**BASIN BÜLTENİ**

**Yaklaşan yaz tatili sezonu, siber saldırganların iştahını kabartıyor**

**Günlük hayatın temposundan uzaklaşmak için benzersiz bir fırsat sunan yaz tatilleri, siber suçlular için de yeni saldırı odağı anlamına geliyor. Sürekli genişleyen siber güvenlik platformundaki 2000 uzmanı ile 7/24 denetlenme imkânı sağlayan BugBounter, tatil planları için hizmet sunan dijital turizm şirketlerini siber saldırılara karşı dikkatli olmaya ve sistemlerinin güvenliğini denetletmeye çağırıyor.**

Şirketlerin güvenlik açıklarını denetleme, bulma ve doğrulama ihtiyacını bünyesindeki 2000 siber güvenlik uzmanıyla esnek, çevik ve güvenilir bir şekilde karşılayan BugBounter ([www.bugbounter.com](http://www.bugbounter.com)), tatil döneminde ziyaretçisi artan şirketleri siber saldırganlara karşı uyarıyor ve bir siber saldırının hedefi olmalarını önleyebilecek ipuçlarını paylaşıyor.

COVID-19 etkisiyle dijitalleşme büyük bir hızla yaygınlaşırken, sunulan hizmetlerin iyileştirilebilmesi için sektörlerin neredeyse tamamında verilerin kıymetini arttı. Siber saldırganlar ise fidye gibi taleplerle yasadışı gelir imkanı yaratmak için odaklarını bu şirketlere döndürdü. Bu süreçte konaklama, araç, seyahat, restoran, konser, parti, plaj rezervasyonu, sportif aktiviteler ile gezi deneyimleri için ziyaret edilebilecek turizm amaçlı web sitelerini veya uygulamaları hedef alarak gelir elde etmek isteyen siber suçlular da mevcut. Dünya Seyahat ve Turizm Konseyi’nin yıllık zirvesinde siber saldırıların küresel ekonomiye verdiği zarar 1 trilyon dolara ulaşmışken 2030’a kadar bu rakamın 90 trilyon dolara ulaşacağı tahmin ediliyor.

Bu tür hizmetler sunan şirketlerin, aşağıdaki yöntemleri kullanarak bünyesindeki hassas müşteri verilerini ele geçirebilecek, verileri değiştirerek haksız kazanç sağlayacak veya erişimleri durdurarak fidye talebiyle karşılaşmasını engelleyecek bir siber saldırıdan kaçınması mümkün.

1. Yenilenen yazılımların ve uygulamaların güvenlik testleri canlıya almadan önce yapılabilir.
2. Çalışanlar farklı tür siber saldırılara karşı eğitilebilir. Siber tehlikeler sürekli geliştiği ve değiştiği için bu eğitimlerin de her zaman yenilenmesi çok önemli.
3. Oltalama saldırıları ile gerçek istekler arasındaki farkı açığa çıkartacak test prosedürleri oluşturulabilir.
4. Kötü niyetli e-postaları en aza indirmek için güçlü spam filtreleri uygulanabilir.
5. Siber saldırganlar bir sisteme sızmanın yeni yollarını keşfettiği için anti-virüs yazılımlarını ve güvenlik duvarlarını 7/24 güncel tutabilir.
6. Habersiz oltalama saldırısı tatbikatıyla ekiplerin farkındalık düzeyi ölçülebilir.
7. Kötü niyetli web sitelerini engellemek için web filtresi kullanılabilir.
8. Çalışanlar güçlü şifreler kullanmaya teşvik edilebilir.
9. Bağımsız siber güvenlik uzmanlarını uygun maliyetle bir araya getiren ödül avcılığı (bug bounty) programları yayına alınabilir ve güvenlik seviyesi bu yolla etkin şekilde artırılabilir.

BugBounter Kurucu Ortağı ve CSO’su Murat Lostar, konuyla ilgili şunları söylüyor: “Yaz tatilleri birçok kişinin günlük hayatın hareketliliğine mola vermek için tercih ettiği ve iple çektiği bir etkinlik. Öte yandan dijitalleşmeyle birlikte müşterilerinin verilerini barındıran şirketlerin önemi artıyor. Bu yüzden araç kiralama ve otel rezervasyonu gibi tatil planlarında kilit rol oynayan şirketlerin siber saldırıya uğradığı haberleriyle karşılaşabiliyoruz. Bu yüzden turizm şirketlerinin kendi BT sistemlerini siber saldırılara karşı düzenli olarak denetletmesi gerekiyor. Bunu da siber saldırganların yöntemlerine aşina olan uzmanlar en verimli şekilde gerçekleştirebiliyor. Biz de BugBounter olarak platformumuzdaki 2000 uzmanımızı sistemlerini gerçek saldırganlar seviyesinde denetletmek isteyen şirketlerle bir araya getiriyoruz. Bizimle çalışan şirketler, sistemlerinde belirledikleri alanları bağımsız siber güvenlik uzmanlarına 7/24 denetletebiliyor. Ödül avcılığı olarak adlandırılan bu programda BugBounter’ın siber güvenlik uzmanları buldukları zafiyetleri platform üzerinden müşteriye raporluyor. Bir sonraki aşamada BugBounter bünyesindeki yetkili ekipler bu raporları kısa sürede doğrulama sürecine tabi tutuyor ve onayladığı zafiyetleri ilgili kuruma iletiliyor. Türkiye'de öncülüğünü üstlendiğimiz bu yöntemle şirketler sadece geçerli açıklar için ve baştan kendi belirlediği ücreti ödüyor. Böylece hizmet süreleri yerine sadece varlığı kanıtlanan başarılı bulgulara ödenen katma değerli bir maliyet oluşuyor.”

**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/