**BASIN BÜLTENİ**

**Siber saldırganlar kamu hizmetlerini sağlayan kurumları hedef alıyor**

**Kamu hizmetlerinden her gün milyonlarca kişi faydalanıyor ve günlük hayatta kritik öneme sahip bu uygulamaların güvenliği hakkında bilgi eksikliği olabiliyor. Kullanılan sistemlerin eski olması veya güvenlik testlerinin modern yöntemlerce güçlendirilmemesi de siber saldırganlara davetiye çıkartıyor. BugBounter.com, platformunda kayıtlı ve sözleşmeli yüzlerce yetenekli siber güvenlik uzmanıyla kurumlara sistemlerini denetletmek için hızlı, güvenilir ve uygun maliyetli bir yöntem sağlıyor.**

Şirketlerin güvenlik açıklarını bulma ve doğrulama ihtiyacını bünyesindeki 900 bağımsız araştırmacıyla hızlı ve güvenilir bir şekilde karşılayan BugBounter.com, belediye, sosyal güvenlik, vergi, sağlık, ulaşım, posta gibi milyonlarca kişinin faydalandığı kamu hizmetlerini sunan kurumları siber saldırılara karşı uyarıyor.

Kamu hizmetleri de dijital dönüşüm sürecinde sunduğu imkanları internet üzerinden sağlayan sektörler arasında yer alıyor. Ancak kamuda geçmişten bu yana kullanılan geleneksel sistemler internet bağlantısı göz önünde bulundurularak geliştirilmediği için bugün sağlanan bağlantıların arayüzleri ve altyapıları saldırganların kolay hedefleri haline geliyor.

Kamu hizmeti sağlayıcılarını risk altına sokan tehditler arasında ilk sıralarda uygulamalardaki kullanıcı hakları yönetimi, veri tabanı erişimleri ve veri girişleri temalı zafiyetler yer alıyor. Uygulamalardaki açıklar siber saldırganların gizli verilere erişimi, verilerin manipülasyonu veya işlemlerin engellenmesi gibi sömürüleri gerçekleştirebilecekleri fırsatları sunuyor. Erişilebilen verilerin büyük ölçekli ve çok noktayla ilişkili yapıları göz önünde bulundurulduğunda saldırının etkisi katlanarak artıyor.

BugBounter Kurucu Ortağı Murat Lostar, konuyla ilgili şunları söyledi: “Dijital dönüşümle birlikte siber saldırganların hedef alabileceği çok daha fazla atak yüzeyi ve zafiyet içeren kolay hedefler var. Kamu kurumlarının sistemlerindeki ve uygulamalarındaki açıklar da düşman ülkelerin hacker’ları için gözde alanlar haline geliyor. Dolayısıyla gelişmiş bir siber güvenliğin vatandaşların internetten kamusal hizmetlere erişimini sağlamak kadar önemsenmesi gerekiyor. Kamu hizmetlerini sağlayan tüm kurumlar için durum aynı. ABD Savunma Bakanlığı, Mart 2021’de kamu hizmeti sağlayan tüm kurumlarının açık “Zafiyet Bildirim Programları” yayınlamalarını ve BugBounter gibi platformlardan bu hizmeti almalarını şart koşan bir genelge yayınladı. Çünkü kurumların sadece kendi ekipleri ile oluşturabilecekleri bütünsel güvenlik seviyesinin günümüzdeki sofistike siber saldırılar karşısında yetersiz kalacağını biliyorlar.

BugBounter.com olarak biz de Türkiye’de kamu kurumlarının sahip olması gereken kapsamlı siber güvenlik testlerini en geniş ekiple, en hızlı şekilde ve en uygun maliyetle sunuyoruz. Platformumuza kayıtlı yüzlerce siber güvenlik uzmanı kurumun belirlediği kapsama göre sistemi veya uygulamayı test ediyor ve bulduğu güvenlik açıklarını BugBounter.com’a iletiyor. Zafiyetin doğrulaması tamamlandıktan sonra da ilgili kurumdaki yetkililer ile paylaşılıyor. Testin kapsamı ve açıkları bulan uzmanlara dağıtılacak ödül gibi başlıklar kurum tarafından belirlendiği için her kurum kendi bütçesine uygun ödül avcılığı programını oluşturabiliyor.”

**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/