**BASIN BÜLTENİ**

**Kurumsal BT dünyasının ilgi gösterdiği yönetilen hizmetler siber saldırganların yeni hedefi haline geliyor**

**Şirketlerin dijitalleşme ihtiyaçlarını önemli ölçüde gideren yönetilen hizmetler, operasyonları iyileştirdiği ve maliyeti azalttığı için birçok kuruluşun başvurduğu bir yöntem haline geldi. Ancak artık şirketler kadar siber saldırganlar da yöntemlerinin etkisini artırmak için yönetilen hizmetleri ve bu hizmetleri sağlayan şirketleri hedef alıyor. Sürekli genişleyen siber güvenlik platformundaki 1800’den fazla uzmanı ile 7/24 denetlenme imkanı sağlayan BugBounter, yönetilen hizmet sağlayıcılarını (MSP) ve MSP’lerle çalışan firmaları siber saldırı riskine karşı uyarıyor.**

Şirketlerin güvenlik açıklarını denetleme, bulma ve doğrulama ihtiyacını bünyesindeki 1800’ün üzerinde siber güvenlik uzmanıyla esnek, çevik ve güvenilir bir şekilde karşılayan BugBounter ([www.bugbounter.com](http://www.bugbounter.com)), artan siber saldırı riskine karşı MSP’leri uyarırken, şirketlere de tedarik zinciri güvenliğini hatırlatıyor.

Şirketlere operasyon ve maliyet avantajları gibi önemli faydalar sağlayan yönetilen hizmet sağlayıcıları (MSP), yapıları itibariyle aynı anda çok sayıda kurumsal şirketle birlikte çalışıyor ve onların sistemine entegre oluyor. Sistemler arasında doğrudan erişim sağlayan bu entegrasyonla şirketlerden birinin güvenliğini istismar edebilen bir saldırgan, diğer şirkete karşı da saldırı potansiyeli elde ediyor. Firmalara yapılan siber saldırıların yaklaşık yüzde 40’ı tedarikçileri üzerinden gerçekleştiği göz önünde bulundurulduğunda, bu risk ciddiyetini daha da artırıyor.

BugBounter Kurucu Ortağı ve CEO’su Murat Lostar, konuyla ilgili şunları söylüyor: “Yönetilen hizmet sağlayıcıları, günümüzün kurumsal BT dünyasında çok önemli bir role sahip. Öte yandan şirketlere sağladığı faydaların yanında bazı riskleri de beraberinde getiriyor. Tedarik zinciri güvenliğini hatırlatan bu riskler, sistemi doğru bir şekilde korunan şirketlerin de siber saldırganlar tarafından ele geçirilme ihtimalini barındırıyor. Temmuz 2021’de bunun bir örneği yaşandı. Birçok MSP, REvil fidye yazılımıyla saldırıya uğradı ve bunun sonucunda 1.500’den fazla firma da bu saldırıdan olumsuz etkilendi. Benzer bir durumun bir daha yaşanmaması için atılabilecek adımlar mevcut. Şirketler bir MSP ile çalışmadan önce o MSP’nin sistemlerini nasıl koruduğuna dair bilgi almalı ve tercihini bu bilgiye göre yapmalı. “Bizim kendi ekiplerimiz var”, “Senede bir kez denetime tabiyiz”, “Güvenlik yazılımları kullanıyoruz” gibi söylemler bugünün zeki ve organize siber suçluları karşısında bir değer ifade etmiyor. Elbette MSP’lerin kendi BT sistemlerini siber saldırılara karşı düzenli olarak denetletmesi gerekiyor. Ancak bunun en verimli yöntemini de siber saldırganların yöntemlerine aşina olan uzmanlar sunuyor. BugBounter olarak platformumuzdaki 1800'den fazla uzmanı şirketlerle bir araya getiriyoruz ve bağımsız siber güvenlik uzmanlarının şirketin belirlediği kapsam çerçevesinde yazılımlarının, web sitelerinin, mobil uygulamalarının ve internete açık olan bulut hizmetlerinin 7/24 denetlenmesini sağlıyoruz. Ödül avcılığı olarak adlandırılan bu programda siber güvenlik uzmanları buldukları zafiyetleri sömürebildiğini kanıtladığı anda BugBounter’a raporluyor. Bir sonraki aşamada BugBounter bünyesindeki yetkili ekipler bu raporları kısa sürede doğrulama sürecine tabi tutuyor ve onayladıklarını kuruma iletiliyor. Türkiye'de öncülüğünü üstlendiğimiz bu yöntemle şirketler sadece geçerli açıklar için ve baştan kendi belirlediği ücreti ödüyor. Böylece sonuçsuz hizmet süreleri yerine sadece varlığı kanıtlanan açıklara ödenen bir maliyet oluşuyor. Ayrıca dönemsel önceliklerine uyacak 7/24 siber güvenlik denetimini istediği esneklikte kurgulayıp yönetebiliyor.”

Kaynak

<https://www.cisa.gov/uscert/ncas/alerts/aa22-131a>

<https://therecord.media/revil-ransomware-executes-supply-chain-attack-via-malicious-kaseya-update/>

**İlgili Kişiler:**

Sezin Bulum - Marjinal Porter Novelli

0537 465 82 25

sezinb@marjinal.com.tr

Beril Tuncay – Marjinal Porter Novelli

0532 054 55 38

berilt@marjinal.com.tr

**BugBounter hakkında**

BugBounter, bağımsız çalışan siber güvenlik uzmanlarının niteliksel ve niceliksel açık keşfetme gücünü yasal ve regüle platformda müşterileri ile buluşturmaktadır. 7/24 sürekliliği olan ödül bazlı sızma testleri ile şirketlerin kendilerini siber saldırılara karşı güçlendirmesini sağlayan BugBounter, tüm süreci hem firmalar hem de araştırmacılar için demokratikleştiren tek platformdur. https://bugbounter.com/