



T.C.

EGE ÜNİVERSİTESİ

Sosyal Bilimler Enstitüsü

**İŞLETMELERİN DİJİTALLEŞME SÜRECİNDE SİBER GÜVENLİK:
SOSYAL AĞ ANALİZİNE DAYALI HAZIR BULUNUŞLUK
ÖLÇEĞİNİN GELİŞTİRİLMESİ**

Yüksek Lisans Tezi

Büşra HİDİROĞLU

İşletme Anabilim Dalı

İZMİR 2023

T.C.

EGE ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü

İŞLETMELERİN DİJİTALLEŞME SÜRECİNDE SİBER GÜVENLİK:
SOSYAL AĞ ANALİZİNE DAYALI HAZIR BULUNUŞLUK
ÖLÇEĞİNİN GELİŞTİRİLMESİ

Yüksek Lisans Tezi

Büşra HİDİROĞLU

Tez Danışmanı: Doç. Dr. HAYDAR YALÇIN

İşletme Anabilim Dalı Pazarlama

Yüksek Lisans Programı

ETİK KURALLARA UYGUNLUK BEYANI

Ege Üniversitesi Sosyal Bilimler Enstitüsü Müdürlüğüne sunduğum “İşletmelerin Dijitalleşme Sürecinde Siber Güvenlik: Sosyal Ağ Analizine Dayalı Hazır Bulunuşluk Ölçeğinin Geliştirilmesi” adlı yüksek lisans tezinin tarafımdan bilimsel, ahlak ve normlara uygun bir şekilde hazırlandığını, tezimde yararlandığım kaynakları bibliyografyada ve dipnotlarda gösterdiğimi onurumla doğrularım.

Büşra HIDIROĞLU

Önsöz

"John Chambers'ın (Cisco Systems'ın eski yönetim kurulu başkanı ve CEO'su) ünlü bir sözünde dediği gibi, 'Yalnızca iki tür kuruluş vardır: Saldırıya uğrayanlar ve henüz bunu bilmeyenler!'"

Bu çalışma ile siber güvenlik alanında işletmelere ve müşterilere rehber olacak bilgilerin sunulması, yapılan sosyal ağ analizi ile siber güvenlik alanındaki öne çıkan konu ve kavramların belirlenmesi, hazırbulunuşluk ölçeğinin sosyal ağ analizinden elde edilen verilere göre geliştirilmesi, işletmelerin olası siber saldırılara hazırlıklı olması için hazırbulunuşluk ölçeğinin hazırlanması amaçlanmıştır. Amacımı gerçekleştirip çalışmamı tamamlayabilmek için birçok kişinin desteği ve katkıları mevcuttur. Desteklerini ve katkılarını esirgemeyen aileme, arkadaşlarıma, profesyonel bilgi birikimi ile ufukumu açarak beni yönlendiren danışmanım Sayın Doç. Dr. Haydar YALÇIN'a, öğrenim dönemim boyunca engin bilgilerini benimle paylaşan çok değerli öğretmenlerime, sorularıma yanıt veren siber güvenlik uzmanlarına, ankete zaman ayırıp katılan işletmelere çok teşekkür ederim.

Büşra HİDİROĞLU

İZMİR, 2023

Özet

Abraham Maslow tarafından geliştirilen bir insan psikolojisi teorisi olan “Maslow'un ihtiyaçlar hiyerarşisi”ne göre “güvenlik gereksinimi” temel “fizyolojik ihtiyaçlar”dan sonra ikinci sırada yer almaktadır. Tıpkı “Maslow'un ihtiyaçlar hiyerarşisi”ndeki gibi, işletmeler de yaşam döngülerini sürdürmek için temel ihtiyaçlarını karşıladıktan sonra “güvenlik gereksinimi”ni sağlamak zorundadır. Güvenlik gereksinimi karşılanmadan işletmeler iç ve dış çevrelerine karşı ait olma, saygı ve kendini gerçekleştirme seviyelerine ulaşamazlar. İşletmenin güvenliği sağlaması gereken alanlardan biri de siber dünyadır. “Siber güvenlik” olarak karşımıza çıkan bu kavram her geçen gün büyüyüp farklılaşma yaşayan teknolojiyle hayatımıza daha fazla entegre olmuş ve gelişmelerin beraberinde getirdiği risklere karşı daha güçlü olmayı zorunlu kılmıştır. Siber dünyada yer alan her ölçekteki işletme ise bu risklere karşı hazır durumda bulunmalıdır.

Bu çalışmanın literatür bölümünde siber güvenlik kavramı ile ilgili; etimolojik geçmişe bakılmış, kavramın önemi açıklanmış, yaşanan gizlilik & güvenlik sorunlarına değinilmiş, yaşanan sorunlar işletmeler ve müşteriler açısından incelenmiş, siber güvenlikteki başarının ve siber güvenliğin dijitalleşme süreçlerindeki önemi hakkında bilgi verilmiştir. Metodoloji bölümünün ilk aşamasında sosyal ağ analizi yöntemiyle yazarlar, kurumlar ve kavramlar arası ilişkiler ortaya konulmuş ve bilimsel haritalama ile ortaya çıkarılan ağ ilişkileri görselleştirilmiştir. Metodolojinin ikinci aşamasında ise “Marka ve Siber Güvenlik”, “Operasyonel Siber Güvenlik”, “İç Ağ Güvenliği”, “Web Uygulamaları Güvenliği” ve “Son Kullanıcı Eğitimi” başlıkları kapsamında “Sosyal Ağ Analizine Dayalı Hazırbulunusluk Ölçeği” hazırlanmıştır. Nicel yöntem esas alınarak veri toplama yöntemlerinden anket seçilmiştir. Anketteki ilk dört soru işletmeye dair genel bilgileri öğrenmeye yönelik iken beşinci soru 5’li Likert ölçeği kullanılarak oluşturulan 150 maddelik bir havuzdan meydana gelmiştir. Uzmanlar tarafından yapılan incelemeler sonucu madde sayısı 55 olarak güncellenmiştir. Ölçek uyarlama veya geliştirme süreçlerinde Açıklayıcı Faktör Analizi (AFA) ve Doğrulamalı Faktör Analizi (DFA) tekniklerden faydalanılmıştır. Açıklayıcı faktör analizinde ölçeğin yapı geçerliğini test etmek için temel

eksen faktör ve promaks döndürme kullanılmıştır. Açımlayıcı faktör analizi sonrası 26 madde çıkarılmıştır. Madde havuzunda işlem sonrası 29 madde kalmıştır. Alt boyutların geçerliliğini göstermek üzere doğrulayıcı faktör analizi uygulanmış olup uyum indekslerine bakıldığında faktörlerin geçerli bir yapıya sahip olduğu tespit edilmiştir. Geliştirilen ölçek ile işletmelerin siber güvenlik önlemleri gözden geçirilerek işletmelerin bu alandaki faaliyetleri artırılabilir ve olası siber saldırılara karşı hazırbulunuşlukları belli bir oranda sağlanabilir.

Anahtar Kelimeler: Siber güvenlik, Dijitalleşme, Dijital pazarlama, Hazır bulunuşluk ölçeği, Siber saldırı, Siber tehlike, Veri güvenliği, Teknolojik gelişme



Abstract

According to “Maslow's hierarchy of needs”, which is a theory of human psychology developed by Abraham Maslow, “security needs” take the second place after basic “physiological needs”. Just like in "Maslow's hierarchy of needs", businesses have to provide "security needs" after meeting basic needs in order to maintain their life cycle. Businesses cannot reach the level of belonging, respect and self-actualization towards their internal and external environments without meeting the security requirement. One of the areas where the business must ensure security is the cyber world. This concept, which appears as "cyber security", has become more integrated into our lives with technology that grows and differentiates day by day, and it has made it necessary to be stronger against the risks brought by the developments. Businesses of all sizes in the cyber world should be prepared for these risks.

In the literature section of this study, about the concept of cyber security; The etymological background was examined, the importance of the concept was explained, the privacy & security problems were mentioned, the problems experienced were examined in terms of businesses and customers, information was given about the success in cyber security and the importance of cyber security in marketing processes. In the first stage of the methodology section, the relationships between authors, institutions and concepts were revealed by the social network analysis method and the network relationships that emerged with scientific mapping were visualized. In the second stage of the methodology, “Readiness Scale Based on Social Network Analysis” was prepared under the headings of “Information Security”, “Application Security”, “Network Security”, “Operational Security” and “Digital Brand Protection”. Based on the quantitative method, a questionnaire was chosen from the data collection methods. While the first four questions in the questionnaire were aimed at learning general information about the business, the fifth question in the first stage consisted of a pool of 150 items created using a 5-point Likert scale. As a result of the examinations made by the experts, the number of items

was updated as 55. Exploratory Factor Analysis (EFA) and Confirmatory Factor Analysis (CFA) techniques were used in the scale adaptation or development processes. In exploratory factor analysis, principal axis factor and promax rotation were used to test the construct validity of the scale. After the exploratory factor analysis, 26 items were removed. There were 29 items left in the item pool after the transaction. Confirmatory factor analysis was applied to show the validity of the sub-dimensions, and when the fit indices were examined, it was determined that the factors had a valid structure. With the developed scale, the cyber security measures of the enterprises can be reviewed, and the activities of the enterprises in this area can be increased and their readiness against possible cyber attacks can be ensured to a certain extent.

Keywords: Cyber security, Digitalization, Digital marketing, Readiness scale, Cyber attack, Cyber danger, Data security, Technological development

İçindekiler

ÖNSÖZ.....	i
ÖZET.....	ii
ABSTRACT.....	iv
İÇİNDEKİLER.....	vi
TABLolar LİSTESİ.....	x
ŞEKİLLER LİSTESİ.....	xi
GRAFİKLER LİSTESİ.....	xii
KISALTMALAR.....	xiii
GİRİŞ.....	1
BİRİNCİ BÖLÜM.....	2
1. SİBER GÜVENLİĞİN TANIMI VE DİJİTAL DÖNÜŞÜMDEKİ ÖNEMİ	2
1.1. SİBER KAVRAMININ TANIMI.....	2
1.2. İŞLETMELERİN DİJİTALLEŞME SÜRECİ VE SİBER GÜVENLİK.....	4
1.2.1. Birleşme ve Satın Almalar	8
İKİNCİ BÖLÜM	11
2. DİJİTAL ORTAMDA GİZLİLİK VE GÜVENLİK ENDİŞELERİ	11
2.1. İŞLETMELERİN DİJİTALLEŞMESİ VE SİBER GÜVENLİK	11
2.1.1. Veri İhlalleri	12
2.1.1.1. Dijital Ayak İzi	14
2.2. DİJİTAL ORTAMDA GERÇEKLEŞEN BAZI GİZLİLİK VE GÜVENLİK SORUNLARI.....	15
2.2.1. Ortadaki Adam Saldırısı (MITM)	15
2.2.2. Bait ve Switch	17
2.2.3. Truva Atı.....	18
2.2.4. Keylogger	19
ÜÇÜNCÜ BÖLÜM	21
3. DİJİTAL PAZARLAMA VE SİBER GÜVENLİK TEHDİTLERİ.....	21
3.1. DİJİTAL ORTAMDA İŞLETMELER İÇİN SİBER GÜVENLİK TEHDİTLERİ	21
3.1.1. Hybrid Çalışma ve Kendi Cihazını Getir Uygulaması (BYOD)	25
3.1.2. İş E-Postası Uzlaşması	25

3.1.2. Deepfake.....	27
3.1.2.1. Deepfake Saldırı Örnekleri	28
3.1.3.2. Endüstri 4.0 Teknolojisi ve Tedarik Zinciri	32
3.1.3.3. Endüstri 4.0 Teknolojisi ve Radyo Frekansı ile Tanımlama (RFID)	33
3.1.3.4. Endüstri 4.0 Teknolojisi ve Dijital İkiz.....	34
3.1.4. Küresel Misli Olmayan Tokenlar (NFT).....	35
3.1.4.1. Web 3 ve Dapp	36
3.1.4.2. Küresel Misli Olmayan Tokenlar (NFT) ve Metaverse	36
3.1.5. Endüstriyel Casusluk	37
3.1.6. Siber Zorbalık.....	38
3.2. DİJİTAL ORTAMDA MÜŞTERİLER İÇİN SİBER GÜVENLİK TEHDİTLERİ	39
3.2.1. Kimlik Hırsızlığı	40
3.2.2. NFT Pazaryerleri	42
3.2.3. Veri Simsarları	45
3.2.4. Geofencing	45
DÖRDÜNCÜ BÖLÜM	47
4. SİBER GÜVENLİKTEKİ BAŞARININ İŞLETMELERDEKİ ETKİSİ.....	47
4.1. SİBER SİGORTA	47
4.2. SİBER DAYANIKLILIK.....	49
4.3. SİBER TEHDİT İSTİHBARATI	49
4.4. DIŞ KAYNAK KULLANIMI	50
BEŞİNCİ BÖLÜM.....	51
5. İŞLETMELERİN DİJİTAL PAZARLAMA FAALİYETLERİNDE SİBER..	51
GÜVENLİĞİN YERİ	51
5.1. E-POSTA PAZARLAMASI.....	51
5.2. E-CRM	51
5.3. WORDPRESS	52
5.4. ARAMA MOTORU OPTİMİZASYONU (SEO).....	53
5.4.1. SEO Zehirlenmesi	53
5.6. E-SKIMMING (MAGECART SALDIRILARI).....	55
5.7. KİTLE KAYNAK KULLANIMI	56
5.7. SATIŞ ORTAKLIĞI.....	57

ALTINCI BÖLÜM	59
6. SOSYAL AĞ ANALİZİNE VE BİBLİYOMETRİK HARİTALAMAYA İLİŞKİN ANALİZLER	59
6.1. SİBER GÜVENLİK KONULU YAYINLARIN ÜLKELERE GÖRE YAYIN SAYISI	60
6.2. SİBER GÜVENLİK KONULU YAYINLARIN DÜNYA GENELİNDE YILLARA GÖRE YAYIN SAYILARI	62
6.3. SİBER GÜVENLİK KONULU YAYINLARIN TÜRKİYE' DE DÜNYA GENELİNDE YILLARA GÖRE YAYIN SAYILARI	63
6.4. SİBER GÜVENLİK KONULU YAYINLARDA EN ÜRETKEN YAZARLAR ..	64
6.5. SİBER GÜVENLİK KONULU YAYINLARDA TÜRKİYE'DEKİ EN ÜRETKEN YAZARLAR	65
6.6. SİBER GÜVENLİK KONULU YAYINLARIN ARAŞTIRMA ALANINA GÖRE DAĞILIMI	66
6.7. SİBER GÜVENLİK KONULU YAYINLARIN TÜRKİYE'DE ARAŞTIRMA ALANINA GÖRE DAĞILIMI	68
6.8. SİBER GÜVENLİK KONULU YAYINLARIN KURUMLARA GÖRE DAĞILIMI	71
6.9. SİBER GÜVENLİK KONULU YAYINLARIN TÜRKİYE'DE KURUMLARA GÖRE DAĞILIMI	72
6.10. SİBER GÜVENLİK KONULU YAYINLARIN YAYINCILARINA GÖRE DAĞILIMI	73
6.11. TÜRK ARAŞTIRMACILARIN SİBER GÜVENLİK KONULU YAYINLARININ YAYINCILARA GÖRE DAĞILIMI	74
6.12. SİBER GÜVENLİK KONULU YAYINLARDA ANAHTAR KELİMELERİN DAĞILIMI	77
6.13. SİBER GÜVENLİK KONULU YAYINLARDA TÜRKİYE'DE ANAHTAR KELİMELERİN DAĞILIMI	79
6.14. SİBER GÜVENLİK KONULU YAYINLARDA SOSYAL BİLİMLER ALANINDA ANAHTAR KELİMELERİN DAĞILIMI	81
6.15. SİBER GÜVENLİK KONULU YAYINLARDA SOSYAL BİLİMLER ALANINDA TÜRKİYE'DEKİ ANAHTAR KELİMELERİN DAĞILIMI	83
6.16. SİBER GÜVENLİK KAVRAMININ DEĞERLENDİRİLMESİNDE HAZIRBULUNUŞLUK ÖLÇEĞİ VE BİBLİYOMETRİK AĞ ANALİZİ YÖNTEMLERİNİN KULLANIMI: BİR SİSTEMATİK DERLEME	84
YEDİNCİ BÖLÜM	86
7. SOSYAL AĞ ANALİZİNE DAYALI HAZIRBULUNUŞLUK ÖLÇEĞİNİN GELİŞTİRİLMESİ	86

7.1. ARAŞTIRMANIN AMACI.....	86
7.2. ARAŞTIRMANIN ÖNEMİ.....	86
7.3. ARAŞTIRMANIN SINIRLILIKLARI.....	87
7.4. METODOLOJİ.....	87
7.4.1. Veri Toplama Yöntem ve Araçları.....	87
7.4.2. Verilerin Analizi.....	87
7.4.3. Araştırma Deseni.....	88
7.4.4. Ölçek Geliştirme Süreci.....	88
7.5. HAZIRBULUNUŞLUK ÖLÇEĞİ BULGULARI.....	89
7.5.1. Katılımcı Bilgileri.....	89
7.5.2. İşletme Bilgileri.....	90
7.6. BETİMSSEL İSTATİSTİKLER ANALİZİ.....	94
7.6.1. Örneklem Büyüklüğü.....	95
7.6.2. Korelasyon Matrisi.....	97
7.7. BİRİNCİ AŞAMA AÇIMLAYICI FAKTÖR ANALİZİ.....	98
7.7.1. Model-Veri Uyum İndeksleri.....	100
7.8. YAPI GEÇERLİĞİ: DOĞRULAYICI FAKTÖR ANALİZİ.....	101
SONUÇ.....	106
KAYNAKÇA.....	110
EKLER.....	129
Ek 1.....	129

Tablolar Listesi

Tablo 1. Siber Güvenlik Sorunlarının Birleşme ve Satın Almalarda Etkisi	8
Tablo 2. 5G Altyapılarına Yönelik Potansiyel Tehdit Vektörleri.....	32
Tablo 3. NFT'ye Özgü Pazarlama Sonuçları	44
Tablo 4. Ölçek Geliştirme Süreci	88
Tablo 5. Ülkelere Göre Yayın Sayısı (İlk 25 Ülke).....	61
Tablo 6. Dünya Geneline Yıllara Göre Yayın Sayıları.....	62
Tablo 7. Türkiye’ de Yıllara Göre Yayın Sayıları.....	63
Tablo 8. En Üretken Yazarlar.....	64
Tablo 9. Türkiye’deki En Üretken Yazarlar	65
Tablo 10. Dünya Geneline Araştırma Alanına Göre Dağılım	66
Tablo 11. Türkiye’de Araştırma Alanına Göre Dağılım	68
Tablo 12. Yayınların Yayıncılara Göre Analizi	73
Tablo 13. Türk Araştırmacılar Tarafından Yayımlanan Yayınların Yayıncılara Göre Analizi	74
Tablo 14. İşletmelerin Sektörleri	94
Tablo 15. KMO ve Barlett’s Sphericity Testi Sonuçları	96
Tablo 16. Maddelerin KMO Testi Sonuçları.....	96
Tablo 17. Birinci Aşama Açıklayıcı Faktör Analizi Sonrası Ölçek Maddelerinin KMO Testi Sonuçları	98
Tablo 18. Birinci Aşama Açıklayıcı Faktör Analizi Sonrası Bartlett'in Küresellik Testi Sonuçları	99
Tablo 19. Birinci Aşama Açıklayıcı Faktör Analizi Sonrası Varyans Açıklama Oranları	99
Tablo 20. Model Uyum Ölçüleri	100
Tablo 21. Tam Uyum Testi.....	101
Tablo 22. Uygunluk Ölçüleri.....	101
Tablo 23. Faktör Yükleri	102
Tablo 24. Faktör Kovaryansları.....	104
Tablo 25. Güvenirlik Analizi.....	104

Şekiller Listesi

Şekil 1. MITM Saldırısı	16
Şekil 2. Yayın Sayısına Göre İlk 25 Ülke.....	60
Şekil 3. Yayınların Kurumlara Göre Bibliyometrik Ağ Analiz	71
Şekil 4. Türkiye’de Yayınların Kurumlara Göre Bibliyometrik Ağ Analizi	72
Şekil 5. Siber Güvenlik Konulu Araştırmalarda Kullanılan Anahtar Kelimeler	77
Şekil 6. Türkiye’de Kullanılan Anahtar Kelimeler.....	79
Şekil 7. Sosyal Bilimler Alanında Kullanılan Anahtar Kelimeler	81
Şekil 8. Sosyal Bilimler Alanında Türkiye’de Kullanılan Anahtar Kelimeler	83



Grafikler Listesi

Grafik 1. İşletme Ölçeğine göre Siber Güvenlik Uzmanlarının Dağılımı	89
Grafik 2. İşletmelerde Çalışan Personel Sayısının Pasta Grafiği ile Gösterilmesi	90
Grafik 3. İşletmelerin Net Satış Hasılatının Daire Pasta ile Gösterilmesi	91
Grafik 4. İşletmelerin Yıllık Mali Bilanço Toplamı	92
Grafik 5. İşletmelerin Sektörleri	93



Kısaltmalar

AI: Yapay Zekâ

API: Uygulama Programlama Arayüzü

AR: Artırılmış Gerçeklik

BEC/ EAC: İş E-Postası Uzlaşması/ E-posta Hesabı Uzlaşması

BIMI: Mesaj Tanımlama için Marka Göstergeleri

BM: İş Modelleri

BT: Bilgi Teknolojisi

BYOD: Kendi Cihazını Getir Uygulaması

C2: Komut ve Kontrol

CIAB: Sigorta Acenteleri ve Brokerleri Konseyi

CISA: Siber Güvenlik ve Altyapı Güvenliği Ajansı

CMS: İçerik Yönetim Sistemi

CPR: Check Point (BT güvenliği sağlayan çokuluslu şirket) Araştırması

CPS: Siber Fiziksel Sistemler

CRM: Müşteri İlişkileri Yönetimi

C-SCRM: Siber Güvenlik Tedarik Zinciri Risk Yönetimi

CTI: Siber Tehdit İstihbaratı

DAO: Merkezi Olmayan Otonom Organizasyon

Dapp: Merkezi Olmayan Bir Uygulama

DDoS: Dağıtılmış Hizmet Reddi

DeFi: Merkezi Olmayan Uçtan Uca Finansal Hizmetler için Kullanılan Şemsiye Terim

DHS: Amerika Birleşik Devletleri İç Güvenlik Bakanlığı

DLP: Veri Kaybı/Sızıntısı Önleme

DMARC: Etki Alanı Tabanlı Mesaj Kimlik Doğrulaması

DNS: Alan İsimlendirme Sistemi

E-CRM: Elektronik Müşteri İlişkileri Yönetimi

EPC: Elektronik Ürün Kodu

ETH: Ethereum Block Zinciri

E-WoM: Elektronik Ağızdan Ağıza İletişim

FTC: Federal Ticaret Komisyonu

FTP: Dosya Aktarım Protokolü

GPS: Küresel Konumlama Sistemi

IC3: İnternet Suçları Şikâyet Merkezi

IDS / IPS: İzinsiz Giriş Savunma Sistemi / Saldırıdan Korunma Sistemi

IoC: Uzlaşma Göstergeleri

IoT: Nesnelerin İnterneti

IP: İnternet Protokol

ISS: İnternet Servis Sağlayıcı

KOBİ: Küçük ve Orta Büyüklükteki İşletmeler

KVKK: Kişisel Verileri Koruma Kurulu

M&A: Birleşme ve Satın Almalar

MAC: Ortam Erişim Yönetimi

MITM: Ortadaki Adam

ML: Makine Öğrenimi

NFT: Değiştirilemez Token

P2P: Eşler Arası

PCI DSS: Ödeme Kartı Endüstrisi Veri Güvenliği Standardı

Phishing: E-posta Kimlik Avı

PST: Geleneksel Fiziksel, Sosyal ve Düşünme Alanları

RDP: Uzak Masaüstü Protokolü

RFID: Radyo Frekansı ile Tanımlama

ROI: Yatırım Getirisi

SASE: Güvenli Erişim Hizmeti

SEO: Arama Motoru Optimizasyonu

Smishing: Sms Kimlik Avı

SPF: Gönderen Politikası Çerçevesi

SSL: Güvenli Soket Katmanı

TCP: İletim Denetimi Protokolü

UDP: Kullanıcı Veri Birimi Protokolü

URL: Tekdüzen Kaynak Bulucu (Bir Web Sitesinin Görüntülediği Kısma Verilen İsim)

Vishing: Sesli Kimlik Avı

VPN: Sanal Özel Ağ

VR: Sanal Gerçeklik



GİRİŞ

Federal Soruşturma Bürosu'nun bir bölümü olan İnternet Suçları Şikâyet Merkezi'nin (IC3) de belirttiği üzere "siber risk, ticari bir risk" olmakla beraber "ulusal bir güvenlik" unsurudur (IC3, 2022). Siber dünyadaki işletmeler ve müşteriler ise bu riskler ile yoğun bir şekilde karşı karşıyadır. Günümüzde teknolojik gelişmelere entegre olup faaliyetlerini siber dünyaya taşıyan işletmeler, bilgisayar korsanlarının çeşitli motivasyonları ile hedef haline gelmiş durumdadır. Erişilebilirliğin artması, dijital platformların zengin bir veri havuzuna sahip olması, yüksek miktarlardaki para akışının dijital ortamlarda gerçekleştirilmesi bunlardan sadece bazılarıdır. İşletmelerin siber güvenlik sorunları sadece işletmeyi etkilememekle birlikte müşterileri veya işletme paydaşlarını da etkilemektedir. Bu sebeple siber güvenlik büyük bir önem arz eder.

Siber güvenlik kavramı farklı disiplinlerle bir bütündür. Literatüre bakıldığında siber güvenlik hakkındaki çalışmaların çeşitlilik sunduğu ve kapsayıcı olduğu görülmektedir. Siber güvenlik kavramının işletmeler açısından incelenmesine bakıldığında Cook (2017) Küçük ve Orta Büyüklükteki İşletmeler (KOBİ'ler) boyutunda, Fritzvold (2017) farklı sektörlerin karşılaştırılması boyutunda, Özkaya (2018) sosyal medya boyutunda ele almıştır. Bu çalışmanın temel amacı siber güvenlik üzerine işletmeler için bir hazırbulunuşluk ölçeğinin hazırlanmasıdır. Diğer bir amacı ise kavramın dijital pazarlama boyutunda ele alınarak işletmeler ve müşteriler açısından değerlendirilmesidir. Çalışma teorik bilgilerin verilmesi, sosyal medya madenciliğinin (sosyal ağ analizi) yapılması, bilimsel haritalama olarak verilerin görselleştirilmesi ve hazırbulunuşluk ölçeğinin hazırlanmasından oluşmaktadır.

BİRİNCİ BÖLÜM

1. SİBER GÜVENLİĞİN TANIMI VE DİJİTAL DÖNÜŞÜMDEKİ ÖNEMİ

Teknoloji her geçen gelişmekte ve çeşitli inovasyonları beraberinde getirmektedir. Yaşanan inovasyonlar ise hayatımızı önemli ölçüde etkilemekte ve değiştirmektedir. Dijitalleşme ise bunlardan biridir. İşletmeler, dijitalleşmenin sağladığı avantajlardan faydalanmak istemesi nedeniyle dijital dönüşüm sürecine dahil olmaktadır. Yaşanan bu dönüşüm siber alanda gerçekleşmekle birlikte bu alandaki tehditler siber risk kavramının, işletmelerin siber risklerden korunma ihtiyacı ise siber güvenlik kavramının ortaya çıkmasına neden olmuştur.

1.1. SİBER KAVRAMININ TANIMI

Siber kelime anlamıyla “bilgisayarları, özellikle interneti içeren, kullanan veya bunlarla ilgili” demektir (Cambridge Dictionary, 2021). Diğer bir tanıma göre, bilgi teknolojisi (BT) ile bir ilişkiyi ifade eden ismin önüne konulan ektir (Webopedia, 2021). Etimolojik olarak bakıldığında siber öneki Yunanca eski bir kelime olan “κυβέρνησις (kybernesis)” kelimesinden türemiştir ve köken olarak “kontrol becerileri” anlamına gelir (Krämer, 2013). Eski Yunanca kybernētēs'den türetilen "sibernetik" ise Siber Uzay'ın ana terimidir (Jenifer Stella S & Dr. Ambika Kumari S, 2022). Siber Uzay (Cyberspace)” geleneksel fiziksel, sosyal ve düşünme alanlarına (PST) dayalı olarak yaratılan ancak karşılığında PST'de büyük bir fark yaratan dijital dünyayı ifade etmektedir. Siber Uzay kavramı ilk olarak 1960'ların sonlarında Danimarkalı sanatçı Susanne Ussing (1940-1998) ve ortağı mimar Carsten Hoff'un (d. 1934) “Atelier Cyberspace” adıyla oluşturdukları görsel sanatlarda ortaya çıkmasına rağmen Carsten Hoff, İskandinav sanat dergisi Kunstkritikk ile 2015 yılında yaptığı bir röportajda kavramın sadece alanları yönetmekle ilgili olduğunu, dijital ortamda bir şeyin olmadığını, Siber Uzay'ın sadece bir araç olduğunu belirtmiştir (Lillemose ve Kryger, 2015).

“Siber Uzay” teriminin, Internet ve daha sonra World Wide Web ile ilişkilendirilmesi ise 1990'larda, özellikle akademik çevrelerde ve aktivist topluluklarda ortaya çıkmıştır. Bu anlamı popülerleştiren yazar Bruce Sterling, John Perry Barlow'u

"günümüzdeki bilgisayar ve telekomünikasyon ağları bağlantısına" atıfta bulunmak için ilk kullanan kişi olarak kabul etmektedir (Wikipedia, 2023).

Günümüzde “Siber Uzay” kavramı ön plana çıkmaya başlamış durumdadır ve önemi sürekli artmaktadır. 2010 Quadrennial Defense Review’da¹ "İnsan yapımı bir alan olmasına rağmen, “Siber Uzay’ın” artık Savunma Bakanlığı faaliyetleri için doğal olarak oluşan kara, deniz, hava ve uzay alanları kadar alakalı bir alan" olduğu söylenmiştir. Ayrıca NATO’nun 2016’da operasyon alanlarına siber alanı eklemesi, dünyanın dört bir yanındaki ulusların, siber uzayı doktriner literatürlerine operasyonel bir savaş alanı olarak dahil etmesi, Siber Uzay’ın artan önemini yeterince vurgulamaktadır.

Siber uzay genişledikçe ve küreselleştikçe sosyal, ekonomik, askeri ve siyasi güvenlik dahil olmak üzere ulusal güvenliğin farklı boyutlarını da etkileyen “siber tehditler” olarak adlandırdığımız uluslara yönelik yeni bir tehdit ortaya çıkmıştır (Abbasi, 2021). Siber tehditler elektronik ortamda gerçekleşmesiyle birlikte oldukça yıkıcı bir etkiye sahiptir ve siber tehditlerin yıkıcı etkilerine karşı korunma ihtiyacı ise siber güvenlik kavramını hayatımıza getirmiştir.

Siber güvenlik, “Siber uzayı ve siber uzay destekli sistemleri fiili mülkiyet haklarından hukuken yanlış hizalayan olaylardan korumak için kullanılan kaynakların, süreçlerin ve yapıların organizasyonu ve koleksiyonudur" (Craig, Diakun-Thibault ve Purse, 2014). Diğer bir tanıma göre ise siber güvenlik; bilgisayarları, sunucuları, mobil cihazları, elektronik sistemleri, ağları ve verileri kötü niyetli saldırılardan koruma uygulamasıdır (Kaspersky, 2022). Ayrıca Siber Güvenlik, “Ağları, cihazları ve verileri yetkisiz erişimden veya suç amaçlı kullanımdan koruma sanatı ve bilgilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlama uygulaması” olarak da ifade edilebilmektedir. (Cybersecurity and Infrastructure Security Agency, 2021).

¹ Quadrennial Defense Review, Amerika Birleşik Devletleri Savunma Bakanlığı tarafından stratejik hedefleri ve potansiyel askeri tehditleri analiz eden bir çalışmadır.

1.2. İŞLETMELERİN DİJİTALLEŞME SÜRECİ VE SİBER GÜVENLİK

Dijital ortamda yapılan işlemlerin kolay ve daha hızlı bir şekilde gerçekleşmesinin yanı sıra dijital ortamda sunulan birçok özellik de bu avantajlardan faydalanmak isteyen işletmelerin, işlemlerini dijital ortama taşımasını sağlamış ve işletmelerin olası siber saldırılara/tehditlere karşı korunması için siber güvenliğini zorunlu hale getirmiştir. İşletmelerin dijital dönüşümü; yeni iş modelleri, süreçler, yazılımlar ve sistemler oluşturmak için teknolojinin uygulanmasını sağlayarak daha çok kâr, yüksek rekabet avantajı ve daha fazla verimlilik gibi fırsatlar sunmaktadır (Schwertner, 2017).

Geniş bir kitleye ulaşmak ve yüksek etkileşim sağlamak isteyen işletmeler özellikle dijital ortamdaki pazarlama faaliyetlerine yoğunlaşmış durumdadır ve dijital pazarlama günümüzün revaçta olan alanlarından biridir. Dijital pazarlama, e-postalar, web siteleri, çevrimiçi forumlar ve haber grupları, etkileşimli televizyon, mobil iletişim vb. etkileşimli teknolojileri kullanarak tüketicileri satıcılarla elektronik olarak bağlayan bir doğrudan pazarlama biçimi olarak tanımlanır (Kotler ve Armstrong, 2009). Web özellikli teknoloji aracılığıyla tüketici satıcı ile karşı karşıya gelmeden tüketicinin bu hizmetlerden yararlanması ise “Siber Tüketici” kavramını ortaya çıkarmıştır (Sushanth IT Law Associates, 2021). Bilgisayar korsanları (hackerlar), bu etkileşimli teknolojileri kullanan işletmelerin veya siber tüketicilerin zaafiyetlerini bularak bunları kendi çıkarları için kullanmaya çalışır.

İşletmeler, dijital ortamdaki birçok bilgiyi müşterilerinden gönüllü veya gönülsüz elde edebilmekte ve bu bilgileri mevcut sistemlerinde barındırabilmektedir. Sistemde bulunan bilgiler işletmeye özgü olabileceği gibi müşteri ya da paydaşlara ait hassas bilgileri içerebilmektedir. Bu sebeple dijital ortamdaki verilerin saklanması ve korunması, sadece işletmeler için önemli olmamakta aynı zamanda müşteri ve ortaklar için de büyük bir önem arz etmektedir. Bilgisayar korsanları (hackerlar) işletme sistemindeki yazılımsal hataları (bug) veya güvenlik açıklarını (vulnerability) bularak, keşfedilen zaafiyeti boyutu ve içeriğine göre kendi lehine kullanabilmektedir. Örneğin, bilgisayar korsanları (hackerlar) siber saldırılarının başarılı olması sonucunda veri tabanındaki kayıtlı bilgilere ulaşabilmektedir. Kayıtlı veri bilgilerini çalan hackerlar, veri tabanındaki kişisel veya kurumsal verileri rakip işletmeye veya Deep Web’in alt kümesi olan Dark Web’de satıp gelir edebilmekte ve çalınan verilerin başka yerlerde kullanılmasına yol açabilmektedir. Bunun

yanı sıra sistemde hackerlar kayıtlı bilgilerden direk gelir edebilmekte veya sistemdeki bu zaafiyet sonrası işletmelerden belli bir ücret de isteyebilmektedir.

Siber saldırı sonucunda, işletme birçok açıdan zarar görür. Bu zararlar; maddi zararlar ve manevi zararlar olarak ikiye ayırabilir. Marka itibarı ve marka güvenilirliğinin zarar görmesi manevi bir zarar iken, işletmenin siber saldırıyı KVKK'ya (Kişisel Verileri Koruma Kurulu) bildirip yaşanan veri ihlali için ceza ödemesi veya hacker'a ücreti vermesi maddi bir zarardır. Maddi zararın boyutu ise birçok etkene göre değişmektedir. 2021 yılında Yemeksepeti'ne yapılan siber saldırıda web uygulama sunucusuna, sunucudaki açık kullanılarak uygulama kurulup ve komut çalıştırmak suretiyle erişildiği, bu ihlalden 21 milyondan fazla kullanıcının etkilendiği, sisteme giren kişi ya da kişilerce, zararlı yazılım ve araçlarla giriş yaptıktan sonra diğer sistemlere de erişilerek bilgi toplandığı, sisteme zararlı yazılımların yüklenip çalıştırılmasının veri sorumlusunca sekiz gün boyunca fark edilemediği dolayısıyla bilişim ağlarında hangi yazılım ve servislerin çalıştığının kontrol edilmesi ve bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının belirlenmesi noktasında veri sorumlusunun kusurunun bulunduğu tespit edilmiştir. Bu olay neticesinde KVKK tarafından Yemeksepeti'ne veri ihlali sebebiyle 1 milyon 900 bin lira idari para cezası uygulanmasına karar verilmiştir (KVKK- “Yemek Sepeti Elektronik İletişim Perakende Gıda Lojistik AŞ veri ihlal bildirimi hakkında” Kişisel Verileri Koruma Kurulunun 23/12/2021 tarih ve 2021/1324 sayılı Karar Özeti, 2021).

İsmi belirtilmeyen bir oyun firmasında 2020 yılında yaşanan veri ihlalinde ise Türkiye’de ihlalden etkilenen kişi sayısının 39.995 olduğu, veri sorumlusu tarafından ihlal öncesi alınması gereken teknik tedbirlerin (güvenlik ajanının ağ sistemine konuşlandırılması, kötü niyetli IP adreslerinin sistemden engellenmesi, oyuncu hesaplarının yetkisiz erişimlerden korunması için gerekli önlemlerin alınması, hackerlar tarafından kullanılan mekanizmaların ve IP’lerin gözlenmesi için 7x24 gerçek zamanlı gözetleme sistemini de içeren, geliştirilmiş gözetleme ve alarm sistemlerinin faaliyete geçirilmesi) ihlal sonrası devreye alınmasının gerekli teknik ve idari tedbirlerin alınmadığının göstergesi olduğu hususu dikkate alınarak KVKK firmaya 1.100.000 TL idari para cezası vermiştir (KVKK- “Bir oyun şirketinin veri ihlal bildirimi hakkında” Kişisel Verileri Koruma Kurulunun 16.04.2020 tarih ve 2020/286 sayılı Karar Özeti, 2020).

Bilgisayar korsanları tarafından yapılan siber saldırılar dışında da veri ihlali yaşanabilmektedir. 2018'de Facebook (Meta) ve Cambridge Analytica, milyonlarca uygulama kullanıcısının verilerini rızaları olmadan topladıkları için ifşa edilmiştir. Veriler, Cambridge Analytica tarafından siyasi alanı etkilemek, özellikle de Trump'ın başkanlık kampanyasına yardımcı olmak için kullanılmıştır. Veri gizliliği ihlali, Facebook'un (Meta) boykot edilmesi ve buna yönelik bir hareket başlatılması amacıyla #DeleteFacebook kampanyasının ortaya çıkmasına neden olmuştur. Bu hareket sonunda sadece Facebook (Meta)-Cambridge Analytica skandalının ötesine geçmiş ve daha büyük bir veri gizliliği hareketine yol açmıştır. #DeleteFacebook kampanyası, şirketi boykot edemese de hükümetler ve şirketler içinde politika değişiklikleriyle sonuçlanan daha büyük bir veri gizliliği hareketi hakkında tüketici bilincini artırmıştır (UC Berkeley, 2020). ABD medyasında yer alan haberlere göre, ABD düzenleyicileri, veri gizliliği ihlalleriyle ilgili bir soruşturmayı sonuçlandırmak için Facebook'a (Meta) 5 milyar dolarlık (4 milyar sterlin) rekor bir cezayı onaylamıştır (BBC News, 2019).

İşletmeler sadece veri ihlali nedeniyle KVKK tarafından maddi kayıplara uğramamaktadır. İşletmelerin maruz kaldığı siber saldırılarda öne çıkan bir kavram olan Fidyeye yazılımları (Ransomware) sonucunda da maddi kayıplar olabilmektedir. Fidyeye yazılımı, bilgisayara belirli bölümlere erişimi kısıtlayan (örneğin verilerini şifreleyerek) ve işlevselliğin tekrar kazanılması için mağdurdan ödeme talep eden, özellikle zararlı bir kötü amaçlı yazılım biçimidir (Simoiu ve diğerleri, 2019). Örneğin, LAPSUS\$ (bir hacker grubu) "Genesis" adlı bir pazarda Electronic Arts oyun geliştiricisinin oturum açma bilgilerini satın alarak 780 GB'lık özel kaynak kodunu ifşa etmekle tehdit etmiş ve yüklü bir ödeme talep etmiştir (Lumifi, 2022). Check Point Research (CPR), 2021 yılı raporu için yapmış olduğu araştırmada küresel bazda her 61 kuruluşun 1'ini her hafta fidye yazılımından etkilendiğini (2020'ye kıyasla %9'luk bir artış) tespit etmiştir (Gmcdouga, 2021). FBI'nın (Federal Soruşturma Bürosu, Amerika Birleşik Devletleri'nin İç İstihbarat ve Güvenlik Gücü) İnternet Suçları Şikâyet Merkezi, Ocak-31 Temmuz 2021 tarihleri arasında 2.084 fidye yazılımı şikâyeti aldıklarını bildirmiştir. Bu sayı ise yıldan yıla %62'lik bir artış olduğunu göstermektedir (Forbes, 2022). Trend Micro'nun (Japonya merkezli bir bilgisayar yazılımı şirketi) veri güvenliği vakalarını incelediği güvenlik raporuna göre küresel bazda bakıldığında fidye yazılımı saldırılarının en fazla yaşandığı ülkeler arasında

Türkiye, Hindistan, Çin, ABD ve Brezilya yer almaktadır (Hürriyet Gazetecilik ve Matbaacılık A.Ş., 2021).

Sophos'un (İngiltere merkezli bir güvenlik yazılım ve donanım şirketi) uzmanlar tarafından fidye yazılımı saldırılarının durumuna ilişkin hazırladığı "State of Ransomware 2022" raporunda Türkiye'den ankete katılan şirketlerin %60'ının 2021 yılında fidye yazılımı saldırılarına maruz kalırken, saldırı sonucunda verileri şifrelenen şirketlerin %47'sinin yedekleme ve diğer veri kurtarma araçlarına sahip olsalar dahi verilerini hızla geri alabilme umuduyla fidye ödemeyi tercih ettikleri tespit edilmiştir (CyberMag, 2021).

MediaMarkt (Almanya merkezli elektronik perakende mağaza zincirine sahip olan Metro Group'un kuruluşu) 8 Kasım 2021 tarihinde uğradığı Hive fidye yazılımı² saldırısında şirketin Almanya ve Hollanda'daki mağazalarının IT sistemleri kilitlenmekle beraber, şirketinin depo işlemleri gibi birçok operasyonunda aksamalar meydana gelmiştir. Özellikle Hollanda'daki mağazalarda kasalarda kredi kartıyla işlem yapılamazken, geçmiş döneme ait kayıtlara da erişilememiştir. RTL Nieuws'un bildirdiğine göre, personelden yazar kasaların internet bağlantısını kesmeleri ve sistemleri yeniden başlatmalarını istenmiştir. Hive Fidyeye Yazılımı Grubu, bıraktığı fidye notunda kişisel bilgilerin, finansal raporların ve önemli belgelerin şifrelendiğini belirterek işletmeyi verileri ifşa etmekle tehdit etmiş ve şirketten 240 milyon dolarlık fidye talep edilmiştir. İstenen fidye talebi ise o zamana kadar başlangıçta görülmüş en yüksek fidye talebi olarak nitelendirilmektedir (Usta, 2021).

Fidyeye yazılımları, siber saldırıya uğramamış işletmeleri dolaylı olarak etkileyebilmektedir. Kaseya (IT yönetimi ve güvenlik yazılımı sağlayan bir bilişim şirketi) yaşadığı fidye yazılımı sonrası şirkete ait SaaS (Hizmet olarak yazılım) sunucularını kapatmıştır. Ayrıca siber saldırı altında olduğunu müşterilerine duyurmuş, güvenliğin ihlal edilmesini önlemek için VSA (Sanal depolama cihazı) sunucularını kapatmaları konusunda müşterilerini bilgilendirmiştir (Greig, 2021). Rus hacker grubu REvil, saldırının sorumluluğunu

² İlk olarak Haziran 2021'de gözlemlenen Hive, siber suçlular tarafından sağlık tesislerine, kâr amacı gütmeyen kuruluşlara, perakendecilere, enerji sağlayıcılarına ve dünya çapındaki diğer sektörlerle yönelik fidye yazılımı saldırıları gerçekleştirmek için kullanılan bağlı kuruluş tabanlı bir fidye yazılımı çeşidi (Varonis, 2022).

üstlenmiş ve bu durumdan etkilenen bilgisayarların kilidini açmak için 70 milyon dolarlık fidye talep etmiştir (Ilascu, 2021).

Kaseya'ya yapılan siber saldırıdan İsveç merkezli Coop şirketi (İsviçre'nin en büyük perakende ve toptan satış şirketlerinden biri) Kaseya yazılımını kullanmasa dahi yazılım sağlayıcılarından biri (Visma Esscom) kullandığı için bu saldırıdan dolayı yoldan etkilenmiştir. Saldırı sebebiyle Coop şirketinin ödeme sistemlerinde sorun çıkmış ve bunun sonucunda Coop süpermarketi 500 mağazasını kapatmıştır (Abrams, 2021). Bu zincirleme siber saldırı etkilerini gösteren önemli bir örnektir.

1.2.1. Birleşme ve Satın Almalar

İşletmelerin birleşme ve satın alma faaliyetleri de dolaylı olarak siber güvenlik sorunlarından etkilenebilmektedir. “Birleşme ve satın almalar (M&A), iki ayrı şirketin tek bir varlık haline gelebildiği finansal işlemlerdir” (Thaxton, 2022). Pozitif ölçek ekonomisi³, genişleme imkânı, risk çeşitlenmesi ve birden çok büyüme fırsatı sağlar (Emmitt, 2021). “Bir devralan şirket satın aldığı anda, esas olarak işletmenin tüm siber güvenlik açıklarını ve tüm risk profilini üstlenir. Siber riskin tek bir yanlış hesaplanması veya hafife alınması, hisse fiyatının aşınması, itibar kaybı ve dava ve soruşturmalara maruz kalma gibi ciddi sonuçlara yol açabilmektedir” (Durbin, 2022).

Tablo 1

Siber Güvenlik Sorunlarının Birleşme ve Satın Almalarda Etkisi

Şirketler	Siber Güvenlik Sorunlarının Etkisi
Spirit AeroSystems/Asco	Spirit'in Asco'yu devralma teklifinin şartları, Asco'nun işinin bir fidye yazılımı saldırısıyla kesintiye uğramasının ardından önemli ölçüde değiştirildi. Sonunda işlem iptal edildi.
Marriott/Starwood	Starwood Hotels'de, Marriott'un Starwood'u satın almasından iki yıl önce başlayan ve satın alma tamamlanana kadar fark edilme- yen bir veri güvenliği olayı, Birleşik Krallık Bilgi Komiserliği Ofisi tarafından Marriott'a 18,4 milyon sterlin para cezası verilmesiyle sonuçlandı.

³ Üretim arttıkça ortalama maliyetlerin düşmesidir.

Verizon/Yahoo!

Yahoo!'da yaşanan veri ihlalleri Verizon'un Yahoo!'yu satın almadan önce 4,83 milyar ABD doları tutarındaki fiyatında 350 milyon dolarlık bir indirim istemesine yol açtı. Ayrıca ihlalin sorumluluğu paylaşıldı.

PayPal/TIO

PayPal, TIO'yu 302 milyon \$'a satın almasının ardından TIO'da keşfedilen bir veri güvenliği olayı, PayPal'ın TIO'nun hizmetlerini kapatmasına ve TIO'yu tasfiye etmesine neden oldu.

Not. Uyarlanmıştır. (Borden Ladner Gervais. (2021, 10 Mayıs). *Managing Cyber Risks in M&A Transactions*. <https://www.blg.com/en/insights/2021/05/managing-cyber-risks-in-m-and-a-transactions>)

Siber güvenlik, işletmeler için her geçen yıl daha ciddi sonuçlar doğuran büyük bir problem olmasına rağmen ulaşılan veriler KOBİ'lerin 2021 yılında yüzde 13 artan fidye yazılımı gibi siber saldırıları tehdit unsuru olarak algılamadığını ortaya koymaktadır (DHA, 2022).

İşletmelere siber tehditlere karşı hazırlık yapmalarını ve merkezi sistemler kullanmalarını tavsiye eden Berqnet Genel Müdürü Hakan Hintoğlu, "Fidye yazılımı saldırganları, ödemelerin yüzde 98'ini Bitcoin olarak talep ediyor. Saldırganlara kimlik ve unvanlarını gizleme imkânı sağlayan kripto para birimlerinin değişken doğası, şirketlerin maliyetlerini de artırıyor" diyerek duruma dikkat çekmiştir. Ayrıca CNBC'nin KOBİ'lerle yürüttüğü araştırmada, işletmelerin yalnızca %5'inin siber güvenliği büyük riskler arasında saydığı görülmüştür. Yüksek güvenlik bütçeleri ve ileri seviye uzmanlıkları olmadığından KOBİ'lerin kapısının ortalama ve fidye saldırılarına daha açık olduğunu vurgulayan Hintoğlu, "Küçük ve orta ölçekli işletmelerin sosyal mühendislik (İnsan psikolojisinden yararlanarak kurbandan hassas bilgileri öğrenme yöntemidir) kategorisi altında değerlendirilen ve insan hatalarını hedef alan saldırılara yüzde 350 daha fazla maruz kaldığını gösteren veriler var. Bu işletmelere ait sistemlerin saldırılara karşı daha kırılgan olduğunu bilen bilgisayar korsanları, gelişmiş bir güvenlik altyapısını hedeflemektense, daha kolay ve kârlı olduğu düşüncesiyle birden fazla KOBİ'ye yöneliyor. İş süreçlerini aksatan ve büyümeyi yavaşlatan bu gibi saldırılara hedef olmamak için, ölçeği ne olursa olsun her şirketin siber güvenliğe yatırım yapması gerekiyor. Bir şirketin siber güvenlik açısından ihtiyaç duyduğu birçok çözümü bir araya getiren ve servis modeliyle sunulan Güvenli Erişim Hizmeti (SASE) mimarisi, ölçeklenebilir yapısı ve kolay uygulanabilirliğiyle KOBİ'ler için de en uygun çözüm oluyor" ifadelerini de kullanmıştır (DHA, 2022).

Günümüzün popüler alanlarından biri olan dijital pazarlamada siber güvenliğin olumlu veya olumsuz etkilerini görmek kaçınılmazdır. Bu yüzden dijital pazarlamada siber güvenlik işletmeler için hayati öneme sahip denilebilir. İşletmeler yaşam döngülerini

sürdürebilmek için siber esnekliklerini⁴ sürekli artırmalı ve zamana uyum sağlamalıdır. Başarılı siber güvenlik stratejileri ve önlemleri işletmelere büyük avantajlar sağlayacağı gibi başarısız bir siber güvenlik stratejileri ve önlemleri işletmelere dezavantajlara ve kayıplara yol açabilmektedir. Dijital pazarlamanın faal olduğu alanlarda yetersiz siber güvenlik neticesinde yaşanan veri ihlalleri, fidye yazılımları gibi siber sorunlar birçok maddi & manevi olumsuz sonuçlar doğurur ve oldukça sık görülmektedir. İşletmeler dijital pazarlamada, en başta güven ihtiyacını karşılayarak müşterileriyle sağlıklı bir iletişim ortamı kurmaya çalışmalıdır. Bu ortam sağlanamazsa işletmeler yaşam döngülerinde sektöre ve zarara uğrayacaktır.

⁴ Siber saldırılara karşı koruma, tespit etme, yanıt verme ve iyileştirme yeteneğidir.

İKİNCİ BÖLÜM

2. DİJİTAL ORTAMDA GİZLİLİK VE GÜVENLİK ENDİŞELERİ

İşletmelerin dijital dönüşümü avantajlara sahip olmakla beraber gizlilik veya güvenlik sorunlarına da yol açabilmektedir. Dijital pazarlama faaliyetleri bunlardan biridir. Sanal ortamda gerçekleşen işlemler bilgisayar korsanlarının saldırısına açık hale gelebilmektedir. Bu siber saldırıların birçok türü ve aracı vardır. Bunlara her geçen gün yenileri eklenmektedir. Hassas verilerin korunması büyük önem arz etmektedir.

2.1. İŞLETMELERİN DİJİTALLEŞMESİ VE SİBER GÜVENLİK

Dijital pazarlamanın ayrılmaz parçalarından biri olan sosyal medya hesapları geniş bir hedef kitleye ulaşip marka bilinirliğinin artırılması amacı dışında ürünlerin/hizmetlerin sergilenmesi, tanıtılması veya satılması amacıyla da kullanılmaktadır. Bu hususta ilk akla gelenlerden biri ücretsiz olarak hesap açılabilen Instagram'dır. Instagram'daki kullanıcıların (özellikle dijital yerliler) en az %90'ı bir işletmeyi takip etmekte, ortalama bir Instagram işletme hesabı, takipçilerini her ay %1,69 oranında artırmakta, 2 kişiden 1'i yeni markaları keşfetmek için Instagram'ı kullanmakta, kullanıcıların %57'si Instagram'da markaların anketlerini ve testlerini görmekten hoşlanmakta ve insanların %44'ü haftalık alışveriş yapmak için Instagram'ı kullanmaktadır (RecroDigitalMarketing, 2022).

İşletmeler veya yaptıklarını satmak isteyen bireyler bu sayede sosyal medyanın olanaklarını kullanarak potansiyel müşterilerine daha hızlı, kolay ve ücretsiz bir şekilde ulaşabilmektedir. Bu şekilde gerçekleştirilen pazarlamaya ise sosyal medya pazarlaması denir. Yeni sosyal etkileşim biçimleri yaratması, etkileşimli bir ortam sağlaması, site kullanıcılarının ilgi alanlarına göre hedefleme yapması ise sosyal medya pazarlamasının tercih edilmesinin diğer nedenleridir (Nadaraja, 2013). Bunun yanı sıra sosyal medyada gizlilik ve güvenlik sorunları oldukça yoğun görülür. Ürünün gönderilmemesi, satın alınmayan farklı bir ürünün gönderilmesi, ürünün orijinal sanılıp aslında orijinal olmaması, ürünün kusurlu gönderilmesi, ürünün resimlerde olduğu gibi olmaması veya ürünün beklentisini karşılamaması ise internet ortamında gerçekleştirilen satın alma işlemlerinde

yaşanabilecek olası problemlerden sadece bazılarıdır. Bu sebeple müşterilerin online satın alma işlemlerinde endişeleri olabilmektedir. Belirtilen problemlerin dışında Federal Ticaret Komisyonuna (FTC) gönderilen raporlar, sosyal medyanın giderek daha fazla dolandırıcıyı bünyesinde barındırdığı göstermekte ve 2021'de dolandırıcılık nedeniyle para kaybettiğini bildiren dört kişiden birinin, bunun sosyal medyada bir reklam, gönderi veya mesajla başladığını bildirmektedir (Fletcher, 2022).

Önceki akademik çalışmalarda belirtilen Instagram'daki hesaplara güven faktörlerine bakıldığında potansiyel müşterilerin Elektronik Ağızdan Ağıza İletişim (E-WoM), Algılanan Yardımseverlik, Algılanan Dürüstlük, Satıcının Tepkisi, Görüntü Kalitesi, Güvenme Eğilimi, Algılanan Bütünlük, Instagram'ın Kullanılabilirliği ve Kolaylığı, Takipçi Sayısı, Hashtag Sayısı, Fiyatın Rasyonelliği, Bilgi Kalitesi gibi faktörlere genelde dikkat ettiği tespit edilmiştir (Din, Ramli ve Bakar, 2018). Ayrıca müşteriler influencerlardan da güven konusunda önemli ölçüde etkilenmektedir. Ancak yaşadığımız siber dünyada bunlar yanıltıcı olabilmektedir. Örneğin takipçi sayısı birçok uygulama tarafından ücretli veya ücretsiz artırılabilir. Yorumlar, satıcılar tarafından veya yorumlar karşılığında para alan bireylerden oluşabilmektedir. Rakip işletme, dijital ortamda ürün/hizmet için aleyhe yorum yaparak müşterinin marka güvenini sarsabilmektedir. Güvenilen influencerların müşterilere doğru bilgi vermeme olasılığı da bulunmaktadır. Bu sebeple internet ortamında alışveriş yaparken dikkatli ve bilinçli olmak oldukça önem arz etmektedir.

2.1.1. Veri İhlalleri

Siber dünyada bilinçsizce yapılan işlemler gizlilik ve güvenlik problemlerine yol açmaktadır. Örneğin, alışverişte internet ortamından ödeme yapılması müşteriler için oldukça riskli sonuçlar yaratabilmektedir. Güvenli olmayan sahte (fake) bir siteye kayıt ve o site üzerinden yapılan alışveriş; kişisel verilerin Deep Web'te satılmasına, kredi kartı bilgilerinin kötü niyetli bilgisayar korsanları tarafından kullanılmasına yol açabilmektedir. Güvenilir görünen sitelerde siber saldırıya uğradıklarında hassas bilgileri tehlikeye atabilmektedir. Örneğin, bir kredi raporlama şirketi olan Equifax'ın web sitesi 2017 yılında bilgisayar korsanları tarafından siber saldırıya uğramıştır. Yaklaşık 200.000 kredi kartı kaydı siteden çalınmıştır. Saldırı sonrası ihlal rapor edilmiş ve şirkete olan güvenin azalmasıyla hisse fiyatı da düşmüştür (Fruhlinger, 2020).

Güvenilir gözükken bir sitedeki bilgiler bile siber saldırı sonrası hassas verilere erişilerek ciddi problemlere neden olabilmektedir. Diğer yandan veri toplayan ve işleyen web siteleri hassas verileri belirli amaçlar için toplamaktadır. Bu web siteleri sayesinde aranan veya ihtiyaç duyulan ürünün/hizmetin reklamlarına (Remarketing) sık sık maruz kalılabilmektedir. Bu gizlilik ve çerez politikasına, sayfaya girişin üçüncü taraflara paylaşmasına izin verilmesinden ötürü karşılaşılan bir durumdur. İşlenen veriler sayesinde kullanıcı hakkında detaylı bilgi sahibi olunabilmektedir. Ancak 2010 yılında 5982 sayılı Kanun’la yapılan Anayasa değişikliği ile Anayasa’nın 20. maddesine ilave bir fıkra eklenerek kişisel veriler, “özel hayatın gizliliği ve korunması hakkı” kapsamında Anayasal güvenceye kavuşmuştur.

Söz konusu fıkra; “Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Ayrıca özel hayatın gizliliğini, Anayasaya uygun olmayan şekilde sınırlayan kanunlara dayanarak yapılan veri işleme faaliyetleri, hukuka uygunluk kriterini karşılamayacaktır” (Kişisel Verilerin Korunması Kanunu ve Uygulaması, 2022).

Örneğin KVKK, mesajlaşma uygulaması WhatsApp’a “WhatsApp uygulamasını kullanmak isteyen kullanıcıların kişisel verilerinin işlenmesine ve yurt dışında bulunan üçüncü taraflara aktarılmasına açık rıza verilmesini içerecek şekilde Hizmet Koşullarının ve Gizlilik İlkesinin güncellendiği, bu kapsamda açık rıza vermeyen kullanıcıların uygulamayı kullanamayacağına ve hesaplarının silineceğine” dair bilgilendirme iletmesinden ötürü 1 milyon 950 bin lira para cezası kesmiştir.

Hukuksal açıdan kişisel verilerin güvenliğine dair maddeler söz konusu olsa da kullanıcılar tarafından kişisel verilerin işlenmesi konusunda genellikle sitelere izin verilmektedir. Örneğin, kabul edilen bir hizmet şartları kişisel verilere erişime ve verilerin saklanması olanak sağlayabilmektedir. 2017’de 2.000 ABD’li tüketiciyle yapılan bir Deloitte araştırmasında, insanların %91’inin hizmet şartlarını okumadan kabul ettiğini tespit etmiştir. 18-34 yaş arası daha genç insanlar için bu oran daha da yüksek seviyede olup %97 oranındadır (Cakebread, 2017). Carnegie Mellon Üniversitesinde yapılan bir araştırmaya göre bir Amerikalı bir yıl boyunca ortalama uzunluğu 2.518 kelime olan

1.462 adet gizlilik politikasıyla karşılaşmaktadır. Bu politikaların hepsinin okunması ise günde 8 saatten, toplam yetmiş altı iş gününü bulmaktadır (Goodman, 2016). Araştırma sonuçları değerlendirildiğinde kullanıcıların siber dünyada birçok etmenle karşılaştığı ve bilgilerinin dışında kişisel verilerinin doğrudan veya dolaylı paylaşımına izin verebildikleri görülmektedir.

İngiliz perakende mağazası GameStation, herhangi birinin hizmet kullanım şartlarını okuyup okumadığını görmek adına 1 Nisan Şaka gününde bir deney yapmıştır. Yaptıkları bu sosyal deney sonrası GameStation, müşterilerin %88'inin şirkete müşterilerinin ruhunun yasal mülkiyetini veren maddeyi okumadığını iddia etmiştir (BBC, 2013). Şirketin gizlilik sözleşmesindeki madde şu şekildedir:

“İnternet sitesi üzerinden bir sipariş vererek, şu an ve sonsuza kadarlık bir dilim için, ölümsüz ruhunuz üzerinde devrolunmaz haklarınızı bağışlamayı kabul etmiş olursunuz. Bu hakkımızı uygulamaya koymak istersek, ölümsüz ruhunuzu ve üzerinde iddia edebileceğimiz tüm hakları, gamestation.co.uk veya yetki verdiği cüceleri tarafından iletilecek yazılı bilgiyi takip eden 5(beş) iş günü içerisinde teslim etmeyi kabul ettiklerini kabul etmiş olursunuz” (Goodman, 2016).

2.1.1.1. Dijital Ayak İzi

Ağ bağlantılı, sayısallaştırılmış, sensör yüklü, bilgi odaklı dünyadaki büyük miktarda veri, “Büyük Veri (Big Data)” olarak tanımlanmaktadır (Chang ve Grady, 2019). Veri kümesinin boyutu (hacim), birden çok yerden gelen veriler (çeşitlilik), özelliklerdeki değişiklik ve hız büyük verinin özellikleridir (NSTAC, 2016). Büyük veri (Big Data) yöntemlerinden bir olan dijital ayak izi ise interneti kullanırken bırakılan veri izidir. Ziyaret edilen web sitelerini, gönderilen e-postaları ve çevrimiçi olarak gönderilen bilgileri içermektedir. Bir kişinin çevrimiçi etkinliklerini ve cihazlarını izlemek için dijital ayak izi kullanılabilir. İnternet kullanıcıları dijital ayak izlerini aktif veya pasif olarak oluşturmaktadır (Kaspersky, 2022). Her İnternet kullanıcısının dijital ayak izi, pazarlama analizi için girdi olarak hizmet edebilecek önemli miktarda veri içerir. Verilerin manuel olarak alınması & analizi zaman alıcı olmakla birlikte yalnızca marjinal olarak düzenlenmektedir (Cheng, Fa-Chang & Wang, Yu. (2018). Analitik araçlar ise günümüzde pazarlama yönetiminde süreçleri sistemleştirmek, karar vermeyi kolaylaştırmak ve işi otomatikleştirmek için kullanılmaktadır. Bu sofistike analitik araçlar, geçmiş verilerden

öğrenmek ve gelecekteki aktivitelerin daha etkili bir şekilde planlanmasına yardımcı olmak için makine öğreniminden (ML) faydalanır (Miklosik, Kuchta, Evans ve Zak, 2019).

Sosyal ağ sitelerinde geçirilen süre artıkça, internet kullanıcısının dijital ayak izleri de artmaktadır. Bir sayfayı veya bir Facebook (Meta) gönderisini "beğenmek" bile, veriler Facebook (Meta) sunucularına kaydedildiği için dijital ayak izine katkıda bulunmaktadır (The European Community of Adult Learning Professionals, 2018).

Facebook'un (Meta) ilk halka arzından sonra Wall Street Journal tarafından yayımlanan bir çalışma, uzun süreli bir Facebook (Meta) kullanıcısının şirkete değerinin 80,95 dolar olduğunu ortaya çıkarmıştır. Facebook kullanıcısının her bir arkadaşı, 62 sent ederken; profil sayfası ise 1.800 dolar değerindedir... Joron Lannier'in dediği gibi "Facebook'un (Meta) 2012'de satın aldığı Instragram'ın 1 milyar dolar etmesinin sebebi on üç çalışanın olağanüstü düzeyde insan olmasından değil, milyonlarca kişinin kişisel verilerinden oluşmasıydı." (Goodman, 2016).

Birleşik Krallık BT Yönetişiminin Haziran 2021'deki son verilerinde kamuya açıklanan güvenlik olaylarından 9.780.931 tanesinin veri ihlal içerikli olduğu tespit edilmiştir. Kullanıcılar, kişisel bilgilerinin merkezi sistemlerde saklandığı konusunda giderek daha bilinçli olurken, bazı yeni siber suç vakaları, merkezi sistemlerde çevrimiçi olarak depolanan verilerin artık güvenli olmadığını veya en azından eskisinden daha savunmasız olduğunu göstermiştir (Blockco, 2022). Veri ihlalleri, işletmeleri dolandırmak ve kişisel bilgileri ihlal edilenlerin kimliklerini çalmak için kullanılabileceğinden, çalınan verilerin değerli olması gibi nedenlerle potansiyel bir tehlikeye neden olmaktadır (Bellemare, 2017). Onaolapo, Mariconti ve Stringhini (2016), suçluların, ihlal edilen bilgileri kendilerine kâr sağlamak, kamuya açıklamak veya darknet'te satmak için kullandıklarını akademik çalışmalarında belirtmişlerdir (Sharma ve diğerleri, 2020).

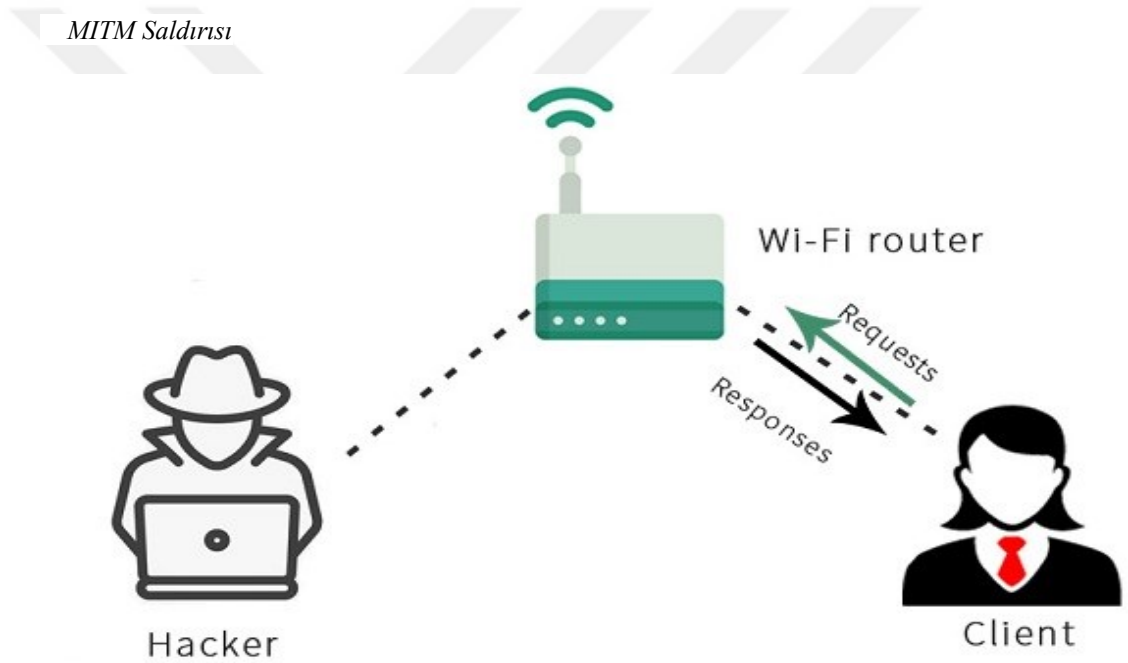
2.2. DİJİTAL ORTAMDA GERÇEKLEŞEN BAZI GİZLİLİK VE GÜVENLİK SORUNLARI

2.2.1. Ortadaki Adam Saldırısı (MITM)

Hassas bilgilerin gizliliği ve güvenliği alanındaki diğer bir risk faktörü ise toplu alanlarda kullanılan ücretsiz Wi-Fi'lerdir. Kullanıcıları için avantajlar sağlamasının yanı sıra büyük potansiyel tehlikeleri de içinde barındırır. Bilgisayar korsanlarının sıklıkla tercih ettiği bir avlanma ortamıdır. Ücretsiz Wi-Fi hizmeti sağlayan alanlar, siber saldırı

türlerinden biri olan “Ortadaki Adam (Man in The Middle)” için oldukça uygun bir zemin hazırlamaktadır. Ortadaki Adam (Man in The Middle) saldırısında bilgisayar korsanı, kullanıcı ile sistem arasında yer alır. Bu sayede kullanıcı ve sistem arasındaki dolaşan verileri ele geçirip değiştirebilmektedir (National Institute of Standards and Technology, 2011). Wi-Fi Dinleme (Wi-Fi Eavesdropping), Oturum Ele Geçirme (Session Hijacking) ve Alan İsimlendirme Sistemi Sahteciliği (DNS Spoofing) MITM Saldırılarının yaygın olarak görülen türleridir.

Şekil 1



Not. Uyarlanmıştır: Sürmelioglu, E. (2022). *Ortadaki Adam MITM Saldırısı Nedir.* <https://hostingdunyam.com.tr/blog/ortadaki-adam-mitm-saldirisi-nedir/>

Örneğin, *şekil 1*’de gösterilen tarayıcı çerez hırsızlığı (Kurabiyelerin Kazınması, Kurabiye Kazıma, Oturum Kaçırma veya Çerez Kaçırma) bir MITM saldırısıdır. Web tarayıcısında özel olarak belirlenmiş bir önbellekte saklanan bir veri parçasına çerez denilmektedir. Kullanıcıya özel tanımlayıcıları veya şahsi bilgileri içerebilmektedir (Örneğin, bu kullanıcı 18 yaşından büyüktür). Çerezler kimlik doğrulama için olmasa da siber dünyada kolay bir geçiş sağlamak için uygun bir zemin sağlamaktadır (Juels, Jakobsson ve Jagatic, 2006). Çerez hırsızlığı ise üçüncü bir tarafın şifrelenmemiş oturum verilerini

kopyalayıp gerçek kullanıcının kimliğine bürünmek için kullandığında meydana gelir (Techopedia, 2011). Kullanıcı adı ve şifre ile gerçekleşen bir girişin lokasyon bilgisi, tarayıcı sürümü, IP ve MAC bilgileri gibi çeşitli bilgileri tarayıcı üzerinde depolandığı için bu bilgileri ele geçiren saldırgan iki aşamalı doğrulamayı bypass (egale) edebilmektedir (Durmuş, 2022). Bu durum sonucunda bilgisayar korsanları başta alışveriş sitelerine kayıtlı kredi kartı bilgileri olmak üzere her bilgiye erişebilmektedir.

2011 yılında Hollandalı yetkili sertifika dağıtıcısı DigiNotar ortadaki adam yöntemi ile hacklenerek, bilgisayar korsanları tarafından pek çok site için sertifika imzalanmıştır. Bu sertifikalarla 300 bin İranlının Gmail kullanımı da dahil olmak üzere pek çok Google servisi kullanımı izlenmiştir. Microsoft konuyla ilgili DigiNotar tarafından en az bir sahte dijital sertifika kullanılarak etkin saldırılar gerçekleştirildiğini, herhangi bir güvenlik açıklarının olmadığını belirtmiştir. Aynı zamanda kullanıcılarını sahte bir sertifikanın kullanabileceği yerleri konusunda ve yeni güncellemesi hakkında bilgilendirmiştir (Microsoft, 2021).

2.2.2. Bait ve Switch

Bilgisayar korsanları, kritik bilgilere ulaşmak ve bu bilgileri istekleri doğrultusunda kullanmak amacıyla birçok yol izleyebilmektedir. Dijital pazarlama tuzağı olarak da kullanılan Bait ve Switch (yem ve anahtar) bunlardan biridir. Bait ve Switch, müşterileri çekmek için bir ürünün çok düşük bir fiyata reklamının yapıldığı ve daha sonra farklı bir ürünün daha yüksek bir fiyata satın almaya ikna edildiği bir satış biçimidir (Cambridge, 2022). Ayrıca Bait & Switch', kullanıcıları kötü niyetli siteleri ziyaret etmeleri için kandırmak için nispeten güvenilir yollar (görüntülü reklamlar) kullanan bir dolandırıcılık türüdür. Bu saldırılar genellikle web siteleri tarafından satılan ve gölgeli şirketler tarafından satın alınan reklam alanı şeklinde gerçekleşir (Cyware Labs, 2019). Müşterinin dikkatini çeken reklam, kötü amaçlı yazılım indirmek, tarayıcıyı kilitlemek veya sistemi tehlikeye atmak için kullanılacak "zararlı" bir bağlantıyla değiştirilir (Malvertising). Alternatif olarak, reklam yasal bir web sitesine bağlantı verebilir ancak müşteriyi zararlı bir siteye yönlendirmek üzere tasarlanmaktadır (Carreiro, 2020). Bunun sonucunda ise saldırıya uğrayan kişi, şahsi özel bilgilerini bilgisayar korsanları ile paylaşmaktadır. Örneğin, Haziran 2016'da web portalı ve çevrimiçi reklamcılık devi Yahoo Malvertising

kurbanı olmuştur. Yahoo kullanıcıları site hızının kontrol edilmesiyle bir reklam görüp tıkladığında bir uzantı indirip bilgisayar korsanları tarafından farklı bir anasayfaya yönlendirilmiştir. Birçok tarayıcı tarafından başarılı olan bu işlem sonrası kullanıcı bilgisayarlarına truva atı bulaştırılmıştır (Vuijsje, 2021). “Clean.io'nun 2020 3. Çeyrek Kötü Amaçlı Reklamcılık İstatistikleri raporu, Malvertising saldırılarının pandemiden sonra ortalama %72 artış gösterdiğini ortaya koymuştur (Mccart, 2022).”

2.2.3. Truva Atı

Meşru görünen ancak aldatma ve sosyal mühendislik kullanarak bilgisayarın kontrolünü ele geçirebilen kötü niyetli kod veya yazılıma “Truva atı” denir. “Verilere veya ağa zarar vermek, bozmak, çalmak veya genel olarak başka zararlı eylemlerde bulunmak için tasarlanmıştır” (Johansen,2020). Çok yönlü bir saldırı aracı olan Truva atlarının Exploit, İndirici, Fidyeye, Arka Kapı (Backdoor), DDoS saldırı, Rootkit, Sahte Av, SMS, Banka (Truva Atı Banker) ve Trojan Game Thief gibi türleri bulunur (Crowdstrike, 2022). Örneğin, 2009 yılında Zeus Truva Atı (Zbot) kötü amaçlı yazılımı, Microsoft Windows işletim sistemini kullanan cihazları hedef alarak hızla yayılmaya başlamıştır. Zeus, Bank of America, NASA, Monster.com, ABC, Oracle, Play.com, Cisco, Amazon ve BusinessWeek gibi şirketlerin web sitelerindeki 74.000'den fazla Dosya Aktarım Protokolü (FTP) hesabını ele geçirmiştir. Sadece ABD bazında bakıldığında 3 milyondan fazla bilgisayar bu saldırıdan etkilenmiştir (Jovanoviç, 2022).

İşletmelerin ve diğer internet kullanıcıların Truva atının zararlarından korunması için: E-postalardaki eklere ve linklere dikkat etmesi, mobil ve sabit sistemleri güncel tutması, Word ve Excel'de makrolara⁵ izin vermemesi, güvenilir kaynaklardan program indirmesi, dosya uzantılarına bakması, ek güvenlik önlemleri kullanması, düzenli bir şekilde virüs taraması yapması ve verilerin yedeklerini alması gereklidir (Kaspersky, 2021).

⁵ Bir görevi otomatik olarak gerçekleştirmek için bir dizi komut ve yönerge.

2.2.4. Keylogger

Bir rootkit⁶ casus yazılım biçimi olan Keylogger, bilgisayarda veya mobil klavyede yazılan her şeyi kaydetmektedir. Görünüşte zararsız yazılım gibi görünebilmekte veya internetten indirilen araçlar içinde saklı olabilmektedir. Kimlik avı e-postaları, sosyal mühendislik, yürütülebilir dosyalar gibi geleneksel kötü amaçlı yazılım sızma yöntemleriyle birlikte de kullanılabilir (Spajic, 2022). Keylogger methodu ile parolalar, dijital bir kayıt formuna girilen kişisel bilgiler (örneğin bir posta adresi veya telefon numarası) ve çevrimiçi bir işlemin parçası olarak sunulan finansal bilgiler dahil bütün bilgiler bilgisayar korsanları tarafından elde edilmektedir (Ahmed, Maarof, Hassan ve Abshir, 2014). Bu durum bireysel internet kullanıcıların veya işletmelerin gizliliğini ve güvenliğini tehlikeye atmaktadır. Bazı işletmelerin çalışanlarını zaman zaman izlemek için keyloggerları kullandığı bilinmektedir “Ancak bir çalışan tuş kaydediciden habersizse, kişisel bilgilerini bir aile üyesi veya arkadaşıyla sohbet veya e-posta yoluyla ifşa edebilir. Bu tür bilgiler oldukça hassas olabilir ve yanlış kullanılırsa yönetici için yasal sonuçlara yol açabilmektedir” (CurrentWare, 2021).

2.2.5. Geofencing Saldırıları

Geofence, akıllı telefonlar ve uygulamalar aracılığıyla tüketicilerin konumlarını gerçek zamanlı olarak takip ederek belirlenen alanın girişini veya çıkışını anında tespit edip şirketlerin ilgili bağlamda kişiselleştirilmiş kampanyaları tetiklemelerine olanak tanıyan sanal bir çittir (Leibbrand, 2017). Geofencing'in çalışma prensibi şu şekildedir; ilki, coğrafi tanım olarak bilinen hedeflenen alanı ayarlamaktır. İkincisi, sanal çevre içindeki verilerin ve/veya bilgilerin toplanması veya dağıtılmasıdır. Çevre, belirli bir noktanın etrafında ya bir yarıçap ya da bir çokgen olarak tanımlanabilir. (Alsaquer, M., Hilton, B., Horan, T., & Aboulola, O. 2015). Bu nokta Küresel Konumlama Sistemine (GPS) göre seçilir, ancak cep telefonu kuleleri, Wi-Fi yönlendiricileri veya beacons (işaretçileri) ile daha doğru hale getirilebilmektedir. Geofencing işletmeler için birçok avantaja sahiptir. Müşterileri ve trafiği işletmeye yönlendirmek, mevcut müşterileri ve potansiyel müşterileri işletmeye çekmek, bağlamsal olarak teklifler promosyonlar ve hediyeler sunarak satış

⁶ Hedef bilgisayar veya ağ üzerinde kontrolü ele geçirmek için kullanılan yazılımdır (Kaspersky, 2022).

hacmini artırmak, ilgili push bildirimleri ile müşterilere bir kazan-kazan iş teklifi sunmak, müşteriler hakkında lokasyona özel verilerle iş zekası elde etmek, iş gücünü uzaktan izleme ve yönetme, karayolu taşımacılığında daha iyi kontrol ve izleme, güvenlik personeli arasında çok daha gelişmiş işbirliği, gerçek zamanlı konum uyarısı ve verileriyle harika etkinlik yönetimi geofence'in sağladığı avantajlardır. Ancak geofence'nin sağladığı faydalar kadar bünyesinde siber güvenlik tehditleri barındırdığı bilinmelidir.

Geofencing, saldırıların beacons tarafından sağlanan verileri toplamasına yardımcı olma potansiyeline sahiptir (Adams, 2020). National Business Investigations, Inc.'de Investigative Case Manager olan Diedre R. Lane, özel bir araştırma firmasıyla yaptığı röportajda, açık kaynak istihbaratı toplamak ve potansiyel olarak hedeflerle ilgili suçlayıcı kanıtları yakalamak için belirli bir konumun coğrafi sınırını belirlemenin kazançlı olmasının mümkün olacağını belirtmiştir (Adams, Lane, 2019).

Gizlilik endişeleri ile gerçek davranış arasındaki tutarsızlık, gizlilik paradoksu olarak bilinir: Kullanıcılar, çevrimiçi gizliliklerini önemsediklerini ancak yine de kişisel ve hassas bilgilerini tereddüt etmeden ifşa ettiklerini belirtmektedir (Acquisti, 2004; Barnes, 2006; Barth ve De Jong, 2017). Bu durum kullanıcıların gizlilik paradoksu yaşadıklarını göstermektedir.

ÜÇÜNCÜ BÖLÜM

3. DİJİTAL PAZARLAMA VE SİBER GÜVENLİK TEHDİTLERİ

Siber güvenlik, dijital pazarlama için büyük önem arz etmektedir. “Siber uzaydaki güvenlik tehditlerin önüne geçmek, çevrimiçi bir iş olan dijital pazarlamada başarı için esastır” (Konyeha,2020). Güvenliği tehdit eden herhangi bir unsur, başta işletmenin kendisi olmak üzere müşterileri, ortakları, işletmenin birlikte çalıştığı kurumları ve domino etkisi yaratarak bu kurumların çalıştığı diğer şirketleri de etkileyebilmektedir. Ayrıca yaşanan güvenlik sıkıntısı işletmenin büyüklüğüne bağlı olarak ülke bazında ekonomik veya sosyal sorunlara neden olabilmektedir. Örneğin, ABD’nin en büyük boru hattını yöneten “Colonial Pipeline” adlı şirketin sistemlerine sızan “DarkSide” isimli bir hacker grubunun bilgisayar korsanları, akaryakıt transferinin devre dışı kalmasına neden olmuştur (Russon, 2021).

“Ülkede 13 eyalette ve Washington DC’de 260 teslimat noktasıyla hizmet veren şirketin boru hattı devre dışı kalmıştır. ABD Ulaştırma Bakanlığı geçici bir kararname yayınlayarak devre dışı kalan akaryakıtın karayoluyla transferinin önünü açarken, yetkililerin tüm uyarılarına karşın kullanıcıların panik halinde benzin stoklaması sonucunda binlerce benzin istasyonunda yakıt sıkıntısı yaşanmıştır. Öyle ki bazı benzin istasyonlarında benzin alımlarına 20 dolar sınır getirilmiştir. Ülke genelinde benzinin fiyatı 2014’ten o zamana kaydedilen en yüksek seviyeye (galon başına 3 doların üstü) ulaşmıştır” (Top, 2021).

3.1. DİJİTAL ORTAMDA İŞLETMELER İÇİN SİBER GÜVENLİK TEHDİTLERİ

Küreselleşen dünya ve her geçen gün gelişen teknoloji ile fiziksel ortamda uygulanan bütün işlemler dijital ortamda gerçekleşmeye başlamıştır. Rachinger, Rauter, Müller, Vorraber ve Schirgi (2019) araştırmalarında günümüzde artan dijitalleşmenin işletmeler arasında yeni iş birliği türlerini mümkün kılarak kurumların iş modelleri (BM’ler) dahil olmak üzere çeşitli iş faaliyetlerini etkilediğini ortaya koymuştur. Dijitalleşme ile işletmeler optimize edilmiş kaynak kullanımı, azalan maliyetler, artan çalışan üretkenliği ve iş verimliliği, optimize edilmiş tedarik zincirleri, artan müşteri sadakati ve memnuniyeti açısından yarar sağlayabilmektedir (Coupette ve diğerleri, 2015). Yeni teknolojilerin

getirdiği dijitalleşmeyle birlikte gelen bu yenilikler, işletmeler içinde değişimi yönlendirme yeteneğine sahip yeni bir dizi uygulama oluşturması sebebiyle pazarları etkilemektedir (Parrales ve Batbayar, 2022). Dolayısıyla dijitalleşmenin getirdiği bu inovasyonlardan etkilenen sektörlerden biri de pazarlamadır.

Pazarlamadaki dijitalleşme, potansiyel müşterilere geniş bir erişim sağlayan yöntemlerde büyük değişimlere yol açmıştır (Bapat, 2018). Ayrıca pazarlama yenilikleri uygulanan işlemlerin daha kısa sürede ve kolay bir şekilde gerçekleştirilmesini sağlamıştır. Bu değişikliklerden birisi olan müşteri ilişkileri yönetimi (CRM) yazılım sistemleri ile dijital pazarlamada müşteri ilişkileri yönetilmekte ve satış öncesinden satış sonuna kadar süreç takip edilebilmektedir. CRM sistemleri aracılığıyla müşterilerini daha iyi tanıyan işletmeler müşteriye özel tanıtımlar yapabilmekte ve fırsatlar da sunabilmektedir. Ancak müşteri ve işletme verilerinin veri tabanında saklanması, müşteri ve işletme bilgilerinin gizliliği, dikkatli bir şekilde korunma gerektirmektedir. Bu durum ise dijital pazarlamada işletmelerin siber güvenliğe vermesi gereken önemi artırmaktadır. Check Point (Siber güvenlik firması) 2021’de yaptığı araştırmada, 2020’ye kıyasla kurumsal ağlara yapılan haftalık genel saldırılarda %50 artış olduğunu ve küresel olarak kuruluş başına haftada 925 siber saldırının gerçekleştiğini tespit etmiştir (Gmcdouga, 2022).

Bilgisayar korsanları (Hackerlar), işletmelerin dijital ortamdaki zaafiyetlerini bulup siber saldırı gerçekleştirerek hassas bilgileri ele geçirebilmekte ve bu bilgileri kendi çıkarları için sömürebilmektedir. Kötü amaçlı yazılımlar (Malware), DNS Saldırıları (Sıfır gün saldırısı (zero day exploit), Önbellek zehirlenmesi (DNS spoofing), Dağıtılmış Hizmet Reddi (DDoS), DNS amplifikasyonu, Fast-flux DNS, DNS tünelleme (DNS Tunneling)) Oltalama (Phishing) bilgisayar korsanlarının uyguladığı dijital ortamdaki siber saldırı türlerinden sadece birkaçıdır.

Kötü amaçlı yazılımların %80’ini komut ve kontrol (C2) oluşturmak için kullanılan DNS oluşturmaktadır. İşletmelerin DNS trafiğini izlemesi ve analiz etmesi bu sebeple son derece önem arz etmektedir. İşletmeler tarafından DNS trafiği izlenmeli, DNS tabanlı tehditler için algoritmalar kullanılmalı, veriler yüksek kaliteli ve işletmeler DNS trafiğinde tam görünürlük ve bağlama sahip olmalıdır (Mandalam, 2021).

Positive Technologies Cybersecurity Threatscape 2021 Q1 raporuna göre, siber saldırıların sayısı 2020’nin ilk çeyreğine kıyasla %17 artmış ve 2020’nin 4. Çeyreğine

kıyasla artış %1,2 olmuştur ve bunun %77'sini hedefli saldırılar oluşturmuştur (Positive Technologies, 2021).

Özellikle KOBİ'ler siber saldırıların hedefi durumunda bulunmaktadır (Duman, 2021). Bunun sebebi ise küçük işletmelerin, büyük işletmelerden daha basit bir hedef olarak görülmesidir. Küçük işletmelerin çoğu kendilerine bir siber saldırı olmayacağını varsayıp önlem almazken, büyük işletmeler son yıllarda karşılaşılabilecekleri siber saldırılardan korunmak için güvenlik sistemlerini daha donanımlı hale getirmektedirler (Çatuk, 2018). Öte yandan dünyanın önde gelen şirketleri her ne kadar siber güvenliğe büyük yatırımlar yapsa da siber saldırılara hala uğrayıp zarar görebilmektedir. Facebook (Meta), Clubhouse, Pegasus Airlines, Acer ve Cd Projekt Red siber saldırılardan etkilenen büyük ölçekli işletmelerden bazılarıdır.

Clubhouse, 2020 yılında yazılım geliştiricileri Alpha Exploration Co. Tarafından başlatılan, yalnızca davetiyeyle kullanılabilen, sesli sohbet içeren bir sosyal ağ uygulamasıdır. Aralık 2020'de yaklaşık 100 milyon ABD doları değerinde olan şirket 21 Ocak 2021 tarihinde bir milyar dolar piyasa değerine ulaşmıştır. App Store'da sekiz milyon kez indirilen uygulama olağanüstü bir ivme yakalamıştır. Elon Musk ve Mark Zuckerberg gibi ünlü isimler bile Clubhouse'a ilgi göstermiştir. Yaşanan olay ise siber saldırıya açık olduğunu ortaya koymuştur. Uygulamaya düzenlenen siber saldırı sonrasında, saldırıyı düzenleyen kişinin Clubhouse'un sohbet odasındaki konuşmaları kendi web sitesinde yayınladığı ortaya çıkmıştır. Siber saldırgan Clubhouse uygulamasına erişebilmek için JavaScript araç takımı etrafında kendi sistemini kurmuştur. İçeriye bu şekilde giriş yapan saldırganın kimliği veya saldırıyı nerede yaptığı ise belirlenememiştir (Sarıkaya, 2021).

Cyber News'in aktardığı habere göre; kullanıcı bilgilerini içeren SQL veri tabanı tamamen ücretsiz bir şekilde yayınlanmıştır. Çalınan bilgiler arasında ise; kullanıcı kimliği, isim, fotoğraf URL'si, kullanıcı adı, Twitter kullanıcı adı, Instagram kullanıcı adı, takipçi sayısı, kullanıcının takip ettiği kişilerin sayısı, hesabın oluşturulma tarihi, hesabın davet edildiği profilin ismi gibi bilgiler yer almaktadır. Siber saldırıdan 1,3 milyon Clubhouse kullanıcısının etkilendiği tespit edilmiştir. Clubhouse sözcüsü; bir kullanıcının birden çok odadaki sesli sohbet akışını kendi internet sitesine yönlendirdiğini ve bu güvenlik açığından faydalanan kullanıcının bir daha Clubhouse'u kullanamayacak şekilde

engellendiğini, bu tür güvenlik açıklarının olmaması için yeni güvenlik tedbirleri aldıklarını açıklamıştır.

Yeni bebeği olmuş bir baba olan Halil Erdoğan'ın bebek bakımıyla ilgili bilgi edinme ihtiyacına istinaden kurduğu e-bebek.com, 2001 yılından itibaren anne-babalara ve anne baba adaylarına hizmet vermek için kurulan bir web sitesidir. Türkiye çapında 52 ilde 161 mağazaya sahip ebebek.com bebek ürünleri alışverişi konusunda Türkiye'nin ilk online mağazası olma özelliğini taşımaktadır.

Bebek ürünleri satışı gerçekleştiren internet siteleri arasında yer alan e-bebek'in sitesine girmek isteyenler 5 Temmuz 2020'de hata kodu ile karşılaşmışlardır. Siber saldırıdan dolayı e-bebek müşterileri, web sitesi ve mobil uygulamalar üzerinden alışveriş gerçekleştirememiştir. Ödeme sistemlerinin de saldırıya uğraması neticesinde fiziksel mağazalarda merkeze bağlanamama sorunu yaşanmış ve bütün işlemler manuel olarak gerçekleşmiştir. Yaşanan bir DDoS saldırısıdır⁷. 5 Temmuz 2020 tarihinde sabah 03:19 itibarıyla yoğun bir şekilde gelen DDoS saldırılarının ardından site tamamen devre dışı kalmıştır. Yetkililerce kullanıcıların kredi kartı bilgilerinin çalınmadığı ifade edilmiştir ancak diğer veriler ile ilgili olarak net bir açıklama yapılmamıştır. E-bebek sitesinin hizmetini durdurmaya yönelik yapılan saldırı sadece DDOS değildir. Aynı zamanda ebebek.com'un verilerinin şifrelendiği ve sanal ortamdaki bilgilere göre hackerların 300 Bitcoin istediği söylenilmiştir.

Türk Veri Koruma Otoritesi (KVKK), 24 Mart 2022'de Yonca Sağlık Hizmetleri Ltd. Şti. bünyesinde bir veri ihlali meydana geldiğini duyurmuştur. KVKK, özellikle 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 12(5) maddesi uyarınca veri sorumlusu olan Martı İleri Teknoloji'nin siber saldırı gerçekleştiğini KVKK'ya bildirdiğini vurgulamıştır. Ayrıca KVKK, saldırının tipik bir fidye yazılımı veya DDoS saldırısı olmadığını ve siber saldırının türünün halen araştırıldığını kaydetmiştir.

Ayrıca KVKK, siber saldırının 15 Mart 2022 tarihinde gerçekleştiğini ve Yonca Sağlık Hizmetleri Bilgi İşlem Müdürü tarafından 16 Mart 2022 tarihinde alınan bir e-posta ile tespit edildiğini vurgulamıştır. Yonca Sağlık Hizmetleri ihlalden etkilenen tahmini kişi sayısı 500.000 ve tahmini kayıt sayısı 2,5 milyondur. Bunun yanı sıra KVKK,

⁷ DDoS, bir sistemi belirli kapasite sınırlarının üstünde veriye maruz tutma yoluyla düzenlenen saldırılar sonucu kullanıcıların sisteme veya siteye girişinin engellenmesidir.

etkilenen kişisel veri kategorilerinin sağlık verileri, ceza mahkûmiyeti ve güvenlik önlemleri verileri gibi hassas verileri ve genetik verileri içerdiğini vurgulamıştır (DataGuidance, 2022).

3.1.1. Hybrid Çalışma ve Kendi Cihazını Getir Uygulaması (BYOD)

İşletmelerin yaptığı yenilikler de siber güvenlikte zafiyetlere sebep olabilmektedir. Günümüzde özellikle pandemi sonrası daha çok görülmeye başlanan Hybrid çalışma modeli (belirli günlerde ofis içerisinde, belirli günlerinde ise ofis dışında çalışma) ve diğer popülerleşen “Kendi Cihazını Getir Uygulaması (BYOD)” siber güvenlikte zafiyetlere sebep olan yeniliklerdendir. İşletmeler tarafından BYOD uygulaması; esnek çalışma sağlamak, verimliliği artırmak, maliyetleri düşürmek ve çalışanlara kendilerini rahat hissettikleri BT’yi kullanma fırsatı vermek amaçlarıyla kullanılmaya başlanmıştır. Ancak “Uzaktan çalışma sonucu kişisel dizüstü bilgisayarlardan ve hatta akıllı telefonlardan gizli şirket verilerine erişim, dikkatsiz bir çalışanın tüm kuruluşun siber güvenliğini tehlikeye atabileceği anlamına gelebilmektedir” (Allen, Bloom, & Janes, 2019). İşletme çalışanın farkında olmadan yaptığı basit bir hata bile işletmenin yaşam döngüsünü olumsuz yönde etkileyebilmektedir. Çalışanın güvenilmeyen mobil işletim sistemi, uygulamaları, ağları kullanması, uzaktan bağlanmak için kullanılan araçların siber saldırıya uğraması, kurumsal e-posta adreslerinin phishing (bilinen birini taklit etmek) saldırısına uğraması, uzak masaüstü protokolünün (RDP) ‘reverse attack’ (tersine saldırı) yöntemiyle BT ağını tamamen ele geçirmesi veya kötü amaçlı yazılım yüklenmesi, fiziksel güvenlik kontrollerinin eksikliği işletmeleri siber tehlikelere daha açık hale getiren etkenlerdendir. Bilgisayar korsanlarının saldırıları dışında, çalışanlar da bazı durumlarda bilinçli bir şekilde getirdikleri cihazları kötüye kullanabilmektedir. Bu sebeple işletmeler bu konu oldukça temkinli olmak zorundadır.

3.1.2. İş E-Postası Uzlaşması

İşletmelerin teknolojinin getirdiği fırsatlardan faydalandığı ancak siber zafiyetlere sebep olabilen bir diğer yenilik ise e-posta pazarlamasıdır. Potansiyel veya mevcut bir müşteriye gönderilen her e-posta, e-posta pazarlaması olarak tanımlanır (Fariborzi ve

Zahedifard, 2012). Maliyet, kısa iletim süresi, izleme ve analiz kolaylığı, verileri kategorize etme ve kişileştirme gibi olanaklardan dolayı birçok işletme e-posta pazarlamasını kullanmaktadır (IOVA, 2019). E-posta pazarlamasına harcanan her 1 ABD doları için ortalama 36 ABD doları yatırım getirisi (ROI) sağlanmaktadır (Link, 2022). Kimlik avı veya sosyal mühendislik saldırıları ile siber suçlular bu pazarlama türünü işletmeyi taklit ederek kendi çıkarları için kullanabilmekte ve işletmelerin itibarını zedeleyebilmektedir. 2021 Tessian araştırmasında, phishing saldırılarında en yaygın olarak taklit edilen markaların Microsoft, ADP, Amazon, Adobe Sign, Zoom olduğunu tespit etmiştir. Tüm bu markaların ortak özelliği ise güvenilir ve çoğunlukla müşterileriyle e-posta yoluyla iletişim kurmalarıdır (Rosenthal, 2022).

Bilgisayar korsanlarının gönderdiği e-postalardan işletmeler veya kurumlarda etkilenmektedir. 1999 yılında David L. Smith isimli bir yazar tarafından tasarlanan “Melissa Virüsü” e-posta ile yayılarak işlerinde Microsoft’un da yer aldığı pek çok firmanın sistem ağlarını etkileyerek 80 milyon dolarlık hasara uğratmıştır (Yeniçağ Gazetesi, 2022). Başka bir örnek ise 4 Mayıs 2000’de yaşanan “ILOVEYOU” yazan bir e-postanın açılıp kullanıcılar arasında yayılmasıyla meydana gelmiştir. Alıcılar e-postayı açarak ILOVEYOU (“aşk mektubu virüsü” ve “aşk böceği solucanı”) virüsünün (aslında solucan) Microsoft Outlook adres defterindeki herkese yeniden gönderilmesine aracılık etmekle beraber alıcıların sabit disklerindeki tüm JPEG, MP3 ve diğer bazı dosyaların kaybolmasına yol açmıştır. Yaklaşık 10 gün içinde ILOVEYOU virüsü tahmini 45 milyon kullanıcıya etkilemiş ve yaklaşık 10 milyar dolar zarara mülk olmuştur. Ayrıca oldukça hızlı bir şekilde yayılan “ILOVEYOU” virüsü, Ford Motor Company, AT&T ve Microsoft gibi birçok işletmenin yanı sıra Pentagon, CIA, ABD Ordusu gibi hükümet kuruluşlarının, Danimarka ve Birleşik Krallık’taki parlamentoların e-posta hizmetlerini kapatmasına neden olmuştur (Awati, 2021).

Gizli iş bilgilerine erişim veya bu bilgilerin değiş tokuşunu gerektiren çeşitli harici satıcılar ve platformlarda pazarlama ekibi, virüslü e-posta mesajını açarak kötü amaçlı yazılımı aktif edebilmektedir. Bunun yanı sıra kimlik doğrulaması olmadan işletmeler, kimlik avı ve spam e-postaları göndermek için alanlarını kullanan siber suçlulara karşı savunmasız kalmaktadır. Etki Alanı Tabanlı Mesaj Kimlik Doğrulaması (Domain-Based Message Authentication), Raporlama ve Uygunluk, e-posta kimlik doğrulaması için

gerekli standartlardır. DMARC'ı (e-posta kimlik doğrulama protokolü) benimseyen işletmeler, yalnızca onaylı kuruluşların kendi adlarına e-posta gönderebileceğini garanti etmektedir. Aynı zamanda DMARC'ın temel katmanını oluşturduğu yetkilendirilmiş sunucu/alan veya dijital imza protokolleri (SPF ve DKIM) etkili bir şekilde kullanılarak e-posta teslim edilebilirliğini artırmaktadır (García-Tobar, 2022). Ayrıca Mesaj Tanımlama için Marka Göstergelerinin (BIMI) kullanılması, İnternet Servis Sağlayıcı (ISS) ve e-posta uygulamaları için markanın logosunu e-posta istemcisinde görüntülemeleri için bir araç sağlamaktadır (Karr, 2022).

İş E-Postası Uzlaşması (Business Email Compromise ya da Email Account Compromise), genellikle farklı ülkelerden ürün tedarik eden ve banka havalelerini, fon transfer etmek için düzenli bir yol olarak kullanan işletmeleri hedef alan gelişmiş bir e-posta dolandırıcılığıdır (Agazzi, 2020). Sosyal mühendislik ve deepfake teknolojisi kullanılarak genellikle BEC dolandırıcılığı gerçekleştirilir.

3.1.2. Deepfake

Deepfake'ler, bir kişinin sana söylemediği veya yapmadığı bir şeyi söylediğini veya yaptığını göstermek için kullanılan çarpıtılmış videolar, görüntüler veya ses kayıtlarıdır (iProov, 2020). BEC dolandırıcılığının beş türü yaygın olarak kullanılır (Panwar, 2022). Bu beş tür şunlardır: CEO Sahtekarlığı (CEO Fraud), Sahte Fatura (Bogus Invoice), Hesap Uzlaşması (Account Compromise), Avukat Kimliği (Attorney Impersonation), Veri Hırsızlığı (Data Theft). CEO Sahtekarlığı adından da anlaşılabilceği gibi siber suçlu CEO gibi davranarak veri ya da ödeme talebinde bulunur. Hesap Uzlaşmasında, siber suçlu işletme çalışanın e-posta hesaplarını ele geçirerek isteklerde bulunur. Sahte Fatura da siber suçlu işletmenin işbirlikçi gibi davranarak sahte fatura gönderir. Avukat kimliğinde saldırgan, bir avukat olduğunu belirtir ve siber suçlu, hesaba para aktarmayı ya da hassas şirket bilgilerini öğrenmeye çalışır (Tavares, 2018). Veri Hırsızlığı türünde ise üst düzey yöneticiler taklit edilerek İnsan Kaynakları departmanındaki çalışanlardan bütün çalışanlar hakkında kişisel bilgiler elde edilmeye çalışılır. Çünkü elde edilen kişisel bilgiler farklı bir siber saldırı senaryosunda işe yarayabilmektedir.

İşletme çalışanları siber saldırganlara karşı oldukça dikkatli olmalıdır. FBI'nın bu konuda önerisi, çalışanların sosyal medya hesaplarında paylaştıkları bilgilere dikkat

etmesi, hesap bilgilerinin doğrulanmasını veya güncellenmesini isteyen maillere temkinli yaklaşılması, maildeki numara yerine şirketin kendi numarasının aranıp işlemin sorgulanması, e-posta adresinin, URL'nin ve yazımın doğruluğunun kontrol edilmesi, bilinmeyen maillerdeki eklerin açılmaması veya herhangi bir indirme yapılmaması, iki faktörlü doğrulamanın kullanılması, mesajda aciliyet belirtiliyorsa özellikle dikkatli olunması şeklindedir (FBI, 2020).

3.1.2.1. Deepfake Saldırı Örnekleri

Şubat 2016'da siber suçlular, sosyal medya şirketi Snapchat'e karşı bir BEC saldırısı başlatmıştır. Saldırganlar, Snapchat'in CEO'sunu taklit ederek "bazı mevcut ve eski çalışanlar hakkında bordro bilgilerini bu sayede elde etmiştir. Yaşanan BEC saldırısı, çalışanların Sosyal Güvenlik Numaraları, vergi bilgileri, maaşları ve sağlık planları dahil olmak üzere bazı son derece hassas verilerin ihlaliyle sonuçlanmıştır. Snapchat, etkilenen her çalışana iki yıl ücretsiz kredi izleme ve 1 milyon dolara kadar geri ödeme teklif etmiştir (Rosenthal, 2022).

Toyota yan kuruluşunun iş ortağı gibi davranan üçüncü taraf bir bilgisayar korsanı, finans ve muhasebe departmanı üyelerine e-postalar göndererek, ödeme için fonların şirket tarafından kontrol edilen belirli bir banka hesabına gönderilmesini talep etmiştir. Daha küçük ölçekli işletmelerde 37 milyon dolarlık bir ödeme her türlü alarm ve uyarıyı tetikleyecek ve ödemeyi yapmadan önce çalışanın birden fazla imza ve onay almasını gerektirecek olsa da Toyota'da bu ödeme makul bir ödeme olarak gözükmüştür. Bu nedenle, Avrupa'daki yan kuruluşun çıkan 37 milyon dolarlık bir fon transferi, başlangıçta orta düzey çalışanların dikkatini çekmemiştir. Yapılan siber saldırı, Toyoto'ya o yıl içinde yapılan üçüncü saldırı olmakla birlikte bunun sonucunda şirket 37 milyon dolar kayba uğramıştır (Rosenthal, 2022).

Haziran 2014'te, Nebraska, Omaha'da bulunan bir şirket olan Scouler Co'da çalışan Keith McMurtry, sözde patronu CEO Chuck Elsea'dan bir e-posta almıştı. E-postada McMurtry'ye Scouler'in bir Çinli şirketi satın almaya hazır olduğu bildirilmişti. Sözde Elsea (CEO), McMurtry'ye muhasebe firması KPMG'den bir avukatın, para transferini kolaylaştırmaya ve anlaşmayı kapatmaya yardımcı olacağını söylemiş ve avukatla

iletişime geçmesi talimatını vermişti. Bu talimat üzerine McMurty “Dadi Co” adına bir Şanghay banka hesabına 17,2 milyon dolar aktarmıştı. Fakat yaşanan bu olayda CEO’nun e-postası sahteydi. Dolandırıcılar hem Elsea’yı hem de KPMG avukatını taklit eden hesaplar oluşturup kendilerine bir e-posta oluşturmuşlardı. Saldırı sonrası Scouler Co, 17,2 milyon dolarlık bir kayba uğramıştır (Rosenthal, 2022).

BEC/EAC dolandırıcıları, genellikle büyük ölçekli işletmeler veya kişileri hedef almak yerine küçük yerel işletmeleri tercih etmektedir. Temmuz 2019 ile Aralık 2021 arasında, iş e-postası dolandırıcılığından kaynaklandığı tespit edilen küresel kayıpların sayısında %65’lik bir artış olduğu tespit edilmiştir. Bu artışın kısmen COVID-19 salgını sonrası getirilen kısıtlamalardan dolayı işletmelerin ve bireylerin sanal ortama daha çok taşınmasından kaynaklandığı tahmin edilmektedir. Haziran 2016-Aralık 2021 zaman diliminde, IC3 tarafından elde edilen veriler ise BEC dolandırıcılığında kripto para kullanımının arttığını göstermektedir. Kripto para birimi, finansal işlemleri güvence altına almak için kriptografiyi⁸ kullanan bir sanal varlık biçimidir. Yüksek derecede anonimlik ve işlemlerin gerçekleşme hızı nedeniyle yasa dışı aktörler arasında popülerdir (IC3, 2022).

Vishing olarak da bilinen Voice phishing (sesli oltalama) telefon aracılığıyla (Telephone Oriented Attack Delivery: Telefona Yönelik Saldırı Dağıtımı) eylemi gerçekleştirmeye veya etkilemeye çalışma uygulamasıdır. Bir sosyal mühendislik tekniğidir. Yaygın bir taktik, otoritenin kullanılmasıdır (U.S. Department of Health and Human Services Health Sector Cybersecurity Coordination Center, HC3: Analyst Note, 2022). Arayan kişi hesapta çıkan bir sorun yüzünden arayan teknik destek çalışanı veya çeşitli sorunlar sebebiyle arayan bir devlet görevlisi olabilmektedir. Kurban aranır ve senaryoya göre kurban ikna edilmeye çalışılır. Bu senaryo kurbanın sistemine kötü amaçlı yazılımı dağıtmak için bir bağlantıya tıklanmasını, talimatları izlemesini sağlamaya yöneliktir (Cyber Security Awareness Newsletter,2022). Aramalarda tanınan kişilerin sesleri de taklit edilebilmektedir. Audio deepfakes gerçek gibi görünen sahte ses oluşturmak için tekrarlama, konuşma sentezi, ses dönüştürme methodlarıyla AI tarafından oluşturulur veya düzenlenir/sentezlenir (Khanjani, Z., Watson, G., & Janeja, V. P. ,2021).

⁸ İletişim güvenliğini sağlamak için kodlanmış mesajların kullanılmasıdır.

Mart 2019’da İngiltere’deki bir enerji sağlayıcısının CEO’su, sesi tam olarak (hafif Alman aksanıyla) patronuna benzeyen birinden bir telefon aldı. Arayan, firmanın Alman ana şirketinin genel müdürünü taklit etti ve kurbanı bir “Macar tedarikçiye” 220.000 € (243.000 \$) göndermesini istedi. CEO taleplere uydu ve parayı “tedarikçinin” hesabına aktardı. Daha sonra hesabın siber dolandırıcıya ait olduğu ortaya çıktı. Dolandırıcı, ana şirketin CEO’su olarak başka bir arama yapmaya çalıştı, bu sefer İngiltere’deki şirkete bir geri ödeme gönderdiklerini iddia ederek ikinci bir transfer yapılmasını istedi. Ancak, kimsenin geri ödeme hakkında hiçbir şey bilmediği ve aramanın Avusturyalı bir telefon numarasından gelmesi nedeniyle, mağdur şüphelendi ve aramayı bildirdi (Jirik, 2022). Bu tarz saldırılarda kişisel veriler asla verilmemeli, iletişime geçen kişinin telefon numarası doğrulanmalı, ödeme olarak hediye kartı veya ön ödemeli krediler kullanılmamalı, asla uzaktan bilgisayar erişimi sağlanmasına izin verilmemeli ve şüpheli olaylar ilgili kişilere bildirilmelidir (Vega, 2022).

3.1.3. Endüstri 4.0 Teknolojisi

İşletmelerin siber güvenliğinde meydana gelen siber zafiyetlere yeni teknolojilerde neden olabilmektedir. Bunlardan biri de Endüstri 4.0 teknolojisidir. Endüstri 4.0, üretimi gerçek zamanlı olarak destekleyen kararlar almak için fiziksel dünyayla bağ kuran “akıllı” ve bağlantılı üretim sistemlerini ifade etmektedir (Sirimanne, 2022). Başka bir ifadeyle “üretimin siber-fiziksel dönüşümüdür” (Daniel, 2022). Yapılan bir araştırmada üreticiler tarafından uygulanan ilk beş Endüstri 4.0 teknolojisi⁹ arasında ilk sırada %85 oranla bulut bilişim yer almaktadır (Wright, 2017). İşletme bulutu; veri yedekleme, olağanüstü durum kurtarma, e-posta, sanal masaüstleri, yazılım geliştirme ve test etme, büyük veri analitiği ve müşteriye dönük web uygulamaları gibi alanlarda kullanabilmektedir (AWS, 2022). Öte yandan yanlış yapılandırılmış bulut hizmetleri; veri kaybı, uygulama programlama arayüzü (API) güvenlik açıkları, kötü amaçlı yazılım saldırıları, yetersiz erişim yönetimi kontrolleri bulut güvenliğinin işletmeler üzerinde yarattığı siber risklerdir (Mehdar, 2022). Bunların dışında; Nesnelerin İnterneti (IoT), Siber Fiziksel Sistemler

⁹ Diğerleri şunlardır: Tesis Operasyonlarında Bağlantılı Sensörler (%65), Ürünlerde Bağlantılı Sensörler (%59), 3D Baskı (%39), Gelişmiş Veri Analitiği Araçları (%34).

(CPS), Büyük Veri ve Veri Analitiği, 3D Baskı, Artırılmış Gerçeklik (AR), İşbirlikçi Robotlar, Katmanlı Üretim, Yapay Zekâ (AI) ve 5G ağlar ise Endüstri 4.0 kapsamında kullanılan ancak içinde siber tehlikeleri bulunduran diğer teknolojilerdir (Ortiz, 2020).

3.1.3.1. Endüstri 4.0 Teknolojisi ve 5G Teknolojisi

Temelleri 2008 yılına dayansa da 2018 yılında dünyada ilk kez Güney Kore’de hayata geçen 5G teknolojisi işletmeleri etkisi altına almaya başlamıştır (Rijmenam, 2022). 5G teknolojinin sağladığı bant genişliği, güvenilirlik ve akış hızlarındaki artışlar; işletmelerin IoT, AI ve Makine Öğrenimi gibi gelişmiş veriye dayalı teknolojileri yüksek verim ile kullanmasına yardım etmektedir (Bandaru, 2021). Sürücüsüz araçlar, sanal gerçeklik (VR), AR, akıllı evler, uzaktan cerrahi operasyonlar ve online medya tüketimi 5G teknolojinin tüketiciler tarafından kullanmasına dair örneklerden bazılarıdır (Aykut, 2021). 5G teknolojisi, işletmeler için de büyük avantajlar sağlamaktadır. Örneğin, hızın artması daha fazla ticari işlemin daha kısa sürede gerçekleştirilmesine, düşük gecikmenin hataların ve gecikmelerin önüne geçmesine, artan kapasite ile daha fazla cihaz & insanla iletişim kurulmasına, fiziksel altyapı üzerinde birçok sanal ağın oluşturulmasına izin veren bir ağ dilimleme (Network Slicing) ile işletmelerin kendi özel 5G ağlarına sahip olmasına olanak tanımaktadır (Taberner, 2020).

Bununla birlikte 5G teknolojisi yeni siber güvenlik açıklarını ve siber tehditleri beraberinde getirmektedir. Merkezi olmayan güvenlik (çok daha fazla trafik yönlendirme nokta), bant genişliğinin mevcut güvenlik denetimini zorlaştırması, birçok IoT cihazının güvenlik eksikliğiyle üretilmesi bunlardan bazılarıdır (Kaspersky, 2020). Amerika Birleşik Devletleri İç Güvenlik Bakanlığı’nın (DHS) bir kurumu olan Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA), bu tehdit vektörlerini “Politika ve Standartlar Alt Tehdit Vektörleri, Tedarik Zinciri Alt Tehdit Vektörleri, 5G Sistem Mimarisi Alt Tehdit Vektörleri” olmak üzere üç başlık altında incelemiştir.

Örneğin, güvenilmeyen tescilli teknolojilerle birlikte çalışabilirlik eksikliği, güvenilir şirketlerin 5G pazarında rekabet etme yeteneğini sınırlamakta, ürünün yaşam döngüsü maliyetini artırmakta ve ekipmanın değiştirilmesi gerekiyorsa 5G dağıtımını geciktirmektedir (Politikalar ve Standartlar Alt Tehdit Vektörleri – Açık Standartlar).

Tablo 2*5G Altyapılarına Yönelik Potansiyel Tehdit Vektörleri*

Politika ve Standartlar Alt Tehdit Vektörleri	Tedarik Zinciri Alt Tehdit Vektörleri	5G Sistem Mimarisi Alt Tehdit Vektörleri
❖ Açık Standartlar	❖ Sahte Bileşenler	❖ Yazılım/Konfigürasyon
❖ Opsiyonel Kontroller	❖ Miras Alınan Bileşenler	❖ Ağ Güvenliği
		❖ Ağ Dilimleme
		❖ Eski İletişim Altyapısı
		❖ Çoklu Erişim Uç Bilgi İşlem
		❖ Spektrum Paylaşımı
		❖ Yazılım Tanımlı Ağ

Not. Uyarlanmıştır: CISA. (2021). *Potential Threat Vectors to 5G Infrastructure*. https://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-infrastructure_508_v2_0%20%281%29.pdf

3.1.3.2. Endüstri 4.0 Teknolojisi ve Tedarik Zinciri

İlk olarak 1980’lerin başında ortaya çıkan ve işletmelerin oldukça önem verdiği “Tedarik Zinciri Yönetimi” kavramı artan küreselleşme ve teknolojinin gelişimi ile popülerleşmeye başlamıştır. Eski ABD Ulusal Güvenlik Ajansı bilgi güvenliği teknik direktörü Richard George, “siber güvenliğin gerçekten bir tedarik zinciri sorunu olduğunu” belirtmiştir (Carter 2020). Teknolojik gelişmelere uyum sağlayan işletmeler tedarik zincirinde Yapay Zekâyı, Makine Öğrenimini, Blok Zincirini ve Dijital ikizleri ile süreçlere daha fazla verimlilik ve şeffaflık getirdiği için kullanmaya başlamıştır. Bu kavramlar teknolojiye bağlı olmakla birlikte işletmeleri siber alandaki saldırılara da açık bir hale getirmiştir. Bilgisayar korsanları yaptıkları siber saldırılar ile işletmelerin tedarik zincirini sekteye uğratmaktadır. Bir saldırı başlatmak için bir kuruluşun sistemine veya verilerine erişimi olan bir üçüncü taraf iş ortağı veya sağlayıcının kullanılması “tedarik zinciri saldırısı” olarak bilinir (Fruhlinger, 2017). Tedarik zinciri saldırıları, “Donanım Yoluyla Gerçekleştirilen Tedarik Zinciri Saldırıları, Yazılım Yoluyla Gerçekleştirilen Tedarik Zinciri Saldırıları, Firmware Yoluyla Gerçekleştirilen Tedarik Zinciri Saldırıları” olmak üzere toplamda üç başlık altında incelenebilmektedir (Kron, 2021).

Örneğin, büyük bir Amerikan bilgi teknolojisi (BT) firması olan SolarWinds, tedarik zinciri saldırısına uğramıştır. Bilgisayar korsanları, 33.000’den fazla şirket tarafından BT kaynaklarını yönetmek için yaygın olarak kullanılan SolarWinds’ın Orion

yazılımını ele geçirmişlerdir (Jibillian 2020). Öncelikle bilgisayar korsanları tarafından kurban kuruluşların hesaplarını ve kullanıcılarını taklit etmek için erişilebilecek bir arka kapı (Backdoor)¹⁰ oluşturulmuştur. Daha sonra bu arka kapı, bilgisayar korsanlarının sistem dosyalarına erişmesine ve Orion etkinliğine karışarak izlerini gizlemesini sağlamıştır. Ayrıca kötü amaçlı kodu antivirüs paketlerinden gizlemesine olanak tanımıştır (Jena, 2022). Yapılan güncelleme ile arka kapı kullanılarak kısa bir sürede 18.000’den fazla kuruluş kötü amaçlı güncellemeyi indirerek en az 9 federal kurumun ve 100’ün üzerinde şirketin bu saldırıdan etkilenmesine yol açmıştır. Adalet ve İç Güvenlik Departmanları, ABD devlet kurumlarının yanı sıra FireEye ve Microsoft dahil olmak üzere teknoloji devleri bunlardan bazılarıdır (Kisielius, 2021).

“Tedarik zinciri boyunca siber güvenlik risklerine maruz kalmayı yönetme ve bu risklerle mücadele etmek için müdahale stratejileri, politikaları, süreçleri ve prosedürleri geliştirmek gereklidir” (Adalet Bakanlığı Genel Müfettiş Ofisi, 2022). Siber Güvenlik Tedarik Zinciri Risk Yönetimi (C-SCRM) olarak tanımlanan bu kavram, bir işletmenin maruz kaldığı siber olaylara tepki yeteneğini geliştirerek tedarik zincirinin tehlikeye girme olasılığını azaltmaktadır (Rouse, 2022).

Tedarik zinciri, 5G teknolojisinin beraberinde getirdiği yüksek erişilebilirlik, yüksek bant genişliği ve IoT cihazlarını yönetecek güçlü ağıyla birçok fırsata olanak sağlamasının yanı sıra siber tehditlere daha çok davetiye çıkartmaktadır. 5G teknolojisinin alt yapısı tedarik zincirine dışarıdan müdahale edilme ihtimalini ve tehdit aktörlerinin sabotaj, manipülasyon, verilere müdahale ve casusluk benzeri faaliyetler sonucunda veri ve fikri mülkiyet hırsızlığı olaylarının artmasına yol açacağı düşünülmektedir (Kron, 2021).

3.1.3.3. Endüstri 4.0 Teknolojisi ve Radyo Frekansı ile Tanımlama (RFID)

Tedarik zincirindeki üretimden tüketici kadar olan süreçte envanteri izlemek için kullanılan Radyo Frekansı ile Tanımlama (RFID) teknolojisi de siber risklerle karşı karşıyadır. RFID teknolojisinin işletmelerde ve tüketicilerin günlük yaşamlarında artan etkileşimi, mahremiyet endişelerini artırmıştır (Khoo, 2011). “RFID etiketler, hassas bilgilere

¹⁰ Backdoor: Belirli bir İletim Denetimi Protokolü (TCP) veya Kullanıcı Veri Birimi Protokolü (UDP) bağlantı noktasındaki komutları dinleyen kötü amaçlı bir programdır (NIST Special Publication 800-83 Revision 1, 2013).

yetkisiz erişime karşı savunmasızdır ve veri gizliliği sorunları yaratmaya eğilimlidir. RFID etiketleri ve RFID okuyucuları, benzersiz Elektronik Ürün Kodu (EPC) aracılığıyla iletişim kurmaktadır. Kötü niyetli bir davetsiz misafir, RFID okuyucularına veya bir EPC'ye erişmeyi başarır, gizli etiketleri ele geçirebilmekte ve okuyabilmektedir. Bu etiketler; gizli dinleme (Eavesdropping), trafik analizi, sahtekarlık gibi amaçlarda kullanılarak hem işletmeleri hem de müşterileri etkilemektedir. “Saldırgan, sistemden ödün vererek gönderilen mesajın frekansını da bozabilmekte ve her koşulda mesajı beklenen alıcıdan uzaklaştırabilmektedir” (Hamid ve diğerleri, 2019). Yetkisiz okuyucular, etiketlere erişerek gizliliği ya da bir trafik analizi saldırısında “konum gizliliği” etkileyebilmektedir (Jia, Feng, Fan ve Lei, 2012).

RFID, aynı zamanda IoT'yi mümkün kılan teknolojilerden biridir. “RFID gibi tanımlama teknolojileri, her bir nesnenin, bireysel nesnelerin otomatik, gerçek zamanlı olarak tanımlanmasına ve izlenmesine olanak tanıyan, uzaktan okunabilen benzersiz bir tanımlayıcıya sahip olmasını sağlamaktadır” (CTEC, 2008). Ancak RFID, IoT'de kullanıldığında bazı siber riskler ortaya çıkmaktadır. Güvenlik ve gizlilik konusunda çıkan siber sorunların temeli ise etiket ile okuyucusu arasındaki hava arayüzünün ihlalindendir (Khoo, 2011). Maliyet ve kaynak kısıtı sınırlamaları nedeniyle, RFID sistemi güvenlik ve gizlilik konusunda siber riskin oldukça yüksek olduğu bir teknolojidir. Bu konuda çözüm önerileri olsa da çözümlerin pahalı olmasından ve güvenlik sorunlarını tam çözemediğinden araştırmalar devam etmektedir (Jia, Feng, Fan ve Lei, 2012).

3.1.3.4. Endüstri 4.0 Teknolojisi ve Dijital İkiz

“Dijital ikiz, fiziksel bir tedarik zincirinin dijital kopyasıdır” (Buck, 2022). Güç üretim ekipmanı, yapılar ve sistemleri, üretim operasyonları, sağlık hizmetleri, otomotiv endüstrisi, kentsel planlama uygulamalarında yaygın olarak kullanılmaktadır (IBM, 2019). İkiz sistem ile fiziksel sistem arasındaki güvenlik açıkları çoğu zaman tam olarak anlaşılamamaktadır. Bu tür boşluklar, dikkate alınmadığı takdirde hem sisteme hem de üreticinin iş modeline yönelik tehditlere yol açabilmektedir. Bilgisayar korsanına saldırıya uğrayacak sistemin dahili bir görünümünü anında verir ve savunmasız saldırı noktalarını belirlemesine yardımcı olur veya bilgisayar korsanı fiziksel bir sistemin arabirimlerine sızma testi yapmak için de kullanılabilir. Dijital ikizin güvenliği bir bilgisayar

korsanı tarafından ele geçirilirse backend sistemlerin bir haritasını açıp istemler için gereken API çağrılarını yapılan kod analizinde (genellikle tersine mühendislik olarak adlandırılır) belirleyerek, ikizin erişim kimlik bilgilerini ortaya çıkarabilir. Bu erişim noktaları elde edildikten sonra; bilgisayar korsanı dijital ikizin davranışını kolayca taklit edebilir, fiziksel sisteme erişebilir (ikizi taklit ederek), potansiyel olarak sistem genelindeki verilere erişim sağlayabilir veya tersine mühendislik yapıp internet protokol (IP) sahibine zarar verebilir” (Hearn ve Rix, 2019).

3.1.4. Küresel Misli Olmayan Tokenlar (NFT)

Fiziksel para ve kripto para birimleri “takas edilebilir” iken küresel misli olmayan tokenlar (NFT) “takas edilemezler” (Conti, 2022). Chainalysis 2021 raporu, NFT pazarının büyüdüğünü ve işlem hacminin 2021 yılına kadar 44,2 milyar dolara ulaştığını tespit etmiştir. Günümüzde hemen hemen bütün varlıkların dijital ortama taşınması “Değiştirilemez Token (NFT)” pazarına verilen önemi arttırmış ve giderek daha fazla bu alana yatırım yapılmasını sağlamıştır. Bu durum, pazarlamacıların öne çıkmasını ve tokenlerini satmasını zorlaştıran bir etkidir. Çünkü müşterilerin paralarını harcamak için daha büyük ve ürün/hizmet skalası geniş pazarlara sahip olduğunu gösterir. NFT’lerin müşterilere satılması zorlaşmıştır ancak pazarlamacılar Web3 teknolojisini geleneksel pazarlamadaki deneyimleriyle birleştirerek iyi belirlenmiş stratejiler ile bunu lehine çevirebilmektedir (Guzman, 2022). Web 3’ün çalışma sürecine bakıldığında geleneksel pazarlama yöntemleriyle bütünleşmiş bir biçimde olduğu görülmektedir. Web 3 pazarlaması, potansiyel müşterilere daha hedef odaklı reklamlar sunmalarını olanak sağlayan zengin ve etkileşimli reklam fırsatları yaratarak pazarlamacıların deneyimini geliştirirken, trendlere ve yeni teknolojilere uyum sağlayarak interneti kullanmaktadır (Aladenika ve diğerleri, 2022).

Web3 platformlarında yapay zekâ ve iş inovasyonu için veri hizmetlerinin kilidini açan “Ocean Protocol” gibi protokoller aracılığıyla şirketler verilerini yayınlayıp bunlardan para kazanabilmekte ve ardından müşteriler bu verileri kendi pazarından satın alabilmektedir (Ocean Protocol Team, 2022; Nyaga, 2022). Kullanıcılarına veri takası üzerinden kripto para kazanma fırsatı veren Ocean Protokol, Ethereum (ETH) block zincirinde çalışmaktadır (Bitlo, 2018).

3.1.4.1. Web 3 ve Dapp

Web 3'ün temeli olan dağıtılmış bilgisayar ağları olan blok zincirleri ve bunlara eşlik eden teknolojiler ve uygulamalar değer kazandıkça bilgisayar korsanları saldırılarını bu alana yönlendirmiştir (Faizullahoy ve Gleason, 2022). Merkezi olmayan bir uygulama (Dapp) bunlardan biridir. “dApp, tek bir bilgisayar yerine eşler arası (P2P) bir blok zincir ağı üzerinde çalışan bir tür dağıtılmış açık kaynaklı yazılım uygulamasıdır” (Gillis, 2022). Dapp’ler veri kontrolünü kolaylaştırması, yüksek ölçeklenebilirlik sunması, esnekliği ve portallar arasındaki ara bağlantıyı desteklemesi, iş kolaylığını sağlaması, kolay veri erişilebilirliği gibi özellikleriyle kullanıcıya avantajlar sağlamaktadır (Verma, 2022). Bunun yanı sıra bilgisayar korsanları tarafından Dapp’ler, ziyaretçilerin oturum açma kimlik bilgilerini veya diğer hassas bilgilerini elde ederek hesaplarına veya cüzdanlarına erişimini sağlayabilmektedir (Coinbase, 2022).

“Birçok airdrop (cüzdana madeni para veya jeton göndermeyi kapsayan pazarlama stratejisi) dolandırıcılığı, bir yatırımcıyı airdrop’larını talep etmek için dijital cüzdanlarını bir kimlik avı eklemeye yönlendirmeye dayanır. Bu dolandırıcılık türünde genellikle web3 adresi bir kullanıcıdan cüzdanını bağlamasını ister. Kullanıcı, gizli ifadesini veya anahtarlarını sağlayarak cüzdanını bağladıktan sonra dolandırıcılık tamamlanır” (Frankenfield, 2022).

3.1.4.2. Küresel Misli Olmayan Tokenlar (NFT) ve Metaverse

NFT’ler aynı zamanda insanların avatarları aracılığıyla metaverse evrenindeki sanat, evler, arabalar gibi farklı nesneleri edinebilecekleri birincil araçlardır (Villasmil, 2022). Metaverse (sanal ve fiziksel öğeleri birleştiren herhangi bir dijital varlık ekosistemi), insanların dijital sanat ve mülk biçimlerini sergilemelerine imkân verirken; NFT’ler, sahiplik kanıtıyla birlikte bu içeriğe bir fiyat koymalarına olanak tanımaktadır (Silva, 2022). Diğer yandan NFT’lerin Metaverse ekonomisinde yer alması ise NFT dolandırıcılığında ve Blockchain ile ilgili dolandırıcılık ve finansal kurumlara yönelik tehditlerde artışa neden olmaktadır. Metaverse ile artan sanal gerçeklik gözlükleri, veri ihlalleri ve kötü amaçlı yazılımlar için yeni olanaklar ortaya çıkarmasının yanı sıra artırılmış gerçeklik cihazları büyük miktarda veri topladığı için (Güner, 2022) yüksek seviyede güvenlik önlemlerini gerekli kılmıştır.

“Veri monarşisi diye bahsedilen büyük ölçekli işletmeler kendi Metaverse ekosistemlerini kurmaya başlamıştır” (BilişimPartisi, 2021). Farklı bir boyuta kapı açan Metaverse, her sanal kavram gibi siber riskleri beraberinde getirmektedir. Meta veri depolarından (veritabanı) yararlanmak isteyen siber saldırganlar bu yeni boyutta kendilerine yer bulmaya başlamıştır. Mahremiyet, veri kullanımı etiği & güvenlik yönergeleri ve biyometrik veriler (yani, VR cihazlarını kullanırken kullanıcı hareketleri ve fiziksel özellikler) meta veri deposu alanında korunması gereken alanlardır (Çorumlu, 2022). Bilgisayar korsanı avatara erişim kazanırsa, “Kişisel Olarak Tanımlanabilir Bilgiler (PII)” dahil her türlü bilgiyi elde edebilmektedir. Bunun yanı sıra siber saldırı, manevi olarak da (ilişki & itibar zedelenmesi, çevrimdışı güvenlik) hasar verebilmektedir. Yapılan bu kimlik hırsızlıklarında deepfake teknolojisinden de faydalanılabilmektedir (Fletcher, 2022).

3.1.5. Endüstriyel Casusluk

İşletmelerin teknolojik olarak ilerlemesini veya yenilikler sunmasını sağlayan Ar-Ge bölümü, pazarlama disiplini ile entegre olmuş durumdadır. Ar-Ge çalışanlarının müşteri ihtiyaçları konusunda bilgilendirilmesi, müşterilerin arzu ettiği ürünlerin geliştirilmesinde pazarlama departmanı ile birlikte çalışması, müşterilerin ürün veya hizmete karşı yorumlarını pazarlama departmanından öğrenmesi, ürünlerin veya hizmetlerin en çok istenen performans özelliklerinin sıralamasının pazarlama departmanı ile belirlenmesi, Ar-Ge çalışanlarının rakiplerin ürün stratejileri hakkında bilgilerini pazarlama departmanı tarafından alması, yeni ürün konseptinin pazarlama çalışanlarıyla doğrulanması, Ar-Ge çalışanlarının Pazar araştırması sonuçları hakkında pazarlama departmanı tarafından bilgilendirmesi, piyasa sinyallerinin etkisi altında tasarımların değiştirmesi, yeni fikir ve teknolojilerin ticari uygulamalarını araştırması ve yeni ürün fikri oluşturma Ar-Ge ve pazarlamanın birbiriyle nasıl entegre çalıştığını göstermektedir (Szopik-Depczyńska ve Cheba, 2021). Ar-Ge çalışmada veya pazarlama alanında meydana gelecek bir siber zarar bu entegre olmuş sistemin sekteye uğramasına yol açacak ve iki alanında durumdan etkilenmesi kaçınılmaz olacaktır

İşletmelerin AR-GE çalışmaları piyasada oldukça rehabet görecek, dünya düzeyini değiştirecek yeni ürünler veya hizmetler ortaya çıkarabilmektedir. Bu durum bazı

rakip firmaların veya devletlerin avantaj sağlamak için bu bilgilere ulaşmasını sağlamak istemesine neden olabilmektedir. Endüstriyel casusluk/istihbarat¹¹ kavramı olarak günümüzde yer bulan bu istihbarat türü özellikle uluslararası bir pazara hâkim olana büyük ölçekli şirketlerde daha çok karşımıza çıkmaktadır. Siber saldırılar ile gerçekleştirilen Ar-Ge faaliyetleri bozulabilmekte, satmak için veriler çalınabilmekte veya işletme rakipleri önemli bilgileri elde ederek bunları lehlerine kullanılabilmektedir. Ancak siber güvenlik önlemleri ve etkili güvenlik kontrolleri ile işletmeler, Ar-Ge çabalarının sonucunu etkileyebilecek potansiyel tehditlerden kendilerini koruyarak çıktılarını ve rekabet avantajını sürdürmeye devam edebilmektedir (Canadian Centre for Cyber Security, 2020).

3.1.6. Siber Zorbalık

İşletmelerin siber dünyada karşılaştığı diğer bir sorun ise siber zorbalıktır. “Siber zorbalık, başka bir kişiyi tekrar tekrar ve kasıtlı olarak taciz etmek, incitmek, utandırmak, aşağılamak veya korkutmak için teknolojinin kullanılmasıdır” (PACER Ulusal Zorbalık Önleme Merkezi, 2022). “Kişiler ya da tüzel kişiler de siber zorbalığa uğrayabilmektedir. İşletme misyonuna, ideolojiye, marka değerine, sunduğu ürün ya da hizmete yönelik kışkırtıcı ve saldırgan bir dil kullanarak, yanlış bilgi yayarak, çalışanlarını ya da mensuplarını etiketleyici, ötekileştirici ya da aşağılayıcı ifadelerle başvurarak siber zorbalık sergilenmektedir” (Atatanır, 2022).

Sergilenen siber zorbalıklarda siber propaganda ve dezenformasyon oldukça yaygın görülmektedir. Örneğin, Starbucks’ın “2015 Birlikte Yarış” kampanyasında şirket, ırk ilişkilerinin durumu hakkında konuşmaları teşvik etmeye çalışmıştır. Ancak şirket bu kampanya sonucu tepki çekmiş ve siber zorbalığa maruz kalmıştır. Bazı internet kullanıcıları, bu kampanyayı Starbucks’ın aleyhine kullanarak ırkçı ve tartışmalı açıklamalara sebep olmuştur. Kampanyanın olumsuz etkilerinden kaçmak isteyen bir Starbucks yöneticisi Twitter hesabını geçici olarak silmiş ve “Bir olumsuzluk silsilesi içinde kişisel olarak saldırıya uğradığımı hissettim” diye açıklamada bulunmuştur. Diğer bir örnek, CEO’nun Trump yönetimiyle bağları nedeniyle Uber’e karşı örgütlenen çevrimiçi

¹¹ “Küresel rekabet ortamında ticari tüzel kişiliklere mutlak ekonomik/finansal avantaj sağlayacak, rakip şirketlere ait ticari sırlar veya tescilli bilgilerin-fikri mülkiyet haklarının, açık kaynak istihbaratı ile temin edilemeyen bir takım yasadışı girişimler yoluyla kurumsal ele geçirme faaliyetleridir” (Altıntaş, 2021).

aktivistlerin (bazıları tarafından siber zorba olarak adlandırılan) #DeleteUber hareketini başlatmasıdır. DeleteUber hareketinden sonra, Uber çevrimiçi kitlenin artan öfkesinin hedefi durumuna gelmiş ve kullanıcıların uygulamayı silmesine neden olmuştur” (Britton, 2022).

Siber saldırıya başarılı bir şekilde karşı koyamayan işletmelerde pazarlama faaliyetleri olumsuz yönde etkilenmektedir. Siber saldırılar; müşteri güveninin, marka imajının ve işletme bütçesinin büyük hasarlar almasına neden olmaktadır. Bu sebeple marka imajını & itibarını korumak isteyen, müşteri ya da maddi kayıplara uğramak istemeyen işletmeler bu konularda bilgilenebilir ve önlemlerini buna göre almalıdır.

3.2. DİJİTAL ORTAMDA MÜŞTERİLER İÇİN SİBER GÜVENLİK TEHDİTLERİ

Değişen tüketici eğilimleri, çevrimiçi ortamın artan karmaşıklığı, yeni risklerin veya düzenlemelerin ortaya çıkışı e-ticarete teknik zorlukları artırmıştır (ABGI UK, 2017). Özellikle güvenlik ve veri gizliliği konusunda karşılan riskler nedeniyle işlemlerini dijital platformlara taşıyan işletmeler oldukça hassas olmalıdır. Çünkü e-ticaret platformları gibi ortamlarda kritik bilgilerin işlenmesi bu ortamda yapılan alışverişi siber saldırıların hedefi haline getirebilmektedir. Çoğu E-ticaret sitesi kredi kartı bilgilerini tutmak yerine sanal pos sistemleri ile entegre olarak kişisel verileri sanal pos üzerinden tutulmasını sağlamaktadır. Bu sayede üst düzey banka seviyesinde şifrelenen verilerin “decode” yani şifrelerinin kırılması oldukça zor olmaktadır. Ancak adres, telefon gibi bilgiler veri tabanında tutulduğu için çalınması daha kolay hale gelmektedir. PayPal gibi üçüncü taraf hizmetler aracılığıyla yapılan ödemeler de bir zafiyet sonrası siber saldırganların eline geçebilmektedir. Siber saldırılar için olağan vektörler, kötü amaçlı yazılımlardır. E-ticarete faaliyet gösteren dijital pazarlamacıların kötü amaçlı yazılımdan koruma önlemlerine aşina olması gerekmektedir. Güvenli Soket Katmanı (SSL) protokolleri ve iki faktörlü kimlik doğrulama süreçleri gibi ek güvenlik önlemleri, daha yüksek düzeyde müşteri konforu sağlamaktadır. Ayrıca, kötü amaçlı yazılımdan koruma önlemleri, Sanal Özel Ağ (VPN) tarafından sağlanan ek veri iletim şifreleme (encryption) katmanını içermelidir.

Şifrelenmiş veriler, ele geçirmeyi başaran saldırgan tarafından kullanışlı olmamaktadır (Bemedia, 2022).

3.2.1. Kimlik Hırsızlığı

Kimlik hırsızlığı sebebiyle birçok internet kullanıcısı kurban olduğu için bu siber saldırı en büyük endişelerden biri olmuştur. Bir kimlik avcısı, internet kullanıcısının mesajına güvenmesi için halka açık veya güvenilir bir kuruluşu yasadışı bir şekilde taklit edebilmektedir. Taklit ettiği kuruluş aracılığıyla kullanıcıların hassas bilgilerine erişim sağlamaktadır. İşletmelerin kullanıcılara kampanyaların, fırsatların veya ürün tanıtımlarının e-posta olarak gönderilmesiyle gerçekleşen e-posta pazarlama, kimlik avı saldırılarında öne çıkmaktadır. Sosyal mühendislik metoduyla işletmeler veya bireyler hedef alınmaktadır. Sonuçta “İnsanlar, en zayıf halkadır”. Saldırgan, kurbandan istediği verileri alabilmek için gerçek bir e-posta gibi duran bir hesap açar. Mail de orijinal logoları, sahte firmaların imzalarını kullanır (Muntode, 2019). Bu şekilde kurbanın güvenini kazanmaya çalışır. Kurbanlar gelen e-postaları pazarlama amaçlı gönderildiğini düşünüp bu sayfalar üzerinden alışveriş yapabilmekte, kişisel verilerini paylaşabilmekte, e-postada yer alan bir bağlantıya tıklayarak kullandığı cihaza virüs bulaştırabilmekte veya bilgisayarlarının olası saldırılarda “zombie” bilgisayar olmasına neden olup bilgisayar korsanlarının hedef saldırılarında bilgisayarlarını kullanmasına yol açabilmektedir. Kimlik avı saldırılarında senaryolar çeşitlilik göstermektedir. “Google tarafından Iphone kazandınız sayfası, farklı ülkelerden gelen paramı sana göndermek istiyorum gibi e-postalar” kimlik avı saldırılarında sıklıkla kullanılan yöntemlerdendir.

Kimlik avı saldırıları, bildirilen güvenlik olaylarının %80’inden fazlasından sorumludur. CISCO’nun 2021 Siber Güvenlik Tehdit Trendleri raporuna göre, veri ihlallerinin yaklaşık %90’ı kimlik avı nedeniyle meydana gelmektedir. Siber güvenlik firması Check Point Software tarafından 6 Ekim 2022’de yayınlanan araştırmaya göre yaklaşık 5 kimlik avı e-postasından 1’i (%18,8) Microsoft’un platform savunmasını atlamış ve 2022’de çalışanların gelen kutularına düşmüştür; bu oran 2020’ye kıyasla %74 artmıştır. Bilgisayar korsanları, Gönderen Politikası Çerçevesi (SPF) gibi güvenlik kontrollerini

geçmek için zero-size *fonts*¹² kullanmak veya kötü amaçlı URL'leri analizden gizlemek gibi bir e-postanın işlevsel bileşenlerini yanıltmak için giderek artan sayıda teknik kullanmaya başlamıştır (Lemos, 2022). Hedefli kimlik avı, tüm kimlik avı saldırılarının %65'ini oluşturan en yaygın kimlik avı saldırısı türüdür (Spanning Cloud Apps, 2022). Bunun dışında pek çok yöntem olsa da Kimlik Avı; Balina Avı (Whaling), Sesli Kimlik Avı (Vishing), Sms Kimlik Avı (Smishing), Fenerli Kimlik yöntemleri de yaygın olarak kullanılmaktadır. Vishing, Phishing ve Smishing saldırılarının ortak noktası finansal kazanç için kullanıcılardan hassas bilgiler elde etmesidir. Vishing saldırıları telefon üzerinden, phishing saldırıları e-postalar aracılığıyla, smishing saldırıları ise SMS mesajları yoluyla gerçekleşmesiyle birbirinden ayrılırlar (Rathnam, 2022).

Kurumlarda müşteri konumunda olabilmekte ve yapılan siber saldırılardan etkilenmektedir. 2017 Mart ayında, ABD Adalet Bakanlığı, Asyalı bir tedarikçi üzerinden 100 milyon dolarlık dolandırıcılık gerçekleştirildiğini ve kurbanların iki önemli teknoloji markası olduğunu açıklamıştır. 27 Nisan'da ise Fortune, iki kurbanın Facebook (Meta) ve Google olduğunu bildirmiştir (Baraniuk, 2017). Gerçekleşen olayda Litvanyalı bir adam (Evaldas Rimasauskas), e-posta kimlik avı saldırısı nedeniyle suçlanmıştır. Olay şu şekilde gerçekleşmiştir: Rimasauskas ve ekibi, Google ve Facebook ile çalışan Tayvan merkezli "Quanta Computer" adlı başka bir şirket gibi davranıp sahte bir şirket kurmuştur (Huddleston, 2019). Rimasauskas ayrıca şirket adına banka hesapları da açmıştır. Siber dolandırıcılar daha sonra hedef aldıkları bazı Google ve Facebook (Meta) çalışanlarına kimlik avı e-postaları göndererek, sağlanan mal ve hizmetler için onları faturalandırmış ve hesaplarına ödeme yapmaları konusunda yönlendirmiştir. Olayın ortaya çıkmasından sonra 2013 ve 2015 yılları arasında Rimasauskas ve ortaklarının, Facebook (Meta) ve Google'u 100 milyon doların üzerinde dolandırdığı tespit edilmiştir (Rosenthal, 2022).

¹² ZeroFont adı verilen teknik, sahtekârlar tarafından yaygın olarak kullanılan, metin öğelerini kontrol ederek kötü amaçlı e-postaları tanımlayan bir araç olan Microsoft Office 365'in doğal dil işlemlerini kandırmak için metin yazı tipi boyutlarının değiştirilmesini içerir (Trendmicro, 2018).

3.2.2. NFT Pazaryerleri

Müşterilerin dolandırılabilirdiği diğler bir ortam ise NFT pazaryerleridir. Dijital varlıkların milyon dolarla alınıp satıldığı dijital ticaret platformları (NFT pazarı) siber saldırganların yeni hedef alanlarından biridir. Örneğın, NFT pazaryerlerinde NFT'leri açık arttırmaya çıkarmak için kullanılan akıllı sözleşmeler bazı açıklara sahip olabilmektedir. “Akıllı sözleşmelerde bulunan bir açıklık, DAO (Merkezi Olmayan Otonom Organizasyon) mekanizmasında bu açıklığın kapatılması için gereken prosedür ve sürecin uzunluğu ile bağlantılı olarak önemli mali kayıpların doğmasına sebebiyet vermektedir” (Öztürk, 2021). Akıllı sözleşmelerin açık kaynaklı olmasından faydalanan bilgisayar korsanları kodu inceleyebilmekte, boşlukları veya açık noktaları bulabilmekte ve sistemi kendi çıkarları için kullanabilmektedir (3Cyber-Sec, 2020). “Günümüzde yapılan DeFi¹³ saldırıları, protokoller ve akıllı sözleşmelerdeki özellikle de flaş kredi protokolleri ve zincirler arası köprülerdeki güvenlik açıklarını tespit eden siber saldırganlar tarafından gerçekleştirilmiştir.” (Australian Cyber Security Magazine, 2022).

Kimlik dolandırıcılığı, NFT dünyasında oldukça yaygın görülmektedir. Özellikle kullanıcılar tarafından tanınmış bir NFT platformunun ya da NFT Pazar sitesinin taklit edilmesiyle ortaya çıkar (Elliptic NFT Raporu, 2022). Siber saldırganlar, kimlik avı yoluyla bir NFT kullanıcısının kripto cüzdanına erişebilmekte ve diğler cüzdanlara veya Pazar yerlerine aktararak belirteçleri kendi lehine kullanabilmektedir. NFT'ler çalındığında, orijinalliğini doğrulamak oldukça zordur (Manjarres, 2022). Kuzey Kore kökenli Lazarus grubu, “Axie Infinity'i” hackleyerek, 173.600 Ethereum jetonu çalmış ve Sky Mavis'in 625 milyon dolar kaybetmesine sebep olmuştur. Bunun yanı sıra siber saldırı sonrası yaşanan güvensizlikten ötürü günlük aktif kullanıcı sayısında düşüş yaşanmış ve Sky Mavis, oyun gelirlerine erişemeyen oyuncuların çıkışını durdurmak için 150 milyon dolar harcamıştır (Byers, 2022; Ahtar, 2022).

Kuzey Kore bağlantılı Lazarus APT, AppleJeus truva atını yüklemek için sahte BloxHolder markası altında sahte kripto para uygulamalarını kullanarak bilgisayar adresleri, bilgisayar adları ve işletim sistemi sürümleriyle ilgili ayrıntıları toplayabilmektedir.

¹³ Merkezi olmayan uçtan uca finansal hizmetler için kullanılan şemsiye terimdir.

Bu ilk erişim adımından sonra bilgisayar korsanları müşterilerin kripto varlıklarını ele geçirmektedir (Paganini, 2022 ve Alper, 2022).

Dünyanın en büyük NFT pazarlarından biri olan OpenSea kullanıcıları, Haziran 2022’de bir kimlik saldırısı yaşamıştır. OpenSea’nin e-posta dağıtım satıcısı Customer.io’ndan bir şirket çalışanı OpenSea kullanıcılarının ve OpenSea haber bültenine abone olanların e-posta adreslerini yetkisiz bir üçüncü tarafla paylaşmıştır. Bu siber saldırı sonrası OpenSea platformundan 1,7 milyon dolar NFT çalınmıştır (Milmo, 2022). Aynı yılın Mayıs ayında da OpenSea’nin resmi Discord sunucusu saldırıya uğramıştır. Discord’a yapılan saldırıda da bir bot, OpenSea’nin YouTube ile iş ortaklığı yaptığına dair sahte bir duyuru yayınlayıp kullanıcıların bağlantıya tıklamasını sağlamak için 100 ücretsiz NFT’den birini vereceğini vaat etmiştir (Lawler, 2022). Siber saldırıya hızlı bir şekilde müdahale eden OpenSea, Discord kanalındaki mesajları ve hesapları kaldırmış, kullanıcılara bağlantıya tıklamamaları konusunda uyarılmış, kanalı geçici süre gizlemiş ve saldırının etkisini bu sayede azaltabilmiştir. Bilgisayar korsanları, OpenSea tarafından verilen hızlı bir tepki sayesinde 10’dan az cüzdan etkilenmiş, toplam 10 ETH’den (27.000 \$) daha az değerdeki varlık çalınmıştır (Copeland, 2022).

Bir başka örnek ise Nisan 2022’de bilgisayar korsanlarının, Bored Ape Yacht Club’a yaptığı siber saldırıdır. Bilgisayar korsanları, NFT platformunun topluluk yöneticisi Boris Vagner’in Discord hesabını ele geçirdikten sonra hesabı hem resmi BAYC’de hem de Otherside’s Discord kanalları adlı ilgili meta veri deposu projesinde kimlik avı bağlantılarını yaymak için kullanmıştır (Eli Tan ve Coindesk, 2022). Paylaşılan bağlantı özel bir hediye dağıttığını belirtse de aslında bir yemleme (phishing) sitesine yönlendirmekteydi. Gerçekleşen siber saldırı sonrasında 200 ETH (360 bin dolar) değerinde NFT çalınmıştır (Smith, 2022).

Keepnet Labs Türkiye Genel Müdürü Erdinç Balcı, “Eserler kendi içlerinde orijinalliğini belgeleyecek şekilde düzenlenseler de hesaplar korunmadığı takdirde dijital alışverişteki diğer tüm riskler NFT Pazar yerlerinde de geçerli. NFT’lerin blok zinciri tabanlı doğası gereği bir NFT çalındıktan sonra Pazar yeri onun kontrolüne sahip olamıyor, etkilenen kullanıcıların kayıp koleksiyonlarını kurtarması da pek olası görünmüyor” diyerek NFT pazarlarının kullanıcılar üzerindeki tehditlerine dikkat çekmiştir (Yalçın, 2021).

Tablo 3*NFT'ye özgü pazarlama sonuçları*

Geleneksel İçerik (Merkezileştirilmiş)	NFT İçeriği (Merkezi Olmayan)	Pazarlama için NFT Etkileri
.mp3 veya .jpg gibi bir dosyanın kopyası orijinaliyle aynıdır.	NFT'ler dijital olarak benzersizdir; iki NFT aynı değildir.	Kıtlık Özgünlüğü
Dijital öğelerin mülkiyet kayıtları, kurumlar tarafından kontrol edilen sunucularda saklanır; onlar adına onların sözlerini almalısın.	Her NFT'nin bir sahibi olmalıdır ve bu, herkese açık bir kayıttır ve herkesin doğrulaması kolaydır.	Sahiplik Kanıtı
Dijital öğeleri olan şirketler kendi altyapılarını oluşturmak zorundadır. Örneğin, etkinlikler için dijital bilet düzenleyen bir uygulamanın kendi bilet değişimini oluşturması gerekir.	NFT'ler, Ethereum gibi aynı blockchain teknolojisi kullanılarak oluşturulan her şeyle uyumludur. Bir etkinlik için bir NFT bileti, her Ethereum pazarında tamamen farklı bir fiyatla alınıp satılabilir. NFT'de örneğin bir alıcı, bir sanat eserini bir bilet karşılığında takas edebilir.	Değiştirilemezlik (Nonfungibility)
Müzik akışı hizmetleri gibi platformlar, satışlardan elde edilen kârın çoğunu elinde tutar.	Pazarlamacılar, markalarının çalışmalarını üzerindeki mülkiyet haklarını elinde tutabilir ve yeniden satış telif ücretlerini doğrudan talep edebilir.	Telif Hakları
Pazarlamacılar, kullandıkları platformların altyapısına ve dağıtımına güvenirler. Bunlar genellikle kullanım koşullarına ve coğrafi kısıtlamalara tabidir.	Pazarlamacılar, markalarının çalışmalarını her yerde satabilir ve küresel pazarlara erişebilir.	Doğrudan Dağıtım Altyapısı

Not. Ethereum'dan uyarlanmıştır: Chohan, R., & Paschen, J. (2021). *NFT marketing: How marketers can use nonfungible tokens in their campaigns*. Business Horizons.

3.2.3. Veri Simsarları

Karaborsadaki satıcılar her zaman bilgisayar korsanı değildir. Veri kaçakçıları, piyasa analistleri ve teknik uzmanlar karaborsa da alıcının ihtiyaçlarına göre uyarlanmış özel hizmetler sunabilmektedir. Veri kaçakçılığı yapan “Veri simsarları¹⁴” müşteri ve sektöre göre birçok farklı şekilde uyarlanabilmektedir. Aracılık edilen veriler için en büyük pazarlar arasında reklam ve pazarlama, sağlık eğitimi, kredi ve casus müşteri hizmetleri, hükümet ve kanun yaptırımı yer almaktadır. Bu pazarlar, veri komisyoncusu hizmetlerini çeşitli amaçlar için kullansa da genellikle işlerini veya karar vermelerini geliştirmek için kullanılmaktadır (Federal Trade Commission, 2014). Birbirinden farklı verilerin toplanması ve verilerin ticareti bazen bütünlükle ilgili sorunlara neden olabilmektedir.

Buna bir örnek, OfficeMax’in 2014 yılında bir müşteriye gönderdiği bir promosyon mektubudur. İkinci satırlarında yer alan “Kızı araba kazasında öldü” kelimeleri yer almıştır ve alıcının kızının vefatından bir yıl sonra tekrar mağdur hissetmesine neden olmuştur. OfficeMax, olayın “üçüncü taraf bir sağlayıcı aracılığıyla kiralanan bir posta listesinin” neden olduğunu, “yanlışlıkla olan bir hata” olduğunu açıklamıştır. Olay aynı zamanda müşteriye OfficeMax ve veri komisyoncusunun kendisi hakkında ne kadar veriye sahip olduğunu ve kızının vefatının hangi bağlamda veri tabanına kaydedildiğini ortaya koymuştur (Goodman, 2016).

İnternette girilen sitelerde paylaşılan veriler sayesinde bireyin en yakınlarının bile bilmediği bilgiler elde edilebilmektedir. Minneapolis kentinde bir baba lisedeki 15 yaşındaki kızına gönderilen bebek kıyafetleri, beşik kuponlarından rahatsız olup, çocuğunu hamileliğe özendirmekten dolayı işletmeden şikayetçi olmuştur. Ancak birkaç gün sonra kızının gerçekten hamile olduğunu öğrenmiştir (Goodman, 2016).

3.2.4. Geofencing

İşletmelerin pazarlama teknikleri gerekli önlemler alınmadığında müşteri gizliliğini ve güvenliğini tehlikeye atabilmektedir. Örneğin, “Birçok uygulama müşterilerine anında iletme bildirimleri göndermek için konum tabanlı hizmetleri kullanmaktadır. Bir

¹⁴ “Veri simsarları (data broker)”, tüketicilerin kişisel bilgilerini toplayan ve bu bilgileri başkalarıyla yeniden satan veya paylaşan Büyük Veri ekonomisinin önemli katılımcıları olan şirketlerdir.

bilgisayar korsanı, sosyal mühendislik girişiminde bulunurken bilgi toplamak veya güvenliği ihlal edilmiş bağlantılar göndermek için bu hizmetlere sızabilmekte ve yanlış push bildirimleri gönderebilmektedir. Saldırganlar, fiziksel yollarla bile gizlice girebilmekte ve cihaza erişim sağlayabilmektedir. Geofencing, saldırıyı hedeflerinin hareketlerine karşı da uyarabilmektedir. Bildirimler alıp ve sürekli izleyebilmektedir. Aynı zamanda bir bilgisayar korsanı izlerini kapatmaya çalışıyorsa ve coğrafi sınırlamanın kullanılan bir araç olduğunu biliyorsa, konum verilerini potansiyel olarak hackleyebilmektedir” (Adams, 2020).

“Geofencing, bir saldırıya bir cihazın IP adresini, hangi uygulamaları hedefleyeceğini ve hedefini çevreleyen insanların ne kullandığını söyleyebilmektedir. Bir saldırıya bir evin veya bir ofis binasının coğrafi sınırlarını belirler ve bir hedefi çevreleyen cihazlara erişim kazanırsa, o hedef cihazlardaki hiçbir koruma onları korumayabilir. Çevredekiler, aile üyeleri, komşular, iş arkadaşları ve müşteriler, saldırının hedefi tehlikeye atmak için ihtiyaç duyduğu güvenlik açıklarını yalnızca yakınlıklarıyla sağlayabilmektedir. Bir coğrafi sınır, saldırının bir hedefin sıklıkla nerede olduğu dahil olmak üzere birçok bilgiyi toplamasına ve sosyal mühendislikle elde ettiği bu bilgileri bir dayanak olarak kullanmasına izin verebilmektedir” (Adams, 2020).

DÖRDÜNCÜ BÖLÜM

4. SİBER GÜVENLİKTEKİ BAŞARININ İŞLETMELERDEKİ ETKİSİ

İnternetteki en önemli unsur güvenlik faktörüdür. İnternet her ne kadar yaşamamızı kolaylaştırırsa da içinde birçok tehdidi de barındırır. Bu tehditler aktif olabileceği gibi potansiyel olarak da karşımıza çıkmaktadır. Paylaşılan veya siber dünyada kaydedilen kişisel/kurumsal bilgiler, kredi kart bilgileri gibi hassas bilgiler potansiyel tehlike arz etmektedir. Herhangi bir aktif saldırıda ele geçirilmesi saldırıya uğrayan şahsı veya kurumu zarara uğratabilmektedir. Aktif tehlikeler ise uğranan siber saldırılardır. Siber alandaki güvenlik özellikle dijital pazarlama için büyük önem taşır ve bu nedenle siber dünyadaki güvenlik tehditleriyle uğraşmak, çevrimiçi bir ortamda faaliyet gösteren dijital pazarlamada başarı için esastır (Konyeha, 2020). İnternet ortamından işlemlerini gerçekleştiren dijital pazarlamacılar, siber tehlikeler karşısında müşterilerinin ve çalıştığı işletmenin güvenliğini sağlamak açısından siber güvenliğe yeterince önem vermelidir.

Dijital pazarlamanın yapıtaşı sayılabilecek verilerin uğradığı ihlaller en sık karşılan sorunlardan biridir. Veri ihlaline uğrayan işletmeler sadece müşterilerin kuruma karşı güvenini riske atmazlar. Bununla beraber potansiyel veya mevcut yatırımcılar için de güven kaybına sebep olabilmektedir. Meydana gelen veri ihlalleri güven kaybı dışında işletmelere mali olarak da zarar verebilmektedir. Genellikle veri ihlali sonrası işletmelerin siber güvenlik yatırımları artsa da olması gereken siber saldırıya uğranmasa da siber güvenliği baştan itibaren sağlamaktır. Verilerin korunmasına ve bilgi güvenliğine verilen önem işletmelerin güvenilirliğini artıracak, olası maddi ve manevi zararları önleyecek ve işletmelerin itibarını zenginleştirecektir.

4.1. SİBER SİGORTA

Küçük, orta, büyük farketmeksizin her ölçekteki işletme iş süreçlerini yönetmek için bilgi ve teknolojiye her geçen gün daha çok güvenmektedir. Süreçlerdeki herhangi bir aksama ise hizmetin ve işletme hedeflerinin olumsuz yönde etkilenmesine yol açabilmektedir. İşletmenin bilgi ve teknoloji kullanımında ortaya çıkabilecek operasyonlar

riskler “siber riskler” olarak adlandırılır. Operasyonel siber riskin kaynakları insan eylemleri, sistem ve teknoloji arızaları, başarısız dahili süreçler ve harici olaylar olmak üzere dört sınıfa ayrılabilir (Peters, Shevchenko ve Cohen, 2017).

İşletmelerin dijital ortamdaki pazarlama faaliyetleri sonucunda iş hacmi büyüdükçe siber risk oranı artar. Siber riskler, işletmelerin siber savunma mekanizması dışında farklı önlemler ile kendisini güvence altına istemesine neden olmuştur. İşletmeler bir siber sigorta güvencesinden faydalanıp dijital ortamda yaşayabilecekleri sorunlardan ötürü gerçekleşebilecek zarar ve siber kayıpların önüne kısmen de olsa geçebilmektedir. Çünkü siber sorumluluk sigortası, gerçekleşen siber saldırı sonrası işletmenin veya müşterinin etkilenmesi durumunda yasal masrafları, kredi izleme hizmetlerini ve diğer kurtarma maliyetlerini belirli bir oranda karşılamaktadır (TechInsurance, 2022).

Örneğin, Target Corporation (Amerika merkezli perakende şirketi) 2013 yılında yaşadığı bir siber saldırı sonrası veri ihlaline uğramıştır. Saldırı sonrası siber suçlular en az 40 milyon kredi kartının bilgisini ve yaklaşık 110 milyon kişinin ise e-posta, telefon numarası gibi kişisel bilgilerini ele geçirmişlerdir. Bu siber saldırının maliyeti ise 290 milyon dolar civarındadır ancak yapılan sigorta sayesinde 90 milyon dolarını sigorta şirketleri karşılamıştır (Stempel & Bose, 2015). Diğer bir örnek ise, 2014 yılında Home Depot (ABD'nin en büyük ev geliştirme perakendecisi) işletmesinin bir bilgisayar korsanı tarafından satıcının kullanıcı adı ve şifresini ele geçirip kötü amaçlı yazılımı piyasaya yaymasıyla meydana gelmiştir. ABD ve Kanada'daki Home Depot mağazalarında otomatik ödeme terminallerini kullanan müşteriler bu saldırıya maruz kalmıştır. 56 milyon kişinin kredi ve banka kartı bilgileri ele geçirilmiştir. Toplam 43 milyon dolara mal olan saldırıda işletme 15 milyon dolarını sigorta kapsamında geri almıştır.

Siber sigorta maddi olarak zararın bir kısmını karşılıyor olsa da işletmelerin sarsılan güvenine bağlı gelirlerinin olumsuz yönde etkilenmesini kapsamaz. Ayrıca siber sigorta, devlet destekli casusluk veya fidye yazılımı gibi bazı büyük saldırılarda politika dışında tutulmaktadır (Newman, 2016).

Günümüzde her büyüklükteki işletme siber riskin oluşturduğu tehditlere karşı daha çok farkındalık kazanmıştır. Bu kazanılan farkındalık ise siber kapsamaya yönelik talebin artmasına neden olmuştur. Sigorta Acenteleri ve Brokerleri Konseyi'nin (CIAB) yapmış olduğu açıklamaya göre siber sigorta primleri 2022'nin ilk çeyreğinde 2021'in

dördüncü çeyreğine kıyasla ortalama %28 oranında artış göstermiştir. Artan sigorta primine yol açan etkenler ise sigorta şirketlerinin risk iştahının (Risk Appetite) azalması ve işletmelerin sigorta kapsamına yönelik artan talebidir (Violino, 2022).

4.2. SİBER DAYANIKLILIK

“Siber dayanıklılık, sistemin, özellikle siber saldırılarla ilişkili olumsuz etkilere hazırlanma, bunları absorbe etme, iyileştirme ve bunlara uyum sağlama becerisini ifade eder” (Linkov & Kott, 2018). Aynı zamanda siber dayanıklılık “siber sözleşmeler için giriş gereklilikleri veya ön koşulları, olay müdahalesi, veri toplama ve kapsam sınırlamaları” gibi çeşitli hizmetlere olan ihtiyaç yoluyla siber sigorta ile bağlıdır. Siber sigortalar aracılığıyla işletmeler daha çok siber güvenlik konusunda önlemler alıp siber dayanıklılığını artırabilmektedir. Siber dayanıklılığı artıran gelişmiş bir siber sigorta, sigorta yaptıran işletme ile siber sigortayı sağlayacak şirket arasındaki sigorta sözleşmelerinin etkin bir şekilde hazırlanması ve takibi ile mümkündür. Bunun sağlanması için işletme ve işletmenin siber sigortasını sağlayan şirket uygun uygulamaları kabul etmeli, siber saldırılara karşı birlik içinde ve maruz kalınan olumsuz etkilere karşı hızlı bir şekilde koordine olmalı, aktörler tarafından sorumluluklar iyi bilinmeli, riskler ve iddialar verimli bir biçimde raporlanmalı, veriler güvenilir bir şekilde toplanmalı, bilgi işlem sistemleri çalışanlarına uygun teşvikler sağlanmalı ve yönetmelikler buna göre ayarlanmalıdır (Hausken, 2020).

4.3. SİBER TEHDİT İSTİHBARATI

“Siber saldırılar küresel ekonomiye yılda yaklaşık 445 milyar dolara mal olmaktadır. Saldırıları azaltmak için birçok işletme siber tehdit istihbaratına (CTI) veya bilgisayarlar, ağlar ve BT ile ilgili tehdit istihbaratına güvenir” (Samtani, Chinn, Chen ve Nunamaker, 2017). Siber tehdit istihbaratı (Cyber Threat Intelligence), bir işletmenin veya varlıklarının güvenliğini tehdit eden mevcut ve potansiyel saldırılar hakkında istihbarat çarkı oluşturmaya odaklanan bir siber güvenlik alanıdır (Martins, 2022). CTI, işletmelere saldırı göstergeleri sağlar; kısa vadeli önceliklerin belirlenmesine yardımcı olur, yönetim kurulunu stratejik görünüm konusunda eğitir; riskin azaltılmasını destekler, güvenlik

operasyonlarının verimliliğini artırır; önceden bilinmeyen tehdit olaylarının ortaya çıkmasına yardımcı olur (Durbin, 2022). Siber tehdit istihbaratı sağlayıcıları tarafından yaygın olarak kullanılan kaynaklar ise şunları içerir: Kötü amaçlı etkinliklerle ilişkili uzlaşma göstergeleri (IoC'ler), İstemciden türetilen veriler, Derin/Dark web, Mesajlaşma platformları, Sosyal medya, İnsan istihbaratı, Kötü amaçlı yazılım analizi, Jeopolitik gelişmeler, Kod havuzları, Yapıştırma siteleri, Bilgi paylaşım platformları (Crest, 2022). Siber tehdit istihbaratına yardımcı olan bir diğer unsur ise siber tehditlerin ve saldırıların çok önceden tahmin edilebilmesi için fütürist içgörülerini ayıklanmasını, görselleştirilmesini ve analiz edilmesini sağlayan Büyük Veri Analitiğidir (Yamini, 2021).

4.4. DIŞ KAYNAK KULLANIMI

İşletmeler başarılı bir siber güvenlik için dış kaynaktan destek alarak koruma sağlayabilmektedir. Diğer taraftan, işletmelerin anlaştığı siber güvenlik şirketleri “ağ ve antivirüs günlükleri, bal küpleri (Honeypot), veritabanı erişim olayları, sistem oturum açma girişimleri ve izinsiz giriş savunma sistemi/saldırıdan korunma sistemi (IDS/IPS) olayları” gibi mekanizmalar aracılığıyla gerçek saldırılardan veya olaylardan toplanan reaktif verilere dayalı çalışsa da kimi zaman yeterli olamayabilmektedir.

Dijital ortamda işlemlerini gerçekleştiren her işletme siber güvenlik alanında proaktif bir yaklaşım benimsemelidir (Samtani, Chinn, Chen ve Nunamaker Jr, 2017). Siber güvenlik seçeneği olmamakla birlikte işletmeler için zaruri bir ihtiyaçtır. İşletmeler güven ihtiyacını karşıladığı sürece dijital pazarlamada başarılı olur.

- ❖ Birleşik Krallık'ta BT ürünleri ve hizmetleri sağlayan bir kuruluş olan AAG tarafından yapılan araştırmada işletmelerin 2022 yılında yaşanan veri ihlalleri sebebiyle ortalama 4,35 milyon dolar zarara uğradığı görülmüştür (Griffiths, 2023).
- ❖ 2022 yılına ait IC3 internet suçları raporunda “Top Uluslararası Mağdur Ülkeler” arasında 590 toplam kurban sayısı ile Türkiye 13.sırada yer almaktadır (IC3, 2023).
- ❖ WatchGuard Tehdit Laboratuvarı'ndan elde edilen verilere göre, Türkiye’de 2022 yılında gerçekleşen 1.015.810 adet kötü amaçlı yazılım saldırısından %5’i sıfırıncı gün (zero-day) saldırısından meydana gelmektedir (CyberMag, 2023).

BEŞİNCİ BÖLÜM

5. İŞLETMELERİN DİJİTAL PAZARLAMA FAALİYETLERİNDE SİBER

GÜVENLİĞİN YERİ

5.1. E-POSTA PAZARLAMASI

Markaların belirli bir hedef kitleye ulaşmak üzere yaptığı tanıtım, bilgilendirme, kutlama mesajlarında elektronik posta yöntemini kullanmasına e-posta pazarlaması denir (Satıcı, 2020). E-posta pazarlaması ucuz olması, iletim süresinin kısa olması, takip ve analiz kolaylığı, veriyi (datayı) kategorize etme kolaylığı, kişiselleştirme imkânı gibi avantajlara sahiptir. Ancak E-postalar, reklam içeriyorsa genellikle güvenlik filtresi tarafından istenmeyen e-posta (spam) olarak sınıflandırılmaktadır. Dijital pazarlamacıların sık olarak kullandığı e-posta pazarlamasında maillerin önemsiz klasörlere düşme olasılığını azaltmak için; uygun listeler oluşturma, beyaz/açık arka planlar kullanması, kırmızı yazı tiplerinden kaçınması, büyük bir abonelikten çıkma bağlantısı da dahil olmak üzere büyük başlık boyutları kullanması (yasal bir gerekliliktir), minimum resim kullanması oldukça önemlidir. Dijital pazarlamacıların kampanyalarını birleştirme etiketleri ekleyerek alıcıya nasıl bağlı olduğunu göstermesi iyi bir uygulama biçimi olmakla beraber alıcıların işletmeleri adres defterlerine eklemelerini sağlamaları da diğer bir yöntemdir (Business Gateway, 2017).

5.2. E-CRM

Pazarlama kavramı satış ve müşteri hizmetlerindeki süreçleri otomatikleştiren iyi yapılandırılmış ve koordine edilmiş bir CRM sürecidir (Akademi4.0, 2020). CRM, kâr getiren ve sadık müşterilerin belirlenmesi, seçilmesi, elde edilmesi ve geliştirilmesi için bir işletmenin yerine getirdiği faaliyetlerdir (Cuthbertson ve Laine, 2004). Elektronik müşteri ilişkileri yönetimi (E-CRM) ise CRM hedeflerine ulaşmak için e-postalar, web siteleri, sohbet odaları, forumlar ve diğer kanallar gibi İnternet tabanlı teknolojilerin uygulanmasıdır. Bir E-CRM sisteminin uygulanması, bir kuruluşun süreçleri düzene koymasına ve satış, pazarlama ve hizmet personeline daha iyi, daha eksiksiz müşteri bilgileri sağlamasına olanak tanır. Sonuç olarak, E-CRM kuruluşların daha kârlı müşteri ilişkileri

kurmasına ve işletme maliyetlerini azaltmasını sağlar (Diksha, 2020). Aynı zamanda günümüz dünyasında şirketlere rekabet avantajı elde etmesine yardımcı olmaktadır. Herhangi bir ticari işlemi gerçekleştirirken, çevrimiçi müşteri ilişkileri yazılımları, yapılan her yeniden satın alma işleminde müşteri satın alma geçmişinin ve verilerinin kayıtlarını tutmakta bu da şirketlerin satın alma modellerine göre müşteriye daha iyi hizmet vermede yeni fikirlere sahip olduğunu göstermektedir (Kampani ve Jhamb,2020). E-CRM sisteminin başarıyla uygulanmasının göstergeleri, e-CRM sisteminin devreye girmesinden sonra belirli bir zaman diliminde artan satışlar ve sistemin aktif kullanımı ile ilgili istatistiksel verilerdir. E-CRM böylelikle toplam satışlara katkı sağlamakta, satış planlamasının ömrünü kısaltmakta, yeni hizmetlerin geliştirilmesine katkıda bulunmakta ve sistemdeki müşterilerle ilgili toplanan ve arşivlenen verilere göre hizmetlerin kişiselleştirilmesi ile eski müşterilerin elde tutulmasını sağlayarak kârlılığın artmasını etkilemektedir (Pestek ve Pepić, 2011). E-CRM verilerine ulaşmak isteyen bilgisayar korsanlarına karşı dijital pazarlamacılar eğitim almalı, güçlü şifreler seçmeli, yetkilendirme sınıfları oluşturmali, CRM yazılımına girilirken log kayıtları oluşturmali.

5.3. WORDPRESS

WordPress, dünyanın en popüler içerik yönetim sistemidir. Ocak 2016 itibariyle, W3Techs'in Web Teknolojisi Anketleri, WordPress'in içerik yönetim sistemi tespit edilebilecek tüm web sitelerinin %59'u tarafından kullanıldığını tahmin etmiştir. Bu, tüm web sitelerinin %25,7'sine eşittir. Bu oran İnternet'teki tüm web sitelerinin dörtte birinden fazlasını oluşturduğunu kanıtlamaktadır (Price, 2016). Ayrıca WordPress, dünya çapında küçük, orta ve büyük işletmeleri temsil eden en büyük ve en iyi web sitelerin yüzde 14,7'sini oluşturmaktadır. Wordpress'in, kullanışlı, pratik, kullanıcı dostu olması dijital pazarlamada tercih edilmesini sağlamaktadır. Wordpress ile dijital pazarlamacılar kodlama bilmeden siteler inşa edebilmekte, istedikleri özellikleri eklentiler ile sağlayabilmekte, sınırsız tasarıma ulaşmakta, kolay bir şekilde arama motoru optimizasyonu (SEO) çalışmaları yapılabilmekte ve maliyet açısından uygunluğu ile büyük avantaj sağlamaktadır. Bunun yanı sıra Wordpress siteleri birçok hacker tarafından hedef alınmaktadır. Bunun nedenlerinden biri ise bilgisayar korsanının, web'deki 75 milyon WordPress web sitesinden birine girmenin bir yolunu bulabilirse, benzer güvenli olmayan kurulumları

çalıştırabilmesi diğer web sitelerini tarayabilmesi ve bunları da hackleyebilmesidir¹⁵ (Wright, 2018).

2021 yılında Patchstack (Estonya merkezli Bilgisayar ve Ağ Güvenliği şirketi) tarafından yapılan analizde WordPress temalarında 82 benzersiz güvenlik açığı bulunurken, eklentilerde 478 güvenlik sorunu bulunmuştur (Sild, 2022). Dijital pazarlamacıların Wordpress siteyi tercih ederken güvenlik önlemlerine oldukça dikkat etmesi gereklidir. DDos Saldırıları, Siteler Arası Komut Dosyası Çalıştırma, SQL enjeksiyon saldırıları, Parola Saldırıları WordPress sitelerinin uğradığı saldırılardan bazılarıdır. Dijital pazarlamacılar; siber saldırıların önüne geçebilmek için WordPress sitelerini eklerini ve uzantılarını güncel tutmalı, parolalarını güçlü seçmeli, mümkünse iki faktörlü doğrulamaları tercih etmeli, web uygulaması güvenlik duvarı kullanmalı, siteyi SSL ile şifrelemelidir.

5.4. ARAMA MOTORU OPTİMİZASYONU (SEO)

SEO, web sitelerinin arama motorlarında daha iyi performans göstermesi için yapılan çalışmaların tümüne verilen isimdir (Karaman, 2020). Site içi (On-Page SEO) ve site dışı (Off-Page SEO) yapılan optimizasyon çalışmaları sonucunda ilgili sitenin en üst sırada çıkması amaçlanır. Dijital pazarlamanın en çok ilgi isteyen ve geri dönüş açısından en yüksek değer alınan yöntemlerinden biridir. SEO'nun avantajları şu şekildedir: Marka bilinirliğini ve ürün/hizmet satışlarını artırır, Web site trafiğini büyütür, Hedef kitle sayısını yükseltmeye çalışır. Öte yandan, günümüzde dijital pazarlamacıların sıklıkla yaptığı SEO çalışmaları da siber güvenlik tehditlerin en biri haline gelmiş durumdadır.

5.4.1. SEO Zehirlenmesi

SEO çalışmalarında kullanılan teknikler, kullanıcı odaklı olan Beyaz Şapka SEO ve direkt arama motorunu hedef alan Siyah Şapka SEO olmak üzere ikiye ayrılır (Aslan, 2018). Siber suçlular, Siyah Şapka SEO tekniğini kullanır “Siyah Şapka SEO saldırısı olarak da bilinen kötü niyetli bir “SEO zehirlenmesi (SEO poisoning)” saldırısı, bilgisayar korsanlarının bağlantılarının yasal sonuçlardan daha yüksek görünmesini sağlamak için arama motoru sonuçlarını manipüle etmesiyle gerçekleşir” (Runald, 2010). SEO

¹⁵ Bir bilgisayar sistemine izinsiz girmek.

zehirlenmesi iki amaca hizmet eder: Kötü amaçlı yazılım dağıtma ve bilgi hırsızlığı. Kullanıcılara genellikle reklam aracılığıyla kötü amaçlı yazılım meşru bir yazılım olarak gösterilir. Sahte (fake) bir web sitesinin kullanıcıdan kişisel bilgilerini isteyerek kullanıcıyı manipüle etmeye çalışması ise bilgi hırsızlığı olarak adlandırılır. Anti-virüs hizmeti için kişisel ve kart bilgilerinin alınması buna bir örnektir (Edwards, 2021). Bir ziyaretçi, saldırıya uğramış siteye tıkladığında, komut dosyaları, kullanıcının arama botu mu yoksa gerçek bir kişi mi olduğunu tespit eder. Arama botları ve gerçek kişiler iki farklı yöne yönlendirilir. Site kullanıcısı yönlendirilirken, sayfa yükleniyormuş gibi gözüксе de site kullanıcıya virüs bulaştırabileceği bir güvenlik açığı aramaktadır (Bavaro, 2022). Black-hat SEO'da Anahtar Kelime Doldurma (Keyword Stuffing), Görünmez Metin (Invisible Text), Köprü Sayfalar (Doorway Pages), Otomatik İçerik Oluşturma (Automatically Generated Content), Sosyal Medyada Spam Yapma, Hacking (Hacklink), Ufak Metin (Tiny Text), Bağlantı Satın Alma (Buying Incoming Website Links), benzer alan adı kullanmak oldukça yaygın görülen tekniklerdir.

SEO zehirlenmesi işletmeler açısından büyük bir tehdit barındırmaktadır. Bilgisayar korsanlarının güvenilir ve meşru bir işletme sitesini kullanması, arama motorlarının siber saldırıya maruz kalmış siteyi tanımlamasını ve kaldırmasını zorlaştırmaktadır. Site kullanıcılarının birçok yönlendirilmeyle karşılaşması veya şüpheli işlemlerin gerçekleşmesi kullanıcıların siteye güvenini sarsmakta ve site ziyaretini olumsuz yönde etkilemektedir. SEO zehirlenmesi sonucu işletme sayfasının arama motorlarındaki sıralaması arka plana düşebilmektedir. SEO zehirlenmesinde arama motorunda çıkan site sürümüyle girilen sitenin sürümü aynı olmamaktadır. Bu durum siteyi şüpheli hale getirmekte ve güvenlik ihlaline yol açmaktadır (Bavaro, 2022). Arama motorlarının belirlediği güvenlik ihlali nedeniyle işletme siteleri bazı cezalar alabilmekte ya da tamamen site silinebilmektedir. Özellikle WordPress, Joomla! veya Drupal gibi içerik yönetim sistemini (CMS'yi) kullanan dijital pazarlamacılar, bu yapıların bilgisayar korsanları tarafından daha çok hedef alındığını göz önünde bulundurmalıdır. Dijital pazarlamacılar bu saldırı tekniğinin önüne geçmek için gerekli güncellemeleri zamanında yapmalı, güvenlik sağlayıcı bir yazılım ve site izleme araçları kullanmalı, trafik ve anahtar kelimeleri kontrol etmelidir. Küçük işletmeler, "Google Web Yöneticisi Araçlarını" kullanarak herhangi bir masraf

yapmaksızın tüm sayfalarını tarayabilmekte ve sayfa değişikliğinde bilgi alabilmektedir (Moradam, 2022).

5.5. KARA CUMA VE SİBER PAZARTESİ

Büyük indirimlerin olduğu Kara Cuma (Black Friday) ve Siber Pazartesi (Cyber Monday), işletmeler ve tüketicilerin bir araya geldiği en çok alışveriş yapılan zamanlardır. Müşteriler bu sezonlarda fiyatların kıyaslanmasına olanak tanınması, web sitesinde daha farklı indirimlerin olması, kısıtlı zaman, yaşanan izdihamlar, salgın hastalıklar veya cazip kuponlar gibi sebeplerle mağazalara gitmek yerine genellikle e-ticaret sitelerini tercih ederek alışverişlerini gerçekleştirmektedir. Kara Cuma (Black Friday) ve Siber Pazartesi (Cyber Monday) sezonunda gerçekleştirilen satışlardan pay almak isteyen siber saldırganlar bu zamanlarda daha aktif olmaktadır. Siber saldırılar karşısında işletmelerin e-ticaret sitelerinden yapılan satışlar durma noktasına gelebilmektedir. Siteler erişime kapatılmakta ve olası satışların bilgisayar korsanları tarafından önüne geçilmesiyle işletmeler kayıplara uğramaktadır.

5.6. E-SKIMMING (MAGECART SALDIRILARI)

Siber saldırganlar genellikle, kimlik avı dolandırıcılıkları, reklam tuzakları, anlık bildirim tuzakları ve ödeme tuzaklarını içeren yöntemlerle kurbanlarına yaklaşp saldırıları için gerekli bilgileri elde etmektedir (DarkReading, 2022). Örneğin, Amazon gibi popüler e-ticaret web sitelerini taklit ederek müşterinin güvenini sağlamakta ve müşterilerin finansal bilgilerini çalarak işlemleri gerçekleştirmektedirler. Diğer bir örnek, “FakeUpdates” veya “SocGholish” olarak da adlandırılan kötü amaçlı yazılımın, site ziyaretçilerini sahte tarayıcı güncellemelerini yüklemeleri yapması gerektiğine dair ikna edip tasarlanan web sayfalarına yönlendirmesidir (Macleod, 2022). Siber saldırganların sistemdeki zafiyetten yararlanıp hedef e-ticaret platformuna kötü amaçlı JavaScript kodu enjekte ederek "ödeme" süreci gibi bölümleri ele geçirmesi ise e-skimming (“Magecart Attacks”) olarak adlandırılmaktadır (O'Neill, 2022). Diğer bir adı olan Magecart, e-skimming saldırılarını gerçekleştirmekten sorumlu bilgisayar korsanlarını veya bilgisayar korsanı gruplarını tanımlamak için kullanılmaktadır (Acanerler, 2021). 2018 yılında British

Airways'in uğradığı e-skimming saldırısında havayolunun web sitesi ve mobil uygulamasına doğrudan kod enjekte edilerek müşteriler tarafından yapılan ödemeler, üç haftalık süre boyunca çalınmıştır. Şirket 380.000'den fazla kredi kartının veri ihlalinde sorumludur. Kart bilgileri dışında isimler, fatura adresi, e-posta adresi kod tarafından toplanmıştır (Whittaker, 2018). Müşteriler verilerin çalınmasından dolayı zarar görürken şirket, müşterilerinin mali ve kişisel verilerini koruyamadığı için 183,39 milyon sterlinlik bir para cezasıyla karşı karşıya kalmıştır (CBR Staff Writer, 2019). E-skimming saldırılarını minimize etmek için; ödeme yazılımında düzenli güncellemeler yapılmalı, ödeme platformu satıcılarından yazılım yamaları yüklenmeli, kod bütünlüğü kontrolleri düzenli olarak yapılmalı, anti-virüs yazılımı güncel tutulmalı, PCI DSS (Ödeme Kartı Endüstrisi Veri Güvenliği Standardı) uyumuna dikkat edilmeli, web günlükleri takip ve analiz edilmeli, Olay Müdahale Planı hazırlanmalıdır (Cybersecurity and Infrastructure Security Agency, 2019).

5.7. KİTLE KAYNAK KULLANIMI

Kitle kaynak kullanımı¹⁶ pazarlamada giderek daha fazla kullanılmaktadır. Kitle kaynaklı pazarlamanın başarısı, büyük ölçüde insanların etkinliklere katılma ve katkıda bulunma motivasyonuna ve istekliliğine bağlıdır. Bu bağlamda hizmet pazarlamasından olan oyunlaştırma, pazarlama stratejilerine giderek daha fazla entegre edilmektedir (Zichermann ve Cunningham 2011; Witt ve diğerleri, 2011). Geliştirilmiş bir pazarlama tekniği olan oyunlaştırma pazarlamasında, oyunlardan faydalanılarak müşteriler yarış içinde olma veya ödül kazanma motivasyonu ile bir eylemi gerçekleştirmeye yönlendirilir (Byrne, 2022). Bunun dışında oyunlaştırma ile birçok veri elde edilebilmekte ve kullanabilmektedir. Oyunlaştırmanın bir örneği olan Nike+Fuel koşu uygulaması, kullanıcıların fiziksel aktivitelerini takip etmelerini ve günlük fiziksel aktivite miktarlarında birbirleriyle rekabet etmelerini sağlayan bir uygulamadır. Nike, içerik pazarlaması için değerli olan kullanıcı verilerini oyunlaştırma ile sağlayarak bilgileri kişiselleştirilmiş hizmetler için veya Ar-Ge ve dijital pazarlama çalışmalarında kullanabilmektedir (Gamewheel,

¹⁶ Geleneksel çalışanlardan veya tedarikçilerden ziyade büyük bir insan grubundan ve özellikle çevrimiçi topluluklardan katkı isteyerek ihtiyaç duyulan hizmetleri, fikirleri veya içeriği elde etme süreci olarak tanımlanır.

2020). Veri elde etmenin dışında hizmetin oyunlaştırılması müşterinin sadakatini de artırmaktadır.

Gamewheel, Urban Sports Club için kaya tırmanışı temalı bir oyun piyasaya sürmüştür. Oyun temasında, kullanıcının 3 aylık ücretsiz bir sözleşme kazanma şansı elde etmesi için mümkün olduğunca yükseğe tırmanması gerekmektedir. İstatistiksel olarak analiz yapıldığında kullanıcıların büyük bir kısmının oyunu 3 defadan fazla oynadığı tespit edilmiştir. Oyunun 3 defadan fazla oynanması çok yüksek bir etkileşim seviyesini göstermektedir. Bunun dışında Urban Sports Club oyuna katılan şahısların bu sayede verilerini kullanarak onları topluluğuna eklemiştir (Gamewheel, 2020).

Target perakende işletmesi, “Holiday Wish” isimli bir oyun geliştirmiş ve çocukların Noel Baba’ya göndermek istedikleri dilek listeleri üzerine odaklanmıştır. Bu özel oyun sınırlı dağıtımla piyasaya sürülmüş ve büyük bir başarı elde etmiştir. Dilek listesindeki 30 ögenin toplam değeri yaklaşık 1.500 dolar olarak belirlenmiştir. Başarılı olan bu uygulama ile birçok kullanıcı verisi toplanmıştır. İşletme, oyunun piyasaya sürülmesi ile 100.000’den fazla dilek listesine ulaşmıştır. Uygulama aracılığıyla Target.com’da 9.200 yeni hesap oluşturulmuştur. Kullanıcıların %61’i uygulamayı haftada birden çok kullanırken günde birden çok kez kullananların %31’i siteye bir milyon fazla girerek site trafiğini önemli ölçüde artırdığı görülmüştür. Uygulama lansmanından tatil sezonunun kapanışına kadar geçen altı haftalık süreçte dilek listelerine toplam yaklaşık 1,7 milyon öge eklenmiş ve toplam 92,3 milyon dolarlık satış potansiyeline ulaşılmıştır (Gamewheel, 2020).

5.7. SATIŞ ORTAKLIĞI

Dijital pazarlamanın bir alt kümesi olan Satış Ortaklığı (Affiliate Marketing), “yayıncıların başka bir perakendeci veya reklamcı tarafından bir bağlı kuruluş bağlantısı kullanılarak yapılan bir ürün veya hizmeti tanıtarak komisyon kazandığı bir süreçtir” (Hayes, 2022). Daha geniş bir pazara erişim, nitelikli müşteri adaylarının daha iyi muhasebeleştirilmesi, düşük maliyetli reklamcılık gibi avantajlara sahiptir. Amazon Associates, Etsy, eBay gibi bilinen siteler satış ortaklığı yaparak kullanıcılarına satışlar için bir komisyon vermektedir (Frankenfield, 2022). Bilgisayar korsanları dolandırıcılık faaliyetlerini gerçekleştirmek için satış ortaklığı yolunu kullanarak tüccarları, bağlı kuruluşları veya

alıcıları mağdur edebilmektedir. İstenmeyen e-posta gönderme teknikleri, satıcının alan adının varyasyonu (yazım hatası), parazit siteler ve trafik yönlendirme, sahte tıklamalar veya yönlendirmeler ve site klonlama satış ortaklığı dolandırıcılığının izlediği yollardan sadece bazılarıdır (Globaldots, 2016). “Satış ortaklığı dolandırıcılığı işletmelere satışlarda %20-65'e varan büyük bir maliyete neden olabilmektedir.” (Loveless, 2022).

5.8. KULLANICI TARAFINDAN OLUŞTURULAN İÇERİK

“Kullanıcı tarafından oluşturulan içerik (UGC), bir markanın kullanıcıları tarafından oluşturulan, yayınlanan ve/veya sunulan herhangi bir içeriktir” (Gallegos, 2021). Tüketiciler kullanıcı tarafından oluşturulan içeriği, markalar tarafından oluşturulan içeriğe kıyasla 2,4 kat daha fazla orijinal görmektedirler (Beveridge, 2022). “Popülerliği ve sosyal medyadaki erişimi nedeniyle bugün dijital pazarlama dünyasının en sıcak konularından biridir” (Das, 2021). Coca Cola "Share a Coke" kampanyasında müşterilerin, kişiselleştirilmiş kola şişeleriyle çekilmiş fotoğraflarını sosyal medyada paylaşmaları kullanıcı tarafından oluşturulan içerik konusunda başarılı olmuş bir örnektir. Coca Cola reklamını bu sayede geniş bir kitleye yaymış ve müşterileriyle bağ kurarak reklamlarını onlara yaptırmıştır (Gallegos, 2021). İşletmeler tanıtım amaçlı gerçekleştirdiği bu süreçte kullanıcı tarafından oluşturulan içeriklere kötü amaçlı kodların enjekte edilmesinin önüne geçmeli, kullanıcılara sosyal mühendislik yapabilecekleri açık kapılar bırakmamalı (kullanıcı adının işletme çalışanını temsil etmesi gibi) ve kötü niyetli bağlantılara ve resmi görünümlü hesaplara dikkat etmelidir (Posey, 2019).

ALTINCI BÖLÜM

6. SOSYAL AĞ ANALİZİNE VE BİBLİYOMETRİK HARİTALAMAYA İLİŞKİN ANALİZLER

Çalışmada siber güvenlik alanında öne çıkan konu ve kavramları belirlemek amacıyla araştırma metotlarından sosyal ağ analizi kullanılmıştır. Bibliyometrik haritalama ise bir araştırma tekniğidir. Siber güvenlik alanında elde edilen veriler bu teknikle görselleştirilerek verilerin anlaşılması ve verilerden bilgi çıkarımının kolaylaştırılması amaçlanmıştır.

Sosyal ağ analizi ile siber güvenlik kavramına ait verilerin ilişkisel boyutu sunulmuştur. Ülkeler, yayın sayıları, yazarlar, araştırma alanları, kurumlar, yayıncılar ve anahtar kelimeler dünya genelinde ve Türkiye kapsamında incelenmiştir. Çıkarılan ağ ilişkileri görselleştirilmiştir. Elde edilen verilerle çıkarımsal istatistiki bilgilere ulaşılmıştır. Bu veriler hazırbulunuşluk ölçeğinin hazırlanmasında esas alınmıştır.

6.1. SİBER GÜVENLİK KONULU YAYINLARIN ÜLKELERE GÖRE YAYIN SAYISI

Şekil 2

Yayın Sayısına Göre İlk 25 Ülke



Not. Yayın sayısına göre ilk 25 ülke MapChart (<https://www.mapchart.net/world-advanced.html>) kullanılarak oluşturuldu.

Tablo 5*Ülkelere Göre Yayın Sayısı (İlk 25 Ülke)*

	Ülke	Yayın Sayısı	Toplam Yayına Göre Oranı
1.	Amerika Birleşik Devletleri	2,546	28.207%
2.	Çin	893	9.894%
3.	İngiltere	835	9.251%
4.	Hindistan	670	7.423%
5.	Avustralya	451	4.997%
6.	İtalya	336	3.723%
7.	Kanada	311	3.446%
8.	Güney Kore	278	3.080%
9.	Almanya	265	2.936%
10.	Suudi Arabistan	263	2.914%
11.	Fransa	208	2.304%
12.	Japonya	205	2.271%
13.	Türkiye	186	2.027%
14.	Norveç	152	1.684%
15.	Rusya	148	1.640%
16.	Güney Afrika	148	1.640%
17.	İspanya	147	1.629%
18.	Yunanistan	143	1.584%
19.	Singapur	143	1.584%
20.	Pakistan	141	1.562%
21.	Malezya	138	1.529%
22.	Hollanda	137	1.518%
23.	İsveç	135	1.496%
24.	Romanya	131	1.451%
25.	Finlandiya	116	1.285%

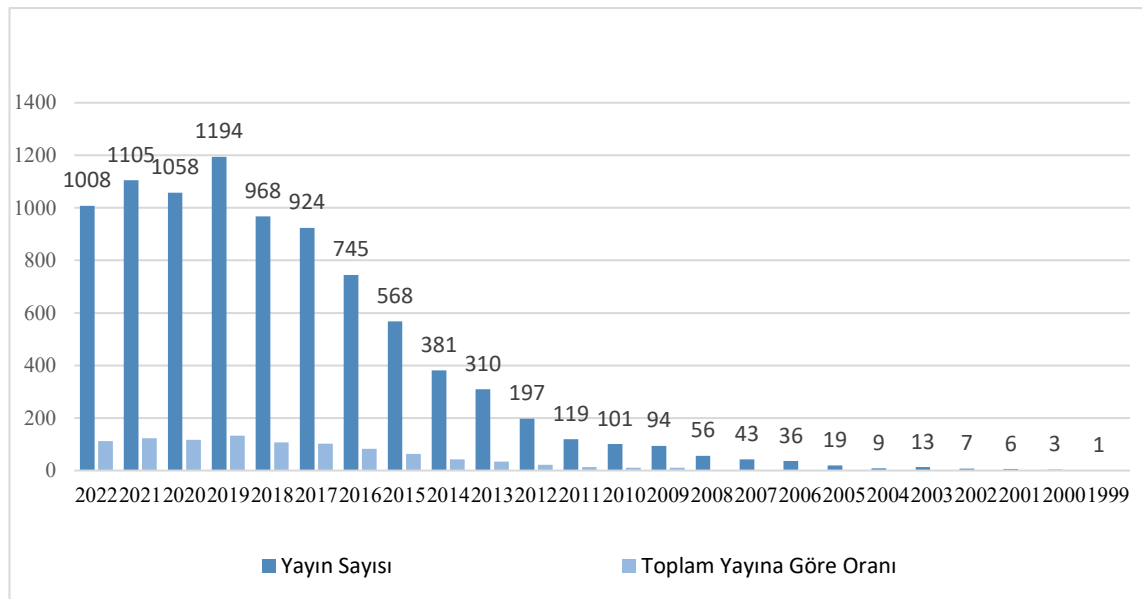
WoS veri tabanından elde edilen bilimsel yayınlarda siber güvenlik konusunu esas alan araştırmalar analiz edilmiştir (Bkz. Tablo 18). Yapılan analiz sonucunda ilk 25

ülkenin yayın sayısına göre sıralaması incelenmiştir. Ülkelerin siber güvenlik konulu bilimsel yayın performansları incelendiğinde, sırasıyla Amerika, Çin, İngiltere, Hindistan, Avustralya, İtalya, Kanada, Güney Kore, Almanya, Suudi Arabistan ülkelerinin ilk on sırada yer aldıkları görülmektedir. Siber Güvenlik konulu bilimsel yayınlarda Amerika'nın diğer ülkelere göre bilimsel yayın performansı açık bir arayla öndedir. Wos temelli siber güvenlik konulu araştırmalara bakıldığında 9,026 sayılı kaynaktan 2,546'sı Amerika'ya ait olmakla birlikte bu alanla ilgili bütün yayınların 28.207%' sini oluşturmaktadır. Amerika Birleşik Devletleri'nin diğer ülkelere oranla siber güvenlik konusunda farkındalığının oldukça yüksek ve aktif olduğu görülmektedir. Sırasıyla diğer ilk beşte yer alan dört ülke; Çin 893 sayılı kaynak ile 9.894%'ünü, İngiltere 835 sayılı kaynak ile 9.251%'ini, Hindistan 670 sayılı kaynak ile 7.423%'ünü, Avustralya 451 sayılı kaynak ile 4.997%'sini oluşturmaktadır. Türkiye ise siber güvenlik alanında yapılan yayınlarda 13.sırada yer almaktadır. Türkiye'de 186 tane yayın tespit edilmiştir. Bu ise toplam kaynak sayısının 2.027%'sini oluşturmaktadır.

6.2. SİBER GÜVENLİK KONULU YAYINLARIN DÜNYA GENELİNDE YILLARA GÖRE YAYIN SAYILARI

Tablo 6

Dünya Genelinde Yıllara Göre Yayın Sayıları



WoS veri tabanından elde edilen bilimsel yayınlarda siber güvenlik konusunu esas alan araştırmalar yıllara göre analiz edilmiştir. 1999-2022 yılları arasında WoS veri tabanında siber güvenlik konulu toplam yayın sayısı 1 ile 1194 arasında değişmekle birlikte 8965 tanedir. Son yıllarda bu konu ile ilgili yapılan yayınlar artsa da düzenli bir artış görülmemektedir. Yaşanan dijitalleşme ile siber güvenlik alanyazınında daha çok yayın olması beklenmektedir.

6.3. SİBER GÜVENLİK KONULU YAYINLARIN TÜRKİYE' DE DÜNYA GENELİNDE YILLARA GÖRE YAYIN SAYILARI

Tablo 7

Türkiye' de Yıllara Göre Yayın Sayıları

Yıl	Yayın Sayısı	Toplam Yayına Göre Oranı
2022	29	15.847%
2021	26	14.208%
2020	31	16.940%
2019	21	11.475%
2018	26	14.208%
2017	18	9.836%
2016	9	4.918%
2015	9	4.918%
2014	9	4.918%
2013	1	0.546%
2012	3	1.639%
2011	1	0.546%

Toplam 186 yayın sayısı incelendiğinde; 31 tanesi 2020 yılında, 29'u 2022 yılında, 26 tanesi 2018 yılında, 26 tanesi 2021 yılında, 21 tanesi 2019 yılına aittir. Dünya genelinde olduğu gibi bu alandaki yayın sayılarında yıllara göre düzenli bir artış veya

azalış görülmemektedir. Dünya genelinde siber güvenlik alanında yapılan yayın sıralamasında Türkiye 13.sırada yer almasına rağmen yayın sayısı oldukça kısıtlıdır. Artan dijitalleşme ve siber güvenlik farkındalığı ile daha çok yayının olması beklenmektedir.

6.4. SİBER GÜVENLİK KONULU YAYINLARDA EN ÜRETKEN YAZARLAR

Tablo 8

En Üretken Yazarlar

Yazar	Yayın Sayısı	Toplam Yayına Göre Oranı	H-indeksi
Choo KKR	68	0.322%	21
Zhang Y	65	0.308%	17
Kumar R	61	0.289%	10
Wang Y	54	0.256%	13
Kim J	53	0.251%	12
Li J	53	0.251%	11
Kotenko I	51	0.242%	7
Govindarasu M	47	0.223%	15
Li Y	46	0.218%	11
Liu Y	46	0.218%	13
Chen Y	45	0.213%	13
Kim S	43	0.204%	9
Liu X	41	0.194%	18
Bou-harb E	40	0.190%	15
Kim H	40	0.190%	7
Lee S	39	0.185%	11
Li X	39	0.185%	15
Kumar A	38	0.180%	7
Moustafa N	38	0.180%	16
Skopik F	37	0.175%	8
Ishii H	35	0.166%	11
Liu CC	35	0.166%	15

Zhu QY	34	0.161%	14
Conti M	33	0.156%	14
Dehghantanha A	32	0.152%	15

Analizden elde edilen bulgulara göre, siber güvenlik alanında etkin ve tanınmış yazarlar; yazarların atıf sayısı belirlenmiştir. “Siber güvenlik” konulu yayınların WoS tabanlı incelenmesine göre en fazla yayının Choo, Kim-Kwang Raymond tarafından yayınlandığı (n=68) görülmektedir. Aynı zamanda Choo, Kim-Kwang Raymond en yüksek H-indeks değerine (n=21) sahiptir. Sonuçlar, araştırmacı yayınlarının frekansını ve etkisini tespit etmektedir. Üretken yazarlar genellikle güncel gelişmeleri titizlikle takip ettikleri için bu yazarların yayınları incelendiğinde sektördeki yenilikler, sorunlar ve çözümler daha ayrıntılı bir şekilde analiz edilebilir. Aynı zamanda, bu yazarlar ile iletişim kurularak ağ oluşturma, bilgi akışı veya yeni projeler için potansiyel fırsatlar elde edilebilir.

6.5. SİBER GÜVENLİK KONULU YAYINLARDA TÜRKİYE’DEKİ EN ÜRET-KEN YAZARLAR

Tablo 9

Türkiye’deki En Üretken Yazarlar

Yazar	Yayın Sayısı	Toplam Yayına Göre Oranı	H-indeksi
Sagiroglu S	7	3.763%	2
Baykal N	6	3.226%	4
Karabacak B	6	3.226%	4
Das R	5	2.688%	3
Gonen S	5	2.688%	3
Karacayilmaz G	5	2.688%	3
Demirci M	4	2.151%	2
Dogru IA	4	2.151%	2
Sahingoz OK	4	2.151%	3
Yilmaz EN	4	2.151%	2
Al-turjman F	3	1.613%	3
Aydin MA	3	1.613%	2
Bicakci K	3	1.613%	3
Catak FO	3	1.613%	2
Ertam F	3	1.613%	3

Gunduz MZ	3	1.613%	3
Samet R	3	1.613%	2
Savas E	3	1.613%	2
Sayan HH	3	1.613%	2
Selcuk AA	3	1.613%	2
Sindiren E	3	1.613%	2
Tatar U	3	1.613%	2
Ustunsoy F	3	1.613%	2
Yurekten O	3	1.613%	2
Zaim AH	3	1.613%	2

Analizden elde edilen bulgulara göre, Türkiye’deki siber güvenlik alanında etkin ve tanınmış yazarlar; yazarların atıf sayısı belirlenmiştir. “Siber güvenlik” konulu yayınların WoS tabanlı incelenmesine göre en fazla yayının Prof. Dr. Şeref Sağıroğlu tarafından yayınlandığı (n=7) görülmektedir. Diğer yandan Prof. Dr. Nazife Baykal ve Dr. Bilge Karabacak en yüksek H-indeks değerine (n=4) sahiptir. Sonuçlar, araştırmacı yayınlarının frekansını ve etkisini tespit etmektedir. Üretken yazarlar genellikle güncel gelişmeleri titizlikle takip ettikleri için bu yazarların yayınları incelendiğinde sektördeki yenilikler, sorunlar ve çözümler daha ayrıntılı bir şekilde analiz edilebilir. Aynı zamanda, bu yazarlar ile iletişim kurularak ağ oluşturma, bilgi akışı veya yeni projeler için potansiyel fırsatlar elde edilebilir.

6.6. SİBER GÜVENLİK KONULU YAYINLARIN ARAŞTIRMA ALANINA GÖRE DAĞILIMI

Tablo 10

Dünya Geneline Araştırma Alanına Göre Dağılım

Araştırma Alanı	Yayın Sayısı	Toplam Yayına Göre Oranı
Bilgisayar Bilimi	5,383	59.639%
Mühendislik	3,535	39.165%
Telekomünikasyon	1,368	15.156%
Otomasyon Kontrol Sistemleri	492	5.451%
Enerji Yakıtları	438	4.853%
Devlet Hukuku	281	3.113%
İş Ekonomisi	269	2.980%
Bilim Teknoloji Diğer Konular	269	2.980%

Uluslararası İlişkiler	228	2.526%
Eğitim	207	2.293%
Yöneylem Araştırması Yönetim Bilimi	204	2.260%
Matematik	168	1.861%
Enstrümanlar Enstrümantasyon	163	1.806%
Fizik	160	1.773%
Kimya	138	1.529%
Bilgi Bilimi Kütüphane Bilimi	132	1.462%
Sosyal Bilimler (Diğer Konular)	118	1.307%
Toplu Taşıma	118	1.307%
Kriminoloji Penolojisi	115	1.274%
Malzeme Bilimi	101	1.119%
Optik	89	0.986%
Çevre Bilimleri Ekoloji	73	0.809%
Kamu Yönetimi	72	0.798%
Psikoloji	65	0.720%
Robotik	62	0.687%

Tabloda görüldüğü üzere Siber Güvenlik çok disiplinli bir alandır. Birçok alanı doğrudan ve dolaylı olarak etkilemektedir. İlk sırada Bilgisayar Bilimleri yer alırken açık bir arayla önde olduğu görülmektedir. Bu durum bilgisayar bilimi alanında siber güvenlik konusuna ilginin yoğun ve literatürün oldukça gelişmiş olduğunu göstermektedir. Bilgisayar bilimlerini sırasıyla Mühendislik, Telekomünikasyon gibi alanlar takip etmektedir.

Analizden elde edilen bulgulara göre:

- ✓ Araştırma alanlarının çeşitliği ve derinliği,
- ✓ Araştırma alanlarındaki siber güvenlik konusunun gelişimi görülmektedir.
- ✓ Sonuçlara göre:
- ✓ Siber güvenlik alanyazınında yayınların düşük olduğu alanlar belirlenip gelecekteki araştırmalar ve keşifler bu doğrultuda yönlendirerek farklı bakış açıları sunulabilir.
- ✓ Siber güvenlik alanyazınında yayınların yüksek olduğu alanlar belirlenip akademik ve endüstriyel olarak bu alanların ilgi gördüğü, kaynak bakımından oldukça zengin olduğu esas alınarak literatür çalışmaları genişletilebilir.

6.7. SİBER GÜVENLİK KONULU YAYINLARIN TÜRKİYE’DE ARAŞTIRMA ALANINA GÖRE DAĞILIMI

Tablo 11

Türkiye’de Araştırma Alanına Göre Dağılım

Araştırma Alanı	Yayın Sayısı	Toplam Yayına Göre Oranı
Bilgisayar Bilimi	118	63.441%
Mühendislik	75	40.323%
Telekomünikasyon	33	17.742%
Bilim Teknoloji Diğer Konular	8	4.301%
Enerji Yakıtları	5	2.688%
Devlet Hukuku	5	2.688%
Uluslararası ilişkiler	5	2.688%
İş ekonomisi	4	2.151%
Yöneylem Araştırması Yönetim Bilimi	4	2.151%
Uzaktan Algılama	3	1.613%
Alan çalışmaları	2	1.075%
Otomasyon Kontrol Sistemleri	2	1.075%
Kriminoloji Penolojisi	2	1.075%
Eğitim Eğitim Araştırması	2	1.075%
Bilgi Bilimi Kütüphane Bilimi	2	1.075%
Matematik	2	1.075%
Optik	2	1.075%
Psikoloji	2	1.075%
Kamu Yönetimi	2	1.075%
Robotik	2	1.075%
Akustik	1	0.538%
Kimya	1	0.538%
İletişim	1	0.538%
Çevre Bilimleri Ekoloji	1	0.538%
Tarih	1	0.538%

Tabloda görüldüğü üzere Siber Güvenlik çok disiplinli bir alandır. Birçok alanı doğrudan ve dolaylı olarak etkilemektedir. Dünya genelinde olduğu gibi ilk sırada Bilgisayar Bilimleri yer alırken, Bilgisayar Bilimleri’nin diğer alanlara göre açık bir arayla önde

olduğu görülmektedir. Dünya genelinde oran 59.639% iken Türkiye’de 63.441% olup daha yüksektir. Dünyada ve Türkiye’de siber güvenlik yayınlarının yarısından fazlası Bilgisayar Bilimleri alanındadır. Bu durum bilgisayar bilimi alanında siber güvenlik konusuna ilginin yoğun ve literatürün oldukça gelişmiş olduğunu göstermektedir. Sonuçlar dünya genelindeki araştırma ile kıyaslandığında;

- ❖ Türkiye’de siber güvenlik konulu en çok araştırma yapılan ilk üç alanın (Bilgisayar Bilimi, Mühendislik, Telekomünikasyon) dünya genelindeki ilk üç alan ile aynı olduğu,
- ❖ Enerji Yakıtları ve Devlet Hukuku araştırma alanlarının her iki listede aynı sırada yer aldığı,
- ❖ Dünya genelinde ilk on alanda Otomasyon Kontrol Sistemleri, Eğitim araştırma alanları bulunurken Türkiye’de bu alanların ilk on alanda olmadığı,
- ❖ Türkiye’de ilk on alanda Yöneylem Araştırması Yönetim Bilimi ve Uzaktan Algılama araştırma alanları bulunurken dünya genelinde ilk on alanda bulunmadığı,
- ❖ İş Ekonomisi alanındaki yayınların her iki listede ilk on sıralamada yer almasına rağmen dünya genelinde 7.sırada Türkiye’de 8.sırada yer aldığı,
- ❖ Bilim Teknoloji Diğer Konular alanındaki yayınların her iki listede ilk on sıralamada yer almasına rağmen dünya genelinde 8. Türkiye’de 4.sırada olduğu,
- ❖ Uluslararası ilişkiler alanındaki yayınların her iki listede ilk on sıralamada yer almasına rağmen dünya genelinde 9.sırada Türkiye’de 7.sırada yer aldığı,
- ❖ Dünya genelinde ilk on alanındaki Otomasyon Kontrol Sistemleri araştırma alanının Türkiye’de 12.sırada yer aldığı,
- ❖ Dünya genelinde ilk on alanındaki Eğitim araştırma alanının Türkiye’de 14.sırada yer aldığı,
- ❖ Türkiye genelinde ilk on alanındaki Yöneylem Araştırması Yönetim Bilimi araştırma alanının dünya genelinde 11.sırada yer aldığı,

- ❖ Türkiye genelinde ilk on alanındaki Uzaktan Algılama araştırma alanının dünya genelinde ilk 25 alanda yer almadığı,
- ❖ Her iki listede araştırma yapılan alanların benzerlik gösterdiği görülmektedir.

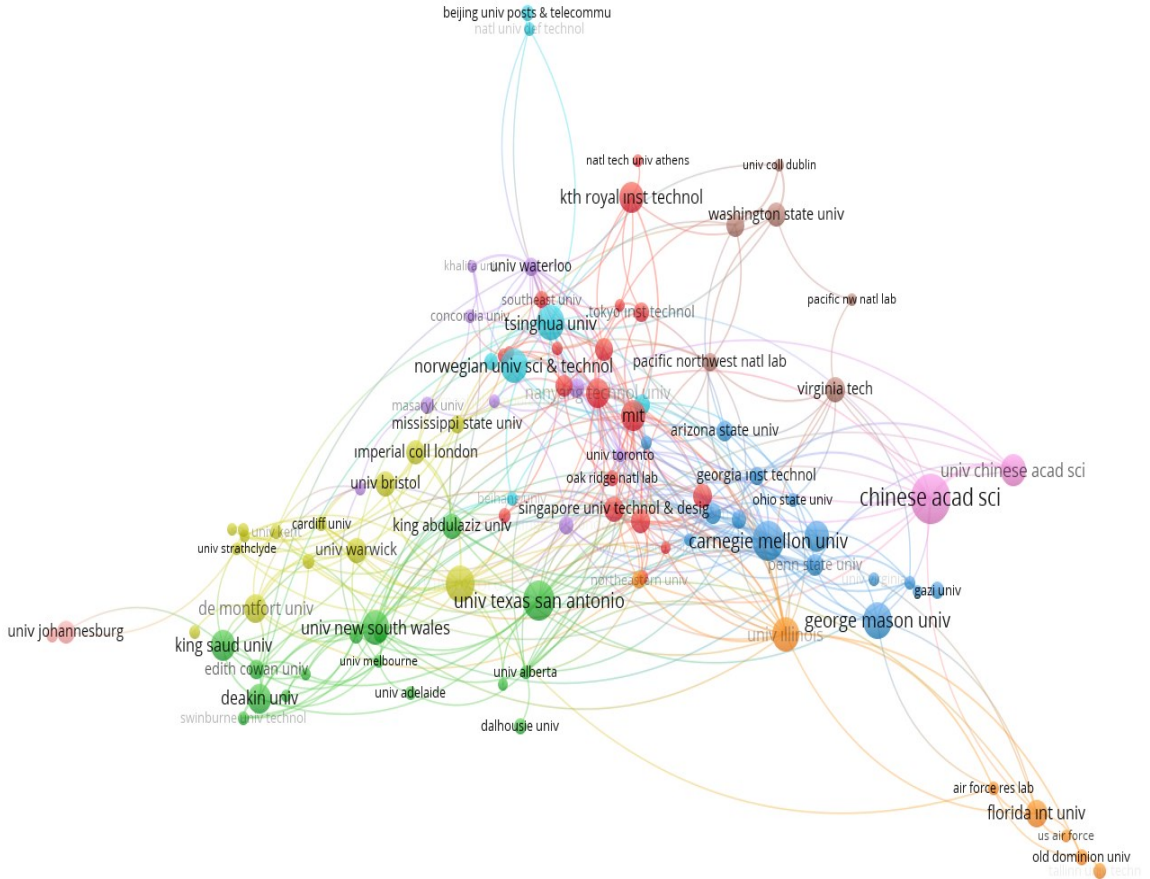
Ayrıca analizden elde edilen bulgulara göre:

- ✓ Araştırma alanlarının çeşitliği ve derinliği,
- ✓ Araştırma alanlarındaki siber güvenlik konusunun gelişimi görülmektedir.
- ✓ Sonuçlara göre:
- ✓ Siber güvenlik alanyazınında yayınların düşük olduğu alanlar belirlenip gelecekteki araştırmalar ve keşifler bu doğrultuda yönlendirerek farklı bakış açıları sunulabilir.
- ✓ Siber güvenlik alanyazınında yayınların yüksek olduğu alanlar belirlenip akademik ve endüstriyel olarak bu alanların ilgi gördüğü, kaynak bakımından oldukça zengin olduğu esas alınarak literatür yayınları genişletilebilir.

6.8. SİBER GÜVENLİK KONULU YAYINLARIN KURUMLARA GÖRE DAĞILIMI

Şekil 3

Yayınların Kurumlara Göre Bibliyometrik Ağ Analizi



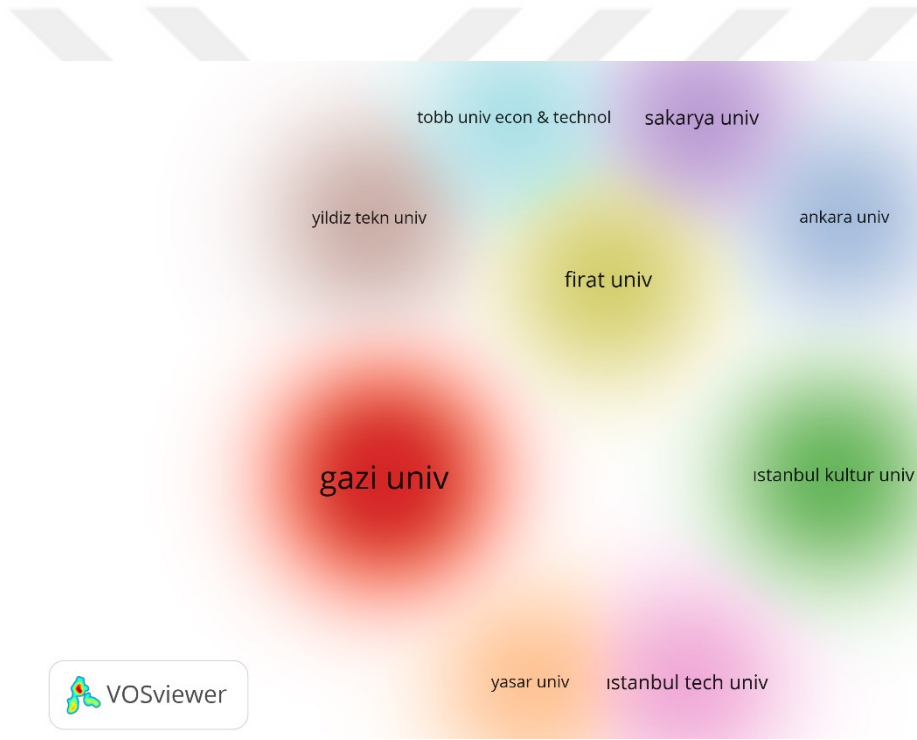
Kurumlar görselleştirilirken en az 20 yayının o kuruma ait olması esas alınmıştır. 6389 kurumdan bağlantılı 97 kurum *şekil 3*’te yer almaktadır. En çok yayın yapan ilk on kurum şu şekildedir: “Chinese Academy of Sciences” (131 adet), The University of Texas at San Antonio” (64 adet),” Carnegie Mellon University” (63 adet), “University of Oxford” (58 adet), “George Mason University” (58 adet), “Tsinghua University” (56 Adet), “University of Illinois” (54 adet), “University of New South Wales” (54 adet), “Norwegian University of Science and Technology.” (54 Adet), “Massachusetts Institute of Technology” (50 adet). Analizden elde edilen bulgular bu kurumların;

- ❖ Siber güvenlik alanında inovatif ve öncü kurumlar olarak öne çıktığını,
- ❖ Siber güvenlik konusunda potansiyel iş birlikleri ve ortak projeler için uygun olduğunu göstermektedir.

6.9. SİBER GÜVENLİK KONULU YAYINLARIN TÜRKİYE’DE KURUMLARA GÖRE DAĞILIMI

Şekil 4

Türkiye’de Yayınların Kurumlara Göre Bibliyometrik Ağ Analizi



Siber Güvenlik Konulu Yayınların Türkiye’de Kurumlara Göre Dağılımı *şekil 4*’te gösterilmiştir. Kurumlar görselleştirilirken en az 4 yayının o kuruma ait olması esas alınmıştır. 206 kurumdan 9 kurum görselde yer almaktadır. En çok yayın yapan ilk on kurum şu şekildedir: “Gazi Üniversitesi” (26 adet), “Fırat Üniversitesi” (10 adet), “Orta Doğu Teknik Üniversitesi” (9 adet), “İstanbul Teknik Üniversitesi” (8 adet), “Sakarya Üniversitesi” (8 adet), “İstanbul Kültür Üniversitesi” (6 adet), “Hacettepe Üniversitesi” (4 adet), “İstanbul Ticaret Üniversitesi” (4 adet), “İstanbul Ticaret Üniversitesi” (4 adet),

“İstanbul Üniversitesi-Cerrahpaşa” (4 adet). Analizden elde edilen bulgular bu kurumların;

- ✓ Siber güvenlik alanında inovatif ve öncü kurumlar olarak öne çıktığını,
- ✓ Siber güvenlik konusunda potansiyel iş birlikleri ve ortak projeler için uygun olduğunu göstermektedir.

6.10. SİBER GÜVENLİK KONULU YAYINLARIN YAYINCILARINA GÖRE DAĞILIMI

Tablo 12

Yayınların Yayıncılara Göre Analizi

Dergi	Yayın Sayısı	Toplam Yayına Göre Oranı
IEEE	3,675	40.702%
Springer Nature	1,109	12.283%
Elsevier	865	9.580%
Mdpi	381	4.220%
Assoc Computing Machinery	337	3.732%
Acad Conferences Ltd	211	2.337%
Taylor & Francis	186	2.060%
Wiley	180	1.994%
Igi Global	104	1.152%
Emerald Group Publishing	87	0.964%
Ios Press	85	0.941%
Spie-Int Soc Optical Engineering	79	0.875%
Sage	73	0.809%
Scitepress	63	0.698%
Science & Information Sai Organization Ltd	57	0.631%
Wiley-Hindawi	51	0.565%
Routledge	49	0.543%
Oxford Univ Press	45	0.498%
Inderscience Enterprises Ltd	34	0.377%
Frontiers Media Sa	33	0.365%
Int Journal Computer Science & Network Security-Ijcsns	32	0.354%
Cambridge Univ Press	27	0.299%

Tech Science Press	26	0.288%
Iated-Int Assoc Technology Education & Development	25	0.277%
Inst Engineering Technology-Iet	22	0.244%

Yayınların dergilere göre analizine bakıldığında ilk sırada IEEE dergisi yer almaktadır. 3,675 yayınlı toplam yayınların 40.702%'sini oluşturmaktadır. Sırasıyla Springer Nature 1,109 yayınlı 12.283%'ünü, Elsevier 865 yayınlı 9.580%'ini, Mdpi 381 yayınlı 4.220%'sini, Assoc Computing Machinery 337 yayınlı 3.732%'sini oluşturmaktadır.

Analizden elde edilen bulgular ile bu dergilerin;

- ✓ Siber güvenlik konusunda yayın performanslarının yüksek olduğu,
- ✓ Siber güvenlik temelli araştırmalarda en prestijli ve etkili dergiler olarak öne çıktığı,
- ✓ Siber güvenlik alanında araştırmacılara yayınlarını yayınlama imkânı verdiği görülmektedir.

6.11. TÜRK ARAŞTIRMACILARIN SİBER GÜVENLİK KONULU YAYINLARININ YAYINCILARA GÖRE DAĞILIMI

Tablo 13

Türk Araştırmacılar Tarafından Yayımlanan Yayınların Yayıncılara Göre Analizi

Dergi	Yayın Sayısı	Toplam Yayına Göre Oranı
IEEE	71	38.172%
Elsevier	24	12.903%
Springer Nature	14	7.527%
Acad Conferences Ltd	8	4.301%
Ios Press	6	3.226%
Taylor & Francis	6	3.226%
Gazi Univ	4	2.151%
Sage	3	1.613%
Wiley	3	1.613%
Assoc Computing Machinery	2	1.075%
Emerald Group Publishing	2	1.075%
Istanbul Univ-Cerrahpasa	2	1.075%
Mdpi	2	1.075%
Spie-Int Soc Optical Engineering	2	1.075%

Uluslararası İlişkiler Konseyi Derneği	2	1.075%
Wiley-Hindawi	2	1.075%
Agh Univ Science & Technology Press	1	0.538%
Ahmet Yesevi Univ	1	0.538%
Assoc Computational Linguistics-Acl	1	0.538%
Assoc Digital Forensics, Security & Law	1	0.538%
Cambridge Univ Press	1	0.538%
Copernicus Gesellschaft Mbh	1	0.538%
Daaam International Vienna	1	0.538%
Dynamic Publishers, Inc	1	0.538%
Engineering & Technology Publishing	1	0.538%

Yayınların dergilere göre analizine bakıldığında ilk sırada dünya genelinde olduğu gibi IEEE yayıncısı yer almaktadır. 71 yayınlı toplam yayınların 38.172%'sini oluşturmaktadır. Sırasıyla Elsevier 24 yayınlı 12.903%'ünü, Springer Nature 14 yayınlı 7.527%'sini, Acad Conferences Ltd 8 yayınlı 4.301%'ini, Ios Press 6 yayınlı 3.226%'sini oluşturmaktadır. Sonuçlar dünya genelindeki araştırma ile kıyaslandığında;

- ❖ IEEE, Springer Nature ve Elsevier her iki listede ilk üçte yer aldığı,
- ❖ Elsevier, Türkiye'de 2.sırada yer alırken dünya genelinde 3.sırada bulunduğu,
- ❖ Springer Nature, Türkiye'de 3.sırada yer alırken dünya genelinde 2.sırada bulunduğu,
- ❖ Acad Conferences Ltd, Türkiye'de 4.sırada yer alırken dünya genelinde 6.sırada yer aldığı,
- ❖ Taylor & Francis, Türkiye'de 6.sırada yer alırken dünya genelinde 7.sırada olduğu,
- ❖ Wiley, Türkiye'de 9.sırada yer alırken dünya genelinde 8.sırada bulunduğu,
- ❖ Assoc Computing Machinery, Türkiye'de 10.sırada yer alırken dünya genelinde 5.sırada bulunduğu,
- ❖ Ios Press, Gazi Üniversitesi ve Sage yayıncılarının Türkiye'de ilk on sırada bulunurken dünya genelinde ilk on sırada bulunmadığı,
- ❖ Mdpi, Igi Global ve Emerald Group Publishing yayıncılarının dünya genelinde ilk on sırada bulunurken Türkiye'de ilk on sırada yer almadığı,

❖ Her iki listede ilk onda yer alan yedi yayıncının ortak olduğu görülmektedir. (*“IEEE”, “Springer Nature”, “Elsevier”, “Acad Conferences Ltd”, “Taylor & Francis”, “Wiley” ve “Assoc Computing Machinery”*)

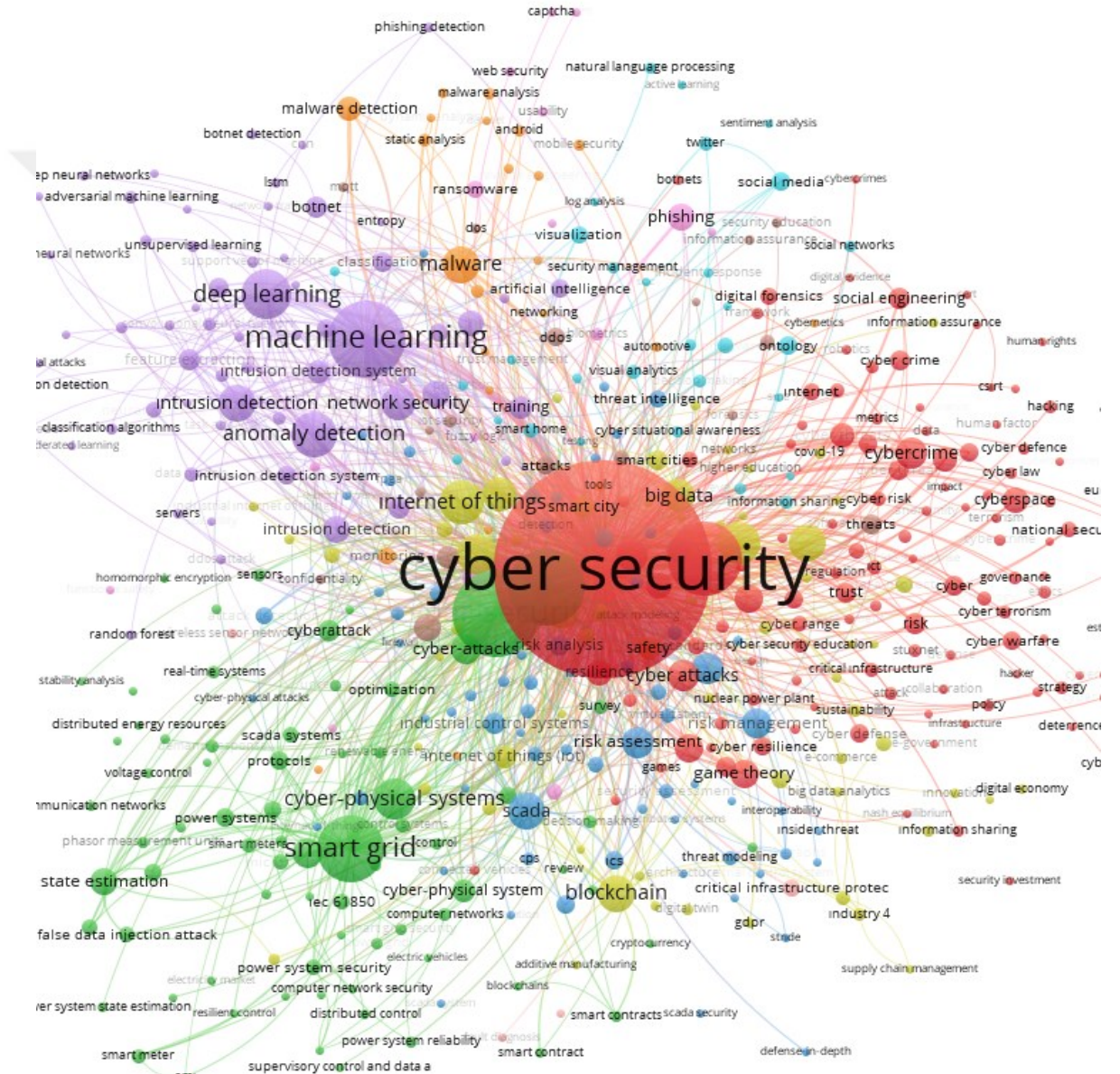
Analizden elde edilen bulgular ile bu dergilerin;

- ✓ Siber güvenlik konusunda yayın performanslarının yüksek olduğu,
- ✓ Siber güvenlik temelli araştırmalarda en prestijli ve etkili dergiler olarak öne çıktığı,
- ✓ Siber güvenlik alanında araştırmacılara yayınlarını yayınlama imkânı verdiği görülmektedir.

6.12. SİBER GÜVENLİK KONULU YAYINLARDA ANAHTAR KELİMELE- RİN DAĞILIMI

Şekil 5

Siber Güvenlik Konulu Araştırmalarda Kullanılan Anahtar Kelimeler



Siber Güvenlik konulu yayınlarda kullanılan anahtar kelimeler *şekil 5* 'te gösterilmiştir. Yapılan ağ görselleştirmesinde; öge etiketleri daire ile, öge ağırlığı etiket ve daire

boyutuyla, öge rengi ögenin ait olduğu sınıfla, öge bağlantıları ise çizgiler ile temsil edilmektedir. Varsayılan olarak, ögeler arasındaki en güçlü 482 bağlantıyı temsil eden en fazla 500 satır görüntülenmektedir. Analizde siber güvenlik için sıklık “10” olarak seçilmiştir. Ağ görselleştirilmesinde seçilen anahtar kelimenin en az 10 kere geçtiği yayınlarda, 482 tanesinin bunu sağladığı görülmüştür. En çok kullanılan ilk on anahtar kelime şu şekildedir: “*Siber Güvenlik*” (4280 Adet), “*Güvenlik*” (510 Adet), “*Makine Öğrenmesi*” (510 Adet), “*Akıllı Şebeke*” (396 Adet), “*Nesnelerin İnterneti (IoT)*” (352 Adet), “*Derin Öğrenme*” (231 Adet), “*Anomali Tespiti (Aykırı Değer Tespiti)*” (200 Adet), “*Gizlilik*” (182 Adet), “*Siber Fiziksel Sistemler*” (172 Adet), “*Kötü Amaçlı Yazılım*” (142 Adet). Bu anahtar kelimelerin, siber güvenlik alanyazınında en çok araştırma yapılan sırasıyla Bilgisayar Bilimi, Mühendislik, Telekomünikasyon, Otomasyon Kontrol Sistemleri alanları ile doğrudan ilişkili olduğuna; siber güvenliğin sofistike ve kapsayıcı yapısını yansıttığına ulaşılabilmektedir.

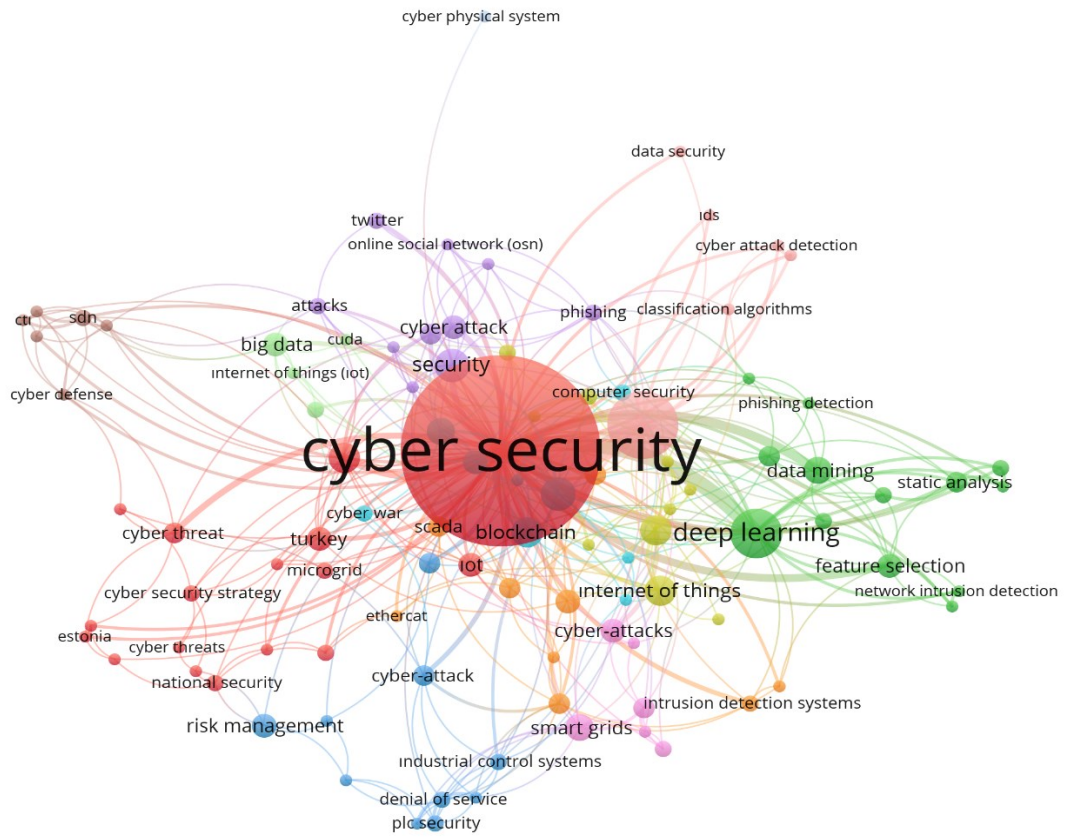
Analizden elde edilen bulgular ile:

- ✓ Siber güvenlik konusunda yapılan araştırmalarda öne çıkan kavramlar, alanlar ve alt başlıklar,
- ✓ Siber güvenlik alanındaki trendler ve gelişmeler,
- ✓ Siber güvenlik ile ilişkili ve araştırma potansiyeli yüksek konular görülmektedir.
- ✓ Sonuçlara göre araştırmacılar:
- ✓ Güncel konulara göre çalışmalarını şekillendirebilir.
- ✓ Spesifik konulara odaklanarak alandaki literatür boşluklarını değerlendirebilir.
- ✓ Gelecek araştırma yönelimlerini belirleyerek çalışmalarını stratejik bir şekilde buna göre planlayabilir.

6.13. SİBER GÜVENLİK KONULU YAYINLARDA TÜRKİYE’DE ANAHTAR KELİMELERİN DAĞILIMI

Şekil 6

Siber Güvenlik Konulu Araştırmalarda Türkiye’de Kullanılan Anahtar Kelimeler



Siber Güvenlik konulu yayınlarda kullanılan anahtar kelimeler *şekil 6*’da gösterilmiştir. Yapılan ağ görselleştirmesinde; öge etiketleri daire ile, öge ağırlığı etiket ve daire boyutuyla, öge rengi ögenin ait olduğu sınıfla, öge bağlantıları ise çizgiler ile temsil edilmektedir. Varsayılan olarak, ögeler arasındaki en güçlü 500 bağlantıyı temsil eden en fazla 500 satır görüntülenmektedir. Analizde siber güvenlik için sıklık “2” olarak seçilmiştir. Ağ görselleştirilmesinde seçilen anahtar kelimenin en az 2 kere geçtiği yayınlarda, 101 tanesinin bunu sağladığı görülmüştür. En çok kullanılan ilk on anahtar kelime şu

şekildedir: “Siber Güvenlik” (110 Adet), “Makine Öğrenmesi” (22 Adet), “Derin Öğrenme” (14 Adet), “Akıllı Şebeke” (13 Adet), “Güvenlik” (8 Adet), “Nesnelerin İnterneti (IoT)” (7 Adet), “Blok Zinciri” (7 Adet), “Veri Madenciliği” (6 Adet), “Siber Uzay” (6 Adet), “Öznitelik Seçimi” (5 Adet). Bu anahtar kelimelerin, siber güvenlik alanyazınında en çok araştırma yapılan sırasıyla Bilgisayar Bilimi, Mühendislik, Telekomünikasyon, Otomasyon Kontrol Sistemleri alanları ile doğrudan ilişkili olduğuna; siber güvenliğin sofistike ve kapsayıcı yapısını yansıttığına ulaşılabilmektedir. Sonuçlar dünya genelindeki araştırma ile kıyaslandığında;

- ❖ Siber Güvenlik, Makine Öğrenmesi, Derin Öğrenme, Akıllı Şebeke, Güvenlik ve Nesnelerin İnterneti anahtar kelimelerinin her iki liste içinde ortak olduğu,
- ❖ Blok zinciri, Veri Madenciliği, Siber Uzay, Öznitelik Seçimi Türkiye’de en çok kullanılan ilk on anahtar kelimeler listesinde yer alırken dünya genelinde ilk onda bulunmadığı,
- ❖ Akıllı Şebekenin her iki listede dördüncü sırada yer aldığı görülmektedir.

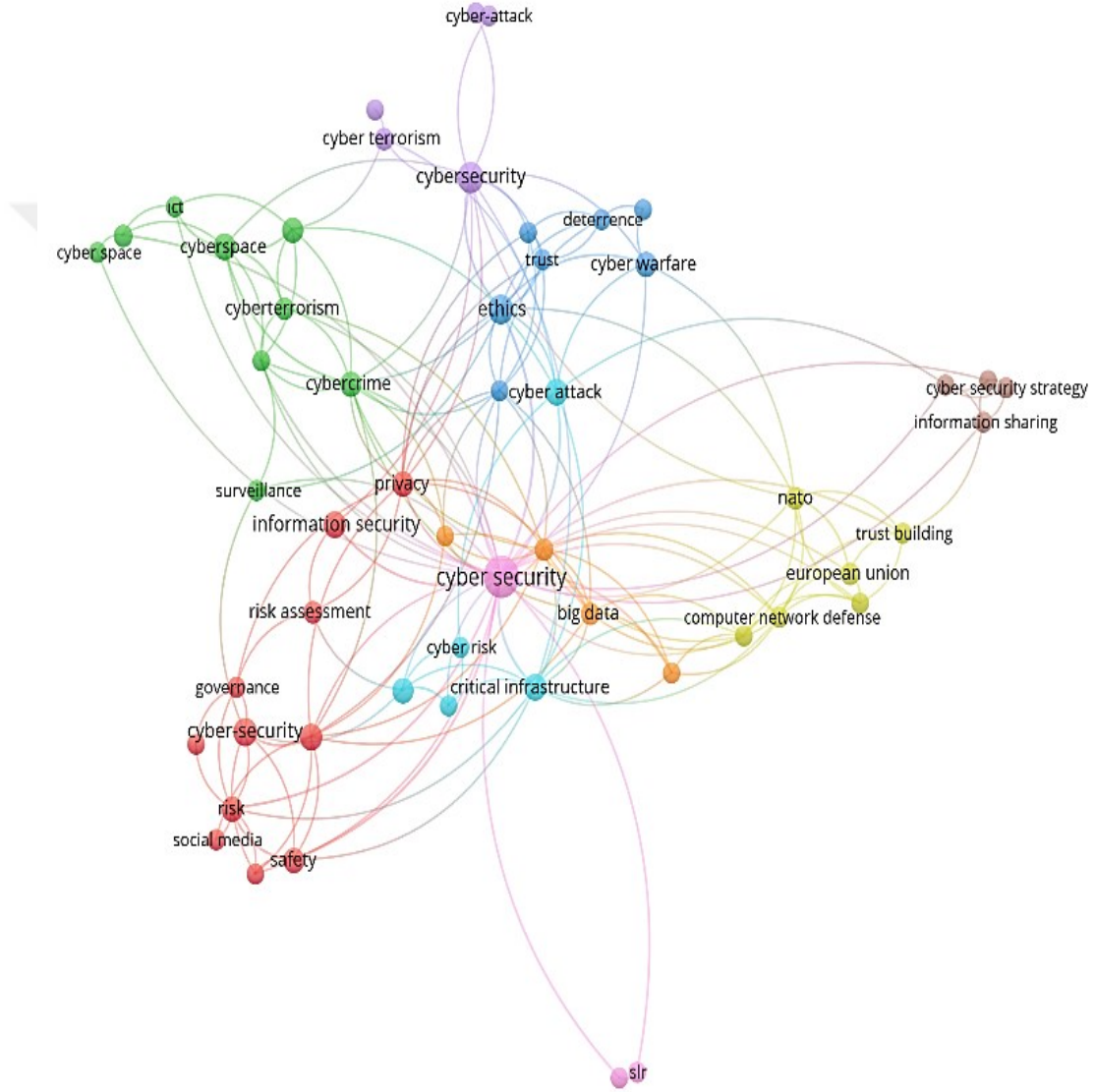
Analizden elde edilen bulgular ile:

- ✓ Siber güvenlik konusunda yapılan araştırmalarda öne çıkan kavramlar, alanlar ve alt başlıklar,
- ✓ Siber güvenlik alanındaki trendler ve gelişmeler,
- ✓ Siber güvenlik ile ilişkili ve araştırma potansiyeli yüksek konular görülmektedir.
- ✓ Sonuçlara göre araştırmacılar:
- ✓ Güncel konulara göre çalışmalarını şekillendirebilir.
- ✓ Spesifik konulara odaklanarak alandaki literatür boşluklarını değerlendirebilir.
- ✓ Gelecek araştırma yönelimlerini belirleyerek çalışmalarını stratejik bir şekilde buna göre planlayabilir.

6.14. SİBER GÜVENLİK KONULU YAYINLARDA SOSYAL BİLİMLER ALANINDA ANAHTAR KELİMELERİN DAĞILIMI

Şekil 7

Sosyal Bilimler Alanında Kullanılan Anahtar Kelimeler



Sosyal Bilimler Alanında Siber Güvenlik Konulu Araştırmalarda Kullanılan Anahtar Kelimeler *şekil 7*'de gösterilmiştir. WoS kaynağına göre Sosyal Bilimler Alanında Siber Güvenlik konulu yayın sayısı “118”dir. Analizde siber güvenlik için sıklık “2” olarak seçilmiştir. Anahtar kelimenin en az 2 kere geçtiği yayınlarda, 55 tanesinin bunu sağladığı görülmüştür. En çok kullanılan on anahtar kelime şu şekildedir: “*Etik*” (8

Adet), “Bilgi Güvenliđi” (6 Adet), “Siber Saldırı” (5 Adet), “Güvenlik” (5 Adet), “Siber Uzak” (5 Adet), “Kritik Altyapı” (5 Adet), “Risk Yönetimi” (4), “Siber Savaş” (4 Adet), “Terörizm” (4 Adet), “Emniyet” (4 Adet). Analizden elde edilen bulgular:

❖ Siber güvenlik ve sosyal bilimler arasındaki bağlantıyı gösteren seçkin kavramları,

❖ Siber güvenlik konusunda sosyal bilimler alanındaki eğilimleri ve trendleri göstermektedir.

Sonuçlara göre araştırmacılar:

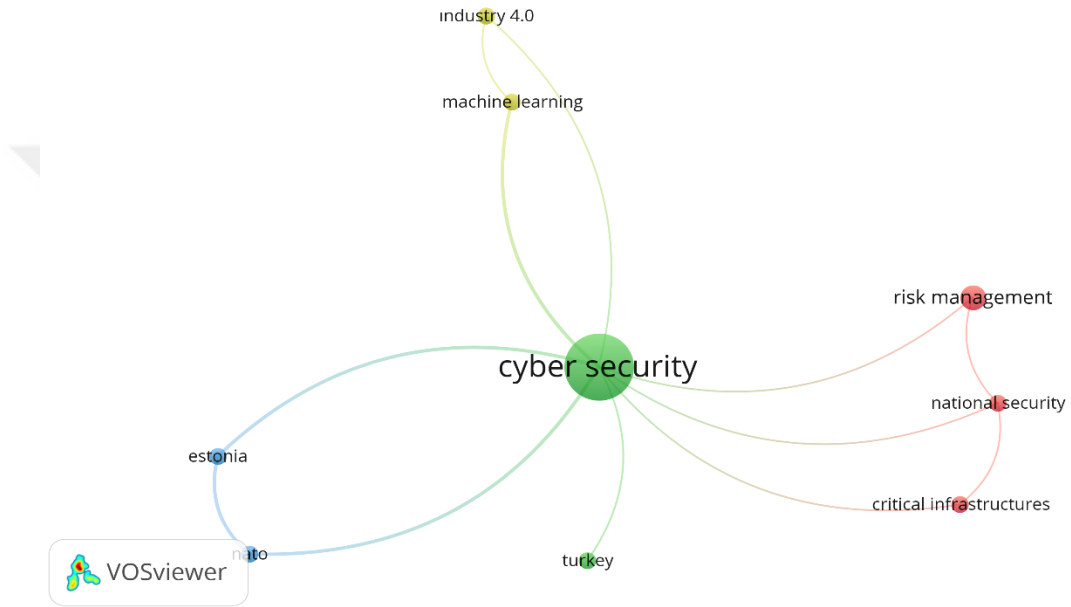
❖ Anahtar kelimeleri inceleyerek yayınlarını bu kapsamda genişletebilir veya yön verebilir.

❖ Siber güvenlik konusunda sosyal bilimler alanındaki eksikleri görebilir ve bu alanda çalışma yapmaya yönelebilir.

6.15. SİBER GÜVENLİK KONULU YAYINLARDA SOSYAL BİLİMLER ALANINDA TÜRKİYE’DEKİ ANAHTAR KELİMELERİN DAĞILIMI

Şekil 8

Sosyal Bilimler Alanında Türkiye’de Kullanılan Anahtar Kelimeler



Sosyal Bilimler Alanında Siber Güvenlik Konulu Araştırmalarda Kullanılan Anahtar Kelimeler *şekil 8*’de gösterilmiştir. WoS kaynağına göre Sosyal Bilimler Alanında Siber Güvenlik konulu yayın sayısı “23”dür. Analizde siber güvenlik için sıklık “2” olarak seçilmiştir. Anahtar kelimenin en az 2 kere geçtiği yayınlarda, 9 tanesinin bunu sağladığı görülmüştür. En çok kullanılan dokuz anahtar kelime şu şekildedir: “*Siber Güvenlik*” (8 Adet), “*Risk Yönetimi*” (3 Adet), “*Makine Öğrenimi*” (2 Adet), “*Kritik Altyapı*” (2 Adet), “*Endüstri 4.0*” (2 Adet), “*NATO*” (2 Adet), “*Estonya*” (2 Adet), “*Türkiye*” (2 Adet), “*Ulusal Güvenlik*” (2 Adet). Analizden elde edilen bulgular:

- ❖ Siber güvenlik ve sosyal bilimler arasındaki bağlantıyı gösteren seçkin kavramları,
- ❖ Siber güvenlik konusunda sosyal bilimler alanındaki eğilimleri ve trendleri göstermektedir.

Sonuçlara göre araştırmacılar:

- ❖ Anahtar kelimeleri inceleyerek çalışmalarını bu kapsamda genişletebilir veya yön verebilir.
- ❖ Siber güvenlik konusunda sosyal bilimler alanındaki eksikleri görebilir ve bu alanda çalışma yapmaya yönelebilir.

6.16. SİBER GÜVENLİK KAVRAMININ DEĞERLENDİRİLMESİNDE HAZIRBULUNUŞLUK ÖLÇEĞİ VE BİBLİYOMETRİK AĞ ANALİZİ YÖNTEMLERİNİN KULLANIMI: BİR SİSTEMATİK DERLEME

Bibliyometrik ağ analizi, belli bir konuda bilimsel yayınların ağ yapısını inceleyen bir yöntemdir. Bu yöntem ile araştırılan konu hakkında nicel veriler elde edilmektedir. Bibliyometrik ağ analizi sonucu elde edilen veriler ile yayın sayıları, öne çıkan kavramlar, alanlar, yazarlar, dergiler veya kurumlar gibi bilgileri sunulmaktadır. Bu bilgiler araştırılan konuya dair bilimsel literatüre uygun bir çerçeve oluştururken konunun daha geniş bir perspektifle değerlendirilmesini sağlar. Hazırbulunuşluk ölçeği ise belirli bir konuda hazır olma düzeyinin değerlendirilmesi için oluşturulan bir ölçme aracıdır.

Bibliyometrik ağ analizine dayalı hazır bulunuşluk ölçeğinin geliştirilmesi ile işletmeler siber alanda ne kadar hazırlıklı veya donanımlı olduğunu inceleyebilmekte veya ölçeği esas alarak siber güvenlik stratejilerini geliştirebilmektedir. Yapılan ağ analizinde ise siber güvenlik hakkındaki yayınların bilimsel ağ yapısı değerlendirilebilmektedir. Öne çıkan alanlar, terimler, kurumlar, dergiler, şahıslar görülebilmektedir. Ağ analizi konuya dair bir çerçeve sunmakla beraber konunun derinlemesine anlaşılmasını sağlamaktadır. Sonuç olarak, bibliyometrik ağ analizi sonuçlarıyla hazırbulunuşluk ölçeği arasında bir korelasyon veya ilişkinin olması konuya dair benzerlikleri veya ayrışmaları ortaya koyabilmektedir. Ortak örüntüler veya farklılıklar konunun daha iyi anlaşılmasını sağlamakla beraber konunun bilimsel gelişimi için önemli bağlantılar sunmaktadır.

“Bibliyometrik Ağ Analizi” ve “Hazırbulunuşluk Ölçeği” yöntemlerinin birlikte kullanılması ile daha etkin sonuçlar elde edebilmektedir. Örneğin, bir işletme siber güvenlik alanında yüksek bir hazırbulunuşluk ölçeği puanına sahip iken bibliyometrik ağ analizi sonuçlarına göre siber güvenlik araştırma ve geliştirme faaliyetleri zayıf

olabilmektedir. Bu durum, işletmenin siber güvenlik uygulamalarının etkililiğini sorgulamasına neden olarak işletmenin siber güvenlik faaliyetlerini bu doğrultuda yönlendirmelerini sağlar.

Yapılan bibliyometrik ağ analizi çalışmasında öne çıkan konu ve kavramlar belirlenerek hazırbulunuşluk ölçeği geliştirilmiştir. Öne çıkan konuların ve kavramların daha çok teknoloji ile alakalı olduğu görülmüş olup ölçek maddeleri bu doğrultuda seçilmiştir.



YEDİNCİ BÖLÜM

7. SOSYAL AĞ ANALİZİNE DAYALI HAZIRBULUNUŞLUK ÖLÇEĞİNİN GELİŞTİRİLMESİ

Anket işletmeyi betimlemeye yönelik sorulan dört seçmeli sorudan ve elli beş likert ölçekli maddeden meydana gelmektedir. Bu bölümde, araştırma problemlerine yönelik gerçekleştirilen istatistiksel analizlerin sonuçları sunulmaktadır.

7.1. ARAŞTIRMANIN AMACI

Yapılan araştırma ile;

- ❖ İşletmelere ve müşterilere siber güvenlik alanında rehber olacak bilgilerin sunulması,
- ❖ Sosyal ağ analizi ile siber güvenlik alanında araştırma yapacaklara ilişkisel boyutların sunulması,
- ❖ Sosyal ağ analizine dayalı hazır bulunuşluk ölçeğinin geliştirilmesi amaçlanmıştır.

7.2. ARAŞTIRMANIN ÖNEMİ

Yapılan araştırma ile;

- ❖ Yeni teknoloji kavramlarının açıklanması ve işletmeler ile yeni teknolojilerin entegre olma süreci,
- ❖ Yeni teknolojilerin işletmeler ve müşteriler üzerindeki siber riskleri,
- ❖ Sosyal ağ analizi ile siber güvenlik alanında araştırma yapacaklara dünya genelinde ve Türkiye kapsamında ilişkisel boyutların gösterilmesi ve verilerin karşılaştırılması,
- ❖ Siber tehditlere karşı işletmelerin korunması için sosyal ağ analizine dayalı hazır bulunuşluk ölçeğinin geliştirilmesi amaçlanarak literatüre bu açıdan katkıda bulunması beklenmektedir.

7.3. ARAŞTIRMANIN SINIRLILIKLARI

Sosyal Ağ analizinde, veriler WoS veri tabanı ile sınırlıdır. Hazırbulunuşluk ölçeği geliştirmesi aşamasında ise pandemi sürecinde meydana gelen kısıtlar nedeniyle e-Governance Academy Foundation tarafından ölçülen ulusal siber güvenlik indeksinde Temel Siber Güvenlik Göstergeleri’nde yer alan “Kişisel Veri Koruma” ve Olay ve Kriz Yönetimi Göstergeleri’nde yer alan “Siber Suçla Mücadele” indeks değerlerinin aynı olması sebebiyle seçilen Almanya ile Türkiye karşılaştırılamamış ve araştırma online olarak gerçekleştirilmiştir. Yaşanan diğer kısıtlar şunlardır:

- ❖ **Örneklem Sınırlılığı:** Gizlilik kısıtlamaları (güvenlik politikaları veya yasal düzenlemeler nedeniyle).
- ❖ **Veri Sınırlılığı:** Çok disiplinli bir alan olması ve araştırmanın belirli bir kitle ve sektörlerle gerçekleştirilmesi.
- ❖ **Zaman Sınırlılığı:** Güvenlik tehditleri ve savunma mekanizmalarının sürekli olarak evrim geçirmesi, bu alanda çalışan kişilerin yoğun olması.
- ❖ **Kaynak Sınırlılığı:** Sosyal bilimler alanında çalışmaların yetersiz olması.

7.4. METODOLOJİ

7.4.1. Veri Toplama Yöntem ve Araçları

Araştırmada nicel yöntem kullanılmıştır. Sosyal ağ analizi için hem veri toplama aracı hem de veri kaynağı olarak WoS veri tabanı kullanılmıştır. Hazırbulunuşluk ölçeğinin geliştirilmesinde ise işletmelerdeki siber güvenlik uzmanları tarafından elde edinilen bilgiler neticesinde R programlama dilinde geliştirilmiş algoritmalar ile istatistiksel testler yapılmıştır. Siber güvenlik uzmanları ve bir dil bilimci tarafından maddeler dikkatlice incelenmiştir. Hazırlanan anketten alınan geri bildirimlere göre faktör yapısı, geçerlilik ve güvenilirlik düzeyi belirlenmiştir.

7.4.2. Verilerin Analizi

Veri analizinin ilk aşamasında sosyal ağ analizi ve bilimsel haritalama yöntemlerinden yararlanılmıştır. Sosyal ağ analizi yöntemleri farklı analiz birimleri arasındaki ör-tük ilişkilerin ortaya konulması ve yorumlanabilir istatistiki değerlerin elde edilmesinde

kullanılmaktadır (Mallek, 2018). Çalışmada sosyal ağ analizi yöntemlerinden yazarlar, kurumlar ve kavramlar arası ilişkilerin ortaya konulması planlanmıştır. Bilimsel haritalama ile ortaya çıkarılan ağ ilişkileri yorumlanabilir görseller ile ortaya konulmuştur. Verilerin görselleştirilmesi için VOSviewer kullanılmıştır. Hazırbulunululuk ölçeğinin geliştirilmesi aşamasında açımlayıcı ve doğrulayıcı faktör analizi kullanılmıştır.

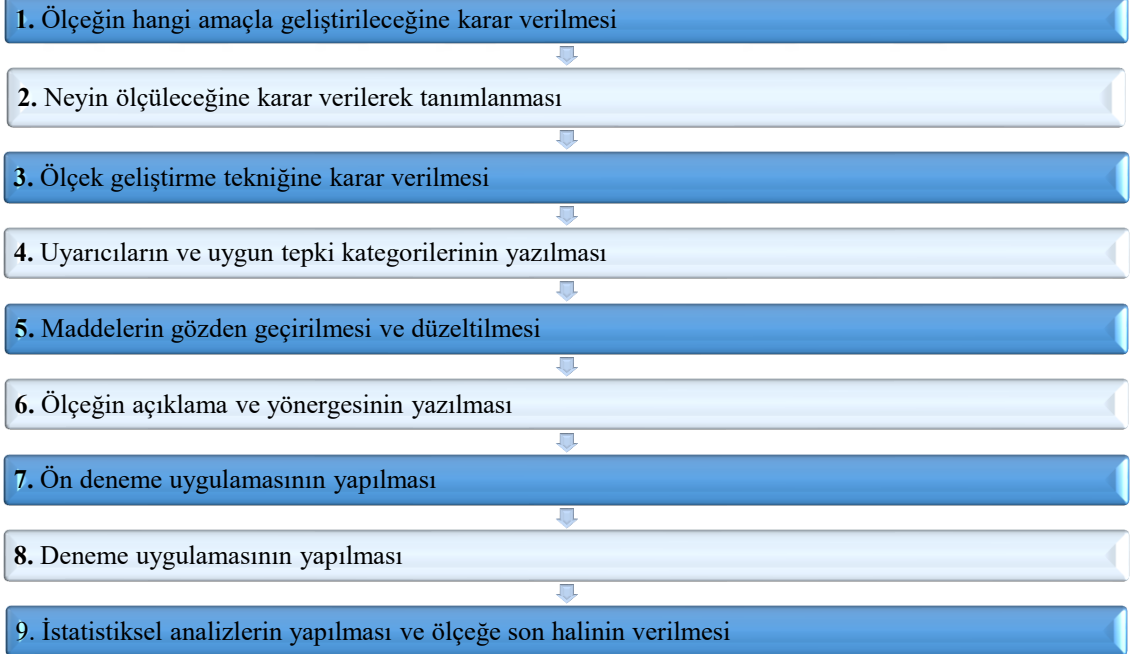
7.4.3. Araştırma Deseni

Nicel araştırma yöntemlerinden korelasyonel araştırma modeli temel alınmıştır. Korelasyonel araştırma modelinde, iki ya da daha çok değişken arasındaki ilişki herhangi bir şekilde bu değişkenlere müdahale edilmeden incelenir.

7.4.4. Ölçek Geliştirme Süreci

Tablo 4

Ölçek Geliştirme Süreci (Erkuş, 2012)



Ölçek işletmelerin siber saldırılara karşı siber alanda gerekli önlemleri alması amacıyla geliştirilmiştir. Oluşturulan 150 madde olası siber senaryolar düşünülerek hazırlanmıştır (CISA, 2020; RSI Security, 2022; Stuart Miller Solicitors, 2022...). 5'li likert ölçek oluşturularak işletmelerin siber güvenliğini sağlayan çalışanların cevapları psikometrik olarak

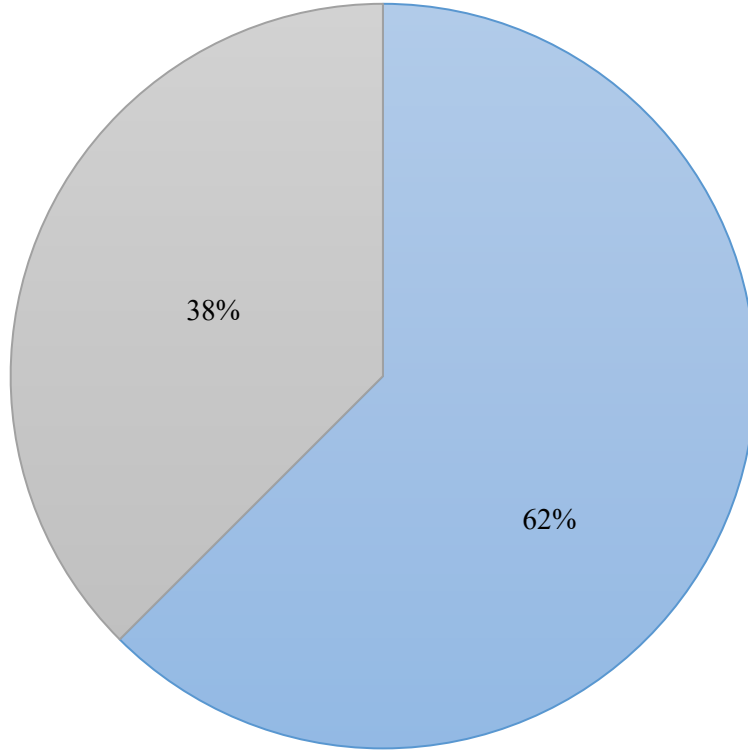
değerlendirilmek istenmiştir. Bir dil bilimci tarafından incelenerek maddelerde gerekli düzenlemeler yapılmıştır. Araştırma öncelikle 52 kişilik örneklem grubuna uygulanmıştır. Siber güvenlik uzmanlarının görüşleri çerçevesinde 95 madde çıkarılmıştır. Geriye kalan 55 maddenin ölçeğe uygun ve kapsayıcı olmasına dikkat edilmiştir.

7.5. HAZIRBULUNUŞLUK ÖLÇEĞİ BULGULARI

7.5.1. Katılımcı Bilgileri

Grafik 1

İşletme Ölçeğine göre Siber Güvenlik Uzmanlarının Dağılımı



■ KOBİ Çalışan Sayısı

■ Büyük Ölçekli İşletme Çalışan Sayısı

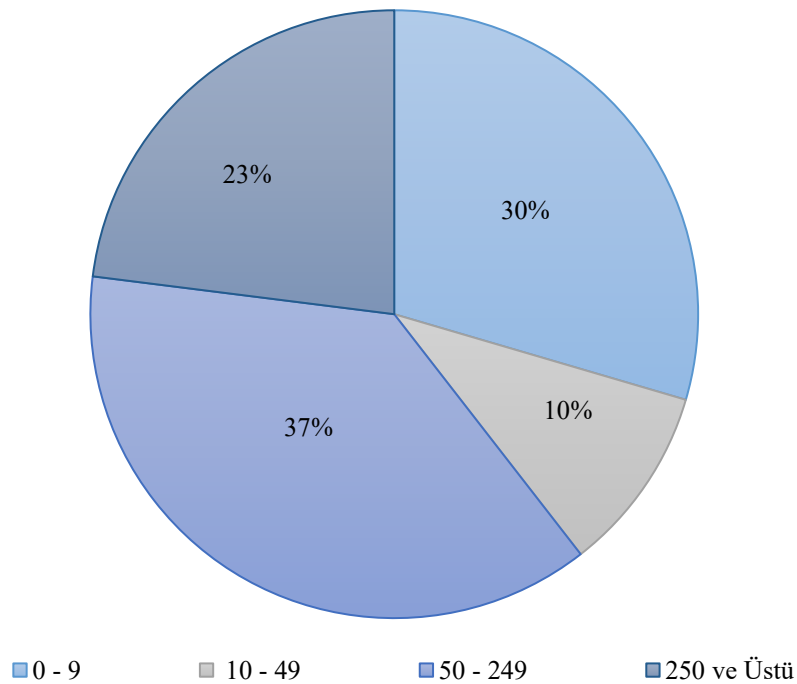
Araştırmaya işletmelerin siber alandaki güvenliğini sağlayan 354 çalışan katılmıştır. Çalışanlar farklı unvanlara sahiptir. Araştırmaya katılan siber güvenlik uzmanlarından

KOBİ’de çalışan sayısı 220 iken büyük ölçekli işletmede çalışan sayısı 132 olarak tespit edilmiştir. İncelemeler sonucu formdaki bütün sorulara aynı cevap veren beş çalışanın verileri yanıltıcı olabileceğinden çıkartılmıştır. Bu sebeple kalan 349 denek verisiyle analizler yapılmıştır.

7.5.2. İşletme Bilgileri

Grafik 2

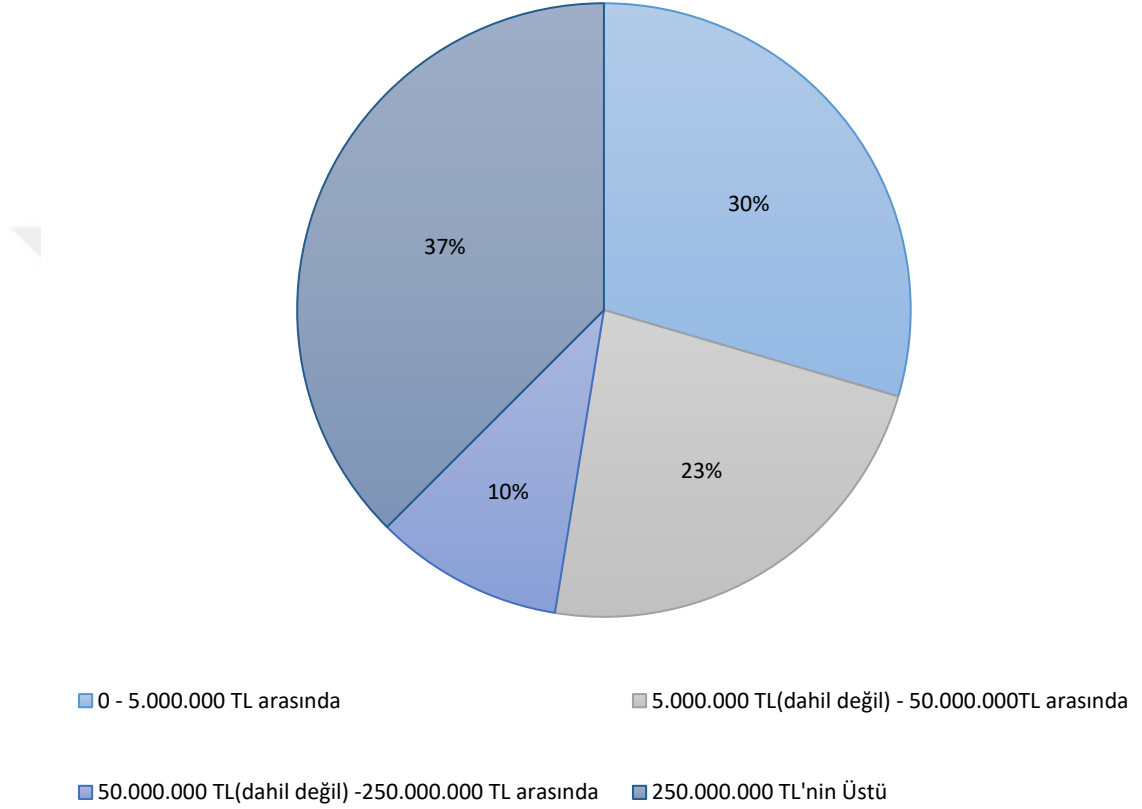
İşletmelerde Çalışan Personel Sayısının Pasta Grafiği ile Gösterilmesi



Anket sonuçları incelendiğinde, anketi yanıtlayan işletmelerden 81 tanesinin 250 ve üstü personel sayısına, 132 tanesinin 50 – 249 personel sayısına, 104 tanesinin 0 – 9 personel sayısına ve 35 tanesinin 10 – 49 personel sayısına sahip olduğu görülmektedir.

Grafik 3

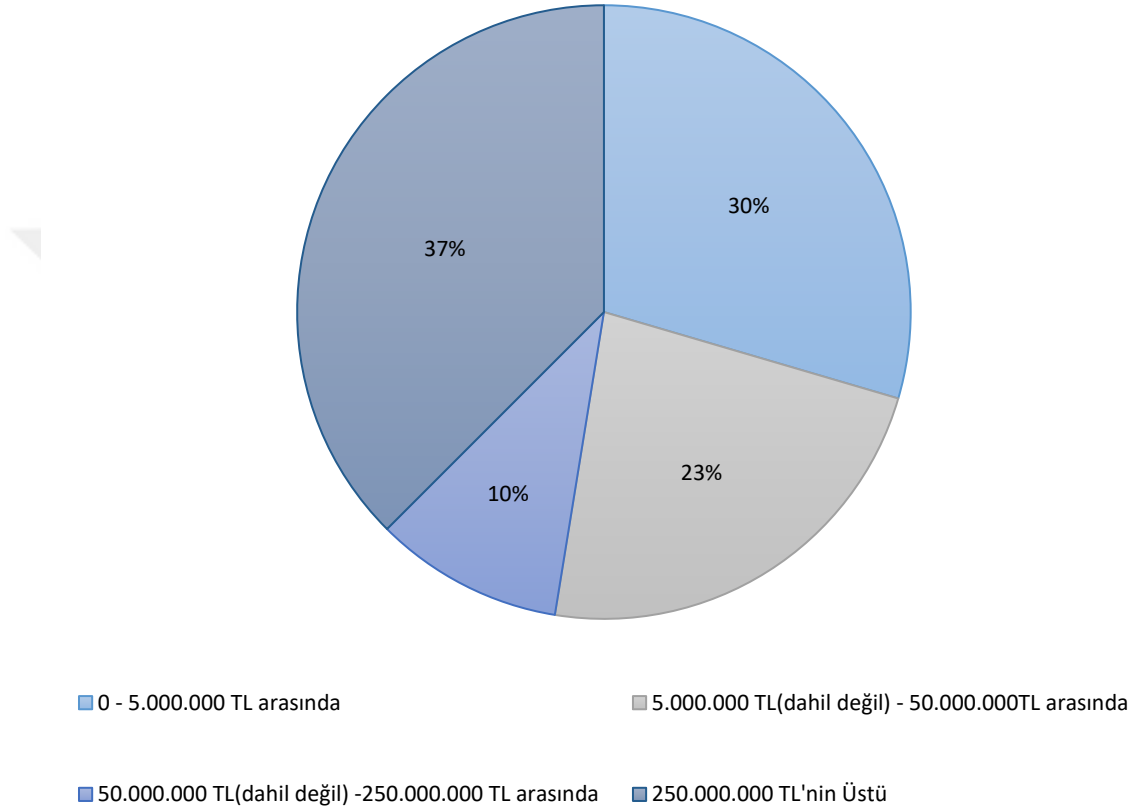
İşletmelerin Net Satış Hasılatının Daire Pasta ile Gösterilmesi



Anket sonuçları incelendiğinde, anketi yanıtlayan işletmelerden 81 tanesinin 0-5.000.000 TL arasında net satış hasılatına, 132 tanesinin 5.000.000 TL (dahil değil)-50.000.000 TL arasında net satış hasılatına, 104 tanesinin 50.000.000 TL (dahil değil)-250.000.000 TL arasında net satış hasılatına ve 35 tanesinin 250.000.000 TL'nin üstü net satış hasılatına sahip olduğu görülmektedir.

Grafik 4

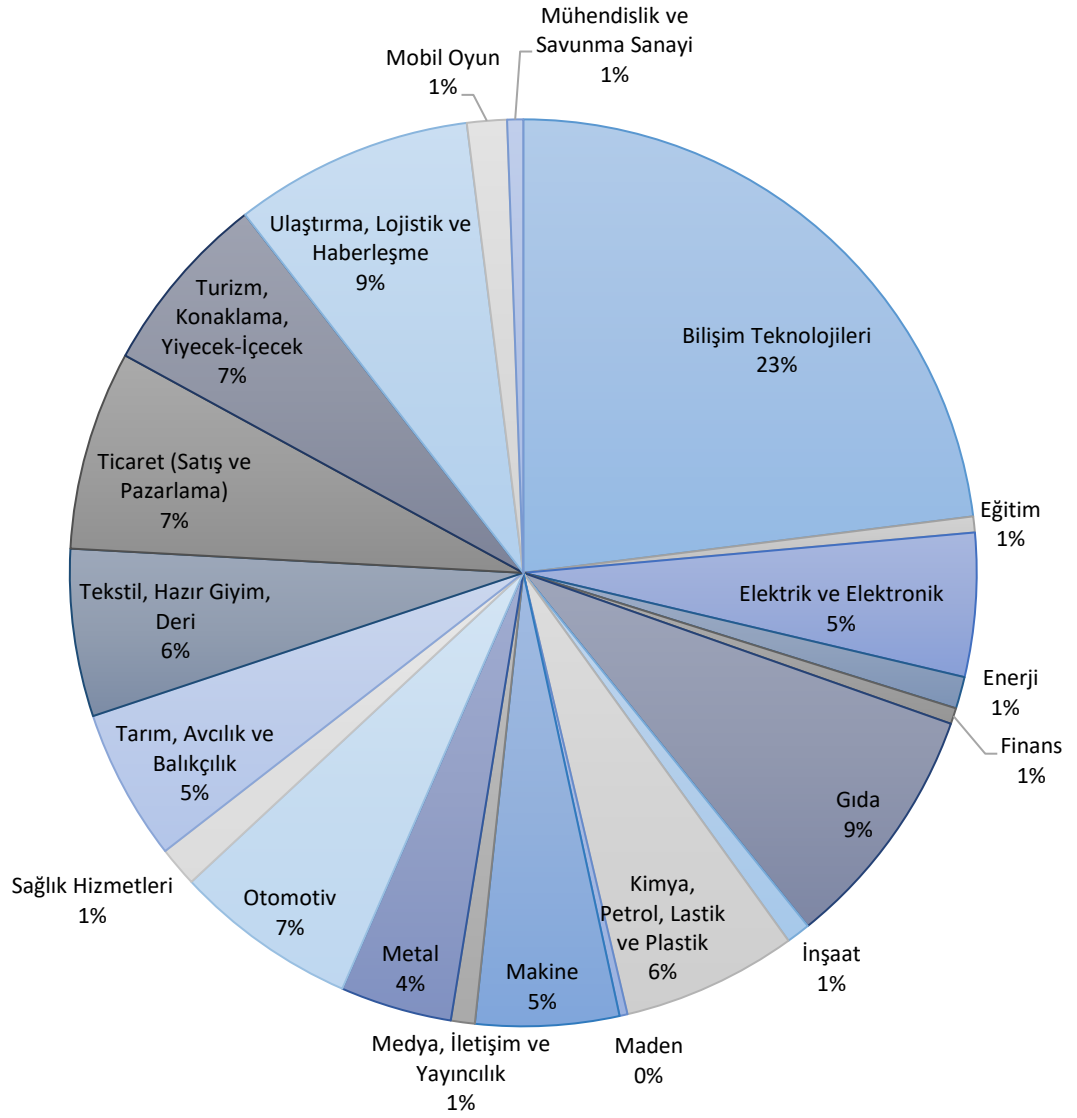
İşletmelerin Yıllık Mali Bilanço Toplamı



Anket sonuçları incelendiğinde, anketi yanıtlayan işletmelerden 81 tanesinin 0-5.000.000 TL arasında yıllık mali bilanço toplamına, 132 tanesinin 5.000.000 TL (dahil değil)- 50.000.000 TL arasında yıllık mali bilanço toplamına, 104 tanesinin 50.000.000 TL (dahil değil)- 250.000.000 TL arasında net satış hasılatına ve 35 tanesinin 250.000.000 TL'nin üstü yıllık mali bilanço toplamına sahip olduğu görülmektedir.

Grafik 5

İşletmelerin Sektörleri



Tablo 14*İşletmelerin Sektörleri*

Sektörler	İşletme Sayısı
Bilişim Teknolojileri	81
Eğitim	2
Elektrik ve Elektronik	18
Enerji	4
Finans	2
Gıda	31
İnşaat	3
Kimya, Petrol, Lastik ve Plastik	30
Maden	1
Makine	18
Medya, İletişim ve Yayıncılık	3
Metal	14
Otomotiv	23
Sağlık Hizmetleri	5
Tarım, Avcılık ve Balıkçılık	19
Tekstil, Hazır Giyim, Deri	21
Ticaret (Satış ve Pazarlama)	25
Turizm, Konaklama, Yiyecek-İçecek	23
Ulaştırma, Lojistik ve Haberleşme	30
Mobil Oyun	5
Mühendislik ve Savunma Sanayi	2

7.6. BETİMSSEL İSTATİSTİKLER ANALİZİ

“Tanımlayıcı istatistikler, bir örneklem veya popülasyondaki değişkenler arasındaki ilişkiyi tanımlayarak verileri organize bir şekilde özetlemek için kullanılır” (Yellapu, 2018). Yapılan betimsel analizde Shapiro Wilk testi sonuçlarının anlamlılık düzeyinin .05’ten büyük olması, maddelerin ortalama ve ortanca değerlerin birbirilerine yakın tespit edilmesi, çarpıklık ve basıklık değerlerinin -2 ile +2 arasında değer alması verilerin normal dağıldığını göstermektedir. Verilerde herhangi bir anormallik tespit edilmemiştir.

7.6.1. Örneklem Büyüklüğü

“KMO testi, verilerin faktör analizine uygunluğunu ölçmeyi amaçlayan bir ölçümdür. Diğer bir ifadeyle, örneklem büyüklüğünün yeterliliğini test etmektedir” (Shrestha, 2021). KMO testi sonucu ulaşılan değerin yüksekliğiyle veri setinin faktör analizine uygun olduğu görülmektedir. (Terzi, 2019). Kaiser-Meyer-Olkin testi için kabul gören alt sınır değer 0.50’dir. KMO testi değerinin 0.50’ye eşit veya altında bir değer olması veri kümesinin faktörlenemeyeceğini göstermektedir. Veri kümesinin faktörlenebilmesi için Kaiser-Meyer-Olkin Testinin 0.50’den büyük çıkması ve Barlett Testi’nin anlamlı olması beklenmektedir (Kaya, 2013). Bartlett testi ise korelasyon matrisinde değişkenlerin en azından bir kısmı arasında yüksek oranlı korelasyon olma olasılığını test etmektedir (Terzi, 2019).

KMO değerinin “0,80 ve üstünde olması mükemmel; 0,70 ve 0,80 arasında olması iyi; 0,60 ve 0,70 arasında olması orta; 0,50 ve 0,60 arasında olması kötü; 0,50’den aşağıda olması ise kabul edilemez” olarak değerlendirilmektedir (Tavşancıl, 2010). Araştırmadaki örneklem büyüklüğünün yeterliliğinin ölçülmesi amacıyla yapılan KMO testi sonucu, KMO değerinin 0.958 olduğu tespit edilmiştir. Sonucun 0.50 değerinin üstünde olması veri kümesinin faktörlenebildiğini, değişkenler arasında oldukça yüksek korelasyon bulunduğunu ve ölçekteki her değişkenin, diğer değişkenler tarafından yüksek bir oranda tahmin edilebileceğini ve faktör analizine uygunluğunun mükemmel seviyede olduğunu göstermektedir. Ayrıca küresel Bartlett testi sonucunda çıkan p değerinin $<0,05$ olması veri setinin faktör analizi için uygun olduğunu göstermektedir.

Tablo 15

İşletmelerin Dijitalleşme Sürecinde Siber Güvenlik: Sosyal Ağ Analizine Dayalı Hazır Bulunuşluk Ölçeği'nin Geliştirilmesi'nin Kaiser-Meyer-Olkin (KMO) ve Bartlett's Sphericity Testi Sonuçları

KMO ve Bartlett's Testi		
Kaiser-Meyer-Olkin Örnekleme Yeterliliğinin Ölçüsü		,958
Bartlett'in Küresellik Testi	Yaklaşık Ki-Kare	15460,502
	df	1485
	Sig.	,000

Tablo 16

İşletmelerin Dijitalleşme Sürecinde Siber Güvenlik: Sosyal Ağ Analizine Dayalı Hazır Bulunuşluk Ölçeği Maddelerinin Kaiser-Meyer-Olkin (KMO) Testi Sonuçları

KMO Örnekleme Yeterliliğinin Ölçüsü	MSA
CS7	0.968
CS8	0.969
CS12	0.969
CS13	0.957
CS14	0.955
CS16	0.971
CS17	0.979
CS20	0.969
CS21	0.977
CS22	0.973
CS23	0.975
CS25	0.916
CS27	0.962
CS28	0.966
CS29	0.939
CS31	0.948
CS32	0.979
CS34	0.957
CS36	0.964
CS37	0.975
CS38	0.946
CS39	0.976
CS51	0.956
CS57	0.943
CS61	0.981
CS67	0.957
CS74	0.971
CS76	0.967
CS77	0.976
CS79	0.974
CS85	0.965
CS86	0.887
CS87	0.884
CS91	0.952

CS92	0.966
CS94	0.949
CS95	0.958
CS98	0.962
CS102	0.957
CS103	0.942
CS105	0.970
CS110	0.884
CS118	0.920
CS122	0.971
CS124	0.885
CS130	0.962
CS134	0.892
CS135	0.968
CS136	0.787
CS138	0.923
CS140	0.957
CS141	0.962
CS145	0.964
CS147	0.952
CS150	0.913
Toplam	0.958

7.6.2. Korelasyon Matrisi

Veriler normal dağılım gösterdiği için Pearson korelasyon katsayısı tercih edilmiştir. Korelasyon matrisinde maddeler arası ilişki değerlerinin 0.20 ile 0.90 arasında bulunması beklenir. Düşük korelasyon katsayısına sahip maddeler diğer maddelerle birlikte hareket etmemekte ve ölçülmek istenen kavramı temsil etmemektedir. Öte yandan, yüksek korelasyon katsayısına sahip (.90 ve üzeri) maddeler ise aynı kavramı ölçen binişik veya aynı maddeler olarak algılanır. Her iki durumda da maddeler ölçeğin yapısına zarar verdiği için madde havuzundan çıkartılmalıdır. Analiz sonucunda değerlerin 0.20 ile 0.90 arasında bulunduğu görülmektedir.

7.7. BİRİNCİ AŞAMA AÇIMLAYICI FAKTÖR ANALİZİ

Faktör çıkarma yöntemlerinden verinin yapısına ve araştırmanın amacına en uygun olan principal axis (temel eksen) methodu, faktör döndürme yöntemi olarak ise büyük örnekleme kullanılan, eğik döndürme yöntemlerinden “promax” tercih edilmiştir. Uzman görüşmeleri ve literatür incelemesinin ardından sonuçlar beş faktör altında incelenmiştir.

Çok faktörlü bir yapıda, birden çok faktörde yüksek yük değeri veren madde, binişik bir madde olarak tanımlanır ve ölçekten çıkarılması düşünülebilmektedir (Şencan, 2014). İki yük değeri arasındaki fark en az 0.10 olmalıdır. Fark, 0.10’dan küçükse bu madde çıkarılır. Tablodaki Madde (8, 22, 23, 25, 28, 29, 31, 32, 34, 37, 51, 57, 61, 67, 74, 76, 91, 92, 95, 102, 103, 105, 118, 134, 140, 145) olmak üzere toplam yirmi altı çıkartılmıştır. Binişik maddelerdeki iki yük değeri arasındaki farkın 0.10’dan az olması, yük değerinin 0.40’tan az olması, uzman tavsiyeleri sebebiyle çıkarılmasına karar verilmiştir. Yapılan açımlayıcı faktör analizi sonucunda madde sayısı yirmi dokuz olarak güncellenmiştir. Analiz sonucu maddelerin KMO değerleri aşağıdaki gibidir:

Tablo 17

Birinci Aşama Açımlayıcı Faktör Analizi Sonrası Ölçek Maddelerinin KMO Testi Sonuçları

KMO Örnekleme Yeterliliğinin Ölçüsü	MSA
CS7	0.976
CS12	0.974
CS13	0.957
CS14	0.970
CS16	0.971
CS17	0.975
CS20	0.981
CS21	0.974
CS27	0.966
CS36	0.954
CS38	0.964
CS39	0.972
CS77	0.970
CS79	0.966
CS85	0.965
CS86	0.871
CS87	0.840
CS94	0.965

CS98	0.960
CS110	0.898
CS122	0.967
CS124	0.903
CS130	0.950
CS135	0.969
CS136	0.775
CS138	0.907
CS141	0.951
CS147	0.955
CS150	0.905
Toplam	0.957

KMO değerinin “0,80 ve üstünde olması mükemmel; 0,70 ve 0,80 arasında olması iyi; 0,60 ve 0,70 arasında olması orta; 0,50 ve 0,60 arasında olması kötü; 0,50’den aşağıda olması ise kabul edilemez” olarak değerlendirilmektedir. Madde 136 faktör analizi için iyi bir uygunluğa sahipken, diğer maddelerin faktör analizine uygunluğu mükemmeldir. Kaiser-Meyer-Olkin Testinin 0.50’den büyük çıkması ve Barlett Testi’nin anlamlı ve beklenmektedir (Kaya, 2013). KMO değerinin 0.958 olması faktör analizine uygunluğunun mükemmel olduğunu göstermektedir. Ayrıca küresel Bartlett testi sonucunda çıkan p değerinin $<0,05$ olması veri setinin faktör analizi için uygun olduğunu göstermektedir.

Tablo 18

Birinci Aşama Açıklayıcı Faktör Analizi Sonrası Bartlett'in Küresellik Testi Sonuçları

Bartlett'in Küresellik Testi		
χ^2	df	p
6877	406	<.001

Tablo 19

Birinci Aşama Açıklayıcı Faktör Analizi Sonrası Varyans Açıklama Oranları

Faktör	Kare Yüklerin Toplamı	Varyans Yüzdesi	Kümülatif%
1	9.011	31.07	31.1
2	4.652	16.04	47.1
3	1.800	6.21	53.3
4	1.339	4.62	57.9
5	0.641	2.21	60.2

Tablo 19

Birinci Aşama Açıklayıcı Faktör Analizi Sonrası Varyans Açıklama Oranları

Faktör	Kare Yüklerin Toplamı	Varyans Yüzdesi	Kümülatif%
--------	-----------------------	-----------------	------------

Varyans açıklama oranlarının birinci faktör için %31.07, ikinci faktör için %16.04, üçüncü faktör için %6.21, dördüncü faktör için %4.62, beşinci faktör için %2.21 olduğu görülmektedir. Beş faktör tarafından açıklanan toplam varyans ise %60,2'dir. Toplam varyansın %50-75'ini açıklayan bir analiz geçerli bir analiz olarak kabul edilir (Şencan, 2014). Bu durumda analizin geçerli olduğu görülmektedir.

7.7.1. Model-Veri Uyum İndeksleri

Tablo 20

Model Uyum Ölçüleri

	RMSEA 90% CI				Model Testi		
RMSEA	Lower	Upper	TLI	BIC	χ^2	df	p
0.0498	0.0432	0.0567	0.945	-1080	506	271	<.001

Model Uyum Ölçüleri tablosundaki “RMSEA değerinin 0.05’ten küçük veya eşit olması iyi bir uyumu, 0.05 ile 0.08 arasında olması yeterli bir uyumu, 0.08 ile 1 arasında olması ise vasat bir uyumu göstermektedir” (Ceyhan, 2020). Diğer yandan 0.95’i aşan TLI değerleri iyi bir model uyumunu gösterir (Hu & Bentler 1998). RMSEA değerinin 0.0498, TLI değerinin 0.945 olması yapılan araştırmada model-veri uyumunun sağlandığını ifade etmektedir.

7.8. YAPI GEÇERLİĞİ: DOĞRULAYICI FAKTÖR ANALİZİ

Tablo 21

Tam Uyum Testi

χ^2	df	p
753	368	<.001

Mevcut verilerin model ile uyumlarına bakıldığında öncelikle Ki-kare (Chisquare) testinin istatistiksel olarak anlamlı olmaması gerekmektedir. Ancak literatürde bu testin örneklem büyüklüğünden etkilendiği ve büyük örneklerde hassas davrandığı kanıtlanmıştır (Bentler ve Bonett, 1980). Alternatif olarak Ki-kare (Chi-square) değerinin serbestlik derecesine (degrees of freedom, df) bölünmesiyle elde edilen değerin 3'ten küçük olması beklenmelidir (Kline, 2011; Sümer, 2000). Mevcut veriler için Ki-kare/sd = $753/368 = 2,04$ olarak hesaplanmıştır.

Tablo 22

Uygunluk Ölçüleri

				RMSEA 90% CI			
CFI	TLI	SRMR	RMSEA	Lower	Upper	AIC	BIC
0.943	0.937	0.0425	0.0548	0.0492	0.0603	30856	31226

Ek olarak, CFI ve TLI değerlerinin .90 civarında olduğu ve RMSEA değerinin .08'e yakın olduğu belirlenmiştir. Çeşitli kaynaklardan alınan referans değerlere bakıldığında belirlenen uyum indekslerinin kabul edilebilir düzeylerde olduğu tespit edilmiştir (Hu ve Bentler, 1999; Tabachnick ve Fidell, 2015).

Tablo 23*Faktör Yükleri*

Faktör	Gösterge	Değerlendirme	SE	Z	p
Siber Güvenlik Perspektifinden Dijital Markanın Korunması	CS38	1.224	0.0698	17.55	< .001
	CS16	1.296	0.0691	18.77	< .001
	CS79	1.324	0.0692	19.14	< .001
	CS21	1.333	0.0719	18.55	< .001
	CS39	1.283	0.0686	18.70	< .001
	CS77	1.237	0.0713	17.36	< .001
	CS7	1.235	0.0696	17.74	< .001
	CS17	1.303	0.0705	18.47	< .001
	CS94	1.185	0.0686	17.27	< .001
	CS27	1.322	0.0717	18.45	< .001
	CS98	1.217	0.0725	16.79	< .001
	CS85	1.155	0.0665	17.35	< .001
	CS36	1.151	0.0675	17.04	< .001
	CS20	1.149	0.0686	16.76	< .001
	CS141	1.162	0.0679	17.12	< .001
Operasyonel Siber Güvenlik	CS14	1.144	0.0684	16.73	< .001

Tablo 23*Faktör Yükleri*

Faktör	Gösterge	Değerlendirme	SE	Z	p
İç Ağ Güvenliği	CS130	1.110	0.0677	16.38	< .001
	CS12	1.199	0.0698	17.19	< .001
	CS122	1.108	0.0684	16.20	< .001
	CS13	1.188	0.0661	17.97	< .001
	CS147	0.989	0.0724	13.67	< .001
	CS135	1.105	0.0702	15.74	< .001
	CS136	0.950	0.0857	11.09	< .001
	CS124	0.883	0.0735	12.02	< .001
	CS150	0.697	0.0737	9.46	< .001
	CS110	0.887	0.0775	11.45	< .001
Web Uygulamaları Güvenliği	CS86	1.253	0.0951	13.18	< .001
	CS87	1.130	0.0950	11.90	< .001
Son Kullanıcı Eğitimi	CS138	1.413	0.0535	26.42	< .001

Tablo 24*Faktör Kovaryansları*

		Estimate	SE	Z	p
Siber Güvenlik Perspektifinden Dijital Markanın Korunması	Siber Güvenlik Perspektifinden Dijital Markanın Korunması	1.000 ^a			
	Operasyonel Güvenlik	0.789	0.0239	33.07	< .001
	Ağ Güvenliği	0.505	0.0523	9.65	< .001
	Web Uygulamaları Güvenliği	0.525	0.0496	10.57	< .001
	Son Kullanıcı Eğitimi	0.421	0.0451	9.33	< .001
Operasyonel Siber Güvenlik	Operasyonel Siber Güvenlik	1.000 ^a			
	Ağ Güvenliği	0.499	0.0539	9.26	< .001
	Web Uygulamaları Güvenliği	0.536	0.0528	10.16	< .001
	Son Kullanıcı Eğitimi	0.477	0.0437	10.91	< .001
İç Ağ Güvenliği	İç Ağ Güvenliği	1.000 ^a			
	Web Uygulamaları Güvenliği	0.470	0.0634	7.42	< .001
	Son Kullanıcı Eğitimi	0.579	0.0465	12.46	< .001
Web Uygulamaları Güvenliği	Web Uygulamaları Güvenliği	1.000 ^a			
	Son Kullanıcı Eğitimi	0.266	0.0586	4.54	< .001
Son Kullanıcı Eğitimi	Son Kullanıcı Eğitimi	1.000 ^a			

Not. ^a Sabit Parametre**Tablo 25***Güvenirlilik Analizi*

Faktörler	Madde Sayısı	Cronbach's α	McDonald's ω
Marka ve Siber Güvenlik	14	0.961	0.961
Operasyonel Siber Güvenlik	8	0.915	0.916
İç Ağ Güvenliği	4	0.712	0.714
Web Uygulamaları Güvenliği	2	0.733	0.733
Son Kullanıcı Eğitimi	1		
Toplam Ölçek	29	0.958	0.959

Ölçek için Cronbach alfa katsayısı .958 ve McDonalds omega katsayısı .959 olarak hesaplanmıştır. Elde edilen değerler .70'in üstünde olduğu için kabul edilebilirdir sonucu çıkartılabilir.



SONUÇ

İnsan yapımı bir alan olmasına rağmen savunma faaliyetleri için doğal olarak oluşan kara, deniz, hava ve uzay alanları kadar siber alan da savunmada gerekmektedir. Siber savunmanın yüksek oranda gerektiği kurumlardan biri ise işletmelerdir. Bilgisayar korsanları çeşitli motivasyon kaynakları ile işletmelere siber saldırılar düzenlemektedir. Siber alanda başarılı bir şekilde kendini savunmayan bir işletmenin maddi ve manevi kayıplara uğraması kaçınılmazdır. Aynı zamanda gerçekleşen saldırılarından işletmelerin müşterileri, ortakları gibi dış çevreleri de zarar görebilmektedir. Bu sebeple siber güvenlik işletmeler için kritik bir önem arz etmektedir.

İşletmelerin iç veya dış çevrelerinde oluşan herhangi bir zafiyet bilgisayar korsanları tarafından kullanılabilir. Zafiyetin kullanılabileceği birçok siber saldırı yöntemi olduğu gibi bu zafiyetler çeşitli senaryolar aracılığıyla aktif bir tehlike yaratabilmektedir. Ayrıca siber saldırı yöntemleri arasına her geçen gün yenileri eklenerek işletmelerin siber tehlikelere maruz kalma olasılığı artış göstermektedir. İşletmelerin KOBİ olması bilgisayar korsanlarının o işletmeye siber saldırıda bulunmayacağı anlamına gelmemektedir. KOBİ'lerin genellikle siber güvenliğe bütçe ayırmaması ya da siber saldırılara karşı düşük önlemler alması siber saldırılarda bilgisayar korsanlarının “kolay ve karlı düşüncesiyle” KOBİ'leri hedef haline getirmesine sebep olabilmektedir.

İşletmelerin dijital ortamda faaliyet göstermesi ve teknolojiyle değişimler yaşaması avantajlara sahip olmakla birlikte siber dünyada tam korunma sağlanamazsa siber güvenlik bakımından büyük dezavantajlara da yol açabilmektedir. 5G, Tedarik zinciri, dijital ikizler, NFT, IoT, RFID, E-CRM, Geofencing, blok zincirler bu teknolojilerden sadece bazılarıdır. Bunların yanı sıra BYOD uygulama, Remote veya hibrid çalışma gibi işletmelerdeki yeniliklerde siber riskler taşımaktadır.

Yapılan çalışma ile etimolojik geçmişe bakılmış, kavramın önemi açıklanmış, yaşanan gizlilik ve güvenlik sorunlarına değinilmiş, yaşanan sorunlar işletmeler ve müşteriler açısından incelenmiş, siber güvenlikteki başarının ve siber güvenliğin dijitalleşme süreçlerindeki önemi hakkında bilgi verilmiştir.

Siber güvenlik alanında öne çıkan konu ve kavramları belirlemek amacıyla araştırma metotlarından sosyal ağ analizi kullanılmıştır. Bibliyometrik haritalama ise bir araştırma tekniğidir. Siber güvenlik alanında elde edilen veriler bu teknikle görselleştirilerek verilerin anlaşılması ve verilerden bilgi çıkarımının kolaylaştırılması amaçlanmıştır.

WoS veri tabanı temel alınarak yapılan sosyal ağ analizi sonuçlarına bakıldığında; Amerika Birleşik Devletleri'nin 2546 yayınlı siber güvenlik alanında en çok çalışma yapan ülke olduğu, Türkiye'nin bu listede 186 yayınlı 13. sırada yer aldığı, siber güvenlik konusundaki yayın sayılarının dünya ve Türkiye genelinde yıllara göre değerlendirildiğinde düzenli olmasa da artış gösterdiği, dünya genelinde en fazla yayının Choo, Kim-Kwang Raymond ve Ishii, Hideaki tarafından yayınlandığı, Türkiye'deki en fazla yayının Prof. Dr. Şeref Sağıroğlu tarafından yayınlandığı ancak Prof. Dr. Nazife Baykal ve Dr. Bilge Karabacak'ın en yüksek H-indeks değerine (n=4) sahip olduğu, dünya genelinde ve Türkiye'de bilgisayar bilimleri alanında en çok araştırmanın yapıldığı, en çok bu alanda yayın yapan kurumun dünya genelinde "Chinese Academy of Sciences", Türkiye bazında ise Gazi Üniversitesi olarak tespit edildiği, dünya genelinde olduğu gibi Türk araştırmacılarında bu alandaki yayınlarını en çok yayınlayan yayıncının "IEEE" olduğu, dünya bazında genel olarak bakıldığında bu alanda en çok kullanılan anahtar kelimelerin; "*Siber Güvenlik*" (4280 Adet), "*Güvenlik*" (510 Adet), "*Makine Öğrenmesi*" (510 Adet), "*Akıllı Şebeke*" (396 Adet), "*Nesnelerin İnterneti (IoT)*" (352 Adet), "*Derin Öğrenme*" (231 Adet), "*Anomali Tespiti (Aykırı Değer Tespiti)*" (200 Adet), "*Gizlilik*" (182 Adet), "*Siber Fiziksel Sistemler*" (172 Adet), "*Kötü Amaçlı Yazılım*" (142 Adet). Türkiye bazında "*Siber Güvenlik*" (110 Adet), "*Makine Öğrenmesi*" (22 Adet), "*Derin Öğrenme*" (14 Adet) olduğu, dünya genelinde sosyal bilimler alanında bakıldığında "*Etik*" (8 Adet), "*Bilgi Güvenliği*" (6 Adet), "*Siber Saldırı*" (5 Adet), Türkiye bazında ise "*Siber Güvenlik*" (110 Adet), "*Makine Öğrenmesi*" (22 Adet), "*Derin Öğrenme*" (14 Adet), "*Akıllı Şebeke*" (13 Adet), "*Güvenlik*" (8 Adet), "*Nesnelerin İnterneti (IoT)*" (7 Adet), "*Blok Zinciri*" (7 Adet), "*Veri Madenciliği*" (6 Adet), "*Siber Uzay*" (6 Adet), "*Öznitelik Seçimi*" (5 Adet) kelimelerinin öne çıktığı görülmektedir.

Sosyal ağ analizi ile siber güvenlik kavramına ait verilerin ilişkisel boyutu sunulmuştur. Ülkeler, yayın sayıları, yazarlar, araştırma alanları, kurumlar, yayıncılar ve anahtar kelimeler dünya genelinde ve Türkiye kapsamında incelenmiştir. Çıkarılan ağ ilişkileri

görselleştirilmiştir. Elde edilen verilerle çıkarımsal istatistiki bilgilere ulaşılmıştır. Bu veriler hazırbulunuşluk ölçeğinin hazırlanmasında esas alınmıştır.

“Marka ve Siber Güvenlik”, “Son Kullanıcı Eğitimi”, “Web Uygulamaları Güvenliği”, “İç Ağ Güvenliği”, “Operasyonel Siber Güvenlik” başlıkları birleştirilerek beş faktörlü “Sosyal Ağ Analizine Dayalı Hazırbulunuşluk Ölçeği” hazırlanmıştır. Ölçeğin kapsam, yapı ve ölçüte dayalı geçerliği ve güvenilirliği sağladığı tespit edilmiştir. Geliştirilen ölçek ile işletmelerin siber güvenlik önlemleri gözden geçirilerek işletmelerin bu alandaki faaliyetleri artırılabilir ve olası siber saldırılara karşı hazırbulunuşlukları belli bir oranda sağlanabilir.

Bibliyometrik ağ analizi sonuçlarıyla hazırbulunuşluk ölçeği arasında bir korelasyon veya ilişkinin olması konuya dair benzerlikleri veya ayrışmaları ortaya koyabilmektedir. Ortak örüntüler veya farklılıklar konunun daha iyi anlaşılmasını sağlamakla beraber konunun bilimsel gelişimi için önemli bağlantılar sunmaktadır. Hazırbulunuşluk ölçeği ile bibliyometrik ağ analizi sonuçları incelendiğinde;

- ❖ Hazırbulunuşluk ölçeğindeki maddelerin bibliyometrik ağ analizinde genel olarak bakıldığında en çok kullanılan anahtar kelimeler ile doğrudan ilişkili olduğu,
- ❖ Bibliyometrik ağ analizinde sosyal bilimler alanında en çok aranan kelimelerden “Etik”, “Siber Uzak”, “Siber Savaş”, “Terörizm” dışındaki kelimelerin hazırbulunuşluk ölçeğindeki maddeler ile doğrudan ilişki olduğu ancak bu kelimelerin ölçekteki maddeler ile farklılık gösterdiği tespit edilmiştir.

Alanyazına bakıldığında dijital pazarlama stratejilerinde siber riski anlamının çok önemli olduğu (Konyeha, 2020); KOBİ’ler için etkili siber güvenlik stratejilerinin geliştirilebildiği (Cook, 2017); sosyal medyada siber güvenlik problemlerinin yaşandığı (Özkaya, 2018); işletmelerin teknoloji sayesinde değişimler yaşadığı ve gelişen teknolojideki siber güvenlik gereksinimini benimsemeleri gerektiği (Fritzvold, 2017) vurgulanmıştır. Bu çalışma;

- ❖ Yeni teknoloji kavramlarının açıklanmasını ve işletmeler ile yeni teknolojilerin entegre olma sürecini,
- ❖ Yeni teknolojinin işletmeler ve müşteriler üzerindeki siber risklerini,
- ❖ Siber tehditlere karşı işletmelerin korunması için hazırbulunuşluk ölçeğinin geliştirilmesini,

❖ Yapılan sosyal ağ analizi ile bu alanda araştırma yapacaklara ilişkisel boyutların gösterilmesini ele almış olup literatüre bu konuda katkı sunması beklenmektedir.

Siber güvenliğin çok kapsamlı bir yapıya sahip olması bu alanda yapılacak çalışmaların önünü açmaktadır. Gelecek çalışmalarda daha büyük veri setleri kullanarak belirli kitleler üzerinde karşılaştırmalar yapmak mümkündür.



KAYNAKÇA

1. 3Cyber-Sec. (2020, July 2). *Cybersecurity in the crypto and NFT industry- what you should know? Blockchain technology is slowly and steadily evolving and penetrating into different fields of life. more and more people are interested in investing in crypto-assets and a larger.* Quora. <https://www.quora.com/profile/3Cyber-Sec/Cybersecurity-in-the-crypto-and-NFT-industry-what-you-should-know-Blockchain-technology-is-slowly-and-steadily-evolv>
2. Abgi Uk. (2017, August). *Ultimate Guide to RD tax relief for Digital and tech companies.* ABGI. https://www.abgi-uk.com/wp-content/uploads/2017/08/Ultimate-Guide-to-RD-tax-relief-for-digital-and-tech-companies_NOV19.pdf
3. Abrams, L. (2021, July 03). *Coop supermarket closes 500 stores after Kaseya Ransomware attack.* Bleeping Computer. <https://www.bleepingcomputer.com/news/security/coop-supermarket-closes-500-stores-after-kaseya-ransomware-attack/>
4. Acanerler, A. (2021, November 24). *Phishing: A growing threat to e-commerce.* SOCRadar. <https://socradar.io/phishing-a-growing-threat-to-e-commerce/>
5. Adalet Bakanlığı Genel Müfettiş Ofisi. (2022, July 07). *DOJ OIG Releases Report on DOJ's Cyber Supply Chain Risk Management Efforts.* U.S. Department of Justice Office of the Inspector General. <https://oig.justice.gov/sites/default/files/2022-07/07-07-2022.pdf>
6. Agazzi, A. E. (2020). *Business email compromise (bec) and cyberpsychology.* Research Gate. https://www.researchgate.net/publication/342783234_Business_Email_Compromise_BEC_and_Cyberpsychology
7. Akartuna, E. A., Nadini, M., DePow, C., & Annison, T. (2022, August 24). *NFTs and Financial Crime.* Elliptic. <https://www.elliptic.co/hubfs/NFT%20Report%202022.pdf>
8. Akhtar, T. (2022, April 06). *Axie Developer Raises \$150 Million as Gamers Flee After Hacking.* Bloomberg. <https://www.bloomberg.com/news/articles/2022-04-06/hack-victim-axie-raises-150-million-to-stem-gamer-defections?leadSource=uverify+wall>
9. Aladenika, B., Hinmikaiye, A., & Edet, E. (2022). Web 3.0 Digital Marketing in US Business Startups: A Literature Review. *Journal of Informatics Information*

System Software Engineering and Applications (INISTA), 12(1), 48-57. ISSN 2225-0506

10. Allen, R., Bloom, R., & Janes, S. (2019, December). *The challenges of mobile workforce security – and how to solve them*, Kingstone Technology. Kingston Technology. https://media.kingston.com/europe/landing/pdf/2019/12/Workforce-Security-eBook_WF498812_EN_1219.pdf
11. Alper, T. (2022, November 15). *North Korea Running 'Trojan-infested Fake Crypto Exchange,' Say Experts*. Cryptonews. <https://cryptonews.com/news/north-korean-running-trojan-infested-fake-crypto-exchange-say-experts.htm>
12. Altıntaş, K. M. (2021). *İstihbarata Karşı Koyma Prensipleri Bakımından Atık İstihbaratının Stratejik Önemi ve Karşılaştırmalı Analizi*. Uluslararası Kriz ve Siyaset Araştırmaları Dergisi, 5(2), 879-914. <https://dergipark.org.tr/tr/download/article-file/2040154>
13. Amazon. (2002). *What is cloud computing*. Amazon. <https://aws.amazon.com/tr/what-is-cloud-computing/>
14. Aslan, G. (2018, March 29). *Beyaz Şapka SEO ve Siyah Şapka SEO*. TEPE SEO Firması. <https://tepeseo.com/seo-rehberi/beyaz-sapka-seo-ve-siyah-sapka-seo/>
15. Atatanır, H. (2022). İş Yaşamında Siber Zorbalık. *Anasay*, 6 (22), 459-486. <http://dx.doi.org/10.33404/anasay.1160888>
16. Australian Cyber Security Magazine. (2022, June 29). *DeFi and Cybersecurity: What Future Holds*. <https://australiancybersecuritymagazine.com.au/defi-and-cybersecurity-what-future-holds/>
17. Awati, R. (2021, August 23). *What is the ILOVEYOU virus and how do you protect against it*. Techtarget. <https://www.techtartget.com/searchsecurity/definition/ILOVEYOU-virus>
18. AWS. (2022). *What is cloud computing*. Amazon. <https://aws.amazon.com/what-is-cloud-computing/>
19. Aykut, A. (2021, November 26). *5G NEDİR? 5G' nin Avantajları ve Dezavantajları*. Turhost. <https://blog.turhost.com/5g-nedir/>

20. Bandaru, N. (2021, October 7). *How 5G Is Changing The Way We Do Business*. *Forbes*. <https://www.forbes.com/sites/forbestechcouncil/2021/10/07/how-5g-is-changing-the-way-we-do-business/?sh=6761a786356a>
21. Barth, S., & De Jong, M. D. (2017). The privacy paradox—Investigating discrepancies between expressed privacy concerns and actual online behavior—A systematic literature review. *Telematics and informatics*, 34(7), 1038-1058. <https://doi.org/10.1016/j.tele.2017.04.013>
22. Bavaro, A. (2022, April 04). *Don't let seo poisoning kill your search rankings*. SMA Marketing. <https://www.smamarketing.net/blog/seo-poisoning>
23. BBC. (2013, November 18). *A case for reading the small print*. BBC. <https://www.bbc.com/news/blogs-magazine-monitor-24992518>
24. Bemedia. (2022). *Web 3.0 advisory blockchain games & nfts*. Bemedia. <https://www.bemedia.com.au/privacy-and-security-digital-marketing/>
25. Beveridge, C. (2022, November 25). *What is User-Generated Content? And Why is it Important*. Hootsuite. <https://blog.hootsuite.com/user-generated-content-ugc/>
26. BilişimPartisi. (2021, November 26). *Metaverse*. Bilişim Partisi. <http://www.bilisimpartisi.com/2021/11/26/metaverse/>
27. Blockco. (2022, November 04). *Mitigating cyber security risks with Blockchain technology*. Block.co. <https://block.co/mitigating-cyber-security-risks-with-blockchain-technology/>
28. Borden Ladner Gervais. (2021, May 10). *Managing cyber risks in M&A transactions*. BLG. <https://www.blg.com/en/insights/2021/05/managing-cyber-risks-in-m-and-a-transactions>
29. Britton, C. (2022). *How business leaders should respond to cyberbullying*. Rock Dove Solutions. <https://www.rockdovesolutions.com/blog/how-business-leaders-should-respond-to-cyberbullying>
30. Byers, J. (2022, September 11). *NFT Video Game Developer Recovers Large Sum After \$625M Hack*. Front Office Sports. <https://frontofficesports.com/nft-video-game-developer-recovers-large-sum-after-625m-hack/>

31. Canadian Centre for Cyber Security. (2020, September 16). *Security considerations for Research and Development (ITSAP.00.130)*. Canadian Centre for Cyber Security. <https://www.cyber.gc.ca/en/guidance/security-considerations-research-and-development-itsap00130>
32. Carreiro, A. (2020, February 10). *8 common hacking techniques that every business owner should know about*. Oceanpoint Insurance. <https://www.oceanpointins.com/ri-business-insurance/cyber-liability-insurance/8-common-hacking-techniques/>
33. CBR Staff Writer. (2019, July 8). *BA Facing £183.39M Fine for 2018 Data Breach*. Techmonitor. <https://techmonitor.ai/technology/cybersecurity/british-airways-fined-hack>
34. Chalmers, D., Fisch, C., Matthews, R., Quinn, W., & Recker, J. (2022). Beyond the bubble: Will NFTs and digital proof of ownership empower creative industry entrepreneurs. *Journal of Business Venturing Insights*, 17, e00309. <https://doi.org/10.1016/j.jbvi.2022.e00309>
35. Chang, W. ve Grady, N. (2019). NIST Big Data Interoperability Framework: Volume 1, Big Data Definitions. *Commerce Department, National Institute of Standards and Technology (NIST) 1500-1r2*. <https://doi.org/10.6028/NIST.SP.1500-1r2>
36. Cheng, F. C., & Wang, Y. S. (2018). The do not track mechanism for digital footprint privacy protection in marketing applications. *Journal of Business Economics and Management*, 19(2), 253-267. <https://doi.org/10.3846/jbem.2018.5200>
37. Chohan, R., & Paschen, J. (2023). NFT marketing: How marketers can use nonfungible tokens in their campaigns. *Business Horizons*. 66(1), 43-50. <https://doi.org/10.1016/j.bushor.2021.12.004>
38. Coinbase. (2022, September 2). *Avoiding crypto scams*. Coinbase. <https://help.coinbase.com/en/wallet/security/avoiding-crypto-scams>
39. Communities, C. (2008). *Future networks and the internet: Early challenges regarding the internet of things*. Technical report, CTEC.
40. Conti, R. & Schmidt, J. (2022, October 17). *What Is An NFT? How Do NFTs Work*. Forbes. <https://www.forbes.com/advisor/in/investing/cryptocurrency/what-is-an-nft-how-do-nfts-work/>

41. Cook, K. D. (2017). *Effective cyber security strategies for small businesses* (Doctoral dissertation, Walden University).
42. Copeland, T. (2022, May 06). *OpenSea discord server hacked to promote scam NFT pass*. Block.co <https://www.theblock.co/post/145432/opensea-discord-account-hacked-to-promote-scam-nft-pass>
43. Copeland, T. (2022, May 06). *OpenSea discord server hacked to promote scam NFT pass*. Block.co. <https://www.theblock.co/post/145432/opensea-discord-account-hacked-to-promote-scam-nft-pass>
44. Crespo, M. (2020). let's collaborate! cyber security. *Technology and Engineering Teacher*, 80(2), 20-21. <https://www.proquest.com/docview/2449678966?pq-origsite=gscholar&fromopenview=true>
45. Crest. (2022, April). *What is Cyber Threat Intelligence and how is it used*. CREST. <https://www.crest-approved.org/wp-content/uploads/2022/04/CREST-Cyber-Threat-Intelligence.pdf>
46. Crowdstrike. (2022, June 17). *WHAT IS A TROJAN HORSE*. Crowdstrike. <https://www.crowdstrike.com/cybersecurity-101/malware/trojans/>
47. CyberMag. (2022, May 17). *Fidye Yazılımları Türkiye'deki Şirketlerin %60'ını Vurdu, Yüzde 47'si Fidyeyi Ödedi*. CyberMag. <https://www.cybermagonline.com/fidye-yazilimlari-turkiyedeki-sirketlerin-60ini-vurdu-yuzde-47si-fidyeyi-odedi>
48. Cybersecurity and Infrastructure Security Agency. (2019, October). *E-Skimming- National Initiative for Cybersecurity Careers and Studies*. CISA. https://niccs.cisa.gov/sites/default/files/documents/pdf/ncsam_eskimming_508.pdf
49. Cybersecurity and Infrastructure Security Agency. (2021). *Potential Threat Vectors to 5g Infrastructure*. CISA. https://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-infrastructure_508_v2_0%20%281%29.pdf
50. Cyware Labs. (2019, September 7). *What is bait & switch attack and how is it different from clickjacking*. Cyware. <https://cyware.com/news/what-is-bait-switch-attack-and-how-is-it-different-from-clickjacking-d33b450a>

51. Çorumlu, O. (2022, February 02). *Metaverse'ün Siber Güvenlikteki Geleceği*. CyberArts. <https://cyberartspro.com/20220202-metaverseun-siber-guvenlikteki-gelecegi/>
52. Daniel, D., & Posey, B. (2021, August 05). *Industry 4.0*. Techtarget. <https://www.techtarget.com/searcherp/definition/Industry-40>
53. DarkReading. (2022, November 17). *CybeReady releases five easy tips to shop safely during Black Friday*. DARKreading <https://www.darkreading.com/vulnerabilities-threats/cybeready-releases-five-easy-tips-to-shop-safely-during-black-friday>
54. Das, R. (2022, July 21). *The Complete Guide To Using User-Generated Content on Social Media*. Statusbrew. <https://statusbrew.com/insights/user-generated-content/#what-is-user-generated-content>
55. Das, R., & Patel, M. (2017). Cyber Security for Social Networking Sites: Issues, Challenges and Solutions. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, 5(4,833-838). <https://doi.org/10.1016/j.jbvi.2022.e00309>
56. DataGuidance. (2022, March 25). *Turkey: KVKK announces Yonca Sağlık Hizmetleri Data breach*. <https://www.dataguidance.com/news/turkey-kvkk-announces-yonca-sa%C4%9Fl%C4%B1k-hizmetleri-data>
57. Department of the Army Criminal Investigation Division. (2021, September 7). *Search engine optimization (SEO) Poisoning*. <https://www.cid.army.mil/assets/docs/2can/SEOPoisoning.pdf>
58. DHA. (2022, June 14). *"Fidye Yazılımı Saldırganları, ödemelerin yüzde 98'ini bitcoin Olarak Talep Ediyor"*. <https://www.dha.com.tr/teknoloji/fidye-yazilimi-saldirganlari-odemelerin-yuzde-98ini-bitcoin-olarak-talep-ediyor-2085487>
59. Durbin, S. (2022, July 06). *Ignoring Cybersecurity Can Sour M&A Deals*. Forbes. <https://www.forbes.com/sites/forbesbusinesscouncil/2022/07/05/ignoring-cybersecurity-can-sour-ma-deals/?sh=69f803ff1c96>
60. Durbin, S. (2022, November 21). *How Cyber Threat Intelligence Provides Security and Value to Business*. Spiceworks. <https://www.spiceworks.com/it->

security/vulnerability-management/guest-article/how-cyber-threat-intelligence-provides-security-and-value-to-business/

61. Durgabhavani, K., & Krishnan, D. A. (2020). Impact of Security and Privacy Issues in Internet Marketing-A Study. *International Journal of Management*, 10(4), 36–43. <https://ssrn.com/abstract=3524195>
62. Durmuş, B. (2022, May 30). *En çok kullanılan 10 hacking yöntemleri 2022*. Webdeyazilim. <https://webdeyazilim.com/en-cok-kullanilan-10-hacking-yontemleri.html>
63. Edwards, S. (2021, December 09). *What is the most common goal of search engine optimization (SEO) poisoning*. Serpwizz. <https://serpwizz.com/blog/seo-poisoning/>
64. Emmitt, J. (2021, April 21). *Mergers and Acquisitions: Pros and Cons for MSPs*. Kaseya. <https://www.kaseya.com/blog/2021/04/21/mergers-and-acquisitions/>
65. Faizullahoy, R., & Gleason, M. (2022, April 23). *WEB3 security: Attack types and lessons learned*. Andreessen Horowitz. <https://a16z.com/2022/04/23/web3-security-crypto-hack-attack-lessons/>
66. Fariborzi, E., & Zahedifard, M. (2012). E-mail marketing: Advantages, disadvantages and improving techniques. *International Journal of e-Education, e-Business, e-Management and e-Learning*, 2(3), 232. <https://doi.org/10.7763/IJEEEE.2012.V2.116>
67. Federal Bureau of Investigation. (2020, April 17). *Business email compromise*. FBI. <https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise>
68. Fletcher, C. (2022, June 26). *Cybersecurity and the metaverse: Identifying the weak spots*. Venture Beat. <https://venturebeat.com/datadecisionmakers/cybersecurity-and-the-metaverse-identifying-the-weak-spots/>
69. Fletcher, E. (2022, August 18). *Social media a gold mine for scammers in 2021*. FTC. <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/01/social-media-gold-mine-scammers-2021>
70. Frankenfield, J. (2022, October 22). *Affiliate Marketer: Definition, Examples, and How to Get Started*. Investopedia. <https://www.investopedia.com/terms/a/affiliate-marketing.asp>

71. Frankenfield, J. (2022, October 24). *Cryptocurrency Airdrop: What Is It and How Does It Work*. Investopedia. <https://www.investopedia.com/terms/a/airdrop-cryptocurrency.asp>
72. Fruhlinger, J. (2017). *Petya ransomware and NotPetya malware: What you need to know now*. CSO. <https://www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html>
73. Gallegos, A. (2022, April 05). *What is User-Generated Content: The Complete Guide to UGC*. TINT Blog. <https://www.tintup.com/blog/user-generated-content-definition/>
74. GameWheel. (2020, April 07). *Top 3 cases how brands use gamification in their business*. <https://www.gamewheel.com/gamification-in-marketing/>
75. García-Tobar, A. (2022, January 21). *Why Marketing and IT Teams Should Share Cybersecurity Responsibilities*. Martech Zone. https://martech.zone/email-authentication-cybersecurity/#google_vignette
76. Gillis, A., & Bernstein, C. (2022, January 25). *What is a decentralized application (DAPP)*. Techtarget. <https://www.techtarget.com/iotagenda/definition/blockchain-dApp>
77. Globaldots. (2021, December 15). *Affiliate Fraud – The Dark Side of Affiliate Marketing*. <https://www.globaldots.com/resources/blog/affiliate-fraud-the-dark-side-of-affiliate-marketing/>
78. Gmcdouga. (2021, October 25). *As battle against Cybercrime continues during Cybersecurity Awareness Month, Check Point Research reports 40% increase in cyberattacks*. Check Point Blog. <https://blog.checkpoint.com/2021/10/06/as-battle-against-cybercrime-continues-during-cybersecurity-awareness-month-check-point-research-reports-40-increase-in-cyberattacks/>
79. Gmcdouga. (2022, January 10). *Check Point Research: Cyber Attacks Increased 50% Year over Year*. Check Point Blog. <https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/>
80. Goodman, M. (2016). *Geleceğin Suçları: Dijital Dünyanın Karanlık Yüzü (1. baskı)*. İstanbul: Timaş Yayınları.

81. Gordiyevskaya, A. (2020). *Ethics in digital marketing*. [Bachelor's thesis, LAB University of Applied Sciences]. Thesus. https://www.theseus.fi/bitstream/handle/10024/340999/Gordiyevskaya_Anastasia.pdf?sequence=2&isAllowed=y
82. Greig, J. (2021, July 2). *Kaseya urges customers to immediately shut down VSA servers after ransomware attack*. Zdnet. <https://www.zdnet.com/article/kaseya-urges-customers-to-immediately-shut-down-vsa-servers-after-ransomware-attack/>
83. Guzman, J. (2022, November 18). *Ultimate Guide For New Technologies in NFT Marketing*. Speed SEO. <https://speed.cy/technology/ultimate-guide-to-ntf-marketing>
84. Güner, M. (2022, May 31). *Siber Güvenlik ve Metaverse*. SİBER GÜVENLİK WEB TR. https://www.siberguvenlik.web.tr/index.php/2022/05/31/siber_guvenlik_ve_metaverse/
85. Hamid, B., Jhanjhi, N. Z., Humayun, M., Khan, A., & Alsayat, A. (2019, December). Cyber security issues and challenges for smart cities: A survey. *IEEE*, 1-7. <https://ieeexplore.ieee.org/document/9024768>
86. Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things*, 11, 100204. <https://hdl.handle.net/11250/2729453>
87. Hayes, M. (2022, January 20). *What Is Affiliate Marketing? A 2022 Guide to Getting Started*. Shopify. <https://www.shopify.com/blog/affiliate-marketing>
88. Health Sector Cybersecurity Coordination Center. (2022). *Vishing attacks on the rise*. (n.d.). <https://www.hhs.gov/sites/default/files/vishing-attacks-on-the-hph-sector-analyst-note.pdf>
89. Hearn, M., & Rix, S. (2019). *Cybersecurity considerations for digital twin implementations*. IIC J. Innov, 107-113. <https://www.iiconsortium.org/news-pdf/joi-articles/2019-November-JoI-Cybersecurity-Considerations-for-Digital-Twin-Implementations.pdf>
90. Hedera. (2022, September 12). *What is an NFT smart contract*. Hedera. <https://hedera.com/learning/smart-contracts/nft-smart-contract>
91. Hürriyet Gazetecilik ve Matbaacılık A.Ş. (2021). *Türkiye, en çok Fidyeye Yazılımı Saldırısı Alan ülkeler Arasında ilk 5'te*. <https://www.hurriyet.com.tr/teknoloji/turkiye-en-cok-fidyeye-yazilimi-saldirisi-alan-ulkeler-arasinda-ilk-5te-41837757>

92. IBM. (2019, February 27). *What is a digital twin*. <https://www.ibm.com/topics/what-is-a-digital-twin>
93. Ilascu, I. (2021, July 05). *REvil ransomware asks \$70 million to decrypt all Kaseya attack victims*. Bleeping Computer. <https://www.bleepingcomputer.com/news/security/revil-ransomware-asks-70-million-to-decrypt-all-kaseya-attack-victims/>
94. Internet Crime Complaint Center. (2022, May 4). *Internet crime complaint center (IC3): Business email compromise: The \$43 billion scam*. IC3. <https://www.ic3.gov/Media/Y2022/PSA220504>
95. IProov. (2020, September 4). *The Threat of Deepfakes*. <https://www.iproov.com/wp-content/uploads/2021/05/iProov-Deepfakes-Report.pdf>
96. Jena, B. (2022, October 13). *Solarwinds Attack & Details You Need To Know about it*. Simplilearn. <https://www.simplilearn.com/tutorials/cryptography-tutorial/all-about-solarwinds-attack>
97. Jia, X., Feng, Q., Fan, T., & Lei, Q. (2012, April). *RFID technology and its applications in Internet of Things (IoT)*. IEEE, 1282-1285. <https://ieeexplore.ieee.org/document/6201508>
98. Jirik, P. (2022, August 08). *3 Examples of Typical Smishing and Vishing Attacks in 2022*. Phonexia. <https://www.phonexia.com/blog/3-examples-of-typical-smishing-and-vishing-attacks-in-2022/>
99. Johansen, A. G. (2020, July 24). *What is a trojan? is it a virus or is it malware*. Norton. <https://us.norton.com/blog/malware/what-is-a-trojan#>
100. Jovanovic, B. (2022, November 18). *Zeus Trojan: The World's Most Widespread Malware*. Dataprot. <https://dataprot.net/articles/zeus-trojan/>
101. Karr, D. (2022, August 24). *E-posta Kimlik Doğrulamanızın DKIM, DMARC, spf ve Bimi için Doğru Olarak Ayarlandığını Nasıl Doğrularsınız*. Martech. <https://tr.martech.zone/how-to-validate-email-authentication-dkim-dmarc-spf/>
102. Karr, D. (2022, August 24). *E-posta Kimlik Doğrulamanızın DKIM, DMARC, spf ve Bimi için Doğru Olarak Ayarlandığını Nasıl Doğrularsınız*. Martech. <https://tr.martech.zone/how-to-validate-email-authentication-dkim-dmarc-spf/>
103. Kaspersky. (2021, October 05). *What is a trojan horse and what damage can it do*. <https://www.kaspersky.com/resource-center/threats/trojans>

104. Kaspersky. (2020, September 23). *5G Teknolojisi Tehlikeli Mi? - 5G Ağının Avantajları ve Dezavantajları*. <https://www.kaspersky.com.tr/resource-center/threats/5g-pros-and-cons>
105. Khanjani, Z., Watson, G., & Janeja, V. P. (2021). How deep are the fakes? focusing on audio deepfake: A survey. *NeuroReport* 15(9), 1519-1522. <https://doi.org/10.48550/arXiv.2111.14203>
106. Khoo, B. (2011, October). *RFID as an Enabler of the Internet of Things: Issues of Security and Privacy*. *IEEE*, 709-712. <https://doi.org/10.1109/IThings/CPSCoM.2011.83>
107. Kisielius, J. (2022, October 23). *Breaking down the Solarwinds Supply Chain Attack: SpyCloud blog*. Spycloud. <https://spycloud.com/solarwinds-attack-breakdown/#:~:text=2.-,Distribution,major%20enterprises%20and%20government%20agencies>
108. Konyeha, S. (2020). Exploring Cybersecurity Threats in Digital Marketing. *Journal of Science and Technology*, 2(3), 12-20. <https://doi.org/10.37933/nipes/2.3.2020.2>
109. Kron. (2021, July 11). *5G döneminde siber tehditlere Karşı Hazırlıklı Olmak*. <https://kron.com.tr/5g-doneminde-siber-tehditlere-karsi-hazirlikli-olmak>
110. KVKK- “Yemek Sepeti Elektronik İletişim Perakende Gıda Lojistik AŞ veri ihlal bildirimi hakkında” Kişisel Verileri Koruma Kurulunun 23/12/2021 tarih ve 2021/1324 sayılı Karar Özeti. (2021). <https://kvkk.gov.tr/Icerik/7168/2021-1324>
111. KVKK- Bir oyun şirketinin veri ihlal bildirimi hakkında” Kişisel Verileri Koruma Kurulunun 16.04.2020 tarih ve 2020/286 sayılı Karar Özeti. (2020). <https://kvkk.gov.tr/Icerik/7168/2021-1324>
112. KVKK. (2020). *Kişisel Verileri Koruma Kurumu: KVKK: "Bir Oyun şirketinin veri ihlal Bildirimi Hakkında" Kişisel Verileri Koruma Kurulunun 16.04.2020 Tarih ve 2020/286 Sayılı Karar özeti*. <https://www.kvkk.gov.tr/Icerik/6763/2020-286>
113. KVKK. (2021). *Kişisel Verileri Koruma Kurumu: KVKK: "Yemek Sepeti elektronik iletişim Perakende Gıda Lojistik AŞ Veri ihlal Bildirimi Hakkında" Kişisel Verileri Koruma Kurulunun 23/12/2021 Tarih ve 2021/1324 Sayılı Karar özeti*. <https://kvkk.gov.tr/Icerik/7168/2021-1324>

114. Lallie, H.S., Shepherd, L.A., Nurse, J.R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X.J. (2021). Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic. *Elsevier*, 105: 102248. <https://doi.org/10.1016/j.cose.2021.102248>
115. Lawler, R. (2022, May 06). *OpenSea's official discord compromised in a phishing attack that stole at least \$18k worth of nfts*. Theverge. <https://www.theverge.com/2022/5/6/23059715/nft-discord-phishing-opensea-youtube>
116. Lemos, R. (2022, October 08). *Email defenses under siege: Phishing attacks dramatically improve*. Darkreading. <https://www.darkreading.com/remote-workforce/email-defenses-under-siege-phishing-attacks-dramatically-improve>
117. Link, J. (2022, February 03). *10 email marketing statistics you need to know*. Constantcontact. <https://www.constantcontact.com/blog/email-marketing-statistics/>
118. Linkov, I., & Kott, A. (2018). *Fundamental concepts of cyber resilience: Introduction and overview*. Cyber resilience of systems and networks, 1-25.
119. Loveless, J. (2022, May 31). *The Most Common Types of Affiliate Fraud: Avoiding Five Finger Discounts on Retailers' Ad Budgets*. <https://martechseries.com/mts-insights/guest-authors/the-most-common-types-of-affiliate-fraud-avoiding-five-finger-discounts-on-retailers-ad-budgets/%20fraud%20is%20a%20type,20%2D65%25%20in%20sales>.
120. Mallek, S. (2018, July 3). *Social Network Analysis: Link prediction under the belief function framework*. <https://www.theses.fr/2018ARTO0204>
121. Mandalam, S. (2021, May 11). *Real-world examples of emerging DNS attacks and how we must adapt*. Paloalto Networks. <https://www.paloalto-networks.com/blog/2021/05/netsec-dns-attacks/>
122. Martins, A. (2022, June 29). *What Is Cyber Threat Intelligence, and Why Do You Need It*. Business News Daily. <https://www.businessnewsdaily.com/11141-cyber-threat-intelligence.html>
123. McCart, C. (2022, March 29). *15 Malvertising Statistics*. Comparitech <https://www.comparitech.com/blog/information-security/malvertising-statistics/>

124. Mehdar, Z. (2022, November 21). *Cybersecurity and cloud computing: Risks and benefits*. Rewind. <https://rewind.com/blog/cybersecurity-and-cloud-computing-risks-and-benefits/>
125. Microsoft. (2011). *Microsoft Güvenlik Danışma Belgesi 2607712*. <https://learn.microsoft.com/tr-tr/security-updates/securityadvisories/2011/2607712>
126. Miklosik, Andrej & Kuchta, Martin & Evans, Nina & Žák, Štefan. (2019). Towards the Adoption of Machine Learning-Based Analytical Tools in Digital Marketing. *IEEE*, vol. 7, 85705-85718. <https://doi.org/10.1109/ACCESS.2019.2924425>
127. Milmo, D. (2022, June 30). *Users of biggest NFT marketplace warned over phishing after data leak*. The Guardian. <https://www.theguardian.com/technology/2022/jun/30/users-opensea-nft-marketplace-warned-over-phishing-after-data-leak>
128. Moradam. (2022, August 23). *Seo Saldırılarından Korunmanın yolları Nelerdir*. <https://www.moradam.com/20180211208833/seo-saldirilarindan-korunmanin-yollarini-nelerdir/>
129. Muntode, A. R., & Parwe, S. S. (2019). An Overview on Phishing-its types and Countermeasures. *International Journal of Engineering Research & Technology (IJERT)*, 8-12. ISSN: 2278-0181
130. National Institute of Standards and Technology (NIST). (2011). *Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters*. 127.129. National Institute of Standards and Technology (NIST). <https://www.govinfo.gov/content/pkg/GOVPUB-C13-a2bba0532e0524ef13848ee9ae64414b/pdf/GOVPUB-C13-a2bba0532e0524ef13848ee9ae64414b.pdf>
131. Newman, C. (2019, January 16). *Target's Cyber Insurance: A \$100 million policy vs. \$300 million (so far) in costs: Data Security Law Blog*. Patterson Belknap. <https://www.pbwt.com/data-security-law-blog/targets-cyber-insurance-a-100-million-policy-vs-300-million-so-far-in-costs>
132. NSTAC. (2016, May 11). *NSTAC Report to the President on Big Data Analytics*. Cybersecurity and Infrastructure Security Agency. <https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Big%20Data%20Analytics%20%285-11-16%29-%20508%20compliant.pdf>

133. Nyaga, C. (2022, October 28). *Best crypto under \$1 to buy in November*. CoinJournal. <https://coinjournal.net/news/best-crypto-under-1-to-buy-in-november/>
134. Ocean Protocol Team. (2022, November 23). *Ocean collaborates with peaq to advance the future of machine-generated data sharing*. <https://blog.oceanprotocol.com/ocean-collaborates-with-peaq-to-advance-the-future-of-machine-generated-data-sharing-23a3da046ee4>
135. O'Neill, E. (2022, January 27). *What is an e-skimming attack*. International Cyber Threat Task Force. <https://community.icttf.org/blog/what-is-an-e-skimming-attack>
136. Ortiz, J. H. (2020). Industry 4.0: Current status and future trends. *IntechOpen Publications*. <https://doi.org/10.5772/intechopen.86000>.
137. Ozkaya, E. (2018). *Cybersecurity Challenges in Social Media*. (Doctoral dissertation, Charles Sturt University).
138. Öztürk, C. (2021, March 19). *Dao, Dac ve Lao*. BTCHABER. <https://www.btc-haber.com/dao-dac-ve-lao/>
139. PACER's National Bullying Prevention Center. (2022). *Cyberbullying*. <https://www.pacer.org/bullying/info/cyberbullying/>
140. Paganini, P. (2022, December 05). *Lazarus APT uses fake cryptocurrency apps to spread AppleJeus Malware*. Securityaffairs. <https://securityaffairs.co/wordpress/139290/apt/lazarus-apt-bloxholder-campaign.html>
141. Panwar, N. (2022, March 28). *What are BEC (business email compromise) scams*. Securityboulevard. <https://securityboulevard.com/2022/03/what-are-bec-business-email-compromise-scams/>
142. Parrales, G. I. S., & Batbayar, B. (2022). *Exploring the impacts of NFTs in marketing strategies and customer relationships*. (Master Thesis, Walden University).
143. Pereira, M. (2021, November). *Hacking season: Why cyber Monday presents a cyber security nightmare*. Darktrace. Darktrace. <https://darktrace.com/blog/hacking-season-why-cyber-monday-presents-a-cyber-security-nightmare>
144. Peters, G., Shevchenko, P. V., & Cohen, R. (2018). Understanding cyber-risk and cyber-insurance. *SSRN Electronic Journal* <http://dx.doi.org/10.2139/ssrn.3065635>

145. Posey, B. (2019, May 29). *User-Generated Content May Be a Security Threat*. Itprotoday. <https://www.itprotoday.com/security/user-generated-content-may-be-security-threat>
146. Rathnam, L. (2022, October 13). *Vishing attacks and how they can affect you and your company*. Techgenix. <https://techgenix.com/vishing-attack-guide/>
147. Regenscheid, A. R., & Beier, G. (2011). Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters. NIST Interagency/Internal Report (NISTIR), 7711. <https://doi.org/10.6028/NIST.IR.7711>
148. Rijmenam, D. (2022, August 31). *The Impact of 5G Technology on Business and When 6G Will Come*. The Digital Speaker. <https://www.thedigitalspeaker.com/impact-5g-technology-business/>
149. Rosenthal, M. (2022, April 12). *14 real examples of business email compromise (BEC) attacks*. Tessian. <https://www.tessian.com/blog/business-email-compromise-bec-examples/>
150. Rosenthal, M. (2022, April 12). *15 examples of real social engineering attacks- updated 2022*. Tessian. <https://www.tessian.com/blog/examples-of-social-engineering-attacks/>
151. Rosenthal, M. (2022, May 13). *Phishing statistics (updated 2022)- 50+ important phishing stats*. Tessian. <https://www.tessian.com/blog/phishing-statistics-2020/>
152. Rouse, M. (2022, May 16). *What is C-SCRM (Cybersecurity Supply Chain Risk Management)*. Techopedia. <https://www.techopedia.com/definition/34782/c-scrm-cyber-security-supply-chain-risk-management>
153. Russon, M. (2021, May 10). *US fuel pipeline hackers 'didn't mean to create problems'*. BBC. <https://www.bbc.com/news/business-57050690>
154. S., J. (2022, October 13). *Cyber corruption: LAPSUS\$*. Lumifycyber. <https://www.lumifycyber.com/3438-2/>
155. Sachdev, R. (2020, April). *Towards Security and Privacy for Edge AI in IoT/IoE based Digital Marketing Environments*. IEEE, 341-346. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9144755>

156. Samtani, S., Chinn, R., Chen, H., & Nunamaker Jr, J. F. (2017). Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence. *Journal of Management Information Systems*, 34(4), 1023-1053. <https://doi.org/10.1080/07421222.2017.1394049>
157. Schwertner, K. Digital transformation of business. *Trakia Journal of Sciences*, 15(1), 388-393. <https://doi.org/10.15547/tjs.2017.s.01.065>
158. Sild, O. (2021, April). *Security vulnerabilities of WordPress ecosystem in 2020*. Patchstack. <https://patchstack.com/wp-content/uploads/2021/04/Security-vulnerabilities-of-WordPress-ecosystem-in-2020-Patchstack-1.pdf>
159. Silva, D. (2022, February 13). *How Metaverse & NFTs are shaping the world of Marketing*. Medium. <https://medium.com/rootcodelabs/how-metaverse-nfts-are-shaping-the-world-of-marketing-74bebc92b019>
160. Sirimanne, S. N. (2022, May 03). *What is 'industry 4.0' and what will it mean for developing countries*. UNCTAD. <https://unctad.org/news/blog-what-industry-40-and-what-will-it-mean-developing-countries>
161. Smith, A. (2022, June 07). *Ünlü NFT Koleksiyonu the bored Ape Yacht Club hacklendi: Kayıp Büyük*. Indyturk. <https://www.indyturk.com/node/519051/ekonomi%CC%87/%C3%BCnl%C3%BC-nft-koleksiyonu-bored-ape-yacht-club-hacklendi-kay%C4%B1p-b%C3%BCy%C3%BCk>
162. Souppaya, M., & Scarfone, K. (2013). Guide to malware incident prevention and handling for desktops and laptops. *NIST special publication 800-83 revision 1*, <https://doi.org/10.6028/NIST.SP.800-83r1>
163. Spanning Cloud Apps. (2022, January 18). *Cyberattacks 2021: Statistics from the last year*. <https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/>
164. Stempel, J., & Bose, N. (2015, December 03). *Target in \$39.4 million settlement with banks over Data Breach*. Reuters. <https://www.reuters.com/article/us-target-breach-settlement-idUSKBN0TL20Y20151203>
165. Subramaniam, T. V. (2020). *Impact of social media on digital marketing: Starbucks marketing strategy on Twitter*. Case study, 2, 1-7.

- https://www.researchgate.net/publication/338448273_Impact_Of_Social_Media_On_Digital_Marketing_Starbucks_Marketing_Strategy_On_Twitter
166. Sushanth IT Law Associates. (2021). *Cyber Consumers*. <https://www.sushanthitlaw.com/cyber-consumers>
167. Szopik-Depczyńska, K., & Cheba, K. (2021). The impact of Internet on marketing activity in R&D departments in Poland. *Procedia Computer Science*, 192, 5030-5038. <https://doi.org/10.1016/j.procs.2021.09.281>
168. Taberner, R. (2020). *How will 5G affect your business*. Cmi. <https://www.newcmi.com/blog/how-will-5g-affect-your-business>
169. Tan, E., & CoinDesk. (2022, June 05). *Bored ape yacht club's discord server was hacked, with \$360,000 in nfts stolen. who's to blame is debated*. Fortune. <https://fortune.com/2022/06/04/bored-ape-yacht-clubs-discord-server-was-hacked-with-360000-in-nfts-stolen-blame-debated/>
170. Tavares, P. (2021, July 12). *Bec attacks: How attorney impersonation works*. Infosecinstitute. <https://resources.infosecinstitute.com/topic/bec-attacks-attorney-impersonation-works/>
171. TechInsurance. (2022, June 29). *Cyber Liability Insurance – Compare quotes*. Techinsurance. <https://www.techinsurance.com/cyber-liability-insurance>
172. Techopedia. (2011). *What is cookie theft*. <https://www.techopedia.com/definition/24633/cookie-theft>
173. Thaxton, R. (2022, April 04). *What are mergers and acquisitions (M&As)*. Forex. <https://www.forex.com/en-us/news-and-analysis/understanding-mergers-and-acquisitions/>
174. The European community of adult learning professionals. (2018). *Managing information and communication through technology- europa*. EPAL. https://epale.ec.europa.eu/sites/default/files/ds4a_io1-managing_information_and_communication-nooru-semaja_estonia.pdf
175. Top, Y. (2021, August 01). *Colonial Pipeline Saldırısı hakkında bilmeniz gereken 5 şey*. Siberbülten. <https://siberbulten.com/kritik-altyapi-guvenligi/colonial-pipeline-saldirisi-hakkinda-bilmeniz-gereken-5-sey>

176. Trendmicro. (2018, June 25). *Phishing emails sidestep Microsoft Office 365 filters using ZeroFont*. Trendmicro. <https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/phishing-emails-sidestep-microsoft-office-365-filters-using-zerofont>
177. Usta, O. (2021, November 09). *Mediamarkt'a Siber Saldırı: Rekor Fidyeye istendi*. Siberbülten. <https://siberbulten.com/siber-saldirilar-2/mediamarkta-siber-saldiri-rekor-fidyeye-istendi/>
178. Vega, R. (2022, May 18). *What is a Phishing Attack*. Checkpoint. <https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/what-is-a-phishing-attack/>
179. Verma, S. (2022, September 23). *Role of Decentralized Applications (DApps) in Web 3.0 in 2022 & Beyond*. Blockchain-Council. <https://www.blockchain-council.org/web-3/role-of-dapps-in-web-3-0/>
180. Villasmil, P. (2022, July 26). *What is the Metaverse and how will NFTs become part of it*. Mitsoftware. <https://mitsoftware.com/tr/meta-veri-deposu-nedir-ve-nft-bunun-nas%C4%B1l-bir-par%C3%A7a-s%C4%B1-olacak/>
181. Violino, B. (2022, October 11). *Rising premiums, more restricted cyber insurance coverage poses big risk for companies*. Cnbc. <https://www.cnbc.com/2022/10/11/companies-are-finding-it-harder-to-get-cyber-insurance-.html>
182. Vuijsje, E. (2021, November 28). *Top Five Malvertising attacks of 2016*. Geoedge. <https://www.geoedge.com/top-five-malvertising-attacks-of-2016/>
183. Whittaker, Z. (2018, September 11). *British Airways breach caused by credit card skimming malware, researchers say*. Techcrunch. <https://techcrunch.com/2018/09/11/british-airways-breach-caused-by-credit-card-skimming-malware-researchers-say/>
184. Wright, I. (2017, June 8). *Study of US manufacturing digitalization exposes significant Data Gap*. Engineering. <https://www.engineering.com/story/study-of-us-manufacturing-digitalization-exposes-significant-data-gap>
185. Wright, K. (2018, October 24). *A Guide To Wordpress Website Security*. Amazonaws. <https://s3.amazonaws.com/downloads.itthemes.com/public/ebooks/WordPress-Security-Guide.pdf>

186. Yalçın, F. (2021, May 17). *NFT Dolandırıcılıklarına Dikkat*. Techtime. <https://fintechtime.com/tr/2021/05/nft-dolandiriciliklarina-dikkat/>
187. Yeniçağ Gazetesi. (2022, March 17). *Dünya Tarihinde çok SES getiren 10 Siber Saldırı*. <https://www.yenicaggazetesi.com.tr/hackerlarin-en-buyuk-siber-saldirilari-lis-tesi-521508h.htm>



EKLER

Ek 1. İşletmelerin Dijitalleşme Sürecinde Siber Güvenlik: Sosyal Ağ Analizine Dayalı Hazır Bulunuşluk Ölçeği

Marka ve Siber Güvenlik
1. Kurumların ağ trafiği network tarama yazılımlarıyla izlenmelidir.
2. Kurumların Server hareketlerine ait kayıtlar Log takip yazılımlarıyla izlenmelidir.
3. Firewallerde tanımlı kurallar IDS ve IPS'lerde de uygulanabilir ve blocklanabilir olmalıdır.
4. Kurumların dış ağında yayınlanan tüm internet sitelerinde SSL Güvenlik Sertifikası olmalıdır.
5. Kurumun dış ağında yayınlanan internet sitesini korumak amaçlı kullanılan SSL Sertifikası aynı zamanda SIEM ürününe girilerek takip edilmeli ve süresi sona ermeden kısa bir süre önce yenilenmelidir.
6. Kurumlar E-Mail Gateway ve Email Protection ürünleri kullanarak Mail trafiklerini güven altına almalıdır.
7. Kurumlar siber saldırı senaryolarını sürekli olarak aktif tutmak için iç güvenlik testlerini sıklıkla tekrar etmeli ve güncel güvenlik prosedürlerini uygulamalıdır.
8. Kurumlarda Firewall tarafında Web Filtreleme uygulanmalı ve kullanıcıların buna uyup uymadığı SIEM güvenlik ürünleriyle takip edilmelidir.
9. İşletme gerektiği zamanlarda üçüncü bir kurum/kuruluş tarafından sağlanan yazılım, donanım ve hizmet alımından yararlanmalıdır.
10. Kurumlar iş birliği yapacağı firmalardan siber güvenlik yetkinliklerini ölçen ve değerlendiren sertifikasyonları ve belgeleri istemelidir.
11. Kurumlar ortalama ve sosyal mühendislik gibi güncel tekniklerle çalışanlarını düzenli bir şekilde test edip, çalışanların güvenlik bilinçlerinin taze kalmasını sağlamalıdır.

12. Kurumlar Microsoft BitLocker, IBM Guardium ve Apple FileVault gibi bir şifreleme programı kullanmalıdır.
13. Kurumlar, siber saldırı öncesini ve sonrasını planlamalıdır. Bu kapsamda siber saldırılara karşı felaket senaryosu (disaster-recovery) üretilmeli ve yılda en az bir kere bu senaryo gerçekleştirilmiş gibi uygulanmalıdır.
14. Kurum yöneticileri siber güvenlik politikalarına, prosedürlerine ve mekanizmalarına hâkim olmalıdır.
Operasyonel Siber Güvenlik
15. İşletme varlıklarının envanteri tamamlandıktan sonra, siber güvenlik risk değerlendirilmesi yapılmalı, mevcut savunmalarının yeterliliği ve varlıkların önemi değerlendirilmelidir.
16. Kurumların rutin ve olağanüstü durumlar için ayrı ayrı yedekleme(back-up) politikası belirlemeleri gerekmektedir.
17. Siber saldırılara karşı işletme iş sürekliliği/felaket kurtarma planı düzenli olarak test edilmelidir.
18. İşletme Veri Kaybı/Sızıntısı Önleme (DLP) yazılımları ile işletme dışına çıkarılması istenmeyen verilerin çıkışı önlenmelidir ya da belirlenen dosyaların kullanım durumları izlenmelidir.
19. İşletmelerde kullanılan kritik uygulamaların erişimleri sık sık denetlenmeli ve erişim politikaları uygulanmalıdır. Bu politikalar mutlaka SIEM ürünleri gibi ürünlerle takip edilmelidir. Kritik dosyalar veya erişim izinleri erişime olmayan kişilerin giriş sağlayamaması için koruma altına alınmalıdır.
20. İşletmedeki yazılım ve donanım erişim izinleri kontrol edilmeli ve yetkilendirme bölümleri bulunmalıdır.
21. Belirlenecek yönetici panellerine sadece VPN ile erişim sağlanmalıdır.
22. İşletmeler uç nokta güvenlik kontrolleri için yardımcı araçlar kullanılmalıdır. (Microsoft Advanced Threat Analytics – ATA, Osquery, Query Packs gibi).

İç Ağ Güvenliği
23. İşletme Yönlendirici ve kablosuz erişim noktası, ideal olarak bir birleşik tehdit yönetimi (UTM) sistemi veya "yeni nesil bir güvenlik duvarı" olan birinci sınıf bir güvenlik duvarı tarafından korunmalıdır.
24. Kurum ağ sistemleri düzenli şekilde ağ yönetim ve tarama yazılımlarıyla kontrol edilmelidir.
25. İşletme donanım yazılımları düzenli aralıklarla güncellenmelidir.
26. İşletme güvenlik yazılımları düzenli aralıklarla güncellenmelidir.
Web Uygulamaları Güvenliği
27. Kurumların internette yayın yapan sitelerinin barındığı hosting barındırma firmalarının siber güvenlik değerlendirmeleri kapsamında güvenlik testlerinin düzenli şekilde yapıldığına dair belgelerin ve test raporlarının istenmesi gerekmektedir.
28. İşletme uygulama yazılımları düzenli aralıklarla güncellenmelidir.
Son Kullanıcı Eğitimi
29. İşletme çalışanlarına siber güvenlik farkındalığı hakkında düzenli aralıklarla eğitimler verilmelidir.