kaspersky GELECEĞİ YAKALAYIN

Covid-19'dan sonra geleceği korumak

2020'den sonra kurumsal siber güvenlik zorluklarıyla başa çıkma yolları

Salgın döneminde geçilen uzaktan çalışma modeli, BT departmanlarının isimsiz kahramanları sayesinde inanılmaz bir başarı hikayesine dönüştü. Yüz yüze etkileşime ihtiyaç duymayan işletmeler, karantina ve kısıtlamalar sırasında hayatta kalıp gelişme gösterirken, çalışanlar da şirket veya kişisel dizüstü bilgisayarları, PC'ler ve diğer cihazlar ile etkili ve güvenli bir şekilde evlerinden çalışmaya devam edebildiler.

Evden çalışma uygulamalarının benimsenmesinin; daha yüksek üretkenlik, işe gitmeme oranında düşüş, işe bağlılık seviyelerinde artış ve düşen ofis alanı masrafları da dahil bir dizi fayda sağladığı görüldü. Bazı çalışanlar için tamamen evden çalışılan bir çalışma hayatına geçmenin getirdiği o ilk heyecan artık zayıflamış olsa da, ev/ofis çalışma modellerinden oluşan bir 'karma' çalışma düzeninin artık bir standarta dönüşebileceği geleceği sabırsızlıkla bekleyebiliriz.

Kaspersky'nin yaptırdığı bir araştırma[1] şu sonuçları ortaya koydu:

- Çalışanların %74'ü, salgından önceki iş yeri dinamiklerinin en azından bir kısmına geri dönmek istemiyor
- %39'u, geleneksel 9–5 mesai yapısından kaçmaya hazır
- %34'ü, artık sabit bir ofis masasından çalışmak istemiyor
- %32'si, haftada beş gün olan çalışma süresini yeniden değerlendirmek istiyor

'Siber suçlardan kaynaklanan zararlar Koranavirüs salgını nedeniyle ikiye katlanmış olabilir'

Cybersecurity Ventures, Temmuz 2020

Siber güvenlik hikayesi

Peki çalışma şekillerinde böyle radikal bir değişim yaşanırken siber güvenlik alanında ne gibi ilerlemeler yaşandı? Uzakta yer alan ve çalıştırılan uç noktaların saldırılara karşı artan savunmasızlığı bunlardan biri; bunlar aracılığıyla tüm kurumsal altyapı da etkileniyor.

Kısaca, siber suçlular bu durumdan oldukça memnunlar.

- Salgından önce, FBI'nın İnternet Suçları Şikayet Merkezi günlük yaklaşık 1.000 siber suç şikayeti alıyordu. Şu anda bu sayı günlük 3.000 ile 4.000 arasında değişiklik gösteriyor[2].
- 2020 yılı Ağustos ayında yayınlanan bir Interpol raporu[3] 'Covid 19 sırasında siber saldırıların endişe verici seviyelerde' olduğunu ortaya koydu.
- Sektörün önde gelen dergilerinden Cybersecurity Ventures[4] evden çalışanlar güvenlik konusunda rahat davranırken, çalışanlara yönelik kimlik avı dolandırıcılıkları ve uzaktan gerçekleştirilen saldırılarda ani bir yükseliş görüldüğünü paylaştı.

Güvenliğe ilişkin sorunlar neler?

- Uzak uç noktalar artık kurumsal bir LAN üzerinden çalışmıyor. Yerel yönlendiriciler aracılığıyla ya da halka açıkl alanlardaki güvenli olmayan Wi-Fi kullanarak internete bağlanıyorlar. Yani bağlantıyı izinsiz izleme saldırılarına karşı daha savunmasızlar.
- Evlerdeki kurumsal cihazlar kişisel e-postaları kontrol etmek, bireysel ilgi alanlarıyla ilgili şeyleri takip etmek vb. için de kullanılıyor. Bu nedenle sıklıkla kişisel bilgisayar yerine de kullanılmış oluyor. Kalabalık bir ofis ortamı yerine evde, daha kişisel bir alanda çalışan kişiler iş dizüstü bilgisayarları aracılığıyla sahte ve potansiyel olarak tehlikeli internet sitelerini ziyaret etme eğiliminde olabilir ve bu da cihazları siber tehditlere daha açık hale getiriyor.
- KCG (Kendi Cihazını Getir) uygulaması benimsendiğinde riskler de artıyor. Burada kullanıcı aynı zamanda yöneticidir – bu durumda, kurumsal altyapınızla arayüz oluşturan cihazlara yüklenen güvenlik önlemleri veya bunların yapılandırmaları üzerinde ya oldukça az bir kontrole sahip olursunuz ya da hiç olmazsınız.

[1] İşin Geleceğini Güvence Altına Almak, Kaspersky, 2020

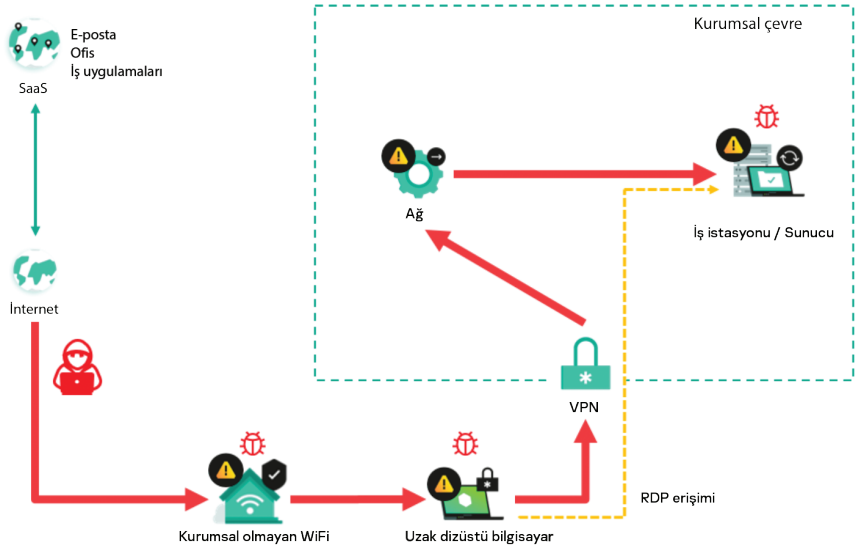
[2] Combatting Cybercrime During COVID-19, Aspen Digital, 2020

[3] COVID-19 döneminde siber saldırıların endişe verici seviyelerde olduğunu gösteren INTERPOL raporu, INTERPOL, Ağustos 2020

Bir uç noktanın güvenliği ihlal edilirse, kullanıcı çalışamaz ve cihazda saklanan değerli veriler risk altına girer. Ayrıca, örneğin, iş e-posta hesapları üzerinden müşterilerinize saldırılar düzenlemek amacıyla bir kullanıcının kimliği ele geçirilebilir. Daha da önemlisi, saldırganlar tek bir uç nokta üzerinden güvenlik çevrenize girerse; ağınız boyunca hareket etmeye, kötü amaçlı yazılımları yerleştirmeye, bunları etkinleştirmeye ve sistemlerinizin kontrolünü ele geçirmeye başlayabilirler. En karmaşık, en gelişmiş ve en geniş kapsamlı (ve pahalı) kurumsal saldırıların bile standart eylem planı şudur: İlk sızmayı tek bir savunmasız cihaz üzerinden gerçekleştirme.

VPN'ler veya RDP, uzak uç noktalar ve ağınız arasında güvenli iletişim kurulmasını sağlar. Ancak bunların da güvenliği ihlal edilebilir. Kaba kuvvet saldırıları, kimlik avı saldırıları veya sosyal mühendislik yoluyla elde edilen çalınmış kullanıcı kimlik bilgileri, size saldırmak isteyen ve sadece birkaç dolara sahip birinin dark web'te rahatlıkla bulabileceği şeylerdir. Ya da, örneğin, bir RAT (Uzaktan Erişim Sağlayan Truva Atları), size ya da kullanıcıya bir şey fark ettirmeden uç noktaya kurulabilir.

Bu giriş yollarından herhangi biri; fidye yazılım yüklemek, yasa dışı finansal işlem gerçekleştirmek ve verilerinizi çalmak için kullanılabileceği gibi, sadece sistemlerinize erişim sağlamak ve bu erişimi çevrimiçi ortamda en çok ücret veren kişilere satmak için de kullanılabilir.



Uzaktan çalışılan cihazlar ofislere getirilip ağa doğrudan erişim sağladıklarında, bu cihazlara bulaşmış olabilecek herhangi bir kötü amaçlı yazılımın da sistemlerinize doğrudan erişim sağlamalarının yolunu açtığını unutmamalısınız.

Çözüm

Genelde siber güvenlikte de karşılaşıldığı gibi, çözüm; özellikle de ilgili savunmasız uzak uç noktalara vurgu yapan çok katmanlı savunmaları kullanan çok yönlü bir yaklaşımda yatmaktadır.

İşte yapabileceklerinizden bazıları:

VPN/RDP düzeyinde

- **Çok faktörlü kimlik doğrulaması uygulayın** - VPN'e uç nokta erişimi için Çok Faktörlü Kimlik Doğrulaması (yani parola + güvenlik token'i)
- **Sadece kurumsal VPN'den gelen IP adresleri ile RDP erişimini sınırlayın**
- **Standart olmayan bir RPD bağlantı noktası numarası kullanarak** (3389 dışında) size saldıran kişinin işini zorlaştırın
- **Tüm web trafiğini güvenli proxy sunucunuz üzerinden yönlendirme** konusunu değerlendirin (bir çoğu için bu mümkün olmasa da gerekli kaynaklara ve kapasiteye sahip olduğunuzu varsayıyoruz)
- **VPN veya RDP üzerinden erişilebilen işlevleri ve uygulamaları sınırlandırın.** Gerekli yapılandırmayı gerçekleştirmek zaman alacaktır. Ancak bu yaklaşımın işletmeniz için kabul edilebilir olması durumunda buna fazlasıyla değer.
- **Çevre korumanızı güncellemeyi düşünün** – tehditlerin büyük bir çoğunluğunu uç nokta düzeyine ulaşmadan önce engelleyen e-posta sunucusu ve web ağ geçitleri güvenlik çözümleri genel olarak sağlam yatırımlardır.

Mart ayının başından bu yana Bruteforce. Generic.RDP saldırılarının sayısı neredeyse tüm dünyada ani bir yükselişe geçti[4]

[4] Remote spring: the rise of RDP bruteforce attacks, Kaspersky, 2020

İşle alakası olmayan internet sitelerine ve uygulamalara olan erişimin kontrol edilmesi; çalışma saatleri içerisinde sosyal medya, internette gezinme, online alışveriş ve diğer zaman kaybettiren faaliyetleri azaltma ve dolasıyla, genellikle uzaktan çalışma modelinin uygulandığı durumlarda ekonomik bir endişe olan verimliliği de artırma gibi ek faydalara sahiptir.

İş istasyonu düzeyinde

Sistemleri güçlendirerek saldırı yüzeyinizi daraltın. İş istasyonun "izin ver" ve "reddet" listeleri üzerinden belirli internet sitelerine erişimini sınırlayın veya yasaklayın ya da belirli uygulamaları çalıştırmasını engelleyin. Ya da bir 'varsayılan olarak reddetme' ilkesini uygulayarak cihazda, yalnızca iş ile ilgili olan ve sistemde yerel olarak bulunan uygulamaların çalıştırılması konusunu değerlendirin. Kurumsal cihazlarını kişisel ekipmanı gibi kullanan ve uzaktan çalışan kişiler bu durumdan memnun olmasalar da bu güçlü bir güvenlik yaklaşımıdır.

Kurumsal verileri korumak için şifreleme kullanın. Ofise tutulmayan cihazlar bazen kaybolabilir; şifreleme sayesinde bu cihazlarda bulunan her türlü gizli verinin yabancılar için erişilemez ve tamamen kullanışsız hale geldiğini unutmayın.

Yama yapmaya devam edin. Bu size sıradan gelebilir ancak doğru zamanda ve öncelik verilen yamalar kesinlikle kritik öneme sahiptir. Yaygın olarak kullanılan uygulamalardaki güvenlik açıklarından faydalanmak, hala kurumsal sistemlere girme konusunda kullanılan en popüler yasa dışı yöntemdir.

Şüpheli uç nokta faaliyetlerini tespit etmek için anormallik kontrolü kullanın. Doğru olmayan bir şeyler mi var? Uzak bir iş istasyonu olması gerektiğinden farklı mı davranıyor? Güvenlik çözümünüzün bu gibi durumları otomatik olarak tespit edebilmesi ve bunlarla hızlı bir şekilde ilgilenmesi gerekir.

Güçlü tespit ve düzeltme araçları kullanın. Güçlü bir EPP (Uç Nokta Koruma Platformu) ile birleştirilen EDR'nin (Uç Nokta Tespiti ve Yanıtı), özellikle de elden kaçabilen siber saldırılar söz konusu olduğunda, etkili uç nokta savunmalarının olmazsa olmazı olduğu artık yaygın şekilde kabul edilen bir konudur. Bunun, çok fazla zamanınızı almasına da gerek yok: Çoğu zaman, otomatik tespitler otomatik yanıtlarla karşılık bulabilir. Ekibiniz, sadece kullandığınız çözüm sizin dikkatinizi gerektiren ciddi bir sorun tespit ettiğinde konuya dahil olmalı.

Peki bunların hepsini kim yapacak?

BT alandaki işe alımların, öngörülen talebi karşılayabilmesi adına dünya genelinde yaklaşık olarak %89 oranında artması gerekiyor.[5]

Tavsiye vermenin uygulamaktan daha kolay olduğunu biliyoruz. Bilhassa bu görevlerin tümünü üstlenmesi gereken ve salgının isimsiz kahramanları olan BT uzmanlarının ve özellikle de BT Güvenliği uzmanlarının sayısı oldukça az. Yeterli sayıda BT güvenliği personelini işe almak (ve işte tutmak) fazlasıyla zor olduğundan BT Departmanlarının birçoğu, çoğunlukla olması gerekenden daha az personelle çalışıyor.

Uzaktan veya ev/ofis karması çalışma düzeninin, beraberinde getirdiği tüm ilave BT endişeleri ile birlikte yer aldığı bir gelecek senaryosunda, siber suç endüstrisi ortaya çıkan yeni fırsatlardan tam anlamıyla faydalanıyor olacak. Bu nedenle, mevcut BT güvenlik personelinizin mesaisini en verimli şekilde kullanmak kritik önem taşıyor.

Otomasyon

Çözümün büyük bir kısmı otomasyonda saklı. Anormallik kontrolü, yamalama ve diğer tespit ve sistem güçlendirme unsurları gibi yukarıda listelenen faaliyetlerin birçoğu, makine öğrenimi ve istihbaratı alanındaki gelişmeler sayesinde tamamen veya büyük bir oranda otomatikleştirilebilir. Hatta bunlara kök neden analizi ve yanıtı gibi çok daha gelişmiş süreçlerin bazıları da eklenebilir. Yani iş yükünüzün büyük bir bölümünü siz ve ekibiniz yerine güvenlik çözümünüz üstleniyor olmalı.

[5] (ISC)2 Cybersecurity workforce study, (ISC)2, 2020

Entegrasyon

Zamandan büyük ölçüde tasarruf edilmesini sağlayan şeylerden bir diğeri entegre bir güvenlik sistemiyle çalışmaktır. Tek bir konsol üzerinden sistemin tamamına tek bir kural dizisi atamak, hem daha etkilidir hem de yönetsel hataların gerçekleşmesi konusunda daha az hareket serbestliği sunduğu için riskleri azaltmanızı sağlar. Bu nedenle her birinin ayrı konsola sahip olduğu süslü ve yeni 'özel amaçlı' ürünlere yatırım yapmadan önce bir kere daha düşünün: Bu tür ürünlerin yapabildikleri çok az şey olmasının yanı sıra zamanınızı ve kaynaklarınızı da tüketebilirler.

Daha az uyarı

Güvenlik ekibiniz çok daha tehlikeli olan elden kaçabilen tehditlere odaklanabilecekken rutin uyarılarla çok fazla vakit kaybediyor olması muhtemeldir. Burada fark yaratacak şey temel EPP seçiminizdir. Sistem güçlendirme, etkili yama yapma ve otomatik tehdit önleme gibi özelliklerin tümü, zaten yoğun olan ekibinizin ilgilenmek zorunda kalacağı uyarı sayısını büyük oranda azaltacaktır. Ayrıca çözümünüzden sıfıra yakın oranda hatalı pozitif almayı beklemek de hakkınız: Ekibinizin vaktini bu gibi şeyler üzerinde harcamaması gerekir.

Yönetilen bir yaklaşım

Artık yönetilen bir güvenlik çözümüne bakmak için de iyi bir zaman olabilir. MDR (Yönetilen Tespit ve Yanıt), günümüzde baskı altında olan BT Departmanları tarafından yaygın olarak benimsenmiş bir çözümdür. Güvenliğinizin fazladan külfet yaratan kısımlarını yönetmesi ve BT Güvenliği Ekibinizin çalışmalarını desteklemesi amacıyla üçüncü taraf bir uzmandan yardım almak bir çok fayda sağlar. Üçüncü taraf bir sağlayıcının, gerektiğinde büyüyen veya değişen ihtiyaçlarınıza uyum sağlayabilecek 7/24 güvenlik izlemesi, gelişmiş kök neden analizi gibi görevleri ele alacak uzman becerileri, tehdit avı ve hatta rehberli ve uzaktan yanıt senaryoları, kaynakları ve üst düzey teknik uzmanlık gibi özellikleri sunabilecek bant genişliğine sahip olmalıdır. Öyle veya böyle, bazı yükleri üzerinizden alarak sizi destek olacak güvenilir bir üçüncü tarafla çalışmak sağlam bir iş yatırımıdır.

Siber farkındalığa sahip bir kültür

"Uzaktan çalışan kişiler bir an önce kendilerini eğitmez ve işletmeler çalışanlarına en kısa sürede, merkezinde evden çalışmaya ilişkin tehditlerin yer aldığı bir güvenlik farkındalığı eğitimi vermezse, bu yıl sonuna kadar küresel olarak siber suçlardan kaynaklanan zararların ikiye katlandığını görebiliriz."

Steve Morgan, Cybersecurity Ventures dergisi kurucusu ve Cybercrime Magazine genel yayın yönetmeni

Kullanıcıların; tehditlerin farkında olduğu, ihmal veya basit bir bilgi eksikliği nedeniyle altyapıyı tehlikeye atmaktan kaçınacak pratik becerilere sahip olduğu ve nerede olursa olsunlar siber hijyeni bir alışkanlık haline getirdikleri kurumsal bir kültürde, BT ekibinin iş yükü de doğal olarak azalacaktır. Her alana yayılmış bir siber farkındalık, kurum içerisindeki siber güvenli davranış kültürü ve temel siber güvenlik becerileri saldırı yüzeyini daraltmanın ve ilgilenmeniz gereken olay sayısını azaltmanın kilit noktalarıdır. İşletmeler genellikle etkili çalışan eğitimi konusunda doğru araçları ve yöntemleri bulmakta zorlanırlar; bunları sıfırdan oluşturmak ise hem karmaşıktır hem de zaman alır. Güvenlik farkındalığına sahip bir kültüre ulaşmak için doğru siber güvenlik eğitiminin uygulanması gerekir ve bu eğitimin, yetişkin eğitimine dair güncel teknikler ile teknolojilere sahip olması ve en önemlisi de uygun ve güncel içerikleri sunuyor olması gerekir.

Mutlu ve motive bir BT departmanı

Güvenlik uzmanları doğal olarak, sıkıcı rutin faaliyetlerle zaman kaybetmekten nefret ederler. Bu nedenle, onların üzerinden bu yükü alıp, çok daha zorlu görevlere zaman ayırmalarını sağlamak hem iş memnuniyetini hem de becerilerin akılda kalma düzeyini artıracaktır. Bu, ekibinizin uzmanlığını geliştirmeye yatırım yapabileceğiniz anlamına gelir (artık becerilerini geliştirebilecekleri eğitim kurslarına katılmak için yeterli bant genişliğine sahiptirler) ve bunun sonucunda başkaları tarafından saldırıya uğrama riskiniz daha da azalır – yani gerçek bir kazan-kazan durumu söz konusudur.

Bilgi teknolojisi (BT) ortamında uygulamaya konulan değişiklikler mevcut siber güvenlik önlemlerini zayıflatırken hızla uyarlanmalarını da birer zorluğa dönüştürdü. Siber güvenlik aynı zamanda dijital hizmetler için ortaya çıkan kullanım senaryolarında güveni temin eder. Bu nedenle söz konusu dönüşümü kolaylaştırma fırsatına da sahiptir.[6]

Nasıl yardımcı olabiliriz?

İster şirket içi ister yönetilen ya da ister her ikisini de tercih ediyor olun, zamandan en çok tasarruf ettiren ve maliyet verimliliği en yüksek olan yaklaşım, genel olarak size eksiksiz çok katmanlı bir EPP/EDR platformunu ve daha fazlasını sunabilen tek bir tedarikçiyi tercih etmek olacaktır. Aynı zamanda bu, uzun vadede sizinle birlikte ölçeklenebilecek bir çözüm aramak anlamına gelir. Bu sayede yatıracağınız parayı, her biri kendi konsoluna sahip ek ürünleri ve ileride ortaya çıkabilecek eğitim ihtiyaçlarını yönetmek zorunda kalmazsınız.

Kaspersky Optimum Security; ölçeklenebilir, kolay yönetilebilen uç nokta koruması becerileriyle büyüyen BT güvenliği ekibinizin, karma çalışma ortamları nedeniyle ortaya çıkan zorluklarla başa çıkmasına ve bu zorlukların üstesinden gelmesine yardımcı olur.

KASPERSKY OPTIMUM SECURITY

Kaspersky Endpoint Detection and Response Optimum

Gelişmiş tehdit görünürlüğü
Kök neden analizi
Otomatik yanıt

Kaspersky Managed Detection and Response Optimum

7/24 güvenlik izlemesi
Otomatik tehdit avı
Rehberli ve uzaktan yanıt senaryoları

Kaspersky Sandbox

Elden kaçabilen saldırıların gelişmiş otomatik tespiti

Kaspersky Treat Intelligence Portal

İnceleme için zenginleştirilmiş veriler

Kaspersky Security Awareness

Çalışanların siber güvenlik becerilerini artıran çevrimiçi eğitim programları

Size, arkasında benzersiz MDR uzmanlığı, beceriler, farkındalık eğitimi ve tabii ki eşsiz özel destek hizmetimiz olan, yüksek düzeyde otomatikleştirilmiş, tamamen ölçeklenebilir ve ödüllü bir EPP'nin güvenilir temellerine dayanan çok katmanlı bir uç nokta güvenlik çözümü sunuyoruz.

Kaspersky Optimum Security'nin, elden kaçabilen tehditlere karşı işletmenizin güvenliğini sağlamaya nasıl yardım ettiği hakkında daha fazla bilgi almak için lütfen http://go.kaspersky.com/optimum adresini ziyaret edin.

[6] ENISA Threat landscape - The year in review, European Union Agency for Cybersecurity (ENISA), 2020

Siber Tehdit Haberleri: www.securelist.com
BT Güvenliği Haberleri: business.kaspersky.com

www.kaspersky.com.tr