**BASIN BÜLTENİ**

**BugBounter, 2021’de siber güvenlik dünyasına dair beklentilerini paylaşıyor**

**//
Yeni yılda şirketlerin siber güvenlik öncelikleri değişiyor**

**2020 yılındaki gelişmeler, birçok alanda büyük dönüşümlere neden oldu. Bu dönüşümlerin etkisi 2021’de de görülmeye devam edecek. Platformuna dahil olan yüzlerce siber güvenlik uzmanıyla şirketleri buluşturup uygulamalarındaki kritik açıkları etkin bir şekilde tespit eden BugBounter, yeni yılda etkisini gösterecek gelişmeleri paylaştı.**

Pandeminin yarattığı birçok değişime ayak uydurulan 2020’de hibrit çalışma modelinin yaygınlaşmasıyla güvenlik planlarının da buna uyumlu hale getirilmesi gerekti. 2020’yi pandeminin neden olduğu veya hızlandırdığı trendlerle geride bırakırken şirketlerin güvenlik açıklarını bulma ihtiyacı katlanarak artmış durumda. Bugbounter.com platformuna kayıtlı yüzlerce uzman araştırmacıyla test ihtiyacını hızlı, hesaplı ve etkin bir şekilde çözen BugBounter, 2021’de siber güvenlik dünyasında yön verecek öngörülerini aktardı.

**Siber güvenlik, kurumların temel harcamaları arasında daha büyük paya sahip olacak.**

Şirketler, gelişmiş saldırıları belirleyici ve net yaklaşımlarla tespit eden çözümler kullanmaya önem gösterecek. Aynı zamanda siber korumaya ve siber tehditleri tespit etmeye yapılan harcamalar, önümüzdeki 6 ayın öncelikleri arasında yer alacak. Gelirleri azalan şirketlerde bile başka alanların harcamalarından kesinti yapılarak siber güvenliğe kaynak aktarıldığı gözleniyor.

**Şirketler, e-posta güvenliği için başka yaklaşımlar benimseyecek.**

2021’de e-posta güvenliği alanında sadece güvenilir alıcıların e-postasının ulaşmasına izin vererek taklitçi oltalama saldırılarının önüne geçebilen sıfır güven yaklaşımı öne çıkacak. Başka bir deyişle, sıfır güven yaklaşımı, sınırsız mail arasından kötü olanları belirlemek yerine sınırlı sayıdaki gerçek göndericileri seçiyor.

**Sadece çalışanlar değil, tüm işleyiş uzak noktalara yayılacak.**

Salgınla birlikte ortaya çıkan düşük temas ekonomisinin ihtiyaçlarını karşılamak için oluşan yeni iş modelleri ve özel hizmetler günlük hayatlarda yer almaya devam edecek. Tam görünürlüğün nasıl sağlanacağını ve aynı tedarik zincirindeki yeni uzak kuruluşlar arasındaki karşılıklı ilişkinin nasıl güvence altına alınacağını açıklığa kavuşturmak, kilit önem taşıyacak.

**Bütçelerin azalmasıyla CIO’lar güvenlik çözümlerini tek çatı altında toplayacak.**

Düşük bütçeye rağmen şirketlerin CIO’ları dijital dönüşüm yolculuklarını tamamlamak için çalışacak. Bu yüzden sistemlerin birleşmesi ve basit bir yapıya sahip olması çok önemli hale gelecek. Bu yüzden birçok hizmeti tek bir platformda buluşturan teknolojilere yönelecek.

**Kurumlar uzaktan çalışmaya imkan tanıyan daha uzun vadeli çözümlere öncelik verecek.**

Uzaktan çalışanları desteklemek için birbirine benzeyen VPN, VDI, DaaS gibi çözümleri tercih eden şirketler, ölçeklenme sınırına ek olarak kullanıcı deneyimi, güvenlik ve maliyet alanlarında sorunla karşılaşabilirler. Zoom, Teams, Slack gibi modern, bulut tabanlı çözümler kullanıldıkça geleneksel uzaktan erişim çözümlerinin eksikliği kendisini gösterecek.

**Şirketler, siber güvenlik ve kurumsal ihtiyaçlar arasında riske göre bir denge oluşturacak.**

BT ekipleri, ölçeklenebilirlik ve erişilebilirlik gibi kurumsal ihtiyaçları giderirken güçlü bir güvenliğin de olmasını sağlayacak. Yüzde 100 güvenlik sağlamak gibi gerçekleşmesi çok zor bir beklenti, yerini belirli bir düzeye kadar riski göze alma ve dayanıklılığı da buna paralel olarak artırma stratejisine bırakacak.

**Sıfır güven yaklaşımının benimsenmesiyle geleneksel VPN’ler daha az kullanılacak.**

Pandemi sırasında birçok şirketin tüm kurumsal BT ve güvenlik stratejilerini yeniden oluşturması gerekti. Hemen ilk aşamada monolitik VPN sunucuları hemen değiştirmeseler de şirketler zamanla kurumsal BT mimarilerinin büyük çaplı uzaktan çalışma yöntemini destekleyebileceğini gözlemleyecek. Ayrıca daha yeni protokolleri kendisine temel alan VPN’ler tercih edilecek.

Konuyla ilgili görüşlerini belirten BugBounter Kurucu Ortağı Murat Lostar, şunları söyledi: “Tüm dünya olarak çok zorlu bir yılı geride bıraktık. 2021’nin ne getireceğini bilemesek de siber tehlikelerin artmaya devam edeceğini rahatlıkla söyleyebiliriz. Geçtiğimiz yıl, özellikle hayatımıza giriş yapan uzaktan çalışma yöntemiyle siber güvenlik stratejilerinin de temelden değiştiği bir dönem oldu. Bu yıl, yaşanan değişimin yaratacağı etkileri göreceğiz. Kurumların siber güvenlik önceliklerini yeniden değerlendirerek sistemlerinde eksik veya eskiden kalan bileşenleri güncellemesi gerekiyor. Bu sırada sistemlerini de bir bütün olarak siber güvenlik uzmanlarına denetlenmesi ve bunu belirli sıklıkta yapması çok önemli. Bugüne kadar alınan sızma testleri hizmetlerinin sağladığı dönemsel faydaların yanına bug bounty programları ile sürekliliğin sağlandığı ve güvenlik testlerinin çok daha geniş bir kitle tarafından yapılabildiği yenilikçi çözümler de kurumların öne çıkan tercihi olacak.”

**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/>