**BASIN BÜLTENİ**

**Dijitalleşme ile birlikte şirketleri tehdit eden sekiz siber risk**

**Şirketlerin yeni iş fırsatları elde etmek ve pazardaki rekabetçi güçlerini arttırmak amacıyla teknolojik dönüşümlerini hızlandırması, yeni ve beklenmedik siber riskleri de beraberinde getiriyor. Aon’un, hızla dijitalleşen şirketlerin karşı karşıya kalabileceği sekiz farklı alandaki riskleri inceleyen 2019 Siber Güvenlik Risk Raporu, şirketlere teknolojinin kazanımlarından faydalanırken siber risklere karşı hazırlıklı olmalarını tavsiye ediyor.**

Risk, emeklilik ve sağlık konularında veri ve analitiğinden faydalanarak profesyonel hizmetler sunan Aon’un “2019 Siber Güvenlik Risk Raporu” yayınlandı. Aon’un Siber Risk Çözümleri Birimi, 2019’da dijitalleşme sürecindeki şirketlerin karşı karşıya kalması muhtemel olan sekiz risk alanına odaklanıyor. Bu riskler; teknoloji, tedarik zinciri, nesnelerin interneti, iş faaliyetleri, çalışanlar, şirket birleşmeleri ve satın almalar, yasal düzenlemeler ve yönetim kurulu başlıkları altında inceleniyor.

İşletmeler, her geçen gün iş yapış şekillerini değiştirerek maliyetlerini düşürmek, verimliliklerini artırmak, hızlanmak ve müşterileriyle daha etkin bir şekilde etkileşime geçerek rakiplerinin önüne geçmelerini sağlayacak dijital teknolojilere ve veri tabanlı sistemlere daha fazla yatırım yapıyorlar. Bütün bu gelişmeler potansiyel siber saldırı alanını hızla genişletiyor ve kurumlar için daha önce geçerli olmayan yeni riskler oluşturuyor. Siber suçlular da, eş zamanlı olarak yetkinliklerini daha ileri seviyelere taşımaya devam ediyor. Özellikle organize suç örgütleri ve devlet destekli siber saldırıların sıklıkları artıyor ve kapsamları genişliyor.

Şirketleri etkileyebilecek siber tehditler, şirketlerin faaliyet gösterdiği sektöre, büyüklüklerine ve bağlı oldukları bölgeye göre değişkenlik gösteriyor. Aon, bu anlamda, şirketlerin, maruz kaldıkları siber riskleri doğru analiz etmeleri gerektiğini savunuyor ve bunları proaktif bir temelde ele almalarını öneriyor.

Raporun bulgularını değerlendiren Aon Türkiye Eş CEO’su Selda Oknas şunları söyledi: “2018’de dünya genelinde proaktif bir yaklaşımla siber saldırı riskini azaltacak önleyici tedbirlere yatırım yapan şirketlerin kazançlı çıktığını görüyoruz. 2019’da dijitalleşen dünyada oluşan büyük fırsatlar büyük riskleri de beraberinde getiriyor ve bu nedenle siber risklere karşı tedbir alma ihtiyacının katlanarak artacağını öngörüyoruz. Teknoloji ve dijital dönüşümün sunduğu fırsatlardan yararlanırken, şirketleri siber saldırılara karşı koruyacak tedbirleri de eş zamanlı olarak hayata geçirmelerini yönetim kadrolarına tavsiye ediyoruz. Aon’un 2019 Siber Riskler Raporu, kurumların özellikle tehdit istihbaratı paylaşımına destek vermelerinin önemini ortaya koyuyor. Farklı sektörler ve kurumlar arasındaki siber güvenlik dayanışması, şirketlerin en değerli varlıklarının başında yer alan dijital bilgilerin güvenliğinin sağlanmasına önemli katkıda bulunacaktır.”

**Kurumlar teknolojinin kazanımlarından faydalanırken siber riskleri unutmamalı**

Aon her yıl kurumları tehdit eden kritik siber güvenlik risklerini inceliyor ve bu analizlerin sonucunda siber saldırıların kapsamının genişlediğini ve etkilerinin yoğunlaştığını gözlemliyor. Aon’un Siber Güvenlik Risk Raporu ise, şirketlerin dijital dönüşüm seviyelerindeki hızlı yükseliş, teknolojideki hızlı gelişmeler ve sürekli evrilen risk ortamı sebebiyle, siber saldırganların kurum içine sızabileceği temas noktalarının her geçen gün arttığının altını çiziyor.

Aon’un raporunda öne çıkan tespitler şöyle:

**Teknoloji:** Bugüne kadar fiziki ofisler ve mağazalar vasıtasıyla müşterilerine ulaşan geleneksel şirketlerin bulut bilişim vasıtasıyla hızla dijital ekonominin XaaS servis sağlayıcılarına dönüşmesi, onları yeni ve potansiyel olarak henüz bilinmeyen risklerle karşı karşıya bırakıyor. Teknolojinin daha yoğun ve geniş kapsamda kullanılması şirketlerin iş yapış biçimlerinde köklü değişikliklere neden oluyor ve siber saldırılara yönelik yeni zafiyetler yaratıyor. Şirketler, bu yeniliklerin farklı riskleri beraberinde getirebileceğinin farkında olmalı ve dijital dönüşüm süreçleri devam ederken bu riskleri yönetebilmelidir.

**Tedarik zinciri:** Tedarik zinciri tarafında yaygın görülen iki eğilimin, önümüzdeki yıllarda siber risklerin bariz biçimde artmasına neden olabileceği öngörülüyor. Bunlardan biri, mobil ya da nesnelerin interneti özellikli yeni nesil cihazlar vasıtasıyla bulut ortamlarına genişleyen ve siber saldırı riskine maruz operasyonel verilerin hızla artması olarak kabul ediliyor. İkincisi ise, şirketlerin her geçen gün daha fazla bel bağladığı üçüncü ve hatta dördüncü taraf tedarikçilerin ve hizmet sağlayıcılarının, siber saldırganların şirketlerin tedarik zincirine ulaşabilecekleri yeni arka kapılar sunması olarak öne çıkıyor. Ponemon Institute’un 2018 yılında yaptığı bir araştırma, ABD ve İngiltere’deki şirketlerin yüzde 59’u üçüncü taraf aracılığıyla en az bir kez veri ihlaline maruz kaldıklarını belirtirken, yalnızca yüzde 35’i üçüncü taraf risk yönetimi programlarının yeterli olduğunu düşünüyor.

**Nesnelerin interneti:** Günümüzde artık yaşamın her alanına dahil olan nesnelerin interneti cihazları potansiyel bir güvenlik riski teşkil ediyor. Pek çok şirketin, işlerini yürütürken kullandığı ağ bağlantılı nesnelerin interneti cihazlarının (konferans sistemleri, güvenlik kameraları, yazıcılar, bina otomasyon sistemleri, vb.) sayısı şirketlerin yönetimindeki bilişim teknolojileri varlıklarının sayısını aşabiliyor. Öyle ki, 2018 Ponemon Institute anketine göre, şirketlerin yüzde 52'si 1000 adet cihazın yer aldığı bir nesnelerin interneti envanterini yönettiğini söylerken, çalışmanın sonucunda ortalama 15 binin üzerinde nesnelerin interneti cihazının kullanıldığı ortaya çıktı. Yani, şirketler nesnelerin interneti cihazlarının tamamını güvenli bir şekilde yönetemiyor, hatta bu cihazların envanter kaydını dahi tutmuyor. Bu da şirketlerin veri ihlaline uğramasına neden oluyor.

**İş faaliyetleri:** Endüstriyel kontrol sistemleri ve kritik kamu hizmetleri altyapıları geleneksel anlamda bağımsız ağlar olarak işletilmekle birlikte her geçen gün bu sistem ve altyapıların büyük bir kısmı internete bağlanmakta ve geleneksel Bilişim Teknolojileri ortamlarına entegre olmaktadır. Bu durum operasyonel verimliliği artırırken potansiyel siber saldırı alanını da genişletmekte ve saldırganlar için şirketin BT ağının tamamına ulaşabilmeyi kolaylaştırarak iş durması riskini artırmaktadır. Öte yandan, yetersiz olan yedekleme süreçleri de siber saldırıların, kurumların iş faaliyetleri üzerindeki etkisinin daha şiddetli olmasına yol açıyor.Kurumların, WannaCry saldırısının 230 bin bilgisayarı etkisiz hale getirdiği ve tüm dünyada büyük bir kaosa sebep olduğunu unutmadan, siber saldırıların potansiyel etkilerinin farkında olmaları ve iş sürekliliğini sağlayacak gerekli tedbirleri almaları önem arz ediyor.

**Çalışanlar:** Gerek kötü niyetli olsun, gerekse ihmal sebepli olsun**,** çalışanlar, veri ihlali vakalarının en yaygın nedenlerinden biri olmaya devam ediyor. Aon’un anketine göre, katılımcıların yüzde 53’ü 2018 yılında şirketlerinin içeriden kaynaklı bir siber saldırı yaşadığını söyledi. Çalışanlar, çalıştıkları kurumun siber güvenliği için büyük bir tehdit oluşturduklarının çoğu kez farkında olmayabiliyor. Kurumların, kurum içi siber güvenlik risklerini azaltmak için kapsamlı bir yaklaşım geliştirmeleri gerekiyor. Bu doğrultuda, güçlü veri yönetimi, kurum genelinde siber güvenlik politikalarının iletişimin yapılması, etkin erişim ve veri koruma kontrollerinin uygulanması gerekiyor.

**Şirket birleşmeleri ve satın almalar:** IMAA Institute’un verilerine göre, 2018’de şirket birleşmeleri ve satın almaların tüm dünyada toplam değerinin 4 trilyon dolara ulaştığı düşünülüyor. Birleşme ve satın almalar artarken siber güvenlik riskleri de hızla artıyor. Siber saldırganlar, sıklıkla daha büyük firmalar tarafından satın alınma sürecinde olan firmaları hedefliyor. Yeni bir birleşme veya satın alma sürecinde, anlaşma tamamlanmadan önce meydana gelebilecek bir siber saldırı, satın alma fiyatını ciddi oranda düşürebiliyor.
Satın alan şirketin kendi kurumsal siber güvenlik yaklaşımları ne kadar güçlü ve sorunsuz olsa da, özellikle satın alınacak ya da birleşilecek hedef şirketin aynı şekilde siber güvenlik önceliklerini yerine getirdiğinden emin olması gerekiyor.

**Yasal düzenleme:** Özellikle 2018’de tüm dünyada siber güvenlikle ilgili çeşitli yasal düzenlemeler yürürlüğe girdi. Buna bağlı olarak şirketlerin yasal düzenlemelere uyum riskinin 2019’da daha dikkatli bir şekilde değerlendirmesi ve gerekli tedbirleri alması gerekiyor.2018 mayıs ayında yürürlüğe giren ve Avrupa Birliği üyesi ülkelerde uygulanmaya başlanan GDPR (Avrupa Birliği Genel Veri Koruma Yönetmeliği), ihlali durumunda, siber güvenlikle ilgili olarak 20 milyon Euro’ya ya da bir kuruluşun yıllık global cirosunun yüzde 4’üne varan ciddi yaptırımları da beraberinde getiriyor.Öyle ki, 2018’deki çok büyük veri ihlallerinin sorumlusu olan şirketlerin GDPR kapsamındaki ihlallerinin netleşmesi durumunda şirket başına 500 milyon dolar ile 1 milyar doların üzerinde bir para cezası alabileceği tahmin ediliyor.

**Yönetim Kurulu:** Siber güvenlik yönetimi, yönetim kurulları için önemli bir gündem maddesi olmaya devam ediyor. Ancak yakın geçmişe bakıldığında, yönetim kurulu üyeleri, siber yönetimle ilgili artan kişisel sorumluluk riskiyle de karşı karşıya kalıyor. Hissedarların, yüksek profilli veri ihlallerinden bazılarında yöneticilere karşı tazminat talebinde bulunduğu gözleniyor. Yönetim kurulu üyelerinin, siber güvenlikle ilgili daha kararlı bir tutum sergileyerek, hem siber güvenlik yönetimiyle ilgili alınan aksiyonlar, hem de proaktif tedbirler konusunda tüm şirkete bu anlamda da önderlik etmesi büyük önem arz ediyor.Aon’un raporu, 2018 yılında BDO Center for Corporate Governance and Financial Reporting tarafından yapılan bir araştırmaya katılan yönetim kurulu üyelerinin dörtte üçünün bir yıl öncesine göre siber güvenliğe daha fazla dahil olduğunu ortaya koyuyor.

**İlgili Kişi**

Ayşe Ekin Gündüz

Marjinal Porter Novelli

0212 219 29 71 - 0533 921 43 53

ayseg@marjinal.com.tr

**Aon Türkiye hakkında**

Aon Türkiye, dünya çapında 120 ülkede 50.000 çalışanıyla risk, emeklilik ve sağlık alanlarında veri ve analitiğin desteği ile profesyonel hizmetler sunan Aon Corporation’ın Türkiye’deki şirketidir ve 1995 yılında kurulmuştur. Aon Türkiye, sigorta ve reasürans brokerliği ile risk yönetimi danışmanlığı konularında Türkiye’de faaliyet gösteren bir kuruluştur. <http://www.aon.com/turkey/tr/>