Siber gelecekte her yerde olacak!

Burak Sadıç
Siber Risk Danışmanlığı Lideri
Deloitte Türkiye

Fiziksel dünyanın sınırları her geçen gün daha da belirsizleşiyor. Siber dünya büyüdükçe yeryüzü küçülüyor.

Dördüncü sanayi devrimi ile değişim ve dijitalleşme heyecan verici bir hızla sürüyor. Bazı şirketler ve pazarlar yok olurken, yepyeni şirketler ve pazarlar ortaya çıkıyor. Hayatımıza giren teknolojiler sayesinde fiziksel dünyanın sınırları her geçen gün daha da belirsizleşiyor. Siber dünya büyüdükçe yeryüzü küçülüyor.

Sabah akıllı telefonumuzun alarmı ile uyanınca kaçımız daha yüzünü bile yıkamadan e-postalarını ve sosyal medya hesaplarını kontrol ediyor? Peki ya evden çıkmadan önce hava durumunu öğrenmek için pencereden dışarı mı bakıyoruz yoksa telefonumuzdaki bir uygulamaya mı? Sırada çevrim içi yol yardımı ile ofise gidecek en uygun rotayı bulmak var. Yola çıktıktan sonra önerilen rota üzerindeki kaza sebebiyle harita uygulaması bize yeni bir rota da öneriyor. Ofise gelince plaka tanıma uygulaması otoparkın kapısını açıyor, park ettikten sonra binaya girerken kameraya gülümsüyoruz ve binaya giriş yapıyoruz. Tam bu sırada kolumuzda bir titreşim, akıllı saatimiz bize toplantımızın hangi odada olduğunu hatırlatıyor. Oda kapısındaki tablette toplantı başlığını görüp emin olduktan sonra toplantı odasından içeri girip günlük mesaimize başlıyoruz. Bu sırada saatte bir titreşim daha. Bu sefer de çocuğunuzun akıllı saatinden gelen bir uyarı, çocuk evden çıkmış ve servisle okula doğru yol alıyor.

Sıradan bir gün başlangıcını anlatan bu kesit bile her yerde siber kavramını yaşamaya başladığımızın altını çizmeye yetiyor. Artık sadece kurumsal hayatta değil bireysel hayatımızda da siber teknolojiler yaşamımızın bir parçası oluyor ve onlara giderek daha da fazla bağlanıyoruz. Akıllı şehir yönetim sistemlerinde elektrik, doğalgaz, trafik ve su başta olmak üzere tüm şehir siber olarak yönetiliyor. Akıllı fabrikalar ve akıllı depolarda yakın bir gelecekte sadece makineler çalışacak. Gelecekte alışverişler de sanal asistanlar yardımıyla yapılacak.

Geçmişte sadece bilim kurgu filmlerinde gördüğümüz sahneler artık günlük hayatımızın değişmez parçaları haline geldi. Peki ya bu rüya kâbusa dönüşebilir mi? Siber kâbus dediğimizde bu kurumlar için neler ifade ediyor biraz açmamızda fayda var.

Siber güvenlik stratejisini hayata geçirmek için çizilecek yol haritasının üç tane temel bileşene sahip olması gerekiyor: Güvenli olmak, farkında olmak ve dirençli olmak.

Siber dünyada kurumları bekleyen riskler neler?

Birinci risk kurum sistemlerinin çalışmaz hale gelmesi. Tehdit altındaki sistemlere örnek olarak, e-posta sistemleri, sipariş takip sistemleri ile rezervasyon ve müşteri yönetimi sistemlerini gösterebiliriz. Sadece kurum bilgi teknolojileri değil, üretim teknolojileri de dâhil olmak üzere dijital bir bileşen içeren tüm sistemler bu riski taşıyor.

İkinci risk ise kurumların gizli bilgilerinin çalınması. Ticari sırlar, yatırım planları ya da kurum çalışanları ve müşterilerin kişisel bilgileri bu başlıkta ilk akla gelenler. Bu risk gerçekleştiğinde sadece rekabet avantajının kaybedilmesi ya da kurum itibarının zedelenmesi değil kişisel verilerin korunması kanunu gibi kanunların cezai yaptırımları da söz konusu.

Üçüncü ve son risk de geçtiğimiz yıllarda birçok banka ile kripto para borsasının başına geldiği gibi, kurumlardan paranın direkt olarak çalınması. Kurum çalışanlarının kandırılarak sahte hesaplara para transfer ettirilmesi veya fidye yazılımları aracılığıyla şantaj yapılması da bu alana örnek olarak gösterilebilir.

Tüm sistemlerin çalışmaz hale gelmesi ve amaçları dışında kullanılması ya da kurumsal sırlarımız ve sanal dünyayla paylaştığımız kişisel bilgilerimizin açığa çıkması kulağa korkutucu geliyor. Bu senaryoların gerçekleşmemesi ya da gerçekleştikleri durumların en az kayıpla atlatılması da hayati önem taşıyor.

Kurumlar bu risklerle başa çıkabilmek için ne yapmalı?

Kurumların ilk yapması gereken siber güvenlik alanında bir sorumlu atamak. Bu sorumlunun ilk işi ise kurum stratejileri ve öncelikleri ile örtüşen bir siber güvenlik stratejisi oluşturmak olmalı.

Siber güvenlik stratejisini hayata geçirmek için çizilecek yol haritasının üç tane temel bileşene sahip olması gerekiyor: Güvenli olmak, farkında olmak ve dirençli olmak.

İlk bileşen olan güvenli olmayı, kurumların siber risklere karşı alacakları önlemler ile kendilerini koruma altına almaları olarak özetleyebiliriz. Nasıl evimizin pencerelerini ve kapısını kapatıp kilitliyorsak, siber alanda da bazı temel önlemleri muhakkak almalıyız. Bu koruyucu önlemler de sadece teknoloji çözümleri olarak düşünülmemeli ve dengeli bir insan-süreç-teknoloji üçgeni oluşturarak devreye alınmalıdır.

İkinci bileşen de farkında olmak. Aldığımız tüm güvenlik önlemlerine rağmen saldırganlar savunmalarımızı aşabilir ya da bir çalışanımızın hatası sonucunda beklenmedik bir problemle karşılaşabiliriz. Saldırıları ve problemleri mümkün olan en kısa zamanda tespit etmek kurumlar için hayati önem taşımaktadır. Siber olayları bir yangına benzetirsek, ne kadar erken tespit edilirse o kadar çabuk söndürülür ve o kadar az zarar verir.

Üçüncü ve son bileşen ise dirençli olmak. Güvenlik seviyesinden bağımsız olarak her kurum bir gün kritik bir güvenlik olayı yaşayacak ve farkındalığı ne kadar yüksek olursa olsun bu olay kuruma belli bir zarar verecektir. Kurumların siber olaylara karşı dirençli olması, siber olay sırasında kurumsal süreçlerin olabildiğince az kesintiye uğraması ve olay sonrasında da en doğru zamanda operasyonların normal seyrine dönmesi kurumsal süreklilik açısından çok önemlidir.

Yeni bir çağın başlangıcındayız

Sadece bireyler ve kurumlar değil, her şeyin birbiriyle bağlantılı olduğu bu çağda değişimin asla hız kesmemesi için sürekli desteklenmesi gerekiyor. Büyük dönüşümlerin yaşandığı bu çağın en önemli gereksinimlerinden birisi de siber kavramına sadece bir risk yönetimi, teknoloji ya da uyumluluk problemli olarak değil, bütün bu dönüşümlerin anahtarı olarak bakmaktır.

Güvenli olmanız, farkında olmanız ve dirençli olmanız dileğiyle...

Büyük dönüşümlerin yaşandığı bu çağın en önemli gereksinimlerinden birisi de siber kavramına sadece bir risk yönetimi, teknoloji ya da uyumluluk problemli olarak değil, bütün bu dönüşümlerin anahtarı olarak bakmaktır.