9 SİBER TEHLİKEYE DİKKAT!

Sanal dünya neredeyse gerçeğinden daha hızlı dönerken bu hızı sağlayan teknolojik alt yapılar da giderek artan siber risklerle karşılaşıyor. Bilgi güvenliği, entegrasyon ve danışmanlık şirketi Innovera da dijital dönüşüm yolculuğuna çıkanlar için başta kişisel verilerin gizliliği olmak üzere dikkat edilmesi gereken 9 siber tehdide karşı uyarılarda bulunuyor.

%55

2021 yılında

GÜVENLİ YAZILIM ORANI YÜZDE 55'E YÜKSELECEK

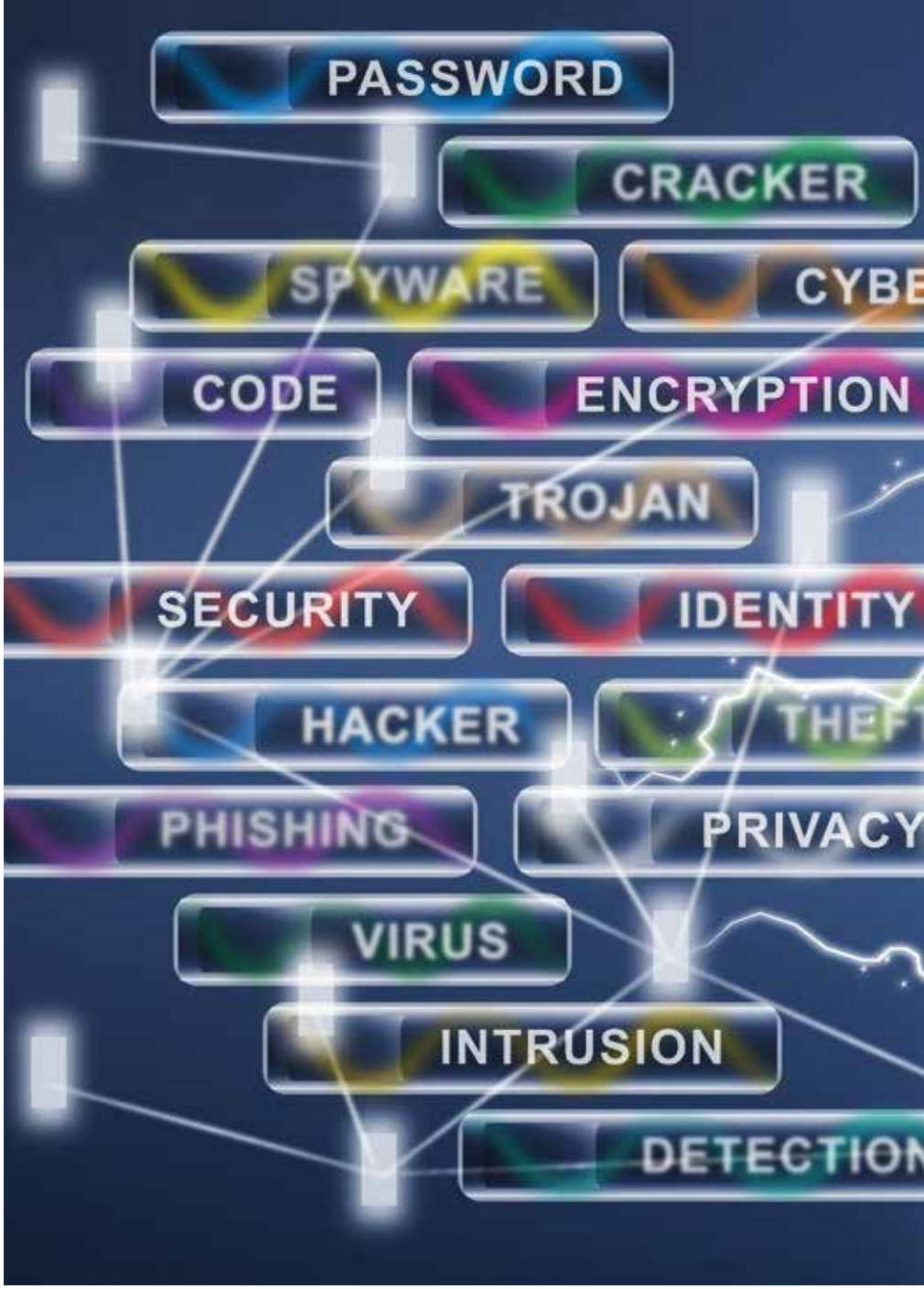
772

milyar dolar

2018'DEKİ KÜRESEL IOT HARCAMALARININ TAHMİNİ MİKTARI

Fotoğraflar: Dünya Gazetesi Fotoğraf Arşivi

Dijitalleşmeyle 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 alt yapıları 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. Bu yıl karşılaşılması öngörülen tehlikelere karşı kurumları uyaran Innovera Genel Müdürü Gökhan Say da hangi konularda önlem alınması gerektiğini sıralıyor.



1 YAPAY ZEKÂ

Henüz emekleme safhasında olsa da 2017'de başlayıp 2020'de hızlanan ve 2025 sonrası olgunlaşan bir yapay zeka 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*

2 NESNELERİN İNTERNETİ (IoT)

Dijital dönüşüm yolculuğunuzda Endüstri 4.0 varsa nesnelerin interneti ile yolunuz kesişecek demektir. Bu yıl 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.*

3 KİŞİSEL VERİLERİN GİZLİLİĞİ

Özellikle Avrupa Birliği bünyesinde alınan ve yeni 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 alt yapısına sahip olmalısınız.

Kritik sektörler: *Finans, bankacılık, perakende, sağlık.*

4 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.*

5 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.*

6 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.

Kritik sektörler: *Üretim, telekom, perakende, enerji.*

7 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.*

8 PHISHING 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 alt yapınızı koruyacak önlemleri devreye sokmalısınız.

Kritik sektörler: *E-posta iletişimi yoğun olan tüm sektörler.*

9 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.*

Ekonomiye zararı 600 milyar dolar

Diğer yandan McAfee, Stratejik ve Uluslararası Araştırmalar Merkezi (CSIS) iş birliğiyle hazırladığı, siber suçun dünyanın dört bir yanındaki ekonomiler üzerindeki dikkat çeken etkisini ele alan "Siber Suçun Ekonomik Etkisi – Azalma Yok" başlıklı küresel raporu yayımladı. İşlenen siber suçlarla şirketlere verilen toplam hasarın 600 milyar dolara ya da başka bir deyişle küresel gayrisafi hasılanın yüzde 0.8'ine yakın olduğunu ortaya koyan rapor, bu rakamın 2014 yılındaki araştırmada belirlenen 445 milyar dolarlık küresel zarardan kayda değer ölçüde yüksek olduğunu vurguluyor.

Üç yıl içinde gerçekleşen bu büyümenin sebebi ise raporda siber suçluların yeni teknolojilere hızla aya uydurması, bir dizi "siber suç merkezi" sayesinde bu tür suçları işlemenin kolaylaşması ve daha büyük ölçekli suçluların kullandığı finansal yöntemlerin her geçen gün daha karmaşık hâle gelmesi olarak açıklanıyor.

En yoğun eylemler Rusya Kuzey Kore ve İran'da

Bankaların siber suçlular için en yaygın hedef olmaya devam ettiğini belirleyen rapora göre bu alanda en tehlikeli suç kaynağı ise ulus devletler. Finansal kuruluşlara yönelik hack saldırılarında en yoğun eylemlerin Rusya, Kuzey Kore ve İran'da gerçekleştiği belirlenirken, Çin ise siber casusluk alanında en aktif konumda yer alıyor.

Hacker topluluklarının bu işteki uzmanlığı ve ülkenin genel olarak Batı ülkelerindeki kanunları reddetmesi gibi unsurlar sonucunda Rusya'nın siber suçta lider olduğunu bu araştırmayla gün yüzüne çıkardıklarını ifade eden CSIS Kıdemli Başkan Vekili James Lewis, "Kuzey Kore ise kendi rejimini fonlamak için gerçekleştirdiği kripto para hırsızlıkları neticesinde ikinci sırada yer alıyor. Üstelik artık 'siber suç merkezlerinin' sayısında artış görüyoruz ve buna sadece Kuzey Kore değil, Brezilya, Hindistan ve Vietnam gibi ülkeler de dahil" diye konuştu.