İSTANBUL BİLGİ ÜNİVERSİTESİ
LİSANSÜSTÜ PROGRAMLAR ENSTİTÜSÜ
BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

TEKNİK VE HUKUKİ BOYUTLARIYLA ELEKTRONİK ÖDEME SİSTEMLERİNDE SİBER GÜVENLİK

CEMAL ARAALAN
1186922044

Doç. Dr. LEYLA KESER BERBER

İSTANBUL

2020

TEKNİK VE HUKUKİ BOYUTLARIYLA ELEKTRONİK ÖDEME SİSTEMLERİNDE SİBER GÜVENLİK

Elektronik Ödeme Sistemlerinde Siber Güvenlik / Cyber Security Concerning Electronic Payment Systems

Cemal Araalan
1186922044

Tez Danışmanı : **DOÇ. DR. LEYLA KESER BERBER** (İmza)

.....

İstanbul Bilgi Üniversitesi Hukuk Fakültesi

Jüri Üyeleri : **DR. MEHMET BEDİİ KAYA** (İmza)

.....

İstanbul Bilgi Üniversitesi Hukuk Fakültesi

DOÇ. DR. MESUT SERDAR ÇEKİN (İmza)

.....

Türk Alman Üniversitesi Hukuk Fakültesi

Tezin Onaylandığı Tarih : 27.11.2020

Toplam Sayfa Sayısı : 345

Anahtar Kelimeler (Türkçe)	Anahtar Kelimeler (İngilizce)
1) Siber güvenlik	1) Cyber security
2) Elektronik ödemeler	2) Electronic payments
3) Siber saldırılar	3) Cyber attacks
4) Bankacılık ve finans	4) Banking and finance

ÖNSÖZ

Dava avukatlığı olarak mesleğimin, gündelik hayatta da risk hassasiyetimin gelişmesi ve olası risklere karşı hazır olmak gibi bir yetenek kazandırdığına inanıyorum. Ancak, yüksek lisans sürecinde, mesele siber güvenlik olduğunda tez yazım sürecinde bu çalışmadan da öğrendiğim kadarıyla, siber uzayda riskler davalara nazaran hem daha öngörülemez hem de sonuçları oldukça ciddi. Yeni teknolojik çözümlerle beraber değişimin çok hızlı olduğu elektronik ödeme sistemlerinde özellikle Covid-19 sürecinde, insanların dijital ortamda işlerini halletmesi adeta bir zorunluluk haline geldi. Tez yazım sürecimin Covid 19 pandemi salgınına denk gelmesi ise; dijitalleşme zorunluluğunun birçok süreci kolaylaştırmakla beraber, siber korsanların bu dönemi adeta fırsata çevirdiğine tanıklık etmeme neden oldu. Bu dönemde Türkiye'de ve dünyada regülasyon açısından tez konumu ilgilendirebilecek birçok yeni yasal düzenleme yürürlüğe girmekle beraber her geçen gün siber korsanlar tarafından yaratıcı birçok yeni siber saldırı yöntemi geliştirildi ve gelecekte de geliştirilmeye devam edecek. Bu bağlamda, çalışmamın özellikle siber güvenliğin herkesi ilgilendiren boyutu itibariyle elektronik ödeme sistemleri gibi önem taşıyan bir alanda katkı sağlamasını temenni ederim.

Tez sürecinde öncelikle Tez Danışmanım olarak değerli katkılarını hiçbir surette benden esirgemeyen ve konuya kendi sınırlı algım dışımda bakmamı ve çalışmamda yeni ufukları keşfetmeme imkân sağlayan kıymetli Hocam Doç. Dr. Leyla Keser Berber'e teşekkürü bir borç biliyorum. Yüksek lisans sürecinde özellikle Seminer derslerinde ve tezin ilk taslak aşamasında fikirlerini aldığım değerli Hocam Dr. Mehmet Bedii Kaya'ya da teşekkür ederim. Ayrıca, yine yüksek lisans sürecinde "Bir Dersten Daha Ötesi" sloganıyla gerçekten derslerine katılmakla özellikle tez konumu ilgilendiren birçok regülasyon bakımından kendisinden çok şey öğrendiğim Hocam Mustafa Aydın'a da teşekkür etmek isterim. Ayrıca, Covid-19 sürecinde eve kapanmaya başladığımız 2020 Mart ayından itibaren tez sürecinde zaman zaman yalnız bırakmak zorunda kaldığım, ancak bana tüm yüksek lisans sürecinde sabırla destek

vermiş hayat arkadaşım ve sevgili eşim Merve'nin desteği bu tezi bitirmemde en büyük ilham kaynağım oldu.

Son olarak, bu çalışmamı başta 31 Ekim 2020 tarihinde yaşanan üzücü İzmir depreminde annesi, kızkardeşi ve teyzesini yitiren can dostum Okan Gidiş olmak üzere tüm depremzede ailelerine ithaf ederim.

İstanbul, 2020

Cemal Araalan

KISALTMALAR

ABC	:	Agricultural Bank of China
AEA	:	Avrupa Ekonomik Topluluğu
API	:	Application Programming Interfaces (Uygulama Program Arayüzü)
APT	:	Advanced Persistent Threats (Gelişmiş Sürekli Tehdit)
ATM	:	Automated Telling Machines (Otomatik Vezne Makinesi)
BCG	:	Boston Consulting Group
BDDK	:	Bankacılık Düzenleme ve Denetleme Kurulu
BGD	:	Bilgi Güvenliği Derneği
BGYS	:	Bilgi Güvenliği Yönetim Sistemi
Bkz./bkz.	:	Bakınız
BSI	:	British Standards Institute (İngiliz Standartlar Enstitüsü)
BTK		Bilgi Teknolojileri ve İletişim Kurumu
B2B	:	Business-to-business (İşletmeden işletmeye)
B2C	:	Business-to-consumer (İşletmeden tüketiciye)

CCE	:	The Consequence-driven Cyber-informed Engineering (Sonuca Dönük Siber Destekli Mühendislik)
CHIPS	:	Clearing House Interbank Payments
CIWIN	:	Critical Infrastructure Warning Information Network (Kritik Altyapı Uyarı Bilgi Ağı)
CPU	:	Central Processing Unit (Merkezi İşleme Birimi)
CSIRT	:	Computer Security Incident Response Team (Bilişim Güvenliği Olay Müdahale Ekibi)
Çalıştay	:	Siber Güvenlik Çalıştayı
DCEP	:	Digital Currency Electronic Payment (Dijital Para Birimi Elektronik Ödeme)
DDoS	:	Distributed Denial of Service (Dağıtık Hizmeti Engelleme Saldırısı)
DNS	:	Domain Name System (Alan Adı Sistemi)
DLT	:	Distributed Ledger Technology (Dağıtık Veri Tabanı Teknolojisi)
DoD	:	Department of Defense (ABD Savunma Bakanlığı)
DoS	:	Denial of Service (Hizmeti Engelleme Saldırısı)
DTPS		Dijital Tek Pazar Stratejisi
dp.	:	Dipnot

EBA	:	European Banking Authority (Avrupa Bankacılık Kurumu)
ECPA	:	Electronic Communications Privacy Act (Elektronik İletişim Ve Mahremiyet Kanunu)
EÇT	:	Elektronik Çek Transferi
EFT	:	Electronic Fund Transfer (Elektronik Fon Transferi)
EMA	:	Electronic Money Association (Elektronik Para Kurumu)
ENISA	:	European Union Agency for Network and Information Security (Avrupa Birliği Ağ Ve Bilgi Güvenliği Teşkilatı)
EPCIP	:	European Programme for Infrastructure Protection (Avrupa Kritik Altyapıların Korunması Programı)
e-ID	:	Elektronik Kimlik
e-RMB	:	Electronic Renminbi
EV SSL	:	Extended Validation SSL (Geniş Kapsamlı SSL)
FED	:	Federal Reserve (Amerikan Merkez Bankası)
FOMO	:	Fear of Missing Out (Gelişmeleri Kaçırma Korkusu)
FSTC	:	Financial Services Technology Consortium (Finansal Hizmetler Teknoloji Konsorsiyumu)

GSM	:	Global System for Mobile Telecommunication (Mobil Telekomünikasyon Açısından Global Sistem)
ICO	:	Initial Coin Offering (Kitle Fonlama Kampanyası)
IDL	:	International Idaho Lab (Uluslararası Idaho Laboratuvarı)
ISO	:	International Standards Organization (Uluslararası Standartlar Kurumu)
IP	:	Internet Protocol (İnternet Protokolü)
IVR	:	Interactive Voice Response (Etkileşimli Ses Cevaplama)
KHK	:	Kanun Hükmünde Kararname
KVK Kurulu	:	Kişisel Verileri Koruma Kurulu
Kurumsal SOME	:	Kurumsal Siber Olaylara Müdahale Ekibi
MFA	:	Multi-factor Authentication (Çok Faktörlü Kimlik Doğrulama)
MGKÇ	:	Müşteri Güvenlik Koruma Çerçevesi
NFC	:	Near Field Communication (Yakın Alan Haberleşmesi)
NIST	:	National Institute of Standards and Technology (Ulusal Standartlar Ve Teknoloji Enstitüsü)

OWASP	:	Open Web Application Security Protocol (Açık Web Uygulama Güvenliği Protokolü)
P2P	:	Peer to peer (Eşler Arasında)
POS	:	Point of Sales (Satış Noktası)
PUKÖ	:	Planla-Uygula-Kontrol Et-Önlem Al
PTT	:	Posta ve Telgraf Teşkilatı Anonim Şirketi
QR	:	Quick Response (Hızlı Cevap)
RFID	:	Radio Frequency Identification (Radyo Frekansı Kimlik Tanımlama)
SCA	:	Secured Customer Authentication (Güçlü Müşteri Onayı)
SDML	:	Signed Document Markup Language (İmzalı Doküman Biçimlendirme Dili)
SEPA	:	Single Euro Payments Area (Tek Avro Ödemeler Alanı)
Sektörel SOME	:	Sektörel Siber Olaylara Müdahale Ekibi
SET	:	Secure Electronic Transactions (Güvenli Elektronik İşlem)
SFNB	:	Security First Network Bank (Güvenli İlk Ağ Bankası)
SMS	:	Short Messasing Service (Kısa Mesajlaşma Hizmeti)

SSI	:	Self-Sovereign Identity (Kendiliğinden Bağımsız Kimlik)
SSL	:	Secure Socket Layer (Güvenli Giriş Katmanı)
SWIFT	:	Society for Worldwide Interbank Financial Telecommunication (Bankalar Arası Global Finansal Telekomünikasyon Örgütü)
TBB	:	Türkiye Bankalar Birliği
TBD	:	Türkiye Bilişim Derneği
TCMB	:	Türkiye Cumhuriyeti Merkez Bankası
TİB	:	Telekomünikasyon İletişim Başkanlığı
UBGÜK	:	Ulusal Bilgi Güvenliği Üst Kurulu
UBKB	:	Ulusal Bilgi Güvenliği Kurumu
UDHB	:	T.C. Ulaştırma, Denizcilik Ve Haberleşme Bakanlığı
USGS	:	Ulusal Siber Güvenlik Stratejisi
USOM	:	Ulusal Siber Olaylara Müdahale Merkezi
vb.	:	Ve benzeri
vd.	:	Ve devamı

İÇİNDEKİLER

ŞEKİL LİSTESİ

TABLO LİSTESİ

ABSTRACT

As it can be understood from the headline of the thesis, it is hereby aimed to analyze the matter of "cyber security concerning electronic paymet systems". Therefore, in order to clarify the conceptual basis of cyber security and as well as the methods of cyber attacks, the basic electronic payment systems that are subject to cyber attacks are technically indicated. In the meantime, taking the possible cyber attacks into consideration, in this thesis the possible precautions to be followed have been searched in broad sense. Precaution, in this study, has been evaluated not only for its technical perspective such as CEE Methodolgy but also it is emphasized the legal and administrative methods to be applied in case of cyber attacks. In this regard, while the basic nine types of cyber attack vectors are determined considering the case study relating to sector-spesific incidents in banking and finance sector, the precautions that are fit to this spesific attacks have been also observed and interpreted in detail. On the other hand, the regulatory amendments that concern the subject of thesis are analyzed in terms of comparative law and as well as considering the recent legislative changes in Turkey. Taking into account of comparative law analysis, it has also been conducted a research on the legislations of European Union, United States and Republic of China concerning the subject of this study and the reflections in this respect are speficied. This thesis also sets for the possible impacts of the regulatory changes in these countries and more importantly, their reflection to each other and Turkey and Turkey's position in that regard. Last but not least, the innovative approaches in respect of the cyber security for electronic payment systems are subject to this research (i.e. blockchain technology, artificial intelligence, open banking and the effects of Covid-19 pandemic) and have been evaulated in order to contribute for the clarification of this matter.

Key Words: Cyber security, electronic payments, cyber attacks, banking and finance.

ÖZET

Tezin başlığından da anlaşılacağı üzere, bu çalışmada elektronik ödeme sistemlerinde siber güvenlik meselesinin teknik ve hukuki yönleriyle ayrıntılı olarak incelenmesi amaçlanmıştır. Bu konuda özellikle başta elektronik ödeme sistemlerinde siber güvenlik denildiğinde, bu konun kavramsal çerçevesinin ne olduğu, siber saldırı yöntemlerinin anlaşılabilmesi açısından bu saldırıların yöneltiği elektronik ödeme sistemlerinin neler olduğuna ilişkin temel bilgiler ile elektronik ödemelere yöneltilen temel siber saldırıları vektörlerinin neler olduğu ve bu kapsamda bu saldırılara karşı alınabilecek önlemler de detaylı şekilde irdelenmiştir. Tedbir denildiğinde, tez içeriğinden de görüleceği üzere, özellikle bütünsel açıdan CEE Metodolojisi gibi teknik açıdan mühendislik çözümlerinin yanı sıra hukuki ve idari açıdan alınabilecek tedbirlerin neler olduğu incelenerek; elektronik ödeme sistemlerine yöneltilebilecek ve çalışma kapsamında tespit edilen dokuz saldırı yöntemine yönelik olarak da bankacılık ve finans sektörüne yönelik sektör spesifik olaylardan yola çıkılarak konunun uygulama noktasına ışık tutulmaya çalışılmıştır. Tez içeriğinde konunun teknik detaylı analizlerini, özellikle bu alanda karşılaştırmalı hukuk ve Türkiye'de bu konuyu ilgilendirebilecek mevzuat değişiklikleri bakımından da neler öngörüldüğü konusunda kapsamlı bilgiye yer verilmiştir. Karşılaştırmalı hukuk açısından özellikle Avrupa Birliği, Amerika Birleşik Devletleri ve Çin Halk Cumhuriyeti açısından incelenen her ülkenin bu alana özgü regülasyonları ve bunların zaman zaman birbirlerine yönelik etkileri ile özellikle Türkiye'deki kanun koyucu açısından olası etkilerinin neler olabileceği konusunda da çıkarımlar yapılmıştır. Türkiye'de ise, elektronik ödeme sistemlerinde siber güvenlik denildiğinde akla gelebilecek tüm yasal düzenlemeler ile taslak halindeki düzenlemeler de değerlendirilerek regülasyon bakımından Türkiye'nin hangi konumda durduğuna ilişkin ışık tutulmaya çalışılmıştır. Son olarak ise; elektronik ödeme sistemlerinde siber güvenlik bakımından yeni yaklaşımların neler olabileceği (blokzincir teknolojisi ve yapay zeka ile sağlanabilecek çözümler, açık bankacılık ve Covid-19 pandemi salgının bu konuya olası etkileri gibi) konusunda

detaylı değerlendirmelere yer verilerek elektronik ödeme sistemlerinde siber güvenliğin sağlanmasında yenilikçi çözümlerin neler olabileceği hususunda katkı sağlanması amaçlanmıştır.

Anahtar Sözcükler: Siber güvenlik, elektronik ödemeler, siber saldırılar, bankacılık ve finans.

GİRİŞ

İnternetin gündelik hayatımıza girmesi, geçmişte matbaanın bulunması gibi insanlık açısından bilgi transferinde adeta devrim yaratmış ve bilim insanlarına göre, insanoğlunun iki bin yıl içerisinde ürettiği bilgi, yapılan kaba bir hesaplama ile günümüzde bir gün içerisinde üretilebilir hale gelmiştir[1]. Ancak, bu denli verinin işlenmesi, depolanması ve transferi günümüzde bilgi güvenliğinin en zayıf katmanı olan "insan" faktörü dikkate alındığında[2], bu bilgiye sahip olmak isteyen ve bu yolda gayri yasal yollara başvurmayı göze alan bazı kişileri "saldırgan", bu konuda bilinçsizce hareket eden bazı kişileri ise "kurban" haline getirmiştir. Dolayısıyla,

[1] Biliminsanlarının tahminlerine göre insanoğlu, hiyerogrifler, kitaplar, resimler, filmler, plaklar, bantlar, disketler, CD'ler, DVD'ler, ses verileri de dahil olmak üzere akla gelebilecek tüm veriler dikkate alındığında, iki bin yıl içerisinde toplamda yaklaşık 2 eksabayt veri üretmiş olup günümüzde bu miktarda verinin tek bir günde üretildiği belirtilmiştir. Konu ile ilgili ayrıntılı bilgi için Bkz. Ulrich Eberl, "Akıllı Makineler Yapay Zeka Hayatımızı Nasıl Değiştiriyor", Paloma Yayınevi, Temmuz 2019, 1. Baskı, (*"Eberl"*), s. 49'da 1 no'lu dp.'da belirtilen John Gantz/David Reinse ve Gitta Rohling.

[2] Bu noktada önemli bir tespit olarak doktrinde Yılmaz tarafından sosyal mühendisliğin kişisel ve kurumsal verilerin korunması açısından dikkate alınması gereken ciddi bir tehdit olduğu, bir kurumdaki güvenlik seviyesini belirlemek için en zayıf halkaya bakıldığı, en zayıf halkanın insan faktörü olduğu, dolayısıyla teknik olarak ne kadar önlem alınırsa alınsın, bilinçsiz bir kullanıcının bulunduğu bir ortamda güvenliği sağlamanın mümkün olmayacağına özellikle vurgu yapılmaktadır. Bkz. Hasan Yılmaz, "TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması ve Bilgi Güvenliği Risk Analizi", Kidder, Denetişim /2014-15, (*"Yılmaz"*), s. 48: https://dergipark.org.tr/en/download/article-file/208742 (Gözden Geçirilme Tarihi: 29.10.2020). Öte yandan, 2014 yılında IBM şirketi, incelediği güvenlik vakalarının yüzde 95'inin "insan hatası" içerdiğini açıklamıştır. Bkz. IBM, "IBM Security Services 2014 Cyber Security Intelligence Index": https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligence_20450.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

Endüstri 4.0[3] kapsamında nesnelerin interneti (Internet of Things – IoT)[4], yapay zeka[5] ve bulut bilişim[6] gibi teknolojilerin gelişmesi ile gelecekte siber saldırıların kapsam, sınır ve sayı itibariyle artan bir ivme ile çoğalacağını söylemek yanlış olmayacaktır. Bu

[3] Esas itibariyle, Endüstri 4.0 kavramından, çağdaş üretim otomasyonu, akıllı okuyucular, yeni nesil mobil internet teknolojileri, nesnelerin interneti, büyük veri, bulut bilişim, birbirleri ile iletişim kurabilen üretim cihazları ve robotlar, üç boyutlu yazıcılar, kısaca en son teknoloji ile donatılmış yeni nesil akıllı üretim fabrikaların da dahil olduğu siber devrim anlaşılmaktadır. Endüstri 4.0 kavramı dünyada ilk olarak 2011 yılında Almanya'da Hannover Fuarı'nda ortaya çıkmıştır. 2011 yılında gerçekleşene fuardan sonra çeşitli çalışmalar ve üretimler yapılarak Almanya'da dördüncü sanayi devriminin ilerlemesine ve yayılmasına destek olunmuş, bu bağlamda Ekim 2012'de Endüstri 4.0 çalışma grubu başkanlığını Ekim 2012'de Siegfried Dais (Robert Bosch GmbH) ve Hennig Kagermann (Acatech) üstlenerek Alman Federal Hükümeti'ne Endüsrti 4.0 ile ilgili uygulama tavsiyelerinde bulunmuşlardır. 08.04.2013 tarihinde ise Hannover Fuarı'nda bu çalışma grubu tarafından Endüstri 4.0 raporu sunulmuştur. Bu konuda ayrıntılı bilgi için bkz. Ogan Özdoğan, Endüstri 4.0 Dördüncü Sanayi Devrimi Ve Endüstriyel Dönüşümün Anahtarları, Pusula, İstanbul, 2018, (*"Özdoğan"*), s. 27, vd. (Gözden Geçirilme Tarihi: 29.10.2020)

[4] Nesnelerin interneti, İngilizce'de "Internet of things" (kısaca *"IoT"*) olarak ifade edilen bir kavram olup birbiriyle bağlantılı aygıtların teknolojik olarak algılayıcılar/sensörler vasıtasıyla birbirlerine bağlanarak haberleşmesi anlamına gelmektedir. Bu konuda detaylı bilgi için bkz. Müjdat Gökçe, "Nesnelerin İnterneti": file:///C:/Users/cemal/Downloads/NESNELERIN_INTERNETI_Internet_of_Things.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[5] Literatürde yapay zekanın tanımı konusunda zengin bir içerik söz konusu olup yapay zekanın tek bir tanımı olmadığı görülmüştür. Yapay zekayı tanımlamak açısından her şeyden önce bazı bu kavramın bazı kriterlere dayandırılması gereklidir: Yapısal yapay zeka (Structure-AI) insan beyninin nasıl çalıştığı konusunda yapay zeka çalışmalarına katkı sağlamaktadır. Davranışsal yapay zeka (Behaviour-AI), insan davranışlarının bilgisayarların kullanılmasına nasıl etki edeceği konusuna yoğunlaşmaktadır. Yetisel yapay zeka (Capability-AI) yapay zekanın değişik uygulamalar sayesinde değişik problemleri nasıl çözebileceğine katkı sağlamaktadır. İşlevsel yapay zeka (Function-AI) ise bilişim teknolojisi açısından yeni yazılımlar üreterek (bazen donanım da olabilir) yapay zekada bilişimin hangi farklı türleri olabileceğine katkı sağlamayı amaçlamaktadır. İlkesel yapay zeka (Principle AI) ise değişik varsayımlar ve hedefler çerçevesinde yapay zeka açısından bilginin en efektif şekilde nasıl işleneceğine katkı sağlamaktadır. Tüm bu kriterleri tek bir tanım altında toplamanın yapay zekayı açıklamak açısından yetersiz olacağı ifade edilmiştir. Bu konuda detaylı bilgi için Bkz. Pei Wang, "What Do You Mean by "AI"?" (*"Wang"*): file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/What_Do_You_Mean_by_AI.pdf (29.10.2020). Türk doktrininde ise, Zafer Zeytin ve Eray Gençay tarafından kaleme alınan "Hukuk Ve Yapay Zeka: E-Kişi, Mali Sorumluluk Ve Bir Hukuk Uygulaması" başlıklı makalede ise, benzer şekilde yapay zekanın kabul görmüş tam ve tek bir tanımı bulunmadığına dikkat çeken yazarlar, yapay zekanın "genel olarak insan benzeri bir zekanın simülasyonu olduğunu" ifade etmektedir. Diğer bir ifade ile, Zeytin/Gençay'a göre, yapay zeka ile bugün insan zekasına benzer şekilde çalışabilen, algıladığı olguları nitelendirebilen ve bu nitelendirmelere dayanarak değerlendirme yapabilen, tüm bunların sonucunda ise karar verebilen ve uygulayabilen robotik bir sistemin oluşturulmasının amaçlandığı belirtilmiştir. Bkz. Zafer Zeytin/Eray Gençay, "Hukuk Ve Yapay Zeka: E-Kişi, Mali Sorumluluk Ve Bir Hukuk Uygulaması", TAÜHFD/ZtdR- 2019/1, s. 42 vd. (*"Zeytin/Gençay"*), ilgili makaleye ulaşmak için: https://docs.google.com/viewerng/viewer?url=https://robotic.legal/wp-content/uploads/2020/05/HUKUK-VE-YAPAY-ZEKA-Zeytin-Gen%C3%A7ay.pdf&hl=tr (Gözden Geçirilme Tarihi: 29.10.2020).

bağlamda, dijital dünyada Thomas Hobbes'ın deyimiyle "insan insanın kurdudur"[7] deyimi her geçen gün daha geçerli hale gelmiştir ve saldırganlar, gerçekleştirdikleri siber saldırıları çoğu kez maddi bir menfaat sağlamak amacıyla kurbanlarının ödeme sistemlerine yöneltme eğilimindedir. Ödemelerin ise zamanla nakitten dijital ortama kayması elektronik ödeme sistemlerini siber saldırılar açısından ulaşılması cazip bir hedef haline getirmiştir. Siber uzay denilen, saldırıların yaratıcılığın sınırlarını zorladığı ve saldırganların çoğu kez yılmaz bir motivasyon içerisinde olduğu bir ortamda, siber güvenliğin elektronik ödemeler açısından ne şekilde temin edileceği konuyu siber hijyen gibi klasik yöntemlerin dışına çıkılarak bir çözüm aranmasını zorunlu kılmıştır. Çalışmanın, tam olarak odak noktası da siber güveliğin yediden yetmişe herkesi ilgilendiren boyutu ile siber atakların teknoloji ile evrilen yönü ve elektronik ödeme sistemlerinin kaçınılmaz gelişimi neticesinde aslında hangi konularda zayıf olduğumuza ve bu konuda ne gibi önlemler alabileceğimize hukuki ve teknik açıdan ışık tutabilmektedir. "Elektronik ödeme sistemlerinde siber güvenlik" denildiğinde, bu çalışmanın merkezindeki iki kavram olan "elektronik ödemeler" ve "siber güvenlik" adeta madalyonun iki yüzü gibi dinamik bir konu olduğu bilinciyle hareket edilmiştir. Çalışma açısından, madalyonun bir yüzünde elektronik ödeme endüstrisinde özellikle Covid-19 pandemi salgının dijitalleşmeyi zorunlu kıldığı koşullar nedeniyle sistemin sürekli evrildiği ve günümüzde her an dinamik şekilde

[6] Bulut bilişim kavramını kısaca özetlemek gerekirse, "bulut" kavramı iletişim ağ yapısı içerisinde, verilerin transferleri esnasında karmaşık yapıda içerisinden geçtiği yollardan oluşan alanı, "bilişim" kavramı ise insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve verinin düzenli bir şekilde işlenmesi sonucu ortaya çıkan bilgiyi ifade etmektedir. Bulut bilişimin tanımı, bulut bilişim ile ilgili temel kavramlar ve ayrıntılı açıklamalar konusunda Bkz. Murat Topaloğlu/Harun Özkişi/Egemen Tekkanat, "Bulut Bilişim", Seçkin Yayıncılık, 2017, Ankara, s. 19-20 (*"Topaloğlu/Özkişi/Tekkanat"*). Bulut bilişimin bu tanımından da anlaşılacağı üzere, bulut teknolojisi internetin zaman içerisinde gelişmesiyle beraber bilginin elektronik ortamda işlenmesi, kullanılması ve depolanması amaçlarına hizmet etmektedir. Bkz. Metin Turan, Bulut Bilişim, Seçkin Yayınevi, Ankara, 2019, (*"Turan"*), s. 27.

[7] "İnsan insanın kurdudur" şeklindeki bu aktarım, "Homo homini lupus est" şeklinde ilk olarak, milattan önce üçüncü yüzyılda yaşamış Romalı ozan ve oyun yazarı Titus Macchius Plautus tarafından kullanılmış olmakla beraber, Thomas Hobbes'un tasvir ettiği insan doğasını ifade etmek için kullanılan Latince bir deyimdir. Bkz. Hümeyra Karagözlü, "Homo Homini Lupus, Thomas Hobbes'un Ahlak Felsefesi Üzerine" adlı makalesi (*"Karagözlü"*): https://dergipark.org.tr/en/download/article-file/162706 (Gözden Geçirilme Tarihi: 29.10.2020)

elektronik ödemelerde sürekli yeni bir ürün ve çözümün tartışıldığı hesaba katılarak elektronik ödemelerde birtakım yeni teknolojik çözümler siber güvenlik perspektifiyle ele alınmıştır. Madalyonun diğer yüzünde ise, siber saldırganların dijital ortamın kendilerine sağladığı konfor alanı içerisinde her geçen gün daha etkin bir rol oynadığı da dikkate alınarak siber güvenlik alanında genel geçer klasik bazı yöntemler yerine dinamik, güncel ve inovatif çözümlerin neler olabileceğine cevap aranmıştır. Bu bağlamda, elektronik ödeme sistemlerinde siber güvenlik açısından ne gibi sorunlarla karşılaşılabileceği irdelenerek bu kapsamda bu sorunların aşılabilmesi amacıyla teknik ve hukuki açıdan ne gibi önlemler alınması gerektiği, Türkiye'deki mevzuat ve dünyada bazı ülkeler özelindeki hukuki düzenlemeler de dikkate alınarak karşılaştırmalı hukuk açısından da ele alınmıştır.

Çalışma, temelde altı ana bölüm içermektedir:

İlk Bölümde, bilgi güvenliği kavramı, bilgi güvenliğinin unsurları ve siber güvenlik kavramının bilgi güvenliğinden hangi açılardan farklı bir kavram olarak değerlendirildiği konusunda literatürde gerekli kaynaklar incelenerek özellikle elektronik ödeme sistemlerinde siber güvenlik denildiğinde ne anlaşılması gerektiği konusunda genel bir giriş yapılmak istenmiştir.

İkinci Bölümde, elektronik ödeme sistemlerinde saldırganların sık tercih ettiği siber saldırı yöntemlerinin neler olduğu tek tek ele alınarak bu kapsamda temelde şu dokuz adet siber saldırı vektörü açısından teknik birtakım değerlendirmelere yer verilmiştir: (i) Kartlı Ödeme Sistemlerine Yönelik Siber Saldırılar, (ii) Oltalama (Phishing) Saldırıları, (iii) Sosyal Mühendislik Saldırıları, (iv) SWIFT Sistemine Yönelik Siber Saldırılar, (v) Elektronik Finans Sektöründe Zararlı Yazılımların Etkileri, (vi) Ağlara Yönelik Gerçekleştirilen Siber Saldırılar, (vii) Kripto Paralara Yönelik Siber Saldırılar, (viii) APT denilen "Sürekli Gelişmiş Tehdit" (ix) İnternet Bankacılığı Ve Mobil Bankacılığa Yönelik Siber Saldırılar.

Üçüncü bölümde ise, genel itibariyle siber güvenlik alanında alınması gereken genel tedbirler ile elektronik ödemeler açısından da inovatif bir yaklaşım olduğu düşünülen ve kısaca CCE denilen "Siber Destekli Mühendislik Metodolojisi" hakkında detaylı analizlere yer verilmiştir. Ayrıca, bu bölümde ikinci bölümde belirtilen dokuz adet siber saldırı yönteminin her biri konusunda alınabilecek tedbirlerle ilgili elektronik ödeme endüstrisinden somut örneklerle siber güvenliğin ne şekilde temin edilebileceği sorusuna çözüm aranmıştır.

Dördüncü bölümünde, dünyada regülasyonlar açısından başta ISO Standartları çerçevesinde konunun incelenmesi akabinde, karşılaştırmalı hukuk kapsamında esas itibariyle bu alanda dikkate alınması gerektiği düşünülen (i) Avrupa Birliği, (ii) ABD ve (iii) Çin Halk Cumhuriyeti açısından elektronik ödeme sistemlerinde siber güvenliğe yönelik mevzuatta hangi hukuki düzenlemelerin öngörüldüğü ve bu konudaki yeni gelişmeler ayrıntılı şekilde değerlendirilmiştir.

Beşinci bölümde, genel itibariyle Türkiye'de elektronik ödeme sistemlerinde siber güvenlik ile ilgili yasal düzenlemeler hakkında kapsamlı bilgiye yer verilmiştir. Bu kapsamda dikkate alınan mevzuat hükümleri açısıdan (i) yürürlükte bulunan mevzuat hükümleri, (ii) çalışmanın tamamlandığı tarih itibariyle bu konuda yeni yürürlüğe giren mevzuat hükümleri ile yakın zamanda yürürlüğe girmesi beklenen yasal düzenlemeler ile (iii) bu alanda taslak halinde olan yasal düzenlemeler hakkında da tez kapsamında detaylı bilgiye yer verilmiştir.

Altıncı ve son bölümde ise, "elektronik ödeme sistemlerinde siber güvenlik ile ilgili yeni eğilimler" başlığı altında, yukarıda da belirtildiği üzere konunun dinamik ve hızlı evrilen yönü dikkate alınarak dünyada bu konuda takip edilen inovatif yaklaşımlar şu başlıklar altında irdelenmek suretiyle tez kapsamında durum tespitinin bir adım ötesine geçilmesi hedeflenmiştir: (i) Kripto Paralarda Siber Güvenlik ve Blokzincirin Siber Güvenliğin Sağlanmasındaki İşlevi, (ii) Biyometrik Ödemelerde Siber Güvenliğin

Temini, (iii) Açık Bankacılık ve Siber Güvenlik, (iv) Yapay Zekanın Siber Güvenlik Alanında Bankacılığa Etkileri, (v) Covid-19 Pandemi Salgının Dijital Bankacılığa Etkileri.

Sonuç itibariyle; bu çalışmada siber güvenliğinin toplumdaki her bireyi doğrudan ilgilendiren bir mesele olması ve özellikle dünyada gelişmekte olan elektronik ödeme sistemlerinde siber güvenliğin temininde teknik ve hukuki açıdan ne tür problemlerle karşılaşıldığı, bu saldırılara karşı hangi önlemlerin alınması gerektiği ve özellikle karşılaştırmalı hukuk açısından konunun irdelenmesi neticesinde dünyada ve Türkiye'de yasal açıdan hangi adımların atılması gerektiği ortaya koyularak bilimsel açıdan katma değer yaratılması amaçlanmıştır.

METODOLOJİ

Metodolojik olarak çalışmanın yazım aşaması öncesinde içerik itibariyle temelde "siber güvenliği" ilgilendirmekle beraber aynı zamanda "elektronik ödeme sistemleri"ni de ilgilendirmesi sebebiyle, başlangıçta özellikle yeni nesil ödeme sistemleri de dâhil olmak üzere elektronik ödeme sistemlerinin (özellikle siber güvenlik boyutu açısından) neler olduğu ve Covid-19 salgını ile birlikte elektronik ödeme sistemlerindeki dünyada ve Türkiye'deki yeni eğilimlerin neler olduğuna ilişkin güncel gelişmeler takip edilerek detaylı bir kaynak araştırması yapılmıştır. Ayrıca, teknik olarak günümüzde yaygın şekilde karşılaşılan siber saldırı vektörlerinin neler olduğu konusunda da kaynak taraması yapılarak özellikle bazı siber saldırılar ve bu saldırılara karşı alınabilecek önlemler konusunda finans ve bankacılık sektörü özelinde sektör-spesifik saldırı türleri konusunda kapsamlı şekilde literatür incelenmiştir. Ayrıca, konunun teknik boyutlarının netleştirilmesi açısından bazı uzmanlardan çalışma kapsamında fikir de alınmıştır. Konunun bu belirtilen teknik yönleri ile ilgili daha detaylı bir bilgi edinilmesi akabinde ise, elektronik ödemelerde siber güvenlik dünyada ve Türkiye'de mevcut hukuki düzenlemeler çerçevesinde regülasyon boyutu ile de incelenmiştir. Bu noktada ise, elektronik ödemelerde siber güvenlik açısından

önce ISO ve sonraki aşamada sırasıyla AB, ABD ve Çin'de bu alandaki dikkat çeken regülasyonlar karşılaştırmalı hukuk anlamında incelenerek ilerleyen kısımda ise Türkiye'deki siber güvenlik alanında özellikle çalışmaya katkı sağlayabilecek önemli düzenlemelere yer verilmiştir.

Çalışma içeriğinden de anlaşılacağı üzere, aslında elektronik ödeme sistemlerinde siber güvenlik meselesi kapsam itibariyle konunun teknik ve hukuki olmak üzere iki ana çerçevede dengeli bir şekilde ele alınmak istenmiştir (tezin 1., 2., 3. ve kısmen 6. bölümlerinde teknik, 4. ve 5. bölümlerinde ise ağırlıklı olarak hukuki boyutu ele alınmıştır) ve anlatım açısından okuyucuya kolaydan zora (özellikle teknik açıklamaların yer aldığı bölümlerde) gidecek şekilde bir aktarım yöntemi tercih edilerek konunun daha kolay anlaşılması hedeflenmiştir.

Tezde metodolojik olarak belirli sınırlamalar çerçevesinde hareket edilmesi uygun görülmüştür. Herhangi bir elektronik ödeme sisteminde siber güvenliğinin ne olduğunun anlaşılabilmesi için öncelikle söz konusu ödeme sisteminin ne olduğu ve nasıl çalıştığının anlaşılması gerekeceğinden, çalışmanın ilk kısıtı olarak kapsam itibariyle sadece aşağıda belirtilen elektronik ödeme sistemleri siber güvenlik boyutuyla ele alınacaktır[8]:

1) Kartlı Ödeme Sistemleri (Kredi Kartları, Debit Kartlar ve ATM Cihazları, Akıllı Kartlar)

2) Kartsız Ödeme Sistemleri (Havale, EFT, SWIFT, SEPA ve Diğer Elektronik Ödeme Yöntemleri[9])

[8] Yazar tarafından elektronik ödeme sistemlerinde siber güvenlik açısından kartlı ve kartsız ödeme sistemleri olarak incelenen iki ana başlığa ilaveten "elektronik ödemelerde siber güvenlik açısından yeni eğilimler (trendler)" şeklinde bir üçüncü başlık da eklenmesi düşünülmüştür. Ancak, üçüncü başlık olabilecek bu konunun önemi dikkate alınarak elektronik ödemelerde yeni eğilimler esas itibariyle çalışmanın 6. bölümünde ayrıca kapsamlı şekilde irdelenmiştir.

[9] "Diğer Elektronik Ödeme Yöntemleri" başlığı altında hangi ödeme sistemlerine yer verildiği çalışmanın 1.2.2.5 no'lu başlığı altındaki açıklamalarda belirtilmiştir.

İkinci kısıt olarak, zaman açısından bu çalışma yazıldığı tarih sadece 2020 yılı Ekim ayına dek "elektronik ödemelerdeki siber güvenlik" konusundaki gelişmelerin aktarılması hedeflenmiştir.

BİRİNCİ BÖLÜM

ELEKTRONİK ÖDEME SİSTEMLERİNDE SİBER GÜVENLİK İLE İLGİLİ GENEL BİLGİLER

İlk bölümde, öncelikle elektronik ödeme sistemlerinde siber güvenlikle ile ilgili genel açıklamalara yer verilerek çalışmada diğer bölümlerde derinlemesine tartışılacak konular hakkında genel bir fikir verilmesi hedeflenmiştir. İlk bölüm, çalışmada ilerleyen bölümlerde özellikle regülasyon ve bir sonraki aşamada ise bankacılık sektörüne özgü sektör-spesifik siber saldırı vektörleri ve bu bağlamda alınabilecek teknik önlemlere geçilmeden önce konunun temel kavramlarının anlaşılması açısından çalışmanın ısınma turları olarak düşünülebilir. Zira, elektronik ödeme sistemlerine yönelik teknik tespitlere ve konu ile ilgili dünyada ve Türkiye'de regülasyon çalışmalarına yer verilmeden önce elektronik ödemeler endüstrisinin temel yapı taşlarının neler olduğu ve her ödeme sisteminin nasıl çalıştığı ilerleyen aşamalarda yer verilecek teknik tespitlerin daha iyi anlaşılmasına imkân sağlayacaktır.

Çalışmanın ilk bölümünde, öncelikle bilgi güvenliği ve siber güvenliğin kavramsal çerçevesinin ne olduğu belirtilerek "elektronik ödeme sistemlerinde siber güvenlik" denildiğinde literatürde bu konseptten ne anlaşıldığına dair farklı değerlendirmeler analiz edilerek bu kapsamda ayrıca yazarın bu konudaki anlayışına yer verilecektir. Öte yandan, elektronik ödeme sistemleri bakımından dünyada yaygın şekilde kullanılan elektronik ödeme sistemlerinin temel itibariyle (i) işleyişi, (ii) siber güvenlik nasıl değerlendirilmesi gerektiğine ilişkin soruya cevap aranmıştır.

1.1. GENEL OLARAK BİLGİ GÜVENLİĞİ VE SİBER GÜVENLİK

Öncelikle bu çalışmanın birer üst başlığı olarak "siber güvenlik" ile "bilgi güvenliği" kavramlarının literatürde gerçekleştirilen kaynak taraması sonucunda doktrinsel açıdan ne anlama geldiği ve bu kavramların hangi açılardan birbirinden farklı olduğu belirlenecektir. Bunun dışında, aşağıda da görüleceği özellikle bilgi güvenliği kavramı incelenirken bu kavramın hangi unsurları barındırdığı belirlendikten sonra, "elektronik ödeme sistemlerinde siber güvenlik"ten kastedilen anlamın ne olduğu yine bilimsel açıdan farklı yazarların görüşleri çerçevesinde ele alınarak ayrıca bu çalışma açısından hangi yaklaşımın benimsendiği de aşağıda belirtilmiştir.

1.1.1. Bilgi Güvenliği Kavramının Tanımı

Siber güvenlik kavramı çoğu kez bilgi güvenliği kavramı ile ilintili olarak kullanılsa da[10], aslında bilgi güvenliğinden farklı bir kavramdır[11]. Bilgi güvenliği, bilgi sistemlerinde muhteviyatı itibariyle yetki sahibi olmayan kişilerin söz konusu bilgiye erişimine, incelenmesine, kullanılmasına, ortaya çıkarılmasına, değişik yapılmasına, zarar verilmesine veya yok edilmesine karşı korunması ve bu hususta gerekli her türlü önlemin alınmasıdır[12].

1.1.2. Bilgi Güvenliğinin Unsurları

Bilgi güvenliğinin üç temel unsuru gizlilik, bütünlük ve kullanılabilirlik (elverişlilik) olup ve her üç temel unsurun da gerek siber uzayın güvenli olması açısından[13], gerekse

---

[10] Mehmet Eren, "Avrupa Birliği'nin Siber Güvenlik Politikası", Beta, İstanbul, 2017, (*"Eren"*) s. 22.

[11] Aşağıda detaylı şekilde açıklanacağı üzere, siber güvenlik çoğu kez "bilgi güvenliği" kavramı ile karıştırılsa da, siber güvenlik aslında tüm bilişim sistemlerini kapsayan genel bir güvenlik kavramıdır. Bu bağlamda, bilgi güvenliğinden daha geniş kapsamlı olup aslında "siber" kelimesinin literatürde "internet" kelimesine karşılık geldiği belirtildiğinden "siber güvenlik", internete dair akla gelebilecek tüm hususlarda "güvenli" olmaya karşılık gelmektedir. Bu konuda detaylı bilgi için bkz. Mustafa Altınkaynak, "Uygumalı Siber Güvenlik Ve Hacking", Abaküs, 5. Baskı, 2018, (*"Altınkaynak"*), s. 1.

[12] Bilgi güvenliğinin tanımı ve unsurları konusunda ayrıntılı bilgi için Bkz. Turan Okul/Güntekin Şimşek/Büşra Hafçı/Zafer Barış, "Konaklama İşletmesi Yöneticilerinde Bilgi Güvenliği Farkındalığı: Kuşadası'ndaki Beş Yıldızlı Oteller Örneği" isimli makalesi, (*"Okul ve Diğerleri"*) s. 190-191, Erişim adresi: https://dergipark.org.tr/tr/download/article-file/604273, (Gözden Geçirme tarihi: 29.10.2020)

[13] *Eren*, s. 23.

de bilgi güvenliğinden söz edilebilmek açısından olmazsa olmaz unsurlar olduğu kabul edilmektedir[14]. Söz konusu unsurları tek tek incelemek gerekirse:

Şekil-1.1: Bilgi Güvenliğinin Unsurları[15]

Gizlilik *(Confidentiality)*: Bilgiye erişme yetkisi olmayanların erişmesinin engellenmesi, başka bir deyişle elektronik ortamda sadece bilgi erişme yetkisi olan kişilerin bilgiye erişmesini ifade eder. Elektronik ödeme sistemlerinde gizlilik noktasında ise, ödeme sisteminin türüne göre kimlik teşhisi açısından birçok farklı yöntem akla gelse de (PIN, parola, elektronik imza, kullanıcının parmak izi, yüzü, göz retinası, DNA'si gibi kişisel özelliklerine göre) bu noktada ödeme işleminin ağırlık noktasının veri transferi olması sebebiyle asimetrik ve simetrik şifrelemenin karması

[14] Bilgi güvenliğinin üç ana şartı olan gizlilik, bütünlük ve kullanılabilirlik konusunda ayrıntılı bilgi ve konunun özellikle ISO/IEC 27001: 2005 boyutu itibariyle ayrıntılı bilgi için Bkz. *Yılmaz*, s. 52.
[15] https://steemit.com/staj/@coinwhales/bilgi-guevenligi-nedir-ve-bir-kurum-icin-neden-hayati-oenem-tasir-staj-arastirma-konulari-1 (Gözden Geçirme tarihi: 29.10.2020)

olan hibrit şifreleme yöntemlerinin[16] tercih edilmesi, gizliliğin sağlanması açısından daha etkin bir yöntem olarak görülmektedir[17].

Bütünlük *(Integrity)*: Bilginin bütünlüğü, bilginin kısmen veya tamamen bozulmadan, tahrip olmadan veya orijinal halinden farklılaştırılmadan özgün yapısının korunması anlamına gelmektedir. Elektronik ödeme sistemlerinde ise bütünlük, (i) ödeme sistemlerinde sadece yetkili olan kullanıcıların sisteme girebilmesi ve münhasıran ödemenin gerçekleştirilmesi için gerekli olan haklara sahip olması ile (ii) ödeme

[16] Elektronik ödemelerde de geçerli olmak üzere şifreleme işlemleri ile gerçekleştirilen deneysel çalışmalarda simetrik ve asimetrik şifrelemelerin bir karması olan "hibrit şifreleme" modellerinin, mesajların şifrelenmesi (*encyrption*) ve şifrelemenin çözülmesi (*decyrption*) açısından daha hızlı sonuç vermesi, her iki yapının kullanılması neticesinde hızlı ve güvenilirlik bir arada sağlanabileceğinden verimliliğin artması nedeniyle daha etkin bir yöntem olduğu belirtilmiştir. Kısaca, asimetrik şifreleme yönteminde açık anahtarlı algoritmalar kullanılmakta olup anahtarlar çift olarak üretilir ve bu anahtar çiftinde, şifreleme anahtarı açık anahtar veya genel anahtar (*public key*) ve şifre çözme anahtarı ise gizli anahtar veya özel anahtar (*private key*) olarak adlandırılır. Bu şifreleme tekniğinde bilgiler genel anahtarla şifrelenip özel anahtar ile çözülebileceği gibi özel anahtarla şifrelenip genel anahtarla da çözülebilir. Simetrik algoritmalarda ise, şifrelemede kullanılan algoritmalar özel, tek veya gizli anahtarlı geleneksel algoritmalar olup çoğunda şifreleme anahtarı ile şifre çözme anahtarı aynıdır. Hibrit şifrelemenin avantajı noktasında ise, uzmanlar, simetrik algoritmaların hızlı olması, asimetrik algoritmaların ise güvenilir ancak yavaş olması sebebiyle karma bir yaklaşım olan hibrit şifrelemenin uygulamada daha tercih edilebilir olduğunu ifade etmektedir. Bu yaklaşımın temel mantığı, bilginin simetrik bir algoritma ile şifrelenmesine, kullanılan anahtarın ise asimetrik bir algoritma ile şifrelenip gönderilecek bilgi ile iletilmesine dayanır. Bu sayede, bilginin şifrelenmesi, simetrik algoritmadan dolayı hızlı olacak ve aynı zamanda anahtarın iletimi ise, asimetrik algoritmadan dolayı ise güvenilir olacaktır. Bkz. *Sağıroğlu/Alkan*, 52-56, *Özkaya/Sarıca/Durmaz*, 322-329 ve benzer yönde görüş için bkz. Leyla Keser Berber "İnternet Üzerinden Yapılan İşlemlerde Elektronik Para Ve Dijital İmza", Yetkin Yayınları, Ankara 2002, (*"Keser Berber, Elektronik Para"*), s. 147 ve ayrıca bkz. Misbha Irum, Aihab Khan, Malik Sikander, Hayat Khiyal, "Confidentiality of Messages in a Cardless Electronic Payment Systems", International Journal of Reviews in Computing, 2011, (*"Irum Ve Diğerleri"*) ilgili makale ulaşmak için web sitesi: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/ijric629-32.pdf (Gözden Geçirilme Tarihi: 29.10.2020)

[17] Doktrinde Keser Berber'e göre, gizlilik ödeme işleminin yerine getirilmesinde en zor unsur olan "güvenilirlik" (reliability) unsurunun bir alt başlığı olup (güvenilirlik kriterleri olarak kullanıcıyı tanıma, yapılan işleme onay verilmesi, bilgilerin üçüncü kişilerin müdahalesine karşı korunması, gizlilik ve güvenlik belirtilmiştir) güvenilirlik açısından atılacak ilk adımın ödeme işlemlerinde dijital imza kullanılması olduğu ve ayrıca bir elektronik ödeme işleminin güvenilirliğinden bahsedebilmek için özellikle, transfer edilen meblağın miktarını korumak için, nakit akışının güvenilirliğinin sağlanması ve ödeme işleminin anonimliğinin ve üçüncü kişiler tarafından görülmemesinin sağlanması gerektiğini belirtmiştir. Bu konuda detaylı bilgi için Bkz. *Keser Berber*, *Elektronik Para,* s. 37, 38.

sisteminde gönderici tarafından alıcıya iletilen verilerin içeriğinde herhangi bir değişiklik olmaksızın alıcıya ulaşmasını ifade eder[18].

Kullanılabilirlik *(Avaliability)*: Kullanılabilirlik ilkesi ise, bilgiye ulaşılmak istenildiği anda bilgiye ulaşmak isteyen yetki sahibi kişinin söz konusu bilgiyi herhangi bir engel olmaksızın ulaşabilmesi ve kullanabilmesi anlamına gelmektedir. Ödeme sistemleri açısından konuya bakıldığında, kullanılabilirlik veya diğer bir adı ile elverişlilik ilkesi ödeme sisteminin teknik açıdan sağlam olması, özellikle ödeme vasıtalarının kusura dayanmayan kaybı, tahrip olması durumunda yeniden devreye sokulması olanağı kapsamında değerlendirilmektedir[19].

1.1.3. Siber Güvenliğin Tanımı ve Kavramsal Çerçevesi

Çalışmanın ana temasını oluşturan siber güvenlik kavramı üzerinde literatürde kavramsal bir uzlaşıya varılamadığı ve tek bir tanımının bulunmadığı görülmüştür[20]. Bunun nedenlerinden birisi, hiç kuşkusuz bilişim teknolojisinde yaşanan hızlı devinim sonucunda siber saldırıların boyutunun ve sayısının her geçen gün değişmesi ve özellikle hayatımıza yeni giren teknolojilerle beraber yeni siber saldırı yöntemlerinin de saldırganlar tarafından keşfedilmesidir. Öte yandan, siber güvenliğin multidisipliner ve dinamik yapısı gereği bilgisayar bilimi, kriptografi (şifre bilimi) ve hukuk gibi birçok farklı disiplini de ilgilendirmesi ve her bilim dalının siber güvenlik kavramını farklı açıdan ele alması, bu konuda yeknesak bir tanıma ulaşılmasını zorlaştırmaktadır.[21]

---

[18] *Keser Berber*, *Elektronik Para,* s. 38-39.
[19] *Keser Berber*, *Elektronik Para,* s. 39.
[20] *Eren*, s. 22.
[21] Dan Craigen/Nadia Diakun-Thibault/Randy Purse, "Defining Cybersecurity", Technology Innovation Management Review, Ekim, 2014, (*"Craigen/Thibault/Purse"*) s. 13, ilgili makale için Bkz. https://timreview.ca/sites/default/files/article_PDF/Craigen_et_al_TIMReview_October2014.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

Literatüre bakıldığında, siber güvenliğin tanımı ile ilgili farklı yaklaşımlar şu şekilde özetlenebilir:

ABD'nin siber güvenlik standartlarının belirlenmesi konusunda etkin bir kuruluş olan NIST'e göre[22], siber güvenliğin siber uzayın siber atak faaliyetlerine karşı kendini koruma ve savunma kabiliyeti olduğu ifade edilmiştir. NIST'ın tanımına benzer şekilde Craigen/Thibault/Purse, siber güvenlik kavramı açısından kavramın merkezine siber uzayı koyarak siber güvenliği, siber uzaydaki kaynakların, süreçlerin ve yapıların korunması ile hukuki hakların (*de jure*) fiiliyattaki (*de facto*) izdüşümü açısından, siber uzay tabanlı sistemlerde meydana gelebilecek her türlü uyumsuzluk konusunda ilgili organizasyonun bu süreçte kendisini koruma kabiliyeti olarak tanımlamıştır[23]. Türkiye'de bu konuda literatüre bakıldığında, Taner, siber güvenliği, ağa bağlı sistemlerin ve verilerin yetkisiz kişilerin erişip zarar vermesini veya ele geçirmesini önlemeye yönelik çalışmaların bütünü olarak nitelendirmiştir[24]. Eren, bu kavramı kurum, kuruluş ve kullanıcıların varlıklarına ait özelliklerini siber uzayda bulunan güvenlik tehditlerine karşı korumak amacıyla kullanılan araçlar, güvenlik teminatları, politikalar, kılavuzlar, risk yönetim yaklaşımları, eğitim ve teknolojiler ile bu kapsamdaki faaliyetlerin bütünü şeklinde ele almaktadır[25]. Sağıroğlu/Alkan'ın "Siber Güvenlik Ve Savunma Farkındalık Ve Caydırıcılık" adlı eserinde ise, bu kavramın "siber ortamlarda karşılaşılabilecek tehdit ve tehlikeler ile oluşabilecek riskleri öngörüp bunlara karşı önceden önlem alma girişimi, siber varlıkların tehdit ve tehlikelerden korunması için doğru teknolojiler, yöntemler, çözümler, önlemler, politikalar, standartlar, testler gibi girişimlerin doğru amaç, hedef veya şekilde

[22] NIST tarafından yayınlanan "Bilgi Güvenliği İle İlgili Anahtar Kavramlarla İlgili Rehber"de (NIST IR 7298 Revision 2, Glossary of Key Information Security Terms) orijinal metinde siber güvenlik kavramı, "The ability to protect or defend the use of cyberspace from cyber attacks" olarak tanımlanmıştır. Bu konuda detaylı bilgi için bkz. https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf (Gözden Geçirilme Tarihi: 29.10.2020).
[23] *Craigen/Thibault/Purse*, s. 13.
[24] Cemal Taner, "Herkes İçin Siber Güvenlik", Abaküs, 1. Baskı, İstanbul, 2019, ("*Taner")*, s. 23.
[25] Mehmet Eren, "Avrupa Birliği'nin Siber Güvenlik Politikası", Beta, İstanbul, 2017, ("*Eren")*, s. 24-25.

kullanılarak siber varlıkların veya sistemlerin istenilmeyen kişiler/sistemler tarafından elde edilmesini önleme girişimi veya siber ortamlarda oluşacak riskleri minimize etmek ve yönetmek" olarak olduğu ifade edilmiştir[26]. Erdem/Özocak, siber güvenliği siber ortamda kişi, kurum ve kuruluşların varlığını korumak amacıyla geliştirilen plan, program ve uygulamalar bütünlüğü olarak tanımlamıştır[27]. Özkaya/Sarıca/Durmaz tarafından siber güvenlik bilgi güvenliğinden farklı olarak bireylerin, kurumların ve hükümetlerin bilgi işlem hedeflerine güvenli ve bütünlük içerisinde ulaşmalarına olanak veren ortak etkinlikler kaynaklar ve standartlar olup kişisel veya kurumsal bilgi veya bilgi kaynaklarının yetkisiz erişim, saldırı, hırsızlık veya veriye zarar verme gibi çeşitlilik gösteren birçok siber saldırıya karşı korunması şeklinde tanımlanmaktadır[28].

Çalışmada, literatüre yönelik yukarıda yer verilen görüşlerden hareketle siber güvenlikle ilgili en geniş kapsamlı yapılacak tanımın şu olduğu sonucuna varılmıştır: Siber güvenlik, siber uzayda[29] bireylerin, kurumların ve devletlerin bilişim sistemleri vasıtasıyla her türlü riske, saldırıya ve ilgili paydaşların menfaatlerine zarar verebilecek nitelikte olan ve/veya risk teşkil edebilecek duruma karşı korunma ve güvenliği sağlama kabiliyetidir.

1.1.4. Elektronik Ödeme Sistemlerinde Siber Güvenliğin Kavramsal Çerçevesi

Dünyada ve Türkiye'de başta bankacılık sektörü olmak üzere birçok işlemin günümüzde internet üzerinden gerçekleştirildiği ve elektronik ortamda gerçekleştirilen bu işlemlerin gerek maliyet açısından fayda sağladığı gerekse hız açısından etkin bir

[26] Şeref Sağıroğlu/Mustafa Alkan, "Siber Güvenlik Ve Savunma Farkındalık Ve Caydırıcılık", BGD Siber Güvenlik ve Savunma Kitap Serisi 1, Ankara, 2018, (*"Sağıroğlu/Alkan"*), s. 26.
[27] Merve Erdem/Gürkan Özocak, "Siber Güvenliğin Sağlanmasında Uluslararası Hukukun Ve Türk Hukukunun Rolü, Ankara Üni. Hukuk Fak. Dergisi, 68 (1) 2019, (*"Erdem/Özocak1"*), s. 167, ilgili makaleye internet ortamında ulaşmak için: https://dergipark.org.tr/tr/download/article-file/695490 (Gözden Geçirilme Tarihi: 29.10.2020).
[28] Erdal Özkaya/Raif Sarıca/Şükrü Durmaz, "Siber Güvenlik Saldırı Ve Savunma Stratejileri", Buzdağı Yayınevi, Ankara, 2019, *("Özkaya/Sarıca/Durmaz")*, s. 34.
[29] Sanal bir bilgisayar dünyası olarak düşünülebilen siber uzay, günlük hayatı devam ettirecek hizmetleri sunabilen global bir bilgisayar ağını oluşturabilmek amacı ile kurulan elektronik bir ortamdır. Siber uzay konusunda ayrıntılı bilgi için bkz. *Sağıroğlu/Alkan*, s. 87 vd.

hizmet olarak görüldüğü bilinen bir gerçektir. Özellikle 2020 yılı Mart ayından itibaren etkisini yoğun şekilde gösteren Covid-19 pandemi salgını ile beraber kişilerin adeta eve kapanması neticesinde çalışmamızı da ilgilendiren elektronik ödeme endüstrisinin imkânlarından yararlanılmasını adeta bir zorunluluk haline gelmiştir.

Literatürde Yeşilyurt, elektronik ödeme işlemlerinin, elektronik şekilde başlatılan, süreçlendirilen ve elektronik olarak alınan ödemeler olduğunu ve elektronik ödemeler kapsamında değerlendirilebilecek, elektronik ticaret işlemlerinin[30] şirketler ve tüketiciler arasında (B2C)[31] ya da elektronik ödemelerin doğrudan şirketler arasında (B2B)[32] gerçekleştirildiğine dikkat çekmiştir[33]. Öney/Öksüzoğlu/Rizvi ise elektronik

[30] Elektronik ticaret işleminden kastedilen, mal ve hizmet satışının ve bu konuda siparişlerin alınmasının bilgisayar ağları ile yürütülerek gerçekleştirilmesidir. Mal ve hizmet siparişinin elektronik ortamda gerçekleştirilmesi halinde, bir işlemin elektronik ticaret işlemi addedilebilmesi için mal ve hizmet ödemesinin ve son dağıtımının online olarak yürütülmesi zorunluluğu bulunmamaktadır. Bu noktada önemli olan, bir işlemin elektronik ticaret işlemi olarak değerlendirilmesi için ilk siparişin online ortamda verilmesi gerekmektedir. Bir e-ticaret işleminin ise, işletmeler, hane halkları, bireyler, hükümetler veya farklı kamu ve özel kurum ve kuruluşlar arasında gerçekleştirilebileceği kabul edilmektedir. Bu konuda daha detaylı bilgi için Bkz. Burcu Zengin, Aybegüm Güngördü, "Elektronik Ödeme Sistemlerinin Olası Etkileri Üzerine Bir İnceleme", Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 15/3 (2013) 129-150, s. 131, (*"Zengin/Güngördü"*) makaleye ulaşmak için: http://dergipark.org.tr/en/download/article-file/287247 (Gözden Geçirilme Tarihi: 29.10.2020)

[31] "B2C" kavramı, İngilizce'de "Business to Consumer" sözcüklerinin kısaltması olarak Türkçe'de "İşletmeciden Tüketiciye" şeklinde tercüme edilebilir (Serbest Çeviri). Bu kavram günümüzde şirketlerin, doğrudan tüketicilerle doğrudan kurduğu her türlü ticari ilişkiyi açıklamak üzere kullanılmakta olup B2C iş modelinin iki çeşit uygulaması söz konusudur: (i) E-ticaret uygulamalarının her geçen gün etki alanı genişlediğinden, sanal mağazalar tarafından VPOS denilen sanal POS aracılığıyla Türkiye'de iyzico gibi şirketler tarafından B2C kanalıyla internet ortamında alışveriş için tercih edilmektedir. VPOS ile ilgili ayrıntılı bilgiye çalışmanın 1.2.1.1. numaralı başlığı altında "Kredi Kartı" ile ilgili açıklamalar kapsamında yer verilecektir. (ii) İkinci uygulama olarak ise, üretici şirket fabrika çıkış fiyatları üzerinden arada herhangi bir alışveriş mağazası olmaksızın B2C iş modeli ile ürünlerini tüketicilere satmaktadır. Bu konuda detaylı bilgi için bkz. https://www.iyzico.com/blog/b2b-b2c-ve-c2c-nedir-arasindaki-farklar-nelerdir/ (Gözden Geçirilme Tarihi: 29.10.2020).

[32] İngilizce karşılığı "Business To Business" olan ve Türkçe'de "Şirketten Şirkete" olarak kullanılan bu kavram, şirketler arası ticaret, pazarlama ve satış çalışmalarına verilen kısa ad olup bir şirketin ürün ve hizmetlerinin başka bir firmaya pazarlanması anlamına gelir. Elektronik ödeme endüstrisi açısından B2B ise, doğrudan şirketler arasında gerçekleştirilen elektronik ödeme işlemleri için kullanılmaktadır. Bkz. https://www.paradurumu.com/girisimcilik/b2b-b2c-ve-c2c-nedir-haberi-3935 (Gözden Geçirilme Tarihi: 29.10.2020).

[33] Hamdi Yeşilyurt, "Finansal Hizmet Sektöründe Siber Güvenlik Riskleri Ve Çözüm Yolları: Ödeme Sistemleri Ve Tedarik Zinciri Bütünlüğü, (*"Yeşilyurt"*) s. 99, ilgili esere aşağıdaki web sitesinden ulaşılabilir:
https://www.academia.edu/22347134/Finansal_Hizmet_Sektöründe_Siber_Güvenlik_Riskleri_ve_Çöz

ödeme işlemlerini, bireyler ve kurumlar arasında elektronik ticari işlemlerin güvenli şekilde gerçekleştirilmesine olanak tanıyan her tür ödeme sistemi olarak tanımlanmaktadır[34].

Doktrinde Yeşilyurt, siber güvenlik açısından en önemli korunması gereken bileşenlerin internet dünyasında oldukça açık bir şekilde hizmet veren elektronik finans sektörü olduğunu belirtmiştir. Bu nedenle anılan yazar e-ödemelerde bilişim altyapısı güvenliğinin finans sektörü açısından dünya çapında önemli bir problem olduğuna dikkat çekerek elektronik ödeme sistemlerinde siber güvenlik sorununu kartlı ve kartsız online bankacılık, e-ticaret ve tedarik zincirlerinin siber güvenlik riskleri çerçevesinde ele almıştır[35]. Urs, elektronik ödemelerde teknolojinin gelişmesi ile birlikte her geçen gün yeni bir e-ödeme sistemi ile karşı karşıya kalmanın gündemde olduğuna dikkat çekmekle beraber elektronik ödeme sistemlerinde siber güvenlik sorununu (i) akıllı kartlara dayanan e-ödemeler, (ii) mobil cihazlar üzerinden gerçekleştirilen ödemeler, (iii) e-cüzdan ödeme sistemleri ve (iv) elektronik çek ödeme sistemi ekseninde incelemiştir[36]. Camenish/Piveteua/Stadler ise, elektronik ödeme sistemlerinde temelde banka, müşteri ve alışveriş mağazası olmak üzere üç temel süje açısından farklı işlemlerin eş zamanlı veya farklı zamanlarda işlem gerçekleştirilebildiğini ve elektronik ödeme işlemlerinde güveliğin fiziken alınan önlemler ile kriptpgrafik yöntemlerin bir karışımı olduğunu belirtmiştir[37].

üm_Yolları_Ödeme_Sistemleri_ve_Tedarik_Zinciri_Bütünlüğü (Gözden Geçirilme Tarihi: 29.10.2020).

[34] Bu tanım için bkz. Emrah Öney/Gizem Öksüzoğlu Güven/Wajid Hussain Rizvi, "The determinations of electronic payment systems usage from consumers' perspective, Routledge Economic Research, s. 395, (*"Öney/Güven/Rizvi"*) söz konusu makalenin tam metnine aşağıdaki linkten ulaşılabilir: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/Thedeterminantsofelectronicpaymentsystemsusagefromconsumersperspective.pdf (Gözden Geçirilme Tarihi: 29.10.2020)

[35] *Yeşilyurt*, s. 99-100.

[36] Bogdan-Alexandru Urs, "Security Issues And Solutions In A E-Payment Systems", Fiat Iustatia, No:1, 2015, (*"Urs"*), s. 173, ilgili makaleye ulaşmak için bkz. http://oaji.net/articles/2016/2064-1452602042.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[37] Jan Camenish/Jean-Marc Piveteau, "Security in Electronic Payment Systems", (*"Camenish/Piveteaue"*), bahsi geçen makaleye aşağıdaki link üzerinden ulaşılabilir: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/Security_in_Electronic_Payment_Systems.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

Çalışmada, "elektronik ödeme sistemlerinde siber güvenlik" konsepti açısından literatürde yukarıda yer verilen hiçbir tanım ve değerlendirme tek başına tercih edilmemiştir. Bu bağlamda, elektronik ödeme sistemlerinde siber güvenlik kavramının çalışmada kartlı ödeme sistemleri, internet bankacılığı, mobil bankacılık ve internet ortamında teknolojinin gelişmesi ile beraber gelişmekte olan her türlü elektronik ödeme işlemine yönelik buna bağlı olarak yine teknolojinin etkisi ile evrilmekte olan her türlü siber saldırı tekniğine, tehdide, riske, zafiyete ve olumsuz duruma karşı herhangi bir kişiye, kuruma ve şirkete ait bilişim teknolojisi sisteminin korunma, direnç gösterme ve bu durumu bertaraf etme yetisi olarak tanımlanması uygun görülmüştür.

1.2. ELEKTRONİK ÖDEME TÜRLERİ AÇISINDAN SİBER GÜVENLİK

Elektronik ödeme sistemleri açısından siber güvenlik denildiğinde, elektronik ödeme sistemleri yukarıda da belirtildiği gibi üç ana başlık altında aşağıda detaylı birtakım teknik analizlere yer verilmiştir: (i) Kartlı Ödeme Sistemleri, (ii) Kartsız Ödeme Sistemleri, (iii) Diğer Ödeme Sistemleri.

Konunun ödeme sistemleri açısından üç ana başlığa ayrılmasının sebebi ise, elektronik ödeme sistemleri siber güvenlik perspektifi ile incelendiğinde, teknik açıdan konunun kartlı ve kartsız olmak üzere öncelikle ikiye ayrılarak açıklanması daha uygun görülmüştür. Üçüncü Bölüm'de daha detaylı şekilde dikkat çekildiği üzere, genelde kartlı ödeme sistemlerine yöneltilen siber saldırılar nitelik olarak birbirine benzerlik göstermekle beraber kartsız ödeme sistemlerinde ise, elektronik ödeme sisteminin teknolojik özelliğine ve bu saldırıyı gerçekleştiren siber saldırganın teknik bilgisi ve yaratıcılığına bağlı olarak siber saldırılar farklılık arz edebilmektedir. Ancak, yaklaşım açısından kartsız ödeme sistemlerinde gerçekleştirilen siber saldırılar açısından çalışmada her elektronik ödeme sistemine yönelik siber saldırı konusunda detaylı bir teknik analize yer verilmesi gayesinden ziyade özellikle kullanım açısından revaçta olan EFT, SWIFT gibi elektronik ödeme sistemlerine yönelik ayrıntılı analiz yapılması hedeflenmiştir. Son olarak, bu başlık altında "Diğer Elektronik Ödeme Yöntemleri" başlığı altında siber güvenlik değerlendirmelerine yer verilmesinin gerekçesi ise, e-

posta aracılığıyla online para gönderme, mobil ödeme sistemleri ve mobil bankacılık, internet bankacılığı, elektronik para ve elektronik çek gibi elektronik ödemelerde her geçen gün yeni bir teknolojik gelişmenin yaşanması ve buna bağlı olarak, gerçekleştirilen siber atakların niteliğinin hızlı değişimidir.

1.2.1. Kartlı Ödeme Sistemleri

Kartlı ödeme sistemleri, aşağıda kredi kartı, debit kart ve akıllı kartlar kapsamında değerlendirilmiştir.

1.2.1.1. Kredi Kartı

Kredi kartı ile yapılan bir alışverişte karta ilişkin bilgiler (kart numarası, son kullanma tarihi, kart sahibinin adı, CVV[38] numarasının) ilgili web sitesindeki ilgili alanlara girilmektedir. Bu bilgilerin online olarak sisteme girilmesi akabinde, web sitesi anlaşmalı finans kurumunun sistemi üzerinden bir sanal POS[39] erişimi yaparak bu kart bilgileri ile ilgili alışveriş tutarı için provizyon almakta ve son olarak bilgisayar karşısındaki müşteriye, sisteme girilen bilgilerin doğruluğu ve yanlışlığına bağlı olarak olumlu veya olumsuz sonucu göstererek işlemi tamamlamaktadır. Bu noktada, bahsi geçen işlem akışından da anlaşılacağı üzere, ilk aşamada müşteriye ait kart bilgilerinin

[38] İngilizce orijinal adıyla "card verification value", Türkçe'ye "kart doğrulama değeri" olarak tercüme edilebilir (Serbest Çeviri). Bu değer, kredi kartının arkasında kart sahibine o kartın hamili olduğu belirtmek amacıyla her kart kullanıcısına özgü verilen numaradır. (American Express Card'da CVV dört haneli bir numaradır. CVV numarası, kredi kartı dolandırıcılıklarını azaltmak amacıyla müşteriye o kartın hamili olduğunu ortaya koymak amacıyla tasarlanmış olup kredi kartı üzerindeki en hassas bilgi olarak bilinmektedir. Bkz. https://itlaw.wikia.org/wiki/Card_Verification_Value (Gözden Geçirilme Tarihi: 29.10.2020)

[39] Sanal POS, POS (point of sale, Türkçe adıyla satış noktası) sisteminin elektronik ticaret sitelerinde yapılan alışverişlerin gerçekleşmesinde kullanılmasıdır. VPOS (Virtual POS) olarak da isimlendirilen bu sistem kredi kartı vasıtasıyla internet üzerinden alışveriş yapma imkânı sağlar. Sanal POS, basitçe ifade etmek gerekirse şu şekilde çalışır: İnternet sitesi üzerinden alışveriş yapmak isteyen müşterinin kredi kartı bilgilerinin ilgili sitedeki ödeme ekranlarına girmesi sonucunda, bu bilgiler ilgili bankaya ulaşır ve işlemin provizyonu alınır. Provizyonu alınmış işlemlerin tutarı ilgili müşterinin kredi kartı limitinden düşülerek müşterinin çalıştığı banka hesabına geçirilir. Bu açıklamalardan da anlaşılacağı üzere, sanal POS fiziki bir POS olmayıp web üzerinden çalışan bir POS'tur. Konu ile ilgili ayrıntılı bilgi için: https://www.kuveytturk.com.tr/kobi/kartlar-ve-pos/pos-hizmetleri/sanal-pos (Gözden Geçirilme Tarihi: 29.10.2020)

kötüniyetli üçüncü şahısların eline geçmesi ile dolandırıcılık gerçekleştirilmesi mümkündür[40].

Kredi kartlarının siber güvenlik boyutu itibariyle incelenmesi noktasında, kredi kartlarının şifrelenmesi açısından SET ve SSL olarak adlandırılan iki protokol söz konusudur[41]:

SET (Secure Electronic Transactions)

Şekil-1.2: SET Protokolü[42]

[40] Keser Berber, kredi kartlarıyla yapılan ödemelerde ödemenin gerçekleştirilmesi için sadece uygun bir yazılımın yeterli olduğunu, ancak bu yazılımda kredi kartına ait verilerin güvenli bir şekilde internette karşı tarafa iletilmesi bakımından ek güvenlik tedbirlerinin mevcut olması gerektiğini ifade etmektedir. Keser Berber, ayrıca kredi kartı bilgilerinin gönderilmesi sırasında başkaları tarafından görülmesi ve elde edilmesi tehlikesi bulunduğunu, bu konuda anonimliğin sağlanmasını hedefleyen birçok yöntem ve protokol olduğunu, ancak gerçekte anonimliğin sayıca çok az sistemde sağlandığını belirtmiştir. Bu konuda ayrıntılı bilgi için Bkz. *Keser Berber, Elektronik Para,* s. 55.

[41] Armağan Ebru Bozkurt Yüksel, "Elektronik Para, Sanal Para, Bitcoin Ve Linden Doları'na Hukuki Bir Bakış, Aristo Yayınevi, İstanbul, 2018, (*"Bozkurt Yüksel, Elektronik Para"*), s. 16 ve *Keser Berber*, *Elektronik Para,* s. 55-56.

[42] https://www.slideshare.net/ArmaganBOZKURT1/elektronik-para-sanal-para-bitcoin-rnei-74079438 (Gözden Geçirilme Tarihi: 29.10.2020)

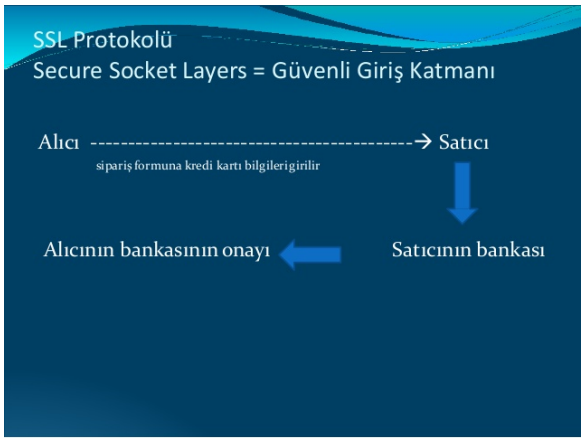
SET standardının çalışma mantığından kısaca bahsetmek gerekirse, başta müşterinin internet üzerinde satın almak istediği hizmet veya ürünü belirledikten sonra bir sipariş formu doldurması akabinde kredi kartı ile alışveriş yapabilmesi amacıyla kart bilgilerini ve ödeme için gerekli olan bilgileri sisteme girecektir. Müşteri tarafından doldurulan sipariş formu internet aracılığıyla satıcının bilgisayarına iletilecektir. Eş zamanlı olarak sipariş ve ödeme bilgileri birbirinden tamamen ayrı olarak şifrelenir ve şifrelenen bu işlemlerin onaylanması ise dijital imza ile gerçekleştirilecektir. Bu esnada satıcının sistemi, şifrelenmiş ödeme bilgilerine, satıcı ve ilgili ödeme işlemini tespit etmeye yarayacak olan söz konusu dijital imzayı ekleyecktir. Bu bilgiler ise tamamen ilgili bankanın iletişim protokolü olan SET sunucusuna iletilecektir. Bankanın sunucusu şifrelenen bilgileri deşifre ederek alıcının kredi kartı şirketinden çevrimiçi (online) şekilde bir teyit isteyecektir. Kredi kartı şirketinin ise bu işlemi teyit etmesi halinde alıcının kredi kartı otomatik borçlandırılır. SET sunucusu ile, son olarak satıcının sistemine bir mesaj göndermek suretiyle ödemenin gerçekleştiği veya gerçekleşmediği durumları bildirmek amacıyla mesaj gönderecektir[43].

Keser Berber, SET'in özel bir ödeme sistemi olmadığını, daha ziyade kredi kartı işlemleri için bir şifreleme standardı olduğunu belirtmiştir[44].

Günümüzde SET'in yerini 3D Secure denilen sistem almıştır. 3D sisteminin debit kartlar ve kredi kartları açısından ödeme sırasında anlık olarak bankanın kart sahibinden şifresini talep ederek müşterisini güvence altına aldığı ve özellikle şifreyi bilmeyen yetkisiz kişilerin sisteme girişinin bu sayede engellediği bilinmektedir[45].

SSL (Secure Socket Layer)

[43] *Bozkurt Yüksel, Elektronik Para*, s. 18.
[44] *Keser Berber*, *Elektronik Para,* s. 55.
[45] *Bozkurt Yüksel, Elektronik Para*, s. 21, *Keser Berber*, *Elektronik Para,* s. 58 ve benzer yönde görüş için bkz. Özgür Eralp, "İnternet Bankacılığı Ve Kredi Kartı Dolandırıcılığının Teknik, Hukuki Ve Cezai Boyutu, Eralp Kitap, Ankara, 2012, ("*Eralp")*, s. 26.



Şekil-1.3: SSL Protokolü[46]

Yukarıda şematik olarak gösterilen SSL[47] ise, SET gibi kredi kartı işlemlerinde güvenliği sağlamak amacıyla Netscape şirketi tarafından geliştirilen bir iletişim protokolüdür[48]. SSL protokolünde bir gizli, bir de açık anahtar olmak üzere iki anahtar vasıtasıyla işlemler şifrelenmekte olup SSL protokolünde tarafların bilgisayarları vasıtasıyla birbirleri ile haberleşmeleri esnasında bir dizi kurallar öngörülmektedir. Bu sistemde, SET protokolünde olduğu gibi SSL'de de satıcı internet sayfasında almak istediği mal veya hizmete ilişkin bir sipariş formu doldurarak kredi kartı numarasını sisteme girdikten sonra satıcı, alıcının sisteme girdiği bilgileri kendi bankasına yönlendirmektedir. Bu aşamadan sonra bankalar devreye girerek satıcının bankası, alıcının bankasından işlem hakkında onay isteyecek, bu onayın verilmesi akabinde ise satıcının bankasını işlemin gerçekleştiğine ilişkin satıcının bankasını bu konuda bilgilendirecektir[49].

---

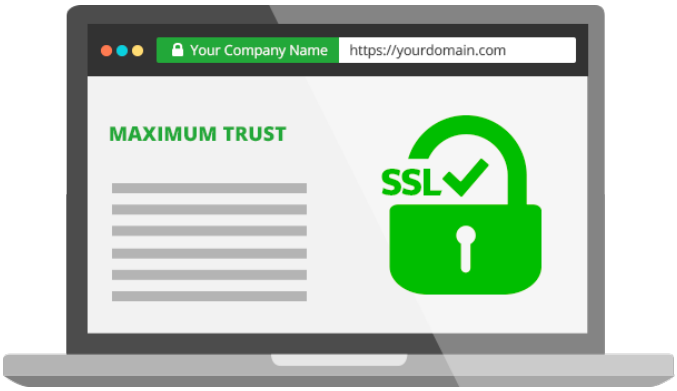
[46] https://www.slideshare.net/ArmaganBOZKURT1/elektronik-para-sanal-para-bitcoin-rnei-74079438 (Gözden Geçirilme Tarihi: 29.10.2020)

[47] İngilizce'de "Secure Socket Layers" ibaresi, yazar tarafından "Güvenli Giriş Katmanı" olarak Türçe'ye tercüme edilmiştir (Serbest Çeviri). SSL konusunda detaylı bilgi için bkz. *Çakır/Kılıç*, s. 104-105.

[48] *Bozkurt Yüksel, Elektronik Para*, s. 18.

[49] *Bozkurt Yüksel, Elektronik Para*, s. 19.

Teknik açıdan bakıldığında, kullanıcının web tarayıcısında aşağıdaki görselde[50] gösterildiği üzere yeşil renkli bir asma kilit gösterilmesi, işlemin SSL ile gerçekleştiğine işaret etmektedir[51].



Şekil-1.4: SSL Simgesi

Çalışmayı ilgilendirmesi açısından ayrıca bu başlık altında Geniş Kapsamlı SSL Sertifikası'ndan (*"EV SSL Sertifikası"*)[52] bahsedilmesi uygun görülmüştür. EV SSL Sertifikası, uygulamada tüzel kişilere[53] tanınan bir sertifika olup esas itibariyle bu sertifika ise (i) ilgili tüzelkişiye kullandığı internet tarayıcısı üzerinden tanımlanmış olan işyeri unvanı ve adresi gibi bilgiler neticesinde, ilgili tüzel kişinin kullandığı web sitesi üzerindeki internet trafiğinin ve kullanıcı ile web sitesi arasındaki iletişim ve bilgi akışının uçtan uca şifreli şekilde gerçekleştirilmesinin sağlanması ile (ii) oltalama,

[50] İlgili görsel internet ortamda şu link üzerinden aktarılmıştır: https://www.google.com/search?q=SSL&sxsrf=ALeKk02f8EM6M9h4gIz9w3c6vK-OQC0XVQ:1590997700863&source=lnms&tbm=isch&sa=X&ved=2ahUKEwipkbGmkODpAhXSGuwKHS91AQQQ_AUoAXoECBQQAw&biw=1451&bih=657#imgrc=T6r_VQ_Z-6VFgM (Gözden Geçirilme Tarihi: 29.10.2020).

[51] *Bozkurt Yüksel, Elektronik Para*, s. 19.

[52] İngilizce'de bu kavram "Extended Validation SSL Certificate" olarak belirtilmekte olup çalışmada Türkçe'ye "Geniş Kapsamlı SSL Sertifikası" olarak tercüme edilmiştir (Serbest Çeviri). Ancak, yabancı kaynaklarda ve bilişim literatüründe yaygın olarak "EV SSLCerfificate" kavramı kullanılması sebebiyle çalışma içeriğinde kısaltma olarak "EV Sertifikası" kullanılması tercih edilmiştir.

[53] Tüzel kişilerden kastedilen, EV SSL Sertifikasının, sadece özel kuruluşlar, kamu kuruluşları, ticari işletmeler ile ticari iştigal amacı olmayan işletmelere verilebilmesidir.

zararlı yazılım ve farklı nitelikteki kimlik dolandırıcılıkları gibi siber saldırılara karşı koruma sağlamaktadır[54].

Günümüzde, özellikle kartlı ödeme sistemlerinin her yıl kullanımının artmasının bir sonucu olarak, bu artış hızı dolandırıcıların özellikle iştahını kabartmış ve tüm bunların bir sonucu olarak kredi kartı dolandırıcıları, çoğunlukla kredi kartları üzerinde depolanmış olan verileri ele geçirmek amacıyla, işyerleri ve ATM cihazlarına çeşitli aparatlar yerleştirmek suretiyle kartlar üzerindeki bilgileri ele geçirmekte ve yasadışı yollardan edindikleri bilgilerden yararlanarak haksız kazanç elde etmektedir[55]. Öte yandan, son zamanlarda özellikle kredi kartları ile yapılan işlemler açısından en dikkat edilmesi gereken meselelerden bir diğeri ise phishing denilen oltalama saldırılarıyla bu konuda muhtelif banka ve finans kurumları tarafından gönderilmiş gibi gözüken acil ve çok önemli konular içeriyormuş gibi duran sahte elektronik postalardır. Bu elektronik postalarda verilen linkler aracılığı ile müşterilerden, kart bilgileri, kart şifreleri, internet şubesi şifrelerinin istenerek ve bu yolla insanların banka ve kredi kartları her geçen gün daha fazla suistimal edilmektedir[56].

Kredi kartları ile ilgili sanal kart uygulaması, günümüzde dünyada ve Türkiye'de farklı bankaların ve finansal kuruluşların kredi kartına yönelik bilgilerin kötüniyetli üçüncü kişiler tarafından ele geçirilmesinin önlenmesi amacıyla kredi kartına bağlı bir ürün olmakla beraber sadece internet üzerindeki alışverişlerde kullanılmak üzere ve sahte kullanımı önlemek amacıyla sanal kart numarasının fiziken kabartma olarak

[54] https://cabforum.org/about-ev-ssl/ (Gözden Geçirilme Tarihi: 29.10.2020).

[55] Hamdi Yeşilyurt, "Finansal Hizmet Sektöründe Siber Güvenlik Riskleri Ve Çözüm Yolları: Ödeme Sistemleri Ve Tedarik Zinciri Bütünlüğü, (*"Yeşilyurt"*) s. 104, ilgili esere aşağıdaki web sitesinden ulaşılabilir:
https://www.academia.edu/22347134/Finansal_Hizmet_Sektöründe_Siber_Güvenlik_Riskleri_ve_Çözüm_Yolları_Ödeme_Sistemleri_ve_Tedarik_Zinciri_Bütünlüğü (Gözden Geçirilme Tarihi: 29.10.2020) Bu konu tez içeriğinde ise 2.1. numaralı "Kartlı Ödeme Sistemlerine Yönelik Siber Saldırılar" başlığı altında ele alınmıştır.

[56] Feridun Kaya, "Türkiye'de Kredi Kart Uygulaması", Türkiye Bankalar Birliği, Yayın No: 263, İstanbul, 2009, ("*Feridun Kaya")*, s. 138. İlgili esere internet üzerinden ulaşmak için: https://www.tbb.org.tr/Dosyalar/Yayinlar/Dokumanlar/263.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

basılmadığı ve CVC numarasının görüntülenemediği sanal ortamdaki ödeme uygulamasını ifade etmektedir[57]. Sanal kartların çıkış noktası kullanıcılarına internet üzerinden güvenli olarak mal ve hizmet satın alabilmelerine olanak sağlamak olup sanal kartlar, ana karta bağlı olarak çalışır ve başlangıç limiti 0 TL'dir. Sanal kart limitini, kullanıcısı dilediği şekilde belirleyebilir ve sanal kart kullanıcısına yapacağı alışverişte istediği limit kadar harcama yapmasına ve daha sonraki süreçte ise kullanılabilir limitini sıfırlayarak sanal kartı kapatmasına olanak tanımaktadır[58]. Özellikle günümüzde kredi kartlarına yönelik yapılan kimlik hırsızlıklarının önlenmesinde sanal kart uygulaması güvenli bir yöntem olarak kabul edilmektedir[59].

1.2.1.2. Debit Kartlar ve ATM Cihazları

Debit kart, para taşıma riskini ortadan kaldıran ve hesapta bulunan para miktarı kadar harcama yapılmasını sağlayan bir üründür[60]. Başka bir deyişle, debit kartlar banka hesabında nakit bulunan veya kredili hesabı bulunan müşterilere bu karttan yararlanmak suretiyle mal ve hizmet alımı işlem yapmalarına imkân sağlamaktadır. Günümüzde özellikle "nakitsiz toplum projesi"[61] açısından önem arz eden debit kartlar,

---

[57] Bu konuda başlıca örnek olarak sanal kart limitinin 0 olduğu Garanti kart uygulaması ile CVC numarasının görüntülemediği sanal kart uygulaması olarak Pamukbank'ın tasarladığı sanal kart örnek olarak gösterebilir. Her iki sanal kart uygulaması ile ilgili ayrıntılı bilgi için Bkz. *Keser Berber*, *Elektronik Para,* s. 89 Ayrıca Garanti Bonus Sanal Kart konusunda güncel bilgi için Bkz. https://www.garantibbva.com.tr/tr/bireysel/kredi_kartlari/Sanal-Card.page (Gözden Geçirilme Tarihi: 29.10.2020)

[58] *Feridun Kaya*, s. 19

[59] Didem Topçuoğlu, "Nakitsiz Bir Toplum ve Türkiye Üzerine Bir Araştırma", T.C. İstanbul Üniversitesi, Para Sermaye Piyasaları Ve Finansal Kurumlar Ana Bilim Dalı, Yüksek Lisans Tezi, İstanbul, 2019, (*"Topçuoğlu"*) s. 18, ilgili teze ulaşmak için: http://nek.istanbul.edu.tr:4444/ekos/TEZ/ET001010.pdf (Gözden Geçirilme Tarihi: 29.10.2020)

[60] Timur Madenci, "Kredi Kartı ve Debit Kart Uygulamaları ve Karlılık Açısından Değerlendirme", T.C. Marmara Üniversitesi, Bankacılık Ve Sigortacılık Enstitüsü Bankacılık Ana Bilim Dalı, Yüksek Lisans Tezi, İstanbul, 1996, (*"Madenci"*) s. 34, Bkz. https://katalog.marmara.edu.tr/eyayin/tez/T0043416.pdf (Gözden Geçirilme Tarihi: 29.10.2020)

[61] Nikola Fabris, "Cashless Society – The Future of Money or a Utopia?" isimli makalesinde "nakitsiz toplum felsefesinin pozitif ve negatif yönleri konusunda şu değerlendirmelere yer vermektedir: Nakitsiz toplum anlayışının pozitif yönlerini özetlemek gerekirse, genel itibariyle malvarlığına doğrudan işlenen suçlar ve kara para aklama açısından yararlı olduğu, teknolojik gelişmelere uygun alternatif ödeme imkânları sunduğu, kayıt dışı ekonominin azaltılmasına olanak sağladığı, bilişim teknolojilerinde hızlı bir gelişme imkânı sağladığı ve özellikle akıllı telefonlar ve elektronik uygulamaların desteği ile

nakit para taşımanın azaltılması ve dolayısıyla para çalınmasının önüne geçilmesi açısından daha güvenli olduğu düşünülerek tercih edilmektedir.

Debit kartlar da, kredi kartlarına benzer şekilde siber saldırgınlar tarafından zararlı yazılım, oltalama saldırıları, kartın manyetik bilgilerinin kopyalamasını sağlayan "skimmer" denilen cihazlar, kart üzerinden ödeme işleminin gerçekleştirildiği esnada POS cihazlarına[62] ve ATM[63]'lere bazı aparatlar yerleştirmek suretiyle istismar edilebilmektedir.

1.2.1.3. Akıllı Kartlar

Değer yüklemeli kart (*store value card*) veya elektronik cüzdan (*electronic pursue*) denilen akıllı kartlar, kredi kartı ve debit kartlara benzer şekilde içine yerleştirilen çip sayesinde işlem yapılan (para yükleme, ödeme veya jeton harcama vb.) kartlardır[64].

elektronik ödemelerde destek sağladığı ve para transferleri açısından doğabilecek masrafları asgari düzeye indirme noktasında imkân sağladığı üzerinde durulmuştur. Anılan yazar tarafından nakitsiz toplum felsefesinin negatif yönleri olarak yaşlı ve eğitimsiz kişilerin bu sürece uyum sağlamakta zorlanacağı, siber suçların artışına sebebiyet vereceği, mahremiyet açısından sakıncalar içerdiği ve bilgi güvenliği açısından riskler içerdiği üzerinde durulmuştur. Ayrıntılı bilgi için Bkz. Nikola Fabris, "Cashless Society – The Future of Money or a Utopia?" (*"Fabris"*), s. 56-60, ilgili makaleye aşağıdaki link üzerinden ulaşılabilir: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/Cashless_Society_-_The_Future_of_Money_or_a_Utopia.pdf (Gözden Geçirilme Tarihi: 29.10.2020)

[62] POS'un açılımı İngilizce'de "Point of Sales Terminal" olup Türkçe karşılığı ile "Satış Noktaları Terminali"dir. POS cihazları kredi kartları ve debit kartların çiplerindeki bilgileri okumaya, otomatik olarak onay alma ve satışı tamamlamaya yarayan elektronik cihazlardır. Bu sayede, kredi kartları ve debit kartlar ile müşterilerin ödeme noktalarında nakit kullanmadan ödeme yapması sağlanır. Bu konuda detaylı bilgi için bkz. https://www.eticaret.com/e-ticaret-sozlugu/pos-cihazi-nedir/ (Gözden Geçirilme Tarihi: 29.10.2020).

[63] Orijinal ismi İngilizce'de "Automatic Teller Machine" olarak bilinmekte olup Türkçe'ye bankamatik veya otomatik vezne makinesi şeklinde tercüme edilebilir. https://tr.wikipedia.org/wiki/ATM (Gözden Geçirilme Tarihi: 29.10.2020). ATM'ler, bankaların veya finansal kuruluşların belirli bölgelerde müşterileri açısından para çekme, ödeme yapma, talimat verme ve para transferi yapma gibi bankacılık işlemleri yapmasına imkân veren bankamatik cihazları olarak bilinmektedir. ATM'lerin en temel işlevi, banka şubelerine uğramaksızın müşterilerine para çekme konusunda daha etkin ve hızlı bir hizmet verilmesidir.

[64] *Bozkurt Yüksel, Elektronik Para,* s. 42, *Feridun Kaya*, s. 84.

Akıllı kartlar temaslı/temassız, tek kullanımlık/çok kullanımlık, tek amaçlı/çok amaçlı olmak üzere çeşitli ayrımlara tabi tutulabilir[65].

Kredi kartları ve debit kartlarda olduğu gibi akıllı kartlar bakımından da sık gerçekleştirilen siber saldırılar, kullanıcılar tarafından gerçekleştirilen temassız ödemelerde çalıntı ve klonlanmış kartların kullanımı ile kartın manyetik bilgilerinin kopyalanmasıdır[66].

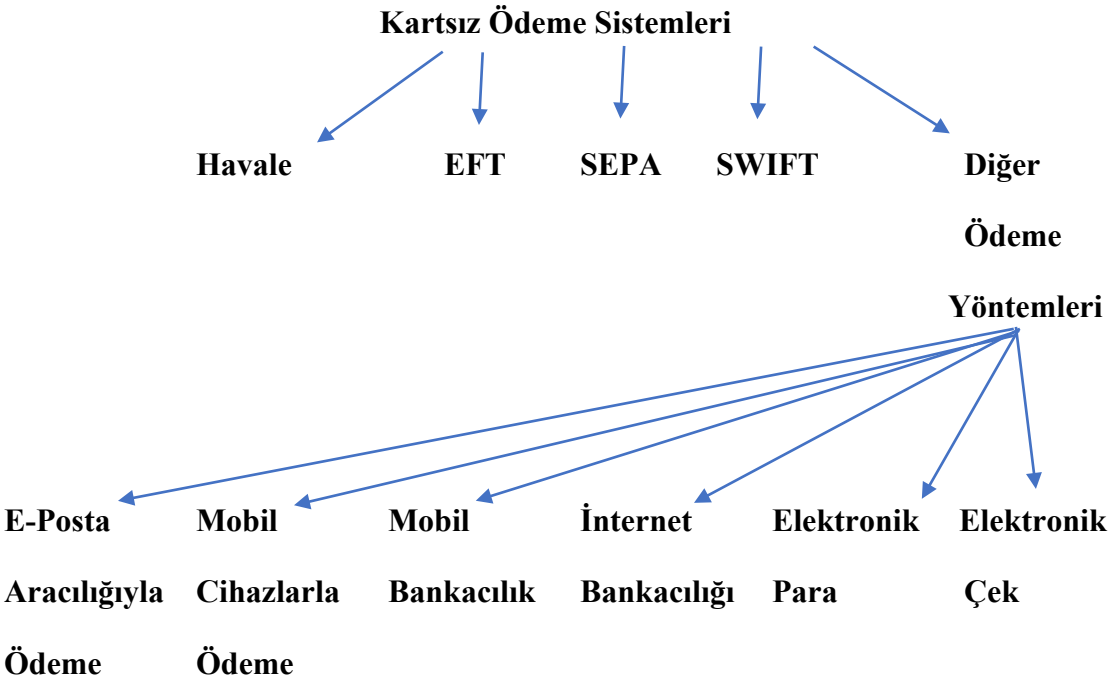
1.2.2. Kartsız Ödeme Sistemleri

Aşağıdaki tablodan da görüleceği üzere, bu başlık altında kısaca havale, EFT (elektronik fon transferi), SEPA, SWIFT ve "Diğer Ödeme Sistemleri" (bu alt başlık altında ise alt başlıklar olarak e-posta aracılığıyla online ödeme, mobil ödeme ve mobil bankacılık, internet bankacılığı, elektronik para ve elektronik çek kavramları) tek tek siber güvenlik bakış açısıyla ele alınacaktır.

---

[65] Akıllı kartlardaki bu ayrımları kısaca belirtmek gerekirse, temaslı akıllı kartlarda kredi kartlarındaki gibi POS ve ATM cihazlarında kart okuyucuya temas etmesi suretiyle bilgi akışı gerçekleştirilirken temassız akıllı kartlarda ise okuyucu ile temas yerine uzaktan gösterilerek işlemin gerçekleştirilmesi mümkündür. Tek kullanımlık akıllı kartlar adından da anlaşılacağı üzere bir kez kullanılıp atılırken çok kullanımlık kartlar ise kartın içindeki para bittikten sonra tekrar yükleme yapılabilen kartlardır. Kartın tek amaçlı olması ise telefon, ulaşım, yemek hizmeti gibi sadece belirli bir mal ve hizmet karşılığı ödeme yapılmak için kullanılmasını ifade ederken elektronik cüzdan olarak da ifade edilen çok amaçlı kartlarda birden çok mal veya hizmet alımı gerçekleştirilebilir. Bu konuda detaylı bilgi için bkz. *Bozkurt Yüksel, Elektronik Para,* s. 43 vd.

[66] Akıllı kartlarda özellikle okuyucu cihaz vasıtasıyla yapılan ödemelerde NFC teknolojisi kullanıldığından NFC teknolojisi ve bu teknolojiye yönelik gerçekleştirilen siber saldırılar konusunda çalışmanın 1.2.2.5. no'lu "Diğer Elektronik Ödeme Yöntemleri" başlığı altında kapsamlı teknik değerlendirmelere yer verilmiştir. Ayrıca bu konuda çalışma kapsamı itibariyle 2.1.5. no'lu "Kart Dolandırıcılıkları" başlığı altındaki değerlendirmeler de dikkate alınabilir. Literatüre bakıldığında ise, Taheerdoost/Sahibuddin/Jalaliyoon tarafından akıllı kartlarda çok faktörlü şifre doğrulama ve biyometrik verilerle doğrulama gibi yöntemlerin tercih edilmesi suretiyle siber güvenliğin temin edilebileceği değerlendirilmiştir. Bu konuda detaylı bilgi için bkz. Hamed Taheerdoost/Shamsul Sahibuddin/Neda Jalaliyoon, "Smart Card Security, Technology and Adoption", International Journal of Security (IJS), C. 5, S. 2, 2011,
(*"Taheerdoost ve Diğerleri"*), s. 76-83. İlgili makaleye internette şu link üzerinden ulaşılabilir: https://www.cscjournals.org/manuscript/Journals/IJS/Volume5/Issue2/IJS-84.pdf (Gözden Geçirilme Tarihi: 29.10.2020)



Şekil-1.5: Kartsız Ödeme Sistemleri

1.2.2.1. Havale

Havale, gerçek zamanlı olarak aynı banka veya finansal kuruluş bünyesindeki hesaplar arasında para, fon gibi değerlerin transfer edilmesi amacıyla oluşturulmuş ödeme sistemine verilen isimdir[67]. Havale işleminde, aşağıda belirtilen EFT ödeme sisteminden farklı olarak aynı finansal kuruluşun farklı hesapları arasında işletim söz konusu olup hesap sahibi, havale işleminde transfer işlemini aynı finansal kuruluştaki farklı hesapları arasında yapabileceği gibi diğer kişi ya da kuruluşların aynı finansal kuruluşa ait hesaplarına da para transferi sağlanabilir[68].

[67] Şerif Çay, "Elektronik Ödeme Sistemlerinin Finansal Piyasalara Etkisi", T.C. Bahçeşehir Üniversitesi, Yüksek Lisans Tezi, Ankara, 2015, ("*Çay")*, s. 30, ilgili teze ulaşmak için: https://www.academia.edu/25098362/ELEKTRON%C4%B0K_%C3%96DEME_S%C4%B0STEMLER%C4%B0N%C4%B0N_F%C4%B0NANSAL_P%C4%B0YASALARA_ETK%C4%B0S%C4%B0 (Gözden Geçirilme Tarihi: 29.10.2020).
[68] *Çay*, s. 30.

İnternet üzerinden yapılan satışlar vasıtasıyla gerçekleştirilen dolandırıcılıklarda kurbanların algısını istismar etmek suretiyle genelde internet üzerinde zor bulunan bir ürünü düşük bir fiyat üzerinden vermeyi teklif ederek ancak kurbanlarını ürünlerin tesliminden önce gerçekleştirilen havale işlemleri ile haksız kazanç elde edildiği bilinmektedir[69].

1.2.2.2. EFT

İngilizce'de Electronic Fon Transfer sözcüklerinin kısaltması olan EFT, genel itibariyle tarafların ödemelerini farklı finansal kuruluşlar arasındaki hesaplar arasında elektronik ortamda transfer etmesine olanak sağlayan bir ödeme sistemidir[70]. İnternet aracılığıyla EFT işlemi yapabilmek için, kişinin banka hesabının bulunduğu banka ile bu konuda anlaşmış olması gerekmekte olup EFT ile ödeme yapmak isteyen taraf ya ilgili paranın alacaklının hesabına geçmesi konusunda kendi bankasına talimat verecek ya da bu işi bilgisayar üzerinden gerçekleştirecektir[71].

EFT sistemi, Türkiye'de Türk Lirası üzerinden yapılan ödeme işlemlerinin bankalara arasında elektronik ortamda gerçekleştirilmesini sağlayan bir ödeme sistemi olup

---

[69] İnternet üzerinden gerçekleştirilen bu dolandırıcılık türünde, genelde mağdur konumundaki kişiler, aradıkları ve zor bulunan bir ürünü internette iyi bir fiyata bulur ve mağdurların karşılarına bu konuda talepleri yakından takip eden dolandırıcılar çıkmaktadır. Mağdur kişi, ilgili ürünü satın almak için ödeme yaptıktan sonra ya malı hiç teslim alamaz yahut ilanda belirtilenden daha düşük değerde bir mal kendisine gönderilir. Bu dolandırıcılık türünün somut örnek üzerinden bakılığında özellikle ikinci el araçlar üzerinden yapılanı geçmişte yaygın şekilde gerçekleştirilmiştir. Satıcı konumundaki dolandırıcılar, genellikle bir ihtiyaç halinden dolayı aracını acele satmak zorunda olduğunu, bu yüzden de normalden daha ucuz bir fiyat istediğini, alıcılarla yüz yüze görüşmesinin mümkün olmadığını, ücretin belirtilen hesaba havalesinden sonra aracın alınabileceğini belirtmektedir. Hesaba gerçekleştirilen havale sonucunda ise karşıdaki kişiye ulaşılamamaktadır. Crime Complaint Service'in rakamlarına göre 2011 yılında bu şekilde 88,2 milyon dolar dolandırıcılara kaptırıldığı belirtilmiştir. Bu konuda ayrıntılı bilgi için Bkz. Hakan Hekim/Oğuzhan Başıbüyük, "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", Uluslararası Güvenlik ve Terörizm Dergisi, 4 (2) 2013 (*"Hekim/Başıbüyük"*), s. 138: http://www.acarindex.com/dosyalar/makale/acarindex-1423936102.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[70] https://www.nbwa.org/sites/default/files/EFT.pdf (Gözden Geçirilme Tarihi: 29.10.2020)

[71] *Bozkurt Yüksel, Elektronik Para,* s. 23-24.

üçüncü nesil EFT sisteminin iki işlevsel bileşeni bulunmaktadır[72]: (i) Müşteriler arası TL aktarım sistemi bileşeninde, bankaların müşterileri adına gerçekleştirdikleri ödemeler yer almaktadır. (ii) Bankalar arası TL aktarım sistemi bileşeninde ise, bankaların birbirleri arasında gerçekleştirdikleri ödemeler ile yurtdışı finansal kuruluşlara sağladıkları muhabirlik hizmetlerine ilişkin bankacılık ödemeleri gerçekleştirilmektedir.

EFT ve havale işlemlerinde gerçekleştirilen dolandırıcılıklarda bir başka yöntem olarak, dolandırıcıların sahte kimlik bilgileri ile şubeye başvurarak hesap açmayı talep etmesi dikkat çekmektedir. Bu bağlamda, dolandırıcılar genelde sahte isim üzerinden açtıkları hesap üzerinden para transferi gerçekleştirmekte ve daha sonraki süreçte ise genelde bu işlemlerden sonra şubeye uğramamaktadır. EFT ve havale işlemleri açısından etkin bir siber güvenliğin sağlanmasında bankaların özellikle güvenlik birimlerindeki personellerin yurtdışında kaynağı belli olmayan şüpheli işlemler konusunda mümkün olan en hızlı şekilde müşterilerden bu işlemlerin doğruluğunu teyit etmeleri önem taşıdığı gibi müşterilerin de özellikler şüpheli işlemler konusunda farkındalığının yüksek seviyede olması ve periyodik olarak banka hesap hareketlerinin incelenmesi kritik düzeyde önemlidir. Dolayısıyla, EFT ve havale işlemlerinde siber saldırıların önlenmesi açısından banka görevlileri tarafından hesap açmak isteyen müşterilerin kimlik bilgileri dikkatle kontrol edilmeli ve EFT ve havale işlemleri ile hileli şekilde para transferi sağlanması halinde hesap hareketlerinin incelenerek paranın hangi kanaldan aktarıldığı da dikkatle incelenmelidir. Ayrıca, şüpheli işlemler açısından ise ilgili bankanın güvenlik ekipleri ve hileli şekilde aktarılan paranın iadesi sağlanamıyor ise parası çalınan müşterinin ilgili Cumhuriyet Savcılığına suç

[72] EFT sistemi, ilk kez Türkiye'de 1992 yılında faaliyete geçmiş olup 2000 yılında ikinci nesil EFT sistemine geçilmiş, son olarak yukarıda belirtilen üçüncü nesil EFT sistemi ise 2013 yılında işletmeye alınmıştır. Birinci, ikinci, üçüncü nesil EFT sistemleri ve EFT'nin işlevsel bileşenleri konusunda ayrıntılı bilgiye aşağıdaki link üzerinden ulaşılabilir:
https://www.tcmb.gov.tr/wps/wcm/connect/TR/TCMB+TR/Main+Menu/Temel+Faaliyetler/Odeme+Sistemleri/Turkiyedeki+Odeme+Sistemleri/Elektronik+Fon+Transfer+%28EFT%29+Sistemi (Gözden Geçirilme Tarihi: 29.10.2020).

duyurusunda bulunurken, kendi çalıştığı banka ve şubesi aleyhine de dava açabileceği bu konuda üzerinde durulması gereken önemli konulardandır[73].

1.2.2.3. SEPA

SEPA[74], en basit anlamda Avrupa Birliği sınırları içerisinde ödeme sistemlerini yeknesak hale getirmek amacıyla nakit olmaksızın Avro transferi yapılmasını sağlayan bir ödeme platformudur[75]. SEPA ödeme sistemi[76], coğrafi açıdan tüm Avrupa Birliği ülkelerinde ve bunun dışında İzlanda, Norveç, İsviçre, Lihtenştayn, Monako, San Marino, Vatikan'da geçerlidir. Bu ödeme sistemi, Avrupa Birliği'ndeki tüketicilere, işletmelere, kamu kurum ve kuruluşlarına kredi transferleri, doğrudan borç ödemeleri, kart ödemeleri gibi finansal işlemleri gerçekleştirmesini sağlamaktadır[77].

Avrupa Birliği'nin 260/2012 Sayılı (EU) SEPA Tüzüğü[78], Avrupa Birliği ülkeleri arasında Avro para birimine bağlı olarak kredi transferi ve doğrudan borçlanmaya yönelik hukuki düzenlemeler ile Avrupa Birliği ülkeleri dışındaki ülkelere yönelik Avro cinsinden para transferine yönelik hukuki düzenlemeleri içermektedir[79].

---

[73] Tuğsan Yılmaz, "İnternet Bankacılığı İle Yapılan Dolandırıcılık": http://www.tugsanyilmaz.av.tr/fikri-haklar-ve-bilisim-hukuku/internet-bankaciligi-ile-yapilan-dolandiricilik (Gözden Geçirilme Tarihi: 29.10.2020).

[74] Orijinal adıyla "Single Euro Payments Area" Türkçe'ye "Tek Avro Ödeme Alanı" olarak tercüme edilebilir (Serbest Çeviri).

[75] *Çay*, s. 30-31

[76] SEPA'nın şu avantajları olduğu belirtilmiştir: (i) Avrupa Birliği sınırları içerisinde banka transfer işlemleri açısından yeknesak bir sistemdir. (ii) Avrupa Birliği'ndeki farklı bir ülke vatandaşının diğer bir Avrupa Birliği ülkesinde aldığı bir ürün veya hizmet karşılığında Avrupa Birliği sınırları içerisinde sınır-ötesi borçlandırma işlemlerine imkân vermektedir. (iii) Avrupa Birliği'ndeki bir bireyin kendi ülkesinde açtığı bir hesap üzerinden başka bir SEPA ülkesinde çalışması veya öğrenim görmesi halinde, maaşını veya ödemelerini bu SEPA ülkesinden alabilmesi mümkündür. (iv) Daha ucuz, güvenli ve hızlı bir sınır-ötesi ödemeleri temin etmesi ve daha şeffaf bir fiyatlandırma ve yeknesak bir ödeme standardı öngörmektedir. Bu konuda detaylı bilgi için bkz. https://ec.europa.eu/info/business-economy-euro/banking-and-finance/consumer-finance-and-payments/payment-services/single-euro-payments-area-sepa_en (Gözden Geçirilme Tarihi: 29.10.2020)

[77] https://ec.europa.eu/info/business-economy-euro/banking-and-finance/consumer-finance-and-payments/payment-services/single-euro-payments-area-sepa_en (Gözden Geçirilme Tarihi: 29.10.2020)

[78] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R0260&from=EN

[79] https://ec.europa.eu/info/law/single-euro-payments-area-regulation-eu-260-2012_en (Gözden Geçirilme Tarihi: 29.10.2020)

Literatüre bakıldığında, SEPA'daki siber güvenlik analizi açısından Fischer'e göre, SEPA gibi Avrupa Birliği içerisinde anında ödeme yapılmasına imkân tanıyan ödeme araçları her zaman siber saldırılara başlangıçta daha açık olmuş, zaman içerisinde ancak sistem içerisinde zafiyetlerin analitik yöntemlerle üstesinden gelinmesi ve bu tarz problemlere çözüm bulunması mümkün hale gelmiştir[80]. Gimigliano da Fischer'e benzer şekilde, SEPA ile para transferinin geleneksel para transferi yöntemlerine kıyasla hız konusunda daha iyi olmadığı gibi, özellikle SEPA sisteminin siber güvenlik açısından bazı zafiyetleri içerdiğini ve bu durumun kullanıcıların hesapları üzerinde herhangi bir ihlali engellemeye yeterli olmayacağını belirtmiştir[81]. Görüldüğü üzere, SEPA ödeme sistemi ile ilgili olarak SEPA'nın AB içerisinde yeknesak bir ödeme sistemi olması sebebiyle yukarıda öngörülen bazı avantajları olmakla beraber gelinen aşamada siber güvenlik noktasında henüz yeterli bir koruma sağlamadığı değerlendirilmiştir.

1.2.2.4. SWIFT

SWIFT[82], 1973 yılında Brüksel'de kurulan "Society for Worlwide Interbank Financial Telecommunication"[83] isimli kuruluşun baş harflerinden oluşan kelime topluluğunun kısaltması olup Türkçe'ye "Bankalar Arası Global Finansal Telekomünikasyon Örgütü" şeklinde tercüme edilebilir. Günümüzde, SWIFT ödeme sistemi ile dünya çapındaki bankalar gibi finansal kuruluşların güvenilir bir ortamda gerçekleştirilen

---

[80] Christoph Fischer, "Digital Payments and Cyber Security: trends, risks and solutions" (*"Christoph Fischer"*): https://www.europeanpaymentscouncil.eu/news-insights/insight/digital-payments-and-cybersecurity-trends-risks-and-solutions (Gözden Geçirilme Tarihi: 29.10.2020).

[81] Gabriella Gimigliano, "Money, Payment Systems and the European Union, The Regulatory Challenges of Governance", Cambridge Scholars Publishing, 2016, (*"Gimigliano"*), s.101: https://books.google.com.tr/books?id=M-y2DQAAQBAJ&pg=PA111&lpg=PA111&dq=sepa+cyber+vulnerabilities&source=bl&ots=KHmyNiBe4s&sig=ACfU3U0eX0Rn0_H0BCUaeszLYlNPjbk6MQ&hl=en&sa=X&ved=2ahUKEwietYWSl8zqAhVbVBUIHdjMD4w4ChDoATADegQICBAB#v=onepage&q=sepa%20cyber%20vulnerabilities&f=false (Gözden Geçirilme Tarihi: 29.10.2020).

[82] SWIFT ile ilgili bu kısımda yer alan açıklamalar genel itibariyle SWIFT'ın resmi web sitesi olan https://www.swift.com içeriğindeki bilgilerle de doğruluğu teyit edilerek bu kısma aktarılmıştır.

[83] Anılan organizasyon ile ilgili ayrıntılı bilgi için Bkz. https://www.swift.com/about-us (Gözden Geçirilme Tarihi: 29.10.2020)

SWIFT kuruluşunun öngördüğü standartlar çerçevesinde ödeme talimatlarına yönelik işlemlerin gerçekleştirilmesi, aynı zamanda söz konusu ödemelerle ilgili tarafların doğru şekilde bilgilendirilmesi amaçlanmıştır[84]. 2015 yılı verilerine bakıldığında ise, 11.000 civarında finansal kuruluşun yaklaşık 200 ülkede günde 32 milyondan fazla mesaj[85] ile SWIFT vasıtasıyla birbiri ile etkileşime geçtiği 2018 yılından itibaren, dünya çapında büyük montanlı sınır ötesi ödemelerin yaklaşık yarısının SWIFT vasıtasıyla gerçekleştirildiği kayıt altına alınmıştır[86]. Dolayısıyla SWIFT kimi zaman bazı eleştirilere[87] maruz kalmakla beraber dünya çapında özellikle ödemeler ve diğer finansal işlemler açısından yaygın kullanılan bir mesajlaşma sistemi olduğu görülmektedir.

Özellikle son on yıl içerisinde uluslararası bankacılık işlemleri açısından SWIFT'ın yoğun şekilde rağbet görmesi nedeniyle, SWIFT sistemi üzerinde farklı ülkelerdeki bankalar nezdinde farklı dolandırıcılık faaliyetleri nedeniyle ciddi ölçüde maddi

---

[84] Türkiye Cumhuriyeti Merkez Bankası'nın resmi web sitesinde SWIFT ile ilgili yer verilen açıklamaya göre, SWIFT'in bir ödeme sistemi olmadığı, güvenilir bir uluslararası haberleşme yöntemi olduğu, bankaların, merkez bankalarının, menkul kıymet merkezlerinin, şirketlerin, network sağlayıcılarının ve kuruluşların üye olabildiği, SWIFT'in müşterilerinin eksiksiz ve güvenilir bir şekilde finansal bilgilere ulaşmalarını ve bu bilgileri değiş-tokuş yapmalarına imkân sağlayan platform, ürün ve hizmetleri sağladığı belirtilmiştir. https://www.tcmb.gov.tr/wps/wcm/connect/73289f67-d210-4f49-8902-6e14ecae055d/OdemeSistemleri.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE-73289f67-d210-4f49-8902-6e14ecae055d-m5lk6L- (Gözden Geçirilme Tarihi: 29.10.2020)

[85] 1995 yılında günlük SWIFT mesaj adedinin 2,4 milyon olduğu belirtilmiştir. 1995 yılından 2015 yılına kadar aradan geçen yirmi yıl içerisinde SWIFT mesajlaşma yaklaşık 13 katın üzerinde artış göstermiştir. http://www.digitaljournal.com/news/politics/us-special-envoy-to-iran-tries-to-force-eu-to-follow-us-sanctions/article/553066 (Gözden Geçirilme Tarihi: 29.10.2020)

[86] https://www.fintechmagazine.com/fintech/how-technology-changing-financial-messaging#:~:text=As%20of%202018%2C%20it%20was,worldwide%20used%20the%20SWIFT%20network.&text=SWIFT%2C%20which%20stands%20for%20the,Telecommunication%2C%20is%20headquartered%20in%20Belgium. (Gözden Geçirilme Tarihi: 29.10.2020).

[87] SWIFT işlemi, Ripple gibi Blokzincir ağı üzerinde çalışan diğer ödeme yöntemlerine kıyasla daha fazla zaman alması ve ilgili bankaların para transferlerini komisyon karşılığında yapmaları sebebiyle daha maliyetli olduğu ve alınan bu komisyon ücretleri konusunda yeterli şekilde şeffaflığın sağlanamaması açısından eleştirilmektedir. Özellikle 2018 yılında "Financial Times" isimli dergide yayınlanan "Ripple and SWIFT slug it over cross border payments" isimli makalede, Blokzincir ağı üzerinde çalışan Ripple isimli kripto paralar vasıtasıyla yapılan ödemelerin SWIFT ödemelere kıyasla, çok daha hızlı, ucuz ve güvenilir şekilde gerçekleştirileceği belirtilmiştir. Bkz. https://www.ft.com/content/631af8cc-47cc-11e8-8c77-ff51caedcde6 (Gözden Geçirilme Tarihi: 29.10.2020)

kayıplar yaşanmıştır. Bu konuda IMF'in verilerine bakıldığında[88] (aşağıdaki tabloda sırasıyla hangi bankada, hangi tarihte saldırının gerçekleştirilmesi neticesinde başlangıçta ne kadarlık bir kaybın olduğu ve son sütunda ise sigorta ve farklı mekanizmalar neticesinde kalıcı zararın ne olduğu belirtilmiştir):

SWIFT Saldırılarına Maruz Kalan Kurumlar	**Tarih**	**Başlangıçtaki Zarar (Milyon Amerikan Doları)**	**Mevcut Zarar (Milyon Amerikan Doları[89])**
Banco del Austro (Ekvator)	Ocak 2015	12.2	9.4
Bangladesh Central Bank	Şubat 2016	81	66
Union Bank of India	Temmuz 2016	171	0
TP Bank (Vietnam)	Mayıs 2016	1	0
Akbank (Türkiye)	Aralık 2016	4	4

[88] Yukarıda belirtilen Tablo-1.1, Antoine Bouveret'in "Cyber Risk for the Financial Sector: A Framework for Quantitive Assesment" (*"IMF Working Paper"*), adlı çalışmasından (s. 13) aktarılmıştır. IMF Working Paper için: https://www.google.com.tr/search?sxsrf=ALeKk02knfYvxIFYxicCmhJLiQN9At7AXA%3A1605632909716&ei=jQO0X4WTK5HhUP2Ur-AJ&q=%C4%B1mf+working+paper+swift+attacks+banks&oq=%C4%B1mf+working+paper+swift+attacks+banks&gs_lcp=CgZwc3ktYWIQAzIFCCEQoAE6BAgAEEc6CAghEBYQHRAeOgQIIRAVOgcIIRAKEKABUJCvA1jh0gNg7NkDaABwAngBgAHGAYgBog-SAQQwLjE0mAEAoAEBqgEHZ3dzLXdpesgBA8ABAQ&sclient=psy-ab&ved=0ahUKEwjFjeTZiIrtAhWRMBQKHX3KC5wQ4dUDCA0&uact=5# (Gözden Geçirilme Tarihi: 29.10.2020).

[89] Yukarıda yer verilen tabloda, "Mevcut Zarar" başlağı altında rakamsal olarak aktarılan zararların SWIFT saldırılarına maruz kalan kurumların kamuoyu ile resmi şekilde paylaştıkları zarar kalemi olduğu bilinmektedir. Bkz. *IMF Working Paper*, s. 13.

Far Eastern International Bank (Tayvan)	Ekim 2017	60	0.5
NIC Asia Bank	Ekim 2017	4.4	0.6
Globex (Rusya)	Aralık 2017	1	0.1
Rusya'da olan ancak bilenmeyen bir banka	Aralık 2017	Bilinmiyor	6
City Union Bank (Hindistan)	Ocak 2018	2	Bilinmiyor

Tablo-1.1: SWIFT Sistemine Yöneltilen Saldırılarda Kurumların Zararları

Yukarıdaki tablo, saldırganların özellikle son beş sene içerisinde SWIFT sistemine yönelik ciddi saldırılar gerçekleştirdiğini ortaya koymaktadır[90]. Özellikle 2016 yılında gerçekleştirilen Bangladeş Merkez Bankası'na yönelik siber saldırı, bu zamana kadar SWIFT sistemine yöneltilen en nitelikli ve zarar noktasında en büyük zararın yaşandığı bir saldırı olarak dikkat çekmiştir. Bu saldırı sonucunda, SWIFT sisteminin özellikle siber saldırılara karşı güvenli olmadığı ve bu konuda ek birtakım tedbirlerin alınması gerektiği anlaşılmıştır[91]. Bu saldırıdan sonra, SWIFT tarafından Customer Security Controls Framework (*"CSCF"*) olarak belirtilen ve Türkçe'ye "Müşteri Güvenlik

[90] Bu başlık altında yukarıda sadece SWIFT saldırılarının neler olduğu kısaca tablo halinde açıklanarak konuya genel bir giriş yapılmıştır. SWIFT saldırılarından yukarıda dikkat çeken bazı örneklere ilişkin ayrıntılı değerlendirmelere çalışmanın 2.4. numaralı "SWIFT Sistemine Yönelik Saldırılar" başlığı altında yer verilecektir.

[91] 2016 yılında, "Lazarus" denilen bir grup siber korsanın SWIFT ağı aracılığıyla New York Federal Rezerv Bankası'nı Bangladeş Merkez Bankası'nda bulunan 81 milyon Amerikan Doları değerindeki paranın korsanların Filipinler'de bulunan hesabına aktarılmasına ikna ettiği bilinmektedir. Bu bağlamda, her ne kadar 81 milyon USD aktarılsa da, resmi kayıtlara yansıyan zarar miktarı yaklaşık 66 milyon USD civarındadır. Bu konuda detaylı bilgi için bkz.https://www.cigionline.org/articles/mitigating-cyber-risk-across-financial-sector?gclid=Cj0KCQjw9b_4BRCMARIsADMUIyrR20hnIdnMix8BWPa_qw5ZpqiC1DJSPTSOR0R1N8N_O8UngmXbBnQaAjVjEALw_wcB (Gözden Geçirilme Tarihi: 29.10.2020).

Koruma Çerçevesi" olarak tercüme edilebilecek bir güvenlik programı uygulamaya alınmıştır. SWIFT kurumunun, Nisan 2019 tarihli ISAC Raporu'nda[92], 2017 yılında Mart ayında yayınlanan CSCF ile emredici ve tavsiye niteliğinde olmak üzere SWIFT kullanıcılarına uyulması gerekli bazı güvenlik tedbirleri bildirilmiştir. Bu bağlamda, söz konusu tedbirlerin aslında hâlihazırda bilgi güvenliği konusunda dünyada yaygın şekilde uygulanan standartlar olan PCI DSS, ISO 27001 ve NIST standartlarına uyumlu olduğu ve CSCF kapsamında öngörülen kuralların aslında SWIFT ile bağlantılı olan altyapıyı korumak üzere tasarlandığı görülmüştür.

SWIFT sistemi ile ilgili dolandırıcılıklarda en klasik yöntem genelde siber saldırganlar tarafından uluslararası ticaret yapan firmaların e-mail adresleri ve uluslararası ticaret işleminin detayları (bu işlemin kimler arasında yapıldığı ve özellikle ödemenin kime, hangi hesabına ve hangi tarihte yapılacağı gibi) öğrenilerek ödemenin yapılacağı SWIFT kodu yerine saldırganların kendi SWIFT kodlarını belirtmek suretiyle ödemeyi kendi hesaplarına yönlendirmesi şeklinde gerçekleşmektedir[93]. Ayrıca, aşağıda teknik açıdan detaylı şekilde açıklanacağı üzere, SWIFT sistemine yönelik siber saldırılar daha ziyade sisteme izinsiz giriş (*system hacking*) ve zararlı yazılım (*tailored malware*) vasıtasıyla SWIFT dolandırıcılığı şeklinde gerçekleştirilmektedir.

1.2.2.5. Diğer Elektronik Ödeme Yöntemleri

Bu başlık altında kısaca e-posta aracılığıyla online para gönderme, mobil ödeme sistemleri ve mobil bankacılık, internet bankacılığı, elektronik para ve elektronik çek şeklindeki elektronik ödeme sistemlerinin genel itibariyle işleyişi siber güvenlik perspektifi ile ele alınmıştır.

---

[92] file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/isac_report_201903_57412_v13.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[93] Türkiye Bankalar Birliği, "Bankacılıkta Dolandırıcılık Eylemleri Tespit Ve Önleme Yöntemleri", Ekim 2015 (*"TBB"*), s. 35, ilgili makaleye ulaşmak için bkz. https://www.tbb.org.tr/gec/KTPV14.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

E-Posta Aracılığıyla Online Para Transferi: Bu ödeme yönteminde, kullanıcılar elektronik posta ile bankalarına ödeme talimatı vererek, herhangi bir hesaptaki paradan başka bir hesaba para aktarılmaktadır. Talimatı alan banka ise alıcı tarafa özellikle benzer şekilde elektronik posta göndererek parayı çekebileceğini alıcıya bildirmektedir[94]. X.com[95], PayPal[96] ile Bank One'ın eMoneyMail[97] uygulaması e-posta ile online para transferi yapılmasına imkân tanımaktadır[98].

E-posta vasıtasıyla gerçekleştirilen ödeme işlemlerinde sık gerçekleştirilen siber saldırı yöntemlerinin aradaki adam saldırısı (*Man-in-the-Middle*)[99], oltalama ve sosyal mühendislik saldırıları şeklinde gerçekleştirildiği görülmektedir.

Mobil Ödeme Sistemleri: Mobil ödeme sistemleri, "alınan ürün ve hizmet karşılığında mobil cihazlar vasıtasıyla yapılan yetkilendirme ve onaylama işlemleri sonucunda temassız ve diğer mobil iletişim teknolojilerin imkânlarından yararlanmak suretiyle yapılan ödemeler" şeklinde tanımlanabilir[100]. Mobil ödemelerin gündelik yaşamda birçok farklı uygulama ve yöntem içerdiği bilinmektedir. Farklılaşan tüm uygulama ve yöntemler bir kenara bırakıldığında, sistemin işleyişi özetle şu şekilde gerçekleşmektedir: Öncelikle mobil ödeme hizmetinden yararlanmak isteyen kişi, mobil ödeme hizmet sağlayıcısı açısından müşteri (kullanıcı) olarak kaydedilecektir. Mobil ödeme hizmetinin kullanılması esnasında ise, mobil ödeme uygulamasının bilgi

---

[94] *Keser Berber*, *Elektronik Para,* s. 57-58.
[95] https://techcrunch.com/2017/07/10/elon-musk-x-dot-com/ (Gözden Geçirilme Tarihi: 29.10.2020).
[96] https://www.paypalobjects.com/webstatic/mktg/integration-guides/email-payments.pdf(Gözden Geçirilme Tarihi: 29.10.2020).
[97] https://jpmorganchaseco.gcs-web.com/static-files/0fc6bdc3-88e1-4957-b4bf-c6f657fa93d0 (Gözden Geçirilme Tarihi: 29.10.2020).
[98] *Keser Berber*, s. 58.
[99] Bu saldırı türü ile ilgili uygulamada özellikle mobil cihazlarda yapılan ödemelerde NFC teknolojisinin yaygın kullanıldığı durumlarda karşı karşıya kalınması gündeme geldiğinden, çalışmada, aşağıda 1.2.2.5 numaralı "Diğer Elektronik Ödeme Yöntemleri" alt başlığı altında "NFC Teknolojisi İle Ödeme" ile ilgili açıklamalarda detaylı analizlere yer verilmiştir.
[100] Tanım konusunda Bkz. Tomi Dahlberg/Niina Mallat/Jan Ondrus/Agnieszka Zmijewska, "Mobile Payment Market and Research – Past, Present and Future", Working Papers on Information Systems, ISSN 1535-6078, (*"Dahlberg ve Diğerleri"*) elektronik ortamdan ulaşmak için: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/Mobile_payments2006HelsinkiMobilityRoundtable.pdf (Serbest Çeviri), (Gözden Geçirilme Tarihi: 29.10.2020).

güvenliği açısından güvenilir şekilde kullanılmasından mobil ödeme hizmet sağlayıcısı, ağ operatörü ve var ise güvenli unsur[101] (*secured element*) sağlayıcı ile güvenilir servis sağlayıcı sorumludur[102]. Mobil ödeme sisteminde herhangi bir mal veya hizmet sağlayan şirket, üye işyeri anlaşması yapan kuruluşla sözleşme imzalayarak ve kabul etmeyi planladığı mobil ödeme teknolojilerinin gerektirdiği donanım yatırımını yaparak işyeri haline gelir. Müşteri fiziksel olarak veya internet üzerinden bir işyerinden alışveriş yaptığında, mobil ödeme uygulaması kullanan müşterinin kart bilgisinin güvenli unsur olarak kullanılması halinde kart çıkaran kuruluş tarafından, bulut teknolojisinde güvenli unsur kullanılması halinde ise mobil ödeme hizmet sağlayıcısı ve sonrasında kart çıkaran kuruluş tarafından doğrulanması gündeme gelecektir[103]. Tüm bu aşamalar şifreli olarak gerçekleştirilir ve her paydaş ilettiği verinin şifreli olarak iletilmesinden sorumludur. Ancak, veri iletiminin gizlilik, bütünlük ve erişilebilirliğinden ağ operatörü sorumludur. İşlem sonunda ödeme meblağı kart çıkaran kuruluş tarafından müşteriden tahsil edilir ve üye işyeri anlaşması yapan kuruluş tarafından işyerine ödenir. Bu iki paydaş arasındaki mutabakat ve finansal netleştirmeler mutabakat kuruluşu tarafından yapılır[104].

Mobil ödeme sistemlerinin işleyişi kısaca aşağıdaki şekilde şematize edilebilir[105]:

[101] Güvenli unsur (*secured element*), çip seviyesindeki bir güvenlik bileşeni olup cep telefonları içerisinde ödeme bilgilerini kriptografik anahtarlar aracılığıyla muhafaza edilmesini sağlayan izole bir alan sunan, ödemelerin güvenilir şekilde gerçekleştirilmesini sağlayan ve sistemi bu anlamda koruyan unsur şeklinde ifade edilmektedir. Bkz. Barış İşler, Hakan Gülaç, "Mobil Ödemeler, Güvenlik Sorunları Ve Çözüm Önerileri, BDDK Bankacılık ve Finansal Piyasalar C: 11, S: 2, 2017, (*"İşler/Gülaç"*), s. 62, ilgili makaleye ulaşmak için: https://www.bddk.org.tr/ContentBddk/BddkDergi/dergi_0022_05.pdf. (Gözden Geçirilme Tarihi: 29.10.2020)

[102] *İşler/Gülaç*, s. 59-60.

[103] İşler/Gülaç, 59,60.

[104] *İşler-Gülaç*, s.60.

[105] *İşler-Gülaç*, s.60'da tablonun aktarıldığı eser: Wang, Y., Hahn, C. ve Sutrave, K. (2016).

Şekil-1.6: Mobil Ödeme Sistemlerinin İşleyişi

Mobil ödemelerin müşterilerine, ürünlerin farklı yerlerdeki fiyatına, indirimlere ve diğer kampanyalara ait bilgiye erişim ve kıyaslama kolaylığı sunarak daha etkin kullanımı sağlamak gibi avantajlarının yanı sıra, birçok güvenlik sorunu ile karşı karşıya kaldığı da bilinmektedir[106].

Mobil cihazlarla yapılan ödemeler literatürde farklı ayrımlara tabi tutulsa da[107], çalışmanon ana merkezinde siber güvenlik olduğu göz önüne alınarak mobil ödeme sistemleri aşağıda yaygın şekilde kullanılan iletişim teknolojisi uygulamaları çerçevesinde incelenmiştir:

[106] *İşler/Gülaç*, s.83.

[107] İşler/Gülaç'a göre, mobil ödemeler şu şekilde kategorize edilebilir: (i) Ödeme şekline göre mobil ödemeler kişiden kişiye (P2P) ödemeler, uzaktan mobil ödemeler, temassız mobil ödemeler, (ii) risk paydaşına göre yapılan sınıflandırmada ise GSM operatörünün riski üstlendiği yapılar, bir kartlı sistem kuruluşunun riski üstlendiği yapılar ve müşterinin riski üstlendiği yapılar ile (iii) günümüzdeki iletişim teknolojisine bağlı olarak müşterinin kimlik doğrulama verilerinin iletişiminde kullanılan teknolojiye göre mobil ödemeler, NFC, QR Kodu, SMS/USSD ve internet yoluyla mobil ödemeler olarak dört ana başlık altında kategorize edilebilir. Ayrıntılı bilgi Bkz. *İşler-Gülaç*, s. 60-70. Tezin merkezindeki konunun siber güvenlik olması sebebiyle yazar tarafından tez içeriğindeki konu bütünlüğünü bozmamak adına sadece iletişim teknolojileri açısından mobil ödeme sistemleri noktasında yapılan sınıflandırmalar ve bu bağlamda her teknolojik uygulama siber güvenlik bakış açısıyla irdelenmiştir.

(i) NFC Teknolojisi İle Ödeme: NFC[108] teknolojisi, temel itibariyle mobil cihazdaki verilerin bir cihazdan diğerine 10 cm kısa mesafede aktarılmasını sağlayan ve günümüzde yaygın şekilde kullanılan iletişim teknolojisi uygulamasıdır. Bu teknolojiyle veri aktarılabilmesi için veri aktarımının 13.56 Mhz frekansında 424 kilobit/saniye hızında olması gerekir[109]. Sistemin çalışma mantığı, NFC özelliğine sahip cihazlardaki çipler[110] üzerinden verinin iletilmesine dayanmaktadır. Konuya teknik açıdan bakıldığında NFC özelliğini haiz cihazlar, ödemeyi gerçekleştirebilmek açısından on santimetrelik bir mesafeye yaklaştırıldığında etkin hale gelir. Bu nedenle cihazlar arasındaki ödeme işleminin tamamlanabilmesi açısından söz konusu cihazlarda NFC teknolojisinin etkin hale gelmesini sağlayan yongaların ve antenlerin bulunması gerekir. Bu teknolojinin kullanımı sırasında cihazlar arasındaki kablosuz bağlantı, kablosuz izleme uygulamalarında kullanılan radyo frekansı tanımlama (RFID)[111] uygulamasına benzer şekilde radyo dalgalarından faydalanmaktadır. NFC

[108] İngilizce açılımı "Near Field Communication" olup Türkçe'ye "Yakın Alan Haberleşmesi" olarak tercüme edilmiştir (Serbest Çeviri).
[109] *Özkaya/Sarıca/Durmaz*, s. 88.
[110] Çip, teknik açıdan silisyum bir altlık üstüne birbirlerine alüminyum ve altın teller vasıtasıyla bağlanmış olan çok miktarda transistörün yerleştirilmesi ile meydana getirilen ufak elektronik bir parça olarak tanımlanabilir. Günümüzde çipler, bilgisayarlar da dâhil olmak üzere eğitim araçları, projelendirme uçaklar, suni organlar, elektronik duyma cihazları, kalp atışlarını düzenlemekle görevli aletler, elektronik birden farklı alanda kullanılabilmektedir. Bkz. https://www.mediaclick.com.tr/blog/cip-nedir (Gözden Geçirilme Tarihi: 29.10.2020).
[111] Türkçe'de radyo dalgaları tanımlama sistemi (orijinal adı "radio frequency identification system"dır) olarak nitelendirilen RFID, cihazlar ve bilgisayarlar arasında nesnelerin tanınmasını, üst verinin (*metadata*) kaydedilmesini ve bireysel amaçlar çerçevesinde hedeflerin kontrol edilmesini sağlayan otomatik teknolojiye verilen isimdir. Tipik bir RFID sistemi iletici (*transmitter*) ve cevaplayıcı (*responder*) denilen parçalar ile okuyuculardan - bu terim bilişim terminolojisinde iletici (*transmitter*) ve alıcı (*receiver*) olarak ifade edilmektedir – oluşmaktadır. Sistemin içindeki parçalar, sistemi tanımlamak üzere anten ve bu antene bağlı bir mikroçiptir. RFID okuyucusu, RFID parçaları ile radyo dalgaları bağlantısı ile iletişim kurar. RFID teknolojisinin en avantajlı yönünün, geniş işlem aktivitelerinin takip edilmesini sağlayan ve barkod gibi eski tip teknolojik araçların maliyetlerini asgariye düşürmeyi sağlayan otomatik bir tanımlayıcı ve veri toplayıcısı olduğu belirtilmiştir. RFID teknolojisi aslında uzun yıllar öncesinde keşfedilen bir teknoloji olmasına rağmen, maliyet açısından diğer ödeme sistemlerine kıyasla avantaj sağlaması sebebiyle özellikle son on yıl içerisinde özellikle gelişen ve daha yaygın kullanılan bir teknoloji haline gelmiştir. Bkz. Xiaolin Chia, Quanyuan Feng, Taihua Fan, Quanshui Lei, "RFID Technology and Its Applications in Internet of Things (IoT)", (*"Feng/Lei"*) söz konusu makaleye aşağıdaki web sitesi üzerinden ulaşılabilir: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/RFIDTechnologyandItsApplicationsinInternetofThingsIOT.pdf (Gözden Geçirilme Tarihi: 29.10.2020)

teknolojisinin dikkat çeken özelliği, mobil telefonun aslında fiziksel olarak bir POS cihazı ile aynı ortamda bulunduğu ödemelerde kullanılmasıdır. Daha yalın bir anlatımla, mobil cihazında NFC teknolojisi tanımlı bir müşterinin ödeme işlemini tamamlayabilmesi için telefonunu okuyucu cihaza yaklaştırması yeterlidir. NFC teknolojisi ile yapılan ödemelerde genelde hız ve kolaylık amaçlandığı için ödeme işlemlerinde ayrıca PIN girilmesi gerekliliği bulunmamaktadır. Günümüzde özellikle toplu taşıma, kartlı geçiş sistemleri, öğrenci kimlikleri, ödeme işlemleri gibi uygulamaların her birisi için farklı kartlar kullanılması yerine tek bir cihaz üzerinden bu işlem ve uygulamaların gerçekleştirilmesi NFC teknolojisine dayanmakta olup akıllı telefonlar sayesinde NFC teknolojisi ile tüm bahsi geçen bu işlemlerin gerçekleştirilmesi mümkün kılınmıştır[112].

NFC özellikli cihazlar kapsamında hattın dinlenmesi, veri bozma, veri değiştirme, veri ekleme ve uygulamada sık şekilde yukarıda belirtilen ortadaki adam saldırısı[113] gibi saldırılar gerçekleştirilebileceği gibi NFC tabanlı teknolojiye dayanılarak yapılan temassız ödemelerde en kritik güvenlik risklerinin çalıntı ve klonlanmış kartlar ile kart bilgilerinin çalınması olduğu üzerinde durulmaktadır[114].

Covid-19 salgının dünyada ve Türkiye'de etkisi sonucunda NFC tabanlı teknolojiye ilginin arttığı gözlemlenmiştir[115]. Özellikle NFC ödeme süreçlerinin kullanıcıları

[112] *Özkaya/Sarıca/Durmaz*, s. 88.
[113] İngilizce'de "man in the middle" olarak ifade edilen "ortadaki adam saldırısı", doktrinde Altınkaynak tarafından bir ağ üzerindeki hedef bilgisayar veya mobil cihaz ile ağ cihazı arasına girerek trafikten bilgi almaya dayanan saldırı tipi olarak ifade edilirken Çakır/Kılıç ise "ortadaki adam saldırılarının "phisher" olarak nitelendirilen saldırganın internet bankacılığı işlemlerinde müşteri ile banka arasına girerek ve özellikle kullanıcı konumundaki kişilere kendisinin oluşturduğu sunuculara gönderdikleri link ile kendisinin oluşturduğu sunuculara yönlendirdiklerini değerlendirmiştir. Bu saldırı tipinde (i) transparan proxy, (ii) DNS önbelleği zehirlemesi ve (iii) kullanıcı tarayıcı ayarının değiştirilmesi gibi üç tür aldatmaca yöntemi söz konusudur. Bu konuda detaylı bilgi için bkz. *Altınkaynak*, s. 208 ve *Çakır/Kılıç*, s. 115.
[114] *Özkaya/Sarıca/Durmaz*, s. 89.
[115] Bu konuda bazı şirketlerin son zamanlarda NFC kapsamındaki yeni ürünlerine Samsung Pay'in dijital kredi platformu SoFİ ile işbirliğine gitmesi, Huawei'in Huawei Pay ödeme projesi, Turkcell'in PayCell uygulaması, Google Pay konusunda yukarıda belirtilen "Cache" projesi örnek gösterilebilir.

açısından kolay, hızlı ve güvenli ödeme imkânı sağlaması sebebiyle "Apple Pay" ve "Google Pay" gibi ödemelerin NFC tabanlı ödemeler olduğu ve tüketiciler açısından hızlı bir şekilde tercih edilen bir ödeme yöntemi olduğu üzerinde durulmuştur[116]. Bu kapsamda Google Pay ve Apple Pay'den kısaca bahsetmek gerekirse:

Apple Pay: Apple şirketi tarafından 2014 yılı Eylül ayında, Apple Pay denilen bir mobil ödeme sisteminin uygulanacağı açıklanmıştır. Apple Pay, iPhone 6 (iOS işletim sisteminin çalıştığı) ve Apple Watch (Watch OS) üzerinden kullanıcıların hem biyometrik verilerinin (parmak izi ve nabız) cihaza yüklenmesini ve cihaza yüklenen mobil uygulamalar ile temassız ödemeye olanak tanıyan bir ödeme hizmetidir. Apple Pay vasıtasıyla ödemelerin gerçekleştirilmesi için, işletmecilerin NFC tabanlı ödeme teknolojisini tanıyan sistemlere sahip olması gerekmektedir. Apple şirketi, bu ödeme işlemlerinin gerçekleştirilmesi için MasterCard, Visa ve AmEx gibi kredi kartı firmaları ile kart düzenleyen şirket ve işletmeci arasında ödemenin gerçekleştirilmesini sağlayan muhtelif bankalarla iş birliğine gitmiştir. Bu noktada sistem şu şekilde işlemektedir: Öncelikle, Apple Pay kart sahibi şirket ile işletmecinin bankası arasında aracılık faaliyeti yürütmektedir. En basit şekliyle, güvenli unsuru barındıran NFC çipi ile Apple sisteme giriş hakkını münhasıran elinde bulundurur ve kredi kartı şirketi tarafından kontrol edilen ödeme jetonları (*tokens*) ve bankalar tarafından kontrol edilen kriptografi gibi tekniklerle ödeme bilgilerini saklar. Müşteri, cep telefonuna indirdiği Apple Pay uygulaması ile kredi kartı bilgilerini girmeksizin iOS işletim sistemi aracılığıyla ödeme yapmaktadır. Ödeme hizmeti, mobil cihazın özgün hesap numarası vasıtasıyla okuyucu ekrana cihazın okutulması, başka bir ifadeyle NFC teknolojisi vasıtasıyla gerçekleştirilir[117]. Ödeme işleminin gerçekleştirilmesi için Apple Pay

[116] NFC teknolojisine dayanan ödemeler konusunda ayrıntılı bilgi için Bkz. *İşler/Gülaç*, s. 64,65 ve *Özkaya/Sarıca/Durmaz*, s. 88.

[117] Erol Kazan, "The Innovative Capabilities of Digital Payment Platforms: Comparative Study of Apple Pay & Google Wallet", (*"Kazan"*) ilgili makaleye internetten ulaşmak için: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/TheInnovativeCapabilitiesOfDigitalPaymentPlatforms%20(1).pdf (Gözden Geçirilme Tarihi: 29.10.2020)

uygulamasında işlemin güvenliği açısından "Touch ID" denilen parmak izi doğrulaması ile gerçekleştirilir.

Literatüre bakıldığında, Jawale/Park'a göre parmak izi konusunda dahi günümüzde siber saldırganlar tarafından kopyalanabilir yöntemlerinin geliştirilebildiği ve bu nedenle Apple Pay uygulamasının yeni bir uygulama olmakla beraber siber güvenlik açısından bazı zafiyetlerinin olabileceği belirtilmiştir[118].

Google Pay: Google Pay ödeme uygulaması olarak Apple Pay'e benzer bir dijital ödeme hizmeti olarak Google şirketi tarafından 2011 yılında geliştirilmiştir. Bu ödeme uygulaması kullanıcıların cep telefonlarına Google Pay uygulamasını yükleyerek online alışveriş ve para transferi yapmaları için tasarlanmıştır. Google Pay ödeme uygulaması, NFC tabanlı ödeme teknolojisine dayanan bir uygulama olup cihazların akıllı telefon veya Google Wallet sistemini destekleyen mağazalarda sanal POS üzerinden ödeme yapmalarına imkân vermektedir.

Google Wallet, kullanıcıların tüm ödeme ve hesap bilgisi geçmişine dair kayıtların Google tarafından sunucularda depolanması sebebiyle bu sunuculara siber saldırganlar tarafından yapılabilecek ataklarda bu bilgilerin ele geçirilme riski olması sebebiyle eleştirilmiştir[119].

(ii) QR Kodu İle Ödeme: QR[120] kodu, iki türevli bir barkod türevi olarak nitelendirilmekte olup hem yatay hem de dikey bilgileri içerdiğinden, QR teknolojisinde geleneksel barkod teknolojisine kıyasla daha fazla bilginin saklanması

[118] Ashay S. Jawale/Joon S. Park, "A Security Analysis on Apple Pay", 2016 European Intelligence and Security Informatics Conference, (*"Jawale/Park"*) s. 161, ilgili makaleye elektronik ortamda ulaşmak için: http://www.csis.pace.edu/~ctappert/papers/proceedings/2016EISIC/data/2857a160.pdf, (Gözden Geçirilme Tarihi: 29.10.2020)
[119] Bkz. *Jawale/Park*, s. 160.
[120] QR, İngilizce'de "Quick Response" olarak kullanılmakta olup Türkçesi "Hızlı Cevap" olarak tercüme edilebilir. (Serbest Çeviri).

mümkündür[121]. QR kodlarının mobil cihazlarda yaygın şekilde kullanılması sebebiyle[122] "mobil kodu" olarak nitelendirilmiş, mobil kodlamanın ise mobil cihazlar yoluyla ve iki boyutlu barkod kullanılarak yerleşik kameralı bir mobil cihaz tarafından okunabilir veri elde etme süreci olduğu belirtilmiştir[123]. İletişim teknolojisi olarak QR kodunun mobil ödemelerde kullanılması üç şekilde gerçekleştirilebilir: (i) İşyeri tarafından üretilen QR kodu, müşterinin cep telefonu tarafından okunarak ödemeye ilişkin bilgiler (alışveriş tutarı, işyeri unvanı, adresi, vb.) müşterinin cep telefonuna iletilmesi sonucunda ödeme gerçekleştirilir. (ii) Benzer şekilde işyeri tarafından üretilen QR kodu müşterinin cep telefonu tarafından okutularak bir internet sitesine yönlendirilir ve bu internet sitesi üzerinden müşteri alışveriş yaparak ödemeyi tamamlar. (iii) Son olarak ise, müşterinin ödeme bilgisini içeren QR kodu işyeri tarafından QR kod tarayıcısı tarafından okunarak ödeme işlemi gerçekleştirilir[124].

QR Kodu ile gerçekleştirilen ödemelerde siber saldırılar, bilgisayar korsanları tarafından QR kodunun alınacağı web siteleri ve mobil uygulamalar bakımından müşterilerin oltalamanın gerçekleştirileceği web sitelerine yönlendirilmesi, SQL enjeksiyonu[125] denilen yöntem ile QR kod okuyucularına veri enjekte edilmesi,

---

[121] Erdat Çataloğlu, Armağan Ateşkan, "QR Kodunun Eğitim Ve Öğretimde Kullanımının Örneklendirilmesi, (*"Çataloğlu/Ateşkan"*) s. 7, file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/QRcodes.pdf, (Gözden Geçirilme Tarihi: 29.10.2020)

[122] QR kodları tüm akıllı cep telefon uygulamalarında yaygın olarak kullanılmakta olup aynı zamanda web kamerası olan masaüstü ve dizüstü bilgisayarlar ile sadakat programı uygulamalarında da yayın şekilde QR kodu uygulaması tercih edilebilmektedir. Bunun dışında, QR kodu uygulamasında görsel şifreleme yöntemi kullanılarak 7089 sayısal ve 4296 alfasayısal verinin (yaklaşık 3kb veriye tekabül etmektedir) saklanması mümkün olup bu uygulamanın diğer avantajlarının, hem yatay hem de dikey olarak veri depolama imkânı olması sebebiyle geleneksel barkodlara kıyaslara on kat daha fazla veri depolama kapasitesini haiz olduğu ve kısmi olarak yırtılsalar ve kirlenseler bile işlevlerine devam edebileceği belirtilmiştir. Bkz. *Çataloğlu/Ateşkan*, s. 7.

[123] *İşler/Gülaç*, s. 65.

[124] *İşler/Gülaç*, s. 66.

[125] Web uygulamaları genel itibariyle web kullanıcısından parametreleri alarak veri tabanında SQL sorgulamaları gerçekleştirmektedir. Örnek vermek gerekirse, bir kullanıcı oturum açarken, web saiyfasının girdiği kullanıcı adı ve şifreyi alarak geçerli olup olmadığını kontrol için SQL veri tabanını sorgular. Girilen kullanıcı verisine SQL ifadesi gömülmesi ile SQL enjeksiyonu gerçekleşir. Bu konuda detaylı bilgi için bkz. Özkaya/Sarıca/Durmaz, s. 207-208.

bilgisayar korsanları tarafından zararlı yazılım uzantısı içeren QR kodları vasıtasıyla müşterinin ödeme yaptığını düşündüğü yer yerine siber korsana ödeme yapılmasının sağlanması gibi yöntemlerle gerçekleştirilebilir[126].

(iii) SMS/USSD İle Ödeme: İngilizce'deki adı ile "Short Messaging Service"[127] denilen SMS, GSM[128] teknolojisinin bir ürünü olarak müşteriler arasında kısa mesaj iletilerinin gönderilmesini sağlayan bir hizmettir[129]. USSD[130] ise, GSM standardının bir parçası olarak telefonların servis sağlayıcısına ait sunucular[131] üzerinden iletişimi gerçekleştirilen protokolü ifade eder. SMS'nin USSD'den farklı yönü, SMS'de mesaj gönderen tarafından mesaj iletildiğinde, mesaj öncelikle servis sağlayıcısına ait bir merkezde saklanır, "sakla ve ilet" tekniği kullanılarak mesaj alıcının GSM ağına bağlanması yoluyla iletilir. USSD protokolünde ise, SMS'de olduğu gibi mesajın belirli bir merkezde saklanması söz konusu değildir, burada mesaj iletimi oturum bazlı ve gerçek-zamanlı olarak gerçekleştirilir[132]. Telefon görüşmesi başlatmak en klasik

---

[126] Ram Sagar, "25 Years Of QR Codes: A Look At Vulnerabilities Of This Popular Payment Method": https://analyticsindiamag.com/25-years-of-qr-codes-a-look-at-vulnerabilities-of-this-popular-payment-method/ Gözden Geçirilme Tarihi: 29.10.2020)

[127] Türkçe'ye yazar tarafından "Kısa Mesajlaşma Hizmeti" olarak tercüme edilmiştir (Serbest Çeviri).

[128] GSM, İngilizce'de "Global System for Mobile Telecommunications" olarak belirtilmekte olup Türkçe'ye Mobil Telekomünikasyon Açısından Global Sistem" olarak tercüme edilmiştir (Serbest Çeviri).

[129] *İşler/Gülaç*, s. 67, ayrıca Bkz. www.smsexplorer.com › smshakkinda (Gözden Geçirilme Tarihi: 29.10.2020).

[130] İngilizcesi "Unstructured Supplementary Service Data" olup Türkçe'ye "Yapılandırılmamış Tamamlayıcı Hizmet Verisi" olarak tercüme edilebilir (Serbest Çeviri).

[131] Server (Sunucu), bilgisayar ağlarında, istemcilerin (kullanıcıların) erişebileceği, kullanımına ve paylaşımına açık kaynakları veya elektronik posta web sitesi gibi internet üzerinden edinilen bazı servisleri çalıştıran bilgisayar birimlerine verilen genel bir addır. Bu tanımdan hareketle, sunucu bilgisayar sunduğu servise göre web sitesi yayınlıyorsa web Sunucusu, elektronik posta servislerini yayınlıyorsa e-posta sunucusu veya veritabanı sunucusu olarak isimlendirilir. https://www.hosting.com.tr/bilgi-bankasi/server-nedir-turleri-nelerdir/ (Gözden Geçirilme Tarihi: 29.10.2020)

[132] SMS ve USSD konusunda ayrıntılı bilgi için Bkz. İşler/Gülaç, s. 67-68. Ayrıca bu konuda Bkz. Nadire Çavuş/Dambudzo Netsai Christina Chingoka, "Information Technology in the Banking Sector: Review of Mobile Banking" başlıklı makalesinde (*"Çavuş/Chingoka"*) bankacılık uygulamalarında SMS ve USSD teknolojisi konusunda detaylı teknik değerlendirmelere yer verilmiştir, bu konuda ilgili makaleye aşağıdaki link üzerinden ulaşılabilir: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/Informationtechnologyinthebankingsector-Reviewofmobilebanking-2.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

USSD yöntemi olarak bilinmektedir. Günümüzde SMS ve USSD teknolojilerinin her ikisi de bir mobil ödeme yöntemi olarak kullanılmaktadır. Müşteri, bu yolla cep telefonu üzerinden abonesi olduğu operatöre kısa mesajla veya USSD koduyla bir ödeme talebi gönderir. Bu mesaj neticesinde işleme dair bedel abone olan müşterinin ya telefon faturasına yansıtılır veya ya da cep telefonu faturası yerine mobil cüzdanından tahsil edilir. Bu süreçte işlemin diğer tarafı, yani üye işyeri de, ödemenin durumu hakkında bilgilendirilir. Bu servis kapsamında müşteriye ait bir teslimat adresi paylaşılmaması sebebiyle söz konusu bu yöntemle alınan ürün genellikle dijitaldir[133].

Siber güvenlik açısından bu konuda literatüre bakıldığında, Nyamtiga/Sam/Laizer'e[134] göre USSD teknolojisinin oturum bazlı ve gerçek zamanlı çalışması ve özellikle mesaj iletilerinin SMS'de olduğu gibi depolanmaması nedeniyle daha güvenilir bir sistem olduğu belirtilmiştir. Ancak ilgili yazarlar her iki teknolojinin de temelde GSM ağı üzerinde işletilen teknolojiler olması sebebiyle burada önemli olan olgunun ilgili GSM ağının güvenliği olduğuna özellikle dikkat çekmektedir. USSD'ye kıyasla SMS teknolojisi sadece mobil cihazlar bakımından Java yazılımı ile gerçekleştirilebildiğinden (USSD teknolojisinde İngilizce'de "mobile secure gateway" denilen mobil cihaz teknolojisine eklemlenebilecek ek güvenlik önlemleri SMS'deki Java yazılımına kıyasla daha karmaşıktır) SMS teknolojisi kripto sistemler ve anahtar yönetim tasarımları gibi siber güvenliğin temini açısından alınabilecek yazılımsal ve donanımsal güvenlik tedbirlerinin uygulanması açısından daha elverişli bir teknolojidir.

---

[133] *İşler/Gülaç*, s. 68.

[134] Baraka W. Nyamtiga/Anael Sam/Loserian S. Laizer, "Security Perspectives For USSD Versus SMS In Conducting Mobile Transactions: A Case Study Of Tanzania", International Journal of Technology Enhancements And Emerging Engineerıng Research, C: 1, Sayı 3/38 ISSN 2347-4289, (*"Nygamtiga/Sam/Lazier"*), s. 42-43: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/Security-Perspectives-For-Ussd-Versus-Sms-In-Conducting-Mobile-Transactions-A-Case-Study-Of-Tanzania%20(1).pdf (Gözden Geçirilme Tarihi: 29.10.2020).

(iv) İnternet Üzerinden Yapılan Mobil Ödemeler: İnternet üzerinden yapılan mobil ödemelerde, ödeme verileri bulut bilişim teknolojisi ile saklanır. Bu ödeme işlemlerinde genelde ödeme bilgileri (müşterinin cep telefonu, işyerine ait bilgiler, ürüne ve alışverişe ait bilgiler, vb.) internet üzerinden mobil cüzdan sağlayıcısına iletilmektedir. Siparişi internet üzerinden alan şirket ise ödeme bilgilerini onayladıktan sonra arka planda ödeme işlemi gerçekleşir. İnternet üzerinden yapılan mobil ödemelere örnek olarak PayPal[135], Square[136], Seamless[137], Venmo[138], GoPago[139] ve Dwolla[140] gibi uygulamalar gösterilebilir[141].

Doktrinde İşler/Gülaç tarafından internet üzerinden hassas bilgilerin aktarımının her zaman güvenli olmayacağı, ödeme verilerinin şifreli (*encrypted*) olarak iletilmesinin tercih edilmesi gerektiği, şifrelemenin ise iletişimde belirli bir yavaşlamaya neden olabileceği üzerinde durulmuştur[142].

Mobil Bankacılık: Mobil yöntemlerle ödemelerde olduğu gibi mobil bankacılık günümüzde gelişen cep telefonu teknolojisi ile başvurulan bir yöntem olup bireylerin bankacılık işlemlerini bir ağ üzerinden bağlanan mobil cihazlarla gerçekleştirmesini ifade eder. Başlıca mobil bankacılık türleri günümüzde "Etkileşimli Ses Cevaplama" (*IVR-Interactive Voice Response*)[143], "Kısa Mesaj Servisi (*SMS – Short Messaging*

---

135 https://www.paypal.com/np/webapps/mpp/pay-with-app#:~:text=PayPal%20is%20accepted%20on%20thousands,financial%20information%20with%20the%20seller.&text=Shop%20online%20or%20in%20apps%20using%20your%20mobile.&text=Choose%20PayPal%20as%20the%20payment%20method. (Gözden Geçirilme Tarihi: 29.10.2020).

136 https://squareup.com/guides/mobile-payments?country_redirection=true (Gözden Geçirilme Tarihi: 29.10.2020).

137 https://www.seamlesspay.com/(Gözden Geçirilme Tarihi: 29.10.2020).

138 https://venmo.com/(Gözden Geçirilme Tarihi: 29.10.2020).

139 https://archive.is/20130124212125/http://gopago.com/live (Gözden Geçirilme Tarihi: 29.10.2020).

140 https://www.dwolla.com/ (Gözden Geçirilme Tarihi: 29.10.2020).

141 *İşler/Gülaç*, s. 63.

142 *İşler/Gülaç*, s. 69.

143 Etkileşimli ses cevaplama teknolojisi (IVR), insan-makine etkileşimine izin veren temel bir teknolojidir. Müşteriler konuşarak veya tuşlama yaparak IVR sistemleriyle etkileşime girerken; IVR sistemleri de önceden kaydedilmiş veya dinamik olarak üretilen ses aracılığıyla müşterilerle etkileşime girerler Bkz. https://www.sestek.com/tr/ivr/ (Gözden Geçirilme Tarihi: 29.10.2020).

Service)", "Kablosuz Erişim Protokolü" (*WAP – Wireless Application Protocol*)[144] ve "Standalone[145]"dur. Günümüzde, özellikle tüketicilerin daha karmaşık mobil hizmetlere olan ihtiyacının güçlü olmamasına rağmen, mobil bankacılık tüketiciler tarafından genel mobil ticari hizmetlere kıyasla daha basit bir uygulama görülmesi sebebiyle tercih edilmektedir[146].

Uzmanlar, mobil bankacılık işlemlerinde siber güvenliğin temini açısından finans sektöründeki tüm kullanıcılarda bilgi güvenliği farkındalığı yaratmanın hayati derecede önem taşıdığını ve özelikle kullanıcılara Android ve iOS işletim sistemlerinin[147] öngördüğü mobil uygulamalar dışında dışarıdan kaynağı bilinmeyen ve zararlı yazılım içerebilecek uygulamalar yüklenmemesi gerektiği ile ilgili eğitimler verilmesinin önem taşıdığını vurgulamıştır[148]. Genel kanı, her ne kadar iOS işletim sisteminin Android'e kıyasla daha güvenilir olduğu yönünde olsa dahi, yakın zamanda

---

[144] Kablosuz uygulama protokolü (WAP), mobil telefonlar, avuç içi bilgisayarlar gibi mobil iletişim araçları üzerinde herhangi bir kabloya bağlanmaksızın hareket halindeyken internet içeriği sağlayan teknolojiyi ifade etmektedir. https://tr.wikipedia.org/wiki/Kablosuz_uygulama_protokolü (Gözden Geçirilme Tarihi: 29.10.2020).

[145] Standalone kelimesi, Türkçe'ye kendi başına çalışan şeklinde tercüme edilebilir. Esas itibariyle, standalone teknolojisi herhangi bir başka bilgisayar gerektirmeden veya herhangi bir cihazın parçası olmaksızın kendi başına çalışabilen teknolojiye verilen isimdir. https://dictionary.cambridge.org/dictionary/english/standalone (Gözden Geçirilme Tarihi: 29.10.2020).

[146] Krassie Petrova, Auckland University of Technology, "Mobile Banking: Background, Services, Adoption" (*"Petrova"*), s.3: https://www.academia.edu/3334874/MOBILE_BANKING_BACKGROUND_SERVICES_AND_ADOPTION?auto=download (Gözden Geçirilme Tarihi: 29.10.2020).

[147] İşletim sistemleri açısından konuya bakıldığında Android işletim sisteminin pazarda en büyük paya sahip olması, kullanıcıların genelde yama yapılmamış eski Android versiyonlarını kullanmaları, bu işletim sisteminin açık kaynak kodlu olması sebebiyle kolaylıkla düzenlebilir bir yapıda olması, Google Play Store'a ilave olarak bilinmeyen kaynaklardan uygulama yüklenmesine izin verilmesi gibi faktörler dikkate alındığında diğer mobil cihaz işletim sistemlerine kıyasla zararlı yazılımlar açısından en riskli işletim sistemi olduğu belirtilmiştir. Buna karşın Apple şirketi tarafından geliştirilen iOS işletim sisteminin en büyük özelliğini Android'in aksine açık kaynak kodlu olmaması sebebiyle uygulama yüklemelerinde Android kadar esnek olmadığı ve bu nedenle Android'e kıyasla iOS açısından siber ataklar noktasında daha etkin önlemler alındığı belirtilmiştir. Bu konuda detaylı bilgi için Bkz. *Özkaya/Sarıca/Durmaz*, s. 96, 97.

[148] *Özkaya/Sarıca/Durmaz*, s. 95 ve bu konuda ayrıntılı bilgi için Bkz. Martín Steven Bedoya Rodríguez, Jhon Hegel Gutiérrez, "An Overview of Cybersecurity for Mobile Banking Applications", (*"Rodríguez/Gutiérrez"*) https://medium.com/@everisUS/an-overview-of-cybersecurity-for-mobile-banking-applications-e4e99dff5061 (Gözden Geçirilme Tarihi: 29.10.2020).

uzmanlar tarafından iPhone ve iPad üzerinde iOS (özellikle iOS 12 ve iOS 13 sürümleri açısından) işletim sisteminde özellikle e-mail uygulamaları açısından güvelik açıkları olduğu belirtilmiştir[149].

İnternet Bankacılığı: İnternet bankacılığı, müşterilerin kendilerine özel müşteri numarası ve şifreleri ile internet üzerinden sisteme giriş yaparak yine müşterilerin sistem tarafından verilen izin ve limitler çerçevesinde belirli işlemleri şubeye gitmeden zamandan ve yerden bağımsız şekilde bankacılık işlemleri yapabilmelerini sağlayan alternatif bir dağıtım kanalı olarak tanımlanabilir[150]. İnternet bankacılığı, başka bir ifade ile internetin olanak sağladığı uzaktan erişim yoluyla bankacılık işlemlerinin (para transferi, hesap hareketlerinin incelenmesi, yatırım işlemleri, ödeme yapılması vb.) yapılabilmesini ifade etmektedir[151].

Bankaların, internet bankacılığı konusundaki tüm önlemlerine rağmen, bilgi güvenliğindeki en zayıf katmanın insan faktörü dikkate alındığında internet bankacılığı açısından da şifre korumadaki özensizliklerden dolayı internet bankacılığındaki en büyük zafiyetin müşteri kaynaklı olduğu görülmektedir[152]. Bunun yanı sıra, internet bankacılığı konusunda yapılan araştırmalar, bankaların bu konuda yeterli güvenlik önlemlerini almadığını, siber güvenlik açısından daha yeni teknolojik olanakların kullanılması gerektiğini, internet bankacılığında yeterli güvenlik önlemlerinin alınmamasının bir sonucu olarak bankaların daha büyük maliyetle ve müşteri güveni kayıplarıyla karşı karşıya kaldığını göstermektedir[153].

---

[149] Zecops Araştırma Grubu, 20.04.2020 Tarihli Raporu (*"Zecops Raporu"*): https://blog.zecops.com/vulnerabilities/youve-got-0-click-mail/ (Gözden Geçirilme Tarihi: 09.05.2020).
[150] *Çakır/ Kılıç*, s. 98.
[151] *Eralp,* s. 6.
[152] *Çakır/Kılıç*, s. 98
[153] *Yeşilyurt*, s. 101.

Elektronik Para: Elektronik para, genel itibariyle internet üzerinden para transferini mümkün kılan ödeme sistemleri olarak tanımlanmakta[154] olup kullanıcıların chip kart vasıtasıyla veya bilgisayara kopyalanarak ödeme yapmasına imkân sağlamaktadır[155]. Elektronik paranın donanım tabanlı ürünler veya yazılım tabanlı uygulamalarla kullanılması mümkündür. Donanım tabanlı ürünlerde (çipli kart vb.) güvenlik öğeleri donanım içerisinde bulundurulmakta ve para transferi, donanım üzerindeki verinin güncellenmesi ile çevrimiçi olma gerekmeksizin gerçekleştirilmektedir. Yazılım tabanlı çözümlerde ise elektronik para ile ödeme işlemi ancak akıllı telefon, tablet veya bilgisayarlar üzerinde kurulu software uygulama ile çevrimiçi olunarak yapılır[156]. Basel Bankacılık Gözetim ve Denetim Komitesi'nin 1998 yılında yaptığı tanıma göre ise, elektronik para ödeme noktası terminalleri yolu ile (POS – Point of Sale) veya iki araç arasında doğrudan veya internette açık bilgisayar ağları üzerinden borçların ödenmesi için depolanmış değer veya önceden ödeme mekanizmasıdır[157].

Dünyada elektronik para konusunda mevzuat açısından, 2000 yılında ilk kez Avrupa Birliği'nde 2000/46/EC Sayılı E-Para Direktifi, 16 Eylül 2009 tarihinde yürürlüğe

---

[154] Elektronik para, Avrupa Komisyonu'nun resmi web sitesinde nakit paraya alternatif olarak dijital ortamda yaratılan internet aracılığıyla veya herhangi bir kart veya mobil cihaza yüklenerek nakit olmaksızın ödeme imkanı veren ödeme sistemi olarak tanımlanmıştır. Elektronik para konusunda Avrupa Birliği tarafından elektronik para hizmetlerinin yeni, inovatif ve güvenilir bir ortamda gerçekleştirilmesinin, yeni kurulan şirketlere elektronik para piyasasına girme fırsatının tanınmasının ve tüm piyasadaki paydaşlara elektronik para konusunda etkin bir rekabet ortamının teşvik edilmesinin amaçladığı belirtilmiştir. Bkz. https://ec.europa.eu/info/business-economy-euro/banking-and-finance/consumer-finance-and-payments/payment-services/e-money_en (Gözden Geçirilme Tarihi: 20.04.2020). Çakır/Kılıç'a göre, elektronik para yatırılmış değer veya satış noktası terminalleri aracılığıyla, iki cihaz arasında doğrudan transferleri veya internet gibi açık bilgisayar ağları üzerinden ödemeleri yapmak için önceden ödenmiş mekanizmalara verilen isimdir. Bkz. *Çakır/Kılıç*, s. 101'de bahsi geçen Kalem.

[155] Bu tanımla ilgili ayrıntılı bilgi için Bkz. *Keser Berber, Elektronik Para,* s. 48'deki 29 no'lu dp.dan: Stolpmann, Markus, Elektronisches Geld im Internet, s.1) ve 30 no'lu dp.da belirtilen Bericht aus Brüssel, Electronic Commerce: Electronisches Geld.

[156] *Çay*, s. 33.

[157] *Bozkurt Yüksel*, *Elektronik Para,* s. 30'daki 57 no'lu dp.dan: Cenan Aykut, "Basel II Standartları".

giren 2009/110/EC Sayılı Direktif ile yürürlükten kaldırılmıştır[158]. 2001 yılında ise EMA[159] denilen Elektronik Para Kurumu İngiltere'de kurulmuştur.

Türkiye'deki mevzuat açısından ise, 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanunun "Tanımlar" başlıklı 3. maddesinin ç bendindeki tanıma göre elektronik para, elektronik para ihraç eden kuruluş tarafından kabul edilen fon karşılığı ihraç edilen, elektronik olarak muhafaza edilen, anılan kanun kapsamında tanımlanan ödeme işlemlerini gerçekleştirmek için kullanılan ve elektronik para ihraç eden kuruluş dışındaki gerçek ve tüzel kişiler tarafından da ödeme aracı olarak kabul edilen parasal değer olarak tanımlanmıştır[160]. 6493 Sayılı Kanun'daki bu tanımın, Türkiye'deki yasa koyucu tarafından Avrupa Birliği mevzuatı dikkate alınarak yapıldığı belirtilmiştir[161].

Elektronik para, aşağıda VI. Bölümde "Elektronik Ödemelerde Siber Güvenliğin Sağlanmasında Yeni Yaklaşımlar: Yenilikler, Vaatler ve Potansiyel Riskler" başlığı altında açıklanan kripto paradan farklı bir kavram olup elektronik para doktrinde Bozkurt Yüksel tarafından, sözleşmedeki para borcunun değeri ile orantılı şekilde elektromanyetik şekilde kaydedilmiş ve kaydeden tarafın sözleşmesel ilişkisine dayalı olarak, transferi sözleşmeye uygun olarak parasal borcun yerine getirilmesi etkisi olan

---

[158] 2009/110/EC Sayılı Direktif'in internet ortamında tam metnine ulaşmak için: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32009L0110 (Gözden Geçirilme Tarihi: 29.10.2020).

[159] İngilizce'de Elektronic Money Association (*"EMA"*) olarak ifade edilmektedir. EMA konusunda ayrıntılı bilgi için Bkz. https://www.e-ma.org/ (Gözden Geçirilme Tarihi: 29.10.2020).

[160] 6493 Sayılı Kanun kapsamında yukarıda belirtilen elektronik para ile ilgili tanıma ulaşmak için bkz. https://www.tcmb.gov.tr/wps/wcm/connect/2f1f7375-31cb-4c3b-b5c6-72d8561140a7/%C3%96deme+Sistemleri+Kanunu+22.11.2019.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE-2f1f7375-31cb-4c3b-b5c6-72d8561140a7-m-JzLp5 (Gözden Geçirilme Tarihi: 29.10.2020).

[161] Doktrinde Bozkurt Yüksel, kanunda belirtilen yukarıdaki tanımın yapılırken 2007/64/EC Sayılı Ödeme Hizmetleri Direktifi, 2009/44/EC Sayılı Direktif ile değişik 1998/26/EC Sayılı Ödeme Ve Menkul Kıymet Mutabakat Sistemlerinde Mutabakatın Nihailiği Direkifi ile 2009/110/EC Sayılı Elektronik Paraların Kurulması, Faaliyetlerinin Sürdürülmesi, Denetimi Direktifi'nin dikkate alındığına dikkat çekilmiştir. Bkz. *Bozkurt Yüksel*, *Elektronik Para*, s. 34'de 68 no'lu dp.dan aktarılan: 6493 Sayılı Kanun, Genel Gerekçesi.

bir veri topluluğu olarak devletlerin Merkez Bankaları tarafından ihraç edilen ve piyasada tedavül edilen, karşılığı fiziksel para olan dijital veriler olarak tanımlanmıştır[162]. Buna karşın kripto paralar ise aşağıda detaylı şekilde açıklanacağı üzere blokzincir teknolojisinin bir ürünü olarak dağıtık veri tabanı teknolojisine bağlı olarak çalışan ve herhangi bir merkezi otoritenin varlığına ihtiyaç duyulmaksızın piyasaya tedavül edilebilen bir dijital para birimidir[163]. Elektronik paranın üç uygulama şekli olduğu belirtilmiştir[164]: i) Kişilerin bankalardaki mevduat hesabına bağlı olan, ATM[165]'lerden para çekilmesini sağlayan, POS makinelerinde ödeme yapılmasını sağlayan ve internette alışveriş yapılmasını sağlayan *debit kartlar*. ii) en gelişmiş versiyonu akıllı kartlar olan, önceden karta yüklenmiş değerle satın alma işlemi yapmayı sağlayan değeri *depolanmış kartlar* (örnek vermek

[162] *Keser Berber*, s. 48.

[163] Şahin Çetinkaya, Kripto Paraların Gelişimi Ve Para Piyasalarındaki Yerinin Swot Analizi İle İncelenmesi, Uluslararası Ekonomi Ve Siyaset Bilimleri Araştırmalar Dergisi – C:2 S: 5 Yıl: 2-2018, (*"Çetinkaya"*) s. 13 https://dergipark.org.tr/en/download/article-file/619560 (Gözden Geçirme Tarihi: 29.10.2020).

[164] Yukarıda belirtilen elektronik para uygulama çeşitleri doktrinde *Bozkurt Yüksel (Elektronik Para)*, s. 45-46'dan aktarılarak özetlenmiştir. Yukarıda yer verilen üç tür elektronik paranın sadece uygulama şekline ilişkin olup Bozkurt Yüksel tarafından elektronik para şu şekilde sınıflandırılmıştır: (i) Kullanım Amacına Göre Sistemler, (ii) Bakiye Ve Banknot Tabanlı Sistemler, (iii) Kart Tabanlı Ve Ağ Tabanlı Sistemler, (iv) Kapalı Ve Açık Dolaşımlı Sistemler, (v) Tek Çıkarıcılı Ve Çok Çıkarıcılı Sistemler. Cenk Çavuşoğlu ise, "Elektronik Paranın Gelişimi Ve Merkez Bankası Bilançosu İle Para Politikası Uygulamaları Üzerine Etkisi" başlıklı Uzmanlık Yeterlilik Tezi'nde, elektronik paranın sistemin işletildiği ortama göre, çıkarılma yöntemine göre ve elektronik parayı ihraç eden kuruluşun türüne göre farklı sınıflandırmalara tabi olacağını belirtmiştir. Çavuş'un belirttiği ayrıma göre sistemin işletildiği ortama göre kart tabanlı elektronik para araçları ve yazılım tabanlı elektronik para araçları olarak iki geniş kategoriye ayrılmaktadır. İhraç edilen kuruluşun türüne göre ise, elektronik para, merkez bankaları tarafından ihraç edilen elektronik para, bankalar tarafından ihraç edilen elektronik para, elektronik para kuruluşları tarafından ihraç edilen elektronik para, kıyı ötesi kuruluşlar tarafından ihraç edilen elektronik para gibi ayrımlara tutulmaktadır. Son olarak yazar tarafından elektronik paranın, ihraç edilme yöntemine göre ise merkez bankası parası karşılığında ihraç edilen elektronik para ve bağımsız para birimi olarak ihraç edilen elektronik para gibi farklı kategorilere tabi tutulmaktadır. Bkz. Cenk Çavuşoğlu, "Elektronik Paranın Gelişimi Ve Merkez Bankası Bilançosu Ve Para Politikası Uygulamaları Üzerine Etkisi", Uzmanlık Yeterlilik Tezi, T.C. Merkez Bankası Muhasebe Genel Müdürlüğü, Ankara, Haziran, 2015, (*"Çavuşoğlu"*) s. 26-34, teze ulaşmak için: https://tcmb.gov.tr/wps/wcm/connect/1cb8e855-0840-4425-9f48-3b91a1deaac5/CenkCavusoglu.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE1cb8e855-0840-4425-9f48-3b91a1deaac5 (Gözden Geçirilme Tarihi: 29.10.2020).

[165] ATM (İngilizce'de "Automated Teller Machine" sözcüklerinin kısaltmasıdır), bankaların müşterilerine para ödeme, ekstre basma, para yatırma, para transferi, fatura ödeme gibi farklı bankacılık hizmetlerini kullanmasını sağlayan bir dağıtım kanalıdır.

gerekirse tüketicilerin görüşme yapmadan önce ödeme yaparak kontör yükledikleri telefon kartları) ve iii) günlük hayatta birçok çeşidi olan E-cash, CyberCash, Netcash, Mondex, GeldKarte, Proton, Netchex, Mini-Pay, Millicent gibi *elektronik nakit (e-cash)*[166].

Doktrinde Bozkurt Yüksel'e göre, elektronik para ile ilgili siber güvenlik noktasındaki endişeler özellikle elektronik paranın kara para aklama gibi yasa dışı faaliyetler ve vergilendirmede yaşanabilecek sorunlarda artışa sebebiyet verebileceği gibi özellikle çifte harcama gibi problemlere yöneliktir. Dolayısıyla, elektronik paranın sistemde takibinin zor olabileceği belirtilmekle beraber çifte harcama konusunda ise elektronik paranın kopyalanması ve birden fazla kez kullanılmasının mümkün olduğu, çifte imzanın önlenmesi açısından ise açık anahtar kriptografisi ve gizli ayırma (*secret splitting*)[167] denilen yöntemlerle mümkün olacağı ileri sürülmektedir[168]. Elektronik para olgusu, siber güvenlik açısından analiz edildiğinde ise, her ne kadar yukarıda belirtilen ve doktrince yöneltilen endişelerde haklılık payı olsa dahi, yazar tarafından özellikle elektronik paranın aslında merkez bankası tarafından tedavül edilen kağıt paranın dijital bir yansıması olması sebebiyle aşağıda ayrıntılı şekilde açıklanacağı üzere kripto paralara kıyasla özellikle teknik açıdan siber güvenlik risklerinin daha rahat takip edilebileceği ve yukarıda belirtilen kriptografik yöntemler ve gizli ayırma

[166] Elektronik nakit çeşitleri konusunda detaylı bilgi için Bkz. Bozkurt Yüksel, s. 53. Doktrinde, Keser Berber ise elektronik nakit kavramını bu değer birimlerini rekabet parası formunda ve bir çok defa kullanım olanağı ile birlikte yaratmak isteyen, banka statüsünde olmayan kurumların çıkardığı özel "dijital cash sistemleri" olarak tanımlamakta ve bu konuda en bilinen e-para birimlerine örnek olarak Netcash, Ecash, Cybercash, Cybercoin, CheckFree, Mondex, Netchex, Millicent, Mini-Pay, Open Market, SG 2-Payline gibi para birimlerini örnek göstermektedir. Bkz. *Keser Berber*, *Elektronik Para,* s. 58-80.

[167] Gizli ayırma (secret splitting), parola ve şifre gibi bir gizlilik unsurunun bu gizlilikten menfaati olacak kişiler arasında bazı parçalara ayrılarak paylaşılmasını ifade etmektedir. Örnek vermek gerekirse, söz konusu gizlilik unsuru, bu gizlilikten yararlanacak kişilerce bir rakam dizini olabilir ve bu rakamlar ilgili grup üyelerine parça parça verilir. Bu sayede her kişinin sahip olduğu rakam tek başına bir anlam ifade etmemekle beraber ancak grup üyelerinin doğru bir kambinasyonla bu rakam dizinine ulaşılması doğru şifre ve parolaya ulaşılmasını sağlayacaktır. Bu konuda detaylı bilgi için bkz. Adi Shamir, "How to Share a Secret" (*"Shamir"*), s. 612-613: https://cs.jhu.edu/~sdoshi/crypto/papers/shamirturing.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[168] *Bozkurt Yüksel, Elektronik Para*, s. 57'de 128 no'lu dp.da belirtilen Clifford/Gennady.

gibi teknik açıdan alınabilecek tedbirler ile siber güvenliğin bir noktaya kadar temin edilmesinin mümkün olabileceği sonucuna ulaşılmıştır.

Elektronik Çek: Özü itibariyle kâğıt çekin dijital ortama aktarılmasını ifade eden dijital çek uygulamasından tamamen farklı olarak elektronik bir altyapı sayesinde kağıt çek ile ilgili ticaret hayatında gerçekleştirilen tüm işlemlerin elektronik ortamda gerçekleştirilmesini ifade etmektedir. Başka bir ifade ile, elektronik çek, e-ticaret gerçekleştiren sitelerin ödemeleri çek olarak kabul etmelerini ve işleyebilmelerini sağlayan bir ödeme sistemidir[169]. Normal çekte nasıl imza atılıyor ise elektronik çek uygulamasının esasını, müşterinin dijital imzası ile imzalaması oluşturmaktadır[170]. Elektronik çek sisteminde, müşterinin bir bankada hesabının olması gereklidir ve ödemeler kredi kartına ihtiyaç duyulmaksızın banka hesabı bilgilerinin elektronik ticaret sitesine girilmesi yoluyla yapılır. Müşteri, internet üzerinden sipariş vererek daha sonrasında bir elektronik çeki düzenleyip dijital imza ile imzalayarak satıcıya iletir. Satıcı ise bunu kendi bankası üzerinden hesabına alacak olarak kaydeder. Başka bir ifade ile, müşteri bir anlamda ticaret sitesine elektronik ortamda çek keserek ödeme yapmış olur. Bankalar, elektronik çekle kapsamında yapılan transferleri ve hesapta alışverişin tamamlanması için gerekli şartların yeterli olup olmadığını kontrol ederler ve bu hususla ilgili olarak e-ticaret sitesini şifreli kanallarla haberdar ederler.

Doktrinde Karabıyık tarafından elektronik çekin kullanılması kolay bir sistem olmakla birlikte, daha yaygın kullanımı için gerekli sistemlerin finans sektörü tarafından kabul görmesinin gerekli olduğu belirtilmiştir[171]. Ayrıca anılan yazar tarafından elektronik çekin genel anlamda, güvenli bir veri denetimi ve yönetimi sağlaması[172], birçok

---

[169] Ayşegül Karabıyık, "Alternatif Ödeme Aracı Olarak: Elektronik Çek Sistemi (E-Çek)-1, ("*Karabıyık")*, s. 81, ilgili makaleye ulaşmak için: https://dergipark.org.tr/tr/download/article-file/426470 (Gözden Geçirilme Tarihi: 29.10.2020) .

[170] *Keser Berber*, s. 53.

[171] *Karabıyık*, s. 82.

[172] Kağıt çeklerde klonlama olarak belirtilen bir yöntemle bir çekten birkaç çek üretebilme ve aynı zamanda kağıt çekin kaybolma ve çalınma ihtimali söz konusu iken elektronik çekin gelişen güvenlik uygulamaları ile tüm bahsi geçen riskleri ortadan kaldıracağı ve kullanıcı için son derece güvenli bir veri denetim ve yönetimi sağladığı üzerinde durulmaktadır. Bu konuda detaylı bilgi için Bkz. Alpay Geze,

suiistimali önlemesi[173], karar süreçlerini hızlandırması, kredi riskini ve işlem maliyetlerini azaltması[174], otomatik kredi kararı ile müşteri analizlerini birleştirmesi, sistemlerin bakım maliyetlerini azaltması, müşteri memnuniyetini geliştirmesi, iletişim güvenliğini ve hızını artırması gibi avantajlarının olduğu belirtilmiştir[175].

Elektronik çeke örnek olarak Netcheque[176] ve elektronik ortamda çek benzeri diğer ödeme sistemleri ise Online Check[177], Netbill[178], Netchex[179] ve Check Free[180], verilebilir[181].

Türkiye'de mevzuat açısından 6102 Sayılı Türk Ticaret Kanunu m. 1526/f. 1'de[182] poliçe, bono, çek, makbuz senedi, varant ve kambiyo senetlerine benzeyen senetlerin güvenli elektronik imza ile düzenlenemeyeceği düzenlenmektedir. Buna karşın, güncel bir gelişme olarak Ticaret Bakanlığı ve Kredi Kayıt Bürosu tarafından hazırlanan ve

---

"EÇT (Elektronik Çek Transferi) Sisteminin Tanıtımı ve Gerekliliği", (*"Geze"*) ilgili makaleye elektronik ortamda aşağıdaki link üzerinden ulaşılabilir: https://www.academia.edu/27812943/EÇT_Elektronik_Çek_Transferi_SİSTEMİNİN_TANITIMI_VE_GEREKLİLİĞİ_Elektronik_Çek_Elektronik_Çek_Transferi_Online_Çek_Online_Çek_Transferi_EÇT_Nedir, s. 2 Gözden Geçirme Tarihi: 29.10.2020) Elektronik çek sisteminin Türk Bankacılık Sektöründe uygulanmasıyla %3 seviyelerinde takip eden karşılıksız çek oranlarının ortadan kalkabileceği, ayrıca KOBİ'ler tarafından düzenlenen çekler olmak üzere tüm çeklerin sistem içinde güvenilir olmasının sağlanacağı, bankaların elektronik çeki hızlı ve efektif olarak uygulanabilmesini sağlayan dünya çapındaki teknolojilere sahip olması nedeniyle kredi ve banka kartlarına alternatif bir ödeme aracı olarak piyasaya sunulabileceği düşünülmüştür. Bkz. *Karabıyık*, s. 89.

[173] *Karabıyık,* s. 90

[174] Elektronik çeklerin, sürekli işlem maliyetlerini ve çek ödemelerinden doğan kayıpları önemli oranda azaltacağı, e-çeklerin en yaygın iletişim araçlarından birisi olan internet ortamında kullanıldığı ve böylece kağıt çekler için gerekli olan birçok manuel adıma gerek duyulmayacağı düşünülmektedir. Bkz. s.89. Özellikle, Elektronik Çek Transferi (*"EÇT"*) adı altında oluşturulacak sistemde yeni bir algoritma oluşturulmasına gerek kalmadan para transferlerinin ve çeklerin ciro edilmesinin IBAN üzerinden sağlanmasının, yanlış hesap numarasına para transferi yapılmasını önleyeceği, para transferlerinin hızı ile kalitesini artıracağı ve bankaların operasyonel maliyetlerinde ciddi sebep olacağı üzerinde durulmaktadır. Bkz. *Geze*, s. 3.

[175] *Karabıyık*, s. 86.

[176] http://www.netcheque.org/gost.info/netcheque (Gözden Geçirilme Tarihi: 29.10.2020)

[177] http://www.onlinecheck.com/mag.html (Gözden Geçirilme Tarihi: 29.10.2020)

[178] http://www.netbill.com (Gözden Geçirilme Tarihi: 29.10.2020).

[179] http://www.netchex.com (Gözden Geçirilme Tarihi: 29.10.2020).

[180] http://www.check-free.com (Gözden Geçirilme Tarihi: 29.10.2020).

[181] Elektronik çekle ilgili örnekler konusunda Bkz. *Keser Berber*, *Elektronik Para,* s. 54.

[182] https://mevzuat.gov.tr/mevzuat?MevzuatNo=6102&MevzuatTur=1&MevzuatTertip=5 (Gözden Geçirilme Tarihi: 29.10.2020).

ilgili kamu kurum ve kuruluşlarının da görüşleri alınarak nihai hale getirilen ve alt metin çalışmaları devam eden Elektronik Çek ve Bono Kanunu taslağının bu yıl yürürlüğe girmesi beklenmektedir. İlgili kanun taslağının Türkiye'de çek ve bonoların elektronik ortamda işlem görmesine imkân veren Elektronik Çek ve Bono Sistemi ile piyasaya tedavül edilen e-çeklerin bankalar ve diğer elektronik kuruluşlar tarafından teyit edileceği ve böylelikle çekin sahtesinin ve klonlanmış kopyasının engelleneceği belirtilmiştir[183]. Bu düzenlemenin yürürlüğe girmesi halinde yasa koyucu tarafından TTK m. 1526/f. 1'deki yasağın da Türkiye'deki elektronik çek sistemine uyumlu hale getirileceği öngörülmektedir. Özellikle, Türkiye'de e-çek uygulamasının yürürlüğe girmesi halinde elektronik çek sistemini işletilecek kurumların, dünya çapında kabul görmüş teknoloji, güvenlik ve iletişim altyapılarının eş değer biçimde güçlendirilmesi gerektiği, siber güvenliğin e-çek sisteminde sağlanabilmesi açısından çek işlemleri yapılırken lisansız cihazların kullanılmaması, sistemde kaydı olan veya yeni kayıt açtıracak olan kişiler açısından kolay ve tahmin edilebilir şifreler yerine güçlü parola yönetiminin tercih edilmesi ve sanal ortamda veya telefon üzerinden gerçekleştirilecek sosyal mühendislik saldırılarına karşı dikkatli olunması gerektiği vurgulanmıştır[184].

İKİNCİ BÖLÜM

ELEKTRONİK ÖDEMELERE YÖNELTİLEN SİBER SALDIRI YÖNTEMLERİ

Boston Consulting Group (*"BCG"*)'nın raporuna göre diğer sektörlere kıyasla bankacılık ve finans sektöründe üç yüz kat daha fazla siber saldırı

[183] İlgili haber konusunda Bkz. https://katilimfinansdergisi.com.tr/yeni-elektronik-cek-kanunu-neler-getiriyor/ (Gözden Geçirilme Tarihi: 29.10.2020)

[184] https://www.katilimfinans.com.tr/yeni-elektronik-cek-kanunu-neler-getiriyor/ (Gözden Geçirilme Tarihi: 29.10.2020).

gerçekleştirilmektedir[185]. Hiç kuşkusuz, bunun en önemli sebeplerinden birisi finans sektöründe siber saldırganların özellikle ele geçirmeyi hedefledikleri kritik düzeyde değerli kişisel ve finansal bilgiler bulunmaktadır[186]. Bankalar gibi finansal kurumların siber saldırılar karşısında diğer kurumlara kıyasla daha kırılgan ve zayıf olabilmelerinin sebeplerinden birisi, bu tarz kurumların geniş organizasyonel yapılara sahip olması (bir bankanın binlerce şubesi ve çalışanı olması gibi) ve siber güvenlik yönetim sürecinin tüm organizasyon çatışı altında yeknesak şekilde uygulanmasında ve önlemlerin alınmasındaki zorluktur[187]. Öte yandan, blokzincir teknolojisi bakımından yaşanan gelişmeler, 5G, IoT denilen "nesnelerin interneti"nin her geçen gün hayatımıza daha da girmesi ve finans sektörünün yeni teknolojilere açık bir alan olması da siber saldırganların daha yaratıcı yöntemlerle saldırı yapmasına imkân sağlamaktadır. Ancak, finans kuruluşları ve bankalar nezdinde yaşanan siber saldırılar

---

185 https://medium.com/@kratikal/cyber-attacks-are-the-biggest-risk-to-the-financial-sector-c862b8ffd123 (Gözden Geçirilme Tarihi: 29.10.2020).

186 Scott Berinato ve Matt Perry tarafından hazırlanan "Rakamlarla Güvenlik Trendleri" isimli makalede kullanıcı bilgileri ve kredi kartı verilerini korumak için yapılan onlarca çalışmaya karşın siber saldırganlar tarafından en sık ele geçirilen varlıklar bunlardır. Berinato/Perry, 2018 yılındaki Verizon şirketinin "Veri İhlali Soruşturma Raporu"ndan hareketle farklı sektörlere yönelik şu örnekleri vermiştir: 2018 yılında finans ve sigorta sektörü açısından çalınan verilerin % 36'sı kişisel verilerdir, konaklama ve gıda sektöründe çalınan tüm verilerin % 93'ü ödeme bilgilerine ilişkindir, benzer şekilde parekendecilik sektöründe ise çalınan bilgilerin % 73'ü ödeme bilgileridir. Bkz. Scott Berinato/Matt Perry, "Rakamlarla Güvenlik Tespitleri", Harvard Business Review Press, Dijital Dönüşüm Siber Güvenlik, Optimist, 1. Baskı, Ocak 2020, (*"Berinato/Perry"*) s. 49.

187 Berinato/Perry, 2018 yılına ilişkin başta finans, eğitim, konaklama, sağlık hizmetleri sektörleri olmak üzere farklı siber saldırı türlerine ilişkin siber saldırı türleri ve saldırıların sayıları konusunda ayrıntılı analizlere yer verilmiştir. İlgili makalede, yazarlar tarafından siber güvenlik noktasında ayrıntılı yer verilen tablolar çerçevesinde özellikle finans sektörü konusunda şu tespitleri dikkat çekicidir: Tıp, konaklama ve gıda gibi sektörler çok büyük ölçüde tek enformasyon türünü içerecek ihlallerle karşılaştığı için zaman içerisinde siber saldırılara karşı bu sektördeki firmalar istedikleri takdirde savunmalarını keskinleştirebilir. Oysaki finans sektörü bu sektörlerden farklı olarak genelde ihlallerin çoğunlukla tek bir hedef üzerinde toplanmadığı ve siber güvenlik konusunda birkaç cephede birden savaşmayı gerektirdiği için özellikle finans sektörü daha esnek bir risk azaltma stratejisine ihtiyaç duymaktadır. İlgili makalede, bir başka dikkat çekici tespit ise, 2017 yılı açısından (Accenture ve Ponemon Enstitüsü, "2017 Siber Suçların Maliyeti Araştırması: Fark Yaratan Güvenlik Yatırımlarına İlişkin İçgörüler) dünya çapında sektörler bazında yıllara dağıtılmış ortalama siber suç maliyeti açısından en yüksek maliyete sahip sektörün finans sektörü olduğunu belirtmiştir. Bu konuda detaylı bilgi için Bkz. *Berinato/ Perry*, s. 50, 54.

sadece bu kuruluşlar açısından salt finansal kayıp yaratmamakta, daha önemlisi müşterileri nezdinde itibar kaybına da sebebiyet vermektedir.

Siber saldırıların sektörel açıdan ciddiyetine dikkat çekmek adına, aşağıda bankalar ve finans sektöründe yaşanan siber saldırılar konusunda istatiksel açıdan da değerlendirebilecek birtakım farklı analizlere yer verilmiştir:

Juniper Research denilen araştırma şirketinin 30.03.2020 tarihli raporuna göre, AB'de yukarıda belirtilen SCA sistemine rağmen online ödemelerdeki dolandırıcılık nedeniyle İngiltere'de 2020 yılında 17 milyar Dolar meblağındaki zararın 2024 yılına gelindiğinde 25 milyar Dolar'a çıkması beklenmektedir. Araştırma şirketine göre, 2020 yılına kıyasla 2024 yılında online ödemeler açısından öngörülen bu zararın dört yıl içerisinde toplamda %52 oranında artacağına işaret etmektedir[188].

BBC, İngiltere'de bankalarda siber güvenlik saldırılarının 2017 yılında 69 adet iken, 2018 yılında bu sayının 819'a çıktığını rapor etmiştir (Başka bir ifade ile bu oran %1000'den daha fazla bir artışa işaret etmektedir).

Forbes'un haberine göre ise, ABD'li şirketlerde diğer sektördeki herhangi bir şirketin siber saldırıya maruz kalması halinde bunun şirkete ortalama maliyeti 12 milyon Amerikan Doları iken, herhangi bir finans şirketinde bu saldırının maliyeti yaklaşık 18 milyon Dolardır. Öte yandan, ABD'de diğer tüm sektörler açısından yılda yaklaşık dört milyon civarında siber atak gerçekleştirilirken ABD'deki finans kuruluşlarında ise siber atak sayısı yılda bir milyarı bulmaktadır[189].

Çalışmanın bu bölümünde özellikle elektronik ödemelerde sıklıkla karşılaşılan siber saldırı vektörlerinin neler olduğu sorusuna cevap aranarak bu konuda ayrıntılı teknik birtakım analizlere (siber saldırılar noktasında olası saldırı türleri bazı görsellerle de

[188] https://www.juniperresearch.com/press/press-releases/ecommerce-losses-to-online-payment-fraud-to-exceed (Gözden Geçirilme Tarihi: 29.10.2020).

[189] https://www.forbes.com/sites/bhaktimirchandani/2018/08/28/laughing-all-the-way-to-the-bank-cybercriminals-targeting-us-financial-institutions/#67c103646e90 (Gözden Geçirilme Tarihi: 29.10.2020).

netleştirilmeye çalışılacaktır) yer verilmiştir. Bu bağlamda, bu başlık altında özellikle aşağıda da görüleceği üzere elektronik ödeme sistemlerine yöneltilen ve uygulamada sıklıkla karşılaşılan dokuz saldırı tipi aşağıda özellikle teknik boyutlarıyla irdelenmiştir:

(i) Kartlı ödeme sistemlerine yöneltilen siber saldırılar

(ii) Elektronik ödemelerde oltalama (phishing) saldırıları

(iii) Bankacılık ve finans sektörüne yöneltilen sosyal mühendislik saldırıları

(iv) SWIFT sistemine yönelik siber saldırılar

(v) Zararlı yazılımlar ve bunların elektronik ödemelerdeki yansıması

(vi) Finans sektöründe DDoS ve Botnetler gibi ağlara yönelik gerçekleştirilen saldırılar

(vii) Kripto paralara yönelik siber saldırılar

(viii) APT denilen "Sürekli Gelişmiş Saldırı"

(ix) Mobil bankacılığa ve internet bankacılığına yönelik siber saldırılar

Bu bölümde anılan saldırı türleri konusunda özellikle bankacılık ve finans sektörüne yönelik ayrıtılı birtakım değerlendirmeler yapılarak kimi zaman sektörde bu saldırılarla ilgili yaşanan somut olgular tablolar ve ayrıntılı analizler çerçevesinde ele alınmış, kimi zaman ise konunun anlaşılabilmesi açısından genel birtakım değerlendirilmelerin (örneğin bankacılık truva atlarının açıklanmasından önce zararlı yazılım türleri olarak virüs, solucan, truva atı, casus yazılımlar vb. konulardaki açıklamalar) yer verilmesinde fayda görülmüştür.

2.1. KARTLI ÖDEME SİSTEMLERİNE YÖNELİK SİBER SALDIRILAR

İlk bölümde kredi kartları ve debit kartlar ile ATM'lere yönelik genel birtakım açıklamalar yapılarak konunun siber güvenlik boyutu fazla detaya girilmeksizin genel hatlarıyla açıklanmıştı. Bu bölümde ise, ATM dolandırıcılıkları, kart kopyalama, aparat

yerleştirmek suretiyle gerçekleştirilen dolandırıcılık yöntemleri gibi uygulamada kartlı ödemelere yönelik sık karşılaşılan saldırı yöntemleri ele alınacaktır.

2.1.1. ATM Dolandırıcılıkları

Günümüzde özellikle elektronik ödemeler de dâhil olmak üzere birçok bankacılık işleminin ATM'ler aracılığıyla yapılması sebebiyle, dolandırıcılar tarafından ATM'lere yönelik birçok farklı dolandırıcılık yöntemi gelişmiştir. Bunlardan bazıları, ATM'ye kart sıkıştırma, para sıkıştırma ATM aracılığıyla kart kopyalama, ATM'ye zararlı yazılım yükleme gibi muhtelif ATM dolandırıcılığı yöntemleri aşağıda somut örnekler ışığında incelenecektir:

2.1.2. ATM'ye Kart, Kâğıt Para Veya Aparat Sıkıştırma

ATM'ler açısından bilinen en eski ve kolay bir yöntem olması sebebiyle geçmişten bugüne kadar dolandırıcılar tarafından ATM'deki kart okuyucu bölmesine kart, yapışkan madde içerikli kâğıt veya yabancı herhangi bir madde sıkıştırmak suretiyle ATM'deki bankamatik kartının çıkışını engellemektedir[190]. İlk aşamada, ATM'deki okuyucu bölmesine herhangi bir yabancı madde sıkıştırıldığını bilmeyen kurban, bankamatik kartını ATM'ye yerleştirdikten sonra kartı sıkışır. Bunun üzerine ise, dolandırıcı ekibinden birisi kurbanın yanına gelerek yardımcı olmak istediğini belirterek kurbana şifre girmesi için yönlendirir. Bu esnada ise genelde ATM'ye yerleştirilen gizli bir kamera veya kurbanın parola girdiği esnada fark etmediği başka bir dolandırıcılık şebekesinin üyesi tarafından kurbanın şifresi görülür. Genelde, kurbanın yanındaki dolandırıcılık şebekesi üyesi kurbanın bankayı telefonla arayarak kartı iptal etmesini engellemek için kendi doğrudan şebeke üyelerinden birini arayarak bu kişiyi banka görevlisi olduğunu söyler. Böylelikle gerçekten bankamatik kartının iptal edildiğini zanneden kurban, ATM'yi terk ettiğinde ise bu fırsatı gören dolandırıcılık şebekesi okuyucu bölmesine sıkışan kartı bir apart vasıtasıyla kolayca

[190] *TBB*, s. 59 ve *Eralp*, s. 81.

çekip alır ve bankamatik şifresini tekrar ATM'de girerek bu sefer kurbanın hesabından para çekme işlemini gerçekleştirmiş olacaktır. Aşağıda ATM'lerde para sıkıştırma konusunda dolandırıcıların kullandığı farklı aparatların görseli yer almaktadır. Şekil-2.1'de, görüldüğü gibi tamamen sıkışan bankamatik kartını ATM'den almayı sağlayan bir aparattır[191].

Şekil-2.1: Sıkışan Kartı Almayı Sağlayan Aparat

Aşağıda görülen Şekil-2.2'de ise, aşağıda görseli bulunan aparat vasıtasıyla ön yüzü para verme haznesinin ön kapağına benzeyen arka kısmında ise bir yapışkan bant ile kurbanların çekmek istedikleri tutarı ele geçirmeye çalışmaktadır. Bu aparat vasıtasıyla sıkışan para bu aparat ile dolandırıcılar tarafından çekilmektedir[192].

Şekil-2.2: Yapışkan Bantlı Aparat

[191] Şekil-2.1 ve açıklamalar konusunda bkz. *TBB*, s. 60 vd.
[192] Şekil-2.2'de yer alan para sıkıştırma için kullanılan aparat konusundaki görsel *TBB*, s. 60'dan alınmıştır.

2.1.3. ATM'ye Zararlı Yazılım Yüklenmesi

ATM'ler de aslında birer bilgisayar programı içeriğine sahip olmaları nedeniyle dolandırıcılar tarafından dolandırıcılar tarafından ATM'nin bilgisayar sistemine yüklenen zararlı yazılım vasıtasıyla ATM kasasındaki tüm para çekilebilmektedir. Bu zararlı yazılımların en yaygın bilineni "Tyupkin"dir[193]. Zararlı yazılım türleri ve bu yazılımların genel çalışma prensipleri aşağıda detaylı şekilde açıklanmıştır[194].

2.1.4. ATM Aracılığıyla Kart Kopyalama

En popüler ATM dolandırıcılığı yöntemlerinden bir diğeri ise, genelde "skimmer"[195] denilen kart okuyucu cihaz ile kurbana ilişkin kart bilgileri dolandırıcılar tarafından ele geçirilmektedir. Doktrinde Eralp[196] bu konuda iki yöntem olduğunu belirtmektedir: İlk yöntem olarak siber saldırganlar tarafından banka kartının aslı kurbanın kendisinde kalmasına rağmen, banka kartının manyetik alan bilgileri kopyalamaktadır. Saldırganlar aslında "skimmer" denilen ve aşağıda görseli yer alan kart okuyucu aparat ATM'deki kart okuyucu bölmenin ön kısmına monte edilerek kurbanın ATM'de işlem gerçekleştirmesi sırasında kartın manyetik alanı ile ilgili tüm bilgileri ele

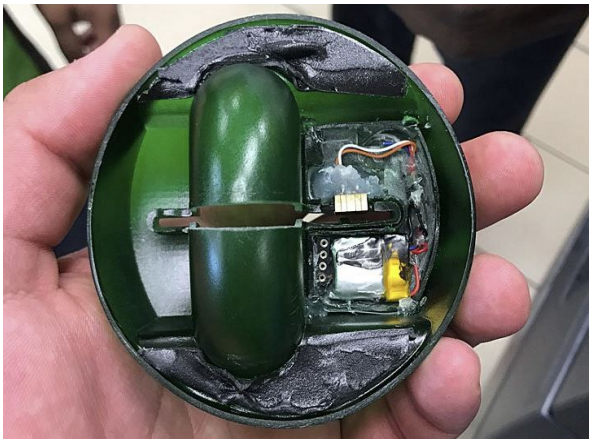
[193] *TBB*, s. 61. Ayrıca, "Tyupkin" zararlı yazılımı ile ilgili detaylı bilgi için Bkz. https://securelist.com/tyupkin-manipulating-atm-machines-with-malware/66988/ (Gözden Geçirilme Tarihi: 29.10.2020).

[194] Bkz. çalışmanın 2.5 numaralı "Zararlı Yazılımların Bankacılık Ve Finans Sektörüne Olası Etkileri" başlığı altında yer alan değerlendirmeler.

[195] "Skimmer" cihazları konusunda detaylı bilgi için Bkz. Nolen Skaife/Christian Peeters/Patrick Traynor, "Fear the Reaper: Characterization and Fast Detection of Card Skimmers", (*"Skaife/Peeters/Trayonor"*), Usenix, s. 1, 2: https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-scaife.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[196] *Eralp*, s.82-83.

geçirmektedir. Tek bir skimmer vasıtasıyla yaklaşık 200'e yakın bankamatik kartının kopyalanabildiği bilinmekte[197] olup görseli aşağıda Şekil-2.3'de gösterilmiştir[198].



Şekil-2.3: Skimmer

Şekil-2.4[199] olarak gösterilen aşağıdaki görselde ise, ATM klavyesi üzerine yerleştirilen bir klavye vasıtasıyla kart bilgilerinin saldırganlar tarafından ele geçirildiği görülmektedir.

[197] Nana Kwame Gyamfi/Mustapha Adamu Mohammed/Kwaku Nuamah-Gyambra/Ferdinand Katsriku/Jamal-Deen Abdulah "Enhancing the Security Features of Automated Teller Machines (ATMs): A Ghanaian Perspective", International Journal of Applied Science and Tecnology, C:2, S:1, Şubat 2016, (*"Gyamfi ve Diğerleri"*), s. 104: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/15.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[198] Şekil-2.3'de belirtilen görsel için bkz. https://www.u1cu.org/Online_Security_Articles_613.html?article_id=91

[199] http://sureswipewirelesscardmachines.blogspot.com/2014/04/how-to-avoid-credit-card-skimming.html (Gözden Geçirilme Tarihi: 29.10.2020).

Şekil-2.4: ATM Klavye Aparatı

2.1.5. Kart Dolandırıcılıkları

Uygulamada kartlar üzerinde (kredi kartı ve debit kartlar) açısından çok farklı çeşitte kart dolandırıcılıkları görülmektedir. Bu konuda en yaygın şekilde rastlanan dolandırıcılık yöntemlerinden bazıları şu şekildedir:

2.5.1.1. Kart Kopyalama (Skimming): ATM ile ilgili yukarıda yer verdiğimiz açıklamalarla benzer şekilde, dolandırıcılar tarafından bu kez ATM'ler yerine kart çekim cihazları üzerinde yukarıda belirtilen "skimmer" denilen özel bir kart okuma cihazı vasıtasıyla kredi veya debit kartların manyetik alan bilgileri başka kartlara kopyalanabilmektedir. Genelde bu yöntemle gerçekleştirilen kart dolandırıcılıklarında, dolandırıcı şebekenin üyeleri sahte belgelerle açılmış bir işyeri veya sahte bir kimlik kullanarak alışverişlerini bu konudan habersiz işyerlerinde gerçekleştirir. Debit kartların manyetik bilgilerinin kopyalanması halinde ise herhangi bir ATM'den müşteri hesabı üzerinden para çekilmesi veya harcama yapılması mümkündür[200].

[200] *TBB*, s. 62-65, Eralp, s. 90-92.

Aşağıda skimmer denilen cihazlar ve "White Plastic" denilen kartların kopyalandıkları boş kartlara ilişkin birtakım görsellere[201] yer verilmiştir.

Şekil-2.5: White Plastic (Kopya Kart)

2.5.1.2. Kart Hesabını Ele Geçirme (Account Takeover): Bu yöntemde, dolandırıcılar tarafından kartla işlem yapabilmek açısından gerekli asgari bilgiler ele geçilerek kullanıcının kredi kartı limiti veya karta bağlı hesap bakiyesi boşaltılır[202]. Terminolojik olarak "account over" deilen bu yöntemle kart hamili bilgileri ile ele geçirilen bilgiler sayesinde müşteri adına yeni ürün başvurusu, ek kart çıkarma gibi amaçlar için de kullanılabileceği belirtilmiştir[203].

2.5.1.3. POS Kaynaklı Kart Kopyalama: Yukarıda belirtilen "skimmer" cihazı ile yapılan kart kopyalamalarına benzer şekilde, bu kez dolandırıcılar "fastfood" denilen ve çalıştıkları taksi ve restoran gibi yerlerde müşterilerin kendilerine ilettikleri kredi

---

[201] Şekil-2.5: http://www.identitytheft.info/credit-card-skimmer-pictures.aspx (Gözden Geçirilme Tarihi: 29.10.2020).
[202] NESTA, "Crime Online: Cybercrime and legal innovation", ("*NESTA*"), s. 18: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/Crime_Online_Cybercrime_and_illegal_innovation.pdf (Gözden Geçirilme Tarihi: 29.10.2020).
[203] *TBB*, s. 62.

kartı bilgilerini, POS cihazının içine düzenek yerleştirmek suretiyle veya POS cihazı izlenimi veren cihazlar vasıtasıyla ele geçirmektedir[204].

Aşağıda Şekil 2.6[205]'da sahte slip örneğinin gösterildiği görselden de anlaşılacağı üzere, normalde slipteki onay kodu altı haneli olması gerekirken aşağıda yedi haneli olarak belirtilmiş ve ilgili POS bankasına ilişkin bilgilere yer verilmemiştir.

Şekil-2.6: Sahte Slip

Türkiye'de, 2014 yılında en dikkat çeken kredi kartı dolandırıcılıklarından birisi HSBC bankası nezdinde yaşanmış olup toplamda 2,7 milyon kişinin kart bilgilerinin (kartın bağlı bulunduğu hesap numarası, kartın son kullanma tarihi ve kart sahibi bilgisi olduğu belirtilmiştir) siber saldırganlar tarafından ele geçirildiği basına yansıyan konulardan birisi olmuştur. HSBC, bu olay neticesinde kamuoyuna BDDK ve ilgili diğer resmî kurumlarla ulusal ve uluslararası düzeyde işbirliği içerisinde devam ettiğini, konu ile ilgili ayrıca Cumhuriyet Başsavcılığı'na suç duyurusunda bulunduğunu belirtmiştir[206].

[204] *TBB*, s. 65.
[205] Şekil-2.6 için bkz. *TBB*, s. 65.
[206] https://www.fortuneturkey.com/hsbc-turkiye-27-milyon-musterinin-kart-bilgileri-calindi-2942 (Gözden Geçirilme Tarihi: 29.10.2020).

2.2. ELEKTRONİK ÖDEMELERDE SİBER GÜVENLİK BAKIMINDAN OLTALAMA (PHISHING) SALDIRILARI

Oltalama, bilişim terminolojisinde İngilizce'de balık tutma anlamına gelen "fishing" kelimesinin ilk harfinin "ph" harfleriyle oluşturulmuş bir terimdir[207]. Doktrinde, Eralp[208] tarafından phishing yöntemini "online dolandırıcılık" şeklinde tanımlarken, Taner[209] ise oltalamanın bir tür "kimlik avı" olduğunu belirtmiştir. Çakır/Kılıç'a[210] göre elektronik ödeme sistemlerine yöneltilen oltalama saldırıları sosyal mühendislik uygulamaları yardımı ile kullanıcıları sahte bir içerikle kandırma ve ikna etme suretiyle illegal olarak kişiye ait hesap, şifre, pin ve tan numaraları, kredi kartı bilgilerinin ele geçirilmesi faaliyetidir. Özkaya/Sarıca/Durmaz[211] ise oltalama yerine "yemleme" terminolojisini tercih ederek bu siber saldırı yönteminin daha ziyade bir işletme veya kişi hakkında hileli şekilde hassas bilgi toplama tekniği olduğunu ifade etmektedir. Tez kapsamında yazar tarafından, oltalama tekniğinin özellikle elektronik finansal işlemlerde siber saldırganlar için aşağıda belirtilen zararlı yazılımlar vasıtasıyla kurbana ait kimlik ve ödeme bilgilerinin ele geçirilmesi amacıyla sahte bir elektronik posta ve yönlendirilen bir web sitesi vasıtasıyla kurbanın güven duygusundan faydalanılarak kullanılan bir aldatma tekniği olarak değerlendirilmesi gerektiği sonucuna varmıştır.

Farklı oltalama yöntemleri söz konusudur[212]:

---

[207] "Phishing" sözcüğü İngilizce'de "Password harvesting fishing" sözcük öbeğinden türetilmiştir. Bkz. Leyla Keser Berber/Murat Lostar, "Bilişimde Biyometrik Yöntemler", Yetkin Yayınları, Ankara, 2006, (*"Keser Berber/Lostar"*), s. 30. Doktrinde, Eralp bu özgün isimlendirmenin, siber suçluların sanal ortamda yaptıklarını tanımlarken sözcüğün gerçek hayattaki karşılığından ayırt etmek zeka ve ileri teknoloji kullanıldığını vurgulamak amacıyla tercih edildiğini ifade etmiştir. Bkz. *Eralp*, s. 71.
[208] *Eralp*, s. 71.
[209] *Taner*, s. 37.
[210] *Çakır/Kılıç*, s. 110.
[211] *Özkaya/Sarıca/Durmaz*, s. 184.
[212] Oltalama yöntemleri ile ilgili detaylı bilgi için Bkz. *Çakır/Kılıç*, s. 108-114 ve James Graham/Richard Howard/Ryan Olson, "Cyber Security Essentials", CRC Press Taylor&Francis Group, 2011 ("*Graham/Howard/Olson*"), s. 87-92.

2.2.1. Sahte veya Ele Geçirilen Web Sitesi Vasıtasıyla Oltalama

Ziyaretçileri siber saldırganlar tarafından yaratılan web sitelerine çekmek yoluyla oltalama faaliyetine başvurulabilir. Bu yöntemde saldırganlar, daha ziyade banka gibi finansal kuruluşların sanal ortamda reklam resimleri ile kurbanlarını ele geçirilen veya sızılan web sitesi içeriğine yönlendirmek suretiyle kandırmaya çalışmaktadır. Özellikle günümüz teknolojisinin geldiği aşama itibariyle, deneyimli bir web tasarımcısının kolaylıkla birkaç saat içerisinde herhangi bir bankanın web sitesine birebir benzeyen bir sahte web sitesi yaratabileceği bilinmektedir[213]. Saldırganların bir sonraki adımı ise yönlendirdikleri kurbanlarının "keylogger" denilen tuş kaydedici gibi zararlı yazılımlar vasıtasıyla kişisel ve banka bilgilerini ele geçirmektir[214].

2.2.2. Elektronik Posta İletileri Vasıtasıyla Oltalama

Bu oltama yönteminde ise bu kez sahte bir web sayfasına yönlendirmek yerine siber saldırganlar tarafından gönderilen elektronik posta iletileri vasıtasıyla kurbanlar, saldırganlar tarafından yaratılan sahte web sitelerine yönlendirilmektedir. Kurban, sahte web sitesine tıkladığında doğrudan zararlı yazılımı bilgisayarına veya mobil cihazına yüklenmektedir. Literatürde bu saldırının İngilizce'de "spear phishing" denilen hedefe yönelik bir oltalama faaliyeti olduğu belirtilmiştir[215]. Saldırıların hedefli olmasından kasıt, elektronik posta iletilerinin içeriğinin kurbanın adı ve soyadı

---

[213] *Eralp*, s.71.

[214] Doktrinde, Dülger bu saldırıyı "yemleme" olarak nitelendirmekte ve yemlemenin genelde bir kişinin şifresini veya kredi kartı ayrıntılarını öğrenmek amacıyla kullanıldığı, bir banka veya resmi bir kurumdan geliyormuş gibi hazırlanan e-postalar yardımıyla kullanıcıların sahte sitelere yönlendirildiğini, bu sitelerde ise kullanıcılardan özlük bilgileri, kart numarası, kart şifresi gibi bilgiler talep edilerek kişilerin aldatıldığını ifade etmiştir. Bu konuda detaylı bilgi için bkz. Murat Volkan Dülger, "Bilişim Suçları Ve İnternet İletişim Hukuku", Seçkin, Güncellenmiş 8. Baskı, Ankara, 2020, (*"Dülger, Bilişim Suçları")*, s. 117.

[215] *Taner*, s. 37, *Özkaya/Sarıca/Durmaz*, s. 185. "Spear phishing" denilen hedefe yönelik oltalama faaliyeti genelde bir kişiye veya kuruma yönelik olarak genelde sosyal mühendislik tekniklerinden faydalanmak suretiyle nitelikli oltalama faaliyeti olarak tanımlanmıştır. Bkz. Cybersecurity Threats Challenges Opportunities, ACS, Kasım 2016, s. 58: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/ACS_Cybersecurity_Guide.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

belirtilmek ve hatta hedefin özellikle belirli bir ilgi alanına duyduğu ilgili ve meraktan yararlanılarak kurbanın kandırılmasıdır. Bu sayede kurbanın ilgisi çekilerek linke tıklayacağı web sitesindeki zararlı yazılımın kurbanın bilgisayarına yüklenmesi sağlanmış olur[216]. Genelde sisteme enjekte edilen bu tarz yazılımların sistem koruma yazılımlarını devre dışı bırakma, bilgisayarın DNS[217] ayarlarını manipüle ederek sahte web sayfalarına yönlendirme, tuş kaydediciler sayesinde basılan her tuşu ve hatta bazılarının ekran görüntüsünü dahi alarak şifreleri ve kişisel bilgileri kaydetme işlevleri olduğu bilinmektedir[218].

Aşağıda görselde de gösterilen emsal bir phishing mesaj örneğinden görüleceği üzere[219], başta finans sektörü olmak üzere birçok farklı sektörde bu tarz oltalama yöntemleri söz konusudur:

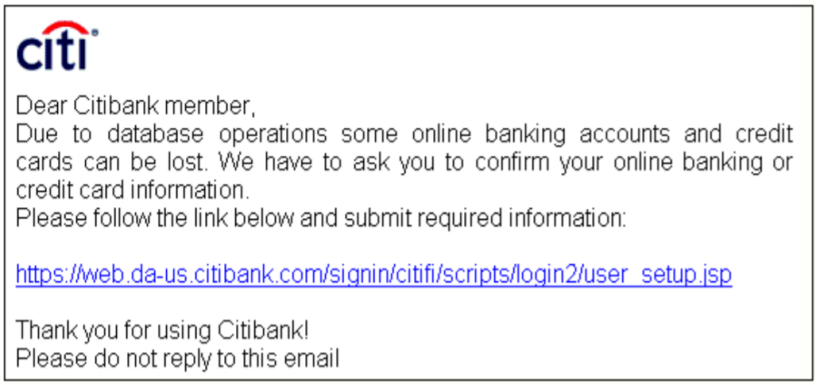
---

[216] Doktrinde, Taner bu konuda örnek olarak saldırganın başta sosyal mühendislik yöntemleri aracılığıyla hedefindeki kurbanın arabalarla ilgilendiğini öğrenerek saldırganın hedefin üye olduğu araba tartışma forumuna katılacağı, bir araba satışı teklifi verebileceğini ve böylelikle e-posta göndererek kurbanı kandırabileceğini belirtmiştir. Bkz. *Taner*, s. 37. Eralp ise e-posta yoluyla oltalamanın, daha ziyade saldırganın kurbanına, banka veya alışveriş sitesi gibi bir ticari kurumdan geliyormuş gibi izlenim yaratarak e-posta gönderilmesinin uygulamada daha yaygın olduğunu, bu tarz e-postanın içeriklerinin ise kişisel bilgilerin güncellenmesi, sistemdeki yeniliklerin kurbanın hesabında aktif olması için şifre girilmesini talep eden mesajlar şeklinde olabileceğini ifade etmiştir. Detaylı bilgi için Bkz. *Eralp*, s. 71. Özkaya/Sarıca/Durmaz, oltalama içeren mesaj içeriklerinin daha ziyade bazı bilgilerin doldurulmasını içeren ve bir problemi açıklayan mesajlar, büyük bir para kazanıldığı belirten mesajlar ile insanların cömertlik ve yardım duygularını sömürmek amacıyla görünürde yardım maksadı içeren mesajlar şeklinde olduğuna işaret etmektedir. Bkz. *Özkaya/Sarıca/Durmaz*, s. 143.

[217] İngilizce'de "Domain Name Service" sözcüklerinin kısaltması olarak kullanılan DNS, internet uzayını bölerek bölümleri adlandırmaya ve bölümler arası iletişimi organize etmeye yarayan bilgisayarları, servisleri ve diğer kaynakları internet veya özel bir ağa bağlayarak hiyerarşik ancak merkezi olmayan şekilde belirlemeyi sağlayan adlandırma sistemini ifade etmektedir. İnternet ağını oluşturan her birim sadece bir IP (Internet Protocol) adresine sahiptir. DNS sunucuları, internet adreslerinin IP adresi karşılığını kayıtlı tutmaktadır. DNS konusunda detaylı bilgi için bkz. https://tr.wikipedia.org/wiki/DNS (Gözden Geçirilme Tarihi: 29.10.2020).

[218] *Çakır/Kılıç*, s. 111.

[219] Şekil 2.7'deki görselin aktarıldığı web sitesi:
https://www.google.com/search?q=citibank+dear+citibank+member+email+phishing&tbm=isch&ved=2ahUKEwiPlpGB5evqAhUNixoKHaSsBYkQ2-cCegQIABAA&oq=citibank+dear+citibank+member+email+phishing&gs_lcp=CgNpbWcQA1C78AFYpZwCYLuvAmgBcAB4AIAB1gGIAawUkgEGMi4xOS4xmAEAoAEBqgELZ3dzLXdpei1pbWfAAQE&sclient=img&ei=2-sdX8-8F42WaqTZlsgI&bih=657&biw=1451#imgrc=UdmoxNljS8RquM
(Gözden Geçirilme Tarihi: 29.10.2020).



Şekil-2.7: Phishing Mesajı

2.2.3. Smishing

"Smishing" kavramının açılımı İngilizce'de "SMS Phishing" ibareleri olup oltalama faaliyetlerinin kullanıcıların mobil cihazlarını hedef almak suretiyle gerçekleştirilmesi anlamına gelir. Bu saldırı türünde de cep telefonuna gelen kısa mesaj vasıtasıyla kurbanın mobil cihazına zararlı yazılım yüklenmesi sağlanabilir. Bu yöntem oltalamanın dışında kontör dolandırıcılığı için de kullanılabilir[220].

Sonuç itibariyle, oltalama tekniği elektronik ödemelerde sistemi zafiyete uğratmak açısından saldırganlar tarafından kullanılan genelde öncü bir saldırı tekniği olarak kullanılmakta, deyim yerinde ise hedefteki kişinin oltaya gelmesinden sonra ise zararlı yazılımlar ve benzeri yöntemlerle bilişim sistemi zafiyete uğratılmaktadır.

2.3. SOSYAL MÜHENDİSLİK (SOCIAL ENGINEERING) SALDIRILARI

2.3.1. Sosyal Mühendisliğin Tanımı Ve Finans Sektöründe Somut Uygulama Örnekleri

Literatüre bakıldığında, "sosyal mühendislik" kavramı ile ilgili farklı yazarların konu ile ilgili farklı yaklaşımları bulunmakta olup sosyal mühendislik, kısıtlanan alanlar ve

[220] *Graham/Howard/Olson*, s. 89, *Çakır/Kılıç*, s. 112-113.

sistemler açısından sistemin en zayıf unsuru olan "insan faktörü"nü hedef alarak sisteme ilişkin hassas bilginin ele geçirilmesi veya sisteme giriş izni ve yetkisi olmayan kişilerin sisteme giriş yapmasını sağlayan bir insan aldatma sanatı tekniğini ifade etmektedir[221]. Sosyal mühendisliğin çalışmayı ilgilendiren boyutu itibariyle sosyal mühendislik, hedefteki kurban ile kurulan sosyal temas sonucu her türlü zafiyetten ve menfaat sağlayacak bilgiden yararlanmak suretiyle haksız kazanç elde elde etmek şeklinde tanımlanabilir.

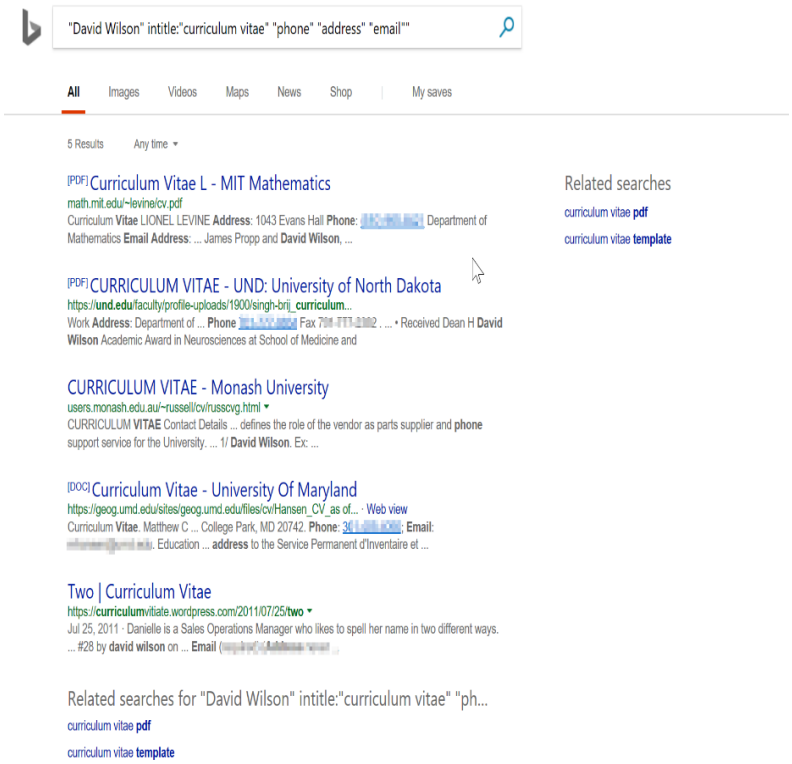
Yukarıda da belirtildiği üzere, sosyal mühendislik saldırılarında dikkate alınması gereken en kritik faktör bilgi güvenliğinin en zayıf katmanı olan "insan" faktörü olup özellikle finans sektörüne yönelik yaratıcılık ve zeka gerektiren bu saldırılarda, saldırganların başarıya ulaşmalarında başvurdukları en zengin kaynağın sosyal medya olduğu görülmektedir. Günümüzde, basit bir şekilde çoğumuzun LinkedIn, Instagram, Facebook gibi sosyal paylaşım sitelerinde hesabı bulunmakta olup bireylere ilişkin birtakım alışkanlıkların bu mecralarda takibi kolaydır. Bazen sosyal medyada paylaşılan ve basit görünen bu bilgiler ise siber korsanların kurbanlarına ilk adım atmalarında ve kritik düzeyde önem teşkil eden finans bilgileri gibi nitelikli bilgilerin

[221] Bu tanım literatürde "sosyal mühendislik" ile ilgili diğer tanımlara ve açıklamalara bakılarak yazar tarafından çalışma içeriğinde en kapsayıcı tanım olduğu düşünülerek *Graham/Howard/Olson*, s. 176-177'den derlenerek aktarılmıştır. Doktrinde, bu konuda diğer tanımlar incelendiğinde, Taner sosyal mühendisliğin bireyleri eylemleri gerçekleştirmeye veya gizli bilgileri yönlendirmeye çalışan bir erişim saldırısı olduğu ve sosyal mühendislerin genellikle insanların yararlı olma isteklerini kullanarak ve insanların zayıf yönlerini avlayarak bu saldırıyı gerçekleştirdiklerini belirtmiştir. Çakır/Kılıç'a göre, sosyal mühendislik saldırıları kişisel beceri ve kabiliyete dayanan, basit ama oldukça etkili saldırılar olarak hedefteki kişi veya kurumun yapısı, çalışanların/yöneticilerin kişisel bilgileri, şifreler ile birlikte saldırıda kullanılabilecek her türlü materyallerin toplanmasına olanak sağlamaktadır. Bkz. *Çakır/Kılıç*, s. 119-120. Sağıroğlu/Alkan ise sosyal mühendislik kavramının zararlı yazılımlarla bütünleşik saldırılara orta hazırlamasıyla beraber insan faktörünün yönetilmesi gereken en önemli bileşen haline dönüştüğü üzerinde durmuştur. Bkz. *Sağıroğlu/Alkan*, s. 112. Son olarak, bu konuda Özkaya/Sarıca/Durmaz ise sosyal mühendislik kavramının tanımından ziyade özellikle geçmişte 2014 yılında Yahoo şirketinin maruz kaldığı ve 500 milyon üzerinde kullanıcının bilgilerinin çalındığı sosyal mühendislik saldırısı, 2015 yılında Ubiquiti Networks şirketinin maruz kaldığı sosyal mühendislik saldırısı gibi geçmişte yaşanan ciddi ölçekli sosyal mühendislik saldırılarına dikkat çekerken özellikle günümüzde siber saldırganların eskiye nazaran çok daha şanslı olduğu, insanların Facebook, Twitter, Instagram, LinkedIn, Snapchat gibi sosyal ağlarda kişilerin kendilerine ait çok fazla hassas nitelikteki bilgiyi de paylaşması nedeniyle sosyal mühendislerin günümüzde insanları çok daha fazla kandırma imkanı olduğu özellikle vurgulanmıştır. Bkz. *Özkaya/Sarıca/Durmaz*, s. 119.

ele geçirilmesinde önem taşımaktadır. Sosyal mühendislik döngüleri ve konu ile ilgili somut örneklere geçilmeden önce, özellikle çarpıcı bir örnek olması noktasında şu yöntemin dahi başlı başına sosyal mühendislik saldırılarının gerçekleştirilmesi açısından etkin bir uygulama olduğu görülmektedir:

Arama motorları sosyal mühendislik saldırıları açısından önemli bir yer teşkil etmektedir. Arama motorları özellikle birçok siteyi indeksleme imkânı sunduğu için çoğu kez kullanıcılardan temin edilen bilgileri tek bir merkezi yerde tutarlar. Örneğin, Google bu açıdan eşsiz bir kaynak olup bir şahıs hakkında bilgi edinilmek istenildiğinde farklı arama teknikleri söz konusudur. Örnek vermek gerekirse, hedefte "David Wilson" isimli bir şahıs düşünüldüğünde, Google arama motoruna aşağıda yazılacak sözcükler bu kişi ile birçok bilgi sunabilecek niteliktedir:

"David Wilson" intitle:"curriculum vitae" "phone" "address" "email""



Şekil-2-8: Sosyal Mühendislik – Google Araması

Yukarıda da görüldüğü üzere, Google arama satırına yukarıda bilgiler girildiğinde hakkında sadece bilgi toplanılmak isteyen "David Wilson" ile ilgili bu ismin geçtiği tüm web siteleri sıralanmayacak, ayrıca özgeçmiş, telefon, adres ve email de olmak üzere bu kelimelerin geçtiği web sitesi içeriklerine de yer verilecektir[222].

Aşağıda salt finans ve bankacılık sektörüne yönelik gerçekleştirilen sosyal mühendislik saldırılarından bazılarına yönelik somut örnekler şunlar gösterilebilir[223]:

Sahte Çağrı Merkezleri: Genelde dolandırıcılar kendilerini polis veya bir şekilde kamu görevlisi olarak tanıtarak veya kurbanlarına ödül kazandığı için mesaj göndermesi veya kart aidatı veya banka hesap işletim ücreti gibi gereksiz masrafların iade edileceği vaadiyle kandırarak haksız kazanç elde etmektedir. Sahte çağrı merkezlerinin ilk çıktığı zamanlarda daha ziyade mobil cihazlardaki kontörlere yönelik gerçekleştirilen bu dolandırıcılık yöntemi, zaman içerisinde teknolojisinin gelişmesi ve dolandırıcıların yaratıcı ikna yöntemleri dikkate alındığında, elektronik ödemelerde kartsız para transferi, mobil cihazla para transferi, hızlı kredi tahsisi ve internet bankacılığı gibi yöntemlerle dolandırıcıların şube, ATM gibi farklı mecralardan sosyal mühendislik yöntemleri ile kazanç elde etme imkanı ciddi ölçüde kolaylaşmıştır. Sahte çağrı merkezleri vasıtasıyla dolandırıcılar tarafından doğrudan ilgili kişilerin kredi kartı bilgilerini (onaltı numaralık kredi kartı numaraları, kartın son kullanma tarihi, CVV

[222] Şekil-2.9 ve yukarıda açıklamalar *Özkaya/Sarıca/Durmaz*, s. 129'den derlenerek aktarılmıştır.

[223] İbrahim Kudret Elçiboğa, "Sosyal Mühendislik Yöntemleriyle Dolandırıcılık" adlı makalesi, Fintechtime: http://fintechtime.com/tr/2018/07/sosyal-muhendislik-yontemleriyle-dolandiricilik/ (Gözden Geçirilme Tarihi: 29.10.2020). Çakır/Kılıç'a göre ise, sosyal mühendislikte kullanılan yöntemler bilgi toplama (fiziksel girişimler), güven kazanma (psikolojik girişimler), güveni kötüye kullanma (bilgisayara komut gönderme ve program yükletirme) ve saldırı süreçlerinin birleşimidir. Sosyal mühendislik saldırılarında bilgi toplama amacıyla kullanılan yöntemler ise, çalışma ofisi ziyaretleri, çöp kurcalama işlemleri, telefon görüşmesi, tersine sosyal mühendislik ve psikolojik girişimler olarak kategorize edilebilir. Bu konuda detaylı bilgi için bkz. *Çakır/Kılıç*, s. 119-125.

kodu) edinmek suretiyle internet ve mobil bankacılık üzerinden gerçekleştirilen işlemler ile mağdur konumundaki kişiler dolandırılmaktadır.

Çöp Karıştırma: Bu deyim, genelde şirket çalışanlarının ofis yaşamında ve bireylerin gündelik hayatında önemsiz gibi görülen bilgilerin (kimlik belgesi fotokopileri, kurumun iş yaptığı kişilere ilişkin telefon bilgileri ve adres rehberi, özgeçmiş, hesap ekstreleri, dekont vb.) sosyal mühendislik gerçekleştirmek isteyen dolandırıcılar tarafından kullanılarak menfaat elde edilmesini ifade etmektedir. Bu durumun en yaygın örneği, şirket çalışanların unutmak istemedikleri masaüstü parolaları gibi bilgileri bir post-it vasıtasıyla kolay ulaşılabilir bir yerde tutmaları veya çoğu kez kâğıt öğütücüden geçirmeksizin kendi kişisel bilgilerini içeren belgeleri çöpe atmaları sonucunda kelimenin gerçek anlamıyla bu çöpü karıştırarak kendilerine menfaat sağlayacak dolandırıcıları hesaba katmadıkları görülmektedir. Çöp karıştırma somut eylemlerine dolandırıcılık amaçlı kurulan bir şirketin bankadan çek karnesi temin etmesi neticesinde piyasada birçok karşılığı olmayan çek keşide etmesi, cep telefonu hattı temin eden suçluların şantaj, terör amaçlı olarak bu telefon hattını kullanması, bankadan sahte kimlik ile kredi veya kredi kart başvurusu yapan kişilerin birçok harcama yaptıktan ortadan kaybolması gibi örnekler verilebilir.

Ön Ödeme Dolandırıcılığı: Bu dolandırıcılık yönteminde, genelde saldırganlar kurbanlarına internetten okunan bir ilan veya telefon üzerinden ulaşarak kredi geçmişine bakılmaksızın uygun kredi faizleri karşılığında kredi vereceklerini teklif eder. Sosyal mühendisler özellikle bu konuda kredi talepleri olumsuz sonuçlanan kişileri takip eder. Dolandırıcılar, genelde bu yöntemde sağlanan tüm olumlu koşullar karşılığında krediye ihtiyaç duyan kişiye iyiniyet göstergesi olarak kredinin ilk taksidinin geri ödemesini bir nevi teminat olmak üzere önceden yatırılmasını talep eder. Para yatırıldıktan sonra ise dolandırıcıların amaçları gerçekleşmiş olur ve kurban konumundaki kişinin genelde bu kişilerden bir daha haber alması mümkün olmaz.

2.3.2. Sosyal Mühendislik Döngüleri

Finans kuruluşlarına ve bankalara yönelik sosyal mühendislik ataklarının en iyi şekilde anlaşılması açısından çalışmada metodolojik açıdan sosyal mühendislik atağını belirli aşamalara bölerek somut örnekler üzerinden açıklanmasının en uygun yöntem olabileceğini düşünülmüştür. Literatürde, "Sosyal Mühendislik Döngüsü"nün şu aşamaları içerdiği belirtilmektedir[224]:

2.3.2.1. Bilgi Toplama (Information Gathering)

İlk aşamada, hedefteki kurbanla ilgili sosyal mühendis tarafından değişik teknikler kullanılarak bilgi toplanır. Bilgi toplama aşaması genelde herhangi bir ortalama insan tarafından hassas bilgi değerlendirilmemekle beraber sosyal mühendis açısından amacına ulaşmasında hedefteki kurbanı ile her çeşit bilgi kapsayabilmektedir. Sosyal mühendis hareket geçmeden önce başlangıçta yukarıda belirtilen Google arama motoru da dahil olmak üzere kamuya açık platformlardan kendisine fayda sağlayacağını

[224] Literatürde genel olarak sosyal mühendislik kavramı ve sosyal mühendislik döngüsüne yönelik genel içerikli birçok değerlendirmeye yer verilmiştir. Sosyal mühendislik tanımı ve sosyal mühendislik döngüleri hakkında ayrıntılı bilgi için Bkz. Malcolm Allen, "Social Engineering: A Means to Violate A Computer System", SANS Institute Information Security Reading Room", 2007, (*"Allen"*), s. 5: https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529 ve ayrıca Bkz. Rebecca M. Long, "Using Phishing To Test Social Engineering Awareness of Financial Employees", Thesis, Eastern Washington University, Master of Science, 2013, (*"Long"*), s.6, file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/rlong_thesis_v4.5_FINAL%20(1).pdf (Gözden Geçirilme Tarihi: 29.10.2020). Bu konuda literatürde kaynak taraması yapıldığında, Özkaya/Sarıca/Durmaz sosyal mühendislik saldırısındaki işlem döngüsünün altı aşamadan meydana geldiğini belirtmektedir: (i) Bilgi Toplama: Kısaca sosyal mühendislik faaliyetleri açısından en zor ve zahmetli olan bilgi toplama aşamasında, saldırgan tarafından kendilerine yarar sağlayacak teknik olan veya teknik olmayan her türlü uygun veriyi toplama ve bu bağlamda kullanılabilecek yazılım araçlarını iyi tespit etmek. (ii) Çıkarım: Bu aşamada, görünüşte masumane bir sohbet sırasında istenilen bilginin kurbana fark ettirilmeden elde edilmesini ifade etmektedir. (iii) Başkasının Yerine Geçme: Bu aşamada, sosyal mühendis herhangi bir pozisyon veya makamdaki birinin yerine geçerek hedefindeki kurbanı bazı kararlar vermesi için ikna eder. (iv) İkna: Hedefini ikna edebilmek için sosyal mühendisin öncelikle hedefinin ilgisini çekebilmesi için hedefteki kurbanın beyninde sorgulanamayan bir etki sağlanması gereklidir. (v) Hedef Seçme: Saldırgan tarafından istismar edilecek en uygun hedefin seçilmesini ifade etmektedir. (vi) Keşif: Bu son aşamada ise, artık sosyal mühendis tarafından tüm gerekli bilgiler elde edilmesi akabinde artık harekete geçilmesi hazır hale gelinmiştir ve saldırgan artık harekete geçerek sosyal mühendislikle hedeflediği sonuçları elde edip edemeyeceğini keşfe gider. Bkz. *Özkaya/Sarıca/Durmaz*, s. 126-141.

düşündüğü telefon listeleri (güncel veya eski tarihli), doğum tarihleri, sosyal mühendislik uygulanacak kuruluşa ait organizasyon şeması da dahil olmak üzere muhtelif birçok bilgiye erişmeye çalışır. Finans kuruluşlarına yapılacak sosyal mühendislikle ilgili bu aşamayı somutlaştırmak için şu örnek verilebilir: Öncelikle sosyal mühendislik tekniği uygulayacak saldırgan tarafından ilgili bankanın kurumsal web sitesi ile hedefteki banka çalışanın blog yazılarının, makalelerinin ve videolarının incelenmesi gereklidir. Sosyal mühendis, banka çalışanına oltama tekniği ile hassas bilgileri ele geçirme, soğuk arama, favori hobilerini sorma, kendini polis, savcı gibi devlet memuru tanıtma ve hatta ilgili bankaya kendisini müşteri olarak tanıtarak fiziken ziyaret etmeye kadar birçok birçok eylem gerçekleştirecektir. Doktrinde Özkaya/Sarıca/Durmaz[225] bu aşamada aslında sosyal medyanın günümüzde birçok kuruluşa ve hatta bu kuruluşun çalışanlarına ait hassas bilgiyi de içerdiği göz önüne alındığında kamuya açık bilgilerin bilgi toplama aşaması açısından kamuya açık olmayan bilgilere kıyasla dahi birçok açıdan günümüzde yeterli olduğunu belirtmiştir. Bu aşamada, kamuya açık bilgilerden kendisine fayda sağlayacak bilgileri dikkate ayıklayabilecek sosyal mühendis konumundaki saldırgan, derini kazma (digging deeper) denilen yöntem ile ilgili banka çalışanı veya yardım masası personelini arayarak ilgili bankanın kritik roldeki müdürleri ve çalışanların isimlerini, telefon numaralarını veya bankanın kendi bilgi sistem altyapısında kullandığı bazı yazılımları öğrenmeyi başaracaktır.

[225] Bahsi geçen yazarlara göre, günümüzün siber saldırganlarının eskiye kıyasla çok daha şanslı olmasının yegâne sebebi, Facebook, Twitter, Instagram, LinkedIn gibi sosyal ağlarda insanların kimlik bilgilerinden arkadaşlarına, çalıştığı şirket ve kurumlara, iş arkadaşlarına, yediği yemekten, katılım gösterilen aktivitelere kadar birçok bilgiyi fütursuza paylaşabilmesidir. Bu anlamda, yazarlar sosyal ağlara yönelik bu bağımlılıklar neticesinde Gelişmeleri Kaçırma Korkusu (Fear of Missing Out – kısaca FOMO) adı verilen bir hastalığın dahi ortaya çıktığını ve bu paylaşım çılgınlığının sosyal mühendislerinin arayıp da bulamadığı bilgi hazinesi haline geldiğine özellikle dikkat çekmiştir. Bu konuda daha detaylı bilgi için Bkz. *Özkaya/Sarıca/Durmaz*, s. 119-120.

2.3.2.2. İlişki Geliştirme (Developing Relationships)

Bu aşamada, saldırgan tarafından hedefteki kurban ile samimiyet kurulması açısından kurbana ilişkin hassas bilgilerin istismar edilebilmesi amacıyla sosyal temas gerçekleştirmeye çalışılır. Saldırgan, bilgi toplama aşamasında elde ettiği bilgiler vasıtasıyla genelde bir veya birden çok telefon görüşmesiyle hedefteki kişi ile ilişki kurulmaya çalışılır. Genelde, saldırgan kurbanı arayarak ya kendisini ilgili finans kuruluşundaki yeni bir çalışan olarak yardım amacıyla aradığını belirtir ya da "tersine sosyal mühendislik" (*reverse social engineerig*)[226] denilen yöntemle sosyal mühendis tarafından bilinçli yaratılan bir problemi çözmek kisvesi altında hedefteki kişi aranarak istismar edilmeye çalışılır. Somut örnek üzerinden konuya bakıldığında, sosyal mühendis ilgili banka çalışanını arayarak nasıl iki kuruluş arasında para transferi yapılacağını sorarak ve bu konuda mevcut kullandığı yazılım veya uygulamada problem yaşadığını belirterek hedefteki kurbandan kritik bazı bilgileri almayı başarır. Genelde, yardım kisvesi altında sosyal mühendis tarafından gerçekleştirilen aramalar

[226] Tersine sosyal mühendislik, kurbanın temelde kendi rızasıyla sosyal mühendisten yardım istediği ve sobatoj, pazarlama ve destek adımlarından oluşan bir sosyal mühendislik tekniğidir. İlk adımda, saldırgan kurbanın kullandığı sistemde basit erişimler elde ederek sistemi bozar veya kurbana bozulmuş izlenimi verir. Pazarlama denilen ikinci adımda ise, saldırgan takip ettiği kurbana ancak sistemi kendisinin düzelteceği izlenimi vererek kurbanını kandırmış olur. Son adımda ise, çaresiz kalan kurban sistemin bir an önce düzelmesi için saldırgana talep ettiği kritik bilgiyi paylaşır. Bkz. Mustafa Yasir Şentürk, "Güncel Siber Saldırı Yöntemleri, Sızma Testi Araçları Ve Temsili Kurumsal Bir Ağ Üzerinde Kullanılması", Türk Hava Kurumu Üniversitesi Fen Bilimleri Enstitüsü, Elektrik Ve Bilgisayar Mühendisliği Anabilim Dalı, Eylül 2018, (*"Şentürk"*), s. 100: https://afyonluoglu.org/PublicWebFiles/Reports-TR/Akademi/2018_Mustafa%20Yasir%20Sent%C3%BCrk_G%C3%BCncel%20siber%20sald%C4%B1r%C4%B1%20y%C3%B6ntemleri.pdf (Gözden Geçirilme Tarihi: 29.10.2020). Tersine sosyal mühendislik, Çakır/Kılç tarafından yöntem olarak saldırganın hedefini, aslında var olmayan bir sorunu olduğuna inandırarak kendi ağına düşürmesi şeklinde tanımlanarak genel bilgisayar bilgisi zayıf olan kişilerin bir uygulama veya kodun verebileceği zararla ilgili hiçbir bilgisi olmadığı için saldırganların gönderdikleri bağlantıdaki programı bilgisayarlara kurulması yönündeki talebin bu kişiler tarafından olumlu karşılanması sebebiyle amaca ulaşma olasılığının yüksek olduğu değerlendirilmiştir. Bkz. *Çakır/Kılıç*, s. 124. Ayrıca tersine sosyal mühendislik kavramı ile ilgili ayrıntılı bilgi için Bkz. Kevin D. Mitnick, "The Art of Deception", (*"Mitnick"*), s. 99: https://repo.zenk-security.com/Magazine%20E-book/Kevin_Mitnick_-_The_Art_of_Deception.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

bu aşamada izlenebilecek en iyi yöntemdir. Bundan sonraki süreçte ise, artık saldırgan tarafından istismar denilen bir sonraki aşamaya hazır hale gelinmiş olunacaktır.

2.3.2.3. İstismar (Exploitation)

"İstismar" aşamasında ise hedefteki kurban, güven kazanılan sosyal mühendis tarafından manipüle edilerek bilgi alınması (parola vb.) veya herhangi bir eylemde bulunması (örneğin hesap açmak veya telefon ücretlerini yansıtmak gibi) kendi rızasıyla farkına varmadan istismar edilir.

Bu aşamada, sosyal mühendis hedefindeki kurbanla ilgili ulaşmak istediği ve kendisine yarar sağlayabilecek bilgileri edinmiş ve hedefteki kişi ile gerekli samimiyeti kurmayı başarmıştır. Artık bu aşamadan sonra sosyal mühendisin hedeflediği amaca ulaşabilmesini sağlayacak daha riskli bir adım atarak hedefindeki kişiden daha kritik düzeydeki gizli bilgiyi paylaşma veya kurbanın hiç aklında olmayan bir eylemi (kurbanın bilgisayar sistemine uzaktan bağlanma gibi veya intranet konumundaki sisteme girebilmek için login bilgisini paylaşma gibi) gerçekleştirmesi konusunda talepte bulunur. Bu kritik bilgiye ulaşan saldırgan açısından geriye tek kalan husus eyleme geçerek ilgili bankadan haksız şekilde kazanç sağlamaktır.

2.3.2.4. İcraat (Execution)

Nihai aşama olan icraat aşamasında sosyal mühendis tarafından kurbana ilişkin hassas bilgiler toplanması akabinde hedeflenen amaç gerçekleştirilir. İcraat aşamasında, sosyal mühendis genelde kendisine yardımcı olmak isteyen banka çalışana o bankanın belirli bir hesabındaki paranın kendi hesabına aktarılmasını talep eder veya önceki aşamalarda ilgili bankanın bilişim sistemlerine uzaktan erişim imkânına sahip olması sebebiyle genelde sisteme zararlı yazılım enjekte ederek müşterilerin kendisine fayda sağlayacak kimlik bilgilerini veya ödeme bilgilerini ele geçirir ve bunları bir şekilde ya kendi hesabına aktarır veya yasa dışı şekilde müşteri bilgilerini başka kötüniyetli üçüncü kişilere satar.

2.4. SWIFT SİSTEMİNE YÖNELİK SİBER SALDIRILAR

İlk bölümde genel itibariyle dünyada hangi SWIFT dolandırıcılıklarının yaşandığı ve SWIFT kurumunun dolandırıcılara karşı ne gibi tedbirler öngördüğüne ilişkin genel bir bilgi verilmiştir. Bu başlık altında ise SWIFT dolandırıcılığında saldırganların ne tarz yöntemler izlediği aşağıda teknik açıdan daha detaylı şekilde açıklanacaktır[227]. Bu açıklamalara geçilmeden önce, SWIFT sistemi ile ilgili teknik birtakım bazı bilgilere yer verilmesinin en azından bu sisteme yönelik saldırıların anlaşılması açısından faydalı olacaktır:

SWIFT şirketi, SWIFTNet denilen SWIFT mesajlaşma ağı hizmeti kapsamında özellikle FIN, Interact, FileAct ve Browse denilen dört tip mesajlaşma hizmeti vermektedir. Aynı zamanda, bahsi geçen ağ sayesinde finansal içerikli mesajlaşmada güvenlik noktasında yeni çözümler, mesaj trafiği kontrol yönetimi, mesajların işlenmesi ve mesajların doğru şekilde aktarılması amaçlanmaktadır. Buna karşın, saldırganlar genelde sisteme enjekte ettikleri zararlı yazılımlar sayesinde SWIFT sistemindeki müşteri hesapları üzerinde kontrolü ele geçirerek sistemi istismar etmeyi başarmaktadır[228].

SWIFT, müşterilerinin kendi yerel ağları ve bu ağların altyapısının güvenliğine ilişkin herhangi bir sorumluluk üstlenmemekle beraber siber ataklara maruz kalan müşterilerine bu ataklarla mücadele etme konusunda destek vermektedir[229]. Buna

[227] Deloitte, "SWIFT Systems and the SWIFT Customer Security Programme: https://www2.deloitte.com/content/dam/Deloitte/be/Documents/risk/be-ra-swift-customer-security-programme.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[228] F-Secure, "Threat Analysis, SWIFT Systems and the SWIFT Customer Security Program", (*"F-Secure Raporu"*), s. 4, ilgili raporun tam metnine elektronik ortamda ulaşmak için: https://www.f-secure.com/content/dam/f-secure/en/business/common/collaterals/f-secure-threat-analysis-swift.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[229] *F-Secure Raporu*, s.4.

örnek olarak, İngilizce'de "Customer Security Program" (*CSP*) denilen "Müşteri Koruma Programı"[230] gösterilebilir.

Geçmişte SWIFT'e yöneltilen ve bilinen örnekler üzerinden konuyu incelemek gerekirse, yukarıda da belirtildiği gibi bu zamana dek SWIFT sistemine yönelik gerçekleştirilen en nitelikli ve rakamsal açıdan zarar boyutu en yüksek SWIFT saldırısının 2016 yılında Bank of Bangladesh'e yöneltildiği bilinmektedir[231]. Aslında, saldırının hedef aldığı toplam rakam 951 milyon Dolar olup 81 milyon Dolar transferinde saldırganlar tarafından başarı sağlanmıştır. Saldırganlar bir sene gizli şekilde sürdürdükleri bu saldırıda öncelikle bankanın iç sistemine sızarak Windows yazılımdaki açıktan (*bug*) faydalanarak banka çalışanlarının aktivitelerini takip etmiş ve bu sayede bankanın SWIFT uzantılı sistemine ulaşmayı başarmıştır. SWIFT sistemine ulaşıldığında ise SWIFT Alliance Access uygulamasına başarılı şekilde enjekte edilen zararlı yazılım sayesinde tüm güvenlik tedbirleri geçilerek SIWFT mesajlarında tek bir iz bırakılmaksızın saldırı başarılı şekilde sonuçlandırılmıştır. Bu sayede, toplamda 951 milyon dolar değerinde toplamda 35 adet SWIFT işlemine yönelik saldırı gerçekleştirilmiştir. Ancak, SWIFT mesajlarındaki bazı uyumsuzlukların fark edilmesi neticesinde saldırılar büyük ölçüde engellenmişse de, toplamda 81 milyon Dolar'ın saldırganların Filipinler'de bulunan hesaplarına aktarılması engellenememiştir. Diğer bir örnek ise, Bank of Bangladesh saldırısından yaklaşık bir sene öncesinde Banco del Austroz'a yönelik gerçekleştirilen ve toplamda 12 milyon Dolar zarara sebebiyet veren saldırıdır. Bu saldırıda, saldırganların Bank of Bangladesh saldırısına benzer şekilde ismi bilinmeyen bir banka çalışanın Outlook email hesabına ulaşarak önce bankanın yürütmekte olduğu bazı SWIFT transfer

[230] CSP denilen Müşteri Koruma Programı, özetle SWIFT müşterilerinin kendi lokal sistemlerinde uygulamaları gereken birtakım kapsamlı güvenlik tedbirlerine yönelik programı ifade etmektedir. Bu konuda detaylı bilgi için bkz. F-Secure Raporu, s. 10 ve ayrıca SWIFT'in kendi web sitesi üzerinden bilgi edinmek için bkz. https://www.swift.com/myswift/customer-security-programme-csp (Gözden Geçirilme Tarihi: 29.10.2020).

[231] Bank of Bangladesh'e yöneltilen saldırının teknik detayları ile ilgili ayrıntılı bilgi için bkz. *F-Secure Raporu*, s. 8.

taleplerini iptal ettiği ve SWIFT sistemi üzerinde bazı detayları değiştirerek 12 milyon değerinde haksız kazanç elde ettiği kaydedilmiştir[232]. Türkiye'de yaşanan SWIFT sistemine yönelik saldırı bakımından ise Akbank'a karşı 2016 yılında gerçekleştirilen saldırı örnek gösterilebilir. 08.12.2016 tarihinde Akbank'ın SWIFT Yurtdışı Para Transfer Sistemleri'ne yönelik gerçekleştirilen saldırı sonucunda Akbank yetkilileri tarafından kamuoyuna aktarılan bilgi kapsamında saldırının Akbank'ın operasyonlarını ve mali tablolarını etkileyebilecek önemli bir etkisi bulunmadığı, Akbank'ın maruz kalabileceği azami risk tutarının 4 milyon Amerikan Doları civarında olduğu ve olası zararın Akbank'ı koruyan Bankers Blanket sigortası kapsamına girdiği belirtilmiştir[233].

SWIFT sistemine yöneltilen nitelikli siber saldırılarda ilk göze çarpan ortak olgu, atakların genelde hedefteki bankanın sistemine enjekte edilen zararlı yazılım sayesinde gerçekleştirildiğidir[234]. Buna ilaveten, 2014 yılında yayınlanan IBM'in Siber Güvenlik İstihbarat Endeksi[235] uyarınca ise SWIFT'e yöneltilen atakların %95'inin insan kaynaklı hatalarla desteklendiği, dolayısıyla insan faktörünün SWIFT saldırılarında özellikle dikkate alınması gereken bir unsur olduğu sonucuna varılmıştır.

Görüldüğü üzere, SWIFT gerek işlem hacmi gerekse finansal açıdan müşteriler tarafından sık tercih edilen bir mesajlaşma sistemi olduğundan saldırganlar tarafından büyük ölçüde rağbet görmüş ve zaman zaman APT saldırıları[236] gibi uzun bir zaman ve sabır gerektiren ancak başarıya ulaşılması halinde bir o kadar getirisi olan saldırıların merkezinde olmuştur.

---

[232] *F-Secure Raporu*, s.7.
[233] https://businessht.bloomberght.com/piyasalar/haber/1336981-akbanktan-siber-saldiri-aciklamasi (Gözden Geçirilme Tarihi: 29.10.2020).
[234] *F-Secure Raporu*, s.10.
[235] https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf (Gözden Geçirilme Tarihi: 29.10.2020).
[236] APT saldırıları konusunda çalışmanın 2.8. başlığı altında yer alan değerlendirmeler dikkate alınabilir.

SWIFT'e yöneltilen siber saldırılarda sık rastlanan ve aşağıda açıklanan iki temel yöntemin benimsendiği görülmektedir[237]:

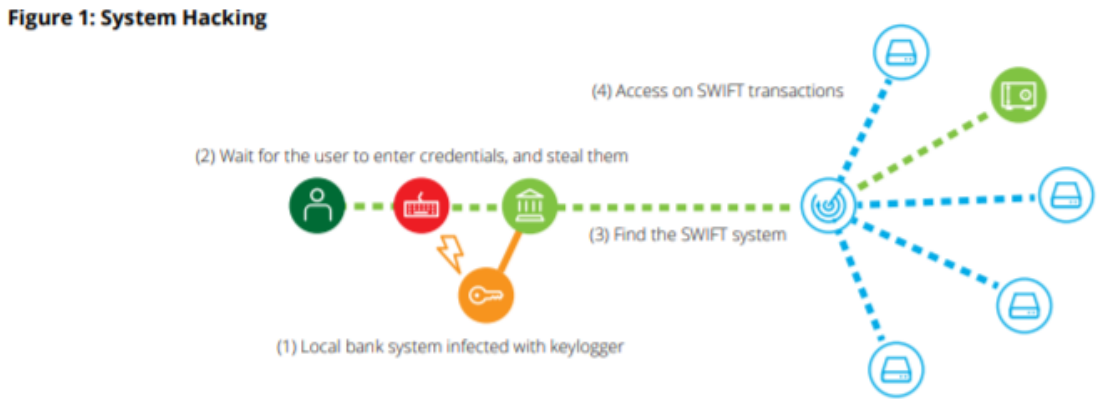
2.4.1. Sisteme İzinsiz Giriş (System Hacking)

Saldırgan, bu yöntemde öncelikle kendi yararına istenmeyen işlemi gerçekleştirmek için SWIFT sisteminin kontrolünü ele geçirecektir. İlk adım, saldırganın banka sistemine girişi ile gerçekleştirilir. Bu senaryoda, bankanın iç sisteminde açıklardan yararlanılarak sisteme izinsiz giriş sağlanır. Sisteme izinsiz giren saldırgan, "keylogger" denilen tuş kaydedici gibi bir yazılımı sisteme yükler. İkinci adımda ise, saldırgan tuş kaydedici sayesinde müşterinin klavyesinde yazdığı tüm parolaları ele geçirir. Bu sayede müşterinin kullanıcı bilgileri ve parolasını girerek müşteri gibi sisteme girmiş olur. Bu senaryoda saldırganın ağa girdiği (diğer bilgisayar sistemlerine / bankanın iç sisteminin bağlı olduğu diğer sistemlere) varsayılarak son aşamada ağı istediği gibi tarayarak istediği SWIFT sistemine giriş yaptığı varsayılmaktadır. Bu aşamadan itibaren, saldırgan, SWIFT sistemi içerisinde istediği işlemleri yapmaya ve istediği talimatları vermeye hazır hale gelmiştir.

SWIFT sistemlerine yönelik "sisteme izinsiz giriş saldırılarının aşamaları aşağıdaki şemada özetlenmiş olup kısaca bu saldırıdaki şemada belirtilen adımları özetlemek gerekirse: (i) Tuş kaydedici yazılımının yerel bankanın sistemin enjekte edilmesi, (ii) kullanıcının giriş parolasını çalmak amacıyla sisteme giriş yapılmasının beklenilmesi, (iii) SWIFT sisteminin bulunması, (iv) SWIFT işlemlerine saldırganlar tarafından erişim sağlanması[238].

[237] Deloitte, "SWIFT Systems and the SWIFT Customer Security Programme: https://www2.deloitte.com/content/dam/Deloitte/be/Documents/risk/be-ra-swift-customer-security-programme.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[238] Şekil –2.9'da yer alan İngilizce açıklamalar yazar tarafından tercüme edilmiştir. Şekil 2.9'un aktarıldığı web sitesi: https://www2.deloitte.com/content/dam/Deloitte/be/Documents/risk/be-ra-swift-customer-security-programme.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

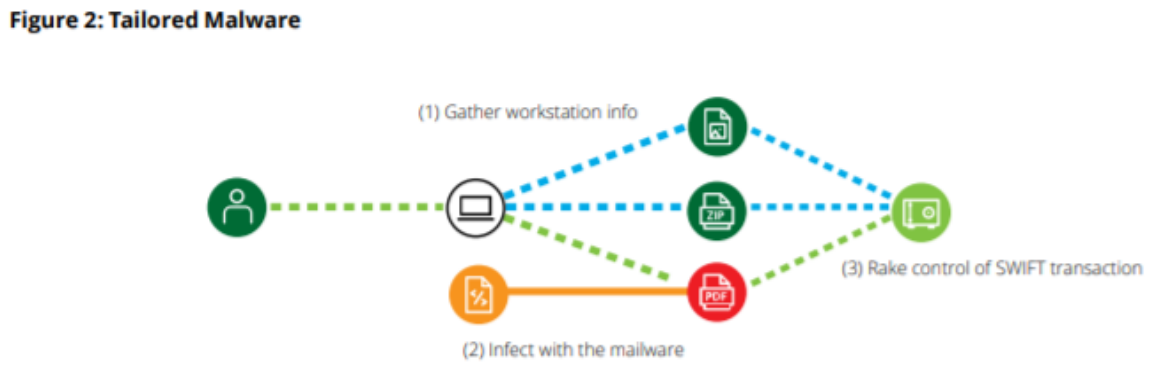


Şekil -2.9: Sisteme İzinsiz Giriş

2.4.2. Zararlı Yazılım Vasıtasıyla SWIFT Dolandırıcılığı (Tailored Malware)

Bu yöntemde genelde siber saldırgan, bankanın kullandığı yazılıma kolaylıkla uyum sağlayacak ve fark edilmesi zor bir yazılım vasıtasıyla SWIFT dolandırıcılığını gerçekleştirir. Bu yöntem için ilk adım bilgi toplama aşamasından oluşur. Bu aşamada, saldırgan öncelikle zararlı yazılım enjekte edeceği ve banka çalışanlarının kullandığı yazılım ile ilgili gereken bilgiye (örneğin yazılımın hangi versiyon olduğu, güncel olup olmadığı vb.) sahip olmalıdır. Bu bilgiye genelde saldırgan, sosyal mühendislik tekniklerini kullanarak ulaşır. Bu bilgiye ulaşılması akabinde ise, yazılım içeriğindeki herhangi bir boşluktan yararlanacağı varsayılmaktadır. İkinci adımda ise, bulunan açıktan faydalanılarak saldırgan tarafından sisteme zararlı yazılım enjekte edilir. İstismar denilen son aşamada ise, ilgili yazılım üzerinde işleyen SWIFT işlemlerinde, saldırganın sisteme yüklenen zararlı yazılım sayesinde arzu ettiği gibi işlemleri değiştirme imkânı söz konusudur. Örneğin, saldırgan paranın havale edileceği hesabı değiştirerek SWIFT sistemi üzerinden paranın kendi hesabına gönderilmesini sağlayabilir. Bu aşama açısından, saldırgan açısından önem arz eden husus, sistem üzerinde herhangi bir iz bırakılmamasıdır.

SWIFT sistemine yönelik zararlı yazılımlar vasıtasıyla gerçekleştirilen saldırıların aşamaları ise aşağıda Şekil 2.10'da belirtilmiş olup kısaca şu şekilde özetlenebilir: (i) İşyerine ilişkin bilgi edinilmesi, (ii) Zararlı yazılımın sisteme enjekte edilmesi, (iii) SWIFT işlemlerinde kontrolün ele geçirilmesi[239].



Şekil 2-10: Zararlı Yazılım Vasıtasıyla SWIFT Dolandırıcılığı

2.5. ZARARLI YAZILIMLARIN BANKACILIK VE FİNANS SEKTÖRÜNE ETKİLERİ

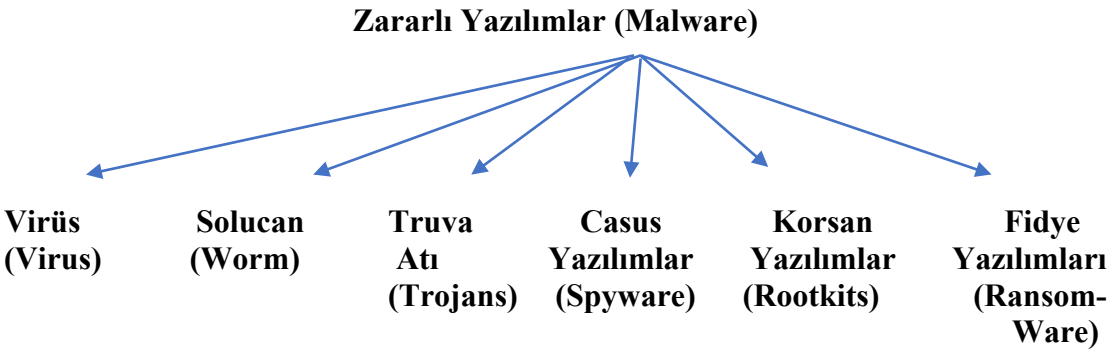
İngilizce "malware" olarak ifade edilen zararlı yazılım kavramı, aslında "malicious software" kelimelerinin kısaltmasıdır. Genel itibariyle zararlı yazılımlar ile bilişim sistemlerine çoğu kez fiziken zarar verilmeyip ilgili kurbanların verilerinin silinmesi, çalınması, şifrelenmesi veya bilgi ve rızaları olmaksızın aktivitelerinin takip edilerek gayri yasal yollardan paralarının çalınması amaçlanmaktadır[240].

Bilgisayar teknolojilerinin gelişmesi ile birlikte özellikle elektronik ödemelerde bilgi güvenliği açısından en ciddi tehditlerin başında zararlı yazılımlar gelmektedir. Bu yazılımlar bulaştığı bir bilgisayar sisteminde veya ağ üzerindeki diğer makinelerde

[239] Şekil –2.10'da yer alan İngilizce açıklamalar yazar tarafından tercüme edilmiştir. Şekil 2.10'un aktarıldığı web sitesi: https://www2.deloitte.com/content/dam/Deloitte/be/Documents/risk/be-ra-swift-customer-security-programme.pdf (Gözden Geçirilme Tarihi: 29.10.2020).
[240] *Özkaya/Sarıca/Durmaz*, s. 43, *Çakır/Kılıç*, s. 114, *Sağıroğlu/Alkan*, s. 228.

zarara yol açmak veya hedefteki sistemin çalışmasını aksatmak amacıyla hazırlanmış yazılımların genel adıdır[241]. Forumların, sosyal paylaşım sitelerinin, cinsel içerikli sitelerin ve kaynağı belli olmayan ücretsiz program sunan web sayfalarının, saldırganların başta başkalarına ait finansal bilgiler olmak üzere değerli bilgileri elde etmeye ve kurbanlarının bilgisayarlarına casus yazılımlar yüklemeye çalışabileceği yerler olduğu ve özellikle güvenilir olmayan kaynaklardan, bilinen bir yazılım görüntüsünde indirilen programlarla, P2P[242] havuzunda bulunan torrent[243] gibi paylaşma ağlarından indirilen dosyalarla kullanıcının erişimindeki sistemlere yerleşebileceği dikkate alınmalıdır[244].

Zararlı yazılımlar şu alt kategorilere ayrılarak sınıflandırılabilir:



Şekil-2.11: Zararlı Yazılım Türleri

[241] *Çakır/Kılıç*, s. 29.

[242] "P2P", İngilizce'de "peer to peer" kelime öbeğinin kısaltması olarak kulanılmakta ve Türkçe'de ise "eşler arasında" şeklinde ifade edilmektedir. P2P network denilen "eşler arasındaki ağ programı protokolünde, iki veya daha fazla makine arasında veri kopyası oluşturmak için kullanılan bir ağda her bilgisayarın kendi kaynaklarından sorumlu olduğu ve her bilgisayarın hem sunucu hem de istemci görevi üstlendiği kabul edilmektedir. Dolayısıyla, P2P ağında her bilgisayar kendi kaynaklarını kullanıma açtığı durumda ağdaki diğer bilgisayarların, kendilerine tanınan erişim haklarına bağlı olarak o bilgisayarın kaynaklarına erişme ve kullanma imkânı söz konusudur. Bu konuda ayrıntılı bilgi için bkz. https://www.beyaz.net/tr/ipucu/entry/604/esten-ese-baglanti-p2p-nedir (Gözden Geçirilme Tarihi: 29.10.2020).

[243] Torrent, internet üzerinden film, müzik, kitap, oyun, yazılım gibi programları indirmeye yarayan bir dosya paylaşma tekniğidir. Bu konuda ayrıntılı bilgi için Bkz. https://tr.wikipedia.org/wiki/BitTorrent ve Euegiene Dementiev/Norman Fenton, "Bayesian Torrent Classification by File Name and Size Only": https://www.researchgate.net/publication/322635993_Bayesian_Torrent_Classification_by_File_Name_and_Size_Only/link/5a65b76ca6fdccb61c58d5c4/download (Gözden Geçirilme Tarihi: 29.10.2020).

[244] *Çakır/Kılıç*, s. 114.

2.5.1. Virüs

Teknik açıdan bilgisayar virüsleri, erişim kontrollerini atlatarak bilişim sistemlerinin normal çalışmasını değiştirmek, zarar vermek, bir bilgisayardan diğerine bulaşmak, veri çalmak için tasarlanarak yazılmış ve genellikle meşru programlara ekli olan kötü amaçlı yürütebilir kod ve programlar şeklinde tanımlanabilir[245]. Virüsün bulaştığı bilgisayar açısından en önemli etkinliği aktive olabilmesi için virüsün içinde saklandığı program ya da dosyanın çalıştırılmasının gerekli olmasıdır[246]. Bu şekilde, herhangi bir virüs bir programa, dosyaya veya dokümana bulaştıktan sonra bilgisayar işletim sistemi tarafından çalıştırılmasını müteakip ilgili bilgisayardaki sadece şifrelerin veya verilerin çalınması ve dosyalara zarar verilmesi ile yetinmez, aynı zamanda bir kez bilgisayara bulaştıktan sonra aynı ağda bulunan diğer bilgisayarlara bulaşmaya devam edecektir. Teknik açıdan başlıca virüs türleri olarak, açıldığında bilgisayarın kontrolünü ele geçiren önyükleme (*boot*) virüsleri[247], web sayfalarındaki ve web tarayıcılarındaki açıkları istismar eden web scripting virüsleri[248], web tarayıcısındaki bazı fonksiyonları ele geçirerek otomatik şekilde bazı web sitelerine yönelten browser hijacker[249], bir bilgisayar sisteminin hafızasını yerleşerek işletim sistemi çalıştığı sürece çalışabilen yerleşik (*resident*) virüsler[250], virüs içeren bir dosya çalıştırıldığında aktif olan aksiyon

[245] *Özkaya/Sarıca/Durmaz*, s. 45.
[246] *Graham/Howard/Olson*, s. 198.
[247] https://searchsecurity.techtarget.com/definition/bot-worm (Gözden Geçirilme Tarihi: 29.10.2020).
[248] https://combofix.org/what-are-web-scripting-viruses-how-to-detect-and-remove-it.php (Gözden Geçirilme Tarihi: 29.10.2020).
[249] Browser, bilişim terminolojisi olarak Türkçe'ye "tarayıcı" olarak tercüme edilebilir. Bilişim dünyasında "browser" basit şekilde açıklamak gerekirse "World Wide Web" olarak adlandırılan bilgi ağı üzerinde site ve sayfa incelemek için kullanılan ve bunun için tasarlanmış yazılım ve programa verilen isimdir. Web browser konusunda ayrıntılı bilgi için Bkz. http://www.cs.kent.edu/~svirdi/Ebook/wdp/ch01.pdf (Gözden Geçirilme Tarihi: 29.10.2020). "Browser hijacking virus" denilen ve Türkçe'ye "tarayıcıyı ele geçirmeyi sağlayan virüs" ise saldırgan tarafından kurbanın bilgisayarına enjekte edilen bu zararlı yazılım ile kurbanın bilgisayarındaki browser ayarlarının kontrolünü ele geçilerek kurbanın, saldırganın istediği web sitelerini yönlendirilmesini sağlar. Bu konuda ayrıntılı bilgi için ise Bkz. https://en.wikipedia.org/wiki/Browser_hijacking (Gözden Geçirilme Tarihi: 29.10.2020).
[250] https://www.computerhope.com/jargon/r/resiviru.htm (Gözden Geçirilme Tarihi: 29.10.2020).

virüsleri[251], antivirüs programlarından kurtulabilmek için virüs içeren dosya her çalıştığında kendi kodunu değiştiren poliformik virüsler (*polymorphic virus*)[252], zararlı kodları bir sistemdeki belli fonksiyonları yerine getiren uygulamalara yerleşik olan dosyalara bulaşan virüsler, yazılımlar için aynı makro dilinde yazılmış, sıklıkla e-mail eklentileri aracılığıyla bulaşan makro virüsler[253] olmak üzere değişik türde virüsler bulunmaktadır[254].

2.5.2. Solucan

Bilgisayar virüsleri gibi bilgisayar ağlarını kullanarak bir sistemden diğerine bulaşan ve bulaştığı sistemlerde genelde izinsiz girişlere nedenlere sebep olan programlardır[255]. Virüslerden farklı olarak solucanlar, kendilerini başka bir çalışabilir programa veya dosyaya iliştirmeyip yayılmak için başka bir programa veya insan etkileşimine ihtiyaç duymaksızın kendi kendilerini çoğaltarak bir bilgisayardan diğerine bulaşabilirler. Solucanlar bulaştıktan sonra sessiz sedasız çalışarak kendilerini kopyalayıp, bant genişliği ve sabit disk kapasitesi gibi kaynakları tüketerek bilgisayarı çalışamaz hale getirebilirler[256]. Doktrinde, Sağıroğlu/Alkan tarafından, solucanların genelde sistemlerde arka kapı (*backdoor*)[257] açarak bu sistemleri başka saldırılarda kullandıkları belirtilmekte olup Taner ise solucanların ağları yavaşlattığı üzerinde

[251] *Özkaya/Sarıca/Durmaz*, s. 46.
[252] https://www.pwc.com.tr/tr/medya/kose-yazilari/gokhan-muharremoglu/metamorfik-ve-polimorfik-zararli-yazilimlar.html (Gözden Geçirilme Tarihi: 29.10.2020).
[253] https://www.kaspersky.com.tr/resource-center/definitions/macro-virus (Gözden Geçirilme Tarihi: 29.10.2020).
[254] Virüs türleri ile ilgili örnekler konusunda Bkz. *Özkaya/Sarıca/Durmaz*, s. 45-46.
[255] Bu tanım *Sağıroğlu/Alkan*, s. 229'den aktarılmıştır.
[256] *Graham/Howard/Olsom*, s. 195-198, *Özkaya/Sarıca/Durmaz*, s. 46. Doktrinde, Sağıroğlu/Alkan (s. 229) tarafından, genelde sistemlerde arka kapı açarak bu sistemleri başka saldırılarda kullandıkları belirtilmekte olup Taner (s. 35) ise solucanların, genelde ağları yavaşlattığı üzerinde durmaktadır. Eralp, solucanların en büyük tehlikesinin, bir kez sisteme girdikten sonra kendilerini büyük ölçüde çoğaltma becerisi olduğunu ve kendisini bir bilgisayardan diğerine kopyalamak için tasarlandığını ve bunu otomatik yaptığını ifade etmektedir. Bkz. *Eralp*, s. 73-74.
[257] Arka kapılar (*backdoors*), geleneksel güvenlik mekanizmalarını atlatarak kullanıcı bilgisi dışında sistemi uzaktan erişime açan programları ifade etmekte olup arka kapılar genelde truva atları kullanılarak kurban sistemlere yüklenmekte ve bu doğrultuda sadece arka kapı oluşturan kişiler tarafından bilinmekte olup genelde arka kapılar saldırganlar tarafından daha sonra gerçekleştirilecek olan karmaşık saldırılar için virüs ve solucanlar tarafından kullanılmaktadır. Bkz. *Sağıroğlu/Alkan*, s. 230.

durmaktadır. Bilinen ilk solucan Robert Morris tarafından 1988 yılında internet üzerinden yayılan ve Morris solucanı olarak bilinen, Unix yazılımlarındaki açıklardan faydalanarak ve çoğu kişinin kişinin bilgisayar sisteminde DoS[258] denilen internet servisinin hizmet dışı kalmasına sebebiyet veren ilk büyük çaplı atak olarak tarihe geçmiştir[259]. Cod Red, Nimda, MyDoom, Conficker ve Stuxnet'in en yaygın bilinen solucanlar olarak gösterilmiştir[260].

2.5.3. Truva Atı

Truva atı, en basit şekliyle bir faydalı yazılım içerisinde normal bir program gibi gözüken ya da çeşitli yöntemlerle hedefli olarak gönderilen ve içinde kötü amaçlı kodlar barındıran[261], gönderildiği yerde çalıştırıldığında göndericisine menfaat sağlayan ve istenen operasyonun kılığına girerek kötü amaçlı operasyonlar yapan zararlı yazılımlar olarak tanımlanabilir[262]. Mitolojide, nasıl bir armağan gibi gözüküp aslında tuzak kurmak amacıyla bir şehrin ele geçirilmesine fayda sağladı ise, truva atlarının günümüzde yararlı yazılımlar gibi gözükerek aslında bilgisayarı çeşitli şekillerde tehlikeli duruma atan[263] bilgisayar programları olduğu bilinmektedir. Truva

[258] Bu kavram çalışmanın 2.6.1. başlığı altında "Hizmeti Engelleme Saldırıları Ve Botnetler başlığı altında ayrıntılı şekilde açıklanmıştır.
[259] *Graham/Howard/Olson*, s. 195.
[260] *Sağıroğlu/Alkan*, s. 229.
[261] Doktrinde, Eralp tarafından normal bir program olarak gözüken ancak içinde kötü amaçlı yazılımlar içeren bir truva atına örnek olarak, Microsoft'un güvenlik güncelleştirilmeleri olduğu iddia edilen eklerin bulunduğu bir elektronik posta görünümündeki truva atının, daha sonradan saldırganlar tarafından Microsoft'a yönelik virüsten koruma ve güvenlik duvarı yazılımlarını devreden çıkarmayı amaçlayan virüsler olduğunun fark edildiği ifade edilmiştir. Söz konusu yazara göre kullanıcıları daha iyi korumak için Microsoft ve benzeri kuruluşların elektronik posta vasıtasıyla güvenlik bültenleri gönderdikleri ancak bu elektronik postalarda hiçbir zaman ek bulunmayacağı belirtilmiştir. Bkz. Eralp, s. 75.
[262] *Taner*, s. 35, *Özkaya/Sarıca/Durmaz*, s. 46, *Sağıroğlu/Alkan*, s. 229, *Eralp*, s. 75-76, ayrıca Bkz. Kaspersky Lab., "What is a Trojan Virus?": https://www.kaspersky.com/resource-center/threats/trojans (Gözden Geçirilme Tarihi: 29.10.2020)
[263] Özkaya/Sarıca/Durmaz, truva atlarının aktive edilmesi sonrasında bilgisayarı gizlice izleyebildiği, bilgisayara yetkisiz bir şekilde erişim sağlayabildiği, internet hız genişliğinin bir bölümünü kullanarak bilgisayar hızını yavaşlatabildiği, hassas bilgileri çalabildiği, dosyaları silebildiği veya dosyalar üzerinde değişiklik yapabildiğini ifade etmektedir. Bkz. *Özkaya/Sarıca/Durmaz*, s. 47.

atlarının, virüsler ve solucanlardan farklı olarak yayılma özelliği bulunmamaktadır[264]. Sağıroğlu/Alkan[265] truva atlarının sistemleri etkileyebilmeleri için bu tür yazılımların daha ziyade sistemde arka kapılar (backdoor) açarak sisteme izinsiz olarak uzaktan erişime neden olabildiği üzerinde durmakta iken, Özkaya/Sarıca/Durmaz[266] ise truva atlarını kullanan saldırganların güvenliği üst düzeyde olan bilgisayar sistemlerine doğrudan saldırmak yerine, sistem içerisindeki ağın en zayıf halkası olan nesnelerin interneti teknolojisinin hâkim olduğu arabalar, lambalar, bebek takip sistemleri, evler, ofisler ve oyuncak bebekler gibi aygıtların kontrollerini ele geçirmek suretiyle siber saldırıların gerçekleştirildiğini belirtmektedir.

Elektronik ödeme sistemlerinde en büyük risklerden birisi bankacılık truva atlarıdır *(banking trojans)*. Bankacılık truva atları, esas itibariyle casus yazılımlar *(spyware)* olup bankalar ve finansal kuruluşlardan parola ve kimlik bilgilerini çalmak maksadıyla veya online bankacılık işlemlerinde oturum çalmak amacıyla tasarlanmış yazılımlardır. Bu noktada, saldırganlar genelde kullanıcılara gönderdikleri bir elektronik posta eklentisine sakladıkları istismar kiti ile kurbanların bilgisayarlarına truva atı bulaştırır. Daha sonraki süreçte ise kurbanın bilgisayarında ilgili internet bankacılığına ziyaret etmesi halinde tekrar harekete geçen saldırgan bu kez tuş kaydediciler (*keylogger*)[267]

---

[264] *Çakır/Kılıç*, s. 28. Literatüre bakıldığında, Graham/Howard/Olson ise virüs, truva atı ve solucanlar konusundaki ayrımı teknik açıdan şu şekilde ifade etmektedir: Truva atlarının etkisi, aslında meşru ve hukuka uygun olduğu düşünülen bir zararlı yazılımın bilgisayar sistemini etkilemesi iken solucanlar ise kendi kendine çoğalabilir ve başka bilişim sistemlerine aktarılabilir bir zararlı yazılım olarak karşımıza çıkmaktadır. Virüsler ise, solucan ve truva atından farklı olarak kendi kendine çoğalma imkânı olmayan ve kurbanın bilişim sistemine enjekte edilebilmesi için bir web sitesi veya e-mail yoluyla genelde aktarılması mümkün olan zararlı yazılımladır. Bkz. *Graham/Howard/Olson*, s. 198.

[265] *Sağıroğlu/Alkan*, s. 229-230.

[266] *Özkaya/Sarıca/Durmaz*, s. 46-47.

[267] Tuş kaydediciler (*keyloggers*) da esas itibariyle casus yazılım olarak klavyeden girilen bilgiler, ziyaret edilen web siteleri, elektronik posta haberleşmesi, sohbet odaları mesajlaşmaları ve diğer sistem bilgilerini toplamak amacıyla tasarlanmış zararlı yazılımlardır. Bkz. *Özkaya/Sarıca/Durmaz*, s. 51, *Graham/Howard/Olson*, s. 224. Keylogger programlarına örnek olarak, iSpyNow, Perfect Keylogger, Phantom, KeySnatch ve KeyLoggerPro gibi programlar örnek gösterilebilir ve keylogger çeşitleri şunlardır: (i) Yazılımla Çalışan Keylogger, (ii) Donanımla Çalışan Keylogger, (iii) Güvenlik Amaçlı Keylogger. Keylogger konusunda detaylı bilgi için bkz. İsmail Bülbül/Poyraz Emre Bingöl, "Etik Hackerlığa Giriş, Ofansif Siber Güvenliğin ABC'si", Hayykitap, İstanbul, 2019, (*"Bülbül/Bingöl"*), s. 50. Mitnick/Simon ise, "Sızma Sanatı" adlı kitabında tuş kaydedici yazılımların ve parola kırma

aracılığıyla klavyeden girilen bilgileri ve bu konuda gerekli tüm formları çalma imkânına kavuşur. Bu konuda ikinci bir yöntem ise bankacılık truva atları vasıtasıyla saldırganın kendisinin yarattığı ve kullanacağı internet bankacılığına ait web sayfasının benzerini yaparak ve kurbanı sahte olan sayfaya yönlendirerek kullanıcının parola ve ödeme bilgilerini çalmasıdır[268].

2018 yılı açısından öne çıkan bankacılık truva atlarına, Emotet, Trickbot, Panda Banker (Zeus), URLZone (Bebloh), Ursnif (Gozi), TrickBot, IcedID, GootKit, Dridex, Corebot ve TinyNuke (NukeBot) örnek verilebilir[269].

2.5.4. Casus Yazılımlar (Spyware)

Kısaca kullanıcı ve parola bilgileri gizlice toplayıp saldırgan veya üçüncü kişilere gönderen yazılım olarak tanımlanabilir[270]. Casus yazılımların en belirgin özelliği, özellikle bilgisayarlara ve mobil cihazlara bulaşarak kullanıcı hakkında internet kullanım alışkanlıklarından, elektronik posta adresleri, kredi kartı bilgileri olmak üzere kişiler açısından hassas ve kritik derecede önem taşıyan bilgilerin saldırganlar tarafından ele geçirilmesini sağlamasıdır[271]. Farklı casus yazılım tiplerine parola

saldırılarının önemini ortaya koymak açısından şu çarpıcı örneği vermiştir: Yazar, Gabriel denilen bilgisayar korsanının öncelikle bankanın güvenlik duvarına giren parolayı bularak sisteme giriş sağlamış, ardından "Spy Lantern Keylogger" denilen tuş kaydedici yazılım sayesinde banka yöneticilerinden birisinin parolasını ele geçirerek banka ile ilgili şu işlemleri yapabilecek yetkinliğe ulaşmıştır: (i) banka gişesindeki bir memurun gerçekleştirebileceği tüm faaliyetler, (ii) müşteri hesap bilgilerinin görüntülenmesi ve değiştirilmesi, (iii) bankanın dünya çapında ATM faaliyetlerinin izlenmesi, (iv) kredi kontrolleri için Equifax erişimi, (iv) bankaya ait geçmişe yönelik çekler için mahkeme dosyalarının incelenmesi. Bu konuda detaylı bilgi için bkz. Kevin D. Mitnick/William L. Simon, "Sızma Sanatı", Odtü Yayıncılık, 2017, (*"Mitnick/Simon"*), s. 178-179.

[268] *Özkaya/Sarıca/Durmaz*, s. 49.

[269] *Özkaya/Sarıca/Durmaz*, s. 49.

[270] *Sağıroğlu/Alkan*, s. 231.

[271] *Özkaya/Sarıca/Durmaz*, s. 48,49. Bu konuda Graham/Howard/Olson ise casus yazılımların özellikle yayılma özelliği bakımından virüs ve solucanlardan teknik açıdan farklılık gösterdiğini belirtmektedir. Detaylı bilgi için Bkz. *Graham/Howard/Olson*, s. 224.

çalıcılar (*password stealers*)[272], bankacılık truva atları (*banking trojans*), Emotet[273], bilgi çalıcılar, tuş kaydediciler (*keyloggers*) ve istenmeyen e-postalar (*spam*[274]) örnek olarak gösterilebilir[275].

2.5.5. Korsan Amaçlı Kullanılan Yazlımlar (Rootkits)

Bilişim dünyasında "Rootkit" olarak bilinen korsan amaçlı yazılımları, kurbanın kullandığı bilgisayarın işletim sistemi çekirdeğine sızarak saldırganlara bilgisayarlar üzerinde tam yetki vermesi sebebiyle en tehlikeli zararlı yazılım türü olarak değerlendirilmektedir. Rootkit vasıtasıyla yapılan siber saldırının karakteristik özellikleri şunlardır: Öncelikle söz konusu zararlı yazılım işletim sistemi çekirdeğinde çalışması sebebiyle bilgisayarda tespiti, analizi ve yok edilmesi oldukça zordur[276].

---

[272] Parola çalıcılar, bulaştığı bilgisayardan parola bilgilerini toplamaya çalışır. Toplanan parolalar web tarayıcıda depolanan e-mail veya başka bir hesaba girmek için kullanılan kimlik ve yetkilendirme bilgi ve formları olabilir. Bu sayede, saldırganlar ya kendileri parola çalıcılar sayesinde elde ettikleri bilgiler ile kurbanların parolalarını kullanarak kritik düzeyde bilgilerine ulaşır ya da bu bilgileri toplayıp istedikleri başka bir adrese gönderebilir. Bkz. *Özkaya/Sarıca/Durmaz*, s. 49.

[273] Burada bireylerin doğrudan ödeme kapasitelerine bağlı olarak kurbanlarına fidye yazılım şeklinde zarar veren bir yazılım olması sebebiyle Emotet hakkında bahsedilmesinde fayda görülmüştür. "Emotet", ilk olarak 2014 yılında bankacılık truva atı olarak ortaya çıkarak polimorfik yapısı gereği zaman içerisinde kendisini geliştirerek 2018 yılında "TrickBot" denilen diğer bir zararlı yazılım ile birlikte çalışması neticesinde Almanya'da ciddi bir siber saldırı gerçekleştirilmiştir. Saldırganlar, bu bahsi geçen zararlı yazılımlar ile önce kurbanların ödeme bilgilerini elde ederek ödeme kapasitelerini öğrenmiş, akabinde ise bir fidye yazılımı saldırısı ile kurbanların önemli bilgilerini şifrelemiştir. Bu yazılım ile istenen fidye her kurban açısından ödeme kapasitesine göre farklılık teşkil etmiş ve Alman Federal Bilgi Güvenliği Dairesi (BSI) raporlarına göre bu zararlı yazılımlar sonucunda talep edilen fidye rakamları birkaç yüz Avro ile yüz binlerce Avro arasında değişmektedir. Bu konuda ayrıntılı bilgi için Bkz. *Özkaya/Sarıca/Durmaz*, s. 50 ve Chip Dergisi, Sayı: 2020/24, ISSN: 1300-9419, Yıl: 24, 2020 Hacker Raporu, (*"Hacker Raporu"*), s. 47.

[274] "Spam" kelimesi, bir Amerikan şirketinin baharatlı domuz eti için kullandığı "spiced pork and ham" baş harflerinden oluşan İngilizce kökenli bir kelimedir. Spam genellikle pazarlama ve reklam amaçlı kendi tanıtımını yapmak isteyen şirketlerin veya kişilerin kendi tanıtımlarını ilettikleri kişilerin rızası olmaksızın cep telefonu, e-posta gibi istenmeyen mesaj içeriklerine verilen isimdir. Bkz. *Eren*, s. 45.

[275] *Özkaya/Sarıca/Durmaz*, s. 49-51.

[276] Literatürde Sağıroğlu/Alkan, korsan amaçlı yazılımların en tehlikeli yazılım türü olmasını, bu yazılımların asıl amacının varlığını çoğaltmak yerine gizlemek olduğunu ve bu yazılımların özellikle virüs, truva atı ve solucan gibi diğer zararlı yazılımlar ile birleşerek yıkıcı bir saldırıya neden olabileceği üzerine vurgu yapmıştır. Bkz. *Sağıroğlu/Alkan*, s. 231. Özkaya/Sarıca/Durmaz tarafından bu konuda yapılan araştırmada ise rootkitler konusunda bu zararlı yazılımların kendilerini gizleme konusunda yıkıcı bir etkisi olması değerlendirmekle beraber aslında bu yazılımın verdiği en kritik zararın söz konusu korsan yazılımın bilgisayardaki hangi platforma yerleştiği ve yerleştiği alandaki etkinin değerlendirilmesi ve gerekli önlemlerin alınmasının özellikle ileri bir işletim sistemi ve donanım bilgisi

Buna ilaveten, rootkit yüklenebilmesi için saldırganın ileri düzeyde işletim sistemi ve donanım bilgisine sahip olması gerektiğinden, rootkit yükleyen saldırganın gerçekten profesyonel bir saldırgan olduğu kabul edilmelidir. Bu noktada saldırganın rootkit ile kredi kartı bilgilerini ele geçirilmesi, web kamerası veya mikrofon gibi donanımları kurcalayarak mahremiyeti ihlal etmesi ve aşağıda ayrıntılı şekilde açıklanacak DDoS ve Botnet saldırıları gibi sanal saldırılar yapma imkânı olduğundan rootkit ile yapılan saldırının neredeyse sınırlarının olmadığı sonucuna varılmaktadır[277].

Korsan amaçlı yazılımların bilgisayarda bulaştığı platforma göre "Kernel Rootkit[278]", "Firmware Rootkit"[279], "Application Rootkit"[280], "Memory Rootkit"[281] gibi türleri söz konusudur.

2.5.6. Fidye Yazılımları (Ransomware)

Fidye yazılımları, diğer zararlı yazılımlarda olduğu gibi bilgisayarların işletim sistemine bulaşarak dosyaların kullanılmasını ve erişimini şifreleme yöntemi ile

---

gerektirmesi sebebiyle bu yazılımların özellikle kullanıcılar açısında risk teşkil ettiği değerlendirilmiştir. Bu konuda ayrıntılı bilgi için Bkz. *Özkaya/Sarıca/Durmaz*, s. 51 ve benzer değerlendirme için bkz. *Graham/ Howard/ Olson*, s. 219-223.

[277] Korsan amaçlı yazılımlar konusunda detaylı bilgi için Bkz. *Özkaya/Sarıca/Durmaz*, s. 52, *Taner*, s. 35, *Sağıroğlu/Alkan*, s. 230-231.

[278] İngilizce'de "kernel" kelimesi çekirdek anlamına gelmekte olup bilişim açısından konuya bakıldığında işletim sistemi çekirdeğini ifade etmektedir. Çekirdek, işlevsel açıdan işletim sistemi üzerinde herşeyin üzerinde denetimi olan merkezi bir bileşen olması sebebiyle kullanıcı ile doğrudan etkileşime geçmez. Çekirdek, uygulamalar ile CPU, bellek ve disk sürücü gibi donanımsal bilgi işlemleri arasında etkileşimi sağlar. Bu konuda ayrıntılı bilgi için Bkz. http://www.linfo.org/kernel.html (Gözden Geçirilme Tarihi: 29.10.2020). Çekirdek seviyesinde işletilmesi sebebiyle saldırgana bilgisayar üzerinde tam bir yetki veren ve sisteme büyük zarar verebilen yazılımlardır. *Graham/Howard/Olson*, s. 221-223.

[279] Firmware rootkit, genelde network cihazları gibi donanım gömülü aygıtlar üzerinde etkili olup cihaz açık olduğu sürece aktivitelerine devam etmektedir. Bkz. *Özkaya/Sarıca/Durmaz*, s. 52.

[280] Application rootkit, adından da anlaşılacağı üzere, bu tür yazılımlar uygulama düzeyinde çalışarak uygulama dosyalarını rootkit yazılımları ile değiştirerek veya kod yerleştirerek uygulamanın normal çalışmasını değiştirir veya tamamen engeller. Bkz. *Özkaya/Sarıca/Durmaz*, s. 52.

[281] Bu yazılımlar ise bilgisayarın RAM performansını düşürmeye yönelik yazılımlardır. İngilizcesi "Random Access Memory" olan RAM, bir bilgisayarın işletim sistemi ile uygulama programlarının bulunduğu ve bilgisayar işlemcisinin hızlı şekilde veriye erişmesini sağlayan donanımını ifade etmektedir. Bkz. Peter Haugen/Ian Myers/Bret Sadler/John Whidden, "A Basic Overview of Commonly Encountered Types of Random Access Memory (RAMs) (*"Haugen Ve Diğerleri"*): https://www.rose-hulman.edu/Class/ee/yoder/ece332/Papers/RAM%20Technologies.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

engelleyen ve belirli bir ödemenin yapılması karşılığı şifrelemenin kaldırılacağını vaad eden yazılımların genel adıdır[282].

Günümüzde fidye yazılımların yaygınlaşmasında en önemli faktörlerden birisi kripto paraların yaygın kullanılmasıdır. Zira, kripto paralar merkezi bir para kuruluşu tarafından tedavül edilmediği ve takibinin zor olması sebebiyle fidye yazılımların karşılığında ödemelerin saldırganlar tarafından genelde bitcoin ile yapılması talep edilmektedir. En yaygın olarak bilinen fidye yazılımlara, "WannaCry"[283], "NotPetya", "SimpleLocker", "CyroptoLocker", "TB-Locker", "Winlock" örnek olarak gösterilebilir[284].

Bankacılık truva atlarının yanı sıra doktrinde, SpyEye ve ZeuS gibi zararlı yazılımların internet bankacılığı işlemlerinde kullanıcıların bankacılık bilgileri, web e-posta servisi ve diğer finansal servis bilgilerini (örneğin PayPal hesapları) çalmakta kullanıldığı ve siber suçluların hedef kullanıcıların bilgilerini elde etmek için WebInject dosyaları gibi pop-up pencereler kullanmak yerine Otomatik Transfer Sistemleri ("ATS") gibi

---

[282] Bu tanım *Özkaya/Sarıca/Durmaz*, s. 53'den aktarılmıştır. Doktrinde Sağıroğlu/Alkan, fidye yazılımların bulaştığı sistemin bir kısmını veya tamamını şifreleyerek verilerin kullanıcı tarafından görüntülenmesini engelleyen programlar olduğunu ve özellikle saldırganın talep ettiği paranın ödenmesinin sistem verilerine erişimi garanti etmeyeceğini belirtmektedir. Bkz. *Sağıralu/Alkan*, s. 230. Taner ise fidye yazılımlar konusunda özellikle fidye yazılımların genelde indirilen veya yazılım güvenlik açığından faydalanarak sisteme bulaştığı ve bilgisayardaki verileri kullanıcı tarafından bilinmeyen bir anahtarla şifrelediği için neredeyse fidye yazılımın kırılmasının imkânsız olduğuna dikkat çekmektedir. Bkz. *Taner*, s. 34.

[283] 2017 yılında Shadows Brokers adı verilen bir siber saldırgan grubu tarafından sızdırılan "WannaCry" yazılımının dikkat çeken özelliği hem bir fidye yazılımı hem de solucan gibi hareket ettiği bilinmekte olup bu zararlı yazılım teknik açıdan "ransomware kripto solucanı" (*ransomware crypto-worm*) olarak nitelendirilmiş ve yüzden fazla ülkede farklı sektörlerden yüz binlerce kişisel ve kurumsal sistemi etkisi altına aldığı görülmüştür. WannaCry yazılımının kısaca çalışma mantığından bahsetmek gerekirse, bu zararlı yazılım öncelikle bulaştığı bilgisayardaki yerel ağdaki diğer bilgisayarları da tarayarak bu bilgisayarlar arasında EternalBlue açığı bulunan bilgisayarlarda etkisini göstererek sisteme "DoublePulsar" denilen zararlı yazılımı enjekte edip, öncelikle klasik bir fidye yazılımı gibi cihazdaki dosyaları şifrelemiş, akabinde ise süre vererek bu şifrelemenin çözülebilmesi için Bitcoin karşılığında ödeme talep etmiştir. Bu konuda detaylı bilgi için bkz. *Özkaya/Sarıca/Durmaz*, s. 53-54. Ayrıca, Bitcoin gibi kripto paraların illegal faaliyetlerde kullanılma meselesi ise çalışma kapsamında ayrıntılı şekilde 2.7.3. numaralı "İllegal Faaliyetler" başlığı altında değerlendirilecektir.

[284] *Sağıralu/Alkan*, s. 230.

görünmez nesneler kullanmaya başladıklarını ve bu ATS'lerin kullanıcıların bilgisi olmaksızın sistemde kaldığı sürece etkin şekilde illegal transferlere olanak sağlaması sebebiyle internet banka dolandırıcılığına olumsuz yönde katkı sağladığı üzerinde durulmuştur[285].

2.6. AĞLARA YÖNELİK GERÇEKLEŞTİRİLEN SİBER SALDIRILAR

Ağa yönelik saldırıların açıklanmasından önce, konunun teknik boyutu itibariyle anlaşılması açısından kısaca bazı terimlerin ne anlama geldiğinin açıklamasında fayda görülmektedir.

Ağ (network), günümüzde bilgisayarların iletişim hatları aracılığıyla birbiriyle iletişime geçebilmesini ve veri aktarımını gerçekleştirmesini sağlayan sistem bütünüdür[286]. IP adresi, internete bağlı olmasına bakılmaksızın her bilgisayara hizmet sağlayıcılar ya da yerel IP sağlayıcılar tarafından belirlenen adres ile internette ve iç ağlarda iletişim haline olunmasını sağlayan bir araç şeklinde nitelendirilebilir[287]. Günümüzde IPv4[288] ve IPv6[289] olmak üzere iki farklı adresleme türü bulunmaktadır.

Üçüncü Bölüm'de özellikle ağ güvenliğinin temini açısından ağ katmanlarının oluşturulmasında bir standart olarak kabul edilen OSI modeli hakkında daha detaylı bilgi verilecektir. Ağ güvenliğinin önemi, günümüzde tüm veri aktarım işlemleri büyük ölçüde ağ üzerinden gerçekleştirildiğinden aktarma işlemleri esnasında buna hizmet eden ünitelerden birisinin görevini yerine getirememesi veya daha kötüsü yönetiminin

---

[285] Loucif Kharouni, "Automatic transfer system: "The latest cybercrime toolkit feature trend micro incorporated research paper", (*"Kharouni"*), Trend Micro: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_automating_online_banking_fraud.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[286] *Altınkaynak*, s. 187.

[287] *Altınkaynak*, s. 187.

[288] İngilizce'de "Internet Protocol version 4"ün kısaltmasıdır. IPv4 adreslemesi 32 bit olup, 2 üzeri 32 üzerinden hesaplandığında, dört milyardan fazla adreslemeye imkân tanımaktadır. Bu konuda detaylı bilgi için bkz. *Altınkaynak*, s. 188.

[289] IPv6'da adresleme ise, 128 bit olup 2 üzerinden 128'den hesaplandığında IPv4'e kıyasla çok daha fazla adresleme imkânı tanıdığı (rakamsal olarak 340282366920938463463337460743176821145 6) bilinmektedir. Bkz. *Altınkaynak*, s. 188.

başkası tarafından ele geçirilmesi tüm kontrolün kaybedildiği anlamına gelecektir. Bu nedenle, ilerleyen kısımlarda daha teknik detayları aşağıda açıklanacağı üzere ağ güvenliği açısından OSI modeli, OSI modelini meydana getiren katmanların neler olduğu ve her bir katmanın ayrı ayrı güvenliği ağ güvenliğinin temini açısından önem taşımaktadır.

Bilgisayar ağlarında cihaz ve ağ protokollerinin çalışma prensiplerindeki açıklardan faydalanmak suretiyle gerçekleştirilen ve ağ ortamlarını tehdit eden yaygın saldırı çeşitleri aşağıda sistematik şekilde açıklanmıştır:

2.6.1. Hizmeti Engelleme (DoS/DDoS) Saldırıları Ve Botnetler

Başta finans sektörü olmak üzere birçok sektör açısından en yaygın siber saldırı türü olan DoS ve DDoS saldırıları aynı zamanda ağlara yönelik en bilinen saldırı türüdür[290].

Hizmet dışı bırakma saldırısı[291] denilen DoS saldırısı, tek bir kaynaktan hedefe doğru, hedef olarak belirlenen sistemin kaynaklarını tüketmek ve sistemin hizmet vermesini engellemek amacıyla gerçekleştirilen siber saldırıyı ifade etmektedir. Bu saldırı türünde bilgi güvenliğinin özellikle yukarıda değinilen erişebilirlik (*avaliability*) denilen unsuru hedef alınarak sistemin erişilmez kılınması amaçlanmaktadır. DDoS[292] ise, saldırının şiddetini, etkisini ve süresini artırmak amacıyla çok sayıda kaynaktan eş zamanlı ve kümülatif gerçekleştirilen DoS saldırılarını ifade etmek için kullanılan bir siber saldırı yöntemidir. DoS/DDoS saldırılarında asıl amaç sistemin mevcut ağ kapasitesinin üzerinde anlık istek, anlık bağlantı talebi ile sistemin kapasitesinin

[290] Gartner şirketinin siber güvenlik uzmanı olan Avivah Litan'a göre bankalara ve finansal kuruluşlara yönelik gerçekleştirilen siber atakların % 30'u dolaylı yollardan gerçekleştirilmekte olup DDoS saldırısı bu anlamda siber saldırganlar tarafından daha ziyade dikkat dağıtmak maksadıyla kullanılmaktadır. Bu konuda detalı bilgi için Bkz. https://www.cnet.com/news/cybercrooks-use-ddos-attacks-to-mask-theft-of-banks-millions/ (Gözden Geçirilme Tarihi: 29.10.2020).
[291] İngilizce'de "Denial of Service" teriminin kısaltması olarak "DoS" terimi kullanılmaktadır.
[292] İngilizce'de "Distributed Denial of Service" teriminin kısaltması olarak kullanılmakta olup Türkçe'ye "Dağıtık Hizmet Dışı Bırakma" şeklinde tercüme edilebilir.

doldurularak sistemin işleyişini engellemektedir[293]. Başka bir ifade ile DoS/DDoS ataklarında, telekomünikasyonun omurgasını[294] teşkil eden ve internet üzerinden bilgi alışveriş imkânını sağlayan web siteleri veya FTP[295] olarak ifade edilen dosya iletim protokolü servisini hedef alarak sunucuların ve internet servisinin çalışmasının engellenmesi hedeflenmektedir. Aslında teknik açıdan bakıldığında, bir bilgisayar ağında belirli bir zaman aralığında sadece o ağın bant genişliğine bağlı olarak sınırlı sayıda verilerin transfer edilmesi mümkündür. DoS ve DDoS saldırılarında ise ağın bant genişliğinin kaldırılabileceği kapasitesinin üzerinde bir veri alışverişi gerçekleştirilerek ağ trafiğinin sistemden faydalanmak isteyen diğer kullanıcıların sisteme erişememesi amaçlanmaktadır[296].

Doktrinde Altınkaynak'a göre, DDoS saldırılarında teknik açıdan en önemli konulardan birisi paket boyutu olarak değerlendirilerek saldırıya maruz kalan paket boyutunun küçülmesinin veri aktarımında hız bakımından performansı düşürmekle beraber maruz kalınan saldırının şiddetini azaltmada etkili olduğu belirtilmiştir. Bahsi geçen yazar, aynı zamanda DDoS saldırılarında bant genişliği hedef alındığı takdirde bunu önlemenin imkânı olmadığını özellikle vurgulayarak saldırıda amacın ağ cihazlarını yormak üzere kurgulandığı takdirde ise bu saldırının başarısının, ağ cihazlarının kapasitesine bağlı olduğunu belirtmiştir[297].

---

[293] *Özkaya/Sarıca/Durmaz*, s. 68, *Eralp*, s. 68-69.

[294] İngilizcesi "backbone" olan bu kavram aslında Türkçe'ye "omurga" olarak tercüme edilse de, bilişim terminolojisinde telekomünikasyon ağı üzerindeki temel geçiş yollarını (*pathway*) oluşturan yüksek hızlı hat ve bağlantıların oluşturduğu yapıyı ifade etmektedir. https://www.nolto.com/telekomunikasyon/telekomunikasyon-nedir/ (Gözden Geçirilme Tarihi: 29.10.2020).

[295] FTP, İngilizce'de "File Transfer Protocol" sözcüklerinin kısaltması olup, dosya transfer protokolü anlamına gelmektedir. FTP, aslında internet ağına bağlı olan bir bilgisayardan diğerine kurulan bağlantı sonucu dosya aktarımı yapılması için tasarlanan bir internet protokolü, başka bir ifade ile bu işi yapmayı sağlayan uygulama programlarına verilen genel isimdir. Bu konuda daha detaylı bilgi için Bkz. https://destek.kmk.net.tr/file-transfer-protocol-ftp-nedir.html (Gözden Geçirilme Tarihi: 29.10.2020).

[296] *Graham/Howard/Olsom*, s. 159-160.

[297] *Altınkaynak*, s. 200.

DDoS kavramı ile bağlantılı şekilde kullanılan diğer bir kavram ise Botnet olup Botnet kısaca şu şekilde açıklanabilir: Botnet aslında verilen komutlara uyan ve tasarlanma amacına uygun şekilde hareket eden "robot" sözcüğü ile ağ anlamına gelen "network" sözcüklerinin karması olup DDoS saldırılarında zombi olarak adlandırılan köle bilgisayar topluluğunu ifade etmek için kullanılmaktadır. Saldırganlar yukarıda açıklanan truva atı gibi kurbanlarına bazı zararlı yazılımlar bulaştırarak birden çok kurbanın bilgisayarlarını Botnet üyesi köle bilgisayar haline getirir ve bu bilgisayarlar üzerinde çoğu kez kurbanların dahi bilgisi olmaksızın hâkimiyet sağlar. Bu sayede saldırgan birden çok Botnet üyesi köle bilgisayar üzerinden çevrimiçi oldukları zamana bağlı olarak eş zamanlı birden fazla siber atak gerçekleştirme imkânına sahip olur[298]. DDoS saldırısının özellikle dağıtık bir saldırı türü olması ve özellikle saldırının yöneltildiği IP adreslerinin farklı subnetlerde yer alan sahte veya botnet ağlarında yer alan IP adresleri olması sebebiyle teknik açıdan saldırganların yakalanmasının ve engellenmesinin zor olduğu bir saldırı türü olarak kabul edilmektedir[299]. Doktrinde Özkaya/Sarıca/Durmaz'a göre, dağıtık bilgisayar sistemleri olan botnetler çevrim içi (online) bilgisayar sistemlerinin karşı karşıya kaldığı en büyük tehdit olup finansal dolandırıcılık, DDoS saldırıları, istenmeyen e-posta (spam) gönderme, oltalama, bilgi ve bilgisayar kaynaklarının çalınması, kimlik hırsızlığı ve online reklamlarda tıklama sahteciliği (click fraud) gibi birçok saldırıda kullanılabilmektedir[300]. Dülger ise, DDoS saldırılarından farklı olarak tek bir IP adresi yerine daha yüksek sayıdaki IP adresinden gelecek taleplerin log taşması nedeniyle firewall denilen güvenlik duvarı servislerini durduracağını ve DDoS saldırılarını DoS saldırılardan ayıran en önemli özelliğin ise saldırıların farklı sistemlerden yönetilmesi neticesinde sistemin bu şekilde engellenmesi olduğunu belirtmiştir[301].

---

[298] DDoS ve Botnet konusunda detaylı bilgi için Bkz. *Graham/Howard/Olsom*, s. 105-107, *Özkaya/Sarıca/Durmaz*, s. 69, *Eralp*, s. 67-68, *Taner*, s. 38-39.
[299] *Altınkaynak*, s. 200.
[300] *Özkaya/Sarıca/Durmaz*, s. 69.
[301] *Dülger, Bilişim Suçları,* s. 117.

Bilgi güvenliği uzmanlarına göre, DDoS atakları başta internet bankacılığı ve online e-ticaret platformları olmak üzere finans sektöründe en yaygın şekilde rastlanan siber atak türü olarak bilinmekte olup siber saldırganlar tarafından bilgi hırsızlığı ve veri sızıntısı gibi siber saldırılar gerçekleştirilirken dikkat dağıtmak, sistemin hacklenememesi halinde özellikle sisteme zarar vermek veya siber saldırıların salt etkisini göstererek bankaların ve finansal kuruluşların sürekli şekilde işleyişini engelleyerek bu kurumlara zarar vermek noktasında değişik amaçlara yönelik olarak kullanılabilmektedir[302]. Bu noktada, DDoS ataklarının özellikle elektronik ortamda banka ve finans kuruluşlarına her zaman veri sızıntısı gibi bir sonucu bulunmamasına rağmen, çalışmamızda özellikle internet bankacılığı hizmetinden yararlanamayan müşteriler açısından bankaların karşı karşıya kaldığı itibar kaybının (bu konuda veri koruma otoritelerine yapılan bildirim, görsel ve yazılı medyaya bu durumun yansıması vb.) çoğu kez yaşanan finansal kayıptan çok daha ağır sonuçları olduğu değerlendirilmiştir.

Finans sektöründe bazı ülkeler bazında yaşanan DDoS saldırı örneklerine aşağıda yer verilmiştir[303]:

ABD'de 2012 yılında Eylül ayında, Bank of America, PNC, JPMorgan, US Bancorp, Wells Fargo ve aynı yıl tam bir ay sonra ise BBT, Capital One, HSBC, Region Financial, SunTrust web sitelerine yönelik DDoS saldırıları düzenlenmiştir.

---

[302] Warwick Ashford'un 01.02.2016 tarihli haberine göre, bilgi güvenliği uzmanları açısından özellikle HSBC online bankacılık işlemlerinde DDoS ataklarına aşina olunduğu ve 2015 tarihli Verizon Veri İhlali Raporu'na göre finansal işlemlerde gerçekleştirilen saldırıların % 32'sinin DDoS saldırıları olduğu, Arbor Networks'ün "Dünya Genelinde Altyapı Güvenliği Raporu'na göre ise finans kuruluşlarının % 57'sinin DDoS saldırılarına maruz kaldığı ve bu oranın bu sektörde rastlanan en yayın siber saldırı türü olduğunu gösterdiği belirtilmektedir. Söz konusu habere elektronik ortamda ulaşmak için: https://www.computerweekly.com/news/4500272230/DDoS-is-most-common-cyber-attack-on-financial-institutions (Gözden Geçirilme Tarihi: 29.10.2020).

[303] Antoine Bouveret, "Cyber Risk for the Financial Sector: A Framework for Quantitive Assesment", IMF Working Paper, (*"IMF Working Paper"*), s. 13: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/wp18143%20(3).pdf (Gözden Geçirilme Tarihi: 29.10.2020).

Çek Cumhuriyeti'nde 06.03.2013 tarihinde, başta merkez bankası ve üç büyük banka olmak üzere aynı zamanda sermaye piyasasına gerçekleştirilen DDoS saldırısı sonucunda toplamda beş yüz milyon Dolar değerinde bir zararın meydana geldiği belirtilmiştir.

08.07.2014 tarihinde Norveç'te yedi büyük finansal kuruluşa gerçekleştirilen DDoS saldırıları sonucunda bu kuruluşlarda tüm gün boyunca internet hizmeti verilemediği bilinmektedir.

Finlandiya'da 2014 yılı sonlarına doğru Op Pohjola, Danske Bank ve Nordea bankalarına yöneltilen DDoS saldırıları nedeniyle bu bankalar müşterilerine tüm gün boyunca online hizmet verememiş ve özellikle bu bankalardan bir tanesi müşterilerine nakit temini ve kredi kartı ödeme hizmeti dahi sunamamıştır.

Türkiye'de ise özellikle 24.12.2015 tarihinde Garanti Bankası, Ziraat Bankası, İş Bankası ve Akbank gibi bazı bankaları hedef alan DDoS saldırıları neticesinde, bahsi geçen bankaların bilgi sistemlerinde kalıcı hasarlar olmasa da internet bankacılığı kullanan vatandaşlar açısından sorun yaşandığı, günde yaklaşık bir milyar adet işlemle ilgili online bankacılık işlemlerinde aksamalar olduğu ve anılan bankaların POS sistemlerinin etkilendiği bilinmektedir[304].

2.6.2. Pivoting Ve Port Yönlendirme Yöntemleri

"Pivoting"[305], en basit haliyle bilişim dünyasında ele geçirilmiş sistemler üzerinden başka sistemlere saldırmak anlamına gelmektedir. Bu saldırı yönteminde, şirketlerin bilişim sistemlerine izinsiz giriş senaryolarını simüle etmek ve açıkları bulmak için

[304] Konu ile ilgili internet üzerinde ilgili haberlere ulaşmak için bkz. https://www.ahaber.com.tr/gundem/2015/12/28/siber-saldiri-degil-savas; http://www.guncel-haber.com/haber/garanti-bankasi-akbank-is-bankasi-ziraat-bankasi-internet-subelerine-siber-saldiri; https://www.memurlar.net/haber/555161/siber-saldiri-degil-savas.html (Gözden Geçirilme Tarihi: 29.10.2020).

[305] Pivoting işlemi ile ilgili ayrıntılı bilgi için Bkz. *Özkaya/Sarıca/Durmaz*, s. 71, 72.

klasik bir yöntem olan sızma testlerinde (*penetration tests*)[306] pivoting sıkça kullanılan bir saldırı yöntemidir. Sızılmak istenen kurumun ağında pivoting yöntemi ile saldırgan önce o ağa giriş izni olan bir makineyi ele geçirir ve daha sonraki süreçte ise ele geçirilmiş makine vasıtasıyla sistem üzerindeki ağ ile diğer makinelere ulaşma imkânı bulur. Pivoting yöntemi aslında port yönlendirme amacıyla kullanılmakta olup teknik açıdan konuya bakıldığında, port yönlendirmede, sızma testini yapanlar ele geçirdiği konağı (*host*) pivot olarak kullanarak açık olan TCP/IP[307] portuna erişir. Bu işlemin akabinde ise, pivoting metodunu kullanarak erişilen TCP/IP portundan trafik başka bir alt ağdaki (*subnet*)[308] başka bir konağın portuna yönlendirilir.

[306] Sızma testleri, bilişim sistemlerinde olası istismar edilebilecek açıkları kontrol ve tespit amacıyla bilinçli olarak simüle edilen siber saldırıları ifade etmektedir. Sızma testleri herhangi bir kuruluşun bilgi güvenliği açısından savunma hattının etkinliğini değerlendirmek amacıyla işletim sistemlerinde, servislerde, ağda veya uygulamalardaki açıkları veya yanlış yapılandırma ve son kullanıcı hataları nedeniyle meydana gelen açıkları gerçekte siber saldırı gerçekleştiriyormuşçasına test etme süreci anlamına gelmektedir. Sızma testleri konusunda detaylı bilgi için Bkz. *Özkaya/Sarıca/Durmaz*, s. 454-469 ve *Eralp*, s. 31.

[307] TCP/IP İngilizce'de "Transmission Control Protocol/Internet Protocol" kavramlarının kısaltması olarak kullanılmakta olup günümüzde bilgisayarların karşılıklı haberleşmesi ve internetin çalışmasını sağlayan bir iletişim protokolleri bütünü olduğu ifade edilmiştir. Bu açıdan, TCP/IP aslında birçok protokolün toplandığı bir protokol ailesi olmasına rağmen bu referans modelinde en çok kullanılan protokollerin TCP ve IP olması sebebiyle bu iki protokolün adı verilmiştir. Söz konusu referans modelinde dört farklı katman (uygulama, taşıma, ağ ve fiziksel katmanları) olduğu ve toplamda on beşten fazla protokol yer aldığı bilinmektedir. Veriler, söz konusu bu katmanlar arasında sırasıyla paketlenmek suretiyle gönderilmektedir ve alıcı ise paketlemenin tersi sırayla açarak aktarılan verilere ulaşmaktadır. Bu konuda ayrıntılı bilgi için Bkz. https://www.elektrikport.com/teknik-kutuphane/tcpip-nasil-calisir/9004#ad-image-0 (Gözden Geçirilme Tarihi: 29.10.2020). Doktrinde Dülger ise, internet hizmetlerini kullanabilmek için gerekli olan tüm yazılımlar ve bağlantı yazılımlarının, TCP/IP protokolüne göre iletişim kurarak işlev gördüğünü, bu protokolün aslında iki ayrı protokolün bir araya gelmesinden oluştuğunu değerlendirmiştir: Buna göre, (i) "TCP" iletilerin doğru yere aktarılmasından, (ii) IP ise adresleme sisteminden sorumludur. Bkz. *Dülger, Bilişim Suçları,* s. 81.

[308] Teknik detaylara girmeden basitçe açıklamak gerekirse, IP adreslerinin yer aldığı alanın alt sınıflara ayrılmasına bilişim terminolojisinde "subnetting" denilmekte olan ayrılan her alt sınıf ise subnet (*alt ağ*) şeklinde ifade edilmektedir. Subnetler sayesinde internet ortamında network trafiğinin azaltıldığı, network performasının optimize edildiği ve network yönetiminin kolaylaştığı bilinmektedir. Bu konuda teknik açıdan daha detaylı bilgi için Bkz. http://www.ciscotr.com/subnetting-alt-aglara-bolme.html (Gözden Geçirilme Tarihi: 29.10.2020).

2.6.3. Oturum Çalma Ve Parola Saldırıları

Oturum çalma (*session hijacking*) saldırısında, saldırgan tarafından farklı yöntemler kullanılarak "session sniffing" denilen "oturum koklama"[309], ortadaki adam saldırısı, truva atları vb.) web sunucusuna erişim sağlayabilmek amacıyla geçerli bir oturum tokenlarını (*Session ID*) çalarak web oturum mekanizmaları istismar edilmektedir[310].

Parola saldırıları ise teknik açıdan online ve offline olmak üzere iki gruba ayrılmakta olup online parola saldırılarında kullanıcı parolasını tahmin etmek veya THC Hidra[311] gibi bazı parola kırma araçları kullanılarak canlı bir sistemde saldırgan tarafından oturum açmaya çalışma şeklinde gerçekleştirilir. Offline parola saldırılarında ise saldırgan tarafından parolaya ait hash[312] veya hash setlerine ait değerler ele geçirilerek

[309] Sniffing yöntemi ile en basit şekilde ifade etmek gerekirse saldırgan iki veya daha fazla network arasında gidip gelen verileri izleyerek, bu verileri süzmekte ve kaydetmektedir. Sniffing denilen hacking yöntemi günümüzde sadece şirketler açısından değil ulusal güvenlik açısından da ciddi bir risk olarak addedilmekte olup siber saldırganlar açısından şifrelerin yakalanmasında kullanıldığı ve saldırganların genelde sisteme girmeksizin iki nokta arasındaki veri nakilleri rahatça izleyebilme imkânı sağlamaktadır. Bkz. *Erdem/Özocak1*, s. 182.

[310] Oturum çalma konusunda detaylı bilgi için Bkz. *Özkaya/Sarıca/Durmaz*, s. 77-78.

[311] THC Hydra, offline olarak çalışan ve Windows, Linux ve macOS gibi işletim sistemlerinde network login parolalarını kırmaya yönelik bir parola kırma yazılımıdır. Hydra yazılımının, saldırganın hedefin online sistemlerinden herhangi birinin login sayfasını Hydra'ya vererek bu yazılımın olası bütün kullanıcı adı ve şifre kombinasyonlarını denemeye yönelik çalıştığı belirtilmiştir. Bkz. *Özkaya/Sarıca/Durmaz*, s. 81. Hydra yazılımı ile ilgili teknik detaylar konusunda ise bkz. *Altınkaynak*, s. 181.

[312] Hash fonksiyonu, kriptografi ve veri endeksleme gibi birçok bilgisayar biliminde farklı alanlarda kullanılan bir kavramdır. Kriptografi bilimi açısından hash değeri, özellikle orijinal bir verinin bozulmadan şifrelenmesi ve daha sonra orijinal biçimine uygun şekilde söz konusu şifrenin çözülmesi amacına hizmet eder. https://techterms.com/definition/hash (Gözden Geçirilme Tarihi: 29.10.2020). Teknik açıdan konuya bakıldığında hash fonksiyonu girdi (input) olarak bir mesajı alarak bu girdiden, hash kodu, hash sonucu, hash değeri, mesaj özeti veya kısaca hash seti denilen bir çıktı (output) üretir. Giriş kısmında verileren veriyi her zaman aynı boyuttaki özgün bir değere dönüştürmektedir ve hash fonksiyonlarının gücü, güvenilirliği genellikle çakışma oranı ile ölçülmektedir. Hash fonksiyonları, kriptografik alanda veri bütünlüğü ve dijital imza tasarıları için kullanılır. Basit bir örnekle konuyu açıklamak gerekirse, siber güvenlik polislerinin suç unsuru içerdiği düşünülen bir flash bellek içerisindeki verilere el koyması halinde veri bütünlüğünün bozulmaması açısından polis tarafından ilgili bilginin hash değeri alınır ve böylece verinin bütünlüğünün korunması sağlanmış olacaktır. Zira, flash bellek içindeki bu bilginin değiştirilmesi veya silinmesi halinde bu veriye ilişkin hash değeri de değişmiş olacaktır. Hash algoritmalarına örnek olarak md5, sha1, sha256, sha512, LM ve NTLM verilebilir. Hash fonksiyonu ile ilgili ayrıntılı bilgi için Bkz. Apdullah Yayık, "Yapay Sinir Ağı Ve Kriptoloji Uygulamaları", Mustafa Kemal Üniversitesi Fen Bilimleri Enstitüsü Enformatik Anabilim Dalı, Yüksek

sisteme giriş sağlanır. Bu saldırı yönteminde, saldırgan tarafından yetkilendirme sistemini çözmekle uğraşılmaksızın sadece hash setleri karşılaştırmak suretiyle sisteme giriş sağlanır. "John the Ripper"[313] denilen yazılım offline parola kırma aracına örnek olarak gösterilebilir[314].

2.7. KRİPTO MADENCİLİĞİ SALDIRILARI (CRYPTOJACKING) VE KRİPTO PARALARA YÖNELİK SİBER SALDIRILAR

Kripto madenciliği saldırıları, saldırganlar tarafından kurbanların bilgisayarları ve cep telefonları kullanılarak kripto madenciliği için kullanılan siber saldırıları ifade etmektedir[315]. Yukarıda da ayrıntılı şekilde açıklandığı üzere, 2009 yılında Satoshi Nakamoto isimli kimliği bilinmeyen bir kişi tarafından ilk kripto para birimi olan Bitcoin'in ortaya çıkması ve blokzincir teknolojisinin günümüzde geldiği aşama, siber saldırganları "cryptojacking" denilen ve Türkçe'ye kripto madenciliği saldırıları olarak tercüme edilen farklı siber saldırı yöntemlerine itmiştir. Kripto madencilik saldırılarının anlaşılabilmesi açısından öncelikle madencilik (mining) denilen kripto para üretiminden kısaca bahsetmek gerekirse, madencilik terimi kripto paralar açısından bilişim kaynaklarını kullanarak piyasaya kripto paraların dolaşımı sunulması anlamına gelmektedir[316]. Bu konuda Bitcoin'den örnek vermek gerekirse, Bitcoin'in arzı 21 milyon ile sınırlı tutulmuştur. Kripto madencilik açısından Bitcoin arzı sınırlı olması sebebiyle kripto para sahipleri arasında güvenli şekilde sanal cüzdanlarında tutulan Bitcoin'in bir kişiden diğerine aktarılabilmesi açısından özel bilgisayarlar

---

Lisans Tezi, Hatay, 2013, (*"Yayık"*), s.24: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/APDULLAHYAYIK_Tez_24.06.2013.pdf (Gözden Geçirilme Tarihi: 29.10.2020) ve bu konuda ayrıca bkz. *Altınkaynak*, s. 11.

[313] "John the Ripper" denilen yazılım, saldırganlar tarafından sözlük saldırısı yaparak parolaları kırmak amacıyla kullanılan, Linux ve Windows işletim sistemlerinde sürümleri mevcut olan güçlü bir parola kırma aracıdır. Özellikle bu yazılım ile şifrelenmiş (encrypted) web tabanlı sistemler ve uygulamalar veya kullanıcılara ait veri tabanından kullanıcı parolası çıkarılabilir. Bu konuda detaylı bilgi için bkz. *Özkaya/Sarıca/Durmaz*, s. 80.

[314] Parola çalma saldırıları konusunda ayrıntılı bilgi için Bkz. *Özkaya/Sarıca/Durmaz,* s.78-80 ve *Altınkaynak*, s. 181-185.

[315] *Özkaya/Sarıca/Durmaz*, s. 92.

[316] *Bozkurt Yüksel, Elektronik Para,* s. 70-71.

arasında blokzincir teknolojisinde bu işleme ait merkezi olmayan herkese açık dijital bir kasaya girmesi gerekir. Bu sırada özel bilgisayarlar belirli bir zaman aralığında Bitcoin'a ait işlemlerin verilerini toplayıp onları karmaşık bir matematiksel bulmacaya çevirir. Madencilik işlemi ise, bu algoritma niteliğindeki matematiksel işlemin çözümü neticesinde gerçekleşir. Başka bir ifadeyle, Bitcoin'in sanal cüzdanlar arasında transferi açısından blokzincir sistemindeki diğer bir katılımcı kategorisi üyesinin bağımsız olarak bu karmaşık algoritmayı çözmesi sonucunda bu işlemin doğruluğu dağıtık veri tabanı teknolojisi gereği sistemdeki diğer paydaşlar tarafından da teyit edilir ve bunun sonucunda ise kripto paranın transferi bir sanal cüzdandan diğerine aktarılır. Ancak, blokzincir teknolojisinde söz konusu algoritmayı çözen ilk kişiyi madenci (*miner*) olarak adlandırır ve sistem genellikle bu kişiye kripto para vererek bu kişiyi ödüllendirir[317].

Yukarıda da ifade edildiği üzere, kripto madenciliği saldırılarında siber saldırganlar madencilik işleminde blokzincir teknolojisinin öngördüğü karmaşık algoritmaları çözmek açısından kendi bilgisayar sistemlerini kurmak yerine başkalarının bilişim sistemlerinden yararlanmak suretiyle madencilik işlemlerini gerçekleştirirler[318]. Bu yol ile sistemdeki karmaşık algoritmaların çözülmesi için yüksek maliyetlerin yapılmasının önüne geçilmiş olur. Saldırganlar, kripto madenciliği saldırılarında genelde farklı yöntemler kullanmaktadır. İlk yöntemde kurban olarak belirlenen kişinin oltalama yöntemiyle bilgisayar sistemine bir e-mail vasıtasıyla zararlı yazılım bulaştırılır ve bu sayede bu saldırıya izin veren cryptojacking kodu bilgisayara enjekte edilir. Diğer bir yöntem ise saldırgan tarafından herhangi bir web sayfasına JavaScript kodu yerleştirerek kurbanın yönlendirilen web sitesi vasıtasıyla kurbanın farkında

[317] *Özkaya/Sarıca/Durmaz*, s. 58.
[318] *Özkaya/Sarıca/Durmaz*, s. 57.

olmadan arka planda işleyen JavaScript kodu vasıtasıyla kripto madenciliği işleminin yapılmasıdır[319].

Kripto madenciliği saldırılarının yanı sıra kripto paralarda blokzincir teknolojisine özgü sık rastlanan bazı güvenlik problemleri şunlardır[320]:

2.7.1. Özel (Gizli) Anahtar Hırsızlığı

Bilindiği üzere, blokzincir teknolojisinde temel itibariyle sisteme giriş yapmayı sağlayan açık anahtar (*public key*) ile kullanıcının kimlik ve kullanıcı tarafından üretilen ve güvenlik bilgilerini içeren gizli anahtar (*private key*) bulunmaktadır. Kullanıcı tarafından söz konusu bu gizli anahtarın bir şekilde unutulması, kaybolması veya kötüniyetli birtakım kişiler tarafından ele geçirilmesi halinde kullanıcının sistemi kullanması imkânsız hale gelmekte ve sistemin kontrolü bu kötü niyetli kişilere geçmektedir. Siber saldırganlar genelde blokzincirindeki süreçlerde kullanılan

[319] Kripto madenciliği saldırılarına yönelik yukarıda yer verilen değerlendirmeler, genel itibariyle *Özkaya/Sarıca/Durmaz*, s. 56-59'da "Cryptojacking" başlığı altındaki açıklamalardan özetlenerek aktarılmıştır. Özellikle kripto madenciliği saldırılarına yönelik yukarıda belirtilen yöntemler bu yazarların anılan eserinden ayrıntılı şekilde aktarılarak çalışmada belirtilmiştir. Ayrıca, kripto madenciliği saldırıları, Geng Hong/Zhemin Yang/Sen Yang/Lei Zhang/Yuhong Nan/Zhibo Zhang/Min Yang/Yuan Zhang/Zhiyun Qian/Haixin Duan (*"Hong Ve Diğerleri"*) tarafından kaleme alınan "How You Get Shot in the Back: A Systematical Study about Cryptojacking in the Real Wold" isimli makalesinde detaylı şekilde incelenmiştir. Söz konusu yazarlar, bu makalede kripto para madenciliğine dünyada artan eğilim nedeniyle saldırganların daha güçlü bilişim platformlarına ve bilgisayar sistemlerine ihtiyaç duyduğunu belirterek özellikle internette bazı web siteleri üzerinden aktarılan zararlı yazılımlar vasıtasıyla kripto madenciliği saldırılarının da artan bir ivme ile çoğaldığını Alexa isimli şirket tarafından 2017 yılı Kasım ayında yayınlanan raporda 100.000'in üzerinde kripto madenciliği saldırılarına yönelik web sitelerinin tespit edildiği belirtilmiştir. Bu konuda detaylı bilgi için Bkz. http://www.cs.ucr.edu/~zhiyunq/pub/ccs18_cryptojacking.pdf (Gözden Geçirilme Tarihi: 29.10.2020). Malwarebytes'ın tespitlerine göre Android tabanlı kripto para madenciliği saldırılarının 2018'in ilk çeyreğinde yüzde 4000 civarında bir artış gösterdiğini belirtmiştir. Bkz. Malwarebytes, "Cybersecurity basics: Everthing you need to know about cybercrime": https://www.malwarebytes.com/cybersecuirty/. (Gözden Geçirilme Tarihi: 29.10.2020).

[320] Yukarıda başlıklar altında açıklanan blokzincir sistemine özgü güvenlik açıklarına yönelik açıklamalar Şeref Sağıroğlu (Editör)'nun "Siber Güvenlik Ve Savunma Standartlar Ve Uygulamalar", BGD Siber Güvenlik Ve Savunma Serisi 3, (*"Sağıroğlu"*), s. 285 vd. özetlenerek aktarılmıştır.

algoritmalarda çeşitli açıkları keşfederek gizli anahtarların kontrolünü ele geçirmektedir[321].

2.7.2. % 51 Saldırısı

Uzmanlar blokzincir teknolojisinin karşılıklı güvenlik açısından gerektirdiği dağıtık veri tabanı ve mutabakat mekanizmasının blokzincir tabanlı sistemlerde %51 saldırısı denilen güvenlik zafiyetini de beraberinde getirdiğini belirtmektedir. Teknik açıdan konuya bakıldığında, alında %51 güvenlik açığı genel itibariyle yukarıda belirttiğimiz kripto para madenciliği ile yakından ilintilidir. Konuyu basit şekilde aktarmak adına somut bir örnek üzerinden açıklamak gerekirse, yukarıda açıklanan Bitcoin ve Ethereum gibi kripto paralarda işlem gerçekleştirebilmesi işlem kanıtı (*proof of work*)[322] denilen sistemdeki tüm paydaşların blokzincirde bu işlemi onaylamasına bağlıdır. Madencilik kısmında yer verdiğimiz açıklamalarda da belirtildiği üzere, sistemde onay mekanizması bakımından ilgili algoritmayı çözen kullanıcıyı sistem ödüllendirdiği için bu durumda tek bir madencinin tüm blokzincirin toplam hesaplama gücünün sistemin %50'sinden fazlasına ulaşması halinde, bu kişinin %51 saldırısı başlatabileceği kabul edilmektedir[323]. Blokzincir teknolojisi paydaşların sistemdeki mutabakatına bağlı olduğundan, sistemin %50'sinden fazla hesaplama (özetleme) gücüne ulaşan madenci bu sistemi dilediği şekilde kullanabilir hale gelecektir. Örneğin

---

[321] S*ağıroğlu*, s., 286.

[322] "Proof of work", Türkçe'ye işlem kanıtı veya emeğin ispatı şeklinde tercüme edilebilecek olup çalışmada "işlem kanıtı" teriminin yukarıdaki açıklamalara daha uygun olması sebebiyle bu terim tercih edilmiştir. İşlem kanıtı mekanizmasında, bloğa yeni bir zincir eklemek isteyen işlemcinin bu teknolojinin ürettiği bir algoritmayı çözmesi gerekir. Algoritmayı ilk çözen işlemciyi sistem ödüllendirir (örneğin, Bitcoin açısından algoritmayı çözen işlemciye sistem yeni bir Bitcoin verir) ve yukarıda da belirtildiği üzere bu işleme madencilik denilmektedir. Bu konuda detaylı bilgi için bkz. Sevgi Çetin, "Hukukta Yeni Ufuklar, Yeni İhtilaflar: Blokzincir Uygulamaları Ve Akıllı Sözleşmelere Eleştirel Bir Bakış", (*"Çetin"*): https://www.academia.edu/38413617/HUKUKTA_YEN%C4%B0_UFUKLAR_YEN%C4%B0_%C4%B0HT%C4%B0LAFLAR_BLOKZ%C4%B0NC%C4%B0R_UYGULAMALARI_ve_AKILLI_S%C3%96ZLE%C5%9EMELERE_ELE%C5%9ET%C4%B0REL_B%C4%B0R_BAKI%C5%9E (Gözden Geçirilme Tarihi: 29.10.2020).

[323] S*ağıroğlu*, s. 287.

2014 yılında, "ghash.io" isimli madencilik havuzunda madencilerden birisinin bitcoin hesaplama gücünün %45'ine ulaştığı fark edildiğinde bir grup madencinin bu havuzdan gönüllü olarak ayrıldığı bilinmektedir[324]. Öte yandan, blokzincir tabanlı çalışan her para biriminin diğerinden ayrışan kendisine özgü bir özelliği bulunduğundan, gerçekleştirilen %51 saldırıları da her kripto para biriminin bağlı olduğu teknolojiye göre farklılık göstermektedir[325].

2.7.3. İllegal Faaliyetler

Blokzincir teknolojisi ile birlikte kripto para birimlerinin ortaya çıkması akabinde, en önemli sorunlardan birisi de kripto paraların illegal faaliyetlerde kullanılmasıdır. Blokzincir teknolojisi özünde merkezi olmayan bir mutabakat sistemine dayanması, para transferinin devletler tarafından takip edilmesini çoğu zaman zorlaştırmakta ve hatta imkânsız kılmaktadır. Özellikle "Dark Web"[326] denilen internetin yer altı dünyasında çoğu kez uyuşturucu cinayeti, kara para aklama, çocuk pornografisi açısından sağlanan gelirler, terör örgütlerinin finansmanı gibi illegal faaliyetler çoğu kez başta Bitcoin olmak üzere kripto paralar vasıtasıyla gerçekleştirilmektedir. Siber dünyada ise, saldırganlar çoğu kez oltalama faaliyetleri ile kurbanlarının bilgisayarlarına bulaştırdıkları fidye yazılımlar gibi zararlı yazılımları kaldırmak karşılığında kendilerine Bitcoin gibi kripto para ile ödeme yapılması konusunda şantaj

---

[324] https://www.theguardian.com/technology/2014/jun/16/bitcoin-currency-destroyed-51-attack-ghash-io (Gözden Geçirilme Tarihi: 29.10.2020).

[325] S*ağıroğlu*, s. 287.

[326] "Dark Web" olarak niteledirilen internet ortamında yasa dışı faaliyetlerin yürütüldüğü bu konsepte ilişkin pek çok yanlış bilginin kamuoyunda yer aldığı görülmektedir. Dark Web'e ulaşılması teknik açıdan daha ziyade Google gibi normal arama motorları yerine genelde bilgisayar korsanları açısından "Tor browser" denilen özel birtakım yazılımların yüklenmesini gerekli kılmaktadır. Securelist tarafından yapılan araştırmada, Dark Web'de yer alan web sitelerinin kısa ömürlü olduğu, çoğunlukla en az 200 gün boyunca aktif olduğu ve genelde bu ortamda yer alan web sitelerinin 300 günü geçmeden genelde kapatıldığı belirtilmiştir. Bu konuda ayrıntılı bilgi için bkz. Kaspersky Lab, "Dark Web: Myths, Mysteries and Misconceptions": https://go.kaspersky.com/rs/802-IJN-240/images/Dark%20Web%2010172017.pdf?aliId=521973948 (Gözden Geçirilme Tarihi: 29.10.2020).

yapmaktadır[327]. Öte yandan, yukarıda açıklanan DDoS ve Botnet saldırıları vasıtasıyla kurban durumundaki kişinin bilgisayarları ve diğer cihazları kripto paralar üzerinden yürütülen bu illegal faaliyetleri esnasında kurbanların bilgisi dahi olmaksızın aracı olabilmektedir.

2.7.4. Mahremiyet Problemi

Blokzincir teknolojisine dayalı sistemlerin en büyün problemlerinden birisi de, günümüzde özellikle blokzincirde gerçekleştirilen işlemlerin gizliliğinin çoğu kez sağlanamamasından kaynaklanan mahremiyet sorunudur. Mahremiyet açısından blokzincir teknolojisinde doğrudan kişisel verilerin işlenmesi ve depolanması gibi faaliyetler çerçevesinde veri sorumlusunun sorumluluğu gündeme geleceğinden bu konunun devletlerin mahremiyet ve veri koruma mevzuatları ile Avrupa Birliği ülkeleri açısından ise GDPR[328] kapsamında da değerlendirilmesi gereken bir mesele olduğu üzerinde durulmuştur[329].

---

[327] *Sağıroğlu*, s. 287-288.

[328] GDPR ile ilgili kapsamlı değerlendirmeye, tezin 4.2.5 numaralı başlık altında yer verilmiştir. Konuyu ilgilendirmesi açısından, kısaca değinmek gerekirse GDPR m. 4/f. 7'de, veri sorumlusu, kendi başına veya başkaları ile beraber kişisel verilerin işlenmesi hususuna yönelik amaçları ve yöntemleri belirleyen gerçek ve tüzel kişiler ile kamu kurum ve kuruluşları ile diğer herhangi bir organı ifade etmektedir. GDPR m. 4/f. 8'de ise, veri işleyen, veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişiler ile kamu kurum veya kuruluşu veya diğer herhangi bir organ şeklinde tanımlanmıştır. GDPR'ın ilgili düzenlemeleri konusunda bkz. https://gdpr-info.eu/ (Gözden Geçirilme Tarihi: 29.10.2020).

[329] Bu konu Avrupa Parlamentosu Araştırma Birimi (European Parliament Research Service veya kısaca *"EPRS"*) tarafından "Blockchain and the General Data Protection Regulation Can Distributed Ledgers be squared with European data protection law?" adlı raporunda kapsamlı şekilde değerlendirilmiştir. Yukarıda yer verilen açıklamalar doğrultusunda EPRS tarafından yayınlanan söz konusu raporda, blokzincir teknolojisinin GDPR ile ilgili çatıştığı yegâne hususların öncelikle blokzincir teknolojisindeki dağıtık veritabanı (DLT) nedeniyle veri sorumlularının tespit edilmesinin güçlüğü ve verinin bu teknoloji kapsamında bir nevi silinemez olduğu gerekçesiyle GDPR m. 17'de yer alan unutulma hakkına ("right to be forgotten" veya "right to erasure") aykırılık teşkil ettiği belirtilmiştir. Bu konuda kapsamlı bilgi için bkz. EPRS, "Blockchain and the General Data Protection Regulation Can Distributed Ledgers be squared with European data protection law?"), 2019: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

GDPR açısından özellikle unutulma hakkı (*right to be forgotten*)[330] gibi talepler açısından blokzincir teknolojisinde sistemin bu tarz taleplere ne şekilde cevap verebileceği tartışma konusu olmuştur. Bu noktada, özellikle blokzincir teknolojisinde yaygın bir ayrım olan açık blokzincir platformları (*public blockchains*) ile özel blokzincir platformları (*private blockchains*) açısından ikili bir ayrıma gidilmek suretiyle[331] konunun incelenmesinde fayda görülmüştür. Özel blokzincir platformlarında, blokzincir ağı kullanılarak işlenen veri bakımından, bu veriyi kullanan tüm kullanıcılar, teorik açıdan veri sorumlusu olarak değerlendirilerek bu veri sorumlularının sorumluluk rejiminin kapsamının belirlenmesi gündeme gelecektir. Konuya açık blokzincir platformları açısından bakıldığında ise, bu blokzincir ağlarında herkese açık şekilde söz konusu kullanıcıların ağa dahil olması söz konusu olduğundan, sistemde yer alan kişisel verinin tanımlanması açısından uygun veri sorumlusunun kim olacağı ve bu veri sorumlusunun/sorumlularının belirlenmesi halinde ise bu veri sorumlulularının kişisel veriler bakımından sorumluluk rejiminin ne olacağının belirlenmesi gibi ikili bir meselenin çözümlenmesi gerekmektedir[332].

Öte yandan, blokzincir teknolojisinin doğası ve tasarımı gereği bu teknoloji, verinin bir kez sistemde işlenmesi neticesinde verinin silinmesi ve değiştirilmesini imkânsız

---

[330] Doktrinde Soysal'a göre, unutulma hakkı, özünde kişinin belirli bir zaman süreci geçtikten sonra kendisine ait bilgilerin farklı ortamlarda ve farklı bağlamlarda kullanılmasına karşı çıkma ve özellikle belirli bir zaman geçmesi akabinde kişinin internet üzerinde arama motorlarında endekslenmesinin kişi açısından belirli sakıncalar doğurabilmesi sonucunda ortaya çıkan bir hak olarak kabul edilmektedir. Bu konuda detaylı bilgi için bkz. Tamer Soysal, "Unutulma Hakkının Avrupa Birliği'nin Genel Veri Koruma Tüzüğü Çerçevesinde Değerlendirilmesi": https://dergipark.org.tr/en/download/article-file/742611 (Gözden Geçirilme Tarihi: 29.10.2020).

[331] Bitcoin gibi kamuya açık blokzincir ağlarında, ağa girerek kayıtlara erişebilmek açısından herhangi bir izin almak gerekmemektedir. Özel blokzincir ağlarında ise bazı şirketler, organizasyonlar ve kamu kurumları herkese açık blokzincir ağları üzerinde veri bulundurmak yerine güvenlik, gizlilik gibi birtakım gereksinimler nedeniyle ağ üzerindeki verinin herkes tarafından değil sadece sistem içerisinde tanımlanan paydaşları tarafından görüntülenmesini ve sistemin güvenliğinin blokzincir ağı üzerinde şifrelenerek saklanmasını tercih edebilir. Kamuya açık blokzincir ile özel blokzincir konusunda detaylı bilgi için: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/ (Gözden Geçirilme Tarihi: 29.10.2020).

[332] https://fpf.org/2020/11/04/understanding-blockchain-a-review-of-fpfs-oct-29th-digital-data-flows-masterclass/ (Gözden Geçirilme Tarihi: 29.10.2020).

kılmaktadır. Özellikle Bitcoin gibi kamuya açık blokzincir platformlarında sisteminin temeli, aslında işlemi gerçekleştiren kullanıcı dışında diğer tüm paydaşların da işlemi onaylamasına bağlı olduğundan işlemi gerçekleştiren kullanıcı tarafından işlemin silinmesi hiçbir zaman mümkün değildir. İşlemler silinemeyeceği için çoğu kez farklı bir işlem yapılmak istendiğinde, yeni olan işlem sistemin blok şeklindeki yapısına adeta yeni bir zincir olarak eklenir. Ancak, adından da anlaşılacağı üzere aslında blokzincir teknolojisinde sisteme her eklenen işlem bir zincir olarak eklendiğinden sistemde kalıcı hale gelir. Sistemde mahremiyetin uygulanması ise bazı prosedürler uygulanarak her sistemin kendisine özgü olarak öngördüğü karakteristik teknoloji ile çoğu kez şifreleme (*hashing*)[333] ve maskeleme (*pseudonymisation*)[334] gibi birçok farklı yöntemle gerçekleştirilebilir. Ancak, hiç kuşkusuz her kripto para açısından maskeleme noktasında farklı yöntemler izlenmektedir. Örnek vermek gerekirse, Bitcoin para biriminde kullanıcılar gerçekleştirecekleri işlemler açısından tek sefere özgü hesaplar kullanırken Monero para biriminde ise, sistem geçerli olmayan para birimlerinin eklenmesine de imkân vermektedir. Bu durum ise Monero üzerinde gerçekleştirilen bir çalışmada bazı kötü niyetli kişiler tarafından Monero'ya katılan bazı geçersiz para birimleri sayesinde saldırganların mahremiyeti ortadan kaldırdığını açıkça göstermiştir[335].

[333] Şifreleme yaklaşımında (hashing-out approach) blokzincir içeriğinde yer alan kişisel veri, blokzincirin dışına çıkarılarak "hash" denilen bir şifre değeri ile değiştirilir ve şifre değerinde sadece ilgili saklanan veriye yönelik bir referans noktası oluşturulur. Böylelikle, kişisel verinin sahibi kişi tarafından bu verinin silinmesi gibi talep söz konusu olduğunda, blokzincir ağının dışında saklanan verinin silinebilir halde olduğu kabul edilmektedir. Bu konuda detaylı bilgi için: https://fpf.org/2020/11/04/understanding-blockchain-a-review-of-fpfs-oct-29th-digital-data-flows-masterclass/ (Gözden Geçirilme Tarihi: 29.10.2020).

[334] GDPR m. 4/f. 5 kapsamında konuya bakıldığında, maskeleme *(pseudonymisation)* kişisel verilerin tanımlanan veya tanımlanabilir bir gerçek kişi ile herhangi bir şekilde bağlantı kurulmaması amacı gözetilerek ek birtakım bilgilerin ayrı tutulması, teknik ve organizasyonel önlemler çerçevesinde söz konusu ek bilgi olmaksızın veri sahibi ile ilişkilendirilememesi olarak tanımlanmıştır. Veri maskeleme ile ilgili ayrıntılı değerlendirme için Murat Lostar, "Veri Maskeleme": https://lostar.com.tr/2012/04/veri-maskeleme.html (Gözden Geçirilme Tarihi: 29.10.2020).

[335] *Sağıroğlu*, s. 289.

Son olarak, blokzincir teknolojisinin GDPR kapsamında önem taşıyan verilerin işlenmesinde "amaçla sınırlama"[336] ve "veri küçültme"[337] prensipleri ile çatıştığı ileri sürülmektedir. Blokzincir teknolojisinde, doğası gereği kayıt altına alınan verinin tüm geçmiş sürecine ilişkin işlemler silinemez şekilde kayıt altına alındığından, bu durum verinin sadece ilgili işlemin amacına uygun şekilde verinin asgari şekilde işlenmesi prensiplerine aykırılık teşkil etmektedir[338].

2.7.5. Çift Harcama

Geçmişte saldırganlar tarafından bazı kripto para birimleri üzerinde sık gerçekleştirilen saldırı yöntemlerinden birisinin de kripto paralar üzerinde çift harcama olduğunu göstermektedir. Çift harcama, basit şekliyle saldırganların aynı kripto parayı birden çok kez kullanması anlamına gelmektedir. Bu saldırı modelini basitçe açıklamak gerekirse:

Dağıtık veri tabanı teknolojisine dayanan blokzincir tabanlı sistemlerde işlemin doğrulanabilmesinin sistemdeki tüm paydaşların mutabakatına dayandığı yukarıda belirtilmişti. Bu noktada, saldırganlar blokzincirinde gerçekleştirilen tek bir harcamayı birden fazla şekilde yapılmış gibi göstererek geçmişte zaman zaman sistemi suiistimal edebilmiştir. Saldırganlar, burada herhangi bir işlem gerçekleştiren kullanıcıyı takip ederek proof of work denilen işlem kanıtının gerçekleştirilmesinden önce, işin başlangıç ve doğrulama aşamaları arasında geçen süreyi kendi çıkarlarına kullanmaktadır. Diğer bir ifade ile, ilk işlemin çıktısı elde edilinceye dek geçen süre

[336] GDPR kapsamında "amaçla sınırlama" prensibi, temel olarak kişisel verilerin işlenmesinin belirli bir iyi tanımlanmış amaç için ve yalnızca bu amaçla uyumlu ek, tanımlanmış amaçlarla yapılması gerektiği anlamına gelmektedir. Bu konuda detaylı bilgi için bkz. FRA, "Avrupa Veri Koruma Mevzuatı El Kitabı, (Türkçe Tercümesi), 2018, (*"FRA"*), s. 239.

[337] Veri küçültme (*data minimisation*) prensibi ise, özünde verilerin sadece toplandıkları ve/veya işlendikleri amaçlarla ilgili olarak yeterli, ilgili ve aşırı olmayacak şekilde işlenmelerini, başka bir ifade ile veri işleme için belirlenen veri kategorilerinin, beyan edilen veri işleme operasyonun ana amacının gerçekleştirilmesi için gerekli olmasını ve veri sorumlusunun veri işlenmesinde belirli amaç ile doğrudan ilgili bilgilerin veri olarak toplanmasının katı bir şekilde sınırlandırılması gerektiğini ifade etmektedir. Bkz. *FRA*, s. 242.

[338] https://fpf.org/2020/11/04/understanding-blockchain-a-review-of-fpfs-oct-29th-digital-data-flows-masterclass/ (Gözden Geçirilme Tarihi: 29.10.2020).

içerisinde aynı kripto para ile birden fazla işlem başlatıp bu işlemler geçersiz sayılmadan birden çok işlem gerçekleştirilmesi çift harcama olarak adlandırılmaktadır[339].

2.8. FİNANS SEKTÖRÜNDE GELİŞMİŞ SÜREKLİ TEHDİT (APT)

Bilişim terminolojisinde yaygın olarak APT[340] olarak bilinen bu saldırı türünde, özellikle ulusal ve uluslararası kuruluşlar veya kimi zaman ülkeler de hedef alınarak bilgi sızdırmak ve önemli ölçüde zarar verilmek istenmektedir. APT, teknik açıdan nitelikli bir siber saldırı türü olup diğer saldırı vektörlerinden farklı olarak stratejik olarak belirli bir hedefe yöneltilmekte ve saldırı öncesi çok detaylı bir planlama yapılmaktadır. APT saldırılarının kapsamlı şekilde gerçekleştirilmesi, hedefteki sistemde fark edilse bile saldırganların istedikleri amaca ulaşmadan çoğu kez sistemi terk etmemeyi tercih etmeleri ancak bu agresif saldırı yöntemine rağmen saldırganların yakalanmamaları APT saldırılarının arkasında derin bir yazılım bilgisi ve tecrübesi olmasını gerektirir. Başka bir deyişle, APT saldırılarının en karakteristik özelliği, belirli bir hedefe odaklanılarak organize şekilde gerçekleştiren nitelikli bir siber saldırı olmasıdır[341]. Finans sektörünün korkulu rüyası olarak görülen bu saldırılarda ağa giren siber korsanlar genelde bir vur-kaç saldırısı yapmayarak mümkün mertebe en fazla veriyi sistemden çalabilmek amacıyla ağda kalmayı tercih etmektedir.

APT saldırılarını anlayabilmek açısından kısaca APT'nin yaşam döngüsünden[342] bahsetmek gerekirse:

Hazırlık ve keşif aşamasında saldırgan genelde uzun ve kapsamlı araştırmalar yaparak hedefin ağı ve sistemleri hakkında olabildiğince çok bilgi toplar ve buna göre mevcut zafiyetler çerçevesinde uygulayacağı istismar yöntemlerini belirler.

---

[339] *Sağıroğlu*, s. 289.
[340] APT, İngilizce'de "Advanced Persistent Attack" kelimelerinin kısaltmasıdır. Türkçe'ye yazar tarafından "Gelişmiş Sürekli Tehdit" olarak tercüme edilmiştir (Serbest Çeviri).
[341] *Özkaya/Sarıca/Durmaz*, s. 164-165.
[342] *Özkaya/Sarıca/Durmaz*, s. 166-168.

Saldırgan gerekli hazırlıkları ve keşfi tamamladıktan sonra, ilk sızmada genelde kurbana phishing yöntemi ile zararlı yazılım içeren bir dosya paylaşarak veya kurbanı zararlı bir linke yönlendirerek kurbanın bilgisayarına "payload" denilen zararlı yazılım yükünü enjekte eder. Bu sayede, saldırgan bu yazılımı atlama taşı olarak kullanarak sistemin dışarı ile olan bağlantısını kontrol ettikten sonra ilk sızma testinin başarılı olarak gerçekleştiğini görmüş olacaktır.

Yayılma safhasında, hedef ağa sızan saldırgan tarafından fark edilmeden ağ içerisinde dolaşma özgürlüğü elde edebilmek amacıyla sistemde hak/yetki yükseltmesi *(privilege escalation)* gerçekleştirerek ağa, sistemlere ve cihazlara üst bir erişim sağlayacaktır.

Çıkarım aşaması, APT'de esas saldırının başladığı aşama olup saldırganın bu aşamaya gelebilmesi halinde teknik açıdan kurbanın bilgisayar ağında serbestçe dolaşma hakkına sahip olduğu ve bütün sistemdeki hassas verilere erişme imkânı olduğu kabul edilmektedir.

İdame aşamasında, APT saldırısını düzenleyen saldırgan sistemde kalmayı amaçlayarak bilgi hırsızlığının da ötesinde, sisteme daha fazla zarar vermek amacıyla zaman kazanmaya çalışmaktadır. Bu aşamada, kurban ya saldırganı sistemde tespit edemez haldedir veya kurbanın güvenlik araçları saldırının ilerlemesini durdurma konusunda yetersiz kalmaktadır.

APT saldırılarının saldırı aşaması, genelde en korkulan aşama olarak değerlendirilir. Saldırgan, sistemde sadece verilere ve yazılımlara değil kurbanın donanımlarını da tamamen devre dışı bırakarak, fonksiyonlarını bozarak imha edebilecek kabiliyettedir.

Zaman zaman siber saldırganların göz ardı edebildiği son aşama, temizlik safhasıdır. Saldırgan bu aşamada sızdığı sistemdeki izleri silmeyi amaçlayarak genelde saldırı sonrası yapılacak adli bilişim (*forensic*) aşamasını etkisiz kılmak hedeflenir.

Avrupa Ödeme Konseyi'nin 2019 yılında yayınlanan Ödemelere Yöneltilen Tehditler ve Dolandırıcılık Eğilimi başlıklı raporunda[343], yukarıda belirtilen APT saldırıları karşısında özellikle Europol ve Interpol gibi uluslararası kuruluşların siber korsanların yakalanması konusunda etkin çalışmalar yürüttüğü belirtilmekle beraber, bu konuda özellikle Cobalt ve Carbanak gibi suç örgütlerinin özellikle 2018 yılında etkin siber saldırılar gerçekleştirdiğine dikkat çekilmiştir. Cobalt, denilen siber saldırgan grubu "SpicyOmelette" denilen zararlı yazılım sayesinde hedefindeki finansal kuruluşlardan ciddi ölçüde kazanç elde ederek neredeyse dünya genelinde yaklaşık 1 milyar Dolar civarında zarar verdiği bilinmektedir. Carbanak ise benzer şekilde sadece tek başına siber suç örgütü olarak dünyadaki bankalardan APT saldırıları sayesinde yaklaşık 1 milyar Dolar civarında haksız kazanç elde etmiştir. APT saldırıları açısından, finans kuruluşlarına "hedefe yönelik oltalama"dan "zararlı yazılımlara" ve çoğu kez SWIFT sistemlerine de yansıyan saldırılarda kimi zaman bankaların ATM işlemlerine yönelik kart harcamalarında da APT saldırıları sonucunda sınırsız bir yetki elde edilmektedir. FireEye şirketinin "Tehdit İstihbarat Araştırma Takımı"nın özellikle "M-Trends 2019 Özel Raporu'nda[344] Kuzey Kore menşeli Reaper ve APT 38 isimli siber suç örgütü ile Lazarus isimli meşhur siber korsan grubunun bankalara ve finansal kuruluşlara yönelik aktif şekilde APT saldırıları gerçekleştirdiği belirtilmiştir.

2.9. İNTERNET BANKACILIĞI VE MOBİL BANKACILIĞA YÖNELİK SİBER SALDIRILAR

İnternet bankacılığında çevrimiçi bankacılığın güvenliği önem taşıdığından, bu konuda özellikle Zeus/ZBot, Mevade, SpyEye, Fatma, Tinba gibi zararlı yazılımlar (bankacılık

[343] European Payments Council, "2019 Payment Threats and Fraud Trends Report", EPC302-19, /Versiyon 1.0 / Yayınlanma Tarihi: 09.12.2019, (*"EPC Raporu"*), s. 33. İlgili raporu internet üzerinde ulaşmak için bkz. https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2019-12/EPC302-19%20v1.0%202019%20Payments%20Threats%20and%20Fraud%20Trends%20Report.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[344] M-Trends 2019 Özel Raporu, s. 14-17: https://content.fireeye.com/m-trends/rpt-m-trends-2019 (Gözden Geçirilme Tarihi: 29.10.2020).

truva atları, fidye yazılımları, vb.) siber güvenlik alanında kritik derecede risk teşkil eden bir hususdur[345]. İnternet bankacılığı konusunda yukarıda da belirtildiği gibi çift faktörlü kimlik doğrulama yayın bir uygulama olup Hesperbot isimli virüs, bankaların kullandığı çift faktörlü kimlik doğrulama yöntemini aşabileceğinden burada kısaca bahsedilecektir. Hesperbot virisü, bazı firmalar tarafından müşterilerine gönderilen uyarı mesajları sonucunda önce internet bankacılığı kullanan kullanıcının bilgisayarına, daha sonrasında ise cep telefonunda aktive olabilen bir virüs türüdür. Hesperbot bulaştığı sistemde, web tarayıcısı üzerinden internet bankacılığı sitelerine girildiğini tespit edebilmekte ve ilgili bankaya özel hazırlanmış zararlı JavaScript kodlarını tarayıcıya enjekte etmektedir. Bilgisayara sızılması akabinde ise bu zararlı yazılım cep telefonuna sızararak kullanıcının banka şubesine başarılı bir şekilde giriş yapması sonrasında müşteri numarası ve gerekli şifreleri bu yazılımdan faydalanan siber korsana iletir. Aktivasyon kodu ise mobil cihaza bulaşana zararlı yazılım tarafından aynı zamanda siber korsana iletilir. Böylelikle banka müşterisi aslında sisteme çift faktörlü kimlik doğrulaması ile güvenli şekilde giriş yaptığını düşünmesine rağmen, aslında siber saldırgan Hesberbot denilen bu zararlı yazılım sayesinde katmanlı güvenlik uygulamasını aşarak sisteme girme ve internet bankacılığı üzerinden istediği işlemi yapma imkânına kavuşacaktır[346].

Doktrinde, Yeşilyurt internet bankacılığı işlemlerinde doğrulamaya yönelik siber atak türlerinin zararlı yazılımlardan başka bir türünün ise ortadaki adam saldırıları gibi teknik açıdan nitelikli saldırılar olan çevrimiçi kanal bağlantı kesimi atakları olduğunu belirtmiştir. Zararlı yazılımlardan farklı olarak bu saldırı türünde, kullanıcı bilgilerin elde edilmesi yerine bilgisayar ve banka sunucusunun iletişimi fark edilmeden dinlenerek saldırgan tarafından sunucuya istemciymiş gibi, istemciye ise sunucuymuş gibi ağ üzerinde tanıtılması mümkündür[347].

---

[345] *Yeşilyurt*, s. 103.
[346] Hesperbot virüsü ile ilgili detaylı bilgi için bkz. *Bingöl/Karakoç*, s. 28-31.
[347] *Yeşilyurt,* s. 102'de belirtilen Hiltgen, Kramp ve Weigold.

İnternet bankacılığı konusunda diğer kullanılan siber saldırı yöntemleri ise oltalama, yalak (*watering hole*)[348], pharming[349] saldırıları örnek olarak gösterilebilir[350].

İnternet bankacılığına benzer şekilde zarar yazılımlar mobil cihazlara yönelik siber saldırılar ve mobil bankacılıkta siber güvenliğin temini açısından dikkate alınması gereken bir risk faktörüdür[351]. Özellikle mobil telefonlara yöneltilen çeşitli zararlı yazılımlar (örneğin 2007 yılında ortaya çıkan Flexispy denilen casus yazılım, İos işletim sistemine yönelik IKee ve Zeus trojanın mobil versiyonu olan Zitmo vb.) sayesinde salt kişilerin yalnızca telefon görüşmeleri ve adres defterleri kaydedilmekle kalmamış, aynı zamanda mobil bankacılık işlemlerinde siber güvenlik açısından önem taşıyan SMS mesajlarının da ele geçirildiği görülmüştür[352].

[348] Yalak (*watering hole*) denilen saldırı türünde, saldırganlar tarafından bankaların veya saldırı gerçekleştirilecek kamu kurumlarının ziyaret edebilecekleri web sitelerine zararlı yazılım enjekte edilir. Bu sayede, ilgili banka veya kurum çalışanın zararlı yazılım enjekte edilen web sitesini ziyaret etmesi sonucunda kullanıcı bilgileri ve parolalar söz konusu zararlı yazılım vasıtasıyla elde edilir. Bu konuda ayrıntılı bilgi için bkz. https://searchsecurity.techtarget.com/definition/watering-hole-attack (Gözden Geçirilme Tarihi: 29.10.2020).

[349] Pharming saldırılarında ise, banka ve kamu kurumlarına ait resmi siteleri barındıran sunucular ile ziyaretçi akınına uğrayan blog sayfaları ile forum sitelerini barındıran sunucuların açıklarından yararlanılarak ilgili sitelere zararlı yazılım yerleştirilmektedir. Sitenin ziyaret edilmesi sonucunda arka planda kurbanların bilgisayarlarına truva atı türevi bir zararlı yazılım yüklenmekte ve bu yazılım vasıtasıyla kullanıcıların geçmişte girdiği sitelere ait bilgilerin saklandığı çerez ve tanımlama dosyaları ile DNS ayarları manipüle edilmektedir. Bu konuda detaylı bilgi için bkz. *Çakır/Kılıç*, s. 118, 119.

[350] *Yeşilyurt*, s. 103'de belirtilen Kharouni.

[351] Çalışma açısından mobil cihazlara ve mobil cihazlara yönelik siber güvenlik riskleri genel itibariyle *Sağıroğlu/Alkan*, s. 320-323'den özetlenerek yukarıda aktarılmıştır.

[352] Buna örnek olarak, 2016 yılında keşfedilen Xbot denilen bir fidye yazılımı verilebilir. Xbot yazılımı, Google ödeme arayüzüne benzer şekilde bir oltalama sayfası kullanarak kullanıcıların kredi kartı ve bankacılık bilgilerini çalmaya çalışmaktadır. Aynı zamanda, söz konusu yazılım mobil bankacılık işlemlerinde ise SMS mesajlarını, iletişim bilgilerini mobil bankacılık onay mesajlarını ele geçirmiş ve kurbanlarının gerek bilgisayar gerekse bilgisayarlarını şifreleyerek bu şifrelerin kaldırılması için fidye ödenmesi talep edilmiştir. Bu konuda detaylı bilgi için *Sağıroğlu/Alkan*, s. 322.

ÜÇÜNCÜ BÖLÜM

ELEKTRONİK ÖDEMELERDE SİBER SALDIRILARA KARŞI ALINABİLECEK ÖNLEMLER

Yukarıda yer verilen elektronik ödeme sistemlerine yönelik siber saldırı yöntemlerine karşı, bu bölümde hukuken ve teknik açıdan siber güvenliğin sağlanması noktasında hangi önlemlerin alınması gerektiği değerlendirilmiştir. Bu kapsamda, öncelikle siber güvenlik alanında hangi genel önlemlerin alınması gerektiği irdelenerek siber güvenliğin sağlanmasında hangi metodolojik yöntemin izlenmesi gerektiği konusunda yazarın tespitlerine de yer verilecektir. Son kısımda ise, özellikle bankacılık sektörüne özgü olarak elektronik ödeme sistemleri bakımından siber güvenliğin temininde farklı siber saldırı vektörlerine bağlı olarak hangi önlemlerin alınması gerektiğine ilişkin de tespitler çerçevesinde tez içeriğinde siber güvenliğin tesis edilmesinde aranan sorulara cevap verilmeye çalışılacaktır.

3.1. SİBER HİJYEN VE SİBER DESTEKLİ MÜHENDİSLİK METODOLOJİSİ (CCE)

Bir kurum özelinde siber güvenliğin sağlanmasında klasik bir yaklaşım olarak "siber hijyenin"[353] sağlanması gerektiği önemli olarak düşünülse de, Idaho Ulusal Laboratuvarı (orijinal adı "International Idaho Lab" olup metin içerisinde "IDL" olarak belirtilecektir) tarafından inovatif, kademeli ve sonuca yönelik bir yaklaşım olan *Siber*

[353] Bochman, siber güvenlik açısından klasik bir yaklaşım olarak siber hijyenin şunları kapsadığı belirtmektedir: (i) Şirketin donanım ve yazılım varlığının kapsamlı bir envanterini çıkarmak, (ii) güvenlik, koruma duvarı ve saldırı tespit gibi en yeni koruyucu donanım ve yazılım araçlarını satın alıp kullanmak, (iii) çalışanları, olta e-postaları tanıma ve bunlardan sakınma konusunda sürekli eğitmek, (iv) "hava aralığı" yaratmak (teoride önemli sistemleri diğer ağlardan ve internetten ayırmak), pratikte gerçek bir hava aralığı yaratmanın mümkün olmadığı belirtilmiştir, (v) yukarıdakileri yapmak için çeşitli servis ve servis sağlayıcılarla desteklenen geniş bir siber güvenlik kadrosu oluşturmak. Bochman, siber hijyenin şirket içi uygulamalar açısından mükemmel bir şekilde uygulansa bile, finansal açıdan güçlü şekilde destek alan, sabırlı ve sürekli şekilde gelişime açık usta hacker'ları durdurmak açısından yetersiz olduğunu belirtmiştir. Bkz. Andy Bochman, "İnternet Güvenliği", Harvard Business Review Press Dijital Dönüşüm Siber Güvenlik, (*"Bochman"*), s. 20-25.

Destekli Mühendislik (CCE)[354] *Metodolojisi*nden bahsetmekte fayda bulunmaktadır. Özellikle elektronik ödeme endüstirisi bakımından yöneltilen siber saldırılar sonucunda, çoğu kez bankaların finansal kuruluşların yaşadığı finansal kayıplar ciddi olmakla beraber özellikle "güven" kurumu olarak görülmek istenen bu kurumların müşterileri nezdinde yaşayabileceği itibar kaybı da dikkate alındığında, siber güvenlikte klasik yaklaşımlar yerine inovatif yaklaşımların daha kayda değer olacağı değerlendirilmektedir.

Genel itibariyle, CCE bir kereye mahsus olmak üzere bir risk değerlendirmesinden ziyade, stratejik olarak üst düzeydeki yöneticilerin riskleri düşünme ve değerlendirme yönetimini değiştirmeyi amaçlayan kurumsal nitelikte siber güvenlik kültürü yaratmayı amaçlamaktadır. Buna göre, CCE metadolojisi temelde dört adımdan meydana gelmektedir[355]:

3.1.1. En Önemli İşlemleri Tespit Etmek (Consequence Priorization)

İlk adım, siber güvenlik konusunda olası tüm felaket senaryoları ve bunların neden olacağı büyük sonuçları, vakaları dikkate alarak *"sonuçları önceliklendirme yaklaşımı"* denilen en önemli ve öncelikle yapılması gereken işlemleri tespit etmektedir. Bu noktada, önemli olan bazı soruların cevapları aranarak olası bir siber saldırı sonucunda sekteye uğrayacak ve doğrudan şirketin varlığını tehdit edecek işlem ve süreçlerin saptanmasıdır. Örneğin, bir elektrik dağıtım şirketi açısından abonelerine

[354] Anılan metodoloji, İngilizcede orijinal ismi itibariyle "The Consequence-driven Cyber-informed Engineering (CCE) Methodology" olarak belirtilmiş olup Türkçe'ye "Sonuca Dönük Siber Destekli Mühendislik Metadolojisi" olarak tercüme edilebilir. Söz konusu metadolojinin henüz deneme aşamasında olduğu, 2019 yılında CCE'nin tam kapsamlı kullanılmasının hedeflendiği, 2020'ye kadar ise bazı servis sağlayıcılara uygulama lisansı verilmesinin planlandığı belirtilmiştir. Ayrıntılı bilgi için Bkz. *Bochman*, s. 27 (Gözden Geçirme Tarihi: 29.10.2020).

[355] CCE metadolojisi ve bu konuda atılacak adımlarla ile ilgili bu kısımda yer alan bilgiler Bochman'ın Harvard Business Review "İnternet Güvenliği" isimli makalesinden derlenerek özetlenmiştir. Bu konuda ayrıntılı bilgi için Bkz. Bochman, s. 29-39. CCE metadolojisi hakkında genel bir fikir almak açısından ise (The Consequence-driven Cyber-informed Engineering (CCE) Methodology başlıklı) aşağıdaki link üzerinden belirtilen sunum gözden geçirilebilir: https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1521570876.pdf (Gözden Geçirme Tarihi: 29.10.2020)

bir ay süreyle elektrik sağlamasını engelleyecek ya da bir doğalgaz dağıtım şirketinin kompresör istasyonlarına yapılacak ve müşterilere doğalgaz sevkini aksatacak bir siber saldırının sonuçları neler olur? Veya bir bankanın bilgi sistemlerine yöneltilen siber saldırıda sistemin ayağa kaldırılması konusunda maksimum dayanma süresi nedir ve bu sürenin aşılmasının ne gibi sonuçları olabilir? Bir diğer örnek ise bir siber saldırının kimya tesisi veya petrol rafinerisinin güvenlik sistemini hedef alması ve basıncı güvenlik sınırının üstüne çıkarması halinde yüzlerce insanın ölümüne veya yaralanmasına sebebiyet verir mi? Bu tarz bir siber atak söz konusu petrol şirketi açısından büyük tazminat davalarına yol açarak şirketin borsadaki hisse değerinin düşmesi ve şirketin iflas etmesine neden olur mu? Veya herhangi bir kurum nezdinde müşterilerinin kişisel ve ödeme bilgilerinin kötüniyetli kişilerce ele geçirilmesi halinde ilgili veri koruma otoritesine[356] (Türkiye'de Kişisel Verileri Koruma Kurumu) veri ihlali bildirimi nasıl ve en geç ne kadarlık bir süre içerisinde (Türkiye'de kanunda açık bir hüküm olmamasına rağmen KVK geçmiş kararlarında GDPR ile paralel şekilde bu süreyi 72 saat olarak belirtmiştir) yapılmalıdır? Kısacası, siber düşmanların nasıl davrandığını bilen analistler tarafından bazı soruların cevapları aranarak, aksadığında yıkıcı sonuçlar doğuracak işler ve saldırıya en elverişli hedefler olası senaryolar halinde üst yönetimin bilgisine sunulabilir.

3.1.2. Dijital Alanın Haritasını Çıkarma (Systems Analysis)

CCE metodolojisinde ikinci atılacak adım, şirketin mevcut dijital alanının haritasını çıkarmaktır. Bu noktada, tüm donanım, yazılım ve iletişim teknolojileri ve senaryodaki destekçi kişi ve diğer süreçlerin (üçüncü taraf tedarikçiler ve alınan servisler gibi) haritasını çıkarmak gerekir. Dijital harita, şirketin üretim aşaması, tüm kontrol ve otomasyon sisteminin yerini ayrıntısı ile belgelemeyi, süreç için gerekli fiziksel girdi

[356] Veri sızıntısı halinde Türkiye'de Kişisel Verileri Koruma Kurulu'na 72 saat içerisinde veri ihlali bildirimi yapılmalıdır. Veri ihlali bildiriminin nasıl ve ne şekilde yapılacağına ilişkin ayrıntılı değerlendirmelere çalışmanın 5.2.10 no'lu "Kişisel Verilerin Korunması Kanunu" başlığı altında yer verilmiştir.

ve olası tüm veri girişlerini takip etmeyi, kısacası şirketin internet ile bağlantılı tüm olası süreçlerini içermektedir.

3.1.3. Olası Saldırı Yollarına Işık Tutma (Consequence-Based Targeting)

Üçüncü adım ise, siber saldırganların olası saldırı yollarını tespit etmektir. Lockheed Martin[357] tarafından geliştirilen bu yöntemde, birinci adımda belirtilen hedeflere ulaşmak için siber saldırganın hareket edeceği en kısa ve en olası geçiş yollarını saptamak bu aşamada önemlidir. Bu konuda CCE uzmanları tarafından saldırganlar ve saldırı yöntemlerine aşina olunması sebebiyle dünyanın değişik yerlerinde benzer saldırılar hakkında devlet kaynaklarından alınan bilgiler ve tecrübeler danışmanlık verilecek şirkete veya kuruluşa aktarılır. Buradan hareketle, ilgili şirket özelinde mevcut güvenlik sisteminin ne olduğu, nasıl geliştirilmesi gerektiği, şirketin siber saldırıya karşılık verme gücü gibi faktörler ile olası saldırı yollarına ilişkin bir liste sunulur.

3.1.4. Riski Azaltma ve Riskten Korunma Olanakları Üretme (Mitigations and Protections)

Son atılacak adım ise, aslında en kritik adım olup bu noktada siber riskleri etkisizleştirme ve risklerden korunma olanakları ve yöntemleri hakkında çözüm üretmek önem taşımaktadır. Örneğin saldırganın hedefe ulaşabilmesi açısından on geçiş yolu var ise ve bunlar aynı bağlantı noktasından geçiyorsa siber saldırgan için tuzak kurmaya en elverişli olan noktanın burası olduğu tespit edilir. Bu örnekte olduğu gibi, bu noktaya ilk tehlike ikazında savunma ekibini uyararak hızla harekete geçmeyi sağlayacak ve saldırıyı yakında izlemek üzere algılayıcı (sensör)[358] yerleştirilebilir. Bu

[357] Michael J. Assante/Robert M. Lee, "The Industrial Control System Cyber Kill Chain", SANS Enstitüsü makalesi, 2015, (*"Assante/Lee"*) söz konusu makaleye ulaşmak için Bkz. https://www.sans.org/reading-room/whitepapers/ICS/paper/36297 ve Lockheed Martin, "The Cyber Kill Chain", (*"Martin"*), ilgili makale için Bkz. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (Gözden Geçirilme Tarihi: 29.10.2020).

[358] Algılayıcılar (sensörler), fiziksel ortam ile endüstriyel amaçlı elektrik / elektronik cihazları birbirine bağlayan bir köprü vazifesi görerek kontrol, koruma ve görüntüleme gibi çok farklı işlev ve kullanım

konuda diğer verilen bir örnek ise şirket sistemine felakete yol açabilecek dijital komutlar geldiğinde sistemi korumaya yönelik cihazlar eklenebilir, sisteme basınç veya ısının belirli bir seviyenin üzerine çıkmasını engelleyecek mekanik bir valf veya düğme yerleştirilmesi de bir önlem olarak dikkate alınabilir. Ancak, bu aşama ile ilgili olarak özellikle bir süreci izlemek ve kontrol sinyali göndermek için dijital bir kanala ihtiyaç var ise, bu kanalda dijital giriş ve çıkış yollarını asgariye indirmenin önemine dikkat çekilmiştir. Bu konuda büyük resme bakıldığında, şirket açısından eğer en kritik fonksiyonları destekleyen sisteme güvenilmez hale gelinmesi halinde devreye sokulabilecek bir B planı olarak şirketin asli operasyonlarını sınırlı düzeyde de olsa sürdürme imkânı yaratmak amacıyla back-up sisteminin[359] özellikle dijital teknolojilere ve bir ağa (özellikle internete) bağlı olmaması kritik derecede önem taşımaktadır.

3.2. GENEL ÖNLEMLER

Siber güvenliğin temini açısından, aşağıda ayrıntılı olarak izlenebilecek bazı metodojiler ile bankacılık ve finans sektörüne yönelik sektör-spesifik önlemlere geçilmeden önce aşağıda belirtilen bazı adımların kurumlar açısından önem taşıdığı düşünülmektedir:

imkanını haizdir. Diğer bir deyişle, sensörler ya da algılayıcılar otomatik kontrol sistemlerinde insanların duyu organlarına benzer şekilde çevrelerinde basınç, hız, sıcaklık ve benzeri değerleri olup bitenleri algılamasına olanak tanıyan teknolojik cihazlara verilen isimdir. Bkz. http://www.imajteknik.com.tr/alan-tarama-sensoru (Gözden Geçirilme Tarihi: 29.10.2020)

[359] Back-up sistemi, kurumlar açısından sahip oldukları bilgilerin kopyalanarak orijinal kaynağın bulunduğu yerden farklı bir alanda depolanması anlamına gelmektedir. Back-up temel itibariyle şu aşamalardan oluşmaktadır: (i) Öncelikle yedeklenmesi düşünülen belgeler (kayıtlar, veri tabanları, yazılı dokümanlar, vb.) belirlenir. (ii) Bu belgeler güvenli bir ortamda back-up media denilen (flash bellek, bulut bilişim, vb.) yerde kopyalanır. (iii) Orijinal belgelerde değişiklikler yapılması halinde (i) ve (ii) denilen adımlar periyodik olarak tekrarlanır. Back-up sistemi ile ilgili ayrıntılı bilgi için Bkz. https://www.baylor.edu/content/services/document.php/192120.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

Çalışma kapsamında birçok kez vurgulandığı üzere, siber güvenlikteki zafiyetler açısından en zayıf faktörün "insan faktörü" olduğu göz önüne alındığında[360], bu konuda kurum içerisinde çalışanlar nezdinde siber güvenlik farkındalığının artırılması ve bu konudaki eğitimlerin ne kadar önem taşıdığı ortadadır[361]. Ancak gündelik hayatta özellikle siber güvenlik alanındaki eğitimlerde çalışanların çoğu kez konuyu işe ara vermek amacıyla katıldıkları bir eğitim olarak görerek önemsemedikleri bilinen bir gerçektir. Öte yandan siber güvenlikle ilgili verilen eğitimlerin kuramsal düzeyde kalması ve siber ataklar bakımından uygulamaya yönelik birtakım tedbirlerin çalışanlara doğru bir şekilde aktarılamaması bu eğitimlerin etkinliğini azaltmaktadır. Bu nedenle, özellikle çalışanların aldıkları siber güvenlik eğitimleri akabinde eğitimciler tarafından kurgusal olarak bazı siber ataklar (örneğin phishing, sosyal mühendislik saldırıları, vb.) sanki gerçek hayatta gerçekleştiriliyormuş gibi çalışanlara yöneltilmeli ve gündelik hayatta çalışanların aldıkları bu eğitimleri gerçek hayatlarına yansıtıp yansıtmadıkları test edilmelidir[362]. Bu çalışmalar ve özellikle çalışanlara güvenlik açısından yaptıkları hatalarla ilgili geri bildirimler ile kurumda gerçekten yeni bir eğitime ihtiyaç duyulup duyulmayacağı ve özellikle eğitimde öne çıkarılması gereken konuların neler olduğu saptanmalıdır.

---

[360] 2014 yılında IBM, incelediği güvenlik vakalarının yüzde doksan beşinin "insan hatası" içerdiğini açıklamıştır. Bkz. IBM, "IBM Security Services 2014 Cyber Security Intelligence Index": https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligence_20450.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[361] Siber güvenlik eğitimlerinin içeriğinin ne olması gerektiğine ilişkin ayrıntılı bilgi için Bkz. Marc Dupuis, "Cyber Security for Everyone – An Introductory Course", 2017: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/CyberSecurityforEveryone-AnIntroductoryCourse.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[362] Siber güvenlikte farkındalık eğitimlerinin etki gücünü artırmak adına çalışanların hangi hataları ne zaman yaptıkları ve bu hatalardan kaçınabilmek açısından eğitimciler tarafından geri bildirim yapılması önem taşımaktadır. Örneğin bir kurum içerisinde personeli saldırılara daha dirençli hale getirmek için, tuzak e-postalar göndererek oltaya takılmalarını sağlamak ve akabinde ise bu tarz zaafların iyileştirilmesi açısından "Phisme" gibi yazılımlar kullanılmasını çalışanlara tavsiye etmek etkin bir yöntem olarak değerlendirilmektedir. Bkz. Alex Blau, "Siber Güvenlikte Çalışanların Alışkanlıkları", Harvard Business Review Press Dijital Dönüşüm Siber Güvenlik, (*"Blau1"*) s. 112. Sağıroğlu/Alkan'a göre ise, siber güvenlik açısından farkındalık eğitim faaliyetlerinin bilgilendirme, örnek prolem çözümleri ve alınan dersler, uygun sıklıkla tekrar ve güncellemeler, güvenli davranış biçimlerini otomatikleştirme (refleks gelişimi), etkin takip ile teşvik ve ödüllendirme içermesi gereklidir. Bu konuda detaylı bilgi için bkz. *Sağıroğlu/Alkan*, s. 155-156.

Siber güvenlik açısından diğer önemli bir mesele, maalesef bazı şirketlerin üst yönetim düzeyinde konunun ciddiyetinin anlaşılamaması ve konuya sadece finans perspektifinden bakılarak siber güvenlik meselesine yöneticiler tarafından sadece bir masraf kalemi olarak değerlendirilmesidir[363]. Oysaki, yukarıda ayrıntılı şekilde açıklandığı üzere siber ataklar bunu yaşayan firmalar açısından salt bir masraf kalemi olarak kalmamakta, aynı zamanda şirketlerin iflasına dahi yol açabilecek bir itibar kaybına sebebiyet vermektedir. Bu nedenle, diğer sektörlere kıyasla siber ataklar karşısında çok daha büyük finansal kayıp yaşayan finans ve bankacılık sektörleri açısından özellikle C düzeyinde siber güvenlik uzmanlığı bulunan bir yöneticinin bulunması hayati derecede önemlidir. Gelişen teknoloji ile birlikte, İngilizce'de "Chief Information Security Officer" (*CISO*)[364] olarak belirtilen bu yöneticinin, aldığı kararlar

[363] Doktrinde Alex Blau, "Yöneticilerin Siber Güvenliğe Yetersiz Yatırım Yapması" isimli makalesinde, şirketlerde siber güvenlik açısından zihinsel modellemenin kusurunun, siber güvenliği devamlı sürüp giden bir süreç olarak değerlendirmeyip çözüp bitirilebilecek bir problem görüldüğüne dikkat çekilmiştir. Yo-Jud Cheng ve Boris Groysberg ise, yöneticilerin hâlihazırda yöneticilerin siber güvenliği acil küresel bir sorun olarak gördüğü, ancak siber tehditlerin inatçılığı ile şirketlerin kırılganlığı arasındaki bağlantıyı yeterince iyi kuramadıklarını belirtmiştir. Detaylı bilgi için Bkz. Alex Blau, "Yöneticilerin Siber Güvenliğe Yetersiz Yatırım Yapması", Harvard Business Review Press (Dijital Dönüşüm Siber Güvenlik), (*"Blau2"*) s. 75. Yazarlar ayrıca günümüzde çoğu şirketin yönetim kurullarının, siber riskleri düzenli tartışma ve ihlal karşısında uygulanacak olağanüstü durum planını gözden geçirmeyi kapsayan sağlam bir siber güvenlik sürecinden yoksun durumda olduğunu, yönetim kurullarında siber güvenlik alanında yeterli uzmanlığa sahip olmayan kişilere bu alanda denetim yetkisi verildiğini bu durumun ise uzun vadede şirketlerin zararına olacağını ifade etmiştir. Bu konuda ayrıntılı bilgi için Bkz. J. Yo-Jud Cheng/Boris Groysberg, "Yönetim Kurulları Neden Siber Tehditle İlgilenmiyor", Harvard Business Review Press (Dijital Dönüşüm Siber Güvenlik), (*"Cheng/Groysberg"*), s. 59-71.

[364] CISO, Türkçe'ye "Bilgi Güvenliği Başkanı" olarak tercüme edilebilir (Serbest Çeviri). Literatürde, CISO'nun bulunduğu kuruma karşı şu görevlerinin olduğu belirtilmektedir: (i) Bulunduğu organizasyonun personelini, politikaların, süreçlerini siber tehditlere karşı korumak ve kurumsal olarak siber direncini artırmak, (ii) Kurumun mevcut personelinde, politikalarında, süreçlerinde veya süregelen operasyonlarında siber güvenlik açısından riskli durumları saptayarak bu durumu yönetime raporlamak, (iii) Kuruma karşı herhangi bir siber atak yöneltiğinde bu siber atağın etkilerini azaltmak ve kurumun mevcut faaliyetlerini ayağa kaldırmak noktasında ilgili personel, tedarik zinciri gibi diğer paydaşları teknik açıdan doğru yönlendirmek, (iv) Siber güvenlik ile ilgili kurum içerisindeki tüm personelin, politikaların, süreçlerin, uygulamaların ve teknolojilerin siber güvenlikle ilgili uyumlu olmasını sağlamak. CISO ile ilgili ayrıntılı bilgi için Bkz. Julia H. Allen/ Gregory Crabb/ Pamela D. Curtis/ Brendan Fitzpatrick/ Nader Mehravari/ David Tobar, "Structuring the Chief Information Security Officer", Software Engineering Institute Carneige Mellon University, Technical Note, Eylül 2015 (*"Allen Ve Diğerleri"*): file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/15tn007.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

açısından diğer yönetim kurulu üyelerinden bağımsız şekilde şirketin yönetim kuruluna raporlama yapması ve sadece şirketin yönetim kuruluna karşı sorumlu olmasının önemli olduğu değerlendirilmektedir.

Diğer bir önemli konu ise, elektronik ödemelere yönelik siber saldırılar yaşanması halinde zararı asgariye indirebilmek açısından şirketlerin "siber güvenlik sigortası"na olan ilgilerini artırmaktır. Bilindiği üzere, siber atak gerçekleştirilmesi akabinde çoğu kez siber atağı gerçekleştiren kişilerin izinin sürülmesi ve yakalanması imkânsız olduğundan, bu aşamada kurumların bu atak öncesinde özellikle sigorta şirketleri ile anlaşarak sigorta poliçelerindeki hangi klozların hangi siber saldırıları kapsayacağı özellikle kurumların hukukçuları tarafından üzerinde hassasiyetle durulması gereken bir meseledir[365].

Siber güvenliğin sağlanmasında, IT güvenliğinden sorumlu personelin gerek uzaktan erişim gerekse kişisel cihaz kullanım konularında en düşük hak (*least privilege*)

[365] Doktrinde, Lawrence A. Gordon, Martin P. Loeb ve Tashfeen Sohail tarafından kaleme alınan "A Framework for Using Insurance for Cyber-Risk Management" adlı makalesinde, yazarlar tarafından siber güvenlik sigortası açısından şirketlerin yaptığı başvuruda özellikle bu sigortayı alıp almama noktasında meydana gelebilecek zarar ile sigorta kapsamında tazmin edilebilecek meblağ dikkate alınarak bir karar verileceğini belirtmektedir. Yazarlara göre, özellikle siber güvenlik sigortasının kapsamını belirlerken şirketlerin, ticari sırların ifşası ve çalınması ile doğrudan sigorta edilen malvarlığına (yazılımsal ve donanımsal) yönelik kar kaybı gibi doğrudan meydana gelebilecek zararlara ilişkin riskleri (first-party risks) olabileceği gibi, kişisel bilgileri ve ödeme bilgileri çalınan kişiler nedeniyle üçüncü tarafların maruz kalabileceği zararlar konusunda da bir risklerinin (third-party risks) olabileceğini belirtmiştir. Bu nedenle, siber güvenlik poliçeleri konusunda kapsamın geniş tutularak poliçe meblağlarının 50 milyon Dolar ila 200 milyon dolar arasında tutulması gerektiği belirtilmiştir. Son olarak kurumların siber güvenlik sigortası yaptırmaya karar vermeleri açısından şu adımlar izlenmelidir: (i) Kurumun mevcut bilgi güvenliğine risklerine yönelik bir denetim gerçekleştirmek, (ii) Halihazırda şirketin eğer var ise mevcut sigorta şirketleri ile imzaladığı sigorta poliçelerinin olası siber ataklar karşısında şirketin ne kadarlık bir zararını tazmin edebileceği konusunda ayrıntılı değerlendirme yapmak, (iv) Son olarak ise, siber saldırı karşısında kurumun uğrayacağı zarar ile siber güvenlik poliçesi kapsamında sigorta poliçesinde ilgili kurumun ne kadarlık bir zararının tazmin edileceği arasındaki dengeyi gözeterek doğru siber güvenlik poliçesine karar vermek. Bu konuda detaylı bilgi için Bkz. Lawrence A. Gordon/Martin P. Loeb/Tashfeen Sohail, "A Framework for Using Insurance for Cyber-Risk Management" (*"Gordon/Loeb/Sohail"*): file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/FrameworkUsingCyberInsurance.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

prensibinin[366] göz önünde bulundurulması, bu kapsamda kimin, neye, nereden ve niçin erişeceğine dair ilke tabanlı bir erişim kısıtlaması getirilerek, bu kısıtlamanın tüm cihazlarda, ağlarda, uygulamalarda ve bulut ortamlarında gerçek zamanlı olarak uygulanması, erişim kontrolünde çok faktörlü kimlik doğrulama *(Multi-factor Authentication – MFA)*[367] yöntemlerinin kullanılması gerektiği siber güvenliğin sağlanmasında özellikle üzerinde durulması gereken yöntemler arasında sayılmıştır[368].

Son olarak, aşağıda özellikle CCE metodolojisinde de vurgulanacağı üzere, siber ataklar gerçekleşmeden önce kurumlar nezdinde gerçekten böyle bir atak gerçekleştirildiğinde hangi zararların ortaya çıkabileceği, hangi sistemlerin en çok bu tarz ataklardan etkilenebileceği ayrıntılı şekilde belirlenerek bir risk değerlendirmesi yapılmalı ve özellikle siber ataklar karşısından kurumların alternatif planlarının neler

---

[366] En düşük hak prensibi *(least privilege principle)*, her kullanıcının her program üzerinde asgari düzeyde yetki kullanarak sisteme giriş yapması esasına dayanmaktadır. Bu prensip ile sisteme giriş yapanların kaza veya hata sonucu sebep olabilecekleri zararların asgariye indirgenmesi amaçlanmaktadır. Başka bir ifade ile, bu prensiple yetki tanınan yazılımlar açısından sisteme tanımlanan yetkili kullanıcıların potansiyel temas sayını da minimuma indirerek programlara giriş yetkisi tanınması sonucu istenmeyen veya hatalı kullanımların da sınırlandırılması amaçlanmaktadır. Bu konuda daha detaylı bilgi için Bkz. Fred B. Schneider, "Least Privilege And More", Cornell University, ABD, s. 20 (*"Schneider"*): https://www.cs.cornell.edu/fbs/publications/leastPrivNeedham.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[367] Çok faktörlü kimlik doğrulama, kısaca kullanıcının bir sisteme girerken kimlik doğrulaması işlemi açısından iki veya daha fazla katmandaki bilgiyi (cep telefonuna gelen SMS mesajı, parmak izi, giriş şifresi gibi) girmesini gerektiren bir sistemin öngörülmesi anlamına gelmektedir. Siber güvenlik açısından çok katmalı güvenlik yapısının siber saldırganlar açısından daha caydırıcı olduğu ve siber güvenlik açıklarını azaltmak açısından günümüzde etkin bir yöntem olarak kullanılmaktadır. Bu konuda detaylı bilgi için bkz. Bkz. Monther Aldwairi/Saoud Aldhanhani, "Multi-Factor Authentication System", file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/MFA-ASL_CamReady.pdf (Gözden Geçirilme Tarihi: 29.10.2020). Marc Goodman ise, "Geleceğin Suçları Dijital Dünyanın Karanlık Yüzü" adlı kitabında siber güvenlik açısından günümüzde Google, Microsoft, PayPal, Apple, Twitter ve çok sayıdaki şirket tarafından kullanıcı adı ve parolayı bir şifrematik, anahtarlık ya da cep telefonu gibi kullanıcıların sahip oldukları şeylerle birleştiren iki aşamalı doğrulama sisteminin yaygın şekilde kullanıldığını ve geleneksel şifreleme yöntemlerine kıyasla nispeten dahi olsa bu yöntemin güvenilir olduğunu ifade etmektedir. Goodman, iki aşamalı kimlik doğrulamayı güvenlik açısından önemli bir adım olarak değerlendirmesine rağmen, günümüzde hacker'ların yaygın şekilde telefon virüsleri ile kısa mesajlara müdahale edilen "aradaki adam" (man-in-the-middle) saldırıları ile bozulabildiğine dikkat çekmiştir. Bu açıdan Goodman'a göre özellikle geçmişteki yaşanan somut siber saldırılar üzerindeki örneklerden hareketle çok faktörlü kimlik doğrulama açısından biyometrik verilerin de kullanılması çok daha etkin bir çözüm sağlayacaktır. Bu konuda detaylı bilgi için Bkz. Marc Goodman, "Geleceğin Suçları Dijital Dünyanın Karanlık Yüzü", Timaş Yayınları, İstanbul, 2016, (*"Goodman"*) s. 508-509.

[368] *Özkaya/Sarıca/Durmaz*, s. 33.

olabileceği (hangi bilgilerin backup sisteme aktarılması gerektiği, sigorta var ise hangi zararların karşılanabileceği vb.) en başta tespit edilmelidir.

Yukarıda, genel itibariyle siber güvenliğin temini açısından atılması gereken genel adımlar belirlendikten sonra ise özellikle yazar tarafından birçok güvenlik önlemine kıyasla daha etkin ve inovatif bir yaklaşım olduğu düşünülen CCE metodolojisi ayrıntılı şekilde açıklanmıştır. Aşağıda ise finans sektörüne özgü sektör-spesifik siber güvenlik önlemleri hakkında ayrıntılı değerlendirmelere yer verilecektir.

3.3. ELEKTRONİK ÖDEME TÜRÜNE BAĞLI OLARAK SİBER SALDIRILARA KARŞI ALINMASI GEREKEN ÖNLEMLER

Bu başlık altında İkinci Bölüm'de teknik itibariyle detaylı şekilde incelenen dokuz adet saldırı türüne karşı teknik ve hukuki açıdan hangi önlemlerin alınması gerektiği aşağıda kapsamlı şekilde değerlendirilmiştir.

3.3.1. Kartlı Ödeme Sistemlerine Yönelik Alınması Gereken Önlemler

Kart dolandırıcılıklarının, genel itibariyle daha ziyade kart üzerinde depolanmış olan verileri ele geçirmek maksadıyla, işyerlerine veya ATM cihazlarına dolandırıcılar tarafından çeşitli aparatlar yerleştirmek suretiyle gerçekleştirildiği ve bu verilerin daha sonra yasa dışı yollarla harcama yapılmasına hizmet ettiği yukarıda belirtilen olgular arasındadır[369]. Bu tarz dolandırıcılıkların önlenmesi noktasında çalışmada özellikle ATM'lerin, kameraların bulunduğu alanlara yerleştirilmesini ve bu bağlamda bankaların müşterilerinin kart kullanımında bilinçlendirilmesinin önemli olduğunu değerlendirilmektedir. Öte yandan, kartlı ödeme sistemlerinde siber güvenlik açısından üzerinde durulması gereken bir diğer husus klavuz niteliğindeki PCI SSC standartlarıdır. PCI SSI, 2006 yılında kurulmuş olup kurucuları American Express, Discover, JCB International, Mastercard ve Visa Inc. Şirketleridir ve bu şirketlerin yönetimde eşit haklara sahip olduğu bilinmektedir. İngilizce açılımı "Payment Card

[369] *Yeşilyurt*, s. 104.

Industry Security Standards Council"[370] olan bu kurum, dünyada özellikle kart ödemelerinde global açıdan bilgi güvenliğinin sağlanması konusunda ve özellikle kart hamilleri açısından eğitim, farkındalık ve etkin uygulama noktasında dünya çapında uygulanabilecek kılavuz niteliğinde standartları ve kuralları düzenlemektedir[371]. Kısaca özetlemek gerekirse, PCI SSI şu hususları içermektedir: (i) güvenli ağ ve sistemlerin oluşturulması ve bakımı, (ii) kart sahibinin verilerinin korunması, (iii) güvenlik açıkları yönetimi programı takibi, (iv) güçlü erişim kontrol tedbirlerinin hayata geçirilmesi, (v) ağların düzenli olarak takibi ve testleri, (vi) bilgi güvenliği prensiplerinin korunması[372].

Ayrıca, PCI SSC'nin özellikle ilgili pazara katılımın ve bilgi düzeyinin artırılması, güvenlik standartları ve geçerliliğin geliştirilmesi, gelişmekte olan ödeme kanallarının korunması ve iş birliği standartlarının ve tutarlığın geliştirilmesi olmak üzere dört stratejik hedefi bulunmaktadır[373].

PCI SSC çerçevesinde alınması gereken tedbirlerle ilgili olarak aşağıdaki şekilden de görüleceği üzere, PCI ile ilgili sürekli bir döngü olduğu kabul edilen üç adımın gerçekleştirilmesi gerektiği kabul edilmektedir[374]:

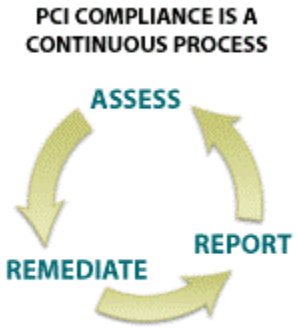
Değerlendirme: Kart haliminin sahip olduğu veriler, bu hususta bir bilgi işlem envanteri çıkarılarak her aşamada (ödeme kartının işlenmesi, sistemdeki zafiyetlerin analizi) değerlendirilmesi.

İyileştirme: Zafiyetlerin düzeltilmesi ve gerekli olmadığı sürece kart sahibi bilgilerinin depolanmasının önüne geçilmesi.

---

[370] Yazar tarafından Türkçe'ye "Ödeme Kart Endüstrisi Güvenlik Standartları Kuruluşu" olarak çevrilmiştir (Serbet Çeiviri). Bu konuda ayrıntılı bilgi için bkz. https://en.wikipedia.org/wiki/Payment_Card_Industry_Security_Standards_Council (Gözden Geçirilme Tarihi: 29.10.2020).
[371] https://www.pcisecuritystandards.org/about_us/ (Gözden Geçirilme Tarihi: 29.10.2020).
[372] *Yeşilyurt*, s. 110-111.
[373] https://www.pcisecuritystandards.org/about_us/ (Gözden Geçirilme Tarihi: 29.10.2020).
[374] https://www.pcisecuritystandards.org/pci_security/how (Gözden Geçirilme Tarihi: 29.10.2020).

Raporlama: banka ve kart bilgilerinin derlenerek gerekli raporların sunulması.



Şekil-3.1: PCI 3 Adım Süreci[375]

Yukarıda belirtilen PCI SSC ile ilgili güvenlik standartlarının yanı sıra kartlı işlemler konusunda SET ve SSL güvenlik protokolleri de yaygın uygulamalar olarak dikkate alınabilir[376].

Günümüzde neredeyse herkesin kredi kart bilgileri bir şekilde siber korsanlar tarafından ele geçirilerek ya kendi yasa dışı amaçları için kullanılmakta ya da Dark Web denilen ve internetin sanal suç ortamında kötü niyetli üçüncü kişilerle bir şekilde paylaşılmaktadır. Kredi kartlarının özellikle son zamanlarda yaygın şekilde kullanılması ve bilgisayar korsanları tarafından kolaylıkla ele geçirilmesi nedeniyle siber güvenlik açısından tavsiye edilen yöntemler şu şekilde sıralanabilir: Kredi kartları ile e-ödeme işlemi gerçekleştirilmesi akabinde mümkün mertebe internet alışverişlerine müşterileri tarafından banka personeli ile iletişime geçilmek suretiyle kredi kartı internet ortamında kullanıma kapatılmalıdır. Kart şifresi açısından güçlü parola yönetimi benimsenerek parolalar periyodik olarak yenilenmeli ve hatta kredi kartları ve debit kartları da bankalar tarafından periyodik olarak yenilenmelidir. Müşteriler tarafından kredi kartlarında harcama yapılırken sanal kart[377] uygulamasının

[375] Şekil-3.1'in aktarıldığı görsel için bkz. https://security-scanning.com/security-scans/pci-avs-compliance-scans/ (Gözden Geçirilme Tarihi: 29.10.2020).
[376] SET ve SSL konusunda ayrıntılı değerlendirmelere çalışmanın 1.2.1.1. başlıklı "Kredi Kartları" ile ilgili başlık altında yer verilmiştir.
[377] Sanal kart konusunda çalışmanın 1.2.1.1 no'lu başlık altında ayrıntılı analizlere yer verilmiştir.

tercih edilmesi siber güvenlik açısından daha güvenilir bir yoldur. Yukarıda belirtildiği üzere, sanal kart ya da kredi kartı ile gerçekleştirilen alışverişlerde 3D Secure özelliğinin devreye alınmasında fayda bulunmaktadır. Bu özelliğin devreye alınmasında ilgili banka görevlileri ile iletişime geçilebilir. Çalışmada özellikle "kart dolandırıcılıkları" ile ilgili yer verilen detaylı analizlerden anlaşılacağı üzere kredi kartlarında sık rastlanan bir dolandırıcılık yöntemi kart bilgilerinin kopyalanması suretiyle gerçekleştirilmektedir. Bu noktada POS cihazlarında kart ile ödeme gerçekleştirilmesi esnasında özellikle kredi kartları gözden ayrılmamalı, POS cihazının çalışmadığı veya yenisinin getirileceğinin belirtilmesi halinde kredi kartının gözden uzak bir yere gitmesine izin verilmemeli, eğer karttan ödeme yapılmadığı belirtilmişse ilgili slipten karttan para çekilmediği veya ödeme işleminin iptal edildiği kontrol edilmelidir. Yine aşağıda teknik detaylarına yer verileceği üzere, özellikle phishing denilen oltalama saldırılarına karşı internet üzerinden kart bilgilerinin girildiği web sitesi kullanıcılar tarafından dikkatle kontrol edilmeli ve özellikle bankaların kurumsal web siteleri ile kart üzerinden ödeme yapılacak web sitelerinin aynı olup olmadığı kontrol edilmelidir. Ayrıca yukarıda belirtilen SSL sertifikalı web sitelerinden yapılan alışverişlerde kredi kartı bilgileri korunacağından özellikle SSL sertifikasına sahip web sitelerinden alışveriş yapılması işlem güvenliği açısından daha uygun olacaktır. Yukarıda incelenen PCI SSC'in kılavuz niteliğindeki kuralları ve standartları kart güvenliğinin sağlanmasında önem taşımaktadır.

3.3.2. Finans Sektöründeki Oltama Faaliyetlerine Yönelik Alınması Gereken Önlemler

Oltalama saldırısı, finans ve bankacılık sektöründe diğer sektörlere kıyasla daha sık rastlanan bir saldırı vektörüdür. Oltalama saldırısı, genelde saldırganlar tarafından hedeflerindeki sistemlere zararlı yazılım enjekte edilmesi veya sosyal mühendislik saldırılarının gerçekleştirilmesi amacına hizmet eden öncü bir siber saldırı vektörü olduğundan, öncelikle finans kuruluşlarında çalışan personelin hangi içerikteki oltalama e-maillerinin phishing saldırısı olduğu konusunda yüksek bir farkındalığa

ulaşması önem taşımaktadır. Başka bir ifadeyle, finans sektöründe çalışanların özellikle organizasyon yapısı iitibariyle geniş bir kitle olduğu dikkate alındığında saldırganlar devamlı surette oltalamaya yönelik e-mailler veya spear phishing denilen hedefe yönelik oltalama saldırıları vasıtasıyla sistemi istismar etmek konusunda yoğun bir çaba ve motivasyon içerisindedir.

Aşağıda finans sektörüne özgü oltalama saldırıları açısından alınabilecek bazı önlemler şu şekildedir[378]:

3.3.2.1. E-mail Veya Web Sayfası Kişiselleştirme

Bankaların ve diğer finans kuruluşlarının phishing saldırıları konusunda alabilecekleri en basit yöntem, müşterileri ile kurulacak e-mail veya web sayfasına yönelik iletişim kanallarında mümkün mertebe ilgili banka personeline yönelik kişiselleştirilmiş bilgi ile müşteriyle iletişime geçilmesini sağlamaktır[379]. Konuyu somutlaştırmak açısından örnek vermek gerekirse, banka tarafından müşterilerine gönderilen her e-mail içeriğinde müşterinin adı-soyadı bilgisine yer verildiği takdirde, zamanla müşteriler banka tarafından gelen e-maillerde kendi ad ve soyadlarının olacağı konusunda bir algıya ulaşacaktır. Dolayısıyla müşteriler açısından zaman içerisinde banka imajı altında saldırganlar tarafından ad ve soyadları olmayan emaillerin banka tarafından gönderilmediği konusunda bir farkındalık oluşacaktır. Müşterilerin ayrıca web siteleri üzerinden internet bankacılığı ile gerçekleştirdikleri işlemlerde kişisel bilgileri girilmek suretiyle bankanın sistemine girilmesi de kişiselleştirme kapsamında değerlendirebilir[380].

---

[378] Finans sektöründe phishing saldırılarına yönelik alınması gereken tedbirlerle ilgili daha detaylı bilgi için Bkz. Alhuseen Omar Alsayed/Anwar Bilgrami, "E-Banking Security: Internet Hacking, Phishing Attacks, Analysis And Prevention of Fradulent Activities", International Journal of Emerging Technology and Advanced Engineering, C: 7, S: 1, Ocak 2017 (*"Alsayed/Bilgrami"*): file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/E-BaningSecurityHuseenandBilgrami2017.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[379] *Alsayed/Bilgrami*, s. 112-113.

[380] *Alsayed/Bilgrami*, s. 113.

3.3.2.2. Koruyucu Yazılım

Daha önceden de belirtildiği üzere, oltalama saldırganlar tarafından sık kullanılan bir yöntem olup oltalama neticesinde saldırganlar hedefteki sisteme genelde zararlı yazılım enjekte etmeyi amaçladığından, anti-virüs ve anti-spyware denilen koruyucu yazılımların kullanıcılar tarafından kullanılması önemli bir güvenlik tedbiri olabilir[381]. Özellikle yukarıda belirtildiği gibi saldırganlar kimi zaman banka müşterilerinin şifrelerini kaydetmek amacıyla keylogger gibi yazılımlar kullandığından bu yazılımlara karşı antilogger denilen ve şifre kaydedilmesini engelleyen yazılımların kullanılması bu tarz saldırılara karşı korunma açısından yarar sağlamaktadır[382].

3.3.2.3. Çok Unsurlu Kimlik Doğrulama (Multi-factor Authentication)

Yukarıda da belirtildiği gibi, günümüzde bankalar açısından çok unsurlu kimlik doğrulama oltalama saldırıları ile mücadale noktasında en etkin yöntemlerden birisi kabul edilmektedir. Genelde bankalar müşterilerine sisteme girmeleri açısından birisi müşterilerinin bildiği, diğeri ise müşterilerinin sahip olduğu bilgiyi girerek sisteme erişmelerine imkân sağlamaktadır[383]. Bunun nedeni ise, en az iki katmanlı kimlik doğrulamada phishing saldırıları birbirinden bağımsız olan kimlik doğrulama katmanlarından birisi saldırganlar tarafından istismar edilse dahi diğer katman ihlal edilmeyeceğinden banka müşterisi siber ataklara karşı korunmuş olacaktır.

3.3.2.4. Müşteri Farkındalığının Artırılması

Aşağıda özellikle sosyal mühendislik saldırılarına karşı alınması gereken önlemlerde de açıklandığı gibi, phishing saldırılarında banka müşterilerinin bu konuda farkındalığının artırılması önem taşımaktadır. Phishing ile ilgili müşteri farkındalığının artırılması eğitimle olabileceği gibi banka tarafından email veya farklı bildirim kanalları ile periyodik olarak müşterilerin bilgilendirilmesi suretiyle de yapılabilir.

---

[381] *Alsayed/Bilgrami*, s. 113.
[382] *Alsayed/Bilgrami*, s. 113.
[383] *Alsayed/Bilgrami*, s. 113-114.

Örneğin, müşterilere bankaların kesinlikle müşterilerin ad, soyad, kredi kartı numarası ve şifresi gibi hassas nitelikle kişisel ve ödeme bilgisini talep etmeyeceği, banka müşterilerinin kendilerine yöneltilen acil talepli ve doğrudan kişisel email adreslerine gönderilen email içeriklerine kesinlikle cevap vermemesi gerektiği, bankalar tarafından asla gayri resmi emailler aracılığıyla bir linke ulaşılması ve form doldurulmasının talep edilmeyeceği gibi hususlarda banka müşterilerinin periyodik olarak bilgilendirilmesinin önem taşıdığı üzerinde durulmuştur[384].

3.3.3. Elektronik Ödemelerde Sosyal Mühendislik Saldırılarına Karşı Alınması Gereken Önlemler

Yukarıda da belirtildiği üzere, oltalama yöntemi (phishing e-mailleri veya spear phishing denilen hedef odaklı oltalama) zaman zaman sosyal mühendislik saldırılarında da kullanılan teknikler arasındadır. Bu tür oltalama e-maillerinde sosyal mühendisler genelde bir problem açıklayan mesajlar, büyük bir para kazanıldığını içeren mesajlar ve yardım isteyen mesajlar ile hedeflerindeki kurbanlarına yönelerek kimlik ve ödeme bilgileri gibi hassas bilgileri çalmak amacıyla kurbanlarını manipüle etmeye çalışmaktadır[385]. Dolayısıyla burada sosyal mühendislik saldırılarında özellikle banka ve finans kuruluşları açısından kritik faktör, eğitimler sonucunda ilgili personelin bu konuda yüksek seviyede bir farkındalığa sahip olup olmadığıdır. Bankaların bilgi sistemlerinde özellikle yazılımlardaki açıkların istismar edilmesinde yama yönetimi önemli bir olgu olarak görülse de, çalışmada insanlardaki siber güvenlik konusundaki bilgi açığının ancak bu konuda iyi bir eğitim ile giderilebileceği değerlendirilmiştir. Genelde, özellikle banka personeli açısından görülen problem saldırganlar tarafından sahte bir web sitesi kullanılarak veya emaille belirli bir linke yönlendirmek suretiyle müşterilerinin genelde kandırılmasıdır. Oysaki bankaların hiçbir zaman müşterilerine ait özel bilgileri e-mail yoluyla talep etmeyeceği veya herhangi bir link gönderip bir form doldurulmasını talep etmeyeceği bilinmesi gereken

[384] *Alsayed/Bilgrami*, s. 114.
[385] *Özkaya/Sarıca/Durmaz*, s. 143.

bir gerçektir[386]. Öte yandan, sosyal mühendislik saldırıları açısından ilgili bankanın veya finans kuruluşunun personeli, içeriğini bilmediği e-mailleri kesinlikle açmaması gerektiği konusunda uyarılmalıdır.

Öte yandan sosyal mühendislik saldırıları ile mücadele farkındalık eğitimi gibi insan faktörünü eğitmeye yönelik etkinlikler olabileceği gibi, aynı zamanda ilgili kuruluşun donanım, yazılım ve ağ bağlantıları gibi sistemleri de korumaya yönelik teknolojik içerikli güvenlik önlemlerini içermelidir. Söz konusu teknolojik önlemler, kriptorafik şifreleme yöntemlerinin kullanılması, güvenlik duvarı ve antivirüs yazılımları gibi teknolojik çözümleri içerebilir. Bu çerçevede, bankalar en iyi teknik önlemleri almakla beraber doktrinde de ifade edildiği üzere, en iyi bilgisayarla en iyi teknik önlemler alınsa dahi, konu dönüp dolaşıp insan faktörüne dayandığı noktada, siber saldırganlar tarafından riskin tamamen bertaraf edilmesi mümkün olmayıp sadece azaltılabilmesi söz konusudur[387].

3.3.4. SWIFT Sistemine Yönelik Gerçekleştirilen Saldırılar Karşısında Alınması Gereken Tedbirler

SWIFT'e yönelik CSP Programı'nda SWIFT kaynaklı siber tehditlere yönelik sektördeki siber güvenlik alanında uzman kişilerle iş birliği içerisinde hareket edilmesi gerektiği vurgulanarak özellikle aşağıda belirtilen üç temel amaç çerçevesinde hareket edilmesi gerektiği belirtilmiştir[388]:

(i) Bulunduğun Ortamı Koru *(Secure Your Environment)*

(ii) Erişimin İle İlgili Bilgi Sahibi Ol ve Sınırla *(Know and Limit Access)*

(iii) Tespit Et Ve Cevap Ver *(Detect and Response)*

Yukarıda belirtilen temel amaçlar toplamda CSP çerçevesinde yirmi yedi adet güvenlik kontrolüne tabi tutularak her bir kontrol tedbirinin SWIFT müşterinin maruz

[386] *Özkaya/Sarıca/Durmaz*, s. 146.
[387] *Long*, s. 13.
[388] *F-Secure Raporu*, s. 10.

kalabileceği spesifisik riskleri azaltmada etkin yöntemler olacağı ileri sürülmüştür[389]. Bu güvenlik tedbirleri ile izin verilmeyen SWIFT mesajlaşmasının ve sistem üzerindeki finansal işlemlerin istenmeyen şekilde değiştirilmesinin engellenmesi, yetkisi olmayan üçüncü taraflar ile iş yapılmasının önlenmesi, bilgisayar sistemleri, operatör bilgileri ve ticari bilgilerin sızdırılmasının önüne geçilmesi hedeflenmiştir[390].

CSP ile ortaya konulan güvenlik tedbirlerinin müşterilerin yerel SWIFT altyapısı bakımından güvenli alan yaratacağı ve böylelikle tüm yerel SWIFT sistemlerinin daha geniş içerikteki girişim ağlarını sınırlandırma ve bu güvenli alanın korunmasında etkinlik sağlayacağı öngörülmüştür. CSP kapsamında kontroller yedi ilke ile açıklanmaktadır[391]:

1. İç Erişim Alanlarının Sınırlandırılması Ve Kritik Sistemlerinin Korunması

2. Atağa Maruz Kalabilecek Yüzeyin Ve Zafiyetlerin Azaltılması

3. Fiziksel Olarak Ortamın Korunması

4. Sisteme Giriş Açısından Gerekli Olan Bilgilerin Uygunluğunun Kontrol Edilmesi

5. Kimliklerin Yönetimi Ve Tanınan Yetkilerin Ayrıştırılması

6. Sisteme Yönelik Anormal Aktivitelerin Saptanması Ve İşlem Kayıtlarının Tutulması

7. Ataklara Verilecek Cevapların Planlanması Ve Bilgi Paylaşımı.

3.3.5. Elektronik Finans Sektöründeki Zararlı Yazılımlara Karşı Alınması Gereken Önlemler

Özellikle bankacılık sektörü gibi geniş bir bilişim ağına sahip sistemlerin özellikle zararlı yazılımlardan kaynaklanabilecek siber risklere daha açık olduğu görülmektedir. Bu noktada, zararlı yazılımlara karşı alınabilecek bazı tedbirler şunlardır[392]:

---

[389] *F-Secure Raporu*, s. 10.
[390] *F-Secure Raporu*, s. 10.
[391] *F-Secure Raporu*, s. 11.
[392] *Özkaya/Sarıca/Durmaz*, s. 186.

Bankaların şubeleri aracılığıyla da olmak üzere kredi, ödeme mutabakatı vb. olmak üzere binlerce finansal işlem gerçekleştirdiği dikkate alındığında kullanılan işletim sistemlerindeki güvenlik güncellemelerinin düzgün şekilde yapıldığı periyodik şekilde kontrol edilmelidir[393].

Çalışanlara özellikle yasal olmayan hiçbir web sitesine girilmemesi ve yasal olmayan web sitelerinden dosya indirilmemesi konusunda siber güvenlik eğitimleri sırasında yazılı bildirim yapılmalıdır.

Finans sektöründe ve bankalarda çalışan bilgi işlem uzmanlarının kullanmayı düşündükleri yazılımları aracı siteler yerine doğrudan resmi kaynaktan indirmeleri sağlanmalıdır.

Bankacılık ve sektöründe "yama yönetimi"[394] denilen anlayış, zararlı yazılımlar karşısında etkin bir yöntem olup güvenlik güncellemelerinin uç cihazlara ve altyapısı kritik diğer sistemlere yüklenmesi anlamına gelmektedir.

Özellikle fidye yazılımı saldırılarının yayılmasını engellemek açısından sistem içindeki tüm ağların birbirinden ayrılması ve ağ paylaşımlarının kapatılması önemlidir.

Yukarıda da belirtildiği üzere, minimum yetki (*least privilege*) prensibi çerçevesinde hareket edilerek ihtiyacı olmayan kullanıcılar açısından admin denilen yönetici yetkileri kapatılmalıdır.

Çalışmanın 3.1. numaralı "Genel Önlemler" başlığında da belirtildiği üzere, zararlı yazılımların öncü olarak kullanıldığı oltalama saldırısı ile fidye yazılım saldırılarını

---

[393] Kaspersky, "Avoiding A Trojan Virus: Keeping the Gates Closed" (*"Kaspersky"*): https://www.kaspersky.com/resource-center/preemptive-safety/avoiding-a-trojan-virus (Gözden Geçirilme Tarihi: 29.10.2020).

[394] Yama (*patch*), yazılımların güncellenerek ve/veya hatalarından arındırmak için hazırlanan paketlere verilen isimdir. Bkz. http://csirt.ulakbim.gov.tr/dokumanlar/YamaYonetimi.pdf (Gözden Geçirilme Tarihi: 01.09.2020). Yama yönetimi ise, bu çalışma kapsamında yukarıda da belirtildiği üzere zararlı yazılımların engellenmesi amacıyla ağ üzerinde olası tüm açıkların tespit edilerek bu bağlamda sistemin güncellenmesi ve olası açıklara karşı öngörülen yazılımların sisteme entegre edilmesi sürecini ifade etmektedir. Yama yönetimi ile ilgili detaylı bilgi için bkz. https://cenkercetin.com/yama-yonetimi-en-iyi-2020-best-practices/ (Gözden Geçirilme Tarihi: 29.10.2020).

önlemek açısından siber güvenlik eğitimleri ile çalışanların bu konudaki farkındalığı artırılabilir.

Ağ geçitleri vasıtasıyla e-mail ve web erişimi kontrol altına alınmalıdır.

Şüpheli işlemlerin takip edilmesi amacıyla kapsamlı bir uç cihaz güvenliği uygulanmalıdır.

3.3.6. Finans Sektöründe Ağ Saldırılarına Karşı Alınması Gereken Önlemler

Finans sektörü ve bankalar özellikle bilişim teknolojileri altyapısı itibariyle geniş bir ağı yönetmek durumunda oldukları için kimi zaman siber güvenliğin bütün bir organizasyon açısından sağlanması uygulamada zorluk teşkil etmektedir. Aşağıda açıklanacağı üzere, bankalar açısından katmanlı ağ güvenliği, derinlikte savunma stratejisi, fiziksel ve sanal ağ bölümlendirmesi, saldırı tespit ve önleme sistemleri ile güvenlik duvarı özellikle bazı siber saldırıların bertaraf edilmesinde etkin koruma yöntemidir.

3.3.6.1. Ağ Güvenliğine Katmanlı Yaklaşım ve Derinlikte Savunma Stratejisi

Katmanlı güvenlik, başta güvenlik duvarı olmak üzere saldırı tespit ve önleme sistemleri ile veri kaybı önleme sistemleri de dahil olmak üzere bu kavram savunma hattının birçok safhasının bütüncül bir şekilde dikkate alınarak sistem ve verileri saldırılara karşı koruma yaklaşımı olarak tanımlanabilir[395]. Bu noktada, bankalar açısından duruma bakıldığında katmanlı güvenlik sistemleri birçok etmenin birleşiminden meydana gelmesi sebebiyle aslında karmaşık ve maliyetli olmasına rağmen, bankaların siber ataklar noktasında müşterilerine karşı güven kurumu olarak itibarının korunması ve güvenlik sistemleri itibariyle değişik saldırı vektörlerine karşı hassasiyeti olduğu dikkate alındığında optimum güvenliği sağlamada etkin bir araç olduğu değerlendirilmiştir. Konuyu teknik detaylardan sıyrılarak basitçe açıklamak gerekirse, temel itibariyle her bir katman, diğer katmanın zayıflıklarını gidermek

[395] *Özkaya/Sarıca/Durmaz*, s. 343.

açısından ağ üzerinde maksimum düzeyde alabileceği tüm güvenlik tedbirlerini alır. Ağ Güvenliğinde Katmanlı Yaklaşım açısından katmanların şu şekilde dikkate alınması gerekmektedir[396]:

DLP:

Veri Kaybını Önleme Yazılımı[397] olarak Türkçe'ye tercüme edilebilen DLP, hassas nitelikteki verilerin bir ağdan çalınmasını veya bir ağdan kaçmasını önlemek amacıyla tasarlanan yazılım ve donanım sistemini ifade etmektedir. DLP sistemleri temel itibariyle, kullanım halindeki veriler, veri hareketsizliği ve hareket halindeki veriler olmak üzere üç farklı durumda izleme ve koruma amacıyla tasarlanmıştır[398].

IDS/IPS:

IDS[399], Türkçe'de "Saldırı Tespit Sistemi" anlamına gelmekte olup güvenliğin sağlanması açısından insan faktöründeki hatayı bertaraf etmek amacıyla akıllı olarak tanımlanabilecek bir sistem olarak ağa yönelmiş olan tüm trafiği algılama, veri paketinin içeriğini kontrol etme ve bir saldırı olduğunun fark edilmesi halinde otomatik olarak (ne şekilde tanımlandı ise) bağlantıyı tamamen kesmek veya kesme yeteneğini haiz başka bir cihazı uyarmak, sistem yöneticisine haber vermek ve raporlama yapmak gibi yetkinlikler açısından tasarlanmıştır[400].

---

[396] *Özkaya/Sarıca/Durmaz*, s. 344.
[397] DLP, İngilizce'de "Data Loss Protection" olarak ifade edilmektedir. DLP yazılımı ve araçları, uç nokta etkinliklerinin izlenmesi ve kontrol edilmesi amacıyla kullanılmaktadır. En önemli işlevlerinden birisi şirket veya herhangi bir kurum içerisinde veri akışlarını filtreleyerek transfer halindeki veya kullanımdaki verileri koruyabilmek için bulutta saklanan verileri de izlemektedir. Bu konuda detaylı bilgi için bkz. https://www.netsmart.com.tr/veri-guvenligi/?gclid=Cj0KCQjw6uT4BRD5ARIsADwJQ1-_5krKG68H2x9vEPAMC2D--BKlcT1w9XaZF6YrDjXEO5RZr8fTN_caAsAvEALw_wcB (Gözden Geçirilme Tarihi: 29.10.2020).
[398] *Taner*, s. 61.
[399] İngilizce'de "Intrusion Detection System" olarak adlandırılmaktadır.
[400] *Altınkaynak*, s. 196.

IPS denilen "İzinsiz Giriş Önleme Sistemi" ise, ağ üzerinde pozitif bir kural veya imza eşleşmesine dayalı olarak trafiği engelleme özelliğidir[401]. IDS'ten farklı olarak, IPS saldırıyı raporlamaktan ziyade sistemi korumaya yönelik bir çözümdür.

Günümüzde en bilinen IDS/IPS sistemlerinden birisi "Snort" yazılımıdır[402].

SIEM: Türkçe'ye "Güvenlik Bilgisi Ve Olay Yönetimi Sistemi" olarak tercüme edilebilecek SIEM (*Security Information and Event Management*), bilişim terminolojisinde güvenlik uyarılarını, günlüklerini ve diğer gerçek zamanlı verileri ağdaki güvenlik aygıtından toplayan ve analiz eden bir yazılım olarak bilinmektedir[403].

Güvenlik Duvarı (Firewall): Güvenlik duvarı, en basit şekliyle kullanıcının yerel ağı ile dış ağlar arasındaki iletişimin güvenliğini sağlayan yazılım ve donanımıdır[404]. Güvenlik duvarının aslında en önemli işlevi, bir cihaza veya ağ izin verilen trafiği geçiren, izin verilmeyen trafiği ise engelleyen bir ağ cihazı olmasıdır[405]. Ana bilgisayar tabanlı güvenlik ağı (örneğin Windows güvenlik duvarı) bir bilgisayarın bağlantı noktalarının filtrelenmesi ve sistem hizmetinin tek bir bilgisayar işletim sisteminde çalışırken ağ katmanı güvenlik ağının işlevi ise, kaynak ve hedef IP adreslerine göre filtreleme yapmaktır[406].

Güvenlik Politika ve Prosedürleri

Güvenlik duvarı üzerinde politikalar belirlenir ve belirlenen her bir politikaya bilişim terminolojisinde, Türkçe'de kural anlamına gelen "rule" denilmektedir. Tanımlanan politikalar çerçevesinde hangi data paketlerinin aktarılıp aktarılmayacağı, erişime yönelik engellemeler, kimlerin birbiri ile iletişime geçebileceği ve kimlerin hangi servislere erişebileceğine ilişkin kontroller yapılır[407].

---

[401] *Taner*, s. 61.
[402] *Taner*, s. 61.
[403] *Taner*, s. 61.
[404] *Altınkaynak*, s. 191.
[405] *Taner*, s. 51.
[406] *Taner*, s. 52.
[407] *Altınkaynak*, s. 191.

Katmanlı güvenlik yaklaşımda değinilmesi gereken bir diğer kavram ise derinlikte savunma stratejisidir. Bu strateji göre, kurum güvenlik kontrollerinden hiçbirisinin ağ üzerinde tamamıyla uygulanabilir olmadığı varsayımından hareketle, birbirini tamamlayan ağ güvenliği katmanlarından her birisi siber saldırının etkilerini azaltan bir ağ trafik barikatı olarak kabul edilmektedir[408]. Derinlikte savunma stratejisinde, yukarıda belirtilen katmanlar kademe kademe saldırıyı yavaşlatarak saldırganın ağ üzerinde gerçekleştirdiği saldırıdan vazgeçmesi veya etkisinin azaltılması amaçlanmıştır.

3.3.6.2. DDoS Saldırılarına Karşı Alınabilecek Önlemler

T.C. Cumhurbaşkanlığı Strateji Dijital Dönüşüm Dairesi[409] tarafından 10.07.2020 tarihinde yayınlanan Bilgi Ve İletişim Güvenliği Rehberi'ne göre, DoS/DDoS saldırılarına karşı şu tedbirlerin alınması gerektiği belirtilmiştir[410]: (i) Kurumun güvenlik sistemi ve ürünlerinde DoS/DDoS saldırılarına karşı özel konfigürasyonların yapılması, (ii) DDoS engelleme sistemlerinin sınırları ve yetkinlikleri düzenli periyotlar halinde test edilmesi, sürekli iyileştirilmesi ve güncellenmesi (iii) DDoS koruma hizmetinin bir servis sağlayıcıdan temin edilmesi halinde, servis sağlayıcıdan

[408] *Özkaya/Sarıca/Durmaz*, s. 343-344.

[409] 24.10.2019 tarihli Resmi Gazete'de yayınlanan 48 numaralı Cumhurbaşkanlığı Kararnamesi gereğince, T.C. Cumhurbaşkanlığı nezdinde Dijital Dönüşüm Ofisi kurulmuştur. Dijital Dönüşüm Ofisi'nin (48 Sayılı Kararname, m. 9 gereğince), Cumhurbaşkanı tarafından belirlenen amaç, politika ve stratejilere uygun olarak kamunun dijital dönüşümüne öncülük etmek, Dijital Türkiye (e-devlet) hizmetlerinin sunıumuna aracılık etmek, kurumlar arası işbirliğini artırmak ve bu alanlarda koordinasyonu sağlamak, kamu dijital dönüşüm yol haritasını hazırlamak, bilgi güvenliğini ve siber güvenliği artırıcı projeler geliştirmek gibi görevleri söz konusudur. Bu konuda detaylı bilgi için: https://www.resmigazete.gov.tr/eskiler/2019/10/20191024-1.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[410] T.C. Cumhurbaşkanlığı Strateji Dijital Dönüşüm Dairesi, Bilgi Ve İletişim Güvenliği Rehberi, Temmuz, 2020, (*"Rehber"*), s. 50. Ayrıca, Rehber'de ağ güvenliği konusunda alınması gereken tedbirlerle ilgili olarak s. 49-56 arasında ayrıntılı teknik analizlere yer verilmiştir. İlgili rehbere internet üzerinden şu link ile ulaşılabilir: https://cbddo.gov.tr/SharedFolderServer/Genel/File/BG_REHBER.pdf (Gözden Geçirilme Tarihi: 12.08.2020).

yukarıda belirtilen şartlara göre hizmet verildiğine dair taahhüt alınması, tedarik şartname ve sözleşmelerinde bu hususların belirtilmesi.

Yukarıda da belirtildiği üzere, ağ güvenliği noktasında her haberleşme katmanında alınabilecek farklı yöntemler bulunmakla beraber konunun elektronik ödeme sistemlerinde siber güvenlik olması sebebiyle bu açıdan DDoS saldırılarında en kritik düzeydeki katman olan "uygulama katmanına" yönelik alınabilecek teknik birtakım önlemler şu şekilde sıralanabilir[411]:

İstek Sayısı Sınırlandırması: DDoS saldırıları açısından, en etkin yöntemlerden birisi bir IP adresinden belirli bir süre zarfından gelen istek sayısını sınırlandırmaktır. Bu kısıtlama yönteminde, belirli bir adedin üzerinde gelen isteklere karşı belirli bir süre yanıt verilmeyebilir veya cevabın tamamı değil veri akışı olarak belirli bir kısmı gönderilebilir. Bu noktada, kural ihlali yapan ve belirlenen sayının üzerinde istek gönderen IP adresine düşük kaynak gerektiren (örneğin boş bir sayfa) gönderilmesi ve belirlenen süre sınırları içerisinde bu sayfanın görüntülenmesi kararlaştırılabilir. Bir diğer yöntem ise, kural ihlali yapan ve istekte bulunan IP adresine her zaman CAPTCHA (resim yazısı)[412] sorgusu yapılabilir.

Örtük Engelleme: Bu yöntemde ise, diğerine kıyasla daha hassas bir yaklaşım benimsenir. Bu açıdan, sisteme giriş yapmak isteyen ve talepte bulunan herkes DoS

[411] Harun Bingöl/Mehmet Mehdi Karakoç, "İnternet Bankacılığı ve Telekomünikasyon Alanında Siber Güvenliğe Genel Bakış", Türk Doğa Ve Fen Dergisi, C:4, N:1, 2015, (*"Bingöl/Karakoç"*), s. 33, ilgili makaleye internet üzerinden ulaşmak için: https://www.researchgate.net/profile/Mehmet_Karakoc/publication/320149627_An_overview_of_Cybersecurity_in_Internet_Banking_and_Telecommunication_Sector/links/59d0fc09a6fdcc181ad3a96c/An-overview-of-Cybersecurity-in-Internet-Banking-and-Telecommunication-Sector.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[412] "CAPTCHA", İngilizce'de "Completely Automated Public Turing test to tell Computers and Humans Apart" ibarelerinin kısaltmasıdır. (Türkçe'ye yazar tarafından "İnsan Ve Bilgisayarların Ayrışması İçin Tamamen Kamuya Açık Turing Testi" olarak tercüme edilmiştir) Esas itibariyle, Alain Turing'in "Turing testi" olarak ifade edilen makinelerin insana dair sorulara yüzde yüz doğru cevap veremeyeceği varsayımından hareketle web sitelerinin güvenliğinin sağlanmasına yönelik bir güvenlik çözümüdür. Bot saldırılarına karşı ilk aşamada, web sitesinin güvenilirliğini sağlamak açısından kullanıcıya sisteme giriş esnasında gündelik hayatta bilinen bir nesneyi seçmesi gibi testlerle kullanıcıların bot yazılımlarından farklılaşmasını sağlayan bir uygulamadır. Bkz. https://www.milliyet.com.tr/captcha-nedir-captcha-cesitleri-nelerdir--molatik-15782/ (Gözden Geçirilme Tarihi: 29.10.2020).

saldırganı olduğu varsayımından hareketle her bir talepte CAPTCHA sorgusu yapılır ve kural ihlali yapan istemciler tespit edilerek güvenlik duvarı ile engellenir.

3.3.7. Kripto Paralara Yönelik Siber Saldırılar Karşısında Alınması Gereken Önlemler

Kripto paraların ve bu sistem üzerinde işlerlik kazanan blokzincir teknolojisinin gerek ekonomik açıdan gerekse bazı teknik ve hukuki riskler noktasında henüz oturmuş bir ekosistem olmadığı gözlenmiştir. Bu açıdan konuya bakıldığında, kripto paralarla ilgili problemler kişinin yukarıda da belirtildiği gibi özel anahtara yönelik kendi parolasını unutması olabildiği gibi saldırganların çoğu kez yukarıda belirtilen oltalama faaliyetlerinden de kaynaklanabilir[413]. Bu noktada problemi doğru teşhis edebilmek açısından çalışmada, genelde kripto paralar üzerinde alım satımı yapacak kişilerin bazıları yurt içi kaynaklı ve çoğu yurt dışı kaynaklı sitelere kayıt olarak hesap açmak suretiyle işlem (bu işlemler esnasında web sitesi aracılığıyla sisteme kişisel bilgiler, T.C. kimlik kartının açıkça göründüğü kişisel fotoğraf gibi bilgiler girilmektedir) gerçekleştirildiği bilinmektedir. Dolayısıyla, kripto paralara ilişkin giriş yapılan bu web sitelerindeki güvenlik ve gizlilik mekanizmalarının önem taşıdığı ve bu web sitelerinin çoğu kez siber ataklarla istismar edilmesinin imkân dahilinde olduğu sonucuna varılmıştır[414]. Siber ataklara maruz kalabilecek bu siteler karşısında ise, çalışmada kullanıcıların oltalama faaliyetleri, zararlı yazılımlar konusunda dikkatli olmaları ve bu tarz saldırılara karşı güvenlik duvarı, antivirüs programları, çok faktörlü kimlik doğrulama gibi mekanizmaları etkin şekilde kullanmaları gerektiği değerlendirilmiştir.

Ayrıca, kripto paralar açısından siber güvenlik noktasında önem arz eden diğer bir mesele ise "elektronik cüzdan"[415] denilen kripto paraların ne şekilde muhafaza

---

[413] Kripto paralara yönelik gerçekleştirilecek siber atak türleri olan kripto madenciliği saldırıları (cryptojacking) ile kripto paralara ilişkin (i) özel anahtar hırsızlığı, (ii) %51 saldırısı, (iii) kripto paraların illegal faaliyetlerde kullanılması, (iv) mahremiyet problemi, (v) çifte harcama gibi sorunlara ilişkin çalışmanın 2.7 başlığı altında detaylı analizlere yer verilmiştir.

[414] *Sağıroğlu*, s. 299.

[415] Doktrinde Zengin/Güngördü tarafından elektronik cüzdan, kredi kartı veya elektronik para gibi dijital ortamda ödeme yapılmasını sağlayan elektronik ödeme sistemlerinde kullanıcının kimlik ve adres

edildiğidir. Kripto paraları saklamanın en iyi yolunun günümüz teknolojisinin şu an için verdiği en iyi imkân olan "cold wallet" veya "cold storage" denilen internet ile herhangi bir bağlantısı olmayan ve kripto paraları depolamayı sağlayan "donanım cihazları" olduğu üzerinde durulmuştur[416]. Bu donanım cihazlarının kripto paraları siber güvenlik noktasında etkin şekilde saklayabilme işlevi internete bağlı olmamaları halinde mümkündür. "Hot wallet" denilen kripto paraların internete bağlı özel anahtarlar ile kullanılması uygulamasından farklı olarak "cold storage" uygulamasında, kullanıcılara blokzincir platformunda işlem yapmalarına olanak sağlayan özel anahtarların flash bellek, CD, donanımsal herhangi bir cihaz veya internete bağlı olmayan bir bilgisayar ile saklanan özel anahtarın dijital ortamda imza attığı esnada internetten ortamından kaynaklabilecek siber risklerden uzak tutulması amaçlanmaktadır. Kripto paraları saklamak ve siber güvenliğin temin edilmesi açısından donanım cihazları etkin bir yöntem olmakla beraber yine de buna sahip olmanın tek başına bir çözüm olarak görülmemesi ve bu konuda ek bazı önlemlerin de alınması gereklidir[417].

3.3.8. APT Saldırılarına Karşı Alınması Gereken Önlemler

APT, saldırıları genel itibariyle çalışan süreçleri, dosyaları ve sistem bilgilerini işletim sisteminden gizleyerek varlığını gizlice sürdüren bir program veya programlar grubu olan rootkitlerin etkin olduğu ve bu sayede yetkilendirmenin artırılması ile ağdaki diğer bilgisayarların bilgilerinin ele geçirildiği bir yöntem olarak kabul edilmektedir[418]. Yukarıda APT saldırı vektörünün derin bir teknik bilgiyi gerektirmesi nedeniyle

bilgilerini saklayan ve e-ticaret işlemleri esnasında bu bilgileri otomatik olarak sağlayan yazılım olarak tanımlanmıştır. Bu konuda detaylı bilgi için bkz. *Zengin/Güngördü*, a.g.e., s. 137'de belirtilen Gökçen.

[416] https://www.investopedia.com/terms/c/cold-storage.asp (Gözden Geçirilme Tarihi: 29.10.2020).

[417] *Sağıroğlu*, s. 298.

[418] Şeref Sağıroğlu/Mustafa Şenol, "Siber Güvenlik Ve Savunma, Problemler Ve Çözümler", BGD Siber Güvenlik ve Savunma Kitap Serisi 2, (*"Sağıroğlu/Şenol"*), s. 428, ilgili esere internet üzerinden ulaşmak için bkz. https://www.sasad.org.tr/uploaded/BGD-Siber-Guvenlik-ve-Savunma-Kitap-Serisi-2-Problemler-ve-Cozumler.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

nitelikli bir saldırı türü olduğu açıklanmıştı. Bu başlık altında ise APT saldırılarını önleme açısından etkin yöntemlerin neler olabileceği sorusuna cevap aranacaktır.

Doktrinde, Sağıroğlu/Şenol APT saldırılarına karşı temelde kullanıcıların kontrol edilerek farkındalığın artırılması gerektiğini, kullanıcılara oy verme yöntemi uygulanarak oylama mekanizmasının sağlayacağı güven değeri ile bir IP adresinin kötü amaçlı DNS ve trafik vektörlerinden etkilenip etkilenmediğinin belirlenebileceğini, iyi bir savunma yapabilmek için değişen saldırıları iyice anlamak ve nasıl yürütüldüğünü bilmenin gerektiğini, saldırganlar tarafından hedeflenen son noktayı kontrol altına almak veya geçici olarak kilitlemenin uzun süreli bir koruma sağlayacağını, mevcut ağ sisteminin tüm trafiğinin izlenmesinin APT saldırılarına karşı etkin bir yöntem olduğunu belirtmiştir[419]. Özkaya/Sarıca/Durmaz ise APT saldırılarına karşı izlenebilecek en iyi yöntemin "Tehdit Yaşam Döngüsü Yönetimi (*TYDY*)" olduğuna dikkat çekmiştir. TYDY, aşağıda da açıklandığı üzere normalde toplamda altı aşamadan meydana gelmekte olup APT saldırılarının uygun araç ve yöntemlerle herhangi bir zarar vermeden toplam altı aşamada önlenmesi hedeflenmiştir:

Adli Amaçlı Veri Toplama: Bu aşama açısından önemli olan olgu, tamamen olgunlaşmış bir tehdidin tespitinden önce organizasyonun IT ekibi ve siber güvenlik uzmanları tarafından güvenlik olayları ve bazı riskli durumlara karşı veri toplanmasıdır. Veri toplamak açısından yararlanılabilecek bu araçlardan bazıları, yukarıda belirtildiği üzere kimi zaman uyarı vermek için bir sensör olabileceği gibi organizasyonun log kayıtları ve makine verilerinin düzenli olarak muhafaza edilmesidir.

Keşif: Organizasyon içerisinde ağ görünürlüğünü elde edip saldırıları erken şekilde tespit ettikten sonra APT saldırılarını etkisiz kılmak açısından bir sonraki aşama keşiftir. Keşifte arama analizi ve makine analizi gibi iki yöntem söz konusudur. Arama analizinde, özetle IT personeli veya var ise kurumun siber güvenlik uzmanı öncelikle

[419] *Sağıroğlu/Şenol*, 428-430.

raporları gözden geçirir, ağ ve antivirüs yazılımlardan bilinen veya raporlanan zafiyetleri tespit eder. Bu hareket tarzı büyük bir zaman ve emek gerektirebileceğinden organizasyonunu güveneceği tek bir analiz kaynağının olmaması tavsiye edilir. Diğer bir yöntem ise, makine analizinde tamamen yapay zeka tabanlı sistemler aracılığıyla büyük hacimli veriler taranarak bu verilerden hareketle keşif aşaması için özet ve anlaşılır sonuçlar elde edilir.

Tanımlama: Tehditlerin ve siber risklerin keşfedilmesinden sonra bunların potansiyel etkileri, öncelik sıralaması, çözüm aciliyetleri ve mevcut risklerin nasıl bertaraf edileceğinin tespiti tanımlama denilen aşamada gerçekleştirilir. Tanımlama aşamasında, zaman kritik bir faktör olabileceği gibi daha önemlisi aynen bir hastalığın tedavisinde olduğu gibi doğru bir teşhis (özellikle *false positiveness* denilen yanlış alamların dikkate alınmaması ve *true positiveness* denilen doğru alarmların dikkate alınması) APT saldırılarının bertaraf edilmesinde belirleyici niteliktedir.

Araştırma

Doğru alarmların tanımlanması akabinde kök neden analizi (*root reason analysis*) yapılarak tanımlanan tehditlerin bir siber güvenlik vakası oluşturup oluşturmayacağını tespit etmek teknik açıdan detaylı bir araştırmayı gerektirir. Adli bilişim (*forensic*) bilgisi ve yetkinliği olan IT personeli tarafından risk teşkil edebilecek vakalar hakkında derin bir araştırma gerçekleştirilerek mevcut durumun sebebiyet verebileceği potansiyel zarara bakılır ve toplanan bilgilere göre siber güvenlik ekibine karşı koyması açısından gerekli bilgi altyapısı aktarılmış olur.

Etkisizleştirme

APT saldırıları çoğu kez kaynağını tek bir siber saldırıdan almayan ve nitelikli saldırılar olarak birden fazla saldırının bir birleşimi şeklinde yansıdığından, daha önce etkisizleştirme olarak belirlenen eylem planı saldırının türüne göre vakit kaybetmeden gerçekleştirilir. Bu aşamada, siber atağa karşı koyulmasının iş birliği içerisinde ve

mümkün mertebe otomatik şekilde gerçekleştirilmesi saldırının etkisizleştirilmesinde elde edilecek başarı açısından önemlidir.

Toparlanma

Toparlanma, ancak karşılaşılan riskin etkisizleştirildiği ve neden olabileceği riskin kontrol altına alındığı emin olunduktan sonra geçilebilecek bir aşamadır. Tanımlama ve etkisizleştirme gibi zaman faktörünün kritik olmayabileceği toparlanma aşamasında zaman zaman dikkatli olunması gerekebilir. Bunun nedeni, saldırı ve tepki esnasında yapılan değişikliklerin hata olmaksızın eski hale getirilmemesi halinde ve özellikle saldırganlar açısından arka kapı (*back door*) bırakılmadığı emin olunmadığı takdirde APT saldırısı maruz kalan kurum açısından deyim yerindeyse adeta bir kabusa dönüşebilir.

3.3.9. İnternet Bankacılığı ve Mobil Bankacılığı Yönelik Siber Saldırılara Karşı Alınması Gereken Önlemler

Aşağıda internet bankacılığının siber güvenliğin temini noktasında güvenilir şekilde kullanılabilmesi için dikkat edilmesi gereken hususlar şu şekilde özetlenebilir:

İnternet kafeler gibi birden çok bilgisayarın kullanıldığı ortak kullanım alanları internet bankacılığı açısından risklidir. Bu gibi yerlerde parola kırma saldırıları, ortadaki adam saldırıları gibi değişik yöntemlerle siber saldırı gerçekleştirilebileceğinden bu ortamlarda internet bankacılığı işlemlerinin gerçekleştirilmemesi daha uygundur.

İnternet bankacılığının kullanıldığı cihazlarda antivirüs programları kullanılarak her aşamada bu programlarda gerekli güncellemeler gerçekleştirilmelidir.

Yukarıda belirtilen keylogger yazılımlarına karşı antilogger yazılımlar yüklenerek tedbir alınmalıdır.

Crackli yazılımlara[420] zararlı yazılım bulaşma riski bulunduğundan lisanslı işletim sistemleri ve programları tercih edilmelidir.

İnternet bankacılığında çok faktörlü kimlik doğrulama açısından mobil cihazdan SMS doğrulaması talep edileceğinden mobil cihazın güvenliği de önem taşımaktadır. Kullanılan mobil cihazlara yüklenen yazılımlara dikkat edilmeli ve mobil cihazlarda da antivirüs programları kullanılmalıdır.

Çevrimiçi bankacılık hesabı için dinamik IP yerine statik IP[421] adresinin tanımlanarak tek bir IP üzerinden erişime izin verilmelisi siber güvenliğin temini açısından daha uygun bir yol olacaktır.

İnternet bankacılığı işlemlerinde VPN kullanılması güvenilir bir yöntemdir.

Man in the Browser[422] (*Aradaki Tarayıcı*) saldırılarına karşı internet tarayıcıları güncel tutulmalıdır ve kaynağı belirsiz eklentiler yüklenmemelidir.

---

[420] Crackli yazılımlar, açık kaynaklı yazılım platformlarından elde edilen lisansız yazılımları ifade etmektedir. Crackli yazılım kullanmanın sebepleri olarak (i) zararlı yazılım bulaşma riski, (ii) crackli yazılımın genelde kaynağı belli olmayan web sitelerinden bilgisayar ve diğer cihazlara indirildiğinden indirilen cihaza zararlı yazılım bulaşma riskli, (ii) crackli yazılımın umulduğu şekilde çalışmama olasılığı, (iii) crack'li yazılımların lisanslı bir ürün olmaması sebebiyle potansiyel hukuki süreçlere sebebiyet vermesi, (iv) crack'li yazılım sonucunda ilgili cihaza zararlı yazılım yüklenmesi halinde bu zararlı yazılımın ağdaki diğer cihazlara da bulaşma ihtimali belirtilebilir. Bu konuda detaylı bilgi için bkz. Chip Dergisi, "Crack'li Yazılım İndirmemek İçin Beş Neden" başlıklı yazısı, ilgili yazıya internetten ulaşmak için: https://www.chip.com.tr/haber/crack-yazilim-indirmemek-icin-5-neden_86560.html (Gözden Geçirilme Tarihi: 29.10.2020)

[421] Statik IP, adından da anlaşılacağı üzere, değişken olmayan, durağan IP sistemini tanımlamak için kullanılmaktadır. Statik IP adreslerinin değişmediği ve atandığı cihaz veya sunucu için sabit kaldığı kabul edilmektedir. Statik IP adreslerinin değişmemesi sebebiyle özellikle DNS kayıtlarının değişmemesinin DNS güvenliğini üst düzeyde sağlama açısından avantajlı olduğu bilinmektedir. Bu konuda detaylı bilgi için bkz. https://berqnet.com/blog/siber-guvenlik-nedir (Gözden Geçirilme Tarihi: 29.10.2020).

[422] İngilizce'de Man-in-the-Browser (*"MitB"*) saldırıları denilen ve Türkçe'ye "Aradaki Tarayıcı" olarak tercüme edilecek bu saldırı tekniği "aradaki adam saldırıları"nın (*"Man-in-the-Middle"* veya *"MitM"*) bir türü olarak kabul edilmektedir. Teknik açıdan, bu yöntemi kullanan saldırganlar kurbanlarının internet tarayıcılarını öncelikle kurbanlarının tarayıcılarına enjekte ettikleri truva atları vasıtasıyla tarayıcı içindeki bilgileri ele geçirmektedir. Bu saldırıların en bariz özelliklerinden birisi, anti-virüs yazılımlar tarafından fark edilmeksizin kullanıcı bilgilerini çalma kabiliyeti olduğundan oldukça tehlikeli bir saldırı vektörü olduğu kabul edilmektedir. Bankacılık sektörü açısından ise, MitB saldırılarında saldırganların kullanıcıların kimlik bilgilerini çalma kabiliyeti olduğundan, kolaylıkla bankaların kullandıkları iki-faktörlü kimlik doğrulama mekanizmalarını da kolayla aşarak bankaların kullandıkları ağ seviyesinde çalışan IDS ve IPS sistemleri gibi anti-fraud teknolojileri de kolaylıkla

Sosyal mühendislik saldırılarına karşı internet bankacılığı parolaları banka çalışanları da dahil olmak üzere kimse ile paylaşılmamalıdır[423].

İkinci bölümde de detaylı şekilde açıklandığı üzere, internet bankacılığında olduğu gibi özellikle mobil cihazlarla gerçekleştirilen mobil bankacılık işlemlerinde de zararlı yazılımlara karşı mobil cihazların güvenliği önemlidir. Yukarıda yer verilen örneklerden de anlaşılacağı üzere, özellikle bazı zararlı yazılımların bilgisayar dışında mobil cihazlara da bulaşarak bankaların çoğunlukla kullandıkları çift güvenlik katmanını kolayca atlatabildiği bir ortamda kullanıcıların en büyük yanılgısı cep telefonlarının güvenliğini göz ardı edilmesidir. Oysaki herhangi bir zararlı yazılımın cep telefonuna bulaşması ile bilgisayara bulaşması noktasında teknolojik açıdan farklılık bulunmadığından cep telefonlarında da virüs önleyici yazılımların kullanılması ve kullanıcıların cep telefonlarında olası oltalama faaliyetlerine karşı farkındalıklarının yüksek bir seviyede olması mobil bankacılık işlemlerinde de siber güvenliğin sağlanmasında önemi haiz meselelerden birisidir.

DÖRDÜNCÜ BÖLÜM

KARŞILAŞTIRMALI HUKUK AÇISINDAN ELEKTRONİK ÖDEME SİSTEMLERİNDE SİBER GÜVENLİK MESELESİNİN DEĞERLENDİRİLMESİ

Çalışmanın bu bölümünde özellikle elektronik ödeme sistemlerinde siber güvenliğe ilişkin farklı ülkelerin bu konuda dikkat çeken düzenlemeleri karşılaştırmalı hukuk ekseninde incelenmiştir.

---

devre dışı bırakabildikleri kabul edilmektedir. Man-in-the-Browser saldırıları konusunda detaylı bilgi için bkz. https://www.slideshare.net/bgasecurity/man-inthebrowser-saldrlarnn-analizi (Gözden Geçirilme Tarihi: 29.10.2020).

[423] *Bingöl/Karakoç,* s. 31.

Ülkeler bazında elektronik ödemelerde dijital ekonominin aktörlerine bakıldığında, dijital ekonomideki katma değerin %70'inin Amerikan, %25'inin Çinli ve sadece %5'inin diğer coğrafyalarda (%4 Avrupa ülkeleri ve %1 diğer) merkezleri bulunan şirketler tarafından yaratıldığı görülmektedir[424]. Siber güvenlik alanında farklı devletlerin konu ile ilgili regülasyonlarına bakıldığında ise, dünya genelinde yasa koyucular kişisel verilerin koruması ve veri güvenliğine yönelik çevrimiçi tehditlere karşı farklı stratejiler ve amaçlar çerçevesinde hareket etmektedir[425].

Bu bölümde, öncelikle ilk alt başlık altında, bu çalışmayı ilgilendiren bir üst başlık olarak bilgi güvenliği konusunda içerik itibariyle sadece teknik açıdan değil, aynı zamanda hukuksal açıdan da önemli kurallar ve standartlar öngören ve bu nedenle hukukçular tarafından da irdelenmesi gereken ISO Standartları'na yer verilmiştir. İlerleyen kısımda ise, elektonik ödeme sistemlerinde siber güvenliği ilgilendirdiği düşünülen Avrupa Birliği (*"AB"*) regülasyonları incelenmiştir. Başta, AB Siber Suç Sözleşmesi olmak üzere, özellikle Avrupa Birliği'nde siber güvenlik alanındaki regülasyonlar açısından başta 910/2014 Sayılı eIDAS Tüzüğü ve 2019/881 Sayılı Tüzük dikkate alındığında, yakın zamanda AB'de bu alanda birçok yeni gelişmenin yaşandığı ve bu gelişmelerin Türkiye'de siber güvenlik alanındaki mevzuat çalışmalarına katma değer sağlayabileceği değerlendirilerek bu kapsamdaki AB mevzuatına aşağıda detaylı şekilde yer verilmiştir. Öte yandan, ABD'nin yazılım endüstrisinde devrim niteliğindeki birçok gelişmenin yaşandığı ülke olması ve bu gelişmelere paralel şekilde siber güvenlik alanında öncü bir ülke olduğu dikkate

[424] Yusuf Gökhan Penezoğlu, "Dijital Ekonomilerin Vergilendirilmesi", Ekonomist, Mayıs 2020 (*"Penezoğlu"*): https://www.ekonomist.com.tr/genel/telefona-indirdigimiz-uygulamalarin-vergisi-var-mi.html (Gözden Geçirilme Tarihi: 29.10.2020).

[425] Örneğin, ABD'de spesifik olarak halka açık şirketlerin yatırımcılara mevcut tüm sistem açıkları ve riskleri ifşa etme zorunluluğu düzenlenmişken, Çin Hukuku gereğince verilerin Çin'de yerel olarak saklanması gerekliliği ve AB açısından ise 2019/881 Sayılı Tüzük uyarınca ağ donanım üreticileri için sertifikasyon oluşturulmasına ilişkin bir regülasyonun yakın zamanda yürürlüğe girmesi gibi örnekler devletlerin siber güvenlik konusundaki farklı yaklaşım sergilediklerini ortaya koymaktadır. Bu konuda detaylı bilgi için bkz. Lothar Determann, "Kişisel Verilerin Uygulama Klavuzu", Oniki Levha Yayınları, 1. Baskı, İstanbul, 2020, (*"Determann"*), s. XXI, XXII.

alınarak[426] elektronik sistemlerinde siber güvenlik noktasında ABD'de dikkat çeken yasal düzenlemeler de irdelenmiştir[427]. Ayrıca, aşağıda da belirtildiği üzere, ABD'de özellikle elektronik ödemelerde siber güvenlik alanında yasal düzenlemeler açısından konsolide bir regülasyon bulunmamasına, sektörel ve özellikle federal/eyalet yasaları açısından bu alanda parçalı bir yapının söz konusu olmasına rağmen, AB'nin Siber Suç Sözleşmesi'ni imzalayarak kendi iç hukuk sisteminde yürürlüğe sokması dikkat çekicidir. Son kısımda ise, elektronik ödemelerde özellikle son zamanlarda yeni gelişmelerin yaşandığı ve bu alanda aktif bir oyuncu olan Çin açısından elektronik ödeme endüstrisinde yaşanan yeni gelişmelerin neler olduğuna ışık tutularak Çin'in bu konuda dikkat çeken yasal düzenlemeleri siber güvenlik perspektifi ile ele alınmıştır. Yazar tarafından, Türkiye'de özellikle son zamanlarda "veri lokalizasyonu"[428] açısından yoğun tartışmaların yaşanması ve bu konuda aşağıda da irdeleneceği üzere başta 5651 Sayılı Kanun açısından yasa koyucunun öngördüğü değişiklikler noktasında Çin'deki düzenlemelerin doğru anlaşılması gerektiği ve Türkiye'nin Çin örneğini dikkate alarak, sahip olduğu veriler konusundaki stratejisini bu bariz örnekten yola çıkarak doğru konumlandırması gerektiği değerlendirilmiştir.

[426] Doktrinde ABD'nin, teknolojik ilerlemelerin en hızlı olduğu ve buna bağlı olarak teknolojik yöndeki düzenlemelerin de paralel şekilde en hızlı şekilde yürürlüğe girdiği bir ülke olduğu ve bunun bir doğal sonucunun ise siber güvenlik alanında hem öğretideki tartışmalar hem de yasal düzenlemeler ve uygulama örnekleri bakımından öncü bir ülke konumunda olduğuna dikkat çekilmiştir. Bkz. *Çakır/Kılıç*, s. 194'de belirtilen eser olarak Karagülmez, 2011:91, bu konuda ayrıca bkz. *Erdem/Özocak1*, s. 196.

[427] ABD'de siber güvenlik konusundaki regülasyonlara bakıldığında, federal düzeyde uygulanan genel düzenlemelerin yanı sıra eyaletler bazında sektör-spefisik (başta finans, sağlık ve sigorta olmak üzere) düzenlemelerin yer aldığı, dolayısıyla siber güvenlik alanında AB'de olduğu gibi bütünsel ve tüm Birlik açısından geçerli olan kurallar yerine daha ziyade farklı sektörlere yönelik düzenlemeler ile eyaletler açısından parçalı bir yapının yer aldığını belirtmek uygun olacaktır.

[428] Doktrinde Kaya'ya göre, verinin ülke içerisinde barındırılmasını sağlamak, başka bir ifade ile veri lokalizasyonu temin etmek konusunda Türkiye'de muhtelif bazı düzenlemeler yürürlüğe girmiştir. Kaya, bu yaklaşımın, bir devlet politikası ve özünde bireylerin daha pratik şekilde verilerine ulaşmalarının sağlanması nedeniyle makul sonuçları da dikkate alınarak tamamen dışlanmasının mümkün olmadığını belirtmiştir. Ancak, Kaya tarafından özellikle bu konuda tutarlı bir politika geliştirilmesinin ve bu amaçla geliştirilen kuralların da tutarlı şekilde uygulanması gerektiğine dikkat çekilmiştir. Bu konuda detaylı bilgi için bkz. Mehmet Bedii Kaya, Elektronik Ticaret Hukuku Ticari Elektronik İletiler, On İki Levha Yayıncılık, 2. Baskı, İstanbul, 2020, (*"Kaya, Elektronik Ticaret"*), s. 154, 155.

4.1. ISO STANDARTLARI

ISO 27000 ailesinden olan ve ISO/IEC 17799'un yerine geçen ISO/IEC 27001 Standardı[429], bilgi güvenliği standardı olarak bilgi güvenliği yönetiminin daha verimli hale getirilmesi için tasarlanmıştır[430]. ISO/IEC 27001, bir organizasyon içerisinde belgelenmiş bir Bilgi Güvenliği Yönetim Sistemi (*"BGYS"*)[431] kurmak, uygulamak, işletmek, incelemek, sürdürmek ve iyileştirmek için bir model oluşturmak amacıyla ISO tarafından 14.10.2005 tarihinde yayınlanmıştır[432].

BGYS, bilgi sistemlerine yönelik risklerin mümkünse ortadan kaldırılmasını, bu mümkün değil ise de etkisini minimize etmeyi amaçlayarak sürekli geri beslenme ve iyileştirme metodu olarak da bilinen Deming Döngüsünü (aşağıda Şekil 4.1[433]'de görseline yer verilmiştir), başka bir ifade ile aşağıda görseline yer verilen Planla[434] -

[429] Orijinal adı "Information Technology – Security Techniques – Information Security Management Systems-Requirements" olan bu standart, Türk Standartları Enstitüsü tarafından Türkçe'ye "Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler" olarak tercüme edilmiştir.

[430] *Yılmaz*, s. 50, Ayrıca ISO/IEC 27001 ile ilgili kapsamlı bilgi bilgiye erişmek için şu makaleler dikkate alınabilir: Volkan Evrin/Mehmet Demirer, "Kurumsal Bilgi Güvenliği Süreç Çalışmaları: ISOIEC-27001 Örneği (*"Evrin/Demirer"*): http://www.emo.org.tr/ekler/135c9b87ad18ef4_ek.pdf, Mehtap Çetinkaya Kılıç, Orhan Gökçöl, "Türkiye'deki İşletmelerin Bilgi Güvenliği Yönetim Sistemi Altyapısının Değerlendirilmesi" (*"Kılıç/Gökçol"*): http://www.emo.org.tr/ekler/e07b4f2c678f096_ek.pdf (Gözden Geçirilme Tarihi: 29.10.2020)

[431] Doktrinde Çubukçu tarafından Bilgi Güvenliği Yönetimi Sistemi'nin (BGYS), ISO/IEC 27001:2013 standardı içerisinde, bilgi güvenliğini sağlamak üzere kurumların hassas bilgilerini yönetebilmek amacıyla benimsenen sistematik bir yaklaşım olarak tanımlandığı belirtilmiştir. Bkz. Faruk Çubukçu, "Bilgi Güvenliği Yönetim Sistemi ISO 27001 – Uygulama Kılavuzu", Pusula, İstanbul, 2018, (*"Çubukçu"*), s. 92.

[432] ISO 27001'in tarihçesi konusunda Bkz. *Özkaya/Sarıca/Durmaz*, s. 276 ve ayrıca https://en.wikipedia.org/wiki/ISO/IEC_27001#History_of_ISO/IEC_27001 adresinden gerekli bilgi temin edilebilir.

[433] Şekil-4.1 için bkz. https://www.umutalkan.com/wp-content/uploads/2020/02/puko2.png (Gözden Geçirilme Tarihi: 29.10.2020).

[434] Planlama, uygulama safhasına geçilmeden önce neyin, nasıl yapılacağının belirlenerek BGYS politikasının, amaçlarının, hedeflerinin, süreçlerinin ve prosedürlerinin oluşturulduğu aşamadır. Bkz. *Özkaya/Sarıca/Durmaz*, s. 278.

Uygula[435] - Kontrol Et[436] – Önlem Al[437] Döngüsünü (*"PUKÖ Döngüsü"*) [438] temel almaktadır.

Şekil-4.1: PUKÖ Döngüsü

PUKÖ döngüsü, yukarıda süreçlerden de anlaşılacağı üzere bilgi güvenliği konusunda yapılacak tüm işlemler ve süreçler hakkında önceden karar verilmesi, alınan bu kararların uygulanması, bu doğrultuda süreç ile ne kadar ilerleme kaydedildiğinin sürekli olarak kontrol edilmesi ve hedefe uymayan sapmalar konusunda kök nedeninin araştırılarak iyileşmeye gidilmesini hedefleyen döngüsel bir süreç olarak karşımıza çıkmaktadır[439]. Bu bağlamda, kurumlar bünyesinde BGYS'nin kurulması ile yukarıda

[435] Uygulama, planlanan faaliyetlerinin kararlaştırılan kişi, yöntem ve zamanlarda gerçekleştirildiği aşamayı ifade etmektedir (Bkz. *Çubukçu*, s. 97).
[436] Kontrol, uygulama aşamasından sonra geriye bakılarak planlanan hedeflere ne kadar ulaşıldığı, hedeften sapmaların tespit edilip ilgili kişi ve birimlere rapor edildiği aşamadır (Bkz. *Çubukçu*, 100).
[437] Önlem alma, BGYS kapsamında en başta planlanan faaliyetler ile gerçekleşen sonuç arasında ortaya çıkan farklılıklar ve sapmaların kök nedenlerinin araştırıldığı ve bunlara ilişkin ne gibi önlemlerin alınabileceğinin belirlendiği aşama olarak bilinmektedir (Bkz. *Çubukçu*, 101).
[438] W. Edwards Deming tarafından ortaya konan PUKÖ (Orijinal adı ile Plan-Do-Check-Act/PDCA) döngüsünde faaliyetlerin başta planlama ile başladığı ve planlamada amaç ve hedeflerin belirlendiği, uygulama sürecinde prosedürlerin yerine getirildiği, ardından gerekli kontrollerin yapıldığı ve önlem alma aşamasında süreçlerin iyileştirilmesinin sağlandığı sürekli iyileştirmeyi amaçlayan bir dizi işlemi ifade ettiği belirtilmiştir. Bu konuda ayrıntılı bilgi için Bkz. *Çubukçu*, s. 94 ve ayrıca Ronal Moen, "Foundation and History of PDCA Cycle" (*"Moen"*), https://deming.org/uploads/paper/PDSA_History_Ron_Moen.pdf (Gözden Geçirilme Tarihi: 29.10.2020).
[439] *Özkaya/Sarıca/Durmaz*, s. 278.

belirtilen süreçlerin hayata geçirilmesi sağlanmış olup kurum içerisinde birçok departman istihdam edilen kişilerden oluşan BGYS komitesi tarafından bu kapsamda öngörülen süreçlerin gerçekleştirilmesi beklenmektedir[440].

Son olarak, çalışmayı ilgilendirmesi sebebiyle özellikle ISO 12812 Standardından kısaca bahsetmek gerekirse, bu standart mobil finansal hizmetlere yönelik bir standart olup mobil cihazlarla gerçekleştirilen ödemelerde asgari güvenlik önlemleri ile şifreleme protokolleri ve mobil cihazlara bilgi güvenliğinin tesisi açısından yol gösterici nitelikte kurallar içermektedir[441].

4.2. ELEKTRONİK ÖDEME SİSTEMLERİNDE SİBER GÜVENLİKLE İLGİLİ AVRUPA BİRLİĞİ'NDEKİ YASAL DÜZENLEMELER

4.2.1. Avrupa Birliği Siber Güvenlik Tarihçesi

AB'nin siber güvenlik tarihçesine kısaca değinmek gerekirse, AB'nin ortak siber güvenlik politikası[442] için oluşturduğu Strateji Belgesi'nden[443] önce, siber güvenliğin

---

[440] *Çubukçu*, s. 93.

[441] Bu konuda ayrıntılı bilgi için bkz. https://www.iso.org/search.html?q=ISO%2012812 (Gözden Geçirilme Tarihi: 29.10.2020). Ayrıca, bu standart beş bölümden oluşmakta olup (i) ISO 12812-1:2017'de Genel Çerçeve (General Framework), (ii) ISO/TS 12812-2:2017'de Mobil Finansal Hizmetlerde Güvenlik Ve Veri Koruması (Security and Data Protection for Mobile Financial Services), (iii) ISO/TS 12812-3:2017'de Finansal Uygulamalar Yaşam Döngüsü Yönetimi (Financial Application Lifecycle Management, (iv) ISO/TS 12812-4:2017'de Kişilere Yönelik Mobil Ödemeler (Mobile Payments to Persons) ve (v) ISO/TS 12812-5:2017'de ise Şirketlere Yönelik Mobil Ödemeler (Mobile Payments to Business) düzenlenmiştir (Serbest Çeviri).

[442] Avrupa Birliği siber güvenlik politikası konusunda detaylı bilgi için Bkz. Annegret Bendiek, "European Cyber Security Policy", SWP Research Paper, (*"Bendiek"*), s. 19 vd., ilgili makaleye internet üzerinden ulaşmak için bkz. file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/EuropeanCyberSecurityPolicy.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[443] AB Strateji Belgesi'nde, internetin ve daha geniş anlamda siber uzayın toplumun tüm kesimlerinde muazzam bir etkiye sahip olduğu, temel haklarımızın, sosyal etkileşimlerimizin ve ekonomik bağımlılığımızın bilgi ve iletişim teknolojilerine olan bağlılığı vurgulanarak dijital dünyanın sağladığı inanılmaz faydaların yanı sıra, aynı zamanda savunmasız bir alan olduğu ve siber güvenlik olaylarının özellikle bağlı olunan su, bakım, elektrik, mobil servisler gibi kritik altyapıları tehdit ettiğine ve bu tehditlerin suç içeren, siyasi amaçlı, terörist veya devlet destekli tehditler olmak üzere farklı kaynaklara sahip olabileceğine dikkat çekilmiştir. Strateji Belgesi'nde ayrıca AB'de ilk kez siber güvenlik politikasının da temelleri çizilerek siber güvenlik ilkeleri olarak AB'nin temel değerleri, temel hakların, düşünce özgürlüğünün, kişisel bilgilerin ve gizliliğin korunması, herkes için erişim, demokratik ve etkili

sağlanması hususunda özellikle kritik altyapıların korunmasına temel itibariyle öncelik verilmesi gerektiği belirtilerek kritik altyapıların belirlenmesinde[444] kapsamın, büyüklüğün ve zamanın önemine vurgu yapmıştır.[445] 24.11.2005 tarihinde, Avrupa Komisyonu tarafından yayınlanan Avrupa Kritik Altyapıların Korunması Programı (*"EPCIP"*[446]) hakkındaki Bildiri Metni'nde (Green Paper)[447], kritik altyapıların korunması amacıyla alınacak önlemler, hazırlıklar ve sorumluluklar genel olarak belirlenerek bu çerçevede yerellik, tamamlayıcılık, gizlilik, paydaş işbirliği ve ölçülülüğün EPCIP'ın temel değerleri olduğu belirtilmiştir[448]. Söz konusu Bildiri Metni'nde, ayrıca Avrupa Birliği açısından Kritik Altyapı Uyarı Bilgi Ağı (*"CIWIN"*[449]) hakkında da bilgi verilmiştir. Tüm bu gelişmeler doğrultusunda ise, AB tarafından yürütülen kurumsallaşma çalışmalarının bir sonucu olarak 05.06.2003

çok paydaşlı yönetişim ve güvenliği sağlamak için paylaşılmış sorumluluk olmak üzere beş ilke özellikle vurgulanmıştır. Bu konuda detaylı bilgi için bkz. *Eren*, s. 80-84.

[444] Doktrinde Eren tarafından kritik bilgi altyapısı, kesilmesi veya tahrip olması durumunda vatandaşların sağlığı, güvenliği ve ekonomik refahı veya hükümetin ve ekonominin işleyişi üzerinde önemli etki doğuracak birbiriyle bağlantılı bilgi sistemleri ve ağları olarak tanımlanmış olup kritik altyapılar olarak enerji üretim ve dağıtım sistemleri, telekomünikasyon altyapısı, finansal servisler, su ve kanalizasyon sistemleri, güvenlik servisleri, sağlık servisleri ve ulaştırma servislerinin en başta gelen kritik altyapılar olduğu belirtilmiştir. Bkz. *Eren*, s. 70-71.

[445] *Eren*, s. 71.

[446] Orijinal adı "European Programme for Infrastructure Protection" olup Türkçe'ye Avrupa Kritik Altyapıların Korunması Programı şeklinde tercüme edilmiştir (Serbest Çeviri). Bu konuda ayrıntılı bilgi için Bkz. https://en.wikipedia.org/wiki/European_Programme_for_Critical_Infrastructure_Protection (Gözden Geçirilme Tarihi: 29.10.2020).

[447] Söz konusu orijinal metne ulaşmak için Bkz. https://www.ab.gov.tr/files/ardb/evt/1_avrupa_birligi/1_6_raporlar/1_2_green_papers/com2005_green_paper_on_critical_infrastructure.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[448] *Eren*, s. 72.

[449] Orijinal adı "Critical Infrastructure Warning Information Network" isimli kuruluşun baş harflerinden oluşan *"CIWIN"* Türkçe'ye Kritik Altyapı Uyarı Bilgi Ağı şeklinde tercüme edilebilir. Bu kuruluş, Avrupa Komisyonu tarafından kritik altyapılara ve güvenlik açıklarına ilişkin verilerin, üye devletler ile kolay akışının sağlanması amacıyla oluşturulan bir kuruluştur. Üye devletlere, AB kurumlarına, kritik altyapı sahiplerine ve işletmecilere ait ortak tehditler, güvenlik açıkları, güvenlik ihlallerine karşı alınması gereken tedbirler ve izlenecek stratejiler hakkında destek vermek suretiyle risklerin azaltılmasını ve yardımı amaçlamaktadır. Bkz. *Eren*, s. 73. Ayrıca bu konuda detaylı bilgi için Bkz. https://ec.europa.eu/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network_en (Gözden Geçirilme Tarihi: 29.10.2020).

tarihinde Avrupa Birliği Ağ Ve Bilgi Güvenliği Teşkilatı (*"ENISA"*[450])'nın kurulması kararlaştırılmış ve ENISA ile AB'nin siber güvenliğinin sağlanması konusunda koordinasyonu sağlamak ve Avrupa genelinde üst düzeyde ağ ve bilgi güvenliğinin sağlanması amaçlanmıştır[451].

Tez içeriğinde kapsam itibariyle, elektronik ödeme sistemlerinde siber güvenlik incelendiğinden bu konuda Avrupa Birliği'nin aşağıda dikkat çeken düzenlemeleri incelenmiştir.

4.4.2. Avrupa Birliği'nin 2015/2366 Sayılı Direktifi ("PSD2")

AB'deki elektronik ödeme sistemlerinin hukuki çerçevesi, temel itibariyle 2007/64/EC Sayılı Direktifi'nin (*"PSD1"*)[452] yerine yürürlüğe giren ve kısaca PSD2 denilen 2015/2366 Sayılı Direktifi ile düzenlenmiştir. PSD2 ile Avrupa Komisyonu tarafından teknolojik gelişmeler de dikkate alınarak, ödeme sistemlerinin ve ödeme hizmet sağlayıcılarının AB ve Avrupa Ekonomik Alanı (*"AEA"*) ile sınırlı olarak yeniden

[450] Türkçe'ye Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı şeklinde tercüme edilen kurumun orijinal adı "European Union Agency for Network and Information Security" olup AB'ne ilişkin tüm belgelerde ve literatürde ENISA olarak geçtiğinden, çalışma kapsamında ENISA olarak kısaltılmıştır. ENISA'nın amaçları, (i) Avrupa Birliği'ne üye devletler ve diğer paydaşlar (*stakeholders*) açısından Avrupa'nın siber güvenlik politikasına katkı sağlamak, (ii) geniş-ölçekli siber ataklara karşı Avrupa Birliği sınırları içerisinde bu durumdan etkilenen iki veya daha fazla üye devlete sınır ötesi saldırılar açısından destek sağlamak ve (iii) böylelikle Avrupa Birliği'nin "Dijital Tek Pazar Stratejisi"nin *(Digital Single Market Strategy)* düzgün şekilde işletilmesini sağlamaktır. Bkz. https://www.enisa.europa.eu/about-enisa (Gözden Geçirilme Tarihi: 29.10.2020).

[451] *Eren*, s. 73, ayrıca Bkz. AB Strateji Belgesi, s.3.

[452] PSD1 denilen 2007/64/EC Sayılı Ödeme Hizmetleri Direktifi, 25.12.2007 tarihinde yürürlüğe girmiş olup AB'ye üye devletlerin iç hukuklarında 01.11.2009 tarihinde kabul edilmiştir. PSD1'nin amacı, AB'ne üye devletler içerisinde sadece kendi ulusal sınırları içerisinde değil, üye devletlerin Avrupa Birliği sınırları içerisinde ödeme hizmetleri konusunda kapsayıcı ve modern kuralların öngörülmesidir. Ödeme hizmetleri endüstrisinde özellikle bankalar dışındaki diğer finansal kuruluşlar ve aktörler de bahsi geçen regülasyon kapsamına alınarak bu alanda tüketicilerin korunması konusunda yeknesak kuralların öngörülmesi ve AB sınırları içerisinde uygun rekabet koşullarını yaratarak bu kapsamdaki ödeme hizmet sağlayıcılarının ve kullanıcıların hak ve yükümlülüklerinin düzenlenmesi, ödeme işlemlerinin daha hızlı gerçekleştirilmesinin temin edilmesi ve ödemeler konusunda kullanıcılara daha net bilgiler sağlanması hedeflenmiştir Aynı zamanda, PSD1'nin bir başka amacı ise, SEPA denilen "Tek Avrupa Ödeme Alanı"na yönelik gerekli hukuki altyapının sağlanmasıdır. Ayrıntılı bilgi için bkz.https://web.archive.org/web/20150227172900/http://ec.europa.eu/finance/payments/framework/options_en.htm (Gözden Geçirilme Tarihi: 29.10.2020)

regüle edilmesi amaçlanmıştır[453]. Bu noktada, 16.11.2015 tarihinde Avrupa Komisyonu tarafından PSD2 ile online ödemeler, mobil ödemeler, açık bankacılık gibi ödeme işlemlerinin daha güvenli bir hukuki altyapıya dayandırılarak Avrupa Birliği'nde tüketicilerin korunması hedeflenmiştir. Başka bir ifade ile, AB'de PSD1 ile AB'ye üye devletler açısından ödeme hizmetleri pazarında hukuken bağlayıcı kurallar ve standartlar öngörülmüş iken, PSD2 ile ödeme sistemlerindeki yeni teknolojik gelişmelere uyumlu olarak üçüncü taraf hizmet sağlayıcılar (*third party providers*) açısından da kapsamlı düzenlemeler öngörülmüştür.

16.11.2015 tarihinde PSD2'nin yürürlüğe girmesinden sonra, AB'ye üye devletler açısından kendi iç hukuklarına uyumlu şekilde mevzuat değişikliğine gitmeleri açısından iki senelik bir zaman tanınmıştır. 27.11.2017 tarihinde ise, Avrupa Komisyonu tarafından PSD2'ye eklemlenecek ve PSD2'deki SCA mekanizmasına ilişkin teknik standartlar ile yeknesak uyum konusunda (EU) 2018/389 Sayılı Tüzüğü[454] yürürlüğe konulmuştur. Ancak, PSD2'nin her ne kadar gecikmeli olarak 14.09.2019 tarihinde yürürlüğe girmesi öngörülmüşse de, aşağıda ayrıntılı şekilde açıklanan SCA sisteminin uygulamaya dair bazı problemli hususları içermesi sebebiyle, Avrupa Bankacılık Kurumu (*European Banking Authority*)[455] tarafından Avrupa Birliği'ne üye devletlerin SCA sistemine en geç 31.12.2020 tarihinde geçilmesine olanak tanınmıştır[456].

---

[453] https://ec.europa.eu/commission/presscorner/detail/en/IP_15_5792 (Gözden Geçirilme Tarihi: 29.10.2020).

[454] Orijinal metne internet üzerinden ulaşmak için Bkz. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R0389&from=IT (Gözden Geçirilme Tarihi: 29.10.2020).

[455] https://eba.europa.eu/ (Gözden Geçirilme Tarihi: 29.10.2020).

[456] Avrupa Bankacılık Kurumu (*"EBA"*), 21 Haziran 2019 tarihinde yayınladığı görüşünde, PSD2'nin tüm AB sınırları içerisinde uygulanması gerektiğine vurgu yaparak özellikle SCA'nın Avrupa Birliği nezdindeki tüm ödeme hizmet sağlayıcılar ve kullanıcılar açısından yeknesak şekilde uygulamasındaki zorluğu dikkate aldığını ifade etmiş ve bu sebeple SCA sisteminin en geç 31 Aralık 2020 tarihinden itibaren sistemdeki tüm paydaşlarca uygulanmasına izin verildiğini belirtmiştir. İlgili görüş için bkz. https://eba.europa.eu/sites/default/documents/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

Çalışmanın odak noktasının elektronik ödeme sistemlerinde siber güvenlik olması sebebiyle bu noktada üzerinde durulması gereken iki husus söz konusudur[457]:

Güçlü Müşteri Onayı ("SCA"): PSD2, öncelikle hizmet sağlayıcıları açısından, müşterilerin ödeme dolandırıcılığı gibi risklere korunması açısından ödeme hesabına online sistem üzerinden erişilmesi halinde "Güçlü Müşteri Onayı" (*"Strong Customer Authentication"* veya *"SCA"*)[458] denilen bir sistemin hayata geçirilmesini zorunlu kılmaktadır. SCA, ödeme kanallarındaki web ve mobil uygulamalarında temel itibariyle içeriğinde "Bilgi" (*Knowledge*), "Aidiyet" (*Possesion*) ve "Özgülük" (*Inherence)* denilen hususlardan en az iki veya daha fazla unsuru gerektiren bir müşteri onay mekanizmasını ifade etmektedir. Kısaca bu unsurları açıklamak gerekirse:

Bilgi, ödeme sistemi ile ilgili onay mekanizmasında sadece müşterinin *bildiği* bilgi (örneğin parola, PIN vb.) ile sisteme giriş imkânının olduğunu ifade eder.

[457] PSD2 ile ilgili olarak bilgi güvenliği konusundaki değerlendirmeler genel itibariyle Goode Intelligence adlı kuruluşun bu konuda yayınladığı "The Impact of Payment Services Directive II on Authentication & Security" başlıklı White Paper'ından derlenerek bu kısma aktarılmıştır. İlgili White Paper metnine internet ortamında şu link üzerinden ulaşılabilir: https://www.rsa.com/content/dam/en/white-paper/impact-of-psd2-on-authentication-and-security.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[458] Yukarıda PSD2'nin orijinal metninde "strong customer authentication" olarak belirtilen ibare, yazar tarafından Türkçe'ye "güçlü müşteri onayı" olarak tercüme edilmiştir. PSD2'ye göre güçlü müşteri onay mekanizmasında yukarıda belirtilen bilgi, aidiyet ve özgülük olan üç unsurdan en az ikisinin olması gerektiği öngörülmektedir. Güçlü müşteri onayı, aynı zamanda bu unsurların, en az ikisini haiz olan kullanıcı açısından her bir unsurun diğerinden bağımsız olduğu, herhangi bir unsurun ihlalinin sistemin güvenilirliği açısından diğer unsurları etkilemediği ve sistemin onay bilgilerini koruduğu bir onay mekanizması anlamına gelmektedir. (Bkz. *PSD2*, Başlangıç, para. 30). PSD2'nin 74. maddesinde ise, ödeme hizmet sağlayıcısının güçlü müşteri onay sistemini (SCA) sağlamadığı takdirde, ödeyen tarafın hileli şekilde davranmadığı müddetçe meydana gelebilecek finansal kayıplardan ötürü herhangi bir sorumluluğun olmayacağı belirtilerek açıkça bu konudaki sorumluluğun ödeme hizmet sağlayıcıya ait olması hüküm altına alınmıştır. Anılan düzenlemeye göre, ayrıca ödemeyi alan tarafın veya onun ödeme hizmet sağlayıcısının güçlü müşteri onay mekanizmasını kabul etmemesi halinde ise, zarar halinde bu konuda ödeyenin hizmet sağlayıcısına meydana gelen zararı tazmin etmesi gerektiği düzenlenmiştir. SCA konusunda PSD2'nin diğer düzenlemeleri olan 93.madde (rücu hakkı), 97. madde (onay) ve 98. madde (onay ve iletişim konusunda düzenleyici teknik standartlar) dikkate alınabilir.

Aidiyet, sisteme girişin onayı açısından sadece müşterinin *sahip olduğu* bir araç (örneğin kart, bir kez verilen onay kodu, vb.) ile sisteme giriş yapılabilmesi anlamına gelmektedir.

Özgülük, sisteme ancak müşteriye *özgü bir yöntem*le (parmakizi, ses veya retina taraması gibi biyometrik verilerle) girişin mümkün olduğuna işaret eder.

PSD2'de, yukarıda belirtilen her unsurun birbirinden bağımsız olması gerektiği ve herhangi bir unsurun ihlal edilmesi halinde sistemin güvenilirliği açısından diğer unsurların bu ihlalden etkilenmemesi gerektiği düzenlenmiştir. Onay çözümü, teknik açıdan onay bilgisini veya kullanıcının kimlik bilgilerini koruyacak şekilde tasarlanmalıdır. Online ödemeler gibi sisteme uzaktan erişim ile giriş gerektiren onay mekanizmasına dair güvenlik önemleri daha sıkı olmalı ve hileli veya hatalı işlemlerdeki riskleri asgariye indirgeyecek şekilde belirlenmelidir. Örnek vermek gerekirse, kullanıcının hesabından paranın transfer edileceği hesap sahibine paranın transfer edilmesi açısından bir kereliğine özgü olmak üzere sistem üzerinden link verilmesi gibi dinamik çözümler özellikle tercih edilmelidir.

Uygulama Programlama Arayüzleri (API) ve Açık Bankacılık: PSD2, özellikle ödemelerde yenilikçi yaklaşımları desteklemekte olup üçüncü taraf hizmet sağlayıcılar açısından "API" denilen uygulama program arayüzleri[459] vasıtasıyla müşteri hesaplarına giriş yapılmasına imkân tanımaktadır. Bu noktada, API'lerin özellikle açık bankacılıkta bilgi güvenliği açısından etkin bir mekanizma olup olmadığı konusunda literatüre bakıldığında, kullanıcı giriş onay mekanizmasının saldırganlar tarafından kırılabileceği, API'lerde özellikle "endpoints"[460] denilen sorgu adreslerinde

[459] API'lerle ilgili ayrıntılı analizlere ve bu kapsamdaki PSD2 düzenlemelerine çalışmanın 6.3. numaralı "Açık Bankacılıkta Siber Güvenlik" başlığı altında yer verildiğinden, bu kısımda API'ler sadece bilgi güvenliği çerçevesinde kısaca ele alınmıştır.

[460] Kurtuluş Şahin tarafından kaleme alınan "Hiç Bilmeyenler İçin; API nedir?" başlıklı yazı içeriğinde API kavramı, Twitter uygulaması üzerinden somut bir örnekle basit ve anlaşılabilir şekilde açıklanmıştır. Bu makaleden çıkan sonuç, yazılımlarda manuel şekilde girilen uygulamaların API denilen arayüz uygulamaları ile otomasyon imkânı vermesi ve süreçleri hızlandırmasıdır. Örnek vermek gerekirse, Twit

saldırganlar tarafından sayısız güvenlik ihlalinin keşfedilebileceği, bu nedenle API'lar için öngörülen OWASP[461] Risk Ölçeklendirme Metadolojisi gibi bazı yöntemlerin uygulanması gerektiği üzerinde durulmuştur[462].

Yukarıda belirtilen PSD2 dışında elektronik ödeme sistemlerinde siber güvenlik açısından dikkati çeken diğer AB regülasyonları şunlardır:

4.2.2. Avrupa Birliği Siber Suç Sözleşmesi ("Budapeşte Sözleşmesi")

Türkiye Cumhuriyeti'nin de taraf olduğu[463], 23.11.2001 yılında Budapeşte'de imzaya açılan ve 01.07.2004 yılında birçok AB'ne üye devlet nezdinde yürürlüğe giren 185 Sayılı Avrupa Siber Suç Sözleşmesi (*Convention on Cybercrime*)[464] ile internet üzerinden işlenen suçlar ile diğer bilgisayar ağları vasıtasıyla telif hukuku ihlalleri,

---

atılırken tarayıcıda twitter.com adresi görülür, kullanıcı tarafından aktive edilen API'ye sorgu yaparken (varsayımsal olarak belirtilmiştir) Twitter örneğinden yola çıkıldığında ise, API'deki endpoint, API uygulamasının çalışacağı ilgili sorgu adresini ifade etmektedir. (Örn: https://api.twitter.com/1.1/statuses/update.json endpointi kullanılır.) Bkz. Kurtuluş Şahin, "Hiç Bilmeyenler İçin; API nedir?" (*"Şahin"*): https://medium.com/@kurtulussahin/api-nedir-462dff9922d0 (Gözden Geçirilme Tarihi: 29.10.2020).

[461] *"OWASP"*ın İngilizce'deki açılımı "Open Web Application Security" olup Türkçe'ye "Açık Web Uygulama Güvenliği Projesi" olarak tercüme edilebilir (Serbest Çeviri). OWASP, güvensiz yazılımların oluşturduğu problemlerle mücadele etmek için kurulmuş bir topluluktur. Bu topluluğun tüm araçları, belgeleri, listeleri ve bölümleri ücretsiz olarak yazılım güvenliği meraklılarına sunulmuştur. Bu konuda detaylı bilgi bkz. *Altınkaynak*, s. 35. Ayrıca, OWASP denilen kuruluş API güvenliği sağlanması ve bu konudaki uygulamaların geliştirilmesi konusunda bazı standartlar öngörmüş olup bu hususta standartlar ile ilgili ayrıntılı bilgi için Bkz. https://www.owasp.org/index.php/OWASP_API_Security_Project (Gözden Geçirilme Tarihi: 29.10.2020).

[462] Bu konuda ayrıntılı bilgi için Bkz. raw.githubusercontent.com (Gözden Geçirilme Tarihi: 29.10.2020).

[463] Türkiye Cumhuriyeti, Avrupa Siber Suçlar Sözleşmesi'ni 10.11.2010 tarihinde imzalamış ancak 22.04.2014 tarih ve 6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun ile onaylanmış ve Kanun'un 02.05.2014 tarihinde Resmi Gazete'de yayımlanmasıyla yürürlüğe girmiştir. Sözleşme'nin resmi tercümesi "Sanal Ortamda İşlenen Suçlar Sözleşmesi" olarak belirtilmiştir. Türkiye Sözleşme'nin madde 2, 7, 14/3 (b), 22, 24, 27/2, 29/4, 35/1, 40 ve 42 hükümlerine toplam 8 başlık altında beyan ve çekince koymuştur. (Serbest Çeviri) Bkz. https://tr.wikipedia.org/wiki/Sanal_Ortamda_İşlenen_Suçlar_Sözleşmesi (Gözden Geçirme Tarihi: 29.10.2020).

[464] Avrupa Siber Suç Sözleşmesi'nin orijinal metnine ulaşmak için Bkz. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN, ayrıca Türkçe tercümesi için ayrıca Bkz. https://afyonluoglu.org/PublicWebFiles/cyber/legislation/2001-Avrupa%20Birliği%20Siber%20Suçlar%20Sözleşmesi-TR.pdf (Gözden Geçirme Tarihi: 29.10.2020).

çocuk pornografisi ve ağ güvenliği ihlali ile ilgili birçok hukuki mesele bakımından ayrıntılı düzenlemelere ve özellikle ihlale konu internet ağı üzerinden ilgili devlet otoritelerinin inceleme yapılabilmesine olanak veren bir dizi düzenlemeye yer verilmiştir. Sözleşmenin Açıklayıcı Raporu'nda[465], bilişim suçlarıyla ilgili taraf devletlerin yasal mevzuatlarını ve bağlantılı hükümlerini uyumlu hale getirmek, siber suçların ve elektronik delil içeren diğer klasik suçların soruşturma ve kovuşturulması ile ilgili ulusal usul hukuku mevzuatına temel oluşturarak uluslararası muhakeme kurallarının yeknesaklaştırılmasını sağlamak ve uluslararası adli yardım ve işbirliği alanında hızlı ve etkili bir sistem oluşturmak Avrupa Siber Suç Sözleşmesi'nin temel amaçları olarak belirtilmiştir[466]. Avrupa Siber Suç Sözleşmesi'nin önemli bir özelliği, Avrupa Konseyi'ne üye olmamasına rağmen aralarında bilişim konusunda çok gelişmiş ülkelerin de bulunduğu birçok ülke tarafından imzalanması ve kendi iç hukuk sistemlerinde yürürlüğe sokulmasıdır.

Avrupa Siber Suç Sözleşmesi'nde içerik itibariyle, bilgisayar veri ve sistemlerinin varlığına, bütünlüğüne ve gizliliğine karşı suçlar[467], bilgisayarla ilişkili suçlar[468], içerikle ilgili suçlar[469] ve telif hakları ve benzer hakların ihlali[470] ile ilgili suçlar olmak

[465] Söz konusu raporun orijinal metni için Bkz. https://rm.coe.int/16800cce5b (Gözden Geçirme Tarihi: 29.10.2020).
[466] Avrupa Siber Suçlar Sözleşmesi konusunda ayrıntılı bilgi için Bkz. Jonathan Clough, "A World of Difference: The Budapest Convention on Cybercrime And The Challenges of Harmonisation", Monash University Law Review, C: 40, No:3, (*"Clough"*) ilgili makaleye aşağıdaki link üzerinden ulaşılabilir: https://web.archive.org/web/20160430024621/https://www.monash.edu/__data/assets/pdf_file/0019/232525/clough.pdf. Bu konuda Avrupa Siber Suç Sözleşmesi'nin Türk Hukuku'na etkileri hakkında detaylı bilgi için ise ayrıca Merve Erdem/Gürkan Özocak, "Avrupa Konseyi Siber Suç Sözleşmesi Ve Türk Hukuku'na Etkileri" (*"Erdem/Özocak2"*): http://www.ozocak.com/Dosyalar/27669f.pdf (Gözden Geçirilme Tarihi: 29.10.2020).
[467] Avrupa Siber Suçlar Sözleşmesi'nde "Bilgisayar veri ve sistemlerinin varlığına, bütünlüğüne ve gizliliğine karşı suçlar üst başlığı altında illegal giriş (m. 2), gayrimeşru ele geçirme (m. 3), verilere müdahale (m. 4), sisteme müdahale (m. 5) ve donanımların suiistimali (m. 6) olmak üzere gibi farklı suç kategorilerine yönelik ayrıntılı düzenlemelere yer verilmiştir.
[468] Sözleşme kapsamında "bilgisayarla ilgili suçlar" kategorisi bakımından bilgisayarla ilişkili sahtekârlık (m. 7) ve bilgisayarla ilgili dolandırıcılık (m. 8) olmak üzere iki suç tipine yer verilmiştir.
[469] İçerik ile ilgili suçlar bakımından, Avrupa Siber Suçlar Sözleşmesi'nde yer verilen tek suç tipi 9. maddede düzenlenen çocuk pornografisine ilişkin suçlar şeklinde düzenlenmektedir.
[470] Bkz. Avrupa Siber Suçlar Sözleşmesi, m. 10.

üzere üst başlıklar halinde birtakım siber suçlara yönelik ayrıntılı hükümler öngörülmüş olup aynı zamanda söz konusu suç ve cezalara yönelik usuli hükümler ile uluslararası işbirliği açısından da ayrıntılı birtakım düzenlemelere yer verildiği görülmektedir.

Avrupa Siber Suç Sözleşmesi, doktrinde kolay çekince konmasına imkân tanıması, değişiklik rejiminin hantal olması, hazırlıklar aşamasında taraf ülkelerin eşit şekilde ve yeterli temsil edilmemiş olması gibi bazı zayıf yönleri nedeniyle eleştirilmesine rağmen, Aliusta/Berber'e göre anılan sözleşmenin, yukarıda sayılan amaçlara büyük ölçüde hizmet ettiği ve taraf devletlere bilişim suçlarıyla mücadele etmek için gerekli maddi ceza hukuku ve usul hukukunun temel çatısını sağladığı ve sınır aşan soruşturma ve kovuşturmalarda devletlerin birbirleriyle hızlı ve etkili bir şekilde koordine olabilmelerine uygun zemin sunduğu belirtilmektedir[471].

01.03.2006 tarihinde, Avrupa Siber Suçlar Sözleşmesi'nin "İçerikle Bağlantılı Suçlar" olarak ifade edilen çocuk pornografisiyle bağlantılı suçlar şeklindeki suç kapsamı Sözleşme'ye 28.01.2003 tarihinde eklenen ve her türlü ırkçı ve yabancı düşmanlığı içeren hareket ve tehdit söylemlerinin bilişim sistemleri aracılığıyla yayınlanmasının suç sayılmasını öngören Ek Protokol ile genişletilmiştir[472]. Ek Protokol, niteliği gereği, hukuken Avrupa Siber Suç Sözleşmesi'nden ayrı bir yasal belge olarak değerlendirilmekte olup ana sözleşmeyi imzalayan devletlerin Ek Protokol'ü imzalamak veya yürürlüğe koymak gibi bir yükümlülüğü bulunmamaktadır[473]. Ek

[471] Cahit Aliusta/Recep Benzer, "Avrupa Siber Suçlar Sözleşmesi Ve Türkiye'nin Dahil Olma Süreci", Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt: 4, No: 2, 2018, (*"Aliusta/Benzer"*), s: 35-42: https://www.researchgate.net/publication/331007406_Avrupa_Siber_Suclar_Sozlesmesi_ve_Turkiye'nin_Dahil_Olma_Sureci (Gözden Geçirilme Tarihi: 29.10.2020).

[472] *Aliusta/Benzer,* s. 39. Ayrıca Bkz. https://web.archive.org/web/20060209153034/http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm#topicE (Gözden Geçirilme Tarihi: 29.10.2020).

[473] Burak Cesur Aköz, "Türk Ceza Kanunu Kapsamında Bilişim Suç Ve Cezaları İle Örnek Yargısal Kararların Analizi Ve Mevzuat Önerileri", Bilgi Teknolojileri Ve İletişim Kurumu, Bilişim Uzmanlığı Tezi, Ankara, 2018, (*"Aköz"*), s. 55: https://www.btk.gov.tr/uploads/thesis/burak-cesur-akoz-b-uzm-tezi-5d10d910e20e8.pdf. (Gözden Geçirilme Tarihi: 29.10.2020).

Protokol Avrupa Siber Suç Sözleşmesi gibi Türkiye tarafından 19.04.2016 tarihinde imzalanmasına rağmen, henüz kanunla uygun bulma ve yürürlük aşamalarını gerçekleştirmemiştir[474].

Doktrinde özellikle birtakım yazarlar tarafından Avrupa Siber Suç Sözleşmesi'nin otoriter bir yapısı bulunduğunu ve bu yapının temel hak ve özgürlükleri kısıtlayıcı ve kamusal otoriteyi güçlendirici bir yapısı olması sebebiyle eleştirilse de, Dülger sözleşmenin onaylanarak iç hukukumuzun bir parçası haline getirilmesinin faydalı olduğunu belirtmiştir. Çalışmada, Dülger ile benzer bir değerlendirme yapılarak Avrupa Siber Suç Sözleşmesi'nin iç hukukumuzda yürürlüğe sokulmasının yazar tarafından özetle şu faydaları olabileceği sonucuna varılmıştır: Herşeyden önce, Türkiye'de bilişim suçları büyük ölçüde Türk Ceza Kanunu (*"TCK"*) kapsamında düzenlenmiş olup 2005 yılında yürürlüğe giren TCK ile halihazırda bilişim suçları bakımından her geçen gün yeni saldırı tekniğinin geliştirildiği bir ortamda, TCK'nın işlenen tüm bilişim suçları açısından gereken ihtiyacı karşılamaktan uzak olduğu aşikardır. TCK, içeriği itibariyle suç ve cezaların düzenlendiği normatif bir metin olmakla beraber Türkiye'de özellikle salt bilişime yönelik suçlar bakımından özel bir kanun düzenlemesi olmaması sebebiyle en azından Avrupa Siber Suç Sözleşmesi'nin Türkiye'de yürürlükte olması kısmen dahi olsa bu ihtiyacı karşılamak açısından iyi bir kazanım olarak değerlendirilebilir. Öte yandan, T.C. Anayasası m. 90/f. 5 uyarınca, normlar hiyerarşisi bakımından usulüne uygun yürürlüğe giren uluslararası antlaşmalar, kanun hükmünde olup temel hak ve özgürlükler bakımından aslında kanunların da üzerindedir. Uygulamada maalesef her ne kadar ilk derece mahkemeleri tarafından Anayasa'nın bu hükmü dikkate alınmaksızın uluslararası antlaşmalar zaman zaman yok sayılarak ilk derece mahkemeleri tarafından bazı hükümler tesis edilmişse dahi, en azından yüksek yargı makamlarınca (Yargıtay, Danıştay, Anayasa Mahkemesi) tarafından m. 90/f. 5 hükmünün dikkate alındığı durumlarda özellikle

[474] *Aköz*, s. 55.

Avrupa Siber Suç Sözleşmesi kapsamında tesis edilecek emsal nitelikteki içtihatlar yargının doğru karar vermesine ve doktrinsel açıdan TCK dışında bazı üzerinde anlaşmaya varılamayan hususların netleştirilmesine ışık tutacaktır. Son olarak, Avrupa Siber Suç Sözleşmesi içeriğinde siber güvenliğin temini açısından uluslararası iş birliğini sağlamaya yönelik mevcut düzenlemelerin[475] Türkiye'nin bu alanda diğer devletlerle olan ilişkileri ve özellikle işbirliğini teşvik etmesi nedeniyle yarar sağladığı değerlendirilmiştir[476].

4.2.3. Avrupa Birliği'nin 2016/1148 Sayılı Ağ ve Bilgi Sistemlerinin Korunması Direktifi ("NIS Direktifi")

AB'de siber güvenlik konusunda en önemli regülasyonlardan bir diğeri ise, tüm AB'yi kapsayan ve her aşamada siber güvenlikle ilgili alınması gereken önemleri içeren bir düzenleme olan Ağ Ve Bilgi Sistemlerinin Korunması Direktifi (*"NIS Direktifi"*)[477]'dir.

NIS Direktifi'nde öncelikle üzerinde durulan meselelerden birisi, Avrupa Birliği nezdinde malların, hizmetlerin ve insanların sınır-ötesi işlemler açısından taşınması noktasında, AB iç pazarındaki trafiğin bu kapsamda güvenli şekilde gerçekleştirilmesi bakımından ağ ve bilgi sistemlerinin güvenliğinin önem taşıdığına özellikle dikkat çekilmiştir[478]. Ne var ki, NIS Direktifi içeriğinde de belirtildiği üzere bazı sektörlere yönelik kritik altyapılardan örnek vermek gerekirse, deniz taşımacılığı ve bankacılık gibi kritik altyapı olarak değerlendirilebilecek bazı sektörler bakımından her AB'ye üye devlet açısından o devletin öngördüğü bazı özel düzenlemeler bulunmakla beraber

[475] Bkz. Avrupa Siber Suç Sözleşmesi, III. Bölüm, m. 23 vd.
[476] *Dülger, Bilişim Suçları*, s. 636, 637.
[477] İngilizce'de söz konusu Direktif, "The Directive on Security of Network And Information Systems" olarak belirtilmiş olup yazar tarafından, Avrupa Birliği dokümanlarında ve uluslararası platformda "NIS Direktifi" olarak bilinmesi sebebiyle tez içeriğinde "NIS Direktifi" kısaltması ile yer verilmişir. NIS Direktifi'nin orijinal metnine internet üzerinden ulaşmak için bkz. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN (Gözden Geçirilme Tarihi: 29.10.2020).
[478] NIS Direktifi, Başlangıç, Para. 3.

bazı sektörler bakımından AB nezdinde uygulanan bazı ortak düzenlemeler de bulunmaktadır[479].

NIS Direktifi, Avrupa Parlamentosu nezdinde Ağustos 2016 tarihinde yürürlüğe girmiş olup Avrupa Birliği'ne üye devletlerin en geç 09.05.2018 tarihine kadar iç hukuklarında NIS Direktifi ile ilgili gerekli yasal düzenlemeleri yürürlüğe sokmaları ve bu bağlamda kritik servislerini en geç 09.11.2018 tarihine kadar belirlemeleri gerektiği öngörülmüştür. Kısacası, NIS Direktifi ile, üye devletlerin CSIRT[480] denilen bir kuruluş tarafından siber güvenlikle ilgili her türlü gerekli önlemi alabileceği düzenlenmiştir. Bu kuruluşun amacı, üye devletler açısından siber güvenlik alanında stratejik bir işbirliği sağlanarak bu alandaki bilgi birikiminin etkin şekilde iletilmesidir[481]. Ayrıca, NIS Direktifi'nde Avrupa Birliği'ne üye devletler nezdinde bilgi güvenliği kültürünün yaratılmasının önem arz ettiği belirtilerek çalışmayı

[479] Örnek vermek gerekirse, NIS Direktifi'nde deniz taşımacılığı sektöründe güvenlik denildiğinde bu olgunun ilgili sektörde hangi süjeleri ilgilendirdiği açıkça belirtilmiştir. Siber güvenlik ihlalleri olması halinde ise, bu sektöre ilişkin siber güvenlik ihlali bildiriminin üye devletler nezdinde genelde lex specialis ilkesi (özel kural genel kuralı dışlar) çerçevesinde düzenlendiği, ancak üye devletler nezdindeki tüm bu düzenlemeler bakımından, alınabilecek asgari güvenlik önlemlerinde özellikle NIS Direktifi'nde öngörülen bazı asgari standartların sağlanması gerektiğine dikkat çekilmiştir. Bkz. NIS Direktifi, Başlangıç, Para. 10. Bu çalışmayı ilgilendirmesi bakımından ise, NIS Direktifi'nde özellikle bankacılık ve finans pazarına ilişkin altyapının regüle edilmesi ve denetiminin ise, su taşımacılığı sektörüne kıyasla nispeten Birlik nezdinde büyük ölçüde ortak şekilde düzenlendiği ve bu düzenlemelerin özellikle Avrupa Merkez Bankası (European Central Bank) gibi bir üst kurul tarafından denetlendiği belirtilmiştir. Bkz. NIS Direktifi, Başlangıç, Para. 13. Avrupa Merkez Bankası'nın 25.07.2014 tarihli görüşünde de dikkat çekildiği üzere, ödeme ve mutabakat sistemleri bakımından Birlik nezdinde uygulanan kurallara NIS Direktifi'nin herhangi bir doğrudan etkisi olmamakla beraber, NIS Direktifi'nin sadece bu alanda özellikle AB üye devletler bakımından ağ ve bilgi güvenliğinin temini bakımından deneyimin üye devletler tarafından birbirlerine aktarılması noktasında önem taşıdığı üzerinde durulmuştur. Bkz. NIS Direktifi, Başlangıç, Para. 14. Son olarak, NIS Direktifi'nde kritik altyapılar bakımından siber güvenlik ihlalinin yıkıcı bir etkisi olup olmadığının tespitinde, sınır ötesi etmenlerin yanı sıra, ilgili kritik altyapının ilgilendirdiği sektöre ilişkin sektör-spesifik etkenlerin de dikkate alınması gerektiği değerlendirilmiştir. Tezi ilgilendirmesi açısından bankacılık ve finans kuruluşlarının altyapısına yönelik gerçekleştirilen bir siber güvenlik ihlalinde sektör-spesifik olarak dikkate alınması gereken olgu, NIS Direktifi'ne göre siber saldırının hedef aldığı ilgili kuruluştaki toplam malvarlığı ve bu toplam malvarlığının Gayri Safi Yurtiçi Hasıla'ya oranıdır. Bu konuda ayrıntılı bilgi için bkz. NIS Direktifi, Başlangıç, para. 28.

[480] İngilizce açılımı "Computer Security Incident Response Team" olup Türkçe'ye "Bilişim Güvenliği Olay Müdahale Ekibi" olarak tercüme edilebilir. (Serbest Çeviri).

[481] NIS Direktifi, m. 2/f. 1/c.

ilgilendirmesi açısından başta finans sektörü olmak üzere, enerji, taşımacılık, bankacılık, finansal piyasa altyapıları, içme suyu tedarik ve dağıtımı, sağlık ve dijital altyapı gibi kritik altyapılar açısından[482] siber güvenlik meselesinde daha hassas davranılması gerektiği belirtilmiştir.

Özellikle bahsi geçen bu sektörlerde faaliyet gösteren üye devletlere ait işletmelerin bu konuda uygun her türlü uygun tedbiri alarak ve kendi ulusal makamlarına her türlü risk konusunda gerekli bildirimleri yapması gerektiği öngörülmüştür. Buna ilaveten, bulut bilişim hizmet sağlayıcılar gibi dijital alanda kilit durumda olan aktörlerin özellikle NIS Direktifi'nde öngörülen kurallara ve düzenlemelere uygun davranması gerektiğine de dikkat çekilmiştir[483].

Avrupa Birliği'ne üye devletler açısından 09.05.2018 tarihini kendi iç hukuklarında NIS Direktifi'ni kabul etmeleri için son tarih belirlenmesi sebebiyle, Avrupa Komisyonu söz konusu Direktif'in Avrupa Birliği'nde etkin şekilde uygulanması sağlamak amacıyla 13.09.2017 tarihinde COM/2017/476 Sayılı Bildiri[484] (*Directive on Security of Network And information systems*) yayınlamıştır. NIS Direktifi'nin tamamlayıcısı olan bu bildiri ise, NIS Direktifi'nin nasıl uygulanması gerektiğine ilişkin yol gösterici bir belge olmakla beraber NIS Direktifi kapsamında CSIRT denilen kuruluşun ne şekilde kurulacağı ve işleyişine ilişkin birtakım düzenlemeler içermektedir[485].

---

[482] Hangi sektörlerin siber güvenlik açısından kritik altyapı olarak değerlendirilmesi gerektiği konusunda detaylı bilgi için bkz. NIS Direktifi, Ek-2 (Annex II).

[483] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive (Gözden Geçirilme Tarihi: 29.10.2020).

[484] Söz konusu Bildiri'nin tam metni için Bkz. https://eur-lex.europa.eu/resource.html?uri=cellar:d829f91d-9859-11e7-b92d-01aa75ed71a1.0001.02/DOC_3&format=PDF (Gözden Geçirilme Tarihi: 29.10.2020).

[485] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive (Gözden Geçirilme Tarihi: 29.10.2020).

4.2.4. 2019/881 Sayılı ENISA Ve Bilişim Ve İletişim Teknolojilerinde Siber Güvenlik Sertifikasyon Tüzüğü ("2019/881 Sayılı Tüzük")

AB'de yakın zamanda siber güvenlik açısından en dikkat çekici düzenlemelerden birisi olan 2019/881 Sayılı ENISA Ve Bilişim Ve İletişim Teknolojilerinde Siber Güvenlik Sertifikasyon Tüzüğü (*"2019/881 Sayılı Tüzük"*)[486] 27.07.2019 tarihinde yürürlüğe girmiştir[487]. 2019/881 Sayılı Tüzük'ün temel itibariyle özellikle aşağıda belirtilen iki hususta öngördüğü yenilik önem taşımaktadır[488]:

İlk olarak, Avrupa Birliği'nin "Dijital Tek Pazar Stratejisi"nin (*Digital Single Market*)[489] etkin bir şekilde uygulanabilmesi ve bu konuda siber güvenliğin kritik

[486] 2019/881 Sayılı Tüzük orijinal belgede *"Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013"* olarak belirtilmiş olup İngilizce belgelerde "Cybersecurity Act" olarak kısaltılmıştır. Söz konusu tüzüğün tam metnine ulaşmak için Bkz. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN (Gözden Geçirilme Tarihi: 29.10.2020).

[487] Bu konuda Avrupa Birliği düzenlemeleri açısından ENISA'ya bakıldığında, ENISA ilk kez Avrupa Birliği'nin (EC) 460/2004 Sayılı Tüzüğü ile kurulmuş olup bilgi ve ağ güvenliği konusunda etkin standartların getirilmesi ve Avrupa Birliği vatandaşlarının, tüketicilerinin, kamu kurum ve kuruluşları nezdinde siber güvenlik kültürünün yaratılması amacıyla kurulmuştur. 1007/2008 Sayılı Tüzük ile ENISA'nın görev süresi 2012 yılı Mart ayına kadar uzatılmış, 580/2011 Sayılı Tüzük ile 13.09.2013 tarihine kadar tekrar uzatılmış ve 526/2013 tarihli Tüzük ile en son 19.07.2020 tarihine kadar uzatılmıştı. Son yürürlüğe giren 2019/881 (EC) Sayılı Tüzük ise hâlihazırda uygulanmakta olan 526/2013 Sayılı Tüzük'te ENISA'nın görev süresi belirtilen zaman sınırlamasını ortadan kaldırarak ENISA'nın siber güvenlik alanında daimi bir organ olarak hareket etmesi öngörülmüştür.

[488] 2019/881 Sayılı Tüzük'ün amacı konusunda detaylı bilgi için Bkz. https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity (Gözden Geçirilme Tarihi: 29.10.2020).

[489] Avrupa Birliği tarafından, ilk kez 06.05.2015 tarihinde Dijital Tek Pazar Stratejisi'nin (*"DTPS"*) açıklandığı görülmüştür. DTPS çerçevesinde AB tarafından dijital dönüşümün Birlik kapsamında sağlanması ve kolaylaştırılması hedeflenmiştir. Temel itibariyle, dijital verinin, Avrupa Birliği açısından ekonomik büyüme, rekabet edebilirlik, inovasyon, yeni iş olanaklarının yaratılması (örneğin yeni start-up girişimciliğe imkan sağlayarak Avrupa Birliği'nde faaliyette bulunan 500 milyon kişiye yeni bir istihdam alanı yaratılması ve DTPS'nin tamamlanması halinde yıllık 415 milyon Avro kazanç elde edilmesi) ve genel itibariyle sosyal kalkınma açısından temel bir kaynak olduğu üzerinde durulmaktadır. Avrupa Birliği Dijital Tek Pazar Stratejisi ile malların, kişilerin, hizmetlerin, sermayenin ve artık verinin de serbest dolaşımını ve bu sayede Avrupa Birliği sınırları içerisinde hukuka uygun, güvenilir ve daha az maliyetli şekilde iş imkânlarını sağlamayı hedeflemektedir. Bu konuda ayrıntılı bilgi için Bkz. https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market (Gözden Geçirilme Tarihi: 29.10.2020). Özellikle, 2014-2019 DTPS ardından, 19.02.2020 tarihinde Avrupa Komisyonu Avrupa'nın dijital geleceğini şekillendirmesi beklenen bir dizi belge yayınlamış olup Dijital Strateji

düzeyde önem taşıdığı düşünülerek özellikle yeni yürürlüğe giren Avrupa Siber Güvenlik Sözleşmesi ile ENISA'nın siber güvenlik alanında hak ve yetkileri genişletilmiştir[490].

İkinci olarak ise, Avrupa siber güvenlik sertifikasyon çerçevesi oluşturulmuştur. Bu açıdan ENISA'nın 2020-2022 dönemine ilişkin Program Belgesi[491] incelendiğinde, ENISA tarafından Siber Güvenlik Sözleşmesi'nin etkin şekilde uygulanabilmesi açısından ve bu alanda belirli gelişmelerin sağlanabilmesi amacıyla "Siber Güvenlik Sertifikasyon Çerçevesi"nin[492] (*The Cybersecurity Certification Framework*) altyapısına ilişkin önemli bilgiler paylaşılmıştır. Buna paralel olarak, ENISA 5G'ye bağlanma konusunda siber güvenlik noktasında çıkabilecek sorunlar, siber-kriz

Belgesi kapsamında Avrupa'yı veriler açısından özellikle önümüzdeki beş sene içerisinde belirlenen dijital teknolojilerle ilgili hedefler aracılığıyla nasıl lider konumuna getirmeyi amaçladığı ortaya konulmuştur. (Bkz. "The European Digital Strategy – Shaping Europe's Digital Future": https://ec.europa.eu/digital-single-market/en/content/european-digital-strategy, Gözden Geçirilme Tarihi: 29.10.2020). Avrupa Veri Stratejisi belgesinde yer alan temel başlıklardan birisi de "Dijital Güvenlik (Siber Güvenlik Ve Mahremiyet)"tir. Bu konuda detaylı bilgi için ayrıca bkz. Leyla Keser Berber, "Kurumsal Güven Bağlamında Güven Hizmet Sağlayıcı (Trust Service Provider), Güven Hizmetleri Ve Karşılıklı Tanıma Sorunu", Oniki Levha Yayıncılık, 1. Baskı, İstanbul, 2020. ("*Keser Berber, Güven Hizmetleri"),* s. 12.

[490] ENISA'nın kurulduğu 2004 yılından itibaren siber güvenlik ihlallerinde gerek Avrupa Birliği gerekse dünyada önemli bir artış yaşanmış olup bu konuda özellikle üye devletlerin desteklenmesi gerektiği, bu yönde uygun politikalar geliştirerek siber güvenlik uygulamalarının bu kapsamda geliştirilmesi gerektiği üzerinde durulmuştur. ENISA'nın özellikle aşağıda detaylı şekilde açıklanacak olan siber güvenlik sertifikasyon çerçevesinin temin edilmesi ve konunun teknik altyapısı ile ilgili gerekli hazırlıkları yaparak sertifikasyona ilişkin gelişmeleri kamuya açık resmi bir web sitesi üzerinden duyurmasının ve bu konuda kamuoyunu da bilgilendirmesinin önemli olduğuna vurgu yapılmıştır. Bu konuda daha detaylı bilgi için bkz. https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity (Gözden Geçirilme Tarihi: 29.10.2020).

[491] https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-202020132022 (Gözden Geçirilme Tarihi: 29.10.2020).

[492] ENISA tarafından "Siber Güvenlik Sertifikasyon Çerçevesi"nin iletişim teknolojileri konusundaki ürün ve hizmetlerin (örneğin akıllı kartlar) siber güvenlik açısından uyumlu olduğunu ölçmeye ve belgelendirmeye yarayan ve bu konuda bir dizi teknik gereklilik ve kapsamlı kurallar içerecek bir metin olacağı belirtilmiştir. Bu sertifikasyon sayesinde Avrupa Birliği'ne üye devletler arasında özellikle gerçekleştirilecek sınır ötesi ticari işlemler açısından siber güvenlik noktasında ne gibi önlemler alınması gerektiği ile ilgili daha net bir belirlemenin yapılmasının mümkün olacağı belirtilmiştir. Bu konuda ayrıntılı bilgi için Bkz. file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/TheEUCyberActataglance%20(2).pdf (Gözden Geçirilme Tarihi: 29.10.2020).

yönetimi yaklaşımına blueprint[493] konseptini de dahil ederek bu alanda bilgi yönetimi sürecinin desteklenmesi amaçlamıştır. Son olarak, siber güvenlik alanındaki açıkların giderilmesi noktasında klasik yöntemlerin özellikle yapay zeka, robotik bilimi, 5G ağları, nesnelerin interneti gibi hızlı gelişen alanlarda etkin şekilde cevap vermeyebileceği üzerinde durularak yakın gelecekte özellikle kuantum bilgisayarların daha etkin şekilde kullanılması halinde günümüzde kullanılan geleneksel kriptografi yöntemlerinin çağın gerisinde kalacağı ve gelecekte Avrupa Birliği'nin siber güvenlik ihtiyaçlarına cevap vermeyeceği de üzerinde durulan hususlardan birisidir[494].

4.2.5. Genel Veri Koruma Tüzüğü Kapsamında Elektronik Ödemelerde Siber Güvenlik Açısından Dikkat Çeken Düzenlemeler

2016/679 Sayılı AB Genel Veri Koruma Tüzüğü (*"GDPR"*)[495] olarak bilinen "Kişisel Verilerin İşlenmesi Karşısında Gerçek Kişilerin Korunması Ve Bu Tür Verilerin Serbest Dolaşımına İlişkin Tüzük", 25.05.2018 tarihinde yürürlüğe girmiş olup bu kapsamda Avrupa Birliği'ne üye ülkeler tarafından uygulanmakta olan 95/46/EC Sayılı Direktifi kaldırarak AB'ye üye ülkeler nezdinde kişisel verilerin korunması[496] kurallarının tüm üye devletler açısından yeknesak şekilde uygulanması

[493] "Blueprint for Coordinated response to large-scale cross-border cybersecurity incidents and crises" isimli belgede, herhangi bir siber saldırı karşısında iyi organize edilmiş bir kriz yönetiminin nasıl olması gerektiği ve Avrupa Birliği nezdindeki kuruluşların bu konudaki işbirliği mekanizmalarının dahil edildiği süreç belirtilmiştir. Bu belge, Avrupa Birliği'nin "Büyük Ölçekli Siber Güvenlik Olayları Ve Krizlere Koordineli Şekilde Cevap Verilmesi Hakkında Komisyon'un Tavsiyesi" (Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises) isimli dokümanın eki niteliğindedir. Bu konuda orijinal metne ulaşmak için Bkz. https://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-6100-F1-EN-ANNEX-1-PART-1.PDF (Gözden Geçirilme Tarihi: 29.10.2020).

[494] ENISA programming document 2019-2021: https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-2019-2021 (Gözden Geçirilme Tarihi: 29.10.2020).

[495] GDPR orijinal metnine ulaşmak için Bkz. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (Gözden Geçirilme Tarihi: 29.10.2020).

[496] GDPR'a göre, GDPR'ın öngördüğü veri koruma kuralları tanımlanan veya tanımlanabilir tüm gerçek kişilere uygulanacaktır. (Başlangıç, 26. paragraf) Özellikle GDPR m.1'de Tüzüğün kişisel verilerin işlenmesi ve kişisel verilerin serbest dolaşımının korunmasının amaçlandığı belirtilmiş, 2. maddede içeriksel kapsamına dair ayrıntılı bir düzenleme öngörülmüş, 3. maddede ise GDPR'ın veri işleme faaliyetinin Avrupa Birliği sınırları dışında gerçekleştirilse dahi, veri sorumlusunun veya veri işleyenin Avrupa Birliği sınırları içerisinde kişisel veri işleme faaliyetleri açısından uygulanacağı belirtilmiştir.

amaçlanmıştır[497]. GDPR'ın temel amaçları, kişisel verilerin korunmasına yönelik daha yüksek standartlar benimsemek, AB veri koruma hukukunun teknolojik ve toplumsal gelişmelere uyumunu sağlamak ve birlik genelinde veri koruma hukukunun uygulamasını yeknesak hale getirmektir[498]. GDPR, salt Avrupa Birliği açısından değil tüm dünyada kişisel verilerin korunması alanında konu ile ilgilenen akademisyenler, hukukçular ve uygulamacılar açısından öngördüğü kurallar ve getirdiği sınırlamalar açısından önemli bir adım niteliğindedir. Elektronik ödemelerde siber güvenlik açısından konuya bakıldığında, GDPR gibi kişisel veriler alanında özellikle regülasyon noktasında yaşanan gelişmeler, hiç kuşkusuz siber güvenlik alanında atılacak adımlarla iç içe olup çoğu kez elektronik ödeme işlemlerine yönelik gerçekleştirilen siber ataklar neticesinde meydana gelebilecek veri sızıntılarının özellikle kişisel verilerin korunmasındaki menfaati de ihlal etmesi sebebiyle bu alandaki düzenlemeler ve alınacak tedbirler çoğu kez siber güvenliğin temin edilmesi noktasında da önem taşımaktadır. Bu kapsamda, kişisel verilerin korunması açısından kabul edilen genel ilkeler olan hesap verilebilirlik, şeffaflığın sağlanması ve güvenlik önlemlerinin alınmasının bilgi güvenliği dikkate alındığında, veri ihracını yasaklamaktan ziyade anılan ilkeler çerçevesinde hareket edilmesinin daha doğru bir yaklaşım olacağı kabul edilmektedir[499].

Ayrıca, konunun bu çalışmayı ilgilendiren siber güvenlik açısından dikkat çeken bir diğer önemli yönü ise, GDPR'da kişisel verilerin işlenmesi noktasında ağ ve bilgi güvenliğinin temin edilmesi açısından gerekli ve ölçülü birtakım önlemlerin alınması gerektiği düzenlenmiştir. Bu konuda, GDPR'da somut örnekler olarak depolanmış veya aktarılan kişisel verilerin her türlü yasa dışı ve zararlı girişimlere karşı ilgili bilgi güvenliği ve ağ güvenliği sistemlerinde özellikle söz konusu bilginin bütünlüğü,

[497] *FRA*, s. 11.
[498] Yusuf Mansur Özer, "Kişisel Verilerin Korunmasında Blok Zinciri Modeli: Vaatler Ve Hukuki Engeller", On İki Levha Yayıncılık, 1. Baskı, İstanbul, 2020, (*"Özer"*), s. 38.
[499] Armağan Ebru Bozkurt Yüksel, "Bulut Bilişimde Kişisel Verilerin Korunması", Yetkin Yayınları, Ankara, 2016, (*"Bozkurt Yüksel, Bulut Bilişimde Kişisel Verilerin Korunması"*), s. 169.

gizliliği, erişebilirliği açısından gerekli önlemlerin alınması ve bu konuda bilgi güvenliği olay müdahale ekiplerine (*computer security incident response teams*) gerekli her türlü bildirimin veri sorumlusu tarafından derhal yapılması gerektiği hüküm altına alınmıştır. Somut örnekler üzerinden konuya bakıldığında ayrıca GDPR'a göre elektronik sistemlerde her türlü izinsiz girişe izin verilmemeli, zararlı yazılımların kullanıcıların sistemlerine enjekte edilmesi engellenmeli, DoS saldırıları durdurulmalı ve bilişim ile elektronik iletişim sistemlerine yönelik her türlü zararlı ve yasa dışı eylem engellenmelidir[500].

4.2.6. Avrupa Konseyi'nin Kişisel Verilerin İşlenmesi Karşısında Bireylerin Korunması İçin Sözleşme ("Sözleşme 108")

1960'larda bilgi teknolojisinin ortaya çıkması ve 1970'lerin ortalarına gelindiğinde ise Avrupa Konseyi Bakanlar Komitesi'nin Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesine dayanarak kişisel verilerin korunması konusunda çeşitli kararlar vermesi neticesinde, 1981 yılında Kişisel Verilerin Otomatik Olarak İşlenmesi Karşısında Bireylerin Korunması Hakkında Sözleşme (*"Sözleşme 108"*) imzaya açılmış ve Sözleşme 01.10.1985 yılında Avrupa Birliği'ne üye devletler nezdinde yürürlüğe girmiştir. Türkiye'nin 28.01.1981 tarihinde Sözleşme 108 metnini ilk imzalayan ülkelerden birisi olmasına rağmen ancak Sözleşme 108 Türkiye Cumhuriyeti'nde 17.03.2016 tarihinde yürürlüğe girmiştir[501].

Sözleşme 108 içeriğine kısaca değinmek gerekirse, yargı ve kolluk kuvvetleri tarafından veri işleme dahil olmak üzere hem özel hem de kamu sektörleri tarafından gerçekleştirilen tüm veri işlemlerine uygulanır nitelikte olup Sözleşme 108'de esas itibariyle bireylerin, kişisel verilerin işlenmesine eşlik edebilecek suiistimallere karşı korunması ve aynı zamanda, kişisel verilerin sınır ötesi transferinin düzenlenmesi amaçlanmıştır. Sözleşme 108'de belirtilen ilkeler kısaca özellikle meşru ve amaca

[500] GDPR, Başlangıç, para. 26.
[501] *Sağıroğlu/Alkan*, s. 297.

yönelik olarak verilerin adil ve hukuka uygun şekilde toplanmasının ve otomatik işlenmesinin, bu verilerin niteliği ile orantılı olması ve doğru olması ile ilgilidir. Sözleşme 108'de ayrıca bireyin kendisine ait hangi bilgilerin saklandığını bilme ve gerektiği takdirde bireylerin hatalı olabilecek verilerin düzeltilmesini talep etme hakkı da düzenlenmiştir.

Sözleşme 108, 2001 yılında 181 Sayılı Ek Protokol ile genişletilmiş, bu kapsamda sözleşmeye taraf olmayan ülkelere yapılacak veri aktarımlarına yönelik bir kısım kurallar öngörülmüş ve ulusal düzeyde kişisel verilerin korunması mevzuatlarına uyumu temin etmek üzere taraf devletlerin denetleyici kurumlar oluşturulması zorunlu hale getirilmiştir[502]. Türkiye, 181 Sayılı Ek Protokolü 2016 yılında 6705 Sayılı kanun[503] ile iç hukukunda etkin kılmıştır[504].

4.2.7. Avrupa Konseyi'nin Kişisel Verilerin İşlenmesi Karşısında Bireylerin Korunması İçin Modernize Edilmiş Sözleşmesi ("Sözleşmesi 108+")

Sözleşme 108+, 18.05.2018 tarihinde yürürlüğe girerek yukarıda belirtilen Sözleşme 108'i içerik itibariyle değiştirmiştir.

Sözleşme 108+'nin temel amacının, Açıklayıcı Rapor'da, bireyleri, başkaları tarafından kişisel verilerinin işlenmesi noktasında bu durumu bilmek, anlamak ve kontrol etmek açısından gerekli güvencenin sağlanması olduğu anlaşılmaktadır[505].

---

[502] *Özer*, s. 36.
[503] 05.05.2016 tarihinde yayınlanan 29703 sayılı Resmi Gazete ile yürürlüğe giren 6705 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar Ve Sınıraşan Veri Akışına İlişkin Protokolün Onaylanmasının Uygun Bulunduğuna Dair Kanun" metnine elektronik ortamda ulaşmak için bkz. https://www.resmigazete.gov.tr/eskiler/2016/05/20160505-1.htm (Gözden Geçirilme Tarihi: 29.10.2020).
[504] *Özer*, s. 38.
[505] Sözleşme 108+, Açıklayıcı Rapor, s. 2.

Türkiye Cumhuriyeti'nin de taraf olduğu Sözleşme 108+'nin[506] elektronik ödeme sistemlerinde siber güvenlik kavramı açısından bu çalışmayı ilgilendiren düzenlemesi "Veri Güvenliği" başlıklı 7. maddedir. Bu düzenlemeye genel olarak bakıldığında veri güvenliği açısından, veri sorumlusu ve uygulanabilir durumlarda veri işleyenin hem teknik hem de organizasyonel nitelikteki özel güvenlik önlemlerini alması gerektiği[507] belirtilmiştir. Özel güvenlik önlemleri ile ilgili detaylı düzenlemelerin yer aldığı 7. maddede özetle güvenlik önemleri açısından veri işleme alanındaki veri güvenliği yöntem ve tekniklerinin mevcut durumunun göz önünde bulundurulması, bunların maliyetleri, potansiyel risklerin ciddiyeti ve olasılığı ile orantılı olması gerektiği, güvenlik önlemlerinin gözden geçirilmesi ve gerektiğinde güncellenmesi gerektiği ve güvenlik önlemlerinin birtakım risklerin önlemeyi amaçlarken bireylerin temel hak ve özgürlüklerine ciddi bir şekilde müdahale edebilecek bir veri ihlali yaşanması durumuna karşı özel bir yükümlülük içerdiği belirtilmiştir[508]. Sözleşme 108+ 7. madde düzenlemesini, konu açısından somutlaştırmak gerekirse elektronik ödeme sistemlerine yöneltilen siber saldırılar karşısında veri ihlali meydana gelmesi halinde veri sorumluları tarafından ilgili gözetim otoritesine iletilmesi gereken bildirim (i) ihlale konu olan olay, (ii) ayrıca ihlale ve olası sonuçlarına karşı alınan ve/veya önerilen önlemleri, (iii) mevcut ise diğer ek bildirimleri[509] içermektedir.

---

[506] Avrupa Konseyi'nin Kişisel Verilerin İşlenmesi Karşısında Bireylerin Korunması İçin Sözleşmesi ve Açıklayıcı Rapor'un Türkçe tercümesi için Bkz. https://itlaw.bilgi.edu.tr/tr/haberler/avrupa-konseyi-108-konvansiyonu-ve-aciklayici-rapo-90/ (Gözden Geçirme Tarihi: 08.12.2019).

[507] Sözleşme 108+'de teknik ve organizasyonel açıdan alınacak özel güvenlik önlemlerine örnek olarak birey için olası olumsuz sonuçlar, kişisel verilerin niteliği, işlenmiş kişisel verilerin hacmi, işleme için kullanılan teknik mimarinin saldırıya açıklık derecesi, verilere erişimi kısıtlama ihtiyacı, uzun süreli saklama ile ilgili şartlar vb. durumlar gösterilmiştir. Bkz, 108+, m. 7, para. 62.

[508] Sözleşme 108+, m. 7. para. 63 ve para. 64.

[509] Elektronik ödemelere yönelik gerçekleştirilen siber ataklarda çoğu kez veri sorumlulularının bireylerin korumakla yükümlü olduğu kimlik ve finansal bilgileri hedef alınmaktadır. Bu bağlamda, Sözleşme 108+ kapsamında veri sorumlusunun özellikle veri ihlalinin kimlik hırsızlığı, maddi kayıp, itibar kaybı gibi önemli bir riskle sonuçlanarak bireylerin hak ve özgürlükleri ile ilgili konularda önemli bir riskle karşı kaşıya kalınması halinde, ilgili kişilere bu durumu bildirmekle ilgili ek bildirimde bulunabileceği hüküm altına alınmıştır. Veri sorumluları, bu şekilde bir ihlal yaşanması halinde ilgili kişilere bildirimde bulunmakla beraber Sözleşme 108+ düzenlemesine göre, ihlalin olumsuz etkilerinin azaltılması konusunda temas noktaları ve olası önlemlerle ilgili yeterli ve anlamlı bilgiler sağlamak ihtiyacı duyulabilir. Daha da önemlisi, Sözleşme 108+, veri sorumlusunun veri ihlali halinde ilgili

4.2.8. eIDAS Tüzükleri ve 2020 Tarihli SSI eIDAS Hukuk Raporu

Elektronik ödeme sistemlerinde siber güvenlik denildiğinde, hiç kuşkusuz konunun merkezinde irdelenmesi gereken en önemli meselelerden birisi "güven"dir. Elektronik ödeme işlemlerinin gerçekleştirilmesinde güvenin temin edilmesi açısından ise, AB'nin en önemli regülasyonlarından birisi dijital işlemlerde güven tesis etmeye yarayan ve elektronik kimlik (*"eID"*) ve e-imza konularında detaylı düzenlemeler içeren Elektronik Kimlik ve Güven Hizmetleri Regülasyonu (*"eIDAS Regülasyonu"*)'dur[510].

Elektronik ödemelerde siber güvenlik bakımından çalışma kapsamında ele alınan ve güven noktasında teknik ve hukuki açıdan tartışmalı bir mesele olan blokzincir teknolojisi ve yeni nesil eID çözümleri gibi elektronik ortamda güven tesis etmeyi amaçlayan yeni teknolojilere, SSI eIDAS Hukuk Raporu çerçevesinde güven hizmetleri listesinde yer verildiği belirtilmiştir[511]. 2020 yılı Nisan ayında yayınlanan 138 sayfalık SSI eIDAS Hukuk Raporu[512]'nda, eIDAS'ın temel itibariyle Avrupa Birliği'nde Dijital Tek Pazar[513] stratejisi açısından önemli kurumlar olan "dağıtık defter teknolojisi" ve "dijital kimlik" hakkında ayrıntılı hukuki değerlendirmelere yer verilmiştir.

---

kişileri kendiliğinden bilgilendirmediği hallerde ihlalin olumsuz etkileri konusunda ilgili gözetim otoritesini, veri sorumlusundan bunu talep etmekle yükümlü kılmıştır. Bu konuda detaylı bilgi için bkz. Sözleşme 108+/m. 7/para. 66.

[510] *Keser Berber, Güven Hizmetleri,* s. 1.

[511] *Keser Berber, Güven Hizmetleri,* s. 3.

[512] Ignacio Alamillo Domingo, "SSI eIDAS Legal Report How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market" (Yazar tarafından "eIDAS güvenilir Dijital Tek Pazarda Dağıtık Defter Teknolojisine dayalı işlemler ve dijital kimliği hukuken nasıl destekleyecektir" şeklinde tercüme edilmiştir. (Çalışmada kısaca *"SSI eIDAS Hukuk Raporu"* olarak anılacaktır.) Söz konusu raporun orijinal metnine internet ortamında ulaşmak için Bkz. https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[513] AB'nin "Dijital Tek Pazar" stratejisi ile ilgili ayrıntılı bilgi, çalışmanın 4.2.4. başlıklı 2019/881 Sayılı Tüzük başlığı altında yer verilmiştir.

SSI eIDAS Hukuk Raporu ile ilgili çalışmayı ilgilendiren detaylı açıklamalara yer verilmeden önce, 19.02.2020 tarihinde Avrupa Komisyonu tarafından yayınlanan Dijital Strateji Belgesi'nde AB'nin dijital strateji hedeflerinden birisi de "Dijital Güvenlik (siber güvenlik ve mahremiyet)" olarak belirtilmiştir[514]. Bu noktada, elektronik ödemelerde siber güvenlik açısından bir üst başlık olarak düşünülmesi gereken "güven ve güvenlik" kavramları ve "güven hizmetleri", Avrupa Dijital Stratejisi'nin merkezinde yer almakta olup 2013 yılından itibaren siber güvenlik alanında rehberlik edebilecek bir dizi düzenleme ile (yukarıda belirtilen 2019/881 Sayılı Tüzük, GDPR ve e-Gizlilik (*e-Privacy*) taslağı[515] gibi) düzenlenmesi amaçlanmıştır[516]. AB sınırları içerisinde elektronik ödeme işlemlerinin güvenli bir şekilde gerçekleştirilmesi açısından elektronik imza sistemi, güvenli elektronik ticaret bu kapsamda yukarıda belirtilen AB regülasyonlarının yanı sıra özellikle eIDAS Regülasyonu çerçevesinde detaylı şekilde düzenlenen konulardandır[517]. Ayrıca, bu çalışma kapsamında belirtmek gerekir ki, siber güvenlik ve güven, Dijital Avrupa 2021-2027 Programı[518] (*Digital Europe*) Recital 24'de spesifik olarak ulaşılması gereken beş hedeften birisi olarak gösterilmiştir[519].

---

[514] *Keser Berber, Güven Hizmetleri,* s. 12.

[515] Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Revealing Directive 2002/58/EC. Orijinal metin için: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52017PC0010 (Gözden Geçirilme Tarihi: 29.10.2020).

[516] Konu ile ilgili AB regülasyonları hakkında detaylı bilgi için bkz. *Keser Berber, Güven Hizmetleri,* s. 25.

[517] *Keser Berber, Güven Hizmetleri,* s. 25.

[518] Dijital Avrupa 2021-2027 Programı (*Digital Europe*), Recital 24'ü orijinal İngilizce metinden Türkçe'ye tercüme etmek gerekirse: "Güven, Dijital Tek Pazar'ın işlerlik kazanabilmesi açısından ön koşuldur. Dijital kimlikler, kriptografi, mahremiyet ihlalinin tespiti veya bu olgunun finans, endüstri 4.0, enerji, taşımacılık, sağlık veya e-devlet hizmetleri gibi alanlarda uygulanması güvenliğin temin edilmesi ve vatandaşlar, kamu kuruluşları ve şirketler arasındaki online aktivitelerde güvenin sağlanması bakımından önem taşımaktadır." (Serbest Çeviri). Bkz. Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027 COM/2018/434 final – 2018/0227 (COD), (*"Digital Europe"*), s. 18. Söz konusu orijinal metne internet ortamında ulaşmak için: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A434%3AFIN (Gözden Geçirilme Tarihi: 29.10.2020).

[519] *Keser Berber, Güven Hizmetleri,* s. 26.

SSI eIDAS Hukuk Raporu ise içerik itibariyle (AB sınırları içindeki) sınır-ötesi işlemler açısından elektronik kimliklendirmenin hukuken ne anlama geldiği, elektronik imza ve elektronik mühür ile güven hizmetleri bakımından hukuki rejimin nasıl düzenlemesi gerektiğine ilişkin önemli sayılabilecek bazı tespitlere yer verilmiştir. Bu bahsi geçen hususlara rapor kapsamında kısaca değinmek gerekirse:

Dijital Kimlik (Electronic Identification)

SSI eIDAS Hukuk Raporu'nda "dijital kimlik" (e-ID) kurumu[520], bu kuruma uygulanacak hukuki rejim kurumsal veya sosyal ağ hizmet sağlayıcılarının desteği ile kişilerin internet ortamında yaratmış oldukları ve kullanıcı konumda oldukları kişilik haklarının korunması perspektifinden ele alınmıştır. Bu bağlamda, ağ içindeki kullanıcıların kişilik hakları üçüncü tarafların yönetimine karşı hukuki rejim olarak üç kavram çerçevesinde düzenlenmiştir: (i) kimlik, (ii) mahremiyet, (iii) hukukun icra edilebilirliği[521].

DLT Ve Bağımsız Kimlik (DLT & Self-Sovereign Identity):

DLT (*Distributed Ledger Technologies*)[522] terminolojisi, blokzincir teknolojisinde kullanıcıların merkezi olmayan bir sistem üzerinden, açık anahtar kriptolojisi (*public key cryptography*) üzerinden erişim sağlanan, paydaşların verdikleri onay sonucunda işlemin tasdik edildiği ve bu kaydın her paydaşın onaylaması sonucunda sistemde kaydedildiği imkanı ifade etmekte olup blokzincir teknolojisi ile neredeyse özdeşleşmiş bir kavramdır[523]. Raporda SSI denilen bağımsız kimlik kavramının (*self-*

[520] eIDAS Regülasyonu m. 3/f. 1 kapsamında, "elektronik kimlik tespiti", gerçek ya da tüzel kişiliği temsil eden gerçek bir kişiyi elektronik ortamda benzersiz biçimde temsil eden kimlik doğrulama süreci olarak tanımlanmıştır. Ayrıca, elektronik kimlik konusunda kapsamlı bilgi için bkz. https://ec.europa.eu/digital-single-market/en/e-identification (Gözden Geçirilme Tarihi: 29.10.2020).
[521] *SSI eIDAS Hukuk Raporu*, s. 8.
[522] İngilizce'deki bu kavram Türkçe'ye "Dağıtık Veri Tabanı Teknolojisi" olarak tercüme edilebilir (Serbest Çeviri).
[523] *SSI eIDAS Hukuk Raporu*, s. 12.

sovereign identity)[524] ise gerçek kişilerin kendiliğinden belirlenmesi (*self-determination*) ve kişisel bağımsızlık (*personal-autonomy*) kavramları ile yakından ilintili olduğu belirtilerek özellikle DLT teknolojisinin dijital kimliklendirme bakımından en azından gerçek kişilerin bağımsız şekilde belirlenerek kişilik haklarının elektronik ortamda uygulanması noktasında önemli bir rolü olabileceğine dikkat çekilmiştir[525].

Güven Yönetimi (Trust Governance):

SSI eIDAS Hukuk Raporu'nda ayrıca "güven yönetimi" adı verilen süreç açısından Batubara, Ubacht ve Jansenn isimli bazı akademisyenlerin özellikle blokzincir teknolojisinin e-devlet uygulamalarına uyumlu hale getirilmesi bakımından bazı sorunlar bulunduğu ve bu bağlamda hukuken gerekli desteğin verilerek yeni yönetim çerçevelerinin belirlenmesi gerektiği ifade edilmektedir[526]. Bahsi geçen yazarlara göre, blokzincir teknolojisinin güvenlik, ölçeklendirebilirlik, işlerlik, güvenilirlik ve esneklik ilkelerini hayata geçirebileceği e-devlet uygulamaları açısından genel bir platformun bulunmaması, bu konuda e-devlet süreçleri açısından spesifik gerekliliklerin belirlendiği ve tasarım mimarisi açısından düzgün bir mimari çözüm gerektiği ve blokzincir teknolojisinin faydalarından yararlanmak açısından bu bağlamda dikkatli şekilde belirlenmesi gereken hukuki çerçevelerin ve yönetim gerekliliklerinin birçok belirsizliğin aşılması konusunda çözüm olabileceği raporda özellikle dikkat çeken hususlardandır.

---

[524] Kendiliğinden bağımsız kimlik (*self-sovereign identity*), kullanıcıların kendi hesap bilgilerini oluştururken herhangi bir aracı veya merkezi kuruluştan hesaplarının açılması konusunda herhangi bir onaya tabi tutulmaksızın kendi kişisel bilgilerinin paylaşımı ve kullanımı konusunda tam bir hakimiyeti haiz olarak kimlik oluşturma sürecini ifade etmektedir. Bu konuda ayrıntılı bilgi için bkz. "eIDAS Supported Self-Soverein Identity" başlıklı yazı, s.1, ilgili yazıya internet üzerinden ulaşmak için bkz. https://ec.europa.eu/futurium/en/system/files/ged/eidas_supported_ssi_may_2019_0.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[525] *SSI eIDAS Hukuk Raporu*, s. 12-21.

[526] *SSI eIDAS Hukuk Raporu*, s. 12'den aktarılan: Batubara, F., Ubacht, J., & Jansenn, M. (2018).

Özellikle elektronik ödeme işlemlerinde siber güvenlik açısından önem taşıdığı düşünülen ve yukarıda kısaca özetlenen kavramlarla beraber raporda bahsi geçen bazı eIDAS düzenlemeleri hakkında da kısaca dikkat çeken tespitler şunlardır:

Yukarıda belirtilen eIDAS Regülasyonu[527] internet ağındaki gerçek ve tüzel kişilerin Avrupa Birliği ve Avrupa Ekonomik Alanı sınırları içerisinde haklarının korunması açısından güven çerçevesini oluşturan ve kişilerin haklarını bu bağlamda yargısal açıdan güvence altına alan önemli bir kilometre taşı niteliğindeki ilk düzenlemelerden birisidir[528].

eIDAS Regülasyonu m. 1/a'da üye devletlerin, elektronik kimliğin AB'ye üye devletlerin hangi koşullar altında gerçek ve tüzel kişiler bakımından elektronik kimliği tanıyacağı, bazı elektronik işlemler açısından güven hizmetlerinin[529] teminin sağlanabilmesi amacıyla kuralların öngörüldüğü, elektronik imza[530], elektronik

[527] eIDAS Regülasyonu, İngilizce'de *"The Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market"* olarak belirtilmektedir. İlgili tüzükle ilgili internet ortamında orijinal metne ulaşmak için: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN (Gözden Geçirilme Tarihi: 28.05.2020). İlgili Tüzük metninin Türkçe tercümesi için bkz. *Keser Berber, Güven Hizmetleri*, s. 239-276.

[528] eIDAS kapsamında yasal açıdan hem nitelikli hem de niteliksiz güven hizmetleri, mahkemeler nezdinde delilde ayrımcılık yapmama kuralından yararlanır, başka bir ifadeyle güven hizmetleri hâkim tarafından sadece elektronik ortamda bulunduğu gerekçesi reddedilemez. Bu konuda ayrıntılı bilgi için bkz. *Keser Berber, Güven Hizmetleri,* s. 41-42.

[529] Keser Berber, güven hizmetlerinin güvenilecek teknolojiler olarak kavramlaştırılabileceğini ve kullanıcının dâhil edildiği bir süreçte, güven hizmetini, aslında yeterince güvenli ve güvenilir olarak tanıması gerektiğini belirtmiştir. Keser Berber'e göre, eIDAS'ın yaklaşımı, bu hizmetlere duyulan güvenin yalnızca kendi teknik özelliklerinden ziyade, yasal olarak düzenlenmiş olmasından kaynaklanması anlamında önemli olanın güçlendirilmiş bir güven hizmetleri düzeyinin oluşturulmasıdır. Bkz. *Keser Berber, Güven Hizmetleri*, s. 32.

[530] eIDAS m. 25/f. 1 uyarınca bir elektronik imzanın hukuki işlemlerde delil olarak hukuki etkisi ve kabul edilebilirliği, yalnızca elektronik biçimde olduğu veya nitelikli elektronik imzaların şartlarını karşılamadığı için reddedilemez.

mühür[531], elektronik zaman damgası[532], elektronik teslimat hizmetleri[533] ve web sitesi onayları açısından sertifikasyon hizmetleri[534] ile ilgili bir hukuki çerçeve belirlenmiştir.

Raporda özellikle eIDAS Regülasyonu'nun yukarıda belirtilen SSI teknolojisinin kullanımı açısından özellikle elektronik kimliklendirmenin ne anlama geldiği, elektronik imza ve elektronik mühür ile iç pazardaki işlemler açısından güven hizmetlerinin hukuki rejimi konusunda önemli düzenlemeler içerdiği üzerinde durulmuştur.

Rapor içeriğinde ayrıca Avrupa Komisyonu'nun (EU) 2015/1502 Sayılı ve 08.10.2015 Tarihli elektronik kimliklendirme aşamalarının temininde asgari teknik özelliklerin ve usullerin belirlenmesine yönelik Tüzük'e (*"eIDAS Güvenlik Tüzüğü"*)[535] de değinilmiştir. eIDAS Güvenlik Tüzüğü'nün ise, özellikle bahsi geçen tüzüğün Başlagıç bölümündeki 2. paragrafında elektronik kimliklendirme konusunda güven katmanın sağlanması noktasında özellikle birlikte çalışabilirliğin (*interoperability*)[536]

---

[531] eIDAS'taki tanıma göre, elektronik mühür, elektronik formdaki başka bir verinin kaynağını ve doğruluğunu sağlamak açısından, elektronik formdaki başka bir veriye eklenen veya böyle bir veri ile mantıksal bir bağlantısı olan elektronik formdaki bir veriyi ifade eder. Elektronik mühür sadece veri/belgelerin kaynağını ve bütünlüğünü doğrulamak için tüzel kişiler tarafından düzenlenebilir ve kullanılabilir. Bu konuda detaylı bilgi için bkz. *Keser Berber, Güven Hizmetleri*, s. 118 vd.

[532] Elektronik zaman damgası, bir verinin belirli bir zamanda var olduğunu ispatlamak maksadıyla, veri ile tarihi birbirine bağlayan elektronik formdaki bir veridir. Bkz. *Keser Berber, Güven Hizmetleri*, s. 153.

[533] eIDAS Regülasyonu m. 43 kapsamında kayıtlı elektronik posta hizmetlerinin hukuki etkisi, m. 44 gereğince ise nitelikli elektronik kayıtlı teslimat hizmetleri için isterler kapsamında ayrıntılı düzenlemelere yer verilmiştir. Ayrıca bu konuda detaylı bilgi için bkz. *Keser Berber, Güven Hizmetleri,* s.155-158.

[534] Nitelikli web sitesi doğrulama sertifikaları (QWAC) konusunda detaylı bilgi için bkz. *Keser Berber, Güven Hizmetleri*, s. 158-172.

[535] Yukarıda kısaca eIDAS Güvenlik Tüzüğü olarak belirtilen düzenleme İngilizce'de*"Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) Nº 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market"* olarak belirtilmektedir.

[536] "İnteroperability" sözcüğü İngilizce'de ortak çalışma, karşılıklı kullanabilirlik veya birlikte çalışabilirlik gibi kavramlar için kullanılmaktadır. (Bkz. https://dictionary.cambridge.org/dictionary/english/interoperability, Gözden Geçirilme Tarihi: 22.07.2020). Yukarıda yer alan açıklamalar açısından Türkçe'ye en iyi "birlikte çalışabilirlik" teriminin

sağlanması açısından ortak anlayışın temin edilebilmesi için asgari düzeyde uygulanması gereken teknik gerekliliklerin, standartların ve prosedürlerin neler olduğunun belirlenmesinin amaçlandığı belirtilmiştir.

4.3. ELEKTRONİK ÖDEME SİSTEMLERİNDE SİBER GÜVENLİK İLGİLİ AMERİKA BİRLEŞİK DEVLETLERİ'NDEKİ YASAL DÜZENLEMELER

Bilindiği üzere, ABD başta kripto para birimleri olmak üzere dünyada elektronik ödeme sistemlerine yönelik yeni eğilimler konusunda özellikle birçok farklı teknolojik alanda (özellikle yazılım teknolojisinde dönüm noktası olarak kabul edilen 2007 yılı ve sonrasında) öncü ülke olma özelliğine sahiptir[537]. "GAFAM" şeklinde ifade edilen Google, Amazon, Facebook, Apple ve Microsoft gibi dünyada teknolojik alanda öncü şirketler Amerikan menşeli olup elektronik ödemeler de dahil olmak üzere birçok teknolojik atılıma ve inovasyona bu şirketler yön vermektedir. Özellikle elektronik ödeme endüstrisinin siber saldırılar karşısında kırılgan ve hassas yapısı dikkate alındığında, elektronik ticaretin başarısı ve Covid-19 pandemi salgını döneminde bu alanda dijitalleşmede sistemin güvenilir olduğu kanısı uyandırılması bir ihtiyaçtır.

---

uygun olacağı değerlendirilmiştir. Bu kapsamda, doktrinde Keser Berber tarafından Avrupa Komisyonu'nun "Dijital Tek Pazar Stratesi" noktasında uygulamaya alınan "European Interoperability Framework" kapsamında şu somut önerilerin sunulduğu belirtilmiştir: (i) Birlikte çalışabilirlik faaliyetlerine ilişkin yönetişim yapısının nasıl geliştirileceği, (ii) kurumlar arasındaki ilişkilerin ne şekilde oluşturulması gerektiği, (iii) uçtan uça dijital hizmetlerin sunulmasını destekleyen süreçlerin nasıl kolaylaştırılabileceği, (iv) mevcut ve yeni regülasyon çalışmalarının, birlikte çalışabilirliğin sağlanmasına yönelik çalışmaların önüne geçmeksizin nasıl yürütülebileceği. Bu konuda detaylı bilgi için bkz. *Keser Berber*, *Güven Hizmetleri,* s. 23-24.

[537] Thomas L. Friedman, "Geciktiğin İçin Teşekkür Ederim" adlı kitabında, özellikle 2007 yılının ABD açısından yazılım teknolojisi bakımından dönüm noktası olduğunu, Steve Jobs'un 9 Ocak 2007 tarihinde Moscone Center'da mobil telefonları baştan icat ettiğini duyurduğunu, Hadoop adlı şirket sayesinde programlama ve hesaplama yapmak için depolama kapasitesinde bir patlama yaşandığını, büyük verinin (big data) herkes açısından mümkün hale geldiğini, anılan yılda GitHub adlı açık-kaynaklı bir platform üzerinde gelişmeler yapılmaya başlandığı, bloglama şirketi olan ve büyük bir startup'ın parçası olan Twitter'ın kendi başına ayrı bir platform olarak ortaya çıktığını, popüler bir sosyal mobilizasyon sitesi olan change.org'un da 2007 yılında ortaya çıktığı, akıllı telefonların küresel ölçekte yayılmasına yardımcı olan bir açık-standartn platformu olan Android'in aynı yıl hayata geçtiğini belirtmiştir. Bu konuda detaylı bilgi için bkz. Thomas L. Friedman, "Geciktiğin İçin Teşekkür Ederim", Boyner Yayınları, 2018, İstanbul, (*"Friedman"*), s. 21-32.

ABD'de bilişim suçları ile mücadele açısından ve bu suçların önlenmesi için yürürlüğe giren her hukuki düzenleme ile ilgili bir sivil toplum hareketi doğmaktadır[538].

ABD elektronik ödeme sistemlerinde siber güvenlikle ilgili en çok çalışma yapan ülkelerden birisi olup ABD'de bilişim suçları ve siber güvenlikle ilgili düzenlemelerin yanı sıra, siber suçlulukla mücadele eden özel birimlerin kurulduğu, bu birimlerin teknik araçlarla donatılarak yapılandırılmalarının sağlandığı, üniversitelerde de bu kapsamda akademik çalışmalar yapıldığı ve özellikle akademik çevrelerin dışında birçok kamu kurum ve kuruluşunda da siber suçlarla mücadele etmek için eğitim veren birimlerin çalıştığı bilinmektedir[539]. Bunun dışında, ABD Savunma Bakanlığı'nın 2018 yılı Siber Strateji Belgesi Özeti'nde ABD'nin siber güvenlik konusunda yaklaşımının, siber uzayda başta Çin ve Rusya olmak üzere bazı devletlerle "aktif rekabet gerektiren" bir alan olarak görüldüğü anlaşılmaktadır[540].

---

[538] *Dülger, Bilişim Suçları,* s. 214'de 375 no'lu dp.da belirtilen Karagülmez.

[539] Bu birimlere örnek olarak, ABD'de FBI National Infrastructure Protecture Center, Information Technology Association of America, Trap and Trace Center Authority, Carnegie Mellon's Emergency Response Team sayılabilir. Ayrıca, ABD'de üniversitelerde de bu hususla ilgili çalışmalar yapılmakta, sadece akademik ortamda değil, birçok farklı kamu kurum ve kuruluşu nezdinde de siber suçlarla mücadele etmek için eğitim veren birimler çalışmaktadır. Bu konuda en üst merci olan Adalet Bakanlığı bünyesinde teşekkül eden "Computer Crime and Intellectual Property Section' (*CCIPS*)" adlı birim siber güvenlik alanında çalışmakta, eğitim faaliyetleri vermekte, siber güvenlikle ilgili uzman yetiştirmekte ve diğer kamu kurumlarıyla işbirliği içerisinde siber suçluluğun önlenmesi çalışmaları yapmaktadır. Bkz. *Erdem/Özocak2*, s. 197'deki 206 no'lu dp.da belirtilen Dülger ve Karagülmez.

[540] Amerikan Savunma Bakanlığı'nın yayınlamış olduğu 2018 tarihli Strateji Belgesi Özeti'nde özellikle siber güvenlik noktasında diğer devletlerle arasındaki stratejik ilişki bakımından bazı dikkat çekici tespitlere yer verilmiştir. İlgili strateji belgesinde ABD'nin, özellikle Çin ve Rusya ile uzun-dönemli ilişkiler açısından stratejik bakımından rekabet içinde oldığı belirtilmiştir. Bu devletlerin, ABD ile müttefik olmasına rağmen, aynı zamanda ABD halkına stratejik açıdan risk teşkil edecek şekilde siber uzayda düzenli kampanyalar gerçekleştirdiğine dikkat çekilmiştir. ABD'nin bakış açısına göre, Çin ABD'deki kamu kuruluşları ve özel sektördeki şirketlerden düzenli olarak veri sızıntısı sağlayarak ABD'nin askeri üstünlüğüne ve ABD halkının ekonomik refahına zarar veren faaliyetlerde bulunmaktadır. Rusya ise siber kaynaklı bilgi operasyonları ile ABD halkını etkilemeye çalışarak ABD'nin demokratik süreçleri ile mücadele halindedir. Siber alanda, ABD'nin diğer aktörler olarak belirttiği devletler İran ve Kuzey Kore olup bu devletler de ABD vatandaşlarına zarar verici eylemlerde bulunmakta ve ABD çıkarlarını tehdit etmektedir. Bu bağlamda ABD'nin siber uzayda bağımsızlığının her vatandaşı ve askeri alandaki faaliyetleri için her geçen gün kaçınılmaz bir gerçek olduğuna dikkat çekilmiştir. Detaylı bilgi için ilgili strateji belgesine aşağıdaki link üzerinden ulaşılabilir: https://afyonluoglu.org/PublicWebFiles/strategies/America/USA%202018%20DoD%20Cyber%20Security%20Strategy.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

Ayrıca, ABD'nin siber güvenlik alanındaki bir diğer özelliği ise ABD, Avrupa Konseyi üyesi olmamasına rağmen, Avrupa Siber Suç Sözleşmesi'ni imzalayıp usulüne uygun şekilde onaylayarak Avrupa Konseyi Genel Sekreterliği'ne depo etmiştir. Bunun neticesinde, Avrupa Siber Suç Sözleşmesi'nin kendi iç hukuk sisteminde yürürlüğe girdiği ve hukuken bağlayıcılığı bulunduğu kabul edilmiştir[541].

ABD'deki hukuk sistemi Avrupa Birliği'ndeki farklı olarak "Common Law" (Anglo-Amerikan Hukuk geleneği) sistemi geçerli olması sebebiyle elektronik ödeme sistemlerindeki siber güvenlik alanında konuya AB'de yürürlükte olan mevzuattan farklı şekilde yaklaşılması gerekecektir[542]. Bu itibarla, ABD'de elli tane eyalet söz konusu olup her eyaletin diğerinden farklı hukuk düzenlemeleri bulunmakta ve merkezi konumdaki federal devlet yasaları da belirli açılardan Common Law sisteminin uygulandığı eyaletlerin federe yasalarından farklılık göstermektedir. Bu nedenle, çalışmada ABD'ye ilişkin elektronik ödeme sistemlerinde siber güvenlikle ile ilgili düzenlemeler[543] öncelikle iki alt başlığa ayrılarak ilk alt başlıkta siber güvenlikle ilgili ABD federal yasaları[544], ikinci alt başlıkta ise Kaliforniya Eyaleti'nde olduğu gibi elektronik ödeme sistemlerinde siber güvenlikle ile ilgili bazı eyalet yasaları incelenecektir.

Elektronik ödeme sistemlerinde siber güvenlik konusunda ABD'deki regülasyonlarla ilgili değerlendirmelere geçilmeden önce kısaca ABD'nin siber güvenlik tarihçesi konusunda aşağıda kısaca şu açıklamalara yer verilmiştir:

---

[541] *Dülger, Bilişim Suçları,* s. 214.

[542] ABD'de uygulanan "Common Law" hukuk sistemi ile İngilizce'de "Civil Law" olarak ifade edilen Kıta Avrupası hukuk sistemi ile ilgili farkların ne olduğu konusunda detaylı bilgi için Bkz. "The Common Law And the Civil Law Traditions", Berkeley Law School: https://www.law.berkeley.edu/wp-content/uploads/2017/11/CommonLawCivilLawTraditions.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[543] ABD'de bilişim suçları ile ilgili detaylı bilgi konusunda bkz. *Dülger*, *Bilişim Suçları,* s. 632, 633.

[544] ABD'de siber güvenlikle ilgili federal yasalar konusunda ayrıntılı bilgi için bkz. Eric A. Fischer, "Federal Laws Relating to Cyber Security: Overview of Major Issues, Current Laws, and Proposed Legislation", Congressional Research Service, Aralık, 2014 (*"Eric Fischer"*): https://www.everycrsreport.com/reports/R42114.html (Gözden Geçirilme Tarihi: 29.10.2020).

4.3.1. ABD Siber Güvenlik Tarihçesi

Gizlilik ve mahremiyet konusuda ABD'de ilk federal düzeyde uygulanan yasa, 1974 Sayılı Mahremiyet Yasası (*The Privacy Act of 1974*)'dır [545]. Anılan yasa hükümleri, ABD'de federal kuruluşlar tarafından kişilere ait tanımlanan verilerin toplanması, kullanılması, işlenilmesi ve temin edilmesi ile ilgili kuralları düzenlemektedir. Dünyada kişisel verilerin korunması alanında ilk düzenlemelerden birisi olan bu yasa ile "kayıtlar sistemi" (*system of records*)[546] denilen ve kişisel verilerin yazılı onay sonucunda ancak Federal Sicil Kaydı'nda (*Federal Register*) kaydedilmesini ve ilgili kişilerin onayı olmaksızın ifşa edilmemesini zorunlu kılmaktadır. Ayrıca, ABD Mahremiyet Yasası'na göre isimleri ile sisteme kaydedilmiş kişilerin, kendilerine ait bilgiyi inceleyebilme ve bu bilgilerde herhangi bir yanlışlık görmesi halinde bu verileri düzeltme hakkı olduğu belirtilmiştir.

Siber güvenliğin sağlanmasında en etkin kurumlardan birisi olan ABD Savunma Bakanlığı[547] (*"Department of Defence"* veya *"DoD"*) tarafından 2011 yılında "Siber Uzay Faaliyetlerine Yönelik Savunma Stratejileri" (*"Department of Defense Strategy for Operating in Cyberspace"*) belgesi[548] yayınlanmıştır[549]. 2015 yılında ise, ABD

---

[545] 5 U.S. Code § 552a: https://www.law.cornell.edu/uscode/text/5/552a (Gözden Geçirilme Tarihi: 29.10.2020).

[546] Kayıt sistemi, herhangi bir bireyi adının veya o kişiyi tanımlayabilecek herhangi bir bilginin, sembolün veya o bireye ilişkin herhangi bir ayırt edici özellikle taşıyacak şekilde bir kuruluş tarafından bilgi temin edilmesi halinde o kuruluşun bu bilgi veya bilgilerin kaydı konusundaki kontrol sistemi olarak tanımlanmaktadır. Bkz. 5 U.S. Code § 552a/5: https://www.law.cornell.edu/uscode/text/5/552a (Gözden Geçirilme Tarihi: 29.10.2020).

[547] https://www.defense.gov/news/d20110714cyber.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[548] Söz konusu rehberin, internette tam metnine ulaşmak için bkz. https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[549] Söz konusu rehberde, siber güvenlik konusunda beş temel amaç çerçevesinde hareket edilmesi gerektiğini belirtilmiştir: (i) Öncelikle siber uzaya da operasyonel açıdan etkin faaliyet gösterilecek bir alan olarak bakılacaktır, (ii) DoD ağlarının ve sistemlerinin korunması açısından gerekli savunma stratejileri etkin şekilde uygulanacaktır. (iii) Siber güvenlik alanında bütünsel devlet stratejisinin hayata geçirilebilmesi açısından bu konuda özel ve kamu sektöründe tüm kuruluşlar ile gerekli işbirliğine gidilecektir, (iv) Uluslararası alanda kollektif siber güvenlik işbirliğine gidilmesi açısından bu alandaki tüm müttefiklerle birlikte hareket edilecektir, (v) Siber güvenlik yetkinliğinin geliştirilebilmesi açısından bu alanda teknolojik innovasyon desteklenecektir. Rehberle ilgili detaylar konusunda bkz. Piret

Savunma Bakanlığı tarafından 2011 yılında yayınlanan "Siber Uzay Faaliyetlerine Yönelik Savunma Stratejileri" belgesinin yenilendiği görülmüştür. 2015 yılında çıkarılan strateji belgesi içerik olarak 2011 tarihli rehbere benzemekle beraber, 2011 yılındaki belgede ABD'nin siber güvenliği sağlamada daha savunmacı olduğu, 2015 yılındaki belgede ise 2011 yılından farklı olarak siber güvenliği temin noktasında ABD hükümetinin bazı durumlarda (ABD'nin kendi ülkesinde savunma sistemlerine atak yapılması ve yasaların izin verdiği ölçüde siber riskleri azaltmak maksadıyla ABD Başkanın veya Savunma Bakanı'nın onayı alınmak kaydıyla) "geri sızma"[550] denilen siber operasyonlar yürütebileceği açıkça ifade edilmiştir[551]. Savunma Bakanlığı dışında, ABD'de siber güvenliğin yeknesak olarak uygulanması açısından bazı standartları ve kuralları düzenleyen önemli bir diğer kurum NIST'dir. NIST[552], ABD'de özellikle siber güvenlik alanında "Cyber Security Framework" olarak bilinen siber güvenlik alanında hangi standartların ve kuralların yeknesak şekilde uygulanması gerektiğine ilişkin siber güvenlik çerçeve metinleri yayınlamaktadır[553]. ABD'de ulusal ve ekonomik güvenliğin güvenilir şekilde sağlanabilmesi açısından yayınlanmış olan

---

Pernik/Jesse Wojtkowiak/Alexander Verschoor-Kirss, National Cyber Security Organisation: United States, NATO Cooperative Cyber Defence Center of Excellence, Talinn, 2016, (*"Pernik Ve Diğerleri"*) ilgili makaleye internet ortamından ulaşmak için: https://ccdcoe.org/uploads/2018/10/CS_organisation_USA_122015.pdf(Gözden Geçirilme Tarihi: 29.10.2020).

[550] Bu noktada, siber güvenlik alanında aktif savunma ve geri sızma kavramlarının konuyu ilgilendirmesi sebebiyle kısaca açıklanmasında fayda görülmüştür: Siber güvenlikte her iki kavram birbirinden farklı kavramlar olup "aktif savunma *(active defense)*" dost güç ve varlıklara yöneltilen siber tehdidi ortadan kaldırmak, boşa çıkarmak ya da zayıflatmak için başvurulan bir doğrudan savunma yöntemidir. "Geri hack'leme" veya "geri sızma *(reverse hacking)*" ise, saldırganın yaptığı siber saldırı neticesinde ona fark ettirmeden saldırganın sistemine enjekte edilebilecek bir zararlı yazılım sayesinde saldırganı zafiyete uğratmak için gerçekleştirilen siber ataktır. Geri sızmanın, aktif savunmadan en büyük farkı savunmadan ziyade bir siber atak olmasıdır. Bu konuda detaylı bilgi için bkz. Scott Berinato, "Aktif Savunma Ve Geri Hack'leme, Bir Başlangıç", Harvard Business Review Press, Dijital Dönüşüm Siber Güvenlik, (*"Berinato"*), s. 137-174.

[551] https://www.justsecurity.org/69119/the-defense-departments-measured-take-on-international-law-in-cyberspace/ Ayrıca, 2015 yılındaki ABD Savunma Bakanlığı'nın Siber Strateji Belgesi'ne ulaşmak için: https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[552] NIST'in İngilizce'de açılımı "National Institute of Standards and Technology"dir. Türkçe'ye "Ulusal Standartlar ve Teknoloji Enstitüsü" olarak tercüme edilebilir (Serbest Çeviri). ABD'de Ticaret Bakanlığı'na bağlı olarak çalışan bir kurumdur.

[553] https://www.nist.gov/cyberframework/framework (Gözden Geçirilme Tarihi: 29.10.2020).

13636 Sayılı Başkanlık Kararı gereğince, NIST aynı zamanda ABD'de siber güvenlik noktasında kritik altyapıların geliştirilmesi ve bu kritik altyapılara ilişkin siber güvenlik risklerini azaltmak amacıyla yol gösterici nitelikteki bazı standartları, kuralları ve tavsiye niteliğindeki uygulama örneklerini ortaya koymak amacıyla 2013 yılında Şubat ayında kurulmuştur. NIST'in siber güvenlik noktasındaki faaliyetleri ise, özellikle 2014 yılında ABD'de yürürlüğe giren Siber Güvenliğin Geliştirilmesi Kanunu ile daha da netlik kazanmıştır[554].

4.3.2. Elektronik Ödeme Sistemlerinde Siber Güvenlikle İlgili ABD Federal Devlet Yasaları

ABD'deki elektronik ödeme sistemlerine ilişkin düzenlemelere bakıldığında[555], ATM'lerden POS ödemelerine ve kredi kartı ile debit kart ödemeleri de olmak üzere birçok yasal düzenlemenin bulunmakta, federal düzeyde uygulanan bazı düzenlemeler olduğu gibi eyaletlere yönelik olarak da farklı yasal düzenlemeler yer almaktadır[556]. Buna ilaveten, bankalar arasındaki ödeme işlemleri açısından "Federal Reserv"[557]

[554] https://www.nist.gov/cyberframework/new-framework (Gözden Geçirilme Tarihi: 29.10.2020).

[555] Çalışma kapsamında yukarıda ABD'deki ödeme sistemlerine ilişkin açıklamalar BIS, "Payments in the United States", CPSS - Red Book – 2003 (*"BIS"*) isimli kaynaktan özetlenerek aktarılmıştır. Bu konuda orijinal kaynağa internet ortamından ulaşmak için Bkz. https://www.bis.org/cpmi/paysys/unitedstatescomp.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[556] Tüketicilerin elektronik ortamda gerçekleştirdikleri ödeme işlemleri ve ATM ile POS gibi yöntemler sayesinde gerçekleştirilen fon trasferi gibi işlemler açısından 1978 tarihli "Elektronik Fon Transferi Yasası" ("Electronic Fund Transfer Act" veya kısaca *"EFTA"*) ile FED'in "Regülasyon E" (Regulation E) denilen yönetmelik hükümleri uygulanmaktadır. Söz konusu bu düzenlemeler ile finansal kapanışlar, kart çıkarılmasına yönelik düzenlemeler, kartlı ödeme sistemlerine giriş gibi birçok konuda farklı standartlar ve düzenlemeler öngörülmektedir. Bunun dışında, tüketicilerin elektronik fon transfer işlemleri ile ilgili ABD'de federal düzeyde uygulanan yasal düzenlemeler "Tüketicilerin Para Birimlerinin Korunmasında Finansal Denetleyiciler Hakkında Kanun" (*Comptroller of the Currency's Consumer Protection Guidelines*), FED'in Regulation Z'denilen ve diğer adıyla "Borçlandırmada Doğruluk Kanunu" (*Truth-in Lending Act*) hükümleri tüketici kredilerinde borçlandırma, masraflar ve bu konudaki hüküm ve koşulları düzenleyen diğer birtakım düzenlemelerdir. ABD'de ödeme sistemleri açısından bir başka dikkat çeken yasal düzenleme 1913 tarihli "Federal Rezerv Kanunu" (İngilizce'de Federal Reserve Act veya "FRA" olarak ifade edilmektedir) olup bu kanun genel itibariyle FED'in kurulmasını sağlayarak ABD'de bankacılık konusunda yetkilerini düzenlemektedir. FRA'ya göre FED'in bankacılık konusunda yetkileri tahviller düzenleyerek bunları ödeme sistemlerine tedavül etmek, ABD'nin finansal para otoritesi olarak bankacılık sektörünü düzenlemek ve para politikasını yönetmektir.

[557] 1913 tarihinde kurulan "Federal Reserve", Amerikan merkez bankacılığının yönetildiği kuruluşun adıdır. Bkz. https://en.wikipedia.org/wiki/Federal_Reserve (Gözden Geçirilme Tarihi: 29.10.2020).

denilen Amerikan Merkez Bankası'nın kritik bir rol oynamakta olduğu, ödemeler noktasındaki yasal düzenlemelerin genelde belirli finansal kuruluşları ve belirli işlemleri kapsamaması sebebiyle karmaşık olduğu görülmektedir. Özellikle, ATM ve POS ödemeleri gibi elektronik ödeme işlemlerinin Amerikan piyasasında her geçen gün hızla büyüdüğü ve ABD'de özellikle rekabet ve inovasyonun yeni ödeme sistemlerinin ortaya çıkmasında itici bir güç olduğu görülmüştür. Bu itibarla başta Federal Reserve (*"FED"*) olmak üzere Amerikan finans piyasasının diğer aktörlerinin de ödeme sistemlerinde etkinliği artırmak ve riskleri azaltmak konusunda bazı önlemlere başvurduğu görülmektedir. Ayrıca, ABD'de en kapsamlı şekilde uygulanan elektronik fon transferi sistemleri Fedwire[558] ve CHIPS[559]'dir.

Ayrıca, FED'in kurumsal web sitesi için Bkz. https://www.federalreserve.gov/ (Gözden Geçirilme Tarihi: 29.10.2020).

[558] Fedwire ödeme sisteminin hukuki altyapısı temel itibariyle Uniform Consumer Credit Code (*"UCCC"*) m. 4A ve FED'in Regülasyon J denilen yönetmeliği çerçevesinde düzenlenmektedir. Fedwire sistemi, ABD'de teknik açıdan FED tarafından yönetilen gerçek zamanlı brüt mutabakat sistemi[558] olup katılımcıların kendi adlarına veya müşterileri adlarına ödeme göndermeleri ve almalarını sağlayan bir ödeme sistemidir. Fedwire üzerinden bir ödeme gerçekleştirilebilmesi için, ilgili kuruluşun FED'de bir banka hesabı olmalı ve bunun öncesinde ise ödeme transferini tamamlayabilmesi açısından FED'in öngördüğü güvenlik süreci anlaşmasını imzalamalıdır. Bu konuda ayrıntılı bilgi için bkz. Bkz. M. İbrahim Kirdaban, "Ödeme Sistemlerindeki Gelişmeler Ve Ödeme Sistemlerinin Finansal Sistem İstikrarı Üzerindeki Etkileri, Uzmanlık Tezi, Türkiye Cumhuriyeti Merkez Bankası Bankacılık Ve Finansal Kuruluşlar Genel Müdürlüğü, Ankara, 2005, ("*Kirdaban"),* s. 77, 78.

[559] CHIPS ise İngilizce'de "Clearing House Interbank Payments System"in kısaltması olup bankalar tarafından yaygın şekilde kullanılan diğer bir fon transfer sistemidir. CHIPS bakımından New York Eyalet Hukuku kurallarının geçerli olduğu ve aynı zamanda UCC m. 4A'nın uygulanacağı kabul edilmektedir. CHIPS, 1970'lerde kağıt tabanlı ödeme sistemlerine alternatif olarak uluslararası platformda Amerikan Doları transferlerinin yerine geçmek üzere yaratılmış alternatif bir fon transferi sistemidir. CHIPS ödeme sisteminin sahibi, 1998 yılından itibaren New York Clearing House Association adlı bir kuruluşun iştiraki olan ve aralarında Citibank, ABN Amro Bank, Bank of America, Bank of New York, Bank of Tokyo-Mitsibushi, JP Mogan, Chase&Company, Deutsche Bank, HSBC gibi dev Amerikan bankalarının hissedar olduğu CHIPco isimli kuruluştur. CHIPS ödeme sisteminin, gerçek zamanlı nihai mutabakat sistemi olduğu kabul edilmektedir. Bunun anlamı, sistemde her bir ödeme mesajının serbest bırakılması gönderen tarafından yollanan mesajın alıcı tarafça alınmasına bağlıdır. Diğer bir deyişle, bir ödeme mesajı CHIPS tarafından serbest bırakılan ana kadar, gönderici tarafından alıcıya mesajda belirtilen tutarı ödeme yükümlülüğü bulunmamaktadır. CHIPS sisteminin kullanılabilmesi açısından, başta kullanıcıların kendi hesaplarında "açılış pozisyonu gereksinimi" denilen bir ön fonlama yapılmasına, akabinde gönderenin sistem üzerinden ödeme emrini iletmesine, CHIPS tarafından bu ödeme emrinin bir optimizasyon algoritması ile alıcının talebi ile eşleştirilmesine ve akabinde CHIPS tarafından alıcı nezdinde serbest bırakılmasına bağlıdır. Bu konuda detaylı bilgi için Bkz. *Kirdaban,* s. 79-82.

ABD'de, yukarıda belirtilen 1974 tarihli Mahremiyet Yasası dışında elektronik ödemelerde siber güvenliği ilgilendirebilecek diğer federal yasalara örnek olarak 1997 tarihli Gramm-Leach-Bliley Kanunu[560] ve 2002 yılında yürürlüğe giren Federal Bilgi Güvenliği Yönetimi Hakkında Kanun[561] örnek gösterilebilir[562]. FISMA ise, ABD'de finansal kuruluşlar da dahil olmak üzere her türlü kamu kurum ve kuruluşa uygulanabilir bir yasa niteliğinde olup bilgi güvenliği konusunda emredici nitelikteki bazı kuralların, standartların, politikaların ve yol haritalarının uygulanmasını zorunlu kılmaktadır[563]. Ancak, bu düzenlemelerin genel itibariyle internet hizmet sağlayıcılar ve yazılım şirketleri gibi bilişim dünyasını yönlendiren aktörleri doğrudan referans almamasının ve özellikle siber güvenlik alanında hangi önlemlerin alınacağı belirlemekten ziyade makul ölçüde güvenlik tedbirlerinin alınacağı şeklindeki muğlak düzenlemelerinin uygulamada yorum noktasında bazı problemlere yol açması sebebiyle ABD'de bazı uzmanlar tarafından zaman zaman eleştirildiği görülmüştür[564].

---

[560] GLBA metni incelendiğinde özellikle İngilizce'de "pretexting" denilen (bu kavram kişilerin yetkisi olmadan kamuya açık bilgilere telefon, e-mail, phishing gibi faaliyetlerle erişilmesi anlamına gelmektedir) ve aslında bir nevi sosyal mühendislik saldırısı olabilecek aktiviteler konusunda kurumların gerekli tedbirleri alması gerektiğine ilişkin düzenlemeler içermektedir. Bkz. Subtitle B: Fradulent Access to Financial Information, 15 U.S.C., §§ 6821-6827. Ayrıca, Gramm-Leach-Bliley Kanunu (*"GLBA"*)'nun orijinal metnine ulaşmak için: https://www.sec.gov/about/laws/glba.pdf (Gözden Geçirilme Tarihi: 09.05.2020). GLBA metni incelendiğinde özellikle İngilizce'de "pretexting" denilen (bu kavram kişilerin yetkisi olmadan kamuya açık bilgilere telefon, e-mail, phishing gibi faaliyetlerle erişilmesi anlamına gelmektedir) ve aslında bir nevi sosyal mühendislik saldırısı olabilecek aktiviteler konusunda kurumların gerekli tedbirleri alması gerektiğine ilişkin düzenlemeler içermektedir. Bkz. Subtitle B: Fradulent Access to Financial Information, 15 U.S.C., §§ 6821-6827.

[561] İngilizcesi "Federal Information Security Management Act" olup metin içerisinde orijinal kanun metninde olduğu gibi yazar tarafından "FISMA" olarak kısaltılmıştır.

[562] Kısaca özetlemek gerekirse, FISMA federal düzeyde tüm kamu kurum ve kuruluşlarına uygulanacak olan siber güvenlik alanındaki kuralları düzenlerken Gramm-Leach-Bliley ise kamuya açık olmayan kişisel bilgiler ile müşteri bilgileri konusunda özellikle finans kuruluşları açısından uygulacak geniş kapsamlı kuralları ve düzenlemeleri içermektedir. Bu konuda ayrıntılı bilgi için Bkz. Bruce J. Heiman, "Cyber Security is Coming Here!", 15 Nisan 2003: http://www.klgates.com/files/Publication/b107a7ae-1e01-404e-830d-5f4a20eebd1b/Presentation/PublicationAttachment/dbb0ff0d-33fd-4808-b338-60b3345450f6/CybersecurityRegisHere.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[563] FISMA'nın orijinal metnine şu link üzerinden ulaşılabilir: https://www.govinfo.gov/content/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[564] ABD'de siber güvenlik alanında tanınmış isimlerden birisi olan Bruce Schneier'a göre hükümetin şirketleri siber güvenlik alanında yatırım yapmaya zorlamaması halinde, zaten ABD'de bu alanda faaliyet gösteren şirketler gerekli yatırımı yapmaya kendiliğinden yanaşmayacaktır. Schneier, siber

Siber güvenlik açısından ABD'de ceza hukuku boyutu itibariyle elektronik ödemelerde siber güvenlik açısından öne çıkan federal yasalar şunlardır[565]:

Bilgisayar Sahtekârlığı Ve Bilgisayarları Kötüye Kullanılması Kanunu

CFAA[566] denilen Bilgisayar Sahtekârlığı Ve Bilgisayarları Kötüye Kullanılması Kanunu ile genel itibariyle bilişim korsanlığı, virüs yayma, dolandırıcılık, şifre kaçakçılığı, zorla para sızdırma gibi bilişime yönelik bazı suç tipleri düzenlenmiştir[567]. CFAA kapsamında, 1984 yılında ise ABD'de bilgisayarın suça konu olduğu fiiler bakımından ilk kez klasik suçlara benzemeyen, özel nitelikteki bilişim suçları düzenlenmiştir[568]. Söz konusu yasa ile bilgisayara yasa dışı erişimin ne anlama geldiği (erişilen bilginin bir finansal kuruluş tarafından korunan finansal bir kayıt olması veya kart düzenleyen bir kullanıcıya ilişkin kart bilgisi olması ve ABD'nin herhangi bir kuruluşuna ait bir bilgi olması ve korunan bilgisayar açısından ise bilgisayardaki bilginin herhangi bir eyaletler arası ilişkiye veya dış ticaret veya iletişimde kullanılması) ve bu bağlamda ne tür yaptırımların uygulanacağına ilişkin düzenlemelere yer verilmiştir[569]. CFAA kapsamında başka birçok çeşit suç tipi düzenlenmekle beraber çalışmayı ilgilendirmesi açısından özellikle "bir suç işlemek maksadıyla kasten, bir finansal yapının mali kayıtlarını elde etmek için bilgisayarlara yetkisiz veya yetkili erişme"nin suç olarak düzenlendiği görülmüştür[570].

---

güvenlik açısından ABD'de hükümet tarafından gerekli önlemler alınsa dahi, başarılı siber atakların gerçekleştirilmesinin günümüzde her zaman imkân dâhilinde olduğunu ifade etmiştir. Bu konuda detaylı bilgi için bkz. https://web.archive.org/web/20080302205503/http://news.zdnet.com/2100-1009_22-984697.html (Gözden Geçirilme Tarihi: 29.10.2020).

[565] https://www.lexology.com/library/detail.aspx?g=74807b96-a23e-4cfd-971c-d1359cf4855a#:~:text=The%20Federal%20Information%20Security%20Management,government%20agencies%20and%20their%20contractors.&text=The%20FAR%20rule%20requires%20contractors,required%20under%20the%20DFARS%20rule. (Gözden Geçirilme Tarihi: 29.10.2020).

[566] İngilizce "Computer Fraud And Abuse Act" isimli yasanın kısaltmasıdır. İlgili yasanın tam metnine ulaşmak için: https://www.public.navy.mil/netc/nstc/nrotc/pdfs/cfaa.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[567] *Çakır/Kılıç*, s. 196.

[568] *Çakır/Kılıç*, s. 195'de belirtilen Ditzion/Geddes/Rhodes (2003:82).

[569] U.S.C. 1030, Title 18. Ayrıntılı bilgi için ayrıca Bkz. *Çakır/Kılıç*, s. 196'de yer alan Goodman/Brenner.

[570] *Çakır/Kılıç*, s. 195.

Elektronik İletişim Ve Mahremiyet Kanunu

1986 tarihli Elektronik İletişim Ve Mahremiyet Kanunu (*"ECPA"*)[571] ile yasa dışı elektronik dinleme yasaklanarak aynı zamanda elektronik posta, sesli posta ve uzaktan kumandalı sistemler yoluyla gerçekleştirilen iletişimin korunması amaçlanmıştır[572]. ECPA, aynı zamanda elektronik iletişim hizmetini veren ve bu hizmete dair verileri depolayan kuruluşların sisteme erişiminin değiştirilmesini ve engellenmesini yasaklamaktadır.

Depolanmış Kablolu Ve Elektronik İletişimlere Ve Ticari Kayıtlara Yetkisiz Erişim Kanunu

"Depolanmış Kablolu Ve Elektronik İletişimlere Ve Ticari Kayıtlara Yetkisiz Erişim Kanunu" ile elektronik iletişimin sağlandığı bir tesise yetkisiz ve kasten erişim ya da yetki aşımı ile tesise erişilmesi neticesinde elektronik ortamda depolanmış kablolu veya elektronik iletişime yetkili erişim elde etmek, yetkili erişimi değiştirmek veya önlemek faaliyetleri suç olarak değerlendirilmiştir[573].

4.3.3. Elektronik Ödeme Sistemlerinde Siber Güvenlikle İlgili ABD'de Bazı Eyalet Yasaları

Yukarıda da belirtildiği üzere, ABD'de siber güvenlik alanında federal düzeydeki sektör-spesifik düzenlemelerinin yanı sıra, her eyaletin kendi öngörmüş olduğu Common Law kuralları geçerli olduğundan eyaletler açısından elektronik ödeme

---

[571] İngilizce'de yasa metni "Electronic Communications Privacy Act" (*"ECPA"*) olarak ifade edilmekte olup orijinal metne internet ortamından ulaşmak için Bkz. https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285 (Gözden Geçirilme Tarihi: 28.05.2020). Ayrıca, ECPA ile ilgili ayrıntılı bilgi için bkz. *Eric Fischer*, s. 42-45.

[572] *Dülger, Bilişim Suçları,* s. 217.

[573] Orijinal adı ile "Stored Communications Act" olan ve U.S. Code 2701 olarak literatürde belirtilen bu kanun ile ilgili detaylı bilgi için bkz. Çakır/Kılıç, s. 196. Ayrıca bu konuda detaylı bilgi için bkz. Wilmer Cutler Pickering Hale and Dorr LLP, "Cybersecurity in the USA": https://www.lexology.com/library/detail.aspx?g=74807b96-a23e-4cfd-971c-d1359cf4855a#:~:text=The%20Federal%20Information%20Security%20Management,government%20agencies%20and%20their%20contractors.&text=The%20FAR%20rule%20requires%20contractors,required%20under%20the%20DFARS%20rule. (Gözden Geçirilme Tarihi: 29.10.2020).

sistemleri ile ilgili siber güvenlik konusunda farklı yasal düzenlemeler bulunmaktadır[574]. Bu konuda, en dikkat çekici örnek Kaliforniya Eyaleti'dir. Kaliforniya Eyaleti'nde, izleme teknolojilerinin kısıtlamasına ilişkin ayrıntılı düzenlemeler yer almakla beraber[575], eyalet düzeyindeki ilk veri ihlali bildirimine yönelik bir düzenleme olan ve 2003 yılında Kaliforniya Eyaleti'ne bağlı kişilerin kişisel verilerinde herhangi bir veri sızıntısı yaşanması halinde, veri sızıntısı yaşayan şirketin bu durumu bildirmesini zorunlu kılan Veri İhlali Bildirimi Hakkında Kanun (*"Notice Security Breach Act"* veya kısaca *"NSBA"*) yürürlüğe girmiştir[576]. NSBA'da, bahsi geçen kişisel veriler, kişilerin elektronik ortamda ödeme yapmasını sağlayan kredi kartı numaraları ve banka kartı bilgilerini, sosyal güvenlik numaralarını, sürücü belgesi numaralarını veya kişilere özel herhangi bir finansal bilgileri içermektedir[577] ve bu bilgilerin veri ihlali şeklinde üçüncü kişilerce ele geçirilmesi halinde bu konuda veri sızıntısı yaşayan şirketlerin bildirimde bulunması zorunlu kılınmıştır. Kaliforniya Eyaleti'ndeki anılan bu kanunun yürürlüğe girmesinden sonra başka bazı eyaletler de Kaliforniya gibi veri ihlali bildirimini zorunlu kılan yasal düzenlemelerin yürürlüğe

[574] ABD'de siber güvenlik alanında farklı eyaletlerde yürürlükte bulunan mevuzat hakkında ayrıntılı bilgi için bkz. 2020 itibariyle https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2020.aspx (Gözden Geçirilme Tarihi: 29.10.2020).

[575] ABD'de birçok gizlilik yasası uyarınca yalnız izlenen kişinin makul bir gizlilik beklentisi olması halinde izleme kısıtlanmakta olup Kaliforniya Eyaleti'nde ise işverenler tarafından soyunma odalarında kamera bulundurulması, RFID okuyucularla konum izleme ve benzeri izleme teknolojileri yasaklanmış, ancak belli türdeki araç izlemelerinde açık rıza ile bu yasağın dışına çıkılmaktadır. Bu konuda detaylı bilgi için bkz. *Determann*, s. 159 vd.

[576] NSBA metninde, veri sızıntısı halinde nasıl bir bildirim yapılması gerektiği konusunda ayrıntılı bir düzenlemeye yer verilmiş olup özellikle ilgili kamu kuruluşları sunulacak şablon dilekçe içeriğinin nasıl olması gerektiği belirtilmiştir. Elektronik ortamda ilgili düzenlemeye ulaşabilmek için: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82 (Gözden Geçirilme Tarihi: 01.06.2020). NSBA'nın hukuki kapsamı hakkında detaylı bilgi için Bkz. Timothy H. Skinner, "California 's Database Breach Notification Security Act: The First State Breah Notification Law Is Is Not Yet A Suitable Template For National Identity Theft Legislation", C: 10, S: 1, 2003 (*"Skinner"*): https://scholarship.richmond.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1172&context=jolt (Gözden Geçirilme Tarihi: 29.10.2020).

[577] https://web.archive.org/web/20100613183200/http://www.privacyrights.org/ar/ChronDataBreaches.htm (Gözden Geçirilme Tarihi: 29.10.2020).

girmesini sağlamıştır[578]. Literatürde, Skinner tarafından ABD'de Kaliforniya ve benzeri eyaletlerde özellikle siber güvenlik açısından ihlal yaşayan şirketlerin yasal olarak belirli para cezası ödemelerinin öngörülmesinin, şirketlerin özellikle siber güvenlik alanında bazı önlemleri daha ciddi şekilde almaya sevk ettiği ve söz konusu yasal düzenlemelerin özellikle olası siber ataklar karşısında ekonomik kaybın yanı sıra, ABD'deki şirketler açısından özellikle itibar kaybını önlemek açısından gerekli inisiyatifleri almaya teşvik ettiği üzerinde durulmuştur[579].

4.4. ELEKTRONİK ÖDEME SİSTEMLERİNDE SİBER GÜVENLİK İLE İLGİLİ ÇİN'DEKİ YASAL DÜZENLEMELER

Çin, 2014 yılından itibaren elektronik ödeme sistemlerinde ve özellikle dijital para konusunda aktif şekilde hareket eden bir ülke olup 2020 yılı itibariyle akıllı telefonlardaki elektronik cüzdan uygulamalarına yüklenecek e-Renminbi (*"e-RMB"*) uygulamasına geçileceği bilinmektedir[580].

Elektronik ödemeler açısından Çin'deki regülasyonlara[581] bakıldığında kripto paralar konusunda da ilginç gelişmelerin yaşandığı görülmüştür. Bitcoin açısından, Çin'de ilk

---

[578] ABD'de Kaliforniya'dan sonra Maryland, New Hampshire, New York, North Carolina ve Vermont eyaletlerinde de veri ihlali bildirimini zorunlu kılan yasaların yürürlüğe girdiği bilinmektedir. Bkz. https://web.archive.org/web/20100613183200/http://www.privacyrights.org/ar/ChronDataBreaches.htm#10 (Gözden Geçirilme Tarihi: 29.10.2020).

[579] *Skinner*, s. 3.

[580] https://www.theguardian.com/world/2020/apr/28/china-starts-major-trial-of-state-run-digital-currency (Gözden Geçirilme Tarihi: 29.10.2020).

[581] Çalışmada, Çin Halk Cumhuriyeti'nde kripto paralar ve blokzincir teknolojisine ilişkin regülasyon konusundaki açıklamalar (özellikle 2013 ila 2019 tarihleri arasında) Jacob Blacklock ve Steve Shi tarafından hazırlanan "Blockchain & Cryptocurrency Regulation 2020/China" adlı makalesinden özetlenerek yukarıda aktarılmıştır. Bkz. Jacob Blacklock/Steve Shi, "Blockchain & Cryptocurrency Regulation 2020/China", Global Legal Insights (*"Blacklock/Shi"*): https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/china, ayrıca blokzincir teknolojisinin Çin'deki tarihçesi konusunda detaylı bilgi için ayrıca Bkz. Arthur R. Boss, "Cryptocurrencies and Regulation, a Master Thesis on the best practices for regulating cryptocurrencies within the EU", Leiden Üniversitesi, Yüksek Lisans Tezi, 6 Temmuz 2018, (*"Boss"*) s. 24 vd., teze ulaşmak için ilgili link: https://openaccess.leidenuniv.nl/bitstream/handle/1887/64833/MA%20Thesis%20-%20Arthur%20Bos.pdf?sequence=1 (Gözden Geçirilme Tarihi: 29.10.2020).

düzenleme 2013 yılında "Bitcoin Risklerinin Önlenmesi Hakkında Duyuru[582]" (*"Duyuru"*) olup bu Duyuru neticesinde Çin'de resmi olarak Bitcoin kullanımı yasaklanmıştır. Söz konusu Duyuru metninde Çin'de resmi olarak tek para biriminin "Renminbi" (*"RMB"*) olduğu, Bitcoin'in para birimi olarak tanınmadığı ve bu bağlamda Çin piyasasında tedavül edilemeyeceği belirtilmiştir. Buna rağmen, Çin halihazırda 2013 yılındaki tavrını değiştirerek özellikle blokzincir teknolojisi ve kripto paralar konusunda devletler nezdinde aktif şekilde hareket eden bir aktör haline gelmiştir[583].

---

[582] İlgili kaynakta söz konusu düzenleme, İngilizce "Notice on Preventing Bitcoin Risk" olarak belirtilmiş olup yazar tarafından "Bitcoin Risklerinin Önlenmesi Hakkında Duyuru" olarak Tükçe'ye çevrilmiştir (Serbest Çeviri).

[583] 2017 yılında Çin'de 2013 tarihli Duyuru ile paralel şekilde Çin'in bir kamu otoritesi konumundaki Çin İnternet Finans Kurumu tarafından bu kez "Sanal Paralar Hakkında Risklerin Önlenmesine Dair Bildiri" (*"Bildiri"*) yayınlanmıştır. Söz konusu Bildiri'de ise Bitcoin dışında tedavüle sokulan başka altcoinlerin de bulunduğu, söz konusu kripto para birimlerinin Çin'de kara para aklama, uyuşturucu ticareti, kaçakçılık gibi birçok illegal faaliyet için kullanıldığı, bu nedenle yasalar çerçevesinde Çin'deki tüm finans endüstrisi aktörlerinin bu kripto para birimlerini kullanması yasaklanmıştır. Ancak, Çin'de kripto para ticaretini yasaklamaya yönelik Bildiri ve Duyuru fiiliyatta gerçekten de kripto para kullanımının yasaklanmasını sağlayamamıştır. 2017 yılında Çin'deki tabloya bakıldığında Çin devleti tarafından gerçekleştirilen tüm engellemelere rağmen, özellikle kripto para birimlerinin yükselişe geçtiği bilinmektedir. Özellikle, 2017 yılının ilk yarısında altmış beşin üzerinde "ICO" denilen dijital para arzının gerçekleştirildiği ve bu ICO'lar sayesinde yaklaşık 2,6 milyar RMB'nin (yaklaşık 400 milyon Dolar'a tekabül etmektedir) yasa dışı şekilde kontrol edildiği görülmüştür. Bu durumda, Çin'de öncelikle kontrol edilemeyen bir sermayenin ortaya çıktığı ve bu sermayenin deneyimsiz bazı yatırımcıların bu dijital paralar üzerindeki hâkimiyetinin ekonomik açıdan istikrarsızlığa neden olduğu üzerinde durulmuştur. Bu gelişmeler üzerine, 2017 yılı Eylül ayında bu kez Çin'deki resmi otoriteler açısından bağlayıcı nitelikteki "ICO Risklerinin Önlenmesine İlişkin Duyuru" denilen ikinci bir duyuru yayınlanarak ICO aktivitelerinin izin verilmeyen ve hukuka aykırı fonlama işlemleri olduğu ve ICO aktivitelerinin yasaklandığı belirtilmiştir. Ancak, Çin'de kripto para birimlere ve ICO'lara ilişkin tüm bu dirence rağmen, kripto paralar ve ICO'lara gösterilen rağbet, Çin devleti açısından blokzincir teknolojisini regüle etmeye ihtiyacı doğurmuştur. 2019 yılı Şubat ayında Çin'in Siber Güvenlik Kurumu tarafından "Blokzincir Bilgi Hizmet Yönetimine İlişkin Regülasyon" ("Blockchain Information Service Management Regulations" veya *"BISMR"*) yayınlanarak ilk kez Çin'deki blokzincir teknolojisine dayalı iş modellerinin hukuki çerçevesi çizilmeye çalışılmıştır. Özellikle BISMR metninde kripto paralar açısından blokzincir teknolojisinin gerçekleştirilecek işlemler açısından anonimliği ve mahremiyeti sağlamaya imkan verdiği belirtilerek, bilginin saklanması açısından dağıtık veri tabanı teknolojisinin önemine ve Çin'in bu açıdan "Siber Bağımsızlık" hedefine vurgu yapılmıştır. Çin'in bahsi geçen bu hedeflere ulaşması açısından ise BISMR kapsamında blokzincir tabanlı hizmet verecek girişimcilerin ilgili otoriteler nezdinde gerçek isimlerini ve kimliklerini paylaşarak kayıt yaptırmaları zorunlu kılınmıştır. BISMR kapsamında aynı zamanda blokzincir teknolojisini kullanacak hizmet sağlayıcıların illegal faaliyetleri fark etmesi halinde derhal bu durumu ilgili makamlara bildirmesi gerektiği ve bu konuda her türlü illegal faaliyetten kaçınması gerektiği düzenlenmiştir.

Bitcoin arzının 2013 yılında Çin'de ülke çapında yasaklamasına rağmen, yukarıda belirtilen gelişmelerle de bağlantılı olarak DCEP[584] adı verilen "Dijital Para Birimi Elektronik Ödeme" (*Digital Currency Electronic Payment*) sistemi denilen ve temelinde dağıtık veri tabanı teknolojisine dayanan yeni elektronik ödeme sistemi projesini hayata geçirmek amacıyla Çin bu konuda ciddi adımlar atmaya başlamıştır[585].

Siber güvenlik perspektifinden konuya bakıldığında, ABD ve AB'de olduğu gibi Çin'de de siber güvenlik açısından finansal kuruluşlarının yönetiminde nasıl bir strateji izleneceği netleştirilmesi gereken konulardan birisi olarak görülmüştür. Çin'deki mevzuat açısından elektronik ödeme sistemlerini de dahil olmak üzere siber güvenlik alanında en önemli düzenleme 2017 yılında yürürlüğe giren "Çin Siber Güvenlik

[584] İlgili haberde DCEP açılımı İngilizce'de "Digital Currency Electronic Payment" denilen, yazar tarafından "Dijital Para Birimi Elektronik Ödeme" şeklinde tercüme edilmiştir. DCEP konusunda ayrıntılı bilgi için bkz. https://www.allcryptowhitepapers.com/dcep-whitepaper/ (Gözden Geçirilme Tarihi: 29.10.2020).

[585] DCEP sistemi AliPay gibi uygulamalar üzerinden çalışabileceği gibi mobil bankacılık uygulamalarında da kullanılabilecek şekilde tasarlanmıştır. DCEP uygulamasının test aşamalarında (Tier 1 ve Tier 2) olduğu belirtilen Forbes'un haberinde, özellikle Çin'de Shenzhen, Xiong'an, Chengdu ve Suzhou şehirlerinde uygulamaya geçileceği belirtilmektedir. Bkz. https://www.forbes.com/sites/biserdimitrov/2020/04/16/these-chinese-blockchain-platforms-are-launching-soon-here-is-why/#5e2a11d0207e (Gözden Geçirilme Tarihi: 29.10.2020). DCEP sisteminin uygulamaya geçmesi halinde, offline ödemeler yapılması da mümkün hale gelecektir. Teknik açıdan konuya bakıldığında, DCEP uygulaması aslında tam anlamıyla blokzincir tabanlı bir uygulama olmayıp temel itibariyle "Dağıtık Veritabanı Teknolojisi" (DLT) protokolüne dayanan bir uygulama olarak ön plana çıkmaktadır. Bu açıdan, aslında Çin'deki kripto para olmayan ancak dijital bir para birimi olan dijital Yuan'dan farklıdır. Dijital Yuan'ın da halihazırda Çin'in önemli bankalarından birisi olan Agricultural Bank of China ("ABC") tarafından test edildiği ve yakın zamanda ABC dışında Çin'in en önemli diğer üç bankası olan Bank of China, China Construction Bank ve Industrial and Commercial Bank of China nezdinde de kullanılmaya başlanacağı öngörülmektedir. Aynı zamanda, DCEP sistemi açısından Çin'in en büyük ödeme hizmet sağlayıcı şirketleri olan Alibaba (AliPay) ve Tencent (WeChat Pay) gibi şirketlerle işbirliğine gidilerek AliPay ve WeChat Pay ile entegre şekilde çalışacak şekilde tasarlanması düşünülmektedir. Böylelikle elektronik ödemeler noktasında Çin'de bir yandan dijital Yuan diğer yandan ise DCEP ödeme sistemi ile rahatlıkla dijital ortamda ödemenin yaygınlaştırılmasına imkân tanınmak istenmektedir. DCEP konusundaki gelişmeler açısından Blockchain Türkiye platformunun bu konuda yer verdiği haberler incelenebilir: https://bctr.org/cin-merkez-bankasi-dijital-parasina-yonelik-son-gelismeleri-paylasti-13366/ (Gözden Geçirilme Tarihi: 29.10.2020).

Kanunu"[586] olarak kabul edilmektedir[587]. Siber Güvenlik Kanunu, Çin'de özellikle devlet tarafından kontrol edilebilen bir siber alan yaratmayı hedeflemekle beraber finans ve elektronik haberleşme gibi Çin Devleti açısından kritik altyapıya sahip sektörlerdeki[588] şebeke operatörleri için bilgisayar donanımının zorunlu testini ve siber güvenliğin temini açısından sertifikasyonu amaçlamaktadır[589]. Çin Siber Güvenlik Kanunu'nda öngörülen bu testler ve sertifikalar, ağ operatörlerinin dahili güvenlik yönetim sistemlerini daha iyi bir şekilde formüle etmeleri ve zararlı yazılımlar da dahil olmak üzere tanımlanmamış siber saldırı türleri konusunda önlem alınmasını sağlamayı hedeflemektedir[590]. Başka bir ifade ile Çin'deki Siber Güvenlik Kanunu şirketlere ve bankalar da dahil olmak üzere finansal kuruluşlara gerekli önlemleri almaları, müşteri verilerinin toplanması ve saklanması konusunda en iyi uygulama örneklerini dikkate almalarını sağlayan bir yapının parçası olmaya zorlamaktadır. Ayrıca, Siber Güvenlik Kanunu finans gibi kritik sektörlerdeki ağ operatörlerinin, ülkede bu operatörler tarafından toplanan veya üretilen tüm verileri Çin'de saklamasını zorunlu kılmaktadır[591]. 2019 yılı Eylül ayında yayınlanan "Finans Endüstrisi Standartlarının

[586] Çin'deki Siber Güvenlik Kanunu ile ilgili açıklamalar "Çin'in Siber Güvenlik Kanunu Geleceğe Dair Ne Diyor?" isimli makaleden aktarılmış olup söz konusu makaleye şu link üzerinden ulaşılmıştır: https://www.intell4.com/cinin-siber-guvenlik-yasasi-gelecege-ne-diyor-haber-182701 (Gözden Geçirilme Tarihi: 29.10.2020).

[587] Çin Siber Güvenlik Kanunu'nun İngilizce tercümesine ulaşmak için: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ (Gözden Geçirilme Tarihi: 08.10.2020). Ayrıca, Çin Siber Güvenlik Kanunu ile ilgili genel bilgi için bkz. Dentons, "2019 China Data Protection & Cyber Security Annual Report", 2020, (*"China Report"*), s.7, 8. İlgili rapora internet üzerinden ulaşmak için bkz. https://www.dentons.com/en/insights/guides-reports-and-whitepapers/2020/march/31/2019-china-data-protection-cybersecurity-annual-report (Gözden Geçirilme Tarihi: 29.10.2020).

[588] Çin Siber Güvenlik Kanunu m. 31'de Çin Devleti'nin çok katmanlı siber güvenlik korumasının sağlanması gereken kritik alyapılar olarak kamu iletişim ve bilişim hizmetleri, enerji, su kaynakları, finans ve e-devlet gibi servisler örnek gösterilmiştir.

[589] Bkz. Çin Siber Güvenlik Kanunu m. 5/c. 2 ve *China Report*, s. 10, 11.

[590] Bkz. Çin Siber Güvenlik Kanunu, m. 21 vd ve *China Report*, s. 15-17.

[591] Veri lokalizasyonu kapsamında, bu durum Çin Siber Güvenlik Kanunu'nun 37. maddesinde düzenlenmektedir. İlgili düzenlemeye göre, kritik bilgi altyapısında faaliyet operatörler Çin Halk Cumhuriyeti sınırları çerçevesinde elde ettikleri veya ürettikleri kişisel bilgiyi veya önemli sayılabilecek bilgiyi Çin'de saklamakla yükümlüdür. Herhangi bir ticari gereksinim neticesinde, elde edilen bilginin Çin dışında elde edilmesi söz konusu olduğunda ise, kanunlarda aksi belirtilmediği sürece operatörler Çin Devleti'nin siber güvenlik ve bilişim departmanlarının ve Çin Danıştayı'nın ilgili departmanlarının siber güvenlik değerlendirmeleri neticesinde uygun gördüğü önlemler çerçevesinde hareket etmekle

Yayınlanması Ve Mobil Finansal Uygulamaların Güvenliği Hakkında Bildiri" ile kişisel nitelikteki finansal bilgilerin korunması, bu alandaki güvenlik yetkinliklerinin artırılması, risk görüntüleme ve şikayet yönetimi süreçlerinin geliştirilmesi ve Çin'deki finans endüstrisinin kendi iç disiplin sürecinin güçlendirilmesi hedeflenmiştir[592]. Aynı tarihte, mobil ödemeler ile ilgili Çin'de spesifik bir düzenleme olarak "Mobil Ödemeler Düzenlemesi" (Specification on Mobile Payment) ile mobil ödemelerde kullanıcıların kişisel ve finansal bilgilerinin temini açısından kişilerin rızasının aranması zorunlu kılınarak rıza alınmaksızın işlem yapılması yasaklanmıştır[593].

BEŞİNCİ BÖLÜM

ELEKTRONİK ÖDEME SİSTEMLERİNDEKİ SİBER GÜVENLİK KONUSUNDA TÜRKİYE'DEKİ DÜZENLEMELER

En basit bilişim suçlarının dahi genelde uluslararası bir unsur barındıracak şekilde işlenmesi[594] yukarıda incelendiği üzere karşılaştırmalı hukuk açısından farklı devletlerin farklı strateji izlemelerine rağmen uluslararası iş birliği noktasında devletlerin birbirlerinin mevzuatından kısmen dahi etkilenmesine sebebiyet vermiştir. Bu bağlamda, aşağıda da detaylı şekilde ele alınacağı üzere, elektronik ödeme sistemlerinde siber güvenlik açısından Türkiye'deki düzenlemelere bakıldığında özellikle bu alanda büyük ölçüde Avrupa Birliği regülasyonlarının etkisi olduğu görülmüştür. 1970 yıllarda Avrupa Konseyi'nce elektronik bilgi bankalarında işlenen veriler nedeniyle bireylerin özel hayatlarının korunmasına yönelik başlatılan bir dizi çalışma sonucunda ise Türkiye'de bu hareketten etkilenmiş ve yukarıda da belirtildiği

zorunludur. Veri lokalizasyonu ile bağlantılı olarak ağ güvenliğinin temini bakımından benzer bir düzenleme için bkz. Çin Siber Güvenlik Kanunu, m. 50.

[592] *China Report*, s. 26.
[593] *China Report*, s. 26.
[594] *Dülger*, *Bilişim Suçları,* s. 197.

gibi "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması"na ilişkin 108 Sayılı Sözleşme 28.11.1981 tarihinde ülkelerin imzasına sunulmuş ve anılan sözleşme diğer ülkeler ile birlikte Türkiye tarafından da imzalanmıştır[595]. Öte yandan, çalışmayı ilgilendirmesi açısından bilişim suçları alanında Türk Ceza Kanunu'nda yer alan düzenlemelerin kısmen Avrupa Siber Suç Sözleşmesi'nin bu alandaki düzenlemeler ile paralellik taşıdığı düşünülebilir. Bu hususta zaten Türkiye'nin Avrupa Siber Suç Sözleşmesi'ni iç hukukunda yürürlüğe girmesi Türkiye'de bu alandaki mevzuatın AB'ye ne ölçüde yakınsandığını göstermesi açısından dikkat çekicidir.

Öte yandan, Türkiye'de tüm dünyada olduğu gibi elektronik ödeme sistemlerinde siber güvenlik alanında Covid-19 pandemi salgının etkisi ile akabinde yeni düzenlemeler açısından hareketli bir dönem geçtiği söylenebilir. Dolayısıyla, bu bölümde Türkiye'de siber güvenlik tarihçesi ile elektronik ödemelerde siber güvenlik açısından temel düzenlemeler ayrıntılı şekilde analiz edilmekle beraber bu konuda somut birtakım yeni projelerin yanı sıra, Covid-19'un da etkisi ile yeni yürürlüğe giren veya taslak aşamadaki önemli birtakım yasal düzenlemelere de yer verilmiştir.

Türkiye Cumhuriyeti Cumhurbaşkanlığı Strateji Ve Bütçe Başkanlığı tarafından yayınlanan 2019-2023 yılları arasındaki döneme ilişkin 11. Kalkınma Planı'nda elektronik ödeme sistemleri açısından çalışmayı ilgilendirebilecek hususlar olarak;

(i) Blokzincir tabanlı dijital merkez bankası parası uygulamaya konulacağı,

(ii) Ödeme Hizmetleri ve Elektronik Para Kuruluşları Birliği kurulacağı[596],

(iii) Elektronik çek ve bono sistemi kurulacağı[597],

---

[595] *Dülger*, *Bilişim Suçları,* s. 199'da 335 no'lu dp.da belirtilen Değirmenci.

[596] Türkiye Ödeme Ve Para Kuruluşları Birliği'nin kuruluşuna ve faaliyetlerine yönelik Statü yayınlanmış olup bu hususta çalışmanın 5.10 numaralı başlığı altında detaylı değerlendirmelere yer verilmiştir.

[597] Bu konudaki kanun taslağı konusunda ise çalışmanın 1.2.2.5.5. numaralı "Diğer Elektronik Ödeme Yöntemleri" alt başlığı altında "Elektronik Çek" ile ilgili değerlendirmeler kapsamında ele alınmıştır.

(iv) Açık bankacılık hukuki altyapısını güçlendirmek amacıyla PSD2 ile mevzuat uyumu sağlanacağı[598],

belirtilmiştir[599].

5.1. TÜRKİYE'DE SİBER GÜVENLİK ALANINDA DİKKAT ÇEKEN GELİŞMELER

5.1.1. Türkiye'de Siber Güvenlik Çalışmaları

Türkiye'de 2012 yılı, siber güvenlik açısından önemli bir dönem noktası olmuş ve siber güvenlik konusunda ilk çalışmalar 2012 yılında gerçekleştirilen Siber Güvenlik Çalıştayı (*"Çalıştay"*)'ndan sonra başlatılmıştır. Bu Çalıştay neticesinde, T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (*"UDHB"*)[600] ve Bilgi Güvenliği Derneği (*"BGD"*)[601] tarafından hazırlanan Ulusal Siber Güvenlik Stratejisi (*"USGS"*)[602] kapsamında Türkiye'nin siber güvenlik hedefleri ve bu kapsamda atılması gereken adımlar belirtilmiştir. USGS'de devletin öncülüğünde atılacak bu adımların siber uzayın güvenliğinin artırılması, siber saldırılara karşı kritik altyapıların dayanıklılığın ve koruma sürekliliğinin temin edilmesi, kurumsal ve kişisel verilerin güvenliğinin sağlanması temel hedeflerin yerine getirilmesi amaçlanarak Ulusal Siber Güvenlik Kurulu'nun oluşturulması, siber güvenlik farkındalığının artırılması, siber güvenlik kültürünün yaygınlaştırılması, bu noktada uluslararası işbirliğinin

[598] Özellikle bu konuda yasa koyucu tarafından adım atılmış olup çalışmanın 5.2.5 başlığı altında bir kısım hükümleri 01.07.2020 tarihinde yürürlüğe giren Bankaların Bilgi Sistemleri Ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik kapsamında detaylı açıklamalara yer verilecektir.

[599] Türkiye Cumhuriyeti Cumhurbaşkanlığı Strateji Ve Bütçe Başkanlığı tarafından yayınlanan 2019-2023 yılları arasındaki döneme ilişkin 11. Kalkınma Planı, orijinal metne internet üzerinden ulaşmak için bkz. http://www.sbb.gov.tr/wp-content/uploads/2019/07/OnbirinciKalkinmaPlani.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[600] Türkiye'de Cumhurbaşkanlığı Hükümet Sistemi'ne geçiş ile beraber siber güvenlik konusunda sorumlu bakanlık olan Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nın ismi Ulaştırma ve Altyapı Bakanlığı şeklinde değişmiş, ancak ilgili bakanlığın siber güvenlik konusundaki görev ve sorumlulukları günümüze kadar devam etmiştir.

[601] https://bilgiguvenligi.org.tr (Gözden Geçirme Tarihi: 29.10.2020).

[602] Ulusal Siber Güvenlik Stratejisi taslak metin konusunda Bkz. https://www.bilgiguvenligi.org.tr/wp-content/uploads/2016/03/Ulusal_Siber_Guvenlik_Stratejisi.pdf (Gözden Geçirme Tarihi: 29.10.2020).

güçlendirilmesi ve ulusal siber güvenlik Ar-Ge politikasının oluşturulması ve milli teknolojilerin geliştirilmesinin özendirilmesi olduğu belirtilmiştir[603].

USGS çerçevesinde kritik altyapının ne olduğu belirtilerek bilişim, enerji, mali işler, sağlık, gıda, su, ulaşım, savunma, nükleer, biyolojik ve kimyasal tesisler ile kamu güvenliği kritik altyapılar olarak değerlendirilmiştir[604].

USGS çerçevesinde gerekli adımların atılarak belirlenen hedeflerin hayata geçirilebilmesi amacıyla, ulusal siber güvenlik çalışmalarının yürütülmesi, yönetilmesi ve koordinasyonu konusunda 20.10.2012 tarihli ve 28447 Sayılı Resmi Gazete'de yayınlarak yürürlüğe giren Bakanlar Kurulu Kararı[605] yürürlüğe girmiştir. Bu karar gereğince, Bilgi Teknolojileri ve İletişim Kurumu (*"BTK"*) bünyesinde Siber Güvenlik Kurulu[606] oluşturulmuş, UDHB'na siber güvenlik alanında görev ve yetkiler verilerek siber güvenlikle ilgili çalışma grupları ve geçici kurulların oluşturulabileceği karara bağlanmıştır[607]. Siber Güvenlik Kurulu, ilk toplantısını 21.12.2012 tarihinde gerçekleştirmiş ve bu toplantıda "Siber Güvenlik Kurulunun Görevleri, Çalışma Usul ve Esasları Yönergesi" ve "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" kabul edilmiştir[608]. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı

---

[603] *USGS*, s. 9-10.
[604] *USGS*, s. 12.
[605] Anılan Bakanlar Kurulu Kararı'nın tam metni için Bkz. https://www.uab.gov.tr/uploads/pages/siber-guvenlik/some-bkk.pdf (Gözden Geçirilme Tarihi: 29.10.2020).
[606] 20.10.2012 tarihli Bakanlar Kurulu Kararı'nın içeriği, 06.02.2014 tarihinde yayımlanan 6518 Sayılı Kanun 5809 Sayılı Elektronik Haberleşme Kanunu'na ilave edilen Ek Madde 1 ile kanunlaştırılmış ve bu kapsamda ilave edilen ek fıkralar ile BTK bünyesinde oluşturulan Siber Güvenlik Kurulu'na siber güvenlikle ilgili birtakım görevler verilmiştir. Bu görevler, siber güvenlik ile ilgili politika, strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasına yönelik gerekli kararları almak, kritik altyapıların belirlenmesine ilişkin teklifleri karara bağlamak, siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşları belirlemek ve kanunla verilen diğer görevleri yapmak olarak belirlenmiştir. Bu konuda çalışmada 5.2.7. numaralı başlık altında "5809 Sayılı Elektronik Haberleşme Kanunu" ile ilgili açıklamalarda ayrıntılı bilgiye yer verilmiştir.
[607] Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar: http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm (Gözden Geçirilme Tarihi: 29.10.2020)
[608] 2013-2014 Eylem Planı'nda Türkiye'de ulusal siber güvenliğin sağlanmasında yedi ana başlık altında şu eylemlerin gerçekleştirilmesi planlanmıştır: (i) Yasal Düzenlemelerin Yapılması, (ii) Adli

sonucunda "Ulusal Siber Olaylara Müdahale Merkezi (*"USOM"*) Kurulması, Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin Oluşturulması (*"Sektörel ve Kurumsal SOME'ler"*) başlıklı 4. eylem maddesi uyarınca, Telekomünikasyon İletişim Başkanlığı (*"TİB"*) bünyesinde 15.05.2013 tarihinde USOM kurulmuştur. Siber güvenlik olaylarına müdahalede ulusal ve uluslararası koordinasyonun sağlanmasında görevli USOM ile aynı zamanda internet aktörleri, kolluk güçleri, uluslararası kuruluşlar, araştırma merkezleri ve özel sektör arasındaki iletişim ve koordinasyonun sağlanması amaçlanmıştır. USOM'un kurulması akabinde, UDHB tarafından Sektörel ve Kurumsal SOME'lerin Kuruluş, Görev Ve Çalışmalarına Dair Usul Ve Esaslar Hakkında Tebliğ[609] (*"Tebliğ"*) 11.10.2013 tarihli ve 28818 Sayılı Resmi Gazete'de yayınlanarak yürürlüğe girmiştir[610].

Türkiye'de ulusal güvenliği sağlamakla görevli kamu kurum ve kuruluşlarına ilişkin organizasyonel yapısı aşağıdaki şemada gösterilmiştir[611].

SüreçlereYardımcı Olacak Çalışmaların Yürütülmesi, (iii) Ulusal Siber Olaylara Müdahale Organizasyonunun Oluşturulması, (iv) Ulusal Siber Güvenlik Altyapısının Güçlendirilmesi, (v) Siber Güvenlik Alanında İnsan Kaynağının Yetiştirilmesi Vebilinçlendirme Faaliyetleri, (vi) Siber Güvenlikte YerliTeknolojilerin Geliştirilmesi, (vii) Ulusal Güvenlik Mekanizmalarının Kapsamının Genişletilmesi. Bu konuda ayrıntılı bilgi için bkz. Çakır/Kılıç, s. 51-53. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı ile ilgili internet üzerinde orijinal belgeye ulaşmak için Bkz. https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[609] Söz konusu Tebliğ ile ilgili tam metne ulaşmak için Bkz. https://www.uab.gov.tr/uploads/pages/siber-guvenlik/some-teblig.pdf (Gözden Geçirilme Tarihi: 29.10.2020)

[610] Siber Güvenlik Kurulu'nun 20.06.2013 tarihli ve 2 sayılı kararı uyarınca, elektronik haberleşme, enerji, su yönetimi, kritik kamu hizmetleri, ulaştırma, bankacılık ve finans kritik altyapı sektörleri olarak belirlenmiş olup Sektörel Siber Olaylara Müdahale (*"Sektörel SOME"*) kurulmuştur.

[611] Şekil-5.1'in aktarıldığı web sitesi: https://www.uab.gov.tr/siber-guvenlik (29.10.2020).

Şekil-5.1: Ulusal Siber Güvenlik Organizasyon Yapısı

5.1.2. USOM, Kurumsal SOME'ler Ve Sektörel SOME'ler

Siber olaylara müdahalede organizasyonel açıdan üç temel bileşen şu şekildedir:

1. *USOM*'nun siber olaylara müdahale açısından temel işlevleri, siber olay öncesinde hazırlanan bülten, duyuru gibi paylaşmak suretiyle ilgilileri *uyarı ve bilgilendirme*, siber olay esnasında Kurumsal SOME ve bağlı olduğu Sektörel SOME arasındaki *koordinasyon*un sağlanması ve siber olay öncesi, esnası ve sonrasında USOM ve/veya Kurumsal SOME'nin bağlı olduğu Sektörel SOME tarafından talep edilen rapor, form ve bilgilendirme açısından *iletişim*i sağlamaktır[612].

2. Kurumsal SOME'ler, kurumlarına doğrudan ya da dolaylı olarak yapılan veya yapılması muhtemel siber saldırılara karşı gerekli önlemleri alma veya aldırma, bu tür olaylara karşı müdahale edilebilecek mekanizmayı ve olay kayıt sistemini kurma veya kurdurma ve kurumlarının bilgi güvenliğini sağlamaya yönelik çalışmayı yapmak veya yaptırmakla yükümlüdür. Kurumsal SOME'ler, siber olayların önlenmesi veya

[612] *Tebliğ*, m. 9.

zararların azaltılmasına yönelik olarak kurumlarının bilişim sistemlerinin kurulması, işletilmesi veya geliştirilmesi ile ilgili çalışmalarda teknik ve idari tedbirler konusunda öneri sunarlar[613].

3. Sektörel SOME'lerin ise adından da anlaşılacağı üzere, özellikle düzenleyici ve denetleyici kurumların bünyesinde kendi sektörlerine özgü olarak ve bu kurum, kuruluş ve işletmeleri kapsayacak şekilde kurulması öngörülmüştür. İhtiyaç duyulması halinde, düzenleyici ve denetleyici kurumların yetki alanı dışında kalan sektörlerle ilgili olarak Bakanlık bünyesinde sektörel SOME kurulabilir[614]. Kritik sektörlerde ise, sektörel SOME kurulması zorunludur. Kritik sektörlerin listesi Kurul tarafından belirlenir, ilgililere duyurulur ve güncellenir. Düzenleyici ve denetleyici kurumlardaki sektörel SOME'lerin eşgüdümü ise Bilgi Teknolojileri Kurumu tarafından yürütülür. Son olarak, sektörel SOME'ler, siber olayların önlenmesi ve zararların azaltılmasına yönelik faaliyetlerini, USOM'la koordineli şekilde yürütürler[615].

5.1.3. 2016-2019 Ulusal Siber Güvenlik Stratejisi İle 2016-2019 Ulusal Siber Güvenlik Eylem Planı

2016-2019 Ulusal Siber Güvenlik Stratejisi" ile "2016-2019 Ulusal Siber Güvenlik Eylem Planı'na[616] bakıldığında, gelişen bilgi ve iletişim teknolojileri, artan güvenlik gereksinimi ve edinilen tecrübe doğrultusunda, UDBH tarafından ulusal siber güvenlik

---

[613] *Tebliğ*, m. 5.

[614] Bkz. *Tebliğ*, m. 6/f. 2. Çalışmada, özellikle bilgi güvenliğinin herkesi kapsayan ve ilgilendiren boyutu ve önemi dikkate alındığında, Sektörel SOME'lerin kurulmasında başta her ne kadar siber güvenlik açısından hayati öneme sahip salt bazı kritik sektörlere ağırlık verilse dahi, özellikle ihtiyaç halinde düzenleyici ve denetleyici kurumların yetki alanı dışındaki sektörler açısından Sektörel SOME kurulması yönündeki anılan düzenlemenin isabetli olduğu değerlendirilmiştir. Bu açıdan, Covid-19'un yarattığı dijital ortam ve bu ortamda siber atakların hem sayı hem de yoğunluk olarak artmasının muhtemel olduğu bir ortamda, Sektörel SOME'lerin ülke çapında eğitim, sağlık, tarım, sivil havacılık gibi birçok sektör açısından kurulmaya devam edilmesi Türkiye'de siber ataklarla etkin mücadele noktasında önemli bir kazanım olacağı öngörülmektedir.

[615] *Tebliğ*, m. 7.

[616] 2016-2019 Ulusal Siber Güvenlik Stratejisi'nin tam metnine ulaşmak için: https://www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf, ayrıca Bkz. https://www.btk.gov.tr/siber-guvenlik-stratejisi-ve-eylem-plani (Gözden Geçirilme Tarihi: 29.10.2020).

stratejisinin güncellenmesi ve 2016-2019 dönemini kapsayan eylemlerin belirlenmesi ihtiyacı doğmuştur. Bu kapsamda hazırlanan "2016-2019 Ulusal Siber Güvenlik Stratejisi" ile "2016-2019 Ulusal Siber Güvenlik Eylem Planı" ile mevcut siber risklerin aşağıda belirlenen ilkeler ışığında asgari düzeye indirilmesi hedeflenmiştir: (i) Stratejik açıdan uluslararası kritik altyapı envanterinin oluşturulması, (ii) kritik altyapıların güvenlik gereksinimlerinin karşılanması ve bu kritik altyapıların bağlı oldukları düzenleyici kurumlar tarafından desteklenmesi, (iii) siber güvenlik alanında denetim yaklaşımını da içeren uluslararası standartlara uygun mevzuatın oluşturulması, (iv) toplumun her kesiminde siber güvenlik bilincinin oluşturulması, (v) eğitim kurumlarının çalışmalarına ilave olarak yazılı ve görsel medyada farkındalık çalışmalarının yapılması gibi stratejik amaçlar hedeflenmiştir[617]. Belirtilen stratejik amaçlara ulaşmak için gerçekleştirilecek eylemler ise, (i) siber savunmanın güçlendirilmesi, (ii) kritik altyapıların korunması, (iii) siber suçlarla mücadele, farkındalık ve insan kaynağı geliştirme, (iv) siber güvenlik ekosisteminin geliştirilmesi ve (v) siber güvenliğin milli güvenliğe entegrasyonu olmak üzere beş stratejik eylem altında toplanarak söz konusu eylem başlıkları eylemlere ayrılmış, planlanan bitirilme tarihlerine ve sorumlu/ilgili kuruluşlarına göre "2016-2019 Ulusal Siber Güvenlik Eylem Planı"nda listelenmiştir.

5.1.4. 2020-2023 Ulusal Güvenlik Stratejisi İle İlgili Gelişmeler

BTK'nın resmî web sitesi üzerinden yayınlanan 19.02.2020 tarihli habere göre, 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı Hazırlık Çalıştayı BTK'da gerçekleştirilmiştir. İlgili haberde özetle, ulusal siber güvenliğin Türkiye'de sağlanmasına yönelik dört yıllık bir vizyon belgesi hayata geçirilecek olan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı hazırlık çalışmaları kapsamında düzenlenen çalıştaya Ulaştırma ve Altyapı Bakan Yardımcısı Dr. Ömer Fatih Sayan'ın katıldığı ve

[617] "2016-2019 Ulusal Siber Güvenlik Stratejisi" ile "2016-2019 Ulusal Siber Güvenlik Eylem Planı" içeriğinde belirlenen tüm stratejik amaçlar burada belirtilmemiş olup sadece örnekleme yoluyla birkaçına yer verilmiştir.

bakan yardımcısının siber güvenlik alanında yapılacak fikir birliğinin önemine dikkat çektiği belirtilmiştir[618].

5.1.5. Türkiye'nin "Siber Vatan" Projesi

12.06.2020 tarihli habere göre Türkiye'de Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yapay zeka strateji belgesinin hazırlandığı, Cumhurbaşkanı Recep Tayyip Erdoğan'ın bu çalışmanın arkasında olduğu ve T.C. Cumhurbaşkanlığı İletişim Başkanı Fahrettin Atun'un da siber vatan olgusuna dikkat çektiği, teknolojinin hayatın her alanında olması nedeniyle Türkiye Cumhuriyeti'nin günümüz dünyasında kara, deniz ve hava sınırlarının yanı sıra sahalarına siber sınırları da eklediği ve vatandaşlarına dijital dünyayı tanıttığı belirtilmiştir[619].

Türkiye'de siber güvenlik alanında önemli gelişmelerin yukarıda değerlendirilmesi akabinde, çalışmanın odak noktası olan elektronik ödeme sistemlerinde siber güvenlik açısından dikkat çeken regülasyonlara dair aşağıda ayrıntılı bilgiye ver verilmiştir.

5.2. TÜRKİYE'DE ELEKTRONİK ÖDEME SİSTEMLERİNDE SİBER GÜVENLİK AÇISINDAN DİKKAT ÇEKEN REGÜLASYONLAR

5.2.1. 5411 Sayılı Bankacılık Kanunu ("Bankacılık Kanunu")

Bankacılık Kanunu ile finansal piyasalarda güven ve istikrarın sağlanmasına, kredi sisteminin etkin bir şekilde çalışmasına, tasarruf sahiplerinin hak ve menfaatlerinin korunmasına ilişkin usul ve esasları düzenlemesi amaçlanmış olup[620] kapsam itibariyle

---

[618] İlgili haberde özellikle bir önceki eylem planı olan 2016-2019 Ulusal Siber Güvenlik Stratejisi Ve Ulusal Siber Güvenlik Eylem Planı kapsamında Türkiye'de siber güvenlik organizasyon yapısının oluşumuna yönelik çok ciddi çalışmalar yapıldığı, bu çerçevede öncelikle BTK çatısı altında USOM'un kurulduğunu, USOM'un ise Sektörel SOME'ler ve Kurumsal SOME'lerle şekillendiği ve gelinen aşamada ise USOM koordinasyonunda görev yapan 14'ü sektörel olmak üzere toplamda 1.291 adet SOME'nin Türkiye'de siber sahanın korunmasına yönelik çalışmaları etkin şekilde yürüttüğü ifade edilmiştir. İlgili habere internet ortamında ulaşmak için: https://www.btk.gov.tr/haberler/2020-2023-siber-guvenlik-stratejileri-btk-da-belirlendi (Gözden Geçirilme Tarihi: 29.10.2020).

[619] https://www.memurlar.net/haber/910508/siber-vatan-cumhurbaskani-erdogan-dikkat-cekmisti.html (Gözden Geçirilme Tarihi: 29.10.2020).

[620] 5411 Sayılı Bankacılık Kanunu Gerekçesi: https://www.tbmm.gov.tr/tutanaklar/TUTANAK/TBMM/d22/c113/tbmm22113072ss1078.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

Bankacılık Kanunu Türkiye'de kurulu mevduat bankaları, katılım bankaları, kalkınma ve yatırım bankaları, yurt dışında kurulu bu nitelikteki kuruluşların Türkiye'deki şubeleri, finansal holding şirketleri, Türkiye Bankalar Birliği, Türkiye Katılım Bankaları Birliği, Bankacılık Düzenleme ve Denetleme Kurumu (*"BDDK"*), Tasarruf Mevduatı Sigorta Fonu ve bunların faaliyetlerinin Bankacılık Kanunu hükümlerine tabi olacağı belirtilmiştir.

Türkiye'de bankacılık mevzuatı açısından güncel bir gelişme olarak Bankacılık Kanunu'nda değişiklik yapılmasını öngören 7222 Sayılı Bankacılık Kanunu İle Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun 25.02.2020 tarihinde 31050 Sayılı Resmi Gazete'de (*"7222 Sayılı Kanun"*)[621] yayınlanarak yürürlüğe girmiştir.

Elektronik ödemelerde siber güvenlik meselesi özellikle bankaların müşterilerine ait sır saklama yükümlülüğü ile doğrudan ilintili olduğundan, bu kısımda Bankacılık Kanunu'nda dikkat çeken m. 73/f. 3 düzenlemesi değişiklik de çalışma kapsamında incelenecektir. Bankacılık Kanunu m. 73/f. 3 eski haliyle bankalara veya müşterilerine ait sır saklama yükümlülüğünü düzenlemektedir. Yeni değişiklik neticesinde[622], bu

---

[621] 7222 Sayılı Kanun'un tam metnine internet üzerinden şu link ile ulaşılabilir: https://www.resmigazete.gov.tr/eskiler/2020/02/20200225-12.htm (Gözden Geçirilme Tarihi: 29.10.2020).

[622] 7222 Sayılı Kanun'un 10. maddesi neticesinde Bankacılık Kanunu m. 73/f. 3'de eklenen cümle aşağıdaki gibidir:

"Bankacılık faaliyetlerine özgü olarak bankalarla müşteri ilişkisi kurulduktan sonra oluşan gerçek ve tüzel kişilere ait veriler, müşteri sırrı hâline gelir. Diğer kanunların emredici hükümleri saklı kalmak kaydıyla, müşteri sırrı niteliğindeki bilgiler, bu maddede belirtilen sır saklama yükümlülüğünden istisna tutulan hâller haricinde, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca müşterinin açık rızası alınsa dahi, müşteriden gelen bir talep ya da talimat olmaksızın yurt içindeki ve yurt dışındaki üçüncü kişilerle paylaşılamaz ve bunlara aktarılamaz. Kurul ekonomik güvenliğe ilişkin yapacağı değerlendirme neticesinde, müşteri sırrı ya da banka sırrı niteliğinde olan her türlü verinin, yurt dışındaki üçüncü kişilerle paylaşılmasını ya da bunlara aktarılmasını yasaklamaya, ayrıca bankaların faaliyetlerini yürütmede kullandıkları bilgi sistemleri ve bunların yedeklerinin yurt içinde bulundurulması hususunda karar almaya yetkilidir. Bu maddede belirtilen sır saklama yükümlülüğünden istisna tutulan hâllerde yapılacak paylaşımlar da dâhil olmak üzere, müşteri sırrı ve banka sırrı niteliğindeki bilgiler, sadece belirtilen amaçlarla sınırlı olmak ve ölçülülük ilkesine uygun olarak bu amaçların gerektirdiği kadar veriyi içermek kaydıyla paylaşılabilir."

Sır niteliğindeki bilgilerin, üçüncü ve dördüncü fıkralar uyarınca yapılacak paylaşım ve aktarımlarına ilişkin kapsam, şekil, usul ve esasları belirlemeye veya bunlara ilişkin sınırlamalar getirmeye Kurul yetkilidir."

hüküm artık yasa koyucu tarafından daha detaylı şekilde düzenlenmiş olup müşteri sırı[623] niteliğindeki bilgilere özel bir önem atfederek ve BDDK'yı, kişisel verileri korumakla görevli olan Kişisel Verileri Koruma Kurulu (*"KVK Kurulu"*)'nun da üzerinde bir konuma taşımıştır. İlgili düzenleme uyarınca BBDK müşteri sırrı niteliğindeki bilgiler söz konusu olduğunda müşteri sırrı ya da banka sırrı niteliğinde olan her türlü verinin, yurt dışındaki üçüncü kişilerle paylaşılmasını ya da bunlara aktarılmasını yasaklamaya, ayrıca bankaların faaliyetlerini yürütmede kullandıkları bilgi sistemleri ve bunların yedeklerinin yurt içinde bulundurulması hususunda karar almaya yetkili kılınmıştır. Aynı zamanda, değişiklik neticesinde müşteri sırrı niteliğindeki bilgilerin paylaşım ve aktarımına ilişkin kapsam, şekil, usul ve esasların belirlenmesi veya bunlara ilişkin sınırlamalar konusunda BDDK'ya geniş bir takdir yetkisi tanındığı görülmektedir. Öte yandan, veri koruma hukuku kapsamında dikkat çeken bir diğer husus ise açık rıza alınsa dahi, açık rıza hususunda 6698 Sayılı Kişisel Verilerin Korunması Kanunu kapsamında açık rıza[624] açısından öngörülen düzenlemeler uygulanmayarak müşteri sırrı niteliğindeki bilgiler konusunda

[623] Müşteri sırrı, 21.10.2011 tarihinde hükümsüz kalan tasarıda banka ve ticari işletme gibi kuruluşların kendi iştigal alanlarıyla ilgili olarak müşteriyle olan ilişkilerinde, müşterinin şahsi, ekonomik, mali, nakit ve kredi durumuna ilişkin doğrudan veya dolaylı olarak edinilen tüm bilgi ve belgeler olarak ifade edilmiştir. Bkz. Ticari Sır, Banka Sırrı ve Müşteri Sırrı Hakkında Kanun Tasarısı, http://www.kgm.adalet.gov.tr/tasariasamalari/tbmmkms/tbmmkom/ticarisir.pdf (Gözden Geçirilme Tarihi: 29.10.2020). Ancak, Bankacılık Kanunu'nda yapılan değişiklik neticesinde, müşteri sırrı açısından kanun koyucunun bankacılık faaliyeti "sonrasındaki" verilerle sınırlı tutulduğu görülmektedir. Doktrinde ise bu durum Dülger tarafından birçok kanun ve yargı kararlarındaki tanımlar açısından bankacılık faaliyeti öncesi ve sonrası herhangi bir ayrım öngörülmediğinden eleştirilmiştir. Bkz. Murat Volkan Dülger, "7222 Sayılı Kanun ile 5411 sayılı Bankacılık Kanunu'nda Yapılan Düzenlemenin KVK Hukuku Açısından Değerlendirilmesi" başlıklı makalesi, (*"Dülger, 7222 Sayılı Kanun"*): https://www.hukukihaber.net/7222-sayili-kanun-ile-5411-sayili-bankacilik-kanununda-yapilan-duzenlemenin-kvk-hukuku-acisindan-degerlendirilmesi-makale,7537.html (Gözden Geçirilme Tarihi: 29.10.2020)

[624] 6698 Sayılı Kişisel Verilen Korunması Kanunu m. 3/1/a'ya göre açık rıza, belirli bir konuya dair bilgilendirilmeye dayanan ve özgür iradeyle açıklanması gereken rıza anlamına gelmektedir. Bkz. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf (Gözden Geçirilme Tarihi: 04.06.2020). GDPR'de ise açık rıza, ilgili kişinin beyan veya açık bir onay eylemi sonucunda kendisine ait kişisel verilerin işlenilmesine onay gösterdiğini ifade eden özgür şekilde verilmiş olan spesifik, bilinçli ve açık rıza göstergesi şeklinde tanımlanmıştır. (GDPR, m. 4/11): https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (Gözden Geçirilme Tarihi: 29.10.2020).

müşteriden gelen bir talep ya da talimat olmaksızın yurt içindeki ve yurt dışındaki üçüncü kişilerle paylaşılamayacağına ve aktarılamayacağı hüküm altına alınmıştır.

Bankacılık Kanunu'na eklenen yukarıdaki düzenleme ile ilgili hükmün gerekçesi[625] incelendiğinde, her ne kadar uygulamadaki bazı sorunların giderilmesi amacıyla bu hükmün getirildiği belirtilmişse de doktrinde Dülger tarafından ilgili düzenleme şu açıdan eleştirilmiştir: Dülger'e göre müşteri sırrı kapsamında giren bilgiler açısından bu düzenlemenin 6698 Sayılı Kanun'da açıkça yer alan "rıza metni" ve "açık rıza" gibi prosedürlerin işlerliğini olumsuz yönde etkileyebilecektir. Ayrıca anılan yazar, müşteri sırrı açısından aslında mevzuatta ve yargı kararlarında herhangi bir zamansal ayrım öngörülmemesine rağmen yeni düzenleme neticesinde müşteri sırrının, bankacılık faaliyeti sonrasında oluşan verilerle sınırlı tutulması sebebiyle BDDK'nın bu durumu nasıl yorumlanacağının henüz bilinmediğine ve zaman konusundaki bu sınırlamanın uygulamada bazı sorunlara sebebiyet verebileceğine dikkat çekmiştir. Son olarak, Dülger tarafından normalde kişisel verilerin paylaşılması ve aktarılmasına ilişkin yetkilerin 6698 Sayılı Kanun kapsamında Kişisel Verilerin Korunması Kurulu ("KVK Kurulu")'nda iken banka müşterilerinin kişisel verilerinin paylaşılması ve aktarılmasına ilişkin yetkilerin artık BDDK olup olmadığı hususunun netlik taşımadığı belirtilmiştir[626]. Çalışmada, yazar tarafından Dülger'in bu görüşü doğru bir yaklaşım olarak değerlendirmekle beraber, gerçekten de elektronik ödemeler de dahil olmak üzere bankacılık işlemlerinde müşteri sırrı olması halinde hangi gerekçe ile veri aktarımı ve paylaşımı konusunda KVK Kurulu'nun yetki alanından çıkılarak BDDK'nın yetkin kılındığı anlaşılamamıştır. Özellikle hükmün içerik olarak "bankacılık faaliyetleri sonrasındaki faaliyetlerle" sınırlı tutulması nedeniyle (bankacılık faaliyetlerinden önce müşteri sırrı niteliğindeki veriler konusunda etkin kurumun KVK Kurulu olması ve bankacılık faaliyetlerinden sonra ise BDDK'nın bu alanda yetkin olması nedeniyle) özellikle "hukuki istikrar" ilkesi açısından konuya

[625] 06.02.2020 tarihinde verilen 98 sayılı, 7222 sayılı Kanun'un Gerekçe Metni.
[626] *Dülger, 7222 Sayılı Kanun.*

bakıldığında uygulamada sıkıntı yaratabileceği değerlendirilmiştir. Öte yandan, Türkiye'de birçok mevzuat hükmünde olduğu gibi yasama tekniği açısından bir kurallar bütünü olan ve bu bağlamda sistematiği olan 6698 Sayılı Kişisel Verilerin Korunması Hakkındaki Kanun açısından öngörülen "açık rıza" kurumunun başka bir düzenleme ile etkisiz hale getirilmesi uygulamada farklı sorunlara yol açabilecektir. Bu sorunlara örnek olarak, bankaların müşterilerinden usulüne uygun şekilde aldığı açık rızanın mevcut olmasına rağmen Bankacılık Kanunu'un anılan düzenlemesi gereği bu rızanın geçersiz kabul edilmesinin ve veri aktarımı konusunda ayrıca bir talep ya da talimat beklemenin uygulamaya dair süreçlerle uyumlu olmadığı, düzenleme değişikliği ile müşteri sırrı her ne kadar bankacılık faaliyeti sonrasında oluşan verilerle sınırlı tutulsa da, müşteri ilişkisi kurulmadan önce (başka bankalar tarafından) temin edilen verilerin diğer bankalar açısından müşteri sırrı sayılmayacak şeklinde yorumlanabileceği, ayrıca müşteri sırrı niteliğindeki veriler açısından kanun gerekçesinde her ne kadar uygulamadaki sıkıntıların giderilmesine yönelik bu düzenlemenin öngörüldüğü belirtilse dahi, uygulamada özellikle Bankacılık Kanunu md. 73 anlamında bir veri ihlali olması halinde hem BDDK hem de KVK Kurulu'nun her iki kurum olarak da karar alabilmesi imkânı olması gösterilebilir.

Son olarak, bu kısımda elektronik ödemelerde siber güvenliğin temini özellikle Covid-19 pandemi salgının kişiler arasındaki sosyal mesafeyi zorunlu koşullar itibariyle özellikle uzaktan kimlik erişimi yöntemleri açısından da doğrudan incelenmesi gereken bir mesele olduğundan, bu konuda Türkiye'de yasa koyucu tarafından bu kapsamda öngörülen yasal değişikliğe de değinmek gerekecektir. 7247 Sayılı Bazı Kanunlarda Ve Kanun Hükmünde Kararnamede Değişiklik Yapılması Hakkında Kanun (*"7247 Sayılı Kanun"*)[627], 26.06.2020 tarihli ve 31167 Sayılı Resmi Gazete'de yürürlüğe girmesi sonucunda, Türkiye'de ilk kez bankacılık ve telekomünikasyon sektörlerine

[627] 7247 Sayılı Kanun'un elektronik ortamda tam metnine ulaşmak için bkz. https://www.resmigazete.gov.tr/eskiler/2020/06/20200626-1.htm (Gözden Geçirilme Tarihi: 29.10.2020).

yönelik olarak "digital onboarding"[628] kapsamında düzenlemelere yer verilerek bu kurumun önünün açılmak istendiği görülmüştür. Söz konusu kanunun Genel Gerekçe[629] kısmına bakıldığında, Türkiye Cumhuriyeti'ndeki vatandaşların özellikle finans ve elektronik haberleşme sektörüne yönelik hizmet veren kuruluşlarla yapacakları işlemlerin elektronik ortamda sözleşmelerin elektronik ortamda düzenlenmesine imkân verileceği belirtilmiştir. 7247 Sayılı Kanun neticesinde, 5411 Sayılı Bankacılık Kanunu m. 76/f.2'de değişikliğe gidilerek bankalar ve müşterileri arasındaki ilişkilerin yazılı olarak, uzaktan iletişim araçlarının kullanılması suretiyle mesafeli olarak, mesafeli mesafeli olsun veya olmasın uzaktan iletişim araçlarının kullanılması suretiyle BDDK tarafından belirlenen bir elektronik haberleşme cihazı vasıtasıyla müşteri kimlik doğrulaması yapılması öngörülmektedir. Bu düzenleme değişikliği ile BDDK tarafından özellikle bankacılık sektörüne yönelik hangi elektronik haberleşme cihazları ile ve ne tarz yöntemlerle elektronik ortamda sözleşme gerçekleştirileceği henüz bilinmemekle beraber özellikle finans sektörü açısından Türkiye'de de yaşanan Covid-19 pandemi salgının yarattığı şartlar da gözetildiğinde, bu düzenlemenin önemli bir değişiklik olduğu açıktır. Ancak, BIS tarafından 2020 yılı Mayıs ayında yayınlanan raporda "dijital onboarding" gibi uzaktan mesafe ile finansal işlem gerçekleştirilmesine imkan tanıyan ve bu bağlamda kimlik doğrulama açısından teknolojik alandaki inovasyonların takip edilmesinin özellikle Covid-19 döneminde finans dünyasında müşterilere esneklik sağlayacağı belirtilmekle beraber Covid-19'un yarattığı özel koşullar sebebiyle siber saldırganların daha aktif hale gelebileceği ve

[628] "Digital onboarding" olarak adlandırılan süreçte, eIDAS Tüzüğü kapsamında nitelikli güven hizmeti sağlayıcıların, ilgili prosedürün ulusal seviyede düzenlenmesi ve eIDAS ile uyumlu olması şartıyla, video konferans vasıtasıyla belge düzenleyerek bir kişinin kimliğini doğrulamasının mümkün olduğu kabul edilmektedir. Bu konuda, Almanya'da kurulan ve tamamen dijital olarak çalışan N26 şirketinin kişileri, müşteri yapma süreci somut bir örnek olarak gösterilmiştir. Özellikle doktrinde Keser Berber tarafından eIDAS m. 24/f. 1 (d) gereğince, video konferansın ulusal düzeyde fiziksel varlığa oranla güvenlilirlik açısından eş değer ölçüde güvence sağladığı ve uygunluk değerlendirme kuruluşları açısından bu yöntemin onaylanması durumunda video konferansın bir kimlik doğrulama aracı olabileceği değerlendirilmiştir. Bu konuda detaylı bilgi için bkz. *Keser Berber, Güven Hizmetleri,* s. 42-43.

[629] https://www2.tbmm.gov.tr/d27/2/2-2945.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

digital onboarding de dahil olmak üzere uzaktan mesafeli şekilde gerçekleştirilen finansal işlemlerde özellikle dikkatli olunması gerektiği vurgulanmıştır[630].

5.2.2. 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun

PSD2'nin Avrupa Birliği'nde yürürlüğe girmesinden sonra, yakın bir zaman içerisinde Avrupa Birliği müktesebatına uyum, ödeme ve menkul kıymet mutabakat sistemlerinin altyapısının güçlendirilmesi ve uluslararası standartlara uyum çerçevesinde ilk kez 2008 yılında Türkiye Cumhuriyeti Merkez Bankası (*"TCMB"*)'na ödeme sistemlerine yönelik kanun hazırlama sorumluluğu verildiği bilinmektedir[631]. TCMB tarafından ilk taslağı hazırlanan 6493 sayılı "Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun" (*"6493 Sayılı Kanun"*), 27.06.2013 tarih ve 28690 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir[632].

6493 Sayılı Kanun ile kısaca özetlemek gerekirse, Türkiye'de yukarıda da belirtildiği üzere ödeme sistemlerinin hukuki altyapısı düzenlenerek müşterilere ödeme hizmeti sunan veya elektronik para ihracı faaliyetinde bulunan ödeme hizmeti sağlayıcıları, ödeme kuruluşları ve elektronik para kuruluşları ile ilgili olarak BDDK ve TCMB'yi ilgilendiren kapsamlı düzenlemelere yer verilmiştir[633].

6493 sayılı Kanun uyarınca, Türkiye'de ilk defa "ödeme sistemi", "menkul kıymet mutabakat sistemi", "ödeme hizmeti sağlayıcısı", "ödeme kuruluşu" ve "elektronik para kuruluşu" gibi kavramlar tanımlanmıştır. 6493 Sayılı Kanun'un Genel Gerekçesi

---

[630] Juan Carlos Crisanto/ Jermy Prenio, "Financial crime in times of Covid-19 – AML and cyber resilience measures", BIS, FSI Briefs, No: 7, (*"Crisanto/Prenio"*), s. 10, ilgili rapora ulaşmak için bkz. https://www.bis.org/fsi/fsibriefs7.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[631] *TCMB, Ödeme Sistemleri,* s.5.

[632] 6493 Sayılı Kanun metnine elektronik ortamda ulaşmak için bkz. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6493.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[633] 6493 Sayılı Kanun'un Gerekçesi: https://www.tbmm.gov.tr/sirasayi/donem27/yil01/ss117.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

incelendiğinde ise, elektronik ödeme sistemlerinde siber güvenliği ilgilendiren boyutu itibariyle söz konusu Kanun ile hedeflenen olgulardan birisinin de, ödeme hizmetlerinin temel olarak gönderenden alınan fonun alıcıya ulaştırılması ilkesine dayanması sebebiyle, bu tür işlemlerde sektöre olan güveni olumsuz etkileyebilecek uygulamaların önlenmesi amacıyla banka-dışı kuruluşların ödeme hizmetleri alanında işlem gerçekleştirirken faaliyetlerinin düzenlenmiş olması gerektiğine dikkat çekilmiştir[634].

6493 Sayılı Kanun, toplam 8 bölümden ve 43 maddeden oluşmaktadır. Bu noktada, 6493 Sayılı Kanun açısından özellikle elektronik ödeme sistemleri ve bilgi güvenliği açısından önemli olduğu düşünülen düzenlemeler aşağıda özetlenmiştir:

Genel itibariyle çalışma kapsamında ele alınan elektronik para[635], ödeme hizmeti[636] ve kişisel güvenlik bilgileri[637] gibi kavramların Türk Hukuku açısından tanımlarına yer verilmiştir.

6493 Sayılı Kanun'un İkinci Bölümü'nde özellikle ödeme sistemi ve menkul kıymet mutabakat sistemine ilişkin spesifik düzenlemelere (sistem işleticisinin faaliyet izni alabilmesi için hangi kriterleri taşıması gerektiği, faaliyet izni ile ilgili hükümler, sistem gözetimi ve önlem alınmasını gerektiren haller ve alınacak tedbirler, vb.) yer

---

[634] 6493 Sayılı Kanun'un Genel Gerekçesi'ne şu link üzerinden ulaşılabilir: https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss473.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[635] Elektronik para, 6493 Sayılı Kanun'da ihraç eden kuruluş tarafından kabul edilen fon karşılığı ihraç edilen, elektronik şekilde muhafaza edilen, 6493 Sayılı Kanun çerçevesinde tanımlanan ödeme işlemlerini gerçekleştirmek için kullanılan ve elektronik para ihraç eden kuruluş haricindeki gerçek ile tüzel kişiler tarafından da ödeme aracı olarak kabul edilen parasal değer olarak tanımlanmıştır (*6493 Sayılı Kanun,* m. 3/f. 1/ç).

[636] Ödeme hizmeti ise, üç yahut daha fazla katılımcı arasındaki transfer emirleriyle bağlantılı olarak fon aktarımlarının gerçekleştirilmesini temin etmek amacıyla yapılan takas ve mutabakat işlemleri için gerekli altyapıyı sunan ve yeknesak kuralları olan yapıyı, ifade etmektedir (*6493 Sayılı Kanun,* m. 3/f. 1/v).

[637] Bilgi güvenliği kapsamında 6493 Sayılı Kanun'daki tanımlar bölümüne bakıldığında, kişisel güvenlik bilgileri, ödeme aracı ile işlem gerçekleştirirken kullanılabilecek şifre, son kullanma tarihi, güvenlik numarası gibi ödeme aracını ve ödeme aracı kullanıcısının kimliğini belirleyici bilgilerini içermektedir (*6493 Sayılı Kanun,* m. 3/f. 1/ğ).

verilmiştir. Bilgi güvenliği açısından, 6493 Sayılı Kanun'un m. 9/f. 1/c'de sistemin güvenliğinin, sağlamlığının ve istikrarının tehlikeye düşürülmesinin sistemin işleyişi ile ilgili banka tarafından önlem alınmasını gerektiren bir durum olduğu düzenlenmiştir.

6493 Sayılı Kanun'un 12. maddesinde, ödeme hizmeti olarak kabul edilecek ve kabul edilmeyecek durumların neler olduğu ayrıntılı şekilde belirlenmiş olup özellikle 12.11.2019 tarihinde 7192 Sayılı Kanun[638] ile yapılan değişiklik sonucunda ödeme hizmeti kullanıcısının isteği üzerine başka bir ödeme hizmeti sağlayıcısında bulunan ödeme hesabıyla ilgili sunulan ödeme emri başlatma hizmeti, ödeme hizmeti kullanıcısının onayının alınması koşuluyla, ödeme hizmeti kullanıcısının ödeme hizmeti sağlayıcıları nezdinde bulunan bir veya daha fazla ödeme hesabına ilişkin bir araya getirilen bilgilerin, çevrim içi platformlarda sunulması hizmeti ve ödemeler alanında toplam büyüklük veya etki alanı açısından banka tarafından belirlenecek seviyeye ulaşan diğer işlem ve hizmetleri ödeme hizmeti kapsamında değerlendirilmiştir. Kanun'un 13. maddesinde ödeme hizmet sağlayıcıları, 5411 Sayılı Kanun kapsamındaki bankalar, elektronik para kuruluşları, ödeme kuruluşları ile PTT olarak belirlenmiştir.

6493 Sayılı Kanun'un 23. maddesinde sistem işleticisinin, ödeme kuruluşunun ve elektronik para kuruluşunun 6493 Sayılı Kanun'da yer alan hususlar ile ilgili belgeleri ve kayıtları en az on yıl süreyle güvenli ve talep edildiği anda erişime imkân verecek suretle yurt içinde tutması ve sistem işleticisinin faaliyetlerini yürütmede kullandığı bilgi sistemleri ve bunların yedeklerinin de yurt içinde tutması öngörülmüştür. Özellikle, 23. maddede belirtilen belgeleri ve kayıtları saklama yükümlülüğüne aykırı

[638] 7192 Sayılı "Ödeme Ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri Ve Elektronik Para Kuruluşları Hakkında Kanun İle Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun 22.11.2019 tarihinde 30956 Sayılı Resmi Gazete'de yayınlanarak yürürlüğe girmiştir. Kanunun tam metnine ulaşmak için: https://www.resmigazete.gov.tr/eskiler/2019/11/20191122-2.htm (Gözden Geçirilme Tarihi: 29.10.2020).

şekilde hareket edilmesi halinde, bu düzenlemenin yaptırımı 6493 Sayılı Kanun'un 32. maddesi gereğince bir yıldan üç yıla kadar hapis ve beş yüz günden bin beş yüz güne kadar adli para cezası ile cezalandırılması hükme bağlanmıştır. Bilgi güvenliği açısından dikkati çeken bir diğer düzenleme ise md. 32/2'de ödeme aracını kullanmaya yetkili olanlar dışındaki üçüncü kişilerin ödeme aracı ile ilgili kişisel güvenlik bilgilerine erişimlerinin engellenmesi için gerekli önlemleri almayan, ödeme aracının ve ödeme aracı ile ilgili kişisel güvenlik bilgilerinin ödeme hizmeti kullanıcısına güvenli bir şekilde ulaştırılmasını sağlamayan kuruluşların görevlileri ve işlemi yapan kişiler hakkında bir yıldan üç yıla kadar hapis ve bin güne kadar adli para cezası ile cezalandırılacağı düzenlenmiştir.

6493 Sayılı Kanun'un 32. maddesinde sırların açıklanması suçu, 33. maddede itibarın zedelenmesi suçu, 35. maddede işlemlerin kayıt dışı bırakılması ve gerçeğe aykırı muhasebeleştirme suçu ve 36. maddede zimmet gibi bu kanuna özgü farklı suç tiplerine ve bu suçların nasıl cezalandırılacağına ilişkin ayrıntılı düzenlemeler bulunmaktadır.

22.11.2019 tarihinde 30956 Sayılı Resmî Gazete'de yürürlüğe giren ve 6493 Sayılı Kanun'da değişiklik öngören 7192 Sayılı "Ödeme Ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri Ve Elektronik Para Kuruluşları Hakkında Kanun İle Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun" çerçevesinde özetle çalışmayı ilgilendiren şu hususlarda değişikliğe gidildiği görülmüştür[639]:

7192 Sayılı Kanun'un yürürlüğe girmesi ile ödeme hizmetleri ile elektronik para konusunda BDDK ve TCMB arasındaki yetki noktasındaki ikili yapıya son verilerek ödeme hizmeti sağlayıcıları ile eletronik para kuruluşlarının bağlı oldukları düzenleme ve denetleme yetkilerinin TCMB'ye verilmesi öngörülmüştür. 6493 Sayılı Kanun'un, ilk kez 2013 yılında yürürlüğe girmesi sonucunda, 7192 Sayılı Kanun'un yürürlüğe

[639] 7192 Sayılı Kanun'un tam metnine ulaşmak içib bkz. https://www.resmigazete.gov.tr/eskiler/2019/11/20191122-2.htm (Gözden Geçirilme Tarihi: 29.10.2020).

girmesinden önce, BDDK'nin ödeme hizmet sağlayıcıları konusuda, TCMB'nin ise ödeme hizmet sağlayıcıları veya diğer finansal kuruluşların üye olarak birbirleri arasında gerçektirdikleri işlemler, ödeme sistemler ve menkul kıymet mutabakat sistemleri üzerinde yetkisi mevcut iken, kanun değişikliği ile anılan tüm BDDK'nın bu alandaki tüm yetkilerinin TCMB'ye devri öngörülmüştür. Ayrıca ödeme ve elektronik para ihracı sektörlerini düzenlemek konusunda ikincil düzenlemeleri çıkarma yetkisi de yine TCMB'ye verilmiştir.

AB'nin yukarıda belirtilen PSD2 Tüzüğü düzenlemelerine paralel şekilde, 7192 Sayılı Kanun'un yürürlüğe girmesi sonucunda iki yeni ödeme hizmeti olarak; (i) müşterinin talebi doğrultusunda başka bir ödeme hizmet sağlayıcısında bulunan ödeme hesabıyla ilgili sunulan ödeme emri başlatma hizmeti ve (ii) müşterinin teyidini almak kaydıyla, müşterinin ödeme hizmeti sağlayıcılarında bulunan bir veya daha fazla ödeme hesabına ilişkin konsolide edilmiş bilgilerin çevrim içi platformlarda sunulması hizmeti verilmesi düzenlenmiştir.

Türkiye Ödeme Ve Elektronik Para Kuruluşları Birliği'ne yer verilerek 6493 Sayılı Kanun kapsamında yasal altyapısına ilişkin düzenlemeler öngörülmüştür[640].

Son olarak, yukarıda belirtilen ve "digital onboarding" ile ilgili 7247 Sayılı Kanun neticesinde[641], aynı zamanda 6493 Sayılı Kanun kapsamında da değişikliğe gidilmesi

---

[640] 7192 Sayılı Kanun'un 15. maddesinde, 6493 Sayılı Kanun'a eklenen Ek Madde 1 hükmü ile Birliğin görevlerine, organ seçimine ve uygulacak idari para cezasına ilişkin düzenlemelere yer verilmiştir. Türkiye Ödeme Ve Elektronik Para Kuruluşları Birliği ile ilgili ayrıntılı değerlendirmeler konusunda çalışmanın 5.2.5 numaralı başlığı altındaki açıklamalar dikkate alınabilir.

[641] 7247 Sayılı Kanun'un 16. maddesi şu düzenlemeyi içermektedir:
*"*MADDE 16 – *20/6/2013 tarihli ve 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanunun 12 nci maddesinin üçüncü fıkrasına aşağıdaki cümle eklenmiştir.*
"Çerçeve sözleşme yazılı şekilde veya uzaktan iletişim araçlarının kullanılması suretiyle mesafeli olarak ya da mesafeli olsun olmasın Bankanın yazılı şeklin yerine geçebileceğini belirlediği ve bir bilişim veya elektronik haberleşme cihazı üzerinden gerçekleştirilecek ve müşteri kimliğinin doğrulanmasına imkân verecek yöntemler yoluyla kurulacak şekilde düzenlenir."

öngörülmüştür. Buna göre, 6493 Sayılı Kanun'un müşteriler ve ödeme hizmeti sağlayıcılar arasında akdedilen çerçeve sözleşmeleri düzenleyen m. 12/f. 3 düzenlemesi de tadil edilerek sözleşmelerin yazılı şekil dışında, yukarıda belirtilen 5411 Sayılı Kanun'a benzer şekilde uzaktan iletişim araçlarının kullanılarak veya (TCMB tarafından belirlenen müşteri kimliğinin belirlenmesine imkân sağlayan) elektronik haberleşme cihazı üzerinden geçerli şekilde kurulabilmesine imkân sağlanmıştır.

5.2.3. Ödeme Hizmetleri Ve Elektronik Para İhracı İle Ödeme Kuruluşları Ve Elektronik Para Kuruluşları Hakkında Yönetmelik ("Ödeme Hizmetleri Yönetmeliği")

27.06.2014 tarihinde 29043 Sayılı Ödeme Hizmetleri Yönetmeliği, özellikle 6493 Sayılı Kanun'un bazı hükümlerine (ilgili kanunun 12, 14, 18, 19, 20, 21, 22, 23, 24, 25 ve 26'ncı maddelerine) ilişkin usul ve esasları düzenlemek amacıyla yürürlüğe girmiştir[642].

Ödeme Hizmetleri Yönetmeliği'nin çalışmayı ilgilendiren hükümleri aşağıda özetlenmiştir:

Ödeme Hizmetleri Yönetmeliği'nin 44. maddesi gereğince, ödeme hizmeti sağlayıcısı, ödeme aracının hileli veya yetkisiz kullanımı şüphesini doğuran herhangi bir durum olması halinde ödeme aracını kullanıma kapatır ve ödeme hizmet sağlayıcısının diğer kanunlarda yer alan bilgi verilmesini engelleyici hükümler ile güvenliği tehdit edici objektif nedenlerin bulunması hali dışında göndereni kullanıma kapatma gerekçesi

---

7247 Sayılı Kanun'un tam metnine ulaşmak için: https://www.resmigazete.gov.tr/eskiler/2020/06/20200626-1.htm (Gözden Geçirilme Tarihi: 29.10.2020).

[642] Yönetmelik hükümlerine aşağıdaki link üzerinden ulaşılabilir: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=19816&MevzuatTur=7&MevzuatTertip=5 (Gözden Geçirilme Tarihi: 29.10.2020).

konusunda bilgilendirme yükümlülüğü söz konusudur[643]. Bu konuda, aynı zamanda ödeme hizmeti kullanıcısının benzer şekilde ödeme aracı ile ilgili kişisel güvenlik bilgilerinin kişisel güvenlik bilgilerinin korunmasına yönelik gerekli önlemleri almak ve ödeme aracını ihraç ve kullanım koşullarına uygun olarak kullanmak ve ödeme aracının kaybolması, çalınması veya iradesi dışında gerçekleşmiş herhangi bir işlemi öğrenmesi halinde, ödeme hizmeti kullanıcısı durumu derhal ödeme hizmeti sağlayıcısına veya ödeme hizmeti sağlayıcısı tarafından belirlenmiş kuruluşa bildirmekle yükümlü olduğu belirtilmiştir.

Ödeme Hizmetleri Yönetmeliği'nin 45. maddesinde ise, yetkilendirilmemiş veya hatalı gerçekleştirilmiş işlemlerde tarafların hak ve yetkileri düzenlenmiş olup bu konuda özellikle m. 45/f. 2, ispat yükü açısından önemli bir düzenlemedir. Bu hükme göre, herhangi bir sebepten ötürü ödeme hizmeti kullanıcısı gerçekleşmiş bir ödeme işlemini yetkilendirmediğini veya işlemin doğru bir şekilde gerçekleşmediğini iddia ettiği takdirde, bu durumun aksini (bu işlemin ödeme hizmeti kullanıcısı tarafından onaylandığını, doğru bir şekilde kaydedildiğini ve hesaplara işlendiğini) ispat yükümlülüğü ödeme hizmeti sağlayıcısına ait olduğu düzenlenmiştir.

Ödeme hizmeti sağlayıcının sorumluluklarına yönelik Ödeme Hizmetleri Yönetmeliği'nde spesifik bazı düzenlemelere yer verilmiş olup yönetmeliğinde 54. maddesinde "hatalı kimlik tanımlayıcıları"[644] açısından 55. maddede ise "işlemin

[643] *Ödeme Hizmetleri Yönetmeliği,* m. 44/f. 2.

[644] Yönetmeliğe göre, kimlik tanımlayıcıya doğru bilgilerin girilmesi önem taşımakta olup gönderen tarafından belirtilen kimlik tanımlayıcıya uygun şekilde yapılan ödeme işlemleri doğru gerçekleştirilmiş sayılacağı ve ödeme hizmeti kullanıcısı tarafından kimlik tanımlayıcıya ilave bilgiler verilmiş olsa dahi, ödeme hizmeti sağlayıcısının ödeme işleminin sadece kimlik tanımlayıcı ile gerçekleştirilmesinden sorumlu olduğu belirtilmiştir. Ödeme hizmeti kullanıcısı tarafından belirtilen kimlik tanımlayıcının hatalı olması halinde, ödeme hizmeti sağlayıcısı ödeme işleminin gerçekleştirilmemesinden veya hatalı gerçekleştirilmesinden sorumlu tutulamayacağı düzenlenmiştir.

gerçekleştirilememesi veya hatalı gerçekleştirilmesinden"[645] dolayı ödeme hizmet sağlayıcının sorumluluğuna ilişkin düzenlemelere yer verilmiştir.

5.2.4. Ödeme Hizmetlerinde TR Karekodunun Üretilmesi Ve Kullanılması Hakkında Yönetmelik ("TR Karekodu Yönetmeliği")

Karekodu doğrudan elektronik ödeme işlemlerinde kullanılabilen bir teknolojik enstrüman olması ve elektronik ödeme sistemlerinde siber güvenliği doğrudan ilgilendirmesi sebebiyle, TR Karekodu Yönetmeliği bu çalışma kapsamında incelenecektir. 21.08.2020 tarihinde yayınlanan 31220 Sayılı Resmî Gazete ile yürürlüğe giren TR Karekodu Yönetmeliği[646] ile kısaca belirtmek gerekirse, 6493 Sayılı Kanun kapsamında ödeme hizmetlerinde TR karekodun üretilmesi ve kullanılmasına ilişkin usul ve esasların düzenlenmesi amaçlanmıştır[647].

TR Karekodu Yönetmeliği'nde, karekodu, tarama yöntemiyle ödeme işlemlerinde kullanılmak üzere oluşturulan; alfa numerik verileri, karakterleri ve simgeleri saklanabilen, bakan kişiye göre sol alt köşede, sol üst köşede ve sağ üst köşede üç kare desen işaretleyiciden oluşan ve kare siyah-beyaz noktalar ya da pikseller şeklinde siyah ve beyaz modüllere sahip olan iki boyutlu kod olarak tanımlanmıştır[648]. TR karekodu ise, karekodu ile ilgili yukarıda yer verilen genel tanımdan farklı olarak, teknik

---

[645] Ödeme emrinin gönderen tarafından verildiği ödeme işlemlerinde, öncelikle gönderenin ödeme hizmeti sağlayıcısının, ödeme işleminin doğru gerçekleştirilmesinden gönderene karşı sorumlu olduğu, gönderenin ödeme hizmeti sağlayıcısının ancak ödeme emrinin alındığı tarihte derhal ve her halükarda en geç izleyen iş günü sonuna kadar ödeme işleminin tutarını alıcının ödeme hizmeti sağlayıcısının hesabına aktardığı ve alıcının ödeme hizmeti sağlayıcısının ödeme tutarını aldığını ispatlaması halinde, ödeme işleminin doğru gerçekleştirilmesinden bu sorumluluktan kurtulabileceği ve bu duruma alıcının ödeme hizmeti sağlayıcısı sorumlu olacağı düzenlenmiştir. Gönderenin ödeme hizmeti sağlayıcısının sorumlu, ödeme işleminin gerçekleşmemiş veya hatalı gerçekleşmiş kısmını gecikmeden gönderene iade edeceği ve tutarın ödeme hesabından düşülmüş olması halinde ödeme hesabını eski durumuna getireceği belirtilmiştir.

[646] TR Karekodu Yönetmeliği ile ilgili tam metne ulaşmak için: https://www.resmigazete.gov.tr/eskiler/2020/08/20200821-4.htm (29.10.2020).

[647] *TR Karekodu Yönetmeliği,* m. 1.

[648] *TR Karekodu Yönetmeliği,* m. 3/f. 1/g.

dokümanda[649] yer alan usul ve esaslara göre oluşturulan ve 6493 sayılı Kanun kapsamındaki ödemelerde kullanılabilecek olan karekodunu ifade etmektedir[650].

Elektronik ödeme sistemlerinde siber güvenlik açısından TR Karekodu Yönetmeliği'nin bu çalışmayı ilgilendiren düzenlemeleri kısaca şunlardır:

Öncelikle, bankaların TR karekod kullanılacak ödeme işlemlerine üst sınır getirebileceği, bu bağlamda bankaların, ödeme hizmeti sağlayıcılarından, TR karekod işlemlerinin gerçekleştirildiği sistem işleticilerinden, işyerlerinden, dış hizmet sağlayıcıları gibi faaliyetleri karekod ile ödeme yapılmasıyla ilgili taraflardan gereken bilgi ve belgeleri istemeye ve ihtiyaç halinde yerinde inceleme yapmaya yetkili olduğu hüküm altına alınmıştır[651].

TR Karekodu Yönetmeliği'nin 8. maddesinde yönetmelik kapsamında TR karekod işlemlerinde ödeme hizmet sağlayıcısının yetki ve sorumluluklarına, 9. maddede ise bu bağlamda işyerlerinin yetki ve sorumluluklarına ilişkin ayrıntılı düzenlemelere yer verilmiştir. Yönetmelik kapsamında, ödeme hizmeti sağlayıcısının temel görevi TR karekod kullanılmak suretiyle gerçekleştirilecek ödeme hizmetleri bakımından yönetmelik kapsamındaki teknik dokümana uygun şekilde karekod oluşturulmasını sağlayarak TR karekod ile yapılacak ödemelerin güvenli ve herhangi bir sorun çıkmayacak şekilde gerçekleştirilebilmesi bakımından gerekli tedbirleri almaktır. Bilgi güvenliği açısından ise, özellikle bütünlük (integrity) unsurunun sağlanabilmesi amacıyla ödeme hizmet sağlayıcısının, TR karekodunun üretilmesi esnasında mümkün mertebe karekod kalitesinin ve okunabilirliğinin yüksek olmasına ve karekod bütünlüğünün korunmasına özen göstermesi gerektiği düzenlenmiştir[652]. TR karekod

[649] Teknik Doküman, TR Karekod Yönetmeliği'nin ekinde "TR Karekod İlke ve Kuralları" başlıklı dokümanı ifade etmektedir. İlgili belgeye ulaşmak için: https://www.resmigazete.gov.tr/eskiler/2020/08/20200821-4-1.pdf (Gözden Geçirilme Tarihi: 29.10.2020).
[650] *TR Karekodu Yönetmeliği,* m. 3/f. 1/r.
[651] *TR Karekodu Yönetmeliği,* m. 4.
[652] *TR Karekodu Yönetmeliği,* m. 8/f. 4.

ile gerçekleştirilen ödeme işlemleri akabinde ise, alıcının ödeme hizmet sağlayıcısı alıcıya, gönderenin hizmet sağlayıcısı ise gönderene ödeme işleminin gerçekleştiğine ilişkin telefon, kısa mesaj veya uygulama gibi yöntemlerle en kısa zamanda bilgi temin etmekle yükümlüdür[653]. İşyerleri ise, ödeme hizmet sağlayıcılarına benzer şekilde, TR Karekod Yönetmeliği'ne göre, TR karekod kullanılarak gerçekleştirilen ödeme işlemlerinde ödemenin karekod ile yapılabileceğine ilişkin ödeme hizmet kullanıcılarını bilgilendirmek ve bu ödeme işlemlerinin karekodda yer alan bilgiler ile uyumlu şekilde gerçekleştirilmesini sağlamak ile ödeme işlemi gerçekleştirilirken karekodda yer alan bilgilerin bütünlüğünün korunmasında gerekli özeni göstermekle yükümlüdür. Aynı zamanda, işyerlerinin statik karekod kullanılarak gerçekleştirilen ödeme işlemlerinde karekodun fiziksel güvenliğinin sağlanması ve okunabilirliğinin korunması amacıyla gerekli önlemleri alması gerektiği de düzenlenmiştir.

Son olarak, karekodla ödeme imkânı sağlayan ödeme hizmeti sağlayıcıları ile işyerlerinin bu hususta ilgili altyapılarını en geç 31.12.2021 tarihine kadar TR Karekod Yönetmeliği hükümleri ve bu yönetmeliğin zorunlu kıldığı belgeler (Teknik Doküman ve Teknik İlke Ve Kurallar Rehberi) ile uyumlu hale getirmesi gerektiği öngörülmüştür[654].

5.2.5. Bankaların Bilgi Sistemleri Ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik ("Elektronik Bankacılık Yönetmeliği")

Çalışma açısından, özellikle elektronik bankacılık işlemleri ve bu bağlamda bilgi güvenliği noktasında konu değerlendirildiğinde ise 15.03.2020 tarihinde 31069 Sayılı Resmî Gazete'de yayınlanan Elektronik Bankacılık Yönetmeliği[655]'nin bu konuda önemli birtakım düzenlemeler getirdiği görülmektedir. Başlangıçta Elektronik

[653] *TR Karekodu Yönetmeliği,* m. 8/f. 5.
[654] *TR Karekodu Yönetmeliği,* Geçici m. 1.
[655] Elektronik Bankacılık Yönetmeliği'nin internet üzerinden tam metnine şu link üzerinden ulaşılabilir: https://www.resmigazete.gov.tr/eskiler/2020/03/20200315-10.htm (Gözden Geçirilme Tarihi: 29.10.2020).

Bankacılık Yönetmeliği'nin 01.07.2020 tarihinde yürürlüğe girmesi öngörülmesine rağmen, BDDK tarafından 31161 sayılı ve 20.06.2020 tarihli Resmi Gazete'de Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik[656] neticesinde aşağıda tablo halinde yer verilen ve 01.07.2020'de yürürlüğe girecek olan maddeleri hariç olmak üzere diğer hükümlerinin yürürlük tarihi 6 ay uzatılarak 01.01.2021 olarak belirlenmiştir.

01.07.2020 Tarihinde Yürürlüğe Giren Elektronik Bankacılık Yönetmeliği Hükümleri

Madde Başlığı	Yönetmelik Hükümleri
İz Kayıtlarının Oluşturulması ve Takibi	m. 13
Dış Hizmet Alımı Sürecinin Yönetimi	m. 29
Kimlik Doğrulama ve İşlem Güvenliği	m. 34/f.13 ve f.15
Müşterilerin Bilgilendirilmesi	m. 37/f. 8
Telefon Bankacılığında Kimlik Doğrulama, İşlem Güvenliği ve Hizmet Kalitesi	m. 40 ıncı madde
ATM'lerde Kimlik Doğrulama ve İşlem Güvenliği	m. 42'nci madde

[656] İlgili yönetmelik metnine ulaşmak için Bkz. https://www.resmigazete.gov.tr/eskiler/2020/06/20200620-1.htm (Gözden Geçirilme Tarihi: 29.10.2020).

Tablo-5.1: Elektronik Bankacılık Yönetmeliği'nde 01.07.2020 Tarihinde Yürürlüğe Giren Hükümler

Yönetmelik hükümleri ile birlikte, öncelikle elektronik ödeme sistemleri açısından yukarıda tanımladığımız açık bankacılık, API, biyometrik kimlik doğrulama bileşeni gibi bazı yeni kurumlara ilişkin tanımlara ve bu kapsamda bu kurumlara uygulanacak usul ve esaslar hakkında önemli düzenlemelere yer verildiği görülmektedir.

Öncelikle elektronik bankacılık işlemleri çerçevesinde internet bankacılığı, mobil bankacılık, telefon bankacılığı, açık bankacılık servisleri ile ATM ve kiosk cihazları gibi müşterilerin, uzaktan bankacılık işlemlerini gerçekleştirebildikleri veya gerçekleştirilmesi için bankaya talimat verebildikleri her türlü elektronik dağıtım kanalını kapsamaktadır[657]. Elektronik bankacılık hizmetleri açısından da önem taşıyabilecek bazı önemli kavramların tanımları yönetmeliğe göre şu şekildedir:

Açık Bankacılık

Açık bankacılık, Elektronik Bankacılık Yönetmeliği'nde açıkça tanımlanarak yukarıda açıklanan API kavramına da yönetmelik hükümleri çerçevesinde yer verilmiştir. Buna göre açık bankacılık müşterilerin bankalar tarafından sunulan finansal hizmetlere uzaktan erişebilmesini sağlayan elektronik dağıtım kanalı olup açık bankacılık işlemleri uzaktan erişim API, web servis ve dosya transfer protokolü gibi yöntemlerle gerçekleştirilebilir. Aynı zamanda, elektronik bankacılık hizmetleri sadece müşterilerin veya müşteriler adına hareket eden tarafların salt uzaktan finansal hizmetten yararlanmasına imkân vermeyip aynı zamanda bankacılık işlemleri için bankaya talimat verebilmelerini de sağlamaktadır[658].

API

Elektronik Bankacılık Yönetmeliği'ne göre, API kavramı ise, İngilizce'deki orijinal adı olan "Application Programming Interface" ibarelerinin Türkçesi olarak "uygulama

[657] *Elektronik Bankacılık Yönetmeliği,* m. 3/f. 1/l.
[658] *Elektronik Bankacılık Yönetmeliği,* m. 3/f. 1/a.

programlama arayüzü" olarak tercüme edilerek bir yazılımın başka bir yazılımda tanımlanmış işlevleri kullanabilme işlevi olduğu belirtilmiştir[659].

Hassas Veri

Hassas veri, Elektronik Bankacılık Yönetmeliği'ne göre yukarıda "Kişisel Verilerin Korunması Kanunu" çerçevesinde belirtilen "özel nitelikli kişisel veri" kavramından farklı bir kavram olarak dikkat çekmektedir. Zira, Elektronik Bankacılık Yönetmeliği'ne göre "hassas veri" kavramının merkezinde bankacılık sektörüne yönelik olarak ele geçirilmesi halinde müşterilerin ayırt edilebilme mekanizmalarının zarar görmesi ve dolandırıcılık veya müşteriler adına sahte işlem yapılmasına olanak sağlama bulunmaktadır[660]. Hassas veri konusunda akla gelebilecek ilk örnek, yönetmeliğe göre kimlik doğrulamada kullanılan verilerdir.

Biyometrik Kimlik Doğrulama

Ayrıca, yönetmeliğe göre, biyometrik kimlik doğrulama bileşeni[661], kimlik doğrulama işlemlerinin gerçekleştirilmesini sağlamak amacıyla kullanılan bir kişiye özgü olarak ölçümlenebilen biyolojik veya davranışsal karakteristik olarak tanımlanmıştır.

Diğer Düzenlemeler

Elektronik Bankacılık Yönetmeliği'nde genel itibariyle İkinci Kısım "Bilgi Sistemlerine İlişkin Risk Yönetimi ve Kontrollerin Tesisi" başlığı altında düzenlenmiş olup elektronik bankacılık açısından önem taşıyan bilgi sistemleri, bu sistemlerin yönetilmesine ilişkin hükümlere yer verilmekle beraber elektronik bankacılık hizmetlerinde siber güvenlik açısından da önem taşıyan "bilgi güvenliği yönetimi"[662],

[659] *Elektronik Bankacılık Yönetmeliği,* m. 3/f. 1/c.
[660] *Elektronik Bankacılık Yönetmeliği,* m. 3/f. 1/o.
[661] *Elektronik Bankacılık Yönetmeliği,* m. 3/f. 1/j.
[662] Elektronik Bankacılık Yönetmeliği'nde bilgi güvenliğinin sağlanmasındaki nihai sorumluluk ilgili bankanın yönetim kuruluna ait olup yönetim kurulu, bilgi sistemlerine ilişkin güvenlik önlemlerinin uygun düzeye getirilmesi hususunda gerekli kararlılığı göstererek, bilgi güvenliği yönetimini tesis etmekle ve bu çerçevede yürütülecek faaliyetlere yönelik olarak yeterli kaynağı tahsis etmekle yükümlü kılınmıştır. Ayrıca yönetmelikte bilgi güvenliği yönetim sisteminin ulusal veya uluslararası standartları

ya da en iyi uygulamaları referans almasının esas olduğu belirtilerek hangi faaliyetlerin bu kapsamda değerlendirileceği de ayrıntılı şekilde düzenlenmiştir (*Elektronik Bankacılık Yönetmeliği,* m. 8/f. 1).

"veri gizliliği"[663], "kimlik ve erişim yönetimi"[664], "bütünlük kontrolleri"[665], "iz kayıtlarının oluşturulması ve takibi"[666], "ağ güvenliği"[667], "güvenlik açıkları ve yama

[663] Veri gizliliği açısından ise, yönetmelikte dikkat çeken düzenlemeler özetle şunlardır: Esas itibariyle, bankalar bankacılık faaliyetlerinin yürütülmesinde kullanılan verilerin taşındığı, depo edildiği, transfer edildiği, işlendiği süreçlerde gizliliği temin etmek amacıyla gerekli önlemleri alacaktır. Yönetmeliğe göre, veri gizliliğini sağlamada kullanılan şifreleme teknikleri de önem taşımaktadır. Bu bağlamda, şifrelemede güncel durum itibariyle güvenilirliğini yitirmemiş ve güncel teknolojiye uygun algoritmalar kullanılacaktır. Ayrıca, özellikle hassas veriler bakımından veri gizliliğinin sağlanabilmesi amacıyla, hassas verilerin iletimi halinde "uçtan uca güvenli iletişimin kullanılması" ve bu verilerin şifrelenmiş şekilde saklanmasının esas olduğu hüküm altına alınmıştır. İlgili düzenlemede özellikle bankanın personeline tahsis ettiği hassas veya sır olarak değerlendirilebilecek verilerin masaüstü, dizüstü ve mobil cihazlardaki içeriğinin şifreleneceği ve ağa bağlı sunucu cihazlar üzerinde açık metin halinde hassas verilerin bulunup bulunmadığını belirlemek için sunucu makineleri taranacağı belirtilmiştir (*Elektronik Bankacılık Yönetmeliği,* m. 9).

[664] Elektronik Bankacılık Yönetmeliği'nin 11. maddesi, bankaların "kimlik ve yönetim erişimi"ni nasıl gerçekleştireceğine ilişkin ayrıntılı bir düzenlemedir. İlgili düzenlemede kısaca, bilgi sistemlerinde kullanıcılara uygulanacak kimlik doğrulama mekanizması ve bu mekanizmanın hangi fonksiyonları yerine getirmesi gerektiği (başarısız kimlik doğrulama girişimlerinin belirli bir sayıyı aşması halinde, ilgili kullanıcının erişimini engellemesi, açılan herhangi bir oturumda belirli bir süre hareketsiz kalınarak hiçbir işlem yapılmaması halinde oturumun kendiliğinden kapatılması vb.) , görevler ayrılığı prensibi (bankadaki süreçler ve sistemlerin, kritik bir işlemin tek bir kişi tarafından başlatılması, onaylanması ve tamamlanmasına imkân vermeyecek şekilde tasarlanması ve işletilmesi anlamına gelmektedir), ayrıcalıklı yetkiyi haiz kullanıcılara karşı ne gibi tedbirlerin alınması gerektiği, banka bilgi sistemlerinde kullanıcı parola yönetiminde asgari olarak hangi önlemlerin alınması gerektiğine ilişkin ayrıntılı düzenlemeler söz konudur.

[665] Elektronik Bankacılık Yönetmeliği'nde bilgi güvenliğinin üç unsurundan birisi olan verilerin bütünlüğünün (*integrity*) sağlanması açısından bankaların gerekli tedbirleri alması zorunlu kılınarak aynı zamanda bu unsurla bağlantılı olarak bankaların bilgilerin doğruluğunu, tamlığını ve güvenilirliği sağlamakla yükümlü olduğu belirtilmiştir. Yönetmelik'te, doğruluk ve güvenilirlik (*reliability*) açısından, bankalarda bilgi sistemlerine ilişkin yapılmak istenen işleme ilişkin anahtar önemi haiz bilgilerin, işlemin başlangıcından bitişine kadar doğruluğunu kaybetmemesi ve yapılması arzu edilen işlemin beklenen sonucu yerine getirmesi kastedilmiştir. Bilginin tamlığı ise, madde düzenlemesine göre asgari olarak bütün işlemlerin ortaya hata çıkmadan gerçekleşmesini ve tekrarlanmaması gerektirmektedir. Hiç kuşkusuz, bütünlük unsuru verilerin transferi, saklanması ve işlenmesi gibi her aşamada önem teşkil ettiğinden yönetmelikte bütünlüğün bankalar tarafından tüm bu süreçlerde sağlanması gerektiği hüküm altına alınmıştır (*Elektronik Bankacılık Yönetmeliği,* m. 12).

[666] Elektronik Bankacılık Yönetmeliği m. 13/f. 1 gereğince, bankaların bilgi sistemlerinin ve faaliyetlerinin boyutu ve karmaşıklığı dikkate alınarak bununla orantılı olacak şekilde bilgi işlemlerinde gerçekleştirilen her işlem ve olaya ilişkin etkin bir iz kayıt (*log*) mekanizması tesis etmesi gerektiği düzenlenmiştir. Yönetmeliğe göre log kayıtlarının asgari olarak kaydı oluşturan sistem, kaydın oluşturulduğu tarih, saat ve zaman dilimi bilgisi, kaydı oluşturan işlem ya da olayla birlikte, gerçekleştirilen değişikliğin ne olduğunu gösteren bilgi ve kaydın ilişkili olduğu tekil kullanıcıyı veya sistemi gösteren bilgiyi içermesi gereklidir Yönetmeliğin 13. maddesinin ikinci fıkrasında ise her ne kadar ilgili madde düzenlemesinde "tesis edilecek iz kayıt mekanizmasının, yaşanan bilgi güvenliği olaylarının sonradan incelenmesine ve bunlar hakkında güvenilir delillerin elde edilmesine imkân tanıyacak nitelikte olması sağlanır." hükmüne yer verilmiş ise de bu düzenlemede "bilgi güvenliği olayları" olarak kastedilen olgunun yazar aslında bilgi güvenliği ihlalleri şeklinde yorumlanması gerektiğini değerlendirmektedir. Zira, bu kapsamda salt bilgi güvenliği olayları denildiği takdirde log

yönetimi"[668], yukarıda SOME'lerle ilgili açıklamalarla bağlantılı olabilecek siber olaylara müdahale süreci ve siber istihbarat paylaşımına[669] ilişkin ayrıntılı

yönetimi açısından hükmün değerlendirme kapsamı geniş olacaktır. Oysaki, uygulamada siber güvenlik ihlallerinde de görüldüğü üzere özellikle siber saldırılardan sonraki süreçte savcılık nezdinde yürütülen soruşturma süreçlerinde log kayıtlarının siber saldırıya uğrayan kurumlar nezdinde düzgün tutulup tutulmadığı ve etkin bir log yönetiminin yapılıp yapılmadığı özellikle bilişim suçlarında ilgili suçun işlenmesinde maddi gerçeğe ulaşma noktasında önem taşımaktadır.

[667] Yönetmelikte ağ güvenliği ile ilgili 14. madde düzenlemesindeki dikkat çekici olgulardan kısaca bahsetmek gerekirse, ağ güvenliği bakımından "katmanlı güvenlik mimarisi" kavramına vurgu yapılarak bu kavramın ağ güvenliğinin tesisinde bir güvenlik engelinin aşılması halinde, diğer güvenlik katmanın devreye girmesi anlamına geldiği görülmüştür (*Elektronik Bankacılık Yönetmeliği,* m. 14/1). Ayrıca, ağ güvenliğinin sağlanmasında iç ağ ve dış ağ ayrımına gidilerek özellikle hassas veya sır kapsamındaki verilere sahip sistemlerin özel iç ağda bulunması ve hiçbir şekilde doğrudan internetten erişilemiyor olmasının sağlanması gerektiği düzenlenmiştir. Özel iç ağdaki sistemler açısından sadece vekil uygulamalar veya güvenlik duvarı cihazları üzerinden iletişim kurulması öngörülmüştür (m. 14/4). Bankalarda ağ güvenliğinin tesisinde özellikle zararlı IP adreslerine yöneltilebilecek trafik de önem taşıdığından, bankaların iç ağdan dış ağa akan trafik içeriğinin kontrol edileceği ve yapılacak içerik kontrolünün zararlı IP adreslerine olan trafik akışını ve hassas veriler ile sır niteliğindeki verilerin sızdırılmasını engelleyecek nitelikte olması ve oturum bilgilerini kayıt altına alarak olağan dışı uzun süreli oturumları tespit edeceği ve bunlar için uyarı üretebilecek yetenekte olmasının sağlanacağı hüküm altına alınmıştır (*Elektronik Bankacılık Yönetmeliği,* m. 14/f. 9). Uygulamada herhangi bir ağ üzerinde bilgi sızıntısı olması halinde, savcılık makamları tarafından yapılan ilk girişim genelde atak yapan sistem üzerindeki IP adresinin saptanmasıdır. Dolayısıyla bu çalışma açısından da, yazar bankaların IP adreslerine yöneltilebilecek trafiğin takibinin önemli olduğu görüşünde olmakla beraber, yönetmelikte ilgili düzenlemede değişikliğe gidilerek yönetmelikte bu konudaki teknik çözümlerin (örneğin ne kadarlık bir zaman dilimi geçtiği halde bu durumun olağan dışı uzun süreli oturum olarak belirleneceği, sistemin uyarı üretilebilecek yetenekte olmasından kastın ne olduğu, vb.) somut şekilde belirlenmesinin uygulamada fayda sağlayabileceğini değerlendirmiştir.

[668] Yönetmeliğin 16. maddesinde güvenlik açığı ve yama yönetimi konusunda hangi faaliyetlerin yerine getirilmesi gerektiği ayrıntılı şekilde düzenlenerek zararlı yazılımlar ve spam denilen gereksiz eklentiler içeren e-postalar açısından bankaların kısaca ağa bağlı olan sistem ve cihazlar ile, masaüstü ve dizüstü bilgisayarlar ile e-posta sunucusuna gelen ve giden e-postaların sürekli taranması ve bu bağlamda güvenlik açıklarının tespit edilerek gerekli yama yönetiminin sağlanması noktasında detaylı hükümlere yer verilmiştir.

[669] Kurumsal ve Sektörel SOME'lerin hangi fonksiyonları yerine getirmesi gerektiği ile ilgili düzenlemelere Yönetmeliğin 18. maddesinde yer verilmiştir. Yönetmeliğin ilgili hükmünden de anlaşıldığı üzere kısacası yönetmelik hükümleri gereği Kurumsal SOME kurulması öngörülmüş olup Kurumsal SOME'nin (i) siber olay öncesinde, bilgi işlem varlıkları üzerinde periyodik olarak sızma testi çalışmaları gerçekleştirmekle, kayıt yönetimi sistemi arayüzünden rutin olarak log kayıtlarını takip etmekle, log kayıtları arasında anlamlı sonuçlar doğurabilecek ilişkileri (korelasyonları) kontrol etmekle, (ii) siber olay esnasında ise, bilgi sistemleri fonksiyonunun yapacağı müdahaleyi yönetmekle ve bilgi sistemleri fonksiyonunda görevli ilgili personeli koordine etmekle yükümlü kılınmıştır (m. 18/2). Sektörel SOME'ler bakımından ise, yönetmeliğe göre, bankaların daha ziyade siber olaylar karşısında (bankaların yaşanan bir siber olayın büyüyerek bir krize dönüşmesi, verilerin sızması ya da ifşası ile sonuçlanması, bilgi sistemi hizmetlerinde ciddi kesintilere veya bozulmalara yol açan önemli siber olaylar için kök neden ve etki analizi yapılması ve benzer olayların tekrarlanmasını önlemek amacıyla yapılan çalışmaları gibi) Sektörel SOME'ye bildirim yapması zorunlu kılınmıştır (*Elektronik Bankacılık Yönetmeliği,* m. 18/f. 5 ve f. 6).

düzenlemeler ile bilgi güvenliği farkındalığını artırmaya[670] yönelik hükümlere de yer verilmiştir.

Elektronik Bankacılık Yönetmeliği'nin 34. ila 42. maddeleri arasında Türkiye'de uygulanmakta olan bazı elektronik bankacılık hizmetleri (internet bankacılığı, mobil bankacılık, telefon bankacılığı, ATM bankacılığı) ile yeni bir elektronik bankacılık hizmet modeli olan açık bankacılık gibi bankacılık uygulamalarında özellikle kimlik doğrulama[671] ve işlem güvenliğinin nasıl sağlanması gerektiğine yönelik yeni birtakım düzenlemelere yer verilmiştir:

İnternet Bankacılığı

İnternet bankacılığında işlem güvenliğini sağlamak amacıyla özetle, kimlik doğrulama açısından ilk adım müşterinin bildiği unsurun (örneğin banka şifresi) sisteme girilmesi zorunlu olup kimlik doğrulama işlemi banka tarafından çevrimdışı lokalde değil, çevrimiçi olarak doğrulanacaktır. İkinci aşamada ise, yönetmelik gereği internet bankacılığı oturumu açılmadan önce iki bileşenli bir doğrulama belirleneceği için, ikinci doğrulama açısından bir karşılama mesajı veya resminin müşteriye iletilmesi sağlanacaktır. İkinci doğrulama açısından müşteriye atanmış bir şifreleme gizli anahtarı ile otomatik olarak müşteri tarafından imzalanacak tek kullanımlık bir doğrulama kodu üretilir[672].

Mobil Bankacılık

---

[670] Yönetmeliğin 19. maddesinde bankalar nezdinde çalışanların bilgi güvenliği farkındalık seviyesini artırmak amacıyla kapsamlı bir bilgi güvenliği eğitim programı oluşturulacağına yönelik ayrıntılı bir düzenlemeye yer verilerek kısacası bu programın içeriğinin yılda en az bir defa yeni teknolojiler ve riskler kapsamında program içeriğimim gözden geçirilerek güncelleneceği, bankaların güncel saldırı yöntemlerini dikkate alarak gerekli sosyal mühendslik senaryoları üzerinden çalışanlarına yönelik periyodik testler gerçekleştirileceği hüküm altına alınmıştır.

[671] Yönetmeliğin 34. maddesinde yukarıda açıklanan PSD2 düzenlemesinde öngörüen SCA'ya (güçlü müşteri onayı) benzer bir kimlik doğrulama modeli öngörülmüş olup buna göre, finansal işlem doğurmayan işlemlerde dahi en az iki bileşenden oluşan bir kimlik doğrulama mekanizması uygulanması gerektiği belirtilerek PSD2'de olduğu gibi bu iki bileşenin müşterinin "bildiği", "sahip olduğu" veya "biyometrik bir karakteristiği olan" unsur sınıflarından farklı ikisine ait olmak üzere seçileceği düzenlenmiştir.

[672] *Elektronik Bankacılık Yönetmeliği,* m. 38.

Elektronik Bankacılık Yönetmeliği'ne göre, mobil bankacılık, müşterilerin mobil bir cihazda (akıllı telefon veya tablet) yer alan ve herhangi bir bankaya ilişkin mobil uygulama üzerinden bankacılık işlemlerinin gerçekleştirildiği ve bu sürece özgü internet bankacılığı dağıtım kanalını ifade etmektedir[673]. Mobil bankacılıkta kimlik doğrulama bakımından (i) müşteri tarafından kendisine özgülenen şifreleme anahtarına erişmek için uygulama şifresinin (PIN) sisteme girilmesi, (ii) şifreleme anahtarına ulaşılması halinde ise söz konusu şifreleme anahtarı ile yönetmelikte belirtildiği üzere "müşteriyle ilintili eşsiz bir bilginin" banka nezdinde çevrimiçi olarak doğrulanması yeterli kabul edilmiştir. Mobil bankacılıkta kimlik doğrulama açısından ilk aşamada PIN yerine biyometrik kimlik doğrulama bileşeni de kullanılarak müşteriye özgü bir şifreleme anahtarına ulaşılması ve aynı şekilde bu şifreleme anahtarı ile doğrulama yapılması da kimlik doğrulama açısından aynı etkiyi haizdir[674].

Yukarıda belirtilen ve kimlik doğrulama açısından genel prensip olarak kabul edilen "iki bileşenli kimlik doğrulama"nın bir istinası olarak "tek bileşenli kimlik doğrulama" açısından mobil bankacılık bakımından yönetmelikte bir istisna hükmü bulunmaktadır. Buna göre, müşterinin ilk aşamada sahip olduğu bir kimlik doğrulama unsurunu kullanarak sisteme giriş yapması halinde sadece mobil bankacılıkta:

(i) müşterinin, mobil bankacılık uygulaması aracılığıyla müşteri ve hesap bilgilerini görüntülemek istemesi halinde *veya*,

(ii) daha önceden tanımlanmış güvenli alıcılar listesine para transfer etmek veya ödeme yapmak istemesi halinde,

gerçekleştireceği işlemler açısından tek bileşenli kimlik doğrulamanın geçerli olacağı kabul edilmiştir.

Telefon Bankacılığı

[673] *Elektronik Bankacılık Yönetmeliği,* m. 3/f. 1/çç.
[674] *Elektronik Bankacılık Yönetmeliği,* m. 34/f. 1.

Telefon bankacılığı, günümüzde özellikle siber saldırganlar bakımından sosyal mühendislik saldırıları vasıtasıyla yaygın şekilde istismar edilen bir bankacılık hizmeti olup yönetmelik çerçevesinde telefon bankacılığında bilgi güvenliği ile ilgili olarak ayrıntılı düzenlemelere yer verilmiştir. İlk olarak, iki bileşenli kimlik doğrulama mekanizması telefon bankacılığı açısından da geçerli olup yönetmelikte telefon bankacılığında hizmet veren santral görevlisinin, müşteriye ait bilgileri görememesi veya müşteriye ilişkin işlem menüsünün aktif olmamasının sağlanacağı mobil bankacılıktaki işlem güvenliği hassasiyeti nedeniyle özellikle hükme bağlanmıştır. Kural olarak, müşteri ile görevlinin aktif olarak telefon bağlantısı gerçekleştirmediği takdirde telefon bankacılığı ile herhangi bir işlem gerçekleştirilmeyeceği de düzenlenmiş olup bunun tek istisnası yönetmeliğe göre kayıp, çalıntı ve dolandırıcılık gibi riskli işlem bildirimleridir (m. 40/f. 1). Ayrıca, telefon bankacılığı açısından, müşterinin telefon bankacılığına bağlanmadan önce santral görevlisinin dahli ve erişimi olmaksızın bildiği kimlik doğrulama unsurları ile sisteme girmesi esas olup bunun dışında dolandırıcılık risklerine karşı telefonun başka bir telefona yönlendirme riski olup olmadığı, müşteri temsilcileri ve çağrı merkezi görevlerine sosyal mühendislik saldırıları ve diğer dolandırıcılık yöntemleri konusunda düzenli eğitimler verilmesi, telefon bankacılığında sesli yanıt sisteminin hangi kriterleri sağlaması gerektiğine ilişkin de düzenlemelere yer verilmiştir.

Açık bankacılık

Açık bankacılığın yönetmelik kapsamında ne olduğu yukarıda ayrıntılı şekilde açıklandığından, bilgi güvenliği noktasında burada sadece Elektronik Bankacılık Yönetmeliği'nin 41. maddesine ilişkin düzenlemeye değinilecektir. Yukarıda belirtildiği üzere, çift bileşenli kimlik doğrulamanın bir istinası olarak açık bankacılıkta tek bileşenle yapılabilecek kimlik doğrulama ancak (i) müşteri veya müşteri adına hareket eden taraf ile banka arasındaki iletişimin uçtan uca güvenli bir iletişim şeklinde olması, (ii) banka tarafından telafi edici ek kontroller uygulanması ve (iii) müşterinin bağlantı kurabileceği kaynaklara ilişkin ilave kısıtlamalar getirilmesi koşulları

sağlandığı takdirde kabul edilebilir. Öngörülen bu şartlar, yönetmeliğin lafzından da anlaşılacağı üzere kümülatif olarak aranmaktadır, başka bir ifadeyle tek bileşenli kimlik doğrulama için yukarıda belirtilen üç şartın da bir arada bulunması gerekir.

5.2.6. Türkiye Ödeme Ve Para Kuruluşları Birliği Statüsü Yayınlanmasına İlişkin 2678 Sayılı Cumhurbaşkanı Kararı

22.11.2019 tarihli ve 30956 Sayılı Resmî Gazete'de yayımlanan "Ödeme Ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri Ve Elektronik Para Kuruluşları Hakkında Kanun İle Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun ile 6493 Sayılı Kanun'a eklenen Ek Madde 1 ile Türkiye Ödeme Ve Para Kuruluşları Birliği (*"Birlik"*)'ne ilişkin birtakım düzenlemeler getirilmişti. 28.06.2020 tarihli ve 31169 Sayılı Resmî Gazete'de 2678 Sayılı Cumhurbaşkanı Kararı gereğince ise, "Türkiye Ödeme Ve Para Kuruluşları Birliği Statüsü" (*"Statü"*) yayınlanmıştır. Anılan Statü'nün yürürlüğe konmasına yukarıda belirtilen 6493 Sayılı Kanun'un Ek Madde 1 gereği karar verildiği belirtilmiştir[675].

[675] Birlik'in kuruluşunu ilan söz konusu Cumhurbaşkanı Kararı ile Statü içeriğinde dikkati çeken düzenlemeler şunlardır:
i. Birliğin Amacı: Birliğin amacı, üyelerin ortak ihtiyaçlarını karşılamak, mesleki faaliyetlerini kolaylaştırmak, birbirleri ile veya temsilcileri ve müşterileri ile olan ilişkilerinde dürüstlüğü ve güveni hakim kılmak üzere meslek disiplini ve ahlakını korumak, dayanışma içerisinde çalışmasını, ekonomik menfaatlerinin korunmasını ve mesleki konularda gelişimini sağlamak ve aralarındakş rekabetçi ortamın korunmasını, haksız rekabetin önlenmesini ve ödemeler alanının gelişmesini temin etmektedir.
ii. Birliğe Üyelik: Birliğe üye olacak kuruluşlar, 6493 Sayılı Kanun gereğince lisanslı ödeme kuruluşları ve elektronik para kuruluşlarıdır. Bu bağlamda, üyelik başvuruları Birlik organları oluşuncaya kadar TCMB tarafından sonuçlandırılacaktır.
iii. Disiplin Cezaları: Statü içeriğinde ayrıca meslek onuru veya meslek ilke ve kurallarına aykırı şekilde fiil ve işlemlerde bulunan, müşterisine karşı yükümlülüklerini haklı neden olmaksızın yerine getirmeyen, Birlik üyeliğinin gerektirdiği şekilde davranmayan, sektörün düzeni ile piyasada rekabeti bozan ve haksız rekabete yol açan, dürüstlük kurallarına aykırı hareket eden, faaliyetlerine hile karıştıran, faaliyetlerin açık ve düzenli şekilde yürütülmesine engel olan ve ilgili mevzuata ve kararlara karşı hareket eden, ödemeler alanın dengesini bozan ve gelişimini engelleyen üyeler hakkında fiil ve işlemin ağırlığına göre disiplin cezaları uygulanması düzenlenmiştir.

5.2.7. 5237 Sayılı Türk Ceza Kanunu'nda Yer Alan Bilişim Suçları

Türk Ceza Kanunu (*"TCK"*)'nda bilişim suçları, esas itibariyle "bilişim alanında suçlar" ve "özel hayata ve hayatın gizli alanına karşı suçlar"[676] bölümünde düzenlenmiştir. TCK[677] açısından her ne kadar aşağıda da detaylı şekilde açıklanacağı üzere, kanunun sistematiği gereği doğrudan (dar anlamdaki) bilişim suçlarının toplu şekilde TCK'da ayrı bir bölüm altında düzenlendiği kabul edilse de, hukuki değerlerle ilişkili hırsızlık ve dolandırıcılık gibi geleneksel bazı suç tipleri açısından kanunda bu hükümlere yönelik özel atıflara yer verilmesi nedeniyle bilişim suçlar bakımından TCK'da karma bir sistem benimsenmiştir[678].

Bilgisayar sistemlerine karşı işlenen suçlar, TCK'da "Topluma Karşı Suçlar" kısmının onuncu bölümünde "Bilişim Alanında Suçlar" başlığı altında düzenlenmekte olup Türk Ceza Kanunu'nda bilişim sistemleri aracılığıyla işlenen ancak siber suç nitelendirilemeyecek suç tipleri de düzenlenmektedir[679]. Bilişim alanında suçlar bölümünde, hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma suçu (m. 243), sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu (m. 244), banka ve kredi kartlarının kötüye kullanılması suçları (m. 245) ve yasak cihaz ve programların bulundurulması ve kullanılması suçu (m. 245/A) düzenlenmektedir.

---

[676] Özel hayata ve hayatın gizli alanına karşı suçlar bölümünde ise bilişim suçu olarak nitelendirilebilecek, kişisel verilerin kaydedilmesi suçu (m. 135), kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu (m. 136) ve verilerin yok edilmemesi suçu (m. 138) yer almaktadır. Bu konuda detaylı bilgi için bkz. *Dülger, Bilişim Suçları,* s. 237 vd.

[677] Türk Ceza Kanunu metnine ulaşmak için: https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[678] *Aköz*, s. 59'da belirtilen İsa Başbüyük (2010, s. 153). Bu kapsamda, Dülger TCK'nın muhtelif bölümlerinde bilişim sistemleriyle işlenmesi olanaklı suç tiplerinin şunlar olduğunu belirtmiştir: (i) haberleşmenin gizliliğini ihlal suçu (m. 132), (ii) haberleşmenin engellenmesi suçu (m. 124), (iii) hakaret suçu (m. 125), (iv) bilişim sisteminin kullanılması yoluyla işlenen hırsızlık suçu (m. 142/f. 2/e), (v) bilişim sisteminin kullanılması yoluyla işlenen dolandırıcılık suçu (m. 158/f. 1/f), (vi) müstehcenlik suçu (m. 226) ve (vii) kumar oynanmaması için yer ve imkan sağlama (m. 228/f. 3). Bu konuda detaylı bilgi için bkz. *Dülger, Bilişim Suçları*, s. 237 vd.

[679] *Çakır/Kılıç*, s. 182

Aşağıda çalışmanın konusu itibariyle "elektronik ödeme sistemlerinde siber güvenlik" ile ilgili olacağı düşünülen "Bilişim Alanında Suçlar" açısından TCK'da düzenlenen suç tipleri doktrin görüşleri ve yargı kararları ışığında kapsamlı olarak ayrı ayrı incelenecektir:

Bilişim Sistemlerine Girme Suçu (TCK m. 243)

Bilişim alanında suçlar kapsamında ilk olarak TCK madde 243 kapsamında "bilişim sistemlerine girme suçu düzenlenmiştir. İlgili düzenlemeye bakıldığında, bilişim sistemlerine girme suçunun basit hali açısından "bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girme" veya "orada kalmaya devam etme" eylemleri söz konusu suç tipi haline getirilmiştir. Bu eylemler, TCK gereği bir yıla kadar hapis veya adlî para cezası ile cezalandırılmaktadır[680]. İlgili suçun işlenebilmesi açısından bilişim sistemlerine yetkisiz şekilde girilmesi suçun işlenmesi için yeterlidir. Doktrinde, bilişim sistemlerine girme suçu ile korunan hukuki değerin, bilişim sisteminin güvenliği ve dokunulmazlığı olduğu belirtilmiştir[681].

Sistemi Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme Suçu (TCK m. 244)

TCK 244 maddesi başlık olarak "Sistemi Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme" şeklinde yer almakta olup esas itibariyle bu hüküm altında iki farklı suç

[680] 24.03.2016 tarihinde yürürlüğe giren 6698 Sayılı Kişisel Verilerin Korunması Kanunu m. 30/f. 4 ile TCK m. 243'de bilişim sistemlerine girme suçunun işlenebilmesi suçunun işlenebilmesi açısından "bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girme" ve "orada kalmaya devam etme" eylemleri ilgili hükümde "ve" ibaresi ile düzenlendiği için doktrinde haklı olarak bu suçun işlenebilmesi açısından, her iki eylemin de bir arada işlenmesi gerektiğine ilişkin tartışmalar söz konusu idi. Başka bir deyişle, bilişim sistemlerine girme suçunun işlenebilmesi açısından 2016 yılındaki değişiklik öncesinde, sadece bilişim sistemine hukuka aykırı şekilde girme yeterli olmayıp bu suç bakımından "orada kalmaya devam etme" fiilinin de işlenmesi aranmakta idi. Anılan bu değişiklik sonucunda ise, yasa koyucu tarafından söz konusu bu tartışmaların önüne geçilerek ilgili hüküm içeriğindeki "ve" bağlacının "veya" olarak değiştirilmesi ile her iki eylem de suçun işlenebilmesi açısından seçimlik hareket şeklinde düzenlenmiştir. Bu konuda ayrıntılı bilgi için bkz. Berrin Akbulut, "Bilişim Alanında Suçlar", Adalet Yayınevi, 2. Baskı, Ankara, 2017, (*"Akbulut"*), s. 115.

[681] *Akbulut*, s. 118.

tipi düzenlenmiştir. Bu suç tiplerinden ilki, ilk fıkrada düzenlenen doğrudan bilişim sistemine[682] yönelik bir eylem ve faaliyete yönelik olup diğeri ise ikinci fıkrada bilişim sistemindeki verilere yönelik gerçekleştirilen müdahalelere yönelik bir hüküm öngörülmüştür[683]. Buna göre bir bilişim sisteminin işleyişini engellemek[684] veya bozmak fiili, bir yıldan beş yıla kadar hapis cezası ile cezalandırılırken yasa koyucu bir bilişim sistemi içerisindeki verilere yönelik işlenen suç açısından daha hafif bir ceza öngörmüştür. Bu çerçevede TCK m. 244/f. 2 gereğince bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır[685].

---

[682] Bilişim sistemlerinin esas özelliklerinin klavye, monitör, fare gibi fiziksel varlıkları oluşturan donanımdan ziyade, veriler, programlar, sunucu gibi soyut varlıkları içeren yazılım unsurunun belirlediği ancak verilerin işlenmesi ve saklanması gibi yazılım unsurunun doğru bir şekilde çalışmasının, donanım unsurunun da işlevini doğru şekilde yerine getirmesine bağlı olduğu, dolayısıyla bilişim sistemindeki yazılım ve donanımın birbirine bağlı şekilde işleyen süreçler olduğu ifade edilmektedir. Ancak yazılımda olduğu donanım unsuru açısından da TCK m. 244/f. 1 kapsamında işlenen bir suçtan söz edebilmek için buradaki temel kıstas, müdahalenin amacının mutlaka sistemin işleyişini yönelmesi gerekmekte olup bilişim sisteminin işleyişine yönelmeyen donanıma yönelik fiziksel saldırıların TCK m. 244/f. 1 kapsamında değerlendirilmeyeceği dikkate alınmalıdır. Bkz. *Erdem/Özocak1*, s. 185.

[683] TCK m. 244'de "sisteme ve veriye müdahale şapkası altında, birçok fiilin suç kapsamına alındığı, yasal düzenlemenin içeriğinden failin bir bilişim sisteminin işleyişini engellemesi veya bozmasının sisteme müdahale şeklindeki suçlara ilişkin olduğu, bununla birlikte bilişim sistemi içerisindeki verileri bozmanın, yok etmenin, değiştirmenin, erişilmez kılmanın, bunun yanında sisteme veri yerleştirilmesi veya mevcut verileri başka bir yere göndererek sisteme zarar verilmesinin veriye müdahale şeklinde bir suç olduğu belirtilmiştir. Bkz. *Erdem/Özocak1*, s. 183.

[684] TCK m. 244/f. 1 kapsamında öngörülen "engellemek" fiilinin, doktrinde geniş şekilde yorumlanarak bilişim sisteminin genel olarak çalışmasına ilişkin olabileceği gibi, bu işleyişi katkısı olan veya etkisi olan herhangi bir unsurun işleyişine de engel olunarak sistemin tamamen veya kısmen işlemesinin önlenmesi şeklinde yorumlanması gerektiği üzerinde durulmaktadır. Bkz. *Erdem/Özocak1*, s. 186'daki dp.dan belirtilen Dülger (s. 395) ve benzer yönde görüş için bkz. *Akbulut*, s. 190, Yargıtay'ın bu konudaki değerlendirmesine bakıldığında ise, bilişim sisteminin engellenmesi, "bilişim sisteminin verimli şekilde çalışmasının önlenmesi, icra ettiği faaliyet ve sahip olduğu kapasitesinin müdahale ile sınırlandırılması, yavaşlatılması veya kilitlenme noktasına getirilmesi" şeklinde nitelendirilmiştir. Bkz. Yargıtay 11. HD., 13.03.2013 tarihli, 2011/2816 E. Sayılı ve 2013/4065 Sayılı içtihadı: http://www.kazanci.com/kho2/ibb/giris.html (Gözden Geçirilme Tarihi: 10.07.2020). TCK m. 244/1 kapsamında bilişim sistemine müdahale suçunun en sık görülen yönteminin DoS ve DDoS saldırıları olduğu bilinmektedir. Bkz. *Erdem/Özocak1*, s. 186, *Akbulut*, s. 190. DoS ve DDoS saldırıları ile ilgili ayrıntılı bilgiye tezin 2.6.1. başlığı altında yer verilmiştir.

[685] Akbulut tarafından *verilerin bozulması* verilerin kullanılabilirliğine zarar verilmesi, *verilerin yok edilmesi* verilerin varlığının ortadan kaldırılması, *verilerin değiştirilmesi* kaydedilmiş verilerin başka bir

Yukarıda belirtilen gerek sisteme müdahale gerekse verilere müdahale şeklinde gerçekleştirilen suç tiplerine yönelik olarak söz konusu fillerin bir banka veya kredi kurumuna ya da kamu kurum ve kuruluşuna ait bir bilişim sistemi üzerinde işlenmesi halinde bu suçların ağırlaştırıcı nedeni olarak söz konusu eylemlere verilecek cezaların yarı oranında artırılacağı hüküm altına alınmıştır.

Son olarak, bu başlık altında sisteme ve verilere müdahale şeklinde gerçekleştirilen suçların eylemi gerçekleştiren kişilerin kendisine veya başkasının yararına haksız bir çıkar sağlamasının özellikle başka bir suça sebebiyet vermesi koşuluyla iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılacağı öngörülmektedir. Hükmün içeriği incelendiğinde, yasa koyucunun özellikle sisteme ve verilere yönelik müdahale şeklinde gerçekleştirilen suçlar açısından bu suçları işleyen kişilerin kendisine veya başkasına yarar sağlaması halinde ikili bir ayrıma gittiği anlaşılmaktadır: (i) Eğer bu suçu işleyenler kendisi veya başkası yarar sağlaması halinde söz konusu eylemleri başka bir ceza kapsamında cezalandırılmıyor ise bu takdirde yukarıda belirtildiği üzere TCK m. 244/f. 4 gereğince bu suçların nitelikli hali dikkate alınarak (TCK m. 244/f. 1 ve m. 244/f. 2'e kıyasla) daha ağır bir şekilde cezalandırılacaklardır, (ii) ancak TCK m. 244 kapsamında işlenen suçların ve bu suçları işleyen kişilerin haksız menfaat sağlaması başka ve daha ağır bir suç tipi altında düzenlenmekte ise, TCK m. 244/f. 4 yerine ilgili öngörülen diğer ceza kapsamında cezalandırılması gerektiği düzenlenmiştir.

Banka Veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m. 245)

Türkiye'de özellikle banka ve kredi kartlarının da yaygınlaşması ile birlikte bu konuda işlenen suçlarda yaşanan artışın özellikle yasa koyucuyu bu konuda işlenen suçlar

bilgi içeriği alması, *verilerin erişilmez kılınması* yetkili kişinin verilere ulaşmasının ortadan kaldırılması suretiyle verilerin kullanılmasının engellenmesi, var olan verileri başka bir yere göndermek ise, telekomünikasyon yolları üzerinden veya mevcut olarak ifade edilmektedir. Bu konuda detaylı bilgi için bkz. *Akbulut*, s. 195-203.

açısından bu konunun özel bir hüküm altında düzenlenmesine sevk etmiştir. Bu kapsamda, TCK m. 245//f. 1'e bakıldığında banka ve kredi kartlarının kötüye kullanılması suçunun[686] basit şekli olarak başkasına ait bir banka veya kredi kartını ele geçirenlerin veya elinde bulunduranların kart sahibinin rızası hilafına kullanması veya kullandırtması yahut başkasına yarar sağlaması üç yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılmaktadır. Söz konusu suçun nitelikli hali olarak başkalarına ait banka hesapları ile ilişkilendirilerek sahte banka veya kredi kartı üretmek, satmak, devretmek, satın almak veya kabul etmek fiillerinin ise üç yıldan yedi yıla kadar hapis ve onbin güne kadar adli para cezası ile cezalandırılması öngörülmüştür. (m. 245/f. 2) Anılan suçun m. 245/2'e kıyasla daha ağır bir ceza ile cezalandırılmasının öngörüldüğü diğer nitelikli hali ise, sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlamaktır. Bu durumda, m. 245'de m. 244/f. 4'de olduğu gibi yasa koyucu tarafından ikili bir ayrıma gidilerek bu fiilin daha ağır cezayı gerektiren başka bir suç oluşturması halinde daha ağır suç oluşturan ceza ile bu fiilin daha ağır bir cezayı gerektiren başka bir suç oluşturmaması halinde ise dört yıldan sekiz yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılacağı düzenlenmiştir.

Doktrinde Akbulut tarafından, TCK m. 245 kapsamında düzenlenen suçların, hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının banka ve kredi kartlarının kullanılmak suretiyle işlenen şekilleri olduğu belirtilmiştir[687].

---

[686] Bu suçun, esasen teknik anlamda bir bilişim suçu olmayıp bilişim sistemlerinin kullanılması yoluyla işlenen dolandırıcılık suçunun bir özel görünüşü şeklinde düzenlendiği belirtilmektedir. Bkz., *Erdem/Özocak1*, s. 189.

[687] Bkz. *Akbulut*, s. 276'da 724 no'lu dipnotta belirtilen Özbek/Doğan/Bacaksız/Tepe, Koca/Üzülmez ve Yılmaz. Doktrinde Ali Parlar "Türk Ceza Hukukunda Bilişim Suçları" adlı eserinde benzer şekilde hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının işlenme şekillerinin tümünü içeren bu fiillerin 245. madde kapsamında duraksamaları ve içtihat farklılıklarını önlemek amacıyla bağımsız suç haline getirildiğini ve böylelikle mağdurun malvarlığının korunmasının amaçlandığını belirtmiştir. Bu konuda ayrıntılı değerlendirme için bkz. Ali Parlar, "Türk Ceza Hukukunda Bilişim Suçları", Bilge Yayınevi, Ankara, 2015, (*"Parlar"*), s. 126-127. Ayrıca, banka veya kredi kartlarının kötüye kullanılması suçu ile ilgili kapsamlı bilgi için Bkz. Eylem Baş, "Banka Ve Kredi Kartlarının Kötüye Kullanılması Suçu", Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku (Ceza Ve

Yasak Cihaz Ve Programlara Yönelik Suçlar

TCK kapsamında "Bilişim Alanında Suçlar" bölümü altında düzenlenen son suç tipi TCK md. 245/A kapsamında yasak cihaz ve programlarla[688] ilgili olup söz konusu düzenlemede, bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılmaktadır.

5.2.8. 5809 Sayılı Elektronik Haberleşme Kanunu

5809 Sayılı Elektronik Haberleşme Kanunu (*"5809 Sayılı Kanun"*)'nda çalışmayı ilgilendiren düzenlemeler şunlardır:

Özellikle 19.02.2014 tarihinde 28918 Sayılı Resmi Gazete'de yayınlanan 6518 Sayılı Kanun (Aile Ve Sosyal Politikalar Bakanlığının Teşkilat Ve Görevleri Hakkında Kanun Hükmünde Kararname İle Bazı kanun Ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun)[689] 5809 Sayılı Kanun'da bazı değişiklikler yapılması öngörülmüştür. Buna göre önemli düzenlemeleri kısaca özetlemek gerekirse,

---

Ceza Muhakemesi Hukuku) Anabilim Dalı, Yüksek Lisans Tezi, Ankara, 2013 (*"Baş"*): https://dspace.ankara.edu.tr/xmlui/bitstream/handle/20.500.12575/31099/Binder1.pdf?sequence=1 (Gözden Geçirilme Tarihi: 29.10.2020).

[688] Doktrinde, Erdem/Özocak özellikle son yıllarda crack, keylogger, trojan gibi zararlı yazılımların internet üzerinden, internet forumlarında ve web sitelerinde son derece kolay şekilde ulaşılabilir olmasının, siber suçluluğun artmasında önemli bir payı olduğu dikkate alınarak bu kapsamda önleyici ceza normlarının düzenlenmesinin bir sorun olmadığı belirtilmekle beraber TCK m. 245/A kapsamında özellikle bu suçu teşkil eden hareketlerin çok geniş kapsamlı düzenlenmesinin ve özellikle zararlı yazılımları "bulundurma"nın da suç kapsamına alınmasının uygulamada birçok sorun ve tartışmaya sebebiyet vereceği görüşündedir. Bkz. *Erdem/Özocak1*, s. 188-189.

[689] 6518 Sayılı Kanun'un internet ortamında tam metnine ulaşmak için Bkz. https://www.resmigazete.gov.tr/eskiler/2014/02/20140219-1.htm (Gözden Geçirilme Tarihi: 29.10.2020).

elektronik haberleşme sektörünü düzenleme ve denetleme yetkisini haiz olan BTK'ya bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi[690], izinsiz erişime karşı şebeke güvenliğinin sağlanması[691], elektronik haberleşme sektörüne yönelik olarak mevzuatın öngördüğü tedbirlerin alınması[692], siber güvenlik ve internet alan adları konusunda 6809 Sayılı Kanun'da belirtilen görevlerin yerine getirilmesi[693] gibi görevler verilmiştir.

Yukarıda da ayrıntılı şekilde belirtildiği üzere, Türkiye'de ilk kez kurulan Siber Güvenlik Kurulu'nun yasal altyapısı 5809 Sayılı Kanun'a 2014 yılında eklenen Ek Madde 1 ile düzenlenerek Siber Güvenlik Kurulu'nun siber güvenlik alanında kanunen hangi görevlerinin olduğu ortaya konulmuştur.

2016 yılında KHK'ya eklenen düzenlemeler ile 5809 Sayılı Kanun'un 60. maddesinin 10., 11. ve 12. fıkralarında BTK'nın düzenleyici otorite olarak kurumlardan bilgi ve belge talep etmesine yönelik ek düzenlemeler öngörülmüş olup özellikle m. 60/f. 12 hükmünün Anayasa'ya aykırı olduğu talebi neticesinde Anayasa Mahkemesi ("AYM") tarafından 2019 yılında soyut norm gerçekleştirilmiştir. AYM'nin 13.11.2019 tarihinde Resmi Gazete'de yayınlanan kararında iptal talep edilen 5809 Sayılı Kanun m. 60/f. 11 hükmüne KHK ile eklenen düzenlemeyi[694], BTK'nın düzenlenen yetkilerini belirlilik,

---

[690] *5809 Sayılı Kanun,* m. 4/ f. 1/ı.
[691] *5809 Sayılı Kanun,* m. 12/ j.
[692] *5809 Sayılı Kanun,* m. 6/ f. 1/ş.
[693] *5809 Sayılı Kanun,* m. 6/ f. 1/v.
[694] 671 Sayılı Kanun Hükmünde Kararname ile 2016 yılında eklenen 5809 sayılı Kanun'un 60. maddesine eklenen 10, 11 ve 12 numaralı fıkra şöyledir:
"(10) (Ek: 6757 - 9.11.2016 / m.22) Anayasanın 22 nci maddesinde sayılan sebeplerden biri veya birkaçına bağlı olarak, gecikmesinde sakınca bulunan hâllerde Cumhurbaşkanlığı, alınması gereken tedbirleri belirler ve uygulanmak üzere Kuruma bildirir. Kurum Başkanı, Cumhurbaşkanlığının gerekli gördüğü tedbirlere ilişkin kararını derhal işletmecilere, erişim sağlayıcılara, veri merkezlerine ve ilgili içerik ve yer sağlayıcılara bildirir. Bu kararın gereği, derhal ve kararın bildirilmesi anından itibaren en geç iki saat içinde yerine getirilir. Bu karar, yirmidört saat içinde sulh ceza hâkiminin onayına sunulur. Hâkim kararını kırksekiz saat içinde açıklar, aksi halde karar kendiliğinden kalkar.
(11) (Ek: 6757 - 9.11.2016 / m.22) Kurum, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alır veya aldırır.

özel hayatın gizliliği ve kişisel verilerin korunması hakkı çerçevesinde değerlendiren AYM, md. 60/11'de düzenlenen BTK'nın bilgi ve belge talep etmesi yetkisinin kurumun siber güvenlik göreviyle sınırlı olduğu ve kişisel veriler ile ticari sırların korunması ile ilgili yeterli güvencelerin sağlandığı gerekçesiyle iptal talebini reddederek oy çokluğu ile söz konusu düzenlemenin Anayasa'ya uygun olduğuna karar vermiştir[695]. Doktrinde, Furkan Güven Taştan[696] tarafından özellikle dikkat çekildiği üzere özellikle Zühtü Arslan'ın kaşı oy gerekçesi bu konuda dikkate alınmaya değerdir. Arslan tarafından, karşı oy yazısında iptali istenen hüküm bakımından AYM'nin önceki kararlarından farklı hareket edilmesini gerektiren bir durum bulunmadığı, zira önceki AYM kararlarında TİB'in hangi koşullar ve hangi gerekçelere dayanarak bilgi talep ettiği durumlarda kişisel verilerin korunması hakkının ölçüsüzce sınırlandırılacağına yönelik geçmiş tarihli çeşitli kararları bulunduğu, BTK'nın tek görevinin siber güvenlik olmadığı, siber güvenlik görevinin BTK'nın özellikle 5809 Sayılı Kanun'un 6. maddesinde hüküm altına alınan yirmi sekiz görevinden sadece birisi olduğu ve bu hüküm bağlamında BTK tarafından istenen ve işlenecek olan kişisel veriler konusunda yeterli güvencenin verilmediği gerekçesiyle anılan hükmün Anayasa'ya aykırı olduğu belirtilmiştir. Yazar, bu konuda Arslan'ın 5809 Sayılı Kanun m. 60/f.11 ile ilgili isabetli olduğunu değerlendirerek Anayasa Mahkemesi'nin bu konudaki red gerekçesinin hukuka aykırı olduğu kanaatindedir. Öncelikle, Anayasa

---

(12) (Ek: 6757 - 9.11.2016 / m.22) Kurum, görevi kapsamında ilgili yerlerden bilgi, belge, veri ve kayıtları alabilir ve değerlendirmesini yapabilir; arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilir, bunlarla irtibat kurabilir ve bu kapsamda diğer gerekli önlemleri alabilir veya aldırabilir. Kurum, bu fıkrada belirtilen görevlerin ifasında bakanlıklar, kurum ve kuruluşlar ile işbirliği içerisinde çalışır. Bu kapsamda Kurum tarafından istenen her türlü bilgi ve belge talebi; ilgili bakanlık, kurum ve kuruluşlar tarafından gecikmeksizin yerine getirilir. Bu fıkraya göre bilgi ve belge talebinde bulunulması ve bu taleplerin yerine getirilmesine ilişkin usul ve esaslar ile diğer hususlar Cumhurbaşkanlığınca belirlenir." İlgili düzenlemelere internet ortamından ulaşmak için: http://www.kazanci.com/kho2/ibb/giris.html (Gözden Geçirilme Tarihi: 29.10.2020).

[695] Anayasa Mahkemesi'nin 2017/16 Esas, 2019/64 Karar Sayılı ve 24.07.2019 Karar Tarihli Kararı, söz konusu karara internet ortamında ulaşmak için Bkz. http://kararlaryeni.anayasa.gov.tr/Karar/Content/514c3cc8-6566-4874-a7da-bd28897a04ae?excludeGerekce=False&wordsOnly=False (Gözden Geçirilme Tarihi: 15.05.2020).

[696] Furkan Güven Arslan, "2019'da Türkiye'de Kişisel Verilerin Korunması", 31.12.2019: https://blog.lexpera.com.tr/2019-turkiye-kisisel-verilerin-korunmasi/ (Gözden Geçirilme Tarihi: 15.05.2020).

Mahkemesi tarafından her ne kadar BTK'nın 5809 Sayılı Kanun md. 60/10.,11. ve 12. fıkralarında BTK'nın bilgi ve belge talep etme yetkisinin siber güvenliği temin etme amacıyla sınırlı olduğu belirtilmişse de ilgili düzenlemelerin lafzından BTK'nın bu kapsamdaki görevinin siber güvenlikle sınırlı olmadığı sonucuna ulaşılacaktır. Anayasa Hukuku'nun temel ilkelerinden birisi olan kanunilik prensibi gereğince, T.C. Anayasası'ında temel hak ve özgürlüklere ilişkin her türlü sınırlamanın kanun ile yapılacağı öngörülmesine rağmen, yazar kanunla düzenlenmeyerek KHK ile öngörülen ve özel hayatın gizliliği ve kişisel verilerin korunması hakkında yönelik bu tarzda hükümlerin zaten yasama tekniği açısından sorunlu olduğunu ve açıkça Anayasa'ya aykırı olduğunu değerlendirmiştir. Kaldı ki, Arslan'ın da karşı oy yazısında dikkat çektiği üzere BTK'nın görevleri sadece siber güvenlikle sınırlı olmayıp Türkiye'de özellikle kamu kurum ve kuruluşların ölçülülük ve belirlilik ilkelerine aykırı şekilde bilgi talep ettiği Anayasa Mahkemesi'nin geçmiş tarihli kararlarına da yansıyan bir gerçek olduğundan, kanun koyucu tarafından BTK gibi düzenleyici kurumlara geniş takdir yetkisi tanıyan muğlak düzenlemelerin yazar tarafından her açıdan başta kişisel verilerin korunması hakkı ve özel hayatın gizliliğin korunması hakkı gibi temel hak ve özgürlüklere aykılık teşkil edebilecek düzenlemeler olduğu sonucuna ulaşılmıştır.

Bu kısımda ayrıca yukarıda belirtildiği üzere 5411 Sayılı Kanun ve 6493 Sayılı Kanun'da değişiklik öngörerek Türkiye'de "digital onboarding"[697] uygulamasına

[697] "Digital onboarding", video konferans yöntemi, görüntülü kimlik tanıma sistemleri, elektronik imza, e-ID gibi uygulamalar aracılığıyla uzaktan kimlik tespiti edilerek müşteri edinimini açıklamak amacıyla kullanılan bir kavramdır. Böylelikle bu uygulamalar vasıtasıyla bankalar ve finansal kuruluşlar, müşterilerini fiziken şubelerine yönlendirmeksizin müşterilerinin kimliklerini uzaktan kimlik tespiti yöntemleri ile tespit edebilecek ya da bunu yapmak için, söz konusu müşterilere daha önce kimlik tespiti yapmış başka bir bankadan – açık bankacılık servisleri aracılığıyla – hizmet alabileceklerdir. Bu konuda detaylı bilgi için bkz. https://www.procompliance.net/7247-sayili-kanun-ile-finansal-hizmetlerde-yeni-donem-uzaktan-musteri-edinimi-digital-onboarding/#:~:text=%C5%9E%C4%B0RKETLER%C4%B0%20%2F%20SPK%20%2F%20TCMB-,7247%20say%C4%B1l%C4%B1%20Kanun%20ile%20Finansal%20Hizmetlerde%20Yeni,Uzaktan%20M%C3%BC%C5%9Fteri%20Edinimi%20%E2%80%9CDigital%20Onboarding%E2%80%9D&text=Finansal%20hizmetlerde%20dijitalle%C5%9Fme%20ve%20teknolojinin,bir%20de%C4%9Fi%C5%9Fim%20ve%20d%C3%B6n%C3%BC%C5%9F%C3%BCm%20ge%C3%A7irmektedir. (Gözden Geçirilme Tarihi: 29.10.2020).

yönelik ilk düzenleme olan 7247 Sayılı Kanun çerçevesinde[698] 5809 Sayılı Kanun açısından değişikliğe gidildiğinden, bu değişiklikten bahsetmek uygun olacaktır. 7247 Sayılı Kanun neticeside, bankacılık sektöründe olduğu gibi elektronik haberleşme sektöründe de elektronik ortamda sözleşme yapılmasına imkân sağlayan değişikliğe gidilmesi hedeflenmiştir. 7247 Sayılı Kanun'un 7. maddesinde, 5809 Sayılı Elektronik Haberleşme Kanunu m. 49/f. 2'de abonelerin elektronik haberleşme hizmetine abone olurken abonelik sözleşmelerinin "imzalanması" şartı yerine abonelik sözleşmelerinin "kurulması" şeklinde bir değişikliğe gidilmiştir[699]. Bu düzenleme ile paralel şekilde, 5809 Sayılı Kanun m. 50/f. 1/c.1'de değişikliğe gidilerek abonelik sözleşmelerinin hem yazılı hem de elektronik ortamda kurulabileceği ve elektronik ortamda kurulacak sözleşmelerde başvuru sahibinin kimliğinin doğrulanmasına imkân verecek şekilde BTK tarafından belirlenecek yöntemlerin kullanılacağı düzenlenmiştir. Hüküm değişikliği öngören madde gerekçeleri incelendiğinde incelendiğinde[700], Türkiye'de dijital dönüşüm stratejilerine uyum sağlanması ve son dönemde Covid-19 salgını kapsamında alınan tedbirlere uygun olarak yazılı usulün yanı sıra mobil hizmetlerde - Türkiye'de aylık 2 milyon adet mobil hizmetlerde yeni abonelik sözleşmesi imzalandığı belirtilmiştir - elektronik ortamda abonelik ilişkisinin kurulması ve aynı zamanda abonelik sözleşmesinin feshi konusunda ise fiziken şubeye gidilmeyerek elektronik ortamda işlem yapılabilmesinin önemine dikkat çekilmiştir. Video konferans gibi yöntemlerle uzaktan kimlik bilgilerinin teyit edilmesi netice itibariyle internet ortamında gerçekleştirileceğinden yukarıda belirtilen saldırı vektörlerinden zararlı yazılımlar, port yönlendirme gibi ağa yönelik saldırılar bakımından yukarıda ilgili kısımlarda yer verilen önlemlerin alınması gereklidir.

---

[698] 7247 Sayılı "Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında Kanun" 26.06.2016 tarihinde 31167 Sayılı Resmi Gazete'de yayınlanmıştır. Yazar, tarafından çalışma kapsamında "7247 Sayılı Kanun" şeklinde kısaltılmıştır. İlgili kanun metnine ulaşmak için bkz. https://www.resmigazete.gov.tr/eskiler/2020/06/20200626-1.htm (Gözden Geçirilme Tarihi: 29.10.2020).

[699] 7247 Sayılı Kanun, m. 7.

[700] Bkz. 7247 Sayılı Kanun m. 8 ve m. 9 gerekçeleri, internet ortamında ulaşmak için bkz. https://www2.tbmm.gov.tr/d27/2/2-2945.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

5.2.9. 5070 Sayılı Elektronik İmza Kanunu

İlk bölümde açıklandığı üzere, elektronik para ve elektronik çek olmak üzere dijital ortamda yapılan birçok işlemin temelini elektronik imza[701] oluşturmakta olup elektronik imza elektronik ödeme işlemlerinde siber güvenliğin tesisinde önemli bir işlevi haizdir. Türkiye'de, elektronik imzanın yasal altyapısı 5070 Sayılı Elektronik İmza Kanunu (*"5070 Sayılı Kanun"*)[702]'nda düzenlenmiştir. 5070 Sayılı Kanun'un amacı, elektronik imzanın[703] hukuki ve teknik kullanımına ilişkin esasları düzenlemek olup elektronik imzanın hukuki altyapısı elektronik sertifika hizmet sağlayıcılarının faaliyetlerini ve her alanda elektronik imzanın kullanımına ilişkin işlemleri kapsamaktadır[704]. Çalışmayı ilgilendirmesi açısından 5070 Sayılı Kanun'un gerekçesine bakıldığında ise, yasa koyucu tarafından elektronik ticaretin gelişmesi ve elektronik imzanın kullanıcılar tarafından besinsenebilmesi açısından açık ağ sistemine yönelik güven unsuruna vurgu yapılarak bu güvenin, ancak taraflar arasında iletilen bilgilerin gizlilik ve bütünlüğünün korunması ile tarafların kimliklerinin doğruluğunun güvence altına alınmasına yönelik hukuki düzenlemelerle mümkün olacağı belirtilmiştir[705].

---

[701] Elektronik imzayı teknik açıdan basitçe açıklamak gerekirse, temelde açık anahtar altyapısına (*public key infrastructure*) dayanmakta olup matematiksel olarak ilişkili bir çift anahtar kullanılmaktadır: Anahtarlardan birisine açık anahtar (*public key*) denilmekte olup açık anahtar, güvenilir kabul edilen bir merci tarafından (elektronik sertifika hizmet sağlayıcı) onaylanarak sertifika haline getirilir ve her isteyenle rahatlıkla paylaşılabilir. Diğer anahtar ise gizli anahtar (*private key*) olarak adlandırılır ve bu anahtarın güvenliği son derecede önemlidir. Mevzuat açısından bakıldığında, el ile atılan imza ile aynı hukuki sonucu doğurabilecek işlem bahsi geçen gizli anahtarla yapılır. Gizli anahtarlar ayrıca, hem kimlik doğrulama amacıyla hem de şifreli gönderilmiş mesajları açmak amacıyla kullanılmaktadır. Bu konuda detaylı bilgi için bkz. *Keser Berber/Lostar*, s. 29.

[702] 5070 Sayılı Kanun'un tam metnine ulaşmak için: https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5070.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[703] Elektronik imza, 5070 Sayılı Kanun m. 3/f. 1/b uyarınca başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri olarak tanımlanmıştır.

[704] *5070 Sayılı Kanun,* m.1.

[705] 5070 Sayılı Kanun Genel Gerekçe ve madde gerekçeleri konusunda bkz. https://www.tbmm.gov.tr/sirasayi/donem22/yil01/ss333m.htm (Gözden Geçirilme Tarihi: 29.10.2020).

Elektronik imzanın günümüzde güvenilir bir yöntem olduğu bilinmekle beraber siber güvenlik açısından bu konuda kesin yargıya varmanın mümkün olmadığı ve dijital imza konusunda internet ortamında en güvenilir olduğu düşünülen yöntemlerin dahi saldırganlar tarafından farklı yöntemlerle aşılabileceği unutulmamalıdır[706].

Elektronik ödeme işlemlerinde olduğu gibi elektronik ortamda yapılan işlemler açısından kural olarak güvenli elektronik imza[707], elle atılan imza ile aynı hukuki sonucu doğurmaktadır[708]. Güvenli elektronik imza ile gerçekleştirilmeyecek işlemler şunlardır[709]: (i) Kanunların resmi şekle veya özel bir merasime tabi tuttuğu hukuki işlemler, (ii) Banka teminat mektupları dışındaki teminat sözleşmeleri. Elektronik imza açısından üzerinde durulması gereken bir diğer önemli husus zaman damgasıdır. Zaman damgası, 5070 Sayılı Kanun'da tanımlanmış olup bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve/veya kaydedildiği zamanın tespit edilmesi maksadıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kaydı ifade etmektedir[710]. Günümüzde, hiç kuşkusuz bir elektronik belgenin ispat gücü açısından en önemli olgulardan birisi de işlemin yapıldığı tarihi

---

[706] Doktrinde Keser Berber, dijital imzanın, el yazısı ile atılan imzanın sahip olduğu özellikleri, elektronik belgeler bakımından da sağlamaya çalışan bir yöntem olduğunu, dijital imzanın başkaları tarafından taklit edilmesinin güç olduğunu belirtmekle beraber siber güvenlik noktasında konuya ihtiyatlı bir yaklaşım göstermiştir. Zira, Keser Berber'e göre dijital imzanın taklidi konusunda günümüzde birçok şirketin web sayfalarının taklit edildiği, hacker'ların kol gezdiği bir internet ortamında dijital imzanın %100'e yakın bir garanti temin edeceğini varsaymak sanal bir beklenti olacaktır. Bkz. *Keser Berber, Elektronik Para,* s. 126-127. Sağıroğlu/Alkan da benzer şekilde e-imzanın elektronik mesaj veya iletiye eklenen ve göndereni emsalsiz şekilde tanımlayan veya taklit edilmesi çok zor olan bir sayısal kod olarak tanımladığını, ancak dijital imzanın internet ortamında birçok kolaylık sağlasa da bilgilerin başkaları tarafından elde edilme ve çalınma riski olduğunun kesinlikle unutulmaması gerektiğini belirtmiştir. Bkz. *Sağıroğlu/Alkan*, s. 80-81.

[707] 5070 Sayılı Kanun'un 4. maddesine göre, göre bir elektronik imzanın "güvenli elektronik imza" sayılabilmesi için münhasıran imza sahibine ait olması, sadece imza sahibinin kullanımında olan bir güvenli imza oluşturma aracı ile oluşturulması, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitine imkan vermesi ve imzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlaması gibi kriterleri sağlaması gereklidir.

[708] *5070 Sayılı Kanun,* m. 5 /f.1.

[709] *5070 Sayılı Kanun,* m. 5 /f.2.

[710] *5070 Sayılı Kanun,* m. 3/h.

herhangi bir kuşkuya yer bırakmayacak şekilde saptamak olduğundan zaman damgasının güvenilir olması önem taşımaktadır[711].

5070 Sayılı Kanun'da özellikle güvenli elektronik imza oluşturma araçları, elektronik sertifika hizmet sağlayıcı[712], bu hizmet sağlayıcının görev ve sorumlulukları gibi hususlarda ayrıntılı düzenlemelere yer verilmiştir.

Ayrıca, 5070 Sayılı Kanun'da bilgi güvenliğini ilgilendiren birtakım suçlar da düzenlenmiş olup kanunun 16. maddesinde elektronik imza oluşturma verilerinin izinsiz kullanımı suçu, 17. maddede ise elektronik sertifikalarda sahtecilik suçu düzenlenmektedir[713].

Bu konuda son olarak yazar, elektronik işlemlerde güvenli elektronik imza, zaman damgası, elektronik sertifika hizmet sağlayıcısı açısından 5070 Sayılı Kanun hükümlerinin 2004 yılında yürürlüğe girdiği ve son kanun değişikliklerinin 2016 yılında yapıldığı dikkate alındığında elektronik işlemlerde özellikle işlem güvenliğini sağlamak açısından Türkiye'deki mevzuat düzenlemelerinin yetersiz olduğu

---

[711] *Keser Berber*, s. 151. Ayrıca, zaman damgasının uygulama esasları hakkında detaylı bilgi için bkz. "Tübitak Bilgem Kamu Sertifikasyon Merkezi Zaman Damgası Uygulama Esasları", 21.06.2018: http://kamusm.bilgem.tubitak.gov.tr/BilgiDeposu/KSM_ZDUE/YON.01.02_02_KAMU_SM_ZAMAN_DAMGASI_UYGULAMA_ESASLARI.pdf (Gözden Geçirilme Tarihi: 15.05.2020).

[712] 5070 Sayılı Kanun'unda nitelikli elektronik sertifikanın hangi özellikleri (sertifikanın "nitelikli elektronik sertifika" olduğuna dair bir ibare, sertifika hizmet sağlayıcısının kimlik bilgileri ve kurulduğu ülke adı, imza sahibinin teşhis edilebileceği kimlik bilgileri, elektronik imza oluşturma verisine karşılık gelen imza doğrulama verisi, vb.) taşıması gerektiği belirtilmiştir (m. 9). Ayıca, elektronik sertifika hizmet sağlayıcısı ise kanunda elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişiler olarak tanımlanmıştır (m. 8/f. 1).

[713] 5070 Sayılı Kanun'un 16. maddesinde "imza verilerinin izinsiz oluşturulma suçu"nun basit hali açısından elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında; imza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanların bir yıldan üç yıla kadar hapis ve elli günden az olmamak üzere adlî para cezasıyla cezalandırılacağı belirtilmiştir. Bu suçun nitelikli hali elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenmesi olup bu durumda cezanın yarısına kadar artırılacağı hükme bağlanmıştır. 17. maddede ise, suç tipi olarak tamamen veya kısmen sahte elektronik sertifika oluşturanlar veya geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif edenlerin ve bu elektronik sertifikaları bilerek kullananların, iki yıldan beş yıla kadar hapis ve yüz günden az olmamak üzere adlî para cezasıyla cezalandırılacağı, elektronik sertifika hizmet sağlayıcısı çalışanları tarafından bu suçun işlenmesi halinde ise 16. maddedeki gibi bu cezaların yarısı kadar artırılacağı öngörülmüştür.

kanısındadır. Bu bağlamda, doktrinde de özellikle 2004 yılından bu yana geçen zaman zarfında güven hizmetlerine ilişkin gelişmelerin iç hukukumuza tam olarak yansıtılamamasının ödeme hizmetleri sektörü gibi Avrupa Birliği'nin eIDAS kapsamında düzenlenen kurumlar gibi bu regülasyonlardan beslenen kurumlar açısından uygulamada sorunlara yol açtığına işaret edilmiştir[714]. Yukarıda ayrıntılı şekilde açıklandığı üzere Avrupa Birliği'nde elektronik işlemlerde bilgi güvenliğinin sağlanması açısından başta 2019/881 Sayılı ENISA Ve Bilişim Ve İletişim Teknolojilerinde Siber Güvenlik Sertifikasyon Tüzüğü ve eIDAS Tüzüğü olmak üzere önemli adımlar atılmaktadır. Günümüzde dağıtık veri tabanı, dijital kimlik, blokzincir teknolojisi gibi yeni kurum ve kavramların konuşulduğu bir dünyada, yazar Türkiye'de elektronik işlemlerin güvenliği açısından salt 5809 Sayılı Kanun ve 5070 Sayılı Kanun gibi düzenlemelerle yetinmenin teknolojik gelişmeleri ülke olarak geriden takip etmek anlamına geleceğinden yasa koyucu tarafından bu konuda vakit kaybedilmeden gerekli düzenlemelerin yürürlüğe konulması gerektiği görüşündedir.

5.2.10. 5651 Sayılı İnternet Ortamında Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

5651 Sayılı İnternet Ortamında Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (*"5651 Sayılı Kanun"*) çerçevesinde internet yoluyla işlenen suçlarla mücadele kapsamında ilgili

[714] Doktrinde Keser Berber tarafından, özellikle 2004 yılından bu zamana kadar Avrupa Birliği mevzuatında eIDAS gibi regülasyonların iç hukukumuza aktarılmasının özellikle ödeme hizmetleri gibi bu tarz regülasyonlardan beslenen kuruluşlar açısından sorunlara sebebiyet verdiği ve güven hizmetlerinin mevzuatımızda bu nedenle çeşitlilik kazanamadığına ve uzaktan (remote) imzalama gibi bireyler açısından elektronik imza kullanımını kolaylaştıracak ve yaygınlaştıracak çözümlerin yaşantımıza girmediğine özellikle dikkat çekilmiştir. Bu konuda detaylı bilgi için bkz. *Keser Berber, Güven Hizmetleri*, s. VII, VIII. İlgili yazar tarafından Türkiye'de dijital dönüşüm bakımından gözlemlenen en büyük eksikliğin AB'den farklı olarak, regülasyonlar arasındaki etkileşimin göz ardı edilmesi olduğu değerlendirilerek (s. 17) bu bağlamda eIDAS ile paralel şekilde Türk Hukuku'nda özellikle BTK tarafından yapılacak mevzuat değişikliği ile ilgili ayrıntılı önerilere yer verilmiştir (s. 232-236).

düzenlemeler çerçevesinde içerik sağlayıcılar[715], yer sağlayıcılar[716], erişim sağlayıcılar[717] ve toplu kullanım sağlayıcılar[718] gibi internet ortamındaki aktörlere birtakım sorumluluklar ve görevler yüklenmiştir. Aynı zamanda, internet ortamındaki bu aktörlerin 5651 Sayılı Kanun'da belirtilen bu görev ve sorumlulukları yerine getirilmesi neticesinde internet ortamında işlenen belirli suçlarla mücadele amaçlanmıştır[719]. 5651 Sayılı Kanun ve sonrasında yayımlanan yönetmelikler[720]

[715] 5651 Sayılı Kanun m. 2/f. 1(f)'de içerik sağlayıcı, internet ortamında kullanıcılara her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişiler olarak tanımlanmıştır. 5651 Sayılı Kanun'un 4. maddesinde ise içerik sağlayıcılar internet ortamında kullanıma sunduğu her türlü içerikten sorumlu tutulmuştur.

[716] Yer sağlayıcılar, 5651 Sayılı Kanun'da hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişiler olarak tanımlanmıştır (*5651 Sayılı Kanun,* m. 2/ f. 1/m). Türkiye'de yer sağlayıcı olarak faaliyette bulunmak için Faaliyet Yönetmeliği'nde belirtilen esaslara göre faaliyet belgesinin alınması zorunlu tutulmuştur. Faaliyet belgesini haiz yer sağlayıcıların listesi için Bkz. http://www.tib.gov.tr/YS_listesi.html (Gözden Geçirilme Tarihi: 29.10.2020).

[717] Erişim sağlayıcılar, 5651 Sayılı Kanun'da kişilere internet ortamında erişim olanağı sağlayan gerçek ve tüzelkişiler olarak tanımlanmıştır (*5651 Sayılı Kanun,* m. 2/f. 1/j). Yer sağlayıcılara benzer şekilde erişim sağlayacılar açısından da faaliyet gösterebilmeleri için Faaliyet Yönetmeliği'nde belirlenen esaslara göre faaliyet belgesinin alınması gerekmektedir. Faaliyet belgesine sahip erişim sağlayıcıların listesi için Bkz. https://www.tib.gov.tr/ES_listesi.html. (Gözden Geçirilme Tarihi: 29.10.2020). Ayrıca, 5651 Sayılı Kanun kapsamında konuyu da doğrudan ilgilendirmesi açısından önemli bir düzenleme olarak m. 6/f. 2'de erişim sağlayıcılar, 6 aydan az olmamak ve 2 seneden fazla olmak üzere trafik bilgilerini saklayarak bu bilgilerin doğruluğunu, gizliliğini ve bütünlüğünü muhafaza etmekle yükümlü kılınmıştır.

[718] 5651 Sayılı Kanun'a göre, internet toplu kullanım sağlayıcıları belli bir yerde ve belli bir sürede internet kullanım olanağı sağlayanları ifade etmektedir (*5651 Sayılı Kanun,* m. 2/f.1/i). 5651 Sayılı Kanun'un 7. maddesine gereğince, internet toplu kullanım sağlayıcıları açısından, ticari amaçla hareket edip etmemelerine bağlı olarak farklı hukuki sorumluluk rejimi düzenlenmiştir. Buna göre, ticari amaçlı toplu kullanım sağlayıcılar internet kafeler olup faaliyete başlayabilmeleri açısından yer ve erişim sağlayıcılar gibi izin belgesi almakla yükümlüdür. Ancak, yer ve erişim sağlayıcılardan farklı olarak izin belgelerinin, BTK tarafından değil, bulundukları mahalli mülki amirden alınması ve mahalli mülki amir tarafından denetlenmeleri öngörülmüştür. Toplu kullanım sağlayıcılarının ticari amaçla bir faaliyet gerçekleştirip gerçekleştirmediğine bakılmaksızın suç oluşturan içerikleri önleme yükümlülüğü de 5651 Sayılı Kanun'da ayrıca düzenlenmiştir. Ayrıca anılan yasaya göre internet kafe gibi ticari amaçla hareket eden toplu kullanım sağlayıcılar ailenin ve çocukların korunması, suçun önlenmesi ve suçun tespiti çerçevesinde gerekli tedbirleri almakla yükümlüdür.

[719] *5651 Sayılı Kanun,* m. 1.

[720] 5651 Sayılı Kanun'un yürürlüğe girmesinden sonra, bu kanunla bağlantılı birtakım yönetmelikler yayınlanmıştır (Bkz. https://bidb.trakya.edu.tr/pages/5651-sayili-kanun-ile-ilgili-yonetmelikler):
(i) 24.10.2007 tarihli 26680 Sayılı "Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara Ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul Ve Esaslar Hakkında Yönetmelik", ilgili yönetmelik metnine ulaşmak için Bkz. https://www.resmigazete.gov.tr/eskiler/2007/10/20071024-12.htm (Gözden Geçirilme Tarihi: 29.10.2020).

kapsamında, Bilgi Teknolojileri ve İletişim Kurumu'nun (*"BTK"*) kanun kapsamındaki görev ve yetkileri, internet ortamındaki yayınların düzenlenmesinde uygulanacak usul ve esaslar ile bunlara uyulmaması halinde verilecek cezalar hüküm altına alınmıştır.

5651 Sayılı Kanun düzenlemeleri siber güvenlik açısından doktrin görüşleri ışığında değerlendirildiğinde ise Gök tarafından, 5651 Sayılı Kanun ile internetteki hukuka aykırı içerikle mücadele yönteminin öngörülüyor olmasının beraberinde birçok bilgi güvenliği riskine sebebiyet vermesi nedeniyle eleştirilmiştir[721]. Bu bağlamda, eleştirilerin merkezinde erişim engelleme tekniklerinin geliştiği ölçüde bu engelleri aşma konusundaki tekniklerin de zamanla geliştiği, somut bir örnekten hareket etmek gerekirse Youtube denilen internet platformunun yasaklandığı dönemde yasağa rağmen en çok tıklanan web sitesi olduğu, söz konusu engelleri aşmak için başvurulan yöntemler neticesinde ise kullanıcıların internet ortamında siber saldırılara daha açık oldukları ve bu durumun maddi ve manevi açıdan kişilere zarar verdiği belirtilmiştir[722]. Çakır/Kılıç'a göre ise, 5651 Sayılı Kanun gereğince, internet üzerinden gerçekleştirilen saldırının kimin tarafından yapıldığının tespit edilmesi amacıyla saldırıya maruz kalan kurumun internet üzerinden bilgi alışverişi yapan ve internet bağlantısı olan tüm sunucu ve kullanıcıların etkin logları ile kurum içindeki bağlantıyı gerçekleştiren

(ii) Toplu Kullanım Yönetmeliği, ilgili yönetmelik metnine ulaşmak için Bkz. https://www.resmigazete.gov.tr/eskiler/2007/10/20071024-12.htm (Gözden Geçirilme Tarihi: 29.10.2020).
(iii) 11.04.2017 tarihli 30035 Sayılı "İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik, ilgili yönetmelik metnine ulaşmak için Bkz. https://www.resmigazete.gov.tr/eskiler/2017/04/20170411-3.htm (Gözden Geçirilme Tarihi: 29.10.2020).

[721] Mehmet Salih Gök, "5651 Sayılı Kanun Ve Bilgi Güvenliği İlişkisi", İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü, Hukuk Yüksek Lisans Porgramı (Ekonomi Hukuku), (*"Gök"*), s. 57-59. İlgili teze internet üzerinden ulaşmak için bkz. https://docplayer.biz.tr/2438763-5651-sayili-kanun-ve-bilgi-guvenligi-iliskisi-mehmet-salih-gok.html (Gözden Geçirilme Tarihi: 29.10.2020).

[722] *Gök*, s. 61, ayrıca 5651 Sayılı Kanun'a göre internet erişiminin engellenmesine ilişkin detaylı bilgi için bkz. Mehmet Bedii Kaya, "Teknik Ve Hukuki Boyutlarıyla İnternete Erişimin Engellenmesi, On İki Levha Yayıncılık, İstanbul, 2010, (*"Kaya, Erişimin Engellenmesi"*), s. 85 vd.

kişinin tespiti için DHCP[723] sunucu logları ve kişiyi tespit etmekte kullanılacak diğer etkin logların tutulması gerektiğinin altı çizilerek 5651 Sayılı Kanun'un daha güvenli ve kontrollü bir internet hizmeti açısından önemli olduğu belirtilmiştir[724].

Çalışmayı kapsam itibariyle kısmen ilgilendiren 7253 Sayılı Kanun[725] ile, 5651 Sayılı Kanun kapsamında yasa koyucu tarafından 29.07.2020 tarihinde değişikliğe gidilmiştir[726]. Söz konusu değişiklik neticesinde yeni bir kurum olarak ilk kez "sosyal ağ sağlayıcı" isimli bir kurumun tanımına[727] yer verilerek Türkiye'de Twitter, Facebook, YouTube, Instagram gibi sosyal medya platformlarının regüle edilmesinin amaçlandığı görülmüştür. Bu değişiklik neticesinde, Türkiye'de sosyal medya şirketleri açısından konumuzu da ilgilendirdiği üzere "veri lokalizasyonu" ilkesine öncelik verilerek sosyal ağ sağlayıcılarına verilerini Türkiye'de bulundurma[728] ve günlük erişimi bir milyondan[729] fazla olan yurt dışı kaynaklı sosyal ağ sağlayıcılarına,

---

[723] Açılımı İngilizce'de "Dynamic Host Configuration Protocol" denilen bu protokol, esas itibariyle bir ağdaki IP adreslerinin dağıtım için hızlı, otomatik ve merkezi yönetim imkânı sağlamaktadır. DHCP ayrıca, bilgisayardaki ağ geçidi ve DNS sunucusu bilgilerini alt ağlara bölmek için de kullanılmaktadır. Türkçe'ye "Dinamik Ana Konfigürasyon Protokolü" olarak tercüme edilebilir. Bu konuda detaylı bilgi için bkz. https://www.ihs.com.tr/destek-merkezi/kb/dhcp-nedir/ (Gözden Geçirilme Tarihi: 29.10.2020).

[724] *Çakır/Kılıç*, s. 250. Doktrinde anılan yazarlar, Türkçe'de iz kayıtları olarak adlandırılabilecek log kayıtlarının kanıt olarak değerlendirilebilmesi için değiştirilmediğinden (integrity) emin olunması gerektiği, kurumlarda log yönetiminin belirli bir merkezde toplanması ve analizinin tek bir noktadan yapılması gerektiğini, log kayıtları üzerinden zaman zaman Savcılık kanalıyla yürütülen soruşturmalarda log dosyalarının adli bilişim açısından da önem taşıdığına dikkat çekilmiştir. Bu konuda detaylı bilgi için bkz. *Çakır/Kılıç,* s. 250-255.

[725] 7253 Sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun" tam metnine internetten ulaşmak için:
https://www.resmigazete.gov.tr/eskiler/2020/07/20200731.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[726] Bu kapsamda, 5651 Sayılı Kanun kapsamında değşiklik öngören 7253 sayılı Kanun, 29.07.2020 tarihinde TBMM'nde kabul edilmiş ve 31.07.2020 tarihinde Resmî Gazete'de yayımlanarak yürürlüğe girmiştir.

[727] Sosyal ağ sağlayıcı, sosyal etkileşim amacıyla kullanıcıların internet ortamında metin, görüntü, ses, konum gibi verileri oluşturmalarına, görüntülemelerine veya paylaşmalarına imkân sağlayan gerçek veya tüzel kişiler olarak tanımlanmıştır (*5651 Sayılı Kanun*, m. 2/f. 1/s).

[728] Sosyal ağ sağlayıcının Türkiye'de temsilci bulundurma zorunluluğu konusunda bkz. 5651 Sayılı Kanun, Ek Madde 4/f. 5'de *"Türkiye'den günlük erişimi bir milyondan fazla olan yurt içi veya yurt dışı kaynaklı sosyal ağ sağlayıcı, Türkiye'deki kullanıcıların verilerini Türkiye'de barındırma yönünde gerekli tedbirleri alır"* düzenlemesine yer verilmiştir.

[729] İlgili kanun değişikliği ve gerekçesine bakıldığında günlük erişim açısından neden bir milyon şeklinde bir rakamın belirlendiği ve bu konunun hangi teknik kriterler çerçevesinde bir milyon olarak

Türkiye'de Türk vatandaşı gerçek bir kişinin temsilci bulundurma zorunluluğu[730] getirilmiştir. Böylelikle kişilik haklarının ihlali noktasında bu değişiklikten önce Twitter, Facebook, YouTube, Instagram gibi dev sosyal medya platformlarından özellikle ABD menşeli olmaları nedeniyle IP adresleri konusunda savcılıklar ve kurumlar nezdinde bilgi talep edilmesine gereken bu hususta gerekli bilginin temin edilememesi sebebiyle, 5651 Sayılı Kanun'da bahsi geçen bu değişiklikle Türkiye'de temsilci bulundurmak zorunda olan bu şirketlere Türk Hukuku uyarınca gerekli bildirimde bulunarak bilgi alınma açısından daha etkin bir yöntemin amaçlandığı görülmüştür. Sosyal ağ sağlayıcıların, 5651 Sayılı Kanun kapsamında öngörülen yükümlülüklere uymamaları halinde ise, kademeli olarak eylemin niteliğine göre 10 milyon Türk Lirası'ndan 30 milyon TL'ye kadar idari para cezası ile internet trafiği bant genişliğinin %50 ila %90 oranında azaltılması ve reklam yasağı[731] gibi kadar birtakım idari cezalar düzenlenmiştir[732]. Yazar tarafından, her ne kadar çalışmanın 4.3.3. başlığı altında da tartışıldığı üzere, karşılaştırma hukuk bakımından Çin gibi birtakım ülkelerde verilerin yerel olarak saklanmasını zorunlu kılan geniş kapsamlı düzenlemelerin bulunduğu bilinse dahi, veri lokalizasyonu çerçevesinde 5651 Sayılı Kanun'da öngörülen bu değişikliklerin bulut bilişim teknolojisini kullanan birçok hizmet sağlayıcı şirket açısından Türkiye'de inovasyonu engelleyici bir durum olduğu değerlendirilmektedir[733]. Kaldı ki, yazar tarafından yeni kanun değişikliği neticesinde

değerlendirildiğine ilişkin gerek kanun metninde gerekse gerekçelerde herhangi bir netlik bulunmamaktadır.

[730] Sosyal ağ sağlayıcının Türkiye'de temsilci bulundurma zorunluluğu konusunda bkz. 5651 Sayılı Kanun, Ek Madde 4/f. 1.

[731] Reklam yasağı, 5651 Sayılı Kanun Ek m. 4/f. 2 kapsamında detaylı şekilde düzenlenmiştir. İlgili düzenlemeye göre hangi durumlarda reklam yasağının uygulanacağı, ilgili sosyal ağ sağlayıcı ile bu kapsamda sözleşme kurulamayacağı ve para transferi yapılamayacağı hüküm altına alınmıştır.

[732] Sosyal ağ sağlayıcılara uygulanacak idari yaptırımlar konusunda bkz. 5651 Sayılı Kanun, Ek Madde 4/f. 2.

[733] Literatürde, Determann tarafından özellikle dikkat çekildiği üzere, bazı ülkelerde vergi, defter tuma ve veriler gibi bazı kayıtların ülke içinde tutulmasının öngörülmesi gerekliliği salt belirli kayıtlar açısından geçerli olup bu konudaki genel teamül, verilere ilişkin asılların veya yedek kopyaların gereklilik olması halinde asılların veya yedek kopyaların yerel olarak tutulması kaydıyla verilerin buluta aktarılmasının yasaklanmamasıdır. Bu bağlamda, bahsi geçen bu genel teamülün yalnız Çin, Kazakistan, Endonezya ve Rusya gibi bazı ülkelerde dışına çıkılarak verilerin yerel olarak saklanmasına ilişkin geniş kapsamlı düzenlemeler kabul edilmiştir. Bkz. *Determann*, s. 147 (para. 5.14). Bu konuda Kaya ise bir

sosyal ağ sağlayıcıların temsilci bulundurmama eylemleri açısından 5651 Sayılı Kanun kapsamında açıkça uygulanacak idari para cezalarına yer verilmesine rağmen yukarıda belirtilen veri lokalizasyonu kapsamında öngörülen düzenleme açısından herhangi bir yaptırımın öngörülmemesinin bir eksiklik olduğu da değerlendirilmiştir. 29.07.2020 tarihinde TBMM'de kabul edilen ve yukarıda belirtilen 5651 Sayılı Kanun kapsamında de, sosyal ağ sağlayıcılar açısından yürürlük tarihinden (29.07.2020) itibaren üç ay içerisinde içerisinde değişiklikle öngörülen yükümlülüklerin yerine getirilmesi bakımından gerekli çalışmaların tamamlanması öngörülmüştür[734]. 5651 Sayılı Kanun kapsamında, ayrıca yürürlük bakımından ikili bir ayrıma gidilerek (i) m. 3 ve m. 8 düzenlemelerinin[735] yayım tarihinden itibaren altı ay sonra, (ii) diğer hükümlerin ise değişikliğin yayım tarihinde yürürlüğe gireceği düzenlenmiştir[736].

5.2.11. 6698 Sayılı Kişisel Verilerin Korunması Kanunu ("KVKK")

Kişisel verilerin korunması hakkının anayasal bir hak olması[737] akabinde, 6698 Sayılı Kişisel Verilerin Korunması Kanunu (*"KVKK"*), 2016 tarihinde TBMM Genel Kurulu tarafından kabul edilerek kanunlaşmış ve 07.04.2016 tarih ve 29677 sayılı Resmî

---

verinin yurtiçinde tutulmasının, o verinin güvenli şekilde tutulduğuna karine oluşturmayacağına, özellikle üzerinde dijital keşif (*e-discovery*) yapılmasını sağlayan, arşivleme standarlarına uygun ve log kayıtlarının da doğruluğunun, bütünlüğünün ve gizliliğinin sağlandığı bir bulut bilişim sisteminin kullanılmasının, yurtiçinde tutulan klasik bir barındırma hizmetinden daha makul bir tercih olduğunu belirtmiştir. Bu konuda detaylı bir değerlendirme için bkz. *Kaya, Elektronik Ticaret*, s. 156 vd.

[734] 5651 Sayılı Kanun, Geçici m. 5/a.

[735] 5651 Sayılı Kanun m. 3'de esas itibariyle BTK tarafından verilen idari para cezalarının muhatabın yurtdışında bulunması halinde kanunen 7201 Sayılı Tebligat Kanunu usulleri gereğince bildirimin yapacağı ve bu bildirimin yapıldığı tarihi izleyen beşinci günün sonunda tabligatın yapılmış sayılacağı düzenlenmiştir. 5651 Sayılı Kanun m. 8 ise, belirli katalog suçlara ilişkin olarak yeterli şüphenin olması halinde içeğin çıkarılmasına ve/veya erişimin engellenmesine karar verileceğine ve bu kapsamda adli, idari ve teknik açıdan hangi önlemlerin alınabileceği konusunda ayrıntılı bir düzenlemedir.

[736] 5651 Sayılı Kanun, m. 13.

[737] Doktrinde Yılmaz, kişisel veriler dâhil, özel hayatın anayasal güvence ile koruma altına alınmasındaki temel amacın, insan kişiliğinin serbestçe gelişmesine imkân vermek, kişiye kendisi ve yakınları ile baş başa kalabileceği, devlet ve başkaları tarafından rahatsız edilemeyeceği özerk bir alan sağlamak olduğu belirtilmiştir. Özellikle Yılmaz, kişisel verilerin korunması hakkının son kırk yılda büyük önem kazandığına ve bunda, bilgi ve teknolojilerin gelişmesiyle birlikte veri toplama ve bunları otomatik olarak işleme kapasitelerindeki artış ile bu artışa dayalı olarak kişilerin özel hayat mahremiyet alanında daha savunmasız hale gelmesinin önem bir etken olduğuna vurgu yapmıştır. Ayrıntılı bilgi için Bkz. *Yılmaz*, s. 47.

Gazetede yayımlanarak yürürlüğe girmiştir. KVKK ile kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülüklerin ile uyacakları usul ve esasların düzenlenmesi amaçlanmaktadır.

Öncelikle, elektronik ödeme sistemlerine siber saldırı durumları da dahil olmak üzere bankaların veya finansal kuruluşların siber saldırı sonucunda müşterilerinin kişisel ve finansal bilgileri üçüncü kişilerce ele geçirilmesi halinde, bu durumun KVKK açısından da önemli sonuçları bulunmaktadır[738]. Herşeyden önce, veri sızıntısı yaşayan kurum öncelikle 72 saat içerisinde bu durumu KVK Kurulu'na bildirmekle yükümlüdür[739]. Veri ihlal bildirimlerinin, KVK Kurulu'na online ortam üzerinden yapılması öngörülmüştür[740]. Ayrıca KVK Kurulu'nun 18.09.2019 tarihli ve 2019/271 Sayılı kararında[741] veri sorumlusunun ilgili kişiye ihlal bildirimini açık ve sade bir dil ile belirterek aşağıda asgari belirtilen hususlar olan:

(i) İhlalinin ne zaman gerçekleştiği,

[738] Veri sorumlusunun ve veri işleyenin, veri güvenliğine ilişkin sorumluluk rejiminin düzenlendiği KVKK m. 12 gereğince, veri işleyen kişilerin veri sorumluları ile öğrendikleri kişisel verileri KVKK hükümlerine aykırı şekilde başkasına ifşa edemeyeceği ve işleme amacı dışında kullanamayacağı, hatta bu yükümlülüklerin görevden ayrılmaları halinde dahi sonraki süreçte devam edeceği hüküm altına alınmıştır. Ayrıca, kişisel veriler noktasında veri sızıntısı yaşayan ve bu verilerin kanuna aykırı şekilde başkaları tarafından ele geçirildiğini öğrenen veri sorumlusunun, en kısa zamanda bu durumu Türkiye'de bu konuda yetkili düzenleyici kurum olan "Kişisel Verileri Koruma Kurulu"na bildirmesi gerektiği emredici bir düzenleme olarak karşımıza çıkmaktadır.

[739] KVK Kurulu'nun hukuken bağlayıcı nitelikteki 24.01.2019 tarihli ve 2019/10 Sayılı kararında m. 12'de belirtilen bildirim yükümlülüğün (ihlalin öğrenildiği tarihten itibaren) en az 72 saat içerisinde gerçekleştirilmesi gerektiği öngörülmüştür. Böylelikle KVKK m. 12'de zaman açısından net bir düzenleme bulunmamakla beraber KVK Kurulu'nun bu düzenlemesi ile GDPR'daki düzenleme ile paralel bir uygulamaya gidilmiştir. Söz konusu KVK Kurulu kararına internetten ulaşmak için: https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi (Gözden Geçirilme Tarihi: 29.10.2020).

[740] Online bildirimler, KVK Kurulu'nun https://ihlalbildirim.kvkk.gov.tr adresi üzerinden gerçekleştirilecektir (Gözden Geçirilme Tarihi: 29.10.2020).

[741] İlgili KVK Kurulu'nun kararı için bkz. https://www.kvkk.gov.tr/Icerik/5547/2019-271 (Gözden Geçirilme Tarihi: 29.10.2020).

(ii) Kişisel veri kategorileri bazında (kişisel veri / özel nitelikli kişisel veri ayrımı yapılarak) hangi kişisel verilerin ihlalden etkilendiği (elektronik ödeme sistemlerine yönelik siber saldırı söz konusu olduğunda, bu bağlamda veri sızıntısına konu kişilerin ad-soyad gibi kişisel bilgileri, banka hesap bilgileri ile kişilere ilişkin tüm finansal bilgileri vb. dikkate alınacaktır),

(iii) Kişisel veri ihlalinin olası sonuçları (örneğin veri sızıntısı nedeniyle zarara uğrayan kişilerin maddi zararı, siber atak neticesinde risk altında olabilecek diğer bilgileri, var ise sigortanın zararı tazmin etmesi sonucunda kişilerin uğradığı zararın ne kadarlık kısmının sigorta şirketi karşılanabileceği vb.) ,

(iv) Veri ihlalinin olumsuz etkilerinin azaltılması için alınan veya alınması önerilen önlemlerin neler olduğu (bu bağlamda teknik, idari ve hukuki siber güvenlik tedbirlerinin neler olduğu açıklanmalıdır),

(v) İlgili kişilerin veri ihlali ile ilgili bilgi almalarını sağlayacak irtibat kişilerinin isim ve iletişim detayları ya da veri sorumlusunun web sayfasının tam adresi, çağrı merkezi vb. iletişim yolları,

bildirmesi gerektiği karara bağlanmıştır:

Siber güvenlik noktasında özellikle bu çalışmayı doğrudan ilgilendirmesi sebebiyle Kişisel Verilerin Korunması Kurulu tarafından[742] geçmiş dönemde verilmiş bazı kararlar aşağıda şu şekilde değerlendirilmiştir:

[742] Özellikle KVK Kurulu'nun 31.05.2018 tarihli ve 2018/63 Sayılı İlke Kararı uyarınca özetle veri sorumlularınca uygun güvenlik düzeyini sağlamaya yönelik gerekli her türlü teknik ve idari tedbirin alınması gerektiği hususunda veri sorumlularının bilgilendirilmesine karar verilmiştir. Söz konusu teknik ve idari tedbirlerin kapsam itibariyle geniş içerikte olduğu belirtilmekte olup bu kapsamda *idari tedbirler*e örnek vermek gerekirse (i) risk analizi yapılması, (ii) personelin eğitilerek siber güvenlik konusunda farkındalığının artırılması, (iii) veri işleyenin denetlenmesi, (iv) kişisel veri güvenliğine ilişkin çeşitli politikalar hazırlanmalı ve bunların uygulanması için gerekli altyapı sağlanması, (v) kişisel verilerin azaltılması gibi tedbirler üzerinde durulmuştur. *Teknik tedbirler* ise, (i) siber güvenlik tedbirleri (güncel virüs tarayıcısı programlarının kullanılması, güvenlik duvarının oluşturulması, parola yönetimi,

KVK Kurulu'nun Amazon Turkey Perakende Hizmetleri Limited Şirketi hakkındaki başvuru ile ilgili 27.02.2020 Tarihli ve 2020/173 Sayılı Kararı ("Amazon Kararı")

Kısaca belirtmek gerekirse, KVK Kurulu'nun Amazon Turkey Perakende Hizmetleri Limited Şirketi'ni (*"Amazon Türkiye"*) özetle içeriğinde yurtdışına hukuka aykırı veri aktarımının da bulunduğu farklı birçok gerekçe çerçevesinde 1.200.000,00 TL tutarında para cezasına mahkûm etmiştir.

Bilindiği üzere, Amazon, müşterilerin elektronik ortamda birçok ürün ve hizmete ulaştığı bilinen bir e-ticaret uygulamasıdır. KVK Kurulu'nun bu kararda çalışmayı ilgilendiren yönü ise, ilgili kararda ihlal gerekçelerinden birisi olarak Amazon şirketinin müşterilerinin yurtdışına hukuka aykırı şekilde verilerin transfer edildiği belirtilmiştir[743]. Karar içeriğinde, KVK Kurulu tarafından müşterilerin onayını almak amacıyla taahhütname mektuplarının KVK Kurulu'na sunulmasına rağmen, KVK Kurulu tarafından henüz bu yönde bir karar verilmediği ve yeterli korumaya sahip ülkelerin de henüz belirlenmediği gerekçesiyle zımni irade beyanı ile açık rıza alınmaksızın kişisel verilerin yurtdışına aktarılmasının hukuka aykırı olduğu sonucuna ulaşılmıştır. Yazar, KVK Kurulu'nun bu görüşüne katılmamaktadır[744]. Başta belirtmek

vb.), (ii) log kayıtlarının tutulması yoluyla bir takip mekanizmasının oluşturulması, (iii) ortam güvenliğinin sağlanması, (iv) verilerin bulutta saklanması halinde veri güvenliğinin sağlanması için geleneksel olarak güvenlikli ağ merkezlerinin oluşturulması ve veri tabanlarının denetlenmesi gibi süreçlerden bahsedilmektedir. Bu konuda ayrıntılı bilgi için Bkz. https://www.rskveri.com/kisisel-verileri-koruma-kurulunun-31-05-2018-tarihli-ve-2018-63-sayili-ilke-kararinin-kvkk-gdpr-ve-alman-hukuku-isiginda-degerlendirilmesi/ (Gözden Geçirilme Tarihi: 29.10.2020).

[743] KVK Kurulu'nun Amazon kararına ilişkin karar özetine internette şu link üzerinden ulaşılabilir: https://kvkk.gov.tr/Icerik/6739/2020-173 (Gözden Geçirilme Tarihi: 29.10.2020).

[744] KVKK açısından konuya bakıldığında, kişisel verilerin yurtdışına aktarımı, kural olarak ancak ilgili kişinin aktarıma açık rızasını vermesi ile mümkündür. GDPR ile paralel şekilde bu kuralın iki istisnası bulunmakta olup ancak KVKK'nun 5. ve 6. maddelerdeki (kişisel veri işlerken açık rıza alınmasına gerek olmayan durumlara ilişkin) istisnalardan herhangi birinin mevcut olması ve:
(i) Alıcının KVK Kurulu tarafından yayınlanacak "güvenli ülkeler" listesindeki ülkelerden birinde bulunması veya
(ii) Türkiye'deki ve yurtdışındaki veri sorumlularının yeterli korumayı yazılı olarak taahhüt etmeleri ve Kişisel Verileri Koruma Kurulu'nun izninin olması ile mümkündür.

gerekir ki, her ne kadar son zamanlarda Türkiye'de veri lokalizasyonu ilkesine ağırlık verilerek bu kapsamda yasal düzenlemelerin gündemde olduğu değerlendirilse dahi, KVK Kurulu tarafından kararın verildiği tarih itibariyle verilerin yurtdışına aktarımı konusunda[745] "güvenli ülkeler listesi" yayınlanmamıştır[746]. KVK Kurulu tarafından bu eksiklik giderilmediği gibi siber güvenlik açısından ortada herhangi bir veri sızıntısı olmadığı halde doktrinde Kaya tarafından da dikkat çekildiği üzere verilen bu cezanın niteliği itibariyle özellikle İdare Hukuku'nda sıkça gündeme gelen ve idarenin eylem ve işlemlerinde kanunen öngörülen ceza ile idare tarafından uygulanan yaptırım bakımından ölçülü şekilde hareket etmesini öngören "ölçülülük ilkesi"[747] ile

Bu noktada, Amazon kararı açısından konuya bakıldığında yazar tarafından Kurul tarafından konunun farklı boyutları da dikkate alınarak daha geniş kapsamda değerlendirilmesi gerektiği sonucuna varılmıştır. Birincisi, KVK Kurulu açıkça Amazon'un bu istisnalardan yararlanmak konusunda taahhütname ile ilgili başvuru yapmasına rağmen henüz bu konuda herhangi bir karar vermediğini açıkça kabul etmiştir. İkincisi ise yukarıda da belirtildiği üzere, yurtdışına veri aktarımı konusunda güvenli ülkeler listesi yayınlamak KVK Kurulu'nun görev ve sorumluluğunda olan bir mesele olup KVK tarafından bu yükümlülüğün yerine getirilmediği görülmüştür. Sonuncusu ise, Amazon açısından müşterileri ile ilgili herhangi bir veri sızıntısı olduğuna dair somut bir bulgu veya emare bulunmadığından KVK'nun bu konuda tesis ettiği 1.200.000 TL değerindeki idari para cezasının eylemin niteliğine göre ağır bir ceza olduğu sonucuna varılmıştır.

[745] Yurtdışına veri aktarımı konusunda detaylı bilgi için bkz. https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim (Gözden Geçirilme Tarihi: 29.10.2020).

[746] Av. Mehmet Ali Köksal'ın KVK Kurulu'nun güvenli ülkeler listesi yayınlaması gerektiğine ilişkin görüş ve değerlendirilmesi için bkz. https://siberbulten.com/siber-guvenlik/kisisel-verileri-koruma-kurumunun-karar-ozeti-ortaligi-karistirdi/#3_Kurum_guvenli_ulkeler_listesi_yayinlamali (Gözden Geçirilme Tarihi: 29.10.2020).

[747] İdare Hukuku perspektifi açısından konuya bakıldığında, idarenin düzenleme yetkisini kullanırken uyması gereken en önemli ilke, "ölçülülük ve yerindelik" prensipleridir. İdare, bir düzenleme yaparken veya yaptırımda bulunurken, amaca ulaşmak için gereken en elverişli aracı kullanması (yerindelik) ve ulaşmak istediği amacı elde etmeye yetecek bir oranda (ölçülülük) hareket etmesi gerekmektedir. Danıştay 10. Dairesi'nin özellikle 15.09.2008 tarihli, 2006/946 E. ve 2008/6084 K. Sayılı Kararı içtihadında bu hususta şu tespit ve değerlendirmelere yer verilmiştir: *"(...) Ölçülülük ilkesi (...); amaç ve araç arasında makul bir ilişkinin bulunması, diğer bir deyişle yapılan sınırlamayla sağlanan yarar arasında hakkaniyete uygun bir dengenin bulunması gereğini ifade etmektedir. Bu ilkenin; sınırlayıcı önlem ile sınırlama amacı arasındaki ilişkinin denetiminde, yasal önlemin sınırlama amacına ulaşmaya elverişli olup olmadığını saptamaya yönelik "elverişlilik", sınırlayıcı önlemin sınırlama amacına ulaşma ve demokratik toplum düzeni bakımından zorunlu olup olmadığını arayan "zorunluluk", ayrıca amaç ve aracın ölçüsüz bir oranı kapsayıp kapsamadığını, bu yolla ölçüsüz bir yükümlülük getirip getirmediğini belirleyen "orantılılık" ilkeleri olmak üzere üç alt ilkesi bulunmaktadır."* İlgili içtihada internet ortamında ulaşmak için bkz. http://www.kazanci.com/kho2/ibb/giris.html (Gözden Geçirilme Tarihi: 29.10.2020).

bağdaşmadığı değerlendirilmiştir[748]. KVK Kurulu'nun Amazon kararında, kişisel verilerin korunması, ticari elektronik iletiler gibi birçok hukuki mesele kapsamlı şekilde ele alınmasına rağmen, çalışmanın konusu elektronik ödeme sistemlerinde siber güvenlik olması sebebiyle bu çerçevede söz konusu karar sadece çalışmayı ilgilendiren boyutu ile ele alınmıştır.

KVK Kurulu'nun Bir Banka Hakkında Veri İhlali Sebebiyle Verdiği 26.11.2019 tarihli Ve 2019/352 Sayılı Kararı ("2019/352 Sayılı Karar)

Bir bankanın, KVK Kurulu nezdinde yapmış olduğu kişisel veri ihlali formunda banka personelinin farklı tarihlerde en az altı müşterinin verilerinin banka dışına çıkarak söz konusu personelin yüksek miktarlı dolandırıcılık eylemlerine aracı olduğu veri sızıntısı olayı nedeniyle KVK Kurulu, ilgili banka hakkında KVKK m. 12/f. 1'de veri güvenliği konusunda teknik ve idari tedbirleri almamak sebebiyle 70.000 TL ve KVKK m. 12/f. 5'de veri ihlalini en kısa sürede bildirme yükümlüğüne[749] aykırı davranmak sebebiyle 30.000 TL olmak üzere toplamda 100.000 TL idari para cezası uygulanmasına karar vermiştir. 2019/352 Sayılı kararda özellikle çalışanlar tarafından banka dışına gönderilen e-postalar bakımından veri sızıntısı tespit/önleme sisteminin bulunmasının belirtilmesine rağmen, kurumsal e-postadan kişisel veri sızıntısı olduğu takdirde KVK Kurulu tarafından bu durum alınan tedbirlerin ihlali engellemeye yeterli olmadığı şeklinde yorumlanmış olup karar içeriğinde özellikle kredi kartı numarası içeren e-postaların belirli bir adedin üzerinde olması halinde karantinaya alınması şeklindeki

[748] Doktrinde Kaya tarafından, özellikle Amazon kararı ile ilgili olarak söz konusu karar özetinde bu konuda kapsamlı bir bilgi yer almadığı için varsayımlarla bir değerlendirme yapıldığı, eğer aydınlatma metninde böyle bir ifade yer almasına rağmen fiiliyatta kişisel veriler toplanmadığı veya işlenmediği hallerde, KVK Kurulu'nun işlenmeyen bir kişisel veri kategorisi açısından bu denli ağır bir ceza vermesinin ölçülü olmadığı gerekçesiyle söz konusu karar eleştirilmiştir. Bu konuda detaylı bilgi için bkz. *Kaya, Elektronik Ticaret*, s. 149'daki 213 no'lu dp.'daki açıklamalar.

[749] 24.01.2019 tarih ve 2019/10 sayılı KVK Kurulu kararında GDPR ile uyumlu olarak ihlali bildirim konusunda en kısa süreden kastedilen zaman diliminin 72 saat olduğu belirtilmiştir: https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi (Gözden Geçirilme Tarihi: 29.10.2020).

teknik bir tedbirin de kötü niyetli kişilerce kolayca aşılabilecek nitelikte olduğuna özellikle dikkat çekilmiştir[750].

KVK Kurulu'nun Bir Turizm Şirketi Hakkında Siber Saldırı Neticesinde Verdiği 27.08.2019 Tarihli ve 2019/255 Sayılı Kararı ("2019/255 Sayılı Kararı")

KVK Kurulu'nun 2019/255 Sayılı Kararı'nda, bir turizm şirketinin LAN denilen yerel alan ağı üzerinde bir siber saldırı sonucunda yetkisiz şifre girişi neticesinde personel verileri (banka hesap bilgileri de dahil olmak üzere ad, soyad, TC kimlik numarası, doğum tarihi, medeni durum, eş çalışma bilgisi, çocuk sayısı, anne adı, baba adı, adresi, GSM numarası) ile müşteri bilgilerinin (kredi kartı bilgileri – son kulanım tarihi gibi - de dahil olmak üzere ülke/eyalet, uyruk, doğum tarihi, ad, soyad, telefon numarası, eposta adresi, mektup adresi) gibi verilerde sızıntı olduğu tespit edilerek veri güvenliğini sağlamaya yönelik gerekli teknik ve idari ve tedbirleri almadığı gerekçesiyle KVKK m. 18/f. 1/b uyarınca 400.000 TL, aynı zamanda ilgili şirket tarafından tespit edilen ihlale ilişkin ilgili kişilere bildirim yapılmadığı gerekçesiyle KVKK m. 12/f. 5'de belirtilen en kısa sürede bildirimde bulunma yükümlülüğüne aykırılık teşkil etmesi 100.000 TL olmak üzere toplamda 500.000 TL idari para cezası uygulanmasına karar verilmiştir[751].

KVK Kurulu'nun Facebook Aleyhine Verdiği 11.04.2019 Tarihli ve 2019/104 Sayılı Kararı ("Facebook Kararı")

KVK Kurulu tarafından Facebook şirketi aleyhine verdiği kararda özetle, Facebook platformu üzerinde fark edilen ve bir yazılım hatası olan fotoğraf API hatası neticesinde, üçüncü taraf uygulamalarının Facebook kullanıcılarının bu platform üzerinde paylaşıma açmadığı fotoğraflarını erişime açık hale getirmesi dikkate alınarak

[750] KVK Kurulu'nun 2019/352 Sayılı kararının özetine ulaşmak için: https://www.kvkk.gov.tr/Icerik/6656/2019-352(Gözden Geçirilme Tarihi: 29.10.2020).
[751] KVK Kurulu'nun 2019/255 Sayılı karar özetine ulaşmak için Bkz. https://www.kvkk.gov.tr/Icerik/5537/2019-255 (Gözden Geçirilme Tarihi: 29.10.2020).

bu durumun KVKK m. 12/f. 1 gereğince Facebook'un meydana gelen veri ihlali karşısında gerekli teknik ve idari tedbirleri almadığı gerekçesiyle 1.100.000 TL ve KVKK m. 12/f. 5 uyarınca ise en kısa sürede bildirim yapılması yükümlülüğüne aykırı hareket etmiş olduğu gerekçesiyle 500.000 TL olmak üzere toplamda 1.650.000 TL idari para cezası uygulanmasına karar verilmiştir[752].

5.2.12. Taslak Halindeki Hukuki Düzenlemeler

5.2.12.1. Ulusal Bilgi Güvenliği Teşkilatı Ve Görevleri Hakkında Kanun Tasarısı

Söz konusu kanun taslağı ile devletin ulusal ve ekonomik çıkarlarının güvence altına alınabilmesi için merkezi bir ulusal bilgi güvenliği yönetim yapısı oluşturularak bu yapı ile ulusal güvenliği ilgilendiren meselelerde gerekli bilgilerin korunması, devletin bilgi güvenliği faaliyetlerinin geliştirilmesi gerektiği, kısa ve uzun dönemli planların hazırlanması, bilgi sistemlerinin teknolojiye uyumunun sağlanması ve son olarak bu yasal düzenleme ile kamu ve özel bütün kurum ve kuruluşlar nezdinde bilgi güvenliğine geçilmesi konusunda gerekli yapılanmaya gidilmesi amaçlanmıştır (Genel Gerekçe)[753].

Toplam yirmi yedi madde ve dört bölümünden oluşan kanun taslağı metni ile ilgili dikkat çeken düzenlemeler şunlardır:

Ulusal bilgi güvenliğinin sağlanması amacıyla Başbakanlığa bağlı Ulusal Bilgi Güvenliği Üst Kurulu (*"UBGÜK"*) ile tüzel kişiliğe sahip katma bütçeli Ulusal Bilgi Güvenliği Kurumu (*"UBKB"*) Başkanlığı olmak üzere iki birimin kurulması öngörülmüştür (md. 4). Basitçe açıklamak gerekirse, UBGÜK Hükümet düzeyinde çalışacak bir üst organ UBGK ise bu üst organın direktifleri çerçevesinde ulusal bilgi güvenliğinin korunması amacına hizmet edecek katma bütçeli bir kamu tüzelkişiliğini haiz olacaktır. Bu bağlamda, kanun taslağında UBGÜK'ün, genel direktif organı

---

[752] KVK Kurulu'nun yukarıda belirtilen Facebook kararı için bkz. https://www.kvkk.gov.tr/Icerik/5450/2019-104 (Gözden Geçirilme Tarihi: 29.10.2020).

[753] https://www.tbd.org.tr/ulusal-bilgi-guvenligi-teskilati-ve-gorevleri-hakkinda-kanun-tasarisi/ (Gözden Geçirilme Tarihi: 29.10.2020).

olacağı ve Başbakan'ın başkanlığında üyelerinin de Adalet, Milli Savunma, İçişleri, Dışişleri, Ulaştırma, Sanayi ve Ticaret Bakanları ile Milli Güvenlik Kurulu genel sekreteri, Genel Kurmay Muharebe Elektronik ve Bilgi Sistemleri Başkanı, Milli İstihbarat Teşkilatı Müsteşarı, Türkiye Bilimsel Ve Teknik Araştırma Kurumu ile kurum başkanından teşekkül edeceği belirtilmiştir (m. 5). UBGÜK'ün görevleri, özetle ulusal bilgi güvenliğine yönelik tehdidi değerlendirmek, ulusal bilgi güvenliği siyasetinin belirlenmesi ve uygulamasıyla ilgili kararları almak ve gerektiğinde ulusal bilgi güvenliğine ilişkin mevzuat değişikliği tekliflerini değerlendirmektir (m. 7).

UBKB teşkilatı ise temelde, Plan Program ve Koordinasyon Daire Başkanlığı, Bilgi Güvenliği Daire Başkanlığı, Kriptoloji Daire Başkanlığı, Bilgi Destek Daire Başkanlığı, Denetleme ve Bilgilendirme Daire Başkanlığı olmak üzere beş ana hizmet biriminden oluşmaktadır (md. 6). UBKB'nin görevleri ise UBGÜK'e kıyasla kanun taslağında daha kapsamlı belirlenmiş olup bu görevlerinden bazıları, UBGÜK'ün kararlarını ve direktiflerini uygulamak, kripto sistemlerinde kullanılacak standartları ve materyalleri belirlemek, haberleşme güvenliği sistemlerinin tehdit analizi ve hassasiyet değerlendirmelerini yapmak, ulusal bilgi güvenliği ile ilgili uluslararası mevzuat ve teknolojideki gelişmeleri takip etmektir (m. 8).

Kanun taslağının 18. maddesinde tüm kamu ve özel kurum ve kuruluşlarının, ulusal güvenliği ilgilendiren bilginin korunması konusunda gereken tedbirleri almakla sorumlu olduğu belirtilmiş olup bu hükme uymamanın yaptırımı olarak ise, 25. maddede (suçun basit şekli olarak) bir yıldan beş yıla kadar hapis cezası ile cezalandırılacağı hüküm altına alınmıştır. Aynı hükümde suçun nitelikli hali olarak failin kendisine veya bir başkasına yarar sağlaması veya fiilin bir zarara sebebiyet vermesi halinde ise hapis cezasının iki yıldan az olmayacağı düzenlenmiştir.

UBKB'nin döner sermaye işletmesi kurabileceği ve döner sermaye işletmesinin sermayesinin ise 2,5 trilyondan az olmayacağı düzenlenmiştir (m. 24).

Yazar tarafından, söz konusu kanun taslağının Türkiye'de ulusal bilgi güvenliğinin korunması açısından önemli bir katkısı olacağını değerlendirmekle beraber özellikle kanun taslağı hükümleri ile ilgili yapılan değerlendirmede:

(i) UBGÜK'ün tamamen hükümetin talimatı ile çalışan üst bir organ olduğu dikkate alındığında ulusal bilgi güvenliği gibi hassas ve etkin şekilde hareket edilmesi gereken bir konuda her zaman bağımsız şekilde hareket edemeyebileceği,

(ii) Özellikle kurum üyelerinin tamamen başbakan ve bakanlardan teşekkül ettiği halde asıl uzmanlığı siber güvenlik olan akademisyen ve uygulamacıların kurum içerisinde yer almamasının siber güvenlik gibi teknik uzmanlığı gerektiren bir konuda gerekli kararların alınması bakımından bilgi zafiyetine neden olabileceği,

(iii) Son olarak, taslağın 18. maddesinde belirtilen "tüm kamu ve özel kurum ve kuruluşlarının, ulusal güvenliği ilgilendiren bilginin korunması konusunda gereken tedbirleri almakla sorumlu" tutulmasının içerik itibariyle muğlak şekilde yorumlanabilecek soyut ibareler içerdiği, bu nedenle ilgili kanun hükmünde ulusal bilgi güvenliğinin sağlanmasındaki sorumluluk rejiminin daha net ifadelerle belirtilmesi gerektiği,

gerekçeleriyle kanun taslağı eleştirilmiştir.

5.2.12.2. Bilişim Ağ Hizmetlerinin Düzenlenmesi Ve Bilişim Suçları Hakkında Kanun Tasarısı

Kanun tasarısının Genel Gerekçe bölümü incelendiğinde, Türkiye'de bilişim ağı hizmetlerinin etkin ve doğru bir şekilde verilmesi ve bilişim suçları ile mücadelede internet servi sağlayıcılarının sorumluluklarının belirlenmesinde bir ihtiyaç olduğu ve bu konuyla ilgili hiçbir düzenleme olmadığı belirtilmiştir. Bu noktada, Almanya'daki Tele Hizmetler Kanunu'nun referans gösterilerek bahsi geçen kanun tasarısı ile özellikle bu alandaki boşluğun doldurulmasının amaçlandığı üzerinde durulmuştur.

Tasarı, toplamda otuz dört maddeden ve yedi bölümden oluşmaktadır. İlk bölümde, tasarının amaç ve kapsamına ilişkin düzenlemelere yer verilerek aynı zamanda bazı terimlerin tanımlarına yer verilmiştir. İkinci bölümde internet ortamında hizmet veren yer sağlayıcı[754], içerik sağlayıcı[755], ortam sağlayıcı[756] ve toplu kullanım sağlayıcı[757] gibi aktörlerin sorumluluk rejimine ilişkin düzenlemeler yer almaktadır. "Bilgilerin Gizliliğine, Bütünlüğüne Ve Elde Edilmesine İlişkin Suçlar" başlıklı kanun taslağının üçüncü bölümünde genel itibariyle bilişim sistemlerine ilişkin suç tiplerine (kanun taslağının 15. maddesinde bilişim sistemine girme ve veri elde etme suçu, 16. maddede verilere, programların bütünlüğüne veya sistemin çalışmasına müdahâle suçu, 17. maddede ise hukuka aykırı donanım veya program sağlama suçuna ilişkin düzenlemelere yer verilmiştir), dördüncü bölümde ise bilişim sistemi ile bağlantılı

[754] Taslak metinde yer sağlayıcı, hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri ifade etmektedir (m. 2/1/ö). Yer sağlayıcının sorumluluk rejimi, 8. maddede düzenlenmekte olup kanun taslağına göre genel kural, yer sağlayıcının, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü olmamasıdır. Bu genel kuralın istisnaları (i) yer sağlayıcının hukuka aykırı içerikle ilgili ceza sorumluluğunun saklı olduğu, (ii) kanun taslağının 13. maddesi (içerik sağlayıcılara erişilememesi durumunda yer sağlayıcının içeriğin düzeltilmesini veya erişimin engellenmesini istemesi) ve 29. madde gereği (erişimin engellenmesi kararının yer sağlayıcı tarafından yerine getirilmesi) haberdar edilmesi ve engelleme yeteneği bulunması durumunda hukuka aykırı içeriğe erişimi engellemek zorunda olduğu, (iii) taslağın 5. maddesi gereğince içerik ve ortam sağlayıcılara bilgilendirme yükümlülüğüdür.

[755] Kanun taslağının m. 2/1/h'de içerik sağlayıcı, bilişim ağı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişileri olarak tanımlanmıştır. Burada özellikle dikkat çeken düzenleme 5651 Sayılı Kanun'dan farklı olarak içerik sağlayıcının, bilişim ağı üzerinde kullanıma sunduğu her türlü içerikten sorumlu olacağı hüküm altına alınmıştır. İçerik sağlayıcının sadece başkasına ait içerikten sorumlu olmayacağı, ancak içerikteki sunuş şeklinden, bağlantı sağlandığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise genel hükümlere göre sorumlu olacağı düzenlenmiştir (Tasarı, m. 7).

[756] Ortam sağlayıcı, kanun taslağında bilişim ağı üzerinde, herkese açık olarak kullanıcılarına yardım, bilgilendirme, danışma veya benzer türde hizmet sunanlar olarak tanımlanmıştır (m. 2/1/j). Ortam sağlayıcının sorumluluk rejimi yer sağlayıcıya benzerlik göstermekle (ceza sorumluluğu hükümleri saklı kalmak kaydıyla ve taslağın 13. ve 29. maddeleri gereğince haberdar etme ve engelleme yeteneği bulunması durumunda hukuka aykırı içeriği kaldırmakla yükümlü olduğu belirtilmekle beraber yer sağlayıcıdan farklı olarak ortam sağlayıcının, içerik sağlayıcı bilgilendirme yükümlülüğü bulunmamaktadır (m. 10).

[757] Toplu kullanım sağlayıcı, taslak metnin Tanımlar bölümünde kişilere belli bir yerde ve belli bir süre bilişim ağını kullanım olanağını sağlayan tüzelkişileri ifade etmektedir (m. 2/1/m). Taslağın 12. maddesinde ticarî amaçla toplu kullanım sağlayıcıların, mahallî mülkî amirden ruhsat almakla yükümlü olduğu ve konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almakla yükümlü olduğu belirtilmiştir.

suçlar düzenlenmiştir. Beşinci bölümde ise, spesifik olarak çocuk pornografisi, devletin güvenliğine ve kamu barışına karşı işlenen suçlar, tehdit ve şantaj gibi suç teşkil eden içerikle ilgili düzenlemeler öngörülmüştür. Söz konusu suçlarla ilgili soruşturma ve kovuşturma usullerine ilişkin hükümler yer almaktadır.

Söz konusu kanun tasarısı, TCK'da gerek bilişim sistemleri aracı kılınmak suretiyle işlenen suçlar gerekse de bilişim sektörüne özgü spesifik suçlar düzenlenmesi nedeniyle, konunun yeniden farklı bir kanunla düzenlenmesinin gereksiz yere genel kanun-özel kanun şeklinde tartışmalara yol açacağı ve özellikle TCK'da ve anılan kanun tasarısında benzer suç fiilleri için farklı cezaların öngörülmesinin birçok karışıklığa sebebiyet vereceği gerekçesiyle anılan kanun tasarısı Türkiye Bilişim Derneği tarafından eleştirilmiştir[758].

5.2.12.3. Bankalarca Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine İlişkin Tebliğ Taslağı ("Tebliğ Taslağı")

Tebliğ Taslağı, Türkiye'de yukarıda bahsi geçen 5070 Sayılı Kanun ve 5809 Sayılı Kanun bakımından "digital onboarding" ile ilgili yasal gelişmeler ışığında, bankalar tarafından yeni müşteri kazanımında ve müşteri kimliğinin doğrulanmasında kullanılabilecek uzaktan kimlik tespiti yöntemlerine ilişkin usul ve esasları düzenlenmesi amacıyla BDDK tarafından hazırlanmıştır.

[758] Yukarıda belirtilen husus dışında ilgili kanun tasarısı özellikle muhtelif hükümler çerçevesinde de ayrıntılı değerlendirilerek eleştirilmiştir. Bu konuda ayrıntılı bilgi için Bkz. https://www.tbd.org.tr/bilisim-agi-hizmetlerinin-duzenlenmesi-ve-bilisim-suclari-hakkinda-kanun-tasarisi-gorusleri/ (Gözden Geçirilme Tarihi: 29.10.2020).

Tebliğ Taslağı'nın hukuki dayanağını teşkil eden yasal düzenlemeler, Bankacılık Kanunu m. 76/f. 2[759] ile Elektronik Bankacılık Yönetmeliği'nin 43. maddesidir[760].

Çalışma açısından, Tebliğ Taslağı'nda dikkat çeken düzenlemeler şunladır:

[759] İlgili düzenlemede, 18.06.2020 tarihinde yürürlüğe giren 7247 Sayılı Kanun neticesinde, yazılı yöntemlerin yanı sıra, bankalar ve müşterileri arasındaki ilişkilerin uzaktan iletişim araçlarının kullanılması suretiyle BDDK'nın yazılı şekil koşulunun yerine geçebilecek şekilde belirleyeceği, bir bilişim veya elektronik haberleşme cihazı üzerinden gerçekleştirilebilecek ve müşteri kimliğinin doğrulanmasına imkan verecek yöntemler yoluyla kurulacak sözleşmeler ve bu konuya ilişkin usul ve esasların BDDK tarafından düzenleneceği belirtilmiştir. Bu konuda ayrıntılı bilgi için bkz. https://mevzuat.gov.tr/mevzuat?MevzuatNo=5411&MevzuatTur=1&MevzuatTertip=5 (Gözden Geçirilme Tarihi: 29.10.2020).

[760] Elektronik Bankacılık Yönetmeliği'nin 43. maddesinde, esas itibariyle bankaların, (5549 Sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun ve alt düzenlemelerinde yer alan yükümlülükler saklı kalmak kaydıyla) müşterilerinin veya müşterileri adına hareket eden kişilerin kimliklerini tespit edebilmek maksadıyla uzaktan kimlik yöntemlerini kullanabileceği düzenlenmiştir. https://www.resmigazete.gov.tr/eskiler/2020/03/20200315-10.htm
https://www.resmigazete.gov.tr/eskiler/2020/03/20200315-10.htm (Gözden Geçirilme Tarihi: 29.10.2020)

Tebliğ Taslağı'nda, basit cihazla görülebilen güvenlik öğeleri[761], beyaz ışık[762], gözle görülebilen güvenlik öğeleri[763], kimlik paylaşım sistemi[764], MRZ[765] ve SMS OTP[766] ve yakın alan iletişimi[767] gibi uzaktan kimlik tespiti ile ilgili birtakım teknik kavramların tanımına yer verilmiştir.

Uzaktan kimlik tespitine ilişkin genel ilkelere bakıldığında, siber güvenlik açısından önem taşıyabilecek olan müşteri ile temsilcisinin fiziksel olarak aynı ortamda bulunmaksızın, çevrim için görüntülü olarak iletişim kurması, görüntülü görüşme esnasında yüz yüze yapılan kimlik tespiti yöntemine benzer ve asgari seviyede risk

[761] Gözle net bir şekilde görülmesi mümkün olmayan ve sadece büyüteç ve benzeri basit alet ve yöntemlerle ayırt edilebilen hologram ve mikro yazı gibi güvenlik öğelerini ifade etmektedir (*Tebliğ Taslağı,* m. 3/f. 1/c).

[762] Beyaz ışık, gün ışığına benzer şekilde görünürde renksiz olan ışık anlamına gelmektedir (*Tebliğ Taslağı,* m. 3/f. 1/ç).

[763] Bakıldığı zaman, çıplak göz ile anlaşılması imkan dahilinde olan giyoş, gökkuşağı baskı, optik değişken mürekkep, gizli görüntü ve hologram gibi güvenlik öğeleri olarak tanımlanmıştır (*Tebliğ Taslağı,* m. 3/f. 1/e).

[764] Tebliğ Taslağı'nda bu tanım konusunda 8.12.2006 tarihli ve 26370 sayılı Resmî Gazete'de yayımlanan Kimlik Paylaşımı Sistemi Yönetmeliği'ne atıf yapılmıştır. Kimlik Paylaşımı Sistemi Yönetmeliği m. 4/f. 1/ğ gereğince, kimlik paylaşım sistemi merkezi veri tabanında tutulan verilerin alıcı kurumlar ile paylaşıldığı sistemi ifade etmektedir. Kimlik Paylaşımı Sistemi Yönetmeliği'ne ulaşmak için: https://mevzuat.gov.tr/mevzuat?MevzuatNo=2837&MevzuatTur=21&MevzuatTertip=5 (Gözden Geçirilme Tarihi: 29.10.2020).

[765] MRZ konusunda, 3.12.2019 tarihli ve 30967 sayılı Resmî Gazete'de yayımlanan Türkiye Cumhuriyeti Kimlik Kartı Yönetmeliği'ne atıf yapılmıştır. İlgili yönetmeliğin m. 4/f. 1/aa düzenlenmesi gereğince, MRZ, makine tarafından okunabilen bölge şeklinde tanınlanmıştır: https://mevzuat.gov.tr/mevzuat?MevzuatNo=34949&MevzuatTur=7&MevzuatTertip=5 (Gözden Geçirilme Tarihi: 29.10.2020). Gerçekten de, MRZ, bilişim terminolojisinde İngilizce'de "Machine Readable Zone" olarak ifade edilen ve Türkçe'ye "Makine Tarafından Okunabilir Bölge" olarak tercüme edilebilecek bir terimdir (Serbest Çeviri). MRZ kodu, pasaport, vize veya kimlik kartları üzerinde genelde kimlik sayfasının alt kısmında yer alan ve kişisel bilgilerin bu kod ile elektronik cihazlar tarafından okunmasını sağlayan bir standarttır. MRZ konusunda detaylı bilgi için bkz. http://kimlikokuyucu.com/s.-sorulan-sorular.html (Gözden Geçirilme Tarihi: 29.10.2020).

[766] SMS OTP kavramı ile ilgili olarak ise Tebliğ Taslağı'nda, Elektronik Bankacılık Yönetmeliği'ne atıf yapılmıştır. SMS OTP, Elektronik Bankacılık Yönetmeliği'nin m. 3/f. 1/ii gereğince, elektronik haberleşme işletmecilerinin sunduğu kısa mesaj servisi aracılığıyla iletilen tek kullanımlık parola olarak tanımlanmıştır.

[767] Yakın alan iletişimi, elektronik cihazların güvenilir şekilde temassız olarak işlem yapabilmesini ve sayısal içeriğe ve/veya elektronik cihazlara erişimine imkan sağlayan, veri okuma ve yazma için kullanılan kısa mesafeli kablosuz teknoloji olarak tanımlanmıştır. Çalışma kapsamında, Tebliğ Taslağı'nda yakın alan iletişimi olarak ifade edilen bu kavram "NFC Teknolojisi" olarak ifade edilmekte olup bu konuda 1.2.1.3. numaralı "Akıllı Kartlar" başlığı altında "NFC Teknolojisi İle Ödeme" başlığı altında detaylı teknik analizlere yer verilmiştir.

içerecek şekilde tasarlanması gerektiği, uzaktan kimlik tespitinde kullanılacak görüntülü görüşme yönteminde olası teknolojik, operasyonel ve benzeri riskler dikkate alınarak yeterli güvenlik seviyesi oluşturulacağı gibi düzenlemelere yer verilmiştir[768].

Siber güvenliğin sağlanmasında eğitimin önemi dikkate alındığında, Tebliğ Taslağı'nda eğitim almış banka müşteri temsilcisinin görüntülü kimlik tespitini gerçekleştireceği, müşteri temsilcisinin kimlik tespiti yönteminde kullanılabilecek belgelerin özelliklerini, bu belgeler bakımından uygulanan geçerli doğrulama yöntemlerini öğreneceği ve bilinen dolandırıcılık yöntemlerine karşı bilgi sahibi olmasının sağlanacağı hüküm altına alınmıştır. Aynı zamanda, uzaktan kimlik tespiti sırasında kullanılacak belgelerin yazılı şekilde dokümente edileceği ve bu yöntem ile kimlik tespiti gerçekleştirecek müşteri temsilcisinin periyodik olarak en az yılda bir kez ve her bir güncelleme sonrasında eğitim alması da zorunlu kılınmıştır[769].

Tebliğ Taslağı içeriğinden, uzaktan kimlik tespitine başlanılmasından önce, bu yöntem ile işlem gerçekleştirmek isteyen müşterinin öncelikle bir form ile başvuru yapacağı ve ilgili bankanın ise bu form kapsamında alınan veriler kullanılarak kişi hakkında risk değerlendirmesi gerçekleştireceği anlaşılmaktadır[770]. Aynı zamanda, müşteriden görüntülü görüşme ve uzaktan kimlik tespiti süreci ile ilgili en başta açık rıza alınacağı öngörülmüştür[771]. Bilgi güvenliği açısından bu konuda önem taşıyan husus ise, Tebliğ Taslağı'nda, müşteri temsilcisi ile kişi arasındaki görsel-işitsel iletişimin bütünlüğünün

---

[768] Yazar tarafından Tebliğ Taslağı'nda bazı düzenlemelerin muğlak ve belirsiz ifadeler içerdiği ve siber güvenlik bakımından etkin önlemlerin gerçekleştirilebilmesi açısından netleştirilmesi gerektiği değerlendirilmiştir. Tebliğ Taslağı kapsamında örnek vermek gerekirse, m. 4/f. 2'nin 2. cümlesinde her ne kadar *"Uygulanacak yöntem, yüz yüze yapılan kimlik tespiti yöntemine benzer ve asgari seviyede risk ihtiva edecek şekilde tasarlanır"* şeklinde bir düzenlemeye yer verilmişse de, uzaktan kimlik tespiti yönteminin hangi uygulamalar ile yüze yüze kimlik tespiti yöntemine benzer şekilde ve asgari seviyede risk ihtiva eden şekilde tasaralanabileceği Tebliğ Taslağı içeriğinden anlaşılamamaktadır. Benzer şekilde m. 4/f. 3'de, uzaktan kimlik tespitinde kullanılacak "görüntülü görüşmede olası teknolojik, operasyonel ve benzeri riskler" ibaresinden neyin kastetildiği anlaşılamamakta olup yazar tarafından bu ibarelerin muğlak olduğu değerlendirilmiştir. Çalışma kapsamında da dikkat çekildiği üzere, siber güvenliğin temininde atılacak en önemli adımlardan birisi, risklerin doğru ve detaylı şekilde tespit edilerek bu risklere karşı hangi önlemlerin alınması gerektiğine ilişkin ayrıntılı bir yol haritası çizilmesidir.

[769] *Tebliğ Taslağı,* m. 5.

[770] *Tebliğ Taslağı,* m. 6/ f. 1.

[771] *Tebliğ Taslağı,* m. 6/ f. 3.

ve gizliliğinin yeterli seviyede olması sağlanacağı ve yapılacak görüntülü görüşmenin uçtan uca güvenli iletişim kanalıyla gerçekleştirileceği düzenlenmiştir[772]. Tebliğ Taslağı'nda uzaktan kimlik tespiti açısından kullanılabilecek kimlik belgelerinin doğrulanması[773] ve kimliği tespit edilecek kişilerin doğrulanması[774] açısından da ayrıntılı düzenlemelere yer verilmiştir.

Görüntülü görüşme sırasında, güvenliğin sağlanması açısından kişiye yalnızca yapılan kimlik tespiti işlemi için geçerli, merkezi olarak üretilen SMS OTP iletileceği ve bu iletilen SMS OTP'nin ilgili kişi tarafından çevrim içi olarak uygulama ara yüzü üzerinden geri gönderilmesi sağlanması gerektiği belirtilmiştir.

Tebliğ Taslağı ile ilgili olarak bu çalışmayı ilgilendirmesi açısından en önemli düzenlemenin uzaktan kimlik tespitinde sorumluluğu düzenleyen 12. madde olduğu görülmüştür. İlgili düzenlemede, esas itibariyle uzaktan kimlik tespitinde kullanılan çözümlerin kişiyi yanlış tespit riskini asgariye indirgeyecek şekilde kullanılmasının sağlanmasının bankaların sorumluluğunda olduğu, kişilere ya da üçüncü bir tarafa yükümlülük doğuran işlemlerde itiraz halinde ispat yükümlülüğünün de bankalarda olduğu belirtilmiştir.

Son olarak, Tebliğ Taslağı metninde tebliğin 01.01.2021 tarihinde yürürlüğe gireceği düzenlenmiştir[775].

---

[772] *Tebliğ Taslağı,* m. 6/ f. 5.

[773] Bu husus, Tebliğ Taslağı'nın 7. maddesinde düzenlenmiştir. Görüntülü görüşme esnasında uzaktan kimlik tespiti sürecinde kullanılanabilecek kimlik belgeleri şunlardır: Beyaz ışık altında görsel olarak ayırt edilebilen ve asgari olarak giyoş, gökkuşağı baskı, optik değişken mürekkep, gizli görüntü, hologram ve mikro yazı güvenlik öğeleri, fotoğraf ve ıslak imza (Bkz. *Tebliğ Taslağı,* m. 7/f. 1).

[774] Tebliğ Taslağı'nın 8. maddesi gereğince, görüntülü görüşme ile uzaktan kimlik tespiti esnasında kişinin canlılığını tespit edici teknikler kullanılarak kişinin yüzü ile kimlik belgesinde yer alan fotoğrafın biyometrik karşılaştırması yapılacağına ilişkin detaylı düzenlemelere yer verilmiştir.

[775] Tebliğ Taslağı, m. 13.

ALTINCI BÖLÜM

ELEKTRONİK ÖDEMELERDE SİBER GÜVENLİĞİN SAĞLANMASINDA YENİ YAKLAŞIMLAR: YENİLİKLER, VAATLER VE POTANSİYEL RİSKLER

Bilindiği üzere, internetin hız kazandırdığı birçok sektör gibi siber güvenlik açısından en önemli korunması gereken sektörlerin başında elektronik finans sektörü gelmektedir[776]. Özellikle konu "Elektronik Ödemelerde Siber Güveliğin Sağlanmasında Yeni Yaklaşımlar" olduğunda ise, takdir edileceği üzere kapsam itibariyle geniş bir konu olduğu ve gelişen teknoloji ile her geçen gün yeni bir ödeme yöntemi keşfedildiği dikkate alındığında, yazar tarafından bu başlık altında özellikle elektronik ödeme sistemlerinde dünyada yoğun şekilde rağbet gören bazı yeni birtakım elektronik ödemeleri sistemlerin temini açısından bazı tespitlere aşağıda yer verilmiştir.

Bu bölüm altındaki analizler her ne kadar temel itibariyle konu ile ilgili yeni eğilimlerin incelenmesi olarak gözükse de yeni eğilimler açısından kapsam itibariyle:

(i) eskiden beri kullanılmasına rağmen yeni birtakım çözümlerin bulunması açısından (örneğin biyometrik verilerle siber güvenliğin temini eskiden beri uygulanan bir siber güvenlik çözümü olmasına rağmen biyometrik veriler ve davranışlar eğilimlerin karışımı olan hibrit bir çözüm siber güvenliğin temininde yeni ve daha etkin siber güvenlik önlemi olması nedeniyle bu hususta aşağıda gerekli analizlere yer verilmiştir),

(ii) gerçekten de teknolojik alanda bazı gelişmeler sonucunda bazı yeni eğilimlerin tercih edilmesi noktasında (örneğin yapay zeka teknolojisinin "living of the land"[777]

[776] *Yeşilyurt*, s. 99.
[777] "Living of the land" denilen zararlı yazılımlar ve bu yazılımlara karşı yapay zeka teknolojisi ile ne şekilde mücadele edildiği çalışmanın 6.4. başlığı altında detaylı şekilde analiz edilmiştir.

denilen karmaşık zararlı yazılımların tespitinde kullanılması siber güvenlik açısından doğru ve yenilikçi bir yaklaşım olarak değerlendirilmektedir)

incelenmiştir.

Elektronik ödeme sistemlerinde siber güvenliğin sağlanmasında yeni eğilimler aşağıda belirtilen beş kategori çerçevesinde irdelenecektir:

i) Kripto Paralarda Siber Güvenlik ve Blokzincirin Siber Güvenliğin Temininde Öngörülen Etkileri

ii) Biyometrik Yöntemlerle Ödemelerde Siber Güvenlik

iii) Açık Bankacılıkta Siber Güvenlik

iv) Yapay Zekanın Siber Güvenlik Alanında Bankacılık Sektörüne Etkileri

v) Covid-19 Pandemi Salgının Dijital Bankacılığa Etkileri Ve Konunun Siber Güvenlik Açısından Değerlendirilmesi

Görüldüğü üzere, yukarıda her başlık incelenen konu ile ilgili siber güvenlik alanında farklı fırsatlar sunduğu gibi aynı zamanda risk noktasında konuya bakış açısını da değiştirdiğinden, bu bölüm başlığı altında özellikle "Yenilikler, Vaatler Ve Potansiyel Riskler" olarak adlandırılmıştır. Bu konuda örneğin blokzincir teknolojisi "güven unsuru" sağlamak noktasında siber güvenlik açısından da etkin şekilde kullanabilecek bir teknoloji olmasına rağmen henüz devletler nezdinde yeterli regülasyonların olmaması ve bu teknolojiye yönelik oturmuş bir ekosistem olmaması siber güvenliğin temini açısından halen bazı eksikliklerin olduğunu göstermiştir.

Öte yandan, tüm dünyada ödeme sistemlerinin değişim geçirdiği göz önüne alındığında, Endüstri 4.0 aşamalarında olduğu gibi günümüzde paranın da değişim

aşamalarını belirtmek amacıyla ödeme sistemlerinde gelinen son aşama olarak görülen biyometrik yöntemlerle yapılan ödemeler açısından Para 4.0[778] kavramına vurgu yapıldığından bu başlık altında incelenmeye değer görülmüştür.

Açık bankacılığa Türkiye'de olduğu gibi AB de dahil olmak üzere artan bir ilgi olduğu görülmektedir. Bu alanda gerek AB'nin PSD2 düzenlemesi gerekse Türkiye'de yukarıda belirtilen "Elektronik Bankacılık Yönetmeliği" açısından önemli birtakım bazı kavramlara, tanımlara ve kurallara yer verildiğinden bu konu da aşağıda kapsamlı şekilde değerlendirilecektir.

Yapay zeka teknolojsi ise, günümüzde bilindiği üzere üzerinde çok tartışılan bir mecra olmakla beraber özellikle zararlı yazılımlar ve DDoS gibi siber uzayda artan riskler dikkate alındığında yapay zekanın hangi açılardan siber güvenliğin temin edilmesinde yararlanılacağı incelemeye değer görülmüştür.

Covid-19 pandemi salgını ise aşağıda detaylı şekilde analiz edileceği üzere, gerek elektronik ödemelerin tercih edilmesini adeta zorunluluk haline getirmekle beraber siber korsanların bu ortamda elde etmek istedikleri menfaat açısından iştahlarını kabartmış ve siber güvenliğin teminini başka bir aşamaya taşımıştır. İşte tüm dünyada ve Türkiye'de pandemi koşullarının getirdiği bu zorunluluk ve siber korsanlarla mücadele yöntemlerinin neler olması gerektiği de bu çalışmada cevabı aranan sorular arasındadır.

[778] PayPal'un başkanı David Marcus, nakit para dönemini Para 1.0, kredi kartı dönemini Para 2.0, şimdilerde hayatımızda varlığını hissettirmeye başlayan mobil ödeme dönemini Para 3.0 ve gelecekte yaygın şekilde kullanılacağı düşünülen biyometrik sistemler üzerinden yapılacak ödemeleri Para 4.0 olarak nitelendirmektedir. http://fintechtime.com/tr/2017/04/gelecegin-odeme-sistemleri/ (Gözden Geçirilme Tarihi: 21.02.2020)

6.1. KRİPTO PARALARDA SİBER GÜVENLİK VE BLOKZİNCİRİN SİBER GÜVENLİĞİN SAĞLANMASINDAKİ İŞLEVİ

Kripto[779] para kavramı, kriptografi[780] ve para kelimelerinin bir araya gelmesi sonucu oluşan bir söz dizini[781] olup tüm kripto paraların ortak özelliğinin karmaşık bir matematiksel şifrelemeye dayandığı belirtilmektedir[782]. Diğer bir ifade ile, aslında kripto paralar, blokzincir tabanlı sistemlerde ağa bağlı kişiler arasında serbest şekilde transfer edilmesi mümkün olan, şifrelenmiş ve herhangi bir merkezi otorite tarafından regüle edilmeyen para değerini - söz konusu para değeri, fiziksel bir para olmayıp kod satırlarına dönüştürülmüş elektronik sinyallerdir - ifade etmektedir[783]. Günümüzde en popüler kripto paralar olarak Bitcoin, Ethereum, Litecoin, Ripple, Tether, Bitcoin Cash, Libra, EOS, Bitcoin SV, Binance Coin, Monero akla gelmektedir[784].

Literatür açısından konuya bakıldığında, Fatás/Mauro kripto paraların günümüzde en göze çarpan avantajının, blokzincir teknolojisinin[785] geleneksel ödeme sistemlerine kıyasla herhangi bir merkezi otoriteye bağlı olmaksızın işlem yapılmasını sağlayan bir yenilik olduğunu belirtilmiştir[786]. Ancak, kripto paraların tabi olduğu blokzincir teknolojisinin siber güvenlik riskleri noktasında, ABD'de tanınmış bir siber güvenlik

---

[779] Kripto (crypto) gizli, saklı anlamına gelmektedir. Bkz. https://dictionary.reference.com/browse/crypto- (Gözden Geçirilme Tarihi: 25.04.2020)

[780] Kriptografi ise gizli yazım yöntemleri, kodları ve teknikleri ile ilgilenen bilimdir. Bkz. http://dictionary.reference.com/browse/cyrptography?s=t (Gözden Geçirilme Tarihi: 29.10.2020)

[781] Kripto paranın tanımı konusunda Bkz. https://en.wikipedia.org/wiki/Cryptocurrency (Gözden Geçirilme Tarihi: 29.10.2020).

[782] *Çetinkaya,* s. 13.

[783] *Özkaya/Sarıca/Durmaz*, s. 56.

[784] https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/ (Gözden Geçirilme Tarihi: 29.10.2020).

[785] Günümüzde Blokzincir teknolojisi, merkeziyetçi olmayan, herkese açık ve herkes tarafından erişebilir yapısı ile ülkeler tarafından değerlendirmeye ve düzenlemeye açık bir teknoloji olarak karşımıza çıkmaktadır. Bkz. Blockchain Türkiye, Hukuk, Düzenlemeler ve Kamu İlişkileri Çalışma Grubu, "Dünyada Blokzinciri Regülasyonları ve Uygulama Örnekleri, Karşılaştırma Raporu, Şubat 2019, s. 10: https://bctr.org/wp-content/uploads/2019/04/Dünyada-Blokzinciri-Regulasyonları.pdf (Son Erişim Tarihi: 29.10.2020)

[786] Antonio Fatás/Beatrice Weder di Mauro, "Kripto Paralar Yükselişe Geçmişken Kimin Bankalara İhtiyacı Olur ki?" adlı makale, Harvard Business Review, Dijital Dönüşüm Blok Zinciri, (*"Fatás/di Mauro"*), s. 118.

uzmanı olan Bruce Schneier blokzincir teknolojisinin "güven unsuru" açısından birtakım sorunlar içerdiğini, güvenin yerini başka hiçbir şeyle değiştirilmeyecek türden bir mesele olduğunu belirtmiştir. Schneier bitcoin para biriminin, bitcoin cüzdanın hacklenmesi halinde veya blokzincir teknolojisinin bir ürünü olan akıllı sözleşmelerdeki bir kod içeriğinde, herhangi bir zafiyet (bug) olması halinde kullanıcıların tüm paralarını kaybedebileceğini ve sonuç itibariyle bilgisayar kodlarına güvenmenin insanlar için halen hukuk sistemlerine güvenmekten daha zor bir mesele olduğuna özellikle dikkat çekmiştir[787]. Doktrinde, Keser Berber blokzincir teknolojisindeki son gelişmeler dikkate alındığında, blokzincir teknolojisinin güven işlevini sağlamakla beraber ancak bu konuda halen bazı sorunlar olduğunu belirtmiştir[788]. BKM, Tübitak ve BİLGEM tarafından yayınlanan "Blokzincirlerde Güvenlik Ve Mahremiyet" başlıklı rapor içeriğinde ise, blokzincir teknolojisinin internetteki mahremiyet ve güvenlik açısından tek başına çözüm olarak görülmemesi gerektiği, blokzincir platformlarının mahremiyet ve güvenlik seviyelerinin, basit takma isimlerden tam gizliliğe kadar çeşitlilik gösterdiği belirtilmiştir. İlgili rapora göre, genel itibariyle bu konuda çoklu teknolojilerin kombinasyonunun tek bir teknolojiye kıyasla güvenlik ve mahremiyet açısından daha etkili çalıştığının gözlemlendiği, ancak karmaşık bir sisteme yeni bir teknoloji eklemenin başka sorunlara sebebiyet

[787] Bruce Schneier, "There's No Good Reason to Trust Blockchain Technology", Wired, (*"Schneier"*) 02.06.2019: https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/ (Gözden Geçirilme Tarihi: 29.10.2020).

[788] Keser Berber özellikle blokzincir teknolojisindeki son gelişmeler ışığında, blokzincir teknolojilerinin, merkezi olmayan ve güvensiz ortamlarda anonim ve güvenilir işlem yapılmasını sağlayabileceğini, başka bir ifadeyle blokzincirin özellikle güven yönetimi, sistem risklerinin azaltılması, finansal sahtekârlığın azaltılması ve bilgisayar sistemlerindeki işletim maliyetinin azaltılmasına yardımcı olabileceğini belirtmiştir. Bu avantajlarına rağmen, Keser Berber'e göre blokzincirin dijital dönüşüm gereksinimi, enerji tüketimi, sınırlı teşvik, yazılım hataları, açıklar ve siber ataklar, çatallaşma (fork) gibi uygulamada hukuksal, teknik ve sistemsel açıdan çözülmesi gereken sorunları barındırdığına dikkat çekilmiştir. Özellikle blokzincire yazılan kayıtların değişmezliği ve silinmezliği çocuk pornografisi ve kara para aklama gibi global suçlar ve yeni zincirlere yazılan hukuka aykırı içeriklerin silinemezliği nedeniyle mücadelenin güçleşmesi blokzincirin yarattığı en önemli sorunlar olarak değerlendirilmiştir. Bu konuda detaylı bilgi için Bkz. *Keser Berber, Güven Hizmetleri,* s. 230-231.

verebileceğinden, bazı güvenlik ve mahremiyet tekniklerinin blokzincirlere entegre edilmesiyle ortaya çıkabilecek riskli durumlara dikkat edilmesi gereklidir.[789].

Kripto paralardan özellikle Bitcoin ve Ethereum konusunda geçmişte yaşanan bazı siber saldırı örnekleri şunlardır:

2011 yılında internet korsanları tarafından Bitcoin'e yönelik gerçekleştirilen siber saldırıda, Bitcoin'in kur değeri ile oynanması sonucunda kur değeri 17.50 Amerikan Dolarından 0.01 Amerikan Doları'na indirilmiştir. Söz konusu saldırıda, korsanların Tokyo merkezli Bitcoin değişim/bozdurma (exchange) şirketi olan Mt. Gox isimli veritabanına/platformuna girerek kullanıcıların adları, adresleri, soyadları, şifrelerine de ulaştıkları bilinmektedir. Vahim bu tablo karşısında Mt. Gox veritabanı birkaç gün kullanıma kapatılmıştır. Akabinde ise, Mt. Gox isimli şirket 2014 yılı Şubat ayında iflas ettiğini ilan ederek müşterilere ve şirkete ait sekiz yüz elli bin adet Bitcoin'in internet korsanlarının gerçekleştirdiği siber saldırı sonucunda bulunamadığını belirtmiştir[790].

Ethereum, Bitcoin'den farklı olarak Ethereum'un çalışma mantığı, başlangıçta akıllı sözleşme[791] aracılığıyla jeton üretip bunu "Ether" denilen blokzinciri jetonuyla

[789] BKM/Tübitak BİLGEM, "Blokzincirlerde Güvenlik Ve Mahremiyet" başlıklı Rapor, Nisan 2020, (*"BKM, Blokzincirlerde Güvenlik"*) ilgili rapora ulaşmak için Bkz. https://bkm.com.tr/wp-content/uploads/2015/06/blokzincirlerde_guvenlik_ve_mahremiyet.pdf (Gözden Geçirilme Tarihi: 27.04.2020). Doktrinde, blokzincirde işlem güvenliği bakımından bir başka eleştiri ise Çiçek/Sağlık tarafından getirilmiştir. İlgili yazarlar, blokzincirdeki kayıtların tahrif edilme olasılığının bulunduğunu, sistemin devamlılığının kim tarafından sağlanacağın bilinmediği, düğümler arasındaki blok farklılıklarında hangi bloğun delil olarak kabul edileceğinin de öngörülemediği yanlışlıkla bir varlığı temsil eden jetonun ya da kripto paranın el değiştirmesi ihtimalinin olduğunu, özel anahtarların kaybı olasılığının da bulunduğunu belirtmiştir. Konu ile ilgili ayrıntılı bilgi için bkz. Niyazi Çiçek/Özhan Sağlık, T.C. Ankara Üniversitesi, BİL-GEM, Bilgi Yönetimi Ve Bilgi Güvenliği, e-Belge-eDevlet-eArşiv-Bulut Bilişim-Büyük Veri-Yapay Zeka, Ankara, 2019, (*"Çiçek/Sağlık"*), s. 141-170, s. İlgili makaleye ulaşmak için: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Desktop/Endustri-4.0-Surecinde-Bilgi-Yonetimi-ve.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[790] *Bozkurt Yüksel*, *Elektronik Para,* s. 74

[791] Akıllı sözleşme, merkezi olmayan bir mutabakat neticesinde tarafların sözleşmeye uygulanacak koşulları belirlediği, kendiliğinden uygulanabilir nitelikte olan ve otomatik hale getirilen sözleşmenin taraflarca ifasına yönelik uygulamanın bir zaman damgası ile mühürlendiği dijital nitelikli sözleşmeler

değiştirmesi esasına dayanmaktadır. Ethereum'daki jeton satışının başlangıçta, yoğun bir pazarlama ile toplamda 150 milyon dolar değerinde Ether toplanmasını sağlayan bir kitle fonlama kampanyası (ICO)[792] ile gerçekleştirildiği bilinmektedir. Ethereum'un yaratıcıları başlangıçta vizyon olarak "kod kanundur"[793] felsefesinden hareketle, bilgisayar kodlarına kanun muamelesi yapılması gerektiği felsefesini benimseyerek katılımcılarına her konuda tasarruf hakkının yazılımın kodunda olduğunu duyurmuştur. Ne var ki, dağıtık veri tabanı teknolojisinin başlangıçta Ethereum açısından akıllı sözleşmeler için öngördüğü kod bazı açıklar içermekteydi. Bu açıklardan yararlanan Ethereum içerisindeki bir Ethereum sahibi ise uygulama değerinin yaklaşık üçte birini (yaklaşık 50 milyon dolar) kendi hesabına aktardı. Bu şaşırtıcı durum diğer tüm Ethereum kullanıcıları açısından başlangıçta beklenmedik bir durum olarak değerlendirilse dahi, yukarıda da ifade edilen "kod kanundur" felsefesi açısından bakıldığında bu teknolojinin yaratıcıları açısından aslında kural ihlali anlamına gelmiyordu. Bu durum ise aslında Ethereum topluluğu açısından "Zorunlu Çatallaşma" *(Hard Fork)* denilen Ethereum kullanıcılarının ikiye bölünmesine neden

olarak tanımlanabilir. Bu tanım L. Cong, L. ve Z. He (2018), "Blockchain Disruption and Smart Contracts" (s.8) isimli makalesinden aktarılmıştır ("*Cong/He*"). Söz konusu makalenin tam metnine aşağıdaki web sitesinden erişilebilir: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2985764 (Gözden Geçirilme Tarihi: 29.10.2020).

[792] "ICO", İngilizce'de "Initial Coin Offerings" kısaltması olup yatırımcılara başka bir kripto para edinimi konusunda bir şirketin sermaye veya yatırım sağlamak amacıyla bitcoin gibi kripto paraların geniş kitlelere satılması imkanı veren ve bu satışın hukuken geçerli şekilde ihale usulü ile piyasaya tedavül edildiği kavramı ifade etmektedir. Detaylı bilgi için Bkz. Usman W. Chohan, "Initial Coin Offerings (ICOs): Risks, Regulation, and Accountability", 30 Kasım 2017, University of New South Wales, (*"Chohan"*), s.1: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/SSRN-id3080098.pdf (Gözden Geçirilme Tarihi: 13.05.2020). yatırım almak isteyen bir startupın kendi tasarladığı, sınırlı sayıda kripto paranın kitlelere satılması ve startupın kaynak elde etmesi yöntemlerinden biri olarak ifade edilebilir. ICO'ların hukuki altyapısı konusunda ayrıntılı bilgi için ayrıca Bkz. Iris M. Barsan, "Legal Challenges of Initial Coin Offerings (ICO)" (*"Barsan"*): file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/SSRN-id3064397.pdf (Gözden Geçirilme Tarihi: 13.05.2020). Tez içeriğinde, yazar tarafından dijital para arzı olarak tercüme edilmiş olsa bilimsel literatürde ICO teriminin kullanıldığı dikkate alarak ICO kısaltması ile kullanılmıştır.

[793] Bu konuda ayrıntılı bilgi için Bkz. Lawrence Lessing, "The Code in Law, and the Law in Code" (*"Lessig"*) isimli makalesi incelemeye değerdir. İnternet ortamında söz konusu makaleye ulaşmak için Bkz. https://web.stanford.edu/class/msande91si/www-spr04/readings/week3/Lessig-pcforum.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

oldu[794]. Ethereum topluluğunda aralarında bir grup saygın yöneticinin de yer aldığı çok sayıda üyesi Ether jetonlarının kaybını talep etti. Ethereum yönetimi ise blokzincirinde gerçekleştirilen kalıcı bölünme ile çalınan paralar sistem üzerinden bir grup güvenilir üyeye aktarıldı. Söz konusu mecburi çatallaşma ile yaratılan yeni Ethereum blokzinciri "Ethereum" olarak anıldı ve bu kişiler açısından zararları bazı eleştirmenler açısından bu operasyon aslında Ethereum blokzincirini kurtarma operasyonu idi. Diğer topluluk üyelerince ise, söz konusu bu mecburi çatallaşma Ethereum'a ait temel ilkelerin ihlali anlamına geliyordu. Dolayısıyla yaşanan bu olay neticesinde aslında Ether jetonlarını kaybederek zararı giderilmeyen ve paralarını geri alma şansı olmayan ve Ethereum blokzincirini eski haliyle kullanmaya devam eden grup açısından "Ethereum Klasik" olarak anıldı[795].

Siber saldırı konusunda Ethereum açısından verilebilecek diğer örnek ise, www.wired.com sitesinde yayınlanan ilgili haber içeriğinde, Ethereum Classics platformu üzerinde sisteme birden fazla saldırı yapıldığı, gerçekleştirilen % 51 saldırısı[796] sonucunda network üzerindeki makinelerin en az yüzde elli bir üzerinde kontrolün ele geçirildiği, toplamda on iki kez Ethereum Classics'e ilişkin jetonlar (*tokens*)[797] üzerinde çifte harcama yapılması[798] sonucunda 1.1 milyar Dolar haksız kazanç sağlandığı belirtilmiştir[799].

---

[794] https://fintechistanbul.org/2016/10/15/ethereuma-yine-mecburi-catallasma-geliyor/ (Gözden Geçirilme Tarihi: 29.10.2020).

[795] Ethereum'da yaşanan "zorunlu çatallaşma", "Ethereum" ve "Ethereum Klasik" ağları konusunda ayrıntılı bilgi için Bkz. Patrick Murck, "Blokzincirini Kim Kontrol Ediyor?", Harvard Business Review Press, Dijital Dönüşüm, Blok Zinciri, Optimist, Ocak 2020, s. 74-77.

[796] % 51 saldırısı ile ilgili ayrıntılı bilgiye çalışmanın 2.7. numaralı "Kripto Madenciliği Saldırıları Ve Kripto Paralara Yönelik Saldırılar" başlığı altında yer verilmiştir.

[797] "Token", dijital bir jeton olup kripto paralarda bir platform veya uygulamaya yönelik oluşturulan ve söz konusu o platformdan veya uygulamadan yararlanmayı sağlayan bir dijital varlık olarak kabul edilmektedir. Token hakkında detaylı bilgi için Bkz. https://kriptokoin.com/bitcoinde-6-100-10-500-dolar-ve-daha-fazlasini-bilen-analist-uyardi/ (Gözden Geçirilme Tarihi: 29.10.2020).

[798] "Çifte harcama" blokzincir teknolojisinde kripto paralara yönelik gerçekleştirilen bir siber saldırı türü olup tezin 4.2.5 başlığı altında "Kripto Madenciliği (Cryptojacking) Ve Kripto Paralara Yönelik Saldırılar başlığı altında bu konuda ayrıntılı değerlendirmeye yer verilmiştir.

[799] 08.01.2019 tarihinde yayınlanan ilgili haber konusunda Bkz. https://www.wired.com/story/attack-on-ethereum-currency-highlights-crypto-weakness/ (Erişim Tarihi: 29.10.2020)

Bu başlık altında ayrıca kripto paralardaki siber güvenlik kavramından farklı olarak ayrıca blokzincir teknolojisinin siber güvenliğin temini noktasında ne şekilde kullanıldığına da kısaca değinilecektir. Harvey/Moorman/Toledo blokzincir teknolojisinin özellikle botlar aracılığıyla DoS saldırılarını, sosyal medya hesabı açılması, kullanıcıya aldatıcı mesajlar gönderilmesi, büyük markalardan online reklam paralarının çalınması ve spam denilen istenmeyen e-posta gönderilmesine son verme konusunda etkin bir araç olarak kullanılabileceğini ifade etmektedir. Yazarlara göre, botlar aracılığıyla bir web sitesine milyonlarca istek göndererek sitenin çökmesine veya yavaşlamasına sebep olan DoS ve DDoS saldırılarına karşı ilgili istek sahiplerinden blokzincir teknolojisinin verdiği imkânlar ile mikro ödeme yapılmasının talep edilmesi DDoS ve DDoS gibi internet ortamında istenmeyen aktiviteleri önlemede inovatif bir yöntem olarak kullanılabilecektir[800].

Sonuç itibariyle, blokzincir teknolojisinin zararlı yazılımlar, DDoS saldırıları ve sahte sosyal medya hesaplarına karş mikro ödemeler vasıtasıyla siber güvenliğin temini açısından inovatif birtakım çözümler sunmakla beraber henüz bu konuda teknolojinin oturmamış olması ve siber güvenlik açısından halen bu teknolojiye yönelik bazı yeniliklere ihtiyaç duyulması sebebiyle yüzde yüz güven vermediği değerlendirilmiştir.

6.2. BİYOMETRİK YÖNTEMLERLE ÖDEMELERDE SİBER GÜVENLİK

Biyometri, bireylerin gerçekleştireceği işlemler açısından özgün biyolojik özelliklerinden yararlanmak ve bireyleri birbirinden ayırt etmek suretiyle kimlik doğrulama ve onaylama faaliyetini ifade etmekte[801] olup biyometrik yöntemlerle

[800] Campbell R. Harvey/Christine Moorman/Marc Toledo, "Blok Zinciri Pazarlamacıların Müşterileriyle Daha İyi İlişkiler Kurmasına Nasıl Yardımcı Olur?", Harvard Business Review Press, Blok Zinciri, Dijital Dönüşüm, Optimist, (*"Harvey/Moorman/Toledo"*), 150-152.

[801] Süleyman Çınar, "Mobil Android Ortamında Parmak İzi Tanıma Ve Kimlik Doğrulama Sisteminin Geliştirilmesi", Haliç Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı Bilgisayar Mühendisliği Programı, Yüksek Lisans Tezi, İstanbul, 2014, (*"Çınar"*) s. 5, http://earsiv.halic.edu.tr/xmlui/bitstream/handle/20.500.12473/1318/357287.pdf?sequence=1&isAllowed=y (Gözden Geçirilme Tarihi: 29.10.2020). Leyla Keser Berber ve Murat Lostar tarafından kaleme alınan "Bilişimde Biyometrik Veriler" adlı eserde ise, yunanca kökenli bir kavram olan biyometrinin,

ödeme ise anılan yöntem ile gerçekleştirilen ödeme faaliyetini ifade etmektedir. Biyometrik teknolojilerin günümüzde dolandırıcılık risklerine karşı tüketicileri korumaya yönelik daha doğru ve ucuz bir ödeme kolaylığı sağlamak üzere tasarlandığı, böylelikle nihai tüketici açısından kullanım kolaylığı sağladığı izlenimi revaçtadır[802].

Biyometik yöntemlerin temel özellikleri şunlardır[803]: Kullanılan biyometrik özelliklerin sayısı, parolalardan farklı olarak sınırlıdır. Biyometrik özellikler sır olmayıp birçoğunun gizlenmesi mümkün değildir. Biyometrik yöntemler bilgi teknolojileri sistemlerinde olası tüm manipülasyon ve kopyalama teşebbüslerini engellemeye yarayan veri dizileridir.

Özellikle konuya güvenlik hassasiyeti açısından yaklaşıldığında ise, ödemelerde güvenlik açısından üç katmanın bulunduğu akla gelmektedir:

i) *"Taşıdığımız"* şeklinde ifade edilen güvenlik kategorisinde kartlı ödeme sistemleri akla gelmekte olup söz konusu kartların her an çalınma ve kaybolma tehlikesi bulunmaktadır.

ii) *"Bildiğimiz"* ve ele geçirilmesi daha zor olan seviye olan ikinci kategoride şifre ve dijital imzaların bu kapsamda değerlendirilebilecektir. Ancak şifreleme ve dijital imzalar açısından her zaman unutulma riski gündeme gelmektedir.

iii) Biyometrik verilerin ise üçüncü seviye olan *"olduğumuz"* kategorisinde ise bizi biz yapan yüz, ses, parmak izi ve retina taraması gibi verilerle ilgili olduğu ve en yüksek güvenlik hassasiyetine sahip seviye olduğu ifade edilmiştir[804].

---

canlı bir varlığın biyolojik istatistiği, sayımı ve ölçümünü ifade ettiği belirtilmiştir. Bu konuda ayrıntılı bilgi için bkz. *Keser Berber/Lostar*, s. 20.

802 https://www.accenture.com/t20180911t022838z__w__/us-en/_acnmedia/pdf-94/accenture-br-biometrics-payments.pdf (Gözden Geçirilme Tarihi: 29.10.2020)

803 *Keser Berber/Lostar*, s. 22.

804 http://fintechtime.com/tr/2017/04/gelecegin-odeme-sistemleri/ (Gözden Geçirilme Tarihi: 29.10.2020)

Forcepoint tarafından 2019 yılında yayınlanan Siber Güvenlik Öngörü Raporu[805]'nda ise yüz tanıma gibi biyometrik teknolojilerle doğrulama yöntemlerinin yaygınlaşmasının siber suçluları bu teknolojideki açıkları bulmaya yönlendirdiğini, özellikle bu konuda sosyal medyanın siber suçlulara geniş bir kaynak ve imkân sunduğu ve tüm bu gelişmeler dikkate alındığında salt biyometrik yöntemlerle yapılan kimlik doğrulamanın %100 güven sağlamadığına dikkat çekilmiştir. İlgili raporda biyometrik yöntemlerle kimlik doğrulama işlemlerinin tuşa basma sertliği, fare hareketi, kaydırma hızı gibi fiziksel hareketleri destekleyen ilave bir doğrulama katmanı ile desteklenmesinin siber güvenliğin temini açısından önem taşıdığı üzerinde özellikle durulmuştur[806]. Benzer şekilde doktrinde de biyometrik yöntemlerle kimlik doğrulama ve bu noktada siber güvenliğin temini açısından günümüzdeki teknolojik gelişmeler doğrultusunda yeni eğilimlerin takip edilmesi gerektiği belirtilmiştir[807].

Son olarak, Keser Berber/Lostar biyometrik yöntemlerin avantajlarının kişiye bağlı olan fizyolojik veya davranış bakımından tipik karakteristikleri kapsaması nedeniyle şifre veya parola sisteminden farklı olarak başkasına verilemeyeceği, insana özgü olması sebebiyle eşsiz oldukları, sahteciliklere karşı güvenilirliklerinin yüksek olduğu, geçerlilik sürelerinin de yüksek olduğu ve biyometrik veri elde etme maliyetinin her bir biyometrik yönteme göre değişebilmekle beraber genelde düşük olduğunu

[805] İlgili raporun tam metnine ulaşmak için Bkz. https://www.forcepoint.com/resources/pack/2019-forcepoint-cybersecurity-predictions-assets?form_id=1363&file=35751&resource=27281&category=reports (Gözden Geçirilme Tarihi: 29.10.2020)

[806] Bu konuda ilgili haber konusunda Bkz. https://www.haberturk.com/forcepoint-uyardi-biyometrik-guvenlik-tek-basina-yeterli-degil-2428240-teknoloji (Gözden Geçirilme Tarihi: 27.02.2020). Yukarıda yer alan açıklamalar biyometrik kimlik doğrulama açısından yeni bir eğilim olarak "davranışsal biyometri" çerçevesinde değerlendirilmektedir.

[807] Doktrinde biyometrik yöntemlerle bilgi güvenliğinin sağlanması ve siber atakların önlenmesi noktasında Şeref Sağıroğlu tarafından "Siber Güvenlik Ve Savunma Standartlar Ve Uygulamalar" adlı eserinde özellikle biyometrik sistemlerde meydana gelen güvenlik açıkları ve oluşan tehditler nedeniyle bu açıklara karşı davranışsal biyometri, sosyometrik biyometri, kuantum biyometrisi gibi yeni dirençli sistemler geliştirmek gerektiğini ileri sürmektedirler. Bu konuda ayrıntılı bilgi için Bkz. *Sağıroğlu,* s. 370-380.

belirtmiştir[808]. Buna karşın, ilgili yazarlar tarafından biyometrik yöntemlerin dezavantajları olarak biyometrik yöntemlerin kullanımını sağlayacak aygıtların tesis edilmesi için ortaya çıkan maliyetlerin nispeten yüksek olduğu, aygıta dokunmayı gereken sistemlerin sağlığa uygunluğu açısından çekincelerin ileri sürüldüğü ve bu sistemi kullanmakta çekimser olan kişilerin çoğu kez kişisel verilerin ve kişilik haklarının korunması gerekçelerini ileri sürdüğü belirtilmiştir[809].

Biyometrik yöntemlerle siber güvenliğin temini açısından varılan sonuç, bu alanda yukarıda belirtilen bazı karma çözümlerin siber güvenliğin temini açısından yarar sağlamakla beraber biyometrik verilerin kaydı noktasında veri koruma hukuku ve kişisel hakların korunması gibi hukukun diğer alanları konusunda hassas davranılması gerektiğidir.

6.3. AÇIK BANKACILIKTA SİBER GÜVENLİK

Günümüzde özellikle Covid-19 pandemisinin yarattığı koşulların bankacılık sektörünün dijital açıdan dönüşümünü hızlandıracağı ve yakın gelecekte bu dönüşümün bir parçası olarak gerek dünyada gerekse Türkiye'de "açık bankacılık" gibi yeni finansal teknolojilerin daha çok benimsenmesini sağlayacaktır.

Açık bankacılık (*open banking*) konusunda literatürde birçok farklı tanımı yer alsa da[810], yazar GSG Hukuk Raporu'nda yer alan ve açık bankacılık kavramını üçüncü kişi hizmet sağlayıcıların kullanıcıların finansal bilgilerini Uygulama Programlama

[808] *Keser Berber/Lostar*, s. 21.
[809] *Keser Berber/Lostar*, s. 21-22.
[810] Açık bankacılık konusunda ayrıntılı bilgi için Bkz. Euro Banking Association, "Open Banking: advancing customer-centricity, Analysis and overview", Mart, 2017, (*"EBA"*), https://www.abe-eba.eu/media/azure/production/1355/eba_open_banking_advancing_customer-centricity_march_2017.pdf (Gözden Geçirilme Tarihi: 29.10.2020), McKinsey&Company, "Data Sharing and open banking (*"McKinsey"*), Eylül, 2017, https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking#, BCBS, "Report on open banking and application programming interfaces", (*"BCPS"*), 2019: https://www.bis.org/bcbs/publ/d486.pdf (Gözden Geçirilme Tarihi: 29.10.2020)

Arayüzü (*"API"*)[811]'ler vasıtasıyla rızası alınarak bankacılık hizmeti sunulmasına yönelik yeni bir finansal teknolojinin ürünü olan bankacılık hizmeti şeklinde tanımlanmasının bu kavramı açıklamaya en uygun tanım olduğunu değerlendirmektedir[812].

Yukarıda da açıklandığı üzere, mevzuat açısından açık bankacılık kurumunun temelleri AB'de ilk kez PSD2 ile atılmış olup söz konusu Diretif'te açık bankacılığın net bir tanımı yapılmamakla beraber bankalar tarafından üçüncü kişi hizmet sağlayıcılara sağlanacak veriler açısından bu amacın gerçekleştirebilmesi açısından yukarıda açıklanan API denilen arayüzler kullanılması gerektiği de belirtilmiştir[813].

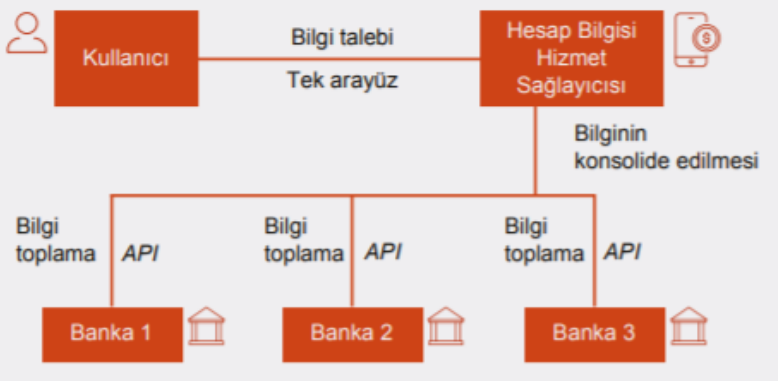
---

[811] İngilizce'de "Application Programming Interface" olarak belirtilmiştir.

[812] Bu tanım PwC (GSG Hukuk), "Açık Bankacılık: Dünya ve Türkiye" başlıklı rapordan (*"GSG Hukuk Raporu"*) aktarılmıştır. İlgili rapora internet ortamından ulaşmak için Bkz. https://www.pwc.com.tr/tr/sektorler/bankacilik/pdf/acik-bankacilik-dunya-ve-turkiye-v2.pdf. Ayrıca, açık bankacılığın diğer tanımları ve konu ile ilgili detaylı bilgi için bkz. MIT Technology Review, Insights/Research, "Open banking: The race to deliver banking as a service": https://www.oracle.com/a/ocom/docs/dc/open-banking-final.pdf, Hao Wang, "Nudging Data Privacy Management of Open Banking Based on Blockchain" (*"Hao Wang"*): file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/blockchain-ispan-camer.pdf, Laura Brodsky/Liz Oakes, "Open banking and data sharing" McKinsey&Company (*"Broadsky/Oakes"*): https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking (Gözden Geçirilme Tarihi: 29.10.2020).

[813] PSD2 hükümleri incelendiğinde açık bankacılık diye bir kuruma metin içerisinde açıkça yer verilmemiş olup PSD2'nin başlangıç düzenlemelerinden olan 28. paragrafta bilgi sistemlerine ilişkin yakın zamanda yaşanan teknolojik gelişmelerin bankacılık alanında özellikle bilgi sistemlerinde bazı tamamlayıcı hizmetleri gerektirdiği ve bu noktada hizmet kullanıcısının, üçüncü kişi hizmet sağlayıcıya yönelik online sistemler üzerinden bilgi paylaşırken bir ya da daha fazla hesabın söz konusu hizmet sağlayıcı tarafından hesaba/hesaplara yönelik online arayüzler a.gvasıtasıyla sağlanacağı belirtilmiştir. PSD2'nin 93. maddesinde ise PSD2 çerçevesinde sağlanacak ödeme hizmetleri açısından ödeme hizmetinin ne şekilde temin edileceğine yönelik açık bir çerçevenin belirlenmesi gerektiği ve bu hizmeti gerçekleştirecek hizmet sağlayıcının hesap sahibinden belirli bir iş modeli çerçevesinde gerçekleştirilecek hizmetler konusunda müşteriden alacağı bilgilerle ilgili kullanıcının mutlaka rızasını alması gerektiği hükme bağlanmıştır. PSD2 orijinal metne ulaşmak için Bkz. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN (Gözden Geçirilme Tarihi: 29.10.2020). API standartları dışında konularda PSD2 yönetmeliğine uyumun, üye ülkelerin Ulusal Yetkili Otoritesi (National Competent Authority – NCA) kurumları tarafından European Banking Association'ın yayınlamış olduğu toplam 14 adet Teknik Standart Düzenlemeleri (Regulatory Technical Standars–RTS), Rehber (Guideline-GL) ve Görüş Bildirgelerinin (Opinion Paper) özellikle teknik süreçlerin anlaşılabilmesi açısından önemli belgeler olduğuna dikkat çekilmiştir. Bkz. Fintech İstanbul, "Dünyada Ve Türkiye'de Açık Bankacılık: Bankacılığın Geleceği", Ekim 2019, s. 19: https://bkm.com.tr/wp-content/uploads/2015/06/Dunyadaveturkiyedeacikbankacilik.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

Çalışma ile doğrudan ilintili olması itibariyle açık bankacılığın ne olduğunun ve açık bankacılıkta siber güvenliğin nasıl sağlanacağının anlaşılabilmesi için öncelikle API'nin ne olduğunun bilinmesi gereklidir. API, kısaca bir yazılım olup bir finansal kuruluşun internet sitesinde bir uygulamanın üçüncü kişi hizmet sağlayıcı tarafından kullanılabilmesini sağlayan bir teknolojik uygulama olduğu belirtilebilir[814]. Açık bankacılıkta API'ler en bilinen yönüyle kullanıcıların hesap bilgisi hizmeti ve ödeme başlatma bilgisi açısından kullanılmakta olup aşağıda şematize edilen Şekil-6.1'de "Hesap Bilgisi Hizmeti", Şekil-6.2'de ise "Ödeme Başlatma Hizmeti" gösterilmektedir[815].



Şekil-6.1: API - Hesap Bilgisi Hizmeti

[814] *Brodsky/Oakes,* s. 1.
[815] Şekil 6.1 ve Şekil 6.2 GSG Hukuk Raporu s. 4-5'den aktarılmıştır.

Şekil-6.2: API - Ödeme Başlatma Hizmeti

Öte yandan, Bankacılık Denetimine İlişkin Basel Komitesi'nin ("Basel Committee on Banking Supervision) "Açık bankacılık ve Uygulama Programlama Arayüzü" isimli Raporu'nda açık bankacılıktaki API uygulamaları açısından özellikle kazıma (*scraping*)[816] ve tersine sosyal mühendislik (*reverse social engineering*)[817] gibi tekniklerin hâlihazırda üçüncü kişi servis sağlayıcıya müşteri hesabına girebilmesi açısından yetki vermesi ve bankaların sahte işlemleri ayırt etmesinin güçleşmesi nedeniyle bilgi güvenliği açısından bazı problemlere yol açabileceği belirtilmektedir[818].

6.4. YAPAY ZEKANIN SİBER GÜVENLİK ALANINDA BANKACILIK SEKTÖRÜNE OLASI ETKİLERİ

Yapay zeka güdümlü siber saldırıların artmasının, ağlara sızma ve kişisel veri hırsızlığı gibi meselelerde hızla artışa sebep olduğu ve akıllı bilgisayar virüslerinin salgın gibi yayılmasına sebep olduğu günümüzde bilinen bir gerçektir. Bu olgu karşısında literatürde kaynak araştırması yapıldığında, yapay zeka hackerliği üzerinde yeterince durulmadığı ve bu konuda yeterli kaynağın bulunmadığını gözlenmiştir. Oysaki, literatürde Yampolskiy[819] tarafından yapay zekanın siber güvenliğin geleceği olduğu

[816] Doktrinde Determann'a göre, kazıma (*scraping*) teknolojisi, şirketlerin arama motoru teknolojilerini desteklemek için internet sitelerini endekslemek ve büyük veri incelemesi için veri toplama gibi işletme amaçlarıyla internet sitelerinden otomatik olarak veri toplama yöntemidir. İlgili yazar, kazıma gibi veri toplama yöntemlerinin gizlilik kanunlarının (toplanan veriler arasında kişiyi tanımlayıcı verilerin bulunması halinde), telif kanunlarını (kazınan internet siteleri kullanım şartlarının otomatik araçlarla kopyalamaya izin vermediği halde) ve kazınan internet siteleri robot, web örümcekleri ve arama botu gibi kazıma teknolojileriyle erişimi açıkça yasakladığı durumda hukuki kuralları ve bilişim kanunlarını ihlal edebileceğini belirtmektedir. Bu hususta detaylı bilgi için bkz. Determann, s. 137, 138.

[817] Bu konuda ayrıntılı bilgi için bkz. 2.3.1 no'lu başlık altındaki açıklamalar.

[818] Basel Committee on Banking Supervision, "Open banking and application programming interfaces", Bank for International Settlements, Kasım 2019, (*"BIS"*), s. 9: https://www.bis.org/bcbs/publ/d486.pdf (Gözden Geçirilme Tarihi: 29.10.2020)

[819] Roman V. Yampolskiy, Louisville Üniversitesi Speed Mühendislik Okulu Bilgisayar Mühendisliği Ve Bilişim Ana Bilim Dalı'nda kadrolu akademisyen olup aynı zamanda üniversitenin siber güvenlik laboratuvarının kurucusu ve şimdiki direktörüdür. Ayrıca Artificial Superintelligence: A Future Approach kitabı gibi, yapay zeka ve siber güvenlik alanında çok sayıda kitabın yazarıdır. Bkz. Roman

belirtilerek yakın gelecekte, yapay zekanın becerileri çoğaldıkça daha ileri düzeyde otonom hale gelmiş ve hassasiyet kazanmış sosyal mühendislik saldırılarının gerçekleştirileceği, bu yapay zeka destekli hacker'lığa karşı siber güvenliğin temin edilmesinde yine çözümün yapay zeka destekli yazılımlar olduğu ileri sürülmüştür[820].

Türk doktrini açısından konuya bakıldığında ise, Henkoğlu[821] yapay zeka uygulamalarının veritabanlarındaki sistem açıklarının tespiti, DoS saldırılarına karşı otomatikleşmiş ve ağ içerisinde çok daha geniş bir alana yayılarak yararlanmanın imkanı olduğunu belirtmekle beraber yapay zekanın, kurumsal bilgi güvenliğinin sağlanması noktasında sorumluluğu bulunan herkes için iki önemli riskin söz konusu olduğunu belirtmektedir[822]: (i) Kurum içi ve kurum dışı tüm tehdit unsurlarının (çalışanlar, rakipler, suçlular vb.) acemi şekilde tasarlanan yapay zeka uygulamalarını manipüle etmesi mümkündür. (ii) Saldırganların, mağdurların savunmasında yer alan güvenlik açıklarından yararlanarak yapay zekâyı kullanabilecektir. Bu nedenle, Henkoğlu, siber tehditlere karşı daha sağlam ve esnek yapay zekâ sistemlerinin geliştirilmesi ve kısıtlamalarının azaltılabilmesi açısından, siber güvenliğin temininde yapay zeka-insan arasındaki iş birliğine ve eğitim ihtiyacına dikkat çekmiştir[823].

Yapay zekanın bankacılık işlemlerindeki uygulamasına yönelik Business Insider 2019 tarihinde önemli bir rapor[824] yayınlamıştır. İlgili raporda, yapay zeka ile ulaşılacak

---

V. Yampolskiy, "Yapay Zeka Siber Güvenliğin Geleceğidir", Harvard Business Review Press, Dijital Dönüşüm Siber Güvenlik, Optimist, 2020 (*"Yampolskiy"*), s. 198.

820 *Yampolskiy*, s. 187-195.

821 Türkay Henkoğlu, "Yapay Zekâ Sistemlerinin Güvenlik ve Hukuk Bağlamındaki Etkilerine İlişkin İnceleme ve Öngörüler", T.C. Ankara Üniversitesi, BİL-GEM, Bilgi Yönetimi Ve Bilgi Güvenliği, e-Belge-eDevlet-eArşiv-Bulut Bilişim-Büyük Veri-Yapay Zeka, Ankara, 2019, (*"Henkoğlu"*), s. 119-135. İlgili kaynağa internet üzerinden ulaşmak için: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Desktop/Endustri-4.0-Surecinde-Bilgi-Yonetimi-ve.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

822 *Henkoğlu*, s. 128.

823 *Henkoğlu*, s. 128.

824 Business Insider Intelligence, 2019, "The impact of artificial intelligence in the banking sector & how AI is being used in 2020", ilgili habere ulaşmak için Bkz. https://www.businessinsider.com/ai-in-banking-report (Gözden Geçirilme Tarihi: 29.10.2020).

çözümleri uygulamaya koyan bankalarda ciddi ölçüde maliyet tasarrufu yapıldığı belirtilmiştir. Bahsi geçen rapora göre, 100 milyar Dolar'ın üzerinde olan bankaların %75'inin yapay zeka stratejileri uyguladığı, varlığı 100 milyar Dolar'ın altında olan bankaların ise ancak % 46'sının bankacılık uygulamalarında yapay zeka stratejileri uyguladığı görülmüştür. Bu noktada, raporun ilginç öngörülerinden bir tanesi de 2023 yılına kadar bankaların yapay zeka stratejileri sayesinde yaklaşık 447 milyar USD'nin üzerinde maliyet tasarrufu sağlayacağı tahmin edilmektedir. Raporda bankaların maliyetlerden tasarruf etmek için yapay zekayı üç ana kanaldan kullanılabileceği tahmin edilmektedir:

i) *Ön Büro – İletişimsel Bankacılık*ta[825], bankalar müşteri tanımlaması ile kimlik doğrulamasını kolaylaştırmak bakımından sohbet botları ve sesli asistanlar vasıtasıyla müşterileri ile iletişim kurmakta ve müşterileri açısından kişiselleştirilmiş bilgiler ve önerilerden yararlanmaktadır.

ii) *Orta Ofis (Dolandırıcılığı Önleme) Bankacılık ise* çalışmanın odak noktası, elektronik ödeme sistemlerinde siber güvenlik olması sebebiyle yapay zekanın bankalar tarafından orta ofis işlevinde sahtekarlıkları tespit etmek ve kara para aklamanın önlenmesi konusunda etkin bir araç olarak kullanılması özellikle dikkat çekicidir.

iii) *Arka Ofis (Kredilendirme)* bakımından ise, bankaların kredi verecekleri müşterilerine dair kredilendirme öncesi araştırma bakımından yapay zeka teknolojisinin de maliyet tasarrufu sağlayacağı öngörülmektedir. Insider'ın raporuna konu aldığı şirketlerin Capital One, Citi, HSBC, JPMorgan Chase, Personetics, Quantexa, and U.S. Bank oldukları belirtilerek bahsi geçen raporda özellikle yukarıda belirtilen yapay zekaya ilişkin ön büro ve orta

[825] İlgili raporda, "Conversational Banking" olarak yer almakta olup yazar tarafından "İletişimsel Bankacılık" olarak tercüme edilmiştir (Serbest Çeviri).

ofis yapay zeka uygulamalarının rekabet noktasında kritik ölçüde maliyet tasarrufu sağlayacağına dikkat çekilmiştir.

Yapay zekanın siber güvenlik alanında bir başka kullanım alanın ise zararlı yazılımlara karşı olacağı öngörülmektedir. Chip Dergisi'nin 2020 yılının Temmuz ayında yayınlanan 2020 Hacker Raporu'nda[826] saldırganların şirketlerde olduğu gibi görev dağılımları yaptığı, farklı işlerde uzmanlaşmış ekiplerin olduğu, örneğin bir grup şirket ağlarına sızma konusunda uzmanlaşırken başka bir grubun veri hırsızlığı ya da veri şifreleme açısından donanımlı olduğu ve bu şekilde sistemli ve başarılı siber ataklar gerçekleştirildiğine dikkat çekilmiştir. Uzmanlara göre, 2020 yılında özellikle *"Living off the land"*[827] gibi zararlı yazılımlarla gerçekleştirilen karmaşık saldırılara karşı, virüs koruma programları bu zararlı yazılımları fark etmekte başarısızlık göstermektedir. Öte yandan, Hacker Raporu'nda ayrıca siber suç modelinin de değişmesi ile beraber saldırganların anlaşılması son derece güç iletiler gönderdiği, ev kullanıcıların Amazon gibi sitelerden geldiğini düşündükleri iletilere teslimat onayı verdikleri belirtilmiştir. Bu açıdan siber saldırıların giderek etkinleştiği ve koruma yöntemlerine bağlı olarak zararlı yazılımların kendilerini geliştirdiği ve kompleks hale geldiği dikkate alındığında, insan gözüyle ayrıştırılması zor olan zararlı yazılımlar konusunda güvenlik uzmanlarının özellikle yapay zeka tabanlı çözümler aradığı ve yapay zekanın büyük miktarda veri alıp bunları hızla öğrenme ve kısa sürede işleyerek yeni şüpheli kalıpları ortadan kaldırma kapasitesine sahip olduğu değerlendirilmiştir[828]. Zararlı yazılımların saptanmasında yapay zeka teknolojisinin kullanılmasına verilecek bir başka örnek ise Deep Instinct olup bu şirketin malware konusunda yapay zeka ajanları kullandığı, kara para aklama faaliyetlerinin ortaya çıkarılmasında ise PayPal ve IBM Technology

[826] Chip Dergisi, S: 2020/2, ISSN: 1300-9419, ("*Hacker Raporu")*, s. 46-49.
[827] Bilişim dünyasında, "living off the land" kavramı, siber korsanların bulunduğu yerin kaynaklarını kullanmak üzere geliştirdiği saldırı yöntemini ifade etmekte olup saldırganların Windows'un Powershell veya Bitlocker gibi yerel araçlardan faydalanmak suretiyle zararlı yazılımların fark edilmeden sisteme enjekte edilmesi anlamına da gelmektedir. Bkz., *Hacker Raporu*, s. 46.
[828] *Hacker Raporu*, s. 48.

tarafından benzer şekilde yapay zeka tabanlı teknolojik ürünlerin kullanıldığı bilinmektedir[829].

Sonuç itibariyle, özellikle birçok farklı teknolojik alanda salt bir teknoloji yerine hibrit sistemlerin ve farklı teknolojilerin kullanılmasının söz konusu teknolojiden beklenen faydayı sağlama noktasında katma değer sağladığı bilinen gerçektir. Özellikle çalışma kapsamında yapay zekanın elektronik ödeme endüstrisi gibi internet ortamında etkin faaliyet gösteren işletmeler açısından yukarıda da belirtildiği gibi orta ofis çerçevesinde kullanılması ve yapay zeka destekli siber güvenlik önlemlerine ağırlık verilmesinin yaratıcı ve sonuca ulaşmak konusunda motivasyonu yüksek siber korsanlar karşısında etkin bir yöntem olacağı özellikle dikkate alınması gerekli bir husustur.

6.5. COVİD-19 PANDEMİ SALGININ DİJİTAL BANKACILIĞA OLASI ETKİLERİ

Dünyada ve Türkiye'de etkisi görülen Covid-19 salgını, banka gibi finansal kuruluşların dijitalleşmesini bir tercih yerine zorunluluk haline getirmiştir. Covid-19 gibi bir salgının yaygın olduğu ve yüz yüze etkileşimin imkânsız olduğu zamanlarda, e-Devlet çözümleri ile yukarıda detaylı şekilde açıklanan AB'nin eIDAS Tüzüğü gibi regülasyonları sayesinde özellikle güven hizmetleri açısından yasal mevzuatta elektronik imzalar gibi hususlarda gidilecek değişiklikler önem taşımaktadır[830].

KPMG'nin hazırladığı "Geleceğin Dijital Bankacılığı" başlıklı raporuna göre iş modellerini hızla dijitale taşıyan bankaların, 2030'lu yıllarda mevduat işlemlerinden ziyade bankaların kişisel verilerin korunacağı en güvenilir alan olacağı, geleceğin bankalarının fintech şirketleri ile iş birliğine gideceği, açık bankacılık sisteminin daha da yaygınlaşacağı, yapay zekâ teknolojisinin geleceğin bankalarının güvenilirliği

[829] Erik Brynjolfsson/Andrew McAfee, "Yapay Zekanın Vaat Ettikleri", Harvard Business Review Press, Dijital Dönüşüm Yapay Zeka, Optimist, 2020, (*"Brynjolfsson/McAfee"*), s. 27.
[830] *Keser Berber, Güven Hizmetleri*, s. 1.

koruma noktasında etkin bir rol oynayacağının öngörülmektedir[831]. 11FS'nin "Covid-19 Dijital Finans Hizmetlerini Nasıl Hızlandıracak?" isimli raporunda ise, özetle Covid-19 pandemi salgınının makro ölçüde ekonomide global bir durgunluğa sebep olacağı ve mikro açıdan konuya bakıldığında ise, finans endüstrisinde diğer tüm sektörlerde olduğu gibi gelirde ve sermayede azalmaya sebebiyet vereceği, bu süreçte finans hizmetleri endüstrisinde dijitalleşmenin daha yaygınlık kazanacağı, finans alanında özellikle dijital alandaki işbirliklerin kritik derecede önem taşıyacağı ancak bu durumun özellikle siber risk ve dolandırıcılık konusundaki riskleri de beraberinde getireceği belirtilmiştir[832].

Türkiye'de ise özellikle Covid-19 dönemi sonrasında, siber saldırılarda ciddi ölçüde bir artış yaşanmış olup somut bir örnek açısından konuya bakıldığında ise siber saldırganların e-devlet uzantılı yeni bir oltalama tekniği ile vatandaşların kredi kartı bilgilerini istismar etmeye çalıştığı bilinmektedir[833]. Covid-19 kriziyle beraber vatandaşların tasarruflu hareket etme gayesinden faydalanmak isteyen saldırganlar, önce kurbanlarına gönderdikleri SMS ile bir bankanın yıllık kart iadesi için e-devlete başvurması gerektiğine yönelik oltalama saldırısı düzenlemektedir. İlgili vatandaş ise mesajdaki linke tıklayarak e-devlet gibi görünen web sitesi üzerinde kart bilgileri ve şifrelerini girmeleri sonucunda tüm kart bilgileri siber dolandırıcıların eline geçmekte ve bu sayede kurbanların kredi kartlarından yüklü miktarda para çekilmesi sağlanmıştır. Daha sonraki süreçte ise bu konuda mağdur olan kişilerin haksız şekilde kartlarından ödeme yapan siber korsanlara ulaşmaları mümkün olmamıştır.

---

[831] Söz konusu habere ulaşmak için Bkz. https://www.bloomberght.com/10-yil-icinde-bankalari-bekleyen-yikici-donusum-ne10-yil-icinde-bankalari-bekleyen-yikici-donusum-ne-2253953 (Gözden Geçirilme Tarihi: 29.10.2020).

[832] https://info.11fs.com/hubfs/How%20the%20COVID-19%20pandemic%20will%20accelerate%20digital%20financial%20services.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

[833] Bkz. Sözcü Gazetesi'nin 07.08.2020 tarihli "E-devlet ile kredi kartı tuzağı" başlıklı haberi. İlgili haberde WatchGuard'ın açıkladığı son veriler ışığında Türkiye'de pandemide 2020 yılının ilk altı ayında üç katlık bir artış yaşandığı ve her dakikada beş adet zararlı yazılım saldırısı gerçekleştirildiği belirtilmiştir. İlgili habere internette ulaşmak için bkz. https://www.sozcu.com.tr/2020/ekonomi/e-devlet-ile-kredi-karti-tuzagi-5925947/ (Gözden Geçirilme Tarihi: 29.10.2020).

SONUÇ

Yukarıda tez kapsamında ele alınan her ödeme sisteminin işleyişi açıklanarak ayrıntılı siber güvenlik analizlerine yer verilmiştir. Konu salt teknik açıdan değil, karşılaştırmalı hukuk ve Türkiye'deki yasal düzenlemeler çerçevesinde de ele alınmıştır. Bu bağlamda, elektronik ödeme sistemlerinde siber güvenlik denildiğinde yapılan araştırma sonucunda genel çıkarımlar şunlar olmuştur:

Elektronik ödeme endüstrisi özellikle deyim yerindeyse saldırganlar açısından çekim merkezi olması nedeniyle her geçen gün yeni saldırı tekniklerinin geliştirildiği bir alandır ve bu anlamda kırılgandır.

Elektronik ödeme sistemlerinde bilgi güvenliği yönetimi, çoğu kez banka gibi birçok şubesi bulunan gelişmiş ve bilgi teknolojisi sistemlerinin karmaşık olduğu yapılarda kilit çözümlerin bulunmasını zorlaştırmaktadır.

Özellikle bankaların günümüzde müşterileri tarafından birer güven kurumu olarak değerlendirilmesi sebebiyle siber saldırılar neticesinde ortaya çıkabilecek büyük ölçekli finansal kayıplardan daha önemlisi, bankaların müşterileri nezdindeki "itibar kaybı"dır.

Yukarıda detaylı şekilde farklı boyutlarıyla açıklandığı üzere, siber güvenlikte en zayıf katmanın "insan faktörü" olması elektronik ödeme sistemlerine yöneltilen siber saldırılarda çoğu kez daha geçerlidir. Saldırganların elektronik finans sistemine yönelttikleri saldırılarda çoğu kez sahip oldukları teknik alandaki tecrübeden ziyade hedefteki insanların basit ve önemsenmeyecek hatalarından faydalanması neticesinde başarıya ulaştıkları görülmüştür.

Tezin bazı bölümlerde de ayrıntılı şekilde irdelendiği üzere, elektronik ödeme sistemlerinde siber güvenlik açısından son zamanlarda en belirliyici etkenlerden birisi de Covid-19 pandemisinin yarattığı sonuçlar olarak değerlendirilmiştir. Bu bağlamda, çalışma açısından büyük resme bakıldığında Covid-19 pandemi salgını kişilerin elektronik ödeme sistemlerini kullanmayı tercih etmesinde adeta bir çarpan etkisi

yaratmış, buna karşın ise siber korsanlar açısından elektronik ödemeler daha cazip hale gelmiştir. Bu açıdan yaratıcılık konusunda üstün meziyetlere sahip siber korsanlar karşısında, gayri meşru yollardan menfaat sağlamak isteyen bu kişilerin sabrı ve yeteneği göz önüne alındığında, özellikle Covid-19 koşulları altında başta ödeme olmak üzere her işlemi elektronik ortamda gerçekleştirmek isteyen kişilere yönelik daha büyük bir risk teşkil etmektedir. Bu süreçte ise, çalışma kapsamında fark edildiği üzere, dünyada ve Türkiye'de elektronik ödemelerde siber güvenlik bakımından birçok yeni düzenleme yürürlüğe girerek hareketli bir dönem yaşanmıştır. Ayrıca, araştırma kapsamında özellikle regülasyonlar bakımından dünyada ve Türkiye'de bu konunun yasa koyucular açısından düzenlenmesi elbette ki, değerli birer kazanım olarak değerlendirilse de siber güvenlik açısından elde edilecek en etkin çözümler Son Bölüm'de de dikkat çekildiği üzere yapay zeka ve blokzincir teknolojisi gibi yeni nesil teknolojilerinin siber güvenliğin temininde etkin şekilde kullanılması olacaktır.

Sonuç itibariyle siber güvenlik meselesi özellikle elektronik ödeme sistemleri açısından asla hafife alınmaması ve üzerinde etraflıca durularak kapsamlı teknik ve hukuki tedbirlerin alınması gereken bir meseledir. Sun Tzu'nun "Savaş Sanatı" adlı eserinde konu ile ilgili olabilecek şu özdeyişi[834] bu çalışmaya ışık tutması açısından anlamlıdır: "Eğer düşmanı ve kendini tanıyorsan, yüz kere de çarpışsan düşmandan korkmana gerek yok. Eğer kendini tanıyorsan ama düşmanını tanımıyorsan, kazandığın her zafer için bir de yenilgi acısı tadarsın. Eğer ne kendini ne de düşmanını tanıyorsan, her savaşta bozguna uğrarsın." Mesele elektronik ödemelerde siber güvenlik gibi bir konu olduğunda ise, kurbanın karşısındaki siber korsanı ve saldırı yöntemlerini önceden bilmesi çoğu kez imkansızdır, dolayısıyla herhangi bir çatışmadan galip çıkması da bu açıdan çoğu kez imkansızdır. Bu nedenle siber uzaydaki düşmanlara karşı en azından elektronik ödemelerde faaliyet gösterenlerin bilinçli olarak kendi

[834] https://tr.wikiquote.org/wiki/Sun_Tzu (Gözden Geçirilme Tarihi: 29.10.2020).

alabilecekleri önlemleri bilmeleri gerekir ki, ancak bu sayede olası risklere karşı meydana gelebilecek zarar asgari düzeyde tutulabilecektir.

KAYNAKÇA

I. ESERLER

AKBULUT : Berrin Akbulut, Bilişim Alanında Suçlar, Adalet Yayınevi, 2. Baskı, Ankara, 2017.

AKÖZ : Burak Cesur Aköz, Türk Ceza Kanunu Kapsamında Bilişim Suç Ve Cezaları İle Örnek Yargısal Kararların Analizi Ve Mevzuat Önerileri", Bilgi Teknolojileri Ve İletişim Kurumu, Bilişim Uzmanlığı Tezi, Ankara, 2018.

ALTINKAYNAK : Mustafa Altınkaynak, Uygumalı Siber Güvenlik Ve Hacking, Abaküs, 5. Baskı, İstanbul, 2018.

BAŞ : Eylem Baş, Banka Ve Kredi Kartlarının Kötüye Kullanılması Suçu, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku (Ceza Ve Ceza Muhakemesi

Hukuku) Anabilim Dalı, Yüksek Lisans Tezi, Ankara, 2013.

BOZKURT YÜKSEL, ELEKTRONİK PARA : Armağan Ebru Bozkurt Yüksel, Elektronik Para, Sanal Para, Bitcoin Ve Linden Doları'na Hukuki Bir Bakış, Aristo Yayınevi, 1. Baskı, İstanbul, 2018.

BOZKURT YÜKSEL, BULUT BİLİŞİMDE KİŞİSEL VERİLERİN KORUNMASI : Armağan Ebru Bozkurt Yüksel, Bulut Bilişimde Kişisel Verilerin Korunması, Yetkin Yayınları, Ankara, 2016.

BLOK ZİNCİRİ : Harvard Business Review Press, Dijital Dönüşüm Blok Zinciri, Optimist Yayın, 1. Baskı, İstanbul, 2020.

BÜLBÜL/BİNGÖL : İsmail Bülbül/Poyraz Emre Bingöl, Etik Hackerlığa Giriş, Ofansif Siber Güvenliğin ABC'si, Hayykitap, 7. Baskı, İstanbul, 2019.

ÇAKIR/KILIÇ : Hüseyin Çakır, Mehmet Serkan Kılıç (Editörler), Güncel Tehdit: Siber Suçlar, Seçkin Yayıncılık, Ankara, 2014.

ÇAVUŞOĞLU : Cenk Çavuşoğlu, Elektronik Paranın Gelişimi Ve Merkez Bankası Bilançosu Ve Para Politikası Uygulamaları Üzerine Etkisi, Uzmanlık Yeterlilik Tezi, T.C. Merkez Bankası Muhasebe Genel Müdürlüğü, Ankara, Haziran, 2015.

ÇAY : Şerif Çay, Elektronik Ödeme Sistemlerinin Finansal Piyasalara Etkisi, T.C. Bahçeşehir Üniversitesi, Yüksek Lisans Tezi, Ankara, 2015.

ÇINAR : Süleyman Çınar, Mobil Android Ortamında Parmak İzi Tanıma Ve Kimlik Doğrulama Sisteminin Geliştirilmesi, Haliç Üniversitesi Fen Bilimleri

Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı Bilgisayar Mühendisliği Programı, Yüksek Lisans Tezi, İstanbul, 2014.

ÇUBUKÇU : Faruk Çubukçu, Bilgi Güvenliği Yönetim Sistemi ISO 27001 – Uygulama Kılavuzu, Pusula, 1. Baskı, İstanbul, 2018.

DETERMANN : Lothar Determann, Kişisel Verilerin Uygulama Klavuzu, Oniki Levha Yayınları, 1. Baskı, İstanbul, 2020.

DÜLGER, BİLİŞİM SUÇLARI : Murat Volkan Dülger, Bilişim Suçları Ve İnternet İletişim Hukuku, Seçkin, Güncellenmiş 8. Baskı, Ankara, 2020.

EBERL : Ulrich Eberl, "Akıllı Makineler Yapay Zeka Hayatımızı Nasıl Değiştiriyor", Paloma Yayınevi, 1. Baskı, İstanbul 2019.

ERALP : Özgür Eralp, İnternet Bankacılığı Ve Kredi Kartı Dolandırıcılığının Teknik, Hukuki Ve Cezai Boyutu, Eralp Kitap, Ankara, 2012.

EREN : Mehmet Eren, Avrupa Birliği'nin Siber Güvenlik Politikası, Beta, 1. Baskı, İstanbul, 2017.

FERİDUN KAYA : Feridun Kaya, Türkiye'de Kredi Kart Uygulaması, Türkiye Bankalar Birliği, Yayın No: 263, İstanbul, 2009.

FRA : European Union Agency For Fundamental Rights (*FRA*), Avrupa Veri Koruma Mevzuatı El Kitabı, 2018.

FRIEDMAN : Thomas L. Friedman, Geciktiğin için Teşekkür Ederim, Boyner Yayınları, 1. Baskı, İstanbul, 2018.

GIMIGLIANO : Gabriella Gimigliano, Money, Payment Systems and the European Union, The

Regulatory Challenges of Governance, Cambridge Scholars Publishing, 2016.

GRAHAM/HOWARD/OLSON : James Graham/Richard Howard/Ryan Olson, Cyber Security Essentials, CRC Press Taylor&Francis Group, 2011.

HENKOĞLU : Türkay Henkoğlu, Yapay Zekâ Sistemlerinin Güvenlik ve Hukuk Bağlamındaki Etkilerine İlişkin İnceleme ve Öngörüler, T.C. Ankara Üniversitesi, BİL-GEM, Bilgi Yönetimi Ve Bilgi Güvenliği, e-Belge-eDevlet-eArşiv-Bulut Bilişim-Büyük Veri-Yapay Zeka, Ankara, 2019.

KAYA, ELEKTRONİK TİCARET : Mehmet Bedii Kaya, Elektronik Ticaret Hukuku Ticari Elektronik İletiler, On İki Levha Yayıncılık, 2. Baskı, İstanbul, 2020.

KAYA, ERİŞİMİN ENGELLENMESİ : Mehmet Bedii Kaya, Teknik Ve Hukuki Boyutlarıyla İnternete Erişimin Engellenmesi 5651 Sayılı Kanun ve Dünya Uygulamaları, On İki Levha Yayıncılık, 1. Baskı, İstanbul, 2010.

KESER BERBER, ELEKTRONİK PARA : Leyla Keser Berber, İnternet Üzerinden Yapılan İşlemlerde Elektronik Para Ve Dijital İmza, Yetkin Yayınları, Ankara 2002.

KESER BERBER, GÜVEN HİZMETLERİ : Leyla Keser Berber, Kurumsal Güven Bağlamında Güven Hizmet Sağlayıcı (Trust Service Provider), Güven Hizmetleri Ve Karşılıklı Tanıma Sorunu, Oniki Levha Yayıncılık, 1. Baskı, İstanbul, 2020.

KESER BERBER/LOSTAR : Leyla Keser Berber/Murat Lostar, Bilişimde Biyometrik Yöntemler, Yetkin Yayınları, Ankara, 2006.

KİRDABAN : İbrahim Kirdaban, Ödeme Sistemlerindeki Gelişmeler Ve Ödeme Sistemlerinin Finansal Sistem İstikrarı Üzerindeki Etkileri, Uzmanlık Tezi, Türkiye Cumhuriyeti Merkez Bankası Bankacılık Ve Finansal Kuruluşlar Genel Müdürlüğü, Ankara, 2005.

LONG : Rebecca M. Long, Using Phishing To Test Social Engineering Awareness of Financial Employees, Thesis, Eastern Washington University, Master of Science, 2013.

MADENCİ : Timur Madenci, Kredi Kartı Ve Debit Kart Uygulamaları Ve Karlılık Açısından Değerlendirme, T.C. Marmara Üniversitesi, Bankacılık Ve Sigortacılık Enstitüsü Bankacılık Ana Bilim Dalı, Yüksek Lisans Tezi, İstanbul, 1996.

MITNICK/SIMON : Kevin D. Mitnick/William L. Simon, Sızma Sanatı, Odtü Yayıncılık, 4. Basım, Ankara, 2017.

ÖZDOĞAN : Ogan Özdoğan, Endüstri 4.0 Dördüncü Sanayi Devrimi Ve Endüstriyel Dönüşümün Anahtarları, Pusula, 2. Baskı, İstanbul, 2018.

ÖZER Yusuf Mansur Özer, Kişisel Verilerin Korunmasında Blok Zinciri Modeli: Vaatler Ve Hukuki Engeller, On İki Levha Yayıncılık, 1. Baskı, İstanbul, 2020.

ÖZKAYA/SARICA/DURMAZ : Erdal Özkaya/Raif Sarıca/Şükrü Durmaz, Siber Güvenlik Saldırı Ve Savunma Stratejileri, Buzdağı Yayınevi, Ankara, 2019.

PARLAR : Ali Parlar, Türk Ceza Hukukunda Bilişim Suçları, Bilge Yayınevi, Ankara, 2015.

SİBER GÜVENLİK	:	Harvard Business Review Press, Dijital Dönüşüm Siber Güvenlik, Optimist Yayın, 1. Baskı, İstanbul, 2020.
SAĞIROĞLU	:	Şeref Sağıroğlu (Editör), Siber Güvenlik Ve Savunma Standartlar Ve Uygulamalar, BGD Siber Güvenlik Ve Savunma Serisi 3, Ankara, 2019.
SAĞIROĞLU/ALKAN	:	Şeref Sağıroğlu/Mustafa Alkan (Editörler), Siber Güvenlik Ve Savunma Farkındalık Ve Caydırıcılık, BGD Siber Güvenlik ve Savunma Kitap Serisi 1, Ankara, 2018.
SAĞIROĞLU/ŞENOL	:	Şeref Sağıroğlu/Mustafa Şenol (Editörler), Siber Güvenlik Ve Savunma, Problemler Ve Çözümler, BGD Siber Güvenlik ve Savunma Kitap Serisi 2, Ankara, 2019.

TANER : Cemal Taner, Herkes İçin Siber Güvenlik, Abaküs, 1. Baskı, İstanbul, 2019.

TOPALOĞLU/ÖZKİŞİ/TEKKANAT : Murat Topaloğlu/Harun Özkişi/Egemen Tekkanat, Bulut Bilişim, Seçkin Yayıncılık, 2017, Ankara.

TOĞÇUOĞLU : Didem Topçuoğlu, Nakitsiz Bir Toplum Ve Türkiye Üzerine Bir Araştırma, T.C. İstanbul Üniversitesi, Para Sermaye Piyasaları Ve Finansal Kurumlar Ana Bilim Dalı, Yüksek Lisans Tezi, İstanbul, 2019.

TURAN : Metin Turan, Bulut Bilişim, Seçkin Yayınevi, 2. Baskı, Ankara, 2019.

YAYIK : Apdullah Yayık, Yapay Sinir Ağı Ve Kriptoloji Uygulamaları, Mustafa Kemal Üniversitesi Fen Bilimleri Enstitüsü Enformatik Anabilim Dalı,

Yüksek Lisans Tezi, Hatay, 2013.

YAPAY ZEKA : Harvard Business Review Press, Dijital Dönüşüm Yapay Zeka, Optimist Yayın, 1. Baskı, İstanbul, 2020.

II. ELEKTRONİK AĞ ADRESLERİ

ALDWAIRI/ALDHANHANI **:** Monther Aldwairi/Saoud Aldhanhani, Multi-Factor Authentication System, file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/MFA-ASL_CamReady.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

ALİUSTA/BENZER **:** Cahit Aliusta/Recep Benzer, Avrupa Siber Suçlar Sözleşmesi Ve Türkiye'nin Dahil Olma Süreci, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt: 4, No: 2, 2018: https://www.researchgate.net/publication/331007406_Avrupa_Siber_Suclar_Sozlesmesi_ve_Turkiye'nin_Dahil_Olma_Sureci (Gözden Geçirilme Tarihi: 29.10.2020).

ALSAYED/BILGRAMI **:** Alhuseen Omar Alsayed/Anwar Bilgrami, E-Banking Security: Internet Hacking, Phishing Attacks, Analysis And Prevention of Fradulent Activities, International Journal of Emerging Technology and Advanced Engineering, C: 7, S: 1, Ocak 2017:

file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/E-BaningSecurityHuseenandBilgrami2017.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

ALLEN **:** Malcolm Allen, Social Engineering: A Means to Violate A Computer System, SANS Institute Information Security Reading Room: https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529 (Gözden Geçirilme Tarihi: 29.10.2020).

ALLEN VE DİĞERLERİ **:** Julia H. Allen/ Gregory Crabb/ Pamela D. Curtis/ Brendan Fitzpatrick/ Nader Mehravari/ David Tobar, Structuring the Chief Information Security Officer, Software Engineering Institute: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=446186 (Gözden Geçirilme Tarihi: 29.10.2020).

ASSANTE/LEE **:** Michael J. Assante/Robert M. Lee, The Industrial Control System Cyber Kill Chain, SANS, 2015: https://www.sans.org/reading-room/whitepapers/ICS/paper/36297 (Gözden Geçirilme Tarihi: 29.10.2020).

BARSAN **:** Iris M. Barsan, Legal Challenges of Initial Coin Offerings (ICO): file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/SSRN-id3064397.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

BCBS **:** BCBS, Report on open banking and application programming interfaces, Kasım, 2019: https://www.bis.org/bcbs/publ/d486.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

BENDIEK **:** Annegret Bendiek, European Cyber Security Policy, SWP Research Paper: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/EuropeanCyberSecurityPolicy.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

BKM **:** BKM/Tübitak BİLGEM, BKM, Blokzincirlerde Güvenlik Ve Mahremiyet başlıklı Rapor, Nisan 2020: https://bkm.com.tr/wp-content/uploads/2015/06/blokzincirlerde_guvenlik_ve_mahremiyet.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

BIS **:** BIS, Payments in the United States, CPSS, Red Book, 2003: https://www.bis.org/cpmi/paysys/unitedstatescomp.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

BLOCKCHAIN TÜRKİYE **:** Blockchain Türkiye, Hukuk, Düzenlemeler ve Kamu İlişkileri Çalışma Grubu, Dünyada Blokzinciri Regülasyonları ve Uygulama Örnekleri, Karşılaştırma Raporu, Şubat 2019: https://bctr.org/wp-content/uploads/2019/04/Dünyada-Blokzinciri-Regulasyonları.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

BRODSKY/OAKES **:** Laura Brodsky/Liz Oakes, Open banking and data sharing, McKinsey&Company: https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking (Gözden Geçirilme Tarihi: 29.10.2020).

BOUVERET **:** Antoine Bouveret, Cyber Risk for the Financial Sector: A Framework for Quantitive Assesment, IMF Working Paper.

file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/wp18143%20(3).pdf (Gözden Geçirilme Tarihi: 29.10.2020).

CAMENISH/PIVETEAU : Jan Camenish/Jean-Marc Piveteau, Security in Electronic Payment Systems: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/Security_in_Electronic_Payment_Systems.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

CHRISTOPHER FISCHER : Christoph Fischer, Digital Payments and Cyber Security: trends, risks and solutions: https://www.europeanpaymentscouncil.eu/news-insights/insight/digital-payments-and-cybersecurity-trends-risks-and-solutions (Gözden Geçirilme Tarihi: 29.10.2020).

CLOUGH : Jonathan Clough, A World of Difference: The Budapest Convention on Cybercrime And the Challenges of Harmonisation, Monash University Law Review, C: 40, No:3: https://web.archive.org/web/20160430024621/https://www.monash.edu/__data/assets/pdf_file/0019/232525/clough.pdf. (Gözden Geçirilme Tarihi: 29.10.2020).

CRISANTO/PRENIO : Juan Carlos Crisanto/ Jermy Prenio, Financial crime in times of Covid-19 – AML and cyber resilience measures, BIS, FSI Briefs, No: 7: https://www.bis.org/fsi/fsibriefs7.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

CRAIGEN VE DİĞERLERİ : Dan Craigen/Nadia Diakun-Thibault/Randy Purse, Defining Cybersecurity, Technology Innovation Management Review, Ekim, 2014: https://timreview.ca/sites/default/files/article_PDF/Craigen_et_al_TIMReview_October2014.pdf

NIST IR 7298 Revision 2, Glossary of Key Information Security Terms: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

ÇATALOĞLU/ATEŞKAN : Erdat Çataloğlu, Armağan Ateşkan, QR Kodunun Eğitim Ve Öğretimde Kullanımının Örneklendirilmesi: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/QRcodes.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

ÇAVUŞ/CHINGOKA : Nadire Çavuş/Dambudzo Netsai Christina Chingoka, Information Technology in the Banking Sector: Review of Mobile Banking: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/Informationtechnologyinthebankingsector-Reviewofmobilebanking-2.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

ÇİÇEK/SAĞLIK : Niyazi Çiçek/Özhan Sağlık, T.C. Ankara Üniversitesi, BİL-GEM, Bilgi Yönetimi Ve Bilgi Güvenliği, e-Belge-eDevlet-eArşiv-Bulut Bilişim-Büyük Veri-Yapay Zeka, Ankara, 2019: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Desktop/Endustri-4.0-Surecinde-Bilgi-Yonetimi-ve.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

CHIA/FENG/LEI : Xiaolin Chia, Quanyuan Feng, Taihua Fan, Quanshui Lei, RFID Technology and Its Applications in Internet of Things (IoT): file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/RFIDTechnologyandItsApplicationsinInternetofThingsIOT.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

CHOHAN : Usman W. Chohan, Initial Coin Offerings (ICOs): Risks, Regulation, and Accountability, 30 Kasım 2017, University of New

South Wales: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/SSRN-id3080098.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

DAHLBERG/MALLAT/ONDRUS : Tomi Dahlberg/Niina Mallat/Jan Ondrus/Agnieszka Zmijewska, "Mobile Payment Market and Research – Past, Present and Future", Working Papers on Information Systems, ISSN 1535-6078: https://www.researchgate.net/publication/269114169_Mobile_Payment_Market_and_Research_-_Past_Present_and_Future/link/548433ab0cf2f5dd63a91741/download (Gözden Geçirilme Tarihi: 29.10.2020).

DEMENTIEV/FENTON : Euegiene Dementiev/Norman Fenton, Bayesian Torrent Classification by File Name and Size Only: https://www.researchgate.net/publication/322635993_Bayesian_Torrent_Classification_by_File_Name_and_Size_Only/link/5a65b76ca6fdccb61c58d5c4/download (Gözden Geçirilme Tarihi: 29.10.2020).

DELOITTE : Deloitte, SWIFT Systems and the SWIFT Customer Security Programme: https://www2.deloitte.com/content/dam/Deloitte/be/Documents/risk/be-ra-swift-customer-security-programme.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

DENTONS, CHINA REPORT : Dentons, 2019 China Data Protection & Cyber Security Annual Report, 2020: https://www.dentons.com/en/insights/guides-reports-and-whitepapers/2020/march/31/2019-china-data-protection-cybersecurity-annual-report (Gözden Geçirilme Tarihi: 29.10.2020).

DIGITAL EUROPE : Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027 COM/2018/434 final – 2018/0227 (COD): https://eur-

lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A434%3AFIN (Gözden Geçirilme Tarihi: 29.10.2020).

DUPUIS : Marc Dupuis, Cyber Security for Everyone – An Introductory Course, 2017: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/CyberSecurityforEveryone-AnIntroductoryCourse.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

DÜLGER, 7222 SAYILI KANUN : Murat Volkan Dülger, 7222 Sayılı Kanun ile 5411 sayılı Bankacılık Kanunu'nda Yapılan Düzenlemenin KVK Hukuku Açısından Değerlendirilmesi: https://www.hukukihaber.net/7222-sayili-kanun-ile-5411-sayili-bankacilik-kanununda-yapilan-duzenlemenin-kvk-hukuku-acisindan-degerlendirilmesi-makale,7537.html (Gözden Geçirilme Tarihi: 29.10.2020).

EBA : Euro Banking Association, Open Banking: advancing customer-centricity, Analysis and overview, Mart, 2017, https://www.abe-eba.eu/media/azure/production/1355/eba_open_banking_advancing_customer-centricity_march_2017.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

EPC : European Payments Council, 2019 Payment Threats and Fraud Trends Report, EPC302-19, /Versiyon 1.0: https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2019-12/EPC302-19%20v1.0%202019%20Payments%20Threats%20and%20Fraud%20Trends%20Report.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

EPRS : EPRS, "Blockchain and the General Data Protection Regulation Can Distributed Ledgers be squared with European data protection law?),

2019:https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

ERDEM/ÖZOCAK1 **:** Merve Erdem/Gürkan Özocak, Siber Güvenliğin Sağlanmasında Uluslararası Hukukun Ve Türk Hukukunun Rolü, Ankara Üniversitesi Hukuk Fakültesi Dergisi, 68 (1) 2019: https://dergipark.org.tr/tr/download/article-file/695490 (Gözden Geçirilme Tarihi: 29.10.2020).

ERDEM/ÖZOCAK2 **:** Merve Erdem/Gürkan Özocak, Avrupa Konseyi Siber Suç Sözleşmesi Ve Türk Hukuku'na Etkileri: http://www.ozocak.com/Dosyalar/27669f.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

ERIC FISCHER **:** Eric A. Fischer, Federal Laws Relating to Cyber Security: Overview of Major Issues, Current Laws, and Proposed Legislation, Congressional Research Service, Aralık, 2014: https://www.everycrsreport.com/reports/R42114.html (Gözden Geçirilme Tarihi: 29.10.2020).

ELÇİBOĞA **:** İbrahim Kudret Elçiboğa, Sosyal Mühendislik Yöntemleriyle Dolandırıcılık, Fintechtime: http://fintechtime.com/tr/2018/07/sosyal-muhendislik-yontemleriyle-dolandiricilik/ (Gözden Geçirilme Tarihi: 29.10.2020).

EVRİN/DEMİRER **:** Volkan Evrin/Mehmet Demirer, Kurumsal Bilgi Güvenliği Süreç Çalışmaları: ISOIEC-27001 Örneği": http://www.emo.org.tr/ekler/135c9b87ad18ef4_ek.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

FABRIS **:** Nikola Fabris, Cashless Society – The Future of Money or a Utopia?: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/Cashless_Society_-_The_Future_of_Money_or_a_Utopia.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

F-SECURE **:** F-Secure, Threat Analysis, SWIFT Systems and the SWIFT Customer Security Program: https://www.f-secure.com/content/dam/f-secure/en/business/common/collaterals/f-secure-threat-analysis-swift.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

GÖKÇE **:** Müjdat Gökçe, Nesnelerin İnterneti: file:///C:/Users/cemal/Downloads/NESNELERIN_INTERNETI_Internet_of_Things.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

GORDON/LOEB/SOHAIL **:** Lawrence A. Gordon/Martin P. Loeb/Tashfeen Sohail, A Framework for Using Insurance for Cyber-Risk Management: https://www.researchgate.net/publication/220421077_A_framework_for_using_insurance_for_cyber-risk_management/link/54d8999f0cf24647581aceeb/download (Gözden Geçirilme Tarihi: 29.10.2020).

GSG HUKUK RAPORU **:** PwC (GSG Hukuk), Açık Bankacılık: Dünya ve Türkiye: https://www.pwc.com.tr/tr/sektorler/bankacilik/pdf/acik-bankacilik-dunya-ve-turkiye-v2.pdf. (Gözden Geçirilme Tarihi: 29.10.2020).

GYAMFI VE DİĞERLERİ **:** Nana Kwame Gyamfi/Mustapha Adamu Mohammed/Kwaku Nuamah-Gyambra/Ferdinand Katsriku/Jamal-Deen Abdulah, Enhancing the Security Features of Automated Teller Machines (ATMs): A Ghanaian Perspective, International Journal of Applied Science and Tecnology, C:2,

S:1, Şubat 2016: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/15.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

HAUGEN VE DİĞERLERİ : Peter Haugen/Ian Myers/Bret Sadler/John Whidden, A Basic Overview of Commonly Encountered Types of Random Access Memory (RAMs): https://www.rose-hulman.edu/Class/ee/yoder/ece332/Papers/RAM%20Technologies.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

HONG VE DİĞERLERİ : Geng Hong/Zhemin Yang/Sen Yang/Lei Zhang/Yuhong Nan/Zhibo Zhang/Min Yang/Yuan Zhang/Zhiyun Qian/Haixin Duan, How You Get Shot in the Back: http://www.cs.ucr.edu/~zhiyunq/pub/ccs18_cryptojacking.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

HAO WANG : Hao Wang, Nudging Data Privacy Management of Open Banking Based on Blockchain: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/blockchain-ispan-camer.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

HEKİM/BAŞIBÜYÜK : Hakan Hekim/Oğuzhan Başıbüyük, Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları, Uluslararası Güvenlik ve Terörizm Dergisi, 4 (2) 2013: http://www.acarindex.com/dosyalar/makale/acarindex-1423936102.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

IBM : IBM, IBM Security Services 2014 Cyber Security Intelligence Index: https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligence_20450.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

IRUM/KHAN/KHIYAL **:** Misbha Irum, Aihab Khan, Malik Sikander, Hayat Khiyal, Confidentiality of Messages in a Cardless Electronic Payment Systems, International Journal of Reviews in Computing, 2011: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/ijric629-32.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

İŞLER/GÜLAÇ **:** Barış İşler, Hakan Gülaç, Mobil Ödemeler, Güvenlik Sorunları Ve Çözüm Önerileri, BDDK Bankacılık ve Finansal Piyasalar C: 11, S: 2, 2017: https://www.bddk.org.tr/ContentBddk/BddkDergi/dergi_0022_05.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

JAWALE/PARK **:** Ashay S. Jawale/Joon S. Park, A Security Analysis on Apple Pay, 2016 European Intelligence and Security Informatics Conference: http://www.csis.pace.edu/~ctappert/papers/proceedings/2016EISIC/data/2857a160.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

KARAGÖZLÜ **:** Hümeyra Karagözlü, Homo Homini Lupus, Thomas Hobbes'un Ahlak Felsefesi Üzerine: https://dergipark.org.tr/en/download/article-file/162706 (Gözden Geçirilme Tarihi: 29.10.2020).

KASPERSKY **:** Kaspersky, Avoiding A Trojan Virus: Keeping the Gates Closed: https://www.kaspersky.com/resource-center/preemptive-safety/avoiding-a-trojan-virus (Gözden Geçirilme Tarihi: 29.10.2020).

KAZAN **:** Erol Kazan, The Innovative Capabilities of Digital Payment Platforms: Comparative Study of Apple Pay & Google Wallet: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/TheInnovativeCapabilitiesOfDigitalPaymentPlatforms%20(1).pdf (Gözden Geçirilme Tarihi: 29.10.2020).

KHAROUNI **:** Loucif Kharouni, "Automatic transfer system: The latest cybercrime toolkit feature trend micro incorporated research paper, Trend Micro: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_automating_online_banking_fraud.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

KILIÇ/GÖKÇÖL **:** Mehtap Çetinkaya Kılıç, Orhan Gökçöl, Türkiye'deki İşletmelerin Bilgi Güvenliği Yönetim Sistemi Altyapısının Değerlendirilmesi: http://www.emo.org.tr/ekler/e07b4f2c678f096_ek.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

LESSIG **:** Lawrence Lessing, The Code in Law, and the Law in Code: https://web.stanford.edu/class/msande91si/www-spr04/readings/week3/Lessig-pcforum.pdf
https://fintechistanbul.org/2016/10/15/ethereuma-yine-mecburi-catallasma-geliyor/ (Gözden Geçirilme Tarihi: 29.10.2020).

LOCKHEED MARTIN **:** Lockheed Martin, The Cyber Kill Chain: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (Gözden Geçirilme Tarihi: 29.10.2020).

LONG **:** Rebecca M. Long, Using Phishing To Test Social Engineering Awareness of Financial Employees, Thesis, Eastern Washington University, Master of Science, 2013:

file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/rlong_thesis_v4.5_FINAL%20(1).pdf (Gözden Geçirilme Tarihi: 29.10.2020).

LOSTAR : Murat Lostar, Veri Maskeleme: https://lostar.com.tr/2012/04/veri-maskeleme.html (Gözden Geçirilme Tarihi: 29.10.2020).

MALAREBYTES : Malwarebytes, Cybersecurity basics: Everthing you need to know about cybercrime: https://www.malwarebytes.com/cybersecuirty/ (Gözden Geçirilme Tarihi: 29.10.2020).

MCKINSEY : McKinsey&Company, Data Sharing and open banking, Eylül, 2017: https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking# (Gözden Geçirilme Tarihi: 29.10.2020).

MIT : MIT Technology Review, Insights/Research, Open banking, The race to deliver banking as a service: https://www.oracle.com/a/ocom/docs/dc/open-banking-final.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

MITNICK : Kevin D. Mitnick, The Art of Deception: https://repo.zenk-security.com/Magazine%20E-book/Kevin_Mitnick_-_The_Art_of_Deception.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

M-TRENDS REPORT : M-Trends 2019 Fireeye Mandiant Services, Special Report: https://content.fireeye.com/m-trends/rpt-m-trends-2019 (Gözden Geçirilme Tarihi: 29.10.2020).

MOEN **:** Ronal Moen, Foundation and History of PDCA Cycle: https://deming.org/uploads/paper/PDSA_History_Ron_Moen.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

NYAMTIGA/SAM/LAZIER **:** Baraka W. Nyamtiga/Anael Sam/Loserian S. Laizer, Security Perspectives For USSD Versus SMS In Conducting Mobile Transactions: A Case Study Of Tanzania, International Journal of Technology Enhancements And Emerging Engineerıng Research, C: 1, Sayı 3/38 ISSN 2347-4289: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/Security-Perspectives-For-Ussd-Versus-Sms-In-Conducting-Mobile-Transactions-A-Case-Study-Of-Tanzania%20(1).pdf (Gözden Geçirilme Tarihi: 29.10.2020).

OKUL VE DİĞERLERİ **:** Turan Okul/Güntekin Şimşek/Büşra Hafçı/Zafer Barış, Konaklama İşletmesi Yöneticilerinde Bilgi Güvenliği Farkındalığı: Kuşadası'ndaki Beş Yıldızlı Oteller Örneği: https://dergipark.org.tr/tr/download/article-file/604273 (Gözden Geçirilme Tarihi: 29.10.2020).

ÖNEY/ÖKSÜZOĞLU/RIZVI **:** Emrah Öney/Gizem Öksüzoğlu Güven/Wajid Hussain Rizvi, The determinations of electronic payment systems usage from consumers' perspective, Routledge Economic Research: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/Thedeterminantsofelectronicpaymentsystemsusagefromconsumersperspective.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

PEI WANG **:** Pei Wang, What Do You Mean by "AI"?:

file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/What_Do_You_Mean_by_AI.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

PERNIK VE DİĞERLERİ : Piret Pernik/Jesse Wojtkowiak/Alexander Verschoor-Kirss, National Cyber Security Organisation: United States, NATO Cooperative Cyber Defence Center of Excellence, Talinn, 2016: https://ccdcoe.org/uploads/2018/10/CS_organisation_USA_122015.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

PETROVA : Krassie Petrova, Auckland University of Technology, Mobile Banking: Background, Services, Adoption: https://www.academia.edu/3334874/MOBILE_BANKING_BACKGROUND_SERVICES_AND_ADOPTION?auto=download (Gözden Geçirilme Tarihi: 29.10.2020).

RODRÍGUEZ/ GUTİÉRREZ : Martín Steven Bedoya Rodríguez, Jhon Hegel Gutiérrez, An Overview of Cybersecurity for Mobile Banking Applications: https://medium.com/@everisUS/an-overview-of-cybersecurity-for-mobile-banking-applications-e4e99dff5061(Gözden Geçirilme Tarihi: 29.10.2020).

SAGAR : Ram Sagar, 25 Years Of QR Codes: A Look At Vulnerabilities Of This Popular Payment Method": https://analyticsindiamag.com/25-years-of-qr-codes-a-look-at-vulnerabilities-of-this-popular-payment-method/ (Gözden Geçirilme Tarihi: 29.10.2020).

SCHEIDER : Fred B. Schneider, Least Privilege And More, Cornell University, ABD: https://www.cs.cornell.edu/fbs/publications/leastPrivNeedham.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

SCHNEIER **:** Bruce Schneier, There's No Good Reason to Trust Blockchain Technology, Wired: https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/ (Gözden Geçirilme Tarihi: 29.10.2020).

SHAMIR **:** Adi Shamir, How to Share a Secret: https://cs.jhu.edu/~sdoshi/crypto/papers/shamirturing.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

SOYSAL **:** Tamer Soysal, Unutulma Hakkının Avrupa Birliği'nin Genel Veri Koruma Tüzüğü Çerçevesinde Değerlendirilmesi: https://dergipark.org.tr/en/download/article-file/742611 (Gözden Geçirilme Tarihi: 29.10.2020).

T.C. Cumhurbaşkanlığı Strateji Dijital Dönüşüm Dairesi, Bilgi Ve İletişim Güvenliği Rehberi: https://cbddo.gov.tr/SharedFolderServer/Genel/File/BG_REHBER.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

SSI EIDAS HUKUK RAPORU **:** Ignacio Alamillo Domingo, SSI eIDAS Legal Report How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market: https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

ŞENTÜRK **:** Mustafa Yasir Şentürk, Güncel Siber Saldırı Yöntemleri, Sızma Testi Araçları Ve Temsili Kurumsal Bir Ağ Üzerinde Kullanılması, Türk Hava Kurumu Üniversitesi Fen Bilimleri Enstitüsü, Elektrik Ve Bilgisayar Mühendisliği Anabilim Dalı, Eylül 2018: https://afyonluoglu.org/PublicWebFiles/Reports-

TR/Akademi/2018_Mustafa%20Yasir%20Sent%C3%BCrk_G%C3%BCncel%20siber%20sald%C4%B1r%C4%B1%20y%C3%B6ntemleri.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

TAHEERDOOST VE DİĞERLERİ : Hamed Taheerdoost/Shamsul Sahibuddin/Neda Jalaliyoon, Smart Card Security, Technology and Adoption, International Journal of Security (IJS), C. 5, S. 2, 2011: https://www.cscjournals.org/manuscript/Journals/IJS/Volume5/Issue2/IJS-84.pdf

TBB : Türkiye Bankalar Birliği, Bankacılıkta Dolandırıcılık Eylemleri Tespit Ve Önleme Yöntemleri, Ekim 2015: https://www.tbb.org.tr/gec/KTPV14.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

TECHNICAL NOTE : Carneige Mellon University, Technical Note, Eylül 2015: file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/15tn007.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

TUĞSAN YILMAZ : Tuğsan Yılmaz, İnternet Bankacılığı İle Yapılan Dolandırıcılık: http://www.tugsanyilmaz.av.tr/fikri-haklar-ve-bilisim-hukuku/internet-bankaciligi-ile-yapilan-dolandiricilik (Gözden Geçirilme Tarihi: 29.10.2020).

URS : Bogdan-Alexandru Urs, Security Issues And Solutions In A E-Payment Systems, Fiat Iustatia, No:1, 2015: http://oaji.net/articles/2016/2064-1452602042.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

YEŞİLYURT **:** Hamdi Yeşilyurt, Finansal Hizmet Sektöründe Siber Güvenlik Riskleri Ve Çözüm Yolları: Ödeme Sistemleri Ve Tedarik Zinciri Bütünlüğü: https://www.academia.edu/22347134/Finansal_Hizmet_Sektöründe_Siber_Güvenlik_Riskleri_ve_Çözüm_Yolları_Ödeme_Sistemleri_ve_Tedarik_Zinciri_Bütünlüğü (Gözden Geçirilme Tarihi: 29.10.2020).

YILMAZ **:** Hasan Yılmaz, TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması Ve Bilgi Güvenliği Risk Analizi, Kidder, Denetişim /2014-15: https://dergipark.org.tr/en/pub/denetisim/issue/22466/240291 (Gözden Geçirilme Tarihi: 29.10.2020).

ZECOPS **:** Zecops Araştırma Grubu, 20.04.2020 Tarihli Raporu: https://blog.zecops.com/vulnerabilities/youve-got-0-click-mail/ (Gözden Geçirilme Tarihi: 29.10.2020).

ZENGİN/GÜNGÖRDÜ **:** Burcu Zengin, Aybegüm Güngördü, Elektronik Ödeme Sistemlerinin Olası Etkileri Üzerine Bir İnceleme, Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 15/3 (2013) 129-150: http://dergipark.org.tr/en/download/article-file/287247 (Gözden Geçirilme Tarihi: 29.10.2020).

ZEYTİN/GENÇAY **:** Zafer Zeytin/Eray Gençay, Hukuk Ve Yapay Zeka: E-Kişi, Mali Sorumluluk Ve Bir Hukuk Uygulaması, TAÜHFD/ZtdR- 2019/1 (Gözden Geçirilme Tarihi: 29.10.2020).

TEZ KAPSAMINDA İNCELENEN DİĞER LİNKLER:

https://www.kuveytturk.com.tr/kobi/kartlar-ve-pos/pos-hizmetleri/sanal-pos (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.pwc.com.tr/tr/sektorler/bankacilik/pdf/acik-bankacilik-dunya-ve-turkiye-v2.pdf. (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.wired.com/story/attack-on-ethereum-currency-highlights-crypto-weakness/ (Gözden Geçirilme Tarihi: 29.10.2020).

file:///C:/Users/Durmu%C5%9F%20CEVLAN/Desktop/Endustri-4.0-Surecinde-Bilgi-Yonetimi-ve.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

https://cabforum.org/about-ev-ssl/ (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.resmigazete.gov.tr/eskiler/2019/11/20191122-2.htm (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.resmigazete.gov.tr/eskiler/2020/06/20200626-1.htm (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=19816&MevzuatTur=7&MevzuatTertip=5 (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.resmigazete.gov.tr/eskiler/2020/08/20200821-4.htm (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.resmigazete.gov.tr/eskiler/2020/08/20200821-4-1.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.resmigazete.gov.tr/eskiler/2020/03/20200315-10.htm (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.resmigazete.gov.tr/eskiler/2020/06/20200620-1.htm (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.resmigazete.gov.tr/eskiler/2014/02/20140219-1.htm (Gözden Geçirilme Tarihi: 29.10.2020).
http://kararlaryeni.anayasa.gov.tr/Karar/Content/514c3cc8-6566-4874-a7da-bd28897a04ae?excludeGerekce=False&wordsOnly=False (Gözden Geçirilme Tarihi: 29.10.2020).

https://blog.lexpera.com.tr/2019-turkiye-kisisel-verilerin-korunmasi/ (Gözden Geçirilme Tarihi: 29.10.2020).

https://www2.tbmm.gov.tr/d27/2/2-2945.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5070.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

http://kamusm.bilgem.tubitak.gov.tr/BilgiDeposu/KSM_ZDUE/YON.01.02_02_KAMU_SM_ZAMAN_DAMGASI_UYGULAMA_ESASLARI.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.resmigazete.gov.tr/eskiler/2007/10/20071024-12.htm (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.resmigazete.gov.tr/eskiler/2017/04/20170411-3.htm (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.resmigazete.gov.tr/eskiler/2020/07/20200731.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.rskveri.com/kisisel-verileri-koruma-kurulunun-31-05-2018-tarihli-ve-2018-63-sayili-ilke-kararinin-kvkk-gdpr-ve-alman-hukuku-isiginda-degerlendirilmesi/ (Gözden Geçirilme Tarihi: 29.10.2020).

https://kvkk.gov.tr/Icerik/6739/2020-173 (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim (Gözden Geçirilme Tarihi: 29.10.2020).

https://siberbulten.com/siber-guvenlik/kisisel-verileri-koruma-kurumunun-karar-ozeti-ortaligi-karistirdi/#3_Kurum_guvenli_ulkeler_listesi_yayinlamali (Gözden Geçirilme Tarihi: 29.10.2020).

http://www.kazanci.com/kho2/ibb/giris.html (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.kvkk.gov.tr/Icerik/5537/2019-255 (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.kvkk.gov.tr/Icerik/6656/2019-352 (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.tbd.org.tr/ulusal-bilgi-guvenligi-teskilati-ve-gorevleri-hakkinda-kanun-tasarisi/ (Gözden Geçirilme Tarihi: 29.10.2020).

https://mevzuat.gov.tr/mevzuat?MevzuatNo=5411&MevzuatTur=1&MevzuatTertip=5 (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.resmigazete.gov.tr/eskiler/2020/03/20200315-10.htm (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.resmigazete.gov.tr/eskiler/2020/03/20200315-10.htm (Gözden Geçirilme Tarihi: 29.10.2020).

https://mevzuat.gov.tr/mevzuat?MevzuatNo=2837&MevzuatTur=21&MevzuatTertip=5 (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.resmigazete.gov.tr/eskiler/2020/06/20200626-1.htm (Gözden Geçirilme Tarihi: 29.10.2020).

http://www.sbb.gov.tr/wp-content/uploads/2019/07/OnbirinciKalkinmaPlani.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

https://bilgiguvenligi.org.tr (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.bilgiguvenligi.org.tr/wp-content/uploads/2016/03/Ulusal_Siber_Guvenlik_Stratejisi.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.uab.gov.tr/uploads/pages/siber-guvenlik/some-bkk.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.uab.gov.tr/uploads/pages/siber-guvenlik/some-teblig.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.btk.gov.tr/siber-guvenlik-stratejisi-ve-eylem-plani (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.btk.gov.tr/haberler/2020-2023-siber-guvenlik-stratejileri-btk-da-belirlendi (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.memurlar.net/haber/910508/siber-vatan-cumhurbaskani-erdogan-dikkat-cekmisti.html (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.tbmm.gov.tr/tutanaklar/TUTANAK/TBMM/d22/c113/tbmm22113072ss1078.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.resmigazete.gov.tr/eskiler/2020/02/20200225-12.htm (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.justsecurity.org/69119/the-defense-departments-measured-take-on-international-law-in-cyberspace/ (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.paypal.com/np/webapps/mpp/pay-with-app#:~:text=PayPal%20is%20accepted%20on%20thousands,financial%20information%20with%20the%20seller.&text=Shop%20online%20or%20in%20apps%20using%20your%20mobile.&text=Choose%20PayPal%20as%20the%20payment%20method. (Gözden Geçirilme Tarihi: 29.10.2020).

https://squareup.com/guides/mobile-payments?country_redirection=true (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.seamlesspay.com/ (Gözden Geçirilme Tarihi: 29.10.2020).

https://venmo.com/ (Gözden Geçirilme Tarihi: 29.10.2020).

https://archive.is/20130124212125/http://gopago.com/live (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.dwolla.com/ (Gözden Geçirilme Tarihi: 29.10.2020).

http://www.netcheque.org/gost.info/netcheque (Gözden Geçirilme Tarihi: 29.10.2020).

http://www.onlinecheck.com/mag.html (Gözden Geçirilme Tarihi: 29.10.2020).

http://www.netbill.com (Gözden Geçirilme Tarihi: 29.10.2020).

http://www.netchex.com (Gözden Geçirilme Tarihi: 29.10.2020).

http://www.check-free.com (Gözden Geçirilme Tarihi: 29.10.2020).

https://fpf.org/2020/11/04/understanding-blockchain-a-review-of-fpfs-oct-29th-digital-data-flows-masterclass/ (Gözden Geçirilme Tarihi: 29.10.2020).

https://ec.europa.eu/info/business-economy-euro/banking-and-finance/consumer-finance-and-payments/payment-services/single-euro-payments-area-sepa_en (Gözden Geçirilme Tarihi: 29.10.2020).

https://ec.europa.eu/info/law/single-euro-payments-area-regulation-eu-260-2012_en (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.intell4.com/cinin-siber-guvenlik-yasasi-gelecege-ne-diyor-haber-182701 (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.law.cornell.edu/uscode/text/5/552a (Gözden Geçirilme Tarihi: 29.10.2020).

https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.tcmb.gov.tr/wps/wcm/connect/73289f67-d210-4f49-8902-6e14ecae055d/OdemeSistemleri.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE-73289f67-d210-4f49-8902-6e14ecae055d-m5lk6L- (Gözden Geçirilme Tarihi: 29.10.2020).

http://www.digitaljournal.com/news/politics/us-special-envoy-to-iran-tries-to-force-eu-to-follow-us-sanctions/article/553066 (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain

https://www.fintechmagazine.com/fintech/how-technology-changing-financial-messaging#:~:text=As%20of%202018%2C%20it%20was,worldwide%20used%20the%20SWIFT%20network.&text=SWIFT%2C%20which%20stands%20for%20the,Telecommunication%2C%20is%20headquartered%20in%20Belgium. (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.ft.com/content/631af8cc-47cc-11e8-8c77-ff51caedcde6 (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.e-ma.org/ (Gözden Geçirilme Tarihi: 29.10.2020).

file:///C:/Users/Durmu%C5%9F%20CEVLAN/Downloads/FrameworkUsingCyberInsurance.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.enisa.europa.eu/about-enisa (Gözden Geçirilme Tarihi: 29.10.2020).

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN (Gözden Geçirilme Tarihi: 29.10.2020).

https://afyonluoglu.org/PublicWebFiles/cyber/legislation/2001-Avrupa%20Birliği%20Siber%20Suçlar%20Sözleşmesi-TR.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN(Gözden Geçirilme Tarihi: 29.10.2020).

https://gdpr-info.eu/ (Gözden Geçirilme Tarihi: 29.10.2020).

https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive (Gözden Geçirilme Tarihi: 29.10.2020).

https://eur-lex.europa.eu/resource.html?uri=cellar:d829f91d-9859-11e7-b92d-01aa75ed71a1.0001.02/DOC_3&format=PDF (Gözden Geçirilme Tarihi: 29.10.2020).

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity (Gözden Geçirilme Tarihi: 29.10.2020).

https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-202020132022 (Gözden Geçirilme Tarihi: 29.10.2020).

https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-2019-2021(Gözden Geçirilme Tarihi: 29.10.2020).

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (Gözden Geçirilme Tarihi: 29.10.2020).

https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52017PC0010 (Gözden Geçirilme Tarihi: 29.10.2020).

https://ec.europa.eu/futurium/en/system/files/ged/eidas_supported_ssi_may_2019_0.pdf (Gözden Geçirilme Tarihi: 29.10.2020).

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN (Gözden Geçirilme Tarihi: 29.10.2020).

https://tr.wikiquote.org/wiki/Sun_Tzu (Gözden Geçirilme Tarihi: 29.10.2020).