**BASIN BÜLTENİ**

**Aon uyarıyor: “Milyon dolarlık siber dolandırıcılık Türkiye’yi de vurabilir”**

**FBI’ın yayınladığı son Siber Suç Raporu sanal ortamda dolandırıcılık sonucu 1,4 milyar dolarlık kayıp yaşandığını tespit ediyor. Rapor, Aon’un global risk öngörülerini doğrular nitelikte çarpıcı veriler ortaya koyuyor. Aon Türkiye Eş CEO’su Selda Oknas’a göre bu veriler, Türkiye’yi bekleyen ciddi siber dolandırıcılık suçları için bir uyarı olarak değerlendirilmeli.**

Şirketlerin itibarlarını alt üst ederek, bilançolarında önemli kayıplar yaratan siber saldırılar tüm dünyanın yakın takibinde. Risk, emeklilik ve sağlık konularında profesyonel hizmetler sunan Aon’un iki yılda bir iş ortaklarıyla paylaştığı Global Risk Yönetimi Anketinde, şirketlerin varlıklarını tehdit eden siber riskler, hem 2017 verilerinde hem de 2020 öngörülerinde ilk 5 risk arasında yer alıyor. Aon’un araştırmalarında, siber risklerin, FBI bulguları ile paralel olarak, Kuzey Amerika ekonomilerinde bir numaralı risk olarak algılandığı görülüyor.

**Bölgelere göre dünya çapında ilk 10 risk**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Asya Pasifik** | **Avrupa** | **Latin Amerika** | **Orta Doğu ve Afrika** | **Kuzey Amerika** |  |
| **1** | Marka imajı ve itibarının zedelenmesi | Ekonomik yavaşlama | Marka imajı ve itibarının zedelenmesi | Ekonomik yavaşlama | Siber riskler |
| **2** | Yasal düzenlemeler | Marka imajı ve itibarının zedelenmesi | İş kesintisi | Yurt dışı politik riskler | Marka imajı ve itibarının zedelenmesi |
| **3** | Artan rekabet | Artan rekabet | Ekonomik yavaşlama | İnovasyon çalışmalarının başarıya ulaşmaması | Yetenekli çalışanı elinde tutamama/kuruma çekememe |
| **4** | İnovasyon çalışmalarının başarıya ulaşmaması | Yasal düzenlemeler | Üçüncü şahıs sorumluluğu | Yetenekli çalışanı elinde tutamama/kuruma çekememe | Yasal düzenlemeler |
| **5** | Ekonomik yavaşlama | İnovasyon çalışmalarının başarıya ulaşmaması | Kurumsal sosyal sorumluluk / sürdürülebilirlik | Marka imajı ve itibarının zedelenmesi | Ekonomik yavaşlama |
| **6** | İş kesintisi | Siber riskler | Yurt dışı politik riskler | Yasal düzenlemeler | İnovasyon çalışmalarının başarıya ulaşmaması |
| **7** | Siber riskler | Ticari malların fiyat risk | Yasal düzenlemeler | Artan rekabet | Artan rekabet |
| **8** | Yetenekli çalışanı elinde tutamama/kuruma çekememe | Karşı taraf kredi riski | Döviz kuru dalgalanması | Siber riskler | İş kesintisi |
| **9** | Önemli, büyük projede başarısızlık | İş kesintisi | Çevresel risk | Döviz kuru dalgalanması | Hava/ doğal felaketler |
| **10** | Yurtdışı politik riskler | Direktörler & çalışanların kişisel yükümlülükleri | Nakit akışı/ likidite riski | Direktörler & çalışanların kişisel yükümlülükleri | Mala yönelik hasar |

Aon Türkiye’nin Temmuz 2018’de yaptığı Türkiye Risk Yönetimi Araştırmasında siber riskler 12. sırada yer almıştı. Siber risklerin 2018 yılı içerisinde dünyanın gelişmiş ekonomilerine göreceli olarak Türkiye’nin risk odağında daha alt sıralara düştüğü görülüyor. Aon Türkiye Eş CEO’su Selda Oknas konuyla ilgili şunları söyledi: “Dijital Dönüşüm Türkiye’de de pek çok CEO’nun öncelikli ajandasında olduğunu gözlemliyoruz, dolayısıyla siber risklerin sıralamadaki yerinin Türkiye’de yükseleceğini beklemekteyiz.”

**Siber risklerle mücadelede en güçlü silah: Veriye dayalı öngörüler**

Siber suçların önümüzdeki yirmi yılda şirketlerin karşı karşıya kalacağı en büyük sorunlardan biri olacağını belirten Aon Türkiye Eş CEO’su Selda Oknas, şunları söyledi: “Siber tehditler karşısında, veri ve analitiğe dayalı öngörüler şirketlerin en güçlü silahı olacak. Biz Aon olarak şirketlere bu zorlu mücadelede rehberlik etmek için iki yılda bir Global Risk Yönetimi Anketi’ni iş ortaklarımızla paylaşıyor, sektöre ışık tutacak risk öngörülerini onlardan dinliyoruz. Bu anket, Türkiye sonuçlarını küresel sonuçlarla beraber görme imkânı da sağlıyor. Örneğin, dünyanın önde gelen firmalarından oluşan 1800’ü aşkın firmalara incelendiğinde, her iki firmadan birinin siber risk değerlendirmesi yaptığı (yüzde 53), her üç firmadan birinin de siber poliçe ile teknoloji risklerini teminat altına aldığı (yüzde 33) görülüyor. Bu istatistiklerin düzenli bir şekilde yükseldiğini gözlemliyoruz. Karşılaştırmalı sonuçlara göre formal bir siber risk değerlendirmesinin yapıldığı sektörler arasında, sigortacılık, bankacılık ve eğitim sektörleri önde geliyor (Bu sektörlerin her birinde, siber risk değerlendirme yapanların yapmayanlara oranı yüzde 70 ya da daha yukarıda). Sağlık sektörünün yüzde 57’si, telekomünikasyon sektörünün yüzde 50’si, perakende sektörünün ise yüzde 47’i siber risklerin kendilerine nasıl zarar vereceğini değerlendirmiş. Buna karşılık inşaat, çimento, plastik, kauçuk ve toptan ticaret sektörlerinin siber risk değerlendirmesinde geriden geldikleri görülüyor (Bu sektörlerin her birinde, siber risk değerlendirme yapanların yapmayanlara oranı yüzde 40 ya da daha düşük).”

**Siber riskler Türkiye için de ciddi bir tehdit**

Türkiye’de inovasyon, dijital dönüşüm ve Endüstri 4.0 konularındaki yoğun çalışmalara değinen Selda Oknas, şöyle devam etti: “Bu dönüşüm süreçleri esnasında firmalar kendilerini yeni risklere açtıklarından gerekli önlemleri şimdiden almaları tedbirli olacaktır. Dünyanın ileri gelen firmalarında çalışan üst düzey yöneticiler ‘siber risklerin ölçülmesini’ sadece BT departmanlarına bırakmıyorlar. Firmaların yüzde 38’inde Risk Yönetimi departmanının, yüzde 19’unda ise Hukuk ve Uyum departmanlarının siber risk değerlendirmesine katıldığını görüyoruz. Bölgeler bazında Kuzey Amerika (yüzde 46) ve Asya Pasifik’teki (yüzde 55) firmaların Risk Yönetimi bölümleri siber riskler konusunda aktif olarak çalışıyorlar. Siber riskler, küresel bazda hem 2017 sonuçlarında hem de 2020 öngörülerinde ilk 5 riskten biri olarak değerlendirilirken, Aon Türkiye 2018 Risk Yönetim Anketi’ne katılan Türk yöneticilerin öngördüğü ilk 10 risk arasında yer almıyor. Bu durum, ülkemizde siber suçlara ilişkin farkındalığın ve/veya önceliğin halen istenilen düzeyde olmadığını gösteriyor. FBI’ın Siber Suç Raporu, siber saldırıların ulaştığı ciddi boyutun bir sinyali. Bu tür suç trendlerinin öncelikle ABD’de başladığını, zaman içerisinde Avrupa ve Türkiye’ye yayıldığını gözlemliyoruz. Bu rakamların hepimiz için bir uyarı niteliği taşıdığını düşünüyorum.”

**17 yılda 4 milyon şikâyet**

Siber tehlikelerin analizi için yeterli bilgi havuzunun oluşturulması siber suçlarla mücadelede kilit rol oynuyor. Bu amaçla 2000 yılında Amerikan Federal Polisi FBI’a bağlı olarak kurulan İnternet Suçları Şikâyet Merkezi (IC3) topladığı siber istihbaratı, kamuoyunda farkındalığı artırmaktan uluslararası operasyonlarda işlevsel hale getirmeye kadar birçok alanda kullanılmak üzere ilgili devlet kurumlarıyla paylaşıyor. Amerikan Federal Polisi FBI’ın yayınladığı İnternet Suç Raporu, FBI’a bağlı İnternet Suçları Şikâyet Merkezi (IC3)’ne, 2017 yılında siber saldırganların faaliyetlerinden etkilenen kişi ve/veya kurumdan gelen **301 bin 580** şikâyet sonucunda**1,4 milyar dolarlık** bir maddi kayıp meydana geldiğini ortaya koyuyor. Kurulduğu 2000 yılından 2017 yılına kadar ise IC3’ye toplamda **4 milyon** şikâyet başvurusu yapılmış. 17 yılda 4 milyon şikâyet bildirimine sebep olan siber suçların önlenebilmesi için saldırıya uğrayan kişi ve/veya kurumların bildirimde bulunması kritik önem arz ediyor.

**Siber suçlarla mücadelede anahtar kelime işbirliği**

Türkiye’de de Emniyet Genel Müdürlüğü bünyesinde faaliyet gösteren Siber Suçlarla Mücadele Daire Başkanlığı siber suçlarla mücadele çalışmalarını sürdürüyor. Selda Oknas, siber suçlarla etkin mücadelede bu tür kurumlarla işbirliğinin önemini vurgulayarak şunları söyledi: “Firmalar başlarına bir saldırı geldiği zaman, itibar kaybı riskini göz önüne alarak çoğu kez bunu gizli tutmayı tercih ediyor. Ancak, durum ne olursa olsun, mutlaka yasal merciler devreye sokulmalı. En azından siber@egm.gov.tr adresine gönderilecek bir e-posta ile Emniyet Genel Müdürlüğü haberdar edilmeli. Saldırı sonrası adli analiz de önemli bir konu. Saldırı sonrasında iş kesintisi endişesine düşen yöneticiler hem delil olarak hem de daha sonraki saldırıları önlemek için kullanılabilecek bulguları toplamayı ihmal edebiliyor. Halbuki siber saldırı sonucu ortaya çıkacak maliyetler sigortalanabilir maliyetler ve uzun vadede siber direncin artmasını sağlayacak önemli bir konu.”

**Türkiye’de siber saldırı endişesi Anadolu’da daha yaygın**

Selda Oknas, Türkiye’nin siber riskler karşısındaki durumu hakkında da önemli paylaşımlarda bulundu. Oknas, “Aon Türkiye bünyesinde yaptığımız bir araştırmada, Google Trends verilerini kullanarak il bazında siber vaka dağılımını inceledik. Elde ettiğimiz veriler sorunun veya endişenin sadece İstanbul, Ankara, İzmir gibi büyük metropollerle sınırlı kalmadığını bize gösterdi. Gelişmiş metropoller ve şehirlerin yanı sıra, Anadolu ve Doğu Anadolu'daki şehirlerimizde de siber saldırı kuşkusu ile sık sık internetten ‘siber ihbar’ araması yapıldığı ortaya çıkıyor. Bu kelimelerle yapılan Google arama verileri sıralamasında, Sivas, Kahramanmaraş, Konya, Kayseri, Elâzığ ve Samsun’un 7. sıradaki İstanbul’dan daha üst sıralarda yer alıyor olması tehlikenin ülkemiz coğrafyasına ne kadar yayıldığını gözler önüne seriyor. Bu veriler bize siber tehlikelere karşı ivedilikle önlem almaya ihtiyaç duyulduğunu gösteriyor” dedi.



**E-posta dolandırıcılığından 676 milyon dolarlık vurgun**

FBI raporunda, 2017 yılında gerçekleştirilen siber suçlar arasında e-posta hesabının kötüye kullanılması yoluyla yapılan siber dolandırıcılık öne çıkıyor. Siber saldırganlar, bu yöntemi kullanarak 2017 yılında 676 milyon dolar kazanç elde etmiş. En büyük maddi kayba yol açan diğer iki siber dolandırıcılık ise; 211 milyon dolar zarara sebep olan “güveni kötüye kullanma ve romantik ilişki yoluyla dolandırıcılık” ile 141 milyon dolar zarar yol açan teslimat/tahsilat dolandırıcılığı.

**Bankacılık sektörü kullanılıyor**

FBI’ın raporu siber ortamda bankacılık ve finansal aldatmaca yoluyla gerçekleştirilen siber saldırılara da dikkat çekiyor. Raporda, 2015’te siber ortamda kendilerini banka çalışanı gibi tanıtan kötü niyetli kişilerin yatırım amaçlı olarak 7 milyon dolar topladığı hatırlatılıyor. Aon Stroz Friedberg uzmanları da, bankacılık sektörüne yapılan saldırıların bir trend oluşturduğunu ve bu trendin 2015’ten beri sürdüğünü paylaşıyor. 2015’ten bugüne kadar dünya genelinde bankacılık sektörüne yapılan siber saldırıların yarattığı toplam kaybın ise en az **200 milyon dolar** olduğu belirtiliyor.

**İlgili Kişi**

Ayşe Ekin Gündüz

Marjinal Porter Novelli

0212 219 29 71 - 0533 921 43 53

ayseg@marjinal.com.tr

**Aon Türkiye hakkında**

Aon sahip olduğu veriye dayalı analitik yetkinlikler sayesinde geniş yelpazede risk, emeklilik ve sağlık çözümleri sunan, konusunda küresel liderliğe ulaşmış profesyonel hizmetler şirketidir.120 ülkedeki 50.000 çalışanı ile veri ve analitiğin desteğiyle finansal kırılganlığın azaltılması ve performansın iyileştirilmesine yönelik öngörüler sağlayarak müşterilerin güçlü sonuçlar elde etmesine yardımcı olan Aon Türkiye, sigorta ve reasürans brokerliği ile risk yönetimi danışmanlığı konularında Türkiye’de faaliyet gösteren bir kuruluştur. İngiltere’nin Manchester United ve İtalya’nın Parma Calcio futbol takımlarının sponsorudur. <http://www.aon.com/turkey/tr/>