19 Kasım 2019 Salı

Siber Güvenlik: Güvenliğiniz Ne Kadar Güvende?

Yazının aslı CPO Magazine'de yayınlanmıştır. Yazar: MATHIEU CHEVALIER· Ekim 24, 2019

Ağ güvenlik kameraları ve diğer güvenlik aygıtları, doğası gereği internete bağlıdır. Kullanıcıların işlerini denetlemek için sistemlerine uzaktan erişmelerine olanak sağlayan ve üreticilerin, yerel ağ dışında da aygıt yazılımlarını güncellemelerini sağlayan olgudur. Ancak bu özellik sistemlerin Aşil'in Topuğu da olabilir. Düzgün bir şekilde güvenceye alınmadığında, Nesnelerin İnterneti (IoT) içindeki herhangi bir kamera veya erişim kontrol aygıtına, yalnızca erişimi paylaşmak isteyenler tarafından değil, herkes tarafından uzaktan erişilebilir. Benzer şekilde, bir sunucu ve istemci uygulaması veya eski donanım yazılımı arasındaki şifrelenmemiş iletişimler, siber suçlular tarafından belirlenebilir ve gizil güç olarak tüm bir kuruluşun ağını riske sokar.

Ve bu elektronik güvenlik endüstrisi için büyük bir sorundur.

Sektör çözümleyici Gartner firmasına göre, 2020 yılına kadar işletmelerdeki siber saldırıların yüzde 25'inden fazlası nesnelerin interneti (IoT) aygıtları kullanılarak gerçekleşecek[1]. Ve evet, bu bizi güvende tutmaya yardımcı olması gereken güvenlik aygıtlarını içerir. Siber saldırıların yüzde 60'ından fazlası şu anda küçük ve orta ölçekli işletmelerdedir ve özellikle küçük işletmeler bu tehditlere karşı savunmasız durumdadır. Küçük işletmelerin %60'ı, büyük bir siber saldırıyı takip eden altı aydan sonra işlerini sürdürememektedir.

Büyük işletmelere yapılan saldırıların da son derece yüksek maliyeti olabilmektedir. IBM ve Ponemon Institute[2] tarafından yapılan 2018 çalışmasına göre, ortalama bir veri ihlali maliyeti 3,86 milyon dolar ve büyük çaplı ihlaller ise 350 milyon doları geçebilir.

Elektronik güvenlik sisteminizi siber tehditlere karşı koruma konusunda risk alamazsınız. **İyi haber, bu savaşta yardımın hazır olması.** Saygın elektronik güvenlik üreticileri ve yazılım geliştiricileri, siber tehditlere karşı korunmanın birçok yolunu belirledi. Bu konuda çalışmalarını da sürdürüyorlar. Kelimelerin tam anlamıyla, ürünlerinin gerçekten dedikleri korumayı sağlayıp sağlamadığını belirlemek için kendilerine "saldırıyorlar" (sızma testleri yaptırıyorlar). Siber tehditlere karşı korunmanıza yardımcı olabilecek bir diğer önemli ortak: elektronik güvenlik çözümlerini öneren güvenilir sistem kurulumcuları.

Siber suçlular güvenlik sistemine nasıl erişebilir?

Güvenliği kötü olan bir kamera, bir sunucu ve istemci uygulaması arasında şifrelenmemiş iletişim veya güncel olmayan bellenim(firmware), siber suçlular tarafından kolayca kullanılabilir. Özellikle fidye yazılımı saldırıları maliyetli ve yaygındır. Ancak eski yazılımları çalıştıran sistemleri hedef aldığı bilinmektedir.

Siber güvenlik ihlalleri söz konusu olduğunda en zayıf halka sıklıkla insanlardır. IoT aygıtlarında varsayılan şifreleri değiştirmeyen çalışanlar, fırsatçı siber suçluların sisteminize erişebilmeleri için kolay bir yoldur. Kaba kuvvet (Brute Force) saldırıları, şifreleri tahmin eden suçlulardan, paket koklama (packet sniffing) ağ trafiğini yakalayan ve ortadaki adam (man-in-the-middle) saldırılarından, kazandıkları bilgiyi kendi yararlarına kullanarak iki sistem arasındaki iletişimleri gizlice dinler.

19 Kasım 2019 Salı

Çoğu elektronik güvenlik çözümü, sistemi genişletmek, eski veya bozuk ürünleri değiştirmek için yeni aygıtların eklenmesiyle devam eden bir çalışmadır. Belki de daha az güvenli standartlara sahip farklı bir üreticiden yeni ekipman ekleme işlemi güvenlik açığı oluşturan başka bir etkendir.

Ağlardaki güvenliğe karşın siber suçlular da saldırılarının kapsamını arttırmış olabilir. Ancak bu, siber saldırılara karşı savunmasız olduğunuz anlamına gelmez.

Bir siber güvenlik çözümünün hangi unsurları olmalıdır?

Siber tehditlerle mücadele etmenin en önemli yollarından biri iyi bir plan yapmaktır. Şirketler, iyi uygulamaların önemi ve şirket politikasına titizlikle uyma konusunda eğitimler geliştirmeli ve çalışanlarını eğitmelidir. Yalnızca en güvenilir üreticileri öneren ve siber güvenliğin önemini vurgulayan bir sistem kurulumcusu seçmek, iyi bir başlangıçtır. Şifreleme, kimlik doğrulama, kritik işler ve güvenlik sistemlerinize yetkilendirme dahil olmak üzere birden fazla siber güvenlik katmanı uygulayan bir çözüm geliştirmeniz gerekir.

Şifreleme; verilerin şifreli olduğu, böylece yetkisiz kullanıcılardan gizlendiği veya erişemeyeceği bir yerde saklanmasıdır. Özel bilgilerin korunmasına, hassas verilerin korunmasına yardımcı olur ve istemci uygulamaları ile sunucular arasındaki iletişimin güvenliğini artırabilir. Verileriniz şifreli olduğunda; yetkisiz bir kişi, bir varlık veya bir siber suçlu tarafından ele geçirilmiş olsa bile, onu okuyamaz veya anlayamaz.

Kimlik doğrulama; önce bir kullanıcının varlığını, sunucu veya istemci uygulamasının kim veya ne olduğunu, ardından o varlığın sisteme erişip erişmeyeceğini ve kimliğinin nasıl doğrulanacağını belirlemektir. Kuruluma bağlı olarak, kimlik doğrulama istemci tarafında veya sunucu tarafında veya her iki ucunda da gerçekleşebilir. İstemci tarafı kimlik doğrulaması, kullanıcı adı ve şifre kombinasyonlarını, belirteçleri ve diğer teknikleri kullanırken, sunucu tarafı doğrulaması güvenilir üçüncü tarafları tanımlamak için sertifikaları kullanır. İki faktörlü kimlik doğrulama, birleştirme halinde kullanılan iki kimlik doğrulama formunu ifade eder. Kimlik doğrulama, verilerinizin yanlış ellere geçmesini önlemek için önemli bir araçtır. Yetkisiz erişimi önler ve aslında güvenlik personeliniz dışında kimsenin sisteminize erişememesini sağlar. Bu, bilgisayar korsanlarının değerli bilgilerinizin kontrolünü ele geçirmek, yönetmek veya önemli verilerinizi kopyalamak için güvenlik sunucusu gibi davranamayacağı anlamına gelir.

Yetkilendirme; güvenlik sistemi yöneticilerinin kullanıcı veya işletmen erişim haklarını ve ayrıcalıklarını belirtmelerini sağlayan işlevdir. Yöneticiler, kaynaklar, veriler veya uygulamalar için birey gruplarına erişim hakları vererek ve kullanıcıların bu kaynaklarla neler yapabileceğini tanımlayarak bir sistemdeki etkiliklerinin alanını sınırlar. Yöneticiler, personellerinin görebildiklerini ve yapabileceklerini yönettiğinde, güvenlik sistemi içinde iletilen ve depolanan verilerin güvenliğini de sağlarlar. Bir bütün olarak sistemin güvenliğini arttırmanın ve ona bağlı diğer sistemlerin güvenliğini arttırmanın anahtarıdır.

Siber güvenlik söz konusu olduğunda asla şikayet edemezsiniz

Neredeyse her gün başka bir hack veya güvenlik ihlali raporuyla görülüyor ki siber güvenlik acıları çekiliyor. Bununla birlikte, hiç kimse siber suçlulara karşı savaşta sızlanmamalıdır. Elektronik güvenlik yatırımınızı korumak için bir kez siber güvenlik izlemi belirleyip yatırım yaptıktan sonra, uyanık kalmak önemlidir.

1. Yalnızca kuruluşunuzu siber tehditlerden koruyabilecek güvenilir ve saygın güvenlik ürünü üreticilerini seçin. Bilginin korunması ve gizliliği söz konusu olduğunda, bir dizi devlet ve örgütsel uyumluluk koşulu vardır. Bu gereksinimleri ciddiye alan bir şirket seçtiğinizden emin olun.

2. Siber güvenlik konusunda ciddi olan bir şirket de kendi sızma testini gerçekleştirecektir. Sızma testleri, ürün geliştirme sırasında gözden kaçırılabilecek tüm zayıf noktaları yakalamak için tekrar tekrar yapılmalıdır.

3. Elektronik güvenlik çözümü geliştirmek veya sürdürmek için bir sistem kurulumcusuyla çalışırken, siber güvenlik hakkındaki endişelerinizi başlangıçta paylaşmak önemlidir. Sistem kurulumcusu, siber güvenliği öncelikli olarak değerlendirmeli ve yalnızca sisteminizi korumayı sağlayabilen, güvenilir üreticilerin ürünlerini önermelidir.

4. Siber saldırıların finansal riskini azaltmak için bazı şirketler siber sorumluluk sigortasına yöneliyorlar. Şirketleri İnternet kaynaklı tehditlere ve veri ihlallerine karşı bir derece korumak için sigorta şirketleri tarafından sunulan yeni bir kapsamdır. Siber sorumluluk sigortası, Hızır olmasa da, kurulumculara gönül rahatlığı, şirketlerin siber saldırıyı yönetmeleri ve işlerini sürdürmeleri için parasal kaynaklara erişmelerini sağlar.

Sonuç

Siber güvenlik, her ölçekteki kuruluş için en önemli iş risklerinden biri haline geliyor. Herkesin elektronik güvenlik sisteminizi siber saldırılardan korumada rolü vardır. Sızma testi yanı sıra şifreleme, kimlik doğrulama ve yetkilendirme gibi birden fazla savunma katmanı kullanan güvenilir satıcıları seçtiğinizden emin olun. Sadece siber tehditlere karşı sürekli koruma sağlama konusunda kararlı olan sistem kurulumcularıyla çalışın. İşinizin başarısı buna bağlı olabilir.

Kaynaklar:

[1] *https://www.gartner.com/en/conferences/la/symposium-brazil/agenda/featured-topics/security-risk*
[2] *https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years*