**BASIN BÜLTENİ**

**Fortinet’in araştırmasında dijital dönüşümün güvenliğe etkileri öne çıkıyor**

**Fortinet’in 2018 Dijital Dönüşüm ve Güvenlik Araştırması dijital dönüşümün bütüncül ve stratejik bir güvenlik yaklaşımıyla yönetilmesi gerektiğini ortaya koyuyor.**

Kapsamlı, entegre ve otomatik siber güvenlik çözümlerinde dünya lideri Fortinet, dünya genelinde kuruluşların siber güvenlik seviyesine dair önemli bilgiler veren 2018 Dijital Dönüşüm ve Güvenlik Etkileri Araştırması’nın sonuçlarını duyurdu. Araştırma bulguları, dünya çapındaki 2500’ün üzerinde çalışana sahip organizasyonların 300’den fazla Bilgi Güvenliği Başkanı (CIO) ve Baş Güvenlik Yöneticilerine (CSO) uygulanan bağımsız bir anketten elde edildi.

**BT’yi güçlendiren baş döndürücü bir trend: Dijital dönüşüm**

Ankete göre, şirketlerin büyük çoğunluğu dijital dönüşüm sürecini başlatmış, katılımcıların yüzde 67’si kurumlarının bir yıldan daha önce dijital dönüşüm uygulamalarına başladığını ve yüzde 95’i de şu an bir çözümü denemekte olduklarını belirtmiş.

Ankete katılan Bilgi Güvenliği Başkanı (CIO) ve Baş Güvenlik Yöneticilerinin (CSO) yüzde 85’i dijital dönüşümün şirketlerinin iş sonuçları üzerinde büyük bir etki yarattığını belirtmesi dijital dönüşümün hızla büyümesinin önemli bir sebebi olarak öne çıkıyor. Dijital dönüşüm söz konusu olduğunda, en hızlı şekilde hayata geçirilen uygulamalar arasında nesnelerin interneti ve yapay zeka/makine öğrenme yer alıyor.

**Dijital dönüşümle gelen güvenlik sorunları**

Dijital dönüşümün bir kurumun işleyişini temelden dönüştürdüğü ve müşterilerine değer sunmasını sağladığı genel olarak kabul edilse de, dijital dönüşüm siber saldırı riskini de arttırıyor. Uç noktaların yaygınlaşması, gitgide dağıtık bir hal alan ağlar ve katlanarak artan veri hacmi ve ağ trafiği hem BT güvenlik ekipleri hem de BT departmanları için endişe yaratıyor. Bilgi Güvenliği Başkanı (CIO) ve Baş Güvenlik Yöneticileri (CSO) de buna katılıyor. Ankete katılan yöneticilerin yüzde 85’i dijital dönüşüm uygulamalarının önündeki en büyük engelin güvenlik olduğunu düşünüyor. Anketin önemli bulguları ise şöyle:

* Katılımcıların ortalama yüzde 25’i ağ altyapılarının güvenlik tehditlerine karşı korunmadığını düşünüyor. Dijital dönüşümle birlikte genişleyen saldırı yüzeyi, tehditlerin sayıca artması ve giderek daha da gelişmiş bir hal alması ve gerekli güvenlik becerilerine sahip olmayan personel gibi faktörler bu durumun sebepleri arasında yer alıyor.
* Ankete katılan katılımcıların geçtiğimiz 24 ay içerisinde ortalama 20 adet siber saldırı bağlantılı ihlale maruz kaldığı, bunların dördünün hizmet kesintisi, veri kaybı ya da uyumla ilgili sorunlara yol açtığı görülüyor.
* Bilgi Güvenliği Başkanı (CIO) ve Baş Güvenlik Yöneticileri (CSO) için özellikle tehdit teşkil eden iki risk kaynağı ise sürekli şekil değiştiren polimorfik (çok biçimli) saldırılar (yüzde 85) ve DevOps ile ilgili zafiyetler (yüzde 81) olarak tespit ediliyor.

Araştırmanın sonuçlarını değerlendiren **Fortinet Bölge Teknoloji Direktörü Melih Kırkgöz** şunları söyledi: “Dijital dönüşüm dalgası önüne çıkan tüm engelleri ortadan kaldırıyor. Siber güvenlik endişeleri de dönüşüm süreci için önemli bir engel teşkil ediyor. Halihazırda dijital dönüşüm yaklaşımını benimseyen kurumlar için en can alıcı siber güvenlik güçlüklerini ise özellikle çoklu bulut ortamlarına odaklanılan bulut bilişim konusu, nesnelerin interneti, gelişen tehdit görünümü ve giderek artan düzenleyici baskılar olarak dört ana başlıkta toplayabiliriz. Kurumlar diğer temel iş hedeflerinin yanı sıra büyüme hedeflerini başarmak için dijital dönüşümü hayata geçirirken, dijital dönüşüm de dijital teknolojinin tüm alanlarına entegre bir güvenliğe sahip eşdeğer bir güvenlik dönüşümü gerektiriyor. Bu da güvenliğin mimarileştirilmesi, konumlandırılması ve işletilmesi konularında kökten değişikliklere yol açarken, kurumların birbiriyle iç içe geçmiş Dijital Dönüşüm ve güvenlik transformasyonu konseptine programlı bir yaklaşım kapsamında yaklaşmasının önemini vurguluyor.

**Bütüncül ve stratejik bir yaklaşımla dijital dönüşümü güvence altına almak**

Veriyi daha detaylı olarak ele alan anket, üst düzey kurumlar arasında önemli farklılıklar olduğunu gösteriyor. Geçtiğimiz iki yıl içerisinde zarar kaybına yol açan bir saldırıya maruz kalmamış kurumlar ve daha alt seviyedeki kurumlar ile aynı zaman diliminde zarar kaybına yol açan 16 saldırıya maruz kalan kurumlar arasında ciddi farklar görülüyor. Her bir grup yaklaşık olarak katılımcıların üçte birini oluşturuyor.

Anket üst düzey kurumların daha bütüncül ve stratejik bir güvenlik yaklaşımı benimsemeye eğilimli olduğunu gösteriyor. Bu bulgulara göre, üst düzey kurumların:

* Yüzde 76’sının birleştirilmiş güvenlik mimarisi oluşturmak için güvenlik çözümlerini entegre etme olasılığı daha yüksek.
* Yüzde 38’nin kurumlarında tehdit istihbaratı bilgileri paylaşma olasılığı daha yüksek.
* Yüzde 34’ünün kurumlarında her yerde (kurum içi bulut, nesnelerin interneti, mobil vb.) işlerinin güvenliğini sağlama olasılığı daha yüksek.
* Yüzde 24’ünün merkezi takip ve raporlama için hem sektör hem de güvenlik standartlarına uyum kontrollerini oluşturma olasılığı daha yüksek.
* Yüzde 24’ünün güvenlik uygulamalarının yarısından fazlasını otomatikleştirme olasılığı daha yüksek.
* Yüzde 20’sinin tüm ortamlarda uçtan uçta görünürlüğü sağlama olasılığı daha yüksek.

**Fortinet Bölge Teknoloji Direktörü Melih Kırkgöz**, “Sonuçlar açıkça gösteriyor ki bütüncül ve entegre güvenlik stratejileri, silolara dayalı, reaktif stratejilere oranla daha efektif. Cihazların yaygınlaşmasıyla kurumların saldırı yüzeyleri genişledikçe, ister mobil iş gücü veya nesnelerin interneti girişimlerinin bir parçası, isterse de bulut ortamlarının, özellikle de çoklu bulut ortamlarının hayata geçirilmesine yönelik olsun, stratejik yaklaşımın önemi daha da artıyor. Ayrıca, ağın tüm kısımlarındaki BT araç ve süreçleri birleştiren kapsamlı bir strateji polimorfik saldırılar ve DevOps kaynaklı zafiyetler gibi gelişmiş tehditlerin ele alınması için gerekli. Aynı zamanda, güvenlik unsurlarının entegrasyonu, iş akışlarını otomatikleştirmek ve tehdit istihbarat paylaşımları yapmak isteyen kurumlar için temel bir gereklilik olarak öne çıkıyor” dedi.

**Araştırmanın metodolojisi**

*‘2018 Dijital Dönüşüm ve Güvenlik Araştırması’*, Avustralya, Asya, Avrupa ve Kuzey Amerika’dan 300 güvenlik yöneticisinin katılımıyla gerçekleştirildi. Bilgi Güvenliği Başkanı (CIO) ve Baş Güvenlik Yöneticisi (CSO) statüsündeki katılımcıların tamamının 2 bin 500’ün üzerinde çalışanı bulunan kurumlarda güvenliğe ilişkin görevleri bulunuyor. Katılımcıların çalıştıkları kurumların eğitim, kamu, finansal hizmetler, sağlık hizmetleri, teknoloji ve enerji gibi pek çok farklı sektörde faaliyet gösteriyor.

Araştırmaya ilişkin raporun tamamına buradan erişebilirsiniz.

**İlgili Kişi:**
Eray Çoşan Akkuş
Marjinal Porter Novelli
0 533 927 23 97
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 360 binden fazla müşteri ticari faaliyetlerini korumak için Fortinet'e güvenmektedir. Daha fazla bilgi için: [http://www.fortinet.com](http://www.fortinet.com/), [Fortinet Blog](https://blog.fortinet.com/) sayfası veya [FortiGuard Labs](https://fortiguard.com/).