6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) uyarınca kişisel veri; kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir.

Kişisel veri, kimliği belirli veya belirlenebilir kişiye ilişkin ad, soyad, TC kimlik numarası, iletişim bilgileri gibi her türlü bilgiyi ifade etmektedir. Kişisel verileriniz; 6698 sayılı Kişisel Verilerin Korunması Kanunu ("KVKK"), 5809 Sayılı Elektronik Haberleşme Kanunu, Bilgi Teknolojileri ve İletişim Kurumu, Kişisel Verileri Korunma Kurumu düzenlemeleri ve sair mevzuat hükümleri çerçevesinde işlenebilecek olup, ilgili mevzuat gereğince şirketimiz kişisel verilerinizin hukuka aykırı olarak işlenmesini önleme, hukuka aykırı olarak erişilmesini önleme ve muhafazasını sağlama amacıyla, uygun güvenlik düzeyini temin etmeye yönelik tüm teknik ve idari tedbirleri almaktadır.

Kişisel Verilerin İşlenmesi ve İşlenme Amaçları
KVKK madde 4 uyarınca;
"(1) Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.
(2) Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:
a) Hukuka ve dürüstlük kurallarına uygun olma.
b) Doğru ve gerektiğinde güncel olma.
c) Belirli, açık ve meşru amaçlar için işlenme.
ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.
d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme."

Kişisel Verilerin Korunması Kanunu'na Uyum Temel Altyapı Oluşturma Süreçleri

- VERBİS Sistemine Kayıt
- Kişisel Veri Envanteri Oluşturma
- Süreç veya Faaliyet Bazında Kişisel Verilerin Tespiti
- Tespit Edilen Kişisel Verilerin Niteliklerinin Belirlenmesi
- İşlenen Kişisel Verinin Hukuki Sebebinin Tespiti
- Kişisel Veri İşleme Amaçlarının Tespiti
- Veri Konusu Kişi Grubunun Belirlenmesi
- İşlenen Kişisel Verilerin Saklama Süresinin Belirlenmesi
- İşlenen Kişisel Verilerin Aktarıldığı Alıcı / Alıcı Gruplarının Belirlenmesi
- Yabancı Ülkelere Aktarılan Kişisel Verilerin Belirlenmesi
- İşlenen Kişisel Veriler İçin Alınan Teknik ve İdari Tedbirlerin Belirlenmesi
- Birim yöneticilerine KVKK sunumu ve bilgilendirmesi
- Farkındalık eğitimleri
- Veri sorumlusu eğitimi
- Aydınlatma politikasının hazırlanması
- Tedarikçi / müşteri/Personel sözleşmelerinin KVKK acısından güncellenmesi
- Genel Aydınlatma metninin hazırlanması
- Çalışanlara ilişkin genel aydınlatma metninin oluşturulması
- Veri saklama ve imha politikasının kurgulanmasıAşağıda belirtilen başlıklar kurum içerisinde gereğiyle yapıldığında verilerin ihlali azaltılmış olur
- Yetkilendirme matrisi oluşturulmalıdır.

- Yetki kontrolü yapılmalıdır.
- Erişim loğları tutulmalıdır.
- Kullanıcı hesapları yönetilmelidir.
- Ağ ortamının güvenliği sağlanmalıdır.
- Uygulamaların güvenliği sağlanmalıdır
- Veriler şifreleme yöntemleri ile şifrelenmelidir.
- Sızma testleri yapılarak kurum güvenliği test edilmelidir.
- Saldırı tespit ve önleme sistemleri oluşturulmalıdır.
- Log kayıtları incelenmeli ve yedeklenmelidir.
- Veri maskelemeleri yapılmalıdır.
- Veri kaybı önleme yazılımları kullanılmalıdır.
- Yedekleme sistemleri kullanılmalıdır.
- Güncel anti-virüs sistemleri kullanılmalıdır.
- Verileri durumlarına göre silme, yok etme veya anonim hale getirme işlemleri yapılmalıdır.

Server Güvenliği

Eskiden sitelerimizi barındırmak için basit standart hosting hesapları ihtiyacımızı görürken artık her site için birer sunucu kiralar duruma geldik. Durum böyle olunca temel seviyede sunucu yönetimini öğrenmek de kaçınılmaz oldu. **Sunucu güvenliği**nin de yönetim başlığı altında en önemli alt başlık olduğunu sanırım hatırlatmama gerek yok. Bu nedenle kendi sunucularınızı yönetirken alabileceğiniz temel güvenlik tedbirlerine bu yazımda kısaca değinmek istedim. İyi okumalar.

Root Girişinin Engellenmesi

Herhangi bir firmadan cloud sunucu (ya da başka tür sunucu) aldığınızda size işletim sistemi kurulu olarak verilir. Bununla birlikte size gelen bilgilendirme epostasında **root** kullanıcısına ait **parola** bulunur. Root kullanıcı adı standart olduğu için sitenize yapılan saldırılarda hackerlara sadece parolayı tahmin etmek kalır. Bu sebepten root kullanıcısı ile girişin derhal yasaklanması/engellenmesi gerekir.

Firewall Kurulumu

CentOS'un en güzel yanlarından birisi de bünyesinde hazır ve oldukça kaliteli bir Firewall servisi olan Firewalld bulunmasıdır. Firewalld'nin birçok ayarı bulunmasına rağmen sadece başlatmak da sizi oldukça sağlam bir şekilde korur. Bu servisi başlatmak için aşağıdaki komuttan faydalanabilirsiniz

Firewall kurulumu artık bütün firmalarda alınması gereken önlemlerin başında yer alıyor

Ağ trafiğini kontrol ederek belirlenen filtreleme yaparak dışarıdan gelen saldırılara karşı sizi 7/24 korur

Açık Portları Kontrol Edin

Bilindiği gibi sunucumuza yapılan bağlantılar “port” olarak adladırılan geçiş noktalarından yapılır. Yani herhangi bir saldırı söz konusu ise mutlaka açık portlardan birisi hedef alınacaktır. Gereksiz servisler gibi gereksiz portları da kontrol edip kapalı tutmakta fayda var. Aşağıdaki komut ile dinlemede (listen) olan portları ve bu portların hangi servisler tarafından kullanıldığını listeleyebilirsiniz.

KVKK ile hayatımıza giren düzenlemeler arasında önem arz eden konulardan biri de **kişisel verilerin Türkiye’de bulundurulması** hususudur. Kişisel verilerin Türkiye’de muhafazasın

Öte yandan Kişisel Verileri Koruma Kurulu 31 Mayıs 2019 tarihinde aldığı bir kararla, yurt dışı kaynaklı pazarlama faaliyeti yürüten, kurumsal mail hizmetini Google ve Yandex gibi verilerini yurt dışındaki sunucularında (server) saklayan firmalardan hizmet alan kurumların işlerini zorlaştırmıştır.

Bir firmanın Kişisel Verileri Koruma Kurulu’na müracaat ederek, kurumsal e-posta hizmetlerinin Gmail üzerinden kullanılıp kullanılamayacağı hususundaki sorusu üzerine Kurul şu yönde bir karara varmıştır.

“Google firmasına ait Gmail e-posta hizmeti altyapısının kullanılması durumunda gönderilen ve alınan e-postaların dünyanın çeşitli yerlerinde bulunan veri merkezlerinde tutulması söz konusu olacağından, böyle bir durumda kişisel verilerin yurt dışına aktarılmış olacağına ve veri sorumlularının söz konusu uygulamayı 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun ‘Kişisel verilerin yurt dışına aktarılması’ başlıklı 9’uncu maddesi hükümlerine uygun olarak gerçekleştirilmesine;

Server’ları yurt dışında bulunan veri sorumlularından / veri işleyenlerden temin edilen saklama hizmetlerinin de Kanunun 9’uncu maddesi hükümlerine uygun olarak gerçekleştirilmesine…”

Söz konusu kararda, sunucuları yurtdışında bulunan firmalardan kurumsal e-posta hizmeti alacak olan kurumların öncelikle ilgili maddedeki şartları yerine getirmesi isteniyor. Maddede özetle, kurumsal e-posta adresi kullanan ya da kurumsal bir e-posta adresine gönderim yapan herkesin açık rızasının alınması isteniyor ki, bu şartı yerine getirmek oldukça zor.

E-posta sunucusu, Kurul’un güvenli ülke olarak ilan ettiği ülkelerden birinde bulunuyorsa açık rıza aranmıyor. Fakat halihazırda Kurul’un güvenli ülke ilan ettiği herhangi bir ülke de bulunmuyor. ABD ve Rusya gibi Google ve Yandex’in merkezi olan ülkelerin güvenli ülke ilan edilmesi de sorunu çözmüyor. Çünkü internet dünyasında tekel konumundaki Google, sunucularındaki verileri ABD haricindeki çeşitli ülkelerde de sakladığından şirket merkezlerinin bulunduğu ülkelerin güvenli ilan edilmesi pek bir anlam ifade etmiyor.

Son olarak yurt dışında sunucusu bulunan firmanın ve ülkenin veri güvenliği konusunda yeterli koruma sağlayacağına dair taahhütte bulunması gerekiyor.

Mevzuatın gerektirdiği şartlar nedeniyle şirketlerin KVKK'ya uygun olarak yurt dışındaki sunucularda verilerini muhafaza etmesi mümkün görünmüyor. Bu durum, şirketlerin, sunucuları yurt içinde bulunan e-posta pazarlama firmalarından hizmet almasını gerekli kılıyor.