T.C.

RADYO VE TELEVİZYON ÜST KURULU

MOBİL İLETİŞİM DÜNYASINDA SİBER GÜVENLİK TEHDİTLERİ VE SALDIRILARLA MÜCADELE YÖNTEMLERİ

UZMANLIK TEZİ

MERT BAHADIR KAYA

ANKARA

EKİM,2024


RTÜK
RADYO VE TELEVİZYON ÜST KURULU

T.C.

RADYO VE TELEVİZYON ÜST KURULU

MOBİL İLETİŞİM DÜNYASINDA SİBER GÜVENLİK TEHDİTLERİ VE SALDIRILARLA MÜCADELE YÖNTEMLERİ

UZMANLIK TEZİ

MERT BAHADIR KAYA

DANIŞMAN: ÜST KURUL UZMANI

İBRAHİM ESER

ANKARA
EKİM, 2024

Radyo ve Televizyon Üst Kurul Başkanlığı'na

Mert Bahadır KAYA adlı Üst Kurul Uzman Yardımcısının hazırladığı "**Mobil İletişim Dünyasında Siber Güvenlik Tehditleri ve Saldırılarla Mücadele Yöntemleri**" başlıklı bu çalışma Tez Değerlendirme Komisyonu üyelerince oy birliği/oy çokluğu ile Uzmanlık Tezi olarak kabul edilmiştir

Komisyon Üyeleri		İmza
Başkan	……	……..
Üye	……	……..
Üye	……	……..
Üye	……	……..
Üye	……	……..

ONAY

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

Ebubekir ŞAHİN
Üst Kurul Başkan

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. 11/10/2024

MERT BAHADIR KAYA

TEŞEKKÜR

Bu çalışmada, konu seçiminden başlamak üzere tüm süreçte görüşleri, katkıları ve yönlendirmeleriyle benden desteğini esirgemeyen saygıdeğer tez danışmanım Üst Kurul Uzmanı Sayın İbrahim ESER'e, yardımlarını ve desteklerini hiç eksik etmeyen değerli çalışma arkadaşımlarım Üst Kurul Uzmanı Sayın Burcu Ezgi VERGİLİ'ye, Üst Kurul Uzman Yardımcısı Sayın İlker EROL'a ve Mühendis Sayın Hacı Veli KÖSE'ye, teşekkürlerimi sunarım.

ÖZET

MOBİL İLETİŞİM DÜNYASINDA SİBER GÜVENLİK TEHDİTLERİ VE SALDIRILARLA MÜCADELE YÖNTEMLERİ

KAYA, Mert Bahadır

Üst Kurul Uzmanlık Tezi

Tez Danışmanı: Üst Kurul Uzmanı İbrahim Eser

Ekim 2024, 98

Mobil iletişim, modern toplumun vazgeçilmez bir parçası haline gelmiştir. Günümüzde akıllı telefonlar ve tabletler gibi mobil cihazlar, bireylerin günlük yaşamlarında ve iş süreçlerinde sürekli olarak kullandığı araçlardır. Bu cihazlar sayesinde internet erişimi, sosyal medya, çevrimiçi bankacılık ve çeşitli uygulamalar üzerinden gerçekleştirilen işlemler kolaylaşmıştır. Ancak, mobil cihazların bu denli yaygınlaşması ve önemli verilerin bu cihazlarda saklanması, siber güvenlik tehditlerinin de artmasına neden olmuştur. Mobil iletişimdeki bu hızlı büyüme ve gelişim, siber güvenlik önlemlerinin de aynı hızda gelişmesini zorunlu kılmaktadır.

Çalışma kapsamında, İkinci Bölümde iletişimin tanımından başlanarak, temel iletişim teknolojilerine değinilmiştir. Çalışmanın araştırma kısmı olan Üçüncü ve Dördüncü Bölümlerinde ise literatür taraması yapılarak, mevcut mobil siber güvenlik tehditleri incelenmiş, bu tehditlere karşı önlem alınması noktasında oluşturulmuş kuruluşlar ve standartlar ortaya konulmuştur. Beşinci Bölümde ise tüm bu literatür değerlendirilmiş ve gerekli öneriler yapılmıştır.

Anahtar Kelimeler: Mobil iletişim, mobil siber güvenlik, veri koruma, oltalama, siber güvenlik standartları, ağ güvenliği.

ABSTRACT

CYBERSECURITY THREATS IN THE MOBILE COMMUNICATION WORLD AND METHODS TO COMBAT ATTACKS

Kaya, Mert Bahadır

Specialization Thesis

Thesis Advisor: İbrahim ESER, Supreme Board Expert

October 2024, 98

Mobile communication has become an indispensable part of modern society. Nowadays, mobile devices such as smartphones and tablets are tools that individuals constantly use in their daily lives and business processes. Thanks to these devices, tasks performed through internet access, social media, online banking and various applications have become easier. However, the widespread use of mobile devices and the storage of important data on these devices have led to an increase in cybersecurity threats. The rapid growth and development in mobile communication necessitate the equally rapid development of cybersecurity measures.

In this study, the second chapter begins with the definition of communication and addresses fundamental communication technologies. In the third and fourth chapters, which constitute the research part of the study, a literature review is conducted to examine existing mobile cybersecurity threats, and organizations and standards established to counter these threats are presented. In the fifth chapter, all this literature is evaluated, and necessary recommendations are made.

Key Words: mobile communication, mobile cybersecurity, data protection, phishing, cybersecurity standarts, network security.

İÇİNDEKİLER

Sayfa

ETİK İLKELERE UYGUNLUK BEYANI iii

TEŞEKKÜR iv

ÖZET v

ABSTRACT vi

İÇİNDEKİLER vii

TABLOLAR DİZİNİ xii

ŞEKİLLER DİZİNİ xiii

KISALTMALAR xiv

BÖLÜM 1 1

GİRİŞ 1

Problem 1

Amaç 1

Önem 2

Sınırlılıklar 2

Tanımlar 2

YÖNTEM 2

Araştırmanın Modeli 3

Evren ve Örneklem 3

Verilerin Toplanması 3

Verilerin Çözümlenmesi 3

BÖLÜM 2 4
ELEKTRİKSEL İLETİŞİM VE SİBER GÜVENLİĞİ 4
2.1. Elektriksel İletişim 4
2.1.1. Elektriksel İletişimin Ortaya Çıkışı ve Tarihsel Gelişimi 5
2.2. Mobil İletişimin Tanımı 6
2.3. Temel Mobil İletişim Teknolojileri ve Kavramları 7
2.4. Mobil İletişimde Siber Güvenliğin Önemi 9
2.5. Kablolu ve Kablosuz İletişimin Avantaj ile Dezavantajları 11
BÖLÜM 3 14
MOBİL İLETİŞİMDE SİBER SALDIRI VE ÖRNEK VAKALAR 14
3.1.Siber Saldırı Yöntemleri 14
3.1.1 Zararlı Yazılımlar 15
3.1.1.1. Virüsler 16
3.1.1.2. Solucanlar 17
3.1.1.3. Trojanlar 17
3.1.1.4. Casus Yazılım 18
3.1.1.5. Reklam Yazılımı 18
3.1.1.6. Fidye Yazılımı 19
3.1.1.7 Kök Kullanıcı Kiti 19
3.1.2. Son kullanıcı Oltalama ve Kimlik Avı Saldırıları 20
3.1.3. Ağ sistemleri Saldırı Türleri 23
3.1.3.1. Aradaki Adam Saldırıları 23

3.1.3.2. Hizmet Engelleme Saldırıları 24
3.1.3.3. Dağıtık Hizmet Engelleme Saldırıları 24
3.1.3.4. Ölüm Pingi Saldırısı 26
3.1.5.3. Smurf Saldırısı 26
3.1.3.6. DNS Maskeleme Saldırısı 27
3.1.3.7. Paket Dinleme Saldırısı 28
3.1.3.8. ARP Maskeleme 28
3.1.3.9. Oturum Kaçırma 30
3.1.3.10. Çapraz Site Betikleme ve Çapraz Site İstek Sahteciliği: 30
3.1.3.11. DNS Yansıtma 31
3.1.3.12. Port Tarama ve Parmak İzi Alma 33
3.1.3.13. SQL Enjeksiyonu 34
3.1.3.14 MAC Maskeleme: 35
3.1.3.15. Sıfırıncı Gün: 36
3.2. Örnek Vaka Analizleri 39
3.2.1. Pegasus Yazılımı 39
3.2.2. Blueborne Zayıflığı 40
3.2.3. XcodeGhost 42
3.2.4 HeartBleed Açığı 43
3.2.5. Equifax Veri Sızıntısı 44
4. BÖLÜM 47
ULUSLARARASI KURULUŞLAR VE STANDARTLAR, TEKNOLOJİK ÇÖZÜMLER 47

4.1. Uluslararası Kuruluşlar ve Standartlar 47
4.1.1. Ulusal Standartlar ve Teknoloji Enstitüsü 48
4.1.2. Avrupa Birliği Siber Güvenlik Ajansı 49
4.1.3. Uluslararası Standartlar Örgütü 50
4.1.4. Siber Güvenlik ve Altyapı Güvenliği Ajansı 51
4.1.5. Internet Güvenliği Merkezi 52
4.1.6. Bilgi Komiserliği Ofisi 52
4.1.7. Avrupa Telekomünikasyon Standartları Enstitüsü 53
4.1.8. NSS Labs 54
4.1.9. Gartner 55
4.1.10. Elektrik ve Elektronik Mühendisleri Enstitüsü 55
4.2. Teknolojik Çözümler 56
4.2.1. Geleneksel Savunma Yöntemleri 57
4.2.1.1. Güvenlik Duvarları 57
4.2.1.2. Mobil Cihaz Yönetimi 58
4.2.1.3. Veri Kaybı Önleme 61
4.2.1.4. Uç Nokta Tespit ve Yanıt / Genişletilmiş Tespit ve Yanıt 62
4.2.1.6. Saldırı Tespit Sistemi / Saldırı Önleme Sistemi 64
4.2.1.7. Güvenlik Bilgi ve Olay Yönetimi 65
4.2.1.8. Sanal Özel Ağ 66
4.2.1.9. Ağ Erişim Kontrolü 67
4.2.2. Yenilikçi Savunma Prensipleri 68

4.2.2.1. Yapay Zeka ve Davranışsal Analiz 69
4.2.2.2. Blockchain 69
4.2.2.3. İleri Düzey Kimlik Doğrulama 70
4.2.2.3.1. Çok Faktörlü Kimlik Doğrulama 71
4.2.2.3.2. Biyometrik Kimlik Doğrulama 71
4.2.2.3.3. Davranışsal Biyometri 72
4.2.2.3.4. Cihaz Tanımlama 72
4.2.2.3.5. Tek Kullanımlık Şifreler 73
4.2.2.4. Uçtan uca şifreleme 73
4.2.2.5. Segmentasyon 73
4.2.2.6. Konteynerleştirme 75
4.2.2.7. Bal Küpleri 76
4.2.2.8. Sıfır Güven Ağ Erişimi 76
BÖLÜM 5 78
SONUÇ VE ÖNERİLER 78
5.1. Sonuçlar 79
5.2. Öneriler 81
KAYNAKLAR 87
ÖZGEÇMİŞ 98

TABLOLAR DİZİNİ

Tablo **Sayfa**

Tablo 1 1G'den 5G'ye Mobil İletişim Teknolojileri Gelişimi 8
Tablo 2 Kablolu ve Kablosuz İletişim Teknolojilerinin Türleri ve Genel Özellikleri 12
Tablo 3 Kablolu ve Kablosuz İletişim Arasındaki Farklar..... 13
Tablo 4 Yakın Tarihteki Kritik Zararlı Yazılımlar..... 16
Tablo 5 Rootkitlerin Temel Çalışma Prensibi 20
Tablo 6 Oltalama Saldırılarının Temel Prensipleri..... 21
Tablo 7 DDoS Saldırı Adımları..... 25
Tablo 8 Temel DNS Yansıtma Saldırısı Süreci..... 32
Tablo 9 EDR ve XDR Teknolojilerinin Temel Farkları..... 63
Tablo 10 IPS ve IDS Sistemleri Arasındaki Farklar..... 65

ŞEKİLLER DİZİNİ

Şekil **Sayfa**

Şekil 1 Temel MITM Saldırı Yöntemi 24
Şekil 2 Örnek bir DDoS Saldırı Görseli 25
Şekil 3 Ölüm Pingi temel saldırı prensibi 26
Şekil 4 Örnek bir Smurf Saldırısı 27
Şekil 5 DNS Maskeleme Saldırısı Gerçekleştirilme Şekli 27
Şekil 6 Paket Dinleme Saldırısı Temel Stratejisi 28
Şekil 7 Örnek ARP Tablosu 29
Şekil 8 ARP Maskeleme 30
Şekil 9 DNS Yansıtma Saldırısı 32
Şekil 10 Port Tarama Yöntemi 33
Şekil 11 Basit bir SQL Enjeksiyon Saldırısı Örneği 35
Şekil 12 MAC Maskeleme Saldırısı Temel Yöntemi 36
Şekil 13 Blueborne Atağının Tespiti 41
Şekil 14 Equifax Sızıntısı Sonrası Kullanıcılara Gelen Oltalama SMS'leri 46
Şekil 15 NIST Siber Güvenlik Çerçevesi 2.0 48

KISALTMALAR

Kısaltma	Açıklama
AIEE	: American Institute of Electrical Engineers
AP	: Access Point
ARP	: Address Resolution Protocol
ARPANET	: Advanced Research Projects Agency Network
BT	: Bilgi Teknolojileri
BYOD	: Bring Your Own Device
CEPT	: European Conference of Postal and Telecommunications
Administrations	
CIA TRIAD	: Confidentiality, Integrity, Availability Triad
CIS	: Central Intelligence Service
CISA	: Cybersecurity and Infastructure Security Agency
CSRF	: Cross-Site Request Forgery
CVE	: Common Vulnerabilities and Exposures
DDoS	: Distributed Denial of Service
DLP	: Data Loss Prevention
DNS	: Domain Name System
DoS	: Denial of Service
EDR	: Endpoint Detection and Response
ENISA	: European Union Agency for Cybersecurity
ETSI	: European Telecommunications Standards Institute
GDPR	: General Data Protection Regulation
GPS	: Global Positioning System
GSM	: Global System for Mobile Communications
HTTP	: Hypertext Transfer Protocol
HTTPS	: Hypertext Transfer Protocol Secure
IDS	: Intrusion Detection System
IEEE	: Institute of Electrical and Electronics Engineers
IPsec	: Internet Protocol Security

IoT	: Internet of Things
IRE	: Institute of Radio Engineers
ISO	: International Organization for Standardization
IT	: Information Technology
L2	: Layer-2 (Data Link Layer)
LAN	: Local Area Network
LTE	: Long Term Evolution
MAC	: Media Access Control
MDM	: Mobile Device Management
MFA	: Multi Factor Authentication
MITM	: Man in the Middle
NAC	: Network Access Control
NFC	: Near Field Communication
NIST	: National Institute of Standards and Technology
NSS	: National Security Service
P2P	: Peer-to-Peer
PC	: Personal Computer
Ransomware	: Ransom Software
SIEM	: Security Information and Event Management
SMS	: Short Message Service
SNMP	: Simple Network Management Protocol
SQL	: Structured Query Language
Spyware	: Spy Software
SSL/TLS	: Secure Socket Layer – Transport Layer Security
VPN	: Virtual Private Network
VoLTE	: Voice over LTE
WiFi	: Wireless Fidelity
WWW	: World Wide Web
XDR	: Extended Detection and Response
XSS	: Cross-Site Scripting

BÖLÜM 1

GİRİŞ

Çalışmanın giriş bölümünde, araştırmanın problemi, amacı, önemi, sınırlılıkları ve araştırmada bahsedilen kavramlara dair tanımlar ile araştırmada kullanılan yönteme yer verilmektedir.

Problem

Bu araştırma, Mobil İletişim Teknolojilerinde Siber Güvenliğin;

- Yeterliliklerinin,
- İhtiyaç duyduğu metotların,
- Karşı karşıya kaldığı tehditlerin ve
- Dünya çapında kabul görmüş savunma yöntemlerinin,

İncelenmesine yönelik sorulara yanıt bulmayı konu edinmektedir.

Araştırmacının, Ulusal ve Uluslararası otoritelerce önlem alınmaya çalışılan mobil siber tehditleri; araştırmasına ve bu teknolojinin geçmişini, bugününü ve geleceğini incelemesine karar verilmiştir.

Radyo Televizyon Üst Kurulu bünyesinde bu tezin konusu ve incelediği problemlerin ilgilendirdiği Bilgi Teknolojileri Network ve Güvenlik alanında çalışmakta olan araştırmacı, kurumumuzda alınabilecek önlemlere de değinecektir.

Amaç

Bu çalışmanın amacı, mobil iletişim dünyasında yaşanan siber güvenlik tehditlerini incelemek ve bu tehditlere karşı etkili mücadele yöntemlerini tartışmaktır. Mobil cihazlarda kullanılan işletim sistemleri, uygulamalar ve iletişim protokollerindeki güvenlik açıklarına odaklanarak, hem bireysel kullanıcılar hem de kurumlar için uygulanabilir çözüm önerileri sunmak amaçlanmaktadır.

Önem

Mobil cihazlar, günlük yaşamın vazgeçilmez bir parçası haline gelmiş olup kişisel, finansal ve kurumsal verilerin büyük bir kısmını taşımaktadır. Mobil iletişim teknolojilerinin güvenliğini sağlamaya yönelik çalışmalar, bireylerin mahremiyetini koruma, finansal kayıpları önleme ve kurumsal ağları güvence altına alma açısından büyük önem arz etmektedir. Çalışmadan elde edilecek bilgiler ile de bu alandaki kurumsal ve akademik literatürdeki boşluğun doldurmasına katkı sağlanacak ve araştırma probleminin çözümü konusunda önerilerde bulunulacaktır.

Sınırlılıklar

Çalışmanın sınırlılığı, iletişim teknolojilerinin temellerinden bahsedilecek olsa da, esasen mobil iletişim teknolojilerindeki siber güvenlik tehditlerini incelemektir. Çalışma sırasında sistemlere tehdit oluşturan çok fazla sayıda saldırı yöntemi olması nedeniyle hepsine değinilemeyecektir. Ayrıca hızla değişen ve gelişen siber tehditler nedeniyle, çalışma bulguları ve sonuçları geçerliliğini zaman içerisinde yitirebilecektir.

Tanımlar

Mobil Siber Güvenlik: Mobil cihazların yazılım, veri ve kullanıcı bilgilerini korumak için alınan önlemlerin bütünüdür.

Elektriksel İletişim: Elektrik sinyalleri aracılığıyla bilgi transferinin gerçekleştirildiği iletişim sürecidir.

Oltalama: Kullanıcıları yanıltarak hassas bilgilerini ele geçirmeye çalışan kötü niyetli bir yöntemdir.

Zararlı Yazılım: Bilgisayar veya diğer dijital cihazlara zarar vermek veya izinsiz erişim sağlamak amacıyla tasarlanmış kötü niyetli yazılımlardır.

YÖNTEM

Çalışmanın bu bölümünde, araştırma modeline, araştırma evreni ve örneklemine, araştırma sonucunda elde edilen verilerin toplanması ve çözümlenmesine dair hususlara yer verilmektedir. Genel olarak küresel çapta kabul görmüş saldırı yöntemleri ile savunma prensipleri incelenecek. Vaka analizi yapılarak, gerçek dünyada meydana gelmiş saldırılar

ile potansiyel saldırılara karşı alınabilecek önlemler analiz edilecektir.

Araştırmanın Modeli

Literatür tarama yöntemi ile veri toplanırken, bu veriler nitel araştırma yöntemleri ile değerlendirilmiştir. Çalışma, mobil cihaz kullanıcılarının karşılaştığı güvenlik tehditlerini analiz etmek ve bu tehditlere karşı uygulanan savunma mekanizmalarını değerlendirmek üzerine kuruludur. Bu çerçevede, mobil iletişim ekosistemindeki farklı katmanlar (cihaz, yazılım, son kullanıcı, ağ ve veri vb.) incelenerek, her bir katmanda karşılaşılan riskler ve çözüm önerileri sunulmuştur.

Evren ve Örneklem

Çalışmanın evrenini, güncel teknolojinin mobil iletişim sistemlerini karşı karşıya bıraktığı siber güvenlik tehditleri ve bu tehditlere karşı alınabilecek tedbirler oluştururken, örneklemini küresel olarak en fazla sistemi veya kullanıcı verisini risk altında bırakmakta olan tehditler oluşturmaktadır.

Örneklem, araştırmacının Ağ Güvenliği alanında çalışması ve çalışmasının uzmanlık tezi niteliğine sahip olması nedeniyle seçilmiştir.

Verilerin Toplanması

Bu tez çalışması kapsamında toplanacak veriler, kitaplardan, web sitelerinden, akademik makalelerden, ulusal ve uluslararası tezlerden elde edilecektir. Literatür taraması, mobil iletişim teknolojilerinde siber güvenlik tehditleri ve çözüm yöntemlerine ilişkin akademik çalışmaların ve küresel çapta kabul görmüş kurum-kuruluşların tavsiyelerinin incelenmesini kapsamaktadır.

Verilerin Çözümlenmesi

Literatür tarama yöntemi ile elde edilen veriler tasnif edilmiş, önce problemin anlaşılması adına tanımlamalar yapılmış, sonra çözüme dair kullanılan yöntemler ve politikalar araştırmacı tarafından incelenmiştir. Bu süreçte, mobil güvenlik tehditlerine ilişkin yaygın sorunlar ve bunlara karşı geliştirilen çözümler arasında ilişki kurularak sonuçlar değerlendirilmiştir.

BÖLÜM 2

ELEKTRİKSEL İLETİŞİM VE SİBER GÜVENLİĞİ

Elektriksel iletişim, modern dünyada bilgi alışverişinin temel taşını oluşturan kritik bir teknolojidir. Elektrik sinyalleri aracılığıyla bilgi iletimini kapsayan bu teknoloji, telefon, radyo, televizyon ve internet gibi pek çok farklı platformda hayati bir rol oynamaktadır. Elektriksel iletişim sistemleri, verici, iletim ortamı, alıcı ve modülasyon/demodülasyon gibi bileşenlerden oluşur ve bu bileşenler arasındaki etkileşim, bilgiyi hızlı ve etkili bir şekilde iletmenin temelini oluşturur (Carlson, Crilly, & Rutledge, Communication Systems, 2006, s. 2-5).

Ancak, bilgi ve iletişim teknolojilerinin hızla evrildiği günümüzde, bu sistemler yalnızca verimlilik ve hız açısından değil, güvenlik açısından da önemli bir odak noktası haline gelmiştir. Elektriksel iletişim sistemleri, siber saldırılara ve diğer güvenlik tehditlerine karşı savunmasız olabilir. Bu bağlamda, siber güvenlik kavramı, elektriksel iletişim ağlarının korunması ve güvenliğinin sağlanması için vazgeçilmez bir gereklilik olarak ortaya çıkmaktadır. Siber güvenlik, bilgi sistemlerinin, ağların ve verilerin izinsiz erişim, kullanım, ifşa, bozulma, değiştirilme veya yok edilme gibi tehditlere karşı korunmasını hedefleyen bir disiplindir. Elektriksel iletişim sistemleri, özellikle internetin yaygınlaşması ile birlikte, kötü niyetli yazılımlar, veri ihlalleri ve hizmet engelleme saldırıları gibi çeşitli siber tehditlere maruz kalmaktadır. Bu tür tehditler, sadece bireylerin değil, aynı zamanda kurumların ve devletlerin de güvenliğini tehlikeye atabilmektedir. Elektriksel iletişim ve siber güvenlik arasındaki ilişkiyi anlamak, hem bireyler hem de kurumlar için daha güvenli ve etkili iletişim ağları kurmak adına kritik bir öneme sahiptir (Stallings, 2011, s. 2-7).

2.1. Elektriksel İletişim

Elektriksel iletişim, elektrik sinyalleri aracılığıyla bilgi alışverişini ifade eder. Bu iletişim türü, iki veya daha fazla nokta arasında elektriksel işaretler kullanarak bilgi iletmek amacıyla kurulan sistemleri ve teknikleri kapsar. Elektriksel iletişim, modern telekomünikasyon sistemlerinin temelini oluşturur ve telefon, radyo, televizyon, internet gibi birçok farklı platformda kullanılır. Elektriksel iletişim; temel olarak verici, iletim ortamı, alıcı ve modülasyon ile demodülasyon bileşenlerinden oluşur. Verici, bilgiyi elektriksel

sinyale dönüştüren cihaz veya sistemdir. İletim ortamı, elektriksel sinyallerin iletildiği kanalı ifade eder ve bu kanal bakır kablolar, fiber optik kablolar veya hava (radyo dalgaları) olabilir. Alıcı, elektriksel sinyali alıp yeniden bilgiye dönüştüren cihaz veya sistemdir. Modülasyon ve demodülasyon ise analog veya dijital sinyallerin iletimini kolaylaştırmak için işaretlerin uygun bir forma dönüştürülmesi ve yeniden orijinal forma çevrilmesi sürecidir (Carlson, Crilly, & Rutledge, 2006, s. 6-7).

2.1.1. Elektriksel İletişimin Ortaya Çıkışı ve Tarihsel Gelişimi

Elektriksel İletişimin temeli, 19. yüzyılın başında geliştirilen telgraf cihazları ile atılmaya başlamıştır. Samuel Morse'nin Morse kodu, telgraf iletişiminde kullanılmak üzere geliştirilmiştir. Telgraf cihazı, elektriksel sinyalleri telgraf telleri aracılığıyla ileten ve karşıda çözülmesine dayanan bir teknolojidir. Bu yenilik ile başka mucitler de ticari kullanıma yönelik ilk telgraf sistemlerini geliştirmişlerdir (Lewis, 2003, s. 8).

1844'te Amerika Birleşik Devletleri'nde Baltimore ve Washington şehirleri arasında ilk ticari telgraf hattı kurulmuştur. 19. Yüzyılın ikinci yarısında kıtalararası iletişim sağlayabilmek amacıyla transatlantik kablo hatları kurulmaya başlanmıştır. Alexander Graham Bell'in 1876'da telefonu icadı ile insan seslerini uzak mesafelere iletmeyi başaran bir cihaz keşfedilmiştir. Telefonun ilk dönemlerinde iletişim, yine kablolar marifetiyle yapılmıştır (Standage, 1998, s. 48).

1890'lı yıllara gelindiğinde ise artık radyo dalgaları ve kablosuz iletişim alanlarında yeni sistemler geliştirilmeye başlanmıştır. Guglielmo Marconi ve çağın mucitleri elektromanyetik dalgalar ile iletilen mobil iletişimin ilk aşamalarını icat etmişlerdir. Bu iletişim metodu özellikle askeri alan, denizcilik ve radyo yayınlarının iletimi için kritik öneme sahiptir. Bu aşamalardan itibaren, kablolu ve kablosuz iletişim paralel olarak gelişmeye devam etmiştir (Sungook, 2001, s. 1).

İnternetin temelleri, ABD'de Soğuk Savaş Döneminde atılmıştır. Savunma Bakanlığı, askeri iletişimin güvenliğini artırmak amacıyla ARPANET projesini başlatmıştır. Bu proje bilgisayarlar arasında güvenli veri transferini sağlamak için ilk kez paket anahtarlama (packet switching) mantığı ile çalıştırılmıştır (Janet, 1991, s. 8).

80'ler ve 90'ların başında, kişisel bilgisayarlar ve ev modemlerinin yaygınlaşmaya başlaması ile bireyler de internete erişebilir hale gelmiştir. Tim Berners-Lee'nin 1989'da World Wide Web(WWW) protokolünü geliştirmesi, internet üzerinde verilerin çok daha kolay paylaşılabilmesine imkân vermiştir. WWW temel bir http protokolüdür ve tarayıcı ile

sunucu arasındaki veri transferini sağlamaktadır. Daha sonra şifreli hale getirilerek https (http secure) protokolü oluşturulmuştur ve halen yaygın olarak kullanılmaktadır (Berners-Lee & Fischetti, 1999, s. 162).

Benzersiz IP adresleri ile akılda kalması daha kolay site adlarını eşleştiren ve amacı kullanıcıya kolaylık sağlamak olan DNS (Domain Name Server) de bu yıllarda oluşturulmuştur. Domain Name Server yani Alan Adı Sunucusu, aslında tüm alan adlarının arkasında benzersiz IP adresleri olması nedeniyle ortaya konulmuştur. Kullanıcıların ziyaret etmek istedikleri her internet sitesinin IP adreslerini hafızalarında tutmaları zor olacağı için IP ve Alan Adı eşleştirmesi yapar. Tarayıcıya "Google.com" yazıldığında aslında 216.58.214.142 IP'sine istek gönderilmektedir. Bu IP adreslerini her internet sitesi için ayrı ayrı ezberlemek ve akılda tutmak neredeyse imkânsıza yakındır. Burada verilen IP adresi ise Google'nin birçok IP adresinden sadece birisidir ve örnek olarak verilmiştir (Mockapetris, 1987, s. 1-2).

90'ların ortalarında, internetin ticari alanda da kullanımının başlanması ve ticari firmaların bu hizmeti sağlaması interneti yaygınlaştırmış, Web tarayıcıların genel kullanıma geçmesi sayesinde internet insanlar arasında da geniş olarak kullanılmaya başlanmıştır. World Wide Web 'in oldukça yaygınlaşması da bu süreci hızlandırmıştır (Shane, 2017, s. 39).

Bulut Bilişim Sistemleri 2010'larda benimsenmeye başlanmıştır. Verinin bulut sunucularında tutulması ile fiziksel veri depolama ihtiyaçları günden güne kurumsallaşmaya yönelmiştir. Ayrıca, yüksek bant genişliği ile çalışan video hizmet sağlayıcıların (YouTube vb.) yaygınlaşması ile kişiler de interneti daha yoğun kullanma imkânına erişmiştir. Sosyal medya platformlarının etkin kullanımı da mobil iletişim tekniklerinin büyüme kaydetmesini hızlandırmıştır (Yener, 2021, s. 73-75).

Günümüzde ise artık mobil iletişim sistemleri, yüksek bant genişliğine sahip, düşük gecikme süreleri ile iletim yapabilen, geniş kapsama alanlarında çalışan, Nesnelerin İnterneti(Internet of Things – IoT) sistemlerini verimli hale getiren ve yüksek veri güvenliği sağlayan bir konumda bulunmaktadır (Buyya & Dastjerdi, 2016, s. 5).

2.2. Mobil İletişimin Tanımı

Mobil İletişim, iki veya daha fazla ve en az biri mobil olan noktalar arasında iletişim kurmak amacıyla çeşitli teknolojik sistemlerin kullanılarak erişimin sağlanması anlamına gelmektedir (Ling, 2015, s. 1).

Her gün gelişen ve genişleyen internet tabanlı teknolojiler, kablosuz ve mobil iletişim sistemlerinin varlığını kaçınılmaz hale getirmiştir. Günümüzde ekonomi, hukuk, altyapı, savunma gibi hayati sektörlerde teknoloji kullanımı, hem mevcut sistemlerin kapasitelerinin artırılması hem de sürekli olarak yeni yaklaşımların ortaya konmasını gerektirmektedir. Neredeyse bir buçuk asırdır kullanılmakta olan elektriksel iletişim, havada dolaşan serbest radyo dalgaları iken, bugün kaynağı: hedefi: yolu belirlenmiş, güvenlik standartlarına sahip, özel şifreleme protokolleriyle veri bütünlüğü korunarak yapılmak zorundadır. Bu nedenlerden dolayı öncelikle elektriksel iletişimin temellerini, tarihçesini ve günümüze kadar aldığı yolu incelemek gerekmektedir (Rappaport T. S., 2002, s. 1-3).

2.3. Temel Mobil İletişim Teknolojileri ve Kavramları

Mobil iletişim, radyo dalgalarının keşfi ve geliştirilmesinden sonra özellikle askeri iletişim alanında başlayarak yoğun olarak kullanılmıştır. Sadece askeri haberleşme değil halkı bilgilendirmek, bilinçlendirmek veya düşmana propaganda yapmak amacıyla kullanılan mobil iletişim 1970'lerde küresel çapta standart hale gelmeye başlamıştır. Bu mobil iletişim minimum düzeyde güvenlik ve doğrulama içeren, dış müdahalelere daha müsait erken bir standarttı (John, 2024, s. 1).

İlk Kuşak İletişim (1G), analog ses iletimi üzerinde çalışmaktaydı ve 1980'lerde geliştirildi. 70'lerdeki erken standartlardan farklı olarak, İlk Kuşak İletişimle beraber güvenlik standartları da oluşturulmaya başlandı. İlk Kuşak İletişim, yalnızca ses hizmeti sunabiliyordu ve mobil değildi. Zamanın teknolojisinin henüz gelişiyor olması nedeniyle erken standart güvenlik şartları olan mobil İletişim ancak İkinci Kuşakta başlayabilmiştir. İkinci Kuşak Mobil İletişim (2G), dijital ses iletimi ile işletiliyor olması sayesinde sesli iletişimin yanında kısa mesaj hizmetini(SMS) de sunabiliyordu. 1990'lardan erken 2000'lere kadar bu teknoloji kullanıldı ve GSM (Global System Mobile Communications) standartlaştırıldı. Bu da veri hızlarının artmasına olanak sağladı. Şu an halen telefon hizmeti olarak kullanılmakta ama hızları sonraki teknolojilere göre düşük kalmaktadır. Üçüncü Kuşak Mobil İletişim (3G) ise yüksek hızlı internet iletişimi, geniş bant veri aktarımları ve videolu çağrılar ile insanlığı tanıştırmıştır. 2000'lerin ortasından 2010'lara kadar olan sürede son kullanıcının mobil iletişime erişim oranları ve hızları oldukça artmıştır. 3G dünyanın halen birçok bölgesinde kullanılmakta ve hızla yerini 4G teknolojilerine bırakmaktadır. Dördüncü Kuşak Mobil İletişim (4G), yüksek hızlı veri transferini düşük gecikmeler ile sunabilen LTE (Long-Term Evolution) teknolojilerini kapsamaktadır. Bu teknolojiler

100Megabit/sn hız, gelişmiş geniş bant bağlantılar, düşük gecikme süreleri, yüksek kapasite, verimlilik, IP tabanlı iletim yani tek bir platform üzerinden tüm verilerin iletilmesi, birden fazla alıcının aynı anda kullanılması, veri kaybının azaltılması gibi yenilikler sunmaktadır. Mobil geniş bant kullanımları bu dönem içerisinde büyük genişleme göstermiştir. 2010'larda başlayan bu teknolojinin kullanımı günümüzde de sürmektedir. Beşinci Kuşak Mobil iletişim(5G), yüksek performanslı 4G teknolojilerinin daha da hızlandırılması ve verimliliklerinin arttırılması amaçları üzerine yoğunlaşmakta, büyük verilerin taşınıp işlenmesine hizmet etmekte ayrıca Nesnelerin İnterneti alanına altyapı oluşturmak için çalışmaktadır. 5G teknolojileri her gün daha da gelişmekte, daha fazla bölgede yaygınlaşmakta ve yeni nesil uygulamaların kullanımını desteklemektedir (Lopa & Vora, 2015, s. 47-53).

1G'den 5G'ye kadar mobil iletişim teknolojisi gelişiminin daha iyi anlaşılabilmesi için, eldeki veriler Tablo 1'de görselleştirilmiştir.

Tablo 1

1G'den 5G'ye Mobil İletişim Teknolojileri Gelişimi

Teknoloji	Tarih	Bant Genişliği (Mbps)	Ana Ağ	Ana Servis İşlevi	Avantajlar	Dezavantajlar
1G	1980'ler	~0.00003 Mbps	Analog	Sadece ses	İlk ticari mobil ağ	Düşük veri hızları, düşük güvenlik
2G	1990'lar	0.014 - 0.2 Mbps	Dijital	Ses ve metin (SMS)	Gelişmiş ses kalitesi, SMS desteği	Düşük veri hızları, temel veri hizmetleri
3G	2000'ler	0.2 - 42 Mbps	Dijital	Veri, ses, görüntü, internet erişimi	Hızlı veri aktarımı, video görüşmeleri	Kapsama alanı sınırlamaları, maliyet
4G	2010'lar	20 - 1000+ Mbps	Dijital	Yüksek hızlı veri, HD video streaming	Yüksek veri hızları, düşük gecikme	Altyapı yatırımı gerektirir, yoğun kullanımda hız düşüşü
5G	2020'ler	50 - 1000+ Mbps	Dijital	Ultra yüksek hızlı veri, düşük gecikme, IoT	Çok yüksek veri hızları, düşük gecikme	Altyapı karmaşıklığı, yatırım maliyeti

Ülkemizde ise şu an güncel ve yaygın olarak kullanılan teknoloji 4.5G'dir. 4.5G, 4G LTE'nin daha yüksek veri hızı ve ağ kapasitesi ile geliştirilmiş bir versiyonudur. Farklı

frekans bantlarını birleştirerek yüksek hızlar elde etme, yoğun nüfuslu bölgelere 4G'ye nazaran daha iyi hizmet sunma ve özellikle VoLTE (Voice over LTE) teknolojileri ile yüksek kaliteli ses iletimini sağlar. Yine 4.5G daha ileri anten teknolojilerine sahip olması sayesinde sinyal güçlerini arttırır ve kapsama alanlarını genişletir haldedir (Holma & Toskala, 2012, s. 1).

Mobil İletişim Teknolojilerinden olan Bluetooth ve NFC (Near Field Communication) teknolojileri cihazların arada bir yönlendirme noktası olmadan P2P (peer-to-peer/ Noktadan Noktaya) iletişime geçmesini sağlamaktadır. Bu sayede cihazlar kendi aralarında kablosuz şekilde haberleşebilirler (Huang & Rudolph, 2007, s. 1).

Wi-Fi teknolojisinin standartlaştırılması da 90'lı yılların sonunda meydana gelmiştir. Bu sayede ev, işyeri veya halka açık alanlarda kablosuz internet erişimleri yaygınlaşmaya başlamıştır. 2000'li yıllarda geniş bant internet erişimi yaygınlaşmış ve yüksek hızlı bağlantılar son kullanıcı için standart kullanıma girmiştir. Mobil internetin de bu yıllarda hizmete sunulması akabinde taşınabilir cihazlar marifeti ile her yerden internete erişilebilir olmuştur. Yine 2000'lerin başından itibaren Bluetooth ve NFC gibi teknolojiler, kablosuz cihazların kısa mesafeli de olsa iletişimleri için kullanılmıştır. Bluetooth teknolojisi genellikle 10 metreye kadar olan mesafelerde 50 Mbps'ye kadar çıkan bant genişliklerinde kullanılır. NFC yani Yakın Çevre İletişimi ise 424 Kbps gibi düşük bant genişliğinde, maksimum 4cm'ye kadar olan mesafelerde kullanılan ve çok düşük enerji tüketimine sahip bir teknolojidir (Rappaport T. S., 1991, s. 52).

Wi-Fi (Wireless Fidelity) teknolojisi, mobil cihazların belli frekanslarda, AP(Access Point) olarak adlandırılan erişim noktaları yardımıyla, önceden belirlenmiş ağlar ve bu ağları kapsayan güvenlik önlemleri korumasında internet erişimlerini sağlamaktadır (Ohrtman & Roeder, 2003, s. 19).

2000'li yılların başından itibaren, acil durum konum belirleme (E-911) için küçük ve düşük maliyetli GPS (Global Positioning System – Mobil İletişim için Küresel Sistem) alıcıları, cep telefonlarına entegre edilmeye başlanmıştır. Akıllı telefonlar ortaya çıktıkça, daha güçlü GPS alıcıları da kullanılmaya başlanmıştır ve sürekli konum belirleme için de geliştirilmeye devam edilmiştir. GPS teknolojisi, mobil cihazların konum tabanlı hizmetleri kullanabilmesi için geliştirilmiştir ve özellikle Sosyal Medya uygulamaları ile haritalar gibi konum tabanlı uygulamaların kullanılabilmesi için çalışmaktadır (Kaplan & Hegarty, 2005, s. 905).

2.4. Mobil İletişimde Siber Güvenliğin Önemi

Mobil cihazların kullanımının hızla artmasıyla birlikte mobil siber güvenliğin önemi de büyük ölçüde artmıştır. Akıllı telefonlar ve tabletler, kişisel ve profesyonel yaşamlarımızın ayrılmaz bir parçası haline gelmiş olup, bankacılık işlemlerinden e-posta yazışmalarına, sosyal medya etkileşimlerinden iş yönetimine kadar pek çok hassas bilgiyi barındırmaktadır. Bu cihazların güvenliği ihmal edildiğinde, kullanıcılar dolandırıcılık, kimlik hırsızlığı ve veri ihlalleri gibi ciddi tehditlerle karşı karşıya kalabilirler. Ayrıca, iş yerlerinde Kendi Cihazını Getir (Bring Your Own Device - BYOD) politikalarının yaygınlaşması, mobil cihazların şirket ağlarına erişimini artırmış ve bu da kurumsal güvenlik açıklarını çoğaltmıştır. Bu nedenle, mobil siber güvenlik önlemlerinin alınması ve sürekli güncellenmesi hem bireyler hem de kurumlar için hayati bir gereklilik haline gelmiştir (Speed & Maor, 2017, s. 30).

Mobil cihazların boyutu, taşınabilirlik açısından belirgin bir avantaj sağlar ve kullanıcıların bu cihazları her zaman yanlarında taşıyabilmesini mümkün kılar. Boş durumdan aktif moda hızlı bir geçiş, bilgi kaynaklarına hızlı erişimi sağlar. Kullanıcılar genellikle mobil cihazlarla sadece birkaç saniye veya birkaç dakika etkileşimde bulunur. Mobil cihazların anında erişilebilirliği ve yaygınlığı, onları belirgin bir şekilde kişisel bir bağlamda kullanılmasına olanak tanır (Bergman, Stanfield, & Jason, 2013, s. 19).

Yakın tarihlerde, kişisel mobil cihazlarda bulunan uygulama mağazalarının aktif kullanımı sebebiyle, buradaki uygulamalara kötü niyetli yazılımların sızma girişimleri başlamıştır. Özellikle kişilerin kimlik bilgilerinin çalınması amacıyla yapılan oltalama tipi saldırılar artmıştır (Bergman, Stanfield, & Jason, 2013, s. 40).

2010'dan itibaren üretilen mobil cihazlar, daha karmaşık uygulamaları ve daha yüksek bant genişliği kullanan internet hizmetlerini desteklemeye başlamıştır. Bununla beraber daha yüksek veri hızı demek daha fazla saldırı alabilecek alan anlamına da gelmektedir. 2010'lardan itibaren ortaya çıkan BYOD trendi, personelin kişisel cihazlarını iş yerlerine getirmesine ve kullanmasına olanak sağlamıştır. Hem iç ağa hem de dış ağa erişebilen ve kişilerin kullanımında olan bu cihazlar kurum ve işletmelerin daha fazla güvenlik açığına maruz kalmasına neden olmaktadır. Bu güvenlik açıkları da bu tezin konusu olan Mobil İletişim Siber Güvenlik kavramının ortaya çıkmasına ve durmaksızın geliştirilmesine ihtiyacı doğurmuştur. BYOD, şirketlere çalışanların kişisel akıllı cihazlarına ağ altyapısı ve verilere erişim sağlama imkânı sunar. Temelde, şirket kendi cihazlarının ötesinde ağını genişletebilir (Rai & Chukwuma, 2016, s. 14).

Siber Güvenliğin 3 temel prensibi bulunmaktadır. "The CIA Triad" adı verilen bu üçlü sacayağı, Confidentality (Gizlilik), Integrity (Bütünlük) ve Availability (Erişilebilirlik)

özellikleri olarak kabul görmüştür. CIA Triad, kurum ve kuruluşlara kapsamlı siber güvenlik politikaları ve stratejileri belirlemeleri yolunda bir çerçeve rehber olarak hizmet eder. Bu üçlü prensip ise şöyle açıklanmaktadır:

Gizlilik, veriye sadece yetkili kişilerin erişimini ve yetkisiz erişiminin engellenmesini bu sayede hassas verinin çalınmaya veya manipülasyona karşı korunmasını içerir. Şifreleme metotları, erişim kontrolleri ve kullanıcı kimlik doğrulama yöntemleri bu amaçla kullanılan önlemlerdir.

Bütünlük, verinin tüm yaşam döngüsü boyunca doğruluğuna, tutarlılığına ve güvenilirliğine odaklanır. Verinin yetkisiz veya uygunsuz şekilde değiştirilmesini engellemek amacı ile veri doğrulama, kontrol toplamları ve sürüm kontrolü gibi önlemler alınmasını öngörür.

Erişilebilirlik, yetkili kullanıcıların bilgi ve kaynaklara ihtiyaç halinde zamanında ve güvenilir şekilde erişim sağlayabilmelerini ifade etmektedir. Donanımsal kesintileri, yazılım hataları ve kötü amaçlı erişimleri önlemeye yönelik koruma içermektedir. Yedekleme sistemleri, felaket kurtarma planları, geri dönüş politikaları bu amaca hizmet eden stratejilerdir (Whitman & Mattord, 2021, s. 8-9).

İlk bakışta, siber güvenlik tamamen teknik gibi görünebilir. Popüler imaj da kesinlikle böyledir: yeşil kod ekranı, kapüşonlu saldırganlar, yanıp sönen ışıklar ve neon ışık akışları. Gerçekte ise, teknoloji elbette siber güvenliğin merkezindedir ancak siber güvenlik disiplini bunun ötesindedir. Bu meslekteki iş türleri geniş bir yelpazeye yayılır; derin teknik rollerden insan odaklı rollere kadar çeşitlilik gösterir (Barker, 2020, s. 19).

2.5. Kablolu ve Kablosuz İletişimin Avantaj ile Dezavantajları

İletişim teknolojilerinin başlangıç evreleri genel itibari ile kablolu teknolojiler üzerine yoğunlaşmıştır. Zamanla kablolu sistemlerin hareket kısıtlılıkları ve geniş alanlardaki iletişim ihtiyaçlarının alt yapı maliyetleri kablosuz iletişimi ön plana çıkarmıştır. Kablolu ve kablosuz iletişim teknolojileri arasındaki farklar, günümüzde detaylı incelenerek, hangi ortamda hangi teknoloji türünün daha kullanışlı olacağının tespitinin yapılması gereklidir. Kablolu ağ, Ethernet kablolarıyla birbirine bağlanmış iki veya daha fazla bilgisayar, yazıcı ve diğer cihazların bir koleksiyonudur. Kablolu ağlar, diğer kablolu ve kablosuz ağların bir parçası olarak da kullanılabilir. Kablosuz ağlar ise iletişim için fiziksel ortam olarak radyo frekans kanallarını kullanan bilgisayar ağlarıdır. Kablolu ve kablosuz ağlar arasındaki en büyük fark, birinin fiziksel ağ kablolarını, diğerinin ise radyo

frekanslarını kullanmasıdır. Kablolu ağ, daha hızlı ve daha güvenli bir bağlantı sağlar ve 600 metreden kısa mesafeler için kullanılabilir. Kablosuz ağlar ise daha az güvenlidir ve iletim hızları dış etkenlerden etkilenebilir (Meenakshi, 2014, s. 63). Kablolu ve kablosuz iletişim teknolojilerinin anlaşılabilmesi amacıyla eldeki bilgiler Tablo 2'de özetlenmiştir.

Tablo 2

Kablolu ve Kablosuz İletişim Teknolojilerinin Türleri ve Genel Özellikleri

Teknoloji	Tip	Bant Genişliği (Mbps)	Ana Ağ	Ana Servis İşlevi	Avantajlar	Dezavantajlar
Kablolu Ethernet	Kabloyla	10 Mbps - 100 Gbps	Evrensel	Veri aktarımı, internet erişimi	Yüksek hız, düşük gecikme	Fiziksel kablo gerektirir, taşınabilirlik sınırlı
Wi-Fi (802.11)	Kablosuz	1 Mbps - 10 Gbps	Yerel	Kablosuz internet erişimi, ağ paylaşımı	Yüksek hareketlilik, kolay kurulum	Sinyal zayıflaması, yoğun frekans kullanımı
Bluetooth	Kablosuz	1 Mbps - 3 Mbps	Kişisel	Veri aktarımı, cihaz bağlantısı	Düşük güç tüketimi, yaygın kullanım	Kısa menzil, düşük veri hızı
LTE (4G)	Kablosuz	20 Mbps - 1000+ Mbps	Geniş Alan	Yüksek hızlı mobil internet, ses iletişimi	Yüksek veri hızları, geniş kapsama	Altyapı maliyeti, yoğun kullanım sırasında performans düşüşü
Fiber Optik	Kabloyla	100 Mbps - 1 Gbps+	Evrensel	Yüksek hızlı internet, uzun mesafe iletişim	Yüksek bant genişliği, düşük gecikme	Kurulum maliyeti, fiziksel altyapı gereksinimi

Kablolu ve kablosuz iletişim teknolojileri arasında bulunan temel avantaj ve dezavantajlar ise şu şekilde açıklanabilir:

- Kablolu iletişim, genel itibari ile verinin fiziksel kablolar marifetiyle taşınması nedeniyle daha güvenli olarak addedilir. Çünkü bu fiziksel kabloların izinsiz erişimden korunması daha kolay ve az masraflıdır. Hâlbuki kablosuz iletişim havada dolaşan – her ne kadar şifreleme metotları kullanılıyor olsa da - serbest haldeki sinyallerdir, isabetli yaklaşımlar ve şifre çözme algoritmaları ile siber saldırılara daha açık ortamlardır.

- Kablolu bağlantılar, daha az dış etkene maruz kaldıkları için – fiziksel kabloların etrafının hem girişim engelleyici korumalara sahip olması hem de fiziksel izolasyon malzemeleriyle kaplı olmaları nedeniyle daha yüksek bağlantı güvenliği ve daha az veri kaybı sağlarlar. Oysa kablosuz bağlantılar çevresel faktörlerden oldukça etkilenir. Buna örnek olarak fiziksel olarak duvarlardan geçerken sinyal zayıflıkları olabilmesi ve sinyal-frekans karışıklıkları verilebilir.
- Kablolu iletişim teknolojileri, kablosuz muadillerine oranla daha yüksek veri hızları sunar. Kablosuz bağlantılar ise daha yavaştır. Özellikle, yoğun kullanım alanlarında basit bir kablonun verebileceği performans kablosuz denklerine oranla çok daha fazla olabilir.
- Kablosuz sistemler, mobilite ve fiziksel serbestlik noktasında avantajlıdır. Fiziksel cihaz kurulumları ve yapısal kablolama gereklilikleri kablolu iletişimi statik hale getirerek mobil alternatiflerine oranla az verimli olmasına neden olur.
- Yapısal kablolama, konektör yerleştirilmeleri ve konfigürasyonları nedeniyle kablolu iletişim teknolojileri kablosuz iletişime oranla daha yüksek altyapı maliyetine ihtiyaç duyar.
- Basit bir yönetim merkezi kurularak hızlıca erişim noktaları kurulması ve ihtiyaç üzerine konfigüre edilebilir – yer değiştirilebilir – yenisi eklenebilir oluşları ile kablosuz erişim yöntemleri çok daha hızlı olarak kurulup kullanılabilir hale gelerek kablolu iletişime oranla yüksek zaman kazancı sağlar (Forouzan, 2012, s. 361-362,435-436).

Kablolu ve Kablosuz iletişim arasındaki farkların daha net ve birlikte görülebilmesi amacıyla Tablo 3'te bulunan görsel hazırlanmıştır.

Tablo 3

Kablolu ve Kablosuz İletişim Arasındaki Farklar

Özellik	Kablolu İletişim	Kablosuz İletişim
Güvenlik	Fiziksel kablolar nedeniyle daha güvenli	Sinyaller havada dolaştığı için daha açık ve saldırıya meyilli
Dış Etkenlere Dayanıklılık	Fiziksel koruma ve izolasyon sayesinde daha az etkilenir	Duvarlar ve sinyal-frekans karışıklıkları gibi faktörlerden etkilenir
Veri Hızı	Daha yüksek veri hızları	Daha yavaş veri hızları
Mobilite	Statik, fiziksel kablolama gerektirir	Mobilite ve fiziksel serbestlik avantajı
Altyapı Maliyeti	Daha yüksek altyapı maliyeti	Daha düşük altyapı maliyeti
Kurulum ve Kullanım Hızı	Daha uzun sürede kurulur	Daha hızlı kurulum ve esneklik

BÖLÜM 3

MOBİL İLETİŞİMDE SİBER SALDIRI VE ÖRNEK VAKALAR

Mobil iletişime yönelik siber saldırılar, sistemleri ve kullanıcıları hedef alan ve genellikle; finansal kazanç veya düzensizlik yaratma, politik amaçlarla veri toplama, panik ve güvensizlik meydana getirme amacıyla veri işleme sistemlerini zayıflatma gayeleri taşır. Mobil iletişimin insan hayatının her noktasına temas ettiği günümüzde, kişisel verilerin ifşası amacıyla sosyal mühendislik yöntemleri ile siber saldırılar düzenlenmektedir. Bu siber saldırılar, kritik verilerin çalınmasını, kopyalanmasını veya manipüle edilmesini, kişisel bilgilerin ifşasını, herhangi bir yolla maddi çıkar kazanılmasını hatta elde edilen veriler ile kişilerin veya sistemlerin daha fazla sömürülmesini amaçlar (Mike, 2021, s. 9-11).

Mobil iletişimdeki güvenlik tehditleri teknik olarak üç ana başlık altında incelenebilir. Bunlar, sistem ve sunucuları hedef alan zararlı yazılımlar, son kullanıcıyı hedef alan oltalama ve kimlik avı saldırıları ile genel ağ topolojisini hedef alan ağ sistemi saldırıları olarak tanımlanabilir.

Mobil iletişimde siber saldırılar, kötü niyetli kişi veya gruplarca kritik verilerin çalınması, fidye amacıyla rehin alınması ya da tamamen yok edilmesi amacıyla kullanılmaktadır. Bu bölümde mobil iletişimi tehdit eden siber saldırı yöntemleri incelenecektir.

3.1.Siber Saldırı Yöntemleri

Dijital çağın getirdiği hızlı gelişmeler ve internetin yaygınlaşması, bilgiye erişimi kolaylaştırmakla birlikte, çeşitli siber güvenlik tehditlerini de beraberinde getirmiştir. Günümüzde bireyler, kurumlar ve devletler, siber saldırılar nedeniyle önemli risklerle karşı karşıya kalmaktadır. Bu tehditlerin ciddiyeti ve karmaşıklığı, her geçen gün artmakta ve yeni saldırı teknikleri ortaya çıkmaktadır. Siber saldırılar, genellikle kötü niyetli yazılımlar, ağ sistemi saldırıları ve oltalama saldırıları şeklinde üç ana başlık altında toplanarak incelenmektedir. Bu yöntemler, siber saldırganların bilgi çalma, sistemleri bozma veya hizmetleri kesintiye uğratma gibi amaçlarına hizmet eder (Coursera Staff, 2024).

3.1.1 Zararlı Yazılımlar

Zararlı Yazılım (Malicious Software), yani kısaltması ile Malware kötü niyetli yazılımları ifade etmektedir. Bilgisayar sistemlerine, kullanıcı cihazlarına veya ağlara zarar vermek, veri çalmak ya da izinsiz bilgi toplamak amacıyla tasarlanan yazılımların tamamı bu alana dâhil edilebilir. Malware'nin alt dalları ve birçok yöntemi bulunmaktadır.

Son yıllarda kötü amaçlı yazılımların yaygın olarak kullanılabilmesinin temel nedeni, kötü amaçlı yazılımlar tarafından kullanılan çeşitli yeni gizleme teknikleridir. Sistemleri, verileri ve bilgileri korumak için, kötü amaçlı yazılımların mümkün olduğunca erken tespit edilmesi gerekmektedir. Bu konuda birçok kötü amaçlı yazılım tespit teknikleri çalışmaları bulunmasına rağmen, kötü amaçlı yazılımları tamamen tespit edebilen bir yöntem yoktur ve her geçen gün kötü amaçlı yazılım tespiti zor bir hale gelmektedir. Statik kötü amaçlı yazılım analizi, bilinen kötü amaçlı yazılımlar için çok etkilidir ancak sıfırcı gün kötü amaçlı yazılımlar için işe yaramaz, bu da dinamik kötü amaçlı yazılım tespiti gereksinimini ortaya çıkarmaktadır. Davranışa dayalı kötü amaçlı yazılım tespiti, imza tabanlı, derin öğrenme tabanlı, Mobil/IoT ve bulut tabanlı tespit gibi teknikler karşılaştırmalı olarak iyi kabul edilmektedir. Ancak yine de tüm sıfırıncı gün kötü amaçlı yazılımlarını tespit edemez ki bu da kötü amaçlı yazılım tespitinin çok zorlu bir görev olduğunu ve kötü amaçlı yazılım tespiti için daha fazla teknik gerektiğini göstermektedir (Heena & Mehtre, 2021, s. 1-2).

İlk çıktığı günden itibaren, sistemleri tehdit eden zararlı yazılımlar, yılları ve etkileri bu yazılımların, başlangıçta genel kullanıma yönelik riskler barındırırken, zaman içinde devletlerin elinde rakiplerini zarara uğratmak amacıyla kullandıkları bir alana dönüşmüştür. Aşağıda verilen ve yakın tarihteki bazı kritik zararlı yazılımları özetleyen Tablo 4'te bu net olarak anlaşılabilir.

Tablo 4

Yakın Tarihteki Kritik Zararlı Yazılımlar

Zararlı Yazılım Adı	Ortaya Çıkış Tarihi	Türü	Saldırı Yöntemi	Ana Hedefler	Hasar / Dikkate Değer Etki
ILOVEYOU	2000	Virüs	E-posta eki	Kişisel bilgisayarlar	Kişisel dosyaları yok etti ve büyük mali hasara yol açtı
CryptoLocker	2013	Fidye Yazılım	E-posta eki	Kişisel ve kurumsal bilgisayarlar	Dosyaları şifreledi ve fidye talep etti; fidye yazılımlarının tehdidini öne çıkardı
MyDoom	2004	Solucan	E-posta eki	Teknoloji şirketleri (ör. Google, Yahoo)	DDoS saldırıları ve spam yayılımı ile 38 milyar dolarlık hasara yol açtı
Storm Worm	2006	Solucan	E-posta bağlantısı	Kişisel bilgisayarlar	Milyonlarca e-postayı enfekte etti, dijital kesintilere neden oldu ve bilgisayarları botlara dönüştürdü
Sasser & Netsky	2004	Solucan	IP adreslerini tarama (Sasser)	Rastgele IP adresleri (Sasser)	Milyarlarca dolarlık hasara yol açtı; 17 yaşındaki bir öğrenci tarafından yaratıldı
Anna Kournikova virüsü	2001	Virüs	E-posta eki	Kişisel bilgisayarlar	Yaklaşık 166.000 dolar hasara yol açtı; popüler figürler üzerinden dijital kesintinin potansiyelini gösterdi
Slammer	2003	Solucan	Sunucu hedefleme	Microsoft SQL Server 2000 kullanan sunucular	Kritik altyapıyı hedef alarak 1 milyar dolar hasara yol açtı
Stuxnet	2010	Solucan	USB bellekler	İran nükleer tesisleri	İran'ın nükleer programını geri çekerek santrifüjlerin kendini imha etmesine neden oldu; jeopolitik önemi ile dikkat çekti
Code Red	2001	Solucan	Sunucu hedefleme	Microsoft IIS kullanan sunucular	Web sitelerini tahrif etti ve yaygın internet kesintilerine neden oldu; ekonomik hasar milyarlarca dolar olarak tahmin ediliyor
Conficker	2008	Solucan	Windows sistem açıkları	Kurumsal, devlet ve kişisel ağlar	Kaldırılması son derece zor; dünya çapında milyonlarca bilgisayarı enfekte etti ve modern bilgisayar virüslerinin kalıcı ve gelişen tehdidini gösterdi

McGowan, Norton Malware, Emma, 2024

3.1.1.1. Virüsler

Bir virüs, kendisini muhtemelen evrimleşmiş bir kopyasını içerecek şekilde değiştirerek diğer programları enfekte edebilen bir programdır. Bir belirli bir programı virüs

olarak sınıflandırmaya çalışırken, programın kendisini özyinelemeli ve açıkça kopyalayıp kopyalayamayacağı önemli bir sorudur. Virüsler, sistemde bulunan dosyalara bağlanıp kendini çoğaltabilen ve daha da fazla dosyayı enfekte edebilen zararlı yazılımlardır. Temel amaçları bilgisayar sistemlerine sızmak bu sayede istenmeyen etkiler yaratmak ve bu sistemlere zarar vermektir. Virüsler genel itibari ile birkaç ana bileşen içermektedir. İlk olarak sisteme sızıp başka dosyaları enfekte etmek amacıyla "Enjekte Edici Kod" çalıştırılmaktadır, daha sonra virüslerin sistemlerde yer edinip çoğalmasını sağlamak üzere "Çoğalma Mekanizma Kodları" devreye girer. Bu iki aşamadan sonra ise virüsün sisteme esas vereceği "Zararlı İşlevleri" aktifleşir (Szor, 2005, s. 18).

3.1.1.2. Solucanlar

Bir solucan, tek bir bilgisayarda başlayan ve Yerel Alan Ağı (Local Area Network-LAN) veya İnternet bağlantısı aracılığıyla bağlı diğer bilgisayarları arayan kötü amaçlı bir programdır. Bir solucan başka bir bilgisayar bulduğunda, kendisini o bilgisayara kopyalar ve kopyalanacak diğer bağlı bilgisayarları aramaya devam eder. Bir solucan, kendisini sürekli olarak kopyalamaya çalışır veya bir otomatik zamanlama mekanizması işlemi durdurana kadar bu işlemi sürdürür (Erbschloe, 2004, s. 23).

3.1.1.3. Trojanlar

Adlarını Truva savaşındaki Trojan Atı'ndan alan, aslında zararsız görünen ama kullanıcılar farkında olmadan sistemlerine sızıp veri hırsızlığı yapabilen veya cihazları köleleştiren zararlı yazılım türleridir. Ana özellikleri, gizlenme yeteneklerinin yüksek olması, cihazlara uzaktan erişimle ulaşabilmeleri ve gerektiğinde kullanılmak üzere arka kapı oluşturma yeteneklerinin olmasıdır (Bhunia & Tehranipoor, 2018, s. 374).

Genel itibari ile zararlı e-posta ve SMS ekleri, güvenilir görünen kaynaklardan indirilen dosyalar ve başka yazılımların içine sızarak arka planla çalışan uygulamalar aracılığıyla sistemlere sızarlar. Truva atları temel bir kötü amaçlı kod türüdür ve başlangıçta saldırganlara sistem dosyalarına erişim sağlama amacıyla tasarlanmıştır. Bu, saldırganlara dosya ayarlarını değiştirme, dosya veya şifre çalma, dosyaları bozma veya ağdaki diğer bilgisayarlardaki kullanıcı etkinliklerini izleme gibi yetenekler sağlamaktadır (Erbschloe, 2004, s. 101).

3.1.1.4. Casus Yazılım

Kullanıcı aktivitelerini izleyen, kaydeden ve gerektiğinde kötü niyetle kullanan zararlı yazılımlar casus yazılımlar olarak kabul edilmektedir, Spy Software olarak adlandırılır ve Spyware olarak kısaltılırlar. Reklamcılık veya kişisel verilerin çalınması amacına hizmet eden bu yazılımlar çeşitli işlevlere sahiptir. Klavye kombinasyonlarının izlenmesi ve kaydı, görüntülenen web sitelerinin kaydı, internette yapılan arama ve araştırmaların kaydı veya yerel disk verilerini taramak en temel casus yazılım amaçlarıdır. Diğer Malware türleri gibi sistemde gizlenerek kullanıcı verilerini tarar, klavye kombinasyonlarına kadar birçok kişisel veriyi kaydeder hatta internet aktivitelerini bile izleyebilirler. Spyware'lerin en büyük yayılma alanı uygulama mağazalarında yer alan ücretsiz uygulamalar üzerindendir. Yine zararlı bağlantılar ve kötü niyetli e-posta-SMS ekleri ile yayılabilirler (Kaspersky, t.y.).

Ticari casus yazılımı, eskiden çoğunlukla ebeveynlerin çocuklarının İnternet'te ne yaptığını izlemek için ve işverenlerin, İnternet'te gezinerek vakit geçiren çalışanların hangileri olduğunu belirlemek adına kullanılmıştır. Daha ciddi bir kullanımı ise bilgi varlıklarının potansiyel hırsızlığını veya endüstriyel casusluğu tespit etmektir. Geliştiriciler, casus yazılımlarını çocukları koruma aracı olarak pazarlayarak, aslında amaçlarının kişisel erişimleri takip etmek isteyen kişilere yardımcı olmak olarak tanıtırlar. Güçlü izleme ve casus programları, arka planda gizlice çalışırken tüm tuş vuruşlarını ve tüm etkin pencerelerin zamanını ve başlığını bir metin dosyasına yakalar. Kayıtlar şifrelenip belirtilen bir e-posta adresine otomatik olarak gönderilebilir veya sadece sabit diske kaydedilebilir. Programların erişimi şifre korumalıdır ve görev yöneticisi menüsünden dahi gizlenebilir (Mitnick & Simon, 2003, s. 207).

3.1.1.5. Reklam Yazılımı

Çoğunlukla kullanıcı mağazalarında bulunan ücretsiz uygulamaların beraberinde gelen ve kullanıcı rızası olmadan reklam gösteren zararlı yazılımlardır. Advertising Supported Software olarak bilinen ve Adware olarak kısaltılan bu zararlı yazılımlar, sadece reklam göstermekle kalmayıp, kullanıcının çevrimiçi davranışlarını incelemek üzere veriler toplar ve kişi temelli reklamcılık sektörüne hizmet eder. Ücretsiz mağaza uygulamaları ve genellikle de sahte güvenlik yazılımlarının içine gömülmüş olarak sistemlere dâhil olurlar (NordVPN, t.y.).

Reklam yazılımı, genellikle gelir elde etmek amacıyla geliştiriciler tarafından bir web tarayıcısında otomatik olarak reklamlar gösteren ve bu reklamlardan gelir elde eden yazılımlar olarak da bilinir. Bu tür yazılımlar genellikle bilgisayarlar için tasarlanmış olsa da mobil cihazlarda da bulunabilir. Bazı reklam yazılımları son derece manipülatif olabilmekte ve zararlı yazılımların sisteme girmesi için bir kapı açabilmektedir. (Kaspersky, t.y.).

3.1.1.6. Fidye Yazılımı

Fidye Yazılımı yani Ransomware ki bu da Ransom Software anlamına gelir, belirli bir ücretin ödenmesini zorlamak amacıyla dijital olarak kurbanlara şantaj yapmak için kullanılan kötü amaçlı yazılımların bir sınıfını tanımlamak için kullanılan genel bir terimdir. Diğer zararlı yazılımlar gibi fidye yazılımları de güvensiz e-posta ve sms ekleri veya harici bellekler ile sisteme dâhil olarak gizlenir, kritik ve geri döndürülemez verileri çalar ya da şifreler, bu aşamalardan sonra ise veri bütünlüğünün tekrar sağlanması için fidye talebinde bulunurlar (Trellix, t.y.).

Fidye Yazılımı, sadece güvensiz ekler değil ağdaki ve işletim sistemlerindeki mevcut güvenlik zafiyetlerinden de faydalanabilirler. Ayrıca güvenilmeyen ve zararlı web siteleri de birçok fidye yazılımı barındırıyor olabilirler. Saldırganlar, solucan yazılımı ile sisteme sızarak, sistem üzerinde yerleşme ve otomatik kopyalama işlemlerini gerçekleştirmeleri akabinde fidye yazılımları ile dosyaları şifreler. Fidye yazılımları popülerlik kazanmıştır çünkü başarılı olmuştur. Bugün ise suçlular, ev kullanıcılarını hedeflemekten vazgeçmiş ve verileri daha fazla değeri olan, belirli çalışma sürelerini sürdürme ve anahtar verilerin korunmasına erişimi sağlama konusunda aşırı düzenleyici baskı altında olan kurumsal kullanıcılara odaklanmıştır (Liska & Gallo, 2017, s. 3,21).

3.1.1.7 Kök Kullanıcı Kiti

Kötü niyetli yazılımın sistemdeki mevcut yönetimi kök üzerinde ele geçirip gizlice çalışmasını sağlamaktadırlar ve kısaca Rootkit olarak bilinirler. En yaygın kullanım amacı ise herhangi diğer bir kötü amaçlı yazılım yöntemi ile sızılan sistemin kök yönetim bölgesini ele geçirip cihazları köle ordusu (bot net) haline getirmek, bu sayede Hizmet Engelleme Saldırıları (DoS-DDoS) için köle ordusuna sahip olmaktır. Sisteme kök yani kernel seviyesinde erişebilmeleri sayesinde çekirdek komutlar üzerinde söz sahibi olur ve

kullanıcıya sezdirmeden derinlemesine sistem kontrolünü ele geçirebilirler. Rootkitlerin, sızdıkları sistemlere bahsedilen tüm zararlı yazılımları bulaştırması mümkündür. Cihazları bot net ordusu haline getirebildikleri gibi fidye işlemlerinde kullanabilir, mevcut verileri zarar vermek amacıyla yok edebilir veya sistemi tamamen çökertebilirler (Fortinet, t.y.).

Rootkit terimi 2005 yılında dahi 10 yıldan daha uzun bir süredir kullanılmıştır. Bir Rootkit, bir bilgisayardaki en güçlü kullanıcı olan roota (kök kullanıcı) erişimi sağlayan küçük ve zararlı programlardan oluşan bir kod parçacığıdır. Başka bir deyişle, bir Rootkit, bir bilgisayarda geçici veya sürekli, algılanamayan bir varlığı mümkün kılan bir dizi program ve kod içerir. "Rootkit" tanımında anahtar kelime "algılanamayan"dır. Bir Rootkit'in kullandığı teknoloji ve hilelerin çoğu, sistemin içindeki kodları ve verileri gizlemek amacıyla tasarlanmıştır. Örneğin, birçok Rootkit, dosyaları ve dizinleri gizleyebilir. Rootkit'in diğer özellikleri genellikle uzaktan erişim ve dinleme içindir; örneğin, ağdaki paketleri dinlemek için. Bu özellikler birleştiğinde, güvenliğe ciddi zararlar verebilir (Hoglund & Butler, 2005, s. 25). Rootkitlerin temel çalışma prensiplerinin daha rahat anlaşılması için eldeki veriler Tablo 5'te özetlenmiştir.

Tablo 5

Rootkitlerin Temel Çalışma Prensibi

Adım	Açıklama
Sızma ve Gizlenme	Rootkit, sistemdeki güvenlik önlemlerini atlatarak gizlice sisteme sızar.
Gizli Kalma ve Yetki Yükseltme	Kendisini gizleyerek yüksek yetkilere erişim sağlamaya çalışır.
Sisteme Entegrasyon	Sistem çeşitli düzeylerine (kernel veya kullanıcı modu) entegre olur.
Güvenlik Açıklarını Sömürme	Bilinen güvenlik açıklarını kullanarak ek kötü niyetli yazılımlar yükleyebilir.
Gizli İletişim ve Kontrol	Gizli iletişim kanalları kurarak dışarıdan komutları veya verileri alır.
Saldırı ve Hasar	Sistemde istenmeyen değişiklikler yapabilir, veri sızdırabilir veya diğer zararlı eylemleri gerçekleştirebilir.

3.1.2. Son kullanıcı Oltalama ve Kimlik Avı Saldırıları

Oltalama, kötü niyetli kişiler veya grupların, sahte web sitelerini, sahte e-postalar, sahte SMS'ler gibi iletileri kullanarak kişisel bilgileri ele geçirmek amacıyla başvurdukları, hatta ele geçirilen bu kişisel veriler ile başkalarının da verilerini ele geçirmek niyeti bulunan

bir siber saldırı yöntemidir. Çağımızda en güçlü silah bilgidir. Bu nedenle kötü niyetli gruplar bilgiye ulaşabilmek için her yolu denemektedirler. Kimlik, adres, tıbbi geçmiş, bankacılık gibi bilgiler özellikle saldırganlar tarafından en çok hedef alınan alanlardır (Hadnagy & Fincher, 2015, s. 2). Oltalama saldırılarının temel prensiplerinin daha iyi anlaşılabilmesi için süreç Tablo 6'da ifade edilmiştir.

Tablo 6

Oltalama Saldırılarının Temel Prensipleri

Adım	Açıklama
Hedef Belirleme	Saldırgan, hedeflerini belirleyerek oltalama saldırısının potansiyel kurbanlarını seçer.
İnanılırlık Oluşturma	Saldırgan, sahte veya manipüle edilmiş iletiler veya web siteleri aracılığıyla inandırıcı senaryolar oluşturur.
Oltalama İletisi Gönderme	Hedeflere sahte e-postalar, SMS'ler veya sosyal medya mesajları göndererek kullanıcıları kandırmaya çalışır.
Kurbanın Tepkisi	Kurbanlar, sahte iletileri inceleyerek veya sahte web sitelerine giriş yaparak saldırganın amaçları doğrultusunda yanıt verir.
Bilgi Toplama ve Saldırı Yönlendirme	Saldırgan, kurbanlardan hassas bilgileri veya giriş bilgilerini çalarak veya yönlendirerek saldırıyı ilerletir.
Zararlı Eylemler	Elde edilen bilgileri kullanarak, kimlik hırsızlığı, mali dolandırıcılık veya diğer kötü niyetli eylemler gerçekleştirir.

Saldırı amacıyla, birçok kullanıcıya sahte e-postalar gönderen kötü niyetli kişiler bu kişileri sömürerek elde ettikleri gerçek e-posta adresleri ile çok daha fazla kişiyi tuzaklarına düşürebilmektedirler. Genellikle güvenilir kurum ve kuruluşların mail adreslerinin taklidi ile atılan ilk sahte e-postalar gerçek e-postaların çalınmasıyla sonuçlanabilmektedir. Örneğin, bilgilendirme@kurumadi.com.tr veya bilgilendirme@kurumadi.gov.tr gibi doğru bir e-posta adresi yerine bilgilendirme@kurumadi.gen.tr, bilgilendirme@kurumadi.mail.tr, bilgilendirme@kurumadi.online.mail benzeri sahte mail adreslerinden alınan ve acilen bankacılık şifresi değiştirilmesi gerektiğini söyleyen, mail sonuna da sahte bir web sitesine yönlendiren bağlantıya tıklamak dahi sistemleri virüsle enfekte edebilmektedir. Açılan sahte web sitesine de güvenilir kuruma ait web sitesi sanıp bilgiler girmek, verilerin bütün güvenliğinin ortadan kalkmasına neden olabilmektedir. Bu aşamadan sonra gerçek kişilere ait mail adreslerinin hesabını ele geçiren saldırganlar daha sonraki oltalama saldırılarını bu gerçek adresleri kullanarak yapar ve ilk oltalama saldırısına kanmayan kullanıcılar dahi

tuzağa düşebilirler. Oltalama ve kimlik avı saldırılarını engellemek için en önemli yol kullanıcı farkındalığının artırılmasıdır (Osho, ve diğerleri, 2019) .

Kötü niyetli kişiler ayrıca, kullanıcıya sahte SMS'ler göndererek bilgilerini ele geçirmeye çalışmaktadır. Sahte SMS'lerde genellikle acil bir durum veya ödül kazanıldığı gibi senaryolar kullanılarak kişilerin mobil cihazlarında bir bağlantıya tıklaması sağlanmaya çalışılır. Bağlantıya tıklandığında ise cihaz zararlı yazılımlarla enfekte olabilmekte ve her türlü tehdide açık hale gelebilmektedir. Unutulmamalıdır ki SMS'in büyük çoğunluğu, sıfır doğrulama, sıfır bütünlük kontrolü ve sıfır gizlilik içerir. Dünyanın herhangi bir yerinden herhangi biri istediği kişiye bir metin mesajı gönderebilir. Ayrıca bu bağlantılar aracılığıyla cihaz hemen enfekte edilmese dahi bağlantının yönlendirdiği sahte web sitesinde bunu sağlayacak zararlı yazılımlar kullanılmaktadır (Bergman, ve diğerleri, 2013, s. 32).

Sesli oltalama (Voice Phishing) yöntemi, kişinin telefon dolandırıcıları tarafından aranıp, önceden elde edilen bazı kişisel verilerini de kullanarak daha fazla kişisel verisini ele geçirmek veya kişiyi korkutarak maddi çıkar sağlamak amacıyla, kötü niyetli gruplar tarafından sömürülmesine dayanır. Yapay zekâ teknolojisinin gelişmesi ile birlikte, kötü niyetleri kişiler bu teknolojiden de faydalanmaya başlamışlardır. Özellikle bir kişiye ait ses kütüphanesi, yapay zekâ algoritmaları yardımıyla incelenebilmekte, frekansları ve karakteristikleri belirlenebilmekte ve buna bağlı olarak neredeyse orijinale yakın şekilde taklit edilebilmektedir (Korkmaz, Koçyiğit, Şahingöz, & Diri, 2022, s. 80).

Hassas faaliyetler için halka açık WiFi üzerinden mobil uygulamaların kullanılmaması gerekmektedir. Bunun yerine hücresel veri kullanılmalıdır. Hassas verilerle ilgilenen çoğu uygulama (bankacılık/finansal uygulamalar gibi) SSL/TLS kullanırken, bu uygulamalar içerisinde Bize Ulaşın, Sıkça Sorulan Sorular ve benzeri, WebKit (web tarayıcısı) kullanan sayfalar da olabilir ve bu sayfalar HTTP üzerinden içerik alır. Tarayıcılarının aksine, kullanıcılar uygulamanın HTTP/HTTPS kullandığını belirleyemez ve dolandırıcılık ve Aradaki Adam (Man-in-The-Middle - MiTM) saldırılarına maruz kalabilir (Bergman, Stanfield, & Jason, 2013, s. 289).

Oltalama saldırıları genel olarak, sahte e-postalardan, web sitelerinden, telefon çağrılarından ve mesaj iletilerinden yararlanılarak yapılır. Son kullanıcıyı tehdit eden bu yöntemlerle ilgili farkındalığın arttırılması ise en az kurum ve işletmeleri koruyan güvenlik uygulamaları kadar önem teşkil etmektedir. Kuruluşlarda düzenli aralıklarla sistem açıklarını tespit etmek üzere sızma testi yapılmaktadır. Bu sızma testleri yapılırken sistemlere yapılan saldırılar haricinde bir de kişilere yönelik oltalama testi yapılmaktadır.

3.1.3. Ağ sistemleri Saldırı Türleri

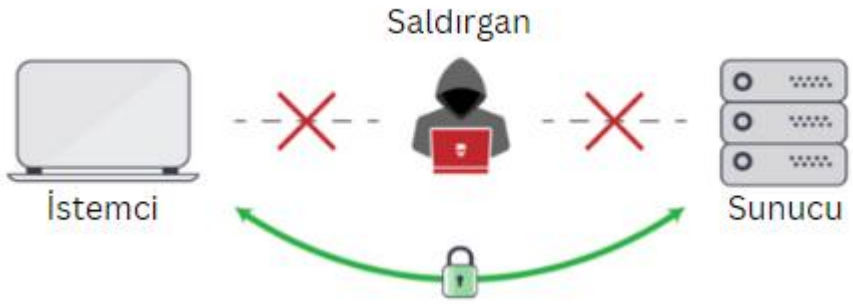
Ağ Sistemi saldırıları, bilgisayar ağları ve sistemlerine zarar verme, kaynaklarını aşırı kullanma ve başka zayıflıkların tespiti ile bu açıkların tekrar sömürülmesi amaçlarını gerçekleştirmek üzere yapılan yaygın ağ saldırılarını içerir. Yeni teknolojilere ayak uyduramayan sistemler, düzenli güncellenmeyip güncel hata çözümleri ile sistemlerini güçlendirmeyen ağ yapıları ve iyi yapılandırılmamış topolojilerle bu topolojilerde bulunan cihazları hedef alır. Ağ sistemleri, tamamen iletişimle ilgilidir ve iki veya daha fazla tarafın düzgün bir şekilde iletişim kurabilmesi için standartlar ve protokoller gereklidir. Nasıl ki sadece İngilizce bilen birine Türkçe konuşmak iletişim açısından pek bir şey ifade etmezse, bilgisayarlar ve diğer ağ donanımları da etkili bir şekilde iletişim kurabilmek için aynı dili konuşmalıdır. Bu, bu dili oluşturmak için önceden belirlenmiş bir dizi standardın olması gerektiği anlamına gelir. Bu standartlar aslında sadece dili değil, aynı zamanda iletişim kurallarını da içerir (Erickson, 2003, s. 114). Bu kuralların esnetilmesi, manipüle edilmesi ve amacından saptırılması neticesinde ağ sistemlerine yönelik saldırılar yapılmaktadır.

3.1.3.1. Aradaki Adam Saldırıları

Aradaki Adam Saldırıları (Man in The Middle-MITM), saldırganın iki taraf arasındaki iletişimi kendi üzerinden geçecek şekilde yönlendirerek tüm trafiği dinlemesini, manipüle etmesini, değiştirmesini veya tamamen kesmesini sağlayacak bir yöntemdir. Tüm trafiği kendi üzerinden yönlendiren saldırgan bir yönlendirici (router) veya erişim noktası (access point) gibi davranarak verilerin üzerinde tam kontrol yetkisini ele geçirebilir. Saldırganlar, MITM tekniğini yerel ağ trafiğini dinlemek ve kötü amaçlı yazılım veya virüs olmadan akan trafiği kullanarak son kullanıcı verilerini çalmak için kullanabilirler. Ayrıca, SSL atlatılarak şifreler elde edilebilir. Bir MITM saldırısını başlatmanın birçok yaygın yolu vardır. En basit yol, kamuya açık bilgisayar ağlarında sahte bir düğüm oluşturmaktır. Havaalanı, alışveriş merkezi veya kafe gibi yerlerde bulunan kablosuz ağlar bu açıdan en riskli yerlerdir ve asla kullanılmamalıdır (Efe, Kalkancı, Donk, Cihangir, & Uysal, 2019, s. 98-99) . Temel MITM saldırı yöntemi Şekil 1’de görülmektedir.

Şekil 1

Temel MITM Saldırı Yöntemi



3.1.3.2. Hizmet Engelleme Saldırıları

Hizmet Engelleme Saldırıları (DoS – Denial of Service), saldırgan tarafından hedef alınan ağın tamamını, bir kısım hizmetleri veya uç noktada yer alan kişisel bilgisayarlar ya da sunucular gibi kritik öneme sahip noktaları aşırı sayıda istek göndermek sureti ile işleyemez hale getirmek üzere çalışır. Bu tarz ataklar Siber güvenlik yöntemleri ile engellenebildiği gibi web sitelerini kapasitelerinin donanımsal veya yazılımsal olarak arttırılması ile de savuşturulabilir. Hizmet Engelleme (DoS) saldırısı, meşru kullanıcıların bir hizmeti kullanmasını engellemeye yönelik bir girişimdir. Bu saldırı tek bir ana bilgisayar veya ağ düğümünden geldiğinde, basitçe DoS saldırısı olarak adlandırılır (Stallings, 2011, s. 366).

DoS Saldırıları tek noktadan yapıldığı için kaynak adresin engellenmesi yöntemi ile engellenebilmektedir.

3.1.3.3. Dağıtık Hizmet Engelleme Saldırıları

Dağıtık Hizmet Engelleme Saldırıları (DDoS - Distributed Denial of Service Attack), zararlı yazılımlar veya kimlik avı yöntemleri ile köleleştirilmiş bilgisayarlardan toplu olarak yapılan ve bir saldırgan tarafından yönetilen bu saldırı türünde, köle ordusu koordineli bir şekilde hedefe aşırı yük bindirecek şekilde istekler yapar. Özellikle web sunucuları genel internet trafiğine açık olduğundan bu tarz saldırıların en büyük hedefleridirler. Hizmet Engelleme saldırıları, meşru kullanıcıların belirli bir ağ kaynağına erişimini durdurmayı amaçlayan saldırılardır ve ağ araştırma topluluğu tarafından 1980'lerin başlarından beri bilinmektedir. 1999 yazında ilk Dağıtılmış DoS (DDoS) saldırı olayı tespit edilmiştir ve o

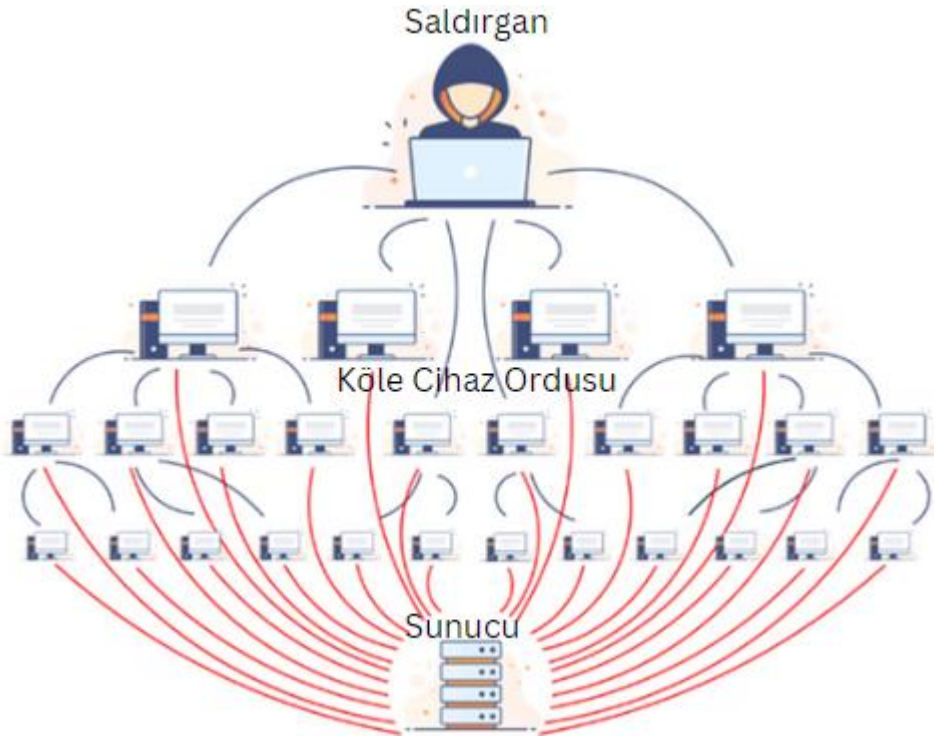
zamandan beri çoğu DoS saldırısı dağıtılmış doğada olmuştur (Zargar, Joshi, & Tipper, 2013, s. 2046-2048). Bu veriler ışığında Ddos Saldırı adımları Tablo 7'de özetlenmiştir. Şekil 2'de ise örnek bir DDoS saldırı mekanizması verilmiştir.

Tablo 7

DdoS Saldırı Adımları

Adım	Açıklama
Hedef Belirleme	Saldırgan, saldırı yapmak istediği hedef sistem veya ağ servislerini belirler.
Botnet Kurulumu	Saldırgan, genellikle botnet adı verilen büyük bir ağ üzerinde kontrol sağlar. Botnet, birçok bilgisayarın ve cihazın saldırıda kullanılması için ele geçirilmesini içerebilir.
Trafik Koordinasyonu	Saldırgan, botnet üzerinden hedefe büyük miktarda trafik gönderir. Bu, hedef sistem veya ağ servislerinin normal çalışma kapasitesinin üzerine çıkmasına neden olur.
Servis Engelleme	Hedef sistem veya ağ servisleri, yoğun trafik nedeniyle normal çalışma kapasitesinin üzerine çıkar ve erişim kısıtlamalarına neden olabilir.
Erişim Kısıtlamaları	Yoğun trafik, meşru kullanıcıların hizmet almasını engeller ve hedef sistemi veya ağ servislerini kullanılamaz hale getirebilir.
Sürekli Saldırı	Saldırgan, hedefin normal işlevselliğini bozmak için sürekli olarak trafik göndermeye devam eder, bu da hizmet kesintilerinin uzun süreli olmasına neden olabilir.

Şekil 2 Örnek bir DdoS Saldırı Görseli



What are Distributed Denial of Service (DDoS) Attacks?, bunny.net, t.y.

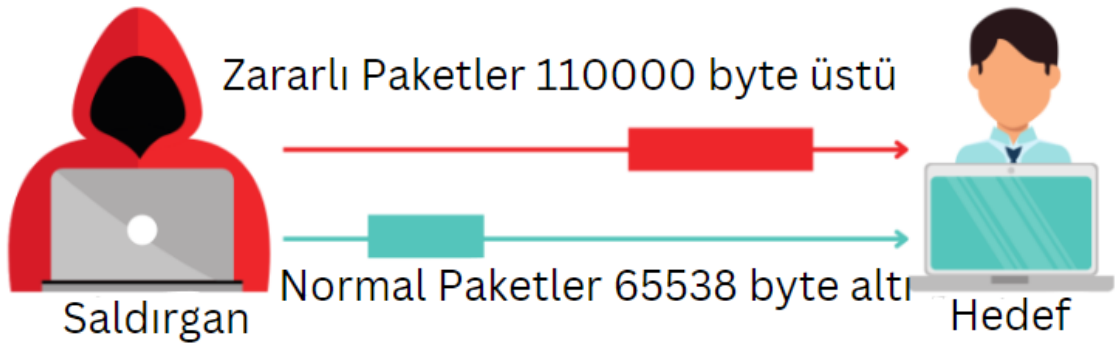
3.1.3.4. Ölüm Pingi Saldırısı

Ölüm Pingi olarak bilinen bu saldırı, hedef cihaz veya ağa aşırı bir ping trafiği yönlendirilmesi ile yapılabilir. Hedefe yoğun olarak gönderilen ping (Internet paket sorgulama) paketleri sistemi işleyemez hale getirebilir. Klasik ping paketi 32 byte boyuttadır. Ping paketi olarak gönderilen verinin boyutlarının manipüle edilerek sisteme aşırı yük sokulması da ping of death saldırısı yöntemlerinden birisi olarak kullanılmaktadır (Fortinet, t.y.).

Saldırgan ve mağdur arasındaki standart ve anormal paketlerin aynı anda gönderilmesi ile yapılan Ping of Death saldırısının tasviri Şekil 3'deki görselde verilmiştir.

Şekil 3

Ölüm Pingi temel saldırı prensibi



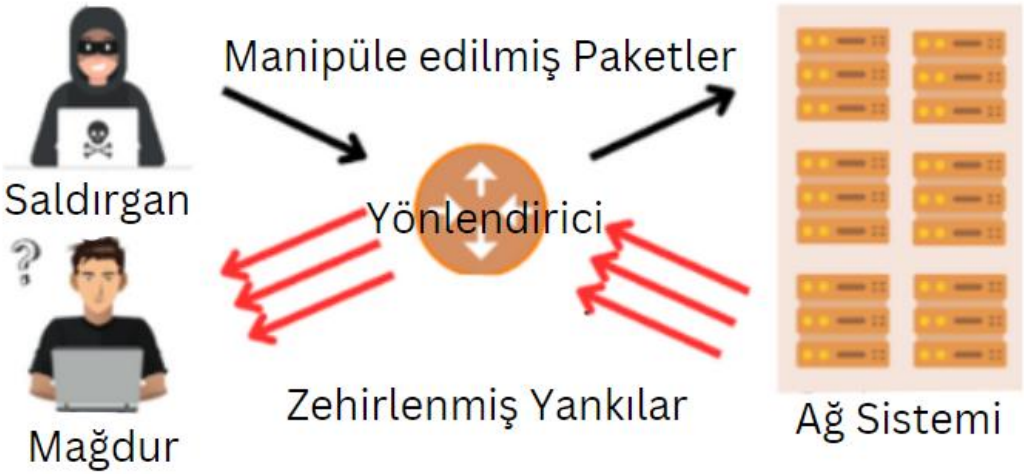
CloudDNS ölüm pingi, CloudDNS, t.y.

3.1.5.3. Smurf Saldırısı

Büyük bir ağı hedef alarak, sahte ip adreslerinden o ağa yönelik ping istek paketlerinin gönderilmesi, bu isteklere cevap olarak gelen yankıların da tekrar ağa verilmesi sureti ile sonsuz bir döngü oluşturarak ağı işleyemez hale getirmek üzere çalışan bir saldırı türüdür. Öncelikle, kötü amaçlı yazılım sahte bir IP adresi içeren bir ağ paketi oluşturur. Bu teknik, "zehirlenme" olarak adlandırılır. Paketin içindeki ping mesajı, paketi alan ağ düğümlerinden yanıt göndermelerini ister. Ardından bu yankılar tekrar ağ IP adreslerine gönderilerek sonsuz bir döngü oluşturulur. Kötü amaçlı paketi ağdaki her IP adresine gönderen IP yayınıyla birleştiğinde, Smurf saldırısı hızla tam bir hizmet reddine neden olabilir (Kaspersky, t.y.).

Şekil 4

Örnek bir Smurf Saldırısı



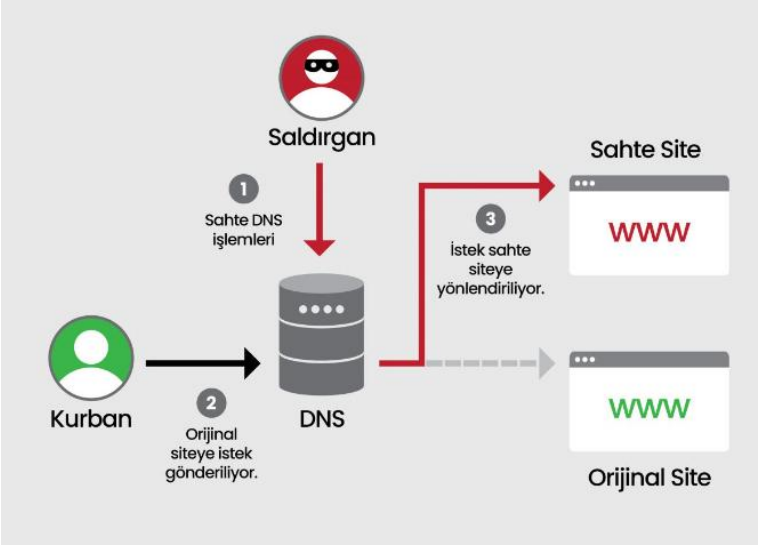
CloudDNS Smurf Saldırısı, CloudDNS, t.y.

3.1.3.6. DNS Maskeleme Saldırısı

Ağ üzerinde dönen DNS (Domain Name Server – Alan Adı Sistemi) sorgularını manipüle etmesi ile kullanıcıları yanlış veya hatalı web sitelerine yönlendirmesini sağlayan bir saldırı türüdür. DNS yanıtları, önceden ele geçirilmiş DNS önbelleğindeki IP adres defterinin değiştirilmesi ile zehirlenmiş olur (Liska & Stowe, 2016). DNS Maskeleme Saldırısı Şekil 5'te görülmektedir.

Şekil 5

DNS Maskeleme Saldırısı Gerçekleştirilme Şekli



Turhost DNS Maskeleme, Turhost, t.y.

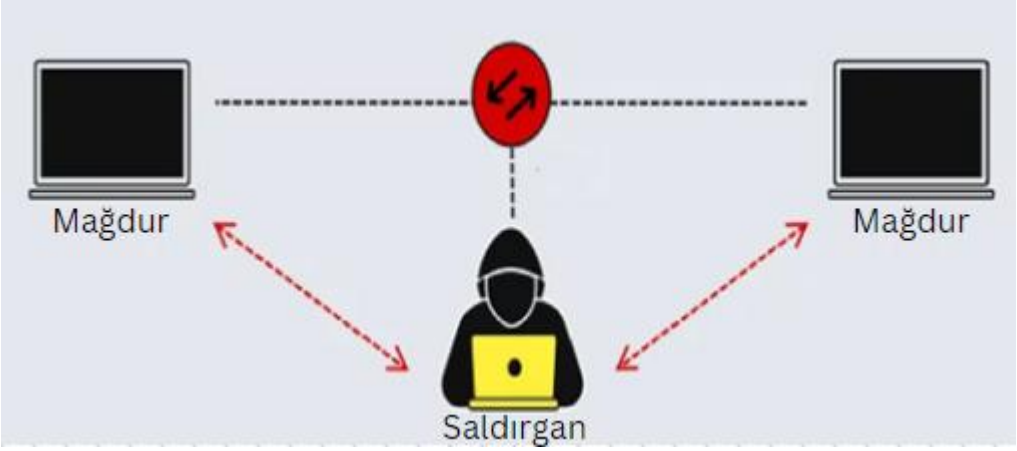
3.1.3.7. Paket Dinleme Saldırısı

Saldırgan, ağ trafiğini izleyerek, ağda bulunan kullanıcı adları, şifreler ve daha birçok kritik veriyi ele geçirmeye çalışır. Ağda mevcut veriyi manipüle etmek istemeyip, saklandığı yerden tüm veriyi çekmek ve kaydetmek isteyen saldırganlarca kullanılır. Ele geçirilmiş bir yönlendirici, omurga anahtarı veya kenar anahtar üzerinde yapılabilir (Bienkowski, 2024).

Packet Sniffing olarak da bilinen paket dinleme saldırılarında amaç trafiği hiçbir şekilde değiştirmeden sadece ortam dinlemesi yaparak kritik verileri ele geçirmektedir. Şekil 6'da temel paket dinleme saldırı tekniği görselleştirilmiştir.

Şekil 6

Paket Dinleme Saldırısı Temel Stratejisi



3.1.3.8. ARP Maskeleme

Adres Çözümleme Protokolü (Address Resolution Protocol-ARP), Ağ Katmanında (Layer-2 yani 2. Katman) çalışarak, iletişim başlatmadan önce belirli bir IP adresine karşılık gelen fiziksel adresi (MAC – Media Access Control) belirlemeye hizmet eder. ARP tablosu, ağda yönlendirme yapan omurga, yönlendirici veya kenar anahtarı gibi cihazların üzerinde bulunan ve ağdaki trafiği yönlendirebilmelerini sağlayan bir eşleştirme tablosudur.

ARP tablosunda, hangi IP'ye hangi yoldan gidileceği ve IP adreslerine karşılık gelen cihazların MAC adresleri güvenlik ve yönlendirme amacıyla tutulur. ARP Maskeleme (ARP Spoofing), kötü niyetli bir aktör ağdaki diğer cihazların ARP tablolarını manipüle ederek

kendisini meşru bir cihaz gibi gösterdiğinde gerçekleşir. Bu aldatmaca, sahte ARP paketlerinin iletilmesi yoluyla gerçekleştirilir ve diğer cihazları, saldırganın MAC adresini gerçek bir IP adresi ile ilişkilendirmeleri için kandırır. Saldırganlar, ARP tablosunu manipüle ederek ağdaki cihazları yanıltmaya ve iletişimi kendi üzerine almaya çalışır. Bu, trafiğin saldırgan tarafından izlenmesine, değiştirilmesine veya engellenmesine neden olabilir. ARP Maskeleme saldırısı, sabotaj amacıyla tüm trafiğin engellenmesini de meydana getirebilir. Saldırgan, ARP tablosundaki girdileri yanlış veriler ile değiştirerek veya yerlerine anlamsız veriler yazarak yönlendirmeyi imkânsız hale getirebilir. Bu durum, ağdaki cihazların doğru bir şekilde iletişim kurmasını engeller ve ağı kullanılamaz hale getirebilmektedir (Hnamte & Hussain, 2024).

Aşağıda standart bir ARP tablosu örneği verilmiştir. Bu tabloda ağ üzerindeki cihazların IP'leri, MAC adresleri ve dinamik ya da statik adresleme metotları bulunmaktadır. Windows cihazlarda komut istemi üzerinde yürütülecek "arp –a" kodu ile erişilebilmektedir.

Şekil 7

Örnek ARP Tablosu

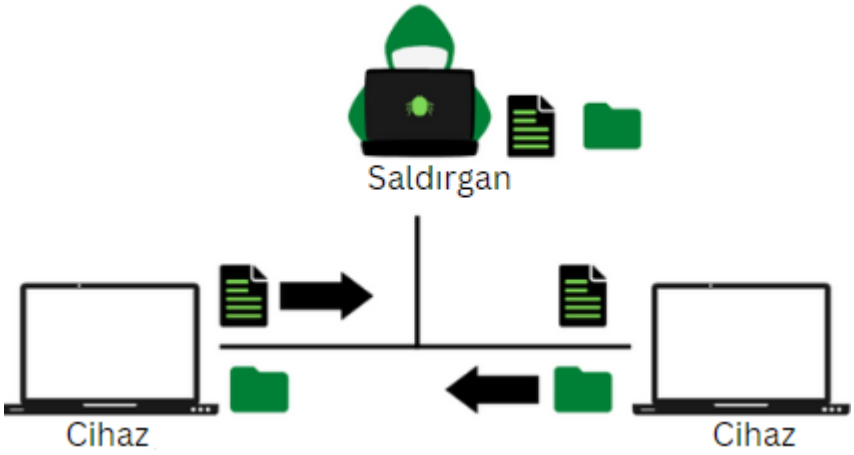
```
Interface: 10.1.21.84 --- 0x6
  Internet Address      Physical Address      Type
  10.1.21.1             00-1c-7f-6d-53-7d     dynamic
  10.1.21.2             00-1c-7f-6d-53-7d     dynamic
  10.1.21.33            64-51-06-44-1b-b9     dynamic
  10.1.21.44            00-d8-61-f2-bd-6f     dynamic
  10.1.21.48            64-51-06-44-1b-b7     dynamic
  10.1.21.49            c8-d9-d2-12-bb-f7     dynamic
  10.1.21.55            c8-d9-d2-12-bb-45     dynamic
  10.1.21.68            64-51-06-43-9c-eb     dynamic
  10.1.21.85            00-d8-61-f2-ed-bd     dynamic
  10.1.21.255           ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  239.255.255.251       01-00-5e-7f-ff-fb     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

ARP Maskeleme Saldırısının nasıl yapıldığının daha iyi anlaşılabilmesi için aşağıdaki görsel eklenmiştir. Burada saldırgan iki cihaz arası trafiği üzerine almak için yönlendirici gibi davranmaktadır ve iki cihaz arası trafiğe girişimde bulunarak ARP Paketleri manipülasyonu yapmaya çalışmaktadır. Standart bir ARP Maskeleme saldırısı Şekil 8'de

ifade edilmiştir.

Şekil 8

ARP Maskeleme



GeeksforGeeks Arp Maskeleme, GeekforGeeks, t.y.

3.1.3.9. Oturum Kaçırma

Oturum Kaçırma (Session Hijacking) saldırısı, genellikle halka açık Wi-Fi ağlarında güvenlik önlemlerinin az olması nedeniyle kullanıcıların trafiğini izlemek ve oturum bilgilerini ele geçirmek amacıyla kullanılan bir saldırı türüdür. Bu saldırı, mevcut web oturum kontrol mekanizmasının sömürülmesini içerir, ki bu genellikle bir oturum belirteci ile yönetilir. HTTP (Hypertext Transfer Protocol) iletişimi birçok farklı TCP (Transmission Control Protocol) bağlantısı kullandığından, web sunucusunun her kullanıcının bağlantılarını tanımlaması için bir yönteme ihtiyacı vardır. En yaygın kullanılan yöntem, web sunucusunun, başarılı bir istemci kimlik doğrulamasının ardından istemci tarayıcısına bir belirteç göndermesine dayanır. Bir oturum belirteci genellikle değişken genişlikte bir dizeden oluşur ve URL'de, HTTP isteğinin başlığında bir çerez olarak, HTTP isteğinin başka bir bölümünde veya hatta HTTP isteğinin gövdesinde kullanılabilir. Session Hijacking saldırısı, geçerli bir oturum belirteci çalmak veya tahmin etmek suretiyle oturum belirtecini tehlikeye atar ve yetkisiz erişim elde etmek için kullanır (OWASP, 2024).

3.1.3.10. Çapraz Site Betikleme ve Çapraz Site İstek Sahteciliği:

Güvenlik Açığı bulunan web uygulamalarının sömürülmesi ile bu uygulamaları kullanan kişilerin tarayıcılarına zararlı kod enjekte edilmesi üzerine yapılan saldırı türleri Çapraz Site Betikleme (Cross-Site Scripting-XSS) kapsamında yer alırken, hedef

kullanıcının saldırgan tarafından hazırlanan web sitesini ziyareti ile zehirlenmesi ve hedef web sayfasında bu zehirlenmiş tarayıcı marifeti ile istenmeyen eylem gerçekleştirmesi Çapraz Site İstek Sahteciliği (Cross-Site Request Forgery-CSRF) kapsamında yer alır. XSS ve CSRF, güvenlik açığı bulunan web uygulamalarının sömürülmesiyle ilgili iki farklı saldırı türüdür. XSS, web uygulamalarının güvenlik açıklarının kullanılmasıyla, bu uygulamalara erişen kullanıcıların tarayıcılarına zararlı kodların enjekte edilmesini sağlar. Bu kodlar, kullanıcıların tarayıcılarında çalışarak çeşitli zararlı eylemleri gerçekleştirebilir. Öte yandan, CSRF saldırısı, hedef kullanıcının, saldırgan tarafından hazırlanan bir web sitesini ziyaret etmesi ve bu ziyaret sonucunda tarayıcılarının "zehirlenmesi" ile gerçekleşir. Daha sonra, hedef web sayfasında bu zehirlenmiş tarayıcı aracılığıyla istenmeyen eylemler gerçekleştirilir. Bu saldırı türünde, hedef web sitesi, kullanıcının kimliği altında yetkilendirilmiş işlemleri gerçekleştirmek için kullanılır, böylece kullanıcının izni olmadan çeşitli eylemler yapılabilir. XSS, hassas bilgileri çalmak, kullanıcı oturumlarını ele geçirmek ve tarayıcı ile altta yatan sistem bütünlüğünü tehlikeye atmak için kullanılabilen bir saldırı vektörüdür. XSS açıkları, Web'in erken günlerinden beri varlığını sürdürmektedir. Bugün ise, e-ticaretin, günlük milyarlarca dolarlık bir endüstri olmasıyla birlikte, en büyük tehditlerden birini temsil etmektedirler (Grossman, Hansen, & Petko Petkov, 2007, s. 68-69).

3.1.3.11. DNS Yansıtma

DNS yansıtma (DNS Amplification) saldırısı bilinen bir tür DDoS saldırısıdır. Bu saldırıda, saldırgan, sisteme büyük miktarda trafik oluşturmak amacıyla az miktarda kaynağını harcayarak DNS sorguları gönderir. Saldırgan, DNS sunucusuna büyük boyutlu cevaplar içeren sorgular gönderir, ancak bu cevapları gerçek hedeflerin IP adreslerine yönlendirir. Bu süreci, köleleştirilmiş cihazlardan da istekler göndererek gerçekleştirir ve kendini anonim olarak saklar. Saldırının hedefi olan gerçek IP adreslerine yönlendirilen bu büyük cevap paketleri, işlenemez hale geldiğinde hizmet engelleme durumu ortaya çıkar. Bu teknikle, son kullanıcılara veya sunuculara yapılan saldırıların yanı sıra, saldırının büyüklüğüne bağlı olarak DNS sunucuları bile hizmet engelleme durumuna gelebilir. DNS trafiğinin akışlarını analiz etmek, sorguların ve cevapların oranıyla başlar. Sorguların cevaplara göre fazlalığı, sorgulayanı bir DDoS saldırısının istekli veya bilmeyen bir katılımcısı olarak gösterebilirken, cevapların sorgulara fazlalığı, cevap alıcısının bir yansıtıcı veya yansıtma saldırısının hedefi olduğunu gösteren olası bir gösterge olabilir (Dooley &

Rooney, 2017, s. 144-145).

Temel bir DNS Yansıtma Saldırısının süreçleri Tablo 8'de görselleştirilmiştir.

Tablo 8

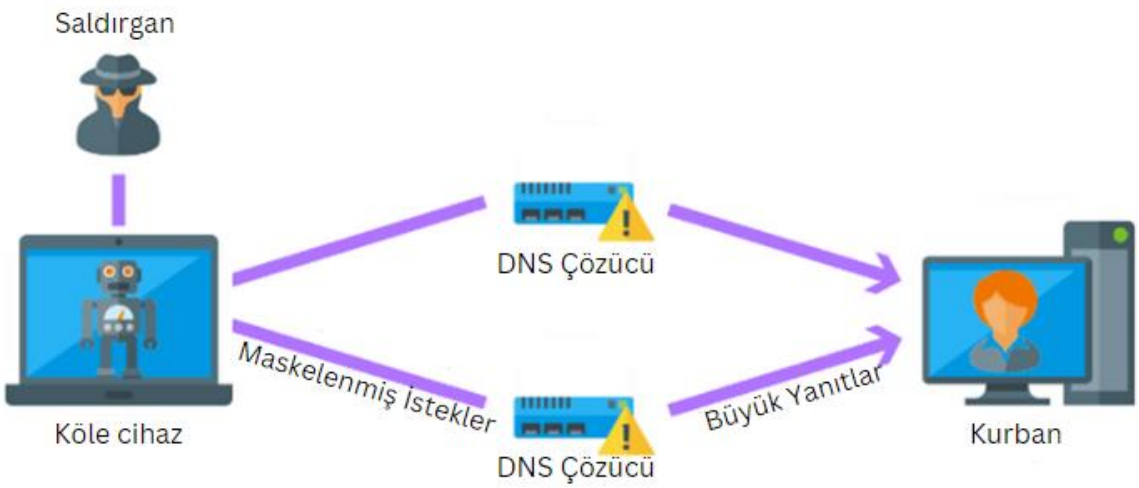
Temel DNS Yansıtma Saldırısı Süreci

Adım	Açıklama
Hedef Seçimi	Saldırgan, büyük miktarda trafik göndermek istediği DNS sunucularını belirler.
Sahte IP Adresleri ile İstekler	Saldırgan, sahte IP adreslerinden DNS sunucusuna büyük miktarda istek gönderir.
Amplifikasyon Etkisi	DNS sunucusu, gelen istekleri yanıtlamak için genişlemiş veri paketleri oluşturur (amplifikasyon).
Hedefe Yönlendirme	Genişlemiş yanıtlar, hedefe doğru yönlendirilir, bu da hedefin ağ kaynaklarını tüketir.
Servis Kesintisi	Hedef DNS sunucusu, normal işlevselliğini kaybeder ve meşru kullanıcıların isteklerini yanıtlayamaz hale gelir.

Şekil 9'da saldırganın köle cihazlar yardımı ile DNS Çözücülere maskelenmiş istekler göndermesini, DNS çözücünün de bu isteklere cevap verebilmek için büyük yanıtlar oluşturup kurbana göndermesini bu işlem sonucunda kurbanın verileri işleyemez hale gelmesi ifade edilmektedir.

Şekil 9

DNS Yansıtma Saldırısı



Purplesec DNS Amplification, Purplesec, t.y.

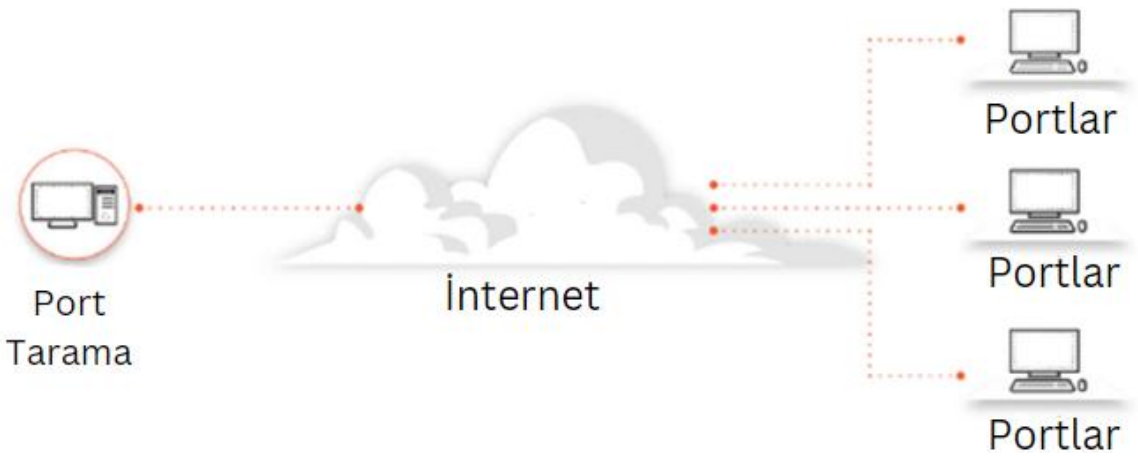
3.1.3.12. Port Tarama ve Parmak İzi Alma

Port Tarama (Port scanning), belirli bir ağı hedef alarak açık portlardaki hizmetleri tespit etmek için kullanılan bir yöntemdir. Saldırgan bu tarama sayesinde sistemde aktif kullanılan alanlardaki zayıflıkları tespit eder ve bu zayıflıklara yönelik saldırılar için planlama yapabilir. Ağ topolojisi, sistem versiyonları ve sistemin çalışma prensipleri tespit edilerek saldırıya dair planlar yapılabilir. Zaman, sızma girişimlerinde saldırganlar için güçlü bir silahtır. Genellikle keşif faaliyetleri sırasında zaman devreye girer. Bir saldırgan, taramalar arasında yeterli zaman bırakırsa, çoğu analistin ve aracın kafasını karıştırabilir. Milyonlarca paketi birkaç dakika içinde yüz binlerce anahtar üzerine serpiştiren bir port taramasından daha net bir saldırı alameti yoktur. Yüksek bir iletim hızı sağlandığında, bazı tarama araçları bir hedefin İnternet'e bağlantısını aşırı yükleyebilir ve performans izleme araçlarını tetikleyebilir. Saldırganın amacı genellikle performans izleme araçlarına yakalanmayacak en büyük çaplı taramayı yapabilmektedir (Bejtlich, 2010, s. 604).

Şekil 10'daki görselde port tarama saldırısını internet ortamından, istenilen hedefe yönlendiren bir saldırgan cihaz görülmektedir. Bu saldırgan sürekli olarak hedefin portlarını taramakta ve zafiyet gördüğü alanlara başka saldırılar yolu ile sızmaya çalışmaktadır.

Şekil 10

Port Tarama Yöntemi



PaloAlto Networks PortScan, PaloAlto, t.y.

Parmak İzi Alma (Fingerprinting) ise hedef sistem ve ağın belirli özelliklerini tarama

ve saldırı planı yapma amacıyla uygulanır. Güncellenmemiş sistemlerde bulunan güvenlik açıkları, konfigürasyonları verimli yapılmamış güvenlik duvarları en büyük fingerprinting hedefleridir. Örneğin, HTTP başlıklarını analiz ederek web uygulamasının yazılım dilini ve sürümünü belirleyebilir ve bu özelliklere göre saldırı planlayabilir. Siber güvenlikte parmak izi tanımlama (fingerprinting), ağ protokollerini, işletim sistemlerini, donanım cihazlarını, yazılımları ve diğer unsurları tanımlamak için kullanılabilecek bir dizi bilgiye atıfta bulunur. Saldırganlar, hedefleri hakkında maksimum bilgiyi toplamak için saldırılarının ilk adımı olarak parmak izi tanımlamayı kullanır. Ancak saldırganlar, hedef sistemlerdeki zafiyetleri belirlemek ve bunları istismar etmek amacıyla bu bilgileri kullanır. Parmak izi tanımlama, saldırganlara işletim sistemi türü, işletim sistemi sürümü, SNMP (Simple Network Management Protocol – Basit Ağ Yönetim Protokolü) bilgileri, etki alanı adları, ağ blokları, Sanal Özel Ağ noktaları ve daha fazlası gibi değerli bilgiler sağlayabilir. Hedef ağ hakkında ayrıntıları toplamak için saldırganlar genellikle özel paketler gönderirler. Bu paketler hedef ağdan dijital imza şeklinde yanıt aldığında, saldırganlar bu yanıtları analiz ederek işletim sistemi, yazılım ve protokolleri belirleyebilirler. Bu, saldırganların saldırılarını özelleştirerek hedef sistemlere maksimum zarar vermelerini sağlar (Cyware, t.y.).

3.1.3.13. SQL Enjeksiyonu

SQL enjeksiyon (SQL Injection) saldırıları, web uygulamaları için ciddi bir güvenlik tehdidi oluşturur. SQL, Structured Query Language olarak kabul edilen Yapılandırılmış Sorgu Dili'dir ve veritabanları üzerinde kullanılır. Saldırganlar, bir web uygulamasının kullanıcı giriş bölümlerini, arama motorlarını veya diğer veri giriş alanlarını hedef alarak kötü amaçlı SQL sorguları enjekte etmeye çalışır. Siteye girilen misafir girdileri protokollere uygun olarak işlenmez ve filtreden geçmezse, zararlı kodlar web sitesine SQL sorgusu şeklinde enjekte edilebilir. Bu tarz saldırılar, SQL sürümüne de bağlı olarak veritabanını manipüle edebilir ve verilmek istenmeyen bilgileri veritabanından çekebilir. Örneğin, veri girişi bölümlerine yazılabilen '1' = '1' girdisi, bu koşulun sürekli doğruluğu sağlaması nedeniyle tüm verileri gösterebilir. Saldırganların bu yöntemle uygulamaların altında yatan veritabanlarına ve potansiyel olarak hassas bilgilere sınırsız erişim elde etmeleri mümkündür. Araştırmacılar ve uygulayıcılar SQL enjeksiyon problemini ele almak için çeşitli yöntemler önermiş olsa da, mevcut yaklaşımlar ya sorunun tam kapsamını ele almakta başarısız olmakta ya da kullanımlarını ve benimsenmelerini engelleyen sınırlamalara sahiptir. Birçok araştırmacı ve uygulayıcı, SQL enjeksiyon açıklarından yararlanmaya

çalışan saldırganların kullanabileceği geniş teknik yelpazenin yalnızca bir alt kümesiyle aşinadır (Halfond, Viegas, & Orso, 2006, s. 1-2).

Şekil 11'deki görselde halka açık bir web sitesinde belirli bir Öğretmen ID'si girilmesi için alan bulunmaktadır. Saldırgan bu alana "teacherId=117 or 1=1" isteğini gönderdiğinde Web Uygulama Sunucusu bu isteği veritabanına 117 numaralı öğretmeni veya tüm verileri gönder şeklinde iletir. Veritabanı da tüm öğretmenlere ait verileri sunucuya gönderir, sunucu da saldırgana.

Şekil 11

Basit bir SQL Enjeksiyon Saldırısı Örneği



Wallarm SQL Injection, Wallarm, t.y.

3.1.3.14 MAC Maskeleme:

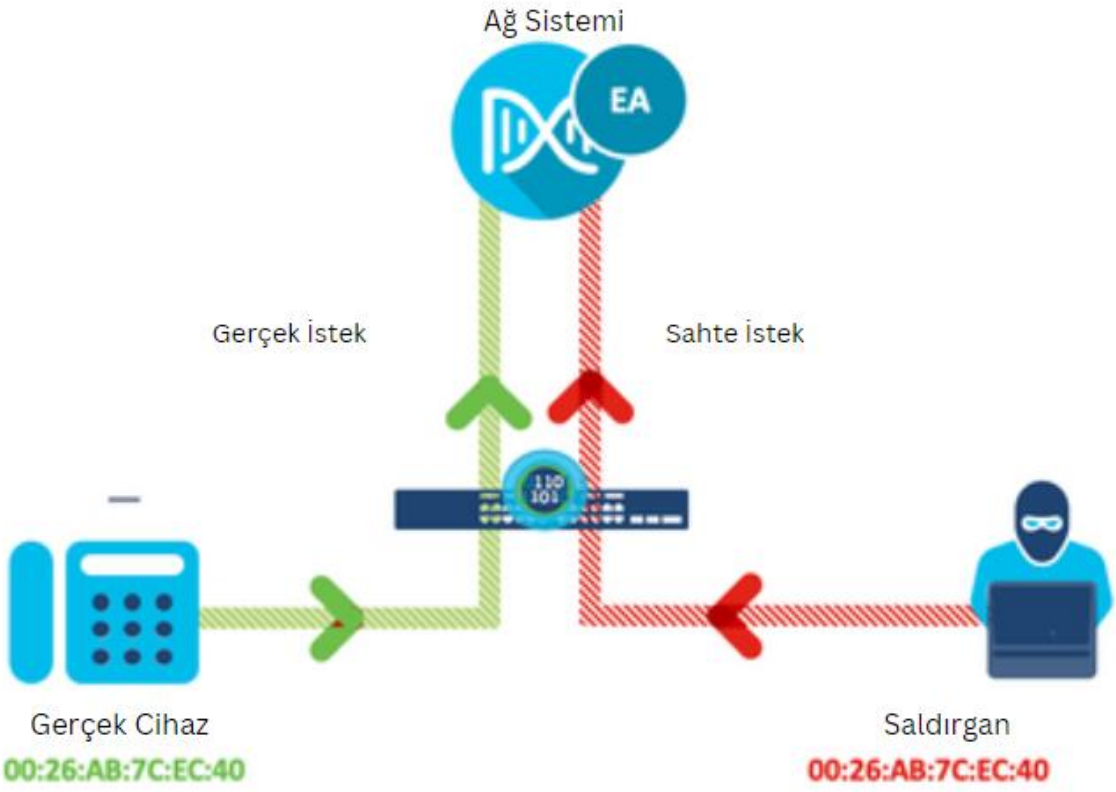
MAC Maskeleme (MAC Spoofing), ağdaki cihazların kimlik doğrulaması için kullandığı MAC adresini taklit etmeyi amaçlayan bir saldırı tekniğidir. Her cihazın, PC'lerden telefonlara, kenar anahtarlardan sunuculara kadar, ağ kartlarında bulunan benzersiz bir MAC adresi vardır. Bu adresler, genellikle donanım üreticisi tarafından atanır ve cihazın ağdaki benzersiz kimliğini temsil eder. MAC adresleri, 12 haneden oluşan bir kod içerir. Genellikle ilk dört hane üretici firmayı, son sekiz hane ise cihazı tanımlayan benzersiz bir kodu temsil eder. MAC Spoofing saldırıları, saldırganın gerçek cihazların üzerinde bulunan MAC adreslerini maskelemesi ve sisteme güvenilir bir cihazmış gibi göstermesiyle gerçekleşir. Bu, bir cihazın gerçek MAC adresinin çalınması ve saldırganın kendi cihazında bulunuyormuş gibi maskelenmesi anlamına gelir. Saldırgan, bu yöntemle sisteme sızdıktan sonra iletişimi izleyebilir, trafiği yönlendirebilir veya tamamen manipüle edebilir. MAC Spoofing genellikle ağ güvenliği testlerinde veya kötü niyetli saldırılarda kullanılır. Ağ

yöneticileri, bu tür saldırılara karşı korunmak için cihazların güvenlik ayarlarını düzenlemeli, ağ trafiğini izlemeli ve güvenlik duvarları gibi koruma önlemlerini uygulamalıdır (Singh, Sharma, Sharma, & Vyas, 2022, s. 10).

Saldırgan gerçek cihazın daha önceden ele geçirdiği, MAC adresi bilgisini kendi MAC adresi üzerine maskeleyerek, sisteme gerçek bir cihaz gibi sızmaya çalışmaktadır. Bu saldırı türü Şekil 12'de görülmektedir.

Şekil 12

MAC Maskeleme Saldırısı Temel Yöntemi



Cisco Mac Spoofing, Cisco Networks, 2022

3.1.3.15. Sıfırıncı Gün:

Sıfırıncı gün (Zero Day Exploit) bir güvenlik açığı, henüz yaması çıkarılmamış ancak açıklanmış bir sistem veya cihazdaki bir zayıflıktır. Bu tür bir güvenlik açığına saldıran bir sızma, sıfırıncı gün sızması olarak adlandırılır. Sıfırıncı gün güvenlik açıkları, henüz güvenlik araştırmacıları ve yazılım geliştiricilerinin farkında olmadıkları için kullanıcılar için daha yüksek risk taşır. Siber suçlular, bu açıkları hızla sömürerek saldırılarını

gerçekleştirmeye çalışırlar. Yama sağlayıcı bir düzeltme yayınlamadan önce, savunmasız sistemler bu tür saldırılara karşı açıkta kalır. Sıfırıncı gün güvenlik açıkları genellikle hedefe yönelik saldırılarda kullanılsa da, birçok saldırganlar hala eski açıkları kullanır. Saldırganın sistemdeki mevcut yazılımsal veya donanımsal güvenlik açıklarını sömürerek ağa tamamen sızabileceği bir saldırı türüdür. Genellikle, yazılım veya donanım sağlayıcılarının henüz bir düzeltme yayınlamadığı güncel güvenlik açıklarını hedef alır. Sağlayıcılar, sürekli olarak sistemlerini iyileştirmek ve düzeltmek için test ekipleri ile çalıştıkları için, genellikle bir süre sonra kapatılan zayıflıkları hedef alır (Trend Micro, t.y.).

Sıfırıncı gün kapsamında bahsedilen atak türleri, üreticilerin test ekipleri tarafından güncel olarak takip ve tespit edilerek en hızlı şekilde çözümlenmeye çalışılmaktadır. Özellikle büyük üreticiler sadece güncel siber tehditleri takip edecek "Zero day Exploit" ekipleri barındırmaktadır. Zero Day Exploit veya Zero Day Attack, sistemlerde henüz tespit edilen zafiyetleri ifade eder. Güvenlik zafiyetinin sıfırıncı günü yani başlangıç günü manasına gelen bu saldırılar her üretici donanımı, yazılımı veya ağ sisteminde meydana gelebilir. Ulusal ve uluslararası bilişim sektörlerinde firmaların en büyük güçleri ise bu açıkları hızlıca çözebilmeleri ve yama geçebilmeleri ile bilinir olmalarıdır. Zero Day Exploit'leri saldırganların devamlı sistem taramaları ve saldırıları, beyaz şapkalı hackerların veya üretici test mühendislerinin sistemlere sürekli olarak düzenlediği zafiyet testleri ile ortaya çıkar ve firmalar tarafından hızlıca yamalanmaya çalışılır. Bu testlerin konuları yazılım kodu inceleme, ağ trafiğini analiz etme ve zararlı enjeksiyon simülasyonları gibi daha bir çok yöntemleri içerir. Eğer zafiyeti saldırganlar yakalarsa, hemen başka zararlı yazılımlar veya kodlar geliştirerek, sistemi istismar etmek üzere pozisyonlanırlar. Sızma işlemini gerçekleştirebilirlerse sisteme daha da zarar verecek her türlü saldırıyı yapabilirler. Eğer savunma tarafında bulunan ekiplerce zafiyet tespit edilirse, üretici hemen yama yapmaya ve zafiyeti onarmaya yönelik yamalar yayınlamak üzere çalışmalara başlar. Zero Day Exploit'leri kullanımı daha yaygın olan ürünler üzerinde daha fazla sayıda meydana gelebilir çünkü saldırganlar en fazla kullanıcıyı enfekte edebilecekleri sistemlere en büyük saldırı ve taramalarını yöneltirler. Üreticinin kullanılırlığının ve güvenilirliğinin fazla olması da sıfırıncı gün açıklarını kapatabilmesi için daha fazla kaynak ve imkana sahip olması ile doğru orantılıdır (Kaspersky, t.y.).

Sıfırıncı gün açıkları o kadar kritiktir ki sadece bu alanda çalışarak mevcut sıfırıncı gün saldırılarını tespit edebilen, siber güvenlik uzmanları veya amatör katılımcılara milyon dolarlara varan ödüller veren Zerodium bilgi güvenliği şirketi kurulmuştur. Bu şirketin resmi web sitesine "zerodium.com" adresinden ulaşılabilir. İşletim sistemleri, web tarayıcıları,

standart uygulamalar, mobil cihazlar, web sunucuları, mail sunucuları, web uygulamaları ve iletişim teknikleri üzerinde bulunacak zero day açıklarına yüklü miktarda ödüller ödeyen bir şirket olarak faaliyet göstermektedir “Zerodium”. Ödenen ödüller 10.000$’dan başlayarak 2.500.00$’a kadar çıkabilmektedir (Zerodium, t.y.).

Siber güvenlik ekipleri ve sistemleri tüm bu Siber Güvenlik Tehditlerini savuşturmak üzere bir çok teknik geliştirmişlerdir. Bunlar temelde, Güçlü Parola ve Kimlik Doğrulama teknolojileri kullanılması, güçlü güvenlik yazılımları kullanılması ve güncellemelerinin düzenli alınması, son kullanıcıların bilinçlendirilmesi, güvenlik duvarları ve olay yönetimi sistemlerinin proaktif olarak kullanılarak sistemin korunması ve trafiğin izlenmesi, gizlilik ve veri şifreleme yöntemlerinin (SSL/HTTPS/TLS/IPSec/VPN) aktifleştirilmesi, güvenlik politikalarının belirlenmesi ve uygulanması, güvenlik zaafiyetlerinin düzenli olarak taranarak sistemlerin güncellenmesi ve elbette fiziksel güvenliğin sağlanması olarak özetlenebilir.

3.2. Örnek Vaka Analizleri

Siber saldırıların tarihi, teknik, politik, ekonomik ve sosyal açılardan ele alınabilir. Teknik açıdan bakıldığında, defalarca tekrarlanan bir ders vardır: Teknoloji ilerledikçe ve evrildikçe, kötü amaçlı saldırı türleri da aynı şekilde gelişir ve evrilir. Hiçbir teknoloji, saldırganlara ve saldırılara karşı tamamen güvenli olamaz. Ancak alınacak önlemler siber saldırı risklerini minimize ederek kabul edilebilir seviyelere çekebilir. Bu önlemler gelişmiş kimlik doğrulama metotları kullanılması, kullanıcı farkındalığı oluşturulması ve sistem kaynaklarının doğru konfigüre edilmesi olarak özetlenebilir. Siber Saldırıların ekonomik boyutları, en iyimser tahminlerle bile şaşırtıcı derecede yüksektir. Yıllar boyunca milyarlarca dolar, kötü amaçlı yazılım, kimlik avı ve ağ sistemleri saldırılarına karşı korunmak ve savunmalar başarısız olduğunda ortaya çıkan hasarı temizlemek için harcanmaktadır. Bu bölümde, geçmiş yıllarda meydana gelmiş, sistemlerde yüksek maddi hasara neden olmuş veya fazla sayıda kullanıcıyı enfekte etmiş olan mobil siber güvenlik saldırılarından örnekler verilecektir. İncelenecek olan bu saldırılardan bazıları hem mobil hem mobil olmayan sistemleri topluca hedef almışken, bazıları ise direkt olarak mobil sistemleri saldırı yüzeyi olarak belirlemiştir (Checkpoint, t.y.).

3.2.1. Pegasus Yazılımı

Pegasus, İsrailli NSO Group tarafından geliştirilen ve iOS ve Android cihazları hedef alan bir casus yazılımdır. Dünyanın dört bir yanındaki gazeteciler, aktivistler ve politikacılar da dahil olmak üzere birçok kişiyi hedef almıştır. Bu casus yazılım, mobil cihazlara sızarak kullanıcıların kişisel bilgilerini, mesajlarını ve aramalarını izleyebilir. Amnesty International ise bu yazılım aleyhinde “Adli Yöntemler Rapor”unu yayınlamıştır. Bu rapor; NSO Group'un Pegasus casus yazılımının yalnızca "terörizm ve suçları araştırmak" için kullanıldığı ve "hiçbir iz bırakmadığı" iddialarının gerçeği yansıtmadığını gösteren, çeşitli kuruluşlar arasındaki işbirliğini ve Amnesty International'ın Güvenlik Laboratuvarı'nın kapsamlı analizlerini içermektedir. Amnesty International'ın Güvenlik Laboratuvarı'nın yürüttüğü derinlemesine adli analizler, dünya genelindeki insan hakları savunucuları ve gazeteciler tarafından yaygın, sürekli ve devam eden yasa dışı gözetim ve insan hakları ihlallerini ortaya çıkarmıştır. Bu Adli Yöntemler Raporu, Pegasus casus yazılımı ile hedeflenen iOS ve Android cihazlarında bırakılan adli izleri belgelemektedir. Bunlar, insan hakları savunucularına yönelik 2016'daki Pegasus saldırılarına kadar uzanan ve bu saldırıları

son döneme kadar takip eden adli kayıtları da içermektedir. Raporda belirtilen Pegasus saldırıları 2014 yılından 2021 yılının Temmuz ayına kadar olan dönemi kapsamaktadır. Bunlar, hedeften herhangi bir etkileşim gerektirmeyen "sıfır tıklama" saldırılarını da içerir. Sıfır tıklama saldırıları, 2018 Mayıs ayından bu yana gözlemlenmiş olup, en son Temmuz 2021'de iOS 14.6 çalıştıran tamamen güncellenmiş bir iPhone 12'yi hedef alan birden fazla sıfır günü kullanılarak başarılı bir şekilde gerçekleştirilmiştir. Raporun 1 ile 8. bölümleri, Pegasus enfeksiyonunu takiben mobil cihazlarda bırakılan adli izleri açıklamaktadır. Bu kanıtlar, farklı ülkelerdeki insan hakları savunucularının ve gazetecilerin telefonlarından toplanmıştır. Son olarak, raporun 9. bölümü, NSO Group'un 2016'dan bu yana Pegasus ağ altyapısının evrimini belgelemektir. Şirket, birden fazla katmanlı alan adı ve sunucu kullanarak saldırı altyapısını yeniden tasarlamıştır. Tekrarlanan operasyonel güvenlik hataları, Amnesty International Güvenlik Laboratuvarı'nın bu altyapıya sürekli olarak görünürlük sağlamasını mümkün kılmıştır (Amnesty International, 2021).

Pegasus genellikle "Zeroday" güvenlik açıklarından yararlanarak hedef cihaza bulaşır. Pegasus'un geliştiricileri, bu tür açıkları kullanarak hedef cihaza kötü amaçlı yazılımı enjekte eder. Kendine özel bir saldırı metodundan ziyade güncel olarak hangi “Zero Day” en fazla cihazı enfekte edebiliyorsa o açığı kullanarak mobil sistemlere sızar. Pegasus yazılımının tam olarak kaç kullanıcıyı etkilediği kesin olarak bilinmemektedir. Çünkü Pegasus saldırıları genellikle gizlice gerçekleştirilmiştir ve tespiti zordur. Bununla birlikte, saldırı türlerinin çeşitliliği ve sıfır tıklama saldırılarının da kullanılması, Pegasus'un geniş bir kullanıcı kitlesini etkilemiş olabileceğini düşündürmektedir.Bugüne kadar yapılan Mobil Siber Saldırıların en dikkat çekeni olan Pegasus Yazılımı’nı özel kılan şeyse kurbanın en ufak bir işlem dahi yapmadan sıfır-tıklama saldırısına maruz kalması ve sonrasında kapsamlı Adli Bilişim yöntemleri ile incelense dahi iz bırakmayabilecek saldırı metotlarının kullanılmış olmasıdı. Pegasus'un yaygın olarak kullanılan bir diğer saldırı vektörü ise sosyal mühendislik yöntemleridir. Bu, hedefin güvenini kazanmak için manipülatif taktikler kullanmayı içerir. Örneğin, sahte bir e-posta veya metin mesajı aracılığıyla, kullanıcının tıklaması için tehlikeli bir bağlantı veya dosya gönderebilirler (Raiu, 2022).

3.2.2. Blueborne Zayıflığı

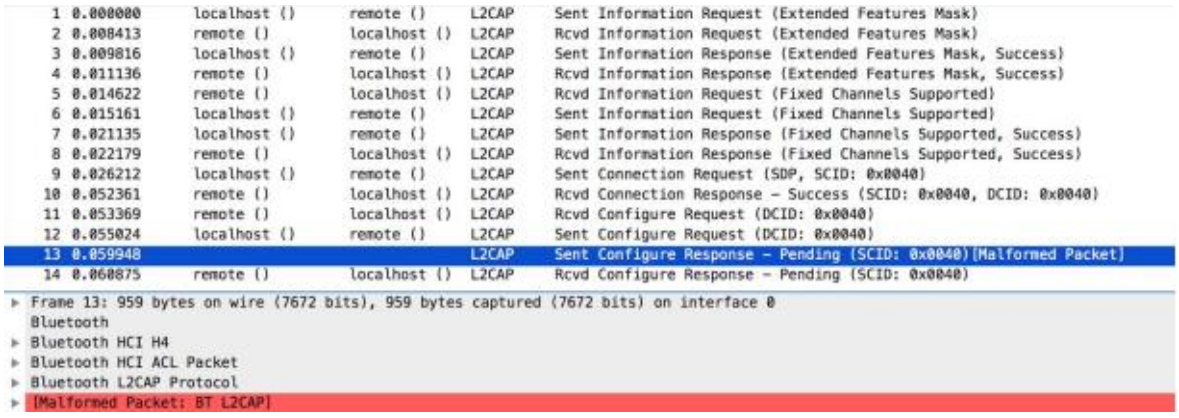
Eylül 2017'de, büyük mobil, masaüstü ve IoT işletim sistemlerini tehlikeye atan yeni bir saldırı vektörü bildirilmiştir. Bu saldırı vektörü, Android, iOS, Windows ve Linux gibi işletim sistemlerini ve bu sistemleri kullanan cihazları etkilemiştir. "BlueBorne" adı verilen

bu yeni vektör, hava yoluyla (airborne) yayıldığı ve cihazlara Bluetooth aracılığıyla saldırdığı için bu adı almıştır. BlueBorne, saldırganların cihazların kontrolünü ele geçirmesine, kurumsal verilere ve ağlara erişmesine, güvenli “air-gapped” yani fiziksel olarak izole ağlara sızmasına ve kötü amaçlı yazılımları bitişik cihazlara yatay olarak yaymasına olanak tanımıştır. Bu güvenlik açıkları Google, Microsoft, Apple, Linux ve Amazon'a bildirilmiştir ve sorumlu açıklama sürecinin bir parçası olarak yamalar belirlenip yayımlanırken onlarla işbirliği yapılmıştır. BlueBorne, birçoğu iş yerinde kullanılan 5,3 milyardan fazla cihazı etkilemiştir. Bu cihazların 1,2 milyardan fazlası “forever day” olarak tanımlanmış ve yamalanamaz durumda kalmıştır.

Blueborne Zayıflığı, Bluetooth'un bazı sürümlerinde bulunan ve kötü niyetli saldırganların cihazlara kötü amaçlı kod enjekte etmesine, hedef cihazları ele geçirmesine ve hatta hassas bilgilere erişmesine izin veren kritik hataları içerir. Blueborne açığının en dikkat çekici yanı, "Bluetooth ile ilgili tam olarak kontrol edilmemiş veri girişleri" olarak bilinen bir kategoriye ait olmasıdır. Bu tür bir saldırı, kötü niyetli bir cihazın hedef cihaza gönderdiği özel olarak oluşturulmuş Bluetooth mesajları aracılığıyla gerçekleştirmesidir. Bu mesajlar, hedef cihazın Bluetooth sürücüsünde bir bellek taşması (Buffer Overflow) veya diğer kötü amaçlı kod enjeksiyonu saldırılarına neden olabilir. BlueBorne ayrıca "yan kanal saldırıları" adı verilen bir tür saldırıyı da içerir. Bu saldırı türü, Bluetooth bağlantısı üzerinden iletilen bilgilerin izlenmesini ve çözülmesini içerir. Bu şekilde, saldırganlar hedef cihazın Bluetooth trafiğini dinleyebilir ve hatta şifreli iletişimi çözebilirler (Seri & Vishnepolsky, 2023, s. 39-40). Şekil 13’te de bozulmuş paketin sistemce tespiti görülmektedir.

Şekil 13

Blueborne Atağının Tespiti



Armis Inc, Armis Inc Blueborne, 2023

Tüm Android telefonlar, tabletler ve giyilebilir cihazlar (yalnızca Bluetooth Low Energy kullananlar hariç) Android işletim sisteminde bulunan dört güvenlik açığından etkilenmiştir. Bu güvenlik açıklarından ikisi uzaktan kod yürütülmesine olanak tanır (CVE-2017-0781 ve CVE-2017-0782), biri bilgi sızıntısına yol açar (CVE-2017-0785) ve sonuncusu saldırganın Ortadaki Adam (Man-in-The-Middle) saldırısı gerçekleştirmesine izin verir (CVE-2017-0783). Google, bu güvenlik açıklarını gidermek için 4 Eylül 2017 tarihinde Eylül Güvenlik Güncellemesi ve Bülteni kapsamında bir güvenlik güncellemesi yayınlamıştır. iOS 9.3.5 ve altı sürümlere sahip tüm iPhone, iPad ve iPod touch cihazları ile 7.2.2 ve altı sürümlere sahip Apple TV cihazları, uzaktan kod yürütme güvenlik açığından (CVE-2017-14315) etkilenmiştir. Bu güvenlik açığı, Apple tarafından iOS 10'da zaten hafifletilmiş olduğundan, bunu gidermek için yeni bir yamaya gerek yoktur (Armis Cyber Security, 2018, s. 1-4).

3.2.3. XcodeGhost

XcodeGhost, Apple'ın resmi yazılım geliştirme aracı olan Xcode'un kötü amaçlı bir sürümüdür. Bu kötü amaçlı yazılım, Xcode'un çeşitli versiyonlarının değişime uğratılarak geliştiricilere dağıtılması sonucu ortaya çıkmıştır. XcodeGhost, geliştiricilerin farkında olmadan uygulamalarına kötü amaçlı kod eklenmesine neden olmuş ve bu uygulamaların da Apple'ın uygulama mağazasına yüklenmesine sebep olmuştur. XcodeGhost, Çin'deki geliştiricilerin Xcode'u Apple'ın resmi kaynaklarından indirmekte zorlanmaları ve bunun yerine üçüncü parti kaynaklardan indirmeyi tercih etmeleri sonucunda yayılmıştır. Üçüncü parti kaynaklardan indirilen bu Xcode sürümleri, kötü amaçlı kod içermiştir. XcodeGhost, Xcode ile derlenen her uygulamanın içine kötü amaçlı bir kod enjekte etmiştir. Bu kod, uygulama çalıştırıldığında kullanıcı verilerini toplayarak belirli sunuculara göndermiştir. Ayrıca, kötü amaçlı yazılım çeşitli komutları uzaktan yürütme yeteneğine de sahiptir (Xiao, 2015).

Kötü amaçlı yazılım, kullanıcıların kişisel bilgilerini (örneğin, cihaz adı, ağ bilgileri, vs.) toplamış ve bu bilgileri uzaktaki bir sunucuya göndermiştir. Saldırganlar, uygulamalar aracılığıyla uzaktan komutlar çalıştırabilmişlerdir. Ayrıca, kullanıcılara sahte bildirimler göndererek kimlik avı saldırıları gerçekleştirme potansiyeli de bulunmuştur. XcodeGhost,

ilk olarak 2015 yılında Palo Alto Networks tarafından keşfedilmiştir. Yapılan analizler sonucunda birçok popüler uygulamanın kötü amaçlı yazılım ile enfekte olduğu tespit edilmiştir. Bu uygulamalar arasında WeChat, Didi Chuxing, ve Çin'de oldukça popüler olan bazı diğer uygulamalar da yer almıştır (Xiao, 2015).

PaloAlto Networks, XcodeGhost'un yüz milyonlarca cihazı etkilediğini raporlamıştır. Apple, etkilenen uygulamaları App Store'dan kaldırmış ve geliştiricilere resmi Xcode sürümünü kullanmaları gerektiği konusunda uyarılar yapmıştır. Ayrıca, etkilenen uygulamaların yeniden derlenip mağazaya yüklenmesi sağlanmıştır. Apple, Xcode'un güvenli sürümlerini ve indirilebilir bağlantılarını geliştiricilerle paylaşmıştır. Geliştiricilere, yalnızca güvenilir kaynaklardan yazılım indirmeleri ve kullanmaları gerektiği konusunda eğitimler vermiştir. XcodeGhost saldırı, siber güvenlik farkındalığını artırmış ve geliştiricilerin yazılım geliştirme araçlarını güvenilir kaynaklardan indirmeleri gerektiğini bir kez daha vurgulamıştır. Ayrıca, Apple'ın uygulama mağazası güvenlik protokollerini gözden geçirmesini ve güçlendirmesini sağlamıştır.

Bu tür olayların tam maliyetini ölçmek zor olsa da, hem kullanıcılar hem de şirketler üzerinde önemli finansal ve güvenlik etkileri olduğu kesindir. Kullanıcı güveninin sarsılması ve veri ihlallerinin yaratabileceği uzun vadeli etkiler de göz önünde bulundurulmalıdır (Intego MAC Security, 2021).

3.2.4 HeartBleed Açığı

Heartbleed, resmi adıyla CVE-2014-0160, 2014 yılında keşfedilen, OpenSSL kriptografik yazılım kütüphanesinde ciddi bir güvenlik açığıdır. Bu zayıflık, normal koşullar altında İnternet'i güvence altına almak için kullanılan SSL/TLS şifrelemesi tarafından korunan bilgilerin çalınmasına olanak tanımıştır. SSL/TLS, web, e-posta, anlık mesajlaşma ve bazı sanal özel ağlar (VPN'ler) gibi uygulamalar için İnternet üzerinde iletişim güvenliği ve gizliliği sağlar. Bunu da uçtan uca şifreleme metodu olarak hizmet ederek yapar. Heartbleed açığı, İnternet'teki herhangi bir kişinin, savunmasız OpenSSL yazılımının koruduğu sistemlerin belleğini okumasına izin vermekteydi. Bu, hizmet sağlayıcıları tanımlamak ve trafiği şifrelemek için kullanılan gizli anahtarların, kullanıcıların isim ve şifrelerinin ve gerçek içeriğin tehlikeye girmesine neden olmuştur. Bu da saldırganların iletişimleri dinlemesine, hizmetlerden ve kullanıcılardan doğrudan veri çalmasına ve hizmetler ve kullanıcılar gibi davranmasına olanak tanımıştır. (Synopsys Inc., 2020).

OpenSSL'in Heartbeat Uzantısı'nın uygulamasında, herhangi bir uç noktanın,

HeartbeatRequest mesajındaki veri miktarından daha büyük bir yük uzunluğu belirterek, eşleştiği cihazın belleğindeki yük mesajını takip eden verileri okumasına izin veren bir güvenlik açığı meydana gelmiştir. Yük uzunluğu alanı iki bayt olduğundan, eş, 216 bayta (~64 KB) kadar bellekle yanıt verir. Hatanın kendisi basitti: Saldırgan tarafından kontrol edilen bir mesajın saldırgan tarafından belirtilen uzunluğuna sistemlerce güvenilmesi. OpenSSL yaması, yük uzunluğu alanı yükün uzunluğunu aştığında HeartbeatRequest mesajını geçersiz kılan bir sınır denetimi eklemiştir. Ancak, hata kolayca kavranabilir ve düzeltmesi basit olmasına rağmen, hatanın potansiyel etkisi ciddidir: bir saldırganın özel belleği okumasına izin verir, bu da güvenli kanal üzerinden aktarılan bilgileri ve kriptografik sırları içerebilmektedir. Açığın yaygın olduğu ve Alexa Top Bir Milyon'daki HTTPS destekli sunucuların %24-55'inin başlangıçta savunmasız olduğu, buna Alexa Top 100'den 44 sitenin de dâhil olduğu tespit edilmiştir. Açığın ortaya çıkmasından sonraki ilk iki hafta içinde siteler yoğun bir şekilde yamalanmıştır, ancak yamalama süreci daha sonra duraklamıştır ve iki ay sonra Alexa Top 1 Milyon HTTPS sitelerinin %3'ü hala savunmasız kalmıştır. Ayrıca, savunmasız sitelerin sadece %10'unun sertifikalarını değiştirdiği, buna karşın %73'ünün yamalandığı ve sertifikalarını değiştiren sitelerin %14'ünün aynı özel anahtarı kullanarak hiçbir koruma sağlamadığı gözlemlenmiştir (Durumeric, ve diğerleri, 2014, s. 476-486).

3.2.5. Equifax Veri Sızıntısı

7 Eylül 2017'de, Equifax 143 milyon kullanıcıyı etkileyen bir siber güvenlik olayı duyurmuştur. Bu sayı kısa sürede 148 milyona yükselmiştir neredeyse Amerika Birleşik Devletleri nüfusunun yarısı ve Amerikan yetişkinlerinin %56'sı. Equifax ABD'deki birkaç büyük Tüketici Raporlama ajansından biridir. Bu ajanslar, tüketicilerden bilgiyi gönüllü olarak toplamazlar ve tüketicilerin bu veri toplama sürecinden çıkmaları mümkün de değildir. Özellikle bilgi paylaşımını kolaylaştırma hizmeti sunmaları nedeniyle bu ajansların elinde büyük miktarda hassas kişisel veri bulunmaktadır. Elbette bu veri büyüklüğü siber suçluları cezbetmektedir. CVE-2017-5638 koduyla bilinen Equifax Veri Sızıntısı, Apache Struts – ki bu açık kaynaklı bir web uygulama çatısıdır - adlı orta yazılımın, "Apache Commons FileUpload" kütüphanesinde bulunan ve karşı taraftan uzak bir kod çalıştırılmasına olanak tanıyan bir zafiyeti nedeniyle meydana gelmiştir. Bu güvenlik açığı, Apache Struts 2.0.0 ile 2.3.33 arasındaki sürümlerde bulunan ve "Content-Type" başlığındaki bir değerin doğrulanmamasından kaynaklanmıştır. Saldırganın özel olarak

oluşturulmuş bir HTTP isteği göndererek uygulamanın yetkilendirme mekanizmasını atlatmasına izin vermiştir. Saldırganlar bu açığı kullanarak uygulamanın sistemlerine sızabilmiş ve hassas bilgilere erişebilmişlerdir. Saldırganlar, sistemler birbirinden yeterince ayrılmadığı için web portalından diğer sunuculara geçmeyi başarmış ve daha sonra düz metin olarak depolanan kullanıcı adlarını ve şifreleri buldumuş, bu sayede daha fazla sistemlere erişim sağlamışlardır. Saldırganlar bu zafiyeti kullanarak Equifax veri tabanlarına sızmış ve büyük miktarda hassas kişisel veriye erişmişlerdir (U.S. House of Representatives, 2018, s. 2-92).

ABD nüfusunun yarısına ait hassas kişisel bilgileri ele geçiren saldırganlar, bu bilgileri kişilere karşı başka saldırılar planlamak üzere kullanmışlardır. ad-soyad, doğum tarihi, sosyal güvenlik numaraları, kredi kartı bilgileri, adresler hatta sürücü ehliyet numaraları gibi kişisel bilgilerin ifşası, mağdurların finansal uygulamalarını, mobil kimlik doğrulama sistemlerini ve diğer kişisel verilerini tehdit altına sokmuştur. Bu veriler kullanılarak birçok oltalama yöntemi ile siber güvenlik suçları işlenmiştir. Sahte telefon çağrıları, kısa mesajlar ve e-postalar üzerinden mobil kullanıcı hedef alınmıştır. Bu oltalama saldırılarında hem finansal uygulamalar ve SMS tabanlı çift faktörlü doğrulama sistemleri güven kaybetmiştir hem de sahte SMS ve e-postalar ile mobil cihazlara sızdırılan zararlı yazılımlar sistem güvenilirliğini azaltmıştır, bu sebeplerle başka saldırılara yüzey alanı meydana getirmiştir. Bu saldırı neticesinde Equifax'a ABD Federal Ticaret Komisyon'u tarafından 700 milyon doların üzerinde para cezası kesilmiştir (Federal Trade Commission, 2019).

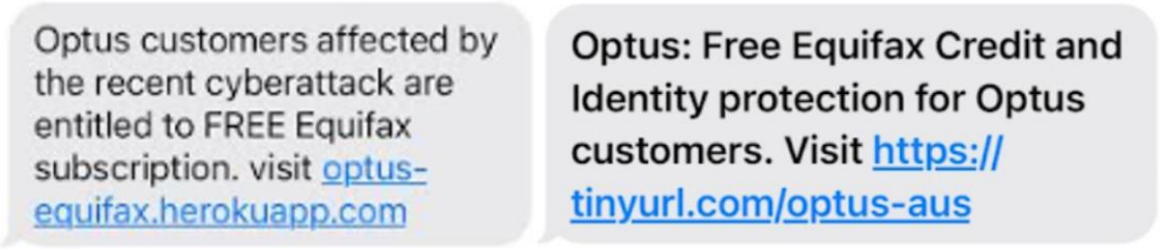
Sızıntının gerçekleşmesinin akabinde birçok siber güvenlik firması, alınması gereken önlemlere dair hızlı raporlar hazırlamışlardır. Bu raporlar son kullanıcıya, dikkatlice kredi raporlarının izlenmesi, sıra dışı veya doğrulanmamış işlemler, tanınmayan şirketlerden gelen kredi sorguları ve yanlış kişisel bilgilerin kontrol edilmesi tavsiyelerinde bulunmuştur. Bu işaretler genellikle kredi kartı dolandırıcılığına işaret etmektedir. Tüm finansal işlemlerin durdurulması ve banka hesaplarının kilitlenmesi gerekebilir. Sızıntı sonrası, hesapların yeniden açılabilmesi için benzersiz PIN belirlenmesi önemlidir. Sahte işlem uyarı sistemi, kişi adına hesap açıldığında, kredi alındığında veya başka finansal faaliyetlerde bulunulduğunda kurbanı uyarır. Ayrıca kişisel vergilerin hızla hazırlanması gerekebilir; çünkü kişisel bilgileri ele geçiren saldırganlar, mağdurlar adına sahte vergi iadeleri dosyalayabilir veya iadeleri mağdurlar adına talep edebilir. Sosyal Güvenlik Numarası değiştirilmesi veya sızıntı sonucunda Ad-Soyad ve adres bilgilerinin yayılması, saldırganların mağdurlar adına bankaları dolandırmalarına, mağdurların Sosyal Güvenlik

haklarından yararlanmalarına ve suç teşkil eden her türlü faaliyette kullanmalarına yol açabilir. En önemli uyarı, mobil oltalama saldırılarına karşı dikkatli olunması gerektiğidir. Çalınan kişisel veriler, mağdurlara yönelik telefon çağrıları, sahte SMS ve e-postalar aracılığıyla kullanılabilir ve bu durum daha fazla verinin çalınmasına neden olabilmektedir (Trend Micro, 2017).

Şekil 14'te Equifax Veri Sızıntısı sonucu, verileri sızmış kişilere gönderilen oltalama SMS'leri bulunmaktadır.

Şekil 14

Equifax Sızıntısı Sonrası Kullanıcılara Gelen Oltalama SMS'leri



(Equifax, 2024)

İncelenen örnekler, alakalı oldukları siber güvenlik konularında dünya çapında bilinen ve otoriteler tarafından incelenerek raporlaştırılmış olaylardır. Pegasus yazılımı; Zero Day açıklarını, Blueborne; Bluetooth sürüm güvensizliklerini, XcodeGhost; Malware'yi, HeartBleed; Ağ sistemleri elemanlarından olan SSL'in manipüle edilmesini, Equifax veri sızıntısı ise uzaktan kod yürütme metotlarını, kullanmışlardır.

4. BÖLÜM

ULUSLARARASI KURULUŞLAR VE STANDARTLAR, TEKNOLOJİK ÇÖZÜMLER

Mobil iletişim, modern dünyada bilgi paylaşımı ve iletişim için vazgeçilmez hale gelmiştir. Ancak bu geniş kullanım alanı, mobil cihazların ve ağların siber tehditlere karşı savunmasız hale gelmesine yol açmaktadır. Sistemlerin ve verilerin korunması için uluslararası kuruluşların standartları uygulanmalı, belirli periyotlarla yayınladıkları raporlar incelenerek tatbik edilmeli ve güncel teknolojinin sunduğu imkânlardan faydalanılmaldır. Bu bölümde mobil iletişim siber güvenliği konusunda önde gelen kuruluşlar ve standartlar ile teknolojik çözümler ele alınacaktır.

4.1. Uluslararası Kuruluşlar ve Standartlar

Mobil iletişim siber güvenliğinde, etkili politikalar, standartlar ve kullanıcı farkındalığı hayati öneme sahiptir. Güvenliğin sağlanması için, uluslararası kabul görmüş standartlar (örneğin, ENISA Threat Landscape, ISO/IEC 27001 ve NIST Cybersecurity Framework) temel alınarak oluşturulan politikalar, mobil cihazların ve verilerin korunmasında kritik rol oynamaktadır. Bu politikalar, cihaz yönetimi, veri şifreleme, kimlik doğrulama ve yetkilendirme gibi alanlarda ayrıntılı yönergeler sunmaktadır. Ancak, teknik önlemler tek başına yeterli değildir; kullanıcı farkındalığının artırılması da esastır. Kullanıcıların bilinçlendirilmesi, sosyal mühendislik saldırılarına karşı dirençlerini artırır ve güvenlik ihlallerini önlemeye yardımcı olur. Eğitim programları ve sürekli farkındalık kampanyaları, kullanıcıların güvenlik tehditleri konusunda bilgi sahibi olmalarını ve güvenlik politikalarına uygun davranmalarını sağlar. Böylelikle, mobil iletişim siber güvenliği alanında bütüncül bir yaklaşım benimsenmiş olur (SANS, t.y.).

Kurum ve kuruluşlar mobil cihazlardaki güvenliği sağlayabilmek amacıyla, güçlü politikalara ihtiyaç duymaktadırlar. Bu politikalar, ağda bulunan cihazların güvenli kullanımlarını ve uygun kişilerce öngörülen şekilde erişim sağlanmasını bu sayede potansiyel risklere karşı savunma yapılmasını sağlamaktadır. Temel olarak cihaz güvenliği, güncelleme politikaları, ağ erişim düzenlemeleri, veri yedekleme teknikleri, izin ve erişim kontrolleri ile bu savunma sağlanabilir. Bu politikaları belirlemek adına küresel çapta birçok organizasyon meydana getirilmiştir. Bahsedilen organizasyonlar aylık veya yıllık periyotlarla siber güvenlik tehditler konusunda farkındalığı artırmak ve kuruluşların yol

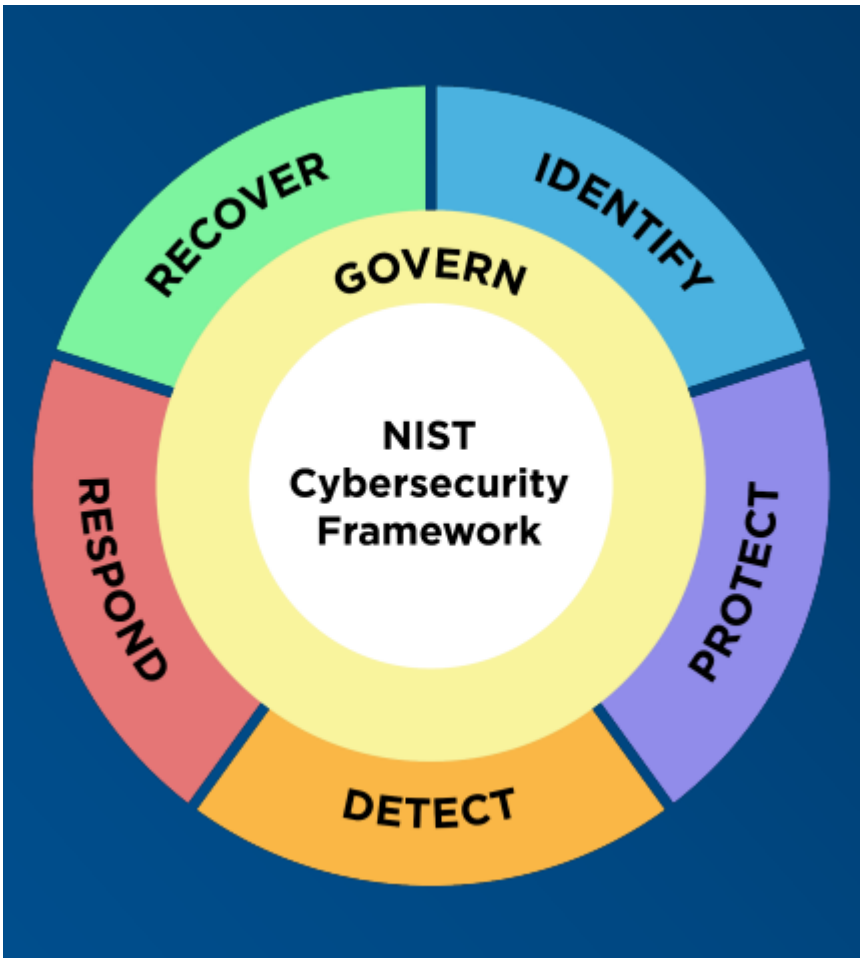
haritalarına öncülük etmek için raporlar hazırlamaktadırlar (ITIC, 2014).

4.1.1. Ulusal Standartlar ve Teknoloji Enstitüsü

Ulusal Standartlar ve Teknoloji Enstitüsünün (National Institute of Standards and Technology-NIST) belirlediği Siber Güvenlik çerçevesi 2.0 (NIST Cyber Security Framework), organizasyonlara, karşı karşıya kalabilecekleri siber saldırıları berteraf etmeleri amacıyla hazırlanmıştır. CSF 2.0, altı adet fonksiyonu içermektedir. Bunlar Govern(Yönet), Identify(Tanımla), Protect(Koru), Detect(Tespit et), Respond(Cevap ver) ve Recover(Kurtar) adımlarıdır. Bu çerçeve Şekil 15'te görsel hali ile verilmiştir.

Şekil 15

NIST Siber Güvenlik Çerçevesi 2.0



Cybersecurity Framework 2.0, NIST, 2024

Kuruluşun siber güvenlik risk yönetimi stratejisi, beklentileri ve politikalarını oluşturarak diğer fonksiyonlar arasında yönetim bağlantıları kurmayı hedefler. Bu kapsamda, mevcut siber güvenlik risklerinin anlaşılması ve belirlenmesi önem taşır. Risklerin yönetilmesi için kullanılan koruma yöntemleri anlaşılmalı ve sürekli olarak güncellenmelidir. Potansiyel siber güvenlik saldırıları ve ihlallerin erken tespiti ve analizi büyük önem taşır; bu sayede hızlı yanıt ve müdahale sağlanabilir. Tespit edilen siber güvenlik olaylarına karşı etkili bir yanıt planı oluşturulmalı ve uygulanmalıdır. Son olarak, meydana gelmiş siber güvenlik olaylarından etkilenen varlıkların ve operasyonların etkili bir şekilde yeniden yapılandırılması ve restore edilmesi gerekmektedir. Bu aşamalardan, Govern, tüm süreçler boyunca aktif bulunmakta ve diğer süreçler arasındaki birlikteliği sağlamaktadır. Identify süreci saldırı meydana gelmeden önce mevcut risklerin incelenmesi ve tam olarak anlaşılması aşamasıdır. Protect, risklerin tespit edilmesi akabinde koruma yöntemlerinin işletilmesidir. Detect, meydana gelen siber ihlallerin tespiti ve analiz edilmesi olarak görev yapmaktadır. Respond, siber güvenlik olaylarına karşı verilecek cevapları ifade etmektedir. Recover ise diğer aşamalardan sonra sistemlerin yeniden eski haline getirilmesi ve ayağa kaldırılmasını ifade etmektedir (National Institue of Standarts and Technology, 2024, s. 5-8).

4.1.2. Avrupa Birliği Siber Güvenlik Ajansı

Avrupa Birliği Siber Güvenlik Ajansı (European Union Agency for Cybersecurity-ENISA), Avrupa Birliği'nin siber güvenlik alanındaki yetkili kuruluşudur ve özellikle mobil tehditler konusunda kapsamlı çalışmalar yürütmektedir. "Mobile Threat Landscape Report" adlı periyodik rapor, mobil cihaz kullanıcıları, işletmeler ve güvenlik profesyonelleri için önemli bilgiler ve rehberlik sunar. Bu rapor, mobil tehditlerin çeşitliliğini, bu tehditlerin nasıl gerçekleştiğini ve alınması gereken önlemleri detaylı bir şekilde açıklamaktadır. En çok kullanılan siber saldırı metotları, fidye yazılımı, kötü amaçlı yazılım, kripto madenciliği, e-posta ile ilgili tehditler, veri tehditleri, kullanılabilirlik ve bütünlüğe yönelik tehditler, yanlış bilgilendirme – dezenformasyon, zararsız tehditler, tedarik zinciri saldırıları olarak tespit edilmiştir (ENISA, t.y.).

ENISA'nın her yıl düzenli olarak yayınladığı "Threat Landscape" raporu, 2023 yılında en yüksek siber güvenlik risklerini şu şekilde özetlemiştir: DDoS ve fidye yazılımı, en önemli tehditler arasında en üst sıralarda yer alırken, sosyal mühendislik, veri ile ilgili tehditler, bilgi manipülasyonu, tedarik zinciri ve kötü amaçlı yazılım bunları takip

etmektedir. Tehdit aktörlerinin servis-görünümlü programları profesyonelleştirmelerinde, çevreye sızmak, kurbanlara baskı yapmak ve onları zorla para koparmak için yeni taktikler ve alternatif yöntemler kullanarak yasadışı işlerini ilerletmelerinde belirgin bir artış gözlenmiştir. En çok hedef alınan sektörler, kamu yönetimi (%19), bireyler (%11), sağlık (%8), dijital altyapı (%7), finans ve ulaşım olarak tespit edilmiştir. Siber suçlular, 2023'te giderek daha fazla bulut altyapılarını hedef almakta ve fidye yazılımlarıyla değil, doğrudan kullanıcıları hedef alarak şantaj operasyonlarını artırmaktadır. Sosyal mühendislik saldırıları, Yapay Zeka (AI) ve yeni tür tekniklerin ortaya çıkmasıyla 2023'te önemli ölçüde artmıştır, ancak oltalama hala en yaygın saldırı vektörü olarak kalmaktadır. Klasik mobil kötü amaçlı yazılımların (örneğin, bankacılık truva atları) azalma gösterdiği bir dönemde, reklam yazılımları mobil cihazlar için yaygın bir tehdit olarak kalmaya devam etmektedir. Bununla birlikte, ticari casus yazılımın kullanımı, kullanıcı etkileşimi olmadan gözetim sağlayan gelişmiş sıfır-tıklama saldırıları tarafından desteklenerek artmaktadır (European Union Agency for Cybersecurity, 2023).

4.1.3. Uluslararası Standartlar Örgütü

Uluslararası Standartlar Örgütü (International Organization for Standardization-ISO), birçok alanda faaliyet gösteren, hiçbir devlete ya da hükümete bağlı olmayan uluslararası standartlar belirleyen bir organizasyondur. Mobil Siber güvenlik alanında ise 27001, 27002, 27017, 27018 ve 27701 standartlarını oluşturmuş, gerekli denetimleri yapmakta ve bilgi sistemlerinin sürekli iyileştirilip, güvenlik politikalarının doğru uygulanması için bu standartları geliştirmektedir.

27001 Standardı, bilgi güvenliği yönetim sistemlerinin kurmak, uygulamak, sürdürmek ve sürekli iyileştirmek için gereksinimleri belirlemektedir. 27002 Standardı, bilgi güvenliği yönetimi için ideal uygulama kontrollerini belirlemektedir. 27017 Standardı, bulut hizmetlerinde bilgi güvenliği kontrollerini kapsamaktadır. 27018 Standardı, kamuya açık bulut hizmetlerinde kişisel veri korunması için ideal uygulama kontrollerini belirlemektedir. 27701 Standardı, gizlilik bilgi yönetim sistemleri için gereksinimleri belirlemektedir. Bu standartlar, mobil iletişim siber güvenliği ile birlikte mobil olmayan iletişime yönelik gereksinimleri de içermektedir (International Organization for Standardization, t.y.).

ISO 27001 Standardı, bilgi güvenliği yönetim sistemlerinin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için kapsamlı bir çerçeve sunmaktadır. Bu standart, bilgi varlıklarının korunmasını sağlayarak kuruluşların itibarını, müşteri güvenini ve yasal

uyumluluğunu güvence altına almaya yönelik etkili bir yaklaşım meydana getirmektedir. Mobil cihaz güvenliği politikalarının oluşturulması ve uygulanmasında ISO 27001 Standardı temel alınması, kuruluşların mobil cihazlar üzerindeki güvenlik risklerini etkili bir şekilde yönetmelerine yardımcı olabilir (International Organization for Standardization, t.y.).

4.1.4. Siber Güvenlik ve Altyapı Güvenliği Ajansı

Siber Güvenlik ve Altyapı Güvenliği Ajansı (Cybersecurity and Infrastructure Security Agency-CISA), ABD İç Güvenlik Bakanlığı'nın (Department of Homeland Security-DHS) siber güvenlik ve altyapı güvenliğini sağlamak üzere 2018'de kurulan bir parçasıdır. Başlıca görevleri, ülkenin siber güvenlik savunmasını güçlendirmek, kritik altyapıların güvenliğini sağlamak, siber saldırılara karşı acil durum müdahaleleri yapmak, kamu ve özel sektör arasında bilgi paylaşımını teşvik etmek ve siber güvenlik konusunda eğitim-farkındalık konularında çalışmaktır. CISA, bu görevleri yerine getirirken, federal, eyalet ve yerel yönetimlerle, özel sektörle ve uluslararası ortaklarla iş birliği yapmaktadır. CISA'nın temel amacı ABD'nin siber ve fiziksel altyapılarını güvenli, dayanıklı ve dirençli hale getirmektir. Bu amaca hizmet etmek üzere, düzenli raporlar ve makaleler yayınlamakta, güvenlik politikaları oluşturarak günce tutmakta, eğitimler vermekte ve güncel tehditleri inceleyip yayınlamaktadır (Cybersecurity and Infastructure Security Agency, t.y.).

CISA, 2023 yılında yeni bir siber güvenlik programı açıklamıştır; "Secure Our World". Bu program son kullanıcının güvenli şekilde çevrimiçi kalabilmesini temelde dört basit adıma indirgeyerek şu şekilde öneride bulunmuştur:

- Tanınmayan veya alakasız mesajlarca istenilen kişisel verilere karşı dirençli olunmalı.
- Uzun, rastgele, sayı ve semboller içeren güçlü şifreler seçilmeli.
- Hesapların korunması adına Çoklu Doğrulama Metotlarının kullanılarak, özellikle mail, sosyal medya ve finansal hesapları güvenli kullanılmalı.
- Kullanılan her türlü uygulama güncel tutularak, en son güvenlik önlemlerini aldıklarından emin olunmalı (Cybersecurity and Infastructure Security Agency, t.y.)

Yine CISA 2022 yılında Mobil Cihaz Güvenlik ve Gizliliğinin korunması amacıyla yayınladığı belgede, güvenilir kaynaklardan yapılan indirmelere dikkat edilmesini, indirilmiş uygulamanın hangi izinlere sahip olduğundan emin olunmasını, ihtiyacı olmayan uygulamaların konum bilgisine erişmemesini, yazılımların güncel olmasını, ihtiyaç

bulunmayan uygulamaların silinmesini, uygulamalar ile sosyal ağların entegrasyonunda dikkatli olunmasını, çalınabilecek fiziksel cihazlarda mutlaka güçlü şifre ile birlikte çoklu doğrulama veya biyometrik doğrulama metotlarının kullanılmasını tavsiye etmektedir. Bu tavsiyeler, son kullanıcının mobil iletişimi kullanırken riskleri en aza indirgemesine yöneliktir (Cybersecurity and Infastructure Security Agency, t.y.).

4.1.5. Internet Güvenliği Merkezi

Internet Güvenliği Merkezi (Center for Internet Security - CIS), insanların, işletmelerin ve hükümetlerin bağlı olduğu online dünyayı daha güvenli bir yer haline getirmek için kurulmuş kâr amacı gütmeyen bir organizasyondur. IT ve veri sistemlerinin güvenliği sağlamak amacıyla "CIS Controls" ve "CIS Benchmarks" isimli standartları oluşturmuş ve düzenli olarak geliştirmektedir. Belirli periyotlarla raporlar yayınlamasının yanında güncel siber tehditlere karşı araştırmalara ve tavsiyelere de yer vermektedir. Dünyanın dört bir yanından iletişim teknolojileri uzmanları ile çalışan bu organizasyon, küresel bir topluluğa liderlik yapmakta ve ortaya çıkan tehditlere karşı proaktif olarak koruma sağlanması amacını gütmektedir (The Center for Internet Security, t.y.).

CIS Kritik Güvenlik Kontrolleri (CIS Kontrolleri), siber güvenlik duruşunu güçlendirmek için kullanabilecek, belirli, öncelikli ve basitleştirilmiş bir dizi en iyi uygulamadır. Bugün, dünyanın dört bir yanındaki binlerce siber güvenlik uzmanı, CIS Kontrollerini kullanmakta ve/veya topluluk mutabakat süreci aracılığıyla geliştirilmesine katkıda bulunmaktadır (CIS Security, t.y.).

CIS Kriterleri, 25'ten fazla satıcı ürün ailesi için belirleyici yapılandırma önerileridir. Bunlar, küresel çapta siber güvenlik uzmanlarının uzlaşmaya dayalı çabalarını temsil eder ve sistemleri tehditlere karşı daha güvenli bir şekilde korumaya yardımcı olur (CIS Security, t.y.).

4.1.6. Bilgi Komiserliği Ofisi

Information Commissioner's Office (ICO), İngiltere'de faaliyet gösteren ve veri koruma, bilgi özgürlüğü ve kamu bilgi hakkı gibi konularda düzenleyici bir rol üstlenen bağımsız bir kuruluştur. ICO, Avrupa Birliği Genel Veri Koruma Yönetmeliği (GDPR) kapsamında veri koruma ve gizlilik konularında standartları belirler ve bu standartların uyumunu denetler. Ayrıca, bilgi özgürlüğü kanunlarına uyum konusunda rehberlik sağlar ve

kamuoyunu bilgilendirir. Genel Veri Koruma Regülasyonu (General Data Protection Regulation-GDPR), Avrupa Birliğinin vatandaşlarını korumak amacıyla 2016 yılında başlattığı bir hukuki düzenlemedir (Information Commissioner's Office, 2020).

Özellikle son kullanıcı verilerinin korunması için bu verilerin kişiden izinsiz kullanılamayacağını, sahibi tarafından kolayca erişilebilir olmasını, bahsi geçen kişi istediğinde değiştirilebilmesini, takma isimler vererek gerçek kişinin korunmasını, başka kişilerden siber olarak korunmasını aksi takdirde cezai sonuçların doğacağını ve sadece belirli güvenilirlikte olan üçüncü partilerce işlenebilmesini hukuki olarak bağlayıcı hale getirir. İstisnai durumları ise ulusal güvenlik meseleleri ve suç oluşturabilecek kapsamlarda incelenebilmesidir. Bu yapısı itibari ile dünyadaki en sert güvenlik ve gizlilik kanunu olduğunu iddia etmektedir (General Data Protection Regulation, t.y.).

Regülasyon kapsamında, kişisel verileri tutmak isteyen kurum veya organizasyonlar, şu yedi şartı kabul etmek zorundadırlar:

- Hukuka uygunluk, adillik ve şeffaflık — Veri işleme, veri sahibine karşı hukuka uygun, adil ve şeffaf olunmalıdır.
- Amaç sınırlaması — Verileri, topladığınızda veri sahibine açıkça belirtilen meşru amaçlar için işlenmelidir.
- Veri minimizasyonu — Belirtilen amaçlar için kesinlikle gerekli olan veriler toplanmalı ve işlenmelidir.
- Doğruluk — Kişisel veriler doğru ve güncel tutulmalıdır.
- Depolama sınırlaması — Kişisel olarak tanımlanabilir veriler, belirtilen amaç için gerekli olduğu sürece saklanmalıdır.
- Bütünlük ve gizlilik — Veri İşleme; uygun güvenlik, bütünlük ve gizliliği sağlayacak şekilde yapılmalıdır (örneğin, şifreleme kullanarak).
- Hesap verebilirlik — Veri sorumlusu, GDPR ile uyumluluğu tüm bu ilkelerle gösterebilmekle sorumludur (General Data Protection Regulation, t.y.).

4.1.7. Avrupa Telekomünikasyon Standartları Enstitüsü

Avrupa Telekomünikasyon Standartları Enstitüsü (European Telecommunications Standards Institute-ETSI), telekomünikasyon, yayıncılık ve diğer elektronik iletişim ağları ve hizmetleri ile ilgilenen tanınmış bölgesel standartlar belirleyen uluslararası bir organizasyondur. 1988 yılında Avrupa Posta ve Telekomünikasyon İdareleri Konferansı (European Conference of Postal and Telecommunications Administrations-CEPT)

tarafından Avrupa Komisyonu'nun önerilerine yanıt olarak kurulmuştur.

Mobil siber güvenlik alanında; ETSI TS 102 165, ETSI TR 103 305 ve ETSI TS 133 501 standartları başta olmak üzere çalışmaları, çalışma grupları ile standartlar oluşturma, geliştirme ve güncelleme misyonu bulunmaktadır. ETSI TS 102 165 Standartı, Mobil ağların ve diğer bilgi sistemlerinin güvenliğini sağlamak için en iyi uygulamaları tanımlamaktadır. Ağ güvenliğinin sağlanması, verilerin bütünlüğü ve gizliliği için kritiktir (European Telecommunications Standards Institute, 2017, s. 16-18).

ETSI TR 103 305 Standartı, Bilgi ve İletişim teknolojisi ürünleri, hizmetleri ve sistemleri için siber güvenlik standartlarını ve en iyi uygulamaları içermektedir. Mobil cihazlar ve hizmetler için güvenlik risklerini ve çözümlerini ele almaktadır (European Telecommunications Standards Institute, 2018, s. 17-19).

ETSI TS 133 501 Standartı, 5G sistemlerinin güvenlik gereksinimleri ve mimarisi hakkında detaylı bilgi sağlamaktadır. Güvenlik mimarisi, kullanıcı ve ağ arasındaki güvenli iletişimi sağlamak için gerekli prosedür ve protokolleri içermektedir (European Telecommunications Standards Institute, 2020, s. 23-25).

4.1.8. NSS Labs

NSS Labs, siber güvenlik ürünlerinin bağımsız testleri ve analizleri konusunda dünya çapında tanınmış bir araştırma ve danışmanlık şirketidir. Şirket, siber güvenlik teknolojilerinin etkinliğini, performansını ve toplam sahip olma maliyetini değerlendirerek, kuruluşlara bilinçli kararlar vermelerinde yardımcı olmayı amaçlamaktadır (NSS Labs, t.y.).

NSS Labs, güvenlik ürünlerini gerçek dünyadaki senaryolarda test ederek, ürünlerin etkinliği hakkında objektif ve tarafsız raporlar sunar. Bu raporlar, kuruluşların güvenlik ürünlerini seçerken güvenilir verilere dayalı kararlar almalarını sağlar. Şirket, çeşitli güvenlik ürünlerini karşılaştırmalı olarak değerlendirir ve bu testler, özellikle ağ güvenliği, uç nokta güvenliği, tehdit istihbaratı ve bulut güvenliği gibi alanlarda yoğunlaşır. NSS Labs, farklı güvenlik ürünlerinin etkinliğini ve maliyet verimliliğini görselleştiren Güvenlik Etkinliği Raporları (Security Value Map) sunar. Bu raporlar, karar vericilere hangi ürünlerin yatırım yapmaya değer olduğunu belirlemelerinde yardımcı olur. Ayrıca, siber güvenlik pazarının dinamiklerini analiz eder ve sektör trendlerini takip eder. Bu analizler, kuruluşların gelecekteki siber güvenlik ihtiyaçlarını öngörmelerine yardımcı olmaktadır (NSS Labs, t.y.).

4.1.9. Gartner

Gartner, bilgi teknolojisi araştırmaları ve danışmanlığı alanında dünya lideri bir şirkettir. Şirket, özellikle büyük ölçekli kuruluşlar ve kamu sektörü için stratejik danışmanlık, araştırma raporları ve analizler sunmaktadır. Düzenli periyotlarla yayınladıkları çeşitli dokümanları, partnerlerinin erişimine açmaktadır.

Gartner'ın en bilinen yayınlarından biri olan Magic Quadrant raporları, belirli bir pazar segmentindeki teknoloji sağlayıcılarını vizyonları ve uygulama yeteneklerine göre dört kategoriye ayırır: Liderler, Meydan Okuyanlar, Vizyonerler ve Niş Oyuncular. Bu raporlar, kuruluşların teknoloji sağlayıcılarını ve çözümlerini değerlendirmelerinde önemli bir rehberdir (Gartner, t.y.).

Hype Cycle raporları, yeni ve gelişmekte olan teknolojilerin olgunluk seviyelerini ve benimseme eğilimlerini gösterir. Hype Cycle, teknolojilerin başlangıçtan olgunluğa kadar olan yolculuğunu beş aşamada sınıflandırır ve kuruluşların bu teknolojilere ne zaman yatırım yapmaları gerektiğine dair öngörüler sunar (Gartner, t.y.).

Gartner, bilgi teknolojisi pazarındaki trendleri ve değişimleri analiz ederek pazar tahminleri ve analizleri sunar. Bu analizler, kuruluşların stratejik planlarını şekillendirmelerine yardımcı olur ve gelecekteki yatırımlar için yol haritası sunar (Gartner, t.y.)

Ayrıca, Gartner, kuruluşlara IT stratejileri, dijital dönüşüm, siber güvenlik ve diğer kritik alanlarda stratejik danışmanlık hizmetleri sunar. Bu hizmetler, kuruluşların teknoloji yatırımlarını optimize etmelerini ve iş hedeflerine ulaşmalarını sağlar (Gartner, t.y.).

4.1.10. Elektrik ve Elektronik Mühendisleri Enstitüsü

Elektrik ve Elektronik Mühendisleri Enstitüsü(IEEE-Institute of Electrical and Electronics Engineers), dünya genelinde elektrik, elektronik, bilgisayar bilimleri ve ilgili mühendislik disiplinlerinde standartlar geliştiren ve teknik yenilikleri teşvik eden profesyonel bir organizasyondur. 1963 yılında AIEE (American Institute of Electrical Engineers) ve IRE (Institute of Radio Engineers) birleşmesiyle kurulmuştur. IEEE, teknik standartların yanı sıra bilimsel dergiler, konferanslar, teknik kitaplar ve eğitim programları gibi geniş bir yelpazede hizmetler sunmaktadır (IEEE, t.y.).

IEEE 802.11, IEEE tarafından geliştirilmiş bir dizi kablosuz ağ protokolü standardıdır. Bu standartlar, yerel alan ağları (LAN) için kablosuz bağlantı sağlamak

amacıyla kullanılmaktadır. "Wi-Fi" olarak bilinen teknoloji, IEEE 802.11 standartlarının çeşitli versiyonlarına dayanmaktadır. IEEE 802.11 standartları genellikle 2.4 GHz ve 5 GHz frekans bantlarında çalışır, daha yeni sürümler ise 6 GHz bandını da desteklemektedir. Standartların her yeni sürümü, önceki sürümlere kıyasla daha yüksek veri hızları ve daha iyi performans sunar. Örneğin, 802.11b maksimum 11 Mbps hız sağlarken, 802.11ac ve 802.11ax (Wi-Fi 6) Gbps seviyesinde hızlar sunabilir. Bu standartlar, WEP, WPA, WPA2 ve WPA3 gibi çeşitli güvenlik protokollerini destekler. Ayrıca, yeni standartlar genellikle önceki sürümlerle geriye dönük uyumluluk sağlar (IEEE, 2018, s. 1-4).

4.2. Teknolojik Çözümler

Mobil iletişim teknolojilerindeki hızlı ilerlemeler, dünya genelinde milyarlarca insanın günlük yaşamını köklü bir şekilde dönüştürmüştür. Akıllı telefonlar, tabletler ve giyilebilir cihazlar gibi mobil cihazlar, kişisel ve profesyonel yaşamlarımızın ayrılmaz bir parçası haline gelmiştir. Bu cihazlar, sosyal medya etkileşimlerinden bankacılık işlemlerine, sağlık hizmetlerinden uzaktan eğitime kadar geniş bir yelpazede hizmet sunarak, bireylerin ve işletmelerin verimliliğini artırmıştır. Ancak, bu yaygın kullanım ve bağlılık, siber güvenlik tehditlerini ve saldırılarını da beraberinde getirmiştir. Mobil iletişim dünyasında siber güvenlik, kullanıcıların ve ağların korunması açısından kritik bir öneme sahiptir. Siber saldırganlar, kişisel verilerden finansal bilgilere, kurumsal sırlar ve devlet sırlarına kadar geniş bir bilgi yelpazesine erişim sağlamak amacıyla çeşitli yöntemler kullanmaktadır. Bu tehditler, kötü amaçlı yazılımlar, kimlik avı saldırıları, ağ saldırıları ve cihaz güvenlik açıkları gibi birçok farklı biçimde ortaya çıkmaktadır. Mobil cihazların çeşitliliği ve mobil ağların karmaşıklığı, bu tehditlerle başa çıkmayı daha da zorlaştırmaktadır (Pierer, 2016, s. 29-30).

Bu tez, mobil iletişim dünyasında karşılaşılan siber güvenlik tehditlerini ve saldırı türlerini kapsamlı bir şekilde incelemeyi amaçlamaktadır. Aynı zamanda, bu tehditlerle etkili bir şekilde mücadele etmek için kullanılan yöntemler ve stratejiler üzerinde durulacaktır. Özellikle, mobil cihaz güvenliği, ağ güvenliği, veri şifreleme teknikleri ve kullanıcı farkındalığının artırılması gibi konular ele alınacaktır. Bu çalışma, mobil iletişim dünyasında güvenliği artırmak için yenilikçi ve uygulanabilir çözümler sunmayı hedeflemektedir.

Sonuç olarak, mobil iletişim dünyasında siber güvenlik tehditleri ve saldırılarıyla mücadele etmek, sürekli gelişen teknolojik ortamda büyük bir önem taşımaktadır. Bu tez, mobil güvenliğin sağlanması konusunda akademik ve pratik bir perspektif sunarak, hem

araştırmacılara hem de uygulayıcılara değerli bilgiler sağlayacaktır. Mobil cihazların ve ağların güvenliğinin sağlanması, sadece bireylerin değil, aynı zamanda toplumsal ve ekonomik sistemlerin de korunması anlamına gelmektedir. Bu bağlamda, siber güvenlik tehditlerine karşı proaktif ve çok yönlü yaklaşımlar geliştirmek, sürdürülebilir ve güvenli bir dijital geleceğin temel taşı olacaktır.

Mobil İletişimde siber tehditler, gün geçtikçe artmakta ve şekil değiştirmektedir. Buna binaen savunma mekanizmaları da benzer hızda değişim ve dönüşüm geçirmektedir. Bu bölümde, savunma prensiplerinin iki farklı yönü olan, geleneksel savunma prensipleri ve yenilikçi savunma prensipleri incelenecektir.

4.2.1. Geleneksel Savunma Yöntemleri

Mobil cihazların kullanımının artmasıyla birlikte, siber güvenlik tehditleri de çeşitlenmekte ve bu cihazları koruma gereksinimi daha da önem kazanmaktadır. Mobil siber güvenlikte kullanılan geleneksel savunma prensipleri ve teknolojiler, çeşitli saldırı türlerine karşı etkili koruma sağlamayı amaçlar. Bunlar iletişim teknolojilerinin gelişimi ile standartlaştırılmış, fiziksel cihazlar veya sanal sunucular yardımı ile kullanılabilen teknolojilerdir (Khan, Abbas, & Al-Muhtadi, 2015, s. 1).

4.2.1.1. Güvenlik Duvarları

Güvenlik duvarları(Firewall), her iki yönde giden trafiğin geçmesi gereken bir bariyer oluşturur. Güvenlik duvarı güvenlik politikası, her yönde hangi trafiğin geçmesine izin verildiğini belirler. Güvenlik duvarları, IP paketleri düzeyinde filtre olarak çalışacak şekilde tasarlanabilir veya daha yüksek protokol katmanlarında çalışabilir (Cisco Network, t.y.).

Merkezi bir veri işleme sisteminde, merkezi bir ana bilgisayar doğrudan bağlı terminalleri destekler. Yerel alan ağları (Local Area Network-LAN'lar), PC'leri ve terminalleri birbirine ve ana bilgisayara bağlar. Yerleşke ağları, PC'leri, sunucuları ve muhtemelen bir veya iki ana bilgisayarı birbirine bağlayan birden fazla LAN'dan oluşur. Kurumsal geniş alan ağları, özel bir geniş alan ağı (Wide Area Network-WAN) ile birbirine bağlanan coğrafi olarak dağılmış birden fazla yerleşke ağını kapsar. İnternet bağlantısı, bu yerleşke ağlarının internete bağlanmasını sağlar ve ayrıca özel bir WAN ile de bağlantılı olabilirler. Güvenlik duvarları, ağ güvenliğini yönetmek için çeşitli kontrol işlevleri sağlar.

Hizmet Kontrolü, giden veya gelen internet hizmetlerinin hangi türlerinin erişilebileceğini belirler. Güvenlik duvarları, IP adresi, protokol veya port numarasına göre trafiği filtreleyebilir. Hizmet isteklerini alıp yorumlayan proxy (vekil) yazılımı sağlayabilir yada Web ve posta hizmetleri gibi sunucu yazılımını barındırabilir.

Yön Kontrolü, belirli hizmet isteklerinin hangi yönde başlatılabileceğini ve güvenlik duvarından geçmesine izin verilip verilmeyeceğini belirler.

Kullanıcı Kontrolü, hangi kullanıcının hizmete erişmeye çalıştığına göre hizmetlere erişimi kontrol eder. Bu özellik tipik olarak güvenlik duvarı çevresi içindeki kullanıcılar (yerel kullanıcılar) için uygulanır, ancak dış kullanıcılardan gelen trafiğe de uygulanabilir ve bu durum, Ipsec (tünelleme) gibi güvenli kimlik doğrulama teknolojisi gerektirir.

Davranış Kontrolü, belirli hizmetlerin nasıl kullanıldığını kontrol eder. Örneğin, güvenlik duvarı spam e-postaları filtreleyebilir veya dış erişimi yalnızca yerel bir web sunucusundaki bilginin bir kısmına izin verebilir (Stallings, 2011, s. 375-377).

Güvenlik Duvarlarının en önemli özelliği, negatif erişim mantığı ile çalışmalarıdır. Yukarıdan aşağıya kural işletme şeklinde çalışırlar ve standart olarak sıfır erişim metodu kullanarak her trafiği engellerler. İhtiyaca binaen erişim izni verilmesi ve düzenli aralıklarla kontrol-konfigüre-update edilmeleri gerekmektedir (Linear Stack, 2023).

4.2.1.2. Mobil Cihaz Yönetimi

Mobil Cihaz Yönetimi (Mobile Device Management-MDM) bir işletmenin mobil cihazlarını merkezi bir noktadan yönetmesini sağlayan bir sistemdir. MDM yazılımları, cihazların güvenlik politikalarına uyumunu sağlar, uygulama yönetimini gerçekleştirir ve cihaz verilerini korur. MDM çözümleri, cihaz kaybolduğunda veya çalındığında uzaktan kilitleme ve veri silme gibi özelliklerle kurumsal bilgilerin güvenliğini sağlar (Hulme, 2012).

BYOD kavramınının yaygınlaşması akabinde, kişisel cihaz güvenliğinin sağlanması için elzem bir teknoloji olarak hergün geliştirilmektedir. Farklı akıllı cihazları, markalarını, işletim sistemlerini ve veri saklama yöntemlerini desteklemektedir.

MDM teknolojisi altında, cihazlar ve ağ arasındaki bağlantı protokolleri, cihazın donanım ve yazılım altyapıları, dosyalama teknikleri, marka-model bilgileri, dolaşım detayları, sertifikaları, şifreleme metodları, antivirüsleri, kişisel verileri gibi birçok bilgi kullanılır ve en iyi çözüme ulaşılmaya çalışılır. Bazı durumlarda, gereksinimlerin tanımlanmasının ardından, organizasyonlar belirli uygulamaların kullanımını yasaklamaya karar verirler. Diğer yandan, kullanımı zorunlu kılmak için uygulamanın kaldırılmasını da

engelleyebilirler. Mobil işletim sistemine bağlı olarak, kullanıcı uygulamayı yükleyebilir veya kaldırabilir. (Pierer, 2016, s. 43).

Sertifikaların korunması, güvenli bir bağlantı kurmak için kullanılır. Bu sertifikalar, kullanıcıları veya web sunucusu gibi diğer cihazları tanımlamak için kullanılabilir. Sertifikaların dağıtımı, kullanıcıya gereken ayrıcalıkları sağlar (örneğin, veri değişimi veya uygulama kullanımı).

Mobil cihaz şifreleme, verileri, klasörleri, e-postaları ve işletim sistemini yetkisiz erişimlere karşı koruyan bir güvenlik özelliğidir. Mobil cihaz şifrelendiğinde, herhangi bir bilgiye erişim mümkün değildir. Özellikle sağlık sektöründe, hassas verilerin varlığı nedeniyle cihaz şifreleme oldukça önemlidir.

Anti-virüs desteği, IT tüketiminin artması ve ikinci nesil kurumsal mobilite ile her ortamda göz önünde bulundurulmalıdır. Kötü amaçlı yazılımlar, casus yazılımlar veya Truva atları mobil işletim sistemleri pazarına girmiştir ve büyük hasara neden olma potansiyeline sahiptir. Bu nedenle, mobil cihazlarda anti-virüs uygulamaları değerlendirilip tanıtılmalıdır.

Cihazın tehlikeye atılmasının tespiti (root/jailbreak), bazı ileri düzey kullanıcıların mobil cihazlarını tehlikeye atmaya çalıştığını ifade eder. Bu, işletim sistemi hakkında daha fazla bilgi ve ayrıcalık elde etmek için root yapmaya çalışmaları anlamına gelir. Diğerleri, istedikleri herhangi bir ağ sağlayıcısını kullanabilmek için cihazlarını jailbreak yapmaya çalışır. Bu tür tehditler gözlemlenmeli ve uygun önlemler alınmalıdır (örneğin, veri silme veya cihaz sıfırlama).

Mobil cihaz eylemleri, mobil cihaz yönetim ürünlerinin, güvenlik ile ilgili olarak büyük miktarda ayarı yasaklamasını veya izin vermesini zorunlu kılar. Organizasyonlar, kamera, mobil hotspotlar, Bluetooth, kablosuz bağlantılar veya konteyner zorunluluğu gibi kullanım için politikalar ve önlemler tanımlamalıdır. Veri kaybı önleme, maddi zararlara neden olabileceği gibi rakipler karşısında rekabet avantajları da sağlayabilir. Bu nedenle, veri kaybı önleme, dünya çapındaki çoğu organizasyon için çok önemlidir. Bu da, organizasyonların, hassas verilerin mobil cihazda şifrelenmemiş olarak saklanmasını önlemek için konteyner uygulamaların kullanımını zorunlu kılmasının bir nedenidir. Teknik mühendisler, mobil cihaz yönetim sistemi tarafından tespit edilen bir veri kaybı durumunda mobil cihazları uzaktan silebilirler (Pierer, 2016, s. 49-54).

Mobil VPN, mobil cihazların yerel bilgi teknolojisi altyapısına bağlanmasına olanak tanır. Bir mobil sanal özel ağ ile, mobil cihazlar organizasyonla doğrudan bilgi alışverişi yapabilir, veri toplayabilir ve sürdürebilir. Organizasyon altyapısına bağlantılar gerekli olduğunda, mobil cihaza bir VPN profili kurulmalıdır.

Tek oturum açma (SSO) desteği, mobil kullanıcının birçok uygulamaya tek bir kimlik bilgisi ile yetkilendirilmesini sağlar. Özellikle, organizasyondaki iş süreçlerini desteklemek için birçok uygulama kullanıldığında, tek oturum açma, mobil kullanıcıyı yetkilendirmenin uygun bir yoludur.

Mobil cihaz kilidini koruma, uzak yapılandırma veya kontrol devreye girdiğinde cihazı uzaktan kilitlemek veya kilidini açmak çok önemlidir. Teknik mühendislerin, yapılandırma ayarlarını değiştirebilmek için cihazın kilidini açması gerekir. Ayrıca, mobil cihazı kilitlemek, hemen bir şifre/parola politikası uygulamak için faydalı olabilir.

Kişisel Bilgi Yönetimi, her mobil kullanıcının temel bir parçasıdır. Müşterilerin iletişim bilgilerini saklamak, takvim ve randevuları yönetmek veya e-postaları kontrol etmek, her çalışanın iş görevlerini yerine getirmesini sağlayan kişisel bilgilerdir.

Veri Senkronizasyonu, yukarıda belirtilen veri yönetimi özelliği gibi otomatik veri senkronizasyonu çok önemlidir. İç ve dış paydaşlarla kârlı etkileşimler sağlamak için esnek iş akışlarını desteklemek, günümüzde her organizasyon için kritik öneme sahiptir.

VPN, çoğu organizasyonun mobil kullanıcılarına ve onların mobil cihazlarına iç bilgi teknolojisi yapılarına erişim hakkı tanır. VPN ile, mobil uygulamaların sanal özel ağ üzerinden iyi tanımlanmış iç kaynaklara erişimini sağlamak mümkündür. Her uygulama, iç altyapıya bağlanır ve verileri şifreli bir tünel üzerinden alıp gönderir (Pierer, 2016, s. 48).

GPS lokalizasyonu, mobil cihazları bulmak için yaygın olarak kullanılan bir işlevdir. Çalınan veya kaybolan mobil cihazları bulmak için sıklıkla kullanılır. Kullanıcıların veya mobil cihazların kesin olarak konumlandırılmasına olanak tanır ve bu nedenle birçok senaryoda kullanılabilir. Donanım yazılımı bilgisi, genellikle işletim sistemi hakkında bilgi verir. Genellikle işletim sistemi sürüm numarası en önemli olanlardan biridir. Teknik mühendislerin sorunları ve endişeleri analiz etmesine yardımcı olur ve mobil cihazların sorunsuz çalışmasını sağlar. Ayrıca, donanım yazılımı bilgisi, uygulama yönetiminin hangi uygulamaların mobil cihazlarda çalıştırılabileceğini belirlemesi için bir dayanak noktasıdır (Pierer, 2016, s. 49-54).

Mevcut dil, uygulama ve güvenlik yönetimi açısından teknik mühendisler için oldukça önemli olabilir. Çok uluslu şirketlerde dil, farklı güvenlik ve uygulama ayarlarını etkiler. Yüklü yazılım ve uygulamalar hakkında detaylı istatistikler, olası güvenlik risklerini belirlemeye yardımcı olur. Organizasyon, belirlenen güvenlik standartlarını uygulamak istiyorsa, mobil uygulamaları dikkate almalıdır. Mobil uygulama yönetiminde kara/beyaz listeleme uygulamaları, mobil ağları güvence altına almak için atılacak sonraki adımlardır. Hizmet geçmişi, mobil cihazın ve mobil kullanıcının faaliyetlerini gösterir. Hangi

faaliyetlerin ne zaman ve kim tarafından gerçekleştirildiği, bu özelliğin merkezi unsurlarıdır. Hizmet geçmişi kaydı için tipik bir senaryo, mobil cihazın kayıt süreci olabilir. Bu, mobil cihaz yönetim sisteminin mobil cihazı kontrol etmeye başladığı tarihi tanımlar. Mobil işletim sistemi desteği, tipik olarak bir istemci/sunucu mimarisinden oluşur. Mobil istemci, mobil cihazlara yüklenir ve sunucu ile iletişim kurarak ilgili verileri paylaşır. Bu, mobil cihaz yönetimi için desteklenen işletim sistemlerini belirtir. IMEI durumu, uluslararası mobil ekipman kimliği, her cihaz için benzersiz olan bir seri numarasıdır. Kullanıcıyla ilişkilendirilir ve hangi cihazın hangi kullanıcı tarafından kullanıldığını belirlemeye yardımcı olur. Dolaşım durumu, teknik mühendisin hangi mobil ağın şu anda kullanıldığını belirlemesine yardımcı olur. Dolaşım, kullanıcıya hangi mobil ağda olursa olsun telefon görüşmeleri yapma veya mobil veri iletimi kullanma olanağı sağlar. Dolaşım maliyetlerini izlemek ve düzenlemek için mobil cihaz yönetim yazılımı satıcıları, dolaşım durumunu kontrol etmek için kontrol mekanizmaları kurar. Pil durumu, her mobil cihaz için pil tüketimi veya şarj seviyesi hakkında bilgi sağlar. Pilin hasar görüp görmediğini belirtmeye yardımcı olur. Bu nedenle, envanter yönetimi için sıkça kullanılır (Pierer, 2016, s. 49-54).

4.2.1.3. Veri Kaybı Önleme

Veri Kaybı Önleme (Data Loss Protection-DLP), hassas bilgilerin yetkisiz kişilere sızmasını önleyen teknolojilerdir. Mobil cihazlarda DLP kullanımı, verilerin nasıl depolandığını, işlendiğini ve iletildiğini denetleyerek veri sızıntılarını engeller. DLP çözümleri, veri sınıflandırma, şifreleme ve kullanıcı aktivitelerinin izlenmesi gibi yöntemlerle kurumsal bilgilerin güvenliğini artırır (Gartner, t.y.).

DLP teknolojileri temelde dört basamakta özetlenir; discover, monitor, protect ve manage.

Discover, verinin kritiklik seviyesini, kaybı üzerine yaşanacak maliyetleri, verilere yönebilecek tehditlerin boyutunu ve içeriğini tespit etme adımıdır. Monitor, ağda bulunan kişi ve cihazları, erişebildikleri verileri, kullanılan uygulamaların yetkilerini ve verilerde yaptıkları değişiklikleri sürekli olarak izleyip kayıt altına almayı ifade eder. Protect, kritik verilerin sadece ilgililerce erişilebilir ve değiştirilebilir olmasını, kötü amaçlı yazılımlara karşı metodların kullanılmasını, erişim izinlerinin düzenli kontrolünü, veri şifreleme tekniklerinin etkili konfigürasyonunu ve yedekleme yapılmasını öngörür. Manage, veri kayıp veya manipülasyonlarının hukuki ve kişisel sonuçlarını incelemeyi, ileride meydana gelebilecek olaylara karşı müdahale yöntemlerini ve elbette ilk üç adımın gerektiğinde

iyileştirilmesini önerir (Cole, 2016, s. 172-183).

4.2.1.4. Uç Nokta Tespit ve Yanıt / Genişletilmiş Tespit ve Yanıt

Genişletilmiş Tespit ve Yanıt (Extended Detection and Response-XDR), çeşitli güvenlik ürünlerinden gelen verileri entegre ederek daha kapsamlı bir tehdit tespiti ve müdahale sağlar. Mobil cihazlar, ağlar, sunucular ve uç noktalar gibi farklı kaynaklardan gelen veriler XDR platformunda birleştirilir ve analiz edilir. Bu sayede, gelişmiş tehditlere karşı daha hızlı ve etkili bir yanıt mekanizması oluşturulur (Trend Micro, t.y.).

Uç Nokta Tespit ve Yanıt(Endpoint Detection and Response-EDR), masaüstü bilgisayarlar, dizüstü bilgisayarlar, sunucular ve mobil cihazlar gibi uç noktalarda güvenlik olaylarını tespit etmeyi ve incelemeyi amaçlayan bir siber güvenlik yöntemidir. EDR çözümleri, uç nokta verilerini, ağ trafiğini ve kullanıcı davranışlarını toplayıp analiz ederek, güvenlik ihlallerine işaret edebilecek anormal etkinlikleri belirler. EDR çözümleri, gerçek zamanlı tehdit istihbaratı, otomatik olay müdahalesi ve adli soruşturma yetenekleri sunacak şekilde tasarlanmıştır. EDR araçları, güvenlik ekiplerinin gelişmiş tehditleri hızla ve etkili bir şekilde tespit etmelerini ve yanıt vermelerini sağlayarak, veri ihlalleri ve diğer siber güvenlik olayları riskini minimize eder (Hoş, 2024).

Organizasyonlardaki uç nokta sayısı giderek artmakta ve artık sadece geleneksel son kullanıcı bilgisayar cihazları ile sınırlı değil. Uzaktan çalışmanın artması, tüm ortam boyunca çeşitli uç noktaları ve uç nokta-ara bağlantıları güvence altına almayı ve izlemeyi daha da gerekli hale getirmiştir. Uç noktalar, siber saldırılar için ana giriş noktası olmaya devam ettiğinden, uç nokta güvenliği stratejileri işletmeler için kritik bir ihtiyaç haline gelmiştir. Sadece antivirüs yazılımı, sofistike siber tehditlere karşı koruma sağlamak için yeterli olmamaktadır.

Uç Nokta Algılama ve Yanıt (EDR), uç nokta güvenliğine odaklanır ve masaüstü bilgisayarlar, dizüstü bilgisayarlar ve mobil cihazlar gibi uç noktalar üzerinde görünürlük ve kontrol sağlar. EDR çözümleri, güvenlik olaylarını tespit etmek ve yanıtlamak için uç nokta etkinliklerini ve davranışlarını izler. Her uç nokta hakkında işlem etkinliği, dosya değişiklikleri, ağ bağlantıları ve sistem olayları gibi ayrıntılı bilgi sağlar; bu da güvenlik ekiplerinin tehditleri hızla tanımlayıp yanıt vermesini sağlar. Öte yandan, genişletilmiş algılama ve yanıt (XDR), daha geniş bir kurumsal yaklaşım benimser ve güvenlik ekiplerine organizasyonun güvenlik duruşunu bütünsel bir şekilde görme imkânı tanır, böylece hızlı ve bilinçli tespit ve yanıt kararları verebilirler. XDR, yerel olarak EDR, ağ güvenliği, bulut

güvenliği ve e-posta güvenliği gibi birden fazla güvenlik ürününden veri entegre eder, böylece organizasyon genelinde güvenlik tehditlerini birleştirilmiş bir bakış açısıyla sunar. Genellikle bu çeşitli güvenlik çözümleri, bir XDR sağlayıcısı tarafından birleşik bir şekilde sunulur, ancak XDR, ortaklıklar veya önceden yapılandırılmış sorunsuz entegrasyonlar aracılığıyla üçüncü taraf teknolojilerini destekleyebilir. XDR çözümleri, tehditleri tanımlamak ve önceliklendirmek için gelişmiş analizler ve makine öğrenimi algoritmaları kullanır, olay yanıt iş akışlarını otomatikleştirir ve güvenlik operasyonlarını iyileştirmek için uygulanabilir içgörüler sunar. XDR ayrıca sürekli güncellenen tehdit istihbaratını uygulayarak bağlam ekler ve daha iyi tespitleri sağlar (Palo Alto Networks, t.y.).

EDR ve XDR farklarının daha iyi görülebilmesi, daha net anlaşılabilmesi için eldeki veriler Tablo 9'da ifade edilmiştir.

Tablo 9

EDR ve XDR Teknolojilerinin Temel Farkları

Özellik	EDR (Endpoint Detection and Response)	XDR (Extended Detection and Response)
Odak Noktası	Uç noktalar üzerinde yoğunlaşır (masaüstü, dizüstü, mobil cihazlar)	Birden fazla güvenlik kaynağına genişler (ağ, uç nokta, sunucu)
Veri Kaynakları	Genellikle uç noktalarla sınırlıdır	Uç nokta, ağ trafiği, sunucu, güvenlik bilgi ve olay yönetimi (SIEM) sistemleri gibi birden fazla kaynaktan veri toplar
Tehdit İstihbaratı	Odaklı ve spesifik uç nokta tehditlerini ele alır	Geniş kapsamlı tehdit istihbaratı sağlar
Yanıt Yeteneği	Uç nokta düzeyinde olay müdahalesi ve yanıt	Birden fazla güvenlik katmanında olay müdahalesi ve yanıt
Veri Analizi	Uç nokta verileri üzerinde yoğunlaşır	Toplanan verilerden entegre bir şekilde analiz yapar
Adli Tespit ve Soruşturma	Uç nokta bazlı adli analiz yapar	Çeşitli güvenlik verilerini birleştirerek kapsamlı adli analiz sağlar
Kapsam	Uç nokta güvenliği üzerinde odaklanır	Gelişmiş tehditlerin tespiti için çoklu güvenlik önlemlerini kapsar
Entegrasyon	Genellikle uç nokta çözümleriyle sınırlıdır	Geniş bir güvenlik ekosistemine entegre olabilir

4.2.1.6. Saldırı Tespit Sistemi / Saldırı Önleme Sistemi

Saldırı Önleme Sistemi(Intrusion Prevention System-IPS), ağ trafiğini gerçek zamanlı olarak izleyen ve potansiyel tehditleri tespit eden bir güvenlik sistemi olarak işlev görür. Tespit edilen tehditlere anında müdahale ederek, güvenlik ihlallerinin gerçekleşmesini önlemeye çalışır. IPS, saldırıları engellemek için çeşitli yöntemler kullanır. Trafikteki anormal davranışları ve güvenlik açıklarını izleyerek potansiyel saldırıları önceden algılar (Fortinet, t.y.).

Saldırı Tespit Sistemi(Intrusion Detection System-IDS), ağ trafiğini izleyerek ve analiz ederek şüpheli faaliyetleri tespit eder, ancak tespit edilen olaylara müdahale etmez. IDS, güvenlik ihlalleri hakkında uyarılar sağlar ve genellikle güvenlik ekiplerinin olaylara tepki vermesini bekler. Ağ trafiği ve etkinliklerini izleyerek anormal veya zararlı aktiviteleri tanımlar. Tespit edilen tehditlere dair raporlar ve uyarılar sunar, böylece güvenlik uzmanları olaylara müdahale edebilir (Turknet, t.y.).

IPS ve IDS'ler veritabanındaki tehdit tanımlarıyla karşılaştırarak bilinen kötü amaçlı yazılımları ve saldırıları tespit ederler. İmza veritabanlarını, kural temelli politikaları, anomali tespiti yöntemlerini kullanırlar (Cisco, 2020).

IPS ve IDS tarasındaki farkların ve işlevlerin daha iyi anlaşılabilmesi için veriler Tablo 10'da ifade edilmiştir.

Tablo 10

IPS ve IDS Sistemleri Arasındaki Farklar

Özellik	Intrusion Prevention System (IPS)	Intrusion Detection System (IDS)
Müdahale Yöntemi	Saldırıları proaktif olarak engeller.	Sadece saldırıları algılar, müdahale etmez.
Amaç	Güvenlik ihlallerini önlemek ve aktif olarak müdahale etmek.	Güvenlik ihlallerini tespit etmek ve raporlama sağlamak.
Operasyonel Yaklaşım	Aktif, tehditleri durdurma ve önleme odaklı.	Reaktif, tehdit tespiti ve olay bildirme odaklı.
Kullanıcı Eylemleri	Otomatik olarak tehditleri önler ve durdurur.	Tehditler tespit edildikten sonra kullanıcı müdahalesine ihtiyaç duyar.
Yaygın Kullanım Alanı	Ağ güvenliği, veri güvenliği, saldırı engelleme.	Ağ izleme, güvenlik ihlallerinin tespiti ve analiz.
Yanıt Süreçleri	Olayları otomatik olarak önler ve durdurur.	Güvenlik ekibine olaylar hakkında bilgi verir.
Geriye Dönük Analiz	Genellikle veri kaydetmez, anlık olaylara odaklanır.	Olay kayıtları tutar, analiz için kullanılabilir.
Entegrasyon	Genellikle güvenlik duvarları ve ağ sistemleriyle entegre çalışır.	Güvenlik sistemleri ile entegre çalışır, daha geniş veri analizi sağlar.

4.2.1.7. Güvenlik Bilgi ve Olay Yönetimi

Güvenlik profesyonelleri ve analistleri, Güvenlik Bilgi ve Olay Yönetimi (Security Information and Event Management-SIEM) sistemini kullanarak güvenlik ihlallerini izler, tanımlar, kaydeder ve bazen bunlara yanıt verir. Bu güvenlik olaylarından bazıları açıktır, örneğin kasıtlı ve zararlı hizmet engelleme saldırıları ve virüs salgınları. SIEM sistemi, daha gizli güvenlik olaylarını da tespit edebilir. Birçok olay, o kadar ince olabilir veya saniyede binlerce olay tarafından o kadar gizlenmiş olabilir ki, güçlü ve hassas ayarlanmış bir SIEM sistemi yardımı olmadan tamamen fark edilmeden geçerler. Bu daha gizli güvenlik olaylarına, politika ihlalleri, yetkisiz erişim girişimleri ve IT ortamınıza metodik ve gizlice girmeye çalışan yüksek becerilere sahip ve odaklanmış saldırganların faaliyetleri dahildir (Miller, Harris, Harper, VanDyke, & Blask, 2011, s. 25).

SIEM sistemleri değişken becerilere sahip olabilir, ancak genellikle üç temel işlev sunarlar. İlk olarak, büyük miktarda veriyi tek bir noktada toplayarak ve düzenleyerek, tehdit, saldırı veya ihlal belirtilerini inceleme imkanı tanırlar. Bu sistemler, olası tehditlerin hızlı bir şekilde algılanabilmesi için veriler arasında ilişkiler kurarak olayları bağlamsal

olarak düzenler. Ayrıca, bir kurumun ağındaki güvenlik olaylarını sürekli izleyerek, olaylarla ilgili tüm etkinlikler için uyarılar ve denetim seçenekleri sunar. SIEM sistemleri, aynı zamanda şüpheli kullanıcı etkinliklerini algılamak, kullanıcı davranışlarını izlemek, erişim girişimlerini sınırlamak ve uyumluluk raporları oluşturmak gibi çeşitli alanlarda siber risklerin azaltılmasına yardımcı olur. SIEM kullanmanın avantajları, bir kurumun genel güvenlik duruşunu güçlendirmeye yardımcı olan birçok fayda sunar. Bu avantajlar arasında, olası tehditlerin tek bir merkezden gözlemlenmesi, gerçek zamanlı tehdit tespiti ve yanıt, gelişmiş tehdit analizi, mevzuata uygunluk denetimi ve raporlamaları ile kullanıcıları, uygulamaları ve cihazları izleme konusunda daha fazla şeffaflık bulunur. Bu özellikler, kurumların güvenlik altyapısını güçlendirirken potansiyel tehditlere karşı daha etkili bir koruma sağlayabilmektedir (Microsoft, t.y.).

4.2.1.8. Sanal Özel Ağ

Sanal Özel Ağ (Virtual Private Network-VPN), cihazlar arasında internet üzerinden özel bir ağ bağlantısı oluşturarak, veri şifrelemesi ve IP adresi gizliliği yoluyla güvenli ve anonim bir internet kullanımı sağlar. Bu, özellikle güvensiz halka açık Wi-Fi ağlarında kişisel verilerin korunması açısından önemlidir. VPN kullanmanın başlıca amaçları arasında, kişisel bilgilerin şifrelenerek üçüncü tarafların bu bilgileri kaydedip kötüye kullanmasını önlemek bulunur; bu, halka açık Wi-Fi ortamlarında özellikle kritiktir. VPN'ler ayrıca kimliğinizi gizleyerek, IP adresiniz ve diğer bilgilerinizin korunmasını sağlar, bu da çevrimiçi aktivitelerinizin izlenemez olmasını sağlar. Ayrıca, VPN'ler internet güvenliğinizi artırarak internet trafiğinizi şifreler ve yetkisiz erişim riskini azaltır. VPN hizmetleri, şüpheli aktiviteler algılandığında otomatik olarak etkinleştirilebilen sistemler sunar, bu da veri ihlalleri gibi durumlarda verilerinizin yetkisiz erişimden korunmasını sağlar. VPN teknolojisi, veri paketlerinizi internet üzerinden uzak bir sunucuya yönlendirerek, tünelleme protokolleri ve şifreleme teknikleri aracılığıyla verilerin güvenli bir şekilde iletilmesini sağlar. Bu süreç, verilerinizi şifreler ve IP adresinizi gizler, böylece ağ güvenliğini artırır. VPN kullanmanın avantajları arasında güvenli genel internet erişimi, arama geçmişlerinin gizlenmesi, küresel içeriklere erişim ve çevrimiçi kimliğinizi koruma yer alır, bu da çevrimiçi etkinliklerinizin güvenliğini artırır ve kişisel verileri korur (AWS Amazon, t.y.).

Temelde üç adımdan oluşur: Şifreleme, Kimlik Doğrulama ve Yetkilendirme:

Şifreleme, verilerin yalnızca hedef alıcı tarafından okunabilir bir forma dönüştürülmesi işlemidir. Mesajı okuyabilmek için, veriyi alan kişinin doğru şifre çözme

anahtarına sahip olması gerekmektedir. Geleneksel şifreleme yöntemlerinde, gönderici ve alıcı veriyi şifrelemek ve şifre çözmek için aynı anahtarı kullanır. Buna karşılık, açık anahtarlı şifreleme yönteminde iki anahtar kullanılır. Anahtarlar arasında biri kamu anahtarı olarak bilinir, bu anahtar şifreleme veya şifre çözme işlemleri sırasında herkes tarafından kullanılabilir. Anahtarın adı "kamu anahtarı" olmasına rağmen, bu anahtar bir entitenin (veya kişinin) malıdır. Eğer ikinci bir entite anahtarın sahibiyle iletişim kurmak isterse, bu kamu anahtarını kullanarak iletişim kurar. Kamu anahtarının bir karşılık gelen özel anahtarı vardır. Özel anahtar, adından da anlaşılacağı gibi, verildiği entiteye (veya kişiye) özeldir. Sonuç olarak, açık anahtarlı şifreleme ile herkes anahtarın sahibinin kamu anahtarını kullanarak bir mesajı şifreleyip gönderebilir. Ancak, yalnızca anahtarın sahibi bu mesajı şifre çözmek için gerekli özel anahtara sahiptir. İletişimde, gönderici mesajı şifrelemek için kendi kamu anahtarını kullanır. Alıcı mesajı alır ve özel anahtarı kullanarak şifrelenmiş mesajı çözer (Hiquet, 2003, s. 4-5).

Kimlik doğrulama, verilerin hedef alıcıya teslim edildiğinden emin olma sürecidir. Ayrıca, kimlik doğrulama, alıcıya mesajın bütünlüğü ve kaynağı konusunda güvence verir. En basit haliyle, kimlik doğrulama, belirtilen kaynağa erişim sağlamak için en az bir kullanıcı adı ve şifre gerektirir. Daha karmaşık biçimlerinde, kimlik doğrulama, gizli anahtar şifrelemesine veya açık anahtar şifrelemesine dayalı olabilir (Hiquet, 2003, s. 4-5).

Yetkilendirme, kullanıcının başarıyla tanımlanıp doğrulandıktan sonra bir ağda bulunan kaynaklara erişiminin verilip verilmeyeceğinin belirleme sürecidir (Hiquet, 2003, s. 4-5).

4.2.1.9. Ağ Erişim Kontrolü

Ağ Erişim Kontrolü (Network Access Controller-NAC), yetkisiz kullanıcıların ve cihazların bir kurumsal veya özel ağa erişimini kısıtlayan bir süreçtir. NAC, yalnızca kimlik doğrulaması yapılmış kullanıcıların ve güvenlik politikalarına uygun olan cihazların ağı girişine izin verir. Son kullanıcıların ve cihazların kullanımının artmasıyla, genellikle kendi cihazını getir politikaları (BYOD) ve Nesnelerin İnterneti (IoT) cihazlarının kullanımıyla daha fazla kontrol gereklidir. En büyük BT organizasyonları bile, kullanılan tüm cihazları manuel olarak yapılandıracak kaynaklara sahip değildir. NAC çözümünün otomatik özellikleri, kullanıcıların kimlik doğrulamasını yapma ve cihazların uyumluluğunu belirleme süresini ve buna bağlı maliyetleri azaltmada önemli bir avantaj sağlar. Ayrıca, siber suçlular bu artan cihaz kullanımının farkındadır ve kurumsal ağlardaki her türlü açığı kullanan

sofistike saldırılar düzenlemeye devam ederler. Daha fazla uç nokta, saldırı yüzeyini artırır, bu da saldırganların erişim sağlama fırsatlarını çoğaltır. NAC çözümleri, ağda olağan dışı veya şüpheli herhangi bir etkinliği algılamak ve cihazı ağdan izole etmek gibi hızlı bir şekilde harekete geçmek suretiyle potansiyel saldırının yayılmasını önlemek için yapılandırılabilir. IoT ve BYOD, NAC çözümlerini değiştirmiş olsa da, NAC aynı zamanda kullanıcıların, cihazların ve erişim seviyelerinin sürekli bir envanteri olarak hizmet eder. Daha önce bilinmeyen cihazları keşfetmek için aktif bir keşif aracı olarak hizmet eder ve bu, BT yöneticilerinin güvenlik politikalarını ayarlamalarını gerektirir. Ayrıca, kuruluşlar NAC'nin, ağa erişim sağlamaya çalışan kullanıcıları nasıl kimlik doğrulayacağını seçebilirler. BT yöneticileri, kullanıcı adı ve şifre kombinasyonlarına ek bir güvenlik katmanı sağlayan çok faktörlü kimlik doğrulama (MFA) seçebilirler. Ağ erişiminin kısıtlanması, genellikle siber suçluların hedefi olan ağ içindeki uygulamalar ve verilerin kontrolünü de ifade eder. Ağ kontrollerinin ne kadar güçlü olursa, siber saldırıların ağa sızması o kadar zorlaşır (Fortinet, t.y.).

Geleneksel Savunma Prensipleri genel anlamıyla iletişim teknolojilerinin yoğun kullanımı ve artan ihtiyaçlarına göre gelişmiş, halen gelişmekte olan metotları ifade etmektedir. Bu yaklaşımlar yıllar içerisinde cihazlar haline gelmiş ve ilgili işin konfigürasyonunu sağlayacak donanım-yazılım paketleri halinde birçok uluslararası şirket tarafından pazarlanmaktadır. Gün geçtikçe artan siber güvenlik tehditleri, siber güvenlik şirketlerini ürün yelpazelerini genişletmeye, önceden modüller şeklinde donanımlar üzerinde bulunan ek özellikleri de güçlendirerek yeni donanımlar üretmeye itmektedir. Veri boyutlarının ve internet trafiğinin de artışı bütün modüllerin bir donanım üzerinde sunulmasını imkânsız hale getirmiştir. Bu bölümde bahsedilen geleneksel savunma prensiplerinin her biri için özellikle büyük ölçekli ağ trafiği olan kurumlarda ayrı ayrı donanımlar kullanılması zorunluluktur. Tabi ki teknoloji firmaları tarafından halen birkaç veya onlarca modülü üstünde barındıran cihazlar üretilmektedir. Ancak bu cihazlar genelde küçük ve orta düzeydeki ağ trafiği olan kurum ve kuruluşlara önerilmektedir.

4.2.2. Yenilikçi Savunma Prensipleri

Mobil iletişim teknolojilerinin güvenliği, hem geleneksel hem de yenilikçi savunma prensiplerinin entegrasyonuyla sağlanmalıdır. Firewall, XDR, EDR, DLP ve MDM gibi geleneksel teknolojiler, temel güvenlik önlemlerini oluştururken; Yapay Zeka, Blockchain, İleri Düzey Kimlik Doğrulama, Biyometrik Kimlik Doğrulama ve Davranışsal Analiz gibi

yenilikçi yöntemler, mobil güvenlikte yeni bir dönem başlatmaktadır. Bu kombinasyon, mobil cihazların daha güvenli, daha akıllı ve daha güvenilir hale gelmesini sağlamaktadır.

4.2.2.1. Yapay Zeka ve Davranışsal Analiz

Yapay zeka, mobil cihazlarda anormal davranışları tespit etmek için kullanılabilir. Makine öğrenimi algoritmaları, normal kullanım desenlerini öğrenerek bu desenlerden sapmaları tespit edebilir; örneğin, kullanıcı alışkanlıklarına dayalı olarak anormal veri transferleri veya beklenmedik uygulama davranışları algılanabilir. Davranışsal analizle YZ, kullanıcıların ve uygulamaların davranışlarını sürekli olarak analiz eder, bu analizler kötü niyetli aktiviteleri erkenden tespit etmek için kullanılır. Örneğin, bir uygulamanın normalden fazla kaynak tüketmesi veya beklenmedik izinler talep etmesi durumunda uyarı oluşturabilir (Parisi, 2020, s. 124-125).

Ayrıca, yapay zeka büyük miktarda veriyi işleyerek ve analiz ederek tehdit istihbaratı sağlayabilir; bu veriler zararlı yazılım imzaları, bilinen zafiyetler ve diğer tehdit göstergeleri gibi çeşitli kaynaklardan gelir. YZ, bu bilgileri kullanarak yeni tehditleri proaktif bir şekilde tespit edebilir. Yapay zeka, tehditlere karşı otomatik yanıtlar verebilir; örneğin, bir tehdit tespit edildiğinde, yapay zeka sistemi otomatik olarak cihazı karantinaya alabilir, belirli işlemleri durdurabilir veya kullanıcıyı bilgilendirebilir. Bu tür otomatik yanıtlar, saldırıların hızla etkisiz hale getirilmesini sağlar (CEPS Think Tank Task Force, 2021, s. 19-21).

Derin öğrenme, karmaşık veri setleri üzerinde yüksek doğrulukla analizler yapabilen bir YZ alt dalıdır; mobil cihazlarda derin öğrenme modelleri kullanılarak zararlı yazılımlar tespit edilebilir, uygulama davranışları analiz edilebilir ve güvenlik açıkları belirlenebilir. Ayrıca YZ, farklı güvenlik tekniklerini bir araya getirerek daha etkili savunma stratejileri geliştirebilir; örneğin, anomali tespiti ile davranışsal analiz birleştirerek daha kapsamlı bir güvenlik katmanı oluşturulabilir (Stamp, Visaggio, Mercaldo, & Troia, 2022, s. 6-7).

4.2.2.2. Blockchain

Blockchain, merkezi bir otoriteye ihtiyaç duymadan işlemleri dağıtık bir ağ üzerinde doğrulayarak mobil cihazlarda kullanıcı verilerinin ve işlemlerinin güvenliğini sağlar. İşlemler değiştirilemez ve geri alınamaz bir şekilde kaydedilir, bu da uygulama güncellemeleri, güvenlik yamaları ve kullanıcı aktivitelerinin güvenli bir şekilde kaydedilmesini sağlar. Verilerin güvenli transferini sağlayarak veri hırsızlığı ve

manipülasyon riskini azaltır. Kimlik doğrulama ve erişim kontrolü için kullanılarak kimlik hırsızlığı ve yetkisiz erişim riskini azaltır. Akıllı sözleşmeler, güvenlik politikalarını ve protokollerini otomatik olarak uygulayabilir. Ayrıca, yazılım güncellemeleri ve yama yönetiminde blockchain'in kullanılması, güncellemelerin bütünlüğünü ve doğruluğunu sağlar (Drescher, 2017, s. 59-62).

Blockchain, merkeziyetsizlik ve şeffaflık gibi temel prensipleriyle mobil uygulama güvenliğini artıran sağlam bir katalizör olarak hizmet eder. Geleneksel güvenlik önlemlerinden farklı olarak, blockchain'in merkeziyetsiz sistemi, tek bir hata noktasına bağlı riskleri minimize eder. Bu özellik, karmaşık verilerin basit modeller üzerine kurulu sistemlere entegre edilmesi için güvenli bir ortam sağlar ve mobil uygulamaları korumada kritik öneme sahiptir. Blockchain, dijital işlemlerin sorunsuz ve güvenli bir şekilde gerçekleştirilmesini sağlar ve hassas bilgileri hedef alan siber saldırı risklerini azaltır. Blockchain özelliklerini benimseyen mobil uygulamalar, savunmalarını güçlendirerek potansiyel tehditlere karşı daha dayanıklı bir koruma sunabilir ve kullanıcılara daha yüksek düzeyde güvenlik sağlayabilir (Appinventiv, 2024).

Blockchain teknolojisi, işlemlerin güvenliğini sağlamak için şifreleme ve mutabakat algoritmaları kullanarak saldırganların sistemi aşmasını son derece zor hale getirir. Her işlem şeffaf ve izlenebilir olup, kullanıcılara tüm aktivitelerin net bir kaydını sunar. Bir işlem blockchain'e kaydedildikten sonra değiştirilemez veya silinemez, bu da tüm işlemlerin kurcalanamaz bir kaydını sağlar. Ayrıca, işlemlerde aracıları ortadan kaldırarak maliyetleri düşürür ve verimliliği artırır. Kullanıcılar için gelişmiş güvenlik ve veri koruması sağlar. Dolandırıcılık ve siber saldırı risklerini azaltır. İşlemlerde güven ve şeffaflığı artırır. İş süreçlerini sadeleştirir ve işletmeler için maliyet tasarrufu sağlar. Mobil uygulamaları gelişen siber tehditlere karşı geleceğe hazır hale getirir (Moldstud, t.y.).

4.2.2.3. İleri Düzey Kimlik Doğrulama

İleri düzey kimlik doğrulama (Advanced Authentication), mobil siber güvenlikte kullanıcıların kimliğini doğrulamak için daha karmaşık ve güvenli yöntemler kullanarak güvenlik seviyesini artıran yenilikçi bir yaklaşımdır. Geleneksel kullanıcı adı ve şifre kombinasyonlarının ötesine geçen bu yöntemler, kullanıcıların cihazlarına ve verilere yetkisiz erişimi önlemeye yardımcı olur. Mobil yetkilendirme ve kimlik doğrulama, birçok nedenle önemlidir, bunlar arasında artan güvenlik, dolandırıcılığı ve kimlik hırsızlığını önleme, hassas verilerin korunması yer alır. Çok seviyeli kimlik doğrulama genellikle ek bir

güvenlik katmanı olarak kullanılır (Jasinska & Hanzel, 2024).

4.2.2.3.1. Çok Faktörlü Kimlik Doğrulama

Çok Faktörlü Kimlik Doğrulama (MFA), kullanıcı hesaplarına ekstra bir koruma katmanı ekleyen bir güvenlik mekanizmasıdır. Kullanıcının kimliğini doğrulamak için şifreler, biyometrik veriler ve güvenlik tokenleri gibi birden fazla faktör kullanır. Günümüz güvenlik uzmanları, beş ana kimlik doğrulama faktörünü tanımlar:

- Bilgi faktörleri – kullanıcının bildiği bir şey (PIN, şifre);
- Mülkiyet faktörleri – kullanıcının sahip olduğu bir şey (akıllı telefon, güvenlik tokeni);
- Varlık faktörleri – kullanıcının kendisi olan bir şey (biyometri);
- Konum ve zaman faktörleri – kullanıcının erişim sırasında bulunduğu yer ve zaman;
- Davranış faktörleri – kullanıcının benzersiz hareketleri ve davranışları (ASEE MFA, 2024).

4.2.2.3.2. Biyometrik Kimlik Doğrulama

Kullanıcıların benzersiz biyolojik özelliklerini kullanarak kimlik doğrulama sağlar. Parmak izi, yüz tanıma, iris tarama ve ses tanıma gibi yöntemleri içerir. Biyometrik veriler, sahtekarlık ve kimlik hırsızlığına karşı yüksek güvenlik sağlar çünkü bu veriler kopyalanamaz veya başkası tarafından kullanılamaz. Geleneksel biyometrik veriler, yüz, iris, parmak izi, avuç izi kayıtlarına dayanır. Yenilikçi biyometrik veriler ise, teknolojinin gelişmesi ile beraber kişisel imza, tuş basışları, yürüyüş tarzı, fiziksel aktivite, ses, nefes alışverişi, kalp ritmi gibi daha spesifik bilgileri kaydederek doğrulama yapmayı öngörür (Lien & Vhaduri, 2023, s. 2-4).

Tüm biyometrik kimlik doğrulama sistemleri temelde iki modda çalışır. Öncelikle, tüm kullanıcıların sistemde kaydedilmesi gereklidir; bu süreç Kayıt olarak adlandırılır. Bu kayıt sürecinde, her birey için referans özellikler sistem ortamında saklanır ve ilgili kişinin kimliği ile ilişkilendirilir. Kayıt işlemine tamamlayıcı olarak, Kimlik Doğrulama, kimlik doğrulama sisteminin kimlik doğrulama veya belirleme sürecini ifade eder. Kimlik doğrulama sonucuna varmak için, sistem, sunulan özelliklerin verilerini saklanan referanslarla karşılaştırma yapar bu sayede sadece yetkili erişimlere izin verilir (Vielhauer, 2006, s. 19-20).

4.2.2.3.3. Davranışsal Biyometri

Davranışsal biyometri, geleneksel biyometrik teknolojilere göre birçok avantaj sunar. Kullanıcıdan habersiz veya müdahale olmadan toplanabilir. Davranışsal verilerin toplanması genellikle özel bir donanım gerektirmez ve bu nedenle oldukça maliyet etkindir. Çoğu davranışsal biyometri, insan kimliğini güvenilir bir şekilde tanımlamak için yeterince benzersiz olmasa da, kimlik doğrulamada yeterince yüksek doğruluk sağlamaktadır. Davranışsal biyometri, işlemin başlangıcında bireysel kullanım kalıplarını tanımlamanın ve anlamanın pasif ve proaktif bir yoludur. Bu sayede organizasyonlar, otomasyon sinyallerini tespit edebilir, tipik davranışlardaki anormallikleri izole edebilir ve tipik dolandırıcılık davranışlarına karşı uyarı durumunda olabilir (Lexis Nesis, t.y.).

Kullanıcı Profili Oluşturma, İzinsiz Giriş Tespiti alanında araştırmacılar tarafından incelenmektedir. Bir kişinin bir bilgisayarla etkileşimini gözlemleyerek bu davranışın bir modelini oluşturur ve bu modeli o kullanıcı için normal davranış olarak kullanır. Eğer aynı kullanıcının davranışı önemli ölçüde farklıysa, sistemimizde profili şablon olarak saklanan kullanıcı yerine farklı bir kullanıcının gizlendiği varsayabilir. Kullanıcı modelleme, pazarlama ve özelleştirme amaçları için incelenir. Kullanıcıya ürün ve hizmetleri daha iyi uyarlamak amacıyla bir kullanıcı temsili oluşturmayı hedefler. Örneğin, yazılım yalnızca bu belirli kullanıcının ilgi alanındaki seçenekleri göstererek karmaşık bir yazılımla daha kolay etkileşimde bulunmasını sağlayabilir (Yampolskiy & Govindaraju, 2009, s. 4).

4.2.2.3.4. Cihaz Tanımlama

Cihaz tanımlama, kullanıcıların kimliğini doğrulamak için cihazın benzersiz özelliklerini ve kullanım geçmişini analiz eden bir güvenlik yöntemidir. Bu yöntem, cihazın IP adresi, coğrafi konumu, cihaz modeli gibi bilgiler kullanılarak gerçekleştirilir. Cihaz tanımlama, kullanıcıların kimliğini doğrulamak için cihazın benzersiz özelliklerini ve kullanım geçmişini analiz eden bir yöntemdir. Bu yöntemde cihazın IP adresi, coğrafi konumu, cihaz modeli, tarayıcı ve uygulama verileri ile cihaz parmak izi gibi bilgiler kullanılır. Her cihazın internete bağlandığında aldığı benzersiz bir IP adresi vardır. Bu adres, cihazın coğrafi konumunu ve internet servis sağlayıcısını belirlemede kullanılabilir. Cihazın bulunduğu coğrafi konum GPS, Wi-Fi veya hücresel ağlar üzerinden tespit edilebilir. Bu bilgi, kullanıcının alışılmış konumundan farklı bir yerden giriş yapılıp yapılmadığını belirlemeye yardımcı olabilir. Cihazın marka, model ve işletim sistemi bilgileri analiz edilir.

Bu bilgiler, belirli bir kullanıcının genellikle kullandığı cihazlarla karşılaştırılarak kimlik doğrulama sürecine katkıda bulunur. Cihazın tarayıcı türü, versiyonu, yüklü eklentiler ve cihazda çalışan uygulamalar gibi bilgiler toplanır ve analiz edilir. Cihazın donanım ve yazılım özelliklerinin birleşimiyle oluşturulan benzersiz bir parmak izi oluşturulur. Bu, cihazın geçmişte kullanılan cihazla eşleşip eşleşmediğini kontrol etmek için kullanılır (Goodman, 2023).

4.2.2.3.5. Tek Kullanımlık Şifreler

Tek Kullanımlık Şifreler (One Time Password-OTP), her oturumda veya işlemde farklı bir şifre kullanılarak kimlik doğrulama sağlayan bir güvenlik yöntemidir. OTP'ler genellikle SMS, e-posta veya özel uygulamalar aracılığıyla gönderilir. Geleneksel şifrelere göre daha güvenli olan OTP'ler, her biri yalnızca kısa bir süre için geçerli olduğundan, yetkisiz erişim riskini önemli ölçüde azaltır (Microsoft, 2024).

4.2.2.4. Uçtan uca şifreleme

Uçtan uca şifreleme, mobil siber güvenlikte kritik bir savunma prensibidir ve kullanıcıların verilerinin güvenliğini sağlamak için kullanılır. Bu şifreleme yöntemi, verilerin gönderici cihazdan alıcı cihazın sistemine kadar yalnızca ilgili kişiler tarafından erişilebilir olmasını garanti eder. Uçtan uca şifreleme, verilerin gönderildiği anda şifrelenir ve alıcıya ulaştığında şifresi çözülür. Bu süreçte, veriler sadece gönderen ve alıcı arasında, hiçbir üçüncü tarafın erişimine izin verilmeden şifrelenmiş bir şekilde iletilir. Taşıma Katmanı Güvenliği (Transport Layer Security-TLS) olarak da bilinir. TLS sunucusu, bir veya daha fazla kamu anahtarı sertifikası ve ilgili özel anahtarlarla yapılandırılmalıdır. TLS sunucu uygulamaları, algoritma ve anahtar boyutu esnekliğini desteklemek için birden fazla sunucu sertifikası ve bunlara bağlı özel anahtarlar içermelidir. TLS sunucularının en az bir RSA (Asimetrik Şifreleme Algoritması) anahtar şifreleme sertifikası ile yapılandırılması gerekmektedir (NIST, 2019, s. 10).

4.2.2.5. Segmentasyon

Segmantasyon (Segmentation), ağdaki farklı bölümler arasındaki trafik akışını kontrol ederek çalışır. Bir segmentteki tüm trafiğin başka bir segmentte ulaşmasını durdurma

seçilebilir veya trafik türüne, kaynağına, varış noktasına ve diğer kriterlere bağlı olarak akışı kontrol edilebilir. Ağı nasıl segment edeceğinizi belirlemek, segmentasyon politikası olarak adlandırılır. Geleneksel segmentasyon teknolojileri, dahili güvenlik duvarları, Erişim Kontrol Listeleri (Access Control Lists-ACL'ler) ve ağ ekipmanlarındaki Sanal Yerel Alan Ağı (Virtual Local Area Network-VLAN) yapılandırmalarını içermektedir. Ancak bu yöntemler pahalı ve karmaşık olabilir. Bugün, yazılım tanımlı erişim teknolojisi, ağ trafiğini gruplayarak ve etiketleyerek segmentasyonu basitleştirir. Daha sonra bu trafik etiketlerini kullanarak segmentasyon politikasını doğrudan ağ ekipmanı üzerinde uygular, böylece geleneksel yöntemlerle ilişkili karmaşıklığı azaltır (Cisco Networking, t.y.).

Büyük bir ağın korunması, ağ büyüdükçe daha zor hale gelir. Büyük, segmentlenmemiş bir ağ, yönetilmesi ve korunması zor olabilecek geniş bir saldırı yüzeyi sunar. Trafik ve uygulamalar tüm ağa erişebildiği için, bir saldırgan ağa girdikten sonra, kritik verilere erişmek için ağda yatay hareket edebilir. Ayrıca, büyük bir ağı izlemek ve kontrol etmek daha zordur. Ağın segmentlenmesi, bir saldırganın bölgeler arasında yatay hareket etmesini engelleyerek, ağda ilerlemesini sınırlar. Bir güvenlik bölgesi, bir veya daha fazla fiziksel veya sanal güvenlik duvarı ara yüzü ve bölgenin ara yüzlerine bağlı ağ segmentlerinden oluşan bir gruptur. Her bölge ayrı ayrı koruma kontrol edilebilir, böylece her bölge ihtiyacı olan özel korumaları alır. Örneğin, finans departmanı için bir bölge, BT bölgesinin izin verdiği tüm uygulamalara izin vermeyebilir (PaloAlto Networks, 2024).

İki ara yüzden fazlasına sahip olan güvenlik duvarları, DMZ (Demilitarized Zone) olarak adlandırılan bölgeleri içerebilir. Bu bölgeler, güvenilmeyen bir alandan erişilmesi gereken sunucuları desteklemek için oluşturulur ve bu süreçte güvenilir konumlar tehlikeye atılmaz.

Güvenilir (Trusted): "Güvenilir" terimi, daha güvenli veya korunan bir alan içinde bulunan kullanıcıları ve bilgisayarları ifade etmek için kullanılır. Bu alan genellikle ağın özel bir bölümüdür ve saldırganlar ile diğer güvenlik tehditlerine karşı korunması gerekmektedir. Güvenilir bölgede güvenlik, ağdaki daha az güvenilir bölümlerinden gelen tüm trafiği engelleyerek sağlanır (Pearson IT Certification, 2003).

Güvensiz (Untrusted): "Güvensiz" terimi, potansiyel olarak kötü niyetli saldırganlar veya diğer güvenlik tehditlerini içerebilecek ağ alanlarını tanımlar. Bu, ağın internet tarafı gibi güvensiz alanlarını veya bilinmeyen erişime maruz kalan iç ağın bölümlerini içerebilir (Pearson IT Certification, 2003).

DMZ (Demilitarized Zone): "DMZ" veya silahsızlandırılmış bölge, hem güvenilir hem de güvensiz bölgeler arasında yer alır ve genellikle bu bölgelerden her ikisine de erişimi

olan bilgisayarlara ev sahipliği yapar. Örneğin, bir DMZ'deki bir Web sunucusuna internetten (güvensiz) erişilebilirken, aynı zamanda özel güvenilir ağdaki kullanıcılar tarafından da erişilebilir. Ağınızın iç, özel ve güvenilir kısmından bakıldığında, DMZ bölgesi güvensiz olarak kabul edilir, bu nedenle DMZ'deki bilgisayarların başlatılan trafiği engellenir (Pearson IT Certification, 2003).

Genel olarak ağ tasarımları TRUST-DMZ-UNTRUST üçlüsü şeklinde yapılarak segmente edilirler. Bu sayede Makro Segmentasyon sağlanır ayrıca güvenliği artırmak için bu üç sekme de kendi içlerinde daha küçük bölümlere (mantıksal veya fiziksel arayüzler) ayrılarak Mikro Segmentasyon yapılabilir (Pearson IT Certification, 2003).

4.2.2.6. Konteynerleştirme

Konteynerleştirme(Containerization), mobil siber güvenlikte kullanılan yenilikçi bir savunma yöntemidir. Bu teknoloji, uygulamaların ve hizmetlerin bağımsız, izole bir ortamda çalışmasını sağlar. Konteynerleştirme teknolojisi, uygulamalarını altyapıdan ayırmaya olanak tanır, böylece yazılımı hızlı bir şekilde teslim edilebilir. Konteynerleştirme teknolojisi ile firmalar, altyapıları uygulamaları yönetme yöntemleriyle aynı şekilde yönetebilir. Konteynerleştirme teknolojisinin, kod gönderme, test etme ve dağıtma yöntemlerinden faydalanılarak, kod yazma ile üretimde çalıştırma arasındaki gecikme önemli ölçüde azaltılabilir. Konteynerleştirme, uygulamaların ve hizmetlerin birbirleriyle etkileşime girmeden bağımsız olarak çalışmasını sağlar. Bu izolasyon, kötü amaçlı yazılımların veya güvenlik açıklarının bir konteynerden diğerine sızmasını zorlaştırarak, tüm sistemi etkileme riskini azaltır. Konteynerler bağımsız olarak güncellenebilir ve güvenlik yamaları uygulanabilir, bu da tüm sistemi güncellemeye gerek kalmadan belirli bir uygulamanın güvenliğini artırır. Ayrıca, konteynerler farklı ortamlar arasında taşınabilir, böylece uygulamalar çeşitli platformlarda ve cihazlarda güvenli bir şekilde çalışabilir. Konteyner yönetim sistemleri, uygulama performansını ve güvenlik durumunu izlemeyi kolaylaştırır, bu sayede kaynak kullanımını ve güvenlik olaylarını izleyerek sorunları proaktif bir şekilde tanımlayıp çözebilir. Ayrıca, Konteynerleştirme, düzenleyici uyumluluk ve güvenlik standartlarına uyum sağlamakta yardımcı olur, güvenlik politikalarının ve denetimlerin konteyner ortamında daha verimli ve etkili bir şekilde yönetilmesini mümkün kılar (Docker Docs, t.y.).

4.2.2.7. Bal Küpleri

Bal Küpleri (Honeypots), mobil siber güvenlikte kullanılan yenilikçi bir yöntemdir ve kötü niyetli saldırganları çekmek amacıyla tasarlanmış bir sahte sistemdir. Gerçek bir sistemin taklit edildiği bu yapı, saldırganların dikkatini çekerek onların yöntemlerini ve hedeflerini anlamak için kullanılır. Honeypotların temel özellikleri ve avantajları arasında saldırganları sahte bir hedefe çekme, saldırı taktiklerini izleme ve anlamaya yönelik veri sağlama, erken uyarı sistemi oluşturma, güvenlik araçlarını test etme ve bilgi toplama yer alır. Bu yöntem, güvenlik açıklarını belirlemede ve savunma stratejilerini geliştirmede faydalıdır. Honeypotlar kritik olmayan gerçek veri ile saldırganları kendine çekebilirken bazen de tamamen kirli bilgi ile doldurularak saldırganları yanıltma amacıyla çalışırlar. Genel olarak, iki tür saldırgan vardır: temel becerilere sahip olanlar, birçok sistemi hedef almakla ilgilenirken, daha gelişmiş becerilere sahip olanlar ise yüksek değere sahip birkaç sistemi hedef alır. Her iki tehdit de sürekli olarak evrim geçirmekte ve yeteneklerini geliştirmekte. Bu tehditleri anlayarak, honeypotların değeri daha iyi kavranabilmektedir (Spitzner, 2002, s. 19).

Honeypot sistemine gelen trafiği izleyerek, siber suçluların kaynaklarını, tehdit düzeyini, kullanılan yöntemleri, hangi veri ve uygulamalarla ilgilendiklerini ve güvenlik önlemlerin siber saldırıları durdurma kapasitesi değerlendirilebilir (Kaspersky Cybersecurity, t.y.).

4.2.2.8. Sıfır Güven Ağ Erişimi

Sıfır Güven Ağ Erişimi olarak bilinen Zero Trust Network Access (ZTNA), siber güvenlikte bir yaklaşım ve strateji olarak kullanılan bir terimdir. Bu yaklaşım, geleneksel ağ güvenliği modellerinden farklı olarak, varsayılan olarak hiçbir kullanıcıya veya cihaza güvenmeme ilkesine dayanır. Temel amacı, her kullanıcının ve cihazın kimlik doğrulamasını ve yetkilendirilmesini gerektiren, ağa erişim kontrollerini sıkılaştıran ve böylece saldırı yüzeyini minimize eden bir güvenlik modeli sağlamaktır. ZTNA, ağ kaynaklarına erişimde "sıfır güven" ilkesini benimser. Bu ilke, kullanıcıların ve cihazların güvenilirliğini her zaman sorgulayan ve her bağlantı isteğini ayrı ayrı değerlendiren bir yaklaşımı ifade eder. Bu değerlendirme süreci genellikle çok faktörlü kimlik doğrulama (MFA), cihaz güvenliği durumu kontrolü, ağ trafik analizi ve diğer güvenlik denetimleri gibi yöntemlerle desteklenir. ZTNA, özellikle mobil çalışanlar, uzaktan erişim gerektiren çalışanlar ve bulut tabanlı

uygulamalara yönelik güvenlik ihtiyaçlarını karşılamak için önemli bir rol oynar. Bu yaklaşım, siber saldırıların önlenmesi ve veri güvenliğinin artırılması açısından etkili bir strateji olarak kabul edilir (Forcepoint, t.y.).

BÖLÜM 5

SONUÇ VE ÖNERİLER

Bu tez çalışması kapsamında, mobil iletişim sistemlerinin karşı karşıya olduğu siber güvenlik tehditlerinin genel bir çatısının oluşturulması ve bu çatı altında, kurum yöneticilerine, bilgi sistemleri çalışanlarına ve son kullanıcıya kendilerini ve sistemlerini her gün gelişen saldırı yöntemlerinden koruyabilmeleri için bir kılavuz oluşturulmaya çalışılmıştır.

Birinci Bölümde, problem belirlenmiş, tezin amacına karar verilmiş, önemi ve sınırlılıklarının çerçevesi çizilmiştir.

İkinci Bölümde, elektriksel iletişimin temelleri, tarihçesi ve temel mobil iletişim teknolojileri ifade edilmiştir. Mobil iletişimin, kablolu iletişime göre avantaj ve dezavantajları ortaya konmuş, mobil iletişimin önemine dair tartışılmıştır.

Üçüncü Bölümde, Mobil iletişimde siber saldırı yöntemleri ve bu yöntemler ile gerçekleştirilerek küresel çapta adını duyurmuş vakalar irdelenmiştir. Bu bölümde Siber Saldırı Yöntemleri başlığı altında, zararlı yazılımlar, son kullanıcı ve kimlik avı saldırıları ile ağ sistemi saldırıları incelenmiştir. Zararlı yazılımların, girdikleri sistemlere bulaşarak yayılan, gerektiğinde kendini kopyalayıp başka sistemleri enfekte etmekte olan kod parçacıklarından oluşması incelenmiştir. Son kullanıcı ve kimlik avı saldırıları kısmında ise günlük kullanıcıların karşı karşıya kaldığı Oltalama ataklarından bahsedilmiştir. Ağ sistemi saldırı türlerinde ise kurum ve kuruluşların, dış dünyaya açık web siteleri ve mobil uygulamalarının veya direkt olarak web bağlantılarının karşı karşıya kaldığı zaaflar incelenmiştir. Yine Üçüncü Bölümün son kısmında küresel çapta meydana gelmiş, en fazla sistemi enfekte etmiş veya en kritik kişisel verilere yönelmiş mobil siber güvenlik tehditlere örnekler verilmiştir.

Dördüncü Bölümde, siber güvenlik konusunda çalışmalar yapıp, periyodik raporlar yayınlayan uluslararası kurum ve kuruluşlar ile bu organizasyonlara ait standartlar incelenmiştir. Yine bu bölümün ikinci kısmında ise geleneksel ve yenilikçi teknolojik çözümler irdelenmiş, teknolojinin önümüzdeki yıllarda sektörü yönelteceği yollar tartışılmıştır. Bugünün Geleneksel teknolojilerinin, 30 yıl öncesinin yenilikçi teknolojilerinin, kullanıldıkça gelişen ve firmalarca cihazlar haline getirilen halleri olduğu, bugün yenilikçi kabul edilen teknolojilerin de gelişip evrilerek, bundan sonraki yılların geleneksel standartlaşmış teknolojileri haline geleceği öngörülmüştür. Bugünün yenilikçi

teknolojilerinin, her gün duyduğumuz ve gittikçe kullanımı artan Blockchain, Yapay Zeka, Makina öğrenmesi, Davranışsal Analiz gibi güvenilir ve insan hatasını minimuma indirecek metotlar üzerine kurulacağı öngörülmüştür.

5.1. Sonuçlar

Bu çalışma, mobil iletişim dünyasında siber güvenlik tehditlerini anlamak ve bu tehditlere karşı etkili savunma stratejileri geliştirmek amacıyla yapılmıştır. Araştırma kapsamında, zararlı yazılım türleri, son kullanıcı ve kimlik avı saldırıları ile ağ sistemi saldırıları olmak üzere üç ana saldırı metodu incelenmiştir.

Zararlı Yazılımlar, mobil cihazlara ve ağlara yönelik ciddi bir tehdit oluşturmaktadır. Bu tür saldırılar, kullanıcıların kişisel verilerini çalabilir ve sistemlerde ciddi zararlara yol açabilir. Bunun yanı sıra verileri manipüle edebilir, geri dönülmez şekilde hasar verebilir veya fidye amacıyla ele geçirebilir. Daha az zararlı olarak da sistemleri veya son kullanıcıları sürekli olarak gözetme altında tutabilir, gözetleme sonucu elde edilen verileri kötü niyetler ile kullanabilir veya istenmeyen reklamlara maruz bırakabilir.

Son kullanıcı ve kimlik avı saldırıları ise kullanıcıların güvenliği açısından büyük bir risk taşır; Oltalama gibi yöntemlerle kullanıcıları kandırarak hassas bilgilerini ele geçirebilirler. Ele geçirilen veriler finans, sağlık, savunma gibi kritik sistemlere aitse devamında başka zafiyetlerin sömürülebilmesi amacıyla saldırı yüzeyi oluşturabilir. Oltalama ve Kimlik Avı Metotları ile gerçek sistem ve kullanıcı yetkilerine erişen saldırganlar, bu yetkiler sayesinde tüm kullanıcı ve sistemleri risk altına sokabilirler.

Ağ sistemi saldırıları ise mobil iletişim altyapısını doğrudan hedef alarak hizmet kesintilerine veya veri sızıntılarına neden olabilir. Bu tür saldırılar genellikle, ağ yüzeyinde yer alan zafiyetler sömürülerek gerçekleştirilir. Doğru konfigüre edilmemiş sistem cihazları ve yeterince güvenli olacak şekilde kodlanmamış yazılımlar, sistemin tamamını risk altına sokabilmektedir.

Saldırı Metotları, esasen üç ana başlık altında işlenmiş olsa dahi unutulmamalıdır ki, bu saldırı vektörleri iç içe geçmiş vaziyettedir. Oltalama ile çalınan gerçek kullanıcı verisi ile sisteme girilerek başka saldırılar için yüzey tespit etme veya saldırı vektörü oluşturmak çokça kullanılan yöntemlerdir. Ağ güvenliği zafiyeti sebebiyle çalınan kişisel verileri kullanan saldırganlar, mağdurlar üzerinde daha inandırıcı oltalama yöntemlerini denemektedir. Bu üç saldırı metodunun ilişkisi üçlü sac ayağına benzemektedir. Ayaklardan birisinin olmaması veya zayıf olması halinde, sistemler büyük risk altında kalabilmektedir.

Siber güvenlik alanında çalışan şirketler, organizasyonlar ve resmî kurumlar, meydana gelmiş siber saldırılardan dersler çıkarılması için düzenli araştırmalar yapmakta ve çözüm önerilerine dair hem periyodik hem olay bazlı raporlar yayınlamaktadır. Avrupa Birliği Siber Güvenlik Ajansı, Avrupa Komisyonu, Avrupa Birliği Siber Güvenlik Olaylarına Müdahale Ekibi, Ulusal Siber Güvenlik Ajansı, Avrupa Telekomünikasyon Standartları Enstitüsü ve Elektrik Elektronik Mühendisleri Enstitüsü gibi organizasyonlar devletler veya birlikler tarafından kurulmuş ve yönetilen, her türlü siber olay karşısında aksiyon alarak, hızlı yamalar ve raporlar hazırlayıp kullanıma sunan resmî kurumlar olarak bilinmektedir. Gartner ve NSS Labs gibi uluslararası teknoloji değerlendirme şirketleri ise yine ürün veya saldırı yüzeyi bağlamında güncel raporlar yayınlamaktadırlar. Bu kurum ve kuruluşların yayınladıkları raporların, ilgililerce yakından takip edilerek hızla uygulanması, sistemlerin ve verilerin güvenliğe en uygun şekilde korunmasını sağlamaktadır.

Mobil iletişimde siber saldırılara karşı alınacak tüm tedbirler ancak bütüncül bir yaklaşım ile kararlı şekilde çalışabilir. Otoritelerce kabul edilmiş standartların ve politikaların her sisteme, o sisteme uygun ve uyumlu olacak şekilde uygulanması gerekir. Güvenlik Duvarları, Mobil Cihaz Yönetim Sistemleri, Veri Kaybı Önleme yöntemleri, Saldırı Tespit ve Önleme Sistemleri, Güvenlik Bilgi ve Olay Yönetimi kullanılarak, güncel veri tabanlarından beslenecek güvenlik katmanları sistemleri güvenli hale getirmektedir. Bu geleneksel savunma mekanizmaları, sistemlerin zaman içerisinde maruz kaldığı tehditlere yönelik geliştirilen ve standartlaştırılmış donanım-yazılım ikilisinden oluşmaktadır.

Ancak teknolojinin ve buna bağlı olarak bu teknolojiye yönelecek siber tehditlerin, saldırı alanları ve yöntemleri her gün değişmekte ve artmaktadır. Bu nedenlerden dolayı, siber güvenliğin sağlanabilmesi amacıyla yenilikçi güvenlik önlemleri de bu sistemlerle entegre çalışmalıdır. Yapay zeka tabanlı yaklaşımlar, biyometrik verilere dayanan ileri düzey kimlik doğrulama metotları, davranışsal analiz yapan algoritmalar, çok faktörlü doğrulamalar, gelişmiş uçtan uca şifreleme yöntemleri ve ağ içerisindeki yeni nesil segmentasyonların da kullanılması, siber güvenlikte yenilikçi önlemlerin arasında yer almaktadır.

Elbette veri tabanları, iletişim protokolleri ve ağlar ne kadar iyi konfigüre edilirse edilsin, her zaman kritik açığı insan hataları oluşturmaktadır. Veri sistemlerine sahip her organizasyonun en üst kademesinden en alttaki çalışanlarına kadar farkındalık eğitimlerine güncel olarak tabi tutulmaları gerekmektedir. Aşılamaz denen sistemler ve kırılamaz denen şifreler, sıradan bir kullanıcının Oltalama metotları ile kişisel verilerini çaldırması nedeniyle risk altında kalabilmektedir.

5.2. Öneriler

Bu çalışma, mobil iletişimdeki siber güvenlik tehditlerini analiz etmek ve bu tehditlere karşı etkili savunma stratejilerini önermek amacıyla yapılmıştır. Literatür taraması ve elde edilen bulgular doğrultusunda, öneriler şunlardır:

İlk olarak, mobil kullanıcıların siber güvenlik konusunda bilinçlendirilmesi gerektiği vurgulanmıştır. Kullanıcı eğitim programları ve bilinçlendirme kampanyaları düzenlenerek, temel güvenlik prensipleri ve riskler hakkında bilgi sahibi olmaları sağlanmalıdır. Oltalama veya kimlik avı saldırılarına karşı her gün değişen ve gelişen saldırı metotları güncel olarak incelenerek son kullanıcıların tamamı bilinçlendirilmelidir. Düzenli aralıklarla siber saldırılara karşı son kullanıcı eğitimleri ve belirli periyotlarda habersiz sızma ve oltalama testleri yapılmalıdır. Bu kapsamda kurumlar, personeline yönelik genelde yıllık periyotlarda oltalama testleri yapmakta, bu testlerde genellikle sahte e-postalar atılarak son kullanıcının kişisel verilerini paylaşmasını istemektedir. Kişilerin dikkatini çekecek konular oltalama e-postalarının konuları olarak seçilmekte ve genellikle e-posta içeriğinde zaman kısıtı konarak, kullanıcının acele karar vermesi sağlanarak test yapılmaktadır. Bu nedenle son kullanıcılar kendilerine gelen sesli çağrı, kısa mesaj ve e-postaları inceleyerek dikkate almalı, uzantılarının doğruluğundan emin olmalı hatta tüm bunlar güvenilir görünse bile içerikte yazılanların doğruluğunu düşünmelidir. Çünkü gelen bu sahte istekler, önceden herhangi bir yöntemle ele geçirilmiş olan sistemlerden veya kaynaklardan dahi geliyor olabilir.

Ayrıca, mobil cihazlarda kullanılan kimlik doğrulama yöntemlerinin güçlendirilmesi önem taşımaktadır; biyometrik doğrulama teknolojileri gibi ileri seviye yöntemlerin benimsenmesi, kullanıcıların cihazlarını ve verilerini daha güvenli bir şekilde korumalarına yardımcı olabilir. Parmak izi, göz retinası, yüz tanıma, ses tanıma ve damar tanıma gibi metotlar biyometrik olarak doğrulama yapılması için kullanılan bazı yöntemlerdir. Geleneksel güçlü şifreler ile biyometrik doğrulama metotlarının birlikte kullanılması ile veriler daha güvenli saklanabilir hale getirilmelidir. Kimlik doğrulamada metodlarından olan Çok Faktörlü Doğrulama yöntemleri verimli şekilde kullanılmalı SMS veya OTP gibi yöntemler aktifleştirilmelidir.

Veri iletimi ve depolama süreçlerinde güçlü şifreleme standartlarının zorunlu hale getirilmesi mobil iletişimdeki siber güvenliği artırmak için kritik bir adımdır. Özellikle Uçtan Uca (end-to-end) Şifreleme protokolleri ve AES (Advanced Encryption Standart-Gelişmiş Şifreleme Standardı) gibi güvenli algoritmaların kullanımı, verilerin güvenliğini sağlamak ve yetkisiz erişimlere karşı koruma sağlamak için önemlidir. End-to-End

Şifreleme, verinin gönderici cihazdan alıcı cihaza kadar tüm iletişim yolunda şifrelenmesini sağlayarak veri transferinin güvenliğini artırır. AES, 128-bit, 192-bit veya 256-bit anahtar uzunlukları ile kullanılarak veri depolama ve iletim sırasında etkili bir şekilde şifreleme sağlar. Ayrıca, güvenli anahtar yönetimi ile şifreleme gücünün yanı sıra anahtarların güvenliği, doğru oluşturulması, değiştirilmesi ve güvenli bir şekilde depolanması da sağlanmalıdır. Uygulama ve protokol seviyesinde güvenlik önlemleri de kritik öneme sahiptir; bu, güvenlik açıklarının düzenli olarak değerlendirilmesini ve güncellenmesini gerektirir.

Mobil iletişim altyapılarında sürekli olarak siber tehditlerin izlenmesi ve olay müdahalesi süreçlerinin geliştirilmesi önemlidir. Bu süreçler, potansiyel saldırıların erken tespit edilmesini ve hızlı tepki verilmesini sağlayarak olası zararların minimize edilmesine yardımcı olabilir. İzleme süreçleri, ağ trafiği analizi ve anomalilerin belirlenmesi gibi tekniklerle sürekli olarak gerçekleştirilmelidir. Ayrıca, güvenlik olaylarına karşı hazırlıklı olmak için detaylı bir olay müdahale planı oluşturulmalı ve bu plan düzenli olarak güncellenmelidir. Siber güvenlik olaylarına hızlı ve etkili müdahale, sistemlerin ve kullanıcı verilerinin korunmasında kritik bir rol oynar. Bu nedenle, mobil iletişim sağlayıcıları ve kuruluşlar, reaktif değil proaktif bir siber güvenlik stratejisi izlemeli ve sürekli olarak güvenlik önlemlerini güçlendirmelidir.

Ulusal çapta ve uluslararası düzeyde mobil iletişim siber güvenlik politikalarının güçlendirilmesi ve uyumun sağlanması kritik bir gerekliliktir. Bu politikaların güçlendirilmesi, mobil iletişim altyapılarının ve kullanıcı verilerinin korunmasını sağlamak için temel bir adımdır. Ulusal düzeyde, mobil iletişim operatörleri ve hükümetlerin işbirliği içinde güçlü siber güvenlik politikaları oluşturulması ve uygulanması gerekmektedir. Bu politikalar, yerel düzeydeki yasal düzenlemelerle desteklenmeli ve mobil iletişim sağlayıcılarına yönelik açık kurallar ve standartlar belirlemelidir. Ayrıca, mobil iletişim sektöründeki en iyi güvenlik uygulamaları ve teknolojik gelişmelerin, takip edilerek entegrasyonu teşvik edilmelidir. Uluslararası düzeyde ise, mobil iletişim siber güvenlik politikalarının uyumu ve iş birliği oldukça önemlidir. Uluslararası standartlar ve protokollerin belirlenmesi ve uygulanması, küresel çapta güvenlik sağlanması açısından hayati öneme sahiptir. Uluslararası organizasyonlar ve kurumlar arasında bilgi paylaşımı ve ortak çözümler geliştirme konusunda iş birliği platformları aktif olarak kullanılmalıdır. Bu politikaların güçlendirilmesi, mobil iletişimdeki siber tehditlere karşı etkili bir savunma sağlamak için gereklidir. Sürekli değişen tehdit ortamında güncellenmiş politikalar ve düzenlemeler, mobil iletişim altyapılarının dayanıklılığını artırarak güvenliği sağlamlaştırır

ve sektörün sürdürülebilir gelişimini destekler. ISO, ETSI, IEEE vb. Uluslararası kuruluşların standartları güvenli mobil erişimler için güncel olarak takip edilmeli, tavsiyeler kurumların özel durumlarına göre yorumlanarak uygulanmalı, GDPR ve KVKK (Kişisel Verilerin Korunması Kanunu) gibi yasal düzenlemeler verimli olarak tatbik edilmelidir.

Sonuç olarak, hiçbir ağ veya sistem tam anlamı ile güvenli denilemez. Güncel politikaların ve standartların uygulanması, son kullanıcıdan bilgi sistemleri çalışanlarına kadar tüm kullanıcıların farkındalığının artırılması ayrıca teknolojik altyapının gelecekte oluşabilecek tehditlere yönelik olarak proaktif yaklaşım benimsenerek tasarlanması sistemlerin kararlı ve güvenli çalışmaları için kritiktir.

Kurumumuzda ise; mobil iletişimde siber güvenliğin sağlanabilmesi amacıyla güvenlik duvarları, özel sanal ağ, kimlik doğrulama metotları, segmentasyon yaklaşımları, saldırı önleme sistemleri yanında trafiğin kayıt altına alınıp incelendiği Güvenlik Bilgi ve Olay Yönetimi cihazları ile yazılımları kullanılmakta, bu sistemler yeni güvenlik açıklarına önlem almak üzere, sürekli olarak güncellenmektedir.

Güvenlik Duvarları marifeti ile izinsiz erişimlerin önüne geçilmekte, özel sanal ağ ile uzaktan kurum ağına güvenli ve şifreli bağlantı sağlanmakta, kurum içi ve dışını kapsayacak şekilde tüm iletişim gelişmiş kriptoloji teknikleri kullanılarak yapılmakta, kullanıcı hesapları ve kişisel şifreleri ile yetkisiz erişimler engellenmekte, ağ segmentlere ayrılarak aralarındaki geçişin sadece ilgililerce ve segmente edilmiş olarak yapılması mümkün kılınmakta, saldırı önleme sistemleri ile güvenlik veri tabanlarından çekilen imzalar yardımıyla şüpheli işlemler bertaraf edilmekte ve SIEM ile tüm trafik kayıt altına alınarak, geçmişte meydana gelen olaylar incelenebilmektedir.

Kurumumuzda uygulanabilecek mobil iletişim güvenliği yöntemlerinden bahsedecek olursak şunlar sayılabilir:

- Kişisel kullanımda olan kablosuz cihazların envanterini tutarak, güvenliklerini sağlamak amacıyla Mobil Cihaz Yönetim sistemleri temin edilip, kurumumuza uygun olarak konfigüre edilmeli ve yönetilmelidir. MDM sistemleri sayesinde, kurum iç ağına dâhil olan her mobil cihazın bilgileri tutulup, yetkisiz erişimlerin önüne daha sağlıklı geçilebilir. Kurum kablosuz veya VPN ağına bağlanacak her mobil cihaz, siber güvenlik ekiplerince kontrol edilmeli, tak-çalıştır veya bağlan-çalıştır şeklinde hiçbir cihaz kullanılamamalıdır. Herhangi kişisel mobil bir cihazla (dizüstü, telefon vb.) kurum ağına sadece kullanıcı adı ve şifre doğrulaması metoduyla bağlantı sağlanması, güvenlik risklerini barındırabilir. Bu tarz kişisel cihazlar herhangi bir şekilde güvenlik açığı veya zararlı veri barındırıyor olabilir. Barındırabildikleri

riskler itibariyle sistemi enfekte edebilir, başka cihazları da zararlı yazılımlara maruz bırakabilirler. Kablosuz ağ sistemleri oldukça büyük saldırı yüzeylerini teşkil etmektedir. Kurumumuzdaki kablosuz ağlar, güncel olarak güvenlik duvarları, uçtan uca şifreleme metotları ve kimlik doğrulama yöntemleri ile korunmaktadır. Ancak kullanılacak Mobil Cihaz Yönetim Sistemi yardımı ile çok daha güvenli hale getirilebilir. Kurulacak MDM sistemi ile her kullanıcı her cihazdan sadece kullanıcı adı ve şifre ile sisteme direkt giriş yapamayacak, ek güvenlik katmanı oluşturulacaktır. Yeni cihazların MDM yöneticileri tarafından kontrolü ve kaydı yapılacak bu sayede herhangi yöntemle ele geçirilebilecek cihazlara karşı kullanıcı adı-parola ikilisi dışında ek güvenlik önlemi alınmış olacaktır. Bu alanda alınabilecek önlemler SMS doğrulama veya Tek Kullanımlık Şifreler (OTP) olabileceği gibi makine öğrenimine sahip sistemler de olabilir.

- Kurumumuzda düzenli aralıklarla sızma testleri yapılmakta ve bu test sonuçlarına göre ilgili birimlerce gerekli önlemler alınmakta, güvenlik yamaları yapılmaktadır. Kurumsal web sitesi başta olmak üzere internet yönüne açık uygulamalar, ağ sistemi, veri tabanları ve sunucular bu testlerin önde gelen saldırı yüzeylerini oluşturmaktadır. Sızma testlerinin son aşamaları genellikle son kullanıcılara yapılan oltalama denemeleridir. Sahte bir mail adresinden atılan e-posta yoluyla gerçek kullanıcıların verileri ele geçirilmeye çalışılmaktadır. Bu duruma binaen, oltalama testi sonucunda, son kullanıcılara eğitimler verilmeli ve farkındalıkları artırılmalıdır. Gelen sahte maile davranışları üzerinden kategorileştirilen kişiler, ilgili konular özelinde eğitilmelidir. Çünkü bazı kullanıcılar mailin sahte olduğunu farkederek ilgili birimlere bilgi verirken, oltalama mailindeki bağlantıya tıklayan hatta bu bağlantının yönlendirdiği sahte web sitesine kişisel veya kurumsal bilgileri veren kullanıcılar bulunmaktadır. Kurumsal bilgilerini çaldıran kullanıcılar, daha dikkatli kullanıcıların da gerçek adreslerden gelen istekler sonucu oltama tuzaklarına düşmelerine neden olabilmektedirler. Her farklı davranışı gösteren gruba kendilerine yönelik eğitimler verilmelidir. Bu test sonucunda tüm kurumda kullanıcı şifrelerinin sıfırlanması ve güncel politikalara uygun güçlü şifreler belirlenmesi zorunlu hale getirilmelidir.
- Kurum ağına XDR-EDR ürünleri dahil edilmeli, bu ürünler marifeti ile sunucular ve son kullanıcılara yönelebilecek tehditlere karşı hem aktif hem proaktif önlemler alınmalıdır. Bu ürünler çok geniş yelpazede veri toplayarak müdahale tavsiyeleri verebilmektedir. Uç noktalardan, sunuculara, ağ düğümlerinden, dış erişimlere kadar tüm trafiği kaydedip inceleyen bu ürünler veri ihlallerinin önüne geçmek için otoritelerce kabul görmüş güvenlik katmanları sağlamaktadır ve kurumumuzda da kullanılmalıdır.
- Veri kaybı önleme (DLP) sistemleri Kurum ağına entegre edilerek uygun şekilde

yönetilmelidir. DLP hassas verilerin yetkisiz şekilde paylaşımını, kullanımını ve transferini tespit edip engelleyen küresel çapta kabul görmüş bir veri koruma metodolojisidir. Kurum içi sistemler, bulut hizmetleri ve uç noktalar DLP korumasına alınarak kritik veriler izlenmeli ve korunmalıdır. Tüm kurum ve kuruluşlar gibi kurumumuz da hukuki olarak, topladığı verileri saklamak ve korumak zorundadır. DLP ürünlerinin verimli kullanılabilmesi için elbette öncelikle kurumsal veriler uygun şekilde tasnif edilmeli, teknik personel ve son kullanıcı veri güvenliği konusunda eğitilmeli ve risk seviyeleri tespit edilmelidir.

- BYOD metodolojisinin aktif olarak kullanıldığı Kurumumuzda cihazların ve kullanıcıların sürekli doğrulanmasını gerektiren Zero Trust Security uygulamaları temin edilmelidir. Bu uygulamalar güvenli olduğundan emin olunmayan hiçbir cihazın Kurum ağına veya verilerine ulaşmamasını sağlayacaktır.

Mobil iletişim teknolojilerinde siber güvenlik, günümüzün dijital dünyasında giderek daha önemli bir hale gelmiştir. Gelişen teknolojilerle birlikte mobil cihazlar, bireylerin ve kurumların vazgeçilmez araçları haline gelmiş, bu durum siber tehditlerin de mobil cihazlara yönelmesine neden olmuştur. Bu çalışmada, mobil iletişimde karşılaşılan siber güvenlik tehditleri ve bu tehditlerle başa çıkmak için kullanılan güvenlik teknolojileri ele alınmıştır. Mobil cihazlar, hem kişisel hem de kurumsal verileri barındırdıkları için siber saldırganların hedefi haline gelmiştir. Kötü amaçlı yazılımlar, kimlik avı saldırıları, veri sızıntıları ve ağ temelli saldırılar, mobil cihazlarda en yaygın görülen tehditler arasındadır. Bu bağlamda, mobil iletişimde güvenliği sağlamak için kullanılan yöntemler arasında şifreleme teknolojileri, çok faktörlü kimlik doğrulama, mobil cihaz yönetimi (MDM) sistemleri ve veri kaybını önleme (DLP) çözümleri yer almaktadır. Ayrıca, gelişmiş tehdit algılama ve müdahale çözümleri olan EDR (Endpoint Detection and Response) ve XDR (Extended Detection and Response) gibi teknolojiler de mobil cihazlar için kritik bir rol oynamaktadır. Çalışma kapsamında incelenen bulgular, mobil güvenlikte sadece teknik çözümlerin değil, aynı zamanda kullanıcı farkındalığının da büyük bir önem taşıdığını göstermektedir. Kullanıcıların siber güvenlik tehditlerine karşı bilinçlendirilmesi, güvenlik protokollerinin etkili bir şekilde uygulanması kadar önemlidir. Ayrıca, siber tehditlerin sürekli evrim geçirdiği göz önüne alındığında, güvenlik çözümlerinin de dinamik ve adaptif bir yapıda olması gerekmektedir.

Sonuç olarak, mobil iletişimde siber güvenlik tehditleri ile başa çıkmak, çok katmanlı bir güvenlik yaklaşımı ve sürekli güncellenen teknolojilerle mümkün olabilir. Gelecekte daha

karmaşık saldırı tekniklerinin ortaya çıkacağı göz önüne alındığında, hem bireylerin hem de kurumların güvenlik önlemlerini güçlendirmesi ve siber güvenlik politikalarını sürekli gözden geçirmesi kritik önem taşımaktadır. Mobil cihazların güvenli bir şekilde kullanılabilmesi için siber güvenliğin hem teknolojik hem de insani boyutlarının dengeli bir şekilde ele alınması gerekmektedir.

KAYNAKLAR

Amnesty International. (2021). *Forensic Methodology Report: How To Catch NSO Group's Pegasus.* Amnesty International Ltd.

Appinventiv. (2024, Temmuz 8). *Appinventiv Blockchain*. Retrieved Temmuz 10, 2024 from Appiventiv Web Sitesi: https://appinventiv.com/blog/blockchain-for-mobile-app-security/#:~:text=Blockchain%20serves%20as%20a%20robust,a%20single%20point%20of%20failure.

Armis Cyber Security. (2018). *Blueborne Explained.* Armis Cyber Security.

Armis Inc. (2023). *The dangers of Bluetooth implementations: Unveiling zero day vulnerabilities and security flaws in modern Bluetooth stacks.* Armis Inc.

ASEE MFA. (2024, Haziran 10). *ASEE Group*. From ASEE Web Sitesi: https://cybersecurity.asee.io/blog/multi-factor-authentication-mfa-best-practices/

AWS Amazon. (t.y.). *AWS Amazon VPN*. Retrieved Haziran 6, 2024 from AWS Amazon Web Sitesi: https://aws.amazon.com/tr/what-is/vpn/

Barker, J. (2020). *Confident Cyber Security* . Kogan Page.

Bejtlich, R. (2010). *The Tao of Network Security Monitoring.* Addison-Wesley.

Bergman, N., Stanfield, M., & Jason, R. (2013). *Hacking Exposed Mobile: Security Secrets & Solutions.* McGraw Hill.

Bergman, N., Stanfield, M., Rouse, J., Scambray, J., Geethakumar, S., Deshmukh, S., . . . Price, M. (2013). *Hacking Exposed Mobile: Security Secrets & Solutions.* McGraw Hill.

Berners-Lee, T., & Fischetti, M. (1999). *Weaving Web.* Harper.

Bhunia, S., & Tehranipoor, M. M. (2018). *The Hardware Trojan War. Attacks, Myths and Defenses.* Springer.

Bienkowski, T. (2024, Ocak 23). *Netscout Sniffer*. From Netscout Web Sitesi: https://www.netscout.com/what-is/sniffer

BunnyNET. (2024, Mayıs 12). *Bunny Net*. From Bunny Net Ddos: https://bunny.net/academy/security/what-are-distributed-denial-of-service-ddos-attacks

Buyya, R., & Dastjerdi, A. V. (2016). *Internet of Things: Principles and Paradigms.* Morgan Kaufmann.

Carlson, B. A., Crilly, P. B., & Rutledge, J. C. (2006). *Communication Systems.* McGraw-Hill.

Carlson, B. A., Crilly, P. B., & Rutledge, J. C. (2006). *Communication Systems.* McGraw-Hill.

CEPS Think Tank Task Force. (2021). *Artificial Intelligence and Cybersecurity.* CEPS.

Checkpoint. (t.y.). *Checkpoint CyberAttack*. Retrieved Haziran 13, 2024 from Checkpoint Web Sitesi: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/

CIS Security. (t.y.). *CIS Benchmarks*. Retrieved Haziran 13, 2024 from CIS Web Sitesi: https://www.cisecurity.org/cis-benchmarks

CIS Security. (t.y.). *CIS Controls*. Retrieved Haziran 6, 2024 from CIS Web Sitesi: https://www.cisecurity.org/controls

Cisco. (2020, Şubat 16). *Cisco IDS IPS*. Retrieved Haziran 2024, 2024 from Cisco Web Sitesi: https://learningnetwork.cisco.com/s/question/0D53i00000KsuxDCAR/cisco-idsips-fundamentals

Cisco Network. (t.y.). *Cisco Firewall*. Retrieved Haziran 13, 2024 from Cisco Web Sitesi: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

Cisco Networking. (t.y.). *Cisco Segmentation*. Retrieved Haziran 10, 2024 from Cisco Web Sitesi: https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html

CloudDNS. (2023, Ekim 10). *CloudDNS Smurf Attack*. From CloudDNS Web Sitesi: https://www.cloudns.net/blog/what-is-smurf-ddos-attack

CloudDNS. (t.y.). *CloudDNS ping of death*. Retrieved Mayıs 11, 2024 from CloudDNS: https://www.cloudns.net/blog/ping-of-death-pod-what-is-it-and-how-does-it-work

Cole, E. (2016). *Data Lose Protection.* SANS Org.

Coursera Staff. (2024, Haziran 12). *Coursera Cyber Attacks*. From Coursera Web Sitesi: https://www.coursera.org/articles/types-of-cyber-attacks

Cybersecurity and Infastructure Security Agency. (t.y.). *CISA : Privacy and Mobile Apps*. Retrieved Mayıs 28, 2024 from CISA Web Sitesi: https://www.cisa.gov/news-events/news/privacy-and-mobile-device-apps

Cybersecurity and Infastructure Security Agency. (t.y.). *CISA Best Practices*. Retrieved Mayıs 28, 2024 from CISA Web Sitesi: https://www.cisa.gov/topics/cybersecurity-best-practices

Cybersecurity and Infastructure Security Agency. (t.y.). *CISA Siber Güvenlik Farkındalığı Ayı*. Retrieved Mayıs 28, 2024 from CISA Web Sitesi: https://www.cisa.gov/cybersecurity-awareness-month

Cyware. (t.y.). *Cyware Social*. Retrieved Mayıs 21, 2024 from Cyware Social Web Sitesi: https://cyware.com/news/what-is-cybersecurity-fingerprinting-de718f94

Docker Docs. (t.y.). *Docker Genel Bakış*. Retrieved Haziran 10, 2024 from Docker Docs Web Sitesi: https://docs.docker.com/get-started/overview/

Dooley, M., & Rooney, T. (2017). *DNS Security Management.* John Wiley and Sons; IEEE Press.

Drescher, D. (2017). *Blockchain Basics.* APress.

Durumeric, Z., Li, F., Kasten, J., Adrian, D., Bailey, M., Li, F., . . . Paxson, V. (2014). The Matter Of HeartBleed. *IMC '14: Proceedings of the 2014 Conference on Internet Measurement Conference* (pp. 475-488). IMC Yayınları.

Efe, A., Kalkancı, G., Donk, M., Cihangir, S., & Uysal, Z. (2019, Nisan). A Hidden Hazard: Man-In-The-Middle Attack in Networks. *Dergipark Akademik,* pp. 96-116.

ENISA. (t.y.). *European Union Agency for Cybersecurity*. Retrieved Mayıs 27, 2024 from ENISA Web Sitesi: https://www.enisa.europa.eu/topics/cyber-threats

Equifax. (2024, Mayıs 23). *Equifax*. From Equifax: https://www.equifax.com.au/knowledge-hub/news-and-media/scam-alert-phishing-campaign-impersonating-equifax

Erbschloe, M. (2004). *TROJANS, WORMS, AND SPYWARE.* Butterworth-Heinemann.

Erickson, J. (2003). *Hacking. The Art of Exploitation.* No Starch Press.

European Telecommunications Standards Institute. (2017, Ekim 17). *ETSI TS 102 165.* Retrieved Temmuz 17, 2024 from ETSI Web Sitesi: https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/05.02.03_60/ts_10216501v050203p.pdf

European Telecommunications Standards Institute. (2018, Eylül 11). *ETSI TR 103 305.* Retrieved Haziran 5, 2024 from ETSI Web Sitesi: https://www.etsi.org/deliver/etsi_tr/103300_103399/10330501/03.01.01_60/tr_10330501v030101p.pdf

European Telecommunications Standards Institute. (2020, Ağustos 10). *ETSI TS 133 501.* Retrieved Haziran 5, 2024 from ETSI Web Sitesi: https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/16.03.00_60/ts_133501v160300p.pdf

European Union Agency for Cybersecurity. (2023, Ekim 1). *ENISA Threat Landscape.* Retrieved Mayıs 27, 2024 from ENISA Web Sitesi: https://www.enisa.europa.eu/publications/enisa-threat-landscape-

2023/@@download/fullReport

Federal Trade Commission. (2019). *Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach.* Federal Trade Commission Web Sitesi.

Forcepoint. (t.y.). *Forcepoint ZTNA*. Retrieved Temmuz 17, 2024 from Forcepoint Web Sitesi: https://www.forcepoint.com/cyber-edu/ZTNA

Forouzan, B. A. (2012). *Data Communications and Networking.* McGraw-Hill.

Fortinet. (t.y.). *Fortinet IPS*. Retrieved Haziran 13, 2024 from Fortinet Web Sitesi: https://www.fortinet.com/resources/cyberglossary/what-is-an-ips#:~:text=An%20intrusion%20prevention%20system%2C%20or,alerts%20and%20blocks%20detected%20attacks.

Fortinet. (t.y.). *Fortinet NAC*. Retrieved Haziran 6, 2024 from Fortinet Web Sitesi: https://www.fortinet.com/resources/cyberglossary/what-is-network-access-control

Fortinet. (t.y.). *Fortinet Ping of Death*. Retrieved Mayıs 17, 2024 from Fortinet Web Sitesi: https://www.fortinet.com/resources/cyberglossary/ping-of-death

Fortinet. (t.y.). *Fortinet Rootkit*. Retrieved Haziran 12, 2024 from Fortinet Web Sitesi: https://www.fortinet.com/resources/cyberglossary/rootkit

Gartner. (t.y.). *Consulting.* Retrieved Haziran 5, 2024 from Gartner Web Sitesi: https://www.gartner.com/en/consulting

Gartner. (t.y.). *Digital IQ*. Retrieved Haziran 5, 2024 from Gartner Web Sitesi: https://www.gartner.com/en/marketing/research/digital-iq

Gartner. (t.y.). *Gartner Data Loss Protection*. Retrieved Haziran 6, 2024 from Gartner Web Sitesi: https://www.gartner.com/reviews/market/data-loss-prevention

Gartner. (t.y.). *Gartner Hype Cycle*. Retrieved Haziran 5, 2024 from Gartner Web Sitesi: https://www.gartner.com/en/research/methodologies/gartner-hype-cycle

Gartner. (t.y.). *Gartner Magic Quadrant.* Retrieved Haziran 5, 2024 from Gartner Web Sitesi: https://www.gartner.com/en/research/methodologies/magic-quadrants-research

GeekforGeeks. (2024, Mayıs 11). *GeeksforGeeks Arp Spoofing*. From GeeksforGeeks: https://www.geeksforgeeks.org/what-is-arp-spoofing-attack/

General Data Protection Regulation. (t.y.). *What is GDPR*. Retrieved Mayıs 28, 2024 from GDPR Web Sitesi: https://gdpr.eu/what-is-gdpr/

Goodman, M. (2023, Ekim 17). *GlobalSign Digital ID*. Retrieved Haziran 10, 2024 from GlobalSign: https://www.globalsign.com/en/blog/digital-id-platforms-defend-

against-ai-threats

Grossman, J., Hansen, R., & Petko Petkov, A. R. (2007). *XSS Attacks.* Syngress Inc.

Hadnagy, C., & Fincher, M. (2015). *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails.* Wiley .

Halfond, W. G., Viegas, J., & Orso, A. (2006). A Classification of SQL Injection Attacks and Countermeasures. *International Symposium on Signals, Systems and Electronics*, 1-11.

Heena, & Mehtre, B. (2021, Mayıs). *Advances In Malware Detection- An Overview.* Cornell University.

Hiquet, S. L. (2003). *Building a Virtual Private Network.* Premier Press.

Hnamte, V., & Hussain, J. (2024). Enhancing security in Software-Defined Networks: An approach to efficient ARP spoofing attacks detection and mitigation. *Telematics and Informatics Reports*.

Hoglund, G., & Butler, J. (2005). *Rootkits: Subverting the Windows Kernel.* Addison-Wesley Professional.

Holma, H., & Toskala, A. (2012). *LTE Advanced: 3GPP Solution for IMT-Advanced.* Wiley Yayınları.

Hoş, S. (2024, Mayıs 5). *Çözüm Park EDR.* Retrieved Temmuz 6, 2024 from Çözüm Park Web Sitesi: https://www.cozumpark.com/endpoint-detection-and-response-edr-nedir-nasil-calisir/

Huang, A., & Rudolph, L. (2007). *Bluetooth Essentials for Programmers.* Cambridge University Press.

Hulme, G. V. (2012, Mart 19). *CSO MDM*. Retrieved Haziran 6, 2024 from CSO Web Sitesi: https://www.csoonline.com/article/535256/mobile-security-mdm-part-of-the-mobile-security-solution.html

IEEE. (2018, Nisan 25). *Introduction to IEEE 802.11 Standarts.* Retrieved Haziran 6, 2024 from Irit Web Sitesi: https://www.irit.fr/~Zoubir.Mammeri/Cours/Introduction_IEEE802-11.pdf

IEEE. (t.y.). *IEEE About Us*. Retrieved Haziran 6, 2024 from IEEE Web Sitesi: https://www.ieee.org/about/index.html

Information Commissioner's Office. (2020, Ocak 01). *ICO Hakkımızda*. Retrieved Temmuz 17, 2024 from ICO Web Sitesi: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/01/new-uk-information-commissioner-begins-term/

Intego MAC Security. (2021, Mayıs 10). *Intego Blog*. Retrieved Mayıs 2024, 14 from Intego

MAC Security: https://www.intego.com/mac-security-blog/xcodeghost-malware-infected-100-million-ios-users-and-apple-said-nothing/

International Organization for Standardization. (t.y.). *ISO 27001 Standardı*. Retrieved Mayıs 27, 2024 from ISO Web Sitesi: https://www.iso.org/standard/iso-iec-27000-family

Invicti. (2023, Ekim 10). *Man in the Middle Attacks*. From Invicti Web Sitesi: https://www.invicti.com/blog/web-security/man-in-the-middle-attack-how-avoid/

ITIC. (2014, Ekim 27). *ITIC Institutions and Organizations*. Retrieved Haziran 13, 2024 from ITIC Web Sitesi: https://www.itic.org/dotAsset/c/c/cc91d83a-e8a9-40ac-8d75-0f544ba41a71.pdf

Janet, A. (1991). *Inventing The Internet.* The MIT Press.

Jasinska, D., & Hanzel, S. (2024, Haziran 10). *Neontri Teknoloji Inovasyon*. From Neontri Web Sitesi: https://neontri.com/enhancing-security-with-advanced-mobile-authentication-techniques/

John, R. R. (2024). *Defense Information Systems Agency*. From Defense Information Systems Agency Web sitesi: https://www.disa.mil/about/our-history

Kaplan, E., & Hegarty, C. (2005). *Understanding GPS: Principles and Applications, Second Edition.* Artech House On Demand.

Kaspersky Cybersecurity. (t.y.). *Kaspersky Honeypot*. Retrieved Haziran 10, 2024 from Kaspersky Web Sitesi: https://www.kaspersky.com.tr/resource-center/threats/what-is-a-honeypot

Kaspersky. (t.y.). *Kaspersky Adware*. Retrieved Mayıs 16, 2024 from Kaspersky: https://www.kaspersky.com.tr/resource-center/threats/adware

Kaspersky. (t.y.). *Kaspersky Cyber Security*. Retrieved Mayıs 22, 2024 from Kaspersky Web Sitesi: https://www.kaspersky.com.tr/resource-center/definitions/zero-day-exploit

Kaspersky. (t.y.). *Kaspersky Smurf Attack*. Retrieved Mayıs 17, 2024 from Kaspersky Güvenlik: https://www.kaspersky.com.tr/resource-center/definitions/what-is-a-smurf-attack

Kaspersky. (t.y.). *Kaspersky Spyware*. Retrieved Mayıs 12, 2024 from Kaspersky Cybersecurity: https://www.kaspersky.com.tr/resource-center/threats/spyware

Khan, J., Abbas, H., & Al-Muhtadi, J. (2015). Survey on Mobile User's Data Privacy Threats and Defense Mechanism. *International Workshop on Cyber Security and Digital Investigation*, 376-383.

Korkmaz, M., Koçyiğit, E., Şahingöz, Ö. K., & Diri, B. (2022). A Hybrid Phishing Detection System Using Deep Learning-based URL and Content Analysis. *Elektronika Ir*

Elektrotechnika, 80-89.

Lewis, J. (2003). *The Telegraph: A History of Morse's Invention and Its Predecessors in the United States.* McFarland & Company.

Lexis Nesis. (t.y.). *Lexis Nesis Behavioral Biometrics*. Retrieved Haziran 10, 2024 from Lexis Nesis Risk Solutions: https://risk.lexisnexis.com/global/en/insights-resources/article/what-is-behavioral-biometrics#:~:text=Behavioral%20biometrics%20is%20a%20passive,Target%20typical%20fraudulent%20behavior

Lien, C.-W., & Vhaduri, S. (2023, Ağustos 25). ACM Dijital Kütüphane. *ACM Computing Surveys*, pp. 1-37. From ACM: https://dl.acm.org/doi/10.1145/3603705

Linear Stack. (2023, Mart 23). *Linear Stack Negative and Positive Model*. Retrieved Temmuz 17, 2024 from Linear Stack Web Sitesi: https://www.linearstack.com/blog/when-to-leverage-the-negative-vs-positive-security-model

Ling, R. (2015). *Science Direct*. From Science Direct: https://www.sciencedirect.com/topics/social-sciences/mobile-communication

Liska, A., & Gallo, T. (2017). *Ransomware. Defending Against Digital Extortion.* O'Reilly Media.

Liska, A., & Stowe, G. (2016). *DNS Security.* Syngress.

Liska, A., & Stowe, G. (2016). *DNS Security Defending the Domain Name System.* Syngress.

Liska, A., & Stowe, G. (2016). *DNS Security: Defending the Domain Name System.* Syngress.

Lopa, M., & Vora, J. (2015, Ekim 1). Evolution Of Mobile Generation Technology: 1G to 5G and Review of Upcoming Wireless Technology 5G. *Internetional Journal of Computer Science and Mobile Computing*, pp. 47-53.

Lough, A. (2015). *The Threat Intelligence Research That Mattered to You This Year*. PaloAlto Networks.

McGowan, E. (2024, Temmuz 3). *Norton Malware*. From Norton Security: https://uk.norton.com/blog/malware/famous-computer-viruses

Meenakshi. (2014, Haziran). Analysis of Performance Metrics in Wired and Wireless Networks. *Journal of Science, Engineering and Management*, pp. 63-67.

Microsoft. (2024, Şubat 4). *Microsoft OTP*. Retrieved Haziran 10, 2024 from Microsoft: https://learn.microsoft.com/en-us/microsoftteams/rooms/create-otp

Microsoft. (t.y.). *Microsoft SIEM*. Retrieved Haziran 6, 2024 from Microsoft Web Sitesi:

https://www.microsoft.com/tr-tr/security/business/security-101/what-is-siem

Mike, A. (2021). *A Profound Guide On Cyber Security*. Independently Published.

Miller, D. R., Harris, S., Harper, A. A., VanDyke, S., & Blask, C. (2011). *Security Information and Event Management(SIEM) Implementation.* McGraw-Hill Companies.

Mitnick, K. D., & Simon, W. L. (2003). *The Art of Deception: Controlling the Human Element of Security.* Wiley Publishing INC.

Mlytics. (2024, Mayıs 16). *Mlytics*. From Myltics Phishing: https://learning.mlytics.com/cyber-attacks/what-is-a-phishing-attack/

Mockapetris. (1987, Kasım 1). Domain Names - Concepts and Facilities. *Internet Engineering Task Force IETF*, pp. 1-54.

Moldstud. (t.y.). *Moldstud Makaleler Bölümü*. Retrieved Haziran 10, 2024 from Moldstud: https://moldstud.com/articles/p-the-role-of-blockchain-in-securing-mobile-app-transactions#:~:text=Blockchain%20technology%20utilizes%20cryptographic%20algorithms,and%20protected%20from%20fraudulent%20activities.

National Institue of Standarts and Technology. (2024, Şubat 23). *NIST Siber Güvenlik.* Retrieved Mayıs 27, 2024 from NIST Web Sitesi: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.pdf

NIST. (2019). *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations: NIST SP 800-52 Rev. 2.* NIST.

NordVPN. (t.y.). *NordVPN Adware*. Retrieved Haziran 12, 2024 from NorvVPN Web Sitesi: https://nordvpn.com/tr/blog/adware-nedir/

NSS Labs. (t.y.). *Nss Hakkımızda.* Retrieved Haziran 5, 2024 from Nss Labs Web Sitesi: https://nsslabs.com/about-us/

NSS Labs. (t.y.). *NSS Labs Rapor Tipleri.* Retrieved Haziran 5, 2024 from NSS Labs Web Sitesi: https://nsslabs.com/types-of-reports/

Ohrtman, F., & Roeder, K. (2003). *Wi-Fi Handbook: Building 802.11b Wireless Networks.* McGraw-Hill Professional.

Osho, O., Oluyomi, A., Misra, S., Ahuja, R., Damasevicius, R., & Maskeliunas, R. (2019). Comparative Evaluation of Techniques for Detection of Phishing URLs. *International Conference on Applied Informatics* (pp. 385-394). Applied Informatics.

OWASP. (2024, Mayıs 21). *Session Hijacking Attack: OWASP*. From OWASP Web sitesi: https://owasp.org/www-community/attacks/Session_hijacking_attack

Palo Alto Networks. (t.y.). *Palo Alto Networks XDR ve EDR*. Retrieved Haziran 6, 2024 from Palo Alto Networks: https://www.paloaltonetworks.com/cyberpedia/what-is-edr-vs-xdr

PaloAlto Networks. (2024, Mayıs 24). *PaloAlto Networks PortScan*. From PaloAlto Networks: https://www.paloaltonetworks.com/cyberpedia/what-is-a-port-scan

PaloAlto Networks. (2024, Temmuz 1). *PaloAlto Zone Protection*. Retrieved Temmuz 5, 2024 from PaloAlto Web Sitesi: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/zone-protection-and-dos-protection/network-segmentation-using-zones

Parisi, A. (2020). *Artificial Intelligence for Cybersecurity.* Packt Publishing.

Pearson IT Certification. (2003, Kasım 7). *Pearson Web Sitesi*. Retrieved Temmuz 17, 2024 from Pearson Firewall: https://www.pearsonitcertification.com/articles/article.aspx?p=101741

Pierer, M. (2016). *Mobile Device Management.* Springer Vieweg.

Pierer, M. (2016). *Mobile Device Management.* Springer Vieweg.

Purplesec. (2024, Mayıs 21). *Purplesec DNS Amplification*. From Purplesec Web Sitesi: https://purplesec.us/prevent-dns-amplification-attack

Rai, S., & Chukwuma, P. (2016). *Security and Auditing of Smart Devices.* Auerbach Publications.

Raiu, C. (2022, Şubat 7). *Kaspersky Cyber Security*. Retrieved Mayıs 2024, 14 from Kaspersky Web Sitesi: https://www.kaspersky.com.tr/blog/how-to-protect-from-pegasus-spyware/10492/

Rappaport, T. S. (1991, 11 1). The Wireless Revolution. *IEEE Community Magazine*, pp. 52-54.

Rappaport, T. S. (2002). *Wireless Communications.* Prentice Hall.

SANS. (t.y.). *SANS Security Awareness*. Retrieved Haziran 13, 2024 from SANS Web Sitesi: https://www.sans.org/security-awareness-training/

Seri, B., & Vishnepolsky, G. (2023). *The dangers of Bluetooth implementations: Unveiling zero day vulnerabilities and security flaws in Bluetooth stacks.* Armis Inc.

Shane, G. (2017). *How the Internet Became Commercial: Innovation, Privatization, and the Birth of a New Network.* Princeton University Press.

Singh, M., Sharma, P., Sharma, R., & Vyas, M. (2022). *Advance Cyber Security*. Arcler Press.

Speed, T., & Maor, E. (2017). *Mobile Security: How to Secure, Privatize and Recover Your Devices.* Packt Pub LTD.

Spitzner, L. (2002). *Honeypots: Tracking Hackers.* Addison Wesley.

Stallings, W. (2011). *Network Security Essentials Fourth Edition.* Pearson Education.

Stallings, W. (2011). *Network Security Essentials: Applications and Standarts Fourth Edition.* Prentice Hall.

Stallings, W. (2011). *Network Security Essentials: Applications and Standarts, Fourth Edition.* Prentice Hall.

Stamp, M., Visaggio, C. A., Mercaldo, F., & Troia, F. D. (2022). *Cybersecurity for Artificial Intelligence.* Springer Publishing.

Standage, T. (1998). *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-line Pioneers.* Walker and Company.

Sungook, H. (2001). *From Marconi's Black-box to the audion.* The MIT Press.

Synopsys Inc. (2020, Haziran 3). *Heart Bleed*. Retrieved Mayıs 13, 2024 from Heart Bleed Web Sitesi: https://heartbleed.com/

Szor, P. (2005). *The Art of Computer Virus Research and Defense.* Pearson Education Incorporated.

The Center for Internet Security. (t.y.). *CIS About Us*. Retrieved Mayıs 28, 2024 from CIS Web Sitesi: https://www.cisecurity.org/about-us

Trellix. (t.y.). *Trellix Ransomware*. Retrieved Haziran 12, 2024 from Trellix Web Sitesi: https://www.trellix.com/security-awareness/ransomware/what-is-ransomware/

Trend Micro. (2017, Eylül 18). *Trend Micro Security*. Retrieved Mayıs 2024, 24 from Trend Micro Web Sitesi: https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/equifax-breach-what-to-do-and-what-to-watch-out-for

Trend Micro. (t.y.). *Info: Trend Micro*. Retrieved Mayıs 21, 2024 from Trend Micro Web Sitesi: https://www.trendmicro.com/vinfo/us/security/definition/zero-day-vulnerability

Trend Micro. (t.y.). *Trend Micro XDR*. Retrieved Haziran 6, 2024 from Trend Micro Web Sitesi: https://www.trendmicro.com/tr_tr/what-is/xdr.html

Turhost. (2023, Ekim 11). *Turhost DNS Spoofing*. From Turhost : https://www.turhost.com/blog/dns-spoofing-nedir

Turknet. (t.y.). *Turknet IPS ve IDS*. Retrieved Haziran 13, 2024 from Turknet Web Sitesi: https://turk.net/blog/ips-ve-ids-nedir-nasil-calisir/

U.S. House of Representatives. (2018). *The Equifax Data Breach.* Majority Staff Report 115th Congress, Amerikan Kongresi.

V. (n.d.). From https://www.varutra.com/understanding-sniffing-attacks-how-they-work-

and-how-to-stay-protected/

Vielhauer, C. (2006). *Biometric User Authentication for IT Security*. Springer Science+Business Media, Inc.

Wallarm. (2024, Mayıs 21). *Wallarm SQL Injection*. From Wallarm Web Sitesi: https://www.wallarm.com/what/structured-query-language-injection-sqli-part-1

Whitman, M., & Mattord, H. (2021). *Principles of Information Security*. Cengage Learning.

Xiao, C. (2015). *More Details on the XcodeGhost Malware and Affected iOS Apps.* PaloAlto Networks.

Xiao, C. (2015). *NovelMalware XcodeGhost Modifies Xcode, Infects Apple iOS Apps and Hits App Store.* PaloAlto Networks.

Yampolskiy, R. V., & Govindaraju, V. (2009). Taxonomy of Behavioural Biometrics. *Research Gate*, 1-43.

Yener, M. E. (2021, Haziran). Bulut Bilişimin Teknik ve İşletimsel Açıdan İncelenmesi: Kamu Bilişim Sistemlerinde Kullanımı. *RTÜK Uzmanlık Tezi*.

Zargar, S. T., Joshi, J. B., & Tipper, D. (2013, Kasım). A Survey of Defense Mechanisms Against Distributed Denial of Service. *IEEE Communications Surveys & Tutorials*, pp. 2046-2069.

Zerodium. (t.y.). *Zerodium Program*. Retrieved Temmuz 17, 2024 from Zerodium Web Sitesi: https://zerodium.com/program.html

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı ve Soyadı : Mert Bahadır KAYA

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

İş Deneyimi :

Unvan	Görev Yeri	Yıl
Üst Kurul Uzman Yardımcısı	Radyo ve Televizyon Üst Kurulu	2021-Devam

Akademik Bilgiler :

Öğrenim Durumu :

Derece	Bölüm/Program	Üniversite	Yıl
Lisans	Bilgisayar Mühendisliği	Erciyes Üniversitesi	2010-2019

RTÜK