15 Şubat 2022

VERİ SORUMLULARI TARAFINDAN ALINMASI TAVSİYE EDİLEN TEKNİK VE İDARİ TEDBİRLERE İLİŞKİN KAMUOYU DUYURUSU YAYIMLANDI

Kişisel Verileri Koruma Kurumu (**"Kurum"**) tarafından hazırlanan, Kullanıcı Güvenliğine İlişkin Veri Sorumluları Tarafından Alınması Tavsiye Edilen Teknik ve İdari Tedbirlere İlişkin Kamuoyu Duyurusu (**"Duyuru"**), 15 Şubat 2022 tarihinde Kurum'un resmi intenet sitesinde yayımlandı.

Duyuru'da kişisel Verilerin Korunması Kanunu uyarınca veri sorumlusunun; (i) kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, (ii) kişisel verilere hukuka aykırı olarak erişilmesini önlemek, (iii) kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğu tekrar edilmiştir. Bu kapsamda Kurum'a intikal eden veri ihlal bildirimleri değerlendirilerek;

- 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,
- Kullanıcı hesaplarını elde eden üçüncü kişilerce anılan veri sorumlularının internet sitelerine kullanıcıların haberi olmadan aktif bir şekilde giriş yapıldığı ve ilgili kişilere ait verilerin bu kapsamda görüntülenebildiğinin tespit edildiği,
- Veri sorumluları sistemlerinden veya son kullanıcı bilgisayarlarındaki güvenlik açıkları kullanılarak elde edilen kişisel verilerin, hukuka aykırı bir şekilde paylaşıldığı ve ekonomik bir değer karşılığında satışa sunulabildiğinin görüldüğü,
- Bununla birlikte ilgili kişilere ait bu veriler elden ele dolaşarak kötü niyetli kişilerce arşivlenerek daha büyük veri setleri halinde yeniden pazarlanabildiği,
- 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 vb. giriş yöntemlerinin kullanılmaması*" gibi teknik ve idari tedbir eksikliklerinin kişisel veri ihlallerine neden olabildiğinin görüldüğü belirtilmiştir.

Yaygın olarak yaşanan veri ihlallerini önlemek veya meydana gelmesi halinde ilgili kişiler üzerinde olumsuz sonuç doğurma olasılığının azaltılmasını teminen, veri sorumluları tarafından bir takım önlemlerin alınmasına ihtiyaç duyulduğu ifade edilmiştir. Bu kapsamda Kurum'ca veri sorumlularına aşağıdaki tavsiyelerde bulunulmuştur:

1) Çift kademeli kimlik doğrulama (two-factor authentication) sistemlerinin kurulması ve kullanıcılarına üyelik başvurusu aşamasından itibaren alternatif güvenlik önlemi olarak sunulması,

2) Kullanıcıların hesaplarına sık erişim sağlayan cihazlar haricinde farklı cihazlar üzerinden giriş yapılması durumunda, giriş bilgilerinin e-posta/sms vb. yöntemlerle ilgili kişilerin iletişim adreslerine iletilmesinin sağlanması,

3) Uygulamaların HTTPS (Hypertext Transfer Protocol Secure - Hiper Metin Aktarma Güvenli İletişim Kuralı) ile veya aynı güvenlik seviyesini sağlayacak bir şekilde koruma altına alınması,

4) Kullanıcı parolalarının, siber saldırı yöntemlerine karşı korunmasını teminen, güvenli ve güncel karma (hashing) algoritmaların kullanılması,

5) IP (Internet Protocol Address) adresinden yapılacak başarısız giriş denemesi sayısının sınırlandırılması,

6) İlgili kişilerin en az son 5 adet başarılı ve başarısız giriş denemeleri ile ilgili bilgilerini görüntüleyebilmelerinin sağlanması,

7) İlgili kişilere aynı parolanın birden fazla platformda kullanılmaması gerektiğinin hatırlatılması,

8) Veri sorumluları tarafından parola politikasının oluşturulması ve kullanıcılara ait parolaların belirli aralıklarla değiştirilmesinin sağlanması veya bu hususun ilgili kişilere hatırlatılması,

9) 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,

10) 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,

11) 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 tedbirlerden risk değerlendirmelerinin yapılarak uygun olanlarının alınması.

Detaylı bilgi için bizlerle iletişime geçebilirsiniz.

Duyuru'nun tam metnine ulaşmak için lütfen buraya tıklayınız.

Mavi & Karadağ Hukuk Bürosu