**BASIN BÜLTENİ**

**Korona virüs, veri ihlallerinin artmasına zemin yarattı**

**Tüm dünyayı hazırlıksız yakalayan korona virüs salgını, iş yapış şekillerinde önemli değişikliklere neden oluyor. Evinden çalışanların ortamlarının da siber güvenlik yapısına dahil edilmesi gereken bu süreçte siber saldırganlar da hassas verilere erişmek için uzaktan çalışanların açıklarını tarıyor. Verilerini kaybetmek ve büyük bir kayıp yaşamak istemeyen şirketler, bağımsız güvenlik araştırmacılarından aldıkları hizmetle yapılarındaki açıkları kolayca bulabiliyor.**

Şirketlerin güvenlik açıklarını bulma ihtiyacını kitle kaynak kullanımıyla hızlı ve şeffaf bir şekilde gideren BugBounter, korona virüsün ortaya çıkardığı kaostan faydalanmak isteyen siber suçluların, kurumların hassas verilerini ele geçirmek için sürekli yeni yollar geliştirdiğine dair şirketleri uyarıyor.

Siber suçlular, şirketlerin ve bireylerin sistemlerine sızabilmek ve verilerini ele geçirebilmek için birçok yönteme başvuruyor. Tüm dünyayı etkileyen COVID-19 sebebiyle evden çalışan insanların sayısının artması, şirketlerin BT kaynaklarının sadece şirket içinde değil, tüm evlerde kullanılmasına neden oluyor. Şirketin veri merkezlerine uzaktan erişim gerektiği için, çok hızlı dönüşen bu süreçte siber güvenlik de fazlasıyla önemli hale geliyor.

Europol’ün gerçekleştirdiği *Catching the virüs* araştırmasına göre siber suçlar, COVID-19 ile faaliyeti en çok artan suç türü olarak listede yer alıyor. Siber suçlular, hedef aldıkları kişilerin korkularını yöneterek amaçlarına ulaşabiliyor. Oltalama (phishing) ve fidye yazılımları, COVID-19 sürecinde en sık kullanılan iki saldırı türü olarak öne çıkıyor ve bundan etkilenenlerin de ilerleyen günlerde katlanarak artması bekleniyor. Avrupa’da vakaların görülmeye başlamasıyla “dark web” üzerinden yapılan satışlarda ciddi bir artış gerçekleşti.

Şirketlerin, gerekli planlama ve hazırlık süreci yapılamadan hızla dönüşen iş modelleri ile birlikte şirket ağına sadece uzaktan bağlanan cihazların yama ve antivirüs imza güncellemesi gibi konularda oluşabilecek riskleri ile fiziksel olarak ofis dışından erişilmeye başlanan hassas iş sırları, özel nitelikli kişisel veriler gibi alanlarda artan siber güvenlik risklerini çok hızlı keşfetmeleri gerekiyor. Aksi takdirde veri ihlali yaşayan şirketler, bu dönemde yüksek maddi ve itibar kayıplarıyla karşı karşıya kalacaklar. Maalesef çok yakında ülkemizden de bu yöndeki kötü haberlerin duyulacağını öngörebiliyoruz.

Konuyla ilgili görüşlerini belirten BugBounter Kurucu Ortağı Murat Lostar, şunları söyledi: “Birçok araştırma, salgın sürecinde veri sızıntılarında dramatik artış gerçekleşeceğinin altını çiziyor. Kurumların bir adım önde olabilmesi için güvenliğe yaptıkları yatırımlarını bu dönemde artırması ve çeşitlendirmesi gerekiyor.

Bu süreçte güvenlik açıklarını keşfetmek için tercih edilebilecek yöntemlerden biri de kitle kaynağı (crowdsourcing). Şirketlerin kısıtlı sayıdaki siber güvenlik ekiplerinden çok daha kalabalık bir kitle, güvenlik sistemlerini hacker zihniyetiyle inceleyerek, kritik zafiyetleri bulma ihtimalini artırıyor. Doğru çözüm platformları bunu hızla ve uygun bir maliyetle sunuyor.”

**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**

Etik hackerların niteliksel ve niceliksel 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 hackerlar için demokratikleştiren tek platformun geliştiricisidir. <https://bugbounter.com/>