thinktech
STM Teknolojik Düşünce Merkezi

2021'de Bizi Bekleyen Siber Tehditler

COVID-19 şüphesiz ki bazı konularda hızlı yol alınmasını sağladı. Bu konuların başında da dijital dönüşüm geliyor. Yıllarca evden veya uzaktan çalışmaya direnen işyerleri bu süreçte çalışma şekillerini değiştirmek zorunda kaldı. Aynı şekilde eğitim kurumları da uzaktan eğitime geçerek teknolojinin nimetlerinden faydalanmaya başladı.

Ancak bu durum çeşitli sorunları da beraberinde getirdi. Altyapısı yeterli olmayan veya gerekli tedbirleri almayan kurumlar bu süreçte birçok siber tehditle burun buruna gelirken hâlihazırda sürekli artan siber tehditler bu açıklarla birlikte iyice yükselişe geçti. Savunma ne kadar gelişirse gelişsin, saldırganlar da yöntemlerini geliştirerek daha etkili hâle gelmeye başladı.

Siber Suçlar 6 Trilyon Dolarlık Hasara Neden Oldu

Cybersecurity Ventures'a göre, siber suçlar nedeniyle oluşan hasarın, 2021 yılı sonuna kadar yıllık 6 trilyon dolara ulaşacağı tahmin edilirken dünya çapında siber güvenlik harcamalarının 2022'de 133,7 milyar dolara ulaşması bekleniyor[1].

Bir veri ihlalinin ortalama maliyeti 3,86 milyon dolar olurken bildirilen olayların yüzde 63'ü dikkatsiz veya ihmalkâr çalışanlardan kaynaklı oldu. Özellikle sağlığın ön planda olduğu pandemi sürecinde bu alandaki siber suçlar daha büyük yaralara yol açtı.

Sağlık hizmetleri, siber tehditlerden etkilenen en pahalı sektör olarak öne çıkarken verilen hasarın 7,13 milyon dolara kadar çıktığı tahmin ediliyor[2].

Siber güvenlik riskleri, küresel şirketler için 2021 yılında da tehdit olmaya devam ediyor. Trend Micro tarafından yapılan bir ankete göre katılımcıların neredeyse dörtte biri (yüzde 23), 2020 yılında kurumlarının ağ veya sistemlerinin yedi veya daha fazla saldırıya uğradığını belirtti[3].

Sağlık Sektörü de Hedefte

Sağlık alanındaki siber saldırılar ne yazık ki sadece maddi kayıplarla sonlanmıyor. Almanya Düsseldorf'taki bir hastanede siber saldırılar nedeniyle sistemler çökünce bir hasta hayatını kaybetti ve cinayet soruşturması

1 https://www.cyber-observer.com/cyber-news-29-statistics-for-2020-cyber-observer/
2 https://www.businessnhmagazine.com/article/2020-in-20-cyber-security-figures
3 https://www.forbes.com/sites/guidehouse/2021/01/08/cybersecurity-threats-remain-a-concern-for-global-corporations/?sh=34f87a9d8343

başlatıldı. Bu bir kovuşturmaya yol açarsa, siber saldırının doğrudan sonucu olarak birinin öldüğü ilk dava olacak.

Ayrıca içinden geçtiğimiz süreçte, hastanelere ve sağlık tesislerine yönelik saldırılar devam ederken, fidye yazılımları üniversiteler ve liseler de dahil olmak üzere eğitim sektörünü hedef aldı. Bununla da kalmayan saldırganlar aşılamadaki soğuk tedarik zincirini hedef alan saldırılar gerçekleştirdi[4].

142 Milyondan Fazla Müşterinin Verisi Çalındı

2020 yılında irili ufaklı pek çok şirket siber tehditlerle uğraşmak zorunda kaldı. Ancak aralarından bazıları çok ses getirdi. 2020'nin ilk altı ayında, hacker'lar, dark web'de birçok Fortune 500 şirketinin finansal kayıtlarına, hesap bilgilerine, hassas gizli verilerine erişebildi ve bunları sattı.

Pandemi sürecinde en büyük veri ihlallerine bakıldığında ilk sırada MGM Resorts müşterilerinin verilerinin çalınması yer aldı. 2020 yılının Şubat ayında gerçekleşen olayda 142 milyondan fazla otel müşterisinin verilerine erişen hacker, bu bilgileri satılığa da çıkarmıştı[5].

Bir başka veri hırsızlığı olayı 2020'nin Mayıs ayında havayolu şirketi EasyJet'in başına geldi. 9 milyon müşterisinin kişisel verileri ve 2.000 kredi kartının detaylarını hacker'lara kaptıran havayolu şirketi, son derece gelişmiş bir saldırıya uğradıklarını açıklamıştı[6].

500 Binden Fazla Kullanıcının Şifreleri Çalındı

Siber suçlara maruz kalınan durumlara bakılınca, olayların sıklıkla zayıf ve yaygın kullanılan giriş bilgileriyle ilgili olduğu görülüyor. Özellikle güvenlik düzeyi yüksek işlemlerde, hassas bilgilere erişimin olduğu durumlarda kalıcı hasarlar almamak için şifrelerimizin güvenliğini sorgulayan destek yazılımlar bulunuyor. Eğer kullandığımız şifre sızmış ve bu şifrenin kullanıldığı hesaplarımız yabancı klavyelerin eline geçmişse, sistem düzenli yaptığı tarama ile uyarı verebiliyor[7].

Veri hırsızlıklarından pandemide yükselen markalar da nasibini aldı. 2020'nin belki de en çok konuşulan markalarından biri olan Zoom'da, Nisan 2020 tarihinde gerçekleşen ihlaller sonucu 500.000'den fazla kullanıcının şifreleri çalındı. Suçlular ele geçirdikleri hesapları dark web'de satarak, gerçek kullanıcılar yerine görüşmeler yapmak isteyenlere verdiler.

Güvenlik uzmanları ise bu mecralardaki siber saldırıların takip edilmesinin zor olduğunu, hızlı gelişen bu tip canlı saldırılara karşı Zoom ve sektördeki diğer popüler uygulamaların daha alacak yolları olduğunu belirtiyor[8].

Bu örnekler sadece dikkat çekenler. STM'nin 2020 yılı boyunca CyThreat Siber İstihbarat Portalı üzerinden paylaştığı verilere göre, IP kara liste verileri olarak bu sene içinde 120.000'in üzerinde paylaşımda bulunulurken bunun 36.0000'den fazlası botnet trafiğine dahil olan IP'ler olarak tespit edildi. 16.000'e yakını ise oltalama saldırılarında kullanıldı. 12.000 civarındaki IP ise C&C olarak etiketlendi. Hash kara liste verileri ise 8,5 milyona yakın örnekle müşterilere ulaştı.

Ayrıca alan adı kara liste verileri sene sonuna doğru 680.000 civarı bir adet ile artan bir eğilim gösterirken 260.000 adet alan adının Malware operasyonlarında kullanıldığı tespit edildi. 260.000'e yakın alan adının zararlı yazılımlarla silahlandırıldığı da notlar arasında. Pandemi sürerken 12.000'in üzerinde alan adı COVID-19 temalı

4 https://techhq.com/2020/12/six-cybersecurity-trends-heading-our-way-in-2021/
5 https://zd.net/2MasaKU
6 https://www.forbes.com/sites/thomasbrewster/2020/05/19/easyjet-hacked-9-million-customers-and-2000-credit-cards-hit/?sh=55f5159b1ae1
7 https://www.infosecurity-magazine.com/blogs/credential-stuffing-recent-attacks/
8 https://em360tech.com/top-10/top-10-cybersecurity-incidents-happened-2020

saldırılarda kullanıldı. Alan adlarındaki sene boyunca süren artma eğiliminde ise pandeminin etkisiyle hızlanan dijitalleşmenin payı olduğu düşünülüyor[9].

İç Tehditlere Dikkat

Herkesin gözü önünde olan bu büyük şirketler bile zaman zaman siber suçlara karşı bir şey yapamadı ve verilerini çaldırdı. İçinde olduğumuz dönemde şirketlerin çok daha fazla önlem alması ve sadece dış değil, iç tehditlere de odaklanması gerekiyor. Çünkü ortaya çıkan ihlallerin büyük bir kısmı kurumiçi çalışanlar veya üçüncü partiler nedeniyle oluyor.

COVID-19 krizinin bir sonucu olarak, evden ve uzaktan çalışma yaygınlaştıkça bağlantılı cihazlarda da büyük bir artış yaşanıyor. Bu da, merkezi veri ve altyapılarla ilişkili risklerin sayısını ve birden çok erişim noktası etrafındaki güvenlik açıklarını artırıyor. 2021'de ise siber güvenliğin sağlanmasının çok daha zor olacağı düşünülüyor. Bunda saldırı yüzeyinin genişlemesi ve güvenlik ve veri politikalarını uygulayıp kontrol etmek için uygun ortam olmaması öne çıkıyor.

2021'de Bizi Neler Bekliyor?

Gerek gelişen teknoloji, gerek yaygınlaşan dijitalleşme siber suçlular için büyük bir oyun alanı yaratıyor. 2020'de artan siber suçlar düşünüldüğünde 2021 yılında da benzer olayları görmek olası. Bu nedenle nelerle karşılaşılabileceğinin öngörülmesi ve önlemler alınması için hazırlık yapmak gerekiyor.

Uzmanlara göre 2021'de karşılaşılacak siber tehditlerden biri "Deepfake". Deepfake, kamera görüntülerindeki kişilerin görüntülerinin yapay sinir ağları aracılığıyla kısmen veya tamamen değiştirilebileceği ortam türünü tanımlamak için kullanılıyor. Bu şekilde fotoğraf veya videolardaki kişiler başkalarıyla değiştirilebiliyor.

Özellikle pandemi döneminde eskisine nazaran büyük bir artış gösteren görüntülü toplantılar da hacker'ların ekmeğine yağ sürüyor. Deepfake ile kötü niyetli kişiler, herhangi bir şirket yöneticisinin, liderin yerini alabilir ve şirket, kurum hakkında birçok gizli bilgiyi öğrenebilir veya diğer çalışanların kimliklerini taklit ederek dolandırabilir. Bu nedenle, Deepfake, özellikle kurumsal alanda 2021'in en önemli siber güvenlik açıklarından biri olarak görülüyor[10].

Siber tehditler sadece kurumsal dünyayı kapsamıyor. Siber güvenlik, Dünya Ekonomik Forumu (WEF) tarafından havacılık endüstrisinin karşı karşıya olduğu en büyük sorunlardan biri olarak öne çıkıyor. Şu anda maruz kalınan ekonomik ve operasyonel etkiler, bu sektörün özellikle önümüzdeki aylarda risk altında olacağı anlamına geliyor.

Havacılığa yönelik en olası tehditler arasında kimlik avı girişimleri, veri ihlalleri ve fidye yazılımı yer alıyor. Siber güvenlik, her ne kadar yönetim kurulları tarafından ciddiye alınsa da, havacılık işletmelerinin siber savunma konusunda dikkatli olması gerekiyor[4].

Dünyada daha fazla bölge daha yüksek internet hızına ve 5G ağ bağlantısına eriştikçe sektör büyüyecek ve bu yeni yüksek hızlı ağdan yararlanmak için pazarda çok sayıda yeni IoT cihazı olacak. Bununla beraber son yıllarda IoT cihazlarının güvenlik ve mahremiyeti için yeterli testler yapılmadan piyasaya sürülmelerine bağlı olarak pek çok sorunla karşılaşılıyor.

9 https://thinktech.stm.com.tr/detay.aspx?id=400
10 https://krontech.com/cyber-security-trends-to-watch-out-for-in-2021

İşletmelerin pazar payı kapmak için attığı bu adımlar nedeniyle sorunun daha da büyümesi bekleniyor. IoT cihazlarındaki zaaflar da siber saldırganların iştahını kabartıyor[11].

Bulut teknolojileri özellikle evden veya uzaktan çalışıldığında pek çok kurum için kurtarıcı oldu. Ancak aynı zamanda önemli bir güvenlik açığı oluşturdu. Buluta geçiş, ekiplerin yeni güvenlik becerilerini öğrenmesini gerektiriyor. Bunun yapılamaması, siber suçlara davet oluyor. Kimlik ve erişim yönetimi (IAM) ve hatalı hizmet yapılandırmaları, genellikle kötüye kullanılabilen güvenlik açıklarına neden oluyor[12].

Siber saldırılar telefonlarımızı, dijital cüzdanlarımızı da hedef alıyor. Dijital cüzdanlara dijital para birimleri de dahil. Özellikle Bitcoin son yıllarda yükselişini sürdürürken salgın ve artan işsizlik sonucunda yavaşlayan veya duran sektörler, dijital para birimlerini giderek daha popüler hâle getirdi. Tüm bu gelişmeler dijital cüzdanları siber saldırganların öncelikli hedeflerinden biri hâline getirdi[13]. Fotoğraflar, finansal işlemler, e-postalar ve mesajların aslında hepsi birer tehdit. Akıllı telefonlara giren virüsler veya kötü amaçlı yazılımlar, 2021'de dikkat çeken konulardan olacak.

Öte yandan herkesi ilgilendiren aşı konusunda da siber saldırıların artacağı öngörülüyor. Sağlık sektöründe güvenlik hiç olmadığı kadar zorlanabilir. STM'nin yaptığı analize göre 2021'de fidye amaçlı saldırılar da artacak. Bu tip saldırılardan en az kayıpla kurtulabilmek için güvenli bir bulut sistemi ve VPN kullanmakta yarar görülüyor[9].

Siber Tehditlerden Nasıl Korunmalı?
Sistemdeki güvenlik açıklarını ortadan kaldırmak için yazılımları güncel tutmak gerekiyor. En son güvenlik önlemlerinden yararlanmak için yazılımın güncel olduğundan emin olmak hatta mümkünse otomatik güncelleme seçeneğini tercih etmek öneriliyor.

Olmazsa olmaz önlemlerden biri de antivirüs programları kullanmak. Virüs ve kötü amaçlı yazılımlara, kimlik avına ve diğer çevrimiçi ve çevrimdışı tehdit türlerine karşı savaşta hayat kurtarıcı olan bu yazılımlar cihazları çok katmanlı bir şekilde koruyabiliyor.

Her ne kadar güncel yazılımlar ve güçlü antivirüs programı geliştirilse de, nihayetinde bu araçları insanlar kullanıyor. Personeli eğitmek, çalışanların temel güvenlik uygulamalarını öğrenmeleri ve kuruluş genelinde bir bilgi teknolojileri güvenlik kültürü oluşturmak pek çok siber tehdidi bertaraf edebilir.

Çalışanların dikkat etmesi gereken en önemli konulardan biri, şüpheli bir mesaj veya onlara bir bağlantıyı tıklamalarını söyleyen e-postalar geldiğinde göndereni her zaman kontrol etmektir. Şüphe durumunda mesajı silip şirketin ilgili birimine bildirmek gerekir[14].

11 https://www.globallearningsystems.com/cybersecurity-outlook/
12 https://www.forbes.com/sites/forbestechcouncil/2021/01/21/cybersecurity-trends-for-2021-five-predictions-for-executives-to-watch-out-for-in-the-new-year/?sh=33de17a6764b
13 https://www.simplilearn.com/top-cybersecurity-trends-article
14 https://www.business2community.com/cybersecurity/cybersecurity-trends-to-watch-out-for-in-2021-02378676