thinktech
STM Teknolojik Düşünce Merkezi

2020'de Etkili Olacak 8 Siber Güvenlik Tehdidi

Yoğun siber güvenlik olaylarıyla geçen 2019'un ardından 2020 yılı da benzer endişeleri beraberinde getiriyor. Mobil cihazlar, dizüstü bilgisayarlar ve bulut teknolojisi herkes için her yerde ve anlık erişime olanak sağlasa da önemli bir risk unsuru olmaya devam ediyor. Yaygın güvenlik tehditleri ve sorunları yüzünden tüm dünyada ciddi sıkıntılar ve maddi kayıplar yaşanıyor.

Siber güvenlik; gizliliğimizi, haklarımızı, özgürlüklerimizi ve fiziksel güvenliğimizi korumaya devam ediyor. Hayatımızın birçok alanında bizi koruyan siber güvenliğin rolünün 2020'de daha da artacağı düşünülüyor. Kişisel bilgilerin sızmasını içeren ihlaller her geçen gün büyürken siyasi müdahaleler ve devlet onaylı siber saldırılar konusunda da artan bir trend ortaya çıkıyor[1].

Microsoft'un verilerine göre bir veri ihlalinin şirkete maliyetinin 4 milyon dolar olduğu günümüzde; siber güvenlik, bir opsiyondan çok operasyonal gereklilik haline geliyor. Microsoft siber suçlarla savaşmak için yıllık 1 milyar dolar bütçe harcıyor. Her ay e-dolandırıcılık ve kötü amaçlı yazılımların tespiti için 470 milyon e-posta taranırken 1.2 milyar cihazın güvenliği sağlanmaya çalışılıyor.[2]

Kasım ayında Amerika Birleşik Devletleri'nde (ABD) yapılacak seçimler, Tokyo'da düzenlenecek olimpiyatlar, çeşitli jeopolitik gerilimler, ekonomik belirsizlikler ve endüstride artan rekabet dijitalleşmeye katkıda bulunarak 2020'de siber saldırıların da artacağına işaret ediyor. Uzmanlar bu artışta özellikle yapay zekâ ve makine öğrenmesi destekli siber savunma araçlarının kullanılacağı üzerinde duruyor. Bu kapsamda 2020 yılında etkili olabilecek 8 önemli siber güvenlik riski göze çarpıyor.

- **1. Teknolojinin Küresel Kutuplaşması**
  Teknoloji küresel ölçekte geliştikçe ülkelerin siyasi ve stratejik yaklaşımları küresel internet, mobil cihazlar ve teknolojinin kullanımının farklı şekilde uygulanmasına ve farklı dijital çevreler oluşmasına neden oluyor. Teknolojinin kutuplaşması, Huawei'nin yazılımını kullanan cihazların hedef alındığı ve Android ile Microsoft cihazların etkilenmediği gibi örnek durumlarda avantaj sağlayabilse de, belirli bölge ve şirketlerde bulunan insanlar için çok büyük bir risk yaratıyor. Kutuplaşan teknoloji hedef alındığında insanların bilgi güvenliği sağlanamazken diğer yandan bölgelere özel sansür veya kanunsal yaptırımlara maruz kalınabiliyor[3].

1 https://www.forbes.com/sites/bernardmarr/2020/01/10/the-5-biggest-cybersecurity-trends-in-2020-everyone-should-know-about/#14d300727ecc
2 https://news.microsoft.com/apac/2019/12/03/the-state-of-cybersecurity-in-2020-five-key-trends/
3 https://www.boozallen.com/c/insight/publication/top-9-cybersecurity-trends-for-2020.html?cid=CyberTrends-ci-e-launch

2019 yılında ABD'nin Çin firması olan Huawei'yi kara listeye alması firmanın zor zamanlar geçirmesine neden olurken, karşılığında küresel ölçekte Çin teknolojilerinin ABD'ye tercih edilme olasığı ise teknolojinin küresel kutuplaşmasının ülkelerin ekonomilerini nasıl etkileyeceğine önemli bir örnek olabilir[4].

- **2. Kusurlu Bileşenler: Klonlar ve Taklitler**
  Elektronik bileşenlerin pazarındaki genişleme ve taleplerde yaşanan artışlar taklitlerin ve klonların da artmasına neden oluyor. Bu yolla üzerinde oynanmış veya kusurlu üretilmiş bileşenler organizasyonların tedarik zincirine sızarak risk oluşturabiliyor[2].

- **3. Siber Saldırılar Araçları Hedef Alıyor**
  Dünya genelinde 330 milyon araç birbirine bağlı ve iletişim halinde olan IoT sistemlerle kullanılıyor. 2020 yılında ABD pazarında sadece birbiriyle bağlı sistem kullanan araçların satılacağı biliniyor. Her türlü akıllı mobil sistemin siber saldırılardan etkilenmesi otomotiv firmalarını, yedek parça üreticilerini, hatta tüketiciler de dahil herkesi olumsuz etkiliyor. Gerçekleşen risklerin başında araç hırsızlıkları, araç sistemlerinin kontrolünün kaybı ve özel verilerin çalınması geliyor. Gelecekte araçların giderek daha bağlantılı ve akıllı sistemler kullanacağı düşünüldüğünde siber güvenlik tehditlerinin de bu alanda artması olası görülüyor[5].

- **4. Drone'lar Ağlara Sızmak için Kullanılıyor**
  Drone'lar bir süredir siber saldırılarda aktif olarak kullanılıyor. 30 dolardan 10.000 dolara kadar çeşitliliği bulunan hava araçları birçok farklı saldırı biçiminde tercih ediliyor. Düşük maliyetli ve kolay kullanımlı drone'lar ağların kullanılmaz hale getirilmesine veya hack'lenmesine yardımcı olabiliyor. Bir işyerinin yakınında Wi-Fi bağlantı noktası olarak yerleştirilip ağ güvenliğini tehdit eden veya bir ofisin bilgisayarlarının uzaktan hack'lenmesinde de aracı olarak bilgilerin çalınmasında kullanılan drone'ların doğru önlemler alınmazsa yaygınlaşan kullanımlarıyla artan bir risk unsuru olmaya devam edecekleri öngörülüyor[6].

- **5. Dünya, Uzay ve İnternet İçin Uyduların Geleceği**
  Günümüz uyduları sadece uzay programlarında değil, askeri ve sivil alanlarda da iletişimde kritik altyapıyı oluşturuyor. Uydular zamanın, navigasyonun, konumun ve iletişimin kusursuzlaşmasını sağlıyor. Uydulara yapılacak bir siber saldırı ise en tehlikeli risklerden birini oluşturuyor.

  Uyduların bağlantılı olduğu yer kontrol sistemleri, kolay erişim imkânları sebebiyle siber saldırıların en önemli hedefi olarak görülüyor. 2018 yılında NASA'nın Jet İtici Laboratuvarlarına gerçekleşen siber saldırı, yer sistemlerinin zayıflığını ortaya koymuştu. Siber saldırıların uyduları hedef alması, kontrollerinin kaybedilmesi veya kötü amaçla kullanılması birçok teknolojik alanda ciddi zararlara yol açabilir.

- **6. "Gelişmiş Kalıcı Tehditler"in (APT) Birbirine Benzeme Riski**
  2020'de siber saldırıların niteliğinin belirlenmesi ciddi ölçüde zorlaşabilir. Siber saldırılarda kullanılan APT'ler yazılımsal anlamda birbirine benzerlik gösterdikçe ülkelerin ve kötü niyetli korsanların birbirini hack'leyerek rakip ülke veya organizasyonların yazılımlarına benzerlik gösteren izler bırakması saldırının nitelenmesini zorlaştırıyor. APT'lerin benzerliği arttıkça kaynağın belirlenmesinin zorlaşması, savunma ve karşı saldırı imkânlarını da olumsuz yönde etkiliyor[2].

- **7. Dijital Seçimlere Müdahale Riski**
  Elektronik oylama sistemlerine yapılacak siber saldırılar 2020'de seçim sonuçlarının etkilenmesine sebep olabilir. Özellikle ABD'de Kasım ayında gerçekleşecek başkanlık seçimlerinde diğer ülkelerin seçim

4 https://www.ft.com/content/0ed49b84-91c1-11e9-8ff4-699df1c62544
5 https://www.helpnetsecurity.com/2020/01/06/automotive-cybersecurity-incidents/
6 https://threatpost.com/drones-breach-cyberdefenses/143075/

sonuçlarını etkileyebilecek saldırılar düzenleme olasılığı endişe veriyor. Seçim güvenliğini sağlamak için geçtiğimiz Aralık ayında 425 milyon dolarlık ek bütçe yaratan ABD Kongresi, 2020 yılında seçim harcamalarının 1.4 trilyon dolara ulaşacağını belirtiyor[7].

- **8. Ulus Devletler 2020 Olimpiyatlarına Müdahale Etmeye Hazırlanıyor**
  2020'de Japonya'da gerçekleşecek olimpiyatların güvenliği de olası siber saldırı tehdidi ile karşı karşıya. Japonya'nın Kamu Güvenliği İstihbarat Ajansı (PSIA) olimpiyat görevlilerince gönderilmiş gibi gösterilen bazı e-dolandırıcılık ve hack'leme e-postalarını tespit ettiğini açıklayarak riske dikkat çekiyor. Her ne kadar yapılan tespitler şimdilik saldırıların arkasında kim veya kimlerin olduğunu göstermese de bu denemelerin arkasında Çin'in olabileceği düşünülüyor. Ancak farklı grupların saldırıları, Çin yapmış gibi göstererek hedef saptırması da olasılıklar arasında görülüyor.

  2016 yılında Rio'da yaşanan DDoS saldırısı ve 2018 yılında Seul'de olimpiyatların ilk gününde bütün bilgi sistemlerini kullanılmaz hale getiren "Olimpik Yok Edici" adlı saldırı, oyunların gidişatına ciddi zararlar vermişti. Doping suçlamalarıyla dört yıl boyunca olimpiyatlardan sınırlama alan Rusya'nın desteklediği bazı hacker gruplarının ise Anti Doping Ajanslarına düzenlediği saldırılar, 2020 olimpiyatlarının hedef alınma olasılığını artırıyor[8].

2020 Siber Saldırı Trendlerini Artıran Etkenler

2020 yılında siber saldırılarda görülen çeşitliliğin artışında etkin rol oynayan bazı unsurlar bulunuyor. Bunlardan ilki olan yapay zekâ, saldırıların gerçekleşme şekilleri, zamanları ve ihtimallerini analiz ederek bir savunma oluştururken tersi durumda karşı strateji olarak saldırı niyetlerini de gizleyebiliyor. Yapay zekâ yaygınlaşarak herkesin kullanımına açıldıkça kredi kartı bilgilerinin çalınabildiği e-postaların niyetini gizleyen veya diğer kişisel bilgilerin çalınmasına neden olan saldırılara karşı savunmamız da zayıflıyor.

Doğu ve Batı arasında yaşanan politik ve ekonomik kutuplaşmalar da siber güvenlik tehditlerinin trendlerini artırıyor. İnternetin bağımsız ve özgür bir ortam olarak ortaya çıkışından sonra her geçen gün artan siber saldırı olasılıkları ülkeleri bağımsız ve izole internet altyapıları kurmaya yöneltiyor. Rusya'nın 2020 yılı içinde test ettiğini açıkladığı bağlantısız internet sadece ülke içinde hiçbir dış kaynağa bağlanmadan çalışan bir ağ sistemi olarak bu duruma örnek gösterilebilir. Ülkeler ve kültürler arası yaşanan kutuplaşmalarla getirilen sınırlama ve yeni düzenlemelerin kötü niyetli kullanıcıları cesaretlendirmesinden endişe duyuluyor.

Hedefli dezenformasyon saldırıları, seçimler gibi ülkelerin iç politikalarına yapılan dijital müdahaleler ve sosyal medyanın saldırı aracı olarak kullanılması da siber saldırı trendlerinin artışında rol oynuyor.

Siber güvenlik sektörünün giderek büyümesiyle duyulan istihdam ihtiyacının karşılanamaması ise siber saldırı trendlerini güçlendiren bir diğer alan olarak öne çıkıyor.

2014 yılında yaklaşık 1 milyon boş siber güvenlik çalışanı pozisyonu bulunurken 2020 yılında bu sayının 3.5 milyona çıktığı görülüyor. Saldırıları gerçekleştiren tarafta sayılar artarken savunan tarafta aynı oranda bir artış gerçekleşmezse iki kutup arasında açılan uçurumun siber saldırıları güçlendireceği öngörülüyor[1].

Siber Saldırı Tehditlerine Nasıl Yaklaşılmalı?

Son yıllarda rekabeti artırmak için dijital dönüşüme büyük yatırım yapılıyor. Bu dönüşüm operasyonel verimliliği ve pazar payını arttırmak gibi pek çok önemli avantaj sağlarken sektörlerde yaşanan dijital dönüşüm birçok güvenlik açığını da beraberinde getiriyor.

7 https://www.theguardian.com/us-news/2020/jan/02/elections-2020-cyber-attacks-democrats-experts
8 https://www.cpomagazine.com/cyber-security/state-backed-cyber-attacks-expected-at-tokyo-2020-games/

Bu nedenle dönüşümü başlatan şirketlerin kullandığı mobil, IoT, bulut vb. bütün sistemlerin siber güvenliğinin bir bütün olarak ele alınması ve kapsamlı planlanması önem kazanıyor. Karşılaşacakları siber saldırı tehditlerini iyi bir şekilde analiz eden şirketlerin çeşitliliği artan saldırılara karşı gelebilecek savunmayı oluşturma ihtimali daha yüksek görülüyor. Bunun yanı sıra ülkelerin yapacağı hızlı yapısal reformlar ve siber güvenlik politikaları da tehditlere karşı atılacak adımların başında geliyor[2].