thinktech
STM Teknolojik Düşünce Merkezi

Siber Saldırıların Geleceği

Siber saldırı, bir kişi veya grubun dijital sistemlere yetkisiz erişim sağlayarak bilgi çalma, sistemleri bozma veya zarar verme amacıyla gerçekleştirdiği kötü niyetli bir girişimdir. Siber saldırılar bağış platformları, web formları ve bulut hizmetleri dahil olmak üzere kurumların internete bağlandığı her yerde, internet üzerinden verdiği/aldığı hizmetlerde, tedarik zinciri ağında ve hatta kapalı sistemlerinde de meydana gelebilir. Bu nedenle giderek daha fazla dijital hâle gelen günümüz dünyasında kurumların siber tehdidini azaltmak için siber güvenliğe öncelik vermesi kritik önem taşıyor.

Özellikle yapay zekâ, makine öğrenmesi ve bulut teknolojilerinin gelişimiyle daha da birbirine bağlı çalışan cihazların varlığı siber saldırı olasılığını artırıyor. Kötü niyetli tarafların bilgi ve iletişim teknolojilerini kullanarak gerçekleştirdiği siber saldırılar her sektörde olduğu gibi güvenlik ve savunma sektörlerinde de sorunlara yol açabiliyor. Toplum iletişim, ticaret ve kritik altyapı için giderek daha fazla dijital teknolojiye güvendikçe siber tehdit olasılıkları katlanarak artıyor[1].

Küresel Ölçekte Siber Saldırının Etkileri

Siber saldırılar birçok biçimde gerçekleşebiliyor. Kimlik dolandırıcılığı, veri hırsızlığı, fidye yazılımı saldırıları, telif hakkı ihlali ve kimlik avı kampanyaları bilinen siber saldırı örnekleri olarak öne çıkıyor. Kuruluşlar, müşterilerin veya çalışanların kişisel olarak tanımlanabilir bilgilerinin kaybını siber saldırıların en tehlikeli sonuçlarından biri olarak değerlendiriyor. Hassas bilgilerin kaybı, şirketler için itibar kaybı ve gelir kaybı gibi ciddi sonuçlar doğurabiliyor[2].

Siber saldırıların etkileri bazen fiziksel bazen de maddi olarak ortaya çıkabiliyor. Dünya çapında veri ihlallerinin saatlik ortalama maliyetinin her yıl daha da arttığı görülüyor. 2001'de bireyler için saatlik ortalama maliyet 2.000 dolarken, 2021 yılında saatlik kayıp oranının artarak 787.000 dolara ulaştığı biliniyor[3].

Dünya genelinde kuruluşlara yönelik artan tehdit, daha fazla kişinin siber güvenliği ciddiye aldığı anlamına geliyor. KOBİ'lerin yüzde 73'ü siber güvenlik endişelerine karşı artık harekete geçilmesi gerektiğini kabul ederken, yüzde 78'i gelecek 12 ay içinde siber güvenlik yatırımlarını artıracaklarını söylüyor[3].

1 https://www.simplilearn.com/top-cybersecurity-trends-article
2 https://www.statista.com/markets/424/topic/1065/cyber-crime-security/#statistic1
3 https://aag-it.com/the-latest-cyber-crime-statistics/

Siber saldırı yöntemleri giderek daha karmaşık hâle geldikçe küresel olarak kuruluşlar daha gelişmiş güvenlik önlemlerine yatırım yapmak, çalışanların eğitimleri güncellemek ve özellikle daha büyük şirketlerde özel siber güvenlik personellerini işe almak zorunda kalıyor. Bu şirketler saldırıya uğradığında, ihlali düzeltmenin ve kesintiden kurtulmanın maliyeti milyonlarca dolara ulaşabiliyor. 2022'de bir siber ihlalin ortalama maliyeti 4,35 milyon dolardı[4]. Siber suçun 2022'de küresel ekonomiye yaklaşık 7 trilyon dolara mal olduğu[3] ve bu rakamın 2025'e kadar 10,5 trilyon dolara çıkacağı tahmin ediliyor[4].

Dünya çapındaki kuruluşlar yalnızca siber saldırılarda kaybolan verileri geri almak için ödeme yapmakla kalmıyor aynı zamanda siber suç nedeniyle operasyonlarda yaşanan kesinti ve aksama ile de mücadele etmek zorunda kalıyor. Günümüzde dünya çapındaki hükümetler kişisel veri korumasını iyileştirmeye yönelik adımlar atarken, kullanıcılar artık çevrimiçi ortamdaki riskleri en aza indirme konusunda daha bilinçli ve ilgili hâle geliyor. 2023 yılından bu yana 10 internet kullanıcısından yedisinin çevrimiçi kimliklerini korumak için adım attığı biliniyor. Aynı zamanda bazı kullanıcılar daha rahat internet kullanımı için riskleri kabul etmeye de istekli. Küresel katılımcıların yaklaşık yüzde 70'i, yıllar öncesine göre kimlik hırsızlığına karşı kendilerini daha savunmasız hissettiklerini söylüyor. Genel Veri Koruma Yönetmeliği (General Data Protection Regulation -GDPR) şirketler ve kuruluşlar tarafından verilerin ve kişisel bilgilerin işlenmesini daha iyi düzenlemek ve vatandaşların hakları ve gizliliği için daha fazla koruma sağlamak amacıyla 2018 yılında Avrupa Birliğinde tanıtılmıştı. Bu yönetmelik günümüzde küresel olarak en kapsamlı veri gizliliği düzenlemesi olmaya devam ediyor. Son yıllarda diğer ülkelerin de kullanıcıların çevrimiçi bilgilerini koruyan benzer yasalar geliştirdiği biliniyor[5].

Siber saldırılarda son zamanlarda öne çıkan yeni bir trend ise QR kodlarla gerçekleşiyor. Restoranlardan alışverişe, bilet işlemlerinden diğer birçok alana kadar gündelik hayatta insanlara kolaylık sağlayan QR kod teknolojisinin kullanımı özellikle pandemi sonrası önemli derecede yaygınlaştı. QR kod tabanlı saldırılar da bu sebeple son zamanlarda hızla artış gösteriyor. Dolandırıcılar sahte QR kodları oluşturuyor ve bunları meşru görünen yerlere yerleştirerek veya cihazlara uygulama indirerek kötü amaçlı yazılımları bulaştırıyor. QR kodların sahte bankacılık ara yüzleriyle, alışveriş sitelerine yönlendirmeyle, kullanıcı bilgilerinin çalınmasıyla veya saldırganların ödeme yapılacak QR kodlarını manipüle ederek parayı kendi hesaplarına yönlendirmesiyle kullanıldığına dikkat çekiliyor[6].

Savunma Sanayiinde Siber Saldırıların Etkileri ve Gelecek Planları

Günümüz silah sistemleri büyük ölçüde sayısallaştırılarak gömülü yazılım ve bilgi teknolojisi sistemleriyle donatılıyor. Silah sistemlerinin siber güvenliği, modern savunma ve güvenlik stratejilerinin vazgeçilmez bir parçasını oluşturuyor. Bu nedenle, siber güvenlik ve siber dayanıklılığı tasarım aşamasında proaktif olarak yönetebilmek önem taşıyor. Araştırmalar bu tür koordine edilmiş siber güvenlik ve siber dayanıklılık yaklaşımlarının programlar için daha verimli ve genel yatırım getirisinin daha iyi olduğunu gösteriyor[7].

Ayrıca siber saldırılar savunma sanayiinde ve ülkelerin savunmasında da çok ciddi etkiler yaratabiliyor. NATO siber kavramını kara, hava ve denizle birlikte önemli bir savunma alanı olarak kabul ediyor. Bu durum savunma sistemlerine ve kritik ulusal altyapıya (Critical National Infrastructure -CNI) yönelik dış saldırıların yıkıcı etkileri olmasından kaynaklanıyor. Devletler veya bireyler gibi siber güvenliğe yönelik dış tehditleri yönetmek, ulusal dayanıklılığın yanı sıra dahili dijital savunmaları oluşturmaya yardımcı oluyor. Ancak hükümetlerin ve küresel savunma örgütlerinin karşı karşıya olduğu siber tehdit manzarası her zaman değişiyor ve son derece karmaşık bir yapıda ortaya çıkıyor. NATO 2023'te "önemli kötü niyetli siber faaliyetlere" yanıt olarak siber caydırıcılığı ve siber savunma duruşunu geliştirmek için yaklaşımını güncellemişti. Bu nedenle 2024'te, hassas

4 https://www.strongdm.com/blog/cost-of-data-breach
5 https://www.statista.com/markets/424/topic/1065/cyber-crime-security/#definition
6 https://www.stm.com.tr/tr/medya/basin-bultenleri/stmden-yeni-siber-tehdit-raporu-qr-kodlar-uzerinden-yapilan-siber-saldirilarda-artis-yasaniyor
7 https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-nisan-haziran-2024

bilgileri ve kritik sistemleri etkili bir şekilde korumak için oluşturulan "gelişmiş saldırı zayıflatma stratejileri (sophisticated mitigation strategies)" yaklaşımı dışarıdan gelen tehditlere karşı uygulanan siber güvenliğinin ön saflarında yer alıyor.

Elbette siber güvenlik açığı değerlendirmeleri savunma ağlarına ve bilgisayarlarına yönelik tehditleri belirlemek, analiz etmek ve önceliklendirmek için hayati öneme sahip olmaya devam ediyor. Ancak bunların izole bir şekilde kullanılmaması gerekiyor. Bunun nedeni karar vericilerin çok aşamalı siber saldırılarda tehdit azaltmalarını önceliklendirmelerine izin vermemelerinden ileri geliyor. Buna karşılık siber tehdit tahmin ve modelleme yazılımı analistlerin daha proaktif olmasını sağlıyor. Geleneksel siber güvenlik açığı değerlendirmeleriyle birlikte kullanıldığında bu durum gelişmiş analitiği desteklemek için "tehdit istihbarat beslemelerini" birleştirebiliyor.

Sonuç olarak, siber koruma ekipleri kritik sistemlere yönelik uygulanabilir saldırı yollarını ve saldırı vektörlerini önceden belirleyebiliyor. Daha sonra siber güvenlik risklerine karşı savunmak için önerilen azaltmalardan seçim yapabiliyor. Siber tehdit tahmin ve modelleme yazılımı ayrıca etkileşimli görselleştirmeler aracılığıyla gerçek zamanlı ve eyleme geçirilebilir bilgiler sağlayabiliyor. Bu, komutanlara gelişmiş siber durum farkındalığı sağlayarak ağ saldırı yüzeylerini azaltmalarına yardımcı oluyor. Ayrıca yanıtları önceliklendirmek için görev bağlamında teknik etkileri anlayabilmelerini de sağlıyor[8].

NATO müttefiklerinin 2024 yılında Washington'da düzenlenen NATO Zirvesi'nde ağ korumasını, durumsal farkındalığı ve siber alanın operasyonel alan olarak uygulanmasını geliştirmek amacıyla NATO Entegre Siber Savunma Merkezinin kurulması konusunda anlaştığı biliniyor[9].

Türünün ilk örneği olması beklenen Entegre Siber Savunma Merkezinin 2028 yılına kadar faaliyete geçirilmesi bekleniyor. Merkez, NATO'nun Belçika Mons'taki üyelerinden gelen personeli fiziksel olarak bir araya getirerek Avrupa Müttefik Kuvvetler Yüksek Komutanı'na (Supreme Allied Commander Europe -SACEUR) askeri operasyonlar için risk oluşturabilecek siber uzaydaki mevcut ve ortaya çıkabilecek tehditler konusunda kesintisiz görünürlük sağlayacak şekilde tasarlanıyor[10].

Türkiye'de Siber Saldırılar ve Gelecek Öngörüleri

Son bir yıl içinde Türkiye'de yaklaşık 1,7 milyon siber saldırı gerçekleştiği düşünülüyor. Özellikle sağlık sektörüne yönelik fidye amaçlı saldırılar dikkat çekiyor. Diyarbakır, Tekirdağ, Siirt ve Kocaeli'deki bazı hastanelerin fidye beklentisiyle siber saldırıya uğradığı biliniyor. Sağlık sektörüne yapılan bu saldırılar genellikle hastaneleri ve kritik tıbbi verileri hedef alıyor. Bu saldırılar hastaların hayatını tehlikeye atabiliyor[11].

Türkiye'de siber güvenlik alanında önemli projelere ve yerli ürünlere imza atan STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş.'nin (STM), Teknolojik Düşünce Merkezi ThinkTech tarafından 2024 Nisan-Mayıs-Haziran tarihlerini içeren yeni Siber Tehdit Durum Raporu yayınlandı. Siber güvenlik alanında farkındalık yaratmak amacıyla STM'nin siber güvenlik uzmanları tarafından hazırlanan raporda yedi ayrı konu başlığı bulunuyor. Raporda, deniz platformlarında siber güvenlik, silah sistemlerinin siber dayanıklılığını artırmak, QR kod tabanlı saldırılar ve güvenlik önlemleri gibi güncel ve ilginç konu başlıkları yer alıyor[6].

Türkiye'de faaliyet gösteren önemli siber güvenlik şirketlerinin aldığı yatırımlar da dikkat çekiyor. Türkiye'den çıkarak dünya çapında bir başarı hikâyesi yazan Picus siber güvenlik şirketi, otomatik sızma testi ve saldırı

8 https://www.riskaware.co.uk/insight/defence-cyber-threat-landscape/
9 https://www.nato.int/cps/en/natohq/topics_78170.htm
10 https://defensescoop.com/2024/07/10/nato-readies-to-launch-integrated-cyber-defense-center/
11 https://www.trtbelgesel.com.tr/bilim-teknoloji/maskelerin-ardinda/maskelerin-ardinda-10906480

simülasyonunu birleştiren yeni bir siber güvenlik kategorisini şekillendirmek için Riverwood Capital liderliğindeki küresel ölçekli yatırım turunu tamamladı. Türk siber güvenlik şirketi Picus, 45 milyon dolarlık yeni yatırımla ürün inovasyonunu güçlendirmeyi ve dünya genelindeki operasyonlarını genişletmeyi planlıyor[12].

Türkiye'nin siber kalesi Ulusal Siber Olaylara Müdahale Merkezinin (USOM) çalışmaları da kritik önem arz ediyor. USOM bünyesinde 2.300'e yakın Siber Olaylara Müdahale Ekibi (SOME), 7.859 uzman personel ve 400 Ulusal Siber Olaylara Müdahale Merkezi personeli bulunuyor. Merkezde anlık olarak 17 milyon IP adresi siber güvenlik zafiyetlerine karşı sürekli taranıyor. Merkez tarafından her gün 422 büyük saldırı, 11 milyon zararlı erişim isteği engellenebiliyor. Bu kapsamda 2023 yılında 140 bin büyük saldırının önüne geçildiği biliniyor[13].

Siber Güvenlik Başkanlığı

Türkiye siber tehditlere karşı savunmayı güçlendirmek amacıyla son olarak yeni bir Siber Güvenlik Başkanlığı kurdu. 8 Ocak 2025 tarihli Resmi Gazete'de yayımlanan Cumhurbaşkanlığı Kararnamesine[14] göre Siber Güvenlik Başkanlığı, siber güvenliği sağlamak amacıyla politika, strateji ve hedefler belirleyecek, eylem planları hazırlayacak ve siber güvenlik ile bilgi güvenliğini destekleyen projeler yürütecek. Siber güvenlik alanında kamu, özel sektör ve üniversiteler arasında işbirliğini artırmaya yönelik çalışmalar yürütecek olan Başkanlık, siber güvenlik ekosistemi ile yerli ve millî ürün ve teknolojilerin geliştirilmesine ve yerli girişimcilerin dünya pazarında rekabetçi konuma gelmesine yönelik çalışmalar da yürütecek[14].

Siber Saldırılar Gelecekte Nasıl Şekillenecek?

Siber saldırıların geleceğinin tahmin edilmesinin çok zor olduğu biliniyor. Sonuçta sektörün her yönü sürekli değişiyor. Siber tehditler gelişiyor ve onlara karşı savunma sağlayan araçlar da bu değişiklikleri yansıtıyor. Bu araçlar giderek karmaşıklaşan ağları daha iyi savunmak için kendi başlarına da gelişebiliyor. Bazı siber saldırı taktiklerinin kalıcı olmasının kaçınılmaz olduğu düşünülüyor. Bunun nedeni ise bu yöntemlerin işe yaradıklarının bilinmesinden kaynaklanıyor[15].

Yapay zekâ, siber suçluların yeteneklerini genişletmelerini sağlarken, siber tehditlere karşı mücadelede de güçlü bir araç olarak ortaya çıkıyor. Yapay zekânın tehdit algılama ve yanıtlama yetenekleri, siber güvenlik uygulamalarında devrim yaratıyor. Makine öğrenmesi algoritmaları, bir siber saldırıyı gösterebilecek kalıpları ve anormallikleri belirlemek için büyük miktarda veriyi analiz edebiliyor. Bu durum da yapay zekâyı siber saldırıların geleceğinde çok önemli bir yere koyuyor.

Kurumların, ortaya çıkan teknolojileri benimseyerek ve sürekli iyileştirme kültürünü destekleyerek siber saldırıların önünde kalması gerekiyor. Kapsamlı siber güvenlik stratejileri geliştirmede sektörler arası ve hükümet kurumlarıyla kurulacak işbirliğinin hayati önem taşıyacağı düşünülüyor[16].

Teknoloji gelişmeye devam ettikçe ve bilgi çağı ilerledikçe siber saldırıların artan oranla büyüyeceği tahmin ediliyor. Savunmadan sivil sektörlere kadar hemen hemen her alanda kullanılan akıllı cihazlar ve IoT teknolojileri siber güvenlik yaklaşımıyla donatılmadıkça güvenli bir alan yaratılması mümkün görünmüyor. Bu nedenle Avrupa Birliği tarafından 2022 yılında tasarlanan ve dijital öğelere sahip ürünler için siber güvenlik gerekliliklerine ilişkin bir düzenleme önerisi olan Siber Dayanıklılık Yasası, daha güvenli donanım ve yazılım ürünleri sağlamak için siber güvenlik kurallarını güçlendirmeyi vadediyor[17].

12 https://www.siberkume.org.tr/haber/976-turk-siber-guvenlik-devi-picus-security-45-milyon-dolarlik-yatirim-aldi
13 https://www.uab.gov.tr/haberler/turkiye-nin-siber-guvenlik-kalkani-usom
14 https://www.resmigazete.gov.tr/eskiler/2025/01/20250108-1.pdf
15 https://fieldeffect.com/blog/what-is-the-future-of-cyber-security
16 https://www.forbes.com/councils/forbestechcouncil/2024/07/11/the-future-of-cybersecurity-emerging-threats-and-how-to-combat-them/
17 https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

Sürekli inovasyon ve gelişen küresel trendlerin yakın takibiyle mücadele edilebilir gibi görünen siber tehditlerin gelecekte daha karmaşık hâle gelmesi kaçınılmazdır. Bu nedenle kurumlar ve bireyler kendilerini sürekli güncel teknolojilerle koruma altına almalı, gelişen tehditlere karşı proaktif stratejiler geliştirmelidir.