsanların eline geçmesi durumunda saldırılarını bu tarafa çevirmeleri ve e-posta adresleri üzerinden gerçekleştirmeye çalışmaları mümkün olabilecektir.

Kurum için kritik olan veriler şifrelenmelidir: Sadece yetkili kişiler tarafından erişilmesi gerektiği düşünülen kritik bilgilerin**,** yetkili kişilerin okuyabilmesi için verinin iletimi veya depolanması sırasında verileri kodlama işlemi yapılarak gizlemek iyi bir güvenlik önlemi olacaktır. Veri sadece yetkili kişinin eline geçtiğinde, yetkili kişi tarafından çözülerek okunabilecektir.

SSL VPN bağlantısı kullanılmalıdır: Özellikle pandemi dönemi ile işyerleri uzaktan çalışma yöntemine geçmeye başlamıştır. Çalışanlar, evlerinden işyerlerine ait sistemlere giriş yaparken SSL VPN sanal ağ teknolojisi üzerinden giriş yaparak işyerindeki sistemler ile evlerindeki kişisel bilgisayarlar arasında gizli ve güvenli bir bağlantı açılarak bu ağ üzerinden verilerin iletilmesini sağlamaktadır. Bu teknoloji ile güvenli bir bağlantı yolu seçilmiş olacaktır. VPN bağlantısı yöntemiyle işyerlerinde alınabilecek önlemler aşağıdadır.

- Ağda bağlı olan tüm ağlar, aynı ağdaymış gibi çalışır.
- Maliyet açısından sadece kurulum maliyeti ile hızlı bir ağ mimarisi oluşturulabilmektedir. Bu teknoloji ile kuruluşlar kendi aralarında veri alışverişini en ucuz ve güvenli şekilde gerçekleştirir.
- Güvenlik için ek bir donanıma gerek kalmamış olur.
- İşyerlerindeki bölgeler, şubeler vb. arasında SSL sertifikalı şifreli bir iletişim sağlanır.

- Merkez ve diğer konumlardaki şubeler arasında merkez tarafından yönetilebilecek bir ağ oluşturulmuş olur.
- Ağlardaki yerel ağ alt yapıları ile İP adresleri değişmeden SSL VPN ile güvenli bir sistemde veri iletim ortamı oluşturulur.
- Yöneticiler tarafından erişim izinleri düzenlenebilir ve kritik kaynaklara erişim kısıtlanabilmektedir. Bunun yanında örneğin, bir yönetici sadece mesai saatleri içinde erişim izni vererek bile sistemi kontrol altında tutabilecektir (Böge, 2018).

Yeni saldırı yöntemlerini takip ederek önlemler alınmalıdır: Dünyada her geçen gün binlerce saldırı yöntemi, kötücül yazılımlar vb. türemektedir. Bu gibi güncel yöntemlerin takibi için kurumsal ortamlarda görevlendirme yapılarak doğabilecek siber tehditler için aksiyonlar alınmalıdır.

Kurumlar, dışarıdan aldığı hizmetler için güvenilir firmalar seçmelidirler: Kurumlardaki bazı BT işlemleri için özel firmalardan hizmetler alınabilmektedir. Bu gibi durumlarda, gelen firmalar kuruma ait kritik bilgilere erişebilmektedir. Bu sebeple tercih edilen firmaların özenli bir şekilde araştırılarak güvenilirliği yüksek olan taraflara verilmesi iyi bir korunma yöntemi olacaktır. Kamu Bilişim Hizmet Alımı Kapsamında Katılımcıların Yetkilendirilmesi Hakkında Yönetmelik kapsamında Sanayi ve Teknoloji Bakanlığı tarafından yetkilendirilen hizmet sağlayıcılarından hizmet alınması gerekmektedir ("Kamu Bilgi ve İletişim Teknolojileri Yatırımları Rehberi", 2022).

Kurumlar, dışarıdan hizmet aldığı firmaları belirli zaman aralıklarıyla değiştirmelidirler: Dışarıdan alınan BT hizmetleri her zaman aynı firmalardan alındığında, gelen çalışanlar her seferinde kritik bilgilere erişebilmekte ve verilere vakıf olabilmektedir. Bu sebeple belirli periyodlarla destek alınan firmalar güvenilir olması şartıyla değiştirilmelidir.

Kurumsal ortamlarda internet trafik kontrolü yapılmalıdır: Günlük olarak internet üzerindeki trafik kontrolü yapılmalı ve çalıntı bilgiler ile yapılmaya çalışılan girişimler kontrol edilmelidir. Başarısız ve çalıntı bilgiler ile yapılmış olan girişimler tespit edilmeli ve engellenmelidir.

Ülke çapında milli yazılım ve donanımların geliştirilmesi ve teşviki yapılmalıdır: Ülkemizde kendi yazdığımız yerli yazılımların sonucunda ortaya çıkmış olan sistemlerin kullanılabilmesi durumunda toplumsal olarak siber kapsamda daha güvenli bir ortam sağlanabilecektir. Aynı zamanda donanımsal olarak da artan siber saldırılar sebebiyle donanım araçlarının da yerli üretiminin teşviki büyük önem teşkil etmektedir. Herhangi bir ulusal saldırı esnasında bu yazılım ve donanım araçlarının yönetimi ve kullanımı açısından

büyük riskler taşımaması adına, ülkemizde kullanılan yazılım uygulamaları ve donanım araçlarının kendi ülkemizde yerli üretiminin ve geliştirilmesinin desteklenmesi özellikle de herhangi bir siber savaş esnasında büyük önem sağlayabilecektir.

Ulusal siber güvenlik strateji ve politikaları oluşturulmalıdır: Ülke genelinde ulusal boyutta etkin bir siber savunma sağlayabilmek için öncelikli olarak Ulusal Siber Güvenlik Stratejisi oluşturulmalı ve bu stratejilerin uygulanması sağlanmalıdır.

Ulusal alanda milli savunma kalkanı, siber ordu vb. tesis edilmelidir: Siber güvenlik henüz tam olarak olgunlaşma sağlayamamış bir yapı konumundadır. Bu konuda güvenlik tedbirleri ve personel sayısı henüz yeterli düzeyde değildir. Her geçen gün giderek artan ve yenilenen tehditler sebebiyle siber güvenlik kapsamında mevcut olan kuruluşlarla koordineli bir şekilde çalışabilecek bir siber oluşum çalışmasına gidilmelidir. Sadece bu sebeple kurulmuş ve siber güvenlik konusuna odaklanmış olan bir yapı sayesinde tehditler için iyi ve güçlü bir otorite sahibi olunabilecektir.

Siber güvenlik alanında konferans ve seminerler düzenlenmeli, yurtdışında gerçekleştirilen organizasyonlara katılım sağlanmalıdır: Ülkemizde siber güvenlik alanında eğitici ve geliştirici olması maksadıyla seminer, konferans, sempozyum vb. çalışmalar düzenli olarak yürütülmelidir. Gelişen teknolojiler takip edilmelidir. Ülkemiz dışında gerçekleşen bu gibi etkinliklere mutlaka katılınmalı, gerekli durumlarda ülkemiz temsil edilmelidir. Diğer ülkelerle siber güvenlik kapsamında dayanışma ve işbirliği içinde olunmalıdır.

Siber güvenlik tatbikatları düzenlenmelidir: Siber güvenlik tatbikatları düzenlenerek görünüşte güvenli olduğu düşünülen kritik sistemlerin açıklarının ortaya çıkarılabilmesi ve tatbikat sonucunda gerekli derslerin alınarak uygun ve alınması gerektiği öngörülen tedbirlerin alınması bakımından oldukça önemlidir.

Uluslararası işbirliği yapılmaya çalışılmalıdır: Ülkemiz, siber güvenlik alanında devletlerarası işbirliği yaparak bu alandaki güncel çalışmaları yakından takip etmeli ve gerekli çalışmalara dahil olmalıdır.

Yeterli miktarda nitelikli insan kaynağı yetiştirilmelidir: Siber güvenlik kapsamında gereksinim halinde olduğumuz nitelikli, bilgili ve donanımlı insanların yetiştirilmesi önemli bir gereksinim haline gelmiştir. Devlet tarafından gerekli teşvik adımları atılmalıdır. Geleceğe yönelik siber saldırıların önlenmesi bakımından oldukça önemlidir.

Siber güvenliği sağlamaya yönelik dersler okullarda verilmelidir: Siber güvenliğin önemi gözardı edilemez bir hal almıştır. Bu sebeple ilkokul hayatından başlamak

kaydıyla siber alanda güvenliğin sağlanmasını hedefleyen bilinçlendirici dersler verilmeli, yerli ve milli yazılımlar geliştirme amacıyla ise de kodlama gibi yazılım derslerini müfredatlara ekleyerek gelecek nesillerde bu ihtiyacı karşılayabilmek adına adımlar atmak gerekmektedir.

Siber saldırıların azaltılmasına yönelik hukuki düzenlemeler yapılmalıdır: Siber saldırganların planladıkları saldırıları azaltabilmek amacıyla caydırıcı önlemler alınması maksadıyla hukuki alanda düzenlemeler yapılmalı, kapsamlı ve güncel olarak caydırıcı bir yasal altyapı oluşturulmalıdır.

SONUÇLAR VE ÖNERİLER

Bu bölümde “Sonuçlar” ve “Öneriler”e ilişkin bilgiler yer almaktadır. Bölüm iki alt başlık altında açıklanmaktadır.

Sonuçlar

Günümüzde teknolojinin gelişimi tahmin edilemez bir hızla ilerlemekte ve hayatlarımıza yenilikler getirmektedir. Hem bireysel hem de kurumsal alandaki yenilikler birçok kolaylığı da beraberinde getirmiştir. Öyle ki artık sağlık, iletişim, turizm, ulaşım, eğitim, haberleşme, bankacılık ve neredeyse akla gelen her türlü bireysel, kurumsal ve ulusal sistemin altyapısı, bilgi teknolojileri üzerine inşa edilmiştir. Hal böyle olunca, bu gibi kritik altyapıların korunmasını sağlayabilmek amacıyla siber güvenlik kavramı önemini günden güne daha da artırmaktadır.

Siber güvenliğin sağlamış olduğu kolaylıkların yanısıra bu denli önemli verilerin güvenliğini, sürekliliğini ve korunabilmesini sağlayabilmek de büyük önem taşımaktadır. Verilerin dijital ortamda olması, güvenlik açıklarının oluşmasına neden olmuştur. Dolayısıyla bu durum, sistemlerin kötüye kullanımı ve suçların işlenebileceği yeni bir alan oluşmasına da sebebiyet vermiştir. Siber ortamda yapılabilecek saldırılar her alanda ciddi ölçüde büyük zararlar verebilmekte olup sonuçları kaos ortamı oluşturabilecek kadar güçlü hale gelmiş bulunmaktadır.

Kontrol etmenin oldukça zor hale geldiği bilgi ve iletişim teknolojilerinin gelişimi, beraberinde güvenliğe duyulan ihtiyacı da ortaya çıkarmaktadır. Siber tehditler, nereden ve nasıl geleceği saptanamayan, tahmin edilemeyen bir problem olarak karşımıza çıkmaktadır. Gelişen teknoloji sebebiyle siber korsanlar da sürekli olarak yeni saldırı çeşitleri üretebilmektedir. Durum böyle olunca siber güvenliğin sağlanabilmesi sorunu hızla ilerlemekte olan bir problem haline gelmiştir. Görüldüğü üzere siber güvenlik kavramı herkesin üzerinde durması gereken bir konu olarak ön plana çıkmaktadır.

Siber uzay, teknolojiyle de paralel olarak 21. yüzyılın başlarından itibaren gelişmeye başlamıştır. Bu gelişimle beraber siber uzayın güvenliği ciddi bir problem olarak görülmüş ve gerekli tedbirlerin alınması gerektiği farkedilmiştir.

Siber saldırı türleri saldırganlar tarafından sürekli olarak geliştirilmekte, artmakta ve güncellenmektedir. Saldırı çeşitleri, sadece bilgisayarlar üzerinden değil sosyal

mühendislik yöntemleriyle de yapılabilmektedir. İnsan faktörü siber güvenlikte en önemli faktördür. Aynı zamanda insan faktörünün en zayıf halka olduğu da akıllardan çıkmamalıdır. Sistemler tarafından her türlü önlem alınsa dahi insanların yapabileceği en ufak bilinçsiz bir eylem; büyük, olumsuz ve bazen geri dönüşü mümkün olmayan sonuçlar doğurabilmektedir.

İnternet hayatlarımızda sadece sosyal medya hesaplarını kullanmak, eğlenceli oyunlar oynamak ve siteler arasında gezinmek gibi faaliyetler olmaktan çıkmış; siber alanda savaşların gerçekleştiği, devletlerin gizli ve kritik bilgilerini sakladığı, ulusal savunma stratejilerinin geliştirildiği, kişisel ve özel birçok işlemin gerçekleştirildiği oldukça önemli bir ortam haline gelmiştir.

İçinde bulunulan pandemi döneminin etkisiyle, uzaktan çalışma yöntemine hızlı bir şekilde geçiş yapılarak adapte olunması gerekmiştir. Hem özel hem kamu kurumları bu sisteme zorunlu bir şekilde geçmek durumunda kalmışlardır. Herkesin evlerinde kalması gerektiği böylesi kritik bir dönemde, günlük işlemlerin tamamen dijital ortama aktarıldığı ve neredeyse tüm işlerin evlerdeki bilgisayarlar vasıtasıyla siber ortamda yürütüldüğü gözlemlenmiştir. Siber ortamdaki her bilginin gizliliği, bütünlüğü ve erişebilirliğinin sağlanabilmesi siber güvenliğin amacı olarak bilinmektedir. Bu dönemde işlerin dijital ortamdan yürütülmesini fırsat bilen siber korsanlar, saldırılarına daha da yoğun bir şekilde devam etmişlerdir. Yaşanılan bu durum içinden geçtiğimiz zorlu günlerde yeniden siber güvenliğin önemini gözler önüne sermiştir.

Günümüzde yapay zeka sayesinde robotlar geliştirilmiş, yüz ve parmak izi tanıma gibi insanların en özel ve ayırt edici özelliklerini bile depolamaya başlayan bir ortam haline gelmiştir. İçlerinde yaşadığımız evler bile akıllı evler olarak nitelendirilmeye başlanmıştır. İnsan hayatının neredeyse her alanında karşısına çıkan bu denli önemli bir konunun güvenliğinin sağlanamaması halinde yaşanabilecek olumsuzluklar oldukça ciddi ve ağır zararlar verebilecek kapasitededir.

Hayatı ve iş yükünü kolaylaştırmak amacıyla hemen hemen tüm devlet işleri elektronik ortamdan yapılmakta ve veriler dijital ortamda saklanmaktadır. Enerji santralleri, ulaşım, elektrik, iletişim, haberleşme, doğalgaz gibi kritik altyapıların yönetimi, bilgi ve iletişim sistemleri kullanılarak yapılmaktadır. Bu durum siber güvenliğin ve siber savunmanın ne kadar önemli olduğunu bir kez daha açığa çıkarmaktadır.

Siber alandaki saldırılar, sürekli artmakta olup farklı boyutlara evrilebilmektedir. Siber saldırganlar kurbanların banka hesaplarını ele geçirebilmekte, kişisel verilerini çalabilmekte, ülkelerin toplumlarına sağladığı yol, su, elektrik, enerji vb. kaynakların yönetimini ele geçirerek kötü amaçlarla kullanabilemektedir. Kurumların verilerini siber

ortam vasıtasıyla ele geçirip gizli bilgilerini sızdırabilmektedir. Bunun yanısıra imaj zedelenmesine neden olabilmektedir. Bireylerin ve kurumların siber ortama olan zorunlu bağlılığı, büyük tehditlere yol açabilmektedir.

Siber güvenlik alanında en önemli ve aynı zamanda en zayıf halka olan insan unsurunun önemi göz ardı edilmemelidir. Günümüzde sosyal medya platformlarının durdurulamayan gelişimi ile birlikte, sosyal medyanın neredeyse her yaş grubundan kullanıcılarının olduğu ve hemen hemen herkesin kolay bir şekilde erişebildiği bir ortam olması sebebiyle; sosyal mecralar siber risklerin en fazla olduğu ortamların başında sayılmaktadır. Sosyal medya vasıtasıyla küçük çocukların kandırılması, farkındalığı olmayan bireylerin duygu sömürüsü yoluyla dolandırılması ve bireylerin aldatılması, son zamanlarda oldukça sık rastlanan bir olay haline gelmiştir. Bireylerin birbirlerine siber zorbalıkta bulunması da günümüzde çok sık karşılaşılan ve mental sağlığı olumsuz yönde etkileyen oluşumların başında gelmektedir. Gözardı edilemeyecek düzeydeki ciddi risklerin yayılım gösterdiği sosyal medya platformlarının kullanımı konusunda toplum bilinçlendirilmesi büyük önem taşımaktadır.

Siber ortamdan gelebilecek saldırıların nereden ve ne şekilde geleceğini kestirebilmek oldukça güçtür. Bu sebeple siber ortam güvenliğinin de tam anlamıyla sağlanabilmesi mümkün olmamakla beraber, güvenlik açıklarının en aza indirgenerek gerekli tedbirlerin alınması büyük fayda sağlayacaktır. Siber güvenlik sadece altyapıların korunması olarak değil bir ülkenin yaşamının devamlılığı, geleceği ve güvenliğinin teminatıdır diye düşünülebilir.

Yaşamın her alanında önümüze çıkan siber saldırılardan korunabilmek amacıyla, riskleri en aza indirebilmek ve tedbir alabilmek için herkesin elini taşın altına koyması gerekmektedir. Alınması gereken araştırılmış bazı önlemler öneriler bölümünde sıralanmıştır.

Öneriler

Bu tez çalışması kapsamında öneri konularını üç temel başlığa ayırabiliriz. Bunlar bireysel, kurumsal ve ulusal alanda incelenecektir. Bireysel alandaki önlem ve öneriler, kurumsal ve ulusal alanda da uyulması gereken her birey için geçerli olan önerilerdir.

Ulusal

- Uluslararası alanda işbirliği diğer ülkeler ile birlikte artırılmalıdır. Siber güvenlik tahmin edilmesi zor ve çok geniş, kapsamlı bir konu olması sebebiyle, diğer ülkeler ile dayanışma ve işbirliği halinde kalınarak üstesinden gelinebilecek bir konu haline gelmiştir.
- Ülkemizdeki yazılım ve donanımlar yerli ve milli seçilmelidir. Gizliliği, kontrol edilebilmesi, erişimi ve yönetimi açısından oldukça önemlidir.
- Siber alanda gerek yurtiçi, gerekse küresel alandaki gelişmeler ve yeni teknolojiler takip edilmeli, konferans, seminer, sempozyum vb. etkinlikler düzenlenmeli, uluslararası alanda yurtdışındaki etkinliklere mutlaka katılım sağlanmalıdır.
- Ulusal siber güvenlik stratejileri ve politikaları oluşturulmalı ve bu stratejilere göre hareket edilmelidir. Daha sistematik ve belirli kurallar içinde çalışılmalıdır.
- Yeterli miktarda ve düzeyde nitelikli insan kaynağı yetiştirilmesi adına teşviklerde bulunulmalıdır. Siber alanda yapılan Araştırma-Geliştirme (AR-GE) çalışmaları desteklenmelidir.
- Siber güvenlik, topluma küçük yaşlardan itibaren aşılanmalı, bilinçlendirilmelidir. Toplumsal alanda eğitimler verilmelidir. İlkokul hayatından itibaren siber güvenlik bilincini ve farkındalığını hedefleyen dersler müfredatlara girmelidir. Yerli ve milli yazılımları desteklemesi amacıyla da yazılım dersleri eklenerek küçük yaşlardan itibaren altyapı oluşturmak gerekmektedir.
- Hukuki açıdan siber saldırıların önüne geçilebilmesi hedeflenmeli ve mevcut yasal altyapı, caydırıcılığını artıracak yönde güncel ve kapsamlı bir hale getirilmelidir. Suç oranlarının azaltılması ve artan siber suç grafiğine müdahale edilmelidir.
- Toplumsal anlamda farkındalık ve bilinçlenmenin sağlanabilmesi için RTÜK ve BTK kurumlarının işbirliği vasıtasıyla kamu spotları oluşturularak sosyal medya ve televizyonlarda yayınlanmalıdır. Siber güvenliğin önemi, siber saldırılardan korunma, sosyal medyanın bilinçli kullanımı, siber zorbalığın önüne geçilmesi vb. konularda kamu spotlarının oluşturulup yayınlanması, siber güvenlik kapsamındaki farkındalığın artmasını sağlayabilecektir.
- Siber alana tahsis edilecek ordu, milli güvenlik kalkanı vb, gibi oluşumlar tesis edilmelidir. Savunma alanında daha güçlü olabilmek hedeflenmelidir. Alınabilecek güvenlik tedbirleri, siber güvenlik alanının henüz yeni ve her geçen gün gelişen bir yapıda olması sebebiyle istenilen düzeyde değildir. Bu alanda çalışan kuruluşların da katkılarıyla güçlü bir

otorite kurulması, ülkemizi daha güçlü ve siber tehditler açısından daha caydırıcı bir hale getirecektir.

- Görünüşte güvenli olduğu düşünülen yapıların açıklarını bulabilmek ve alınması gereken derslerin alınarak iyileştirme sürecine gidilmesi gereken kritik sistemler için siber güvenlik tatbikatları yapılarak gerekli tedbirlerin alınması sağlanmalıdır.

Kurumsal

- Kurumlarda çalışan yetkililer, siber güvenlik alanında personellerinin bilinçlendirilmesi ve farkındalık yaratması açısından eğitimler ve seminerler düzenlemeli; personelin, insan faktörü olarak zayıf halka olması sebebiyle yanlış hamleler yapmasını engellemeye çalışmalıdır. Pandemi döneminde uzaktan çalışmaların da artmasından ötürü personelin her zamankinden daha dikkatli olması gerektiği bu süreçte eğitimin yeri oldukça önemlidir. RTÜK kapsamında ise verilen siber eğitimlerin genişletilerek devam ettirilmesi farkındalık ve bilinçlenme açısından oldukça önemlidir.
- Kurumlarda yer alan kritik sistemler ve altyapıların erişimleri yetkinlendirilmeli, personelin her türlü veriye erişebilmesi yeteneği engellenmeli ve kritik siber ortamların güvenliği sağlanmalıdır.
- Kurumsal bilgisayarlar, çalışan personelin kişisel işlemleri için kullanılmamalıdır. Personelin giriş yaptığı adresler, tehditlerle dolu olabileceğinden kurumsal bilgisayarları riske atmamak gerekmektedir.
- Kurumsal e-posta adresleri, kişisel amaçlarla kullanılan adreslerde kullanılmamalıdır. E-posta adreslerinin siber korsanlar tarafından öğrenilmesi, saldırılarını bu yönde e-posta adresleri üzerinden yapılabilecek oltalama vb. saldırı çeşitlerine çevirmelerine sebebiyet verebilecektir.
- Kurumsal ortamda kritik ve gizli olabilecek veriler şifrelenmeli ve sadece yetkili kişiler tarafından okunabilecek hale getirilmelidir.
- Geçmişteki hataları ve analizleri görebilmek için bilgisayar ve sistemlerde log kayıtları mutlaka açık bırakılmalıdır.
- Güncel siber saldırı yöntemleri takip edilmeli ve alınan önlemler bu güncelliğe göre yenilenmelidir. Bu gibi gelişme ve güncel teknolojilerin takibinin kolaylığı ve maruz kalınmaması açısından farkındalığı için ayrı bir siber ekip kurulmalıdır.

- Pandemi dönemindeki çalışma koşullarının, iş ortamından ev ortamına daha çok taşınması ile birlikte artan riskler sebebiyle uzaktan kurulan bağlantıların güvenli bir ortamda gerçekleştirilmesi zorunluluğu farkedilmektedir. Bu sebeple SSL VPN bağlantısı kurularak işyeri ve ev bilgisayarları arasında güvenli bir bağlantı açılarak yapılan işlemler gerçekleştirilmelidir.
- Kurum dışından alınan BT alanındaki hizmetler tercih edilirken güvenilirliğinden emin olunan Sanayi ve Teknoloji Bakanlığı tarafından yetkinlendirilmiş olan özel firmalar özenle seçilmelidir. Kurumlara ait özel bilgilerin deşifre olmasının önüne geçilmelidir.
- Kurum dışından alınan özel BT hizmetleri veren firmalar sürekli aynı olacak şekilde tercih edilmemelidir. Kurumumuzun bilgilerinin kolay bir şekilde düzenli olarak gözlemlenebilmesinin önüne geçilmelidir.
- Günlük olarak düzenli bir şekilde internet trafiği kontrol edilmeli ve başarısız oturum açma vb. girişimleri denetlenmelidir. Saldırı girişiminde bulunan adresler böylelikle farkedilebilir olabilecektir.
- Siber güvenlik kapsamında kurumlararası işbirlikleri artırılarak gelebilecek olan saldırılara karşı dayanışma içinde kalınmalıdır.

Bireysel

- Bireyler, kullandıkları herhangi bir ortamda parola seçerken parolalarını güçlü ve tahmin edilmesi zor kombinasyonlarda seçmelidirler. Parolalar uzun, farklı karakter ve semboller içeren, büyük-küçük harf bulunduran ve yeterli uzunlukta olan parolalar olmalıdır. Kişiler kendileri ile alakalı tarih, anlamlı bir rakam dizini veya kelime vb. gibi tahmin edilebilmesi kolay ve herkesin aklına gelebilecek standart parola kombinasyonlarını seçmekten kaçınmalıdırlar.
- Kişiler kullandıkları hesapların hepsine aynı parolayı vermemelidir. Ele geçirilen bir hesap olduğunda siber saldırganlar bu şifreyi sistematik bir şekilde diğer platformlarda da deneyebilmektedir. Aynı parola tek bir platformda kullanılmalı, diğer platformların verilerinin de ele geçirilebilirliği engellenmelidir.
- Kullanıcılar parolalarını hiç bir sebeple üçüncü kişilerle paylaşmamalıdır. Farklı sosyal mühendislik becerileri ile ikna olarak kimseyle parolasını, telefonuna gelen herhangi bir güvenlik şifresi vb. bilgileri paylaşmaması gerekmektedir.

- Oturum açma bilgileri gerektiren sayfalarda kullanıcılar, beni hatırla seçeneğini kullanmamalıdır. Aksi halde istenmeyen kişiler tarafından bilgisayarların ele geçirilmesi durumunda oturum bilgileri de ele geçirilmiş olacaktır.
- Belirli ve düzenli periyodlarla kullanıcılar şifrelerini değiştirmelidir. Ele geçirilmiş olan bir şifre olması durumunda değişiklik yaparak önlenmesi daha kolay olacaktır.
- Kullanıcılar, kullanmadıkları hesapları gerekli değil ise kapatmayı tercih etmelidirler.
- Kullanıcıların bilgisayar veya sistemlerinin ilk kez kurulumu yapılırken yetkili kişi tarafından verilmiş olan kullanıcı hesap isimleri daha sonra gizli kalabilmesi açısından kurulum sonrasında değiştirilmelidir.
- Kullanıcılar bilgisayarlarında lisanssız yazılım bulundurmamaya ve kullanmamaya özen göstermelidir. Lisanssız yazılım dosyalarının kurulumu esnasında bu dosya ile bilgisayarlara inebilecek olan kötücül yazılımların varlığı unutulmamalıdır.
- Kullanıcılar bilgisayarlarına mutlaka güvenilir ve kapsamlı bir antivirüs yazılım programı kurmalıdır. Bu programlar yeni teknolojileri ve gelebilecek yeni tür saldırıları çok daha iyi bildiğinden ve bu yeni saldırılara karşı koruma yazılımını güncellediğinden dolayı çok daha güçlü bir şekilde güvenlik sağlamaktadır.
- Sistemlerde kullanılan yazılımların güncellemeleri düzenli olarak, mümkünse ertelemeden gerçekleştirilmelidir. Yeni ve güncel saldırı çeşitlerine karşı yazılımların güncel tutulması ve güncelleme ile gelen güvenlik önlemleri gözardı edilmeden gerekli yeniliklerin yapılması önemlidir.
- Kullanıcılar için önemli ve kritik olduğu düşünülen verilerin, veri kaybını azaltma amacıyla düzenli olarak yedeği alınarak ayrı bir yerde saklanması gerekmektedir. Fiziki olarak da farklı bir ortamda saklanması, başa gelebilecek olan yangın, su basması vb. gibi kötü olaylar için de yerinde bir tedbir olacaktır.
- Kullanıcılar bilgisayarlarını kullanmadıkları zamanlarda, istenmeyen kişiler tarafından görülmesini engellemek maksadıyla mutlaka ekranlarını kapatarak önlem almayı ihmal etmemelidirler.
- Sosyal mühendislik saldırılarına karşı özellikle de kendilerini farklı birileri gibi tanıtıp güven kazanmaya çalışan kişilere karşı tedbirli davranılmalı ve kişisel, kurumsal veya kritik hiçbir bilgi kimseyle paylaşılmamalıdır.
- Kişilere gelen e-posta, mesaj ve sosyal medya üzerinden gönderilen iletilerin kaynağına dikkat edilmelidir. Bireyler tanımadıkları kişilere asla güvenmemeli ve bu iletiler üzerinden herhangi bir bilgi paylaşımında bulunmamalıdırlar.

- Bireyler, kişisel olarak kullandıkları bilgisayar, tablet, telefon, harici bellek gibi fiziki eşyalarının güvenliğine dair tedbirler almalı, herhangi bir şekilde gelişigüzel biryere bırakmamalı ve mümkünse bu gibi cihazlara güçlü parolalar ile şifreleme yapmalıdır. Aynı zamanda bu cihazlar kimse ile paylaşılmamalıdır. Farklı bir bilgisayarda kullanılması durumunda bu cihazlara kötücül yazılım bulaşma riskinin çok yüksek olduğu unutulmamalıdır.
- Kullanıcılar SSL sertifikası bulunmayan internet sayfalarına güvenmemelidir. URL adresinin içeriğinde HTTPS ibaresi olmayan bağlantılara tıklamamalıdır. Güvenliğinin şüpheli olduğu düşünülen bağlantılara girilmemeli ve alışveriş vb. gibi e-ticaret işlemleri için güvenliğinden emin olunmayan adresler kullanılmamalıdır.
- Bilgisayarlarda, kendiliğinden beklenmedik şekilde açılan pencereler engellenmelidir. Bu gibi pencerelerin reklam içerikli ve genellikle potansiyel olarak zararlı yazılımlar içeren sayfalar olduğu unutulmamalıdır.
- Kullanıcılar, sosyal medya hesaplarındaki paylaşımlarında kendilerine ait kişisel özellik ve bilgilerini açığa çıkaracak şekilde paylaşımlar yapmamalıdır. Paylaşılan resimler, resimlere eklenen konum bilgileri, videolar vb. bilgiler dolandırıcılar tarafından kötü amaçlarla kullanılabilmektedir. Hem kişisel hem de iş hayatları ile ilgili bilgilerin sosyal medya hesapları vasıtasıyla tespit edilerek siber saldırganlar veya sosyal mühendisler tarafından kullanılabileceği unutulmamalıdır.
- Sosyal medya kullanıcıları, hesaplarını herkese açık olacak şekilde ayarlamamalıdırlar. Kişisel ipuçları verilmemesi açısından paylaşımlar, sadece arkadaşlara açık olacak şekilde düzenlenmelidir. Tanıdık olmayan kişiler, arkadaş listesine eklenerek yapılan paylaşımların erişimleri açılmamalıdır.
- Kullanıcılara ait akıllı telefonların konum servisleri gerekli olmayan durumlarda kapalı olarak tutulmalıdır. Siber saldırganlar konum bilgilerine erişebilecek nitelikte olabileceğinden saldırılarını buna göre yönlendirebileceği ve değiştirebileceği bilinmelidir.
- Akıllı telefonlara, güvenliğinden emin olunmayan uygulamalar indirilmemeli, bunun yanında kişisel ve telefondaki bilgilere erişim isteğinde bulunan uygulamalara mümkünse izin verilmemelidir.
- Kişisel akıllı telefonlar satılırken veya el değiştirilirken içerisinde varolan tüm bilgiler temizlenmeli ve telefon fabrika ayarlarına döndürülerek yeni kullanıcısına devredilmelidir.
- Sosyal medya hesapları ve e-posta hesaplarının oturum açma bilgilerini girerken giriş yöntemi olarak iki aşamalı doğrulama yöntemi tercih edilmelidir. Böylelikle şifreli girişin

yanısıra kişisel cihazlarımızdan da onay vererek daha güvenli bir şekilde giriş yapabilmeyi sağlamak, siber korsanların saldırı hedeflerinin önüne geçebilecektir.

- Evlerde bulunan modemlerin kullanımı şifreli iletişim olacak şekilde ayarlanmalıdır. Güçlü parolalar seçilmeli ve belirli aralıklarla parolalar değiştirilmelidir. Cihaza ait adres bilgileri dış ortamlardan gizli olacak şekilde ayarlanmalıdır.
- Herkese açık alanlarda sunulan ücretsiz internet bağlantıları, çok acil ve gerekli bir durum olmadıkça kullanılmamalıdır. Unutulmamalıdır ki siber saldırganlar için aynı ağdan saldırı gerçekleştirmek çok daha kolay olabilecektir.

KAYNAKLAR

Ahi, Ş. (2020). Gelişmiş Sosyal Mühendislik Saldırı Analizi ve Tespiti [Yüksek lisans tezi, Gebze Teknik Üniversitesi].

Aile ve Sosyal Politikalar Bakanliğinin Teşkilat Ve Görevleri Hakkinda Kanun Hükmünde Kararname İle Bazi Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapilmasina Dair Kanun. (2014). https://www5.tbmm.gov.tr/kanunlar/k6518.html Erişim tarihi: 12.08.2022

Akarslan, H. (2012). Bilişim suçları (2. bs.). Seçkin Yayınları.

Albayrak, O. (2018). SOME (Siber Olaylara Müdahale Ekibi) Nedir? BGA Security.

Alioğlu, S. D. (2019). Siber Saldırılar ve Ülkelerin Siber Güvenlik Politikaları [Yüksek lisans tezi, İstanbul Bilgi Üniversitesi].

Altınok, E., & Vural, A. F. (2011). Kavramsal Açıdan Bilişim ve Bilişim Suçları. Bilişim Suçları, 75. https://dergipark.org.tr/tr/download/article-file/208853 Erişim tarihi: 05.05.2022

Altınsoy, S., & Çobanoğlu, N. (2020). Ulusal Güvenlik Açisindan Kritik Alt Yapilarin Siber Güvenliği. Global savunma Dergisi.

APWG. (2022). Phishing activity trends reports. APWG | Unifying The Global Response To Cybercrime. https://apwg.org/trendsreports/ Erişim tarihi: 04.06.2022

Arslan, Ö. (2021). Türkiye'nin Siber Güvenlik Politikaları ve Siber Saldırıların Uluslararası Etkileri [Yüksek lisans tezi, Düzce Üniversitesi].

Atatürk Havalimanında Virüs Kabusu. (2009). Habertürk. https://www.haberturk.com/yasam/haber/125013-ataturk-havalimaninda-virus-kabusu Erişim tarihi: 20.07.2022

Aydın, Ö., & Yükçü, S. (2020). Siber Saldırı Önlemede Blokzinciri Teknolojisinin Fayda Maliyet Açısından Değerlendirilmesi. MANAS Sosyal Araştırmalar Dergisi, 9(4), 2523. https://dergipark.org.tr/tr/download/article-file/1112079 Erişim tarihi: 24.07.2022

Ağ Güvenliği Temelleri. (2020, Şubat). CyberMag Dergi. https://www.cybermagonline.com/ag-guvenligi-temelleri Erişim tarihi: 08.03.2022

Belcic, I. (2021, Kasım 19). What is Trojan malware? The ultimate guide. What Is Trojan Malware? The Ultimate Guide. https://www.avast.com/c-trojan Erişim tarihi: 30.05.2022

Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, 24-25.

Bıçakcı, S. (2012). Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu. Uluslararası İlişkiler Dergisi, 9(34), 205-226. https://dergipark.org.tr/tr/pub/uidergisi/issue/39282/462604 Erişim tarihi: 23.07.2022

Bıçakcı, S., Ergun, D., & Çelikpala, M. (t.y.). Türkiye'de Siber Güvenlik ve Nükleer Enerji. https://edam.org.tr/document/CyberNuclear/SiberKitapTR/edam_siber_guvenlik_b2.pdf Erişim tarihi: 26.07.2022

Biju, J. M., Gopal, N., & Prakash, A. J. (2019, March). Cyber Attacks and Its Different Types. International Research Journal of Engineering and Technology (IRJET DERGİ), 6(3), 4851.

Bilen, A. (2021). Akıllı yöntemler ile siber saldırı tespit sistemi geliştirilmesi [Doktora tezi, Fırat Üniversitesi].

Bilgi Güvenliği Derneği Tüzüğü. (2007). https://bilgiguvenligi.org.tr/tuzuk/

Bilisim, R. (2020). Ağ Güvenliği Nasıl Sağlanır? Red Bilişim.

Bizimyer, Ş. (2021, Mayıs 24). Mitm - Man in the middle attack Nedir? - Siber Eğitmen. https://www.siberegitmen.com/man-in-the-middle-attack-nedir/ Erişim tarihi: 15.06.2022

(t.y.). Bursa Uludağ Üniversitesi. Siber Güvenlik Nedir https://uludag.edu.tr/dosyalar/bilgiislem/belgeler/siber_guvenlik_nedir.pdf Erişim tarihi: 22.03.2022

BloombergHt Gazetesi. (2021, Temmuz 7). Akbank: Siber saldırı veya müşteri bilgi güvenliği problemi yok. BloombergHT Gazete. https://www.bloomberght.com/akbank-siber-saldiri-veya-musteri-bilgi-guvenligi-problemi-yok-2283832 Erişim tarihi: 21.07.2022

Bourgeois, D., & Bourgeois, D. T. (2014). Chapter 6: Information systems security – Information systems for business and beyond. Information Systems for Business and Beyond – Simple Book Production. https://bus206.pressbooks.com/chapter/chapter-6-information-systems-security/ Erişim tarihi: 12.03.2022

Böge, S. (2018). Sanal Özel Ağlarda Veri Güvenliği [Yüksek Lisans Tezi]. Karatay Üniversitesi.

Canberk, G., & Sağıroğlu, Ş. (2007). Kötücül ve Casus Yazılımlar-Kapsamlı Bir Araştırma. Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 22(1), 125-126. https://dergipark.org.tr/tr/download/article-file/75575 Erişim tarihi: 02.06.2022

Cengiz, G. (2021). Siber Suçlar, Sosyal Medya ve Siber Etik. İletişim Çalışmaları Dergisi, *7*(3), 412-413. https://doi.org/10.17932/IAU.ICD.2015.006/icd_v07i3001 Erişim tarihi: 10.05.2022

Chapple, M., Bedell, C., & Wright, R. (2021, March 3). What is a computer virus? SearchSecurity.

Choudry, A. (2022). Cyber security basic | Cybersecurity fundamentals for beginners. Edureka. https://www.edureka.co/blog/cybersecurity-fundamentals-introduction-to-cybersecurity/ Erişim tarihi: 12.02.2022

Credential stuffing defense FortiGuard security service. (n.d.). Fortinet. https://www.fortinet.com/support/support-services/fortiguard-security-subscriptions/credential-defense-stuffing Erişim tarihi: 20.06.2022

Dansimp, & Christa. (n.d.). Worms. Developer tools, technical documentation and coding examples | Microsoft Docs. https://docs.microsoft.com/en-us/microsoft-365/security/intelligence/worms-malware?view=o365-worldwide Erişim tarihi: 29.05.2022

Daş, R., Kara, Ş., & Gündüz, M. Z. (t.y.). Casus Yazılımların Bilgisayar Sistemlerine Bulaşma Belirtileri ve Çözüm Önerileri. https://www.bingol.edu.tr/documents/Casus%20Yaz%C4%B1l%C4%B1mlar%C4%B1n%20Bilgisayar%20Sistemlerine%20Bula%C5%9Fma%20Belirtileri%20ve%20%C3%87%C3%B6z%C3%BCm%20%C3%96nerileri.pdf Erişim tarihi: 02.06.2022

Demirol, D., Daş, R., & Baykara, M. (2013, Mayıs). SQL Enjeksiyon Saldırı Uygulaması ve Güvenlik Önerileri. 1st International Symposium on Digital Forensics and Security (ISDFS'13).

Denial of service (Dos) Saldırıları ve Korunma Yöntemleri. (2013). İTÜ (İstanbul Teknik Üniversitesi) Bilgi İşlem Daire Başkanlığı. https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/denial-of-service-(dos)-sald%C4%B1r%C4%B1lar%C4%B1-ve-korunma-y%C3%B6ntemleri Erişim tarihi: 07.06.2022

Dijitalleşen Dünyada Bilişim Suçları ve Mücadele Yöntemleri. (2022). BTK. https://www.btk.gov.tr/uploads/pages/arastirma-raporlari/dijitallesen-dunyada-bilisim-suclari-ve-mucadele-yontemleri.pdf Erişim tarihi: 05.05.2022

Elektronik Haberleşme Kanunu. (2008). T.C Resmi Gazete. https://www.resmigazete.gov.tr/eskiler/2008/11/20081110M1-3.htm Erişim tarihi: 28.07.2022

Eren, M. (2021). Global Siber Güvenlik Politikaları ve Türkiye Özelinde Denetim Açısından Önemi. ISACA. https://politiksoylem.com/wp-content/uploads/2021/04/Global-Siber-Guvenlik-Politikalari-ve-Turkiye-Ozelinde-Denetim-Acisindan-Onemi-1.pdf Erişim tarihi: 17.01.2022

Ermiş, U. (2018, Mayıs). Bir Güvenlik Sorunu Olarak Siber Uzay. TASAM | Bir Güvenlik Sorunu Olarak Siber Uzay. https://tasam.org/tr-TR/Icerik/50249/bir_guvenlik_sorunu_olarak_siber_uzay Erişim tarihi: 31.01.2022

Gantz, J. F., Vavra, T., Lim, V., Soper, P., Smith, L., & Minton, S. (2015). Lisanssız Yazılımlar ve Siber Güvenlik Tehditleri. IDC Analiyze the Future. https://globalstudy.bsa.org/2013/Malware/study_malware_tr.pdf Erişim tarihi: 05.08.2022

Gençöz, T., & Öncül, Ö. (2012). Examination of Personality Characteristics in a Turkish Sample: Development of Basic Personality Traits Inventory. The Journal of General Psychology, 139(3), 194–216.

Gündüz, M. Z., & Daş, R. (t.y.). Sosyal Mühendislik: Yaygın Ataklar ve Güvenlik Önlemleri. Bingöl Üniversitesi. https://www.bingol.edu.tr/documents/Sosyal%20M%C3%BChendislik-yayg%C4%B1n%20Ataklar%20ve%20G%C3%BCvenlik%20%C3%96nlemleri.pdf Erişim tarihi: 05.07.2022

Güner, M. A. (2021). Yaygın Ag Saldırıları ve Genel Hatlarıyla Ag Savunması.

Güven, F. (2022). Siber Saldırılar ve Türk Kamu Yönetiminin Çözümleri [Doktora tezi, Süleyman Demirel Üniversitesi].

Hakkımızda. (t.y.). T.C. İçişleri Bakanlığı Emniyet Genel Müdürlüğü. https://www.egm.gov.tr/siber/hakkimizda2 Erişim tarihi: 02.08.2022

Hakkımızda. (t.y.). Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CBDDO). https://cbddo.gov.tr/hakkimizda/ Erişim tarihi: 03.08.2022

Hatipoğlu, C., & Tunacan, T. (2021). Türkiye'de Siber Saldırı ve Tespit Yöntemleri: Bir Literatür Taraması. Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Dergisi. https://doi.org/10.35193/bseufbd.838732 Erişim tarihi: 22.05.2022

Işık, E. (2021). IP Sahtekarlığı (IP Spoofing) Nedir ve Ne İçin Kullanılır? Teknoportal. https://www.teknoportal.com.tr/ip-sahtekarligi-ip-spoofing-nedir-ve-ne-icin-kullanilir/ Erişim tarihi: 17.06.2022

Kamu Bilgi ve İletişim Teknolojileri Yatırımları Rehberi. (2022). T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı - SBB. https://sbb.gov.tr/wp-content/uploads/2022/07/Kamu_BIT_Yatirimlari_Rehberi-2022.pdf Erişim tarihi: 26.08.2022

KamuNet. (t.y.). T.C. Ulaştırma ve Altyapı Bakanlığı Haberleşme Genel Müdürlüğü. https://hgm.uab.gov.tr/kamu-net Erişim tarihi: 03.08.2022

Kara, I. (2021). Web sitesi tabanlı oltalama saldırılarının adli analizi. Niğde Ömer Halisdemir Üniversitesi Mühendislik Bilimleri Dergisi, 10(2), 450. https://dergipark.org.tr/en/download/article-file/1618219 Erişim tarihi: 04.06.2022

Karabacak, B. (2011). Kritik Altyapılar Dünya ve Türkiye Düzeni. TÜBİTAK BİLGEM, 3(5), 23.

Karadoğan, I. (2016). Ağ İletişiminde Veri Gizleme Tabanlı Bilgi Güvenliği Uygulamaları [Yüksek lisans tezi, Fırat Üniversitesi].

Kaspersky cyberthreat gerçek zamanlı harita. (t.y.). https://cybermap.kaspersky.com/tr Erişim tarihi: 20.05.2022

Kemp, S. (2022, February). Digital 2022: Turkey — DataReportal – Global digital insights. https://datareportal.com/reports/digital-2022-turkey?rq=turkey Erişim tarihi: 15.02.2022

Kirsten, S. (n.d.). Cross site scripting (XSS). OWASP Foundation, the Open Source Foundation for Application Security. https://owasp.org/www-community/attacks/xss/ Erişim tarihi: 21.06.2022

Kolcu, G. (2015). Onlar saldırdı biz fişi çektik. Hürriyet.
https://www.hurriyet.com.tr/teknoloji/onlar-saldirdi-biz-fisi-cektik-40030151 Erişim tarihi: 20.07.2022

Korkutata, Y., & Toprak, Z. F. (t.y.). El-Cezerî ile ilgili yapılan çalışmaların değerlendirilmesi. Mühendislik Dergisi, 4(1), 42. https://dergipark.org.tr/tr/download/article-file/302720 Erişim tarihi: 29.10.2021

Kurbak, E. (2012). Fiziksel Dünyanin Simülasyonu, Düşsel Bir Coğrafya Ya Da Yeni Bir Gerçeklik Olarak Siberuzay [Yüksek lisans tezi, İstanbul Teknik Ünivrsitesi]. https://polen.itu.edu.tr/items/20e2ef47-f792-4bf5-a46b-fc533faf22fc Erişim tarihi: 29.10.2022

Kuruluş. (2017). Bilgi Teknolojileri ve İletişim Kurumu (BTK). https://www.btk.gov.tr/kurulus Erişim tarihi: 28.07.2022

Kurumlarda Bilgi Güvenliği Yönetim Sistemi'nin Uygulanması. (2008). In Akademik Bilişim (s. 511). Çanakkale Onsekiz Mart Üniversitesi. https://ab.org.tr/ab08/kitap/Bildiriler/MCetinkaya_AB08.pdf Erişim tarihi: 26.08.2022

Kurumsal SOME Kurulum ve Yönetim Rehberi. (2014). T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı Haberleşme Genel Müdürülüğü. https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/kurumsal-some-reh-v1.pdf Erişim tarihi: 26.07.2022

Küçükçavdar, M. (2018). Suç Olgusunun Değişen Yüzü: Siber Suçlar. ISophos: Uluslararası Bilişim, Teknoloji ve Felsefe Dergisi, (1), 1-15. https://www.isophos.org/is-cont/uploads/pdf/01/suc-olgusunun-degisen-yuzu-siber-suclar.pdf Erişim tarihi: 07.05.2022

Lathrop, A. J., & Stanisz, J. M. (n.d.). Hackers Are After More than Just Data: Will Your Company's Property Policies Respond When Cyber Attacks Cause Physical Damage and Shut Down Operations? Environmental Claims Journal, 28(4), 291-309.

Leder, F., Werner, T., & Martini, P. (n.d.). Proactive Botnet Countermeasures An Offensive Approach. CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise. https://ccdcoe.org/uploads/2018/10/15_LEDER_Proactive_Coutnermeasures.pdf Erişim tarihi: 12.06.2022

Malware Nedir, Nasıl Temizlenir? - Malware Saldırı Türleri ve Önleme Yöntemleri. (t.y.). Berqnet - Firewall Cihazı ve SASE Platformu.

Menteş, S. (2018). Bilgi Güvenliği Uygulamaları ve Çözüm Önerileri [Uzmanlık tezi, RTÜK].

(2016). Milliyet Gazetesi. https://www.milliyet.com.tr/teknoloji/2023-te-siber-suclarin-turkiye-ye-maliyeti-8-28-milyararasinda-olacak-2325379 Erişim tarihi: 19.07.2022

Microsoft, Rusya'nın Ukrayna'ya siber saldırılarını ortaya çıkardı. (2022). TRT Haber. https://www.trthaber.com/haber/dunya/microsoft-rusyanin-ukraynaya-siber-saldirilarini-ortaya-cikardi-676458.html Erişim tarihi: 02.09.2022

Netpro. (2020). Fidye Yazılımları Nedir? Nasıl Çalışır? (Ransomware). Netpro Bilgisayar. https: //www.netpro.com.tr/fidye-yazilimlari-nedir-nasil-calisir-ransomware/ Erişim tarihi: 10.09.2022

Orak, M. (2021). Siber Ordular ve Siber Savaşlar. Kaytek Dergisi, 3(2), 214-226. https://dergipark.org.tr/en/download/article-file/2194137 Erişim tarihi: 03.08.2022

Pande, J. (2017). Introduction to Cyber Security. Uttarakhand Open University. https://uou.ac.in/sites/default/files/slm/Introduction-cyber-security.pdf Erişim tarihi: 29.05.2022

Phishing Activity Trends Report, 1st Quarter 2022. (2022). APWG.

Ring, T. (2015). Russian Information Operations and the Rise of the Global Internet [Yüksek lisans tezi, University of Washington].

Sack, H. (2021, November 10). Fred Cohen and the first computer virus. SciHi Blog. https://scihi.org/fred-cohen-computer-virus/ Erişim tarihi: 25.05.2022

Sağıroğlu, Ş., & Alkan, M. (2018). Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık. Grafiker Yayıncılık. https://www.sasad.org.tr/uploaded/Siber-Guvenlik-ve-Savunma-Farkindalik-ve-Caydiricilik.pdf Erişim tarihi: 01.06.2022

Seren, M. (2016). Siber Tehditlerle Mücadelede Farkındalık ve Hazırlık. Seta | Siyaset, Ekonomi ve Toplum Araştirmalari Vakfi, (183), 21-22. https://setav.org/assets/uploads/2016/12/SiberGu%CC%88venlikAnaliz.pdf Erişim tarihi: 19.07.2022

Sertçelik, A. (2015). Siber Olaylar Ekseninde Siber Güvenliği Anlamak. Medeniyet Araştırmaları Dergisi, 2(3), 35. https://dergipark.org.tr/tr/download/article-file/506640 Erişim tarihi: 21.07.2022

Siber Güvenlik Dairesi Başkanlığı. (t.y.). Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. https://cbddo.gov.tr/hizmet-birimlerimiz/siber-guvenlik-dairesi-baskanligi/ Erişim tarihi: 03.08.2022

Siber Güvenlik Enstitüsü. (t.y.). TÜBİTAK BİLGEM. https://sge.bilgem.tubitak.gov.tr/tr/kurumsal/sge-tarihcesi Erişim tarihi: 29.07.2022

Siber Güvenlik Kurulu. (2017). Bilgi Teknolojileri ve İletişim Kurumu (BTK). https://www.btk.gov.tr/siber-guvenlik-kurulu Erişim tarihi: 26.07.2022

What is Cyber Security? (2022). www.kaspersky.com.tr. https://www.kaspersky.com.tr/resource-center/definitions/what-is-cyber-security Erişim tarihi: 11.01.2022

Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık (1. bs.). (2018). Grafiker Yayınları. https://www.sasad.org.tr/uploaded/Siber-Guvenlik-ve-Savunma-Farkindalik-ve-Caydiricilik.pdf Erişim tarihi: 02.05.2022

Siber Güvenliğe İlişkin Temel Bilgiler. (2014). USOM. https://some.sdu.edu.tr/assets/uploads/sites/408/files/siber-guvenlige-iliskin-temel-bilgiler-22092017.pdf Erişim tarihi: 30.05.2022

Sivri, T. (2021, Aralık). Credential stuffing Saldırılarını Nasıl Tespit Edebilirsiniz? BGA Security. https://www.bgasecurity.com/2021/12/credential-stuffing-saldirilarini-nasil-tespit-edebilirsiniz/ Erişim tarihi: 20.06.2022

Srinivasan, F., & Simna, S. (2017). Disaster Recovery, An Element of Cyber Security- A Flick Through. International Journal of Management (IJM), 8(4), 125-130. https://iaeme.com/MasterAdmin/Journal_uploads/IJM/VOLUME_8_ISSUE_4/IJM_08_04_016.pdf Erişim tarihi: 19.03.2022

Tanıtım. (t.y.). TBD Türkiye Bilişim Derneği. https://www.tbd.org.tr/calisma-gruplari/kamu-bib-calisma-grubu/tanitim/ Erişim tarihi: 02.08.2022

Topalov, t. (2015). An Overview of Essential Security Measures for Competitive Organizations. İnquiries Journal, 7(10), 1. http://www.inquiriesjournal.com/articles/1269/an-overview-of-essential-security-measures-for-competitive-organizations Erişim tarihi: 21.02.2022

Tosun, A. (2015). A Survey About The Integration Of Social Engineering Attacks With Cyber Security Exploiting Turkish Vulnerabilities In Turkey [Yüksek lisans tezi, Orta Doğu Teknik Üniversitesi].

Touhid. (2019, March 8). Six key elements of cybersecurity. Cyber Threat & Security Portal. https://cyberthreatportal.com/elements-of-cybersecurity/ Erişim tarihi: 09.02.2022

Türkiye, Global Siber Güvenlik Endeksi'nde Avrupa'da 6'ncı. (2021). Ulusal Siber Olaylara Müdahale Merkezi - USOM. https://www.usom.gov.tr/duyurular/turkiye-global-siber-guvenlik-endeksinde-avrupada-6nci Erişim tarihi: 26.07.2022

Tüzük. (t.y.). TBD Türkiye Bilişim Derneği. https://tbd.org.tr/kurumsal/tuzuk/ Erişim tarihi: 29.07.2022

Ulusal Siber Güvenlik Stratejisi Eylem Planı 2020-2023. (2020). T.C Ulaştırma ve Altyapı Bakanlığı UAB. https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf Erişim tarihi: 02.08.2022

USOM Hakkında. (t.y.). Ulusal Siber Olaylara Müdahale Merkezi - USOM. https://www.usom.gov.tr/hakkimizda Erişim tarihi: 27.07.2022

USOM ve Kurumsal Siber Olaylara Müdahale Ekibi. (2017). Bilgi Teknolojileri ve İletişim Kurumu. https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi Erişim tarihi: 28.07.2022

USOM. (t.y.). İstanbul Bilgi Üniversitesi. https://it.bilgi.edu.tr/tr/guvenlik/usom/ Erişim tarihi: 27.07.2022

Veri İhlali Maliyetleri, Pandemi Sırasında Rekor Düzeye Ulaştı. (2021, August 19). CyberMag Dergi. https://www.cybermagonline.com/veri-ihlali-maliyetleri-pandemi-sirasinda-rekor-duzeye-ulasti Erişim tarihi: 11.01.2022

Virus attack strikes at both Istanbul airports. (2013). Hürriyet Daily News. https://www.hurriyetdailynews.com/virus-attack-strikes-at-both-istanbul-airports-51449 Erişim tarihi: 20.07.2022

Vlajic, N., Chowdhury, M., & Litoiu, M. (2019). IP spoofing in and out of the public cloud: From policy to practice. Computers, 8(4), 2. https://doi.org/10.3390/computers8040081 Erişim tarihi: 17.06.2022

Vural, Y. (2007). Kurumsal Bilgi Güvenliği ve Sızma (Penetrasyon) Testleri [Yüksek lisans tezi, Gazi Üniversitesi].

Vural, Y., & Sağıroğlu, Ş. (2010). Veritabanı Yönetim Sistemleri Güvenliği: Tehditler ve Korunma Yöntemleri. Politeknik Dergisi, 13(2), 76.

WannaCry fidye yazılımı nedir? (2021). Kaspersky. https://www.kaspersky.com.tr/resource-center/threats/ransomware-wannacry Erişim tarihi: 02.06.2022

What is cross site scripting (XSS) and how does it work? (2022, July 18). Synopsys | EDA Tools, Semiconductor IP and Application Security Solutions. https://www.synopsys.com/glossary/what-is-cross-site-scripting.html Erişim tarihi: 21.06.2022

What is email spam and how to fight it? (2021). SearchSecurity. https://www.techtarget.com/searchsecurity/definition/spam Erişim tarihi: 22.06.2022

What is information security | Policy, principles & threats | Imperva. (2022). Learning Center. https://www.imperva.com/learn/data-security/information-security-infosec/ Erişim tarihi: 21.02.2022

What is information security? (2022). GeeksforGeeks. https://www.geeksforgeeks.org/what-is-information-security/#:~:text=Information%20Security%20is%20basically%20the,be%20physical%20or%20electronic%20one Erişim tarihi: 21.02.2022

What is network security? (n.d.). Cisco. https://www.cisco.com/c/en/us/products/security/what-is-network-security.html Erişim tarihi: 07.03.2022

What is operational security? OPSEC explained. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/operational-security Erişim tarihi: 26.04.2022

Whitaker, A. (2009). Top 10 social engineering tactics | #10. Social engineering in reverse. InformIT: The Trusted Technology Source for IT Pros and Developers. https://www.informit.com/articles/printerfriendly/1350956 Erişim tarihi: 06.07.2022

XSS güvenlik açığı. (t.y.). SecroMix – SeeWhat'sNext. https://secromix.com/blog/xss-guvenlik-acigi/ Erişim tarihi: 21.06.2022

Yalçın, N., & Avşar, A. (2018). Sosyal Mühendislik Atakları Ve Alınması Gereken Önlemler. 20. Akademik Bilişim 2018 Konferansı Bildirileri – Karabük Üniversitesi. http://indexive.com/uploads/papers/pap_indexive15949787772147483647.pdf Erişim tarihi: 06.07.2022

(2007). Yeni Şafak Gazetesi. https://www.yenisafak.com/gundem/5-bin-mit-ajani-desifre-mi-oldu-62068 Erişim tarihi: 19.07.2022

Ylli, E., & Fejzajb, J. (2021). Man in the Middle: Attack and Protection.

Yücel, T. (2021). Bilgi Güvenliği Derneği Yönetim Kurulu Başkanı Taha Yücel İle Söyleyişi. Cybermag tarafından yapılan röportaj.

Yüksel, M., & Öztürk, N. (2017). SIP Saldırıları ve Güvenlik Yöntemleri. Bilişim Teknolojileri Dergisi, 10(3), 304. https://doi.org/10.17671/gazibtd.331042 Erişim tarihi: 14.06.2022

Yıldırım, E. Y. (2018). Bilişim Sistemlerine Yönelik Siber Saldırılar ve Siber Güvenliğin Sağlanması. 2nd International Vocational Science Symposium [Symposium]. IVSS

Yılmaz, M. (t.y.). Dünyada Ve Türkiye'de Siber Güvenlik gerçekleri-1: İstatistikler, Analizler, Öngörüler. https://www.cubeincubation.com/blog/dunyada-ve-turkiyede-siber-guvenlik-gercekleri-1-istatistikler-analizler-ongoruler Erişim tarihi: 14.05.2022

Yılmaz, O. (t.y.). Küreselleşme Sürecinde Dönüşen Güvenlik Algısı ve Siber Güvenlik Dergipark. https://dergipark.org.tr/en/download/article-file/418736 Erişim tarihi: 22.05.2022

Çelik, Ş. (2013). Stuxnet Saldirisi ve Abd'nin Siber Savaş Stratejisi: Uluslararasi Hukukta Kuvvet Kullanmaktan Kaçinma İlkesi Çerçevesinde Bir Değerlendirme. Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 15(1), 148. https://hukuk.deu.edu.tr/dosyalar/dergiler/dergimiz-15-1/senercelik.pdf Erişim tarihi: 18.07.2022

Özdemir, S., & Şahin, Ş. (t.y.). Siberuzay Nerede? Pivolka Dergi, 4(19), 7. https://www.elyadal.org/pivolka/19/PiVOLKA_19_01.pdf Erişim tarihi: 29.10.2021

Özel, A., & Eken, S. (2014, Ekim). Javacsript Güvenlik Açıkları ve Güncel Çözüm Önerileri. 7. Uluslar Arası Bilgi Güvenliği ve Kriptoloji Konferansı, İstanbul.

Özkaya, E. (2020). Siber Güvenlik Saldırı & Savunma çeşitleri. Buzdağı Yayınevi.

Ünal, C., & Şahin, I. (2017). İstenmeyen Elektronik Postaların (SPAM) Filtrelenmesi için Bir Uzman Sistem Tasarımı ve Gerçekleştirilmesi. Politeknik Dergisi, 20(2), 269. Dergipark https://dergipark.org.tr/tr/download/article-file/385860 Erişim tarihi: 21.06.2022

Ünver, M. (2016). Türkiye'de Siber Güvenlik. CyberMag Dergisi, (1), 20.

Ünver, M. (n.d.). Türkiye'de Siber Güvenlik. Bilgi Güvenliği Derneği. https://www.academia.edu/24842186/T%C3%BCrkiyede_Siber_G%C3%BCvenlik Erişim tarihi: 26.07.2022

Ünver, M., Canbay, C., & Günaydın, Y. (2011). Köle Bilgisayar ve Köle Bilgisayar Ağları. Bilgi Teknolojileri ve İletişim Kurumu (BTK).

Şahinaslan, Ö. (2013). Siber Saldırılara Karşı Kurumsal Ağlarda Oluşan Güvenlik Sorunu Ve Çözümü Üzerine Bir Çalışma [Doktora tezi, Trakya Üniversitesi].

Şenol, M. (2016). Siber Güçle Caydırıcılık Ama Nasıl? Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 2(2), 13. https://dergipark.org.tr/tr/download/article-file/290469 Erişim tarihi: 21.07.2022

"DDos El Kitabı" Bilgi Teknolojileri ve İletişim Kurumu-Telekomünikasyon İletişim Başkanlığı. (2014). Ulusal Siber Olaylara Müdahale Merkezi (USOM-TRCERT). https://dsy.usom.gov.tr/usom/19/02/190211084034_DDoS%20El%20Kitabi.pdf Erişim tarihi: 07.06.2022

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı ve Soyadı : Pelin SAYICI GÜLER

E-Posta Adresi : pelinsayiciguler@rtuk.gov.tr

İş Deneyimi :

Unvan	**Görev Yeri**	**Yıl**
Üst Kurul Uzman Yardımcısı	RTÜK	2019 - …

Akademik Bilgiler

Öğrenim Durumu:

Derece	**Bölüm/Program**	**Üniversite**	**Yıl**
2.36	Bilgisayar Mühendisliği	Süleyman Demirel Üniversitesi	2011-2016

RTÜK