KULLANICI GÜVENLİĞİNE İLİŞKİN VERİ SORUMLULARI TARAFINDAN ALINMASI TAVSİYE EDİLEN TEKNİK VE İDARİ TEDBİRLERE İLİŞKİN KAMUOYU DUYURUSU KİŞİSEL VERİLERİ KORUMA KURUMU TARAFINDAN YAYIMLANMIŞTIR

Kişisel Verileri Koruma Kurumu ("**Kurum**") tarafından kullanıcı güvenliğine ilişkin veri sorumluları tarafından alınması tavsiye edilen teknik ve idari tedbirlere ilişkin kamuoyu duyurusu ("**Duyuru**") 15 Şubat 2022 tarihinde yayımlanmıştır. Duyuru kapsamında:

- 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun kişisel veri güvenliğine ilişkin 12. maddesi çerçevesinde son zamanlarda Kurum'a intikal eden veri ihlal bildirimlerinin değerlendirildiği,
- finans, e-ticaret, sosyal medya ve oyun gibi muhtelif sektörlerde faaliyet gösteren veri sorumlularının internet sitelerine giriş için kullanılan kullanıcı hesap bilgilerinin (kullanıcı adı ve parolalar) bazı internet sitelerinde herkese açık şekilde yayınlandığının görüldüğü,
- söz konusu kullanıcı hesaplarını elde eden üçüncü kişilerce, anılan veri sorumlularının internet sitelerine kullanıcıların haberi olmadan aktif bir şekilde giriş yapıldığının ve ilgili kişilere ait verilerin bu kapsamda görüntülenebildiğinin tespit edildiği,
- veri sorumluları sistemlerinden veya güvenlik açıkları kullanılarak son kullanıcı bilgisayarlarından elde edilen kişisel verilerin hukuka aykırı bir şekilde paylaşıldığının ve ekonomik bir değer karşılığında satışa sunulabildiğinin görüldüğü,
- ilgili kişilere ait bu verilerin elden ele dolaşıp kötü niyetli kişilerce arşivlenerek daha büyük veri setleri halinde yeniden pazarlanabildiği,
- veri sorumluları ve veri işleyenler tarafından veri güvenliği kapsamında alınacak teknik ve idari tedbirlerin olası veri ihlal durumlarını ve ilgili kişiler üzerinde oluşturabileceği riskleri minimize edeceğinin muhakkak olduğu,
- yaygın olarak yaşanan ve veri ihlallerinin oluşmasına neden olan aynı kullanıcı adı ve parolanın farklı platformlarda kullanılması, belirli zaman aralıklarında parola değişiminin yapılmaması, iki kademeli kimlik doğrulama ve benzeri giriş yöntemlerinin kullanılmaması gibi teknik ve idari tedbir eksikliklerinin kişisel veri ihlallerine neden olabildiğinin görüldüğü ve
- yaygın olarak yaşanan veri ihlallerini önlemek veya ihlallerin meydana gelmesi halinde ilgili kişiler üzerinde olumsuz sonuç doğurma olasılığının azaltılmasını temin etmek adına veri sorumluları tarafından birtakım önlemlerin alınmasına ihtiyaç duyulduğu

ifade edilmiş olup, veri sorumlularının kendi risk değerlendirmelerini yaparak:

- çift kademeli kimlik doğrulama (two-factor authentication) sistemlerinin kurulması ve bu sistemlerin kullanıcılarına üyelik başvurusu aşamasından itibaren alternatif güvenlik önlemi olarak sunulması,
- kullanıcıların hesaplarına sık erişim sağlayan cihazlar haricinde farklı cihazlar üzerinden giriş yapılması durumunda giriş bilgilerinin e-posta, SMS ve benzeri yöntemlerle ilgili kişilerin iletişim adreslerine iletilmesinin sağlanması,
- uygulamaların HTTPS (Hypertext Transfer Protocol Secure - Hiper Metin Aktarma Güvenli İletişim Kuralı) ile veya aynı güvenlik seviyesini sağlayacak bir şekilde koruma altına alınması,
- kullanıcı parolalarının siber saldırı yöntemlerine karşı korunmasını teminen güvenli ve güncel karma (hashing) algoritmalarının kullanılması,
- IP (Internet Protocol Address) adresinden yapılacak başarısız giriş denemesi sayısının sınırlandırılması,
- ilgili kişilerin en az son 5 adet başarılı ve başarısız giriş denemeleri ile ilgili bilgilerini görüntüleyebilmelerinin sağlanması,
- ilgili kişilere aynı parolanın birden fazla platformda kullanılmaması gerektiğinin hatırlatılması,
- 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 (örn. CAPTCHA, dört işlem) kullanılması ve erişime izin verilen IP adreslerinin sınırlandırılması,
- sistemlerine giriş yapılan parolaların uzunluğunun asgari 10 karakter olmasının ve büyük-küçük harf, rakam ve özel karakterlerin bir arada kullanılmasına yönelik güçlü parola oluşturulmasının sağlanması ve
- sistemlerine giriş için üçüncü parti yazılımlar veya servisler kullanılması halinde bu yazılımların ve servislerin güvenlik güncelleştirmelerinin düzenli olarak gerçekleştirilmesi ve gerekli kontrollerin yapılması

gibi teknik ve idari tedbirlerinden uygun olanlarını almaları tavsiye edilmiştir.

Duyuru'nun tam metnine **buradan** ulaşabilirsiniz.

NAZALI
Tax & Legal