9 siber tehlikeye DİKKAT!

Sanal dünya neredeyse gerçeğinden daha hızlı dönerken, bu hızı sağlayan teknolojik altyapılar 2018'de de giderek artan siber risklerle karşılaşacak. Innovera Genel Müdürü Gökhan Say, hangi konularda önlem alınması gerektiğini sıraladı

H.Merkezi / E.Çözüm

DİJİTALLEŞMEYLE birlikte şirketlerin varlıkları siber ağlar üzerine taşınıyor; Nesnelerin interneti, giyilebilir cihazlar, artan bulut platformu kullanımı, Endüstri 4.0, finansal dünyanın 'sanalize' olması derken yaşam artık arka planda sorunsuz çalışması gereken ağ altyapıları üzerinde duruyor. Ancak bu durum dijital dönüşüm yolculuğuna çıkan kurumlar için başta kişisel verilerin gizliliği olmak üzere dikkat edilmesi gereken pek çok unsuru da beraberinde getiriyor. 2018 içinde karşılaşılması öngörülen tehlikelere karşı kurumları uyaran Innovera Genel Müdürü Gökhan Say, hangi konularda önlem alınması gerektiğini şöyle sıralıyor:

NESNELERİN İNTERNETİ (IOT):

Dijital dönüşüm yolculuğunuzda Endüstri 4.0 varsa nesnelerin interneti ile yolunuz kesişecek demektir. 2018'deki küresel IoT (Internet of Things) harcamalarını 772 milyar dolar olarak öngören IDC, güvenli yazılım oranının ise 2021'de yüzde 55'e yükselmesini bekliyor. "Ağa bağlı milyarlarca cihaz" olarak tanımlanan bu alanda yapacağınız yatırımlarda güvenlik başlığını ilk sıraya almanız önem taşıyor. Kritik sektörler: Üretim, telekom, kamu, perakende, enerji.

KİŞİSEL VERİLERİN GİZLİLİĞİ:

Özellikle Avrupa Birliği bünyesinde alınan ve 2018 başında yürürlüğe giren MIFID II gibi yeni kriterler bu alandaki siber risklerin boyutunu ortaya koyuyor. Alacağınız önlemlerle hem uluslararası güvenlik normlarına uyumlu hem de müşterilerinizi koruyan bir BT altyapısına sahip olmalısınız. Kritik sektörler: Finans, Bankacılık, Perakende, Sağlık.

SANAL PARALAR:

Bitcoin, Ethereum gibi sanal kripto paralar kısa sürede hızlı kazanç için cazip görünebilir. Ancak kripto para borsaları ile dijital cüzdanlar da siber saldırıların odak noktasında. 2018, dünyanın farklı bölgelerinde çalınan verilerle birlikte başladı. Dijital cüzdanını kaptıran ve şirket içi ağınıza bağlanabilen bir çalışanınız kurumunuza ait veriler için de bir risk oluşturabilir. Kritik sektörler: Finans, Bankacılık, Perakende.

BULUT GÜVENLİĞİ:

Dijital dönüşüm, diğer etkilerinin yanında işinize ait süreçlerin bulut platformlarına taşınması anlamına da geliyor. Bulut platformu sağlayıcınızın gerekli önlemleri almasıyla yetinmeden ek güvenlik önlemleri almalısınız. Kritik sektörler: İş süreçlerini buluta taşıyan tüm şirketler.

OTOMASYON GÜVENLİĞİ:

Dijital dönüşümle eşanlamlı kabul edilebilecek otomasyon süreçleri de 2018'in riskli alanları arasında bulunuyor. Otomasyon için kullandığınız yan ekipmanlardan sistemi oluşturan ana cihazlara kadar risklerin proaktif bir şekilde izlenmesi gerekiyor. Innovera'nın kurucuları tarafından global marka olma hedefiyle çalışmalarını sürdüren Atar Labs'ın Güvenlik Operasyon Merkezleri (Security Operation Center – SOC) için geliştirdiği tipte yazılımlar güvenlik seviyenizi yukarıya taşımanızı sağlayacaktır. Kritik sektörler: Üretim, telekom, perakende, enerji.

UYGULAMA VE VERİ GÜVENLİĞİ:

Gartner'ın 2017-2018 Siber Güvenlik Riskleri raporundaki beş ana başlıktan biri olan uygulama ve veri güvenliğinin önemi bu yıl daha da artacak. Dijital dönüşümle birlikte artan uygulama ve büyük veri miktarının güvenilirliği için önlem almayan şirketler 2018'i pek de iyi hatırlamayacak. Kritik sektörler: Perakende, telekom, enerji.

YAPAY ZEKÂ:

Henüz emekleme safhasında olsa da 2017'de başlayıp 2020'de hızlanan ve 2025 sonrası olgunlaşan bir yapay zekâ kullanımı söz konusu olacak. Dünya Ekonomik Forumu'nun raporlarına da yansıyan bu öngörü dijital dönüşümde önemli bir basamak olma niteliği taşıyor. Şirket içi verimlilik adına verilerinizi emanet ettiğiniz, bulut tabanlı bir yapay zekâ uygulaması ise sisteminiz için güvenliği zayıf arka kapılar anlamına gelebilir. Kritik sektörler: Bankacılık, sigorta, telekom, danışmanlık.

PHİSHİNG KORUMASI:

2017, sistemleri kullanılmaz hale gelen fidye yazılımların son derece aktif olduğu bir yıl oldu. Bu durum, bilinçlenme ile birlikte azalsa da 2018'de sürecek. İşinizi doğrudan sekteye uğratacak bu tip saldırılar için hem kurum içi bilgilendirme hem de ağ altyapınızı koruyacak önlemleri devreye sokmalısınız. Kritik sektörler: E-posta iletişimi yoğun olan tüm sektörler.

DDOS ATAKLARI:

Uzun yıllardır gündemde olan bu saldırı tipi, dijital dönüşüm ve nesnelerin interneti uygulamalarının yaygınlaşmasıyla yükselmeye devam edecek. Ağınızın güvenlik seviyesini gözden geçirmek faydalı olabilir. Kritik sektörler: Orta ve büyük ölçekli, bilgisayar ve ağa bağlı donanım adedi yüksek tüm şirketler.