KARAR BAŞLIĞI: Bir Sigorta Şirketinin Kişisel Veri İhlal Bildirimi hk.

KARAR TARİHİ/NO: 24/11/2020 - 2020/905

İlgili kararı okumak için tıklayınız.

KARARA KONU OLAYIN ÖZETİ

Veri sorumlusu bir sigorta şirketinin Kişisel Verileri Koruma Kurumu'na ilettiği yazılarda yer alan (i) veri sorumlusunun internet sayfasının bulunduğu test sunucusunun siber saldırıya uğradığı ve bu durumun aynı tarihte veri sorumlusu tarafından tespit edildiği, (ii) test sunucusunda bulunan internet sayfasının kullanıcı giriş ekranından birden çok giriş denemesi yapılması sonucunda sisteme yetkisiz giriş sağlandığı ve bunun sonucunda uygulamanın bulunduğu veri tabanının silinerek yerine fidye taleplerinin bulunduğu yeni bir veri tabanının yüklendiği, (iii) veri tabanının siber saldırıyı gerçekleştiren kişi/kişiler tarafından kopyalandığının veri sorumlusu tarafından düşünüldüğü, (iv) giriş denemeleri belirli aralıklarla yapılmış olduğundan SIEM sistemi tarafından algılanmadığı ve yurt dışından çok fazla giriş denemesi yapılmasının herhangi bir anomaliye sebep vermediği ve (v) ihlalden 311 kişiye ait T.C. kimlik no., ad/soyad, e-posta, plaka bilgisinin etkilendiği şeklindeki beyanları üzerine Kişisel Verileri Koruma Kurulu ("**Kurul**") tarafından yürütülen veri ihlali bildirimi incelemesi sonuçlandırılmıştır.

KURUL KARARI VE YAPTIRIMI

İnceleme kapsamında Kurul tarafından (i) veri sorumlusuna ait "BT Veri Güvenlik ve Veri İhlali Prosedürü"nde yer alan tedbirlere uygun şekilde test sunucularının kontrol edilmediği, (ii) veri sorumlusu nezdinde kullanılan parolaların yeteri kadar karmaşık ve güçlü olmadığı, (iii) test sunucularında SSL VPN gibi güvenli iletişim sağlama yöntemlerinin ve iki faktörlü kimlik doğrulama gibi güçlü kimlik doğrulama yöntemlerinin kullanılmadığı, (iv) ilgili kişiler için önem arz eden veri gruplarının gizlilik derecesine göre muhafaza edilmesi bakımından yeteri kadar özen gösterilmediği, (v) test sunucusuna kişisel veri kaydedilmeden de test işlemleri yapılabilecek olmasına rağmen verilerin kaydedilmesi ile veri ihlaline sebep olunduğu, (vi) ihlalinin öğrenilmesinden itibaren 72 saatlik süre içerisinde Kurul'a bildirimde bulunulmadığı ve (vi) internet sitesinde duyuru yapılmış olmasının ilgili kişilere bildirim şeklinde kabul edilemeyeceği gerekçeleriyle sigorta şirketi hakkında gerekli teknik ve idari ve tedbirleri alınmamasından 300.000 TL ve ayrıca "en kısa sürede" bildirimde bulunulmamasından 30.000 TL idari para cezası uygulanmasına karar verilmiştir.

YORUMLARIMIZ

Kurul tarafından verilen karar ile veri sorumluları tarafından belirli dönemlerde sızma testlerinin yaptırılması, güçlü kimlik doğrulama yöntemlerinin kullanılması, kişisel verilerin gizlilik derecesine göre şifrelenerek muhafaza edilmesi ve benzeri yöntemlerle veri güvenliğini sağlamaya yönelik teknik tedbirlerin alınması zorunluluğu ve önemi tekrar vurgulanmış olup, 18/09/2019 tarihli ve 2019/271 sayılı Kurul kararı uygun olarak doğrudan erişilebilir ilgili kişilere bildirim yapma yükümlülüğünün ihlalin yalnızca internet sitesinde yayımlanması suretiyle duyurulmasının yeterli olmadığı açıkça ortaya konmuştur.