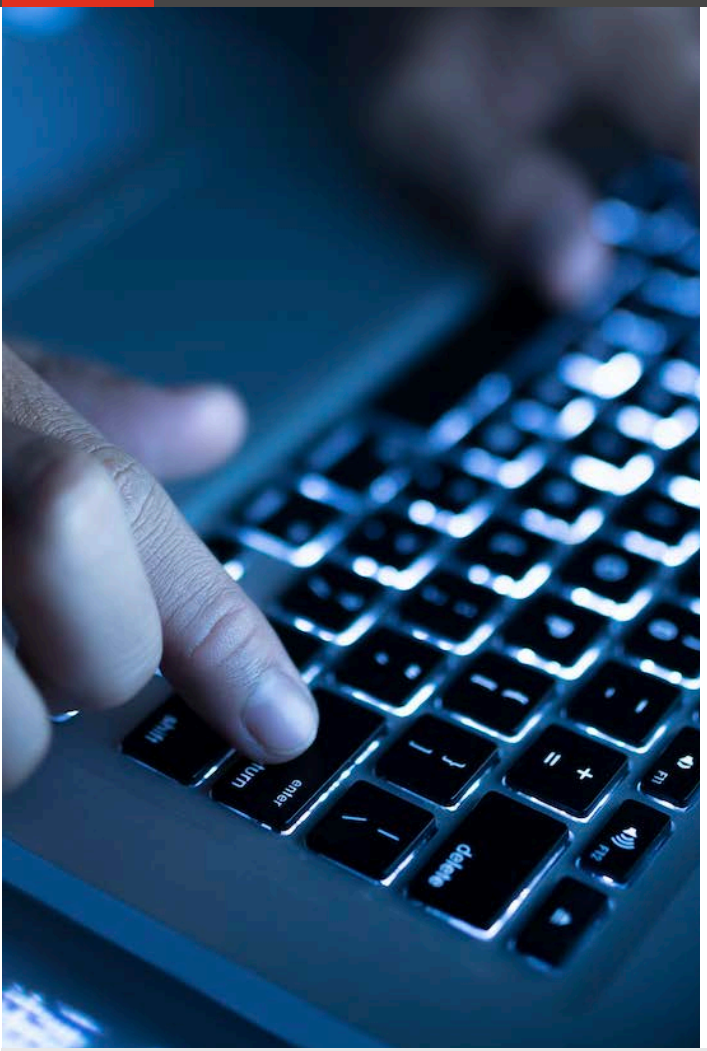
Siber saldırılar:

Bir siber risk olasılığı ile karşılaştığınızda cevaplamanız gereken 5 soru



İş dünyasının lider şirketleri hatta lider siber güvenlik şirketleri ve kamu kurumları bile gelişmiş siber tehditler karşısında savunmasız olabilir. Hem siber suçlular hem de kamu kurumları bu siber tehditlerin kazanan tarafı olabilmek için 7/24 çalışıyor.

Son zamanlarda manşetlerde kendine yer bulan güncel bir siber saldırıda son derece yetenekli bir siber saldırganın yaygın olarak kullanılan, şirketlerdeki yazılımlara ve platformlara geniş ölçüde entegre bir ağ izleme ve yönetim yazılımının güncellemesine kötü amaçlı bir yazılım yerleştirdiği ortaya çıktı. Önemli siber güvenlik şirketlerinden biri de bu saldırıdan etkilenenler arasındaydı ve bir inceleme başlatarak birkaç aydır devam eden, daha geniş çaplı bir saldırılar zincirini ortaya çıkardı. Bu araştırma Kuzey Amerika'da, Avrupa'da, Asya'da ve Orta Doğu'da saldırıdan etkilenen kamu, profesyonel hizmetler, teknoloji ve telekomünikasyon şirketlerinin tespit edilmesine yardımcı oldu.

2020 ilkbaharından beri devam ettiği tespit edilen bu siber saldırı yazılım tedarik zincirlerinin güvenliğine dikkat çekiyor. Yazılım tedarik zincirleri, fiziksel tedarik zincirlerine göre daha basit. Depolama yok, malzeme kaynak temini yok, nakliye yok... Bu yüzden tedarik zincirini sekteye uğratabilecek riskler daha az değil mi? Hayır değil.

Fiziksel tedarik zincirinde bildiğimiz sürecin bir benzeri yazılım tedarik zincirinde de mevcut. En büyük fark, yazılım tedarik zincirindeki bir aksama veya saldırının tüm tedarik zinciri üzerindeki etkisinin katlanarak büyüyebilmesi.

CEO'lar ve yönetim kurulları şirketlerinin CISO'ları ve CIO'ları ile şu konuları ele almalı:

1 Şirket saldırıdan etkilendi mi? Şirket bu saldırı karşısında ne kadar savunmasızdı? Saldırı ekosistemin neresinde gerçekleştirildi?

CIO, CTO ve CISO'lar, şirketin saldırıya uğrayan yazılım ve hizmet sağlayıcılarına ne kadar bağımlı olduğunu bilirler. Sormanız gereken sorular; bünyemizde etkilenen yazılım var mı? Etkilenen yazılımların tam bir dökümü elimizde bulunuyor mu? Siber saldırganın aktif olarak ekosistemimizi hedef aldığı veya ekosistemimizde hareket ettiğini tespit etmemize yardımcı olacak göstergeleri bulmak için ne yapacağız?

2 Halâ risk altındayken, saldırıya nasıl müdahale edebilirsiniz, saldırıyı nasıl kontrol altına alabilirsiniz?

Siber saldırıyı kontrol altına almak için atacağınız adımlar, şirketinizin yüksek riskli bir hedef olup olmadığına bağlı. CISO'nuz danışmanlık desteği veren yazılım ve hizmet sağlayıcılarıyla işbirliği yapabilir. Siber Güvenlik ve BT ekipleri bunu bir öncelik olarak ele alırken, saldırıyla ilgili daha fazla bilgi gün yüzüne çıkmaya devam eder.

Etkilenen yazılımı incelemek ve düzeltmek için neler yapıyoruz (etkilenen sistemleri kapatma, yeni yamalar uygulama)? Şirketin hassas ve gizli verileri üzerindeki etkiyi değerlendirdik mi? Kriz yönetim planımızı devreye sokmalı mıyız?

pwc

3 Siber saldırıların şirketiniz üzerindeki etkisini nasıl sınırlandırabilirsiniz?

Siber saldırıların devam edebilecek bir tehdit olduğunu göz önünde bulundurmalısınız. CISO'nuza: Saldırganın hedefine ulaşmasını nasıl zorlaştırabiliriz? Saldırganın bizi hedeflemesini daha maliyetli hale getirecek yöntemler var mı? Saldırı riskinin başarı ihtimalini nasıl azaltabiliriz? sorularını yöneltin.

Şirketlerin siber ekosistemlerini hedefleyen riskleri sınırlandırmak için hafifletici önlemler bulunuyor.

- Şirkete gelen ve şirketten çıkan bağlantıları sınırlandırmak için ağ mimarisini segmentlere bölün.
- İlave ağ erişim kontrolleri uygulayın.
- Sunucularınızı güçlendirin: Potansiyel güvenlik açıklarını denetleyin, tespit edin, kapatın ve kontrol altında tutun.
- Hesap ayrıcalıklarını sınırlandırın.
- Kurumsal kimlik bilgilerini koruyun ve güçlü kimlik doğrulama ve şifre kontrolleri uygulayın.

4 Saldırıdan doğrudan etkilenmemiş olabilirsiniz. Şimdi atmanız gereken adımlar neler?

Saldırılar zincirinin tam etkisi henüz anlaşılmamış olabilir. İlk belirtiler – bir siber güvenlik şirketinin hackleme araçlarının çalınması, yazılım güncelleme ve yayınlamaları aracılığıyla hedeflerin ağlarına erişim kazanma tekniği ve birçok kamu kurumuna yapılan ilk ilişkili saldırılar – hepsi sadece bir başlangıç. İncelemeler devam ettikçe siber saldırganın amacı ve hedefleri hakkında daha fazla bilgi ortaya çıkacaktır.

Şirketiniz saldırıdan doğrudan etkilenmemiş olsa bile atmanız gereken iki adım var:

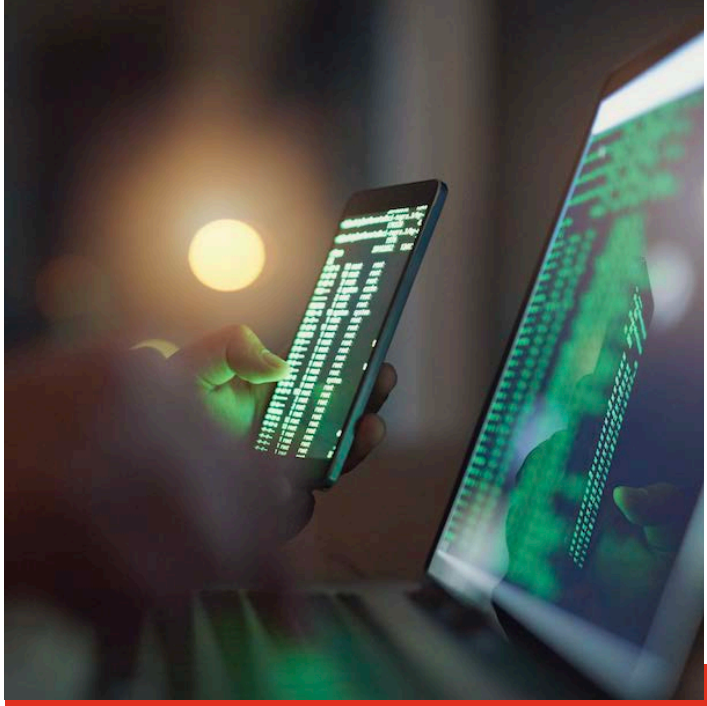
- Veri ve hizmetleriniz dahil olmak üzere önemli varlıklarınız çevresindeki faaliyetleri yakından izleyin. Bu faaliyetlerin takibi sizi saldırıdan etkilenenlerden ayıran şey olacaktır. Siber risklere karşı yüksek dayanıklılığa sahip şirketlerin %91'i varlıklarının ayrıntılı bir dökümünü tutuyor ve gerektiğinde listeyi güncelliyor. Diğer şirketlerde ise bu oran %47.
- Tedarikçilerinizden, iş ortaklarınızdan ve diğer paydaşlarınızdan sistemleri ağınıza bağlı olanların saldırıdan etkilenip etkilenmediğini araştırın. Ekosisteminizdeki yazılım riski yoğunlaşma noktalarını değerlendirin.

5 Daha geniş ölçekte neleri ele almalısınız?

Küresel bir saldırıdan ilk haberdar olduğunuz anda duyduğunuz endişe ve merakı işinize yansıtın. Şirketiniz doğrudan etkilenmemiş olsa dahi CISO, CIO ve CRO'nuzla üç şeyin kontrolünü yapmanız gerekir.

- **Şirketin yazılım tedarik zincirinin güvenlik önlemleri ne durumda?** Gerçek saldırı trendleri ve tehdit vektörlerine karşı savunma için çok katmanlı koruma modeline ihtiyaç var.
- **Dayanıklılık planlarınızı daha geniş ölçekte tehditlere karşı test ettiniz mi?** Küresel Dijital Dünyada Güven Araştırması 2021'e katılan 3.249 yöneticinin %40'ı dayanıklılık testlerini artırarak saldırı nitelikli bir siber risk oluşması durumunda önemli şirket fonksiyonlarının çalışmayı sürdürmesini sağlamayı planlıyor.
- **Yazılım ve güvenlik sağlayıcılarınız açısından yoğunlaşma riskiyle karşı karşıya mısınız?** Bir veya birkaç sağlayıcıda hizmetleri birleştirmenin maliyet ve ölçek avantajlarını yoğunlaşma riskleriyle karşılaştırın.

2021-0017



Daha fazlası için:

- Bulut tabanlı yazılım tedarik zinciri güvenliği
- Tüm senaryolar için hazırlıklı olun
- Dayanıklılık planlarınıza stres testi uygulayın
- Yönetim kurulları siber riskleri nasıl takip edebilir?

İletişim

Özkan Kıvanç
Siber Güvenlik ve Veri Koruma Hizmetleri Şirket Ortağı, PwC Türkiye
ozkan.kivanc@pwc.com

Ulvi Cemal Bucak
Siber Güvenlik ve Veri Koruma Hizmetleri Lideri, PwC Türkiye
cemal.bucak@pwc.com