uğurnakl	**KİŞİSEL VERİ GÜVENLİĞİNE İLİŞKİN TEKNİK TEDBİRLER BEYANI**
Güncelleme No/Tarihi	**00/-**

6698 sayılı kanun ve Kişisel Verilerin Korunması Kurumu tarafından yayımlanan veri güvenliğine ilişkin teknik tedbirler rehberinde aşağıda belirtilen hususlarda gerekli önlemlerin alınması gerekmektedir.Bu kapsamda Komite tarafından,aşağıda belirtilen yükümlülükler esas alınarak,şirket bünyesinde alınan mevcut teknik tedbirlerinin uyumlu olup olmadığını tespit edebilmek ve gerekli eksiklik ve zafiyetleri giderebilmek amacıyla Bilgi İşlem Departmanlığınca rapor hazırlattırılması kararlaştırılmıştır.İlgili departman bünyesinde hazırlanacak olan raporda eksik tüm hususların dikkatle tespit edilmesi ve Komite'yi derhal bilgilendirmesi hususunda ihtar edilmesi gerekmektedir.

1-SİBER GÜVENLİĞİN SAĞLANMASI;

Kişisel veri içeren bilgi teknoloji sistemlerinin internet üzerinden gelen izinsiz erişim tehditlerine karşı korunmasında alınabilecek öncelikli tedbirler, g**üvenlik duvarı ve ağ geçidi**dir. Bunlar, internet gibi ortamlardan gelen saldırılara karşı ilk savunma hattı olacaktır.

Bununla birlikte hemen hemen her yazılım ve donanımın bir takım kurulum ve yapılandırma işlemlerine tabi tutulması gerekmektedir. Ancak yaygın şekilde kullanılan bazı yazılımların özellikle eski sürümlerinin belgelenmiş güvenlik açıkları bulunmakta olup, **kullanılmayan yazılım ve servislerin cihazlardan kaldırılması** potansiyel güvenlik açıklarının azalmasını sağlamaya yardımcı olacaktır. Bu nedenle, kullanılmayan yazılım ve servislerin güncel tutulması yerine silinmesi, kolaylığı nedeniyle öncelikle tercih edilebilecek bir yöntemdir.

Yama yönetimi ve yazılım güncellemeleri olup yazılım ve donanımların düzgün bir şekilde çalışması ve sistemler için alınan güvenlik tedbirlerinin yeterli olup olmadığının düzenli olarak kontrol edilmesi de olası güvenlik açıklarının kapatılması için gereklidir.

Kişisel veri içeren sistemlere erişimin de sınırlı olması gerekmektedir. Bu kapsamda çalışanlara, yapmakta oldukları iş ve görevler ile yetki ve sorumlulukları için gerekli olduğu ölçüde **erişim yetkisi** tanınmalı ve kullanıcı adı ve şifre kullanılmak suretiyle ilgili sistemlere erişim sağlanmalıdır. Söz konusu **şifre ve parolalar** oluşturulurken, kişisel bilgilerle ilişkili ve kolay tahmin edilecek rakam ya da harf dizileri yerine büyük küçük harf, rakam ve sembollerden oluşacak kombinasyonların tercih edilmesi sağlanmalıdır. Buna bağlı olarak veri sorumlularının, erişim yetki ve kontrol matrisi oluşturmaları ve ayrı bir erişim politika ve prosedürleri oluşturarak veri sorumlusu organizasyonu içinde bu politika ve prosedürlerin uygulamaya alınması önerilmektedir.

Güçlü şifre ve parola kullanımının yanısıra, kaba kuvvet algoritması (BFA) kullanımı gibi yaygın saldırılardan korunmak için **şifre girişi deneme sayısının sınırlandırılması**,düzenli aralıklarla **şifre ve parolaların değiştirilmesi**nin sağlanması, yönetici hesabı ve admin yetkisinin sadece ihtiyaç olduğu durumlarda kullanılması için açılması ve veri sorumlusuyla ilişikleri kesilen çalışanlar için zaman kaybetmeksizin hesabın silinmesi ya da girişlerin kapatılması gibi yöntemlerle erişimin sınırlandırılması gerekmektedir.

Kötü amaçlı yazılımlardan korunmak için ayrıca, bilgi sistem ağını düzenli olarak tarayan ve tehlikeleri tespit eden **antivirüs, antispam gibi ürünlerin kullanılması** gerekmektedir. Ancak bu ürünlerin sadece kurulumu yeterli olmayıp güncel tutularak gereken dosyaların düzenli olarak tarandığından emin olunmalıdır.

Veri sorumluları tarafından, farklı internet siteleri ve/veya mobil uygulama kanallarından kişisel veri temin edilecekse, bağlantıların SSL ya da daha güvenli bir yol ile gerçekleştirilmesi de kişisel veri güvenliğinin sağlanması için önemlidir.

2. KİŞİSEL VERİ GÜVENLİĞİNİN TAKİBİ

Veri sorumlularının sistemleri çoğunlukla hem içeriden hem de dışarıdan gelen saldırılar ve siber suçlara veya kötü amaçlı yazılımlara maruz kalmakta olup çeşitli belirtilere rağmen bu durum uzun süre fark edilememekte ve müdahale için geç kalınabilmektedir.Bu durumun önüne geçebilmek için;

a) Bilişim ağlarında hangi yazılım ve servislerin çalıştığının kontrol edilmesi,

b) Bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının belirlenmesi,

c) Tüm kullanıcıların işlem hareketleri kaydının düzenli olarak tutulması (log kayıtları gibi),

ç) Güvenlik sorunlarının mümkün olduğunca hızlı bir şekilde raporlanması,

d) Çalışanların sistem ve servislerdeki güvenlik zaafiyetlerini ya da bunları kullanan tehditleri bildirmesi için resmi bir raporlama prosedürü oluşturulması gerekmektedir. Söz konusu raporlama sürecinde oluşturulacak raporlar, sistem tarafından oluşturulacak otomatik raporlar olabilir. Bu raporların sistem yöneticisi tarafından en kısa sürede toplulaştırılarak veri sorumlusuna sunulması gerekmektedir.güvenlik yazılımı mesajları, erişim kontrolü kayıtları ve diğer raporlama araçlarının düzenli olarak kontrol edilmesi, bu sistemlerden gelen uyarılar üzerine harekete

geçilmesi, bilişim sistemlerinin bilinen zaafiyetlere karşı korunması için düzenli olarak zaafiyet taramaları ve sızma testlerinin yapılması ile ortaya çıkan güvenlik açıklarına dair testlerin sonucuna göre değerlendirmeler yapılması,
-Bilişim sisteminin çökmesi, kötü niyetli yazılım, servis dışı bırakma saldırısı, eksik veya hatalı veri girişi, gizlilik ve bütünlüğü bozan ihlaller, bilişim sisteminin kötüye kullanılması gibi istenmeyen olaylarda deliller toplanmalı ve güvenli bir şekilde saklanması gerekmektedir.

3-KİŞİSEL VERİ İÇEREN ORTAMLARIN GÜVENLİĞİNİN SAĞLANMASI

-Kişisel veriler, veri sorumlularının yerleşkelerinde yer alan cihazlarda ya da kağıt ortamında saklanıyor ise, bu cihazların ve kağıtların çalınması veya kaybolması gibi tehditlere karşı fiziksel güvenlik önlemlerinin alınması suretiyle korunması gerekmektedir. Aynı şekilde, kişisel verilerin yer aldığı fiziksel ortamların dış risklere (yangın, sel vb.) karşı uygun yöntemlerle korunması ve bu ortamlara giriş / çıkışların kontrol altına alınması önemlidir.
Kişisel veriler elektronik ortamda ise, kişisel veri güvenliği ihlalini önlemek için ağ bileşenleri arasında erişim sınırlandırılabilir veya bileşenlerin ayrılması sağlanabilir. Örneğin kullanılmakta olan ağın sadece bu amaçla ayrılmış olan belirli bir bölümüyle sınırlandırılarak bu alanda kişisel verilerin işleniyor olması halinde, mevcut kaynaklar tüm ağ için değil de sadece bu sınırlı alanın güvenliğini sağlamak amacıyla ayrılabilecektir.Aynı seviyedeki önlemlerin veri sorumlusu yerleşkesi dışında yer alan ve veri sorumlusuna ait kişisel veri içeren kağıt ortamları, elektronik ortam ve cihazlar için de alınması gerekmektedir.
Kişisel veri güvenliği ihlalleri sıklıkla kişisel veri içeren cihazların (dizüstü bilgisayar, cep telefonu, flash disk vb.) çalınması ve kaybolması gibi nedenlerle ortaya çıksa da elektronik posta ya da posta ile aktarılacak kişisel verilerin de dikkatli bir şekilde ve yeterli tedbirler alınarak gönderilmesi gerekmektedir. Ayrıca çalışanların şahsi elektronik cihazlarının, bilgi sistem ağına erişim sağlaması da güvenlik ihlali riskini arttırdığından bunlar için de mutlaka yeterli güvenlik tedbirleri alınmalıdır.
Kişisel veri güvenliğinin sağlanması için kişisel veri içeren kağıt ortamındaki evraklar, sunucular, yedekleme cihazları, CD, DVD ve USB gibi cihazların ek güvenlik önlemlerinin olduğu başka bir odaya alınması, kullanılmadığı zaman kilit altında tutulması, giriş çıkış kayıtlarının tutulması gibi fiziksel güvenliğin arttırılmasına ilişkin önlemler de alınmalıdır. Kişisel veri içeren cihazların kaybolması veya çalınması gibi durumlara karşı erişim kontrol yetkilendirmesi ve/veya şifreleme yöntemlerinin kullanılması kişisel veri güvenliğinin sağlanmasına yardımcı olacaktır. Bu kapsamda şifre anahtarı, sadece yetkili kişilerin erişebileceği ortamda saklanmalı ve yetkisiz erişim önlenmelidir. Benzer şekilde, kişisel veri içeren kağıt ortamındaki evraklar da kilitli bir şekilde ve sadece
yetkili kişilerin erişebileceği ortamlarda saklanmalı, söz konusu evraklara yetkisiz erişim önlenmelidir.Bunlarla birlikte şifreleme farklı farklı formlarda kullanılan ve bu formlara göre farklı şartlar sağlayan bir güvenlik sağlama aracıdır. Bu kapsamda, tam disk şifrelemesiyle cihazın tümü şifrelenebilir ya da cihazda bulunan bir dosya şifrelenebilir. Bazı yazılımlar ise verilerde değişiklik yapılmasına izin vermemek için şifre koruması sunmakla birlikte bu yazılımlar kişisel verinin yetkisiz kişiler tarafından okunmasını durdurmaz. Bu nedenle hangi şifreleme yöntemleri kullanılırsa kullanılsın kişisel verilerin tam olarak korunduğundan emin olunmalı ve bu amaçla uluslararası kabul gören şifreleme programlarının kullanımı tercih edilmelidir. Tercih edilen şifreleme yönteminin asimetrik şifreleme yöntemi olması halinde, anahtar yönetimi süreçlerine önem gösterilmelidir.

4. KİŞİSEL VERİLERİN BULUTTA DEPOLANMASI
Kişisel verilerin bulutta depolanması, hukuka aykırı işlemenin ve erişimin önlenmesi ile hukuka uygun muhafaza yükümlülüğü olan veri sorumlusunun kendi bilgi teknolojileri sistemi ağından ayrılmasına ve kişisel verilerin bulut depolama hizmeti sağlayıcıları tarafından işlenmesine neden olduğundan, bu durum birtakım riskleri beraberinde getirmektedir. Bu nedenle, 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.

5. BİLGİ TEKNOLOJİLERİ SİSTEMLERİ TEDARİĞİ, GELİŞTİRME VE BAKIMI

Veri sorumlusu tarafından yeni sistemlerin tedariği, geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimleri göz önüne alınmalıdır. Uygulama sistemlerinin girdilerinin doğru ve uygun olduğuna dair kontroller yapılmalı, doğru girilmiş bilginin işlem sırasında oluşan hata sonucunda veya kasıtlı olarak bozulup bozulmadığını kontrol etmek için uygulamalara kontrol mekanizmaları yerleştirilmelidir. Uygulamalar, işlem sırasında oluşacak hataların veri bütünlüğünü bozma olasılığını asgari düzeye indirecek şekilde tasarlanmalıdır. Arızalandığı ya da bakım süresi geldiği için üretici, satıcı, servis gibi üçüncü kurumlara gönderilen cihazlar eğer kişisel veri içermekte ise bu cihazların bakım ve onarım işlemi için gönderilmesinden önce, kişisel verilerin güvenliğinin sağlanması için cihazlardaki veri saklama ortamının sökülerek saklanması, sadece arızalı parçaların gönderilmesi gibi işlemler yapılması gerekir. Bakım ve onarım gibi amaçlarla dışarıdan personel gelmişse kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması gerekir.

6. KİŞİSEL VERİLERİN YEDEKLENMESİ

Kişisel verilerin herhangi bir sebeple zarar görmesi, yok olması, çalınması veya kaybolması gibi hallerde veri sorumlularının yedeklenen verileri kullanarak en kısa sürede faaliyete geçmesi gerekmektedir. Ayrıca kötü amaçlı yazılımlar da halihazırdaki verilere erişime engel olabilmektedir. Örneğin elektronik cihazlardaki kişisel verileri içeren dosyaları kilitleyen ve bunların açılabilmesi için veri sorumlusunu fidye ödemeye zorlayan kötü amaçlı yazılımlar olabilir. Bu tür kötü amaçlı yazılımlara karşı kişisel veri güvenliğini sağlamak için veri yedekleme stratejilerinin geliştirilmesi önerilmektedir. Öte yandan, yedeklenen kişisel veriler sadece sistem yöneticisi tarafından erişilebilir olmalı, veri seti yedekleri mutlaka ağ dışında tutulmalıdır. Aksi halde, veri seti yedekleri üzerinde kötü amaçlı yazılım kullanımı veya verilerin silinmesi ve yok olması durumlarıyla karşı karşıya kalınabilecektir. Bu nedenle tüm yedeklerin fiziksel güvenliğinin de sağlandığından emin olunmalıdır.