# VERİ GÜVENLİĞİ VE KİŞİSEL VERİLERİN KORUNMASI

7 Nisan 2016 tarihinde, 6698 Sayılı Kişisel Verilerin Korunması Kanunu Resmi Gazetede yayınlanarak yürürlüğe girmiştir. Bu kanunla birlikte kimliği belirli veya belirlenebilir gerçek kişilere ilişkin her türlü bilgi koruma altına alınmıştır.

Teknolojinin hızla gelişmesi ve Endüstri 4.0 kavramının giderek yaygınlaştığı günümüzde, kalite yönetimi kavramı hammadde veya yarı mamul kullanılarak üretim yapılan sektörlerde olduğu gibi yazılım ve IT sektörlerinde de önemini arttırmıştır. Teknolojinin bu kadar hızlı yayılması ve gelişmesi, beraberinde birtakım dezavantajlar gibi güvenlik tehditlerini de getirmiştir. Bu tehditleri bertaraf edebilmek, bilginin gizliliğinin korunmasını sağlayabilmek tüm kuruluşlar için önemli hale gelmiştir. Özellikle yazılım sektörü gibi hizmet sektöründe bilgi gizliliğinin sağlanması zaruri hale gelmiştir. Bu sebeple; yazılımın analiz ve tasarım aşamasından, test ve kontrol aşamalarına kadar her süreçte ihtiyaçlara cevap verebilmesinden, gerekli güvenlik önlemlerinin alınmasına kadar detaylı bir kalite güvence süreci anlamına gelen "Yetenek Olgunluk Model Entegrasyonu CMMI (Capability Maturity Model Integration)" oluşturulmuş ve uygulamaya alınmıştır.

Özellikle, Endüstri 4.0 kavramı gibi sonradan ortaya çıkan "Sosyal Mühendislik" kavramı, veri güvenliği ve bilgi güvenliği için büyük bir tehdit oluşturmaktadır. Peki nedir bu Sosyal Mühendislik? Sosyal Mühendislik, başkası için yapmayacağımız bir şeyi yaptırma sanatıdır. Sosyal Mühendisler şirket çalışanı gibi veya yardıma muhtaç birisi gibi görünüp bilgi sızdırmak amaçlı yöntemler kullanabilirler.

Peki, bu kadar çok tehditle karşı karşıya kalan kuruluşlar ve bizler bu güvenlik tehditlerine karşı neler yapabiliriz? Buna geçmeden önce isterseniz önce veri nedir, veri güvenliği nedir? Bu kavramlardan biraz bahsederek işe başlayalım.

Veri, herhangi bir işleme tabi tutulmadan, gözlem veya ölçüm yöntemleri ile ortamdan elde edilen her türlü değerdir. Veri birçok biçimde bulunabilir. Kağıt üzerinde yazılı olabileceği gibi elektronik olarak saklanıyor olabilir veya posta ya da elektronik posta yoluyla bir yerden bir yere iletilebilir. Veri aynı zamanda kişiler arasında sözlü olarak da ifade edilebilir.

Veri güvenliği ise, elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bu bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür diyebiliriz. Bilgiye sürekli olarak erişilebilirliğin sağlandığı bir ortamda, bilginin göndericisinden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlüğünün sağlanması ve güvenli bir şekilde iletilmesi süreci ise bilgi güvenliği olarak tanımlanabilir.

Veri güvenliği; kurumdaki işlerin sürekliliğinin sağlanması, işlerde meydana gelebilecek aksaklıkların azaltılması veya Ar-Ge verilerinin gizli bilgilerinin çalınması gibi verinin çok çeşitli tehditlerden

korunmasını sağlar. Veri hangi formda olursa olsun, mutlaka uygun bir şekilde korunması sağlanmalıdır.

Veri güvenliğini sağlamak için Uluslararası Standart Organizasyonu olan ISO tarafından yayınlanan ve bu kapsamda bilgi güvenliğinin temelini oluşturan standartlar topluluğu karşımıza çıkıyor. Yaptığı faaliyet ve hizmetler gereği bazı kurumların bu belgeyi alması ve devamlılığını sağlaması zorunlu olmasına rağmen, veri ve bilgi işleyen her firmanın bu standart gerekliliklerini sağlamaları tartışmasız bir fark yaratacaktır.

**ISO/IEC 27001 Standartları Kapsamında Veri Güvenliği**

Kurumsal bilgi güvenliği; kurumların bilgi varlıklarının tespit edilerek zafiyetlerinin belirlenmesi ve istenmeyen tehdit ve tehlikelerden korunması amacıyla gerekli güvenlik analizlerinin yapılarak önlemlerinin alınması ve bu mekanizmaların düzenli kontrollerle takip edilmesi ve geliştirmesi olarak tanımlanabilir. ISO/IEC 27001:2013 – Bilişim Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler Standardı; bir Bilgi Güvenliği Yönetim Sistemini kurmak, geliştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için hazırlanmıştır.

Veri güvenliği temelde 3 (üç) unsuru hedefler:

- Gizlilik (Confidentiality)
- Bütünlük (Integrity)
- Kullanılabilirlik (Availability)

Bu kavramların anlamlarını biraz daha açacak olursak;

**Gizlilik:** Bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesidir.

**Bütünlük**: Bilginin yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı içeriğinin korunmasıdır.

**Kullanılabilirlik:** Bilginin, yetkili kişiler tarafından her ihtiyaç duyulduğunda kullanıma hazır durumda olması anlamına gelmektedir. Herhangi bir sorunun meydana gelmesi durumunda bile bilginin erişilebilir olması kullanılabilirlik özelliğinin bir gereğidir. Bu erişim kullanıcının hakları çerçevesinde olmalıdır.

Bilgi güvenliğinin sağlanması için bilgi varlıklarının korunması gerekmektedir. Fiziksel olarak korunması için, fiziksel güvenliğin, transfer edilmesi gereken bilginin korunması için iletişim güvenliğinin, sistemlere erişimlerin kontrol edilmesi için bilgisayar ve ağ güvenliğinin sağlanması gerekmektedir.

Bir kuruluşun ISO 27001 sertifikasına sahip olması, kurumun güvenlik risklerini bildiği, yönettiği, belli riskleri de ortadan kaldırmak için kaynak ayırdığı anlamına gelmektedir.

Veriler sadece kurumsal bilgiler olmayabilir, korumamız gereken diğer önemli veriler ise kişisel verilerdir. Kişisel verilerin korunması için 2016 yılından beri yoğun çalışmalar sürmektedir. Özellikle Kişisel Verileri Koruma Kurulu tarafından farkındalığın arttırılması için hem sosyal medyada hem de yapılan seminer ve bilgilendirme toplantılarıyla konuya büyük hassasiyet göstermektedirler.

**Kişisel Verilerin Korunması ve Veri Güvenliği**

Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Güvenliğinin sağlanması konusunda, http://kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf URL adresinde bir rehber yayınlayarak kişisel verilerin hukuka aykırı olarak işlenmesini ve kişisel verilere hukuka aykırı olarak erişilmesini önlemek amacıyla veri sorumlusunun alması gereken teknik ve idari tedbirlere ilişkin başlıca yöntemleri kamuya açıklamıştır.

Ayrıca, Kanun'un 12/1 maddesi hükmü uyarınca veri sorumlusu:

Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

Kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır. Söz konusu rehber, uygulamada bu tür tedbirlerin nasıl alınacağı konusunda açıklık yaratmak için yayınlanmıştır.

**Sonuç**

Yukarıda özetlemiş olduğum Veri güvenliği ve kişisel verilerin korunmasına fayda sağlayacak standart ve kanunlara uymayı bir zorunluluk olarak değil, değişen ve gelişen teknoloji koşullarına bir adım daha yaklaşmayı hedef alarak uygulamamız dileklerimle.

Oğuz TAŞBOLAT

KalDer Üyesi

TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.

Kalite Sistemleri Sorumlusu