KPMG

BT

KARŞI SALDIRIYA GEÇMEK

Dijital suçla mücadele için işbirliği yapmak

İçindekiler

Önsöz

Teknolojinin her alana yayıldığı bir dünyada yaşıyoruz. Ticaret, savunma, sağlık hizmetleri veya eğitim gibi tüm insani faaliyetler artık birbirine bağlı karmaşık teknolojilere ve iletişim sistemlerine dayalı.

Bu sistemler artık her zamankinden daha küresel. Bilgi saniyeler içinde tüm dünyayı dolaşıyor ve şirketlerin entegre tedarik zincirlerini işletmelerine, operasyonları için dış kaynak kullanmalarına ve uluslararası pazarlara girebilmelerine imkan tanıyor.

Aynı zamanda, hızla artan bir belirsizlik ve risk ortamında yaşıyoruz. Aslında bu durum tesadüfen ortaya çıkmadı. Bu risklerin bir kısmı doğrudan dijital teknolojiye bağımlılığımızdan kaynaklanıyor.

Teknolojiye olan bağımlılığımız, yöneticileri maliyet, risk ve esneklik arasında sürekli bir denge kurmak zorunda bırakan önemli kurumsal yönetim sorunlarını beraberinde getiriyor. Günümüzde dijital güvenlik, yönetim kurullarının bir numaralı gündem maddelerinden biri haline geldi. Tüm yöneticiler risklerin farkında ve bunları meslektaşlarıyla sürekli tartışıyor.

Ancak bu tartışmalar endişeleri gidermeye pek de yardımcı olmuyor. Şirketlerin gelişmiş performansın bir katalizörü olarak sürekli daha da ileri teknolojileri hayata geçirmeleri suç örgütleri için de önemli fırsatlar doğuruyor. Dijital dönüşüm, suç örgütlerinin hızla bulup maddi çıkar sağlayabildikleri yeni zayıflıkları da beraberinde getirdi.

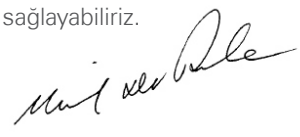
Bu, British Telecom ve KPMG'nin ilk elden tanık olduğu bir durum. CEO'ların ve yönetim kurulundaki meslektaşlarının dijital suçun değişen yüzüne ayak uydurmaya çalışırken yaşadığı zorlukları görüyoruz. Dijital suç ölçeğinin bu denli büyük olmasının riskleri en iyi şekilde yönetebilme ve hem stratejileri hem de teknolojileri sürekli değişip gelişen bir düşmana karşı etkin bir savunma yapabilme konusunda önemli soruları gündeme getirdiğini biliyoruz.

Bu noktada yeni bir düşünce tarzı gerekiyor ve bunun ilk adımı dijital suçluların motivasyon kaynaklarını, izledikleri yöntemleri ve suçu paraya çevirme planlarını anlamak. Sonraki adım ise, elde edilen bilgiyi kapsamlı ve etkin bir yanıta dönüştürmek.

> "Dijital suçluların motivasyon kaynaklarını, izledikleri yöntemleri ve suçu paraya çevirme planlarını anlamak için yeni bir düşünce tarzı benimsemek gerekiyor."

Dijital suç riski arttıkça işletmelerin de daha proaktif olmaları gerektiğini düşünüyorum. Kuruluşların, sadece savunma mekanizmalarını devreye sokmak yerine, hem kendi verilerimizi hem de müşterilerimizin verilerini koruma konusunda harekete geçmenin ortak çıkarımız olduğunu anlamaları gerekiyor. Bunu en etkin yolu ise elbette işbirliği yapmak... İşletmeler, hükümetle, kanun uygulayıcılarla, sektörlerindeki paydaşlarıyla, başka sektörlerdeki kuruluşlarla ve güvenlik uzmanlarıyla ortak çalışarak suçluların faaliyetlerini onlar için daha zor ve maliyetli bir hale getirebilir.

Güvenlik bir rekabet unsuru değil. Çünkü dijital suç, büyümeyi destekleyen ve doğal olarak kârlılığı artıran yeni dijital fırsatlardan tam olarak faydalanmayı tüm işletmeler için zorlaştırıyor. Birlikte çalıştığımız takdirde, suçlulara karşı olan ortak mücadelemizde önemli bir avantaj sağlayabiliriz.



Sir Michael Rake, Başkan, British Telecom Group Plc

Yönetici Özeti

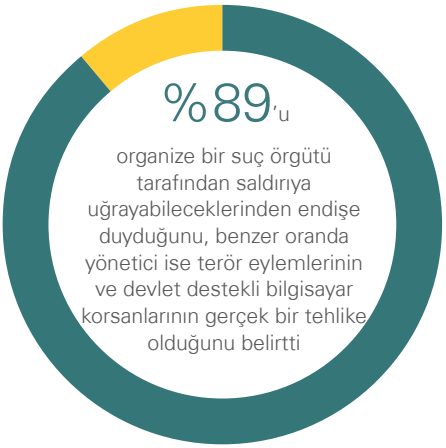
Dünyanın en büyük şirketleri, acımasız suçluların inanılmaz sayıda ve çeşitlilikte dijital saldırısına maruz kalıyor.

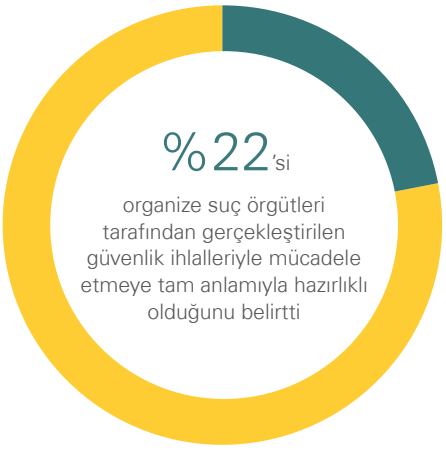
Tehdidin ölçeği ve saldırganların kararlılığı aslında çok da şaşırtıcı değil. İnternet ekonomisinin 2016 yılında 4,2 trilyon dolarlık bir büyüklüğe ulaşacağının tahmin edildiği (Boston Consulting Group[1]) ve e-ticaretin küresel GSYİH'de payının sürekli arttığı bir ortamda suçlular da doğal olarak dijital işletmelerdeki zayıflıkların sunduğu fırsatların peşinde.

Tehdit konusundaki farkındalık her zamankinden yüksek olsa da, işletmelerin büyük bir kısmı saldırganların motivasyon kaynaklarını ve yöntemlerini hâlâ kavrayamamış veya tehdidin ölçeğini tam olarak anlayamamış durumda. İşletmelerin sadece küçük bir kısmı kendilerini bu tehdit karşısında tam anlamıyla hazırlıklı hissediyor. Saldırı araçlarının çeşitlenip geliştiği ve siber suçluların giderek daha yetenekli hale geldiği günümüzde, her ölçekten işletme, verilerini ve sistemlerini korumak için mücadele veriyor.

Bulgularımız ve önerilerimiz, müşterilerle yapılan görüşmelerden ve British Telecom ile KPMG'nin yürüttüğü çalışmalardan elde edilen kanıtlara dayanıyor. Dijital dünyadaki gelişmelerle ilgili bakış açımıza dayanarak hazırladığımız ve bağımsız bir araştırma şirketi tarafından yürütülen anket aracılığıyla işletmelerin endişelerini belirlemeyi amaçlıyoruz.

Araştırmamızın da gösterdiği gibi, önemli şirketler dijital suçla mücadele konusunda oldukça kararlı. Tüm dünyadan pek çok büyük şirketin bilgi teknolojileri (BT), güvenlik ve ticari faaliyetlerden sorumlu yöneticileriyle görüştük ve bunların %73'ü siber güvenliğin en az üç ayda bir veya daha sık aralıklarla yönetim kurulu toplantılarının gündemine alındığını belirtti. Bununla birlikte yöneticiler, kapsamlı ve dinamik bir online suç karaborsasında faaliyet gösteren düşmanlarına karşı zorlu bir savaş veriyor.





Yönetici Özeti

Değişen bir tehdit

Farkındalık seviyesinin bu kadar yüksek olması elbette iyi bir şey ve yönetim kurulları karşılaştıkları tehditlerin türü ve potansiyel saldırı stratejileri konusunda giderek daha da bilgili hale geliyor. Aynı derecede önemli bir başka şey de, şirketlerin, tehditlerin müşteri güveni ve hisse fiyatı bakımından doğurabileceği sonuçları biliyor olmaları.

Ancak, sadece az sayıda şirket saldırıları önlemek için gerekenleri yeterince yaptığını güvenle söyleyebiliyor. Organize suç örgütleri tarafından gerçekleştirilen güvenlik ihlalleriyle mücadele etmek için aldıkları tedbirler sorulduğunda katılımcıların sadece %22'si tam anlamıyla hazırlıklı olduklarını belirtti.

Acımasız sabıkalı girişimciler

Dijital suçlar ağırlıklı olarak kapsamlı bir online suç karaborsasında işleniyor. Bu, sürekli yeni saldırı araçlarının geliştirilip suçlulara satıldığı veya kiralandığı bir pazar ve yüksek Ar-Ge harcamalarıyla destekleniyor. Üstelik bu pazarda faaliyet gösteren sabıkalı girişimcilerin kullandığı yöntemler de sürekli değişiyor. Çok çevik ve hızlı olmaları, yasal işletmelerin bunlara ayak uydurabilmelerini zorlaştırıyor.

Yasal işletmelerin karşılaştıkları tehditler de sürekli gelişerek değişiyor. Her gün yeni saldırı yöntemleri geliştiriliyor ve işletmeler sürekli bilmedikleri araç ve stratejilerle mücadele etmek zorunda kalıyor.

Bu tür saldırıların arkasındaki sabıkalı girişimciler, acımasız olmalarının yanı sıra oldukça rasyonel iş modelleri de yürütüyor. Yasal girişimciler gibi bunların da hedefi kâr etmek ve bunu bilgisayar sistemleri ile ağlarına sağladıkları erişimi ve işledikleri bilgiyi paraya çevirerek gerçekleştiriyorlar.

Kullanılan yöntemler ise, kötü amaçlı yazılım dağıtmak gibi klasik yöntemlerin çok ötesinde. Potansiyel kazanç arttıkça organize suç örgütleri de çalışanları istismar etmeye ve şirket içine kendi adamlarını yerleştirmeye daha hazır hale geliyor.

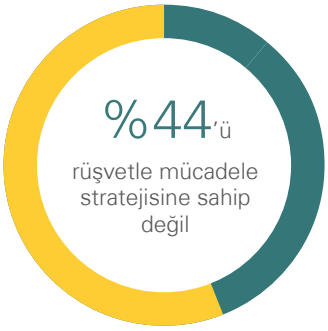
Karşı saldırı

Sabıkalı girişimcilerin yarattığı tehdit, proaktif ve anında yanıtları zorunlu hale getiriyor. Şirketler, saldırganların faaliyetlerine karşılık vermek zorunda. Bu ise kendini ağırlıklı olarak ek güvenlik teknolojilerini devreye sokmak, daha fazla çalışanı görevlendirmek ve güvenlik politikaları ile uygulamalarını hayata geçirmek şeklinde kendini gösteriyor. Ancak, saldırganları anlamak da bir o kadar önemli: Kimler? İş modelleri neler? Amaçları ne? Bu bilgiler, saldırganları ağdan uzak tutmanın ötesinde savunma stratejileri oluşturmak için kullanılabilir.

Çeviklik ihtiyacı

İşletmeler, suç faaliyetlerine karşı koyabilmek için en az saldırganlar kadar esnek ve çevik olmalı, zira onları önemli zorluklar bekliyor. Örneğin bir şirket, bilinmedik olmasının yanı sıra belli bir saldırı için özelleştirilmiş olan kötü amaçlı bir yazılımla nasıl baş edebilecek?

Bu noktada işbirliği ön plana çıkıyor. Aynı sektörde faaliyet gösteren kuruluşlar benzer tehlikelerle karşı karşıya ve suçluların işini zorlaştırmak hepsinin ortak çıkarı. Bankalar, telekom şirketleri, internet servis sağlayıcılar ve tüm sektörlerdeki şirketler ortak bir düşmanla karşı karşıya. Örneğin, perakende sektöründeki bir şirkete yapılan bir saldırı çoğu zaman bir telekom şirketini, internet servis sağlayıcısını veya bankayı da etkiliyor. Ayrıca, hükümetlerin ve kanun uygulayıcıların hedefleri de, yasal olmayan faaliyetleri açığa çıkarmaya ilişkin ticari işletme hedefleriyle örtüşüyor. İşletmeler, hükümetler ve kanun uygulayıcılar, işbirliği yapmak suretiyle istihbaratı, kaynakları ve en iyi uygulamaları paylaşabiliyor ve bu sayede suç çetelerine ayak uydurabiliyor.



Herkes ödülün peşinde: risk ve fırsat

Sağlam bir dijital güvenlik, korunma açısından kritik olmanın yanı sıra aynı zamanda bir kolaylaştırıcı. Daha fazla ürün satmak ve müşterilere daha iyi hizmet sunmak için yeni dijital kanallar geliştirme potansiyelinin açığa çıkarılmasında güvenlik kilit role sahip. Aynı şekilde, güvenlik, şirket içi verimliliklerini artırmak için dijitalden faydalanan şirketler için de kritik önem arz ediyor. Araştırmamızın katılımcıları da bunları birer öncelik olarak görüyor.

Sağlam bir güvenlik tesis edilmediği takdirde dijital teknolojinin sunacağı faydalar da sınırlı kalacaktır. Asıl mücadele ise fırsatları ortaya çıkarmak ve riski yönetmek. Yeni bir düşünce tarzına ihtiyaç var.

İşletmelerin saldırganlarla nasıl mücadele edebileceklerini ortaya koymaya çalıştığımız rapor bu konuları daha detaylı inceliyor. Hızla değişen bir ortamda bunun başarılabilmesi için hükümetler, kanun uygulayıcılar ve diğer işletmeler ile yakın işbirliği yapılması gerekecek.

"Asıl mücadele, fırsatları ortaya çıkarmak ve riski yönetmek. Yeni bir düşünce tarzına ihtiyaç var."

Dijital güvenlik tehdidini yeniden düşünün

01

Dijital suç açığı

Dijital suç baş döndürücü bir hızla yayılıyor; ancak işletmeler riskteki artışın farkındaysa da buna karşı etkin müdahale araçları geliştirmemiş. İşletmelerin büyük bir kısmı bir çeşit saldırıya maruz kalmışsa da sadece küçük bir kısmı artan tehditle yüzleşmeye tam anlamıyla hazırlıklı.

Şirketlerin **%97**'si dijital saldırıların kurbanı olmuşsa da bunların sadece **%22**'si gelecekteki olaylarla mücadele etmeye tam anlamıyla hazırlıklı.

Katılımcıların **%55**'i siber saldırılarda bir artış yaşamış, ancak sadece **%23**'ü olası büyük bir olayın maliyetini karşılayacak bir sigorta poliçesine sahip.

Şirketlerin **%71**'i siber suçluların kullandığı araç ve stratejileri incelemeye yönelik prosedürlere sahip, ancak sadece **%30**'u bunları anlayabiliyor.

Katılımcıların **%73**'ü dijital güvenlik konusunun yönetim kurulu gündeminde olduğunu, **%54**'ü ise yöneticilerini bu konuda eğittiklerini belirtiyor.

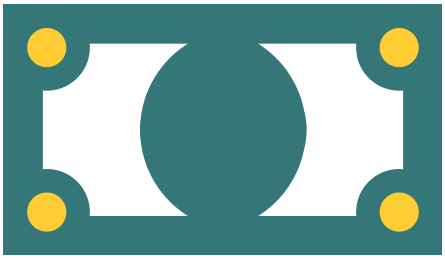
Dijital güvenlik tehdidini yeniden düşünün

01

Dijital suçluların gerçekleştirdiği saldırıların gerçek ve güncel birer tehlike olduğu konusunda herkes hemfikirse de, tehlikenin ölçeği, hızı ve sürekli değişen yapısı çoğu zaman tam olarak kavranamıyor.

Stratejik ve Uluslararası Araştırmalar Merkezi (Centre for Strategic and International Studies, CSIS) tarafından yapılan bir araştırmaya göre, dijital suçun tüm dünyadaki maliyeti yıllık 400 milyar dolar civarında[2]. Üstelik bu henüz buzdağının görünen kısmı ve mevcut riskler dijital ekonominin büyümesinin önünde bir engel teşkil ediyor. Suçluların kapsamlı ve sonu gelmeyen faaliyetlerinin iyice artmaya başladığı günümüzde, geleneksel düşünce tarzı, şirketlerin sistemlerini %100 koruyabildikleri takdirde suçluların başarılı olabilmelerinin ancak şansa bağlı olacağını söylüyor. Oysa bu daha büyük, hatta hükümetlerin kapasitelerini bile aşan bir mücadele. Bu nedenle, sadece savunma ve korunma sistemlerine odaklanmaktan vazgeçip, risk yönetimine ve saldırılara karşılık vermeye ve olası bir saldırıdan sonra kurtarmaya odaklanmanın zamanı çoktan geldi.

Dijital suç tüm dünyada her yıl



400 milyar dolar

zarara yol açıyor

Dijital suç bireysel kullanıcılara da ağır zararlar veriyor. San Diego merkezli Kimlik Hırsızlığı Araştırma Merkezi, geçen yıl tüm dünyada 169 milyon kişisel kaydın izinsiz ele geçirildiğini tahmin ediyor.[3] Üstelik bu rakam buzdağının sadece görünen kısmı; zira bu tür verilere izinsiz erişilmesine yol açan güvenlik ihlallerinin büyük bir kısmı kamuoyuyla paylaşılmıyor.

Veri ihlalleri konusunda hükümetlerin daha fazla şeffaflık istedikleri bir dönemde bu artık kaçınılmaz. Örneğin Avrupa Birliği'nin Genel Veri Koruma Yönetmeliği bir ifşa zorunluluğu hükmü içeriyor.

Dijital suç konusuna öncelik vermek

Sorunun ölçeği hükümetlerin ve resmi makamların da gündeminde. Örneğin, İngiltere Ulusal Suçla Mücadele Ajansı, dijital suçun İngiltere'nin karşılaştığı en önemli tehlikelerden biri olduğunu duyurdu. 2010 yılında İngiltere Ulusal Güvenlik Konseyi, dijital saldırıların ulusal güvenliği tehdit eden en önemli risklerden biri olduğunu duyurdu[4]. Buna yanıt olarak da İngiltere hükümeti, beş yıllık bir döneme yayılması planlanan bir Ulusal Siber Güvenlik Planı'nı[5] desteklemek amacıyla 1,9 milyar sterlinlik bir yatırım yapacağını duyurdu. Diğer taraftan, ABD Sermaye Piyasaları Kurulu Başkanı Mary Jo White, bu yıl yaptığı bir açıklamayla, dijital suçun finans sistemi üzerinde "en büyük baskıyı yaratan" tehdit olduğunu belirtti. ABD hükümeti de savunma mekanizmalarını geliştirmeye yönelik adımlar atıyor. Başkan Obama, önceki yıl 14 milyar dolar olan dijital güvenlik harcamalarının 2017 yılında 19 milyar dolara[6] çıkarılmasına ilişkin bir planı masaya koydu. Resme daha geniş bir açıdan bakan araştırma şirketi Gartner, 2015 yılında dijital güvenlik için yapılan harcamaların 75 milyar dolar olduğunu tahmin ediyor.[7]

Gelişmekte olan bir tehdit

Her saniye yeni bir kötü amaçlı yazılım geliştirilip dağıtılıyor ve yeni e-dolandırıcılık saldırıları başlatılıyor. Üstelik yeni saldırı araçları ortaya çıkınca eski araçlar ortadan kalkmıyor. Örneğin, ağ üzerinden yayılan ilk kötü amaçlı yazılımlardan biri olan Conficker 2008 yılında yeniden ortaya çıktı. Buna rağmen, CERT İngiltere, bu programın halen İngiltere'de en yaygın görülen kötü amaçlı yazılım olduğunu raporladı.[8]

Eski BT sistemleri dijital savunmada önemli bir zayıf halka olabilir. Kötü amaçlı yazılım geliştirenler oldukça kıvrak zekalı; eski sistemlerden faydalandıkları gibi güvenlik ekibinin hamlelerine onların yöntemlerini benimseyerek de karşılık verebiliyorlar. Saldırı araçları çoğu zaman önce ortadan kayboluyor, ardından da yeni bir güvenlik yanıtı vermeyi gerektiren daha gelişmiş bir versiyonla yeniden ortaya çıkıyor.

Kullanıcı adlarını ve parolaları çalmada kullanılan kötü amaçlı bir yazılım olan Gameover Zeus buna bir örnek. Bu program, ilk kez fark edildiği 2011 yılından bugüne kadar bir dağıtık hizmet aksatma (DDoS) bileşenini içerecek ve daha zor tespit edilecek biçimde geliştirildi.

"Sadece sistemleri savunmayı düşünmenin devri kapandı"

Kötü amaçlı yazılımlar değiştikçe bunları yayma yöntemleri de değişiyor. Hem bireyler hem de kuruluşlar phishing olarak bilinen sahte e-postaların kötü amaçlı yazılımlar içerebileceği konusunda geçtiğimiz birkaç yıl boyunca oldukça bilinçlendilerse de, suçluların güvenilir ve kullanıcıyla ilgili olduğu izlenimi veren mesajlar göndermedeki ustalığı bunların fark edilmesini güçleştiriyor. Örneğin, 2015-2016 vergi yılının sonunda, İngiltere'deki pek çok vergi mükellefi, vergi makamları tarafından gönderilmiş tavsiyeler içerdiğini iddia eden pek çok e-posta aldı. Bu trend, vergi beyanı tarihinin yaklaştığı ABD'de de görülüyor.

Phishing taktikleri de sürekli gelişiyor ve e-posta tabanlı hilelere yönelik yeni bir trend doğuyor. Bu trend genellikle "CEO suistimali" veya "whaling" ("balina avı") olarak biliniyor.

Örneğin çalışanlar üst yöneticilerinden gelmiş gibi görünen ve çoğu zaman sahte telefon çağrıları ve metin mesajlarıyla birlikte gönderilen ve kendilerinden bir faturayı ödemelerini veya bir hesaba para yatırmalarını isteyen sahte şirket içi e-postalar alabiliyor. Hatta bazı durumlarda saldırganlar bu kumpas kapsamında profesyonel danışmanların (avukatlar gibi) ağlarını da hackleyebiliyor ve meşru bir kaynaktan gönderilmiş izlenimi veren e-postalar gönderebiliyor. Kuruluşlar her zaman tetikte olmak zorunda.

Zira uğrayabilecekleri maddi zarar oldukça fazla olabilir. Yaşanan bir olayda, bir sağlık hizmetleri şirketinin finansal denetçisi, üst düzey bir yönetici tarafından gönderilmiş izlenimi verilen sahte bir talimat e-postası aldıktan sonra Hong Kong ve Tunus'taki banka hesaplarına 18,5 milyon dolar yatırmıştı.

Suçlular ayrıca, inovatif suç modellerini desteklemek amacıyla mevcut kötü amaçlı yazılımları da yeni yöntemlerle kullanıyor. Örneğin, hedef müşterilerin banka hesap bilgilerini çalmak amacıyla geliştirilen Dridex isimli kötü amaçlı yazılımı kullanan suçlular, büyük bankaların bu programa karşı daha etkin savunma mekanizmaları geliştirdiklerini gördü. Buna karşılık da, bu tür gelişmiş savunma mekanizmaları bulunmayan şirketlere yöneldiler. Suçlular ayrıca, bir bilgisayar veya ağa indirildiği zaman dosyaları şifreleyen bir fidye yazılımı olan Locky'den de yeniden faydalanma yoluna gitti. Bu yolla kurbanlar, belli bir fidye ödeyene kadar dosyalarının şifresini kaldıramıyor.

Fidye yazılımlarındaki bu artışın en önemli nedenlerinden biri de, ödeme yapmayı kolaylaştıran Bitcoin gibi blok zincir para birimlerinin ortaya çıkması. Bunların sonucunda, eski suç yöntemleriyle 21. yüzyılın modern soygunlarının yaşandığı bir döneme girdik. Şirketler artık, ellerinde beyzbol sopalarıyla insanlardan zorla para alan haydutlar yerine, sadece gelişmiş saldırı araçlarıyla ve şirketin zayıflıklarına dair bilgilerle donanmış suçlular tarafından soyuluyor.

Suçlular artık daha geniş bir ağa sahip

Sabıkalı girişimcilerin faydalandıkları ağ giderek genişliyor. Saldırganların maddi çıkar sağlamak amacıyla saldırdıkları başlıca hedefler ilk başlarda bankalar (hesaplardan para çalmak amacıyla hesap bilgilerini ele geçirmek) ve perakende şirketleriydi (saldırgan tarafından kullanılmak veya başkasına satılmak amacıyla kredi kartı bilgilerinin ele geçirilmesi). Oysa suçlular artık daha geniş bir bakış açısıyla düşünüyor ve pek çok şirketin kullandığı iş modelleri konusunda daha bilgililer. Bu da onların, bu iş modellerine saldırmak için yeni yollar geliştirebilmelerine imkan tanıyor. Yani dijital suçlular, yeni güvenlik prosedürlerine karşı yeni saldırı araçları geliştiriyor. Örneğin, parolanın yanında bir de güvenlik sorusu sorma uygulamasına geçilince suçlular her iki bilgiyi de ele geçirmeye yönelik yeni araç ve yöntemler geliştirdi.

Finans sektöründeki önemli bir müşterimizin görüşlerine bakalım: "Finans kuruluşlarının nasıl faaliyet gösterdiği artık çok daha iyi biliniyor ve potansiyel saldırganlar bu kuruluşların değer zinciriyle ilgili artık daha fazla bilgiye sahip." Bu gerçek, eskiden maddi çıkar sağlamanın zor olduğu finans kuruluşlarını artık daha kolay bir hedef haline getiriyor. Barclays İstihbarat Bölümü Başkan Yardımcısı Will Dixon, suçluların daha kolay hedeflere yöneldiklerine işaret ediyor: "Suçluların giderek KOBİ'leri ve hesabı kabarık kişileri daha fazla hedef aldığını görüyoruz."

Bu duruma karşı ise güvenlik ekipleri, dijital hırsızların kaydettiği ilerlemeye ayak uydurmaya çalışıyor. Üstelik bu, kuruluşun "dört duvarının" ötesine geçen bir mücadele. Uzaktan çalışmanın, kendi cihazını getir yönteminin ve karmaşık tedarik zincirlerinin birbirlerine giderek daha fazla bağlandığı bir dünyada işletmeler de saldırılara karşı zayıflıklarını yönetme konusunda daha geniş kapsamlı ve daha toplum odaklı bir yaklaşım benimsemek zorunda kalıyor.

Dijital güvenlik tehdidini yeniden düşünün

01

Hem yazılım tabanlı saldırı araçlarının hızla gelişmesi hem de suç çetelerinin kullandığı taktiklerin gelişmesi ve çevikleşmesi bakımından sürekli değişen bir dijital suç ortamıyla karşı karşıyayız. Üstelik tehdit büyüdükçe, şirketlerin başvurduğu kaynaklar online suç karaborsasındaki kaynakların ve yeteneklerin karşısında yetersiz kalmaya başlıyor. Gelecekte şirketler dijital güvenliklerini yeniden düşünmek zorunda kalacak ve bunun ilk adımı oyunun aktörlerini anlayabilmek.

Dijital Güvenlik Tehdidini Yeniden Düşünün - *Eylem adımları:*

- Değişen suç taktikleri ve yeni tehditler hakkında bilgi toplayın. Çalışanlarınız ve müşterileriniz saldırıları tespit etmede çoğu zaman en iyi yol olduğundan, onların nasıl hedef alınabileceklerini anlamalarını sağlayın. Şirket içi iletişimlerinizde saldırılarla ilgili güncel bilgilere düzenli olarak yer verin ve hem çalışanların hem de müşterilerin olası sorunları iletip gerekli bilgileri paylaşabilecekleri kanallar yaratın. Siber istihbarat konusunda bilinçli bir müşteri olun, harekete geçilebilecek istihbaratlar talep edin ve bunu şirketinizin ihtiyaçlarına ve iş modeline uygun hale getirmek için kendi güvenlik ekibinize başvurun.
- Bir suçlu gibi düşünün. Yönetim ekibinizle çalışarak, suçluların hedefleyebileceği bilgiler ve varlıklar ile bunun nedenlerini belirleyin.
- Yatırımlarınızı en hassas bilgilerinizi korumaya ve ilk anda korumaya geçmeye yoğunlaştırabilmenizi sağlayacak stratejiler geliştirin.

"Güvenlik ekipleri, dijital hırsızların kaydettiği ilerlemeye ayak uydurmaya çalışıyor. Üstelik bu, kuruluşun 'dört duvarının' ötesine geçen bir mücadele"

Acımasız ve rasyonel girişimciler

02

Dijital suç dünyası

Teknolojinin her yeri sardığı, işletmeler daha kapsamlı ve iddialı stratejiler geliştirirken acımasız sabıkalı girişimcilerin de zayıf sistemleri ele geçirip maddi çıkar sağlama fırsatlarını kolladığı bir dünyada yaşıyoruz. Üstelik bu suçluların saldırıları, üstün yeteneklerin bulunduğu, çok çeşitli, son derece kârlı ve sürekli daha gelişmiş saldırı araçlarının alınabildiği veya kiralanabildiği bir online suç karaborsasıyla destekleniyor.

İş dünyasının

%96 'sı

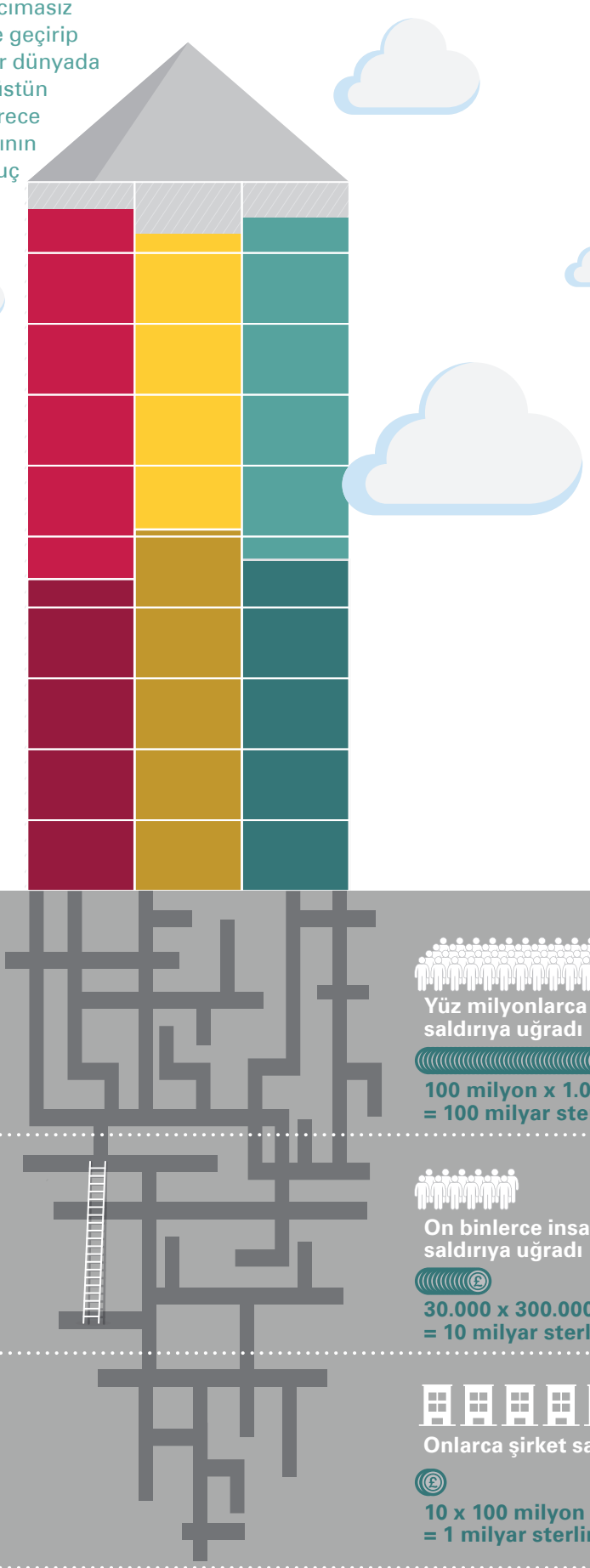
sabıkalı girişimcilerin rüşvet alan kendi çalışanları olabileceğini belirtiyor, ancak sadece %44'ü buna yönelik önleyici tedbirler uyguluyor.

%94 'ü

kendi kuruluşundaki personelin suça karışmasının potansiyel bir sorun olduğunu biliyor, ancak %47'si bununla mücadele etme planına sahip değil.

%95 'i

personelinin şantaja açık olabileceğini düşünüyor, ancak sadece %47'si buna yönelik bir savunma stratejisine sahip.



Siber suç dünyası

3. Seviye
Herkese yönelik metalaştırılmış saldırılar

Yüz milyonlarca insan saldırıya uğradı

100 milyon x 1.000 sterlin = 100 milyar sterlin

2. Seviye
İşletmelere ve varlıklı kişilere yönelik hedefli saldırılar

On binlerce insan saldırıya uğradı

30.000 x 300.000 sterlin = 10 milyar sterlin

1. Seviye
Finans sistemlerine yönelik gelişmiş siber saldırılar

Onlarca şirket saldırıya uğradı

10 x 100 milyon sterlin = 1 milyar sterlin

Acımasız ve rasyonel girişimciler

02

İş modelleri

21.yüzyılın dijital suçluları, oldukça gelişmiş ve hızla gelişen bir online suç karaborsasında faaliyet gösteren acımasız ancak yetenekli girişimciler veya CEO'lar olarak nitelendiriliyor. Dijital suçluların elebaşları, hedef pazarları ustalıkla sekteye uğratarak ve amacı sadece müşterilerine hizmet etmek olan şirketlerin zayıflıklarını suistimal ederek maddi çıkar sağlamaya çalışıyor. Kısacası onlar, herhangi bir yönetmeliğe tabi olmayan veya ahlaki değeri olmayan, ancak talepleri hissedarları için para kazanamadıkları takdirde daha katı cezalarla karşılaşabilen CEO'lar.

Amaçlarına ulaşabilmek içinse, çabalarını nakde çevirebilmelerini sağlayacak pek çok iş modeli geliştirdiler. İzledikleri yöntemler arasında DDoS saldırıları veya fidye programları aracılığıyla gasp yapmak, sistemleri manipüle etmek veya verileri çalmak yer alıyor. Çaldıkları verileri doğrudan kendileri için kullanabildikleri gibi (örneğin banka hesaplarını boşaltmak amacıyla) başkalarına da satabiliyor veya kurbanlarına şantaj yapmak için kullanabiliyorlar.

Sabıkalı girişimciler sadece doğrudan kuruluşlara saldıran kişilerle sınırlı değil. Bir DDoS saldırısı başlatan ve başkalarının kredi kartı bilgilerini çalan bir suçlu, saldırı araçlarının satıldığı veya kiralandığı ve suçun bir hizmet olarak sunulduğu çok yönlü bir online suç karaborsasından da destek alıyor. Bu karaborsadan faydalanan kişiler, sonuca odaklanan girişimcilerin bizzat kendisi. Bazen satmak, çoğu zamansa kiralamak üzere saldırı araçları tedarik ediyorlar. Belli bir ücret karşılığında DDoS saldırıları başlatıyor, kötü amaçlı yazılımlar dağıtıyor veya phishing amaçlı web siteleri kuruyorlar. Bir bilgisayar korsanının yeteneklerine ihtiyaç duyanlar tarafından, ev ağlarını hacklemek ve ağ sahibinin kimliğini kullanmak amacıyla tutuluyorlar.

Ev ağlarının bu şekilde ele geçirilmesi sadece kurbana değil, onun şirketine ve hatta tüm pazara zarar verebiliyor. Örneğin, yaşanan bir olayda, bir bilgisayar korsanı bir CEO'nun hesabını ele geçirdi ve onun kimliğini kullanarak hisse satın aldı. Bu hisse satın alma olayı ise daha sonra piyasayı manipüle etmek için kullanıldı. Bir başka ifadeyle, dinamik ve tepki veren bir piyasayla karşı karşıyayız.

Dijital suçun üç seviyesi

Dijital suçun, hedeflerine göre tanımlanmış üç temel seviyesi var. En üst seviyede, yakın zaman önce yaşanan ve diğer merkez bankalarının ihtiyatlı duruşu sayesinde 951 milyon dolara varabilecek bir olayın önlendiği Bangladeş Merkez Bankası'na yapılan 81 milyon dolarlık bir saldırıda olduğu gibi, finans sistemindeki üst düzey hedefler seçiliyor[9]. İkinci seviyede ise, işletmelere ve varlıklı kişilere yönelik düzenli saldırılar yer alıyor. Son olarak da, hepimizi etkileyen, metalaştırılmış saldırılar var. Bu saldırı seviyelerinin hepsinde, dijital saldırganlar, her girişimcinin yaptığı gibi elde edilebilecek kazanç ile karşılaşılabilecek risklerin ve giderlerin bir karşılaştırmasını yapıyor.

Saldırıların

%89'u

finansal veya casusluk amaçlı bir motivasyon unsuruna sahip

Online suç karaborsası faaliyetlerinin metalaştırılmış ucunda, banka hesaplarından para çekilmesi veya fidye amaçlı bir saldırı neticesinde Bitcoin benzeri bir ödeme yapılması sonucu 100 dolardan 10.000 dolara kadar para kaybedebilen kurbanlar hedef alınıyor.

Oysa bu tür bir saldırıyı başlatmanın maliyeti nispeten daha düşük. Çünkü saldırı araçları, kayda değer maliyetlerin olmadığı, hizmet tabanlı bir suç olarak kiralanabiliyor. Kullanıma göre ödeme yapılan sistemde, bir bilgisayara kötü amaçlı program kurmanın maliyeti sadece 0,50 dolar, savunmak için saatte 40.000 dolarlık[11] bir yatırım yapmayı gerektiren DDoS saldırılarının saatlik maliyeti ise sadece 5 dolar[10]. Elbette suçlu için de bazı riskler var. Bu saldırılar yüksek profilli saldırılar ve güvenlik ekipleri saldırıları önlemek için hemen harekete geçiyor. Kısacası bir kedi-fare oyunu gibi. Saldırılar tespit edildikçe kanun uygulayıcılar da suçu önlemek amacıyla devreye giriyor.

İşletmelere yönelik saldırılarda ise daha özelleştirilmiş bir yaklaşım gerekiyor. Burada da "hizmet olarak suç" temelli saldırı araçları satın alınabiliyor, ancak suçluların hedeflerini daha iyi anlamak ve onların zayıflıklarını paraya dönüştürebilmek için de yatırım yapmaları, hatta bazen ısmarlama kötü amaçlı yazılımlar kullanmaları gerekiyor. Bu tür saldırıların ödülü daha yüksek (10.000 ile 10 milyon dolar arası), ancak suçlular daha güçlü savunma mekanizmalarıyla karşılaşıyor. Kurbanlar kamuoyu nezdinde itibar kaybedebilse de, dolandırıcılık modelleri tespit edilebiliyor.

Finans sistemini hedef alanlar ısmarlama kötü amaçlı yazılımlara ve araştırmalara daha fazla yatırım yapıyor, hatta bazen hedef şirketin içine kendi adamlarını yerleştiriyor. Suçluların zaman ve çaba yatırımları fazla olsa da, neticede elde ettikleri menfaat de bir o kadar fazla oluyor. Kurbanların uğradığı zarar 10 milyon ila 1 milyar dolar arasında değişebiliyor, üstelik sistemlerini yeterince koruyamadıkları için düzenleyici makamlardan pazar cezaları da alabiliyorlar.

Bu, suçlular açısından riskin en yüksek olduğu nokta. Kanun uygulayıcılar finans sistemindeki yüksek profilli hedeflere yönelik saldırıları öncelik haline getirdi ve suçluların çaldıkları paraları aklamaları eskisi kadar kolay olmayacak. Yine de, başarılı bir saldırı deyim yerindeyse saldırganın "hayatını değiştirebilecek kadar" para kazanabilmesini sağlayabileceğinden teşvik unsuru hâlâ oldukça güçlü.

Geniş ölçekli maddi menfaatler

Kamuoyunda da duyulan pek çok olay, elde edilebilecek maddi menfaatin ne kadar yüksek olduğunu ortaya koyuyor. Örneğin geçen sene, Rus bilgisayar korsanı Vladimir Drinkman, çıkarıldığı bir ABD mahkemesinde, 2005 - 2015 yılları arasında gerçekleştirdiği kredi kartı bilgisi hırsızlıkları sonucu kurbanlarını 300 milyon dolar zarara uğrattığını kabul etti. Aynı yıl, Ivan Turchynov, internet gazetelerini ve dergilerini hackleyerek bazı önemli bilgilere önceden sahip olduğunu ve bu bilgileri usule aykırı hisse alım satımında kullandığını kabul etti. Bundan elde ettiği gelir ise 100 milyon dolar civarındaydı.

"Bir DDoS saldırısını başlatmanın saatlik maliyeti sadece 5 dolar iken, buna karşı savunma yapmanın saatlik maliyeti 40.000 dolardan fazla."

Dijital suç tehdidi küresel olduğu gibi bununla mücadele de küresel. Aralık 2015'te Interpol tarafından gerçekleştirilen ve 23'ten fazla ülkenin kanun uygulayıcılarının katıldığı bir operasyonda Çin, Hong Kong, Kore ve Vietnam'daki çağrı merkezlerine baskınlar yapıldı[12]. On beş çağrı merkezi kapatıldı ve 500 kişi tutuklandı. Bu durum, suç faaliyetlerinin ölçeğinin yanı sıra bunlara karşı etkin bir mücadele yapılabilmesi için sarf edilmesi gereken çabayı da ortaya koyuyor.

Acımasız ve rasyonel girişimciler

02

Dijital saldırıların sadece kötü niyetle gerçekleştirilmediğini ve tesadüfi olmadığını bilmek gerekiyor. Saldırganlar ve girişimciler tamamen rasyonel ve maddi çıkar elde etmeyi amaçlıyor. Hatta, Verizon tarafından yapılan bir araştırmaya göre, saldırganların %89'u maddi veya casusluk amaçlı bir motivasyon unsuruna sahip.[13]

Fidye programlarında silahlanma yarışı

Şifreleme, kişisel ve kurumsal verileri kötü niyetli kişilere karşı korumada kritik bir güvenlik aracı olsa da, suçluların elindeyken bir saldırı aracı olarak da kullanılabiliyor. Sabıkalı girişimciler, bireylerden ve şirketlerden fidye almak için fidye programlarını kullanıyor. Bunu genellikle, dosyaları şifreleyen kötü amaçlı bir programı bilgisayara bulaştırarak gerçekleştiriyorlar. Veriler kullanıcı tarafından erişilemez hale getirildikten sonra kurbandan bu verilerin şifresini kaldırma karşılığında fidye isteniyor.

Bu fidye ise, suçluların parayı almasına imkan tanıyan ve yakalanma risklerini en aza indiren sanal para birimi Bitcoin ile ödeniyor. Yaygın olarak 0,5 ila 1 Bitcoin kullanılıyor. Bitcoin'lerin mevcut değerinin ortalama 450 sterlin veya 640 dolar olduğu günümüzde, kurban bu küçük rakamı genellikle hemen ödüyor; ancak etkilenen bilgisayarların sayısı dikkate alındığında saldırgan müthiş paralar kazanıyor.

En bilinen fidye programı ise Locky. British Telecom tarafından incelenen Locky'nin polimorfik (çok biçimli) olduğu, yani kod görünümünün her güncellemeyle birlikte değiştiği ancak temel işlevinin aynı kaldığı belirlendi. Bu sayede her yeni Locky versiyonu görevini aynı başarıyla yerine getirebiliyor, yapılan kod değişiklikleri ise Locky'nin piyasada satılan anti-virüs programları tarafından tespit edilmesini önlüyor. Güvenlik uzmanları bu zararlı programın yayılmasını olabildiğince önleyebilmek için programda ters mühendislik gerçekleştirdi ve belli bir süre için başarı elde edildi.

Ancak Locky hemen yenilendi ve bu tedbirleri etkisiz bırakacak biçimde geliştirildi. Locky deneyiminde de görüldüğü gibi, yeni bir kötü amaçlı yazılıma karşı savunma yapmak, her iki tarafın da birbirinin önüne geçmeye çalıştığı bir silahlanma yarışı gibi.

Acımasız ve rasyonel girişimciler - *Eylem adımları:*

- İşletmenize bir suçlunun gözünden bakın. Yöneticilerinizi siber suçun işletme üzerindeki potansiyel etkisini değerlendirmekle görevlendirerek bunu sadece güvenlik ekibini ilgilendiren teknik bir konu olmaktan çıkarın.
- Daha gelişmiş saldırılar görülebileceğini öngörerek, siber suç yapılarını belirleme ve engelleme konusunda güvenlik ve hileyle mücadele ekipleri arasında yakın bir işbirliği ortamı yaratın. Kuruluşunuzda daha kolay ve daha iyi tespit yapılabilmesini sağlayacak fonksiyonlar arası forumların ve kurumsal yönetim mekanizmalarının hangileri olduğunu belirleyin.
- Siber saldırılara karşı mutlak bir korunma olmayacağı gerçeğini unutmayın. İhlaller her zaman olacaktır ve asıl önemli olan yaygın senaryolarla karşılaştığınızda neler yapabileceğinizdir. Ekibinizi eğiterek ve yanıt süreçlerinizi optimize ederek bu tür senaryoları önceden planlayıp uygulayın.

"Bu karaborsadan faydalanan kişiler, sonuca odaklanan girişimcilerin bizzat kendisi."

Saldırganlara karşı saldırıya geçme

03

Karşı saldırıya geçmek: siber saldırıları daha zor ve daha az kârlı hale getirin

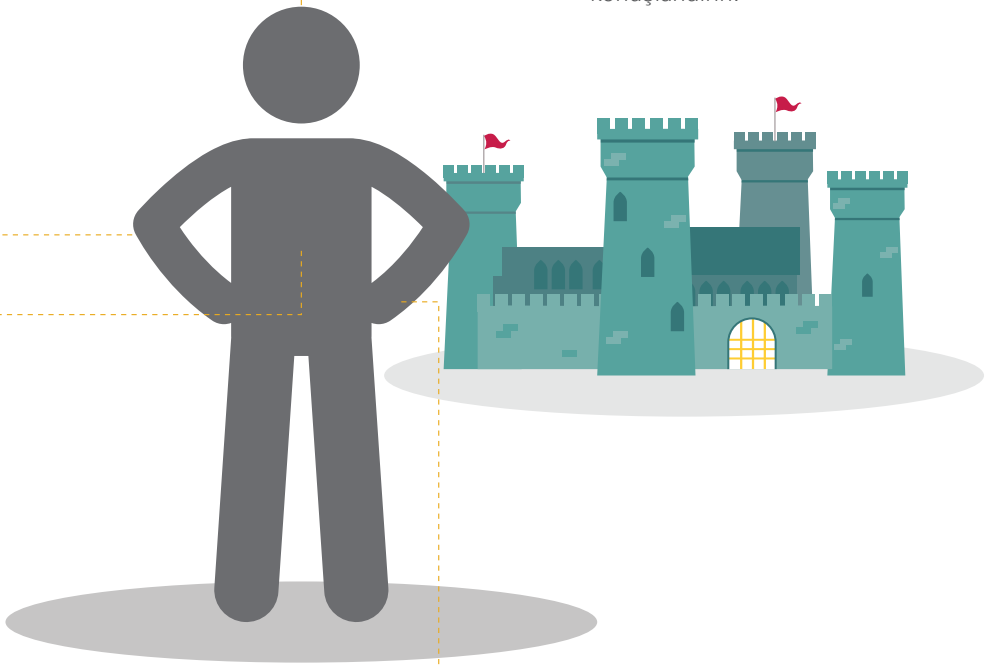
Siber suçluların giderek artan beceri ve azimleri, hiçbir kuruluşun sistemlerini %100 güvenli hale getiremeyeceği anlamına geliyor. Bununla birlikte işletmeler, başarılı saldırıları daha zorlu, daha yüksek maliyetli ve daha az kârlı hale getirmeye yönelik adımlar atabilir.

1

Saldırganların girişimde bulunulan veya başarılı olan bir sistem saldırısından önce, sonra ve saldırı sırasında harekete geçmelerini zorlaştıracak çok katmanlı bir güvenlik yaklaşımı geliştirin.

2

Bir saldırının başarılı olma ihtimalini en aza indirmek için gereken tüm araçları kurun ve güncelleyin. Saldırganlar yine de sisteme sızmayı başarırlarsa, amaçlarına ulaşmalarını zorlaştırın. Bilgilerinizi şifreleme yöntemiyle koruyun veya sistemi yeniden kurmak için kullanacağınız sanal makine teknolojileri konuşlandırın.



3

Çalınan verilerin kullanılabileceği alanları sınırlandırmaya yönelik sistemler ve prosedürler konuşlandırarak suçluların faaliyetlerini nakde çevirebilmelerini zorlaştırın.

4

Mevkidaşlarla, diğer sektörlerdeki işletmelerle, telekom şirketleriyle, internet servis sağlayıcılarla, kanun uygulayıcılarla ve hükümetle işbirliği yapın. İstihbaratı ve kaynakları paylaşın.

Saldırganlara karşı saldırıya geçme

03

Kuruluşlar, online suç karaborsasının verimliliğine ayak uydurma konusunda zorlanıyor. Saldırganlar her gün yeni zayıflıklar tespit edip bunları göz açıp kapayıncaya kadar suistimal ediyor.

Örneğin, OpenSSL şifreleme yazılımı kütüphanesiyle korunduğu düşünülen sistemlerdeki bilgilerin kötü niyetli kişilerce okunabilmesine imkan tanıyan Heartbleed sistem açığını düşünelim. Dijital suçlular, bu sistem açığı duyurulduktan sadece 24 saat sonra harekete geçmişlerdi bile.

Ancak bu hikayenin sadece bir bölümü. Sistem zayıflıklarına dair bilgiler çoğu zaman halka duyurulmadan önce online suç karaborsasında alınıp satılıyor, bu da suçluların işletmeler hazırlık yapmadan önce harekete geçebilmelerine imkan tanıyor.

Kötü amaçlı programların

%99'u

bir dakikadan kısa süreliğine kullanılıyor

İşletmeler aynı zamanda, saldırganların faaliyetlerini gizlemek ve kamufle etmek amacıya taktiklerini değiştirebilme becerilerine ayak uydurmakla da uğraşıyor. Kötü amaçlı yazılım enfeksiyonu bunun tipik bir örneği. Kötü amaçlı yazılımların %99'u bir dakikadan kısa süreliğine kullanılıyor ve kendisini güvenlik yazılımları tarafından algılanamayacak biçimde hemen değiştiriyor. Phishing e-postaları da giderek daha hedefli hale geliyor ve güvenlik tedbirleriyle engellendikten hemen sonra hızla değişiyor.

Sorunun karmaşıklığı bununla da sınırlı değil. Phishing e-postaları suçluların 100 yıl önce bile aşina olabileceği güvenilir hileler ile benzerlikleri olan araçlardan. Oysa e-postayla iletişimin sürekli değiştiği ve kurbanların dikkatle seçildiği günümüzde halen işe yarıyorlar.

"Organize suçun yatırım getirisiyle hareket ettiğini belirten Dixon, 'Suç zincirine baskı yapmak çok önemli' diyor."

Kanun uygulayıcıların eylemleri

Dijital suçun önlenmesi kanun uygulayıcıları için de önemli bir gündem maddesi ve hem ulusal hem de uluslararası emniyet birimleri ve diğer resmi kurumlar kendi eylem planlarını devreye soktu. Bunun bir örneği, spam e-postalar göndermek, daha fazla kötü amaçlı yazılımı yaymak veya DDoS saldırıları başlatmak amacıyla kullanılan enfekte bilgisayar ağları olan robot ağlara Interpol, Europol ve FBI tarafından yapılan baskınlar. Europol, Gameover Zeus, Ramnit, Beebone ve Shylock olarak bilinen dört ana robot ağını 2014 ve 2015 yıllarında kapattı. Bu tür faaliyetler organize suç örgütlerine elbette ağır darbe vuruyor.

Geçici bir çözüm mü?

Elde edilen bu başarılara rağmen, belli bir saldırı aracına karşı girişilen eylemler o aracı sadece bir süreliğine oyun dışı bırakıyor. Örneğin resmi makamlar bankacılık sektörünü hedef alan Dridex isimli saldırı aracını 2015'te yok etmişlerdi, ancak aynı araç sadece üç ay içinde yeniden ortaya çıktı.

İşin en çetrefilli kısmı, online suç karaborsasındaki yazılımların ve saldırı kampanyası stratejilerinin sürekli optimize ediliyor olması. Kötü amaçlı bir programı etkisiz hale getirmek, sadece o program farklı bir versiyonla yeniden ortaya çıkana kadar koruma sağlayacaktır.

Dahası, sabıkalı girişimciler genellikle çok daha güçlü ve zorlu bir şekilde geri dönüyor. Barclays'den Will Dixon, "Robot ağların kapatılması suçluların güvenlik mekanizmalarını geliştirmelerine ve yeni çalışma yöntemleri yaratmalarına da yol açıyor" diyor.

Kanun uygulayıcılar ve şirketler bu mücadelede var güçleriyle savaşıyor olsalar da, ufkun ardındaki yeni tehditleri çoğu zaman göremiyorlar. Bugünün iş modelinde bireylerin ve şirketlerin banka hesap bilgileri çalınırken yarının iş modelinde Locky gibi fidye programları ortaya çıkarak kurbanlara şantaj yapabilir.

Saldırganın hassas noktalarına vurmak

Sadece yaşanan olaylara yanıt vermek yerine, saldırgana karşı saldırıyla da yanıt vermek gerekiyor. Saldırganların kullandığı teknolojileri yasaklama ve kara para aklama faaliyetlerine baskı yapma yetkisine sahip kanun uygulayıcılar, suçla mücadele konusunda savunma yerine saldırıya dayalı bir yaklaşımı giderek daha fazla benimsiyor. İşletmeler de, suçluların harekete geçmesini daha zor ve daha yüksek maliyetli hale getirecek güvenlik araçlarını, prosedürlerini ve stratejilerini devreye sokarak bu mücadelede daha proaktif bir rol oynamak zorunda. Bu, suçluların hem sistemlere sızmasını hem de çaldıkları bilgileri kullanıp maddi çıkar sağlamalarını zorlaştırmak için kanun uygulayıcılarla daha fazla işbirliği yapmayı da içeriyor. Birlikte çalışıldığı takdirde, saldırganların en can alıcı noktalarına vurma şansı doğacak.

Bunun için de çok kademeli bir yaklaşım gerekiyor. Birinci savunma hattı, suçluları bilişim sistemlerinin dışında tutmak. Bununla birlikte kuruluşlar, ihlallerin her zaman olabileceği gerçeğini kabul ederek saldırganın elde ettiği bilgileri kullanabilmesini zorlaştırmalı.

Örneğin:

- Sisteme sızanların hızla tespit edilip çıkarılması.
- Sistemlerin sanal makine teknolojisi gibi yöntemlerle saf hale getirilmesi.
- Veri erişiminin şifreleme yoluyla korunması ve sınırlandırılması.
- En hassas sistemleri korumak için ek güvenlik tedbirlerinin devreye alınması.

Kuruluşlar, bilgiler çalındığı takdirde suçlunun bundan menfaat sağlamasını zorlaştırmalı. Bankalar bu konuda önemli bir yol kat etti. Çip ve pin kodu teknolojileri ile olağanüstü faaliyetleri izleyen sistemleri bir araya getirerek, çalınan kredi kartı bilgilerinin kullanılmasını zorlaştırdılar.

Son olarak da, maddi çıkar sağlayan bir suçlunun bunu hemen paraya dönüştüremediği gerçeği var. Bu da, kara para aklama aşamasındaki pek çok kapıyı kapatma fırsatı veriyor. İngiltere Ulusal Siber Suçla Mücadele Birimi şimdilerde buna odaklanıyor. Dünyanın diğer bölgelerindeki kanun uygulayıcılar da yasa dışı para transferi ve işleme faaliyetlerine dair bazı görüşlere sahip. Örneğin FBI, geleneksel ve dijital suçluların pek çoğu tarafından "tercih edilen banka" haline geldiğini belirterek Liberty Reserve'ü 2013 yılında kapattı.

Meşru kuruluşların savunma mekanizmalarından daha etkin saldırı araçları ve stratejileri geliştiren bir online suç karaborsasından destek alan, iyi kaynaklara sahip, gelişmiş bir düşmanla savaşabilmek için, işletmelerin kanun uygulayıcılarla birlikte çalıştığı koordineli ve sorunsuz bir yaklaşım benimsememiz gerekiyor.

İngiltere Ulusal Siber Suçlarla Mücadele Birimi Direktörü Dr. Jamie Saunders, "Etkin bir suç önleme stratejisinin, iyi bir proaktif güvenlik ile sağlam bir saldırı önleyici yaklaşımını bir araya getirmesi gerekiyor. Suçluların, vatandaşlarımıza ve şirketlerimize saldırdıkları takdirde büyük bir risk alacaklarını anlamalarını sağlamalıyız" diyor.

Saldırganlarla savaşma - *Eylem adımları:*

- Kanun uygulayıcılarla işbirliği yapın. Bu, en kötü senaryo gerçekleştiği takdirde hızla yanıt vermeniz gereken güvenilir irtibatlarınız olmasını sağlayacaktır. Bu ayrıca, ekibinizin, organize siber suçla mücadele forumlarına katılabilmesine de imkan tanıyabilir.
- Mevkidaşlarınızla bilgi paylaşımında bulunun. Siber suç rekabet edilecek bir konu değil, çünkü tüm toplumu hedef alıyor ve siz de o hedeflerden birisiniz. Bu konudaki bilgi paylaşımının gizli ve güvenli bir ortamda yapılabilmesine yönelik çevrimiçi ve fiziki forumlar mevcut. Bu forumların hangilerinin sizinle en çok ilgili olduğunu belirleyin ve bunlara katılın.
- Suçluların, çalmayı başardıkları takdirde bilgilerinizden menfaat sağlama imkanlarını nasıl sınırlandırabileceğinizi araştırın. Bir kötüye kullanımı tespit ve bloke edip edemediğiniz veya bir ihlale hızlı yanıt verip veremediğiniz sorusunu kendinize sorun. Bu sorulara verdiğiniz yanıtlardan yola çıkarak, verilerin kötüye kullanılmasına yol açabilecek en olası senaryoları modelleyin. Verilerin kötüye kullanılması teşebbüslerinin hedefi olabilecek diğer kuruluşlarla (bankalar, kanun uygulayıcılar, tedarikçiler) işbirliği yapın.

Hız ihtiyacı

04

Geride kalmaya neden olan faktörler

Dijital saldırılar, sürekli güncellenen araç ve stratejiler kullanılarak göz açıp kapayıncaya kadar gerçekleştirilebiliyor. İşletmeler de suçlular kadar çevik ve hızlı davranmak zorunda, ancak verdikleri yanıtlar kurumsal, düzenleyici ortamdan kaynaklanan ve teknolojik nedenlerle geride kalabiliyor.

Görüştüğümüz işletmelerin **%49'u** yönetmelikler nedeniyle geri kaldıklarını söylüyor

%45'i gerekli beceri ve çalışanlara sahip değil

%46'sı eski sistemlere güvenmek nedeniyle geride kalmış

%38'i kuruluşlarındaki süreçlerin esnek olmadığını belirtti

%94'ü üçüncü taraflara güvenmek zorunda olmanın bir sorun olduğunu belirtiyor

Hız ihtiyacı

04

Tüm işletmeler hızla harekete geçmenin önemini anlıyor, ancak araştırmamız hızla harekete geçmenin önünde bazı engeller olduğuna işaret ediyor.

Katılımcıların %9'u, tehditlere yanıt verme konusunda bir engelle karşılaşmadığını belirtti.

Dijital güvenlik tehdidine hızla yanıt verme çabalarını engelleyen faktörlerin neler olduğunu sorduğumuz üst düzey karar alıcıların yaklaşık yarısı (%49) yönetmelikler nedeniyle kısıtlandıklarını, %45'i ise doğru becerilere ve insanlara sahip olmadıklarını belirtti. Katılımcıların %46'sı eski BT sistemlerini bir sorun olarak görürken, %38'i esnek olmayan kurumsal süreçlere işaret etti. Üçüncü taraf servis sağlayıcılara olan bağımlılık ve üçüncü taraflarla imzalanan sözleşmeler de, kültür değişimine karşı direnç ve yatırım eksikliği ile birlikte diğer engelleyici unsurlar olarak sayıldı.

En geniş anlamıyla düşünüldüğünde, online suç karaborsasının Ar-Ge faaliyetlerine ayak uydurma sorunu bir kenara bırakıldığında bile dijital güvenlik konusunda dinamik bir yaklaşım sergilemenin önünde pek çok engel olduğu görülebiliyor. Bu noktada da şu soru gündeme geliyor:

- Düzenleyici ortam rejimleri kuruluşların dijital tehditlere yanıt vermesini kolaylaştırmaktan ziyade zorlaştırıyor mu?
- Uyum konusuna odaklanmanın giderek artması, risklere yanıt verme hızını engelleyip kuruluş bünyesinde esnek olmayan bir kültür yaratıyor mu?
- İşletmeler güvenlik ihtiyaçlarını karşılayabilmek için üçüncü taraflara çok mu bağımlı?

Araştırmamız, şirketlerin büyük bir kısmının, güvenliği sağlamak, olayları soruşturmak, kuruluşun olaylara verdiği yanıtları koordine etmek ve diğer önemli fonksiyonlar için büyük ölçüde veya tamamen dış kaynak kullandığını ortaya koyuyor. Bu noktada da, hangi beceri ve kapasitelerin şirket içinde bulunduğu ve dış kaynak sunan hizmet sağlayıcının işletmenin güvenilir bir yanıt verebilmesi için ihtiyaç duyduğu şeyleri sağlayıp sağlayamadığı sorusu gündeme geliyor.

Diğer taraftan, katılımcılara, şirket içi güvenlik ekiplerinden neler beklediklerini de sorduk ve en önemli özellikler olarak hızlı tepki verme, çeviklik ve güven yanıtlarını aldık.

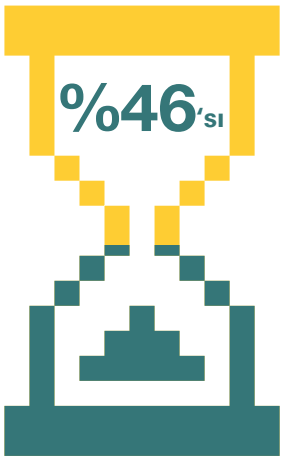
Bulmacayı çözmek

Kuruluşlar, güvenlik ekiplerinin hem hızlı tepki verebilmeleri hem de artan tehditlerle mücadele konusunda çevik olabilmeleri gerektiğini biliyor. Ama aynı zamanda, savunma mekanizmalarının etkinliğinin, güvenlik konusunda dış kaynak kullandıkları üçüncü taraflara güvenebilmek dahil pek çok faktör nedeniyle kısıtlandığını da hissediyorlar.

Bu noktada, değişen tehditleri algılayan ve buna yanıt verebilen bir güvenlik yaklaşımı benimsemek gerekiyor. Bu ise, tehdit ve zayıflık yönetimine odaklanmayı ve sürekli ortaya çıkan yeni tehditler karşısında mevcut savunma mekanizmalarını geliştirebilme kapasitesine sahip olmayı içeriyor. İşletmelerin, oyunda bir adım önde olabilmek için etkin bir dijital/tehdit istihbaratı kapasitesine ihtiyaçları var. Zira yeni trendleri ve tehditleri, bunlara gerektiği gibi yanıt verebilmelerini sağlayacak bir yaklaşımla tespit etmeleri gerekiyor.

Dijital tehdit istihbaratı kabiliyeti oluşturmak, saldırılarda kullanılan sistemler hakkında teknik bilgiler toplamaktan çok daha fazlasını ifade ediyor. Şirketlerin, potansiyel saldırganlar, bu saldırganların kullandığı araçlar, motivasyon kaynakları ve suistimal edebilecekleri zayıflıklar hakkında kanıta dayalı bilgi toplamaları gerekiyor. Şirketler, bu bilgileri birbirleriyle paylaşarak kendi güvenliklerini de geliştirebilir ve istihbarat toplama maliyetlerini düşürebilir. Tüm bunlar ise, mevcut tehditlerden ziyade gelecekte ortaya çıkabilecek tehditlere odaklanarak yapılmalı. Ayrıca, edinilen istihbaratın işe yarayabilmesi için harekete geçilebilir olması ve hızla kullanılabilmesi gerekiyor.

Tehditlere yanıt verme çabalarını en çok neyin etkilediğini CEO'lara sorduğumuzda,



eski BT sistemlerinin sorun olduğunu söyledi

Finans sektöründen önemli bir müşterimiz ise, tehdit istihbaratının önemini vurgulamakla birlikte bunun her zaman kullanılmadığı konusunda uyarıda bulunuyor. "İş zekasıyla istihbarat arasında her zaman bir paralellik var" diyerek ekliyor. Ortak saldırı düzenleri göz ardı edilmemeli. İşletmeler, bilinen tehlikelerle mücadele etmelerini sağlayacak araç ve süreçlere sahip olmak zorunda.

Ayrıca, sistemlerin oluşturulma yöntemini yeniden tasarlamak için de bazı fırsatlar var.

GSK ilaç bölümü Bilgi Güvenliği Başkanı Robert Coles'un da vurguladığı gibi, kuruluş bünyesindeki güvenlik kültürü bakımından insan unsurunun da göz ardı edilmemesi gerekiyor. Coles, "Kuruluş bünyesinde insan unsurunun, farkındalık yaratmanın, eğitimin ve kültürel değişim kaydetmenin önemini biliyoruz" diyerek, güvenlik kültürüne olumlu bir katkı yapmak için neler yapılabileceği konusunda Royal Holloway Üniversitesi'yle işbirliği yaptıklarını vurguluyor.

Uzmanlığı kullanmak

Dijital suç tehdidinin sürekli değiştiği bir ortamda, işletmeler, sahip olmadıkları uzmanlıkları nereden hızla temin edebileceklerini de bilmek zorunda (kendi içlerinden veya üçüncü taraf bir güvenlik sağlayıcıdan). Kısacası, dijital güvenlik sektörünün yanı sıra resmi makamlara ve gelişmekte olan siber sigorta sektörüne de önemli görevler düşüyor.

Çalıştığımız müşterilerle edindiğimiz deneyimlerle de desteklenen araştırmamıza göre, yönetim kurullarının sigorta şirketlerinden temel beklentisi müşterilere tazminat sağlayabilmeleri. Şirketlerin büyük kısmına göre, sigorta şirketlerinin görevi yükümlülükleri ve doğrudan maddi hasarı teminat altına almak ve kimlik sahteciliğine karşı koruma sağlamak.

Bununla birlikte, dijital suçun önlenmesi konusunda sigorta şirketleriyle daha yakından çalışma konusunda da güçlü bir beklenti var. Sektörün sunabileceği hizmetlerden biri de, şirketlerin başlıca güvenlik konuları hakkında üçüncü taraf uzmanlarla iletişim kurabilmelerini sağlamak.

İşbirliği

Kanun uygulayıcı makamlar ile işletmeler arasında işbirliği yapılmasına ihtiyaç var. Örneğin, kanun uygulayıcı makamlar suçluların kullandığı altyapıları kapatma yetkisine sahip, ancak bunu yapabilmelerini sağlayacak kaynaklara her zaman sahip olamayabiliyor. Şirketler ise, kanun uygulayıcı makamların kullanacağı araçların ve yürüteceği kampanyaların finansmanını üstlenebilir.

"Şirketler istihbarat toplasa da, kararlar genellikle içgüdüyle alınıyor. Tehdit istihbaratına ben de inanıyorum, ancak istihbarat harekete geçilebilmesini sağlıyorsa bir anlam ifade ediyor."

Bazı resmi kurumların finansal yardım almasının yasak olması gibi kısıtlamalar var. GSK'dan Robert Coles şunları söylüyor: "Sektör kanun uygulayıcı makamlarla işbirliği yapabilir, ancak bu konuda bazı sınırlar var. Bu noktada, kanun uygulayıcı makamlarla bir bilgi havuzu oluşturmaya odaklanılması gerekiyor."

Hız ihtiyacı

04

İşbirliğinin kapsamı, işletmeler ile kanun uygulayıcı makamlar arasındaki iletişimin ötesinde. Barclays'den Will Dixon, kendi sektörüne atıfta bulunarak şunları söylüyor: "Finans, telekom, internet servis sağlayıcılar ve resmi kurumlar arasında operasyonel ortaklıklar geliştirilerek işbirliğine yönelik operasyonel bir çerçeve oluşturulması gerekiyor. NCSC (Ulusal Siber Güvenlik Merkezi) ise bu konuda kilit bir rol oynayabilir.

Aynı veya benzer sektörlerde faaliyet gösteren şirketlerin ortak tehditler hakkında paylaşabilecekleri bilginin kapsamı çok daha fazlaysa da, bankacılık, telekom ve perakende gibi farklı sektörlerdeki şirketler arasında da suç faaliyetlerinin önlenmesine yönelik kritik işbirlikleri yapılabilir. Örneğin, suçluların banka güvenliğini aşmak için en çok başvurdukları yöntemlerden biri, telefonlarını kaybettikleri konusunda telekom şirketini ikna etmek. Telekom şirketi numarayı yeni bir SIM karta aktarınca hırsızlar da etkinleştirilen cihaz aracılığıyla telefonun gerçek sahibinin bankacılık şifrelerini sıfırlıyor veya iki kademeli kimlik doğrulama sürecini ele geçiriyor. Bankalar ve telekom şirketleri, birbirleriyle bilgi paylaşarak bu tür hırsızlıkları veya iki kademeli kimlik doğrulama mesajlarının suistimal edilmesini daha etkin bir şekilde önleyebilir.

Bilgi paylaşımı, şirketlerin güvenlik şirketlerinden bilgi satın alma zorunluluklarını ortadan kaldırarak önemli bir maliyet tasarrufu yapmalarına da yardımcı olabilir.

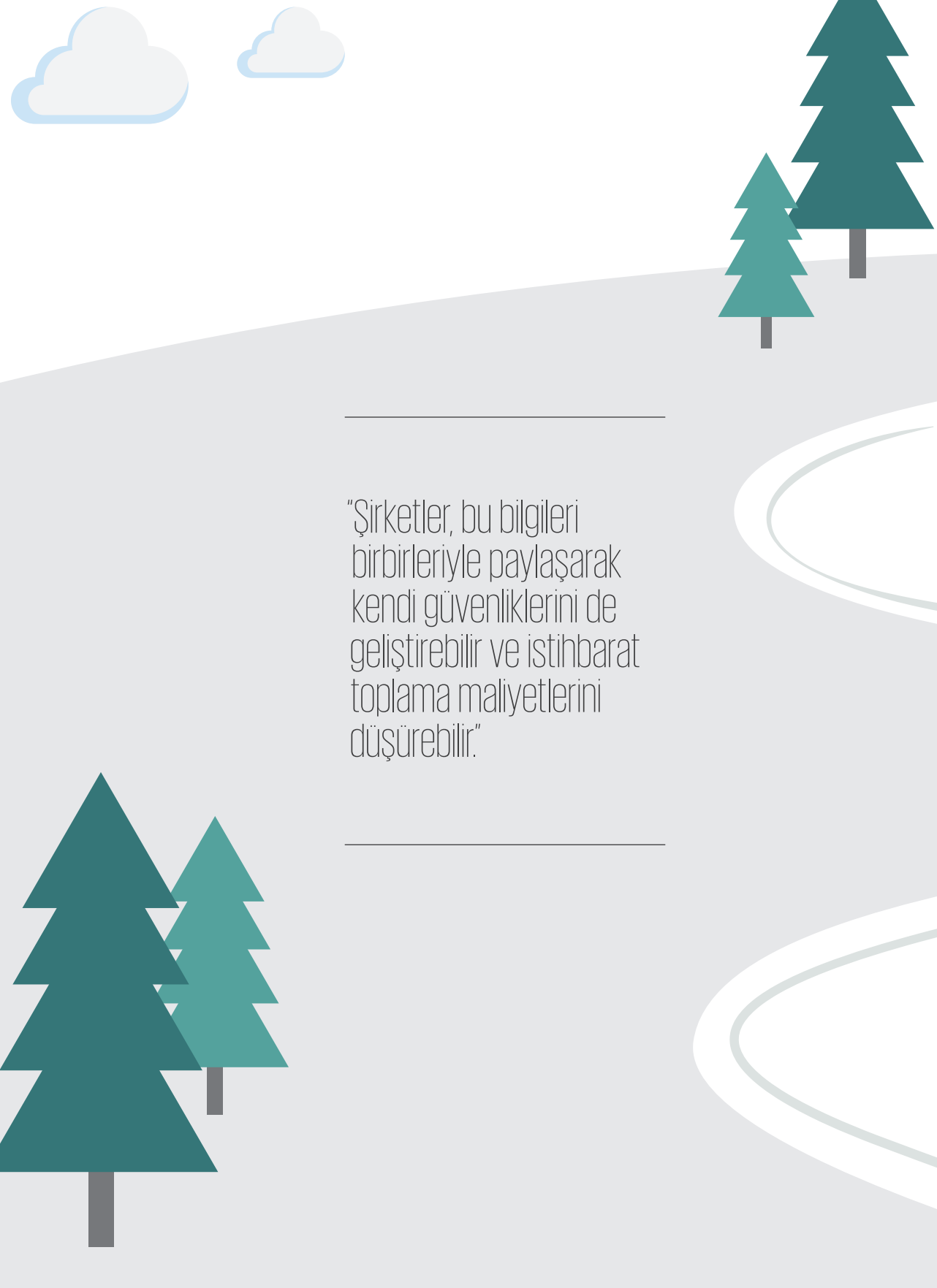
Şirketlerin, inovasyon konusunda ivmelendiricilerden veya iş geliştirmecilerden finansman temin edebilmeleri de mümkün. Bunun bir örneği ise Cylon (Cyber London) laboratuvarı. Özel sektör - kamu ortak finansmanıyla desteklenen Londra merkezli bu iş geliştirme merkezi, yeni açılan güvenlik şirketlerine, pazara sunmak üzere ürün ve hizmet geliştirme konusunda destek sağlamak amacıyla kuruldu.

Şirketler, güvenlik konusunda faaliyet gösteren ivmelendiricilerle veya iş geliştirme merkezleriyle birlikte çalışarak veya onlara finansman sağlayarak inovatif Ar-Ge faaliyetlerini destekleme fırsatı bulabilir.

Güvenlik İngiltere'nin yeni açılan teknoloji şirketleri ekosisteminde önemli bir bileşen ve Malvern Hills etrafındaki bölge hem kurulu hem de yeni işletmeler için önemli bir alan olarak görülüyor. Kuruluşların yapması gereken ise bu inovasyon sürecine katılmak ve proaktif olmak. Bu da, inovasyon fırsatlarının belirlenmesi konusunda kıdemli güvenlik personeline sorumluluk verme anlamına gelebiliyor. Barclays'den Will Dixon, "Bir dijital inovasyon yöneticimiz var" diyerek ekliyor: "Bu kişinin görevi, inovatif teknolojileri belirlemek ve bunlara karşılık vermek."

Hız ihtiyacı - *Eylem adımları:*

- Siber güvenlik ekibinizin değişen tehditlere hızla ve esnek bir şekilde yanıt verebilecek kapasiteye sahip olduğuna dair kanıtlar isteyin ve bunu başarabilmeleri için ihtiyaç duydukları yetki ve desteği onlara verin.
- Önemli bir olayı birlikte tatbik etmek amacıyla başlıca müşterilerinizle ve üçüncü taraflarla çalışın. Zira gerçek bir saldırıya uğrarsanız bunların işbirliğine ihtiyaç duyacaksınız, ayrıca bu sayede yakın bir işbirliği yapmak aranızdaki güven ve şeffaflığı da güçlendirecektir.
- En kötü senaryoya hazırlanın. Olası bir siber saldırıya vereceğiniz yanıtı tatbik edin ve bir "kas hafızası" geliştirin. Bu, bir olayın nasıl ortaya çıkabileceğini ve buna nasıl yanıt verebileceğinizi daha iyi anlamanızı sağlayarak hızlı yanıt vermenize yardımcı olacaktır.
- Siber sigortanın, olası maddi etkileri azaltma ve ihtiyaç duyduğunuzda uzmanlık bilgilerine erişme konusunda size nasıl yardımcı olabileceğini düşünün. İhtiyaç duyduğunuz her beceriye şirket bünyesinde sahip olamayacağınızı unutmayın.



"Şirketler, bu bilgileri birbirleriyle paylaşarak kendi güvenliklerini de geliştirebilir ve istihbarat toplama maliyetlerini düşürebilir."

Risk ve Fırsat

05

Dijital Risk Başkanı'nın dünyası

Dijital riskler ve fırsatlar bir madalyonun iki yüzü gibidir. İşletmeler, dijital dönüşüm süreçlerini kararlı bir şekilde sürdürürken kaçınılmaz olarak daha fazla riske maruz kalır ve sağlam bir güvenlik mekanizmasına sahip olmadıkları takdirde müşterilerine daha etkin hizmet sunma ve şirket içi süreçleri optimize ederek yeni kanallar aracılığıyla satışları artırma konusundaki fırsatlardan yararlanamaz. Günümüzde pek çok işletme, güvenliği stratejik bir kolaylaştırıcı haline getirmeye çalışıyor ve bu gelişme Dijital Risk Başkanı pozisyonunun doğmasına yol açmış durumda.

Digital Risk Başkanı'nın Görevleri

Dijital Risk İnovasyonu

- İnovasyonun İzlenmesi ve İnovasyondan Faydalanma
- Yeni Ürünlerdeki Dijital Suç Kısa Devreleri

Dijital Risklerin Belirlenmesi

- Birinci ve İkinci Seviye Veriler Arasındaki İlişki
- Dahili ve Harici Kayıp Veri Analizi
- İş Süreci Haritalandırması
- Senaryo Analizi
- Nicel Ölçüm ve Karşılaştırma Analizi

Dijital Risklerden Korunma

İzleme ve Raporlama:

- Dijital Hijyen Uygulaması
- Dijital Risk Analizleri

Denetim ve Risk Azaltma:

- Dijital Stres Testleri
- Risk Devri Seçeneklerinin Doğrulanması

Dijital Suç Tespiti

- Gerçek Zamanlı Dijital Risk İstihbaratı Paylaşma
- Dinamik Risk Profili Değerlendirme
- Detaylı Öğrenme Bildirimleri

Dijital Risk Yanıtı

- Uyumlaştırma Aracılığıyla Otomatik Yanıt
- Kontrol Altına Alma Stratejileri: Patlama Çapını Sınırlandırma
- Saldırıya Dayalı Stratejiler: Dijital Suç Avcılığı
- Dijital Riskler Hakkında Finans Makamlarına ve Düzenleyici Makamlara Yapılan İfşalar

Dijital Riskten Sonra Kurtarma

- Dijital İş Sağlamlığı ve Sürekliliği

Risk ve Fırsat

05

Etkin güvenliğin sunacağı ödül sadece sistem ihlallerinin önlenmesiyle sınırlı değil. Dijital riskler ve fırsatlar bir paranın iki yüzü gibidir. İnternet tabanlı e-ticaretin doğduğu 1990'lı yılların ortalarından bu yana işletmeler müşterilerine daha fazla ürün satmak ve daha iyi hizmet sunmak amacıyla bilgisayar, cep telefonu ve tablet gibi yeni kanallardan ve platformlardan faydalandı.

Sahne arkasında ise, işletmeler dahili süreçlerini geliştirmeye ve maliyetlerini azaltmaya devam ediyor. Bu inovasyon büyük ödüller sunmakla birlikte bazı riskleri de beraberinde getiriyor. Örneğin, temel bir e-ticaret seçeneğini mobil platformların yanı sıra ağ tabanlı çoklu kanal stratejilerine de (tıkla ve tahsil et gibi) genişleten bir işletme, aynı zamanda değer zincirinde suçlular için yeni suistimal noktaları da yaratmış oluyor.

Sağlam bir güvenliğe sahip olmak elbette belli bir rekabet avantajı da getiriyor. Barclays'den Will Dixon'ın da vurguladığı üzere, güven, özellikle bankacılık sektöründe marka gücünün temelini oluşturuyor. Güvenlik konusunda proaktif bir yaklaşım benimsenmesi ise bu güvenin yaratılmasında kritik rol oynuyor. Örneğin Barclays, konuyu Digital Eagles (Dijital Kartallar) temasıyla kamuoyuyla paylaşarak güvenliği müşterilerine sunduğu hizmetlerin önemli bir unsuru olarak konumlandırdı. Banka ayrıca, müşterilerine ücretsiz güvenlik yazılımları da sunuyor.

Güven konusu pek çok seviyede karşımıza çıkıyor. En temel seviyede baktığımızda, bir müşterinin belli bir işlem yapmak için öncelikle o sistemin güvenli olduğuna inanması gerekiyor. Pek çok insan, bilgilerinin güvende olacağına ikna olmadan hiçbir bilgisini web siteleri aracılığıyla vermiyor. Daha detaylı baktığımızda ise, güven, marka gücünün ve müşteri sadakatinin korunmasında kilit bir unsur.

Müşteri sadakati ise bir anda ortadan kaybolabiliyor. Önemli bir güvenlik ihlali çoğu zaman müşterilerin o markadan kopmasına yol açıyor.

Daha da önemlisi, günümüzün ticaret ortamında ağların kullanılmadığı çok az satış, müşteri hizmetleri veya idari birim inovasyonu var. Tüm inovasyonun katalizörü olarak nitelendirebileceğimiz güvenlik, yeni fikirler ve yeni kanallar yaratmaya çalışan şirketlerin işini kolaylaştırıyor.

Kullanıcı deneyimi

Bu noktada karşılaşılan zorluk, belirlenen fırsatlar ile risklerden korunma arasında doğru bir denge kurabilmek. Tüketicilere yönelik bir perakende satış sitesinde yaşanabilecek bir müşteri deneyimini düşünelim. Hem bankalar hem de perakende şirketleri kredi kartı sahteciliğini ortadan kaldırmak istiyor ve bunun etkin yollarından biri müşterilerden işlemin tamamlanması için kart şifresini girmelerini istemek.

> "Kullanıcı deneyimi ile güvenlik arasında iyi bir denge kurmak gerekiyor"

Bu tür sistemler, işlemin tamamlanmasının önünde engel de teşkil ediyor. Örneğin, kendisinden şifre girmesi istenen pek çok müşteri işleme devam etmiyor ve alışveriş sepetini öylece bırakıyor. Bu nedenle de, kullanıcı deneyimi ile güvenlik arasında iyi bir denge kurmak şart.

Güvenliğe daha fazla vurgu yapılıyor

Görüştüğümüz yöneticiler, bazı avantajlardan faydalanma konusunda kararlı görünüyordu. Katılımcıların %92'si dijitali yeni fırsatlar yaratmak için bir araç olarak görüyor, %89'u verimliliği artırma konusunda kararlı, %83'ü ise daha iyi müşteri hizmetleri sunabilmeyi hedefliyor.

Katılımcılar ayrıca, fırsatlar peşinde koşmanın güvenlik yöneticilerinin üzerine yeni yükler de bindireceğini söyledi. Katılımcıların %70'i dijital güvenliğe daha fazla odaklanılmasını istediğini, %62'si ise mobil alanına daha fazla odaklanılmasını umduğunu söyledi. Katılımcıların yaklaşık yarısı, güvenlik yöneticilerinin çok daha stratejik bir rol oynamalarını istediğini belirtti.

Dijital Risk Başkanı

Peki bu, uygulamada ne anlama geliyor?

Son yıllarda görülen trendlerden biri de, görevleri genellikle klasik analog işletmelerden dijital işletmelere geçişi denetlemek olan Dijital Başkanı pozisyonunun ortaya çıkması. Bu, içeriği itibarıyla dijital uzmanlığı üst düzey yönetim becerileriyle birleştiren stratejik bir pozisyon. Buna paralel olarak da, Bilişim Güvenliği Başkanı güvenlik sorumluluğunu üstleniyor.

Şu anda yaşadığımız, niteliksel anketimize katılanların verdiği yanıtlarla da kendini gösterdiği üzere, aslında dijital görevlerin yeniden tanımlanması. Bazı şirketler, güvenlik sorumluluğunu üstlenmenin yanı sıra şirketin müşterilere daha iyi hizmetler sunabilmesini ve idari birim sistemlerinin optimize edilebilmesini de sağlayacak inovatif kanallar, politikalar ve uygulamalar geliştirmekle de sorumlu olan Dijital Risk Başkanlarını görevlendiriyor (veya en azından Bilişim Güvenliği Başkanı'nın bu tür bir pozisyona terfi ettirilmesini bekliyor).

Risk ve Fırsat

05

Bunun çok yönlü bir pozisyon olmasını bekliyoruz. Dijital Risk Başkanı, tehditlerin önlenmesini, belirlenmesini ve olay yönetimini çevreleyen tüm sorunları anlamak zorunda. Diğer taraftan, Dijital Risk Başkanı, şirketin satışlarını ve performansını artırmasına yardım eden kilit bileşenin güvenlik olduğu bir "gerçekleşmesini kolaylaştırma" görevini de üstlenecek. Dijital Risk Başkanı ayrıca, kurumsal yönetim, risk yönetimi politikalarının geliştirilmesi, uyum ve denetim gibi fonksiyonlarla da yakın çalışma içerisinde olacak. Bu noktada ise, sadece uyum odaklı bir onay kutusu işaretleme işinden sıyrılıp fırsatlardan faydalanmayı kolaylaştırmaya ve çeviklik sergilemeye odaklanmak gerekiyor.

Risk ve fırsat - *Eylem adımları:*

- Güvenlik, fırsat ile risk arasında denge kurmakla ilgili bir konu. Güvenliği dijital stratejinize ve yeni kanallar geliştirme faaliyetlerinize entegre edin. Bu, doğru yaptığınız takdirde müşteri deneyimini geliştirmenize yardımcı olacaktır. Şirketinizin, yeni uygulama yollarını hayata geçirirken müşterilerinize güvenli bir hizmet sunmak için siber güvenliği nasıl kullandığını düşünün. Güvenlik konusundaki kararlı duruşunuzu şirket dışındaki taraflara nasıl ilettiğinizi değerlendirin.
- Dijital güvenliğin teknik bir konu olmadığını unutmayın. Bu, birbirine dev bir ağ ile bağlanmış dünyamızda iş yapmanın bir parçası ve sizin şirketinizin de stratejik planlama sürecinin bir parçası olması gerekiyor. Dijital güvenliğin şirketinizin yıllık ve stratejik planlama süreçlerine entegre edilmiş bir iş akışı olup olmadığını sorun.
- Dijital stratejinizin merkezine, Dijital Risk Başkanı gibi tamamen farklı bir güvenlik sorumlusu getirmeyi düşünün.

"Tüm inovasyonun katalizörü olarak nitelendirebileceğimiz güvenlik, yeni fikirler ve yeni kanallar yaratmaya çalışan şirketlerin işini kolaylaştırıyor."

Sonuç

Dijital suçla savaş eninde sonunda kaybedilir diye bir şey yok; ancak bolca kaynağa sahip, iyi finanse edilen ve kararlı bir düşmanı yenmek için işletmelerin dijital güvenlik yaklaşımlarını değiştirmeleri gerekiyor.

Sadece savunma odaklı olmak ve suçluları sistemlerden uzak tutmak için güvenlik bariyerleri koymak yeterli değil. İşletmeler bunun yerine proaktif olmayı planlamalı ve saldırılara yanıt vermekle kalmak yerine saldırganların faaliyetlerine karşı aktif hareket etmeli. Ancak bu, özel sektör şirketlerinin başına buyruk bir şekilde uygulayabilecekleri bir eylem tarzı anlamına gelmiyor. Örneğin robot ağlarını yasaklamak veya kara para aklama faaliyetlerine sıkı denetimler getirmek gibi faaliyetler kanun uygulayıcı makamların yetki alanına giriyor.

"Dijital suçla mücadele konusunda işbirliği yapmak tüm sektörlerdeki şirketlerin çıkarına."

İşletmeler, benzer şirketlerle ve kanun uygulayıcı makamlarla işbirliği yapabilir, hatta bunu yapmalı. Telekom şirketleriyle, internet servis sağlayıcılarıyla, bankalarla, kredi kartı şirketleriyle, sigorta şirketleriyle ve güvenlik sektörüyle birlikte çalışmalı ve suçluların hedeflerine ulaşmalarını daha zor ve daha yüksek maliyetli bir hale getirmeliler. Dijital suçla mücadele konusunda işbirliği yapmak tüm sektörlerdeki şirketlerin çıkarına. Şirketler, birlikte çalışarak istihbarat paylaşabilir, inovasyonu birlikte finanse edebilir, en iyi uygulamaları paylaşabilir ve ortak stratejiler geliştirebilir.

İşletmeler ayrıca, şirket içi departmanlar ve fonksiyonlar arasında işbirliğini de desteklemek zorunda. Bunu ise, güvenlik ve hileyle mücadele ekiplerinin birlikte çalışarak sistem ihlallerinden saldırganların çaldıkları verileri kullanarak veya satarak faaliyetlerini paraya dönüştürdükleri noktaya kadar her adımda suç faaliyetleriyle mücadele etmelerini sağlamak gibi yöntemlerle yapabilirler. Diğer taraftan, hiçbir sistemin %100 güvenli olamayacağı ve bu nedenle tüm kuruluşu kapsayan bütüncül bir yaklaşım benimsemek gerektiği unutulmamalı.

Güvenlik stratejilerinizi geliştirirken saldırganlar gibi düşünmeniz ve bu stratejileri denemeniz de oldukça önemli. Proaktif olun, harekete geçirilebilir istihbarat isteyip toplayın, saldırganların motivasyon unsurlarını anlayın, değişen dijital suç trendlerini haritalandırın ve bu bilgileri hem güvenlik ekiplerinizi donatıp yönlendirmek hem de farkındalığı tüm kuruluş bünyesine yaymak için kullanın. Güvenliği sadece bir uyum konusu olarak değil aynı zamanda yeni tehditleri belirlemeye, değerlendirmeye ve bunlara etkin bir şekilde yanıt vermeye yönelik kesintisiz bir süreç olarak gören bir kültür yaratın.

Bunun ödülünü ise daha iyi bir işletme olarak alacaksınız. Güvenlik, dijital inovasyonu kolaylaştıran ve sonuçta kâr getiren bir unsur. Gelecek ise, şirketlerin stratejik hedeflerine ulaşabilmeleri için güvenliği her şeyin merkezine koymalarını gerektiriyor. Bu sayede pek çok sınır ortadan kalkacak. Yarının başarılı şirketleri, düşmanı tanıyan ve sistem ihlalinden suçu paraya çevirmeye kadar her adımda düşmanı korkutmak amacıyla diğer paydaşlarla işbirliği yapan şirketler olacak. Bunun ödülü ise daha az risk ve daha yüksek performans.

Referanslar

1. https://www.bcg.com/documents/file100409.pdf
2. http://www.mcafee.com/uk/resources/reports/rp-economic-impact-digitalcrime2.pdf
3. http://blog.trendmicro.com/the-most-prominent-cyber-threats-faced-by-high-target-industries/
4. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf
5. https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security
6. http://fortune.com/2016/02/09/obama-budget-cybersecurity/
7. http://www.gartner.com/newsroom/id/3135617
8. https://www.cert.gov.uk/wp-content/uploads/2015/05/Annual-Report-including-4th-Quarter-FINAL.pdf
9. http://www.nytimes.com/2016/05/01/business/dealbook/hackers-81-million-sneak-attack-on-world-banking.html?_r=0
10. Belirtilen 5 dolarlık tutar, çeşitli online suç karaborsaları anketlerinden elde edilen, DDoS saldırıları gerçekleştirmenin saatlik maliyetidir
11. Belirtilen 40.000 dolarlık tutar, Kasım 2014'te Incapsula tarafından gerçekleştirilen DDoS Saldırılarını Önleme araştırmasından alınmıştır https://www.incapsula.com/blog/DDoS-impact-cost-of-DDoS-attack.htm
12. http://www.interpol.int/News-and-media/News/2015/N2015-223
13. http://www.verizonenterprise.com/verizon-insights-lab/dbir/

İletişim:

İstanbul
Rüzgarlıbahçe Mh. Kavak Sk. No:29
Kavacık 34805 Beykoz / İstanbul / Türkiye
T: +90 216 681 9000

Ankara
The Paragon İş Merkezi Kızılırmak Mah. Ufuk
Üniversitesi Cad. 1445 Sok. No:2 Kat:13
Çukurambar 06550 Ankara / Türkiye
T: +90 312 491 7231

İzmir
Heris Tower, Akdeniz Mah. Şehit Fethi Bey Cad.
No:55 Kat:21 Alsancak 35210 İzmir / Türkiye
T: +90 232 464 2045

kpmg.com.tr
kpmgvergi.com
kpmgdenetimkomitesi.com