SAFE-T

Keeping Data in the Right Hands

Kişisel Verilerin Korunması Kanunu (KVKK) için BT Altyapınızı Nasıl Hazırlayabilirsiniz?

KVKK, insanların kişisel haklarını ve özgürlüklerini, özellikle mahremiyetlerini korumayı ve kişisel verilerinin güvenli olarak işlenmesini amaçlar. Kanun, Türkiye'de bir ofis, şube veya ajansı olan tüm kuruluşlar kadar Türkiye'deki vatandaşların verilerini toplayan ve işleyen tüm uluslararası işletmelerin de kişisel veri kullanımlarını denetler. Bu yasa halen yürürlüktedir ve uyumsuzluk için para cezalarının başlama tarihi 7 Nisan 2018'dir.

Kişisel veriler, doğrudan veya dolaylı olarak kişiyi tanımlamak için kullanılabilecek gerçek bir kişi veya "Veri Konusu" ile ilgili herhangi bir bilgi olarak tanımlanır. İsim, fotoğraf, e-posta adresi, banka bilgilerinden finansal bilgilere veya bilgisayar IP adresine kadar her şey bu kapsama girebilir.

KVKK'ya uyulmaması büyük para cezalarına (1 milyon TL'ye kadar), kurum hakkında olumsuz bir algıya ve marka hasarına yol açabilir.

Dış ve İç Tehditler

Kurumlar, hassas verileri güvence altına almaya çalışırken bir yandan da birçok iç ve dış tehdide maruz kalabilirler.

Dış tehditler

Bunlar DDoS saldırılarını ve kritik hizmetlere yapılan saldırıları kapsar. Bilgisayar korsanları verilerinizi çalmak, yanlış amaçlar için kullanmak veya tehlikeye sokmanın yollarını bulmaya çalışırlar. Uygulamalar DDoS saldırılarına karşı savunmasızdır. Hassas veriler ve SSL anahtarları bulutta veya şirket içi DMZ alanlarında saklanır ve harici bilgisayar korsanlarına dahili ağlara erişebilme potansiyeli sağlar.

İç tehditler

Sıfırıncı-gün saldırıları, fidye yazılımı, veri kaçırma ve sızıntısı gibi tehditler zaten tehlikelidir. Ayrıca, kullanıcıların kurum içinde veya bulutta depolanan bilgilere doğrudan ve denetimsiz erişimi sözkonusu olduğunda, veri çalınması ve sızıntısı gibi durumlar oluşabilir. Veri depolama alanlarındaki veriler, bilgisayar korsanları tarafından fidye amaçlı yazılımlar bulaştırılarak şifrelenebilir.

KVKK Uygunluğu için Temel Unsurlar

Herhangi bir veri gizliliği uygulamasının başarısını destekleyen en temel unsurlar insan ve teknolojidir. Çalışanlar, mevzuat konusunda ve uyumun sağlanmasındaki rolleri bakımından eğitilebilirler ve bilinçlendirilebilirler. Ancak, teknolojinin KVKK uyumluluğu konusundaki kolaylaştırıcı ve zorlayıcı özellikleri de mutlaka dikkate alınmalıdır. **KVKK uyumluluğu sağlamak için bazı teknik tedbirler kritik öneme sahiptir:**

Kimlik Doğrulama: Sadece yetkili kullanıcılar sistemlere ve verilere erişebilmelidir. Her bir kullanıcıya benzersiz kullanıcı kimlikleri atanmalıdır. Saklanan tüm şifreler şifreli olarak tutulmalıdır.

Erişim Kontrolu: Kullanıcıların, uygulamaların ve hedef klasörlerin erişim izinleri açıkça tanımlanmalıdır. Bu izinler tam kontrol, okuma, yazma, değiştirme, okuma ve yürütme, silme ve listeleme içermelidir. Kullanıcı bazında belirlenebilmesi gereken politikalar, son geçerlilik tarihlerini içermelidir. Ayrıca, kuruluşların erişim mimarileri, hizmetlerini yetkisiz kullanıcılardan gizleyebilmelidir.

Şifreleme ve Kişisel Verilerin Güvenliği: Kullanıcı kimlikleri ve şifreler her zaman şifreli olarak saklanmalıdır. Dahili ve harici tüm bağlantılar, SSH/SSL protokolleri ve 256 bit AES standardına uygun olarak şifrelemeli, güçlü şifre kullanımı bir politika olarak zorlamalıdır.

Bütünlük: Paket düzeyinde ve dosya düzeyinde yapılan bütünlük denetimleri, bozuk ve zararlı verileri önler. Bu nedenle, dijital imzalar kullanılmalıdır.

Audit: Tüm paket ve dosya aktarım etkinlikleri günlüğe kaydedilmelidir - “kim”, “ne”, “ne zaman” ve “nasıl”.

Teknoloji: Kritik Verilerinizi Güvende Tutmak

Zamanla birlikte, organizasyonların veri altyapısı ve bunun etrafındaki sınırlar önemli ölçüde değişir. Safe-T'nin Erişim Tanımlı Yazılım çözümü, kurumunuzun uygulamalarına yetkili erişim sağladığı gibi, hibrit bulut ortamındaki bilgilerinin güvenli bir şekilde paylaşılmasına olanak verir ve sınırlarınız nerede olursa olsun sektörel düzenlemelere uymanıza yardımcı olur.

Safe-T çözümleri KVKK veri güvenliği gereksinimlerini karşılar ve müşterilerinizin verilerinin ele geçirilmemesini sağlayarak düzenlemelere uyumlu olmanızı sağlar. Safe-T’nin sağladıkları aşağıda özetlenmiştir:

- Veri servislerine, ağlara veya API'lere yetkisiz erişimin önlenmesi
- Kimlik doğrulama, erişim kontrolü, şifreleme, bütünlük ve denetim standartları sağlama
- Hareket halindeki veya durmakta olan verileri, Antivirüs ve DLP gibi çözümlere konnektörlerle bağlanarak koruma, SSH ve SSL protokolleri kullanarak şifreleme
- Kesin denetim uyumluluğuna ulaşmak için etkinlik ve eylem günlüğü oluşturma

Kişisel Verilerin Korunması İçin Teknik Tedbirler Özet Tablosu

6698 No.'lu Kişisel Verilerin Korunması Kanununun 12'nci maddesinin birinci fıkrasında;
"Veri sorumlusu;

a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

c) Kişisel verilerin muhafazasını sağlamak

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır." hükümleri yer almaktadır.

Bu kapsamda, kişisel verilerin işlenmesi sürecinde veri sorumlularının alması gereken teknik ve idari tedbirler konusunda uygulamada açıklık sağlanması ve iyi uygulama örnekleri oluşturması amacıyla Kişisel Verileri Koruma Kurulu tarafından Kişisel Veri Güvenliği Rehberi hazırlanmıştır. Bu rehberin 29'uncu sayfasında yer alan Tablo 4.1 veri sorumluları tarafından alınabilecek teknik tedbirleri göstermektedir.

Aşağıdaki tablo, önerilen teknik tedbirler ve bunların Safe-T tarafından nasıl karşılandığını göstermektedir.

Safe-T çözümleri, hassas bilgileri hem veriye erişim, hem de veri alışverişi kapsamında güvenceye alır. Safe-T tarafından KVKK uyumluluğu için sağlanan önlemler aşağıda özetlenmiştir:

- Veri servislerine, ağlara veya API'lere yetkisiz erişimi önleme
- Kimlik doğrulama, erişim kontrolü, şifreleme, bütünlük ve denetim standartları sağlama
- Aktarım halindeki veya duran verileri AES standardına uygun olarak şifreleme
- SSH ve SSL protokollerini kullanarak verilere güvenli erişim sağlama
- Antivirüs, kötü amaçlı yazılımlardan koruma ve DLP sistemlerine konnektörler ile bağlanarak, herhangi bir veri akışı için iş akışları oluşturma
- Sıkı bir denetim uyumluluğu için olay ve eylem günlüğü sağlamak

KVKK Teknik Tedbirleri	*Safe-T Özellikleri*
Yetki Matrisi **Yetki Kontrolu** **Kimlik Doğrulama**	• Safe-T, hassas verilere yalnızca kimliği doğrulanmış kullanıcıları eriştirir. • Benzersiz kullanıcı kimlikleri (her kullanıcı için ayrı kişisel hesap) • Active Directory / SQL DB ile bütünleşir. • Dahili çok faktörlü kimlik doğrulama ve yetkilendirme (MFA) motoru • Tüm kayıtlı şifreler şifreli olarak saklanır. • Sistem yöneticileri ve kullanıcılar için yerleşik role dayalı erişim kontrolü • Son kullanıcılar, yalnızca politikaya göre izin verilen uygulamaları ve verileri görebilir.
Erişim Logları ve Kaydı	• Windows Olay Görüntüleyicisi ile entegrasyon • Tüm paket ve dosya aktarım etkinliğinin günlüğe kaydı • Sistemdeki her etkinlik kaydedilir (konfigürasyon değişikliği, dosya erişimi, dosya transferi, oturum açma hataları ve daha bir çoğu) • Güvenlik bilgi ve olay yönetimi (SIEM) çözümlerine bağlantı
Kullanıcı Hesap Yönetimi, **Erişim Yönetimi**	• Safe-T sistemleri hassas verilere yalnızca yetkili kullanıcıların erişimine izin verir • Klasörlerde ve dosyalara, kullanıcı ve grup bazında erişim izinlerinin ayarlaması • Erişim izinleri şunları içerir: tam denetim, okuma, yazma (dosyaları oluşturma), değiştirme (dosyaları düzenleme), okuma ve çalıştırma (programları çalıştırma), klasör içeriğini silme veya listeleme • Kullanıcı ve grup bazında politikalar (politika sona erme tarihi, bant genişliği sınırlaması, kullanıcı disk alanı kotası, OTP, token teslimat yöntemi, dosya sona erme, indirme sayısı ve dosya boyutu sınırı) • Her bir kullanıcı ve grup için ayrı ve özel klasör • Safe-T, klasör ve dosyalara erişim hakkı verme seçeneğini, bilme hakkı parametrelerinin karşılanması durumunda sağlanması • Sunucu erişimini IP adres ve port aralıklarına göre kontrol etme

KVKK Teknik Tedbirleri	*Safe-T Özellikleri*
Ağ Güvenliği	• Safe-T'nin patentli Tersine Erişim (Reverse Access) teknolojisi üzerine kurulu talep bazında “Yazılım Tanımlı Çevre" (Software Defined Perimeter), şebeke erişim katmanını kimlik doğrulama katmanından ayırarak ve dahili ağları ayırarak, yalnızca yetkili kullanıcılara şeffaf bir şekilde erişim sağlar. IP erişimini sağlamadan önce kullanıcının kimliğini ve ilgili cihazın parmak izini doğrular. • Safe-T SecureStream İlke ve İş Akışı Motoru, ağ içinde giden, gelen veri alışverişi akışları için güvenlik ilkelerini otomatik olarak uygular. • Safe-T SDA sistemi, patentli ters erişim teknolojimizi kullanarak farklı ağlar arasında güvenli erişim sağlar.
Uygulama Güvenliği	Kapsam dışı
Şifreleme, Gizlilik	• Kullanıcı kimlikleri ve şifreleri her zaman şifrelidir • İstemci bağlantıları SSH ve SSL protokolleri üzerinden şifrelenir • 256 bit AES standardı kullanarak veri şifreleme • Safe-T sunucusu ile tüm istemci bağlantılarında şifreleme protokollerinin kullanımının zorlanması • Klasör düzeyine kadar yapılandırılabilir şifreleme • İlke tabanlı şifreleme gücü uygulaması • Şifreli protocol kullanımının zorunlu kılınması
Sızma Testi	Kapsam dışı
Saldırı Tesbit ve Önleme Sistemleri	Kapsam dışı
Veri Maskeleme	Kapsam dışı
Veri Kaybı ve Sızıntısı Önleme (DLP)	• Dosya tipine bağlı dahili DLP özellikleri • Üçüncü taraf DLP çözümleri kullanarak DLP kontrolü • Dijital imza desteği
Yedekleme	Veri yedekleme ve arşivleme çözümleri ile entegrasyon
Güvenlik Duvarları	Safe-T çözümü bir Güvenlik Duvarı değildir. Ancak, Safe-T patentli ters erişim teknolojisi, Güvenlik Duvarlarında dışarıdan içeriye gelen portların her zaman kapalı tutularak tersine erişim sağlar.

KVKK Teknik Tedbirleri	*Safe-T Özellikleri*
Güncel Antivirüs Sistemleri	Safe-T çözümü, diğer güvenlik, antivirüs ve zararlı yazılım önleme ürünleri arasında politikalara dayalı güvenli bir iş akışı sağlayarak trafik aracılığı yapar.
Silme, Yok Etme veya Anonim Hale Getirme	Safe-T Çözümü, verileri şifreleyerek ve yetkisiz kullanıcıların erişimini engelleyerek, verilerin silinmesi ve/veya yok edilmesi seçeneğini gereksiz kılar. Hassas veriye yapılan erişim, kesin bir kullanıcı kimliği ile günlüğe kaydedilir.
Anahtar Yönetimi	Tüm anahtarlar Safe-T sunucusu ile sınırlı ve güvenli bir şekilde erişilebilen diğer depolama alanları arasında bölünerek depolanır. Anahtarlar, sunucu üzerinde kurum ilkelerine göre yönetilir.

Hazırlıklı Olun

KVKK için hazırlık birçok fazı içerir, ancak aşağıdaki unsurlar öncelikle dikkat gerektirir:

- Veri koruma görevlilerinizi belirleyin
- Hesap verebilirlik alyapısını oluşturun ve sürdürün
- Etki/Sonuç değerlendirmeleri yaparak düzenlemelere uyumluluk için kuruluşunuzda, hangi verilerin, kaynakların, hedeflerin, süreçlerin ve bölümlerin gözden geçirilmesi gerektiğini anlayın
- Veri işleme envanterinizi gözden geçirin
- Tüm veri işleme aktivitelerinde hesap verebilirliği gösterebilmeniz için Bilgi Güvenliği Süreç Tasarımınızı tanımlayın
- Bulut uygulamalarını gözden geçirin ve sınır ötesi veri akışlarınızı kontrol edin
- Veri sahiplerinin, kişisel verilerini korunma amacıyla yapabilecekleri girişimler için önceden hazırlıklı olun

BR-3-12