thinktech
STM Teknolojik Düşünce Merkezi

E-hırsıza e-kilit dayanır mı?

Bugün hemen hemen hepimizin çifte vatandaşlığı var; nefes aldığımız gerçek dünya ve tabiri yerindeyse e-dünya. İlkinde kendimizi koruma yöntemlerini biliyoruz; köpeklerimiz, alarm sistemlerimiz, kasalarımız bizi güvende tutuyor. Peki ya diğer taraf?

İnternet, deyim yerindeyse "küresel" sıfatının tanımı; devleti, kökeni yok. Bireyler, kurumlar, devletler işlerini yürütmek için neredeyse ona bağımlı. Bu tek taraflı bir ilişki değil elbet. O tüm olanaklarını bize bilgisayar ya da telefon ekranı aracılığıyla bonkörce sunarken biz de bilgilerimizi, fotoğraflarımızı, anılarımızı onu kullanarak paylaşıyoruz ya da depoluyoruz. Ancak dijital dünya pek o kadar da tekin bir mecra değil. İngiltere'de hastaneleri, Almanya'nın, Fransa'nın demiryollarını bloke eden siber saldırılar Avusturya'daki bir otelin manyetik kapı kartlarına kadar ulaşabiliyor. Hillary Clinton'un seçim kampanyası, arama motoru Yahoo, finans devi Citigroup, teknoloji firması Sony kötü niyetli bir saldırının hedefi olabiliyor. Siz neden olmayasınız?

Güne şöyle bir mesajla uyandığınızı düşünün: "Günaydın, bu e-postayı almanızın sebebi devlet veri tabanına karşı yapılmış talihsiz bir siber saldırı neticesinde kişisel verilerinizin çalınmış olma ihtimaline karşı sizi bilgilendirmektir." ABD Hükümet İş Konseyi'nin (Government Business Council -GBC) yayınladığı "Cesur Yeni Bir Dünya İnşası" adlı rapor, 2015 yılının Haziran ayında, yaklaşık 21 milyon Amerikan vatandaşının benzer bir durumu yaşadığına dikkat çekiyor. Kamu çalışanlarının bilgilerini tutan Office of Personnel Management (OPM) bir siber saldırıya uğramış ve bunun sonucunda 21 milyondan fazla kişinin verileri ele geçirilmişti.

Bu olay, ABD tarihinde yaşanmış en vahim siber saldırılardan biri olarak tarihe geçti. OPM direktörü istifa etti. Tabii ki yetmedi, hükümet kurumsal verileri koruma çabasını iki katına çıkaracağını açıkladı. Aslında çözüm netti; siber güvenlik mevzuatı yeniden düzenlenmeli ve kelime yerindeyse bir reform yapılmalıydı. Devletin farklı birimlerinde görev yapan teknoloji uzmanlarının görüşlerini içeren GBC raporu, siber güvenlik alanında yapılması gereken modernizasyona kılavuz olma özelliği taşıyor.

2017 yılının Ekim ayında yayınlanan bu rapora göre önemli olan, internetin hızını kısmadan gelişime ve yeniliklere açık olarak bu modernizasyonu gerçekleştirebilmekti. Çünkü aşırı tedbirler almak kısa vadede güvenli bir alan sağlasa da gündelik hayatı felce uğratmaktan öteye gidemeyecekti.

Amerikan Ulusal Güvenlik Ajansı Sekreter Yardımcısı Sally Holcomb, internet güvenliğini sağlamak ve içeriden gelen tehditleri tespit etmek için agresif bir biçimde çalıştıklarını söylüyor: "Amaç ülkenin bilişim altyapısını korurken kötü niyetli yazılımların bir adım ötesinde olabilmek, güvenlik sistemini de bir adım daha ötede konumlayabilmek. Yani siber saldırılara karşı verilen savaş aslında birkaç cepheden oluşuyor." Bu süreçte yaşadıkları en büyük sıkıntının internet kullanım hızı olduğunu da dile getiriyor.

İçeriden ya da dışarıdan gelen tehditlerin hep aynı kaldığının, asıl değişimin yeni teknolojilerin sağladığı olanaklarda barındığının altını çizen Holcomb, siber savunma taktiklerinin sonsuz bir yenilenme potansiyeline sahip olması gerektiğini ifade ediyor; "Tehdit hep olacak, sadece ona karşı kullandığımız teknolojiler gelişecek."

Proaktif Strateji

Burada önemli olan internet güvenliği ve internet hızı arasında düzgün bir denge kurabilmek. Bu dengeyi siber uzayda sallanan bir sarkacı merkezde tutma çabasına benzetebilirsiniz, bir yandan tehditler bertaraf edilirken öte yandan sistem de yavaşlamamalı.

ABD Adalet Bakanlığından Melinda Rogers siber saldırıların her geçen gün daha sofistike bir hal aldığını ve sıklaştığını söylüyor: "Bizim hedefimiz güvenlik açıklarını en aza indirmek ve mevcut tehditlere karşı eş zamanlı cevap verebilmek. Bunu sağlamak için de belirli araçlara, yeni teknolojilere ve insan kaynağına yatırım yapıyoruz. Stratejimiz proaktif olup siber bir saldırıya henüz oluşum aşamasındayken müdahale edebilmek."

ABD Savunma Bakanlığının siber stratejisi de diğerlerinden pek farklı değil; internet ağları, veri güvenliği ve askeri taktiksel hedeflerin korunmasını içeren üç ayaklı bu formül siber uzayda ABD'nin çıkarlarını kollamaya yönelik olarak geliştirilmiş. ABD 24. Hava Kuvvetleri sözcüsü, ilk savunma amaçlarının delinemeyecek bir ağ sistemi yaratmak olduğunu söylüyor: "Savunma sistemlerimiz AFNet'i (Hava Kuvvetleri Özel İnternet Ağı) yılda 1.5 milyar zararlı saldırıdan koruyor. Bununla birlikte özel olarak görevlendirdiğimiz hava kuvvetlerine bağlı bir birim olan "Cyber Airmen" gözden kaçmış olabilecek tehditleri sürekli olarak izleyip etkisiz hale getirmeye çalışıyor. Bu çok yönlü siber güvenlik sistemi bize tehditlerin erken tespiti ve engellenmesi konusunda büyük avantaj sağlıyor."

Sally Holcomb'a göre siber saldırılara karşı geliştirilen savunma sistemlerinin en büyük açığı bir standardizasyonunun olmaması, başka bir deyişle her çözüm üreticisine göre değişiklik sergilemesi. Bireysel kullanıcıyı kötü yazılımlardan koruyan bir anti virüs programı, devlet istihbarat kanallarına uygulanmaya çalışıldığında aynı başarıyı yakalayamıyor.

GBC'nin "Cesur Yeni Bir Dünya İnşası" isimli raporu devletlerin siber tehditlere karşı bugünün savaşını verirken yarın için de savaşmak durumunda olduğunun net bir şekilde altını çiziyor. Ancak siber güvenlik sadece devletlerin meselesi değil. Sadece işler ters gittiğinde önemsenecek bir konu hiç değil. Şirketlerde IT departmanının alanıymış gibi algılanması da büyük bir hata çünkü neticesi, tahribat gücü aslında bir yangın ya da deprem kadar reel. Dolayısıyla bir yangın tatbikatı ne kadar sıradansa bir siber saldırı tatbikatı da en az onun kadar sıradan olmalı.