**BASIN BÜLTENİ**

**Sağlık sektörüne yönelik siber saldırılar dünyanın dört bir yanında hala devam ediyor**

**COVID-19 pandemisiyle birlikte tüm dünyanın yakından takip ettiği sağlık sektörü, son zamanlarda hacker’ların en gelişmiş tehditlerinin hedefi oluyor. BugBounter da sağlık sektöründeki paydaşların bu saldırılara neden maruz kaldığına ve siber savunmanın nasıl geliştirilebileceğine dair detayları paylaşıyor.**

Şirketlerin güvenlik açıklarını bulma ve doğrulama ihtiyacını bünyesindeki 900 bağımsız araştırmacıyla hızlı ve güvenilir bir şekilde karşılayan BugBounter.com, siber saldırganların halihazırda hedef aldığı ancak tüm dünyayı derinden etkileyen pandemiyle birlikte öncelik haline getirdiği sağlık sektörüne yapılan saldırılara dikkat çekiyor. BugBounter, aynı zamanda yapılan saldırıların nedenlerine ve çözüm yöntemlerine de ışık tutuyor.

**Elektronik kayıtlar saldırı alanlarını artırıyor**

Siber saldırganlar, hassas kişisel veriler sıklıkla kullanıldığı için sağlık sektörünü hedef alıyor. Bu veriler elektronik ortama aktarıldığında ise hacker’lar için önemli fırsatlar açığa çıkıyor. Son yıllarda elektronik sağlık kayıtlarının artması ve sağlık merkezlerinde kullanılan cihazların da ağ bağlantısı özelliği kazanmasıyla birlikte fidye yazılımlarında ve veri çalma amacıyla yapılan saldırılarda önemli artış gözlemleniyor. Başarıyla gerçekleşen saldırılar da bir ülkenin sağlık sisteminin veya bir hastanenin verdiği hizmetin tamamen aksamasına yol açabiliyor.

**Yamalanmayan sistemler ve geleneksel cihazlar hacker’lara kapı açıyor**

Sağlık cihazlarının maliyeti ve sağlık kurumunu koruyacak gelişmiş bir BT sistemini oluşturmanın zorluğu gibi sebepler, bütçelerde önemli yük yaratabiliyor. Cihazları yenilemek de her zaman mümkün olmadığı için bir cihaz uzun süre kullanılabiliyor. Bu yüzden eski kalan cihazların yazılımları için gereken yamalar oluşturulmuyor ve bu da cihazları siber saldırıya açık hale getiriyor. Yapılan araştırmalara göre hastanelerdeki [medikal görüntüleme ekipmanlarının yüzde 83’ü Windows işletim sisteminin yamalanmayan bir versiyonunu kullanıyor ve sıkça sömürülen açıklara karşı yamalanmıyor](https://fortune.com/2020/03/13/hospital-hacked-ransomware-medical-imaging-machine/).

**Üçüncü parti firmalar üzerinden siber saldırıya uğrama riski bulunuyor**

Sağlık kurumları da klinikler, laboratuvarlar ve yazılım sağlayıcıları gibi üçüncü parti firmalarla çalışabiliyor. Bu durumda kurumun kendisi siber saldırılara karşı son derece dayanıklı olsa bile sistemlerine entegre olan dış yazılım üzerinden siber saldırı gerçekleştiğinde üçüncü parti firmalar hassas verilere erişebildiği için ilgili kurum da fazlasıyla etkilenebiliyor.

**Sistemlerin çalışır durumda olması çok önemli**

Kullanılan sistemlerin faaliyetine her an devam edebilmesi tüm şirketler için hayati öneme sahip ancak sağlık sektöründe elektronik kayıtlara ve klinik sistemlerine erişebiliyor olmak kritik bir konumda bulunuyor. Bu sistemlere erişimde yaşanabilecek herhangi bir aksama, sunulan sağlık hizmetine de engel olabiliyor ve böyle bir durumda hastaların sağlığı risk altına giriyor.

BugBounter Kurucu Ortağı Murat Lostar, konuyla ilgili şunları söyledi: “Sağlık sistemlerine yönelik saldırılar pandemi bittiğinde bile yavaşlayacak gibi görünmüyor. Bu yüzden sağlık kuruluşlarının da hacker’lara karşı sağlam bir duruş sergilemesi gerekiyor. Bunun için de siber güvenliğe yaptıkları yatırımları artırmaları fazlasıyla önemli. Mikro segmentasyon, zamanında yama oluşturma, yazılım güncellemeleri, güvenli veri yedeklemeleri ve detaylı erişim kontrolleri gibi önlemler için büyük kaynaklara sahip olan geniş BT ekibi gerekiyor. Ancak sağlık kurumlarının bu noktada desteğe ihtiyacı olabiliyor. Bug bounty programları ise sistemlerini en uygun maliyetle denetletmek isteyen kurumların sıkça tercih ettiği yöntemler arasında yer alıyor çünkü sadece varlığı kanıtlanmış bir güvenlik açığı için ücret ödeniyor. Ayrılan zaman ve bütçe, yanlış bilgilerle ve hipotez raporlarla boşa gitmiyor. Aynı zamanda kurumlar ödülleri ve zaman aralığını kendi belirlediği için sistemlerinin güvenliğini kendi bütçelerine ve iş planlarına uygun olarak kontrol ettirebiliyor. Platformumuza kayıtlı olan bağımsız siber güvenlik araştırmacıları buldukları zafiyetleri raporladıktan sonra yetkili ekiplerimiz bu zafiyetleri kısa sürede doğruluyor, derecelendiriyor ve şirketin belirlediği güvenlik ekiplerine iletiyor.”

**İlgili Kişiler:**

Önder Kalkancı - Marjinal Porter Novelli

0533 927 23 95

onderk@marjinal.com.tr

Sezin Bulum - Marjinal Porter Novelli

0537 465 82 25

sezinb@marjinal.com.tr

**BugBounter hakkında**

Bağımsız araştırmacıların niteliksel ve niceliksel açık keşfetme gücünü doğrulama süreçlerinden geçirerek sunan BugBounter, hacklenmeyen bir dünya vizyonuyla siber güvenlik uzmanlarından oluşan bir ekosistem kurmaktadır. Şirketlerin kendilerini siber saldırılara karşı güçlendirmesini sağlayan BugBounter, tüm süreci hem firmalar hem de araştırmacılar için demokratikleştiren tek platformun geliştiricisidir. https://bugbounter.com/