MARSH TÜRKİYE VE TÜSİAD İŞ BİRLİĞİ İLE TÜRKİYE'DE İLK KEZ GERÇEKLEŞTİRİLEN 'TÜRKİYE SİBER RİSK ALGI ARAŞTIRMASI'NIN SONUÇLARI AÇIKLANDI…

FİRMALARIN YÜZDE 78'İ SİBER SALDIRI OLMADAN HAREKETE GEÇMİYOR

Marsh ve TÜSİAD iş birliği ile gerçekleştirilen '2020 Türkiye Siber Risk Algı Araştırması'nın sonuçları düzenlenen webinarla açıklandı. Araştırma, Türkiye'de siber riskler konusunda yapılan ilk ve en kapsamlı araştırma olma özelliği taşıyor. Araştırma sonuçlarına göre; firmaların siber riskleri diğer risk başlıkları gibi önemsemeleri ve yönetmeleri gerektiğine ilişkin farkındalık seviyesi hızla artıyor. Buna karşın, siber güvenliğe yönelik farkındalık ve yatırım, büyük ölçüde siber saldırı deneyimi ve hukuki düzenlemelerle tetikleniyor.

Firmaların yüzde 78'i bir tehditle karşılaşmadan siber riski fark etme ve harekete geçme pratiğine sahip değilken, yaşanan saldırının etki gücünün de öngörülenden daha yüksek olduğu görülüyor. Siber ataklar sebebiyle işlerinde yavaşlama, durma veya finansal zarar yaşamayan şirketler ise siber güvenlik riskini gözden kaçırma eğiliminde.

Marsh Türkiye ile TÜSİAD iş birliğinde gerçekleştirilen '2020 Türkiye Siber Risk Algı Araştırması'nın sonuçları açıklandı. Düzenlenen webinarla açıklanan araştırmanın sonuçlarına göre; Türkiye'de, bu alandaki risklerin yönetimi veya bilgi teknolojilerinden sorumlu çalışanların sadece yüzde 9'u şirketlerinin karşı karşıya olduğu en büyük riski siber tehdit olarak görüyor. Geçtiğimiz yıl Marsh'ın global çapta gerçekleştirdiği 'Siber Risk Algı Araştırması'nda ise bu oran yüzde 22 idi.

'2020 Türkiye Siber Risk Algı Araştırması', Türkiye'deki firma ve kurumların siber risklere ve bilgi güvenliğine yönelik farkındalıklarını, tedbir alma reflekslerini ortaya koymak, bu alandaki yatırımlarını, ihtiyaçlarını ve beklentilerini anlamak üzere gerçekleştirildi. Çalışma kapsamında firmaların siber risk yönetim sürecinden sorumlu üst ve orta kademe yöneticileri ve uzmanlarının değerlendirmeleri alındı.

Araştırma, siber riskler konusunda ülkemizde farkındalığın arttığına işaret etse de şirketlerin gün geçtikçe artan bu riski öncelikleri arasına yeterince almadığını ortaya koyuyor.

Siber yatırım, siber saldırının ardından geliyor

Araştırmanın sonuçlarına göre; siber güvenliğe yönelik farkındalık ve yatırım büyük ölçüde siber saldırı deneyimi ve hukuki düzenlemelerle tetikleniyor. Firmaların bu konudaki genel eğilimi 'bekle-gör' davranışı üzerinden şekilleniyor. Firmaların yüzde 78'inin tehditle karşılaşmadan siber riski fark etme ve harekete geçme pratiğine sahip olmadıkları, yaşanan saldırının etki gücünün öngörüden daha yüksek olduğu gözüküyor. Yaşanan siber atakların, bugüne kadar, işlerin yavaşlaması, durması veya finansal zarara sebebiyet verebilecek bir vaka yaşatmamış olması, siber güvenlik konusunun daha az gündemde olmasının temel nedeni olarak görülüyor.

Siber güvenlik yönetimine yatırım yapan firmaların yüzde 77'si hukuki düzenlemelerin teşvik edici etkisi olduğunu belirtiyor. Havacılık, finans, bilgi teknolojileri, enerji ve üretim sektörlerinde yer alan firmaların siber riskin yönetimi konusunda nispeten daha hassas davrandıkları ve bilgili oldukları ortaya çıkıyor. Devletin yasayla çerçevesini çizdiği, takip ettiği konular firmalar tarafından hem daha çok dikkate alınıyor hem daha çabuk içselleştiriliyor ve prosedürlere geçiriliyor. Bu bağlamda KVKK, GDPR gibi kanunlar; ISO, NIST gibi standartlar; EPDK, BDDK gibi sektör denetleme kurumları; halka açılma süreçlerinden geçen kurumlar için SPK tarafından belirlenen zorunluluklar şirketlerin siber risk konusunda harekete geçmeyi etkiliyor ve yol gösterici oluyor.

COVID-19 ve hızla devam eden dijital dönüşüm, riski de artırdı

Araştırmanın sonuçlarına göre; COVID-19 salgınının etkisiyle her alanda hızlanan dijital dönüşümün hem farkındalığı arttıracağı hem de kurumları siber risk yönetimine yönelik daha fazla önlem almaya teşvik edeceği öngörülüyor. COVID-19 salgını süreci ile birçok firmanın tam olarak hazır olmadan ve gerekli tedbirleri alamadan hızlı bir şekilde dijitalleşmesi siber saldırı olasılıklarını da yükseltiyor.

Yetkin ve yeterli insan kaynağı açığı en önemli konulardan biri

Araştırmanın sonuçlarına göre; firmaların yüzde 77'sinde siber risk konusundaki sorumluluk IT/BT ekiplerinin üzerinde. Firmaların yüzde 75'inde siber güvenlik sorumluluğu büyüklük ve sektörel yapıya göre CTO/CIO/CSO/CICO pozisyonlarından biriyle paylaşılıyor. Bir başka deyişle, süreci C seviyesi yönetiyor. Özellikle bu seviyedeki yöneticilerin konuya yaklaşımları kurumun farkındalığını ve stratejisini doğrudan etkiliyor. Firmaların yatırım kararı için en önemli dayanak noktası, yine sektördeki firmaların yaşadığı olumsuz deneyimler oluyor. Firmaların yüzde 56'sı ise, doğru bir strateji kurabilmek için tarafsız bir kurumdan danışmanlık alıyor.

Araştırmaya göre; firmaların yüzde 78'inin risk yönetimi konusundaki öncelikli refleksi riski azaltıcı uygulamaları hayata geçirmek yönünde. Firmalar en çok cihazların güvenliğini arttırmaya, sisteme veya ağlara hem şirket içinden hem de dışından erişimi daha güvenli hale getirmeye yönelik yatırımlar gerçekleştiriyor. Siber riski ölçme, yönetme ve önleme süreçleri belirgin alanlarda yatırım gerektirirken, bu alanların başında altyapı, organizasyon ve insan kaynakları geliyor. Firmaların yüzde 50'si söz konusu yatırımları yapma konusunda çekimser davranırken, daha çok penetrasyon ve zafiyet analizleriyle yetiniyorlar.

Siber risk sigortasının önemi gün geçtikçe artıyor

Şirketlerin siber güvenlik alanındaki olgunlukları siber risk sigortasına yatkınlıklarını olumlu yönde etkiliyor. Firmaların çoğunun siber risk sigortası hakkında yeterli bilgisi bulunmuyor. Siber risk sigortaları hakkındaki bilgi eksikliği ve siber risk sigortalarının kapsamına güvenilmemesi, siber risk sigortası yaptırılmasının önündeki en önemli engeller olarak ortaya çıkıyor. Siber risk sigortası sahibi olan firmaların yüzde 86'sı sigortanın kendilerini koruyacağına güven duyarken, bu oran sigorta sahibi olmayanlarda yüzde 34 düzeyinde kalıyor.

Yeşim Aksüt: "Siber risk sadece firmaların değil, ülkelerin de en önemli gündemi ve yatırım alanı"

Siber risk yönetimi konusunda bütünsel bir bakış açısı değişikliği gerektiğine dikkat çeken Marsh Türkiye Eş CEO'su Yeşim Aksüt, "Bunun için eğitim ve bilgilendirme şart. Siber risk eğitimlerinin şirket oryantasyonlarının bir parçası haline getirildiği, bilinçlendirme pratiklerinin şirketlerin tüm iş birimlerine entegre edildiği yapılar kurulmalı. Siber riskin, şirketin taşıdığı diğer tüm riskler gibi konumlanması ve vizyon planlarının içine alınması önem taşıyor. Ancak araştırmanın da gösterdiği gibi, sektörlerin büyük bölümünde siber riskler konusunda bir farkındalık eksiği söz konusu. Bilgi teknolojilerine her geçen gün daha fazla artan bağımlılığımız, daha verimli ve yaratıcı çalışma şekillerine olanak sağlarken, şirketlerin itibarını ve finansallarını önemli ölçüde sarsabilecek sonuçlar doğurabilecek potansiyele de sahip. Siber saldırılar ve suçlar, artık yalnızca şirketlerin değil ülkelerin en önemli gündem maddesi oldu ve önemli bir yatırım alanı haline geldi. Bu araştırmayla Türkiye'deki şirketlerin siber risklere bakış açısı, şirket içinde nasıl konumlandırdıkları, üçüncü tarafları bu anlamda nasıl gördükleri ve kamu politikalarıyla etkileşimlerini ortaya koymayı hedefledik. Bu sonuçların dinamik olacağını ve şu anda içinde bulunduğumuz COVID-19 pandemi dönemi gibi majör olaylardan etkileneceğini vurgulamakta fayda var. Bu minvalde, araştırmanın belli sıklıklarda tekrarlanması ve değişen trendleri yansıtması kurumlar için yol gösterici olacaktır. Raporumuzun bu yolu açacağına ve öncülük edeceğine inanıyoruz" dedi.

Serkan Sevim: "Firmalar dijital vizyon ve stratejilerini oluşturmalı"

İş dünyası olarak teknolojinin ve dijitalleşmenin fırsatlarından yararlanırken aynı zamanda risklere karşı hazır ve korunaklı olabilmeleri gerektiğini söyleyen TÜSİAD Yönetim Kurulu Üyesi ve Dijital Türkiye Yuvarlak Masası Başkanı Serkan Sevim, "Siber saldırılar karşısında güvenlik çözümleri yeteneklerinin artırılması, geleceğe dair planlamalar yapılırken kurumlarımızın güçlü bir siber saldırıya uğrayabilme riskinin düşünülmesi çok önemli. Bu alanda farkındalık ve yatırımların gerçekleştirilmesi için kurumların gerekli kaynak, personel ve zamanı tahsis etmesi; dijital vizyon ve stratejinin oluşturulması gerekiyor.Bu vizyonun hayata geçirilmesinde dijital dünyanın gerektirdiği yetkinlikler ve becerilerle donatılmış iş gücüne ihtiyaç olacak. Yaptığımız işler hızla dönüşürken gerek kamu gerek iş dünyası olarak dijital dönüşümü bütüncül bir yaklaşımla ele almalı, iş birliği içinde çalışmalarımızı sürdürmeli ve dijital dönüşüm rüzgarının hızına hep birlikte hazırlıklı olmalıyız" dedi.