**BASIN BÜLTENİ**

**Çalıntı sağlık bilgilerinin internetteki çarpıcı fiyatı**

**Sadece 2015 yılında 113 milyondan fazla tıbbi kayıt ihlali yaşandığını beliren Fortinet Bölge Direktörü Derya Aksoy, bu bilgilerin “derin internette” kaç dolara satıldığını ve hangi amaçlarla kullanıldığını açıkladı. Olayın artık sağlık kurumlarının hacklenip hacklenmeyecekleri değil ne zaman hackleneceklerine dönüştüğünü belirten Aksoy, kurumların gerekli önlemleri alması konusunda da uyarılarda bulundu.**

Günümüzde sağlık kurumlarına yönelik tehditler daha derin ve daha hasar verici hale gelmiş durumda. Bu da daha güçlü güvenlik stratejileri geliştirmeleri ve bu alanda yatırım yapmaları için BT’nin elini güçlendiriyor. Bu nedenle global çapta sağlık hizmetleri alında [siber güvenlik pazarının](https://www.grandviewresearch.com/press-release/global-healthcare-cyber-security-market) 2022 yılına kadar yaklaşık 11 milyar doları (32 milyar TL) bulması bekleniyor.

Yüksek performanslı siber güvenlik çözümleri alanında dünyanın önde gelen şirketlerinden Fortinet’in Bölge Direktörü Derya Aksoy, 2014 yılında 5,5 milyar [değerinde](http://www.grandviewresearch.com/industry-analysis/healthcare-cyber-security-market) olan bu pazarın 2020 yılına kadar ciddi bir büyüme sergilemeye meyilli olmasının arkasındaki nedenleri sıralarken birbirinden çarpıcı bilgileri de paylaştı.

**“Konu hacklenip hacklenmeyecekleri değil ne zaman hacklenecekleri”**

Sadece 2015 yılında 113 milyondan fazla tıbbi kayıt [ihlali yaşandığını](http://www.pbs.org/newshour/updates/has-health-care-hacking-become-an-epidemic/) beliren Aksoy, “Bunu daha basite indirgersek eğer bu kayıtlardan her biri bir hastayı temsil ediyorsa bu da Türkiye nüfusundan daha fazla insanın saldırılara kurban gittiği anlamına geliyor. Dahası bu yaz ‘derin internette’ ortaya çıkan bir siber suç reklamında 600 binden fazla hastanın sağlık kayıtları [satışa çıkarıldı](http://www.computerworld.com/article/3088907/security/hacker-selling-655-000-patient-records-from-3-hacked-healthcare-organizations.html). Kayıtlarda kurbanların tam isimleri, sosyal güvenlik numaraları, doğum tarihleri ve dahası yer alıyordu ki tüm bu bilgiler sahtecilikte kullanılabilecek bilgiler.” dedi.

“Siber suçlular; hastanelerin, doktorların ve sigorta şirketlerinin çoğunun MEDJACK, sosyal mühendislik ve fidye yazılım gibi sayıları hızla artan sofistike saldırılara karşı hazırlıklı olmadıklarının farkında. Daha verimli ve etkili sağlık hizmeti vermek için verilerini online ortama taşıyan sağlık kurumlarının sayısı arttıkça, sağlık sektörü siber suçluların bir numaralı hedefleri olmaya da devam edecek.” diyen Aksoy, “Hatta konu birçok sağlık kurumu için artık hacklenip hacklenmeyecekleri değil ne zaman hacklenecekleri meselesine dönüşmüş durumda.” uyarısında bulundu.

**“Ölümcül sonuçlar ortaya çıkabilir”**

Sağlık hizmetleri sektöründe yaşanan her bir dijital ilerlemenin, siber suçluların içeriye sızmaları için bir fırsat yarattığını da vurgulayan Aksoy, “Günümüzdeki organizasyonlar sadece bu amaç için geliştirilmiş yeni teknolojik inovasyonlar ile güçlenen tehditlerin artan saldırısına maruz kalıyor. Veri depolamada bulut servislerini kullanmak, hareket halindeki çalışanların güvenli olmayan ağlar üzerinden bağlantı yapması, kendi cihazını getir (BYOD) fenomeni ve dizüstü, tablet gibi verilerin fiziksel olarak çalınmasını kolaylaştıran cihazlar sağlık hizmetlerini saldırılara karşı daha zayıf hale yaygın dijital uygulamadan sadece birkaçı. Tüm bunlara ek olarak, [Tıbbi Nesnelerin İnterneti](https://blog.fortinet.com/2016/09/12/healthcare-cybersecurity-risks-in-the-internet-of-medical-things)’nin (IoMT) hızla yaygınlaşması da bu güvenlik bilmecesini daha da karmaşık duruma getiriyor. İnsülin pompalarından kablosuz kalp pillerine ve infüzyon cihazlarına kadar tüm bağlantılı cihazlar, sağlık kurumlarını ağ içerisindeki bu cihazları koruyacak ve “konteynır” içine alacak [dahili segmentasyon güvenlik duvarları](https://www.fortinet.com/solutions/enterprise-midsize-business/enterprise-firewall/internal-segmentation-firewall-isfw.html) gibi teknolojilere yatırım yapmaları için zorluyor. Çok katmanlı güvenlik önlemleri alınmadan bağlantılı cihazlar kullanmak tam anlamı ile ölümcül sonuçlar doğurabilir.” şeklinde konuştu.

**“Tek bir çalıntı sağlık kaydı 60 dolara kadar alıcı bulabilir”**

Tüm endüstriler içerisinde sağlık kurumlarının en sık saldırıya uğrayan hedeflerden birisi olmasının nedeninin bu kurumların “derin internette” para kazandıracak değerli veriler bulundurması olduğunu da ifade eden Aksoy, “Derin internette çalıntı bir kredi kartı bir, iki veya üç dolara satılabilir. Sosyal güvenlik numaraların fiyatı ise 15 dolara kadar çıkabilir. Ancak tam bir sağlık kaydı bir altın madeni değerindedir. Bu bilgiler 60 dolara kadar [alıcı bulabilir](http://www.nbcnews.com/news/us-news/hacking-health-care-records-skyrockets-n517686).” diyerek tehlikenin büyüklüğüne dikkat çekti.

Çalıntı kredi kartı bilgilerinin kredi kartı iptali ile kolaylıkla geçersiz hale getirilebilirken tıbbi kayıtların sınırsız bir raf ömrüne sahip olduğunun altını çizen Aksoy, “Eğer bu bilgiler yanlış ellere geçerse sahtecilik yolu ile farklı tedavilerde, reçetelerde hatta çok pahalı ameliyatlarda kullanılabilir ve bu sözde tedaviler için sigortadan yüklü ödemeler talep edilebilir.” dedi.

**Tek bir veri ihlalinin sağlık kurumuna maliyet 4 milyon dolar**

İster uluslararası olsun ister olmasın, siber suçluların saldırılarının her zaman finansal sorunlara da neden olduğunu belirten Aksoy sözlerine şu şekilde devam etti: “Hatta sadece bu yıl sağlık kurumlarında yaşanan tek bir [veri ihlalinin maliyeti](http://www.healthcareitnews.com/news/cost-data-breaches-climbs-4-million-healthcare-events-most-expensive-ponemon-finds) 3,79 milyon dolardan 4 milyon dolara yükseldi. Ayrıca her bir ihlal sonrasında kurumlar daha fazla güvenlik elemanı alıyor, tehlikeler konusunda farkındalık yapmak için çalışanlarına yönelik eğitimler uyguluyor, ticari açıdan sürdürülebilir bir strateji geliştiriyor ve yeni güvenlik sistemleri kuruyor. Tüm bunlar bir araya geldiğinde hem sermaye giderleri hem de işletme maliyetleri üzerinde ciddi bir yük yaratıyor. Ayrıca bu tarz ihlallere izin veren kurumlara yönelik yasal cezalar uygulanabiliyor, dava ve avukat ücretleri de bunun üzerine eklenebiliyor. Tabii tüm bunlar, bir hasta kaybının yarattığı zararın yanında da hiç kalıyor. Sonuç olarak sağlık kurumlarının; kendilerini, hastalarını ve çalışanlarını derin interneti altın bulmak için kazan siber suçlulara karşı korumak için veri güvenlik çözümlerine yatırım yapmaları artık hayati bir öneme sahip hale gelmiştir.”

**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.