TEKNİK TEDBİR LİSTESİ

Kişisel Verilerin Korunması / Teknik Tedbir Listesi

1- Ağ güvenliği ve uygulama güvenliği sağlanmalıdır.

Güvenlik Duvarı, VPN, Antivirüs , IDS (Saldırı Tespit Sistemleri), IPS (Saldırı Önleme Sistemleri) , Web filtreleme çözümleri (URL Filtering), Güçlü Tanılama (Strong Authentication) gibi tedbirlerin alınması gerekmektedir.

2- Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmalıdır.

Ağ sistemlerine dışarıdan erişim sağlanamaması olarak özetlenebilir.

3- Anahtar yönetimi uygulanmalıdır.

Bir simetrik anahtar algoritmasında, bir mesajın hem şifrelenmesi hem de şifrenin çözülmesi için aynı anahtarlar kullanılır. Asimetrik anahtarlar, simetrik anahtarların aksine matematiksel olarak birbirine bağlı iki farklı anahtardır. Bu anahtarlar, iletişim kurmak için tipik olarak birbirlerini tamamlar şekilde kullanılır.

4- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmalıdır.

Veri sorumlusu tarafından yeni sistemlerin tedariki, geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimleri göz önüne alınmalıdır.

5- Bulutta depolanan kişisel verilerin güvenliği sağlanmalıdır.

Bulut depolama hizmeti sağlayıcısı tarafından alınan güvenlik önlemlerinin de yeterli ve uygun olup olmadığının veri sorumlusunca değerlendirilmesi gerekmektedir. Bu kapsamda, bulutta depolanan kişisel verilerin neler olduğunun detaylıca bilinmesi, yedeklenmesi, senkronizasyonun sağlanması ve bu kişisel verilere gerekmesi halinde uzaktan erişim için iki kademeli kimlik doğrulama kontrolünün uygulanması önerilmektedir. Söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi, bulut ortamlarına şifrelenerek atılması, kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekmektedir. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılır hale getirmeye yarayabilecek şifreleme anahtarlarının tüm kopyalarının da yok edilmesi gerekir.

TEKNİK TEDBİR LİSTESİ

Kişisel Verilerin Korunması / Teknik Tedbir Listesi

6- Erişim logları düzenli olarak tutulmalıdır.

Tüm ağ üzerinde bulunan tüm bilgisayar sistemlerinin tam zamanlı yapılan işlemlerin kayıt altına alınması olarak ifade edilebilir.

7- Güncel anti-virüs sistemleri kullanılmalıdır.

Tüm ağ üzerinde bulunan tüm bilgisayar sistemlerinin güncel anti-virüs yazılımlarına sahip olması gerekmektedir.

8- Güvenlik duvarları kullanılmalıdır.

Kişisel verilerin bulunduğu bilgisayarlara sızma işlemi öncesinde gerçekleşen ihlalleri durdurma görevini üstlenmektedir.

9- Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmalıdır.

Tutulan log kayıtlarının dışarıdan erişimin engellenmesi ve log kayıtlarının değiştirilemez, silinemez olması gerekmektedir.

10- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmelidir.

IDS (Saldırı Tespit Sistemleri), IPS (Saldırı Önleme Sistemleri) bulunması gerekmektedir.

11- Şifreleme yapılmalıdır.

Kişisel verilerin çeşitli anahtarlar yardımı ile şifrelenerek saklanması gerekmektedir.

12- Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılmalıdır.

Özel nitelikli Kişisel verilerin çeşitli anahtarlar yardımı ile şifrelenerek aktarılması gerekmektedir.

TEKNİK TEDBİR LİSTESİ

Kişisel Verilerin Korunması / Teknik Tedbir Listesi

13- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmalıdır.

Kişisel verilerin periyodik olarak yedeklenmesi ve bu kişisel verilerin yedeklerininde fiziksel olarak güvenliğinin sağlanması gerekmektedir.

14- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmalıdır.

Her bilgisayarın sahibi tarafından kendine ait bir şifre ile giriş sağlayabilmesi ve periyodik olarak şifrelerin yenilenerek olası bir kişisel veri ihlalinin önüne geçilebilmesi gerekmektedir.

15- Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmelidir.

Özel nitelikli veriler eğer paylaşılacak ise kep veya kurumsal posta hesabı kullanılarak gönderilmesi gerekmektedir.

16- Özel nitelikli kişisel veriler için güvenli şifreleme / kriptografik anahtarlar kullanılmakta ve farklı birimlerce yönetilmelidir.

Özel nitelikli kişisel veriler şifrelenmesi ve şifre çözücü anahtarların sadece bu iş için özel birimlerin yönetiminde işlem yapılmaktadır.

17- Saldırı tespit ve önleme sistemleri kullanılmalıdır.

IDS (Saldırı Tespit Sistemleri), IPS (Saldırı Önleme Sistemleri) bulunması gerekmektedir.

18- Sızma testi uygulanmalıdır.

Sisteme periyodik olarak sızma ve hack testleri yapılması gerekmektedir.

TEKNİK TEDBİR LİSTESİ

Kişisel Verilerin Korunması / Teknik Tedbir Listesi

19- Gerektiğinde veri maskeleme önlemi uygulanmalıdır.

Veri maskeleme, verilerin tanınamaz ve geri döndürülemez hale getirilmesidir. Örneğin anonimleştirme işlemi bir veri maskeleme işlemidir.

20- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmalıdır.

Belirlenen görevli tarafından bu işlemlerin periyodik olarak kontrol edilip; ilgili işlemlerin yapılması gerekmektedir.

21- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmalıdır.

Sadece belirli personellerin içeriye girişleri için güvenlik tedbirlerinin alınması ve bu doğrultuda veri sızıntısının önüne geçilmesi gerekmektedir.

22- Veri kaybı önleme yazılımları kullanılmalıdır.

DLP genel tanımıyla, şirketlerin hassas verilerinin, şirket içinde nasıl yer değiştirdiğini gözleyen ve kontrollü bir şekilde; "dışarı sızmalarını" engelleyen bir teknoloji olarak ifade edilebilir.

23- Çalışanlar için yetki matrisi oluşturulmalıdır.

Kurumlarda hangi veriye kimin, neden eriştiğini, paylaşımdaki klasör yetkileri ve bunların periyodik kontrolleri, departman değiştiren personellerin erişim yetkilerinin kaldırılması gibi konuları içinde barındıran bir yetkilendirme sistemlerinin oluşturulması gerekmektedir.