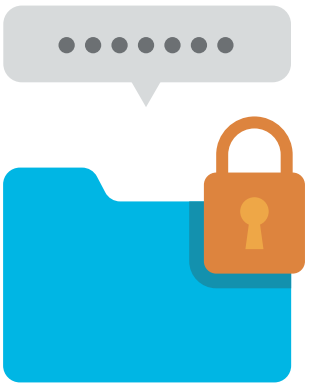
İş teknik incelemesi

Güvenlik Uç Noktada Başlar

Uç nokta güvenliği neden öncelikli olmalıdır

Size sunan

Yönetici Özeti



Kuruluşların %82'si son 12 ayda bir siber güvenlik tehdidi/ihlali yaşamıştır.[1] Siber suç, saldırı sıklığı, ciddiyet ve maliyet bakımından artmaktadır.

Önleme (güvenlik duvarı olan bir ağ çevresini savunma) ve güvenliği koruma paradigması artık tarihe karıştı. Tespit ve müdahale artık çok daha etkin.

Ancak, BT bütçeleri siber güvenliğin değişen yüzüne ayak uydurmakta başarısız kalıyor. Harcamaların %77'si hâlen önleme ve korumaya yapılmaktadır.[2] BT güvenlik yöneticilerinin sadece %36'sı etkin uç nokta güvenliği için geniş bütçeye sahip olduklarını düşünmektedir.[3]

Güçlü veri koruması mümkündür. Doğru teknoloji (bireysel aygıtlara kadar tespit ve müdahale çözümleri), doğru strateji ve yeterli kaynaklar ile kuruluşlar kendilerini siber suça karşı koruyabilirler.

Siber güvenlik yatırımlarını artırmada ve yatırımı gerçekten etkin bir savunmaya yönlendirmede başarısız olunması, artan sıklıkta güvenlik ihlalleriyle ve kuruluşa yönelik artan bir maliyetle sonuçlanacaktır.

Giriş

Sınırları belli olmayan ağlar çağında siber güvenlik
BT liderlerinin %60'ı, siber suçların artan hacminin ve karmaşıklığının kendi savunmalarını aştığını hissetmektedir. Güvenlik liderlerinin %80'i Gelişmiş Kalıcı Tehditlerden (APT'ler), suç örgütlerinden, devlet destekli korsanlardan ve hacktivistlerden gelen tehdidin büyüdüğü ve BT güvenliğine yönelik en büyük zorluk olduğu değerlendirmesini yapmaktadır.[4]

Haksız da değiller. İngiltere'de hükümet, siber suçun ekonomik maliyetini 27 milyar GBP olarak belirlemiştir ve bu rakam işletmelerin kaybını oluşturan 21 milyar GBP ile "önemli ve muhtemelen artmaya devam eden" bir rakamdır.[5] Ponemon'un 2016 Uç Noktaların Durumu Raporunda, işletmelerin %78'i kötü amaçlı yazılım saldırılarının şiddetinde artış olduğunu bildirmiştir (2011'de bu oran %47'ydi).

Ancak, dış tehditlere odaklanmak yanıltıcı olabilir ve kaynakların boşuna çevre savunmasına yoğunlaşmasına yol açabilir.

Dış saldırılar (virüsler, kötü amaçlı yazılım, kimlik avı) daha yaygın olmasına rağmen, kurum içi saldırılar daha maliyetlidir.[6] Ve bu dış saldırıların çoğu, iç güvenlik açıklarından ve güvenlik protokollerini göz ardı eden, güvensiz aygıtları ağa bağlayan ihmalkar çalışanlardan kaynaklanır. Ponemon anketine yanıt verenlerin yaklaşık %81'i bunu BT güvenliğine yönelik en büyük tehdit olarak tanımlamıştır.

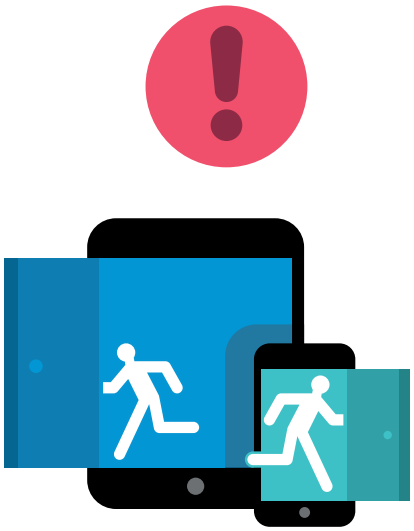
Bu sadece zamanla daha da gerçeğe dönüşecektir. Uç nokta, herhangi bir ağdaki en zayıf düğümdür ve "Kendi Cihazını Getir" politikası, uzaktan çalışma ve Nesnelerin İnternetindeki büyümeyle birlikte uç noktalar katlanarak artmaktadır. Yani, korsanlar için girişlerin sayısı da katlanarak artmaktadır.

Eskinin Ethernet ile birbirine bağlı masaüstü bilgisayarlardan oluşan kontrollü ağlarına karşılık yeni işletme ağları ofis içinde ve dışında çok sayıda WiFi düğümü üzerinden verilere erişilen, iş ve kişisel cihazlardan oluşan ve sınırları belli olmayan birer karmaşık şebekeye dönüştü.

Durum, tartışılmaz değildir. Bu basit biçimde siber güvenliğe yeni bir yaklaşımı benimsemek anlamına gelir. Siber suçun değişen yüzüne yanıt veren yeni stratejiler. Artan tehditten kaynaklanan karmaşıklığın yönünü değiştirebilen yeni teknoloji.

Bu teknik dokümanda, çok sayıda aygıt, güvensiz ağlar ve bulut çağında siber güvenliğin üstesinden nasıl gelineceği sorusunu çözmeden önce (düşmanımızı daha iyi tanımak amacıyla) tehdidin niteliğini ve ölçeğini inceleyeceğiz.

[1] HPI Printer Security Research 2016 (Spiceworks)
[2] PAC Incident Response Management 2015: https://www.pac-online.com/download/19443/155514
[3] Ponemon 2016 State of the Endpoint Report
[4] IBM CISO Assessment 2014
[5] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
[6] https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat-infographic



Tehdidin ölçeği

Bilgi ihlalleri şirketler için ortalama olarak, gelirde %13 kayıpla birlikte 907.053 ABD dolarına mâl olmaktadır. Ortalama olarak, bir kuruluşun kendine gelmesi dokuz hafta sürmektedir.[7]

HP 2015 Yazıcı Güvenliği Raporunda araştırılan şirketlerin yaklaşık olarak %85'i önceki 12 ay boyunca bir güvenlik tehdidi/ihlali yaşadıklarını söylemiştir. Ankete katılan BT uzmanlarının %80'i sonraki üç yıl içinde tehdidin artmasını beklemektedir.[8]

Siber suç, gerçek paraya mâl olmaktadır. Çalınan veya hasar gören varlıklardan kaynaklanan kayıp değer. İtibar zararı ve kayıp üretkenlikten kaynaklanan kayıp gelir. Kurtarma için kullanılan kayıp kaynaklar: destek masası zamanı, yeni güvenlik politikalarının uygulanması, personel kayıpları ve diğer iç müdahaleler. Düzenleyici makamların verdiği para cezaları ve yaptırımlar. Hisse fiyatında gerileme.

Tehdit yalnızca ağa bağlı olan aygıtların sayısı ile birlikte büyümeye devam etmektedir. Nesnelerin İnterneti (IoT) sayesinde, Gartner 2016'da 6,4 milyardan artarak, 2018 itibarıyla 11,4 milyar bağlı aygıt olacağını tahmin etmektedir. 2020 itibarıyla, işletmelerde tanımlanan saldırıların %25'inden daha fazlası IoT ile ilgili olacaktır, ancak IoT güvenlik bütçelerinin %10'undan daha azını oluşturacaktır.[9]

Siber suçtan kaynaklanan tehdit büyüktür ve giderek daha büyümektedir.

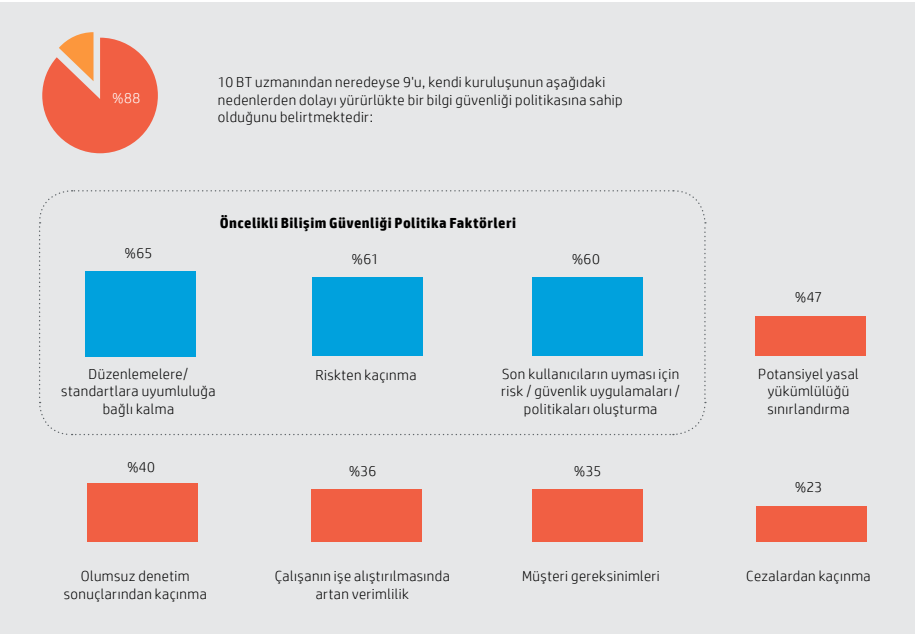
Tehdidin şekli

İşletmeler her gün sayısız siber saldırı yaşarlar. Çoğu düşük düzeyli virüs ve kötü amaçlı yazılım saldırısıdır. 2016'da Ponemon tarafından araştırılan kuruluşların %99'u, önceki 12 ay içinde kötü amaçlı yazılım deneyimini yaşamıştır. Bunun gibi web tabanlı dış saldırılar, ortalama 4.639 ABD doları maliyet ile kuruluşlar için nispeten daha az zararlıdır.[10]

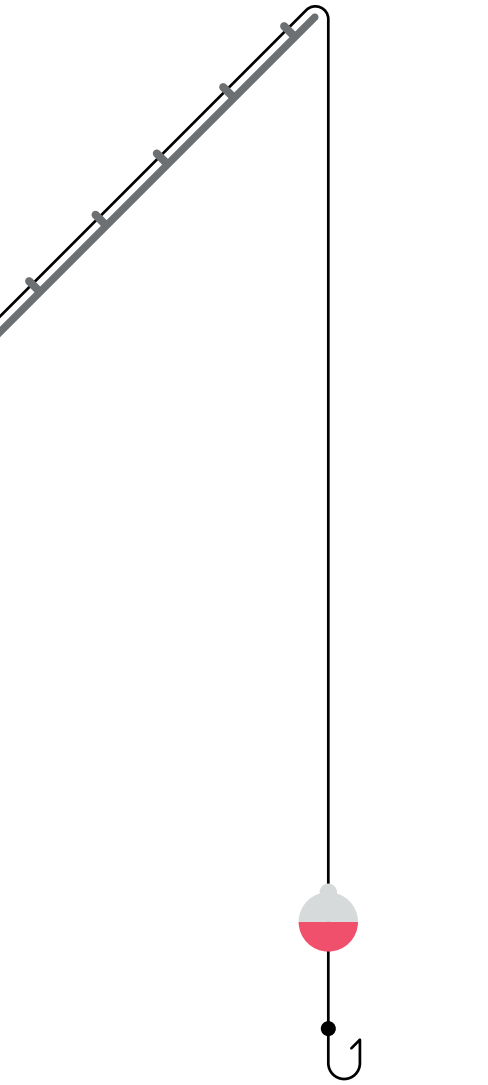
Ancak daha ciddi saldırılar giderek yaygınlaşmaktadır. 2015'te araştırılan kuruluşların %51'i ortalamada 127.000 ABD dolarına mal olarak felç edici olabilen Doğrudan Hizmeti Engelleme (DDoS) saldırılarını yaşamıştır. Daha da uyarıcı olan, %35'i 145.000 ABD dolarlık ortalama bir maliyetle kötü amaçlı iç saldırı yaşamıştır.[9]

Ortaya çıkan resim, dışarıdan ara sıra gelen küçük saldırıların yanı sıra giderek artan oranda büyük saldırılarla karşılaşılmasıdır ve büyük ihtimalle kurum içi çalışanların kötü amaçlı olmayan ihmalleri bunlara olanak tanımaktadır. Kuruluşların %62'si ortalama 86.000 ABD doları tutarında bir maliyet karşılığında çalışanların zayıflığından yararlanan kimlik avı/sosyal mühendislik saldırılarını yaşamıştır.[11]

Spiceworks tarafından (HP adına) yürütülen ayrı bir anket, 90 İngiliz kuruluşu tarafından 2014-2015 yıllarında yaşanan saldırıların dökümünü çıkarmıştır.[12]



[7] NTT Security Risk:Value Report 2016
[8] HP 2Printer Security Report 2015
[9] http://www.gartner.com/newsroom/id/3291817
[10] https://ssl.www8.hp.com/ww/en/secure/pdf/4aa6-8392enw.pdf
[11] https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat-infographic
[12] HPI Printer Security Research, Spiceworks 2016



Güvenlik ihlalleri nasıl oluşur

Manşetler, girişken korsanların, devletlerin ve işletmelerin gelişmiş güvenli ağlarından daha iyi oldukları şeklinde bir portre çizmektedir, ancak gerçek genellikle daha ölçülüdür.

Virüsler, tehlikeye giren ağlardan yararlanabilir, ancak kötü amaçlı yazılımlar genellikle bir çeşit kullanıcı hatası gerektirir. Kimlik avı/sosyal mühendislik saldırıları bunlara dayanır. Büyük DDoS ve bilgi hırsızlığı saldırıları sıklıkla kullanıcının ihmalinin sonucudur.

Herkesin duyduğu Dropbox güvenlik ihlalinin, LinkedIn hesabı ile aynı parolayı kurum içi sistemleri için kullanan dikkatsiz bir Dropbox çalışanından kaynaklandığı söyleniyor.[13] DNC'nin iddiaya göre Ruslar tarafından kırılması görünüşe göre Bayan Clinton'un eski danışmanı olan ve bir yardımcısı tarafından yanlışlıkla 'uygun' olarak işaretlenen bir kimlik avı e-postasındaki bir bağlantıya tıklayan John Podesta sayesinde gerçekleşmiştir.[14]

Korsanların başarılı olmak için aktif bir yardıma ihtiyaçları yoktur. Güvenlik protokollerinin bilinmemesi ve bunlara uyulmaması da aynı ölçüde tehlikelidir. Artan bir tehdit, çalışanların ticari bulut yazılımı kullanarak kendi aygıtlarını işe getirmesidir; bunların her ikisi de aslında güvenli olan bir ağa kurumsal BT'nin denetimi dışında güvensiz unsurların sızmasına ve dikkatlerden kaçan güvenlik açıklarının ortaya çıkmasına neden olur.

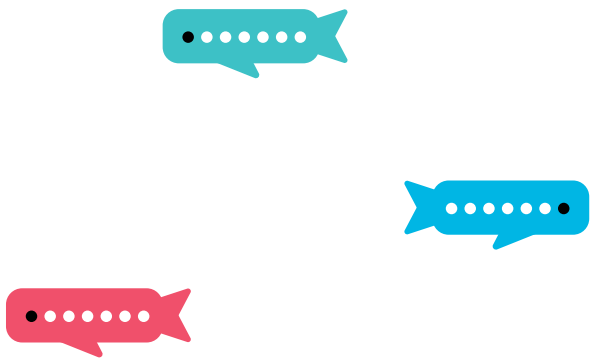
Çoğu zaman, korsanların ileri düzey algoritmaları veya en gelişmiş teknolojiyi kullanmaları gerekmez, sadece birimizin biraz dikkatsiz olması onlar için yeterlidir.

Güvenlik duvarı kırıldı

Siber güvenliğin mihenk taşı bugüne kadar antivirüs ve güvenlik duvarı yazılımıydı. Önleme ve koruma. Güvenli bir çevre oluşturma. Günümüzün çalışma ortamında, bu kesinlikle güvenilir bir strateji değildir.

Ponemon katılımcılarının %81'i ağlarındaki mobil aygıtların kötü amaçlı yazılımların hedefi olduğunu söylemektedir. Güvenlik risklerine yönelik diğer artışlar arasında, çalışanın ticari bulut uygulamalarını kullanımı (katılımcıların %72'si belirtmiştir), "Kendi Cihazını Getir" politikaları (%69) ve ev ofis ve saha dışı konumlarda faaliyet gösteren çalışanlar (%62) yer alır.[15]

Basitçe söylemek gerekirse, bir ağ yöneticisi olarak hangi aygıtın bağlanacağını denetleyebilirseniz güvenlik duvarı anlam ifade eder. Ancak, çalışanların çalışmak için kendi (sıklıkla, BT'nin bilgisi olmadan birden fazla) aygıtını getirdiği ve artan sayıda çalışanın size uzaktan bağlandığı bir çağda, çevreyi kolaylıkla koruyamazsınız. Her bir onaylanmamış aygıt, korsanların yararlanacağı hassas bir uç noktadır.



[13] https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach

[14] https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0

[15] Ponemon 2016 State of the Endpoint Report

HP bakış açısı: ağ güvenliğinin ötesine geçmek

Michael Howard, uç nokta güvenliğini sağlama konusunda HP'nin dünya çapındaki güvenlik uygulaması yöneticisi

Temel ve güncel bir endişe, işletmelerin belirli aygıtlar ve taşıdıkları riskler hakkında farkındalık ve bilgi eksikliği nedeniyle her bir uç noktanın güvenliğini sağlamada zorlanmalarıdır. Saldırılardan korunmak için artık yeterli olmamasına karşın bir güvenlik duvarının ardında kendilerini güvende hissederler. Güvenlik ekipleri, altyapıdaki her uç noktayı bilmeli ve her bir uç noktanın giderek karmaşıklaşan saldırılardan korunmak üzere çok katmanlı korumaya sahip olduğundan emin olmalıdır.

Güvenlik ekiplerinin kendi BT altyapılarının her bir köşesini araştırmaları ve standart ağ çevrelerinin üzerinde ilave bir koruma katmanı oluşturmaları esastır. Güvenlik duvarları yalnız başlarına çok gelişmiş saldırılara karşı koyamazlar ve her uç noktada çok sayıda koruma katmanına sahip bir savunma politikası, işinizin düzenleyici gereksinimleri karşılayabilmesini ve yüksek para cezalarından kaçınmasını sağlamak için olmazsa olmazdır.

HP'nin politikası, geliştirilen her çözüm, hizmet ve üründe ilk dikkate alınan unsurun güvenlik olmasıdır. Geliştirme ekipleri, güvenlik sorularını yanıtlamaları gerektiğini ve bunları ağa güvenli biçimde uygulamaları gerektiğini bilirler.

Önceden hiç olmadığı kadar, güvenlik yalnızca bir dişli olmamalı ancak, ilk sırada yer almalıdır. Bu, yıllardır HP politikasıdır.

Katmanlı güvenlik

Siber güvenliğe yönelik yeni yaklaşımın, çok katmanlı olması gerekir.
Ağ güvenliği hâlâ önemlidir, ancak ayrı ağlardan oluşmalıdır. Pek çok güvenlik ihlali, sistemde her şeye erişimi sağlayan ilk girişte gerçekleşir. John Podesta'nın kimlik avında yanlış adımını düşünün. Hassas bilgileri, bir anahtarın çalınmasının kaleyi fethetmek anlamına gelmeyeceği şekilde çok sayıda erişim katmanında korumak esastır.

Cihazlar tanımlanmalıdır. BT yöneticileri için temel bir sorun, ağa bağlı olan her bir aygıtın (virüslere, kötü amaçlı yazılıma ve casus yazılıma karşı) düzenli olarak güncellenen bir güvenlik yazılımı ile korunmasını ve anormalliklere karşı düzenli olarak taranmasını sağlamaktır. Daha iyisi, aygıtların kendisini parçası oldukları ağ çevresine yönelik ihlalleri ikaz edecek şekilde gerçek zamanlı bilgi toplayan birer sensör olarak kullanmaktır.

Kapsamlı güvenlik yönetimi uygulanmalı ve her bir çalışan siber güvenlik protokolleri konusunda eğitilmelidir. Yanlış bağlantıya tıklamaktan, bir tüketici aygıtına bağlanmaya kadar insan hatası ağa yönelik bir numaralı tehdittir. İnsan hatası, eğitimle azaltılabilir.

Cihaz güvenliği

Belki de çağdaş siber güvenliğin karşılaştığı en büyük sorun, hangi aygıtların ağ erişimine sahip olacağının kontrol edilmesidir.
Birinci basit çözüm, sıklıkla konuklar ve çalışanlar için ayrı WiFi ağlarına sahip olmaktır, böylelikle güvensiz dış aygıtlar ana ağa erişemezler. Bunun yanı sıra, kişisel aygıtlarıyla bu ağı kullanan çalışanlar da eğitilmelidir.

İkincisi, çalışanların aygıtları üzerinde kontrole sahip olduğunuzdan emin olmaktır. Bu endişenin, şirketin "Kendi Cihazını Getir" (BYOD) veya "Kendi Cihazını Seç" (CYOD) politikasında belirtilmesi gerekir ve CYOD lehine güçlü bir argümandır, yani, hangi aygıtların kullanıldığı, daha iyi güvenlik özellikleri olanların seçimi, nasıl yapılandırıldıkları ve bu aygıtların yönetimi ve izlenmesi konusunda daha fazla denetim sağlar.

Örneğin, HP Elite yelpazesindeki bilgisayarlarımızdan birini kullanmak, ekonomik bir dizüstü bilgisayara tercih edilebilir. Her bir HP Elite bilgisayar, BIOS'u 15 dakikada bir kontrol eden ve bir anormallik durumunda istenmeyen yetkisiz giriş yapanları bloke ederek makineyi orijinal durumuna sıfırlayan HP SureStart teknolojisine sahiptir. Bu özellik (ve daha bir çoğu) sayesinde, HP Elite PC 800 serimizdeki bilgisayarlar yakın tarihte "dünyadaki en güvenli bilgisayarlar" olarak ilan edilmiştir.[16] Ancak çalışanların kendi başlarına bir HP Elite bilgisayara sahip olma ihtimalleri yoktur.

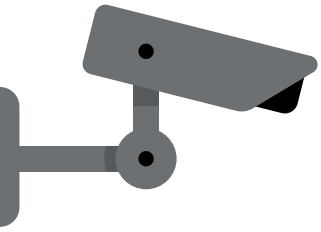
Çalışanlar sıklıkla kendi aygıtlarını iki nedenden dolayı tercih ederler:
1. Tüketici teknolojisi, sıklıkla işyerinin sağladığından daha iyidir
2. Çalışanlar bildikleri teknolojiyi kullanmaktan hoşlanırlar

Düzenli bir güncelleme döngüsü dahilinde en son aygıtları sağlayan iyi kaynak ayrılmış bir CYOD politikası sunularak, kuruluşlar çalışanların sahip olduklarından daha iyi aygıtları sağlayabilir ve bu aygıtlardaki güvenlik üzerinde daha fazla kontrole sahip olabilirler. HP Hizmet Olarak Aygıt (DaaS) çözümümüzle işte bunu satıyoruz.

Sıklıkla unutulanlarla birlikte güvenlik stratejisine tüm aygıtları dâhil etmek esastır. Bir IDC anketinde, katılımcıların %80'i BT güvenliğinin işleri için önemli olduğunu söylemiştir, ancak yarıdan fazlası önceki 12 ay içinde baskı güvenliğini içeren bir güvenlik ihlali yaşamalarına rağmen, sadece %59'u baskı güvenliğinin önemini fark etmiştir. Bu açık bir kör noktadır.

Bir baskı güvenliği politikası uygulanmadan önce güvenlik ihlallerinin ortalama sayısı ortalama 521.400 ABD dolarında bir maliyetle (cezalar dâhil) yıllık 9,9'du. Baskı güvenliğinin uygulanmasından sonra, ihlallerin ortalama sayısı, 1,5'e düşmüş ve yıllık çalışan süresinde 200 saat ve denetim ve uyum dâhil olmak üzere ilgili maliyetlerde 250.000 ABD doları tutarında tasarruf sağlanmıştır.[17]

[16] http://www8.hp.com/us/en/campaign/computersecurity/
[17] IDC The Business Value of Printer Security 2015



Proaktif tespit ve müdahale

PAC araştırmasına göre, BT güvenliği harcamalarının %77'si antivirüs yazılımı ve güvenlik duvarları gibi önleme ve koruma teknolojisine gitmektedir. Ancak bu yaklaşım etkisizdir. Araştırma ayrıca, araştırılan firmaların %67'sinin önceki 12 ay içinde ve %100'ünün geçmişte bir dönemde bir siber güvenlik ihlali yaşadığını da ortaya koymuştur.[18]

Özellikle antivirüs yazılımı şaşırtıcı biçimde etkisizdir. Damballa, antivirüs müdahalesini ölçmek için bir ağa kasıtlı olarak saldırdığı bir test yürütmüştür. Kötü amaçlı dosyaların %100'ünün tanımlanması altı aydan daha uzun sürmüştür.[19] Bu, firmaların saldırıldıklarını anlamaları için bir ila altı ay arasında bir sürenin geçtiği başka bir PAC bulgusu ile örtüşmektedir.

Uç noktaların güvenli tutulması, artık önleme işlevine güvenemez. Artan sayıda virüs/kötü amaçlı yazılım olayı ile birlikte BYOD/mobil çalışmanın doğasında var olan güvenlik eksiği, ihlallerin kaçınılmaz olduğu anlamına gelmektedir. Hiç kimse önleme ve korumanın tamamen terk edilmesini önermiyor, ancak tespit ve müdahalenin kesinlikle gündemin üst sıralarına çıkması gerekiyor.

İdeal olarak uç noktaların sensör olarak kullanılması ve ihlal durumunda ağın kalanının uyarılmasıyla sürekli ve gerçek zamanlı izleme gereklidir. Bu da, BT güvenlik ekibinin şu gibi süreçlerle uzaktan müdahale etmesini sağlar:

- Bir aygıtın uzaktan kapatılması
- Virüs bulaşmış veya kötü amaçlı yazılımı yayan bir işlemin durdurulması
- Belirli bir dosyanın veya dosyalar grubunun karantina altına alınması
- Virüs bulaşmış aygıtları yalıtmak için ağ iletişimin kesilmesi[20]

İhlallerin oluşacaklarını kabul etmek ve uygun protokolleri yürürlüğe sokmak (ayrıca bunları yürütmek için gerekli teknolojiyi uygulamak) önlemeye artık güven kalmadığında, siber güvenliği sağlamanın tek yoludur.

> "İnsanlar göz ardı ettiği takdirde hiçbir teknoloji güvenliği sağlayamaz."
>
> – Joseph Steinberg [21]

Çalışan güvenliği

Aynı derecede, belki de aygıtın güvenliğinin sağlamasından daha da önemli olan, bunu kullanan kişinin güvenliğini sağlamaktır.
Her çalışan siber güvenlikte eğitilmelidir. Kimlik avının, şüpheli web sitelerinde gezinmenin ve şüpheli ekleri indirmenin risklerinin de farkında olmalıdırlar. Güçlü, benzersiz parolaları her hassas oturum açılışında kullanma ve bunları saklamak için doğru parola yöneticisini kullanmayı içeren, güvenli parola politikalarını bilmelidirler.

BT izlemesindeki yükü hafifletmek için kendi aygıtlarındaki güvenlik yazılımını düzenli olarak güncel tutmanın öneminin farkında olmalıdırlar. Kuruluşun ağlarına erişmek için yalnızca güvenli aygıtları kullanma konusunda dikkatli olmalı ve hassas verilere erişmek için dış, güvensiz ağlarda kişisel aygıtları kullanmaktan kaçınmalıdırlar.

Pek çok yüksek düzeyli siber güvenlik uzmanı, her çalışanı eğitmek için sahte kimlik avı web sitelerini oluşturmaya varan simüle edilmiş kimlik avı saldırılarının yürütülmesini ve siber güvenlik eğitiminin resmi bir düzeye taşınmasını önerir. Çünkü çoğu saldırı, ister ihmal yoluyla ister kötü amaçlı olarak insan zayıflığından faydalanır.

Çünkü insanlar, herhangi bir ağda en zayıf halkadır.

[18] PAC Incident Response Management 2015
[19] https://www.damballa.com/time-to-fix-malware-strategies-2/
[20] The Essential Endpoint Detection Checklist – HP Now
[21] https://digitalguardian.com/blog/data-security-experts-answer-what-biggest-misconception-companies-have-about-endpoint-security

Sonuç

IT güvenliği harcamaları, önleme ve korumadan, uç noktada tespit ve müdahaleye kaymalıdır.
Yükselen bir siber suç tehdidiyle ve ağ çevresi üzerinde kontrol kaybıyla yüzleşen bir kuruluşun verilerini mevcut BT ikliminde savunmak iki şeyi gerektirir: kavramsal bir sıçrama ve daha fazla kaynak.

Ağ konseptinin değişmesi gerekir. Ağın aygıtlardan oluşan bir koleksiyonun etrafında çit olması fikri artık geçerliliğini yitirmiştir. Artık gerçeği fark etmenin zamanı geldi. 'Ağ' bir kimeradır, yani çok başlı, çok yönlü ve çok boyutlu bir olgudur. Her biri bir uç noktası olan bağlantılı aygıtlardan ortaya çıkar. Ağın güvenliğini sağlamak, uç noktanın güvenliğini sağlamak demektir. Ve her bir uç da iki unsurdan oluşur: aygıt ve bunu kullanan kişi. Her ikisi de dikkate alınmalıdır.

Ancak bu yeni paradigmada güvenliği dayatmak, artık geçmişin Ethernet ile bağlı masaüstü bilgisayarlardan oluşan ortamlarından çok daha karmaşıktır. Daha fazla kaynak gerektirir ve bu kaynaklar için bastırılmalıdır. Ponemon katılımcılarının %61'i bunun farkındadır.

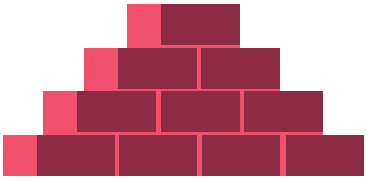
Buradaki ipucu, kuruluşun geri kalanını bu sürece dâhil etmektir. Katılımcıların sadece %36'sı uç nokta güvenliği için geniş bütçeye ve personele sahip olduklarını düşünmektedir. %69, BT departmanının çalışanların daha fazla destek talebini karşılayamadığını söylemektedir. %71, uç nokta güvenlik politikalarının dayatılmasının zor olduğunu söylemektedir.[22]

BT güvenlik yöneticilerinin %80'i düzenlemelerle uyumluluğun, güvenlik programlarının finansmanını gerekçelendirmenin en iyi yolu olduğunu değerlendiriyor, öte yandan uyumluluğu harcama yapmak için en az önemdeki neden olarak görüyor. Uyumluluk, minimum standartların karşılanması anlamına geliyor.[23]

BT karar vericiler, güvenliğin öneminin altını çizmek için en üst kademe yöneticiler ile irtibatta olmalıdır. Gevşek güvenlik maliyetlerini netleştirin (kurtarma harcamaları, kayıp gelir, tükenen hisse değeri) ve uzun vadeli tasarrufları vurgulayın. Pek çok güvenlik çözümü, başka yerlerde de iyileştirmeler sağlar. Baskı güvenliğini uygulamanın sağladığı artan üretkenliği ve abonelik üzerinden (HP DaaS gibi) üçüncü tarafça sağlanan esnek bir CYOD programında düzenli olarak yenilenen teknolojiyi sağlamanın üretkenlik faydalarını düşünün. Ayrıntılı bir olurluk incelemesi oluşturulabilir.

Mücadele, muazzamdır. Ve zamanla, IoT çağındaki aygıtların patlaması ve siber suçların giderek karmaşıklaşması ile bu sadece daha ürkütücü olacaktır. Ancak, aşılamaz değildir. Doğru teknoloji, doğru strateji ve doğru kaynaklar ile uç noktalarımızı savunabiliriz. Verilerimizi güvende tutabiliriz.

HP Hizmet olarak Aygıt çözümü hakkında daha fazlasını öğrenmek ve kapsamlı, esnek ve güvenli bir CYOD programını yürütmenin nasıl yardımcı olabileceğini görmek için **buraya tıklayın.**



Güncellemeler için kaydolun
hp.com/go/getupdated

Meslektaşlarınızla paylaşın

Bu belgeyi değerlendirin

4AA7-1089TRE

[22] Ponemon 2016 State of the Endpoint Report
[23] https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697