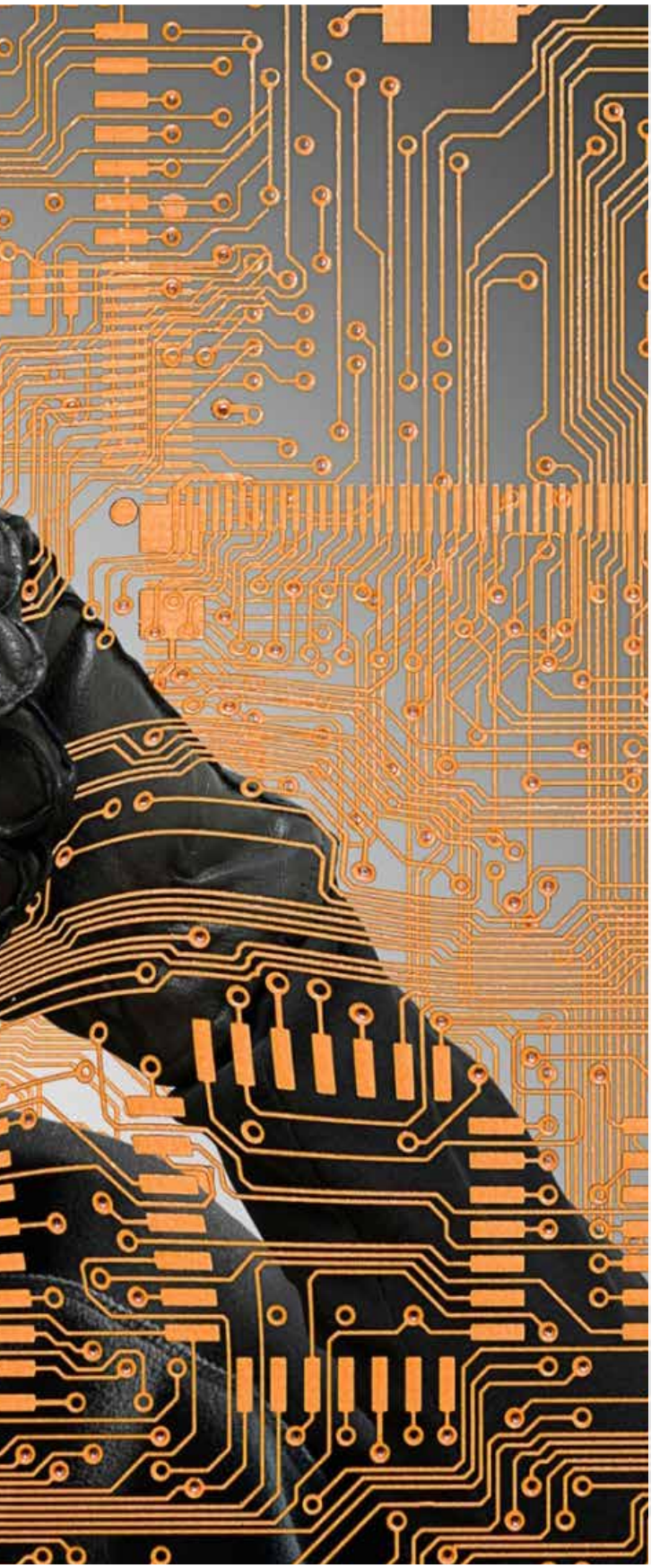
SİBER GÜVENLİK GELECEĞİ ŞEKİLLENDİRİYOR



Günümüzde siber güvenliğin temelinde üç temel unsur yatıyor: **Güvenli, farkında ve dirençli olma...** Dolayısıyla tehdidin farkında olunması, kurumların dirençli olması ve işleri sürdürmek amacıyla güvenli bir ortam yaratılması gerekiyor. Bir kurumun %100 güvenli olması mümkün olmasa da, bu üç temel özelliğe odaklanmak suretiyle siber tehditlerin etkilerini azaltarak, potansiyel iş zararını en aza indirmek mümkün görünüyor.

Önce cep telefonları daha sonra sosyal medya ve bulut teknolojilerinin hayatımıza girişiyle birlikte içinde bulunduğumuz dünya artık makinelerin birbiriyle konuştuğu bir yer. Bugün telefonunuzun, bilgisayarınızın veya tabletinizin birbirine bağlı olduğunu biliyorsunuz ama yarın buzdolabınız, gözlükleriniz, arabanız ve eviniz birbiriyle bağlantı kuruyor olacak. Örneğin buzdolabınız evde yaşayan kişi sayısına göre almanız gereken malzemeleri listeleyebilecek. Evinize gitmeden önce ısı ayarı yapabilecek. Kısaca nesnelerin internetiyle yaşamı kolaylaştıran bu akıllı dünyada riskler de yok değil. Tüm bu gelişmeleri sağlayan bulut ve sanallaşma teknolojisi son zamanların en çok konuşulan risklerinden birini de beraberinde getiriyor. Siber saldırılar ve bunlara karşı alınması gereken güvenlik tedbirleri.

SİBER GÜVENLİK KAVRAMI

Siber uzay, ABD Savunma Bakanlığı'nca "internetin bulunduğu, telekomünikasyon ağlarını ve bilgisayar sistemlerini de kapsayan, birbirine bağlı bilgi teknolojisi altyapılarının olduğu küresel bir alan" olarak tanımlanıyor. Ayrıca şöyle bir tanımlama da yapılıyor:

"İnsanların bilgisayarlar ve telekomünikasyon sistemleri aracılığıyla herhangi bir coğrafi sınırlamaya maruz kalmadan, birbirine bağlı olma durumu."

Siber uzaydan gelebilecek saldırılara ve tehditlere karşı kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan politikalar, güvenlik kavramları, risk yönetimi yaklaşımları ise siber güvenliği oluşturuyor.

2014'ün son dönemleri ve 2015'in ilk günlerinde ülkeler arası siber saldırılara sahne oldu.ABD ile Kuzey Kore arasında bir film nedeniyle başlayan siber saldırı gerginliğinde, devreye devlet başkanları bile girdi.

Siber saldırıların ana hedefi ülkelerin güvenlik, sağlık, enerji, ulaşım, haberleşme, su, bankacılık, kamu hizmetleri gibi

kritik sektörlerinin bilgi sistemi altyapılarını kapsıyor. Siber Güvenlik Derneği üyelerinden Ömer Faruk Altundal tarafından hazırlanan Türkiye'nin 2014 Siber Güvelik Raporu'nda, "2014 yılında ezber bozan, üreticilerin kendi uygulamalarından kaynaklanan zafiyetlerin gölgede kaldığı; bunun yerine, defacto standart olarak kullanılan uygulamalarda bulunan açıkların keşfedildiği bir dönemden geçtik. Bu açıkların halen tamamen giderilmediğini, kalıntılarıyla halen yeni zafiyetlerin keşfedildiğini ve bunları sömürmek için saldırı vektörlerini geliştirildiğini görmekteyiz" deniliyor.

RAKAMLARLA SİBER GÜVENLİK

Siber güvenlik kuruluşu Arbor Networks'ün araştırmasına göre, 2014'ün ikinci çeyreğinde dünya genelinde siber saldırılar %68 oranında hız keserken aynı dönemde Türkiye'ye yönelik saldırılarda %6 artış yaşandığı belirtiliyor. Türkiye'nin en çok saldırı aldığı ülkeler 2014'ün ilk çeyreğinde Malezya, İsviçre ve Rusya olurken, ikinci çeyrekte başı çeken Rusya'yı, ABD ve İsviçre izliyor. Türkiye'yi vuran en büyük saldırılar, bilgisayarların takvim ve saatlerini dünyayla uyumlandırmada kullandığı NTP üzerinden gerçekleştirildiği gözlemleniyor.

Dünyaca ünlü içerik dağıtım ağı Akamai'nin State of the Internet raporunda, siber saldırıların en çok hangi ülkelerden yapıldığı ortaya konuyor. 2014 yılının birinci, ikinci ve üçüncü çeyrek rakamlarına bakıldığında dünya genelinde en çok siber saldırının Çin'den gerçekleştiği görülüyor. İkinci ABD'yi, Tayvan, Hindistan ve Rusya izliyor. Türkiye ise %1,3'lük oranla dokuzuncu sırada yer alıyor.

Kaspersky Lab 2014 Siber Saldırı Raporu'na göre ise Kaspersky Lab antivirüs ürünleri tarafından, kullanıcıların bilgisayarları ve mobil cihazlarına karşı gerçekleştirilen 6.2 milyar kötü niyetli saldırının engellendiği belirtiliyor. Kullanıcı bilgisayarlarının %38'inin, bir yıl içinde en az bir web saldırısına maruz kaldığı ifade edliyor.

TÜRK BANKALARI **KORSANLARIN İLK HEDEFİ**

İşletmelerin de geleneksel sınırları her geçen gün genişleyerek, "sınırsız" hale geldiği dünyada artık küçük, büyük her sektörden organizasyonlar tehdit altına giriyor. Trend Micro'nun 2014 raporuna göre Türkiye çevrimiçi bankacılık alanında Avrupa'da en çok saldırıya uğrayan ülke konumunda. Uzmanlar, son yıllarda kaydedilen olumlu gelişmeler rağmen siber savaşın tam gaz devam ettiğini belirtiyor.

Yaşar Üniversitesi Bilgisayar Mühendisliği Bölüm Başkanı Doç. Dr. Ahmet Koltuksuz, siber güvenlik konusunda dünyada olumlu adımlara rağmen koordineli çalışan bir sistemin olmadığını belirterek, "Siber savaşlar başlayacak, insan eğitelim, ordu kuralım, dediğimiz günler geldi" dedi.

Türkiye'nin siber savaşa karşı müdahaleyi yönetecek orkestra şefinin bulunması gerektiğini belirten Doç. Dr. Koltuksuz, "2012'de Ulusal Siber Olaylara Müdahale Merkezi, 2013'te Siber Olaylara Müdahale Ekibi oluşturuldu. Ulusal Siber Güvenlik Stratejisi yürürlükte. Ancak bu iş Ankara'da 50-100 kişiyle olacak bir iş değil, ülke

geneline yayılması gereken bir ekip işi. Eğitimli insanları bir araya getirmek, yeni uzmanlar eğitmek, bu işin kimin yürüteceğini belirlemek gerekiyor. Bu yüzden daha hazır değiliz" ifadesini kullandı.

Trend Micro'nun 2014 yılı ikinci çeyrek raporuna göre de Türkiye'deki tehditlerin başında çevrimiçi bankacılığa olan siber saldırılar ön plana çıkıyor. Avrupa'da bu alanda en fazla saldırıya uğrayan ülke olan Türkiye, dünyada Japonya, ABD, Hindistan, Brezilya ve Vietnam'ın ardından altıncı sırada yer alıyor.

EN ZAYIF SİSTEMİNİZ KADAR GÜÇLÜSÜNÜZ

Bir saldırganın tehdit, strateji ve yöntemlerini anlamak, kurumlara siber güvenlik stratejisi, önlem almak için bilgi verebilir. Dolayısıyla kurumlar her adımda güvenlik kavramını benimserlerse siber suçluların işini zorlaştırabilirler.

Yapılan araştırmalar bir siber saldırıların genel olarak aşağıda belirtilen aşamalardan geçerek uygulandığını ortaya çıkarıyor:

Keşif: Şirketlerin, kurumların veya kişilerin zafiyetlerinin belirlenmesi. Bunun için internet üzerinden yapılan araştırmalar, çağrı merkezlerinin aranması, sosyal medya üzerinden bilgi toplama gibi yöntemler kullanılıyor.

Saldırı: Zafiyetlerin hedeflenmesi. Saldırganlar tarafından belirlenmiş e-post saldırıları, kullanıcılara güvenilir kaynaktan zararlı dosya gönderimi, ağ, web uygulama veya yazılım zafiyetlerinin istismarı gibi yöntemler uygulanıyor.

İstismar: Yetkisiz erişim. Saldırganlar, bilgisayara hat yükseltilmesi, ağ ve sunucuları izleme veya kontrol etme, atak vektörlerinin artırımı, izleri saklama gibi uygulamalara baş vuruyor.

Amacı Gerçekleştirme: Çalmak, zarar vermek, dikkat dağıtmak. Saldırgan tarafından çalınan veriler şifrelenerek tehdit unsuru olarak kullanılması, uzun süre gizlenerek veri ele geçirme, dijital izleri gizlenmesi şeklinde gerçekleşiyor.

Saldırılara karşı siber savunmanın temelinde üç temel unsur yatıyor: Güvenli, farkında ve dirençli olma... Buna göre, tehdidin farkında olunması, kurumların dirençli olması ve işleri sürdürmek amacıyla güvenli bir ortam yaratılması gerekiyor. Bir kurumun, %100 güvenli olması mümkün olmasa da, bu üç temel özelliğe odaklanmak suretiyle siber tehditlerin etkilerini azaltarak ve potansiyel iş zararını en aza indirmek mümkün görünüyor.

SİBER SALDIRI EN ÇOK WEB SİTELERİNDE GÖRÜLÜYOR

Yapılan araştırmalar, örnek vaka analizleriyle farklı sektörlerdeki siber saldırılar incelendiğinde, bilgi güvenliği olaylarının %35'inin web saldırıları, %22'sinin siber casusluk ve %14'ünün satış noktası ihlalleri (POS) olduğunu gösteriyor.

Siber saldırıların en önemli zararları arasında ise rekabet avantajıyla müşterinin güveninin yitirilmesi, kurumun itibarının ve markasının zedelenmesi olmak üzere kolay telafi edilemeyen varlıklarda görülüyor.

Araştırmalar, siber saldırılara karşı duyarlı yedi sektöre dikkat çekiliyor.

İleri Teknoloji: İleri teknoloji sektörü, elinde bulundurduğu değerli bilgilerle, siber saldırılar açısından hem çok cazip hem de çoğu zaman savunmasız durumda kalıyor. Yeni teknolojileri en erken alan ve uygulayan şirketler olarak henüz olgunlaşmamış teknolojik araçların getirdiği tehlikelere ve muhtemel saldırılara karşı açık ve kırılgan olunuyor. Bu da, ileri teknoloji şirketlerini ve çalışanlarını diğer sektörlere kıyasla ortalama üstü bir risk iştahına sahip kılıyor.

Online Medya: Siber tehditlere karşı en savunmasız alanlardan biri online medya sektörü olarak gösteriliyor. Bu kurumların online çalışıyor olmaları, saldırıya maruz kalma yüzdelerini ciddi anlamda artırıyor. Ürünlerinin yüksek talep gördüğü ve tamamen dijital çalışan bu sektör, izinsiz erişimi amaçlayan ya da değerli içeriğin hedef alındığı şahsi veya örgütlü suç eylem ve saldırılarında çokça hedef haline geliyor.

Telekomünikasyon: Telekom şirketleri büyük ölçekte olmaları ve önemli verilerin iletilmesi ve depolanmasında yaygın olarak kullanılan kritik altyapıyı inşa etmeleri, kontrol etmeleri ve işletmeleri sebepleriyle siber saldırılar için önemli bir hedef oluyor.

E-ticaret ve Online Ödemeler: Şirketler her geçen gün çoğalan şekilde hizmetlerini online platformlara kaydırdığı için suçlular da aynı şeyi yapıyor. Çoğu e-ticaret sitesi veri işleme ve tedarik yönetimi için doğrudan hem internete hem de bir şirketin sunucu uygulama sistemlerine bağlı çalışmakta. Bu da internet sitesini kurum dahilindeki önemli bilgi varlıklarına erişmede önemli bir saldırı noktası haline getiriyor. Online ödeme sistemleri de sıklıkla saldırıya uğrayan kırılgan alanlardan biri haline geliyor.

Sigortacılık: Sigorta şirketleri müşterilerle daha yakın ilişkiler kurmak, müşterilere yeni ürünler sunmak ve müşterilerin finansal portföyünde daha fazla yer edinmek için dijital kanallara yöneliyor. Dolayısıyla sigorta sektöründeki siber saldırılar da gitgide artıyor. Bu dijital yatırımlar yeni stratejik imkânlar sağlasa da, çok kanallı ortamın zorluklarıyla başa çıkmada nispeten deneyimsiz olan kurumlar için yeni siber riskler doğuruyor.

Üretim: Mevcut üretim sistemlerinin çoğu, güvenlik risklerinin daha az olduğu zamanlarda geliştirildiği dikkate alındığında, üretim teknolojilerinin ana odağını geleneksel olarak güvenlik değil emniyet ve performans oluşturuyor. Bu da üretim sistemlerinde önemli güvenlik zafiyetlerinin oluşmasına yol açıyor. Üreticiler artık sadece hackerlar ve siber suçlular gibi bilinen oyuncuların saldırılarına maruz kalmıyor. Rakip firmalar ve kurumsal casusluğa karışan devletler de tehlike arz edebiliyor.

Perakende: Kredi kartı bilgileri hackerlar ve suçlular için yeni gözde para birimine

dönüştüğü için, perakendeciler bu bilgilere fazlasıyla sahip konumda görünüyor. Bu durum perakende sektörünü siber saldırılar için karşı konulamaz bir hedefe dönüştürüyor. Perakendeciler veri bazlı teknolojiler yoluyla satışlarını ve verimliliği artırmak istedikleri için sektörün olası saldırılara açıklığı her geçen gün daha da artıyor.

Siber Güvenlik Derneği, önümüzdeki dönemde siber saldırılardan nasibini alacağı düşünülen bir diğer sektörün de sağlık sektörü olduğunun altını çiziyor. Var oluş sebebi gereği hem Türkiye'de hem de dünyada insanların bir şekilde dâhil olduğu sağlık sektöründeki kurumlarda pek çok fazla bilgi bulunuyor. (Vatandaşların adı-soyadı, adresleri, doğum yeri-tarihi, kan grubu, iletişim bilgileri, sağlık sorunları, kimlik numaraları gibi.)

Siber Güvenlik Derneği'nin 2014 raporunda, "Ayrıca hastanelerin de bilgi alışverişinde bulunduğu Merkezi Nüfus Kayıt Sistemi (Türkiye'de MERNİS) çok daha fazla bilgi barındırabilmektedir. Bu açıdan sağlık kurumları, siber korsanların iştahını oldukça kabartan birer hedef durumundadır.

2014'ün sonlarında yaptığımız bir araştırmada, bir devlet hastanesinde bulunan zafiyetler zinciri nedeniyle 600 bin hastaya ilişkin kritik kimlik bilgileri, iletişim bilgileri ve hastalığın ifşa edilebildiği görülmüştür. Bu zafiyetin Sağlık Bakanlığı'nın ilgili birimleriyle paylaşılarak giderilmesi sağlanmıştır" bilgisi yer alıyor.

TÜRKİYE'DEKİ SİBER GÜVENLİK YAPILARI VE FAALİYETLERİ

Türkiye'de 35 milyonu aşkın internet kullanıcısı olması özellikle de "sosyal ağ" denilen facebook, twitter, linkedin, youtube gibi sitelerin kullanımını da artırıyor. Türkiye'deki internet kullanıcılarının bilgi güvenliği/siber güvenlik farkındalığının artırılması amacıyla TÜBİTAK BİLGEM tarafından Bilgimi Koruyorum E-Öğrenme Projesi http://www.bilgimikoruyorum.org.tr/ adlı bir site kuruldu. Site, kullanıcılara sadece kendilerini korumayı öğretmeyi değil, onları siber saldırılara alet olmamak konusunda bilinçlendirmeyi de amaçlıyor.

Ayrıca Siber Güvenlik Derneği, Bilgi Güvenliği Derneği gibi sivil toplum kuruluşları düzenledikleri konferanslar, seminerler ve eğitimlerle toplumda siber güvenlik farkındalığı oluşturuyor.

Son yıllarda özellikle protesto amaçlı "hacktivizm" faaliyetlerinden büyük kamu kurumları ve özel şirketler de nasibini alıyor. Özellikle servis dışı bırakma, web sayfası içeriği değiştirme gibi saldırılara maruz kalan kurumların verdiği hizmetler sekteye uğruyor. Servis dışı bırakma saldırıları sırasında saldırının etkisinin uzun sürmesi, saldırganların hiçbir bilgi birikimi olmasa da kolaylıkla yapılabilmelerinden ve saldırıya uğrayan kurumun diğer kurumlarla arasındaki koordinasyon eksikliğinden kaynaklanıyor.

Siber suçlara karşı uluslararası düzeydeki ilk sözleşme Avrupa Konseyi tarafından hazırlanan Siber Suç Sözleşmesi'dir. Sözleşmeyi 39 Avrupa Konseyi üyesi, ABD, Kanada, Japonya ve Güney Afrika olmak üzere toplam 43 ülkenin imzaladığı biliniyor. Türkiye'de 10 kasım 2010'da Dışişleri Bakanlığı düzeyinde bu belgeyi imzalamış bulunuyor.

Türkiye için henüz bir siber güvenlik stratejisi belirlenmemiştir. Fakat 20 ekim 2012 tarihli Milli Güvenlik Kurulu kararıyla siber güvenlikle ilgili olarak alınacak önlemleri belirlemek ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla Ulaştırma, Denizcilik ve Haberleşme Bakanı'nın başkanlığında Siber Güvenlik Kurulu kurulmuş, böylece siber güvenliğin devlet seviyesinde ele alınmasına imkân sağlanmıştır.

2012'nin Temmuz'unda TÜBİTAK BİLGEM'E bağlı Siber Güvenlik Enstitüsü'nün açılması, siber güvenlik alanında daha etkin Ar-Ge yapılmasına olanak sağlamıştır.

2023 yılına kadar en az üç nükleer enerji santrali inşa etmek isteyen Türkiye'nin stuxnet/flame/duqu benzeri siber saldırılara hedef olmaması için gerekli siber savunma altyapısını kurması ve hazırlıklarını yapması gerekiyor. Bu bağlamda yasal düzenlemelerin oluşturulması, uluslararası hukuktan kaynaklanan hakların kullanılabilmesi için hazırlık yapılması, ulusal bilgisayar olaylarına müdahale organizasyonunun kurulması, ulusal siber güvenlik altyapısının güçlendirilmesi, siber güvenlik alanında insan kaynağı yetiştirilmesi, siber güvenlikte milli teknolojilerin geliştirilmesi için seferber olunması gerekiyor.

KURUMLAR **RİSKLERİNİ** BELİRLEMELİ

KİM SALDIRABİLİR?

- Siber suçlular.
- Hacktivistler.
- Devletler.
- Kötü niyetli çalışanlar.
- Kötü niyetli tedarikçiler.
- Rakipler.
- Gelişmiş yalnız hackerlar.

NEYİN PEŞİNDELER?

- Hassas bilgiler (şirket ve yönetim raporları, finansal bilgiler, yatırımcı bilgileri vb.)
- Finansal dolandırıcılık (para transferi).
- İş yıkımı.
- Yaşam tehdidi.

NELER KULLANILABİLİR?

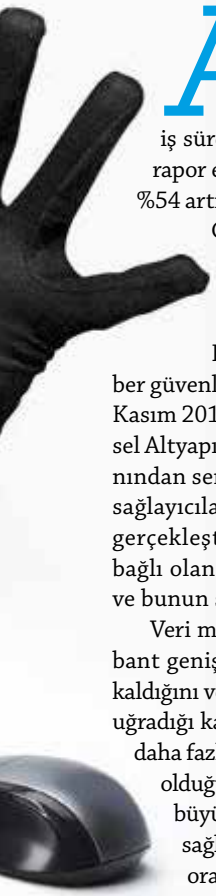
- Oltalama (phishing) saldırıları.
- Yazılım veya donanım zafiyetleri.
- Farkındalık eksiklikleri.
- Çalınan kullanıcı bilgileri.

Kaynak: *Kaynak: Deloitte, 2 Aralık 2014, İstanbul.*

SİBER SALDIRILAR

10 YILDA 50 KAT ARTTI

ABD siber güvenlik kuruluşu Arbor Networks'ün araştırmasına göre, internet üzerinden sunulan hizmetleri engellemeye yönelik saldırılar 10 yıl önce sadece bir sıkıntıyken, bugün kurbanlarının iş sürekliliği ve kârlılığını etkileyen boyutlara ulaştı. **2004'te rapor edilen en büyük saldırı saniyede 8 GB iken, 2014'te yıllık %54 artışla toplamda 50 katına çıktı** ve saniyede 400 GB'a ulaştı.



ABD siber güvenlik kuruluşu Arbor Networks'ün araştırmasına göre, internet üzerinden sunulan hizmetleri engellemeye yönelik saldırılar 10 yıl önce sadece bir sıkıntı iken, bugün kurbanlarının iş sürekliliği ve kârlılığını etkileyen boyutlara ulaştı. 2004'te rapor edilen en büyük saldırı saniyede 8 GB iken, 2014'te yıllık %54 artışla toplamda 50 katına çıktı ve saniyede 400 GB'a ulaştı. Güvenlik duvarlarını bile etkisiz kılabilen saldırıların ilk üç nedeni vandalizm, oyunlar ve ideolojik amaçlar iken, en fazla zarar gören ilk üç grup bireysel kullanıcılar, e-ticaret ve kamu kurumları oldu.

Dünyadaki İnternet servis sağlayıcılarının %90'ının siber güvenliğini sağlayan ABD güvenlik kuruluşu Arbor Networks, Kasım 2013-Kasım 2014 dönemini kapsayan 10'uncu Yıllık Küresel Altyapı Güvenliği Raporu'nu yayımladı. Dünyanın dört bir yanından servis sağlayıcılar, şirketler, bulut ve barındırma hizmet sağlayıcıları ile diğer ağ operatörlerinden 287'sinin katılımıyla gerçekleştirilen anket sonucu ortaya çıkan veriler, internete bağlı olan tüm şirketleri tehdit eden DDoS saldırılarının artışı ve bunun sonuçlarını ortaya koydu.

Veri merkezi operatörlerinin üçte birinden fazlasının internet bant genişliğinin tamamını kullanan DDoS saldırılarına maruz kaldığını ve %44'ün de bir DDoS saldırısı nedeniyle kazanç kaybına uğradığı kayıtlara geçti. DDoS'un kurumlar için bir sıkıntıdan çok daha fazlası, iş süreklilikleri ve kârlılıklarını tehdit eden bir faktör olduğunu ortaya koyan rapor, 2014'te saniyede 400 GB'a ulaşan büyüklükte saldırı yaşandığını açığa çıkardı. İnternet servis sağlayıcısı katılımcıların uğradığı saldırılar ise bir önceki yıla oranla %42 arttı. Servis sağlayıcılar açısından müşterilerine yönelik DDoS saldırıları bir numaralı operasyonel tehdit konumuna geldi.

SİBER GÜVENLİKTE NİTELİKLİ ELEMAN AÇIĞI %59

Arbor Networks'ün 10'uncu Yıllık Küresel Altyapı Güvenliği Raporu'na yönelik bilgi veren Arbor Türkiye Ülke Müdürü Serhat Atlı, savunma becerilerinde insan faktörünün önemini korumaya devam ettiğini belirtiyor. Atlı, raporda güvenlik kuruluşlarında nitelikli personel alımında ve iş akdinin devamında güçlükler yaşadığını rapor eden katılımcı sayısı %14'lük bir artışla %59'lara ulaştığına dikkat çekiyor.

Katılımcıların 10 yıl önce saldırıların "deneme-yanılma" yoluyla yapıldığını ifade ettiklerini, bugün ise %90'ının uygulama katmanı saldırılarına maruz kaldığını belirttiğini söyleyen Atlı, "Kurbanların üçte biri DDoS saldırıları sonucunda güvenlik duvarı ve IPS cihazlarının devre dışı kaldığını rapor ederken, buna karşın nitelikli güvenlik çözümlerinden yararlanılması gerektiği ortaya çıktı" diyor.

Arbor Türkiye Ülke Müdürü Serhat Atlı, TOBB Ekonomik Forum Dergisi'nin konuya yönelik sorularını şöyle yanıtladı:

Siber saldırı çeşitleri ve tanımları hakkında bilgi verir misiniz? Siber atakların dünyadaki artış sebebi nedir?

Arbor'ın odaklandığı iki önemli siber saldırı çeşidi var. İlki günümüzün popüler saldırı türü DDoS saldırıları. Bu saldırı tipinde amaç web sitelerini, uygulamaları ve tüm online servisleri ulaşılamaz hale getirmek. Bu ataklar sürekli olarak gelişerek web sitelerinin, bulut servislerinin erişilebilirliğini tehdit etmektedir. Ayrıca bu ataklar çok etki yaratıyor çünkü web sitesinin çökmesi veya erişilememesi halinde bu sorun çok kısa sürede öğreniliyor ve yayılıyor. Bu da kurumun itibarını etkiliyor ve de rakipleri bu kesintileri aleyhlerinde kullanabiliyor.

Diğer saldırı çeşidi ise gelişmiş saldırılar. Bu saldırılar, herhangi bir organizasyonu, kurumu, şirketi hedef alır. Hedef hakkında olabildiğince bilgi toplanır ve hedefin güvenlik sistemleri incelenir. Amaç şirketin iç ağına girip fark edilmeden orada kalmak ve içeriden bilgi toplayabilmektir. Araştırmalara göre bu tip ataklarda saldırganlar iç ağlarda 200 gün fark edilmeden kalabilmektedir. Saldırganlar iç ağda oldukları zaman, erişimlerini artırarak şirketin gizli bilgilerini çalmaktadır. Bu tip saldırganlar sabırlı ve bilinçli atak yaparak etkili olmaktadır.

Arbor Türkiye Ülke Müdürü Serhat Atlı, Türkiye'deki siber güvenlik sorunlarıyla dünyadaki sorunlar aynı olduğunu belirtti.

Türkiye'nin siber güvenlik alanındaki açıkları nelerdir?

Türkiye'deki siber güvenlik sorunlarıyla dünyadaki sorunlar aynı. Standart güvenlik modelinde çeşitli güvenlik seviyeleri var. Bu model bulut bilişimin ortaya çıkmasından

önce efektif bir modeldi çünkü şirketler bilgilerini dışarıya açmıyordu. Bu yüzden koruma politikaları belli ve çok katıydı. Fakat bulut bilişimle şirketlerin diğer organizasyonlarla bilgi paylaşması, şirket bilgilerini internet ortamından erişilebilir kılması gerekiyor. Örnek olarak; satış yazılımları, CRM bilgileri, İK bilgilerinin paylaşımını veya şirketlerin bazı bölümlerini outsource etmesini söyleyebiliriz. Bu sebeple sizin güvenliğiniz, en zayıf noktanızın güvenliği kadardır. Bu da saldırganlara atak yapabilecek daha fazla nokta sağlamaktadır.

Türkiye'ye yapılan siber atakların büyüklükleri, kaynakları ve yöntemleri hakkında bilgi verir misiniz?

2014 yılının ilk yarısındaki atakların ortalama büyüklüğü saniyede 2 Gb idi. İkinci yarısında ise bu sayı saniyede 0,7 Gb'a düşüyor. 2014 yılının ilk çeyreğinde 20Gb'ten fazla olan atakların %99'u NTP reflection/amplification ataklarıydı. Yılın ilk yarısındaki NTP ataklarının ortalama büyüklüğü saniyede 5,7 Gb idi. İkinci yarısında ise bu altı saniyede Gb'a ulaştı. En çok atak yapılan servis ise www servisleri oldu. Yani e-ticaretler...

Türkiye'ye hangi ülkelerden daha fazla atak geliyor?

Günümüzde siber ataklar küresel niteliktedir. Ataklar bugün bir kaynaktan yapılıyor, ertesi gün ise farklı bir kaynaktan yapılabiliyor. Arbor Networks ile Google Ideas'ın işbirliği sayesinde bunu görsel bir hale getirebiliyoruz. Arbor Networks'ün ATLAS Projesi aracılığıyla 320 servis sağlayıcısı trafik ve atak bilgilerini paylaşmakta. Bu sayede, Arbor Networks saniyede 120 Tb'tan fazla trafiği inceleyerek, dünyadaki atakları gözlemleyebilmekte ve inceleyebilmektedir ki, bu sadece Arbor'a özgüdür. Google Ideas bu bilgiyi alarak görsel bir platforma taşıdı: Digital Attack Map (digitalattackmap.com). Bu harita bize dinamik, görsel ve anlık olarak dünyadaki siber atakları göstermekte.

Siber savunmanın temeli nedir?

Geçtiğimiz yılda, DDoS ataklarından dolayı sistemleri, servisleri ve erişimleri, müşteri bilgileri veya fikri/sınai mülkiyet hakların çalınması ya da hasar oluşan sistem kesintileri gibi sayısız olaylar nedeniyle pek çok

organizasyon zarara uğradı. Bugünkü problem ise kurumların gizli bilgilerini veya iş kritik uygulamalarını hedef alan içerden ve dışarıdan ataklara maruz kalmaları. Artık tehditler iş sürekliliğini veya şirketin gizli bilgilerini hedef alıyor.

Olay tiplerinden bağımsız, tüm kurumlar bu tip tehditlere karşı hazır olmalıdır ve kurumların %60'ında olaya müdahale ekipleri mevcuttur. Fakat kurumların daha zayıf olduğu kısımlar var; saldırıların işe olan etkilerini tahmin edebilmek, saldırıyı 24 saat içinde tespit edebilmek gibi. Maalesef bu iki konu da çok önemli. Özellikle bazı regülasyonlar saldırıların, tehditlerin belli zaman aralıklarında tespit edilmesini istemekte.

Siber riski nasıl tanımlarınız?

Günümüzde siber risk, iş riskidir; bu iki tanım birbiri yerine kullanılabilir. Başarılı siber ataklar müşteri veya şirket bilgilerini hedef alır. Arbor Network'un sponsorluğunda Economist Intelligence Unit'in yaptığı araştırmaya göre, siber ataklara karşı sigortanlanma isteği artmakta. Arbor'ın WISR isimli bu raporunda belirtildiği gibi; servis sağlayıcı olmayan katılımcıların %6'sı sigorta şirketleriyle bu alanda gelişme sağlamak için sözleşme imzalamışlardır.

Siber atakların başarı oranları ve ataklar sonucundaki kayıplar göz önüne alındığında, organizasyonlar güvenlik duruşlarını güçlendireceklerdir. Fakat bugünkü tehditlere karşı organizasyonları korumak sadece teknolojiyle olmaz; insan ve süreçleri de içerir. Güvenlik analistleri bu tehditleri analiz etmeli, önceliklendirmeli ve detaylı araştırmalı. Bunun içinde gerekli tehdit algılama sistemleri ve ürünlerini de kullanılmalı.

Kurumların siber tehditlere karşı neler yapması gerekli?

Günümüzde firmalar güvenlik bütçelerinin çoğunu, atakların ilk ve son safhalarına harcıyorlar. İlk safhada; atağın olmasını engellemeye yönelik oluyor. Ağlarını korumak için; web uygulama firewalls, next-gen firewalls, intrusion prevention systems, antivirus ve bu gibi diğer çözümleri kullanıyor. Son safha ise saldırıyla ilgili tüm alarm ve logların toplanması; saldırı veya tehdit nasıl içeriye girmiş gibi bilgilerdir. Burada eksik olan orta safhada ne olduğu yani tehdit iç ağa girince ne yapmış, nerelere ulaşmış bilgilerine ulaşabilmek. Kurumların kendilerini daha iyi koruyabilmeleri için tehditti daha hızlı algılayıp, müdahale etmeleri gerekir.

Arbor Türkiye Ülke Müdürü Serhat Atlı, şirketlerin siber ataklara karşı kendilerini korumaları için kendi ağlarını denetleyebilmelerinin önemini vurguladı.

Şirketler siber ataklara karşı kendilerini korumak için ne yapmalı?

Şirketler kendi ağlarını denetleyebilmelidir. İç ağlarındaki haberleşmelerden haberdar olmalılar. Bu sayede anormal veya olağan dışı bir olay olduğunda bunu anlayabilirler. Bu olağan dışı olayı fark ettiklerinde ise detaylı olarak analiz etmeliler, atağın nerelere ulaştığını veya ulaşmaya çalıştığını görmeliler ve bu atağı engellemeliler.

Kişiler ve şirketler siber ataklara karşı nasıl hazırlanmalı?

Sonuçta tüm şirketler insanlardan oluşur. Sofistike saldırganlar çoğunlukla şirketlerin çalışanlarını hedef alır. Çalışanların sosyal medya profillerini inceler. Çalışanların bilgisayarlarına malware yüklemek için çalışanın şüphelenmeyeceği bir konu hakkında bir link hazırlanır. Çalışanlar bu linki tıkladığında bilgisayarlarına malware'ı yüklemiş olur. Şirket ağına bilgisayarıyla girdiği zamanda saldırgan amacına yani kurumun iç ağına ulaşmış olur. Bu tip saldırganlar sabırlı ve hedefe odaklanmışlardır.

Efektif güvenlik, sadece gerekli güvenlik cihazlarını kullanmak değildir. Çalışanlar da güvenlik konusunda eğitilmelidir. Birçok firmanın olay müdahale planı var fakat bu planlar üzerinde çalışacak vakitleri yok veya uygulayacak yeterli insan kaynağı yok. Atak olduğunda, atağa yapılan müdahalenin gerektiği kadar sert olmamasının sebebi ise yeterince bu planlar üzerinde çalışılmamasıdır. Efektif güvenlik bahsedilen tüm bu önlemleri karşılamalıdır.