**BASIN BÜLTENİ**

**2017’de finans dünyasını bekleyen zorluklar**

**Araştırma sonuçlarına göre veri ihlallerinin %89’unun arkasındaki motivasyon kaynağı finansal veya casusluk nedenleri iken finansal sistemlerin %15’inde güvenlik ekipleri saldırıları aylar sonra fark ediyor. Bu tehlikeye dikkat çeken Fortinet, finans kuruluşlarının 2017 yılında karşılaşabilecekleri sorunların listesini yayınladı.**

Finans kuruluşları 2016 yılında siber saldırganların başlıca hedefleri arasında yer aldı. Bu kuruluşlar sahip oldukları verilerin değeri nedeniyle 2017 yılında da hedef olmaya devam ediyor. Sonuç olarak bu kuruluşların CIO’ları güvenlik ile ilgili önemli kararlar almak ve bazı zorlukların üstesinden gelmek zorunda.

Bu nedenle yüksek performanslı siber güvenlik çözümleri alanında dünyanın önde gelen şirketlerinden [Fortinet](http://ctt.marketwire.com/?release=11G067974-001&id=7377526&type=0&url=http%3a%2f%2fwww.fortinet.com), hemen hemen tüm finans kuruluşlarının 2017 yılında karşılaşabilecekleri zorlukların bir listesini yayınladı. İşte bu yıl finans dünyasını bekleyen o zorluklar:

**Eski sistemlerin yeni teknoloji ile harmanlanması**

Finansal servisler son 25 yıl içerisinde tarihinde hiç olmadığı kadar büyük bir değişimden geçiyor. “Kendi cihazını getir” (BYOD) akımı ve IoT’un yaygınlaşması 7/24 erişimi de mümkün kıldı. Bu nedenle günümüzde müşteriler ve çalışanlar sistemlere 7/24 erişmek istiyor.

Ancak büyük fırsatlar beraberinde büyük zorlukları da getiriyor. Yeni teknolojileri mevcut sistemlere ve BT altyapılarına entegre etmek bu yılda zorluklar arasında yer alacak. Endüstrinin ve iş dünyasının tümden dijitalleşmesi finans kuruluşlarını bulut sistemlerine (herkese açık, özel ve hibrit) geçmeye ve kurum içi sistemleri bulut sistemlerine bağlamaya zorluyor. Bu da korunması gereken BT ortamların yapısını daha da karmaşık hale getiriyor.

**Çalışanlardan kaynaklan tehditleri azaltmak**

Daha birkaç yıl öncesine kadar finansal kuruluşlarda çalışanların merkezde olduğu [siber saldırıların yaşandığına](https://blog.fortinet.com/2016/09/01/three-ways-insider-security-threats-have-recently-impacted-financial-institutions) şahit oldu. Gittikçe daha akıllanan siber saldırganlar, şirketlere saldırmak için çalışanları da kullanarak yeni yöntemler geliştiriyor. Ek olarak, [sayıları artmakta olan](http://globalworkplaceanalytics.com/telecommuting-statistics) uzaktan çalışanlar da kurumsal güvenliğin olmadığı cihazlara dışarıdan erişiyor. Bu yeni ağ paradigması nedeniyle kurumların çalışanlarını siber güvenlik konusunda bilinçlenmesi de kritik derecede önemli hale geliyor. 2017 yılına girdiğimiz şu aylarda, kurumların kendi çalışanlarından kaynaklanan saldırıların sayısını azaltacak güvenlik çözümlerini uygulaması gerekiyor.

**Artan saldırılar ile başa çıkmak**

Verizon’un 2016 Veri İhlali Araştırma [Raporu](http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/), veri ihlallerinin %89’unun arkasındaki motivasyon kaynağının finansal veya casusluk nedenleri olduğunu ortaya çıkardı. Bu tarz araştırmaların ortaya çıkardığı bu durum nedeniyle 2017 yılında finans kuruluşları “Saldırıya uğrarsak ne olur?” düşünce yapısından “Saldırıya uğrarsak ne yapacağız?” düşünce yapısına doğru bir değişimden geçiyor.

Araştırma sonuçları ayrıca finansal sistemlerin %98’inin saldırının gerçekleştiği ilk birkaç dakika içerisinde ele geçirildiğini, %15’inde ise güvenlik ekiplerinin saldırıları aylar (hatta daha fazla) boyunca fark etmediğini ortaya koyuyor. Bu da saldırganların sistemler sızmak ve finansal verileri çalmak için yeterince zamanları olduğunu gösteriyor. Bu nedenle CIO ve güvenlik ekipleri, verilerini ve müşterilerini korumak için kaçınılmaz tehditleri fark edebilecekleri, ortaya çıkarabilecekleri ve bunlara yanıt verebilecekleri yöntemler bulmak zorunda.

**Uyum yasalarına bağlı kalmak**

Finansal servisler için standart ve şartlar sürekli değişiyor. Bu yıl da bu kuruluşlar şu ana kadar olduğundan daha yüksek standartları uygulamak zorunda kalabilirler. ABD’nin [New York](http://www.dfs.ny.gov/about/press/pr1609131.htm) gibi bazı eyaletleri şimdiden siber güvenlik regülasyonlarını daha da katı hale getirmeye başladı. Vali Andrew M. Cuomo son olarak yeni regülasyonlarla ilgili yaptığı açıklamada bankaların, sigorta şirketlerinin ve diğer finans kuruluşların kapsamlı siber güvenlik programları uygulamak zorunda olacağını belirtti.

Bu regülasyonlara uymamanın finansal ve itibar açısından ciddi sonuçları olabilir. Sonuç olarak 2017 yılında CIO’ların kendilerine uyum yasalarına bağlı kalmalarına yardımcı olacak [siber güvenlik çözümlerini](https://fortinet.com/) hayata geçirmesi gerekecek.

**Güvenlik silolarını ortadan kaldırmak**

Birçok CIO, günümüzde tüm ihtiyaçları karşılayacak tek bir çözüm olmadığından kurumlarını korumak için güvenlik satıcılarına güveniyor. Bu çok satıcılı modelde CIO’ların ortak bir işletim sistemi ve açık APİ’ler ile birbirine sıkı sıkıya bağlı çözümler bulması şart. Böylesi bir birleşik yapı, birden çok çözümü entegre edebilir ve siber güvenlik uzmanlarına tehdit dünyasına tek bir noktadan bakma kabiliyeti kazandırabilir.

**İlgili Kişi:**

Eray Çoşan Akkuş

Marjinal Porter Novelli

0533 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. Dünya genelinde 280 binden fazla müşteri ticari faaliyetlerini korumak için Fortinet’e güveniyor. Daha fazla bilgi için: http://www.fortinet.com, Fortinet Blog sayfası veya FortiGuard Labs.