**BASIN BÜLTENİ**

**İşte 2017’de dünyayı bekleyen siber tehditler**

**Gelecek yıl dünyayı bekleyen tehlikeleri açıklayan Fortinet’e göre ünlü ve siyasilere karşı çok daha güdümlü saldırılar yaşanacak, fidye yazılımlar ile çok sayıda kurbana eş zamanlı saldırılar yapılacak ve her birinden alınacak küçük miktarlarda fidye ile büyük vurgunlar yapılacak, kamu hizmetlerinde kullanılan sistemler siber suçluların en değerli hedefleri arasına girecek.**

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)’in® (NASDAQ: FTNT), tehdit araştırma birimi [FortiGuard Labs](https://fortiguard.com) 2017 yılı ile ilgili altı beklentisini açıkladı. Bu tahminler, Fortinet araştırmacılarının yakın gelecekte ortaya çıkmasını bekledikleri siber suçları ve bu siber suçların global ekonomiye yönelik yaratabileceği potansiyel etkileri içeriyor. Fortinet’in [blog](https://blog.fortinet.com/) sayfası üzerinden detaylarına yer verilen beklentilerin öne çıkan noktaları ise şu şekilde:

1. **Akıllı daha da akıllanacak: Otomatik ve insan benzeri saldırılar daha akıllı savunma gerektirecek:**

Tehditler her geçen dün daha da akıllanıyor ve gittikçe daha fazla otomatikleşiyor. Önümüzdeki yıl “insan benzeri” zararlı yazılımlar görmeyi bekliyoruz. Bu yazılımlar, saldırıların etkisini artırmak için kendilerini duruma göre uyarlayacak ve başarıyı temel alan öğrenme yeteneğini kullanacak.

1. **IoT üreticileri güvenlik açıklarından sorumlu tutulacak**

Eğer nesnelerin interneti (IoT) alanında ürün geliştirenler cihazlarını daha iyi bir şekilde koruyamaz ise bunun dijital ekonomiye etkisi yıkıcı olabilir, tüketiciler siber güvenlik korkusu nedeniyle bu ürünleri satın almakta tereddüt yaşayabilir. Tüketicilerin, şirketlerin ve diğer ilgili grupların, cihaz üreticilerini sorumlu tutan güvenlik standartlarının oluşturulması ve uygulanması yönündeki çağrılarının artmasını bekliyoruz.

1. **20 milyar IoT cihazı, buluta saldırılar açısından zincirin en zayıf halkası**

Bulut güvenliğinin en zayıf halkası mimarisi değil, aksine bulut kaynaklarına uzaktan erişim sağlayan milyonlarca cihazdır. Bu nedenle son kullanıcıların cihazlarındaki açıkları kullanan ve böylece bulut servis sağlayıcılarını daha etkili bir şekilde hedef alan saldırılarda artış bekliyoruz. Daha fazla kurum, IoT ve bulut genelinde; fiziksel, sanal ve özel bulut ortamları arasında kendilerine sorunsuz güvenlik politikalarının oluşturulması, yönetilmesi ve uygulanması imkanını sağlayan “fabric” temelli güvenlik ve segmentasyon stratejileri uygulayacak.

1. **Saldırganlar, akıllı şehirlere baskılarını arttırmaya başlayacak**

Önümüzdeki yıl otomasyon ve yönetim sistemlerinin sayısı arttıkça bu sistemler hackerlar için de hedef olacak. Kamu hizmetlerinin sunulmasında kullanılan bu entegre sistemlerden tek birinin dahi saldırıya uğraması ciddi sonuçlar doğurabilir. Bu nedenle bu sistemlerin siber suçluların en değerli hedefleri arasında yer alması kuvvetle muhtemel.

1. **Fidye yazılımlar zararlı yazılımlar için bir geçit açtı**

Ünlüler, siyasiler ve büyük kurumlar gibi yüksek profile sahip hedeflere karşı çok daha güdümlü saldırılar bekliyoruz. Ayrıca bu alandaki otomatik saldırılar büyük bir fidye yazılım ekonomisi yaratacak. IoT cihazlarına yapılacak eş zamanlı saldırılar ile çok sayıda kurban hedeflenecek. Her birinden alınacak küçük miktarlarda fidye ile büyük vurgunlar yapılacak.

1. **Teknoloji, siber güvenlik alanında yetenekli kişi eksikliğini kapatmalı**

Şu an siber güvenlik alanında yetenekli uzman sayısındaki eksiklik, global çapta dijital ekonomiye katılmaya hazırlanan kurum ve ülkelerin büyük bir risk altında olduğu anlamına gelmekte. En basiti; ağ ortamlarında özgürce hareket edecek kritik varlıklarını koruyabilmelerini sağlayacak güvenlik politikaları geliştirme konusunda bu ülke ve kurumların deneyim ve eğitimleri bulunmuyor. Ayrıca günümüzün sofistike saldırılarını tespit edip bu saldırılara yanıt verebilecek durumda da değiller.

Konuyla ilgili değerlendirmede bulunan Fortinet Global Güvenlik Stratejisti Derek Manky, “Bulut bilişim ve IoT cihazlar gibi teknoloji inovasyonları, siber güvenlik alanında global çapta görülen yetenekli uzman kişi ve zorlayıcı mevzuat eksiklikleri, siber tehditlerin artmasının önemli nedenleri olarak kalmaya devam ediyor. Değişimlerin eşi benzeri görülmemiş hızda olması, siber saldırıların bireysel, siyasi ve ticari sonuçlar doğurabilecek kurbanları hedeflemelerini sağlayacak şekilde, durumu bardağı taşıracak bir noktaya getirdi. İlerisi için birçok seviyede sorumluluk getiren acil adımlar atılmalı. Bu sorumlulukların; şirketler, hükümetler ve tüketiciler üzerinde aynı şekilde gerçekten etkileri olmalı. Hızla harekete geçilmediği sürece global dijital ekonominin gelişimini durduracak ciddi risk devam edecek.” dedi.

**Tehdit beklenti trendleri ve sonuçlar**

Nesnelerin interneti ve bulut, yapılan tahminlerde önemli bir dayanak noktası olarak alınsa da diğer bazı trendler de öne çıkıyor. İş dünyası ve bireylerin ortaya çıkardığı dijital ayak izi dramatik bir şekilde büyüyerek potansiyel saldırı alanını da arttırdı. Buna ek olarak artık her şey bir hedefe dönüştü ve her şey bir silah olarak kullanılabilir duruma geldi. Tehditler daha fazla akıllandı, otomatikleşti ve bu tehditlerin tespiti daha da zorlaştı. Son olarak eski tehditler de geri gelmeye devam ediyor; fakat bu kez tespit ve adli soruşturma sınırlarını zorlayan yeni gelişmiş teknolojileri kullanarak.

**Ek kaynaklar**

* 2017 yılı ile ilgili beklentilerin tamamını Fortinet [blog](https://blog.fortinet.com) üzerinden okuyabilirsiniz.
* Fortinet’in Security Fabric stratejisinin 2017 yılı için BT altyapısı genelinde IoT’tan buluta kadar nasıl entegre, yüksek performanslı güvenlik sunduğu hakkında daha fazla bilgi için [internet sayfamızı](https://www.fortinet.com/corporate/about-us/why-fortinet.html) ziyaret edebilirsiniz.

Fortinet’i [Twitter](https://twitter.com/Fortinet), [LinkedIn](https://www.linkedin.com/company/fortinet) ve [Facebook](https://www.facebook.com/fortinet/) üzerinden takip edin.

**İlgili Kişi:**

Eray Çoşan Akkuş

Marjinal Porter Novelli

0533 927 23 97

erayc@marjinal.com.tr

**FortiGuard Labs hakkında**

FortiGate güvenlik duvarı platformunun da dahil olduğu Fortinet çözümleri, FortiGuard Labs tarafından geliştirilmiş güvenlik servislerinden güç almaktadır. FortiGuard Labs, dünya genelinde 200’den fazla uzman araştırmacı ve analistten oluşmaktadır. Araştırmacılar; tehditleri tespit etmek, bu tehditlere karşı koruma sağlamak ve bu alanda çalışmalar yapmak için kurum içinde geliştirilmiş dünya sınıfı araç ve teknolojiler kullanmaktadır. Takım içerisinde malware, botnet, mobil ve sıfır-gün açıklarının da dahil olduğu tüm kritik alanlarda kendisini çalışmalara adamış uzmanlar bulunmaktadır. Servis analistleri, kodları kırmak ve hafifletici imzalar üzerinde çalışmalar yaparken teknoloji geliştiricileri, sürekli evrim geçiren tehditlere karşı yeni savunma motorları yaratmaya devam etmektedir. FortiGuard Labs, her gün 290 binden fazla kişiyi koruyan dünya genelindeki 2 milyonu aşkın sensörden gelen verileri kullanmaktadır.

**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 290 binden fazla müşteri ticari faaliyetlerini korumak için Fortinet’e güvenmektedir. Daha fazla bilgi için: http://www.fortinet.com, Fortinet Blog sayfası veya FortiGuard Labs.