SAYI: 21

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

KVK & SİBER GÜVENLİK BÜLTENİ

EKİM 2022

GÜNCEL HABERLER

- Ekim Ayında Bildirilen Kişisel Veri İhlalleri
- İlgili Kişinin Hak Arama Yöntemleri ve Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberleri Seslendirildi
- Sigortacılık Verilerinin Toplanması, Saklanması ve Paylaşılmasına Dair Yönetmelik Yürürlüğe Girdi

GLOBAL GELİŞMELER

- ABD'de "ABD-AB Veri Gizliliği Anlaşması" Çerçevesinde Yer Alan Taahhütlerin Uygulanması İçin Kararname Çıkardı
- ICO, Duygu Analizi Gibi Biyometrik Teknolojilerin Kullanımı Konusunda Hazırladığı Rehberi Duyurdu
- OECD, Karanlık Ticari Kalıplara İlişkin Bir Çalışma Yayımladı
- GDPR Kapsamında Veri İhlal Bildirimlerinin Yapılmasına İlişkin 9/2022 Rehberi Kamuoyu Görüşüne Sunuldu
- AİHM, Yeni Teknolojilere İlişkin Kararlarının Yer Aldığı Bilgi Notunu Paylaştı
- İtalya Veri Koruma Otoritesi, Alıcı Adreslerinin "Cc" Kısmına Eklenmesini Hukuka Aykırı Buldu

FİDYE YAZILIMI (RANSOMWARE) NEDİR ?

Malware (kötü amaçlı yazılım) ismi, kötü amaçlı anlamına gelen "malicious" ve yazılım anlamına gelen "software" kelimelerinin birleşiminden oluşmuştur. Kötü amaçlı yazılım, kullanıcılar için tehlikeli olabilecek tüm kötü amaçlı yazılımları kapsayan genel bir terimdir. Virüsler, truva atları ve fidye yazılımlar da bu kapsama dahildir.

Fidye yazılımları da bir mağdurun bilgisayarındaki verilerin genellikle şifreleme yoluyla kilitlendiği kötü amaçlı yazılım türüdür. Etkilenen verilerin şifresinin çözülmesi ve mağdura erişimin geri verilmesinden önce ödeme talep edilir. Fidye yazılımı saldırıları neredeyse her zaman parayla ilişkilidir ve diğer saldırı türlerinden farklı olarak genellikle mağdur saldırı durumunda bilgilendirilir ve saldırıdan kurtulmak için izlemesi gereken talimatları öğrenir. Genellikle ödemelerin, siber suçlu kimliğinin bilinmemesi için kripto paralar ile yapılması talep edilir.

Fidye yazılımlar genellikle şu şekilde mağdurların bilgisayarlarına sokulmaktadır:

- Sosyal Mühendislik (Social Engineering): İnsanları sahte bir ek veya bağlantıyla kötü amaçlı yazılım indirmeleri için kandırmak için kullanılan bir terimdir. Kötü amaçlı dosyalar, genellikle sıradan belgeler (sipariş onayları, makbuzlar, faturalar, bildirimler) olarak gizlenir ve saygın bir şirket veya kurum tarafından gönderilmiş gibi görünür.
- Zararlı Reklam (Malvertising): Fidye yazılımı, casus yazılımı, virüsler ve diğer kötü şeylerin bir tıkla bulaşmasına neden olan ücretli reklamlardır.
- İstismar Kitleri (Exploit Kits) : Kullanıma hazır hackleme aracına yerleştirilmiş, önceden yazılmış kodlardır. Bu kitler eski yazılımların neden olduğu güvenlik açıklarından yararlanmak için tasarlanmıştır.
- Drive-by Downloads: Kullanıcı istemediği halde bilgisayarına yüklenen tehlikeli dosyalardır. Kötü amaçlı web siteleri, kullanıcılar bir web sitesine göz atarken veya bir video izlerken arka planda kötü amaçlı yazılım indirmek için güncel olmayan tarayıcılar veya uygulamalardan yararlanır.

Fidye yazılımlardan korunmak için şirketlere verilen tavsiyeler ise gereksiz servisleri ve yazılımı kaldırarak saldırı yüzeyinin azaltılması, ağların zayıf parolalar kullanan açıklar için taranması, veri yedeklerinin iki veya çok faktörlü kimlik doğrulaması ile güvence altına alınması şeklindedir.

EKİM AYI İÇERİSİNDE BİLDİRİLEN KİŞİSEL VERİ İHLALLERİ

Quick Sigorta Anonim Şirketi

Veri ihlal bildirimlerinde özetle;

- Veri sorumlusunun anlaşmalı olduğu yazılım firması tarafından yönetilen hasar yönetimi programında yer alan maddi araç hasarlarına ilişkin görsellerin yer aldığı URL'nin yetkisiz kişiler tarafından ele geçirildiği,
- Yetkisiz kişiler tarafından çeşitli ihbar ID numaraları denenerek görsellere erişilmesi ile ihlalin gerçekleştiği,
- Yapılan incelemelerde saldırganın sisteme giriş yapma denemelerinin 18.08.2022 tarihinde başarılı olduğu ve 21.08.2022 tarihinde veri çekme girişimlerine başladığının anlaşıldığı,
- İlgili programın çoğunlukla, kazaya karışmış hasarlı araçlara ait görüntülerden oluştuğu; halihazırda konuya ilişkin inceleme devam etmekle birlikte, hasar dosyasında yer alan bilgiler kapsamında:
  - Sürücülerin kimlik görseli iletmesi halinde; isim, soyisim, T.C kimlik numarası, doğum yeri, doğum tarihi, anne adı, baba adı, cinsiyeti ve fotoğrafı,
  - Sürücülerin ehliyet görseli iletmesi halinde; isim, soyisim, doğum tarihi, doğum yeri, T.C. kimlik numarası, kan grubu ve fotoğrafı,
  - Trafik kaza tespit tutanağı kapsamında adres bilgisinin bulunduğu,
- İhlalden etkilenen ilgili kişi sayısını tespit çalışmalarının devam etmekte olduğu,
- İhlalden etkilenen ilgili kişi grubunun müşteriler/potansiyel müşteriler ve trafik kazasına karışan taraflar olduğu

bilgilerine yer verilmiştir.

GÜNCEL HABERLER

EKİM AYI İÇERİSİNDE BİLDİRİLEN KİŞİSEL VERİ İHLALLERİ

Denizli Özel Egekent Hastanesi

Veri sorumlusu sıfatını haiz Denizli Özel Egekent Hastanesi tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Veri sorumlusunun 10.10.2022 tarihinde fidye yazılımı saldırısına maruz kalması sonucu sistemlerinin şifrelendiği ve hastane sistemlerine erişim sağlanamadığı,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, kullanıcılar, aboneler, öğrenciler, müşteriler, hastalar, çocuklar, korunmaya muhtaç yetişkinler olduğu
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, lokasyon, özlük, hukuki işlem, müşteri işlem, fiziksel mekân güvenliği, işlem güvenliği, risk yönetimi, finans, mesleki deneyim, pazarlama bilgileri ile görsel ve işitsel kayıtlar olduğu,
- İhlalden etkilenen tahmini kişi sayısının 295 olduğu

bilgilerine yer verilmiştir.

İnfomag Reklam ve Özel Dergi Yay. Hiz. Tic. A.Ş

Veri sorumlusu sıfatını haiz İnfomag Reklam ve Özel Dergi Yay. Hiz. Tic. A.Ş tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Veri sorumlusunun web sitesine ait veri tabanında yer alan verilerin yetkisi olmayan kişiler tarafından silinmesi ile ihlalin gerçekleştiği ve yetkisiz erişilen veri tabanı klasörüne fidye mesajı bırakıldığı,
- İhlalin 07.09.2022 tarihinde, web sunucusu tarafından iletilen uyarı mesajı ve web editörleri tarafından iletilen siteye erişimin kesildiği yönündeki mesajlar sonucunda tespit edildiği,
- İhlalden etkilenen ilgili kişi gruplarının kullanıcılar ve aboneler/ üyeler olduğu,
- İhlalden etkilenen kişisel verilerin, ücretsiz üyelik oluşturan kullanıcılara ait ad, soyad, e-posta bilgileri, ücretli abonelik gerçekleştirmiş kullanıcılara ait ad, soyad, e-posta, TC kimlik numarası, adres ve telefon bilgileri olduğu,
- İhlalden etkilenen kişi ve kayıt sayısının belirsiz olduğu,
- İlgili kişilerin veri ihlali ile ilgili olarak destek@infomag.com.tr e-posta adresinden bilgi alabileceği

ifadelerine yer verilmiştir.

İLGİLİ KİŞİNİN HAK ARAMA YÖNTEMLERİ VE AYDINLATMA YÜKÜMLÜLÜĞÜNÜN YERİNE GETİRİLMESİ REHBERLERİ SESLENDİRİLDİ

Kişisel Verileri Koruma Kurumu'nun Spotify'daki "Bir Küçük Farkındalık Yeter" isimli podcast serisinde bu ay "İlgili Kişinin Hak Arama Yöntemleri" ve "Aydınlatma Yükümlülüğünün Yerine Getirilmesi" rehberleri seslendirildi.

Kanala ve kanalda seslendirilmiş diğer rehberlere link üzerinden erişebilirsiniz.

SİGORTACILIK VERİLERİNİN TOPLANMASI, SAKLANMASI VE PAYLAŞILMASINA DAİR YÖNETMELİK YÜRÜRLÜĞE GİRDİ

Sigortacılık ve Özel Emeklilik Düzenleme ve Denetleme Kurumu tarafından 18 Ekim 20222 tarihli Resmi Gazete'de Sigortacılık Verilerinin Toplanması, Saklanması ve Paylaşılmasına Dair Yönetmelik yayımlandı.

Yönetmelik kapsamında sigorta sözleşmelerine, sigorta sözleşmesine taraf olan sigorta ettiren ve sigorta şirketlerine, sigorta sözleşmesinden doğrudan veya dolaylı menfaat sağlayan sigortalı, lehtar ve diğer üçüncü kişilere ilişkin veriler ile yanlış sigorta uygulamaları dahil olmak üzere risk değerlendirmesine esas tüm veriler, sigortacılık verisi olarak tanımlanmış ve sigortacılık verilerinin özel hukuk tüzel kişileri ile kamu kurum ve kuruluşlarından, kamu kurumu niteliğindeki meslek kuruluşları ve bunların üst kuruluşlarından, ilgili mevzuatla kurulmuş diğer bilgi merkezlerinden Merkez tarafından toplanarak genel veri tabanında tutulması esası benimsenmiştir.

Yönetmeliğe göre sigortacılık verileri, Sigortacılık Kanunu'nun 31/B maddesi uyarınca Sigorta Bilgi ve Gözetim Merkezi tarafından üye kuruluş olarak tanımlanan sigorta, reasürans ve emeklilik şirketleri ile paylaşılabilecektir. Paylaşılan sigortacılık verileri, sigortacılık sektöründe kamu gözetimi, denetimi ve ekonomik güvenliğin sağlanmasına ve sağlık hizmetleri finansmanının planlanmasına katkıda bulunmak, sigorta uygulamalarını takip etmek, sigorta branşlarında uygulama birliğini sağlamak, zorunlu sigortaların takibini yapmak, yanlış sigorta uygulamalarının önlenmesine katkıda bulunmak, sigortalılık oranlarının artırılmasına yönelik çalışmalar yapmak, sigortacılık sektörüne ilişkin güvenilir istatistikler üretilmesini sağlamak, sigorta puanını hesaplamak amacıyla işlenecektir.

Yönetmelik'in tamamına link üzerinden erişebilirsiniz.

GLOBAL GELİŞMELER

ICO, DUYGU ANALİZİ GİBİ BİYOMETRİK TEKNOLOJİLERİN KULLANIMI KONUSUNDA HAZIRLADIĞI REHBERİ DUYURDU

İBirleşik Krallık Veri Koruma Otoritesi (Information Commissioner's Office, "ICO") veri sorumlularını "olgunlaşmamış" ve "sözde bilimsel" olarak nitelendirdiği duygu analizi gibi biyometrik teknolojilerin kullanımı konusunda uyaran bir rehber hazırladı.

Duygu analizi teknolojileri genellikle yapay zeka (AI) algoritmaları tarafından desteklenmekte ve işlevlerini yerine getirebilmek için bakış izleme, yüz hareketleri, yürüyüş, kalp atışları, yüz ifadeleri ve cilt nemi gibi pek çok kişisel veriyi analiz etmektedir.

Güvenlik amacıyla ses ve yürüyüş verilerini kullanan finans kuruluşları, sınavlarda öğrencilerin vücut, göz ve kafa hareketlerini kullanan okullar ve iş görüşmeleri sırasında potansiyel çalışanları analiz eden işverenler duygu analizi teknolojilerinin kullanımına örnek teşkil etmektedir.

Ancak ICO, algoritmaların şu anda duygusal durumları etkili bir şekilde tespit edemediğini ve bunun da sistemik önyargı, yanlışlık ve ayrımcılığa kapı açma riskini taşıdığı konusunda veri sorumlularını uyardı. Bu, ICO'nun bir teknolojinin etkisizliği hakkında yayınladığı ilk kapsamlı uyarı.

ICO tarafından yayınlanan rehberde ayrıca mevcut gözetim düzenlemelerinin parçalı ve kafa karıştırıcı olduğu ve yürürlükteki mevzuatın bireysel hakları yeterince korumadığı tespit edilmiştir.

Konuyla ilgili detaylı bilgiye link üzerinden ulaşabilirsiniz.

ABD'DE "ABD-AB VERİ GİZLİLİĞİ ANLAŞMASI" ÇERÇEVESİNDE YER ALAN TAAHHÜTLERİN UYGULANMASI İÇİN KARARNAME ÇIKARILDI

Beyaz Saray 7 Ekim'de yaptığı açıklamada, Başkan Joe Biden'in ABD ve Avrupa Birliği arasında paylaşılan kişisel verilerin gizliliğini korumak için yeni bir çerçeve uygulamak için bir yürütme emri imzaladığını duyurdu.

ABD-AB Veri Gizliliği Anlaşması, AB hukuku kapsamında geçerli bir veri aktarım mekanizması olan ABD ve AB arasındaki veri aktarım sözleşmesini Temmuz 2020'de iptal eden Avrupa Birliği Adalet Divanı'nın (CJEU) endişelerini ele almakta.

Bu Anlaşma kapsamında Biden tarafından çıkarılan yeni kararname, ABD'de istihbarat faaliyetleri için yalnızca gerekli ve orantılı olanı yapmalarını gerektiren yeni güvenceler benimsemekte ve iki aşamalı bir tazminat sistemi yaratmakta. Kararname ile ABD istihbarat topluluğu, Anlaşmadaki yeni gizlilik korumalarına uyacak şekilde politika ve prosedürlerini güncellemeye yönlendirilmiştir. Ayrıca, bağımsız bir kurum olan Mahremiyet ve Sivil Özgürlükler Gözetim Kurulu'na bu güncellemeleri incelemesi ve istihbarat topluluğunun bağlayıcı tazminat kararlarına tam olarak uyup uymadığına ilişkin yıllık bir inceleme yapması talimatı verilmiştir.

OECD, "KARANLIK TİCARİ KALIPLAR"A İLİŞKİN BİR ÇALIŞMA YAYIMLADI

Ekonomik İşbirliği ve Kalkınma Teşkilatı ("OECD"), çevrimiçi kullanıcı ara yüzlerinde bulunan ve tüketicileri genellikle kendi çıkarlarına uygun olmayan seçimler yapmaya yönlendiren ya da bununla ilgili tüketicileri manipüle eden karanlık ticari kalıplara (dark commercial patterns) ilişkin çalışmasını kamuoyuna duyurdu.

OECD, çalışmasında karanlık ticari kalıpların çalışan bir tanımını önermekte, bunların yaygınlığı, etkinliği ve zararlarına ilişkin kanıtları ortaya koymakta ve tüketici politika yapıcılarına ve yetkililerine bunları ele almada yardımcı olmak için olası politika ve uygulama yanıtlarını belirlemektedir. Ek olarak tüketicilerin ve işletmelerin karanlık ticari kalıpları azaltmak için alabileceği olası yaklaşımlar da çalışma kapsamında ele alınmıştır.

Çalışmanın tamamına link üzerinden erişebilirsiniz.

GLOBAL GELİŞMELER

AİHM, YENİ TEKNOLOJİLERE İLİŞKİN KARARLARININ YER ALDIĞI BİLGİ NOTUNU PAYLAŞTI

Avrupa İnsan Hakları Mahkemesi, “Yeni Teknolojiler” konusunun ele alındığı kararlara ilişkin bilgi notunun Eylül 2022’de güncellenmiş versiyonunu kamuoyuyla paylaştı. Bu bilgi notu kapsamında; elektronik veri, e-posta, GPS, internet, cep telefonu, kitapların ve müzik eserlerinin telif hakkı, çevrim içi taciz, radyo iletişimi, telekomünikasyon, gizli kamera kullanımı ve video ile izleme başlıkları altında Avrupa İnsan Hakları Sözleşmesi kapsamında verilmiş olan çeşitli kararların özetleri derlenmiştir.

Bilgi notuna link üzerinden erişebilmek mümkündür.

İTALYA VERİ KORUMA OTORİTESİ, ALICI ADRESLERİNİN "CC" KISMINA EKLENMESİNİ HUKUKA AYKIRI BULDU

Bir çalışanın bir bilgi kampanyasının parçası olarak alıcıların adreslerini "Bcc" yerine "Cc" alana ekleyerek e-posta iletileri göndermesi nedeniyle İtalya Veri Koruma Otoritesi'ne yapılan veri ihlali bildiriminde bulunulmuştur. Yaklaşık 2000 diyabet hastasının alıcı olduğu mailde, her alıcının diğer alıcıların e-posta adresini ve dolaylı olarak sağlık verilerini öğrenmesine sebebiyet veren olayda, veri sorumlusu şirkete 45.000,00 Avro idari para cezası verilmiştir.

Karada herhangi bir yasal dayanak bulunmaksızın ve şirket bünyesinde yeterli teknik ve idari tedbirler alınmaksızın kişisel verilerin üçüncü kişilerle paylaştığı ortaya konulmuştur. Ayrıca kararda, uygulamanın indirilmesini takiben alınan kullanıcı rızalarının hukuka uygun olmadığı da tespit edilmiştir.

GDPR KAPSAMINDA VERİ İHLAL BİLDİRİMLERİNİN YAPILMASINA İLİŞKİN 9/2022 REHBERİ KAMUOYU GÖRÜŞÜNE SUNULDU

10 Ekim 2022'de Çalışma Grubu 29 (Working Party 29) tarafından kabul edilen ve 25 Mayıs 2018'de Avrupa Veri Koruma Kurumu ("EDPB") tarafından onaylanan Veri İhlal Bildirimlerine İlişkin Rehber, kabul edilmiş ve kamuoyunun görüşüne sunulmuştur.

EPDB, Çalışma Grubu 29 tarafından kabul edilen WP250 sayılı rehberden farklı olarak bu rehberin 73. paragrafında (AB dışı kuruluşlardaki veri ihlalleriyle ilgili bildirim gereklilikleri) değişikliğe gidildiğini belirterek özellikle bu kısma ilişkin görüş talep etmiştir.

Bu değişiklikle, AB bünyesinde herhangi bir kuruluşu olmayan AB dışı veri sorumlularının bu tür ihlallerden etkilenen ilgili kişilerin bulunduğu her bir AB ülkesine veri ihlallerini bildirmeleri gerekecektir. EDPB, veri ihlallerine ilişkin önceki kılavuzlarında, bir AB kuruluşu olmayan AB dışı veri sorumlularının AB veri koruma temsilcisinin ikamet ettiği üye ülkede tek bir bildirimde bulunulmasını yeterli görmekteydi.

Yeni Rehber 29 Kasım 2022'ye kadar kamuoyu görüşüne açık olup, ilgili tüm taraflar yorumlarını EDPB'ye gönderebilir.

Rehber'in tamamına link üzerinden erişim sağlayabilirsiniz.