thinktech
STM Teknolojik Düşünce Merkezi

Veriyi Silahlandırmak

Yaklaşık 10- 15 yıldır kişisel bilgilerimizi, bizim için önemli olan fotoğrafları, şifreleri, cüzdanlarımız ya da belki kasalarımız yerine telefonlarımızda ve bilgisayarlarımızda biriktiriyoruz. Bilgisayarlar da onları bulut adı verilen sanal depolarda saklıyor. Yani fiziksel anlamda güvenliğinden emin olmadığımız hatta deyim yerindeyse fiziksel varlığı olmayan bir yerlerde en özelimiz saklı.

Kolay erişim imkânı, tasarruf, hız, zamanın ruhu... Kişileri, kurumları hatta devletleri bu yeni saklama alanlarına yönelten sayısız sebep mevcut. Ancak kendi elimizle yarattığımız teknoloji bizi hedef almaya başladı. Son 10 yılda yaşanan siber saldırılar ciddi ivme kazandı, kazanıyor.

Dünyaca ünlü bir siber güvenlik uzmanı olan Kaspersky CEO'su Eugene Kaspersky, 20 yıl önce anti virüs şirketlerinin neredeyse virüs avında olduğunu söylüyor: "Sayısı çok azdı, bir ayda belki 10, bilemedin 15 virüsle karşılaşıyordunuz. Bu ufak rakamlardan bugün ayda milyonlarca farklı saldırı seviyesine ulaştık."

Rusya'nın, ABD gibi siber güvenliğe ciddi miktarda yatırım yapan bir ülkenin seçimlerine siber müdahalede bulunduğuna dair iddialar siber saldırıları dünyanın gündemine tekrar taşıdı. Daha önce İran'a, Ukrayna'ya, Kuzey Kore'ye ve başka birçok ülkeye yapılan saldırılar ciddi neticeler doğurmuştu; elektrik kesintileri, internet erişim engelleri, kişisel veri hırsızlıkları hatırı sayılır ölçüde zarar vermişti. Ancak deyim yerindeyse dünyanın batı ve doğudaki bu iki kutbunun arasında yaşanan böylesine büyük ve sansasyonel bir siber saldırı hepsinden çok dikkat çekti.

Rusya bu saldırıyı reddetti ve bu tavrından hâlâ taviz vermiş değil. CIA Başkanı Mike Pompeo ise bundan birkaç ay önce BBC'ye verdiği bir röportajda ABD istihbarat servislerinin 2016 ABD seçimlerine Rusya'nın müdahale ettiği görüşünü yineledi. Pompeo bununla kalmayıp şunu da ekledi: "Rusya'nın 6 Kasım 2018'de yapılacak kongre ara seçimlerini de hedef alacağını düşünüyorum. Buna karşın ABD'nin seçimleri adil bir şekilde gerçekleştirebileceğinden şüphem yok. Onları güçlü bir şekilde geri püskürteceğiz, seçimimizi etkileyemeyecekler[1]."

Rusya da geri durmadı ve geçtiğimiz ay gerçekleşen devlet başkanı seçimlerine ABD'nin nüfuz etme çabasından kuşku duyduklarını dile getirdi. Sputnik News'a konuşan Kremlin Sözcüsü Dmitriy Peskov, ABD'nin Rusya da dahil birçok ülkenin iç işlerine ve seçimlerine müdahale konusunda zengin bir geleneğe sahip olduğunu ve bunun kimse için sır olmadığını söyledi[2].

1 http://www.bbc.com/news/world-us-canada-42864372
2 https://sputniknews.com/world/201801291061152800-us-kremlin-list-interference-election/

Samanlıktaki İğne

Ülkeler birbirini suçlayadursun, siber saldırıların ardındaki gizemi çözmek hayli zaman alan zor bir süreç. Symantec Norton Security mühendislerinden Eric Chien yaptıkları işi samanlıkta iğne aramaya benzetiyor: "Her gün milyonlarca zararlı yazılımla karşılaşıyoruz, her gün milyonlarca siber saldırı gerçekleşiyor. Aslında yaptığımız kişileri, kurumları ve devletleri bu tür saldırılardan korumaya çalışmak. Ancak hepsinden önemlisi bu kadar çok sayıda saldırıyla karşılaşırken aralarından en etkili, en yıkıcı sonuç doğurabilecekleri bulma çabası"[3].

Kaspersky Küresel Araştırma ve Analiz Ekibi (APAC) Müdürü Vitaly Kamluk virüs araştırmacılarını ağaçkakanlara benzetiyor. Çünkü onlar da aynı ağaçkakanlar gibi ağlardaki parazitleri, solucanları yakalıyorlar. Zaten virüs laboratuvarına siber dünyada verilen isim de "ağaçkakan yuvası".

Kamluk siber saldırganları üç farklı grupta özetliyor: "İlki, amaçları yasadışı kazanç sağlamak olan siber suçlular. İkinci grupta siber dünyadaki adıyla 'hacktivist' dediğimiz aktivistler yer alıyor ki bunlar politik mesaj vermek ya da bazı zamanlarda sadece eğlenmek için saldırıda bulunuyorlar. Üçüncü grupsa devletler açısından yüksek ölçüde önem içeren istihbari bilgileri elde ederek saldırı amacı güdüyor."

Devletlerin ulusal sınırlar ötesinde siber uzayda casusluk yaptığı ve çeşitli saldırılar gerçekleştirdiği muhakkak. Rand Corporation tarafından hazırlanan ve Isaac R. Porche tarafından kaleme alınan rapora göre yaşanan ve gelecekte yaşanması muhtemel savunma açıklarını bertaraf etmek için üç ayaklı bir plan öngörülebilir: Öncelikle savunma hattını sağlam tutmak, saldırıların etkisini ve hızını daha çabuk algılamak ve son olarak da tüm saldırı seviyelerine uygun şekilde cevap verebilme kabiliyetinde olmak[4].

Aynı rapor, açık ve özgür toplumların rakiplerine göre daha savunmasız olduğuna da değiniyor. Sosyal medyanın topluma yayılması ve entegrasyonu bu savunmasızlığı oldukça artırıyor. Kullanıcı verileri ele geçirilip satılabiliyor.

Siber güvenlik gurusu Bruce Schneier, internete daha az bağlı olmanın yollarını aradığını vurguluyor. Çünkü bağlantılılık ciddi bedeller de ödetiyor. Bilgisayarlar tarafından sürülmek üzere tasarlanan gelecek nesil otomobilleri düşünün; can güvenliğinizi her an "hacklenebilecek" bir kontrol mekanizmasına emanet eder misiniz?

Rand Corporation tarafından yapılan araştırma ABD'nin siber suçlara cevap verme kabiliyetindeki zayıflığı da vurguluyor. Askeri kuvvetler, istihbarat ajansları, kolluk kuvvetleri ayrı ayrı rollere sahip olsa da hareket limitleri sınırlı ve bazı zamanlarda biri, bir diğerinin önüne sınır çizebiliyor. Örgütler arasındaki çatışma yaratabilecek bu durum bir siber saldırıya cevap verme refleksinde yavaşlamaya yol açıyor. ABD'li siber güvenlik uzmanı Clint Watts, bu açıdan Rusya'yla tam anlamıyla ters bir konumda olduklarını belirtiyor: "Enformasyon harekatında bize üstünlük sağladılar. Bunun sebebi aslında çok açık; siber operasyonları, istihbarat ve diplomasiyi birbirlerini engellemeyecek şekilde bir arada yürütebiliyorlar." Hukuk kökenli bir araştırmacı olan Lawrence Greenberg bu gerçeği yaklaşık 20 yıl önce öngörmüş ve şu cümlelerle dile getirmiş: "Enformasyon savaşlarında uluslararası hukuk esaslarıyla ilgili ciddi belirsizlikler mevcut. Bu durum düşmanların ABD'ye ve onun sistemlerine daha kolay saldırmasına sebep olabilir"[5].

Devletler vatandaşlarını her tür saldırıdan korumakla mükelleftir. Ancak kişisel veriyi dünyaya açarak onu bir silaha dönüştüren siber saldırı söz konusu olunca bireylerin de tedbirli olması son derece önemlidir. Kuvvetli

3 http://www.zerodaysfilm.com
4 https://www.rand.org/blog/2018/03/getting-ready-to-fight-the-next-cyber-war.html
5 https://www.rand.org/blog/2018/03/getting-ready-to-fight-the-next-cyber-war.html

parola kullanımı (ve bunu sıklıkla değiştirmek), antivirüs yazılımlar, tanınmayan ağlara bağlanmamak, şüpheli e-postaları açmamak akla ilk gelen bireysel tedbirlerdendir. Avusturyalı yazar Ingeborg Bachmann'ın da dile getirdiği gibi "savaş artık ilan edilmiyor" ve düşmanın nereden geldiği belli olmayan bu yeni durum, savunma stratejisini toplumun en küçük parçasına kadar indiriyor.