İNTERNET SİTELERİ KULLANICI GÜVENLİĞİ HAKKINDA KVK KURULU TAVSİYELER DUYURUSU

11/03/2022

Tilegal

www.tilegal.com

Nidakule Ataşehir Kuzey
Begonya Sokak No: 3
Ataşehir, İstanbul, Türkiye

TİLEGAL

Kişisel Verileri Koruma Kurulu (Kurul) Şubat ayında "Kullanıcı Güvenliğine İlişkin Veri Sorumluları Tarafından Alınması Tavsiye Edilen Teknik ve İdari Tedbirlere İlişkin Kamuoyu Duyurusunu" yayınlamıştır.

Kurul bu duyurusunda özetle;

- Kurula iletilen veri ihlali bildirimlerinde finans, e-ticaret, sosyal medya gibi farklı sektörlerde faaliyet gösteren bazı veri sorumlularının internet sitelerine giriş için kullanılan kullanıcı adı, parola gibi kullanıcı hesap bilgilerinin herkese açık bir şekilde yayınlandığını, bu nedenle veri ihlallerinin arttığını,

- Güvenlik açıkları kullanılarak yetkisiz üçüncü kişiler tarafından bu internet sitelerinde elde edilen kişisel verilerin hukuka aykırı bir şekilde paylaşıldığını, ayrıca satışa sunulabileceğini veya veri setleri halinde yeniden pazarlanabileceğini,

- Söz konusu ihlallerin veri sorumluları tarafından alınması gereken idari ve teknik tedbirleri eksikliklerinden kaynaklandığını,

- İlgili kişisel veri sahipleri bakımından olumsuz sonuçları ve veri ihlalleri önlemek bakımından veri sorumluların KVK Kanunu'nun 12. maddesi gereğince kişisel verilerin korunması amacıyla uygun güvenlik düzeyini sağlamak için gerekli idari ve teknik tedbirleri almakla yükümlü olduklarını ifade etmiş ve

- Veri ihlallerinin engellenmesi için internet sitelerinde tavsiye ettiği bir takım idari ve teknik tedbirleri yayınlamıştır.

Tavsiye edilen teknik ve idare tedbirler arasında dikkat çeken bazı örnekler aşağıdadır:

- Çift kademeli kimlik doğrulama sistemlerinin kurulması,

- Farklı cihazlar üzerinden giriş yapılması durumunda, giriş bilgilerinin e-posta / sms vb. yöntemlerle ilgili kişilerin iletişim adreslerine iletilmesinin sağlanması,

- Parola politikasının oluşturulması ve kullanıcılara ait parolaların belirli aralıklarla değiştirilmesinin sağlanması,

- IP adresinden yapılacak başarısız giriş denemesi sayısının sınırlandırılması,

- Aynı parolanın birden fazla platformda kullanılmaması gerektiğinin hatırlatılması,

- Parolaların uzunluğunun asgari 10 karakter olması, büyük - küçük harf, rakam ve özel karakterlerin bir arada kullanılmasına yönelik güçlü parola oluşturulmasının sağlanması,

- Yeni oluşturulan parolaların, eski parolalarla (en az son üç parolayla) aynı olmasının engellenmesi,

- Kullanıcı parolalarının, siber saldırı yöntemlerine karşı korunması için, güvenli ve güncel karma (hashing) algoritmaların kullanılması.

Kurulun tavsiye ettiği diğer idari ve teknik tedbirlere **buradan** ulaşabilirsiniz.

TİLEGAL AVUKATLIK BÜROSU