1882
KONYA TİCARET ODASI
KONYA CHAMBER OF COMMERCE

KÜRESEL SİBER SAVAŞLAR VE TÜRKİYE MENZİLİ

MUSTAFA KESKİN

Araştırma Raporu

Ekonomik Araştırmalar ve Proje Müdürlüğü

KONYA
Haziran, 2024
www.kto.org.tr

İÇİNDEKİLER

KÜRESEL SİBER SAVAŞLAR VE TÜRKİYE MENZİLİ

1. GİRİŞ

Son yıllarda yaşanan küresel olayların (Covid-19 ve Ukrayna-Rusya Savaşı) tetiklediği ekonomik ve sosyopolitik olumsuzluklar siber suç faaliyetlerinde artışa neden olmuştur. Artış gösteren siber saldırıların kurum ve kuruluşlara verdiği maddi ve manevi zararlar ciddi boyutlara ulaşmıştır.

Dijitalleşen cihazların internete olan bağımlılığı, bulut teknolojileri ve yapay zekâ gibi teknolojilerin kullanımının artması, siber saldırıların sayısını da artırmıştır. 2023 yılında 9 milyar veri siber saldırıya uğrarken, küresel ekonomilere maliyeti ise 8 trilyon dolar olmuştur. 2030 yılına kadar siber saldırıların küresel ekonomilere maliyetinin toplamda 10 trilyon dolara ulaşacağı tahmin edilmektedir.

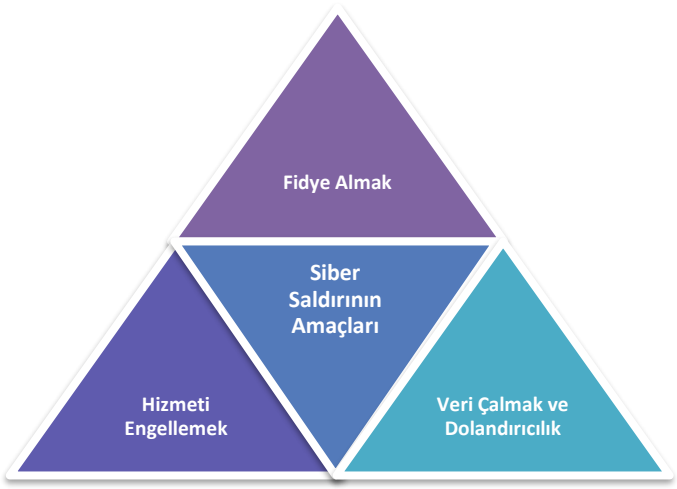
Bu araştırma kapsamında; siber güvenliğin tanımı, en yaygın siber saldırılar, saldırıların etkileri, saldırılara karşı alınacak önlemler ve son iki yıllık periyotta oluşan genel istatistiki veriler dünya, Türkiye ve Konya özelinde incelenmiştir.

2. SİBER GÜVENLİK

Bilişim sistemlerinin açıklarını tespit edip çeşitli yazılımlardan destek alarak farklı sistemlerden veri ve bilgi edinilmesine siber saldırı denilmektedir. Buradaki temel amaç; kurumsal ya da kişisel bilgisayarların ağı içindeki bilgi ve verilere sızarak değiştirilmesi veya çalınmasıdır.

Siber saldırıyı gerçekleştiren kişiler hacker olarak adlandırılmaktadır. Hackerlar genellikle siyasi, kriminal veya kişisel amaçlarla saldırı gerçekleştirerek bireylerin finansal bilgilerini, şirket ya da şahısların özlük bilgilerini ele geçirmektedir.

Şekil 1: Siber Saldırıların Amaçları



Kaynak: Avansas Blog

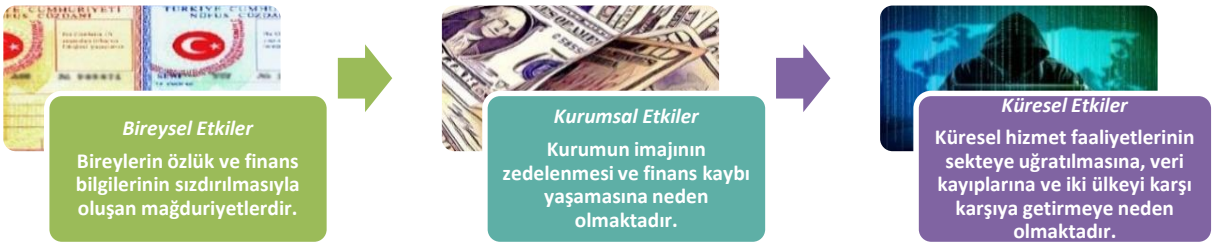
Günümüzde gerçekleşen en yaygın on siber saldırı aşağıda genel tanımlarıyla gösterilmiştir. Özellikle fishing ve fidye yazılımı saldırılarında büyük zararlar verilmektedir.

Şekil 2: Günümüzdeki En Yaygın 10 Siber Saldırı

Kaynak: Avansas Blog

Siber saldırılar bireylerin, kurumların sistemlerini ve verilerini etki altına alıp kontrol etmeyi amaçlamaktadır. Bundan dolayı maddi ve manevi büyük tehdit içeren siber saldırıların küresel, kurumsal ve bireysel etkileri bulunmaktadır.

Şekil 3: Siber Saldırının Etkileri



Kaynak: Avansas Blog

Siber saldırılardan etkilenen sektörlerin başında finans sektörü gelmektedir. Genelde maddi kâr elde etmek amaçlı yapılan siber saldırılar sanal ticarette bireylerin finansal bilgilerini ele geçirmeyi hedeflemektedir.

Şekil 4: Siber Saldırıdan Etkilenen Sektörler

Kaynak: Avansas Blog

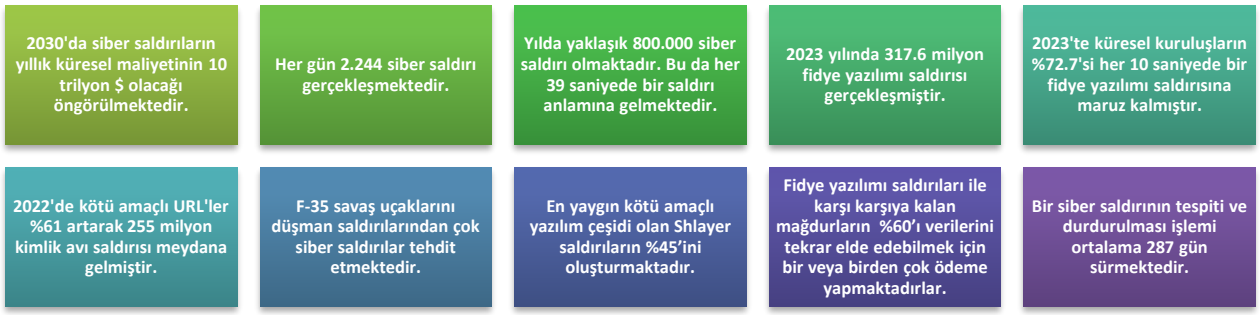
Siber saldırılardan korunma yöntemleri saldırıların başarılı olmasının önüne geçmektedir. Aşağıda siber saldırılara karşı alınan önlemler verilmiştir.

Şekil 5: Siber Saldırıları Önleme Teknikleri

Kaynak: Websiterating.com

2023 yılında küresel siber suç hasar maliyetleri yıllık 8 trilyon dolar olarak tahmin edilmektedir. Aşağıdaki şekilde siber saldırılar hakkında çeşitli istatistikler gösterilmiştir.

Şekil 6: Siber Saldırı İstatistikleri



Kaynak: İlginç Mühendislik

3. KÜRESEL SİBER SAVAŞLAR

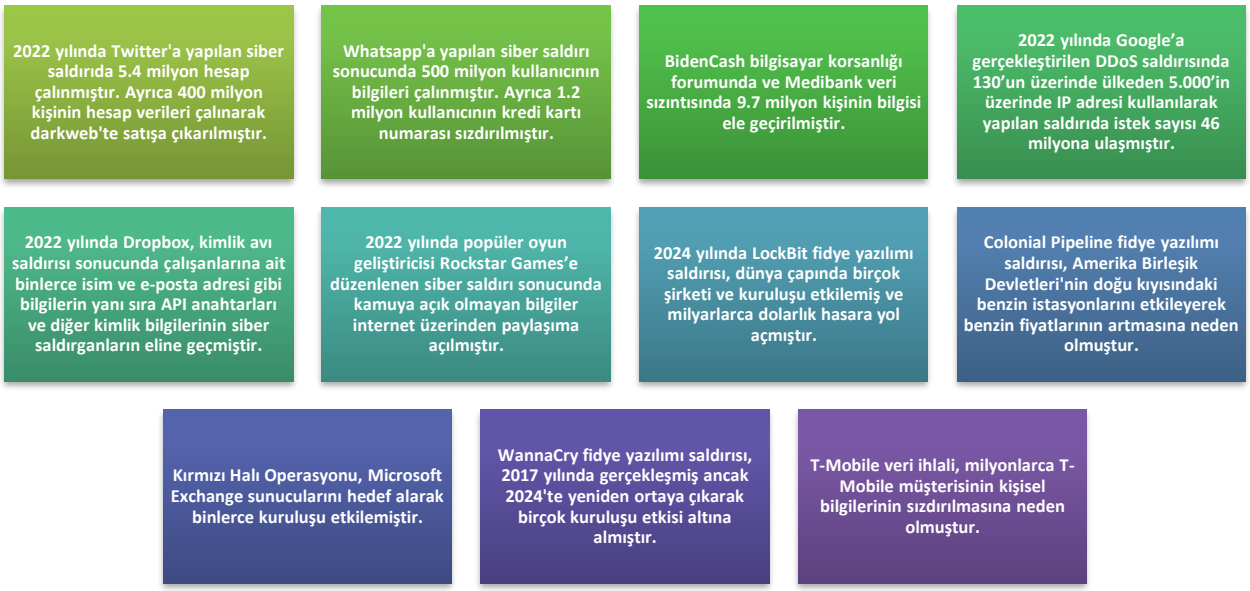
Siber saldırıların çıkış noktası soğuk savaş dönemlerinde başlamıştır. Teknolojinin hızla gelişmesiyle beraber saldırıların çeşitliliği ve hacmi artmıştır. Başta Amerika olmak üzere Rusya, Çin, İsrail ve İngiltere kendi savunma ve saldırı timlerini oluşturmuştur. Ayrıca taşeron hackerler da kullanmışlardır.

Şekil 7: Tarihten Günümüze Önemli Gelişmeler

Kaynak: Teknocak.com

2022 yılında IBM tarafından hazırlanan veri ihlallerinin maliyeti raporunda başarılı olan bir fidye yazılımı saldırısının ortalama maliyeti ödenen fidye dâhil 4,54 milyon dolar olmuştur. Ülkemizde başarılı olan bir siber saldırının ortalama maliyeti ise yine aynı rapora göre 1.11 milyon dolar olarak kaydedilmiştir.

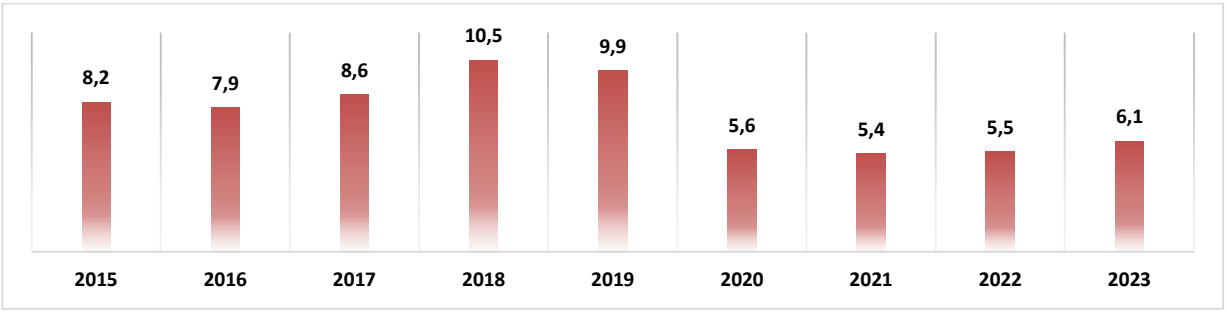
Şekil 8: Küresel Siber Saldırılar



Kaynak: Websiterating.com

2015'ten 2022 yılına kadar küresel kötü amaçlı yazılımlar incelendiğinde, en çok kötü amaçlı yazılım 10,5 milyar adet ile 2018 yılına aittir. 2022 yılına kadar kademeli olarak düşüş göstermiş 2023 yılında 6,1 milyar adet olmuştur.

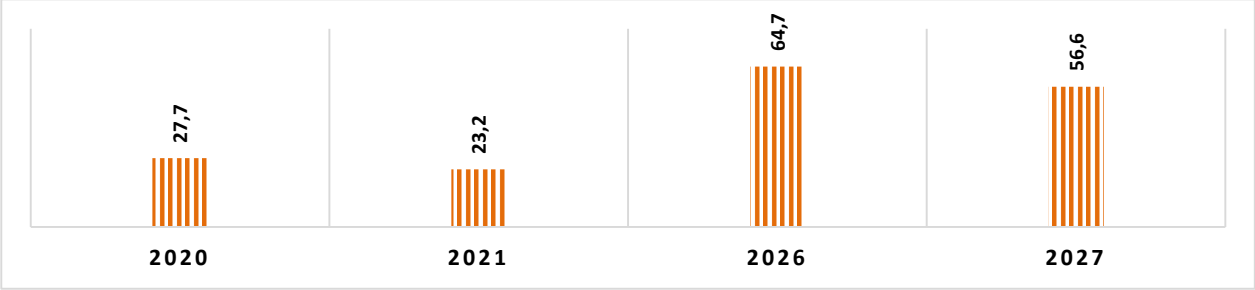
Grafik 1: Küresel Kötü Amaçlı Yazılım Miktarı (2015-2023, Milyar Adet)



Kaynak: Statista

Siber saldırılara karşı oluşturulan küresel siber güvenlik hizmetlerinin pazar büyüklüğü 2020 yılında 27 milyar dolarken 2021 yılında %19'luk bir düşüşle 23 milyar dolar olmuştur. 2026 yılında ise ciddi bir artış sergileyerek 64 milyar dolara, 2027 yılında ise 56 milyar dolara ulaşacağı tahmin edilmektedir.

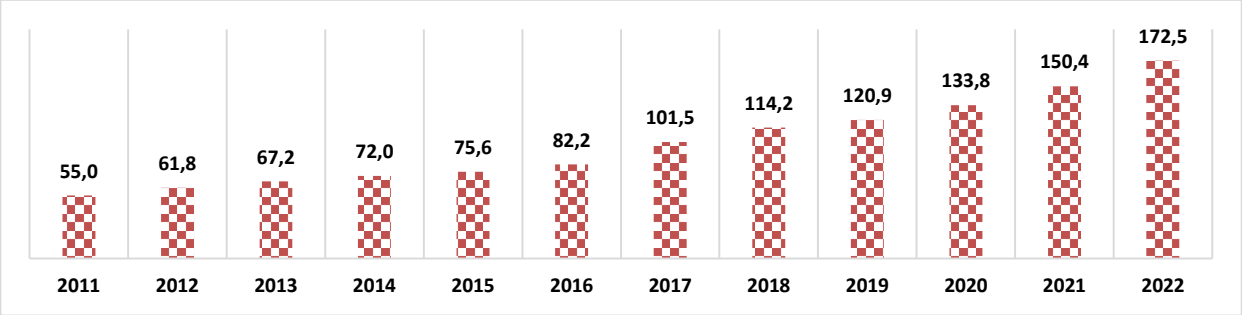
Grafik 2: Küresel Güvenlik Hizmetleri Pazar Büyüklüğü (2020-2027, Milyar Dolar)



Kaynak: Statista

Küresel bilgi güvenliği ürün ve hizmetleri pazar geliri incelendiğinde, 2011 yılında 55 milyar dolar iken kademeli olarak artış göstererek 172 milyar dolara kadar yükselmiştir. Bu istatistik ürün ve hizmetlerin bilgi güvenliği hususunda yıldan yıla ne derece önem kazandığını göstermektedir.

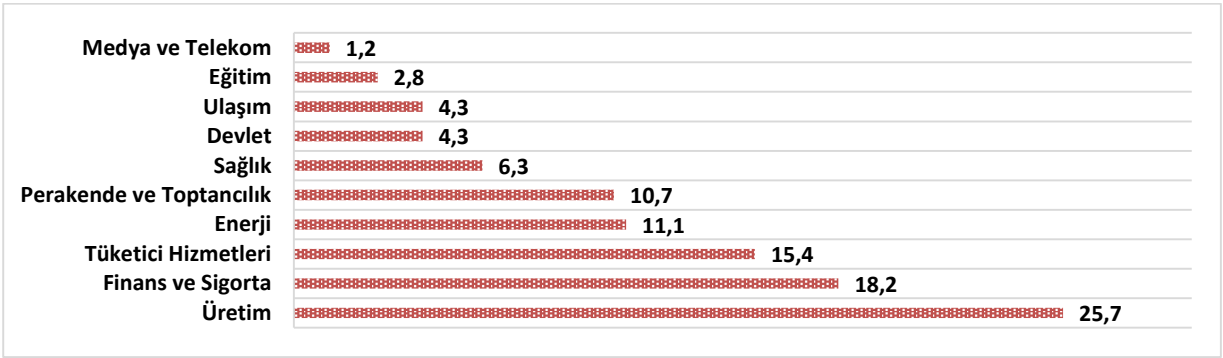
Grafik 3: Küresel Bilgi Güvenliği Ürün ve Hizmetleri Pazar Geliri (2011-2022, Milyar Dolar)



Kaynak: Statista

Küresel olarak siber saldırıların sektörlere göre dağılımı incelendiğinde, %25,7'lik oranla üretim sektörü en çok saldırıya uğrayan sektördür. Finans ve sigorta sektörü ise %18,2'lik oranıyla ikinci sırada konumlanmaktadır.

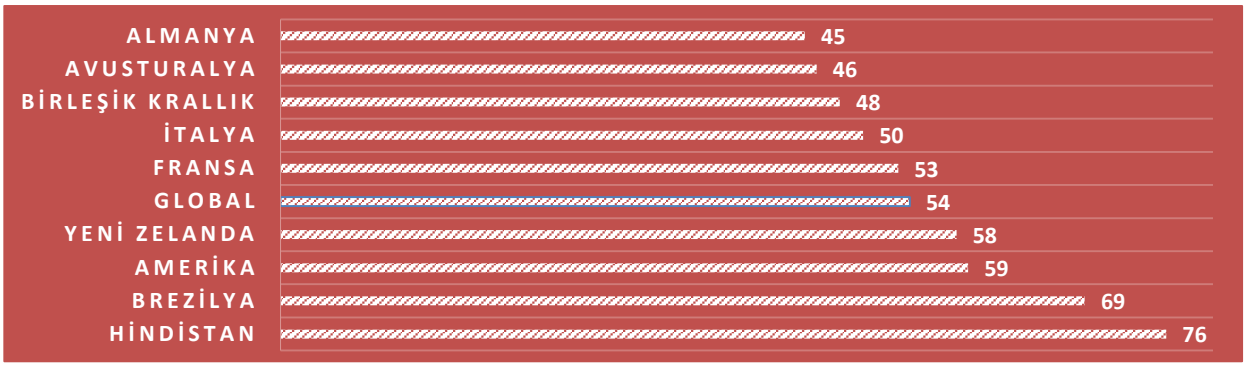
Grafik 4: Dünya çapındaki Siber Saldırıların Sektörlere Göre Dağılımı (2023, %)



Kaynak: Statista

Siber suça maruz kalan ülkelerin kullanıcıları incelendiğinde, Hindistan %76 ile birinci sırada yer almaktadır. Brezilya ve Amerika sırasıyla %69 ve %59 ile Hindistan'ı takip etmektedir.

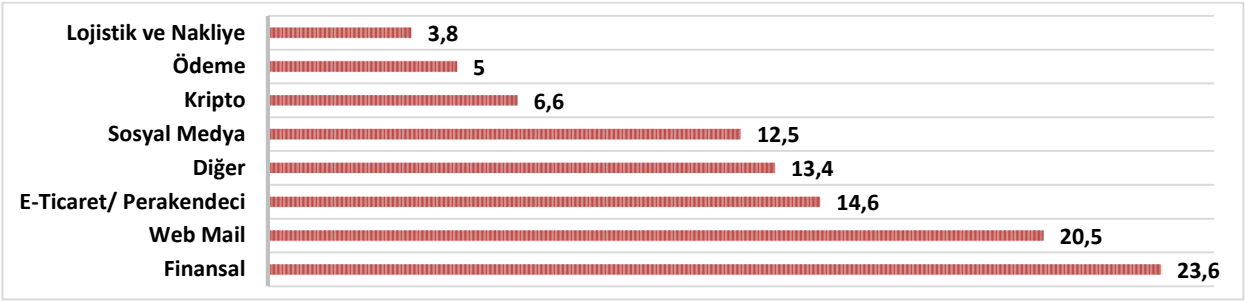
Grafik 5: Siber Suça Maruz Kalmış Ülkelerin Kullanıcıları (2021, %)



Kaynak: Statista

Kimlik avı saldırılarının hedeflediği çevrimiçi sektörlere bakıldığında finans sektörü %23,6, web mail sektörü %20,5, e-ticaret sektörü ise 14,6 ile başı çekmektedir. Son zamanlarda artış gösteren kripto sektörü de %6,6'lık oranıyla altıncı sıradadır.

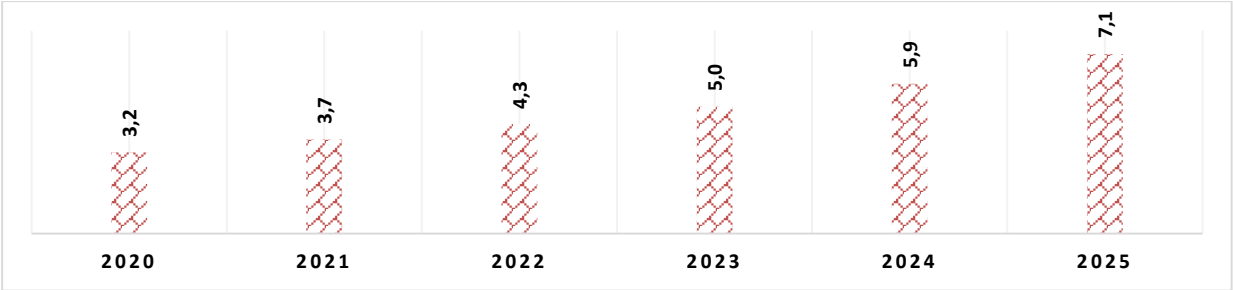
Grafik 6: Kimlik Avı Saldırılarının Hedeflediği Çevrimiçi Sektörler (2022, %)



Kaynak: Statista

Küresel olarak güvenli e-posta ağ geçidi pazar tahmininin 2023'te 5 milyar dolar, 2024'te yaklaşık 6 milyar dolar ve 2025'te 7 milyar dolarlık bir hacime ulaşacağı düşünülmektedir. Grafiğe göre güvenli e-posta pazarının sürekli arttığı görülmektedir.

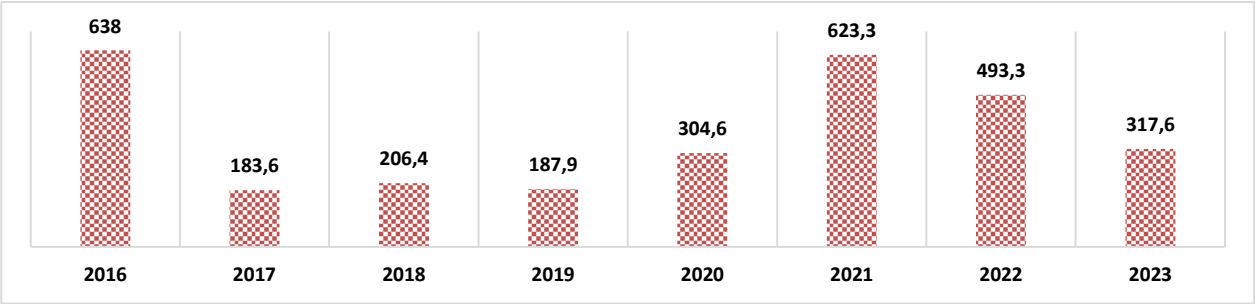
Grafik 7: Küresel Güvenli E-Posta Ağ Geçidi Pazar Tahmini (2020-2025, Milyar Dolar)



Kaynak: Statista

Küresel fidye yazılımı saldırılarının rakamları incelendiğinde 2016 yılında 638 milyon ile en yüksek seviyesine ulaşmıştır. 2023 yılında ise 317 milyon adete kadar gerilemiştir.

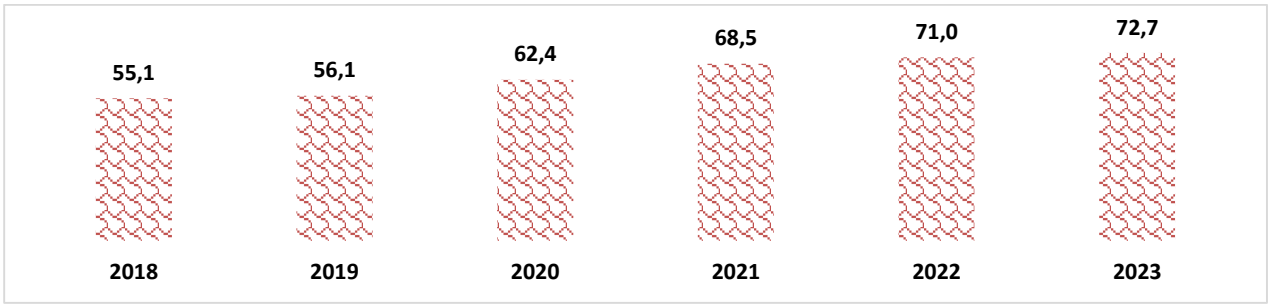
Grafik 8: Küresel Fidye Yazılımı Saldırısı Miktarı (2016-2022, Milyon Adet)



Kaynak: Statista

Küresel fidye yazılımı saldırılarından etkilenen kuruluşların yıllık payları incelendiğinde, 2018 yılında %55,1 olan oran, 2023 yılında %72,7 oranına yükselmiştir. Kademeli yükseliş eğilimi sürmektedir.

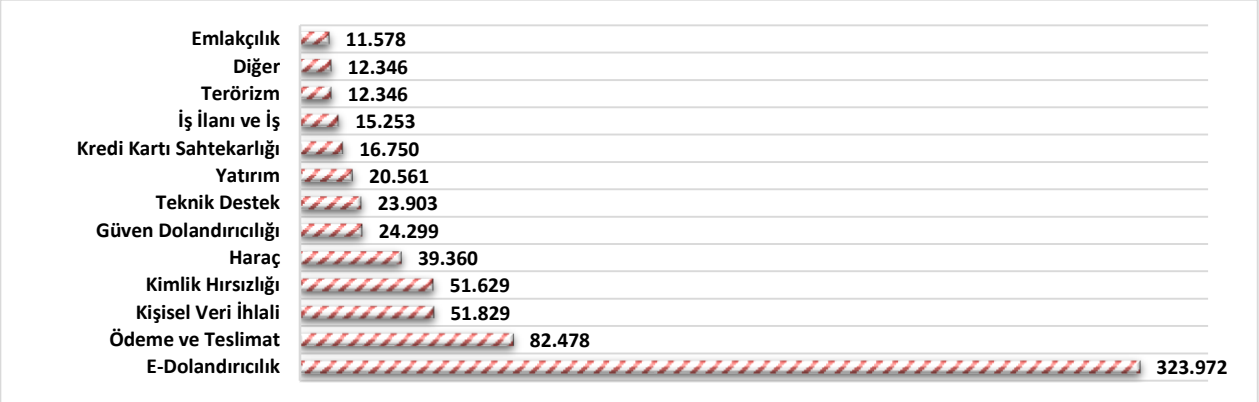
Grafik 9: Dünya Çapında Fidye Yazılımı Saldırılarından Etkilenen Kuruluşların Yıllık Payı (2018-2023, %)



Kaynak: Statista

Siber suç mağdurlarının ihbarlarına bakıldığında e-dolandırıcılık yaklaşık 324 bin iken ödeme ve teslimat 82 bin ihbar, kişisel veri ihlali ve kimlik hırsızlığı 51 bin ihbar şeklinde gerçekleşmiştir. Kalan diğer ihbar çeşitlerinde toplam 12 bin mağduriyet gerçekleşmiştir.

Grafik 10: Siber Suç Mağdurlarının İhbarları (2021)



Kaynak: Statista

2024 yılı için dünyayı bekleyen en riskli siber saldırı türlerinin başında yapay zekâ tabanlı siber saldırılar, fidye yazılım tehditleri ve deepfake teknolojisi gelmektedir. Diğer saldırı türleri şekilde verilmiştir.

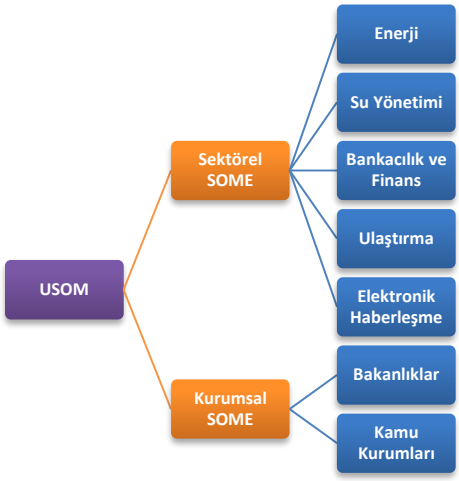
Şekil 9: 2024 Yılında Tahmini En Yaygın Küresel Siber Saldırı Türleri

Kaynak: sigortacigazetesi

4. TÜRKİYE'NİN SİBER GÜVENLİK MENZİLİ

20 Haziran 2013 tarihinde Bakanlar Kurulu tarafından alınan kararla yürürlüğe giren ve Bilgi Teknolojileri ve İletişim Kurumu çatısı altında çalışmalarını sürdüren Türkiye'nin siber savunmasından sorumlu Siber Olaylara Müdahale Ekibi (SOME) kritik sektör ve kurumların korunmasında en önemli birimdir. SOME, Ulusal Siber Olaylara Müdahale Ekipleri (USOM)'nin sorumluluğundadır. Sektörel ve kurumsal SOME yapılanmasında toplam 2 bin 74 siber güvenlik uzmanı bulunmaktadır. SOME ile USOM (Ulusal Siber Olaylara Müdahale Merkezi) bünyesinde ise toplamda 6 bin 99 siber güvelik uzmanı Türkiye'nin siber güvenliğini sağlamaktadır.

Şekil 10: USOM – Sektörel ve Kurumsal SOME İlişkisi



Kaynak: Bilgi Teknolojileri ve İletişim Kurumu

Türkiye'nin siber güvenlik alt yapısının gelişimi ve ulusal güvenlik adına yapmış olduğu gelişmeler aşağıdaki gibidir. Tarihten günümüze kadar çeşitli programlar ve planlamalar oluşturulmuş ve ciddi katkılar sağlayan kurumlar faaliyete geçirilmiştir.

Şekil 11: Türkiye'nin Siber Güvenlik Tarihi

Kaynak: Dijital Dönüşüm Ofisi

Ulusal Siber Olaylara Müdahale Merkezi (USOM) 2022'de 130 binin üzerinde zararlı bağlantının tespitini gerçekleştirerek erişimi kısıtlamıştır. Buna ilave olarak 30 binin üzerinde ihbarı ilgili kurum ve kuruluşlara bildirerek gerekli güvenlik önlemlerinin alınmasını sağlamıştır.

2022 yılının ilk altı ayına kadar olan veriler incelendiğinde 649.349 adet kötü amaçlı yazılım saldırısı tespit edilmiştir. Bu da Türkiye'ye saatte 151 adet siber saldırı gerçekleştirildiğini göstermektedir.

Türkiye'de mobil telefonlara saldırı %2,6, finansal saldırılar %0,4 ve bilgisayarlara kötü amaçlı yazılım oranı %7,2 oranlarında gerçekleşmiştir. Türkiye bu verilere göre siber güvenlik anlamında %5'lik dilime girmektedir.

Şekil 12: Türkiye'nin Siber Güvenlik SWOT Analizi

Kaynak: cubeincubation.com

5. SİBER GÜVENLİKTE KONYA CEPHESİ

Firmaların dijital dönüşüm süreçlerinde, bilgi teknolojileri güvenliği en önemli unsurdur. Saldırı girişimine maruz kalan firmalar hem iktisadi kayıplara hem de zaman kaybına uğramaktadır. Konya'da en çok görülen siber saldırı türleri ddos, kripto ve balıklama yöntemleridir. Konya'da gerçekleştirilen siber saldırılar ile saldırganların hedeflediği veriler aşağıda gösterilmektedir.

Şekil 13: Konya'da Gerçekleştirilen Siber Saldırılarda Hedeflenen Veriler

Kaynak: KTO Siber Güvenlik Merkezi

Konya'da potansiyel siber saldırılara karşı uygulanan güvenlik önlemlerinden oluşan başlıca hizmetler penetrasyon (sızma testi), siber güvenlik danışmanlığı ve veri yedekleme-felaket kurtarma şeklindedir. Konya'da siber saldırılara karşı alınan başlıca önlemler maddeler halinde gösterilmektedir.

- Bilgi Güvenliği,
- Network Güvenliği,
- Uygulama ve Sanallaştırma Güvenliği,
- Bulut Uygulama Güvenliği,
- Saldırı Tespit ve Önleme Sistemleri,
- Log ve Olay Yönetim Hizmetleri,
- Veri Yedekleme ve Felaket Kurtarma Merkezi,
- Yetki Matrisi ve Kontrolü,
- Sızma/Penetrasyon Testleri,
- Veri Kaybı Önleme,
- Veri Maskeleme-Silme-Anonimleştirme,
- Next Generation Firewall,
- Güncel Antivirüs, Son Kullanıcı Güvenliği, XDR,
- Ayrıcalıklı Erişim ve Password Yönetimi.

6. SONUÇ

Siber güvenlik uzmanları 2030 yılında küresel siber suç faaliyetlerinin kurum ve kuruluşlara maliyetinin 10 trilyon dolara yükseleceğini düşünmektedir. Bu gelişmelere göre 2024 yılında ülkeler siber güvenlik alt yapı yatırım ve harcamalarını arttırmıştır.

Küresel ekonomik bunalım, Ukrayna-Rusya Savaşı, Orta Doğuda yaşanan İsrail kaynaklı gerilimler, çip ve petrol krizi, seçimler ve diğer etmenlerden kaynaklanan olumsuzlukların 2024 yılında meydana gelecek siber saldırıların şiddetini artıracağı öngörülmektedir.

Uzmanlara göre tedarik zincirlerinde, bulut ortamında, kimlik avı ve fidye yazılımı saldırılarında 2024 yılında büyük artış yaşanacağı düşünülmektedir. Ayrıca siyasi kaynaklı siber saldırıların ve özlük bilgilerine karşı yapılacak saldırıların seçim ortamında artması beklenmektedir. Uzmanlar kamu kurumlarına yapılacak siber saldırıların da artacağını ön görmektedirler.

7. KAYNAKÇA

- https://www.allianz.com.tr/tr_TR/seninle-guzel/siber-saldiri-nedir.html
- https://www.microsoft.com/tr-tr/security/business/security-101/what-is-a-cyberattack
- https://www.avansas.com/blog/siber-saldiri-nedir-sirketler-siber-saldirilara-karsi-neler-yapmalidir
- https://www.karel.com.tr/blog/siber-saldiri-nedir-turleri-nelerdir
- https://teknocak.com/siber-guvenlik-ve-siber-savaslar/61
- https://epnext.com/2023te-siber-guvenlik-sektorunu-neler-bekliyor/
- https://www.capital.com.tr/sirket-panosu/sirket-panosu-haberleri/2023-siber-guvenlikte-dayaniklilik-yili-olacak
- https://www.dunya.com/gundem/siber-guvenlik-uzmanlarindan-2023-uyarisi-haberi-676974
- https://gazeteoksijen.com/dunya/bloomberg-yazarindan-2023-analizi-bu-yil-beklenmeyeni-bekleyin-167819
- https://www.aa.com.tr/tr/bilim-teknoloji/turkiyeye-yonelik-siber-saldirilar-2021de-bir-oncekiyilagoreazaldi/2516713#:~:text=Ula%C5
- https://www.cubeincubation.com/blog/dunyada-ve-turkiyede-siber-guvenlik-gercekleri-1-istatistikler-analizler-ongoruler
- https://www.websiterating.com/tr/research/cybersecurity-statistics-facts/
- https://www.technologic.com.tr/siber-guvenlik-sektorunde-2023-yili-trendleri-aciklandi/59567/.html
- https://www.cybermagonline.com/2023te-dikkate-alinmasi-gereken-4-siber-guvenlik-trendi
- https://epnext.com/2023-yili-siber-guvenlik-trendleri/
- https://turk-internet.com/turkiyede-2022nin-ilk-yarisinda-siber-saldirilar-yarim-milyonu-asti/
- https://sigutr.org/2022-icin-bilinmesi-gereken-22-siber-guvenlik-istatistigi/
- https://sge.bilgem.tubitak.gov.tr/tr/kurumsal/tarihce
- https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi
- https://www.youtube.com/watch?v=bkZmbKa7Iz0
- https://www.youtube.com/watch?v=-rxWL515lqI
- Statista
- Konya Ticaret Odası Siber Güvenlik Merkezi