Bir Sonraki Güvenlik Yatırımınızı Değerlendirirken Kaçınmanız Gereken 5 Hata

İçindekiler Tablosu

Yönetici Özeti

Dijital dönüşüme ayak uydurmak, özellikle de yeni teknolojileri kuruluşunuza entegre ederken detaylı inceleme, zaman ve çaba gerektirir. Yeni araçlar ve yatırımlar eklemek, kurumsal güvenlik ortamlarının karmaşıklığını ve saldırıya açıklığını artırır. Yeni yazılım ve hizmetler, kullanışsız bir dağılıma yol açarak, iletişim ve işbirliğindeki boşlukları açığa çıkarabilir, silolu sistemler oluşturabilir ve yanıt sürelerini yavaşlatabilir. Kuruluşun yeni nesil siber tehditlere karşı güvenliğini sağlamak, operasyonel verimlilik için otomatikleştirilmiş birleşik, entegre bir güvenlik mimarisi gerektirir; yani, dijital saldırı yüzeyinde riski azaltacak kadar geniş, güvenlik açıklarını kapatacak şekilde entegre edilmiş ve verimliliği artırmak ve yanıt sürelerini hızlandırmak için otomatikleştirilmiş bir güvenlik mimarisi gerektirir.

Giriş

Artık her zaman çevrim içi olan organizasyonlar, dijital dönüşüm ile birleştiğinde, yeni uygulama ve içerik tüketim modelleri yaratıyor. Sürekli bağlantıda olması gereken cihazların artışı, güvenlik sınırlarını kırarak manuel BT yönetiminde ek yüke ve yeni uçları hedefleyen daha fazla saldırı çeşidine neden olmuştur. Nesnelerin İnterneti (IoT) cihazlarının ortaya çıkması ve buna bulut tabanlı veri depolama ve uygulamaların, mobil cihazların, yeni şube konumlarının ve bunların uygun hibrit kullanıcılarının eklenmesi, benzersiz güvenlik açıkları, karmaşıklıklar ve riskler ortaya çıkarıyor. Güvenlik cihazlarının çeşitliliği ve giderek daha fazla üreticinin ekosisteme katılması ile güvenlik açıkları daha da artıyor ve saldırıların algılanmasında gecikmeler yaşanıyor.

Ağların ve dijital saldırı yüzeylerinin genişlemesiyle siber saldırılar, bulut ve otomasyon teknolojilerinden yararlanarak daha otomatik, karmaşık ve ayrıntılı hale geliyor ve bu sayede savunması zayıflamış noktaları tespit ederek planlamalarını gerçekleştiriyorlar.

Bu yeni risklerin ele alınması ve bu saldırı çeşitlerinin güvenliğinin sağlanması, bütünleşik bir güvenlik çözümü gerektirir. İleriye dönük güvenlik duruşları:

- Tüm saldırı yüzeyini kapsamalı ve yeni sınırları da içerecek şekilde kolayca genişlemelidir.
- Yaptırım için tam saldırı döngüsü algılamasını yönetmelidir.
- istem genelinde bağlama duyarlı tekil güvenlik politikasına sahip olmayı hedeflemelidir.
- Bulutta yerel güvenlik ile birden çok sağlayıcıyı ve hibrit bulut ortamını desteklemelidir.
- Zamanında müdahale için riskleri değerlendirmeli ve güvenlik duruşunda otomatik olarak ayarlamalar yapmalıdır.
- Tüm çözümleri izleyip yöneterek yalın BT ekiplerinin kuruluşun güvenlik ihtiyaçlarını karşılayacak şekilde ölçeklendirmesine olanak tanımalıdır.

Dijital inovasyon yolculuğunun başarısı ve kolaylığı açısından, bağlantı ve bilgi işlem katmanlarına yerleştirilmiş içeriğe duyarlı yüksek performanslı güvenlik kritik öneme sahiptir. Cihaz ve kullanıcılarla uygulamalar arasındaki tam bağlantı boyunca birleşik ve kendi kendini onaran bir ortam oluşturmak, güvenlik açıklarını en aza indirir ve saldırının yaşam döngüsü boyunca zamanında ve koordineli önlemeler ve müdahaleler sağlar.

Hata 1: Çok güvenmek

“Güvenilir” cihazların kuruluşların ağ çerçevesinin dışına yerleştirildiği, “güvenilmez” cihazlarınsa ağ içinde serbestçe dolaştığı bu zamanda, eski güvenlik modelleri koruma için etkili değildir. Şirket içinde ve dışında, genel ve özel bulutlarda çalışan karma kullanıcılar, ağa ve uygulamalara ücretsiz erişime ihtiyaç duyar. Bu durum, daha da katı erişim izinleri anlamına gelir.

En iyi uygulamalar, Zero Trust (sıfır güven) güvenlik modelini gerektirir; yani varsayılan olarak, hiçbir kullanıcı veya cihaza güvenilmez. Bunun yerine, kaynaklara erişim, kullanıcının kimliğine bağlı olarak verilir veya reddedilir ve izinler, söz konusu kullanıcının görev ve sorumluluklarına göre tayin edilir. Sıfır güven ilkeleri, özellikle de evden çalışma dünyasında güvenlik yüzeyinin genişlediği ve bölündüğü, uç noktaların büyük ölçüde çoğaldığı düşünüldüğünde, kötü niyetli veya savunmasız cihaz ve kullanıcı risklerini azaltır. Doğru bir şekilde uygulandığında, sıfır güven, yatay hareketin ve iznin kötüye kullanılmasının önlenmesi için daha da fazla yetenekle birlikte, hızlanan ve karmaşık siber saldırıları algılamak ve bunlara müdahale etmek için gerçek zamanlı tehdit istihbaratına erişimi zorunlu kılar.

Çoklu bulut ortamlarında verilere erişmenin ve bunları tüketmenin birden fazla yolu olduğundan, sıfır güvene sahip bir güvenlik modelini uygulamak ve uygulatmak, güçlü ağ bölümlendirmesi ve erişim kontrolü gerektirir. Kuruluşun güvenlik mimarisi, ağa bağlanan cihazları otomatik olarak tanımlayabilmeli, kullanıcının kimliğini güvenli bir şekilde doğrulayabilmeli ve bu kullanıcının hesabıyla ilişkili izinlere göre erişim sağlayabilmeli veya reddedebilmelidir.

Güçlü bir şekilde uygulanan sıfır güven politikası aynı zamanda, saldırganların ve kötü amaçlı yazılımların yanal hareketini sınırlayan ve bir veri ihlalinin olasılığını ve etkisini azaltan dahili ağ bölümlendirmesini de gerektirir. Uygulamaların ağda mı yoksa bulutta mı olduğu önemli değildir; kullanıcılar ve uygulamalar coğrafi olarak bağımsız olabilir ve yine de güvenli bağlantılar oluşturabilir.

"Sıfır güven ağ erişimi (ZTNA)" bu yaklaşımı alıp uygulama erişimine uygular. Bu da islemci, proxy, kimlik doğrulama ve güvenlik gibi çeşitli bileşenleri kullanmayı gerektirir. Bu göründüğünden daha zordur, çünkü çoğu kuruluşta bu bileşenler farklı üreticiler tarafından sağlanır ve bu nedenle farklı işletim sistemlerinde çalışır ve yönetim&konfigürasyon için farklı konsollar kullanırlar. Bu, tüm bu üreticiler arasında başarılı bir sıfır güven ağ erişimi modeli oluşturmayı neredeyse imkansız hale getirir.

Kuruluşların %94'ünden fazlası bulut teknolojisine geçmiştir
ve bunların %84'ü çoklu bulut dağıtımına sahiptir1

Firmalar ortalama olarak neredeyse 5 farklı bulut platformundan yararlanıyor[2]

Hata 2: Bulut platformlarını ve uygulama güvenliğini bir siloda değerlendirmek

Kuruluşlar, çoklu bulut ortamlarında tutarlı güvenlik politikası ve yaptırımı sağlamak için uğraşıyor. Çoklu bulut güvenliğini özel çözümlerle yönetmek karmaşıktır ve tutarlı güvenlik kontrollerini sürdürmeyi, uygulama erişimini yönetmeyi ve optimize etmeyi ve kurumsal geniş alan ağı (WAN) genelinde genel performansı sürdürmeyi zorlaştırır. Bu, birden fazla tedarikçinin birden fazla çözümünün kullanıldığı çeşitli durumlarda daha da zorlaşır.

Çoklu bulut dağıtımlarındaki en kritik riskler, yayılmadan, güvenlik eklentilerinden ve yanlış yapılandırmalardan kaynaklanır. Ağ çevresinin dışında bulunan ve genel internetten erişilebilen hibrit bulut dağıtımları, yetkisiz erişim sorunlarına neden olabilir.

Bulutun vaat ettiklerinden tam anlamıyla yararlanabilmek için güvenlik yetenekleri, bulut kaynaklarının otomatik ölçeklendirme gibi özelliklerle etkili kullanımını desteklemeli ve çoklu bulut dağıtımlarında entegre etmek ve gerçekten bulut yerelliği sağlamak adına gereken ayrıntı düzeyini sağlamak için çevreye duyarlı olmalıdır.

Bu nedenle, bulut koruması için entegre bir güvenlik yapılandırma yönetimi çözümü çok önemlidir. Çoklu bulut ortamları, güvenlikle ilgili yanlış konfigürasyonlardan yararlanan tehditlere hızlı bir şekilde müdahale edebilmek için dijital saldırı yüzeyinde koordineli algılama ve uygulamaya ihtiyaç duyar. Farklı bulut ortamlarında bulunan hibrit bulut uygulamaları, verileri izleyen riskleri değerlendiren ve kendini bu risklere göre otomatik olarak ayarlayan, bulutta yerel, tutarlı, bağlama duyarlı güvenlik çözümleri gerektirir.

Hata 3: Önleme zamanı yerine algılamaya odaklanmak

Siber suçlular, otomatik ve hedefli saldırıları giderek daha fazla kullanır hale gelmiştir. Bu iyi düzenlenmiş saldırı dizileri, siber savunuculara saldırı sırasını kesintiye uğratabilecekleri, yani algılama ve müdahale için sınırlı bir pencere sunar. Bu saldırganlar, bölünmüş çevrelerde daha da karmaşık ve çok biçimli saldırı bileşenlerini kullanmak için otomasyon, bulut ölçeği ve yapay zekadan (AI) yararlandıklarında, manuel algılama ve müdahale bu hıza ayak uyduramaz.

Bir kuruluşu en yeni, hızlı hareket eden saldırı taktiklerine karşı etkili bir şekilde korumak ve saldırıları başarılı olmadan önce engellemek için güvenlik duruşunuzu tam zamanında “yeniden programlayabilmeniz” gerekir. Bu da algılamadan yeni savunmayı devreye almaya geçiş yapma yeteneğinizi değerlendirmek anlamına gelir. Buna algılama yeteneklerinin doğruluk ve hız açısından değerlendirilmesi de dahil olacaktır. Ve değerlendirme süreci burada da bitmemelidir. Belirtilere dayalı algılamaya karşı bütünsel algılamaya olanak tanıyan birleşik veri kümelerini inceleyin. Yapay zekanın kalitesini değerlendirin ve küresel ve topluluk tehdit istihbaratı paylaşımlarına bakın ki “ikinci” bir “İlk Hasta” olmayın. Ve en önemlisi, çözümün saldırı döngüsü genelinde yeni önleme üretme ve bunları farklı teknolojiler ve cihazlara otomatik olarak dağıtma yeteneğini değerlendirin. Bu, savunmanızın başladığı andır.

İkinci olarak, güvenlik ekibinizin en son tehdit istihbaratına gerçek zamanlı erişimi olmalıdır. İyi eğitilmiş bir makine öğrenimi (ML) sınıflandırıcısı, gerçek tehditleri yanlış pozitiflerden ayırt edebilir; böylece güvenlik ekipleri araştırmalarını ve iyileştirme çabalarını gerçek saldırılara yoğunlaştırabilir. Bu sınıflandırıcılar, çok çeşitli güvenlik çözümlerine entegre edilebilir. Sıralı olarak dağıtılan çözümler de davranışsal anormalliklere dayalı olarak tehditleri otomatik olarak algılayabilir ve önceden tanımlanmış yöntemleri kullanarak müdahalede bulunabilir. Makine öğrenimi, veri toplama ve analitiğe yardımcı olmak için de kullanılabilir, tehdit avcılarına ve güvenlik operasyonları merkezi (SOC) analistlerine gelişmiş ve hızlı hareket eden saldırıları hızla tespit etmek ve bunlara yanıt vermek için ihtiyaç duydukları bilgileri sağlar.

Sağlam bir ağ ve güvenlik duruşu, ortam genelinde otomatik olarak neredeyse gerçek zamanlı, kullanıcıdan uygulamaya koruma sağlamak için bulut ölçeğinden ve gelişmiş yapay zekadan faydalanır. Yapay zekanın stratejik kullanımı; uçlar, bulutlar, uç noktalar ve kullanıcılar genelinde yakınsanmış ağ ve güvenlik ile dijital saldırı yüzeyi ve yaşam döngüsü boyunca koordineli algılama, önleme ve müdahale açısından çok önemlidir.

Hata 4: Bağlantıyı yerel güvenlik olmadan genişletmek

Ağlarındaki artan cihaz dizisini ve bunlarla ilişkili siber tehditleri yönetmek için birçok kuruluş, izlemesi veya yönetmesi zor olan bir dizi entegre olmayan (“nokta”) güvenlik ürünü kullanır; hatta bazılarının aynı kullanım durumu için donanım, yazılım ve "Hizmet Olarak Her Şey" genelinde farklı satıcıları olacaktır. Bu, ağ ortamlarının güvenliğini sağlamanın karmaşıklığını artırır.

Bulut tabanlı uygulamalar, işletmelerin dijital inovasyonu çalıştırması ve etkinleştirmesi açısından gereklidir. Bu, ağı genişletmekte ve yeni ağ uçları yaratmaktadır. Nerede çalışırlarsa çalışsınlar, uygulama kullanılabilirliği ve kullanıcı deneyiminin tutarlı olması için şirketlerin çevik ve uyarlanabilir olması gerekir. Ve günümüzün ağları son derece çevik olacak şekilde tasarlansa da, çoğu geleneksel güvenlik çözümü böyle tasarlanmamaktadır. Bu, güvenlik çözümleri ivmeye ayak uydurmaya odaklanmışken, uyarlanabilir bulut ağ ortamının kritik kaynakları ve verileri korumasız bırakabileceği anlamına gelmektedir. Çözüm, güvenlik ve ağ işlevlerini herhangi bir uca genişleyebilen tek, entegre bir sistemde birleştiren bir yaklaşım aramaktır.

Donanım, yazılım ve "Hizmet Olarak Her Şey" tekliflerini tekil bir güvenlik duruşunda karıştırıp eşleştirmenize olanak tanıyacak dağıtım modellerinde tutarlılık arayın. 5G ve Long-Term Evolution (LTE) teknolojilerinden yararlanılarak elde edilen yüksek kullanılabilirliği (HA) ve ayrıca kaynakların daha iyi kullanımı ve toplam sahip olma maliyeti (TCO) için yazılım tanımlı WAN’a (SD-WAN) geçişleri de dikkate almanız gerekir. Bu, dijital yenilik yolculuğu boyunca yeni tekliflerin uyarlanmasının siz ve ekipleriniz için sorunsuz olmasını sağlayacaktır.

32%

BT liderlerinin %32'si, "çok fazla manuel sürece" güvenmenin önde gelen bir güvenlik sorunu olduğunu belirtiyor.[3]

Hata 5: Ekosisteminizin tamamını dahil etmemek

Ağ sınırının hızla genişlemesinin en büyük zorluklarından biri, işlerin yürümesi için gereken teknolojilerin çoğunun birlikte çalışmamasıdır. Çoğu siber güvenlik çözümü birbirinin farkında bile değildir ve bu entegrasyon eksikliğinin sonucunda ortaya çıkan karmaşıklık, güvenlik ekiplerini yavaşlatır ve saldırganlara istismar için açık fırsatlar sunar. Daha da kötüsü, dijital inovasyondaki ilerlemenin çoğu, birleştirici bir güvenlik stratejisi veya çerçevesi olmadan parçalı bir yapıda olmuştur. Sonuç olarak, çoğu kuruluş ağın bir işlevini veya bir bölümünü tek başına korumak üzere tasarlanmış, çok çeşitli yalıtılmış güvenlik araçları biriktirmiştir. Bu, görünürlüğü azaltıp kontrolü kısıtlayarak, gözden kaçan tehditlere ve etkisiz yanıtlara yol açar.

Yardım etmenin bir yolu, tehdit istihbaratı ortakları, araştırma kuruluşları ve satıcılarla koordine olmak ve işbirliği yapmaktır. FortiGuard Labs gibi kuruluşlar, sektördeki en iyi uygulamaları paylaşmak ve saldırıların yayılmasını engellemek için küresel istihbarat topluluğu ile işbirliği yapar. Bu topluluk, küresel yapı dağıtımlarından veya ortaklardan gelen milyonlarca olay karşısında işletmeleri görmek ve korumak için çok çalışıp, topluluk tarafından bilinen tehditlerle ilgili olarak “ikinci” bir “İlk Hasta” vakasını engellemektedir. Birlikte çalışmak, görünürlük, algılama ve koordineli müdahalelerin birleştirilmesine yardımcı olur.

Çözüm, yerel olarak ve genişletilmiş dijital saldırı yüzeyini kapsayacak şekilde tasarlanmış zengin bir ekosistem aracılığıyla, algılama ve müdahale için birleşik bir cephe oluşturmak üzere dağıtımınızın geri kalanıyla kolayca entegre edilebilen bir yaklaşımı benimsemektir. Yeni nesil bir koruma çözümü, uygulama programlama arabirimleri (API'ler), bağlayıcılar ve DevOps otomasyon araçları ve komut dosyaları aracılığıyla çok çeşitli üçüncü taraf üretici teknolojileri ile entegre olabilmelidir.

Açık bir API mimarisi, farklı cihazlar arasında iletişim ve senkronizasyon sağlar. Özel olarak oluşturulmuş bağlayıcılar, ekosistem genelinde gerçek zamanlı iletişim ve otomatik güncellemelere izin vererek daha yüksek düzeyde entegrasyon ve birlikte çalışabilirlik sağlar. DevOps araçları ve komut dosyalarından oluşan bir kitaplık, hızlı, özelleştirilebilir dağıtım ve yönetime olanak tanıyarak, yalın güvenlik ekiplerinin yeteneklerini ölçeklendirir. Bu tür bir entegre güvenlik mimarisi, nerede bulunursa bulunsun, her ağ ucunda tutarlı koruma ve bağlantılar sağlayabilir.

BT liderlerinin %35'i entegre olmayan güvenlik mimarilerine güveniyor.[4]

Sonuç

Değişmeyen tek şey değişimin kendisiyken ve mevcut bir ortama eklenen yeni inovasyonlar hızla tüketilirken, basitlik ve uyarlanabilirlik esastır. Ağlar daha karmaşık ve heterojen hale gelmeye devam ettikçe, kuruluşlar olay algılama, önleme ve müdahale süreçlerini basitleştirmek ve optimize etmek için geniş, entegre ve otomatikleştirilmiş bir güvenlik platformuna ihtiyaç duymaktadır. Bu, operasyonları ve olay yanıtlarını hızlandırırken tüm dijital saldırı yüzeyinde birleşik görünürlük sağlar, güvenlik açıklarını kapatır ve karmaşıklığı azaltır.

Başarılı bir dijital deneyim, çeşitli ve küresel ortamlarda ve bulut yapılandırmalarında kullanıcılar, cihazlar ve uygulamalar arasında güvenilir, yüksek performanslı bağlantılar sağlar. Bunun işe yaraması için siloları birleştirmek tek başına yeterli değildir; ağ ve güvenlik koordinasyonu, birleştirme ve yakınsama ile birlikte ortak işbirliği çözümdür. Bir sonraki güvenlik yatırımınızı değerlendirirken bu beş hatadan kaçınmak, güvenlik açıklarını kapatmanıza, silo halindeki sistemleri birleştirmenize ve müdahale sürelerini hızlandırmanıza yardımcı olacaktır.

[1] "RightScale 2019 State of the Cloud Report from Flexera," Flexera and RightScale, February 27, 2019.

[2] Nick Galov, "Cloud Adoption Statistics for 2021," Hosting Tribunal, January 19, 2021.

[3] "The IT Infrastructure Leader and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, August 18, 2019.

[4] Ibid.

www.fortinet.com

www.exclusive-networks.com/tr

Telif Hakkı © 2021 Fortinet, Inc. Tüm hakları saklıdır. Fortinet®, FortiGate®, FortiCare® ve FortiGuard® ve bazı diğer markalar, Fortinet, Inc.'in tescilli ticari markalarıdır ve buradaki diğer Fortinet isimleri de Fortinet'in tescilli ve/veya genel hukuk açısından ticari markaları olabilir. Diğer tüm ürün veya şirket adları, ilgili sahiplerinin ticari markaları olabilir. Burada yer alan performans ve diğer ölçüler, ideal koşullar altında dahili laboratuvar testlerinde elde edilmiş olup, gerçek performans ve diğer sonuçlar değişiklik gösterebilir. Ağ değişkenleri, farklı ağ ortamları ve diğer koşullar performans sonuçlarını etkileyebilir. Burada yer alan hiçbir şey Fortinet tarafından verilmiş bağlayıcı bir taahhüdü temsil etmemekte olup, Fortinet, Fortinet'in bir alıcıyla, Fortinet'in Genel Danışmanı tarafından imzalanmış, bağlayıcılığı olan, tanımlanan ürünün açıkça tanımlanmış belirli performans ölçütlerine göre performans göstereceğini açıkça garanti eden yazılı bir sözleşme yapması hariç olmak üzere, açık veya zımni tüm garantileri reddetmektedir; sözü edilen türden bir sözleşmenin imzalanması halinde ise yalnızca söz konusu bağlayıcı yazılı sözleşmede açıkça belirtilen belirli performans ölçütleri Fortinet için bağlayıcı olacaktır. Mutlak netlik getirmek adına, böyle bir garanti, Fortinet'in dahili laboratuvar testlerinde olduğu gibi aynı ideal koşullardaki performansla sınırlı olacaktır. Fortinet, açık veya zımni olsun, burada belirtilen tüm taahhütleri, beyanları ve garantileri tamamıyla reddetmektedir. Fortinet, bu yayını önceden haber vermeksizin değiştirme, düzenleme, aktarma veya başka şekilde revize etme hakkını saklı tutar ve yayının en güncel sürümü geçerli olacaktır. Fortinet, açık veya zımni olsun, burada belirtilen tüm taahhütleri, beyanları ve garantileri tamamen reddetmektedir. Fortinet, bu yayını önceden haber vermeksizin değiştirme, düzenleme, aktarma veya başka şekilde revize etme hakkını saklı tutar ve yayının en güncel sürümü geçerli olacaktır.

8 Mart 2021 15:01
5-Mistakes-to-Avoid-eBook 914666-0-0-EN