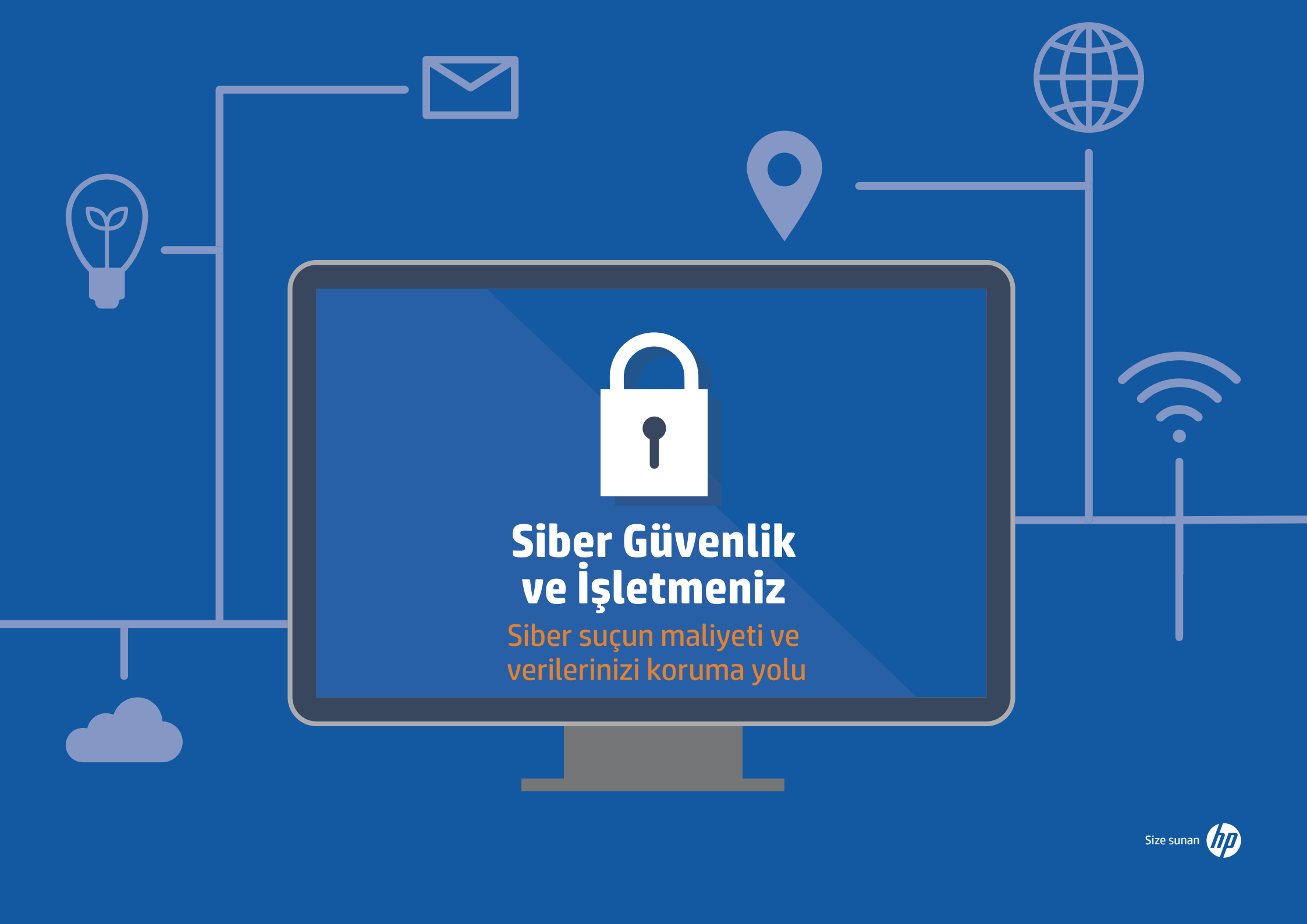


Siber Güvenlik ve İşletmeniz

Siber suçun maliyeti ve verilerinizi koruma yolu

Size sunan

İçindekiler

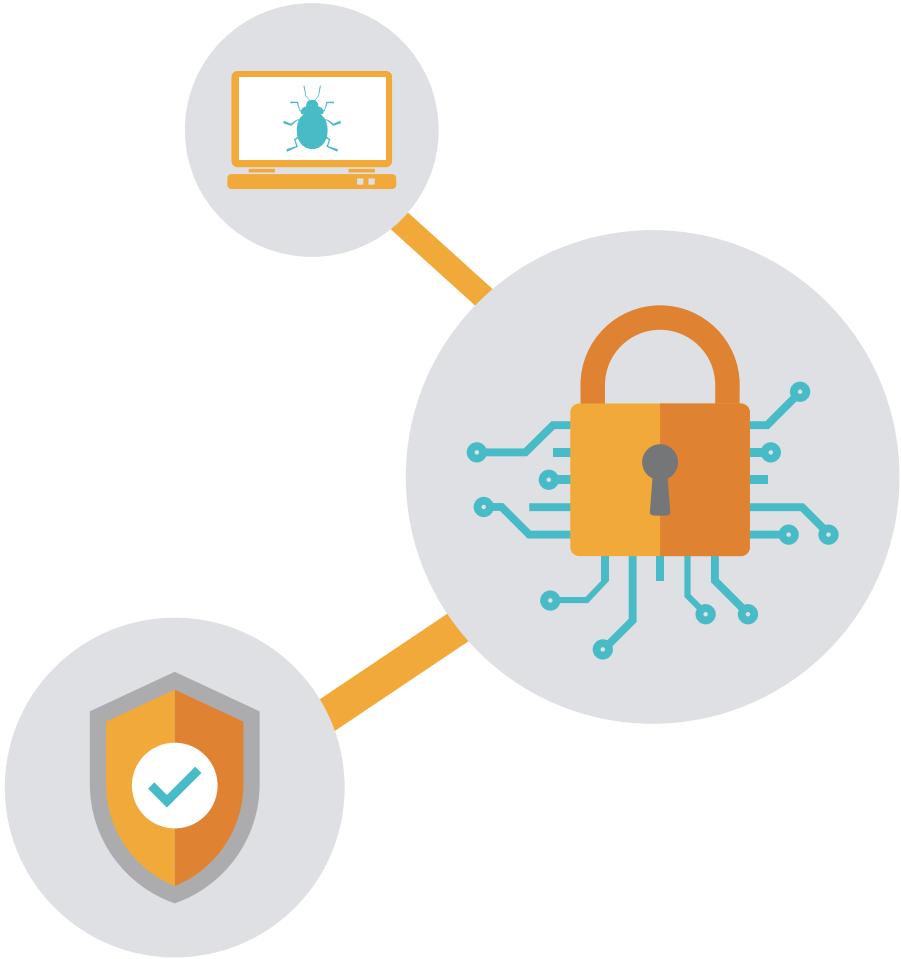
Giriş

“Pek çok yönetici, siberi neslimizi tanımlayacak risk olarak ilan ediyor.” – Dennis Chesley, Global Risk Consulting Leading, PwC[1]

Siber güvenlik, yeni bir tehdit değildir. Ancak büyüyen bir tehdittir. Bilgisayar korsanları her geçen gün daha iyi oluyorlar. Ve bir ağa girmek için daha fazla noktaya sahipler. Nesnelerin İnterneti, sıklıkla en kolay giriş noktası olan uç nokta cihazlarının sayısını katlayarak artırıyor. Hedefler hem boyut olarak hem de ölçek olarak artıyor.

21 Ekim 2016'da, ABD'de yerleşik DNS sağlayıcı Dyn tarihteki en büyük dağıtık hizmeti engelleme (DDoS) saldırısını yaşadı. Dünyanın en büyük web sitelerinden birkaçı – Netflix[2] Amazon ve Twitter dâhil – saatler boyunca çevrimdışı kalmak zorunda kaldı.

Ocak 2017'de, Lloyds Bank önemli çevrimiçi kesintiler yaşadı. Müşteriler hesap bakiyelerini kontrol edemedi veya ödeme yapamadılar. Mobil uygulama tabanlı erişim de çöktü. Lloyds henüz herhangi bir durumu teyit etmemiştir, ancak bunun nedeninin bir DDoS saldırısı olduğu güçlü bir biçimde dillerde dolaşmıştır.[3]



Kaynaklar: [1] PwC: The Global State of Information Security Survey 2016 [2] http://thehackernews.com/2016/10/dyn-dns-ddos.html [3] https://www.theguardian.com/business/2017/jan/23/lloyds-bank-accounts-targeted-cybercrime-attack

Giriş

Bunun gibi ihlaller, kötü reklâmdan daha fazlasıdır. Gerçek paraya mâl olurlar.

Spiceworks kaynaklı 2016 Yazıcı Güvenlik Anketi Raporunda, kuruluşların yüzde 34'ü ihlallerin artan yardım masası aramaları/ destek zamanı anlamına geldiğini, yüzde 29'u ihlallerin üretkenliği/ verimliliği azalttığını ve yüzde 26'sı, bir sorun olarak sistem kesintilerindeki artışı belirtmiştir.[4]

Bir IBM CSO Değerlendirme raporu için mülakat yapılan güvenlik liderlerinin yüzde 60'a yakını saldırganların bilgi düzeylerinin kendi kuruluşlarının savunmalarının ileri düzeyini aşmış olduğunu söylemiştir.[5]

Endişeli CIO'lar, siber güvenliği on yılı aşkın bir süredir ilk 10 sorun olarak belirtmiş ve siber güvenlik şu anda yıllık SIM Trends çalışmasında ikinci sıraya yerleşmiştir.[6]

Bu zararın çoğu önlenebilir. İlerleyen sayfalarda, siber güvenlik hakkındaki yaygın yanlış kanıları ele alacak, siber suçun işletmelere yaptığı etkiye ve saldırılara karşı daha iyi savunma yapmak için neler yapabileceğinize daha ayrıntılı bir biçimde bakacağız. Son olarak, geleceğe bakacak ve gelecekte bizi nelerin beklediğini ve nasıl hazırlanmamız gerektiğini tartışacağız.

Kaynaklar: [4] HP Printer Security Research 2016, Spiceworks [5] IBM CSO Assessment 2014 [6] SIM IT Trends Survey 2015

Çürütülen siber güvenlik efsaneleri

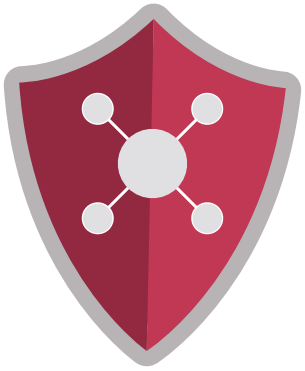
İşletmeleri bir siber suç riskine sokan
Beş Yaygın Yanlış Kanı

Manşetlerde veri ihlalleriyle ilgili olarak tanınmış markaları görebilirsiniz, ancak her türlü kuruluş risk altındadır. Burada, işletmeleri bilgisayar korsanlarına karşı hassas kılan beş siber güvenlik masalı verilmektedir.

Güvenlik İhlali

Güvenlik Sızıntıları

Güvenlik Uygulamaları



Antivirüs Yazılımı

Siber Saldırı

1 İşletmeler herhangi bir ihlalden çabucak kurtulabilirler

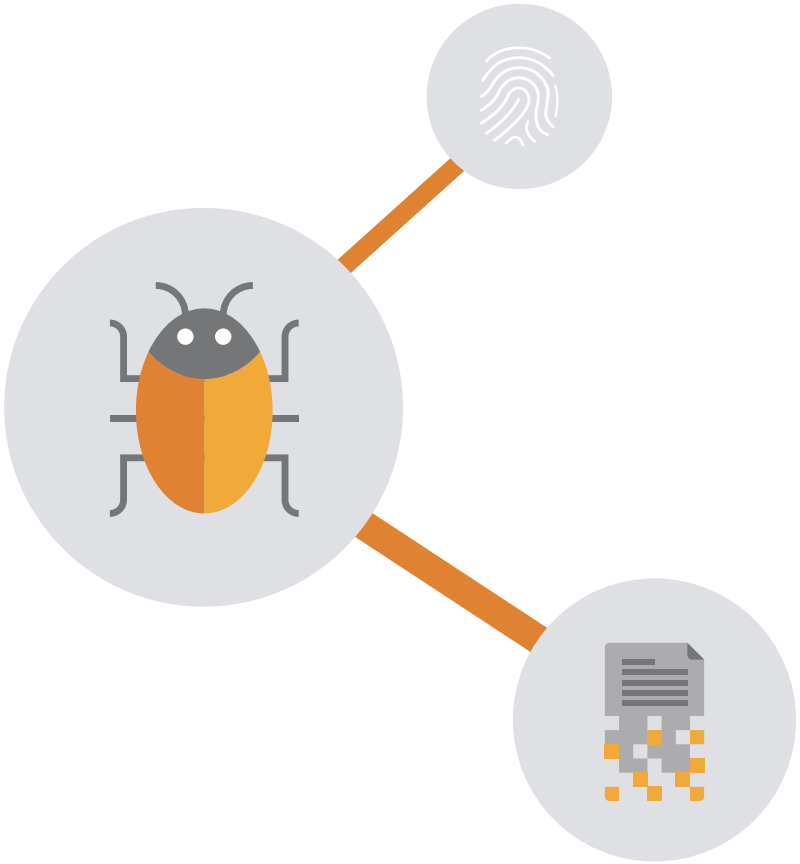
Siber güvenlik ihlallerinin ticari kuruluşlara maliyetini ölçmek hâlâ çok zordur. Önceleri, ihlallerin etkisinin hisse senedi fiyatlarındaki düşüşlerde görülebileceğine inanılırdı.

Ancak, hisse fiyatları hikâyenin sadece bir kısmı ve bunun birinci kısmı. Hisselerin birkaç hafta içinde eski pozisyonlarına dönmelerine karşın, daha uzun vadeli maliyetler birikir. Yeni güvenlik programları. Yedek personel. Yasal harcamalar.

Tüm bu faktörler, bir işi bir ihlali takiben uzun süreler boyunca önemli ölçüde kesintiye uğratabilir. Ve maliyetler artar. Yakın tarihli bir Ponemon çalışmasına göre, bir ihlale dair ortalama yıllık olarak hesaplanmış maliyet 2015'te **7,7 milyon ABD dolarından** 2016'da **9,5 milyon ABD dolarına** artmıştır.[7]

Kaynak: [7] Ponemon Institute Cost of Cyber Crime Study 2016

2 Güvenlik sızıntıları nadiren oluşur, bu nedenle ciddi koruma gerekmez



IDC güvenlik ihlali yaşayan işletmelerin oranının 2016'da yüzde 99'a ulaştığını ortaya koymuştur.[8] İhlal yaşadığını bildiren şirketlerin sayısı 2014'te yüzde 9 iken 2016'da yüzde 18,9'a sıçrayarak bir yılda 6-10 kat artmıştır.[9]

Bu rakamlar iyimser olabilir. İhlaller şirketlerin kendileriyle ilgili olumsuz medya haberlerinden kaçınmayı amaçlamaları nedeniyle, sıklıkla daha az olarak bildirilmektedir.

Bu efsanenin kaçırdığı diğer nokta, bir sızıntının yapabileceği zayıflatıcı etkidir. Belki şirketiniz sadece bir sızıntı yaşar. Ancak bir sızıntı, önemli zorluklara neden olabilir.

Kaynak: [8] IDC [9] Ponemon Institute Cost of Cyber Crime Study 2016

3 Güvenliği ele almak için bir BT uzmanını işe aldık, başka bir şey bilmemize gerek yok.

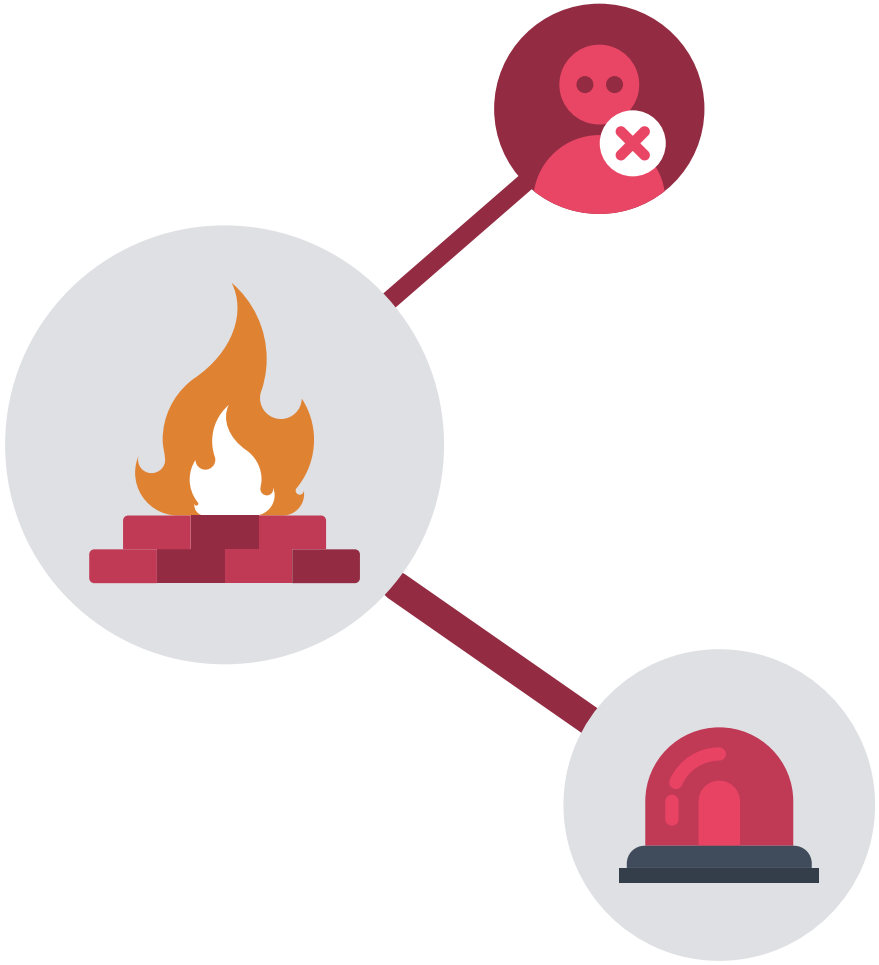
Bir uzmanı işe almak iyi bir fikir olsa da, şirketteki her çalışan da iyi siber güvenlik uygulamalarında eğitilmelidir.

Bir meslekteşınızın şüphelenmeden kötü amaçlı bir e-posta ekini indirdiğini veya güvensiz bir web sitesini ziyaret ettiğini ve böylece şirket ağını enfekte eden bir kötü amaçlı yazılımın bilgisayarları zayıflattığını ya da hassas bilgileri bir siber suçluya gönderdiğini düşünün.

CyberEdge'in hazırladığı 2016 Siber Tehdit Raporuna göre, kuruluşlar güvenlik tehditlerine karşı kendilerini savunmalarını engelleyen önde gelen bir sorun olarak 'çalışanlar arasında düşük güvenlik farkındalığını' sıralamaya almıştır. Bu, 'bütçe eksikliği' ve 'nitelikli personel eksikliğini' daha üst sıraya yerleştirmiştir.[10]

Kaynak: [10] Ponemon Institute Cost of Cyber Crime Study 2016

4 Sistemlerimizde güçlü antivirüs yazılımına sahibiz, böylece iyi korunuruz

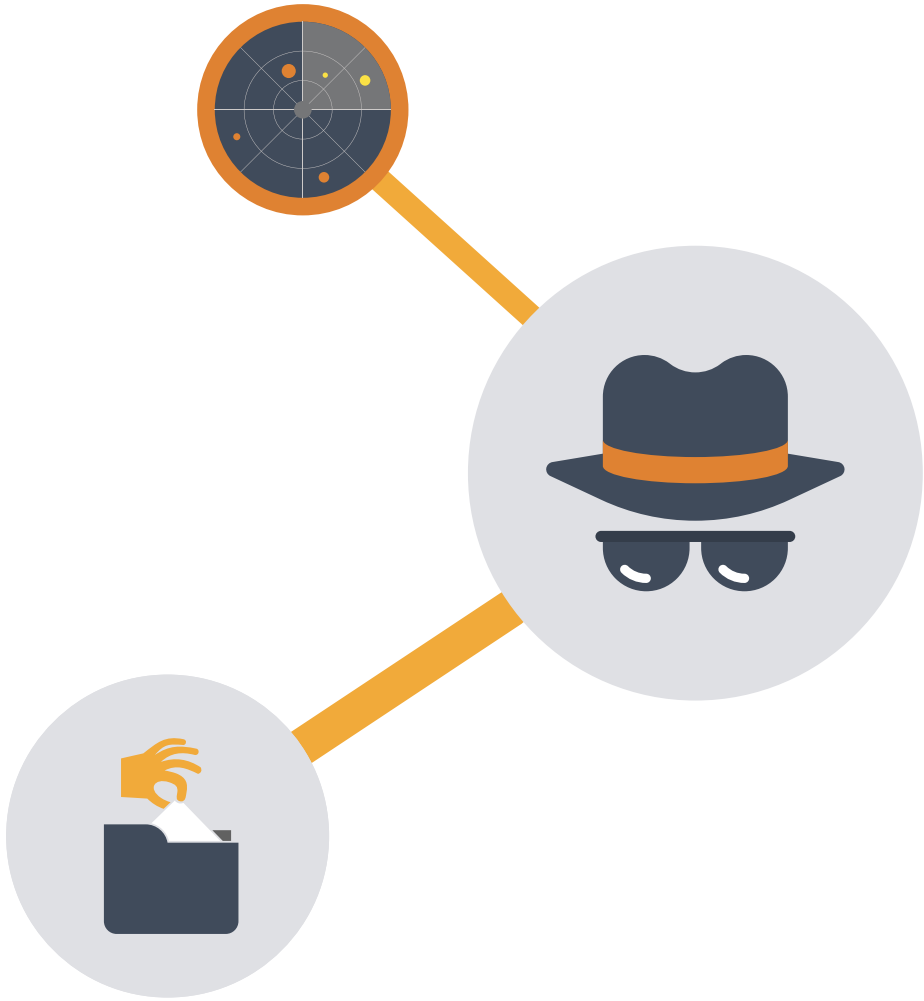


Antivirüs yazılımı, web sitelerinden veya e-postalardan indirilen kötü amaçlı yazılıma karşı sistemleri tarayarak çalışır. Ancak saldırganlar, bu korumayı baypas edecek başka yollara sahiptir.

Antivirüs yazılımı tarafından engellenemeyecek siber saldırılar, bir web sitesinin kendisini yavaşlatan veya çalışmasını durduran çöp posta trafiği ile boğulduğu dağıtık hizmeti engelleme saldırılarını (DDoS); korsanların kötü amaçlı kodları veri hırsızlığı veya uzaktan gözetleme gibi amaçlar için bir siteye yerleştirdiği ve korsanların çalıntı cihazlar yoluyla erişim elde ettiği web tabanlı saldırıları içerir.

5 Bir saldırgan içeri girerse, derhal fark ederiz

Bir siber saldırıyı tespit etmek kolay değildir. Bir sisteme giren kötü amaçlı yazılım operasyonları hemen kesintiye uğratmaz, bunun yerine genellikle tüm ağa erişmek amacıyla daha spesifik hedeflere yönelik saldırılar planlaması için korsana bilgi sağlamak amacıyla sistemi gözetleyebilir.



Belirli sistemlere yönelik bu tür saldırılar, gelişmiş kalıcı tehditler (APT) olarak sınıflandırılır. APT saldırıları, sürekli izleme ve genellikle tespit edilmeden zaman içinde belirli bir bilişim altyapısından veri elde etme eylemleriyle karakterize edilir.

Daisy Group BT danışmanlık şirketi, İngiltere'deki işletmelerin yarısının yarım saatten daha kısa bir süre içinde kırılabileceğini tahmin etmiştir.

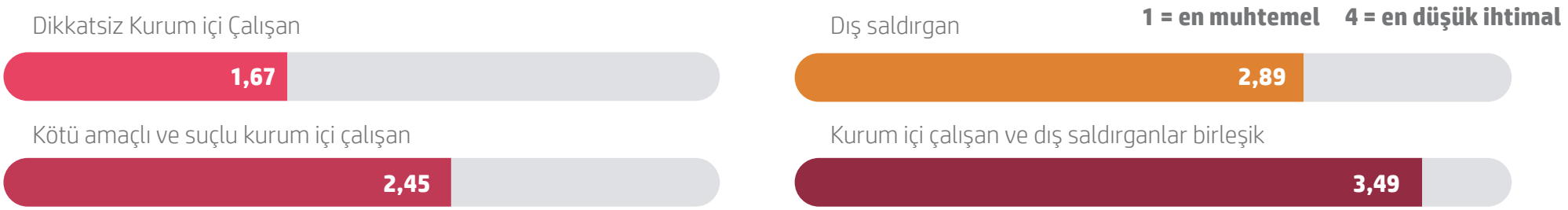
İPUCU:
Normalden daha yüksek hızlarda giden veri trafiğini izlemek, veri hırsızlığının belirlenmesine yardımcı olabilir; bu, bir APT saldırısı olabilir.

EYLEME GEÇİN:
Kötü amaçlı bir saldırı tespit edildiğinde veri tehlikeye girmeden önce ihlalleri durdurarak bilgisayarın BIOS'unu otomatik olarak geri yükleyen HP SureStart gibi veri korumalı bir güvenlik yazılımını seçin.

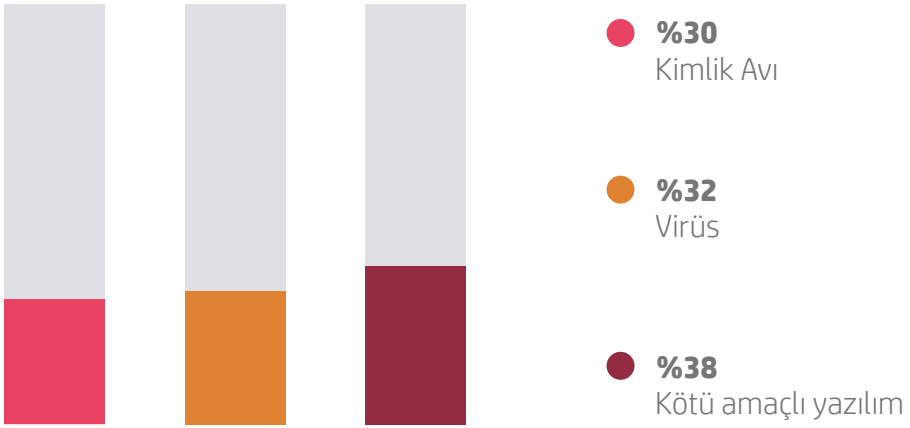
Tehditler nereden gelir?

Ağınızı korumak en zayıf halkaları öğrenmekle başlar

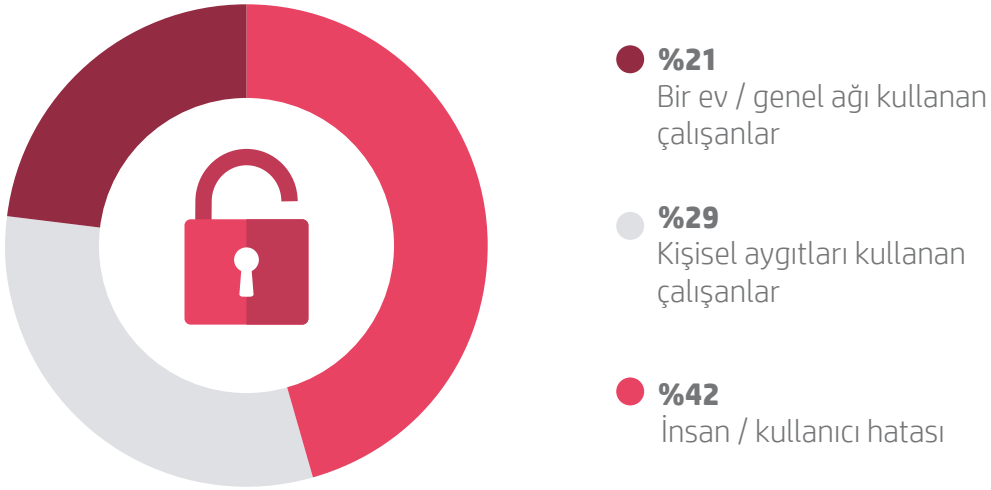
Veri ihlalinin en muhtemel nedeni:[11]



En yaygın türdeki dış tehditler:



İç güvenlik ihlalleri nasıl oluşur:[12]



Kaynaklar: [11] http://www.kilpatricktownsend.com/_assets/Kilpatrick%20Townsend%20Report%20Final.pdf [12] Ponemon Institute Cost of Cyber Crime Study 2015

Siber suçtan kurtulmanın maliyeti nedir?

En maliyetli siber saldırı türleri:

%25

1.000.000£

Kötü amaçlı kod ve kötü amaçlı yazılım

Güvenlik açıkları yaratarak, dosyalara zarar vererek veya veriyi çalarak (komut dizilerini, virüsleri ve solucanları içerir) bir sisteme zarar veren yazılım

%24

960.000£

Dağıtık Hizmeti Engelleme

"DDoS" saldırıları bir şirketin sitesini ve sunucuları çökerten web trafiği selleridir.

%16

640.000£

Web tabanlı saldırılar

Sitenize gelen ziyaretçileri hedefleyen saldırılar örneğin tarayıcıları kötü amaçlı yazılım yüklü sitelere yönlendiren enjekte edilmiş kod gibi

%13

520.000£

Çalınmış cihazlar

Şirket oturum açılışlarına erişimi olan kayıp çalışan cihazları veri hırsızlığına ve kimlik dolandırıcılığa yol açabilir.

%9

360.000£

Kimlik avı ve sosyal mühendislik

Oturum açılışları için meşru istekler gibi davranan e-postalar veya açılır pencereler

%9

360.000£

Kötü amaçlı şirket içi personel

Hassas bilgiyi başkalarına veren çalışanlar

%4

160.000£

Botnet'ler

İstenmeyen posta göndermek gibi kötü amaçlı etkinlik için kontrol edilen kötü amaçlı kod bulaşmış bilgisayarlardan oluşan ağlar

Kaynak: [13] Ponemon Institute Cost of Cyber Crime Study 2015

Siber suçun işlere etkisi

Siber suçun gerçek maliyeti, bir korsanlık faaliyetinden kaynaklanan hasarın tamir edilmesinin ötesine uzanır.

Güvenlik ihlalleri inanılmaz biçimde maliyetlidir. Genel olarak, bir ihlal şirketinizin finansmanını üç şekilde etkileyebilir.

Şirket kaynakları

Elbette işleri düzene koymanız gerekecektir. Bu, önemli miktarda çalışan zamanını ve maliyetini kullanır. Diğer, gelir yaratan işleri beklemeye almanız gerekebilir.

Cezalar / para cezaları

Uyumsuzluk nedeniyle bir para cezası alabilirsiniz (ör. HIPAA). Gelecek yıl AB GDPR yürürlüğe girdiğinde, ihmalkar görülen şirketler global cirolarının %4'üne kadar toplam bir ceza alabilirler. Sızıntı müşteri gizliliğinin ihlali ile sonuçlanırsa, dava edilme riskiyle bile karşılaşabilirsiniz.

Zarar gören itibar

Bu, bir ihlalin en zarar verici etkilerinden biri olabilir. Müşteriler, basın ve kamuoyu genellikle güvenlik ihlalleri konusunda uzun bir belleğe sahiptir. Güvenin eski haline gelmesi uzun bir süre alabilir.

Beklenmedik korsanlık eyleminin anatomisi

Sony Pictures 2014 yılında kırıldığında, korsanlar basit bir şekilde ön kapıdan çıkıp gittiler.[14]

Saldırının sorumluluğunu üstlenen Guardians of Peace (GOP, Barışın Koruyucuları) korsan grubundan "Lena"ya göre, Sony artık fiziksel güvenlik yapmamaktadır." Sony'nin ağına binaya fiziksel olarak girerek ve bir sistem yöneticisinin bilgisayar oturum açma bilgilerini çalarak erişim elde ederler.

İçerideyken, Oracle ve SQL veritabanlarına ilişkin özel dosyaları, kaynak kodunu yakalayan kötü amaçlı yazılımı yerleştirirler. Bundan sonra, film prodüksiyon planlarını, e-postaları, finansal belgeleri ve daha bir çoğunu çalarlar – ve çoğunu çevrimiçi yayınlarlar.

Korsanlar, şirket "The Interview" (Mülakat) adlı filmi sinemalardan çekmediği takdirde, daha gizli ve en gizli veriyi yayınlamakla tehdit ederler.

Sony, gizli tutulan gişe hasılatı gelirlerini kaybetmenin yanı sıra olağanüstü itibar zararı görerek sonunda teslim olur.

Sony iki hata yapmıştır. Yetkisiz giriş yapanlar tarafından şirket verisine fiziksel erişimi dikkate almamak, ve ilk güvenliğin aşılmasını takiben hassas bilgiye erişimi önleyebilecek çoklu güvenlik katmanlarına yatırım yapmamak.

Güvenlik uzmanı Bruce Schneier'ın saldırıdan sonra yazdığına göre, "Yeterince becerikli, finansmanı olan ve motive bir saldırgana karşı, tüm ağlar savunmasızdır." İşin püf noktası, ağınızın neresinin savunmasız olduğunu fark etmektir. Bu, ön kapı olabilir.

EYLEME GEÇİN:
Kurtarma süresini en aza indirmek için BT'den müşteri hizmetlerine her bölüm için bir ihlal müdahale planını oluşturun.

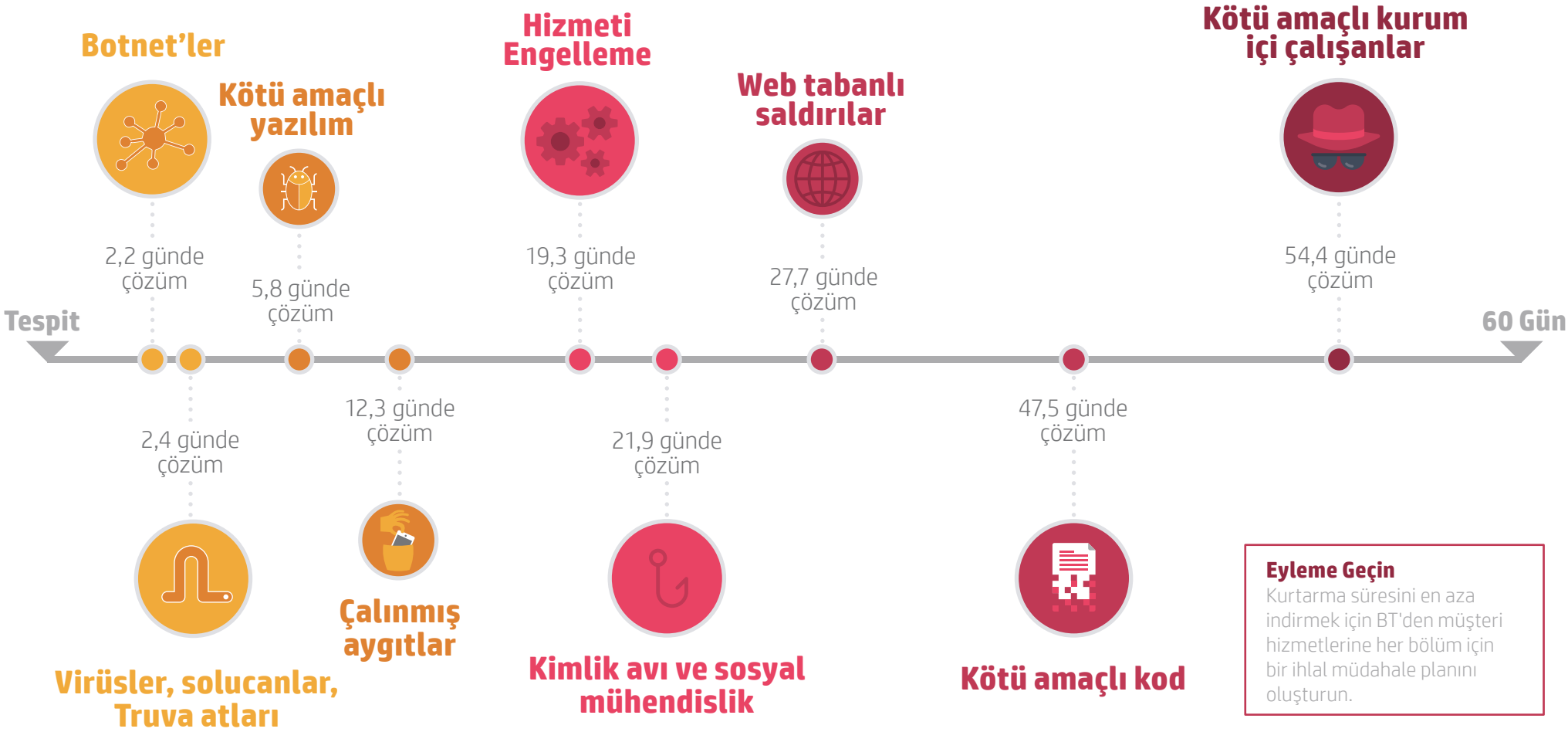
İPUCU:
Birçok kötü amaçlı yazılım türü, e-posta ekleri olarak aktarılır. Personeli meşru belgeler gibi görünen şüpheli dosyaların fark edilmesi konusunda eğitin.

- Siber suçun İngiltere işletmelerine olan tahmini maliyeti: 21 milyar ABD doları[15]
- 2016'da İngiltere şirketi başına siber suçun ortalama maliyeti: 5,7 milyon GBP[16]
- 2015-2016'da bir siber güvenlik ihlali veya saldırısı yaşamış olan İngiltere işletmeleri: %66[17]

Kaynak: [14] http://www.businessinsider.com/how-the-hackers-broke-into-sony-2014-12?IR=T [15] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
[16] https://www.statista.com/statistics/293274/average-cyber-crime-costs-to-companies-in-selected-countries/ Stat is $7.21m – have converted to £
[17] https://www.gov.uk/government/news/two-thirds-of-large-uk-businesses-hit-by-cyber-breach-or-attack-in-past-year

Siber suç: kurtarma süresi

Bir veri güvenliği ihlalinin zararını onarmak ne kadar sürer? Ponemon Institute[18] kesintisiz faaliyete geçme süresini ortalama 46 gün olarak ortaya koyuyor ve bu da İngiltere KOBİ bankacılığı için potansiyel bir felaket.



Eyleme Geçin
Kurtarma süresini en aza indirmek için BT'den müşteri hizmetlerine her bölüm için bir ihlal müdahale planını oluşturun.

Kaynak: [18] Ponemon Institute Cost of Cyber Crime Study 2015

İşinizi siber suça karşı nasıl korumalısınız

İş siber güvenliği için temel ipuçları ve stratejiler

Burada, şirket sistemlerini ihlal eden korsanlarve bugün onlar hakkında neler yapabileceğiniz konusunda altı ortak hedef bulunuyor.

Müşteri Veritabanları

Bulut Hizmetleri

Personel Akıllı Telefonları ve Tabletler

Çalışan Hataları

Nesnelerin İnterneti

Ağ Geçitleri

Veriye her zamankinden daha fazla değer verdiğimiz giderek dijitalleşen bir dünyaya geçiş yaparken siber suç çok çeşitli şekillere girebilir. Siber suçlular sıklıkla bilginin peşinde koşarlar ve işyerinde kullanılan (akıllı telefonlardan, tabletlerden WiFi yazıcılara kadar) bağlantılı cihazların sayısının artmasıyla korsanların hedefleyeceği erişim noktalarının sayısı da artmaktadır.

1 Müşteri veritabanları

Saldırganların tek hedefi finansal veriler değildir, adlar ve e-posta adresleri gibi bilgiler de kimlik dolandırıcılığı, istenmeyen posta veya diğer hesapları kırmak için kullanılabilir.

İddialı korsanlar için en büyük ödüllerden biri de, daha büyük işletmelere hizmet veren işletmelere sızmaktır. Komşu bir ulusal bankanın kasa dairesiyle paylaşılan bodrum duvarına erişmek için bir hırdavat mağazasına girmenin dijital eşdeğeri olarak düşünün.

Saldırganlar daha küçük bir sistemin içindeyken, büyük şirketin müşterileri tarafından tutulan müşteri verilerine erişim elde etmek için daha iyi pozisyondadır. Müşteri veritabanınız nasıl tehlikeye girebilir? Kötü amaçlı sitelerden veya e-postalardan indirilen virüsler, solucanlar ve truva atları bir korsanın girmek ve veriyi çalmak için ihtiyaç duyduğu kodu serbest bırakabilirler.

Müşterilerinizin verilerini nasıl korumalısınız

- İşletmeler için tasarlanan, ağ, e-posta ve uç nokta koruması sağlayan güvenlik yazılımlarını kullanın.
- Gelişen kötü amaçlı yazılımları engellemek için güvenlik yazılımınızı her zaman güncelleyin.
- Eski programların korsanların kötüye kullanabilecekleri belirli güvenlik açıklarının olması nedeniyle, sistem programlarınız için yazılım güvenlik güncellemelerini indirin.

2 Bulut hizmetleri

Müşterilerinizin verilerini nasıl korumalısınız

- En önemli bilgilerinizi şifrelemenin karmaşıklığını belirlemek için erişim politikalarını kullanan PKWARE Smartcrypt teknolojisi gibi araçlardan yararlanarak şifreleyin. Bu şekilde, yetkili kullanıcılar görmeleri gereken verileri görebilirler – ve yetkisiz kullanıcılar hiçbir şey görmezler.
- Bulut hesabınız için güçlü bir parola oluşturun. Ayrıca, bulut hesabınıza ilişkin ayarlarınızda, verinize kimin erişebileceğini ve bununla neler yapabileceklerini kesin bir biçimde tanımlayın.
- İki faktörlü kimlik doğrulamasını kullanın. Örneğin, bulut verilerinde indirme, silme veya dosyaları taşıma gibi değişiklikler yapmak için bir akıllı telefon kodu ile birlikte parola kullanma.

Bulut bilişim, işletme altyapısında bir demirbaş haline gelmiştir.

2016 IDG Bulut Bilişim Anketi[19] işletmelerin yüzde 70'inin bulut ortamında en azından bir kısım altyapısının bulunduğu ortaya koyarken, Tripwire yüzde 90'ının misyon kritik veriler de dâhil olmak üzere altyapı ve/veya veri depolaması için bulutu kullandığını ortaya koymuştur.[20]

Güvenlik elbette bir endişe kaynağıdır, ancak gerçekte veriler, itibarı bu verileri güvende tutmasına bağlı olan bir şirket tarafından tesisiniz dışındaki sunucularda saklanan bulut üzerinde genellikle daha güvendedir.

Bu nedenle, Tripwire tarafından araştırılan işletmelerin yüzde 64'ü bulutu eski sistemlerden daha güvenli olarak görmektedir.

İyi ki, bu güven boşuna değil – 2015 BIS anketine göre,[21] işletmelerin sadece yüzde 7'si (büyük ve küçük) bulut hizmetlerinde ciddi bir güvenlik ihlali yaşamıştır ve bunlar genellikle, erişim izinleri veya yetersiz parolaların sonucu olmuştur. Ancak, güvenli bir bulut hâlâ güçlü bir iç güvenlik yönetimine ihtiyaç duyar. Sadece Sony'nin ön kapısını aklınıza getirin.

Kaynaklar:
[19] https://www.scribd.com/document/329518100/IDG-Enterprise-2016-Cloud-Computing-Survey
[20] https://www.tripwire.com/state-of-security/security-data-protection/enterprise-impressions-of-cloud-security-in-2016/
[21] 2015 Small Business Survey. Department for Business, Innovation & Skills

3 Personel akıllı telefonları ve tabletler

Pek çok kişi, ofis görevleri için kişisel cihazlarını kullanır.

İşletmeler için Kendi Cihazını Getir (Bring-Your-Own-Device, BYOD) politikaları çalışanların zaten sahip oldukları akıllı telefonlardan faydalanmanın etkili bir yoludur. Bu eğilim, kuruluşların %53,2'sinin önümüzdeki iki yıl içinde bir BYOD politikasını uygulamaya alacak olmasıyla giderek artmaktadır.[22] Ancak, cihazlar korsanlar için uygun birer hedef olabilir.

Tahminen her beş Android uygulamasından biri, etkinlikleri izlemek veya bilgi çalmak için şirket dosyalarına ve sistemlerine aktarılabilen türde yetkisiz girişe neden olabilecek kötü amaçlı yazılım taşımaktadır.

Bu tehdit büyümekte ve kuruluşların yüzde 64,9'u mobil aygıtlarını hedefleyen tehditlerin hacminin arttığını belirtmektedir.[23]

Telefonları çalınan çalışanlar da farkında olmadan korsanlar için bir giriş yolu olabilirler. Bir telefon hırsızı, bir aygıtı kurbanın şirketine yetkisiz giriş yapmak veya daha büyük bir müşterinin sistemlerine nüfuz etmek için aygıtı parçalarına ayıran karaborsa satıcısına satabilir. Kuruluşlar mobil aygıtlardan kaynaklanan güvenlik tehditlerine karşı savunma yeteneklerini beş üzerinden 3,54 oranında değerlendirmiştir. Bu, onlara sorulan tüm potansiyel tehdit kaynaklarına ilişkin en düşük değerlendirme olmuştur.[24]

Personelin sahip olduğu cihazlar nasıl güvenli hale getirilebilir

- Android cihazlar için Duo X-Ray gibi bir tehdit tespit aracını, kaçak uygulamaları ve şüpheli kodu daha kolay izlemek için kullanın.
- Çalışanlardan, uzaktan silmeyi (Android, iPhone ve Windows Phone için ücretsiz sunulur; BlackBerry'de abonelikle verilir) etkinleştirmelerini isteyin, böylece kayıp durumunda, hem iş verileri hem de kişisel hassas veriler silinebilir.
- Çalışanlardan veriyi korumak için akıllı telefonlarında aygıt şifrelemesini etkinleştirmelerini isteyin (bu, yeni iOS ve Android telefonlarda varsayılan yapılandırmadır).

Kaynak: [22] 2016 Cyberthreat Defense Report, CyberEdge [23] ibid [24] ibid

4 Çalışan hataları

Personelinize nasıl yardım etmelisiniz

- Personelinizi siber güvenlik en iyi uygulamaları konusunda eğitin ve en son tehditlerin bir adım önünde kalmak için düzenli eğitimi sağlayın.
- İşinize ve işlediği veri türlerine uygun bir güvenlik protokolünü geliştirin.
- Çalışanların yanı sıra müşterilere ve iş ortaklarına siber güvenlik politikanızı iletmek için bir ekip oluşturun.

Siber güvenliğin en temel doktrini, iyi parola politikasıdır ve yine de, 2015'teki en kötü güvenlik ihlallerinin yüzde 31'i personelle ilgili bir olayın sonucu olmuştur.

Zayıf parolaların kırılmasından güvensiz bir bağlantıdan e-postayla gönderilen belgelerin çalınmasına veya belirli bir çalışanı hedefleyen bir kimlik avı e-postasına kadar, saldırganlar sıklıkla insan hatasından yararlanırlar.

5 Nesnelerin İnternetine Hazırlanma

Araştırma firması IDC, internete bağlanan aygıtların sayısının tahmini 13 milyardan, 2020'de 30 milyara yaklaşacağı tahmininde bulunmaktadır.[25]

Ofis bilgisayarlarının güvenliği parolalar ve ideal olarak güvenlik yazılımı ile sağlanırken, baskı kuyrukları ve baskı işleri genellikle benzer güvenlik protokolleri ile korunmaz.

Bu tür güvensiz yazıcılar ve diğer ağ bağlantılı donanım, tümü bir siber suç sunucusuna gönderilen ve geri alınan baskı işlerinin yanı sıra ağ trafiği, kullanıcı adları ve parola bilgisini kaydedebilen 'dinleme programlarına' av olabilirler.

Hakkında çok sayıda yayın yapılan Dyn güvenlik ihlalinin XiongMai Technologies adlı tek bir şirket tarafından yapılan web etkin CCTV kameralarından oluşan bir ağla bağlantılı olduğunun söylendiğini dikkate almak önemlidir. Flashpoint güvenlik firmasına göre.

Bu, ağdaki her bir aygıtın bir uç nokta olduğunu ve ağın en az güvenli aygıt kadar güçlü olduğunu göstermektedir. Kuruluşların %97'si masaüstü/dizüstüler için güvenlik uygulamalarına, %77'si mobil aygıtlar için ve %57'si yazıcılar için yürürlükte güvenlik uygulamalarına sahiptir.[26] Tüm işletmeler için güvende kalmanın tek yolu, her bir uç nokta aygıtı için güvenlik uygulamalarına sahip olmaktır.

Nesnelerin İnternetine nasıl hazırlanmalı

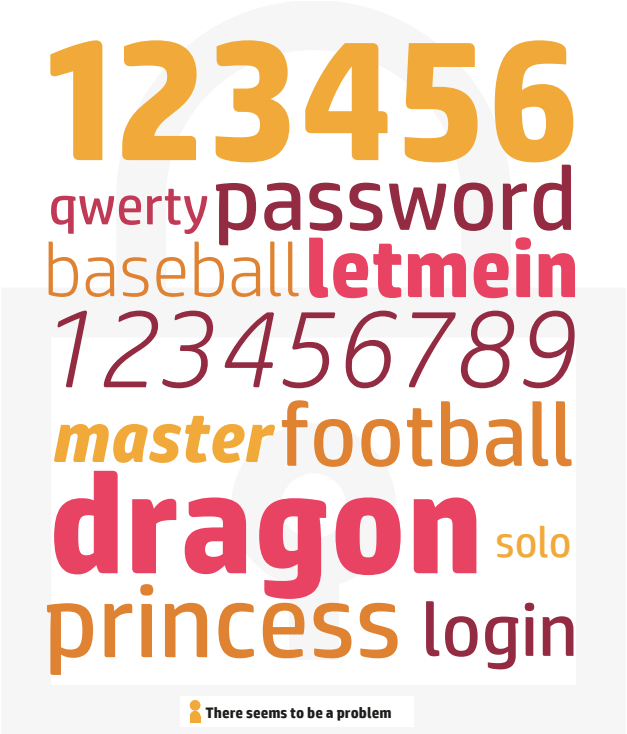
- Daha fazla işlevin saldırganların girmesi için daha fazla ağ geçidi oluşturabilmesi nedeniyle, gereksiz işlevleri kaldırın veya devre dışı bırakın.

Kaynaklar: [25] PwC: The Global State of Information Security Survey 2016 [26] HPI Printer Security Research, Spiceworks 2016

Parolalar ve fidye yazılım

En yaygın parolalar

2013'ün başında, asla bir siber suçlu olmayan veya parola korumalı sistemlere nüfuz etme deneyimi olmayan bir Ars Technica muhabiri bir günde 16.000 şifrelenmiş parolanın 8.000'inden fazlasını kırmıştır*. Peki kararlı bir korsana karşı son derece yaygın parolaların şansı nedir?



Fidye yazılım nedir

Siber suçlular artan biçimde sistemleri rehin alan ve ardından bitcoin olarak bir fidyenin ödenmesi ile kilidinin açılabildiği bir çeşit kötü amaçlı yazılım olan fidye yazılıma geçiş yapmıştır. 2013'te İngiltere Ulusal Suç Dairesi ve Ulusal Siber Suç Birimi'nin dikkatini çeken Cryptolocker adlı bir truva atı salgınında binlercesi etkilenmiştir. Burada, bu türdeki saldırıların nasıl çalıştığına dair ayrıntılı bir açıklama verilmektedir.

	1. Kurulum	Kötü amaçlı kod amaçlanmayan bir indirmeden sonra kendisini bir e-posta veya kötü amaçlı web sitesi yoluyla bilgisayarınıza yerleştirir.
	2. Genel merkezi uyarır	Fidye yazılım bir şifreleme anahtarı oluşturmak için ana bilgisayara bağlanır.
	3. Dosyalarınızı şifreler	Fidye yazılım ağınızdaki dosyaları tarar ve erişimi olanaksız kılacak şekilde şifreler.
	4. Şantaj	Bir zaman sınırını ve silinmeden önce dosyaların şifresini açmak amacıyla ödenmesi gereken miktarı görüntüleyen bir mesaj kullanıcı bilgisayarında açılır.
	5. Ödeme	İşletme sahibi dosyaların şifresini açacak saldırgana aktarmak için bitcoin benzeri bir dijital para birimini satın alabilir.

* Splashdata

6 Ağ geçitleri

Korsanlar bir ağa girmek istediklerinde, bir DDoS saldırısını başlatabilirler – kötü amaçlı yazılım bulaşmış binlerce makine, ağın saldırının ağırlığı altında düşmesine yol açan çok sayıda çöp trafiği oluşturmak üzere birleştirilir.

Sıklıkla, DDoS saldırganları sistem yöneticilerinin dikkatini donan bir sisteme çekmek isterler, diğer yandan da veri çalarlar veya gelecekteki soygunları planlamak için kötü amaçlı yazılımı kurarlar. Bazı DDoS saldırıları da sadece yapabilmeleri nedeniyle bir web sitesini çökertmek isteyen 'genç yazılımcılar' diğer bir deyişle, tecrübesiz korsanlar tarafından yapılır. Birkaç saatlik web sitesi kesintisinin bile işinizin kârı ve itibarı üzerinde yıkıcı etkileri olabilir.

İPUCU:
Gelişmiş kimlik doğrulama ve şifreleme araçları gibi yerleşik koruma sunan donanımlara yatırım yapın.

Ağınızın güvenliğini nasıl sağlamalısınız

- Ağınıza giren ve çıkan trafiği kontrol eden sistemleri kurun. Anlık bir artış bir saldırıya işaret edebilir, öte yandan sabit ancak açıklanamaz etkinlik bir truva atının ana gemisine rapor verdiğini gösterebilir.
- Sadece işletmenizi desteklemek için gereken trafiğin ağınıza ulaşabileceği şekilde tüm trafiği filtreleyin.
- Her bir router, anahtar veya diğer ağ cihazının aynı temel yazılım ve işlevi çalıştırdığından ve her zaman yazılım güncellemelerini indirdiğinizden emin olun.

İşletme siber güvenliğinin geleceği

İşletmelerin bu kadar internet bağımlı olmasıyla birlikte, güçlü siber güvenlik savunmalarının kurulması kritik önem kazandı.

Bugün, çalışanlar çalışmak için kendi cihazlarını getiriyorlar. İşletmeler, bulut bilişim platformlarını kullanıyor ve önemli teknik hizmetleri dışarıdan alıyorlar. Ve şimdi daha fazla insan uzaktan çalışıyor. Siber güvenlik, hiçbir aygıtı, altyapıyı veya çalışma alanını kontrol edemediğinizde daha zorlu hale gelir.

Aynı zamanda, akıllı telefonlar bize, işin herhangi bir anda her yerden yapılabileceğini öğretmiştir. Bir kafeterya, bir ofis gibi çalışılacak iyi bir yerdir. Geniş miktarlarda iş ve kişisel veriyi işlemek için kamuya açık WiFi ağlarını kullanırız (sıklıkla zayıf biçimde korunan akıllı telefonlar üzerinden). Suçlular dönüşümün kesinlikle farkında. İşimizin şartlarına uymadığımızda güvenlik kesinlikle yara alıyor.

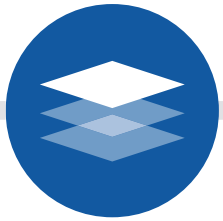
Önümüzdeki yıllarda, bu, aygıtlarımıza antivirüs yazılımı eklemekten veya parolaları her altı ayda bir güncellemekten çok daha fazlası anlamına gelecek. İşletmeler daha çok bir BT yöneticisi tarafından yönetilen bir ofiste olduğu gibi uzaktan da iyi işe yarayan gelişmiş güvenlik tedbirlerini kucaklamalılar.

Yarının dağıtık kuruluşları için, siber güvenlik olağandışı davranışları izole eden ileri analize ve tüm erişim noktalarını koruyan katmanlı güvenliğe dayanıyor.

İşletme siber güvenliğinin geleceği

Analizler:
siber güvenlik dedektifi

Siteniz yoğun bir trafik almasa bile, belirli kalıpları olacaktır. Etkinliği ölçen ve kaydeden analiz araçlarını kullanmak, bir şeyin yanlış olduğuna dair tanının konulmasını kolaylaştırır. Bu araçlar, daha sonra anormallikleri tespit etmek amacıyla, ilk önce normal davranışı izleyerek ve belgelendirerek çalışırlar. Tespit edildiğinde, yöneticiler ofansif bir tutum takınabilir ve saldırıları bir siber kaos başlama şansı oluşmadan önce bertaraf edebilirler.



Katmanlandırma:
saldırganları bir adım arkada bırakmak

Bazen, 'derinlemesine savunma' olarak da atıfta bulunulan katmanlı güvenlik, her bir erişim noktasını çeşitli yollarla korur. Ortak yaklaşımlar arasında, güvenli bir ağa giriş için gerekli oturum açma bilgilerinin sahtelerinin kullanımını zorlaştıran genişletilmiş doğrulama SSL sertifikaları bulunur. Bunu yetkisiz giriş yapanların sadece bir paroladan daha fazlasını kırmalarını gerektiren çok faktörlü kimlik doğrulama ile desteklemek de faydalı olabilir.

Kullanılan teknolojiden bağımsız olarak, katmanlandırmanın ardındaki ilke, iş ağınızdaki her bir hassas alanın bir şekilde kilit altına alınmasıdır. Kullanıcılarınızın ve iş ortaklarınızın önemli verilere erişmek için ilave zamana ve çabaya ihtiyaçları olabilir, ancak size küçük bir rahatsızlık veren bu fazladan çaba, işinizde huzur olarak geri döner.

Şimdi eyleme geçin

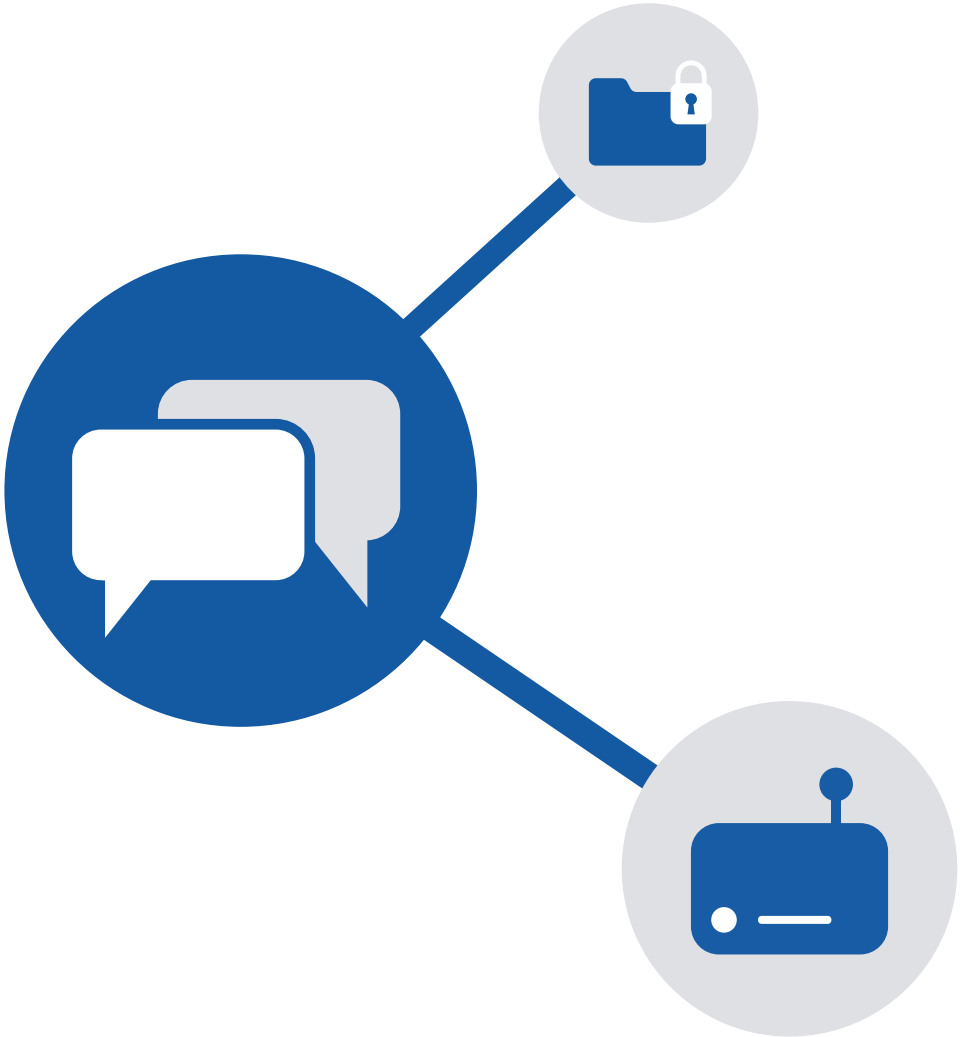
Siber güvenlik yazılımına ve eğitimine yatırım yapmak en iyi savunmadır. Sistemlerinizin ve altyapınızın denetimini yaparak başlayın. Yeterince çaba gösteriyor musunuz? Neyi daha iyi yapabilirsiniz?

Son olarak, Hewlett Packard Inc.'deki uzmanlarımızı arayabilirsiniz. Müşterek bilgi tabanımız, tehditlere sadece müdahale etmez, tehditlerin bir adım önünde kalmaya da odaklanmıştır. Daha fazlasını öğrenmek için HP.com adresini ziyaret edin.

İPUCU:
Daha sonra anormallikleri tespit etmek amacıyla, ilk önce normal davranışı izleyin ve belgelendirin.

Uç nokta aygıtı güvenliğine ilişkin değerlendirmeler

Ağınızdaki her bir aygıtın güvenliğini sağlama



Spiceworks[27] tarafından yürütülen güvenlik araştırması, işletmelerin karşılaştığı güvenlik tehditlerinin ana kaynağının şunlar olduğunu ortaya koymuştur:

- Dizüstüler ve masaüstüler: %81 harici ve %80 dahili
- Mobil aygıtlar: %36 harici ve %38 dahili
- Yazıcılar: %16 harici ve %16 dahili

En acil güvenlik önlemleri bu tehditlerin hangisine karşı alınmalıdır? Yanıt çok kolay: Hepsi! Bu çok açık olmasına karşın, endişe verici bir sayıda kuruluş hâlen hangi aygıtların güvenliğinin sağlanacağı konusunda ince eleyip sık dokumaktadır.

HP bakış açısına göre, ağınıza bağlanan her bir aygıtın güvenliği sağlanmalıdır. Basitçe söylemek gerekirse: ağınız sadece en az güvenli aygıtınız kadar güvenlidir.

Sezgisel mantık, bağlantılı bir yazıcının güvenliğini sağlamanın, dizüstü bilgisayar filonuzun güvenliğini sağlama kadar önemli olmadığını söyleyebilir. Ancak, risk aynıdır. Korsanların yazıcıları ve ağınıza bağlanan diğer akıllı aygıtları hedefledikleri görülmüştür. Bu aygıtların tipik olarak güvenliklerinin pek iyi sağlanmadığını, buna karşın, ağınıza aynı düzeyde erişimleri olduğunu bilirler.

Kaynak: [27] HP Printer Security Research 2016, Spiceworks

HP: Yeni güvenlik ortamında öncülük ediyor

Siber güvenlik değişiyor. Savunmanıza yardımcı olacak araçlarımız hazır.

Siber güvenlikte hızlı çözüm diye bir şey yoktur. Sağlam bir savunma, ağları, aygıtları ve insanları kapsayan çok yönlü bir yaklaşımı gerektirir. Doğru teknolojinin seçilmesi güçlü bir başlangıçtır.

HP'de, önce güvenlik gelir. HP Premium Elite aygıt yelpazesi, dünyanın kendi kendini iyileştiren ilk BIOS'u olan HP SureStart gibi diğerlerinde mevcut olmayan pazarda öncü güvenlik özelliklerine sahiptir.

HP, aygıtlarının sahip olduğu özellikler:

- **Bluetooth kilidi:** Bluetooth kullanılarak, uzaklaştığınızda makine otomatik olarak kilitlenir ve geri döndüğünüzde açılır.
- **Biyometrik güvenlik:** Yüz ve parmak izi tanıma yalnızca biyometrik olarak kimliği doğrulanan kullanıcılara erişimi sağlar.
- **HP SureView ekranları*:** Karartılmış monitör, siz hareket halinde çalışırken gizli materyali koruyarak çevreden gelip geçenlerin ekranınızı görmesini engeller.
- **HP SureStart kendi kendini iyileştiren BIOS:** Her HP Elite kendi BIOS'unu her 15 dakikada bir izler. Anormal bir durum tespit ettiğinde, yetkisiz giriş yapanları sistemden çıkararak bilgisayarı orijinal durumuna sıfırlar.

HP Elite ailesi, kendi başına işinizi koruyamaz. Ancak, çok güçlü bir ön cephe oluşturur. HP Elite ürün ailesinin tamamı hakkında daha fazlasını öğrenmek için www8.hp.com adresini ziyaret edin.

* Seçkin modellerde

HP: Yeni bir baskı ortamında öncülük ediyor

Dünyanın en güvenilir yazıcısı ile ağınızı savunun*

"Baskı güvenliğine yaptığı uzun vadeli yatırımın kanıtı olarak HP, pazardaki en kapsamlı ve en derin güvenlik çözüm ve hizmet portföyüne sahiptir."

– Quocirca, Ocak 2017**

HP aygıtlarının sahip olduğu özellikler:

- **Çalışma sırasında müdahale algılama:** HP'nin çalışma sırasında müdahale algılama teknolojisi, cihazlar çalışırken ve ağa bağlıyken, yani çoğu saldırının gerçekleştiği anda cihazları korumaya yardımcı olur.
- **JetAdvantage Security Manager:** Bu uygulama IT yöneticilerine, önceden belirlenmiş şirket güvenlik politikalarına uygun olarak filo boyunca aygıt güvenlik ayarlarını değerlendirmeleri ve gerekirse düzeltmeleri için standartlaştırılmış bir yaklaşım sunar.
- **HP SureStart kendi kendini iyileştiren BIOS:** HP SureStart, yeniden başlatma esnasında kötü amaçlı kodların yürütüldüğünü tespit ederek önler ve BIOS'u kendi kendine iyileştirir. BIOS, yerleşik bir 'altın' kopya ile yeniden yüklenir.
- **Beyaz listeye alma:** Sadece orijinal ve iyi olduğu bilinen HP kodunun belleğe yüklenmesini sağlar. Bir anormalliğin tespit edilmesi durumunda cihaz yeniden başlatılarak güvenli ve çevrimdışı bir duruma geçer ve IT departmanına bildirim gönderir.

Kaynaklar: *5 En güvenli baskı deneyimi" beyanı aynı sınıf rakip yazıcıların yayınlanmış güvenlik özelliklerine ilişkin 2016 tarihli HP incelemesine dayanmaktadır. Yalnızca HP, bir saldırıyı algılamak için izleyip otomatik olarak durdurabilen ve daha sonra önyüklemede yazılım bütünlüğünü kendi kendine doğrulayabilen güvenlik özelliklerinin bir birleşimini sunar. **Quocirca, "Baskı güvenliği: Nesnelerin İnterneti çağında bir zorunluluk," quocirca.com/content/print-security-imperative-iot-era, Ocak 2017.

Sözlük ve ek okuma kaynakları

Erişim yönetim araçları

Botnet:
Genellikle, İnternete bağlı bilgisayarlarda sahibinin bilgisi dışında erişim ve kontrol için tasarlanan otomatik bir program tipine atıfta bulunur. Bilgisayarlara sıklıkla diğer kötü amaçlı yazılımlar bulaşır. Korsanlar, bir web sitesinde bir **Hizmeti Engelleme saldırısını** başlatmak için botnet'leri kullanırlar.

Çevre denetimleri:
Kamuya açık İnternet veya diğer genel ağın özel ve yerel olarak sahip olunan ve yönetilen bir ağla buluştuğu noktadaki siber güvenliği açıklayan genel kategoridir. **Çoklu katmanlar ve aygıt türleri** sıklıkla ilişkilidir.

Güvenlik duvarı teknolojileri:
Yetkisiz trafiği ve bir ağa giren kullanıcıları bloke etmek için algoritmaları ve diğer teknikleri kullanan bir aygıt tarzını tanımlayan diğer bir kapsamlı terimdir. **Bu aygıtların sonraki nesil sürümleri** farklı aygıtlarca önceden işleme alınmış fonksiyonların nasıl birleştirileceği konusunda önemli olabilir. Örneğin, yetkisiz giriş tespiti. Ayrıca, uygulamaya duyarlı olma eğilimindedirler, böylelikle bir salesforce.com uygulamasından kaynaklanan web trafiği ile bir Facebook sayfasından kaynaklanan web trafiği arasındaki farklı anlarlar.

GRC araçları:
Bir şirket içinde yönetmeliklerle uyumlu olacak şekilde operasyonları yönetmeleri ve yürütmeleri, **bunun sonucu olarak riski azaltmaları hedeflenen geniş ve koordineli girişimlere atıfta bulunması amaçlanmıştır.**

Kimlik Avı:
Genellikle e-posta yoluyla yapılır. Burada, bir saldırgan meşru görünümlü bir diyalog kutusu içinde tanımlayıcı bilgiyi ister.

Kötü amaçlı yazılım:
Zarara neden olabilen ve hatta diğer sistemleri devre dışı bırakabilen geniş bir yazılım kategorisidir. Virüsler, solucanlar ve Truva atları, kötü amaçlı yazılıma ait örneklerdir. Ayrıca, bu eKitap genelinde alıntı yapılan Ponemon çalışmasının amaçları doğrultusunda, kötü amaçlı yazılım, virüslerden ayrı olarak değerlendirilmektedir. Buna göre, “uç noktada bulunurlar ve henüz bir ağa sızmamışlardır”.

Politika yönetim araçları:
Geniş anlamda, politika yönetim araçları, kullanıcıların neleri görüp neleri göremeyeceklerine dair bir standardı belirler ve ardından bu politikayı tüm ağ genelinde yürütürler. Tutarlılık (en azından teoride) güvenliği sağlar.

Şifreleme teknolojileri:
Belirli türde bir kod çözücü olmadan **veriyi kendi başına okunamaz kılan** araçlar. İngiltere Bilişim Dairesi, geçtiğimiz yıllarda çeşitli türlerde şifrelemenin **güçlü bir biçimde lehinde** bir yaklaşımı benimsemiştir. Daha yakın tarihte, hükümet ciddi eleştirilerin ortaya çıkmasıyla **şifreleme teknolojisi konusundaki pozisyonunu değiştirmek** zorunda kalmıştır.

Veri kaybı önleme araçları:
Hedefi, hassas verileri izlemek ve yetkisiz kişilerce erişim ve kopyalama denemelerini bloke etmek olan geniş bir yazılım kategorisidir. Farklı yaklaşımlar, bir ağda veya dosya sisteminde gezerken, erişim noktasında (diğer bir deyişle uç nokta) korumaya izin verir. Gartner’e göre 2013 yılında bu pazar **yüzde 25 büyümüştür**.

Sözlük ve ek okuma kaynakları

Güvenlik istihbarat sistemleri:
Geniş bir güvenlik istihbaratı, tehditlerle ilgili bilgilerin toplanmasına ve sentezlenmesine yardımcı olabilir. Sistemler, kayıt günlüğü yöneticilerinden ağ anormalliklerini tespit eden sistemlere geçmektedir.

Sosyal mühendislik:
Bir saldırganın, yetkili bir kullanıcının vermemesi gereken bir bilgiyi bir saldırgana erişim sağlamak amacıyla vermesi için onu ikna etmeye çalıştığı durumdur.

Truva atı:
Etki bakımından bir virüs veya solucana benzeyen Truva atları, kullanıcı tarafından kurulmalıdır ve bu bakımdan, daha akıllı biçimde gizlenme eğilimindedirler. Etkileri, bilgisayar ayarlarının değiştirilmesinden, bir korsan için daha sonra kullanılmak üzere bir "arka kapı" oluşturacak şekilde dosyaların silinmesine kadar değişiklik gösterebilir.

Virüsler:
Bir ağ genelinde çoğalma ve yayılma kabiliyetine sahip kötü amaçlı kod.

Web tabanlı saldırılar:
Genellikle bir web tabanlı saldırı, bir tarayıcının kötü amaçlı bir siteye yönlendirilmesini içerir.

Solucanlar:
Bir taşıyıcı dosya paylaşıldığında yayılan virüslerin aksine, solucanlar bir taşıyıcı dosyadan bağımsız olarak çoğalabilir, örneğin bir Word dosyası veya Excel çalışma formu ve bu nedenle, zarar vermek için ek bir insan etkileşimi gerekmez. Anlık mesajlaşma sistemlerinin solucanları yaydıkları çok iyi bilinmektedir; Skype'ın saygınlığına 2012 yılında epey bir zarar verdiler.