**BASIN BÜLTENİ**

**BugBounter pandemi sonrası veri güvenliğine dair önemli bilgiler paylaşıyor**

**Pandemiyle birlikte dijital dönüşüm yolculuğunda pek çok konu temelden değişti. Pandemi öncesinde önem sırasında üst noktalarda yer alan siber güvenlik ise daha da kritik hale geldi. BugBounter da pandemi sonrası siber güvenlik hakkında kritik noktaların altını çiziyor.**

Pandemiden önce de şirketlerin en önemli konuları arasında yer alan siber güvenlik, bugün çalışanların işlerine uzaktan devam etmesiyle daha da önemli hale geldi ve bu değişime ayak uyduramayan şirketler bugün daha da zorlanmaya devam ediyor. Şirketlerin güvenlik açıklarını bulma ve doğrulama ihtiyacını bünyesindeki 900 bağımsız araştırmacıyla hızlı ve güvenilir bir şekilde karşılayan BugBounter.com, pandemiyle birlikte son bir yılda önemli etkiler yaratan yeni normalde siber güvenliklerini sağlamak için çalışan şirketlere önemli ipuçları sunuyor.

Gartner’ın yayınladığı bir araştırmaya[[1]](#footnote-1) göre yöneticiler en çok siber güvenliğin kontrol noktalarında yaşanabilecek sorunlardan endişe duyuyor. Daha sonra yeni çalışma modeli ve uzaktan çalışanları yönetme sürecine dair çekinceler yer alıyor. Şirketlerin BT ekipleri uzaktan çalışanlar için VPN erişim kapasitesini artırırken güvenlik ekipleri de uzaktan erişim ilkelerini güncelledi ve ofisten çalışma için belirledikleri ilkelerden uzaklaştı.

Pandemi aynı zamanda şirketlerin güvenlik ihtiyaçlarını da değiştirdi. Bu kapsamda şirketler güvenlik için ayırdığı bütçeyi artırdı. Bu noktada şirketlerin sistemlerini olası güvenlik açıklarına karşı uygun maliyetle denetlemesini sağlayan ödül avcılığı (bug bounty) yaklaşımı da öne çıktı.

BugBounter Kurucu Ortağı Murat Lostar, konuyla ilgili şunları söyledi: “Şirketlerin neredeyse tamamı, pandeminin yarattığı değişime süreç içerisinde cevap verdi. Bu noktada çalışanlar işlerini artık sadece ofisten değil, kendi evlerinde veya seçtikleri noktalarda şirket ağları yerine evlerindeki veya mobil cihazlarındaki bağlantıları kullanarak yapıyor. Başka bir deyişle, çalışanlar şirket kaynaklarına BT’nin güvenliğini doğrudan sağlamadığı ağlar üzerinden erişiyor. Bu yüzden şirketlerin sistemlerini olası zafiyetlere karşı dönemsel değil sürekli kontrol ettirmesi gerekiyor. Bug bounty programları da sistemlerini en uygun maliyetle denetletmek isteyen BT ve güvenlik ekiplerinin en önemli yardımcıları arasında yer alıyor çünkü sadece varlığı kanıtlanmış bir güvenlik açığı için ücret ödeniyor. Yanlış bilgilerle ve hipotez raporlarla BT ekiplerinin zamanı ve bütçesi boşa gitmiyor. Ödül avcılığı sayesinde şirketler kendi belirledikleri ödüller ve zamanlamalar ile sistemlerinin güvenliğini kendi bütçelerine ve iş planlarına uygun olarak kontrol ettirebiliyor. Platformumuza kayıtlı olan bağımsız siber güvenlik araştırmacıları buldukları zafiyetleri raporladıktan sonra yetkilendirdiğimiz 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/

1. <https://www.gartner.com/en/newsroom/press-releases/2021-04-27-gartner-says-cybersecurity-control-failures-topped-executive-concerns-in-1q21?page=,,0> [↑](#footnote-ref-1)