**BASIN BÜLTENİ**

**Siber güvenlik, sadece bir BT yatırımı olarak değil, stratejik bir konu olarak ele alınmalı**

**Fortinet, bilişim teknolojisi uzmanları ile yaptığı Küresel Kurumsal Güvenlik Araştırması’nın sonuçlarını açıkladı. Siber güvenlik artık yönetim stratejinin en önemli konusu haline geliyor.**

Şirketler dijital dönüşüm yolculuklarına başlarken, yeni iş fırsatlarına dokunmaya, operasyonel verimliliği artırmaya ve müşterilere daha iyi hizmetler sunmaya çalışıyorlar. Dijital dönüşüm; işletmelerin bulut teknolojisi, Nesnelerin İnterneti (IoT), büyük veri ve diğer dijital girişimleri benimsemelerine yol açarak onları karar aşamasından müşteri hizmetlerine kadar her şeyi yeniden yaratmaya ve otomatikleştirmeye zorluyor.

Bu imkânlarla birlikte yeni siber güvenlik sorunları ortaya çıkıyor. Gartner, güvenlik ekiplerinin yetersizliği nedeniyle dijital işletmelerin %60'ında büyük hizmet hataları yaşanacağını öngörüyor. Sorunun önemli kısmı, güvenlik konusunun üst düzey yöneticiler ve yönetim kurulu üyeleri tarafından kritik bir iş problemi olarak görülmemesinden kaynaklanıyor.

**Siber güvenlilik, hala yönetim düzeyinde bir konu değil!**

Fortinet’in 1800 BT uzmanıyla yaptığı Küresel Kurumsal Güvenlik Araştırması'na göre, katılımcıların neredeyse yarısı güvenlik konusunun hala yönetim kurulu için en öncelikli tartışma olduğuna inanmadığını söylüyor. Aynı zamanda, katılımcılar şiddetle, siber güvenliğin üst düzey bir yönetim önceliği haline gelmesi gerektiğini ve %77 oranla yönetim kurullarının BT güvenliğini daha ayrıntılı bir şekilde incelemesi gerektiğini belirtiyorlar.

Yeni güvenlik saldırılarının ve onların hedefledikleri işletmeler üzerindeki korkunç etkilerinin bir sonucu olarak yönetim kurulları da bu konuya daha fazla ilgi duyacaklardır. Fakat, yönetimler güvenlik saldırıları meydana geldiğinde tepki gösteriyor olsa da, eylemleri genellikle çözüm odaklı olmaktan çok reaktif olacaktır. Özellikle, yönetim kurulları önlem almadan çok ihlal sonrası yönetiminde yer alıyor gibi görünmektedir. Örneğin, kurulların %77'si bir güvenlik olayı gerçekleştikten sonra neler olduğunu öğrenmek istiyor ve %67'si güvenlik bütçelerini inceliyor veya artırıyor. Güvenlik liderlerinin, güvenlik düzeyini yönetim kurulu seviyesine yükseltmek için hala çok işi var.

Hiçbir şirket, ihlal tehdidi, fidye saldırıları veya operasyonel aksamalara karşı bağışık değildir. Her boyuttaki/ şekildeki şirketler ve tüm endüstri segmentleri hedef haline gelebilir. Fortinet BT uzmanları anketindeki bulgular bu durumu doğruluyor. Ankete katılanların %85'i son iki yılda en az bir güvenlik ihlaline uğradığını ve neredeyse yarısı bir malware veya fidye saldırısı bildirdiğini söylüyor.

**Siber güvenlik neden yönetim kurullarının önceliği olmaya başlıyor?**

Kurulları, yöneticileri ve BT karar organlarını, 2018 yılında siber güvenliği birincil önceliğe geçirmeye yönlendiren bir dizi faktör var. Önemli olanlardan bazıları:

1. Güvenlik İhlalleri ve Küresel Saldırılar: Kuruluşların büyük çoğunluğu son iki yılda bir tür güvenlik ihlali veya saldırı yaşadı. Ankete katılanların %49'u, kuruluşlarının WannaCry gibi küresel bir saldırıyı takiben güvenlik konusundaki yeteneğini artırdıklarını söylüyor. Marka saygınlığı ve işletme operasyonları üzerindeki etkileri ile birlikte artan tanıtım ve ilgi, bu konuyu BT operasyonel işlerinden ziyade yönetim kurulu düzeyindeki bir konu haline getiriyor.
2. Saldırı Yüzeyi: Bulutun benimsenmesi, IoT'nin ortaya çıkması ve büyük verilerin artışı hem saldırı yüzeyinin çevresini hem de karmaşıklığını genişletmektedir. Ankete katılanların %74'ü bulut güvenliklerinin, kuruluşları için artan bir öncelik olduğunu belirtiyor. Katılımcıların yarısı ise, kuruluşlarının önümüzdeki 12 ay içinde bulut güvenliği yatırımlarını planladığını söylüyor. IoT, giderek büyümekte olan saldırı yüzeyi açısından büyük bir faktör. Bağlı IoT cihazlarının, Gartner'a göre, yıl sonuna kadar 8,4 milyardan fazla bir balon oluşturacağı tahmin ediliyor. Bunların 3.1 milyarı işletmelere ait. IoT aygıtlarının güvenliği zor olduğundan, uzmanlar 2020 yılına kadar tüm güvenlik saldırılarının %25'inden fazlasının bu cihazları hedefleyeceğini öngörüyor.
3. Yasal Düzenlemeler: Yeni hükümet ve sanayi düzenlemeleri de güvenliğin önemini artırmaktadır. Ankete katılanların %34'ü, bu düzenlemelerin yönetim kurulu seviyesindeki güvenlik farkındalığını artırdığını belirtiyor. 2018 yılında yürürlüğe giren AB'deki Genel Veri Koruma Yönetmeliği'nin geçerliliği buna bir örnek olarak gösterilebilir.

Bu eğilimler, basit bir BT yatırımından ziyade, sanal güvenlik yönetiminin stratejik bir mesele olarak görülmesini zorunlu kılıyor. Dijital dönüşümü başarmak için BT güvenlik liderleri, saldırı yüzeyinde görünürlüğünü artırmak, tespit ve saldırıyı engelleme arasındaki süreyi kısaltmak, sağlam performans sunmak ve güvenlik istihbaratını ve yönetimini otomatikleştirmek amacıyla siber güvenlik yaklaşımlarını yeniden düşünmelidir.

**İlgili Kişi:**

Eray Çoşan Akkuş

Marjinal Porter Novelli

0533 927 23 97 [erayc@marjinal.com.tr](mailto:erayc@marjinal.com.tr)

**Fortinet hakkında**

Fortinet (NASDAQ: FTNT) dünya genelinde büyük ölçekli şirketlere, servis sağlayıcılarına ve kamu kurumlarına güvenlik sunar. Fortinet, her geçen gün artan sanal saldırılara karşı müşterilerine akıllı ve sorunsuz koruma sağlar, sınırların ortadan kalktığı ağların artan performans ihtiyaçlarını karşılar. Ağlardaki uygulamaların, bulut sistemlerinin ve mobil cihazların karşılaştığı en kritik güvenlik sorunlarına karşı performanstan ödün vermeden güvenlik sunan tek çözüm sadece Fortinet’in Security Fabric mimarisidir. Fortinet global çapta sevkiyatı yapılan en güvenilir çözümler alanında dünyanın bir numarasıdır ve dünya genelinde 320 binden fazla müşteri ticari faaliyetlerini korumak için Fortinet’e güvenmektedir. Daha fazla bilgi için: http://www.fortinet.com, Fortinet Blog sayfası veya FortiGuard Labs.