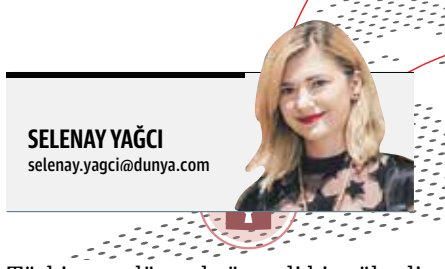
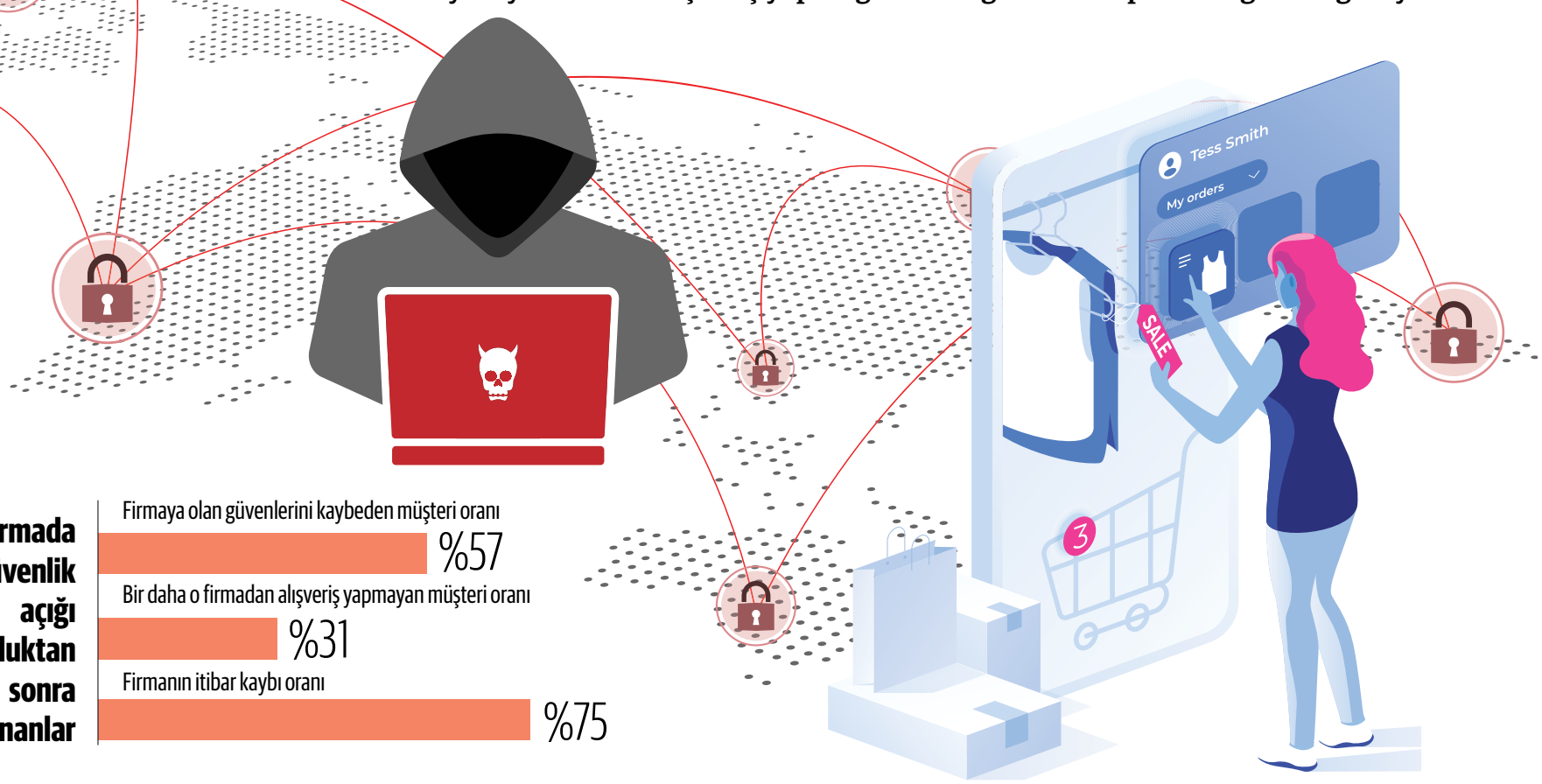
KOBİ'LER SİBER SALDIRILARA KARŞI kendilerini nasıl korumalı?

E-ticarette güvenlik, yalnızca güvenlikten ibaret olmanın ötesinde anlamlar taşıyor. Satışları artırmanın da en önemli koşullardan biri. Milyonlarca tüketici, veri hırsızlığı olaylarıyla birlikte alışveriş yapacağı sitenin güvenli olup olmadığını sorguluyor...



SELENAY YAĞCI
selenay.yagci@dunya.com



Türkiye ve dünyada önemli bir yükseliş trendi yaşayan e-ticaret, her ölçekte girişimciye önemli fırsatlar sunuyor. Ancak giderek artan ve pandemi dönemiyle de belirgin bir ivme kazanan bu yükseliş, e-ticaret platformlarının teknik kapasitesi kadar güvenliğini de öne çıkarıyor. E-ticarette uygun fiyat önemli ama tüketicilerin yüzde 92'si öncelikle güvenli alışveriş endişesi taşıyor. Pek çok tüketici, son dönemde art arda yaşanan veri hırsızlığı olaylarıyla alışveriş yapacağı sitenin güvenli olup olmadığı sorguluyor. Yakın zamanda Yemeksepeti gibi büyük bir platformun dahi kullanıcı bilgilerinin çalındığını açıklamasıyla güvenlik konusunun e-ticarette daha da sıcak gündem haline geldiğini söyleyebiliriz.

KOBİ'ler yüzde 91 ile bu saldırılara en çok maruz kalan firma grupları arasında yer alıyor. Gerek dijital güvenlik için ayırdıkları bütçenin çok az veya hiç olmaması gerek maliyetlerinden dolayı bu iş için bünyelerinde personel eksikliği yaşanması KOBİ'leri bu konuda saldırıya açık hale getiriyor. Uzmanlara göre KOBİ'lerin bu sorunu aşmasında en mantıklı yol ise altyapı hizmeti satın alırken bu konuda yatırım yapmış ve daha da önemlisi bu konuda tüm süreçleri canlı takip eden firmalar ile çalışmak.

E-ticarette güvenliğin, satışları artırmak için ilk ve en önemli koşullardan biri haline geldiğini belirten Projesoft CEO'su Bilgisayar Mühendisi Yüksel Eminoğlu, tüketicilerin yaşadığı güvenlik kaygılarına bu konuda yapılan araştırmalardan örneklerle dikkat çekti. ABD kaynaklı FBI fraud (çalıntı kart kullanımı) şikâyet raporlarından veriler paylaşan Eminoğlu, 2018 yılında 351 bin 937 olan suç duyurusu sayısının 2019 yılında 467 bin 361'e ulaştığını ve bu sayının Mart 2020'ye gelindiğinde 320 bin adeti geçtiğinin söyleyerek, "Bu tarz saldırıların artması ve tüketicilerin her geçen gün daha etkili saldırı yöntemlerine maruz kalması, artık günlük ihtiyaçlarını bile internetten tedarik eden tüketicilerde bir güvensizlik oluşturuyor. trsutedsite.com tarafından yapılan bir araştırma ABD'de online alışveriş yapan kişilerin yüzde 92'sinin kişisel bilgilerinin çalınması konusunda endişeli olduğunu ortaya koymuş durumda" şeklinde konuştu.

VERİ HIRSIZLIĞI EN ÇOK HANGİ ALANLARDA OLUYOR?

Yüksek satış rakamlarına ulaşabilmek için e-ticaret platformlarında tüketiciye güven veren altyapıların bugün daha da önem kazandığına dikkat çeken Eminoğlu, şunları anlattı: "İnternet ve bulut üstünde tutulan bilgiler arttıkça bu konuda ihlaller ve hırsızlıklar da buna istinaden katlanarak artıyor. Bu konuda yapılan pek çok çalışma var. Trustwave 96 ülkeye güvenlik konularında hizmet veren bir firma. Bu firmanın yaptığı araştırmaya bakıldığında saldırıların yüzde 91'i KOBİ'lere gerçekleştiriliyor. Bu grup içinde yüzde 45 ile perakende en çok saldırıya maruz kalan sektör olurken bunu yüzde 24 gıda ve restoran, yüzde 9 ile de konaklama hizmetleri takip ediyor. Bunun sebebi de firmaların bu ihlaller için gerekli bütçeyi ayıracak durumda olmamaları ve gerektiğinde de bu süreçleri takip edebilecek personellerinin olmaması."

KREDİ KARTI BİLGİLERİNİN GÜVENLİĞİ İÇİN ÖZEL TEKNOLOJİ YATIRIMINA MI İHTİYAÇ VAR?

Projesoft CEO'su Eminoğlu "Geçen yıl 4.19 trilyon dolarlık hacme ulaşan e-ticaret ile birlikte kredi kartlarının kullanım oranı da katlanarak arttı. Dünyada kredi kartları konusunda en etkin 3 marka Visa, Master ve American Express. Bu firmalar da 2006'da PCI (Payment Card Industry) konsülünü kurdu ve kredi kartları kullanımı için firmalara belli güvenlik standartları getirdi. Türkiye'ye bakarsak bankalar, ödeme kuruluşları ve yüksek miktarda kredi kartı işlemi yapan firmaların PCI DSS Level 1 sertifika alması zorunlu. Bu yatırımın değeri yıllık en az 100 bin dolar civarı bir maliyetten başlıyor" diye konuştu.


Yüksel Eminoğlu

KREDİ KARTI BİLGİLERİNİN ELE GEÇİRİLMESİ ŞİRKETLERE NELERE MAL OLUYOR?

Eminoğlu ayrıca konuyla ilgili şunları anlattı: "Kredi kartı bilgileri hackerlar tarafından ele geçirilmek için en çok emek harcanan veriler arasında. Sebebi ise her geçerli kartın satışından elde edilen paranın oldukça yüksek olması (5-15 dolar). Bu işi yapan hiçbir hacker kredi kartını kendisi kullanmaz; bu bilgileri toplu halde satar. Dolayısıyla çalınan kredi kartlarından sadece son kullanıcı müşteriler değil, o kartın çalındığı site ve daha da önemlisi o kartı veren banka maddi ve manevi zarara uğrar. Bu olay gerçekleştikten sonra ise;

- Kart bilgilerinin çalındığını düşündükleri siteye PCI Konsülü tarafından yetkili olarak kılınmış bir PFI Umanına Forensic Araştırma yaptırılır. Bu hizmetin ortalama maliyeti 36 bin dolar civarında. Burada tüm sistem bu işin uzmanları tarafından detaylı olarak taranarak ne büyüklükte bir veri çalındığı ve hangi yolla ele geçirildiği araştırılır.
- Bu işten etkilenen tüm müşterilerin bilgilendirilmesi gerekiyor. Bu da firmalara hem maddi bir külfet hem de itibar ve satış kaybı demek.
- Gerçekleşen fraud işlemler için firmalara ceza kesiliyor. Buradaki tutarlar bu firmalardan tahsil edilebiliyor.
- Kredi kartı bilgileri çalınan müşterilerin kredi kartları yenisi ile değiştiriliyor ve bunlar için de sorunun gerçekleştiği firmadan para tahsil ediliyor.
- PFI taramasına göre çıkan açık ve eksiklerin tamamlanması için yaptırım/düzeltmeler yapılması talep ediliyor.
- PCI uyumu için yeniden başvuru yapıp tüm süreçleri baştan geçmesi gerekiyor."

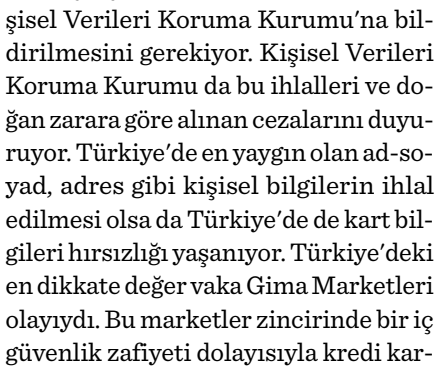
TÜRKİYE'DE ŞİMDİYE KADAR BÜYÜK ÖLÇEKLİ KART BİLGİLERİ HIRSIZLIĞI VAKASI OLDU MU?

Türkiye'de Kişisel Verileri Koruma Kanunu çerçevesinde, bu tür ihlaller, Kişisel Verileri Koruma Kurumu'na bildirilmesini gerekiyor. Kişisel Verileri Koruma Kurumu da bu ihlalleri ve doğan zarara göre alınan cezalarını duyuruyor. Türkiye'de en yaygın olan ad-soyad, adres gibi kişisel bilgilerin ihlal edilmesi olsa da Türkiye'de de kart bilgileri hırsızlığı yaşanıyor. Türkiye'deki en dikkate değer vaka Gima Marketleri olayıydı. Bu marketler zincirinde bir iç güvenlik zafiyeti dolayısıyla kredi kartı bilgileri çalınmıştı ve bu firma tüm dolandırıcılık ve kredi kartı ücretlerini ödemek durumunda kalmıştı. Daha sonra da bu marketler zinciri tarihin tozlu raflarında yerini aldı.

NASIL CEZALARLA KARŞILAŞILIYOR?

Dünya geneline bakıldığında bu konuda son 5 yılda aklında kalan iki büyük olay var

- Marriott Hotel 2018'de gerçekleşen ifşada 500 milyon civarı müşteri datasını kaybetti ve kendilerine kesilen ceza, 124 milyon dolardı.
- Equifax firmasında 2017'de yüzlerce milyon müşteri datası çalındı. Buna istinaden şirkete de 575 milyon dolar ceza kesildi.



- 2013 yılında Adobe 153 milyon kullanıcı bilgisi ve 3 milyon da kredi kartı bilgisi çaldırdı. Bunun karşılığında 1.1 milyon dolar ceza ödedi.

SALDIRILARA MARUZ KALMAMAK İÇİN EN BAŞTA EDR TEKNOLOJİSİ KULLANILMALI

ADEO CSO'su Halil Öztürkci ise şunları söyledi: "Pandemi ile birçok KOBİ için e-ticaretin çok daha hayati bir konuma geldiğini biliyoruz. Bununla birlikte bu süreç siber saldırganların da yeni hedefler belirlemelerine, yeni saldırı teknikleri geliştirmelerine sebep oldu. Hem kendi platformları üzerinden e-ticaret yapan işletmeler hem de pazar yerleri üzerinden e-ticaret yapan firmalar birçok farklı siber saldırıya maruz kaldı. Özellikle müşterilere ait kredi kartı bilgileri ve diğer kişisel verileri ele geçirmeyi amaçlayan saldırılarla birlikte e-ticaret sitelerinin çalıştığı sistemleri ele geçirerek bu sistemlerde çalıştırdıkları fidye yazılımları ile sistemleri şifreleyip para karşılığında şifreyi geri vermeyi vadeden saldırılar son zamanlarda oldukça sık yaşanıyor. Türkiye'den işletmeler de bu saldırılardan fazlasıyla nasibini almış durumda. Bu tür saldırılara maruz kalmamak adına yapılması gerekenlerin başında e-ticaret sitelerinin çalıştığı sunucuların tamamında görünürlüğü sağlayacak bir teknolojinin (EDR teknolojisi) kullanılması geliyor. Bu teknoloji sayesinde sistemlerdeki olası şüpheli hareketler çok hızlı şekilde tespit edilebiliyor ve müdahale gerçekleştirilebiliyor. Bu teknolojilerin çıktılarını yorumlamak için de alanında uzman, iyi yetişmiş siber güvenlik uzmanlarına ihtiyaç var. KOBİ'lerin burada hem teknolojiyi hem de uzmanlığı bir servis olarak birlikte alabilecekleri seçenekler mevcut. ADEO olarak bu konuda birçok KOBİ'ye hizmet sunuyoruz. Ayrıca ilgili e-ticaret platformlarında belirli aralıklarla sızma testlerinin ve kaynak kod analizlerinin yapılması ve olası açıklıkların saldırganlardan önce tespit edilerek kapatılması da siber güvenliği sağlama noktasında hayati bir öneme sahip."

Siber farkındalık eğitimleri düzenleyin

İnfrasis Siber Mühendislik Genel Müdürü **Can Sobutay,** KOBİ'lerin kendini siber saldırılardan koruyabilmesi adına önerilerini şöyle sıraladı:

► Asgari haklar ilkesini uygulayın ve kullanıcıların erişim haklarını yalnızca işlerini yerine getirmek için ihtiyaç duydukları haklarla sınırlayın. Personel kuruluşunuza katılırken, kuruluşunuzdan ayrılırken ve rolleri değiştikçe kullanıcı erişim haklarını güncelleyin.

► Erişimi değerlendirirken, belgelerdeki ve/veya sunucularda depolanan verilerdeki bilgilerin sınıflandırma düzeyini (örneğin; gizli, halka açık) göz önünde bulundurun. Hassas bilgileri; güvenli alanlarda ve erişimi yalnızca ihtiyacı olan kişilerle sınırlayan sistemlerde sakladığınızdan emin olun.

► İşten çıkarılan personellerden ve kısa dönemli kurum dışından destek veren üçüncü partilerden kaynaklı oluşabilecek güvenlik risklerini ortadan kaldırmak için BT ve İK'nın birlikte çalışmasını, hızlı çözüm üretmesini sağlayın.

► Siber farkındalık eğitimleri düzenleyin.

► Personelin kimlik avı dolandırıcılıklarını tanımasına yardımcı olun. Çalışanlardan şüpheli e-postaları veya dosyaları rapor etmelerini isteyin.

► En güvenilir ve doğrulanmış yazılımların ve dolandırıcılıkla mücadele hizmetlerinin kullanıldığından emin olmak için bankalar veya onaylı aracılar ile birlikte çalışın. Bankanız veya aracınızla yaptığınız anlaşmalar da, güvenlik yükümlülüklerinin kapsamlı olmasına dikkat edin.

► Arızalı BT ekipmanının bakım için güvenli bir şekilde iade edilmesine ve yeni BT ekipmanının gönderilip güvenli bir şekilde yapılandırılmasına olanak tanıyan süreçlerin ve kılavuzların devreye alınmasını sağlayın.

► Verileriniz ve siber suçlular arasında bir bariyer sağlamak için bir güvenlik duvarı kullanın ve internet yönlendiricinizde / güvenlik duvarınızda en son ürün yazılımının yüklü olup olmadığını düzenli kontrol edin.

► Cihazlarınızın güvenliğini sağlamak için işletim sisteminiz, web tarayıcınız ve diğer tüm yazılımlarınız için yeni güvenlik yamalarını uygulayın.

► Standart harici güvenlik duvarına ek olarak, birçok şirket ek koruma sağlamak için dahili güvenlik duvarları kurmaya başladı. Evden çalışanların da ev ağlarına bir güvenlik duvarı yüklemeleri önemli.

► Çok faktörlü kimlik doğrulama kullanın, bu size ekstra bir koruma katmanı sağlayacaktır.

► Tüm verileri düzenli olarak yedekleyin.

► Kötü amaçlı yazılımdan (malware) koruma yazılımı yükleyin.