25 Şubat 2025

Kişisel Veri İhlali Bildiriminde "Koyu" Gri Alan
Kimlik Bilgisi Doldurma Saldırıları (Credential Stuffing)
ya da
"Veriler Bizden Sızmadı ki, Neden Veri İhlal Bildirimi Yapalım?"

Bilindiği gibi ülke kapsamında yurtiçi ve yurt dışı kaynaklı siber tehditleri tespit etme ve önleme faaliyetleri yürüten Ulusal Siber Olaylara Müdahale Merkezi (USOM), siber güvenlik faaliyetlerine yönelik yürüttüğü çalışmalar çerçevesinde ilgililere yönelik olarak dönem dönem alarm, uyarı ve duyuru işlemleri yapmaktadır. Bu kapsamda yürüttüğü siber tehdit istihbaratı faaliyetleri kapsamında, bazı kullanıcı hesaplarının siber saldırganlar tarafından ele geçirildiğini değerlendirdiğinde de bu kullanıcı hesaplarının ilgili olduğu şirketlere (veri sorumluları) yazı göndererek durumdan haberdar olmalarını sağlamakta ve önlem almalarını talep etmektedir.

Bu tür yazıları alan veri sorumluları şimdi ne yapmalıyız sorusunun cevabını ararken değerlendirilen akla gelen en son seçenek -o da uzmanların bu konudaki yönlendirmeleri sayesinde- kişisel veri ihlali bildirimi yapmak oluyor. Veri sorumlularının ilk tepkisi "*E kullanıcı adı ve şifre bizden sızmamış ki neden biz kişisel veri ihlali bildirimi yapmalıyız?*" oluyor.

Kimlik bilgisi doldurma saldırısı ile karşılaşan herkesin aklından benzer sorular geçmesi çok doğal. İşte bu sorunun cevabının neden "Evet" olması gerektiğini bu yazımızda sizler için açıkladık.

1. Nedir?

Kimlik bilgisi doldurma saldırıları, siber dünyada hızla yayılan ve kullanıcıların güvenliğini ciddi şekilde tehdit eden sofistike bir saldırı yöntemidir. Bu saldırı yönteminde siber saldırganlar, ya bizzat kendileri bir platforma saldırarak oradan kullanıcı adı ve şifre kombinasyonunu ele geçirirler ya da diğer saldırganlar tarafından halihazırda ele geçirilmiş ve çeşitli platformlarda satılan veri tabanlarını satın alarak bu kullanıcı adı ve şifre kombinasyonuna ulaşırlar. Daha sonra bu kişiler, elde ettikleri bu kullanıcı adı ve şifre kombinasyonlarını, farklı platformlarda deneyerek bu platformdaki kişisel verilere yetkisiz şekilde erişmeye çalışırlar.

Bu saldırılar genellikle otomasyon sağlayan bot yazılımlarla gerçekleştirilir ve kullanıcıların aynı şifre ve kullanıcı adı kombinasyonlarını birden fazla platformda kullanma alışkanlığı nedeniyle büyük oranda başarıya ulaşır.

Bu saldırı yöntemi, klasik parola kırma yöntemlerinden, yani kaba kuvvet saldırılarından (*brute-force attack*) önemli bir farkla ayrılır. Zira kaba kuvvet saldırısında, saldırganlar doğru kullanıcı adı ve şifre kombinasyonuna sahip değildir, amaçları sistematik şekilde çok sayıda deneme yaparak bu doğru kombinasyona ulaşmaktır. Oysa kimlik bilgisi doldurma saldırılarında saldırganlar, doğru kullanıcı adı ve şifre kombinasyonuna sahiptir, yapmaları gereken bu kombinasyonu farklı platformlarda deneyerek hangi platformlarda kullanıldığını

bulmaktır. Dolayısıyla bu saldırıların tespit edilmesi, diğer saldırı türlerine göre daha zordur ve bu nedenledir ki geleneksel güvenlik önlemleri (örneğin, güvenlik duvarları ve standart parola korumaları) bu tür saldırıları önlemekte yetersiz kalabilmektedir.

2. Hangi Riskler Söz Konusu?

Başarılı bir kimlik bilgisi doldurma saldırısı bireyler için oldukça ağır sonuçlar doğurabiliyor. Kredi kartı bilgilerinin çalınması, hassas kişisel verilerin ifşa edilmesi, finansal kayıplar ve itibar zedelenmesi gibi ciddi riskler, bu saldırıların bireyler için yaratabileceği yıkıcı etkiler arasında yer alıyor. Bu tür saldırılar sonrasında özel görüntüleri ele geçirilen bireylerin, saldırganların şantajlarına maruz kaldığı ve bu mağdurlardan bazılarının intihar ederek yaşamına son verdiği de biliniyor.

Bu nedenle bu tür saldırılan başarıya ulaşmasında ilgili kişilerin bilinçlenmesi (örneğin, aynı kullanıcı adı ve şife kombinasyonunu farklı platformlarda kullanmama) önemli olduğu kadar bu platformları işleten veri sorumlularına da bu platformların güvenliğini sağlama ve bu tür saldırıları önlemek için tedbirler alma anlamında çok önemli görevler düşüyor.

3. Kişisel Verileri Koruma Kurulu Bu Soruya Nasıl Cevap Veriyor?

En baştan söyleyelim ki Kişisel Verileri Koruma Kurulu'nun ("**Kurul**") bu soruya cevabı "Evet, Kişisel veri ihlali bildirimi yapılmalıdır" şeklinde. Nitekim bu konu, Kurul tarafından yayımlanan kararlarda (sırasıyla bu kararlar; 2020/421 Sayılı Karar, 2020/567 Sayılı Karar, 2020/715 Sayılı Karar ve 2024/1385 Sayılı Karar) defaatle ortaya konulduğu gibi konunun önemine binaen Kurul bu konuya özel olarak 15 Şubat 2022'de bir duyuruda da ("**Duyuru**") (Bkz. "Kullanıcı Güvenliğine İlişkin Veri Sorumluları Tarafından Alınması Tavsiye Edilen Teknik ve İdari Tedbirlere İlişkin Kamuoyu Duyurusu) yayımlamıştı (Bkz. İlk üç karar ve Duyuru'yu incelediğimiz yazımız).

Tüm bu kararlar ve Duyuru birlikte değerlendirildiğinde söyleyebiliriz ki Kurul, veri sorumluları tarafından alınacak bazı idari ve teknik tedbirlerle bu saldırıların, -ilgili veri sorumlusunun platformu yönünden- önlenebileceği kanaatinde. Bu nedenle de böyle bir saldırı gerçekleşirse, saldırının kaynağı ne olursa olsun, veri sorumlusu, saldırıdan haberdar olur olmaz yetmiş iki saat içerisinde durumu Kurul'a bildirmekle yükümlü, diğer bir değişle kişisel veri ihlali bildirimi yapmalı. Aynı zamanda en kısa sürede ilgili kişilerin bilgilendirilmesi de gerekiyor.

Her ne kadar Kurul, duyurusunda ve kararlarında "Kimlik Bilgisi Doldurma Saldırısı" veya "Credential Stuffing" tabirini kullanmasa da bu duyuru ve kararların içeriğinden saldırı türünün kimlik bilgisi doldurma saldırısı olduğu anlaşılıyor.

4. Ne Yapılmalı?

Yukarıda ifade ettiğimiz gibi bu tür saldırılara muhatap olan veri sorumluları kişisel veri ihlali bildirimi yapmak konusunda yeterince bilinçli olmamalarından kaynaklı isteksiz davranmaktaysalar da yakın zamanda yayımlanan 2024/1385 sayılı kararda verilen idari para cezası miktarının 3.250.000 TL olduğu ve bu miktarın, Kurul'un geçmiş kararlarında verdiği

cezalarla kıyaslandığında rekor seviyede sayılabileceği dikkate alındığında veri sorumlularının, bu tür saldırıların önlenmesi konusunda adım atmaları ve bir saldırı meydana geldiğinde Kurul'a bildirim yapmak konusunda daha dikkatli değerlendirmeler yapmaları gerektiği açık.

Alınabilecek idari ve teknik tedbirler çok çeşitli olsa da Kurul kararlarında ve Duyuru'da yer verilen tedbirleri aşağıdaki gibi sıralamak mümkün:

- Çift kademeli kimlik doğrulama (*two-factor authentication*) sistemlerinin kurulması ve bu sistemlerin kullanıcılara üyelik başvurusu aşamasından itibaren "alternatif" bir güvenlik önlemi olarak sunulması,
- Kullanıcıların hesaplarına sık kullandıkları cihazlar dışında farklı bir cihaz üzerinden giriş yapıldığında, giriş bilgilerinin e-posta/SMS veya benzeri yöntemlerle ilgili kullanıcının iletişim adreslerine bildirilmesinin sağlanması,
- Uygulamaların HTTPS (*Hypertext Transfer Protocol Secure* - Hiper Metin Aktarma Güvenli İletişim Kuralı) kullanılarak veya eşdeğer bir güvenlik seviyesi sağlayacak başka yöntemlerle korunmasının sağlanması,
- Kullanıcı parolalarının, siber saldırılara karşı korunmasını teminen, güvenli ve güncel karma (*hashing*) algoritmaların kullanılması,
- IP (*Internet Protocol Address*) adresinden yapılacak başarısız giriş denemesi sayısının sınırlandırılması,
- İlgili kişilerin en az son beş adet başarılı ve başarısız giriş denemeleri ile ilgili bilgilerini görüntüleyebilmelerinin sağlanması,
- İlgili kişilere aynı parolanın birden fazla platformda kullanılmaması gerektiğinin hatırlatılması,
- Veri sorumluları tarafından parola politikasının oluşturulması ve kullanıcılara ait parolaların belirli aralıklarla değiştirilmesinin sağlanması veya bu hususun ilgili kişilere hatırlatılması,
- Yeni oluşturulan parolaların, eski parolalarla (en az son üç parolayla) aynı olmasının engellenmesi, kullanıcı hesaplarına girişlerde bilgisayar ile insan davranışlarını ayırt edici güvenlik kodu gibi teknolojilerin (CAPTCHA, dört işlem vb.) kullanılması, erişime izin verilen IP adreslerinin sınırlandırılması,
- Veri sorumlularının sistemlerine giriş yapılan parolaların uzunluğunun asgari 10 karakter olması, büyük-küçük harf, rakam ve özel karakterlerin bir arada kullanılmasına yönelik güçlü parola oluşturulmasının sağlanması,
- Veri sorumlularının sistemlerine giriş için üçüncü parti yazılımlar veya servisler kullanılıyorsa bu yazılımların ve servislerin güvenlik güncelleştirmelerinin düzenli olarak gerçekleştirilmesi ve gerekli kontrollerin yapılması gibi teknik ve idari tedbirlerin alınması.

5. Tavsiyemiz

Kurul'un bu tür saldırıların kişisel veri ihlali olarak kendisine bildirilmesini beklediği dikkate alındığında kimlik bilgisi doldurma saldırısına muhatap olan veri sorumluları öncelikle bu tür

saldırıların başarıya ulaşmasını önlemek adına gerekli idari ve teknik tedbirleri almaları, böyle bir saldırıya maruz kalırlarsa da durumu Kurul'a ve ilgili kişilere bildirmeleri önemli. Bu nedenle başta kullanıcı adı – şifre kombinasyonlarıyla giriş yapılabilen internet ve mobil platformları işleten veri sorumluları olmak üzere tüm veri sorumlularının bu önlemleri vakit kaybetmeden hayata geçirmesini tavsiye ediyoruz.

Saygılarımızla,

Bora Yazıcıoğlu
bora@yazicioglulegal.com

Kübra İslamoğlu Bayer
kubra@yazicioglulegal.com

Barış Yiğitcan Duran
barisyigitcan@yazicioglulegal.com

Bu not hukuki görüş niteliğinde değildir. Sadece bilgi amaçlı hazırlanmış ve gönderilmiştir. Konuyla ilgili hukuki görüş almak isterseniz bizimle iletişime geçmenizi rica ederiz.