**BASIN BÜLTENİ**

**Tüketicilerle birlikte siber saldırganlar da kasım indirimlerini heyecanla bekliyor**

**Dünyanın dört bir yanındaki alışveriş severlerin her yıl merakla beklediği kasım ayı indirim dönemleri başlıyor. Ancak siber saldırganlar da online alışveriş hacminin ve alışveriş yapan kişi sayısının büyük ölçüde arttığı bu dönemleri tüketiciler gibi iple çekiyor. E-ticaret sitelerine karşı gerçekleştirilebilecek saldırıların hedefi olmamak ve indirim döneminde dolandırıcılık kurbanı olmamak için platformunda 1000’den fazla bağımsız siber güvenlik uzmanı bulunan BugBounter hem şirketlere hem de tüketicilere yönelik ipuçlarını paylaşıyor.**

COVID-19 ile birlikte artan dijitalleşme ve fiziksel yapılan birçok sürecin online dünyaya taşınması artık tüm dünyada gözlemlenen bir gerçek. Dijital dünyada yapılan işlem hacmindeki artışın siber suçlular için fırsat yarattığı da birçok kişinin farkında olduğu, ancak şirketlerle birlikte daha fazla kişinin dikkat etmesi gereken bir durum. Şirketlerin güvenlik açıklarını denetleme, bulma ve doğrulama ihtiyacını bünyesindeki 1000’in üzerinde bağımsız araştırmacıyla hızlı ve güvenilir bir şekilde karşılayan BugBounter.com, dünya çapında indirimlerin yapıldığı kasım ayında e-ticaret sitelerini ve bu indirimleri değerlendirmeyi planlayan tüketicileri siber saldırılara karşı uyarıyor ve kendilerini korumasına yardımcı olacak bilgiler aktarıyor.

Son birkaç yıl içinde siber saldırıların sıklığına paralel olarak bu saldırıların gelişmişlik düzeyi ve yarattığı yıkıcı etkide artış gösteriyor. Birçok sektörde olduğu gibi e-ticarette de bu artış etkisini gösteriyor. Özellikle 2020’de artan online alışveriş de siber saldırganların iştahını kabartıyor. Sadece Eylül 2020’de online ticaretin büyüklüğü kapanma öncesi Mart 2020’ye kıyasla yüzde 49 arttı.

Kasım itibariyle e-ticaretin adeta doruk yapacağı bir döneme giriş yapıldı. Tüm dünyada beklenen artışın en önemli sebeplerinden birisi olan kasım indirimleri Türkiye’de de heyecanla bekleniyor. Ancak online alışveriş yapacak tüketicilerin yanı sıra siber saldırganlar da bu heyecanı paylaşıyor.

Bu süreçte kullanıcıları oltalama denemeleri, kötü amaçlı yazılımlar, fidye yazılımları ve güvenilir e-ticaret sitelerinin büyük oranda benzerleri gibi birçok tehdit bekliyor. Online alışveriş dönemini mümkün olan en güvenli şekilde gerçekleştirmek için de şirketlerin ve kullanıcıların bazı önlemler alması gerekiyor.

**Şirketler siber güvenlik yapılarını mutlaka denetletmeli**

Konu siber güvenlik olunca sadece kullanıcıların değil, şirketlerin de adım atması gerekiyor. Kampanya döneminde web sitesine gelecek trafiğin ve sosyal medyada markayla ilgili konuşmaların yükseleceği bu dönemlerde siber güvenlik alanında yapılan yatırımları da artırmak gerekiyor. Çünkü e-ticaret siteleri gibi kötü niyetli hackerlar da bu dönemi bekleyip gerek son kullanıcı bilgilerini gerekse e-ticaret şirketinin bilgilerine ulaşmaya çalışıyor. Bu alanda yapılacak bir kontrol, siber suçluların önünü başarıyla kesebiliyor. Öte yandan sahteciliğe karşı korumalarını da güçlendirebilir ve müşteri hizmet ekiplerini olası sorunlara karşı hazırlayabiliyor.

BugBounter.com Kurucu Ortağı Murat Lostar, konuyla ilgili şunları söyledi: “Şirketler alabileceği tüm önlemlere ek olarak uygun maliyetle sistemlerini denetletebilir ve bir siber saldırgan yıkıcı sonuçlar yaratmadan açığını kapatarak bu önemli indirim dönemini daha kolay bir şekilde atlatabilir. Güvenliğin en üst düzeyde olduğundan emin olmak için gerçekleştirilebilecek düzenli bir bug bounty (ödül avcılığı) programı, potansiyel ve mevcut açıkların keşfedilmesinde en etkili adımlardan biri olarak öne çıkıyor. Çünkü şirketler bug bounty programları sayesinde sistemlerini olası bir siber saldırıya karşı en uygun maliyetle, en yetenekli uzman ordusuna denetletebiliyor. İncelemeye birkaç kişi değil, yüzlerce araştırmacı dahil oluyor. BugBounter.com olarak ülkemizde öncülük ettiğimiz bu yöntem sayesinde kurumlar sadece varlığı deneyimli uzmanlar tarafından doğrulanmış güvenlik açıkları için ücret ödüyor ve bu sayede ayırdıkları bütçeleri verimli bir şekilde yönetebiliyor. Ayrıca siber güvenlik uzmanlarına vereceği ödülü, programın takvimini ve kapsamını kendi belirleyebildiği ve her an düzenleyebildiği için sistemlerinin güvenliğini o anki bütçelerine ve iş planlarına uygun olarak kontrol ettirebiliyor. Platformun güvenlik araştırmacıları, buldukları zafiyetleri raporladıktan sonra yetkili ekiplerimiz kısa süre içinde doğrulama süreçlerini tamamlıyor, önemine göre derecelendiriyor ve şirketin belirlediği güvenlik ekiplerine iletiyor. Kapatılan açıkların kontrolü de yine aynı uzmanlarca gerçekleştiriliyor.”

Şirketler siber güvenlik yatırımlarını artırırken bu dönemi bekleyen kullanıcıların da kendi güvenlikleriyle ilgili konulara daha fazla özen göstermesi gerekiyor. Kullanıcıların alabileceği önlemler de aşağıda yer alıyor.

**Güçlü ve özel şifreler kullanılmalı**

Ele geçirilen giriş bilgilerinin yüzde 37’si çalıntı ya da düşük şifreyle korunuyor. Bu yüzden en az 8 karakterli, büyük ve küçük harfin yanı sıra rakam ve noktalama işaretleri içeren bir şifre kullanılması çok önemli. Ayrıca giriş bilgilerinin başkalarıyla paylaşılmamasına ek olarak herhangi bir e-ticaret sitesine giriş için belirlenen bilgilerin başka üyeliklerde kullanılmaması da büyük fark yaratıyor. Şifreleri ezberlemekte zorlanan kişilerin de yardımına şifre yöneticileri koşuyor.

**Cihazların eksiksiz bir şekilde korunması çok önemli**

Bireysel cihazların yanı sıra pandemiyle birlikte evde kullanılmaya başlanan iş bilgisayarları gibi internet bağlantısı bulunan cihazlarda tehditlere karşı koruma için antivirüs yazılımının ve güvenlik duvarının kurulmuş olması gerekiyor.

**Sosyal mühendislik denemelerine karşı tetikte olmak gerekiyor**

Siber saldırganların cihazları ele geçirmesini engellemenin en etkili yollarından birisi, sosyal mühendislik olarak da adlandırılan birçok yanıltıcı yöntemle yanlış linke tıklama ihtimaline karşı dikkatli olmaktan geçiyor.

Yasal kurumlar kullanıcılarından isim ve şifre bilgilerini asla talep etmez. Dolayısıyla herhangi bir sebepten birisi şifre sorduğunda cevap her zaman net bir şekilde “Hayır” olmalı. Ayrıca şüpheli görünen bir e-postadaki bağlantılar da tıklandığı zaman yüksek ihtimal cihazınıza zarar verecektir. Bunun önüne geçmek için e-postadaki gözden kaçmayan yazım hataları, e-postayı gönderen adresin uzantısı ve e-postadaki linkin gönderdiği adrese dikkatli bakmak gerekiyor. Adres uzantısı ve link gibi bilgiler gerçek sayfayla büyük ölçüde benzerlik gösterebileceği için özellikle bu kısımlara karşı tetikte olmak, bir saldırının hedefi olmak ile olmamak arasındaki farkı belirleyebilir.

**Başında HTTPS olan web sitelerini tercih edin**

HTTP ile HTTPS arasındaki tek bir “S” harfi güvenlik açısından çok büyük fark yaratabiliyor. Yalnızca bir web sitesinin kimliğini doğrulayan ve şifreli bir bağlantı sağlayan dijital SSL sertifikasıyla elde edilebilen HTTPS, web sitesinin güvenli olmasına yardımcı oluyor.

**Kaynak**

<https://www.cybervore.com/blog/e-commerce-cybersecurity-enhancing-data-protection-in-2021/>

<https://www.verizon.com/about/news/verizon-2020-data-breach-investigations-report>

**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/