Tarafından derlendi

Fidye Yazılımı Savunması

for dummies®
A Wiley Brand

Cisco Özel 2'nci Baskısı

- Fidye Yazılımı Özelliklerini Tanımla
- Türünün en iyisi bir yeni güvenlik mimarisi inşa et
- Fidye Yazılımı saldırılarından korun

Lawrence Miller, CISSP

Cisco Hakkında

Cisco geniş çaptaki ürünleri dizayn eder ve satar, hizmetler sunar, ve dünya çapındaki ağları geliştirmek ve bağlamak için entegre çözümler sunar, interneti inşa eder.

Bulunduğumuz sektördeki global bir piyasa lideri olarak, müşterilerimize bağlanmaları, dijitalleşmeleri ve ilerlemeleri için yardım ediyoruz. Birlikte, dünyanın işleyişini, yaşayışını, hareket edişini ve öğrenişini değiştiriyoruz.

30 yıldan fazla bir süredir, müşterilerimizin ağlarını inşa etmelerine, otomotize etmelerine, yönetmelerine, entegre hale gelmelerine ve dijital bilgi teknoloji ürünleri ve servisler kurmalarına yardım ediyoruz.

Gittikçe artan bir şekilde bağlı hale gelen dünyada, farklı inovasyonlarla dünya çapındaki hükümetlerin, şehirlerin ve iş merkezlerinin dönüşüme uğrayabilmesi için Cisco yol göstererek yardım etmektedir.

Cisco Fidye Yazılım Savunması
www.cisco.com/go/ransomware

Cisco fidye yazılım savunması Cisco güvenlik mimarisini kullanarak ağadan DNS katmanına, e-maile ve uç noktaya varıncaya kadarbütün bir koruma sağlayarak işleri korur. Basit, etkili, otomatik ve açık olan fidye savunmasına karşı en üst düzey korunma yazılımdır.

www.twitter.com/CiscoUmbrella
www.facebook.com/CiscoUmbrella
www.linkedin.com/company/OpenDNS
www.youtube.com/c/CiscoUmbrella

Fidye Yazılımı Savunması

Cisco Özel 2nci Basımı

Lawrence Miller tarafından

For Dummies Fidye Yazılımı Savunması®, Cisco 2nci Özel Basımı

Yayıncı

John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-68277-6 (pbk); ISBN 978-1-119-68282-0 (ebk)

Amerika Birleşik Devletleri'nde Üretilmiştir.

10 9 8 7 6 5 4 3 2 1

Yayıncının Teşekkürü

Bu kitabın piyasaya sunulmasına yardımcı olan kişilerden birkaçı :

Proje Editörü: Elizabeth Kuball **Satın Alma Editörü:** Ashley Coffey **Editöryal Müdür:** Rev Mengle

İş Geliştirme Temsilcisi: Karen Hattan

Üretim Editörü Tamilmani Varadharaj

Özel Yardım: Rachel Ackerly, Lorraine Bellon, Scott Bower, Mary Briggs, John Damon, Tori Devereux, David Gormley, Dan Gould, Artsiom Holub, Gedeon Hombrebueno, Aivy Iniguez, Kate MacLean, Austin McBride, Ben Munroe, Mark Murtagh, Natalie Pino, Nicole Smith, Christina Soriano, Jolene Tam

Giriş

Fidye yazılımlarının(ransomware) yükselişi, hızlı bir şekilde son derece kazançlı bir suç girişimi haline geldi. Hedef alınan kuruluşlar genellikle fidyeyi ödemenin verilerini geri almanın en uygun ve maliyetli yolu olduğuna inanmakta maalesef ki bu doğru olabilir.

Baltimore Şehri Mayıs 2019'da kaosa neden olan bir fidye yazılımı(ransomware) saldırısına uğradı ve bir haftadan daha fazla bir süre şehir yetkilileri hayati altyapı sistemlerine ulaşamadı. Saldırının arkasındaki suçlular fidye olarak sadece 76.000 dolar istese de, saldırıdan kurtulmak karışıktı ve bu şehre yaklaşık olarak 18 milyon dolara mal oldu.

Ancak Florida'da buluna iki küçük şehir farklı bir yol tercih etti. Lake City ve Riviera Beach hükümetleri, Haziran 2019'daki fidye yazılımı saldırılarından sonra verilerinin geri alınması karşılığında saldırganlarına ödeme yapma kararı aldı, ama çalınan verilerin şifresini çözmek için yine de bazı çalışmalarla karşılaştılar. Şehirler bilgisayar korsanlarına toplamda 1 milyon dolar değerinde Bitcoin ödedi ve araştırmacılar bu tür saldırıların azalmayacağını söylemekteler.

Peki, bir sonraki şehir veya eyalet hükümeti saldırı ile karşılaştığında ödeme yapmalılar mı yoksa verilerini manuel olarak kurtarmak için uzun bir sürece mi girmeliler? Çoğu durumda, şehirlerin bu fidyeyi ödemesi ve verilerinin şifresini çözmek için zaman harcaması, parayı tüm sistemlerini geri yüklemek için harcamaktan daha mantıklıdır.

Öte yandan, IBM tarafından yapılan bir araştırma Amerikalı vergi yükümlülerinin, fidye yazılımının gasp taleplerinin ödenmesine ilişkin vergi paralarını desteklemediğini göstermekte. Anket, ankete katılanların yüzde 80'inin şehirlerine yönelik bir fidye yazılımı saldırısından endişe duyduklarını ve yüzde 60'ının, hükümetlerinin vergi yükümlülerinin dolarlarını kullanarak çalınan verileri geri alma umuduyla saldırganlara ödeme yapılmasını istemediklerini belirtti.

Problem şu ki, dosyalarını kurtarmak için para veren her kuruluş, yeni nesil bir fidye yazılımının(ransomware) geliştirilmesini direkt olarak finanse etmekte. Bunun sonucu olarak, fidye yazılımları(ransomware) daha karmaşık çeşitlerde ve daha spesifik hedefli saldırılarla gelişmeye devam ediyor.

Maliyetleri de artmaya devam ediyor. Cyberse-curity Ventures tarafından yapılan son araştırmalara göre, fidye yazılımı(ransomware) saldırılarının 2021 yılına kadar küresel ekonomiye yıllık bazda 6 trilyon dolara mal olacağını öngörülmekte!

Fidye yazılımlar mümkün olduğunca engellenmeli, bir ağı ihlal etmeyi denediğinde tespit edilmeli ve sistemlere ve uç noktalara bulaştığında olası zararı sınırlandırmak için kontrol altına alınmalıdır. Fidye yazılımı(ransomware) savunması, organizasyonun alan adı sistemi (DNS) katmanının ağ ucundan, veri merkezine ve uç noktacihazlarına kadar, nerede kullanılmış olurlarsa olsunlar kapsam içinde olan, türünün eniyisi yeni bir mimari bakış açısı gerektirir.

Bu Kitap Hakkında

For Dummies Fidye Yazılımı Savunması, fidye yazılımının nasıl işlediği ve tanımlayıcı özelliklerini (Bölüm 1), fidye yazılımının risklerini azaltmak için en iyi güvenlik uygulamalarını (Bölüm 2), türünün en iyisi yeni bir güvenlik mimarisini (Bölüm 2) inceleyen beş kısa bölümden oluşur. 3), Cisco Fidye Yazılımı Savunması çözülümü (Bölüm 4) ve önemli fidye yazılımı savunması tavsiyeleri (Bölüm 5).

Aptalca Varsayımlar

Çoğu varsayımın kendi kullanışsızlıklarından daha uzun yaşadıkları söylenir, ama ben yine de birkaç şeyi varsayıyorum!

Temel olarak, bilgi güvenliğine dair bazı şeyleri bildiğinizi varsayıyorum. Belki de C düzeyinde bir BT yöneticisi, BT yöneticisi, kıdemli BT mimarı, analisti veya yöneticisi veya güvenlik, ağ veya sistem yöneticisisiniz. Bu yüzden bu kitap öncelikle BT ağları, altyapı ve kurumsal sistemler hakkında az da olsa bilgi birikimine sahip olan teknik okuyucular için yazılmıştır.

Bu varsayımlardan herhangi biri sizi tanımlamaktaysa, o zaman bu kitap tam size göre! Bu varsayımlardan hiçbiri sizi tanımlamıyorsa, yine de okumaya devam edin. Bu harika bir kitap ve okumayı bitirdiğinizde fidye yazılımı savunması hakkında (kötü adamlar için) tehlike teşkil edebilecek kadar bilgi sahibi olacaksınız!

Bu Kitapta Kullanılan İkonlar

Bu kitap boyunca, önemli bilgilere dikkat çekmek için özel simgeler kullanıyorum. İşte ne beklenir:

Hatırla

Bu simge, yıldönümleri ve doğum günleri ile beraber kalıcı belleğinize, gri cevherinize veya noggin'inize girmesi gereken bilgileri işaret eder!

Teknik Şeyler

Burada insan genomunun bir haritasını bulamazsınız, ancak NERD-vana'nın yedinci seviyesine erişmek istiyorsanız, harekete geçin! Bu simge, jargonun altındaki jargonu açıklar ve efsanelerin —yani, ineklerin — yapıldığı malzemedir!

İpucu

Okuduğunuz için teşekkürler, umarım kitabı beğenirsiniz, lütfen yazarlarımıza iyi bakın! Gerçekten, bu simge faydalı önerilere ve faydalı bilgi parçacıklarına işaret eder.

Bu simge, annenizin sizi uyardığı şeylere işaret ediyor. Peki, muhtemelen öyle değil.

Uyarı

Ancak yine de dikkate almanız gerekir - kendinize biraz zaman kazandırabilir ve hayal kırıklığıyaşayabilirsiniz!

Bu Kitabın Ötesinde

48 kısa sayfada anlatabileceğimden çok daha fazla şey var, bu nedenle kendinizi bu kitabın sonunda "Tanrım, bu harika bir kitaptı. Daha fazlasını nereden öğrenebilirim?", şeklinde bulursanız, https://umbrella.cisco.com/how-to-stop- ransomware adresine gitmeniz yeterli.

BU BÖLÜMDE

» Fidyeyazılımınıtanımlamaveonu tanımlayan özellikleri

» Fidye yazılımı trendlerini inceleme

» Fidye yazılımının nasıl işlediğini anlamak

Bölüm 1
Fidye Yazılımı Nedir?

Fidye yazılımı, günümüzde en hızlı büyüyen kötü amaçlı yazılım tehditlerinden biridir ve halihazırda bir salgındır. Cybersecurity Ventures'ın araştırmasına göre, yeni bir kuruluş 2019'da her 14 saniyede bir ve 2021'de her 11 saniyede bir fidye yazılımlarının kurbanı olacak. Bu bölümde fidye yazılımının ne olduğunu, nasıl bir tehdit olarak geliştiğini ve nasıl çalıştığını öğreneceksiniz.

Fidye Yazılımını Tanımlamak

Fidye yazılımı, kurbanın verilerini sadece saldırganın bildiği bir şifreleme anahtarı ile şifreleme amacıyla bir siber atakta kullanılan ve böylece bir fidye ödemesi (genellikle Bitcoin gibi kripto para birimi) yapılana kadar kurbanın verileri işlemez hale getiren kötü amaçlı bir yazılımdır (kötü amaçlı yazılım).

Teknik Şeyler

Kripto para birimi, Bit-coin gibi para birimlerinin "basımını" düzenlemek ve taraflar arasında bir aracı öge ya da merkez bankası olmaksızın fon transferini doğrulamak için şifreleme yöntemi kullanan alternatif bir dijital para birimidir.

Fidye miktarları genellikle yüksektir, ancak çoğunlukla fahiş değildir. Mesela, bireyler için talep edilenler çoğunlukla 300 ile 600 dolar arasında değişirken, daha büyük kuruluşlar genellikle daha fazla ödeyeceklerdir. Fidye yazılımının bu karakteri, tasarımı gereği kurbanların kanun uygulayıcılara başvurması ve verilerinin ve olumsuz etkilerinin kaybı

dolayısıyla çok daha büyük çaplı doğrudan ve dolaylı maliyete maruz kalmak yerine, fidyeyi olabildiğince hızlı ödemelerini sağlama çabasındalardır. Ancak, saldırganlar dikkatlerini daha büyük miktarlar ödemeleri (ve daha fazlasını kaybetmek) için daha yüksek mevkiye sahip kuruluşlara odaklamaya başladıkça, bu miktarlar zaman içinde artmaktadır. Siber güvenlik şirketi Coveware tarafından incelenen davalara bakınca, bilgisayar korsanlarının fidye yazılımı saldırıları tarafından şifrelenen dosyaları serbest bırakmaları için verilen ortalama fidye talebi, 2019'da neredeyse iki katına çıkarak 12.000 doların üstüne çıktı.


Uyarı

Fidye miktarları da saldırı kurbanı ne kadar uzun süre beklerse büyük ölçüde artabilir. Yine, bu, kurbanın seçeneklerini sınırlandırmak ve kurbanın fidyeyi olabildiğince hızlıca ödemesine neden olmak amacıyla, tasarım gereği bir faktördür.

Modern Tehdit Varlığında Fidye Yazılımını Tanıma

Fidye yazılımı yeni bir tehdit teşkil etmiyor. PC Cyborg olarak bilinmekte olan en eski fidye yazılımı 1989'da piyasaya sürülmüştü. O zamandan beri fidye yazılımı gelişme gösterdi ve çok daha karmaşık hale geldi. Fidye yazılımı ek olarak aşağıdaki gibi gelişmelerle daha yaygın ve kazançlı hale geldi:

» **Süregelen dijital dönüşüm:** Daha fazla kuruluş işlemlerini dijital hale getirdikçe ve çalışanlar da işlerini yürütmek için e-posta, bulut uygulamaları ve mobil cihazları kullandıkça, saldırganlar açısından potansiyel giriş noktalarının sayısı katlanarak artıyor. Bir ağ ihlal edildikten sonra, kritik sistemler bağlandığında virüsler daha hızlı yayılabiliyor.

» **Kripto para biriminin yükselmesi:** Para birimi (Bitcoin gibi), müşterilere kolay ve neredeyse takip edilemez ödeme imkanları sağlıyor. Anonim siber suçluları, Kripto para spekülasyonlarının fiyatları artmaya devam ettikçe büyük fidyelerin potansiyeli de orantılı olarak artmakta.

» **Hizmet Olarak Fidye Yazılımının (RaaS) ortaya çıkması:** RaaS(küçük bir ücret karşılığında ve/veya fidye ödemesinin belirli bir yüzdesi karşılığında satın alınabilen fidye yazılımı), neredeyse herkesin fidye yazılımını kullanmasını kolay bir hale getirmekte.

ABD Personel Yönetimi Ofisi (OPM), Equifax, Target, Home Depot ve Capital One gibi kuruluşların ve işletmelerin siber saldırılar açısından hedef alınmakta olan büyük veri ihlal durumlarıyla ile alakalı dikkat çeken medya raporlarına karşın, kuruluşlara ve bireylere yönelik fidye yazılımlarının yükselişinden en çok etkilenenler onlar oldu.

Uyarı

Kaspersky tarafından hazırlanan bir rapora göre, fidye yazılımına maruz kalan işletmelerin yüzde 34'ünün verilerine yeniden erişim kazanmalarının bir hafta veya daha da fazla sürdüğünü gösteriyor. Kuruluşunuz bir hafta boyunca karanlıkta olsaydı ne yapardınız?

Locky, agresif bir fidye yazılımı olan bir varyant örneğidir. 2016 yılında, günde 90.000 kadar kurbanı açığa çıkarmaktaydı. O zamanlar, bir Locky saldırısı için ortalama fidye genellikle 0,5 ile 1 Bitcoin aralığındaydı. Cisco'nun Talos tehdit istihbarat grubundan alınan istatistiklere göre, bir fidye yazılımı saldırısında güvenliği ihlal edilen kurbanların yaklaşık olarak yüzde 2,9'u fidyeyi ödeme durumunda. Bu durumda, Locky 12 aylık bir süre içinde potansiyel olarak 33 milyon kurbana bulaşacak ve 287 milyon ile 574 milyon dolar arasında fidye ödemesi yapacaktır (bkz. Tablo 1-1).

TABLO 1-1 Locky Toplam Fidye Ödemelerinin Tahmini Hesabı

Ransom Fiyatı	1 Bitcoin	0,5 Bitcoin
Kurban/gün	90.000	90.000
Ödeme sayısı/gün	2.610	2.610
Bitcoin fiyatı (2 Ekim, 2016)	610.82 $= 1 Bitcoin	$610,82 = 1 Bitcoin
1-günlük karlar	1.594,240 $	$797.120
1-aylık karlar	47.826,206 $	$23.913,603
12-aylık karlar	573.926,472 $	$286.963,236

287 milyon dolarlık ölçülü bir tahmin, tek bir veri ihlali ile karşılaştırıldığında önemsizmiş gibi görünse de (örneğin, Target'e 300 milyon doların üzerinde bir maliyete sahip olduğu tahmin edilen 2013 Target veri ihlalleri gibi), kimlikleri ve/ veya kredi kartı bilgileri çalınan bireysel mağdurlar yerine,

hedeflenen kuruluşa yönelik maliyetler hakkındaki veri ihlalleri kaybı tahminlerinin temel alındığını anımsamak önemlidir. Kuruluşa mal olanlar aşağıdakileri içermektedir:

» Ödeme Kartı Endüstrisi (PCI) gibi çeşitli düzenleyici kurumlar tarafından uygulanan düzenleyici para cezaları

» İhlalden kaynaklanan davalarla ilgili yasal ödemeler

» İş kesintileri, marka itibarının zedelenmesi ve müşteri kaybı nedeniyle iş kayıpları

» Olaya müdahale ve kurtarma, halkla ilişkiler, ihlal bildirimleri ve etkilenen bireyler için kredi izleme hizmetleri dahil hizmet iyileştirme

İpucu

Ponemon Enstitüsü, 2019'da bir kuruluşa mal olan veri ihlallerinin ortalama maliyetinin 2014'e göre yüzde 12 artışla 3,92 milyon dolar olduğunu gösteriyor.

Bu arada Locky, Bitcoin fiyatının on kattan fazla arttığı 2018 yılında hala aktifti - 2 Ekim 2018'de tek bir Bitcoin 6.500 doların üzerine çıkmıştı! Kripto para fiyatlarında herhangi bir üst sınır olmadan, fidye yazılımlarının hedeflenen herhangi bir kuruluş için büyük bir mali yük olma potansiyeline sahip olduğunu görmek basittir.

Siber suçlular genellikle darkweb'de çalıntı kredi kartı ve kimlik bilgilerini özel yazılım, yapılandırma ve /veya erişim yetkisi gibi şeyleri kayıt başına birkaç sentten birkaç dolara kadar fiyatlarla satarlar. Karşılaştırıldığında, bir siber suçlu, bireysel kurbanlar ve kuruluşlar tarafından kendilerine doğrudan ödenen fidyelerden birkaç yüz ile on binlerce dolar arasında kazanabilir.

Javelin Strategy and Research'ün 2016 Kimlik Dolandırıcılığı Çalışmasında, kimlik hırsızlığı ve kredi kartı dolandırıcılığı mağdurlarına gerçek maliyetin 2015 yılında 15 milyar dolar olduğu tahmin edildi. Takip eden araştırmalar, kimlik hırsızlığı ve kredi kartı dolandırıcılığı oranının 2017'de 8,1 milyar dolardan 2018'de 6,4 milyar dolara düşmeye devam ettiğini gösterdi. Kimlik hırsızlığı ve kredi kartı dolandırıcılığı düşmekte olsa da (muhtemelen daha güçlü kart güvenlik önlemleri nedeniyle), fidye yazılımları da dahil olmak üzere diğer birçok siber saldırı artmaya devam ediyor.

Accen-ture tarafından yapılan araştırmalar, yaklaşık 5,2 trilyon dolarlık entegre değerin şu andan başlayarak 2023'e kadar küresel olarak siber saldırıların riski altında olabileceğini gösteriyor.

Fidye yazılımı saldırıları daha büyük ekonomik etkilere neden olmaya devam ettikçe, saldırı kalıpları da değişiyor. Saldırganlar, bireyleri ve küçük işletmeleri fidye için tutmak yerine "nicelikten çok kaliteye" yöneliyor. F-Secure tarafından yapılan bir araştırmada, geniş bir ağ oluşturmak yerine daha fazla saldırganın büyük bir ödeme şansını artırmakiçin belirli hedeflemeyi kullandığını buldu. Örnek vermek gerekirse, Ryuk fidye yazılımı ödemeleri, genellikle ortalama fidye yazılımı ödemesinden çok daha yüksektir. Bu, Ryuk saldırılarının daha yüksek ödeme yeteneğine sahip orta ile büyük ölçek arasındaki kuruluşlara yönelik yüksek hedefli doğasından kaynaklıdır.

Fidye yazılımı vektörleri de değişmekte. Geçmişte suçlular, birkaç şanssız kişinin yanıt vereceğini ve ağlarını fidye yazılımı saldırılarına maruz bırakacaklarını umarak çok miktarda kimlik avı e-postası gönderiyordu. Artık daha fazla fidye yazılımı çeşidi, ağa girmek için uzak masaüstü protokollerindeki güvenlik açıklarından yararlanarak, yama uygulanmamış sistemlerden ve sıfırıncı gün açıklarından faydalanıyor.

Fidye Yazılımının Nasıl Çalıştığını Anlamak

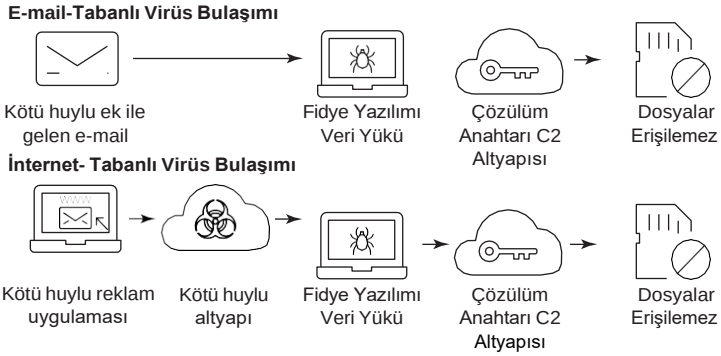
Fidye yazılımlar, genellikle istismar kitleri, sulama deliği saldırıları(water hole attack) (bir kuruluşun sıklıkla ziyaret ettiği bir veya daha fazla web sitesine kötü amaçlı yazılım bulaştığı), kötü amaçlı reklamcılık (kötü amaçlı reklamcılık) veya e-posta kimlik avı kampanyaları yoluyla dağıtılmaktadır (bkz. Şekil 1-1).


İpucu

Bir fidye yazılımı saldırısının anatomisini görmek için https://learn-umbrella.cisco.com/product-videos/ransomware-anatomy-of-an-attack adresine gidiniz.

FİGÜR 1-1: Fidye Yazılımının Virüsle Uç Noktayı Nasıl Etkiler

Fidye yazılımı teslim edildikten sonra, genellikle bir tür gömülü dosya uzantısı listesi aracılığıyla şifrelenecek kullanıcı dosyalarını ve verilerini tanımlamaktadır. Ayrıca, yükün çalışması bittikten sonra fidyenin teslimi için sistem kararlılığını sağlamak için belirli sistem dizinleriyle (WINDOWS sistem dizini veya belirli program dosyaları dizinleri gibi) etkileşimden kaçınabileceği şekilde programlanmıştır. Listelenen dosya uzantılarından bir tanesi ile eşleşme yakalayan belirli konumlardaki dosyalar daha sonra şifrelenir. Aksi takdirde, dosya(lar) yalnız kalır. Dosyalar şifrelendikten sonra, fidye yazılımı genellikle kullanıcıya fidyenin nasıl ödeneceğini içermekte olan talimatlar bildirimleri bırakır (bkz. Şekil 1-2).



FİGÜR 1-2: **Fidye Yazılımı Nasıl İşler**


Uyarı

Hırsızlar arasında onur yoktur. Fidyeyi öderseniz bir saldırgan genellikle dosyalarınız için şifre çözme anahtarını sağlar, ancak saldırganın uç noktanıza verilerinizi diğer suç amaçları için veya gelecekte daha fazla ödeme almak için veya diğer ağ sistemlerine halihazırda başka kötü amaçlı yazılım ve istismar kitleri yüklemediğinin ya da hırsızlık yapmayacağının herhangi bir garantisi bulunmamaktadır.

BU BÖLÜMDE

» Fidye yazılım hakkında proaktif olmak

» Seri cevap için fidye yazılımsavunması otomatikleştirme

» Saldırı gerçekleştikten sonra yeniden gruplandırma

Bölüm 2
FidyeYazılımRisklerini AzaltmakİçinEnİyi YöntemleriUygulama

Bu bölümde, tam ve doğru bir şekilde uygulanırsa kuruluşunuzun fidye yazılımlarına ve diğer siber güvenlik tehditlerine karşı etkin bir şekilde savunma yapmasına yardımcı olacak en iyi güvenlik uygulamalarını ve risk azaltma stratejilerini gözden geçireceğiz.

Saldırıdan Önce:Keşfet,Yürüt, Kuvvetlen

Kar amacı olmayan bir devlet danışma kuruluşu olan MITRE Corporation, özellikle güçlü hücum ve savunma ekipleri birlikte çalışıldığında, hücumun siber saldırılara karşı savunma için en iyi itici güç olduğuna inanıyor. Elbette, kuruluşların bir saldırgan tarafından hedef alınmadan önce proaktif olarak uygulayabilecekleri bir dizi çok iyi uygulamalar bulunmaktadır. Saldırganlar, ilk adımlarını kolayca atamazlarsa, diğer bir deyişle ayaklarını kapıdan içeri sokamazlarsa, kuruluşunuz hedef alınan bir saldırının odağı değilse, muhtemelen daha kolay bir kurban arayacaklardır.

Fidye yazılımı saldırıları fırsatçı olabilir. Saldırganın amacı genellikle mümkün olduğunca az risk ve çabayla kâr etmektir. Bu nedenle, bir saldırganın ağınıza girmesini mimari bir yaklaşımla engellemek bir fidye yazılımı saldırısının başarılı olmasını önlemenin en etkili yoludur.


Hatırla

MITRE ATT&CK matrisi, saldırganlar tarafından sistemlere erişmek ve siber saldırılar başlatmak için çeşitli aşamalarda kullanılan taktikleri, teknikleri ve prosedürleri tanımlayan bir çerçevedir. ATT&CK kategorileri sırasıyla:

- Başlangıç Erişimi
- Uygulama
- Israrcılık
- Ayrıcalık Yükseltme
- Savunmadan Kaçınma
- Kimlik Bilgileri Erişimi
- Keşif
- Yanal Hareket
- Toplanma
- Emir ve Kontrol (C2)
- Sızdırma
- Etki

İlk altı kategori, hedefin ağına ve sistemlerine erişim sağlamaya odaklanmıştır.

Saldırganlar genellikle bir hedefe ilk erişime üç yöntemden biriyle ulaşır:

» Şüphelenmeyenbirkullanıcınınağ kimlikbilgileriniifşaetmesiniveya kötü amaçlı yazılım yüklemesini sağlamak için sosyal mühendislik/kimlik avı

» Çalınan veya satılan, genellikle bir veri ihlali yoluyla açığa çıkan meşru kimlik bilgilerinin kullanılması

» Halka açık (İnternet) bir uygulama veya hizmetteki bir güvenlik açığından yararlanma

Uyarı

2019 Veri İhlali Araştırmaları Raporunda Verizon, kullanıcıların mobil cihazlarda aldıkları sosyal saldırılara karşı çok daha savunmasız olduğunu tespit etti. İki neden var:

» Mobilcihazlarküçüktürvekullanıcıarayüzleri,bire-postanınveya web sayfasının meşru olup olmadığının değerlendirilmesini zorlaştırmaktadır.

» İnsanlar genellikle mobil cihazlarını yürürken, konuşurken, araba kullanırken ve yakın dikkatlerini sınırlayan diğer aktiviteleri yaparken kullanırlar.

İpucu

Saldırganların kuruluşunuzun ağına ve sistemlerine erişmesini önlemek için aşağıdaki en iyi yöntemler uygulanmalıdır :

» Son kullanıcılarınız için düzenli güvenlik farkındalığı ve eğitimleri gerçekleştirin. Bueğitimilgi çekiciolmalıve güvenlik tehditlerive taktikleri hakkında en son bilgileri içermelidir. Aşağıdakileri yaptığınızdan eminolun:

- Kullanıcı kimlik bilgilerinin paylaşılmamasına veya ifşa edilmemesine (BT ve/veya güvenlikle bile), güçlü parola gereksinimlerine ve kimlik doğrulamanın güvenlikteki rolüne ilişkin şirket politikalarını güçlendirin (kullanıcılara "Ben değildim" ifadesini vereninkaredilemezlikkavramı dahil).!" savunması).
- Kimlik avı saldırılarını azaltmanın (veya tamamen ortadan kaldırmanın) bir yolu olarak, e-posta ekleri yerine başkalarıyla belge alışverişinde bulunmak için dosya paylaşım programları gibi şirket onaylı Hizmet Olarak Yazılım (SaaS) uygulamalarının kullanımını teşvik edin kötü niyetli ekler içerir.
- BuluttaPDFveMicrosoftOfficedosyalarıiçinyerelolmayanbelge oluşturmayıdüşünün.AdobeAcrobatReaderve MicrosoftWord gibi masaüstü uygulamaları genellikle istismar edilebilecek yama uygulanmamış güvenlik açıkları içerir.
- Düzenli olarak makro kullanmayan kullanıcılara talimat verin.MicrosoftOfficebelgelerindemakrolarıhiçbirzaman etkinleştirmeyin. Yakın zamanda, algılamadan kaçınmak için karmaşık gizleme teknikleri kullanan makro tabanlı kötü amaçlı yazılımlarda bir canlanma gözlemlendi.
- Olay raporlama prosedürlerini açıklayın ve kullanıcıların "Suçlu değil, mağdur sizsiniz" ve "Gizleme olaydan (zarar açısından) daha kötü" gibi mesajlarla güvenlik olaylarını raporlama konusunda kendilerini rahat hissetmelerini sağlayın.

- Fiziksel güvenliği korumayı unutmayın. Diğer sosyal mühendislik türlerinden daha az yaygın olmalarına rağmen,potansiyel olarak kişisel güvenliklerini ve bilgi güvenliğini tehdit eden çöp kutusuna dalma,omuz sörfü ve sırt üstü binme(veya arkaya bakma)gibi ziyaretçi eskort politikaları ve taktikleri kullanıcılara tekrarlanmalıdır. .

» Kuruluşunuzdaki güvenlik zayıflıklarını ve güvenlik açıklarını belirlemek için sürekli risk değerlendirmeleri yapın ve riski azaltmak için her türlü tehdit maruziyetini ele alın. Aşağıdakileri yaptığınızdan emin olun:

• Periyodikbağlantı noktası ve güvenlik açığı taramaları gerçekleştirin.

• Sağlam ve zamanında yama yönetimi sağlayın.

• Gereksiz ve savunmasız hizmetleri devre dışı bırakın ve sistem güçlendirme kılavuzunu izleyin.

• Güçlü parola gerekliliklerini zorunlu kılın ve iki faktörlü kimlik doğrulamayı uygulayın(mümkünse).

• Güvenli bir günlük toplayıcı veya güvenlik olayı ve olay yönetimi (SIEM) platformunda güvenlik günlüğünü merkezileştirin ve günlük bilgilerini sık sık gözden geçirin ve analiz edin.

Teknik Şeyler

Geçmişte, çoğu fidye yazılımı, bir e-posta ekini açmak veya kötü amaçlı bir bağlantıya tıklamak gibi bir tür kullanıcı etkileşimi gerektiriyordu veya yama uygulanmamış sistemlerden yararlanmayı içeriyordu. Ancak bazı fidye yazılımı türevleri, bir saldırı başlatmak için bir kullanıcının yardımına ihtiyaç duymamaktadır. Sodinokibi fidye yazılımı varyantı, fidye yazılımını etkilenen bir sunucuya indirmek ve durdurmak için bir yama yayınlanmadan önce bir saldırı başlatmak için Oracle WebLogic'te yakın zamanda açıklanan bir güvenlik açığını kullanmıştı.

Maalesef ki, elinizden gelenin en iyisini yapmış olmanıza rağmen, insanlar insandır (ve Soylent Green de insandır!) ve daha önce bilinmeyen ve dolayısıyla kapatılmamış güvenlik açıklarından yararlanan sıfırıncı gün tehditleri her zaman olacaktır. Saldırgan ağınıza erişmeyi başarırsa, bir sonraki adımı C2 iletişimi kurmaktır. Şunlar için:

- Kalıcılık sağlayın
- Ayrıcalıkları yükseltin
- Ağınız, veri merkeziniz ve son kullanıcı ortamınız boyunca yanlamasına hareketedin

Başarılı bir izinsiz girişin etkilerini azaltmak için aşağıdaki en iyi uygulamaları uygulayın:

- Saldırı riskini azaltmaya yardımcı olmak için kötü amaçlı etki alanlarını,IP adreslerinive İnternetaltyapısınıtahminedayalıolarak belirlemenizi sağlayan etki alanı adı sistemi (DNS) katmanı koruması dağıtın.
- Kişisel mobil cihazlar ("kendi cihazını getir" [BYOD] izin veriliyorsa) ve şeffaf olançıkarılabilirortamlar (USB sürücüler gibi) dahil olmak üzere tümuçnoktalardagüvenlikduvarını,gelişmişkötüamaçlı yazılım korumasını, şifrelemeyi ve veri kaybı önlemeyi otomatik olarak etkinleştirin. kullanıcı ve kullanıcı tarafından herhangi bir işlem gerektirmez. Bu, en iyi uygulamalara ve yerleşik politikalara göre yapmalarıgerekeniyapmasalarbile,hemağdakihemdeağ dışındaki dolaşımdaki ve uzak kullanıcıları korumaktadır.
- Yürütülebilir dosyaların ve diğer olası kötü amaçlı ek dosyaların engellenmesi veya kaldırılması, e-posta sahtekarlığını azaltmak için gönderen politikası çerçevesi (SPF) doğrulaması ve olası istenmeyen e-postaların oranlarını daraltmak için e-posta kısıtlaması (veya "gri listeleme") dahil olmak üzere e-posta ağ geçitlerinde güvenlik işlevselliğini etkinleştirin.
- Virüs bulaşmasını ve veri sızmasını önlemek için İnternet trafiğini, e- postaları ve Dosyaları analiz eden güvenlik ürünleri ve hizmetlerini etkinleştirin(Bölüm3 ve4'tedahaayrıntılıtartışılır)ve daha derin bağlam ve hızlı araştırma amacıyla tehdit istihbarat hizmetlerinden yararlanın. Bir saldırganın ortamınızdaki yanal hareketini kısıtlamak için segmentasyon kullanan sağlam, doğası gereği güvenli bir güvenlik mimarisi tasarlayın ve devreye alın.
- En azından saldırganın ayrıcalıkları yükseltme yeteneğini sınırlamak için "ayrıcalık kayması"nı uygulayın ve kullanıcıyı ortadan kaldırın.
- Kritik sistemleri ve verileri düzenli olarak yedekleyin ve geri yüklenebildiklerinden ve iyi olduklarından emin olmak için yedeklemeleri periyodik olarak test edin. Ayrıca yedeklerinizi şifreleyin ve çevrimdışı veya ayrı bir yedekleme ağında saklayın.
- Olay müdahale yeteneklerinizi değerlendirin ve uygulayın ve güvenlik duruşunuzun genel etkinliğini sürekli ve sürekli olarak izleyin ve ölçün.

İpucu

Çoğu fidye yazılımı, örneğin şifreleme anahtarlarını ve ödeme mesajlarını iletmek için sağlam bir C2 iletişim altyapısına dayanır. Bir kuruluş, bir saldırganın ağına bulaşan fidye yazılımıyla bağlantı kurmasını engelleyerek başarılı bir fidye yazılımı saldırısını durdurabilir. Örneğin, saldırgan virüslü bir uç noktaya şifreleme anahtarları iletemezse veya kurbana fidye ödemesinin nasıl gönderileceği konusunda talimat veremezse, fidye yazılımı saldırısı başarısız olur. Tablo 2-1'in gösterdiği gibi, birçok fidye yazılımı türü, C2 iletişimleri için ağırlıklı olarak DNS'ye güvenir. Bazı durumlarda, C2 iletişimleri için bir Tor (The Onion Router) tarayıcısı da kullanılır. Bu nedenle, proxy gibi bir yöntem kullanarak her iki iletişim türünü de engelleyebilmek önem teşkil eder.

Tablo 2-1 Fidye Yazılımında C2 İletişimi Örneği

İsim	Şifreleme Anahtarı	Ödeme Mesajı
Locky	DNS	DNS
TeslaCrypt	DNS	DNS
CryptoWall	DNS	DNS
TorrentLocker	DNS	DNS
PadCrypt	DNS	DNS, Tor
CTB-Locker	DNS, Tor	DNS
FAKBEN	DNS	DNS, Tor
PayCrypt	DNS	DNS
KeyRanger	DNS, Tor	DNS

Saldırı Sırasında: Tespit Et, Blokla, ve Savun

Kurumunuz saldırı altındaysa, mümkün olan hasarları sınırlamak için hızlı ve etkili olay müdahalesi gerekmektedir. Üstlenilecek belirli eylem adımları ve iyileştirme çabaları, her benzersiz durum için farklı bir şekilde olacaktır. Ancak, kuruluşunuzun olay müdahale yeteneklerinin genişliğini ve kapsamını öğrenmenin zamanı bil saldırı anında değildir!

Olaya müdahale çabalarınız iyice anlaşılmalıdır ve koordineli olmalı ve saldırıdan önce gerçekleştirilebilir ve iyi belgelenmiş ve tekrarlanabilir bir halde olmalıdır. Etkili olay müdahalesinin genellikle gözden kaçan önemli bir bileşeni, aşağıdakileri içeren bilgi paylaşımıdır:

» **Zamanında ve doğru bilgileri tüm paydaşlara iletmek:** Müdahale ve iyileştirme için yeterli kaynakların tahsis edilmesini sağlamak için yöneticilere ilgili bilgilerin sağlanması gerekir, kritik ve bilinçli iş kararları alınabilir, ve uygun bilgilersıraylaçalışanlara,kollukkuvvetlerine,müşterilere,hissedarlaravegenel halka iletilir.

» **Mimari boyunca yeni güvenlik istihbaratını otomatik olarak paylaşmak:** SIEM, tehdit istihbaratı ve korumalı alan araçları gibi farklı sistemlerden kritik verileri bir araya getirmek, olay müdahale ekibinin yüksek etkili güvenlik olaylarını hızla ortaya çıkarmasını ve etkin bir şekilde önceliklendirmesini sağlar. Örneğin,bir uç noktada yeni bir kötü amaçlı yazılım yükü algılanırsa ,herhangi bir güvenlik açığı göstergesini(IoC'ler)bulmak ve çıkarmak amacıyla analiz için otomatik olarak bulutta banlı bir tehdit istihbarat platformuna gönderilmelidir. Ardından yeni karşı önlemler otomatik olarak devreye alınmalı vebunlar uygulanmalıdır.

Saldırıdan Sonra: Kapsam, İçerik ve Düzeltme

Bir saldırı sona erdikten sonraki önemli eylemler şunları içerir:

İpucu

» Gerektiğinde yedeklerin geri yüklenmesi ve yeniden görüntüleme sistemleri dahil olmak üzere normal iş işleyişlerinin sürdürülmesi

» Kolluk ve denetim amaçları için kanıtları toplama ve saklama

» Gelecekteki saldırıları tahmin etmek ve önlemek için,örneğin ilişkili IPadresleri, dosya karmaları ve etki alanlarıyla ilgili etki alanlarını ve kötü amaçlı yazılımları belirleyerek adli verileri analiz etme

» Kök- neden analizi yapmak, öğrenilen dersleri belirlemek ve gerektiğinde güvenlik varlıklarını yeniden dağıtıma sunmak

Tahmine dayalı tehdit istihbaratı, kuruluşunuzun saldırganların mevcut ve gelecekteki saldırılar için kullandığı C2 altyapısını görmesini sağlayarak proaktif bir güvenlik duruşu sağlar ve böylece her zaman tehdidin önünde bir duruş sergiler.

BU BÖLÜMDE

» Türünün en iyisi veya hepsi bir arada arasında seçim yapma

» Entegre bir güvenlik portföyü ile her iki dünyanın da en iyisini elde etmek

Bölüm 3
Yeni Türünün En İyisi Güvenlik Mimarisini Oluşturma

Bu bölümde, güvenlik mimarisine yönelik mevcut yaklaşımlardaki çeşitli zorluklar ve fidye yazılımı da dahil olmak üzere modern tehditleri daha iyi ele alabilmek için türünün en iyisi yeni bir mimari hakkında bilgi edineceksiniz.

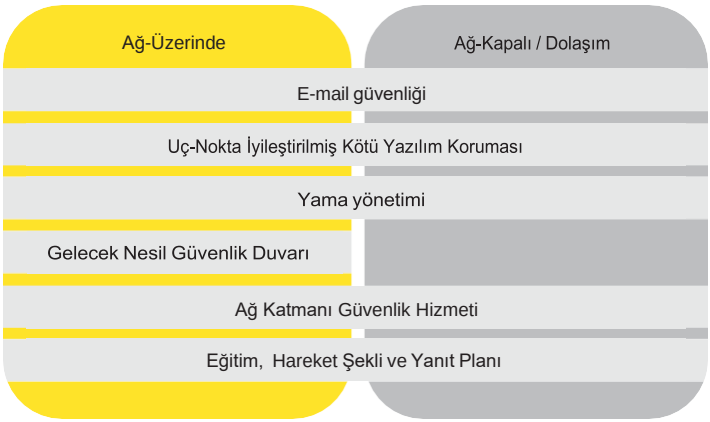
Mevcut Güvenlik Tasarımlarının Sınırlamalarını Kabul Etme

Geçmişte birçok işletme, güvenlik söz konusu olduğunda bir seçim yapmak zorunda kaldıklarını düşünmekteydi:

» Ortaya çıkan belirli tehdit türlerine karşı etkili olan, ancak savunmaları entegre etmek için mimari bir yaklaşıma tam olarak entegre olmayan türünün en iyisi ürünleri kullanabilirler.

» "Yeterince iyi" olan bağımsız(veya nokta)güvenlik ürünlerini akıllı bir sistem mimarisine özümseyen bir sistem yaklaşımı benimseyebilirler.

Günümüzde birçok kuruluş, bir güvenlik duvarı ve/veya web proxy sunucusu gibi bir DMZ veya yerel hizmetler bölgesinde konuşlandırılmış birden çok bağımsız güvenlik ürünü içeren bir erişim, dağıtım ve çekirdek katmandan oluşan hiyerarşik bir ağ mimarisini devreye sokmuştur. Ne yazık ki bu, gerçek "derinlemesine savunma" ile aynı şey değildir (bkz. Şekil 3-1).



FİGÜR 3-1: Güvenlik, riskleri katmanlar aracılığıyla yönetmekle ilgilidir.

Mevcut yaklaşımlarla ilgili sınırlamalar şunları içerir:

» **Entegrasyon veya korelasyon yoktur.** Çok sayıda bağımsız güvenlik ürünü,kaçınılmaz olarak, sınırlı güvenlik kaynaklarını, kolayca analiz edilemeyen ayrıntılı, koordine edilmemiş bilgilerle doldurur ve güvenlik ekiplerini ünlü "samanlıkta iğne" aramaya zorlar.

» **Çevre tabanlı güvenlik, etkili bir mimarinin yalnızca bir parçasıdır.** Ağ kenarında dağıtılan güvenlik duvarları, güvenli web ağ geçitleri ve korumalı alan teknolojisi, yalnızca İnternet'ten geçen kuzey-güney trafiğini görür. Veri merkezindeki doğu-batı trafiği (internet'i asla geçmeyen uygulamalar ve son kullanıcılar arasındaki trafik)tüm ağ trafiğinin yüzde 80'ini oluşturabilir - bu nedenle tüm ağ genelinde tam görünürlük gerekmektedir.

» **Çalışanlar binayı terk etti.** Siber suçlular yalnızca çalışma biçimlerini (taktik ve tekniklerini) değiştirmekle kalmadı, aynı zamanda kullanıcılarımızın çalışma ve dijital olarak etkileşimkurma biçimleri de değişti. Çeşitli cihazlarda doğrudan bulut üzerinden çalışan daha uzak ve dolaşım halindeki kullanıcılarla birlikte, çevre tabanlı güvenlik teknolojileri ve sanal özel ağlar (VPN'ler) artıkcihazları ve kurumsal verileri tam olarak koruyamaz. Birçok buluttabanlı hizmete(Salesforce.comve Office365 gibi)bir VPNbağlantısı olmadan kolayca erişilebilir,bu uygulamalar ve veriler yalnızca kötü amaçlı yazılımdan koruma gibi temel güvenlikle bırakılır. Enterprise Strategy Group'a göre, kuruluşların yüzde 79'u, geleneksel çevre güvenlik cihazlarını atlayarak ve kullanıcıları saldırı riski altında bırakarak uzak ofis konumlarında doğrudan İnternet erişimine (DIA) geçiyor. Modern güvenlik çözümlerinin, işletmenizin bulutu benimsemesine ve herhangi bir cihazdan, herhangi bir yerden, herhangi bir zamanda çalışmasına olanak tanıması gerekir; bu da mevcut korumayı geleneksel ağ çevresinin çok ötesine taşır.

» **Görünürlük eksikliği var.** Geleneksel bağlantı noktası tabanlı güvenlik duvarları, standart olmayan bağlantı noktaları, bağlantı noktası atlama ve şifreleme gibi kaçınma teknikleri kullanan birçok tehdide karşı kördür. Yeterli segmentasyon yoktur ve tipik bir segmentasyon zor hale gelebilir.Ağlar,genellikle yapılandırılması ve bakımı zor olabilen anahtarlarda tanımlanan statik sanal LAN'lar (VLAN'lar) ile "güvenilir" ve "güvenilmeyen" bölgelere ayrılır. Bu keyfi yapı, modern veri merkezlerindeki yeni normale hitap etmiyor - veri merkezleri ve bulutta dinamik olarak hareket eden sanal makineler (VM'ler). Bunun yerine, dinamik yazılım tanımlı segmentasyon ile veri merkezi genelinde ağ cihazlarında çoklu granüler segmentasyonun (mikro segmentasyon dahil) tanımlanması gerekir.

» **Statik güncellemeler yalnızca bir başlangıç noktasıdır.** Kötü amaçlı yazılımdan koruma imza dosyalarını indirmek ve yüklemek, günümüzün hızla gelişen sıfır gün tehditleriyle etkin bir şekilde mücadele etmek için yalnızca bir başlangıç noktasıdır.Sıfır gün tehditlerine ve bilinmeyen tehditlere karşı nasıl korunabilirsiniz ve aniden kötü niyetli hale gelen önceden zararsız dosyalara karşısavunmaya ne kadar hazırlıklısınız? Statik imza dosyalarının gerçek zamanlı, bulut tabanlı tehdit istihbaratı ve daha dinamik ve sürekli bir güvenlik yaklaşımıyla desteklenmesi gerekmektedir.

Yeni Türünün En İyisi Güvenlik Mimarisini Tanımlama

İşletmeleri fidye yazılımlarına ve diğer modern tehditlere karşı korumak için, türünün en iyisi yeni bir güvenlik mimarisi, geleneksel nokta ürünleri yerine basit, açık ve otomatikleştirilmiş, entegre, portföy tabanlı bir yaklaşımdan yararlanır. Bu yeni mimari:

» Tehdit istihbaratını otomatik olarak paylaşır ve hem şirket içinde hem de bulutta diğer güvenlik ürünleri ve hizmetleriyle birleştirilmiş, ilişkili bağlamsağlar

» Karmaşıklığı azaltır ve tüm ortamda tam görünürlük sağlar
» Açık, genişletilebilir standartlar ve teknoloji kullanarak yeni ve mevcut güvenlik yatırımlarıyla daha iyi entegrasyon sağlar

» Otomatikleştirilmiş güvenlik yanıtı sağlamak için bu entegrasyonu dikkate alır, böylece güvenlik daha etkili hale gelir ve diğer BT ekiplerinin üzerindeki yükü azaltır

Bu, işiniz için ne anlama geliyor? Bu yeni, türünün en iyisi güvenlik mimarisi, daha fazla tehdidi daha hızlı ortaya çıkarır ve ileriye dönük daha iyi düzeltme ve önleme sağlar. Platform tabanlı bir yaklaşım, kendi başlarına analiz edildiğinde gözden kaçabilecek tehdit sinyalleri arasındaki noktaları birleştirmek için ihtiyaç duyduğunuz bağlamsal farkındalığı sağlar. Ayrıca, tehdit avcılarının yalnızca ortamlarında ne tür tehditler olduğunu değil,aynı zamanda oraya nasıl geldiklerini anlamalarına ve diğerlerinin içeri girmesini engellemelerine yardımcı olur.

Bu mimari aşağıdaki bileşenlerden oluşur (bkz. Şekil 3-2):

» Yeni nesil güvenlik duvarları(NGFW'ler)ve diğer güvenlik ürünlerinden veri zenginleştirme ile izinsiz giriş olaylarına farkedilebilirlik sağlayan yeni nesil izinsiz giriş önleme sistemleri (NGIPS'ler)

» Daha fazla araştırma ve müdahale için yüksek aciliyeti olay verilerini toplama ve önceliğe dizme özelliğine sahip, sektör lideri kaynaklardan ve bulut tabanlı ürün verilerinden gelen tehdit istihbaratı

» Korumayı kuruluşun güvenlik duvarlarının ötesine taşımak için alan adı sistemi (DNS) katmanı güvenliği

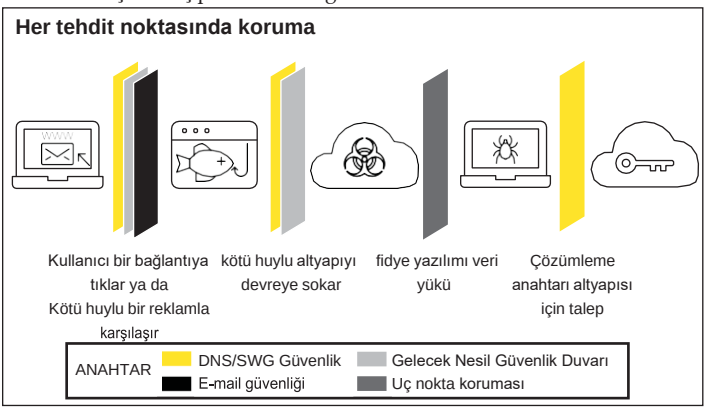
» Tüm bağlantı noktalarında ve protokollerde koruma sağlamak için güvenli web ağ geçidi

» Riskli, yetkisiz bulut uygulamalarına karşı koruma sağlamak için bulut erişim güvenlik aracısı (CASB)

» Konum, cihaz veya IP adresinden bağımsız olarak rol tabanlı politika uygulamasıyla son derece ayrıntılı, yazılım tanımlı ağ segmentasyonu
» Görünürlüğü genişletmek ve tehditleri ilişkilendirmek için e-posta, web ve uç nokta güvenliği

» Ağdan uç noktaya korumalı alan oluşturma özelliklerine sahip gelişmiş kötü amaçlı yazılım(malware) koruması

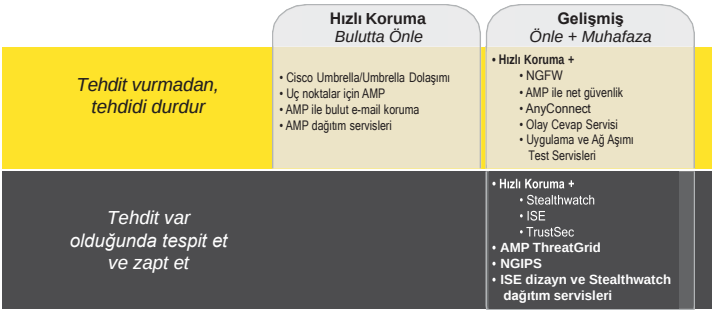
» Bileşenleri birbirine bağlamak ve güvenlik operasyonları ekibiniz için hayatı kolaylaştırmak için merkezi görünürlük ve yönetimin yanısıra otomatikleştirilmiş platform entegresi



FİGÜR 3-2: Yeni türünün en iyisi güvenlik mimarisi, derinlemesine savunma ile mümkün olan en iyi tehdit yüzey kapsamını sağlar.

İpucu

4. Bölümde, Cisco'nun Cisco Ransomware Defense ile türünün en iyisi bu yeni güvenlik mimarisine yaklaşımını öğreneceksiniz. Şekil 3-3, fidye yazılımı saldırılarını önleyen, tespit eden ve bunlara yanıt veren Cisco Güvenlik ürünlerini gösterir.



FİGÜR 3-3: Cisco Fidye Yazılımı Savunması çözüm paketleri mevcuttur.

NHL ÜNİVERSİTESİ ÖĞRENCİLERİNİ VE ÖĞRETMENLERİNİ SİBER TEHDİTLERDEN KORUR

Zorluk: Öğrencileri, öğretim üyelerini ve personeli fidye yazılımı saldırıları

NHL Üniversitesi, 12.000'den fazla öğrencisi ve 1.200'den fazla personeli ile Hollanda'nın en iyi üniversitelerinden biridir. Sınavlar başlamak üzereyken, Şubat 2016'da üniversite bir fidye yazılımı saldırısıyla tehdit edilmişti. İlk fidye yazılımı saldırısı onları savunmasız bıraktıktan sonra, ağlarında en kritik sistemlerini tehdit eden ek siber saldırılar başladı. Devam eden bu saldırılar, NHL yöneticilerini sınavlara devam edip edemeyeceklerini merak etmeye itti.

Ancak Dimension Data ve Cisco'nun yardımıyla NHL, krizlerini çözmeyi ve güvenlik yığınlarını iyileştirmeyi başardı. Kampüste nereye giderlerse gitsinler tüm cihazlar ve kullanıcılar için DNS düzeyinde güvenlik koruması sağlamak üzere Cisco Umbrella'yı kurdular. Daha sonra NHL, kötü amaçlı yazılım bulaşmalarına karşı ek koruma için ağlarındaki 1.900 desteklenen cihaza Gelişmiş Kötü Amaçlı Yazılım Koruması (AMP) ekledi. Yeni oluşan güvenlik mimarisiyle, sınavlar eski programa göre devam etti. Fakat bu sadece bir başlangıçtı.

Çözüm: Güvenilir danışmanların yardımıyla eksiksiz bir güvenlik çözümü sağlayın

Öğrenciler, öğretim üyeleri ve personel kampüste kendi cihazlarını kullanırken, NHL ağlarında hangi güvenlik sorunlarının meydana geldiğini ve bunlar hakkında ne yapmalarıgerektiğini anlamaları gerektiğini biliyordu.Yeni güvenlik çözümlerini uygulamaya başladıktan sonra, değer elde etme süresini hızlandırmak, personeli hızlı bir şekilde eğitmek, tüm işlevleri doğru şekilde kullanmak ve temel performans göstergelerini izlemek için sistemlerindeki araçları birbirine bağlamak için uzmanlardan yardım almaları gerektiğini fark ettiler. (KPI'lar). Bu yardımı almak için NHL, Cisco benimseme ekibiyle çalıştı. NHL ve Cisco, fırsatlara odaklanmak ve güvenlik açısından sorunlu noktaları çözmek için birlikte çalıştaylara ev sahipliği yaptı.

Cisco Umbrella'yı dağıttıktan sonraki görev, NHL ağındaki uç noktaları korumak için AMP teknolojisini başarıyla uygulamaktı. Güvenlik yığınına Cisco Umbrella ve AMP'yi eklediğinden beri, NHL başka fidye yazılımı sorunu yaşamadı. Bu ilk başarının ardından, Cisco benimseme ekibi ayrıca NHL'nin ağlarındaki etkinliği izlemek ve ölçmek için gösterge panoları geliştirmesine ve ayrıca tehditlerin daha önce engellendiğine dair güvence vermek için üst yönetime raporlar sunmasına yardımcı oldu. Son olarak, Cisco ekibi, NHL'nin gelecekte saldırıları önlemek için proaktif adımlar atması için süreçler ve iş akışları geliştirmesine yardımcı oldu.

Etkisi: Ağ görünürlüğü ve zekası kazanmak ve geleceğe hazırlanmak

Birlikte benimseme serüveni burada sonlanmadı. 2018'deNHL,yenibirçokkampüslü üniversite oluşturmak için Stenden Hogeschool ile birleşti: NHL Stenden Üniversitesi. Tüm dünyada on sitede 25.000 öğrenci ve 2.250 personel olmak üzere iki katı büyüklüğündeydi ve bu da birçok potansiyel yeni tehdit anlamına geliyordu.NHL, Cisco ile ortaklaşa olarak, tüm üniversite sistemi genelinde güvenlik mimarisini gözden geçirdi ve birleşme öncesinde güvenlik duruşunu iyileştirmek amacıyla yazılıma ve donanıma önemli yatırımlar yaptı.

Dünyada gerçekleşen artan sayıda fidye yazılımı saldırısı ile, büyük üniversitelerin yüksek profilli hedefler olarak seçilmesi sadece bir zaman meselesidir. Ancak şimdi, NHL Stenden Üniversitesi bu zorlukla yüzleşmeye hazır bir durumda.

BU BÖLÜMDE

- **» Fidye yazılımı savunmasını buluta taşıma**
- **» Uç noktalarda ve e-postada fidye yazılımı saldır vektörlerini kapatma**
- **» Yeni nesil güvenlik duvarları ve segmentasyon ile güvenlik politikalarının uygulanması**
- **» Cisco Güvenlik Danışmanlık Hizmetlerini Kullanma**

Bölüm 4
CiscoFidyeYazılım Savunması Dağıtımı

Cisco Fidye Yazılım Savunması, sanal özel ağ (VPN) dışındayken bile bütün ofis konumları ve kullanıcılar için fidye yazılımlarına karşı koruma sağlayan entegre bir yaklaşım ortaya koyar.

Cisco Talos'un benzersiz tehdit istihbaratıyla desteklenen Cisco'nun birleşik mimarisi, alan adı sistemi (DNS), web, e-posta, uç nokta ve ağ güvenliği dahil olmak üzere tamamlayıcı güvenlik ürünlerini bir araya getiriyor. Bu bölümde, Cisco Fidye Yazılımı Savunması çözümünü ve Cisco çözümlerinin ağdan e- postaya ve uç noktadan buluta fidye yazılımlarına karşı neden en etkili bir koruma sağladığını öğrenmiş olacaksınız.


İpucu

Bu listede çok sayıda araç var gibi görünebilir. İyi haber şu ki, her birinde oturum açmanız ve ayrı ayrı yönetmeniz gerekmiyor! Cisco Threat Response, birçok Cisco güvenlik ürünü arasındaki entegrasyonları otomatikleştirir ve istihbarat kaynaklarını entegre bir platformda toplamaktadır. Bu size daha fazla görünürlük ve bağlam sağlar, bu şekilde ortamınızdaki güvenlik etkinliklerini kolayca araştırabilir ve düzeltebilirsiniz.

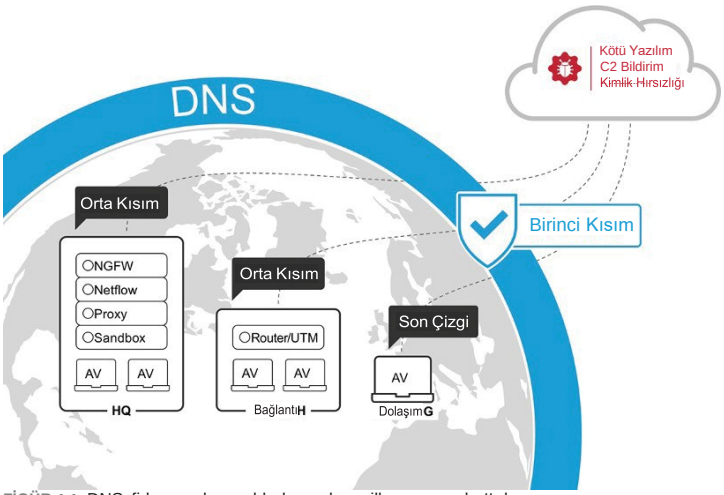
DNS'den Başlayarak Fidye Yazılımlarına Karşı Koruma

Bir fidye yazılımı saldırısının birçok aşaması vardır. Bir saldırı başlatmadan önce, saldırganın yürütme ve komuta ve kontrol (C2) aşamalarını desteklemek için İnternet altyapısını hazırlaması gerekir. Cisco Umbrella, fidye yazılımı sunan kötü amaçlı sitelere yönelik İnternet bağlantılarını engelleyerek fidye yazılımı saldırılarını (ve diğer siber saldırıları) daha erken durdurur. İnternet'in temelinde yerleşik olan Umbrella, DNS ve İnternet Protokolü (IP) katmanlarında güvenliği zorunlu kılar (bkz. Şekil 4-1).

Cisco Umbrella, uydu ofislerinde doğrudan İnternet erişimi kesintileri için fidye yazılımı saldırılarına karşı ek koruma katmanları sağlamak amacıyla Cisco SD- WAN ile de birleştirilebilir. Bu ek denetimler, tek bir bulut tabanlı platformdan sağlanan güvenli web ağ geçidi, bulut tarafından sağlanan güvenlik duvarı ve bulut erişim güvenlik aracısı (CASB) görevini içerir.

Teknik Şeyler

SD-WAN, Yazılım Tanımlı Geniş Alan Ağı anlamına gelir.



FİGÜR 4-1: DNS, fidye yazılımı saldırılarına karşı ilk savunma hattıdır.

Cihazların aksine bulut hizmeti, kurumsal ağdaki ve dışındaki uç noktaları korumaktadır.
Aracıların tersine, DNS katmanı koruması, ağa bağlı her cihaza kolayca yayılabilir.

İpucu

Tüm kullanıcılarınızı korumanın en hızlı yoludur ve 30 dakika gibi kısa bir sürede devreye geçirilebilir.

Daha fazla bilgi edinmek için https://learn-umbrella.cisco.com/ebook-library/ the-umbrella-advantage-what-makes-cisco-umbrella-unique adresinden Umbrella Advantage e-kitabını indiririz.

CISCO IT, FİDYEYAZILIMLARA VE DİĞER YEREL KÖTÜLERE KARŞI KORUMAK İÇİN UMBRELLA UYGULAMASI

Nisan 2016'dan itibaren Cisco, iki temel hedefle dahili BT'si için Umbrella'yı kabul etti:

- Kötü amaçlı yazılımlara, botnet'lere ve ihlallere karşı korumayı artırmak için: Küresel bir DNS sağlayıcı ağı olarak Umbrella, Dünyadaki internet isteklerinin yüzde 2'sini görüyor. Ortaya çıkan tehditleri, bu şekilde zarar verme şansları olmadan hızla öğreniyor ve engelliyor.

- Riskli kullanıcı davranışı hakkında bilgi edinmek için: Umbrella, bağlantı noktasıve protokolden bağımsız olarak internet'teki tüm etkinlikleri gösteren bir günlük oluşturur. Günlükler, Cisco'nun güvenlik ve BT ekiplerine daha fazla görünürlük ve denetim yetenekleri sağlar.

Umbrella'ya geçiş son derece basit bir şekilde oldu. Cisco Bilgi Güvenliği (InfoSec) mimarı Rich West, "Yeni donanım dağıtmaya, ağı yeniden yapılandırmaya, kapsamlı birlikte çalışabilirlik testleri gerçekleştirmeye veya diğer sistemlerimizi değiştirmeye gerek kalmadan güçlü yeni kontroller ekledik" diyor.

Cisco, Umbrella'yı planlamak ve uygulamak için BT ve InfoSec'ten sekiz kişilik bir ekip bir araya getirdi. Geçişin teknik yönleri çok kısa zaman aldı. Ekip üyeleri, zamanlarının çoğunu, geçişin avantajlarını açıklamak ve uygulama veya ağ performansı üzerindeki olası etkilerle ilgili soruları yanıtlamak için uygulama sahipleri ve ağ operasyon ekipleriyle toplantı yaparak geçirdi.

Dönüşüm, sorguları Umbrella'ya yönlendirmek için Cisco'nun dahili DNS sunucularındaki DNS yapılandırma dosyasına dört satır kod eklemek kadar basit birişlemdi.

(devam ediyor)

(devam ediyor)

Artık Cisco IT'nin DNS sunucuları, yukarı akış komşularına sormak yerine Umbrella'dan öz tekrarlamalı DNS sorguları talep ediyor. Dönüşüm o kadar mükemmeldi ki, dahili kullanıcılar bir değişikliğin gerçekleştiğinin bile arkında değillerdi.

Cisco Umbrella, İnternet erişimini güvence altına almak ve ağınızdan, şube ofislerinden ve dolaşımdaki kullanıcılardan bulut uygulaması kullanımını kontroletmek için birden fazla güvenlik hizmetini kullanıcılardan önce tek bir bulut platformunda entegre eder.

Umbrella, herhangi bir çevrimiçi hedefe bağlanır, İnternet için güvenli bir rampa görevi görür ve uyumluluğu desteklemek ve tehditleri engellemek için derinlemesine inceleme ve kontrol altına alır. Umbrella ayrıca olay müdahalesine ve tehdit araştırmasına yardımcı olmak için tehdit istihbaratına etkileşimli erişim yolu sağlar.

KÜRESEL BİR MEDİKAL ÜRETİCİSİ FİDYE YAZILIMINI NASIL ÇIKARIR

Zorluk: Sınırlı kaynaklarla sonsuz güvenlik sorunlarıyla mücadele etmek

1983 yılındaki kuruluşundan bu yana geçen on yıllarda, Octapharma istikrarlı bir şekilde dünyanın en büyük insan proteini üreticilerinden biri haline geldi. Bununla birlikte, üretim kapasitesini ikiye katlamak ve şu anda devam etmekte olan genel verimliliği artırmak için tasarlanmış kurumsal bir girişimle, şirket benzeri görülmemiş bir genişleme yaşıyor.

Bu büyüme hamlesinin etkisi tüm dünyada belirgin hale geldi.

Görevler — iş organizasyonları. Octapharma Global Kıdemli Ağ Mühendisi Jason Hancock, "Daha fazla mobil ve bulut hizmeti aracılığıyla daha fazla sayıda daha çok çalışan eklendikçe, yeni ağ güvenlik açıkları da ekliyoruz" diyor. "Fidye yazılımları da dahil olmak, kötü amaçlı olaylarda bir görünür olacak."

Halihazırda yetersiz tedarikte olan türde eğitimli güvenlik pratisyenlerini işe alarak herhangi bir riskin üstesinden gelmeye çalışmak yerine, bu güvenlik açıklarını ele almak için yeni çözümler belirlemek ve organizasyon verimliliğihedefleriyleuyum sağlamak bir öncelik halinegeldi" diyede ekliyor.

Hancock, "Bu odaklanmaya uygun olarak" diyor, "önce ağın her 15 dakikada bir çökmesini önlememiz ve hem ekibimiz hem de kullanıcılarımız için verimliliği artırmamız gerekiyordu. 2014'te şirkete katıldığımda, ilk hedefim işleri istikrara kavuşturmaktı, böylece odaklanabildim. Karşılaştığımız CryptoLocker ihlali gibi giderek daha agresif hale gelen kötü amaçlı yazılımları önlüyoruz."

Çözüm: Uygun işlevsellik

"BenOctapharma'yagelmedenönceekip,birsüredirşirketiçiwebgüvenlik cihazlarından bir önceki tarafından seçilen aynı satıcının bulut hizmetine geçiş yapmak için çalışıyordu. Başlangıçta bu dağıtımı tamamlamakla görevlendirildim," diye hatırlıyor Hancock. "Neyle çalışmam istendiğini görür görmez, ihtiyaçlarımızı karşılamayacağını biliyordum."

"İnternet işlevselliğinden başlayarak, ürünün çevremizde uygulanabilirliği konusunda endişelere neden olan önemli sorunlarla karşılaştık." Hancock, "Ekibimiz, İnternet hizmetinden memnun olmayan kullanıcılardan, hem bulut hizmetine hem de kullanıcıların makinelerindeki uç nokta istemcisine atfedilen çok sayıda geri bildirim aldı."

"Bunun dışında," diye devam ediyor, "özellik seti ihtiyaçlarımızla tutarsızdı ve ekip genelinde yönetimkonusundayaygınolansıkıntılarvardı.Bu,politikalarınve çeşitli bileşenlerin çok ayrıntılı, sezgisel olmayan yönetimini desteklemek için çok fazla eğitim sağlamamız gerektiği anlamına geliyordu."

"Sorun yüklü bir Kuzey Amerika konuşlandırmasından sonra ağımız düzenli olarak kapalıydı. Bir seferde saatlerce İnternet'e sahip olmamanın güvenilmezliği ekibimize olumsuz yansıdı ve ürünün destek kanalları aracılığıyla çözülemedi," diye açıklıyor Hancock. "Son olarak, [satıcı], istenmeyen ve bazı durumlarda mümkün olmayan 50'den fazla küresel konumdan akışın yeniden yönlendirilmesini gerektiren sanal cihazların iyiliği için buluta geçişimizi bırakmamızı tavsiye etti."

"Şte o zaman elimi kaldırdım ve 'Bu sorunu çözmenin tek yolu Cisco Umbrella'dır ve onu altı hafta içinde devreye alıp küresel ağımızı koruyabilirim' dedim. Şe yaramayan bir çözüme bu kadar yatırım yaptıktan sonra bizim için önceki deneyimlerinden daha başarılı olacağını bildiğim bir çözüme hazır bulunuyorduk: Umbrella."

(devam ediyor)

(devam ediyor)

Sonuçlar: Fidye yazılımlarında ciddi azalma

Kolay bir dağıtımdan sonra, Octapharma anında sonuç aldı. Hancock, "Umbrella'yı yerleştirdiğimizden beri web güvenliğimizden taviz vermedik" diye belirtiyor.

“Fidye yazılımına maruz kalmamızı geniş çapta azalttık ve Umbrella'yı dağıttığımızdan beri kötü niyetli bir bağlantıya tıklamanın sonucu olarak fidye yazılımının kurbanı olmadık. Güvenlik politikası nedeniyle aslında haftada on binlerce bloğa tanık oluyoruz ; bu, kategori politikalarına dayalı blokları saymaz” diye ekliyor. "Fidye yazılımlarının web saldırı vektöründe büyük bir riski ele aldık ve internet bağlantısıyla ilgili kullanıcı deneyimimizi büyük ölçüde geliştirdik."

"Birkaç kimlik avı e-postası bile belirledik ve bunları test ettik. bağlantılarına tıklamaya çalıştık ; Umbrella sayesinde sitelere erişim sağlanamadı.”

Tahmin edilmeyen başka bir fayda mı? Ağ mühendisi, "Umbrella panosundan çıkan mükemmel verileri dahili sistemlerimizle ilişkili hale getirerek, daha önce tespit edilmemiş virüslü makineler bulduk" diye belirtiyor.

GüvenlikyığınıartıkDNSkatmanındakitehditleriengelleyebilenşirket,ağı proaktif güvenlik yönetimiyle güçlendirmeye devam etmenin yollarını aramaya devam etmekte. "Umbrella, kategori politikalarına göre siteleri engelleme konusunda çok yetenekli olsa da, en etkili bir güvenlik aracı olarak ve bununla birlikte dağıtımımızda bir odak noktası olarak derinlemesine savunma stratejimizin kritik bileşenidir. Ağ mühendisi, şu anda bu stratejiyi desteklemeye devam etmek için Cisco'nun güvenlik portföyünün bir parçası olan ek araçlarını araştırmaktayım" dedi.
"Güvenlik duvarı geliştirmelerini, kötü amaçlı yazılımlara karşı korumayı düşünüyorum. Uç noktalar ve ürünlerimiz arasında daha fazla koordinasyon güvenlik araç takımı olarak.”Jason Hancock için görmek her zaman inanmaktı. "Umbrella'yı yıllardır evimde kullanıyorum" diyor."Artık bunun iki farklı kuruluşta da başarılı olduğuna tanık olduğuma göre, meslektaşlarım bana Cisco'nun benzersiz ve son derece etkili güvenlik yaklaşımı hakkında yeterince şey söyleyemediklerini dile getiriyorlar."

Uç Noktaların Güvenliğini Sağlama ve E-posta Tehditlerini Ele Alma

Günümüzdeki kötü amaçlı yazılım tehditleri her zamankinden daha karmaşık. Fidye yazılımı da dahil olmak üzere gelişmiş kötü amaçlı yazılımlar hızla gelişmektedir ve aşağıdakiler de dahil olmak üzere çeşitli yöntemler kullanarak bir sistemi tehlikeye soktuktan sonra tespit edilmekten kurtulabilir:

- Uyku teknikleri
- Polimorfizm ve metamorfizma
- Şifreleme ve gizleme
- Bilinmeyen protokollerin kullanımı

Bununla birlikte, gelişmiş kötü amaçlı yazılım, kalıcı olan bir saldırganın güvenliği ihlal edilmiş olan bir kurumun ağı boyunca yanlamasına hareket etmesi için bir başlatma yükselişi sağlar.

E-posta ile kimlik avı kampanyaları, siber suçlular için favori ve ilginç derecede etkili kötü amaçlı yazılım saldırı vektörüdür. Yaygın fidye yazılımı çeşitleri, kurbanlarınabulaşmak için kimlik avı yöntemlerini temel alır .

Cisco Ransomware Defense çözümleri, uç noktaların güvenliğini sağlar ve e-posta tehditlerini önler ve Uç Noktalar için Cisco Gelişmiş Kötü Amaçlı Yazılım Koruması (AMP) ve AMP ile Cisco Bulut E-posta Güvenliği içerir.

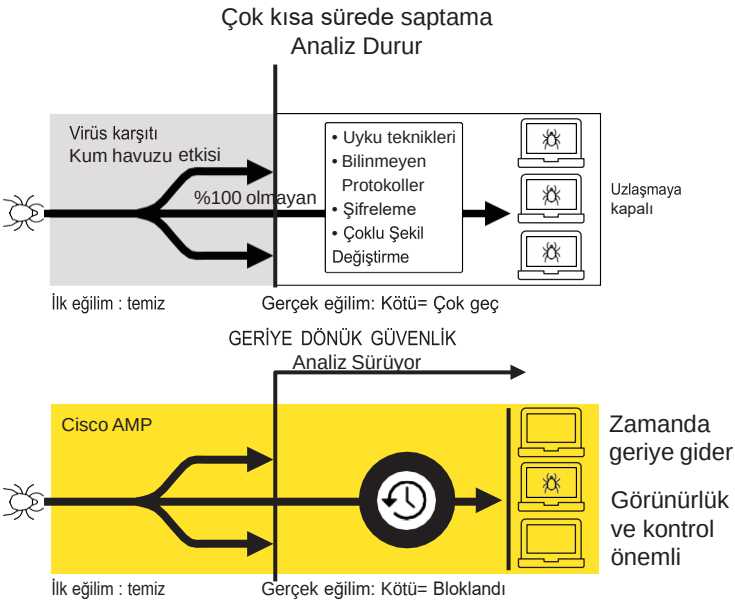
Cisco Gelişmiş Kötü Amaçlı Yazılım Koruması uç noktalar için

Sadece belirli bir noktada algılama tekniklerini tek başına kullanan tipik bir kötü amaçlı yazılımdan korunma yazılımı hiçbir zaman yüzde 100 etkili olmayacaktır. Fakat, bütün ortamı tehlikeye atmak için fark edilmeden kaçan tek bir tehdit yeterlidir. Hedeflenen içeriğe duyarlı kötü amaçlı yazılım kullanan sofistike saldırganlar, belirli bir noktadaki savunmaları alt etmek için kaynaklara, uzmanlığa ve kalıcılığa sahiptir. Anlık tespit aynı zamanda bir ihlalin gerçekleştikten sonra kapsamına ve derinliğine karşı tamamen kördür, bu da kuruluşların bir virüs yayılmasını durdurma konusunda veya benzer bir saldırının tekrar olmasını engelleme konusunda yetersiz kalmasına yol açar.

İpucu

Hiçbir kötü amaçlı yazılımdan korunmamanın sebebi, bir uç noktaya virüs bulaştığında fidye yazılımını kaldıramaması ya da dosyaların şifresini çözememesidir, ancak Cisco kuruluşların proaktif olarak fidye yazılımlarını tespit etmesine ve ağa ulaşmadan önce onu engellemesine yardımcı olur.

Bu kötü amaçlı yazılım(malware) anlayışına dayanarak, Cisco, kötü niyetli davranışın ilk ortaya çıkışında gelişmiş kötü amaçlı yazılım tehditlerini belirlemek ve geriye dönük olarak engellemek için dosyaları ve trafiği sürekli olarak analiz etmek için noksansız bir algılama yeteneği ve büyük veri analitiği çerçevesi ortaya çıkarmak üzereUç Noktalar için AMP'yi oluşturdu. Gelişmiş makine öğrenimi teknikleri, her dosyaylailişkili 400'den fazla özelliği değerlendirmektedir. Gelişmiş arama, güvenlik araştırmalarını önemli ölçüde hızlandırarak uç nokta hakkında her şeyi bilmenizi sağlar. Geriye dönük güvenlik — bir virüs bulaşmasının bütün kapsamını anlamak, temel nedenleri belirlemek ve uç nokta izolasyonu ile diğer engelleme ve düzeltme tekniklerini gerçekleştirmek için zamanda geriye bakma ve süreçleri, dosya etkinliklerini ve iletişimleri izleyebilme yeteneği — ilk düzenlemeden sonra kötü amaçlı hale gelmiş olan dosyaları algılar ve sizi bu konuda uyarır. Bu sürekli analiz ve geriye dönük güvenlik kombinasyonu, tipik belirli bir noktada algılamanın ötesine geçen gelişmiş kötü amaçlıyazılım koruması sağlar (bkz. Şekil 4-2).



FİGÜR4-2: Süreklianalizvegeriyedönükgüvenlikilekarşılaştırıldığındabelirlibir noktada algılama.

Gelişmiş ile Cisco E-posta Güvenliği Malware koruması

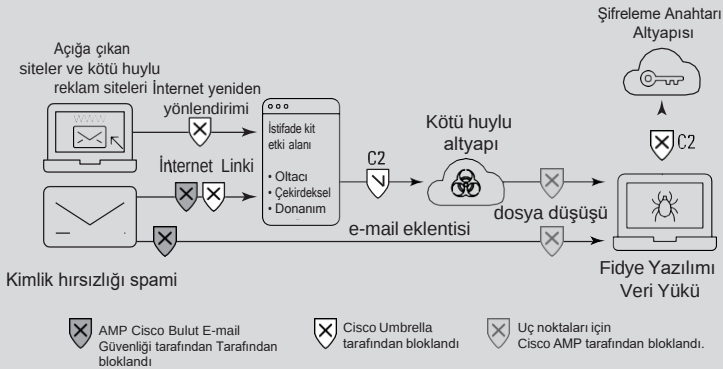
E-posta kritik bir iş iletişim aracıdır, ancak kurumları çok çeşitli karmaşık tehditlere maruz bırakabilir. AMP'li Cisco Email Security, fidye yazılımı dolayısıyla ile önemli saldırı vektörleri halinde olan spam, kimlik avı e- postaları, kötü amaçlı ekleri ve URL'leri engellemektedir. AMP teknolojisi, uç noktaya uygulananla aynıdır, ancak e-posta ağ geçişinde dağıtılır.

AMP'li Cisco E-posta Güvenliği, aşağıdakileri içeren katmanlı korumayla çalışmalar açısından önem arz eden e-postaları koruma altına alır:

- Küresel tehdit istihbaratı
- Spam bloklaması
- Graymail algılaması ve abonelikten çıkma
- Gelişmişzararlıyazılım(malware) koruması

CISCO KENDİ ŞAMPANYASINI İÇER

Cisco BT, tehdit odaklı e-postagüvenlik stratejisiiçinAMP ile CiscoE-posta Güvenliğine güvenir. Aşağıdaki şema, Cisco Umbrella, Uç Noktalar için Cisco AMPve AMP ile CiscoEmail Security fidyeyazılımısaldırılarını başka şekillerde durdurmak için birlikte nasıl çalıştığını gösterir.



» Virüs filtreleri

» Web etkileşim takibi

» Gönderilen mesaj kontrolü

» Sahte e-posta algılaması

» Veri kaybını önleme

Yeni Nesil Güvenlik Duvarları ve Segmentasyon ile Ağı Koruma

Cisco Firepower tehdit odaklı yeni nesil güvenlik duvarları (NGFW'ler), eski bağlantı noktası tabanlı güvenlik duvarlarında mümkün olmayan benzersiz bir görünürlükle saldırı öncesinde, sırasında ve sonrasında tüm saldırı süreci boyunca entegre bir tehdit savunması sunar. Cisco TrustSec teknolojisi, dinamik yazılım tanımlı ağ segmentasyonu ortaya koyar. Kullanıcının konumu veya cihazından bağımsız olarak ayrı ağ kesimlerinde uygulanacak ayrıntılı bir rol tabanlı güvenlik ilkeleri için var olan ağı kullanır. Sonuç, kötü amaçlı yazılımın bir kuruluşun ağı içinde yanal olarak hareket etmesini önlemeye yardımcı olan daha basit bir bölünmedir; bu, bir aykırılık gerçekleştiğinde kötü amaçlı yazılım hasarına sınır konulabilir.

Cisco Firepower Yeni Nesil güvenlik duvarı

AMP ve Threat Grid korumalı alan teknolojisine sahip Cisco Firepower NGFW, bilinmeyen kötü amaçlı yazılım ve tehditler için dinamik bir analiz sağlarken ortadaki tehditlere ve C2 geri aramalarına engel teşkil eder. Cisco Firepower bunları sağlar:

» **Kesinuygulamagörünürlüğü ve kontrolü(AVC):** 4.000'denfazla ticari uygulamayakullanıcıerişiminitanımlayınve kontroledin, ayrıca özel uygulamalar için destek vardır.

» **Cisco Yeni Nesil IPS:** Sonderece etkili bir tehdit etkileme yöntemidir ve kullanıcıların, altyapı, uygulamalar ve içerik hakkında tam bağlamsal farkındalık, çok vektörlü tehditleri saptamanıza ve savunma yanıtını otomatikleştirmesine yardımeder.

» **İtibar ve kategori tabanlı URL filtreleme:** Bu filtreleme, şüpheli web trafiği üzerinde kapsamlı uyarı ve kontrol sağlar. 80'den fazla kategoride yüz milyonlarca URL'de işleyişler uygular.

» **Gelişmiş kötü amaçlı yazılım koruması:** toplam sahip olma maliyeti düşükolmaklabirlikte(TCO)etkiliihlaltespiti, korumadeğerisunar.Basit bir yazılımlisansıylaetkinleştirilendiğergüvenlikkatmanlarıtarafından kaçırılan kötü amaçlı yazılımları ve ortaya çıkan tehditleri keşfedin, anlayın ve durdurun.

Ağı sensör ve uygulayıcı olarak kullanın

Cisco, genel saldırı yüzeyini azaltmak, tehditlerin ağ üzerinde yanal hareketini önleyerek saldırıları kontrol altına almak ve tespit edildiğinde tehditleri izole etmek için gereken süreyi en aza indirmek için tasarlanmış yazılım tanımlı segmentasyon ile güvenlik politikasını dinamik olarak uygulamak için ağ kullanır.

Cisco çözümleri, ağın kendisinin bir sensör ve bir uygulayıcı olarak hareket etmesini sağlar. TrustSec ve Stealth-watch ile Identity Services Engine (ISE), güvenli ağ erişiminin sağlanmasını ve yönetimini kolay hale getirir, anormal ağ etkinliğine daha çokgörünürlük sağlar, güvenlik işlemlerini ivmelendirir ve ağdaki herhangi bir yerde tutarlı bir işleyiş uygular. Ağ topolojisine dayalı erişim kontrol mekanizmalarından farklı bir şekilde , Cisco TrustSec kontrolleri mantıksal ilke gruplamaları kullanma yoluyla tanımlanır, bu nedenle kaynaklar mobil ve sanallaştırılmış ağlarda hareket ederken bile kaynak segmentasyonu ve güvenli erişim tutarlı bir şekilde korunur. Tüm bunlar ne anlama geliyor?

TrustSec ilkesinin uygulanması, bir fidye yazılımı saldırısının ağınızın tamamına yayılmasını önlemesi mümkündür.


Hatırla

Cisco TrustSec işlevi, kurumsal ve veri merkezi ağlarındaki varlıkları ve uygulamaları koruma altına almak için Cisco anahtarlama, yönlendirme, kablosuz LAN (WLAN) ve güvenlik duvarı ürünlerine konulmuştur.

Geleneksel erişim kontrol yöntemleri, sanal LAN'ları (VLAN'lar) ve erişim kontrol listelerini (ACL'ler) kullanarak varlıkları bölümlere ayırır ve korur. Bunun yerine Cisco TrustSec, düz dil matrisinde on yazılı olan ve IP adreslerinden ve VLAN'lardan ayrılmış güvenlik grubu ilkelerini kullanır. Aynı rol sınıflandırmasına sahip kullanıcılar ve varlıklar bir güvenlik grubuna atanır.

Cisco TrustSec ilkeleri, merkezi olarak oluşturulur ve kablolu, kablosuz ve VPN ağlarına otomatik olarak iletilir, bu şekilde kullanıcılar ve varlıklar sanal ve mobil ağlarda hareket ederken tutarlı erişim ve koruma elde etmiş olur. Yazılım tanımlı segmentasyon, ağ mühendisliği görevleri ve uyumluluk doğrulaması için harcanmış olan süreyi kısaltmaya yardımcı olur.

Dağıtımları Kolaylaştırma ve Olay Müdahalesini Destekleme

Cisco Güvenlik Danışmanlık Hizmetleri, Firepower ve AMP dahil olmak üzere Cisco Fidye Yazılımı Savunmaçözümlerinin yanısıraolay müdahalesiiçin dağıtım servislerini kapsar.

Cisco Güvenlik Hizmetleri Olaya Müdahale Ekibi şunları sağlama imkanına sahiptir:

» Kurumunuzun olay müdahale yeteneklerini geliştirmesine ve/veya değerlendirmesine yardımcı olacak proaktif olay müdahale hazırlık servisleri

» Bir fidye yazılımı saldırısı veya diğer güvenlik olayları durumunda reaktif olay cevabı

Ayrıca, Cisco Güvenlik Entegrasyon Hizmetleri, çözüm düzeyindeki mimari zorlukları konu alır. Uç Noktalar için Cisco AMP ve Firepower NGFW'ler gibi çözüm teknolojilerinin dağıtımını kolay hale getirir.


Hatırla

Bu bileşenler, Cisco Fidye Yazılımı Savunması yaklaşımının temelini yaratır. Ancak, Cisco'nun sunduğu daha fazla çözümle kurumunuzun bütün bölümlerinde güvenlik duruşunuzu iyileştirebilirsiniz. Tüm Cisco güvenlik portföyünü www.cisco.com/c/en/us/products/security.

CISCO İLE PERFORMANS

Zorluk: Derinlemesine savunma koruması geliştirmek

Lojistik gayrimenkul alanında dünya lideri olan Prologis, Inc., iki ana kategoride yaklaşık 5.200 müşteriden oluşan çeşitli bir tabana modern dağıtım tesisleri kiralamaktadır: işletmeler arası ve perakende/çevrimiçi sipariş karşılaması olarak. Dört kıtada 20 ülkede 60'tan fazla ofisi bulunmaktadır.

Prologis Güvenlik Çözümleri Mimarı Tyler Warren, "Küresel olmak, her yerde çalışmak anlamına gelir ve bunu başarıyla yapabilmek, bulut bilişime büyük ölçüde güvenmek anlamına gelir" diyor. "Prologis'in BT altyapısının çoğunluğu bulutta olduğundan, güvenlik çözümlerini tanımlamayı zorlaştırabilecek tipik bir altyapımız ya da çevremiz yok."

Topluma açık, bulut merkezli, küresel bir kurum olarak Prologis'in sistemlerini tehlikeye atılmaktan koruması gerekiyor ve güvenlik yığınını oluşturarak bunun olmamasını sağlamak Warren'ın görevi.

"Tehdit etkinliğinin arttığını gördükçe, Prologis'in ağı korumak ve ağdaki ve ağ dışındaki kullanıcıları komuta ve kontrol geri aramaları, kötü amaçlı yazılım ve kimlik avı gibi kötü amaçlı etkinliklere karşı korumak için mevcut güvenlik önlemlerini güçlendirmesi gerektiği ortaya çıktı" diye devam ediyor. "Katmanlı bir güvenlik modeli bizim için mantık çerçevesindeydi çünkü tek bir güvenlik öğesi her şeyi yakalayacak kadar güçlü değildi. "

Çözüm: Yığına ve personele uyan güçlendirilmiş güvenlik

"Güvenlik yığınımızı oluşturmak biraz deneme yanılma süreci gerektirdi. Tüm öğelerin uyumlu olmasını ve kullanıcıları etkilemeden sorunsuz bir şekilde birleşik hale getirilebilmesini istedik. Ve," diye belirtiyor Warren, "bizi çalıştığımız yerde korunmak zorundaydılar: dünyanın her yerinde ve bulutta."

Prologis'in çok özel rahatsız edici içerik türlerinden oluşan kısa engelleme listesi, başlangıçta başka bir satıcı tarafından ele alınan web filtrelemesini gerektirmekteydi. Warren'a göre, "Yönetmeyi zor bulduk. Daha da önemlisi, her şeyi buluta taşıma konusu kurumsal hedefimize uymuyordu."

"Çalışanların internet kullanımından kaynaklanan belirli güvenlik sorunlarıyla mücadele etmemize destek olabilecek bir güvenlik katmanına ihtiyacımız vardı ve ayrıca web filtrelememizi güçlendirmemiz gerekiyordu" diye anlatıyor. "Umbrella'nın kötü amaçlı faaliyetleri engelleyen ilk katman olduğu gerçeğini takdir ettik."

(devam ediyor)

(devam ediyor)

IBu ihtiyaçları karşılamanın en iyi yolunu arayan Prologis, diğer üç satıcı ve Cisco ile kavram kanıtlama denemeleri yaptı. Prologis, donanım gereksinimleri, karmaşıklık, yoğun zaman alan kurulum ve fiyat gibi çeşitli faktörlere dayalı olarak diğerlerini ortadan kaldırdıktan sonra Cisco Umbrella'yı seçti.

Warren, "Umbrella tüm ihtiyaçlarımızı karşılıyor" diyor. "Özel güvenlik endişelerimizi ele alıyor, web filtrelemeyi hallediyor ve uzaktaki kullanıcılarımızı kapsıyor; bunların tümü tek bir bulut tabanlı, kolay dağıtılan çözümde."

Sonuçlar: Dramatik performans kazanımları ile politika uygulama

Warren, "Sonuçları görmek için uzun süre beklemek zorunda kalmadık" diye söylüyor. "Politikaları ağ dışı cihazlar da dahil olmak üzere her yerde tutarlı bir şekilde uygulama kapasitesi, Prologis için son derece önemlidir" diye ekliyor. "Umbrella roaming istemci uygulaması o kadar kusursuzdu ki hiç kimse meşgul olduğunun farkında olmuyor"

Warren, bir başka olumlu sonuç olarak performansta önemli bir artışa işaret ediyor. "Umbrella'yı kurduktan sonra performansta büyük bir gelişme gördük. Prologis'in kullandığı uygulamalarınçoğu bulutta olduğundan performans bizim için son derece önemlidir. Kullandığımız uygulamaların yüzde yüzü, performans artışı yaşadı."

Diğer Umbrella özelliklerinin de yararı olduğu kanıtlanmıştır. "Otomatik raporlama değerli - özellikle Bulut Hizmetleri Raporu - çünkü ağın ne kadar iyi korunduğuna ve bulutta BT'nin ne kadar karanlıkta olduğuna dair net, anlaşılabilir verileri paylaşabiliyorum ve bu gerçekten ufuk açıcı." diyor Warren notlarında.
"Raporlama, herhangi bir sorunu belirlememi kolay hale getiriyor ve derinlemesine savunma güvenlikaltyapımızaduyulan ihtiyacınaltını çizerek birçok insanın hayatını iyileştiriyor."
"Güvenlik yığınımıza Umbrella eklemek harika bir karar oldu. Dağıtımın bir sonucu olarak deneyimlediğimiz gelişmiş güvenlik ve performanstan dolayı herkes kendinden geçmiş bir vaziyette."

BU BÖLÜMDE

- **Fidye yazılım sisteminin zorluklarını anlamak**
- **Kökten güvenlikli bir çevre inşa etme ve yerleştirmek**
- **İşi basit tutmak**
- **Hızla gelişen tehditlerin bir adım önünde olmak için görevleri otomatikleştirme**

Bölüm 5
On Temel Fidye YazılımıSavunması Tavsiyesi

Bu bölümde, fidye yazılımı savunmasıyla ilgili hatırlamaya değer bazı önemli noktaları ele alacağım!

Fidye Yazılımları Gelişiyor

Fidye yazılımı hızla ilerleyen bir tehdittir. Cybersecurity Ventures tarafından yapılan son araştırmalar, 2021 yılına kadar yeni bir organizasyonun her 11 saniyede bir fidye yazılımı saldırısına maruz kalacağını ve sürekli olarak yeni varyantların geliştirildiğini tahmin etmekte! Bu, kurumunuzun verilerini fidye yazılımlarına karşı savunmayı her zamankinden daha kritik bir hale getirir.

Fidye yazılımı saldırıları daha büyük ekonomik etkilere neden olmaya devam ettikçe, saldırı kalıpları "nicelikten çok kalite" olarak değişmekte. Bu, Ryuk gibi fidye yazılımı çeşitlerini kullanan, daha yüksek ödeme kabiliyetine sahip orta ve büyük kuruluşlarda daha yüksek hedefli saldırılar nedeniyle mümkün oluyor.

Fidye yazılımlarının hızlı büyümesine ve gelişimine, dijital dönüşüm girişimleri (potansiyel giriş noktalarının sayısını ve saldırıların yayılma kabiliyetini büyük ölçüde artıran), Bitcoin'in yükselişi (kolay ve neredeyse izlenemez ödemeleri mümkün kılan) dahil olmakla birlikte çeşitli başka faktörler katkıda bulunmuştur. - siber suçlular ve neredeyse herkesin fidye yazılımını kullanmasını kolaylaştıran Hizmet Olarak Fidye Yazılımının (RaaS; sonraki bölümebakın) ortaya çıkışı.

Hizmet Olarak Fidye Yazılımı Ortaya Çıkan Bir Tehdittir

RaaS, neredeyse sınırlı teknik becerilere sahip herkesin siber suçlu olmasını kelimenin tam anlamıyla "bir, iki, üç" kadar kolaylaştıran yeni bir tehdit olarak belirdi. Örneğin, ilk olarak Mayıs 2015'te keşfedilen, bilinen en eski RaaS tekliflerinden biri olan Tox, bir Tor tarayıcı kullanılarak darkweb'den indirilebilir ve ardından aşağıdaki gibikurulabilir:

1. Bir fidye tutarı girin.
2. Bir fidye notu oluşturun.
3. Bir CAPTCHA yazın, böylece Tox'un yaratıcıları sizin bir bot olmadığınızı bilsin.

RaaS yazılımı genellikle ücretsiz veya küçük bir ücret karşılığında indirilebilir. RaaS yazılımının yaratıcıları için gerçek kâr, genellikle yüzde 5'ten yüzde 30'a kadar olan fidye ödemelerinden aldıkları kesinti miktarlarıdır.

Fidye Ödemek Güvenlik Sorunlarınızı Çözmez

Fidye yazılımı kurbanlarının çoğuna göre sorunla baş etmenin en hızlı ve en kolay yolu fidyeyi ödemektir. Ancak fidyeyi ödemeniz (her ne kadar dosyalarınıza erişebilseniz de) sorunlarınızı mutlaka çözmez.

Birçok durumda, fidyeyi öderseniz dosyalarınızın şifresi çözülür, ancak bunun bir garantisi yoktur. Fidyeyi öderseniz dosyalarınızı geri yüklemek siber suçluların yararına olsa da (bir fidye yazılımı kampanyası, fidye ödendiğinde dosyaların şifresini çözmediği için bir itibar kazanırsa, gelecekteki kurbanların fidyeyi ödemesi için bir neden yoktur) , hırsızlar arasında onur yoktur. Bu özellikle RaaS'ın ortaya çıkmasıyla doğrudur çünkü "acemi" bir siber suçlu büyük resmi göremeyebilir. Buna ek olarak şifreleme anahtarı herhangi bir nedenle çalışmıyorsa, müşteri hizmetlerini arayamazsınız!

Ayrıca, failin kuruluşunuza karşı gelecekteki siber saldırıları kolaylaştırmak için başka kötü amaçlı yazılım yüklemediğini veya kitleri kullanmadığının da garantisi yoktur. Dosyalarınızın bir kopyası, kuruluşunuzun hassas bilgilerini dark web'de satmak gibi başka amaçlarla da sızdırılmış olma olasılığı vardır.

Fidye ödemek, gelecekteki siber suçları doğrudan finanse eder ve sürdürür. Rehineler karşılığında teröristlere veya haydut ulus devletlere fidye ödemekle tamamen aynı şeydir. Gelecekte benzer eylemleri cesaretlendirir, destekler ve finanse eder.

Son olarak, fidye ödemek, kuruluşunuzda ciddi bir güvenlik ihlali olduğu gerçeğini ortadan yok etmez. İhlalin niteliğine, kapsamına ve koşullarına ve kuruluşunuzun tabi olduğu sektör yönetmeliklerine ve yasal yargı yetkilerine bağlı olarak, ihlali kamuya açıklamanız ve ciddi para cezaları ve cezalar ödemeniz gerekebilir - bu bir tür tokat gibi zaten fidyeyi ödedikten sonra!


İpucu

Bir fidye yazılımı saldırısından kaynaklanabilecek olası hasarı azaltmak için, kuruluşlar her zaman tüm önemli dosyaların ve tüm kritik sistemlerin mevcut görüntülerinin periyodik, iyi bilinen yedeklerini tuttuklarından emin olmalıdır.

Açık Standartlara Dayalı Katmanlı Bir Güvenlik Mimarisi Oluşturun

Açık ve genişletilebilir standartlar, yeni ve mevcut güvenlik teknolojilerinin kapsamlı bir güvenlik çözümüne kolayca entegre edilmesini sağlayan türünün en iyisi yeni bir mimariye olanak sağlar.

Entegre, Türünün En İyisi Çözümleri Dağıtın

Derinlemesine savunma, köklü bir güvenlik endüstrisinin en iyi uygulamasıdır. Maalesef ki, şimdiye kadar derinlemesine savunma, kuruluşların ortamdaki diğer güvenlik çözümleriyle kolayca entegre olmayan bağımsız (veya nokta) güvenlik ürünlerinidağıtmasını zorunlu kıldı.

Türünün en iyisi yeni mimarileri ile kuruluşlar, güvenlik ortamlarındaki karmaşıklığı azaltan ve genel güvenlik duruşlarını iyileştiren entegre portföy tabanlı çözümler dağıtma imkanına sahip.

Güvenliği Ağ Ortamınıza Yerleştirin

Güvenlik, ağ genelinde, veri merkezi genelinde, uç noktalarda ve mobil cihazlarda ve bulut da dahil olmak üzere kuruluşun tüm bilgi işlem ortamı boyunca normal ve yaygın şekilde olmalıdır.

Güvenlik Ortamınızda Karmaşıklığı Azaltın

Güvenlik teknolojilerinin dağıtımı ve kullanımı basit olmalıdır. Karmaşıklık, yanlış yapılandırma ve hata olasılığı nedeniyle risk doğurur ve potansiyel olarak ciddi tehlike göstergelerini (IoC) ve başka veri noktalarını ağır ve ayrıntılı günlüklere gömebilir. Entegre bir güvenlik planını bir araya getirmek ve gereksiz karmaşıklığı ortadan kaldırmak nedeniyle kuruluşunuzun ortamına ve tehdidine dair kendi derinlemesine bilginizi ve anlayışınızı tamamlamak adına üçüncü taraf güvenlik hizmetlerine dayanmaktan ve onların geniş deneyimlerinden yararlanmaktan çekinmeyiniz.

Bulut Tabanlı, Gerçek Zamanlı Tehdit İstihbaratından Yararlanın

Fidye yazılımları ve diğer siber güvenlik tehditleri hızla ilerliyor. Sıfır günü saldırıları, çoğu kuruluş için en büyük tehdidi temsil eder. Bulut tabanlı, gerçek zamanlı tehdit istihbaratı, BT ekiplerinin yeni tehditler ortaya çıktığında mümkün olan en kısa zamanda en güncel karşı önlemleri dağıtmasına ve kuruluşlarının çok ötesine geçen güvenlik uzmanlığından yararlanmasına olanak tanır.

Cevap Süresini Azaltmak için Güvenlik İşlemlerini Otomatikleştirin

Mümkün olan her alanda, güvenlik eylemleri, dakikalar veya saniyeler içinde tüm kurumsal ağa yayılabilen tehditlere ayak uydurabilmek için otomatikleştirilmelidir.

İşte otomatikleştirilebilecek bazı güvenlik eylemleri örnekleri:

» Kötü amaçlı yazılımdan koruma ve izinsiz giriş önleme sistemi(IPS)imza dosyalarının dağıtımı ve kurulumu

» Güvenlik günlüklerinin ve tehdit verilerinin merkezi anlamda bir araya getirilmesi.

» Kötü hedeflere yönelik istekleri daha bağlantı kurulmadan engelleyen ve tehditleri ağınıza ve uç noktalarınıza gelmeden önce herhangi bir bağlantı noktasında durduran tehdit koruması

» Dinamik erişim kontrol listeleri(ACL'ler),etki alanı ve web sitesi beyaz listeye/kara listeye alma ve güvenlik duvarı kuralı oluşturabilme

» Hesap sağlama/yetkiyi kaldırma ve erişim hakları yönetimi

Bir Şey Gördüğünde, Bir Şey Söyle

ABD Federal Soruşturma Bürosu (FBI), fidye yazılımı kurbanlarını virüs ayrıntılarını bildirmeye davet ediyor ve bu da FBI'a fidye yazılımının yayılması ve etkisi hakkında daha kapsamlı bir görünüm kazandıracak.

FBI, "birçok virüs bildirilmediğinden dolayı fidye yazılımı kurbanlarının gerçek sayısını belirlemenin" zor olduğunu dile getiriyor.

FBI, kurbanların çeşitli nedenlerle virüs bulaşmalarını bildirmemesinden endişe duymakta. Bunun baş nedenlerinden biri, kurbanların bunu yaparken bir anlam görmemeleridir , özellikle de sıkıntıyı fidye ödeyerek ya da kötü amaçlı yazılım bulaşmasını temizleyerek dahili olarak çözmeleri durumlarında.


Hatırla

FBI fidye ödemeyi desteklemiyor. "Fidye ödemek, kurbanın verilerine yeniden erişeceğini garanti etmez". diyor FBI. “Açıkçası, bazı kişilere veya kuruluşlara fidye ödendikten sonra asla şifre çözme anahtarları verilmez. Fidye ödemek, düşmanı kârgütmek amacıyla diğer kurbanları hedef almaya iter ve diğer suçluları mali kazanç için benzer yasadışı faaliyetlerdebulunmaya teşvik edebilir.”


İpucu

Bir virüsü bildirmek için www.ic3.gov adresine gidin ve aşağıdakileri bildirin:

» Virüs bulaşma tarihi ve mağdur şirket bilgileri(sektörtürü ve işletme büyüklüğü gibi)

» Fidye yazılımı çeşidi (fidye sayfasında veya şifrelenmiş dosya uzantısında tanımlanır)

» Virüsün nasıl oluştuğu(örneğin, bir e-posta bağlantısı ,İnternet'tegezinme)

» İstenen fidye ve ödenen miktar (eğer varsa)

» Saldırganın Bitcoin Cüzdan adresi (fidye sayfasında listelenebilir)

» Fidye yazılımı bulaşmasıyla ilişkili genel kayıplar(fidye tutarı ve mağdur etki beyanı dahil olmak üzere)

Cisco Umbrella

Bugünün gelişmiş tehditleri güvenlik hakkında daha modern yaklaşımlar gerektiriyor.

Kurumların %68'i hedef alınmış saldırılara maruz kalıyor ve yan şubelerle dolaşım kullanıcıları açığın kaynağı olarak görülüyor.

Korunma almak için- ziyaret et

*Enterprise Strateji Grubu-2019

*Enterprise Strategy Group, 2019