SAYI: 20

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

KVK & SİBER GÜVENLİK BÜLTENİ

EYLÜL 2022

GÜNCEL HABERLER

- Eylül Ayında Bildirilen Kişisel Veri İhlalleri
- Kişisel Verileri Koruma Kurumu, 2018-2021 Yılları Arasında Verilen Kararları Bir Kitapçıkta Yayınladı

GLOBAL GELİŞMELER

- İrlanda'da Instagram Hakkında Rekor Para Cezasına Hükmedildi
- İrlanda Veri Koruma Otoritesi, TikTok Hakkında Karar Taslağını Tamamladı
- Danimarka'dan Google Analytics Kararı
- Endonezya'da Kişisel Verilerin Korunmasına İlişkin İlk Yasa Meclis Tarafından Onaylandı
- Güney Kore'de Google ve Meta Aleyhine 71 Milyon Dolar İdari Para Cezası Uygulandı
- Birleşik Krallık TikTok'a 27 Milyon Pound Para Cezası Uygulayabilir

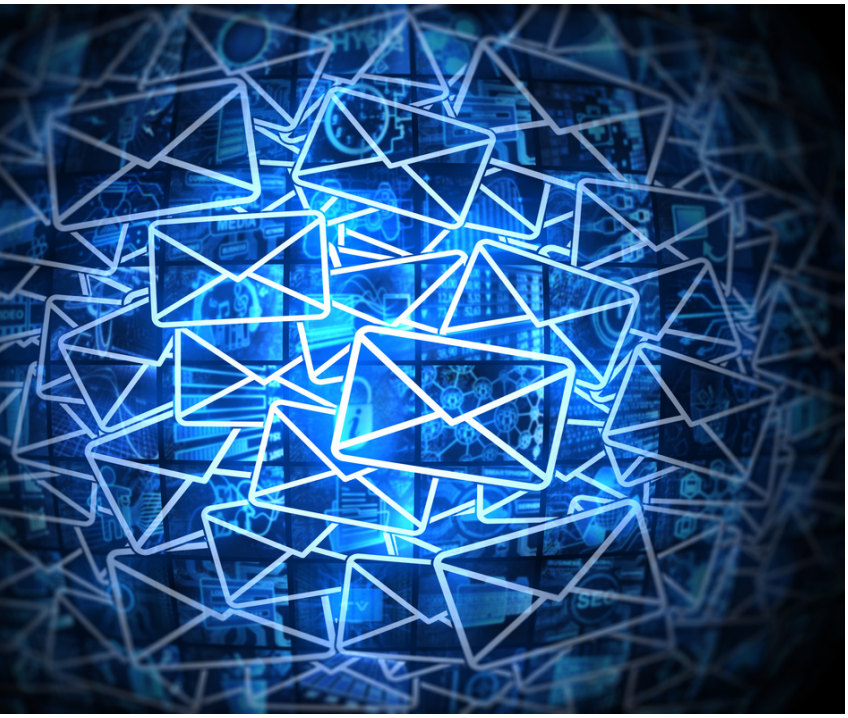
PHISHING (OLTALAMA) NEDİR?

Phishing ya da diğer adıyla oltalama, çevrimiçi saldırı türlerinden biri olup genellikle kullanıcı isimleri, şifreler, kredi kartı bilgileri, ağ kimlik bilgileri gibi hassas ve gizli bilgilere ulaşmak amacıyla yapılmaktadır.
Bu saldırı türünde genel olarak kişilerin e-posta hesaplarına hediye, indirim, veya benzeri cezbedici sahte iletiler gönderilerek yukarıda belirtilen verilerin hukuka aykırı olarak elde edilmesi hedeflenmektedir.
Oltalama yönteminde, saldırgan tarafından özel olarak hazırlanan phishing e-postası resmi bir kurumdan ya da gerçekte mevcut bir şirketten geliyormuş gibi gerçek bir e-posta şeklinde gözükmektedir. Hazırlanan e-postada bulunan linkler yardımıyla kişiler sahte sitelere yönlendirilir ve kişilerin ilgili verilerini kendi rızalarıyla vermeleri sağlanır. Diğer bir yöntem olarak bu e-postalara eklenen dosyaların kişilerin bilgisayarında çalıştırılması ile kişilere ait bilgisayarlar ele geçirilebilir.

Spear Phishing, Whaling, Vishing, Pharming, Hoax, Swattting, Watering Hole Attack, oltalama saldırısının türleri olup aşağıdaki gibi tanımlanmaktadır:

- Spear Phishing: Belirli bir hedefe yönelik gerçekleştirilen oltalama saldırılarıdır.
- Whaling: Geniş bir topluluk tarafından tanınmış kişilere yapılan oltalama saldırısıdır.
- Vishing: Telefonla gerçekleştirilen oltalama saldırılarıdır.
- Pharming: Saldırganın belirlediği sahte web sitesine trafiğin yönlendirilmesidir.
- Swatting: Polis gibi acil durum müdahale ekiplerine yapılan sahte ihbarlardır. Saldırganın hedefindeki kişilerin adresine baskın yapılması için saldırgan hedef adrese sahte ihbar yapar.
- Watering Hole Attack: Saldırganın hedefindeki belirli bir grubun ziyaret ettiği web sitesinin saldırganın hedefine siber saldırı düzenlemek o web sayfasına zararlı kod bulaştırılmasıdır.

EYLÜL AYI İÇERİSİNDE BİLDİRİLEN KİŞİSEL VERİ İHLALLERİ



Posta ve Telgraf Teşkilatı Biriktirme ve Yardım Sandığı

Posta ve Telgraf Teşkilatı Biriktirme ve Yardım Sandığı tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Zararlı yazılımlar vasıtasıyla üyelerin bilgilerinin bulunduğu sisteme yetkisiz erişim sağlandığı,
- Yetkisiz kişiler tarafından, anne kızlık soyadı, cilt seri no gibi PTT çalışanlarının kişisel verilerinin, 3.2 gb veri tabanı yedeğinin ve sitenin tüm dosyalarının ele geçirildiğinin iddia edildiği,
- İhlalin 29.08.2022 ile 30.08.2022 tarihleri arasında gerçekleştiği ve 30.08.2022 tarihinde tespit edildiği,
- İhlalden etkilenen kişisel verilerin kimlik ve üyelik işlemlerine ait bilgiler olduğu,
- İhlalden yaklaşık 38.000 kaydın etkilendiği,
- İhlal ile ilgili çalışmaların devam etmekte olduğu

bilgilerine yer verilmiştir.

Biblos Alaçatı Turizm Yatırımları A.Ş.

Veri sorumlusu sıfatını haiz olan Biblos Alaçatı Turizm Yatırımları A.Ş. tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- İhlalin kaynağının fidye yazılımı saldırısı ve parola saldırısı olduğu,
- İhlalin 19.08.2022 tarihinde başladığı, aynı tarihte veri sorumlusunun iş telefonlarına gönderilen mesajlar ve personeline gönderilen e-postalar aracılığıyla siber saldırının tespit edildiği,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, müşteri işlem, finans, pazarlama, görsel ve işitsel kayıtlar olduğu,
- İhlalden etkilenen özel nitelikli kişisel veri kategorilerinin sağlık bilgileri ve biyometrik veriler olduğu,
- Öte yandan insan kaynakları, ön büro ve finans departmanlarında kullanılan programlar vasıtasıyla personel bordro kayıtlarının, misafir verilerinin ve şirketin mali verilerinin ihlale maruz kalmasının ihtimal dahilinde olduğu,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, müşteriler ve potansiyel müşteriler olduğu,
- İhlalden etkilenen tahmini kişi sayısının 450 olduğu, ancak siber saldırıya uğrayan programlar ve verilerle ilgili envanter çalışmasının devam ettiği,
- İlgili kişilere ait verilerin siber saldırı sonucunda silinmesi nedeniyle bildirim yapılamadığı

bilgilerine yer verilmiştir.

GÜNCEL HABERLER

EYLÜL AYI İÇERİSİNDE BİLDİRİLEN KİŞİSEL VERİ İHLALLERİ

Fuudy Elektronik İletişim Perakende Gıda Lojistik Anonim Şirketi

Veri sorumlusu sıfatını haiz olan Fuudy Elektronik İletişim Perakende Gıda Lojistik Anonim Şirketi tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- İhlalin hangi tarihte başladığının henüz tespit edilemediği, veri sorumlusu tarafından ihlalin 12.09.2022 tarihinde tespit edildiği,
- Veri sorumlusu kurumsal e-posta adresine ihlal iddiasına ilişkin bir e-posta gönderildiği,
- İhlal iddiasına ilişkin e-postada yer alan kayıtların Fuudy bünyesindeki kayıtlarla eşleştiği,
- İhlali gerçekleştiren kişi veya kişilerin bu bilgileri nasıl elde ettiği ve ihlalin hangi yöntemle gerçekleştirildiğinin henüz tespit edilemediği, ihlalin nasıl gerçekleştiği ile ilgili tespit çalışmalarının devam ettiği,
- İhlalden etkilenen kişisel verilerin sistemin test kısmında yer alan ad, soyadı, e-posta adresi, cep telefonu numarası ve adres ID'si olduğu, bu kişisel veriler arasında yer alan adres ID'sinin güncel nitelikte olmadığı,
- İhlalden etkilenen tahmini kişi sayısının yaklaşık olarak 81.452 olduğu, tam kişi sayısının tespitine yönelik çalışmaların devam ettiği

bilgilerine yer verilmiştir.

Marmara Üniversitesi

Veri sorumlusu sıfatını haiz Marmara Üniversitesi tarafından Kurula iletilen veri ihlal bildirimlerinde özetle;

- 15.09.2022 tarihinde veri sorumlusunun Bilgi Yönetim Sistemi (BYS) içerisindeki SMS gönderim servisindeki yetkili kullanıcı hesabının yetkisiz bir kişi tarafından elde edilerek SMS gönderilmesi suretiyle ihlalin gerçekleştiği,
- Ele geçirilen kullanıcı hesabının yeni kullanıcı hesapları tanımlama yetkisi olduğundan 3 yeni kullanıcı hesabı tanımı yapıldığının da tespit edildiği,
- Yetkisiz erişime konu dinamik raporlama ekranı üzerinden "toplu sms gönderimi" yapılabildiği ve üniversitede çalışan akademik ve idari personelin kimlik, iletişim ve özlük bilgilerine erişim sağlanabildiği,
- İhlalden etkilenen kişi sayısının 5698 olduğu,
- İhlalden etkilenen ilgili kişi grubunun çalışanlar ve kullanıcılar olduğu
- İhlal ile ilgili olarak ilgili kişilerin 0216 7771590 numaralı telefonu arayarak veya bidb@marmara.edu.tr adresine e-posta göndererek bilgi alabilecekleri

bilgilerine yer verilmiştir.

EYLÜL AYI İÇERİSİNDE BİLDİRİLEN KİŞİSEL VERİ İHLALLERİ

Özel Keystone Eğitim ve Eğitim Dan. A.Ş.

Veri sorumlusu sıfatını haiz Özel Keystone Eğitim ve Eğitim Dan. A.Ş tarafından Kurula iletilen veri ihlal bildiriminde özetle:

- İhlalin veri sorumlusu nezdinde çalışan eski bir öğretmenin kapatılmış e-posta adresinin açılarak, tüm okul veli ve personeline okulun muhasebe kayıtlarının, Drive'da bulunan ücret skala bilgilerinin, veli ve öğrenci isimlerinin e-posta gönderilmesi suretiyle gerçekleştiği,
- İhlalin 22.09.2022 tarihinde gerçekleştiği ve aynı gün tespit edildiği,
- İhlalden etkilenen kişisel verilerin kimlik, iletişim, özlük, hukuki işlem, işlem güvenliği, risk yönetimi, finans bilgileri ve diğer kategorilerinden oluştuğu,
- İhlalden etkilenen kişi ve kayıt sayısının henüz tespit edilemediği,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, kullanıcılar, aboneler/üyeler, öğrenciler ve müşteriler/potansiyel müşteriler olduğu

bilgilerine yer verilmiştir.

Flo Mağazacılık ve Pazarlama A.Ş.

Veri sorumlusu sıfatını haiz olan Flo Mağazacılık ve Pazarlama A.Ş. hakkında Kurumumuza iletilen ihbar sonucu yapılan değerlendirmede;

- Veri sorumlusuna ait instreet.com.tr internet sayfasının kullanıcılarına ait kişisel verilerin herkes tarafından ulaşılabilir bir internet sayfasında yayınlandığı,
- İhlalden etkilenen kişisel verilerin ad, soyad, kullanıcı adı, kullanıcı şifresi ve bu kullanıcılardan 380 kişiye ait olmak üzere kredi kartı ilk 4 ve son 4 hanesiyle bu kredi kartlarının hangi bankaya ait olduğunu gösteren bilgiler olduğu,
- İhlalden etkilenen ilgili kişi sayısının yaklaşık 3500 kişi olabileceği

tespit edilmiştir.

KİŞİSEL VERİLERİ KORUMA KURUMU, 2018-2021 YILLARINDA VERİLEN KARARLARINI BİR KİTAPÇIKTA YAYINLADI

Kişisel Verileri Koruma Kurumu tarafından 2018, 2019 ve 2020 yılında kişisel verilerin korunmasına ilişkin olarak verilen kararlar ve bu yıllarda Kurum'un sitesi üzerinden duyurusu yapılan veri ihlal bildirimleri bir kitapçık halinde kamuoyuna sunuldu. Kitapçıkta, Kurul verilen kararlara dair karar özetleri kronolojik olarak sıralanmışken kavram dizinine de yer verilmiştir.

Kitapçığın tamamına link üzerinden erişim sağlayabilirsiniz.

GLOBAL GELİŞMELER

İRLANDA'DA INSTAGRAM HAKKINDA REKOR PARA CEZASINA HÜKMEDİLDİ

İrlanda Veri Koruma Otoritesi ("DPC"), 21 Eylül 2020'de Instagram'ın (Meta Platforms Ireland Limited) ABD'li bir veri bilimci olan David Stier'ın çocukların kişisel veri mahremiyetinin ihlal edildiği iddialarına ilişkin olarak soruşturma başlatmıştı. Soruşturma, özellikle Instagram işletme hesabı özelliğini kullanan çocukların e-posta adreslerinin ve/veya telefon numaralarının kamuya açıklanmasını ve çocukların kişisel Instagram hesapları için varsayılan ayar olarak kullanılan "herkese açık" ayarı üzerinde odaklanmıştı.

Soruşturmanın ardından DPC, Avrupa Birliği kapsamında ilgili olan diğer veri koruma otoritelerine taslak kararını iletmiş ve bu taslak karara 6 ülkenin veri koruma otoritesi tarafından itiraz edilmişti. İrlanda ve diğer ülkelerin veri koruma otoritelerinin uzlaşamaması üzerine, Avrupa Veri Koruma Otoritesi ("EDPB") devreye girmiş ve 28 Temmuz 2022'de bağlayıcı kararını açıklamıştı.

DPC'nin orijinal taslak kararı 405 milyon Euro'ya kadar bir para cezası uygulanmasını önermekteydi. DPC, EDPB'nin bağlayıcı kararını dikkate alarak Instagram hakkında 20 milyon Euro'luk kısmı Avrupa Veri Koruma Tüzüğü'nün ("GDPR") 6. maddesinin 1. fıkrası için olmak üzere toplamda 405 milyon Euro ceza uygulanmasına karar verdi.

Bu idari para cezalarına ek olarak, DPC ayrıca bir kınama ve Instagram'ın fiili uygulamalarını düzeltmesine yönelik bir dizi belirli önlem almasına ve veri faaliyetini GDPR ile uygun hale getirmesini gerektiren bir emire de hükmetmiştir.

Konuyla ilgili detaylı bilgiye link üzerinden ulaşabilirsiniz.

İRLANDA VERİ KORUMA OTORİTESİ TİKTOK HAKKINDAKİ KARAR TASLAĞINI TAMAMLADI

Tiktok'a (Tiktok Technology Limited) yönelik veri ihlali iddialarıyla ilgili olarak yapılan soruşturmada GDPR kapsamında baş denetleme kurumu olan İrlanda Veri Koruma Otoritesi, 13 Eylül 2022'de taslak kararını Avrupa Birliği'ndeki diğer veri koruma otoritelerine sundu.

Soruşturma, TikTok platformunun platform ayarları bağlamında çocuk kullanıcıların kişisel verilerinin işlenmesine, özellikle 18 yaşından küçük kullanıcılarla ilgili olarak bu tür platform ayarlarının varsayılan ayar olarak "genel" ayarıyla işlenmesine ve 18 yaşından küçük kişiler için yaş doğrulama önlemlerinin yeterliliğine odaklanmaktadır.

Soruşturma ayrıca TikTok'un 18 yaşın altındaki kullanıcıların kişisel verilerinin işlenmesi bağlamında GDPR'nin şeffaflık yükümlülüklerine uyup uymadığının değerlendirmesini de kapsamaktadır.

GDPR'ın 60. maddesi kapsamında yürütülen süreçte, DPC'nin kararına karşı diğer ülkelerin veri koruma otoritelerinin "ilgili ve gerekçeli itirazları" iletmek için bir aylık süresi bulunmaktadır.

DANİMARKA'DAN GOOGLE ANALYTICS KARARI

Danimarka'nın veri koruma otoritesi Datatilsynet, ek önlemler olmaksızın ABD'ye veri aktarımları için Google Analytics'in kullanılmasının GDPR ile uyumlu olmadığına karar verdi.

Datatilsynet'in kararı Avusturya, Fransa ve İtalya'dan gelen kararları takip etmekte ve farklı ülkelerin veri koruma otoriteleri arasında paylaşılan görüşün "denetim makamları arasında pan-Avrupa bir tutum" ve uyumlu bir yaklaşıma yönelik önemli bir adım olduğunu belirtmektedir.

Datatilsynet, Danimarkalı veri sorumlularına Google Analytics kullanımının GDPR çerçevesinde olup olmadığını değerlendirmelerini tavsiye etti. Buna göre veri sorumluları tarafından ya bu kullanım hukuki bir zemine oturtulmalı ya da Google Analytics kullanımına son verilmelidir.

GLOBAL GELİŞMELER

GÜNEY KORE'DE GOOGLE VE META ALEYHİNE 71 MİLYON DOLAR İDARİ PARA CEZASI UYGULANDI

Yerel basında çıkan haberlere göre, Güney Kore Veri Koruma Otoritesi daha önce Facebook olarak bilinen Google ve Meta'ya, yürürlükteki kişisel verileri koruma mevzuatını ihlal ettikleri için 100 milyar won (yaklaşık 71,9 milyon dolar) para cezası verdi.

İdari para cezasının temelinde, Google ve Meta'nın kullanıcıların rızası olmadan kişisel verilerin toplaması ve bu verilerin kişiselleştirilmiş çevrimiçi reklamcılık ve diğer amaçlar için kullanılması yer almakta.

İdari para cezasına ek olarak ilgili veri koruma otoritesi tarafından veri işleme faaliyetlerinin mevzuata uyumlu hale getirilmesi de emredildi.

BİRLEŞİK KRALLIK TİKTOK'A 27 MİLYON POUND CEZA UYGULAYABİLİR

Birleşik Krallık Veri Koruma Otoritesi ("ICO"), TikTok Inc ve TikTok Information Technologies UK Limited'e yönelik potansiyel bir para cezasından önce gelen yasal bir belge olan bir "niyet bildirimi" ile yayınladı. ICO, TikTok'a karşı başlattığı soruşturmada, veri koruma yasasını ihlal ettiğini ve TikTok'un platformunu kullanan çocukların gizliliğini koruyamadığını tespit etti. TikTok, soruşturma sonrasında 27 milyon sterlin para cezasına çarptırılabilir.

İhlale ilişkin detaylı bilgilere link üzerinden erişebilirsiniz.

ENDONEZYA'DA KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN İLK YASA MECLİS TARAFINDAN ONAYLANDI

20 Eylül 2022'de Endonezya parlamentosunda Endonezya'nın ilk kişisel verileri koruma yasası onaylandı. Yasa, Endonezya'da yürürlüğe giren ilk kapsamlı veri koruma yasası olup ilgili bakanlık tarafından belirlenen bir tarihte yürürlüğe girecektir. Yasaya tabi kuruluşların yasanın gerekliliklerine uyması için iki yıllık bir geçiş süresi öngörülmüş vaziyette.

Yasa, kamu veya özel hukuk kişisi olması fark etmeksizin Endonezya'da ikamet eden kişilerin kişisel verilerini işleyen tüzel kişileri kapsamaktadır. Yasada kişisel verilerin kişisel kazanç için hukuka aykırı olarak kullanılmasından ötürü altı yıla kadar hapis cezası da dahil olmak üzere, çeşitli yaptırımlar getirmektedir.

Yasa, Endonezya cumhurbaşkanına yasa kapsamındaki ihlaller için idari yaptırım uygulamak üzere bir veri koruma otoritesi kurma yetkisi vermektedir. Veri koruma otoritesi, yasanın ihlali halinde, bir veri sorumlusunun yıllık gelirinin yüzde ikisine kadar para cezası uygulayabilecektir. Ayrıca, Kanuna aykırı hareket edenlerin mal varlıklarına el konulabilir veya beş yıla kadar hapis cezası verilebilir.

Yasa uyarınca, Endonezya'da ikamet eden kişiler kişisel verilerinin ihlali için tazminat talep edebilecek ve veri sorumlusuna karşı verilerine erişme, verilerin silmesini talep etme ve veri sorumlusunun kişiye ait kişisel verilere erişiminin kısıtlanması gibi gizliliği sağlamaya yönelik çeşitli haklara kavuşmuştur.