BİLGİ GÜVENLİĞİ FARKINDALIK EĞİTİMİ

BİLGİ GÜVENLİĞİ

Bir varlık türü olarak bilginin izinsiz veya yetkisiz bir biçimde erişim, kullanım, değiştirilme, ifşa edilme, ortadan kaldırılma, el değiştirme ve hasar verilmesini önlemek olarak tanımlanır ve «gizlilik», «bütünlük» ve «erişilebilirlik» olarak isimlendirilen üç temel unsurdan meydana gelir.

Hangi bilgi bu kapsamdadır?

- Basılı halde kağıtlarda
- Telefon konuşmalarında
- Faks mesajlarında
- Masalarda, dolaplarda
- İletim hatlarında
- En önemlisi de kurum çalışanlarının zihinlerinde bulunur

SİBER GÜVENLİK

Manyetik ortamda bulunan ve iletişim halinde olan her bilginin güvenliği «Siber Güvenlik» kapsamında değerlendirilir.

Hangi bilgi bu kapsamdadır?

- Veri tabanındaki
- USB / CD'ler
- Kişisel bilgisayarlar
- Sunucular
- Cloud / Bulut çözümleri

Bilgi Güvenliğine Yönelik İç ve Dış Tehditler

- Bilgisiz ve bilinçsiz kullanım
- Eğitilmemiş personele sistemin önemli görevlerini yaptırmak
- İşten çıkarılan personelin kuruma ait şifre, mail gibi bilgileri bilmesi
- Bir saldırganın kuruma ait web sitesini ele geçirmesi
- Bir saldırganın kurumun korunan bilgilerini çalması
- Bir saldırganın kurumun web sitesini silmeye çalışması veya değiştirmesi
- Bir saldırganın kurumun veri tabanındaki bilgileri çalması

SOSYAL MÜHENDİSLİK SALDIRILARI

- Sosyal Mühendislik, insanlar arasındaki iletişimdeki ve insan davranışındaki modelleri açıklar olarak tanıyıp, bunlardan faydalanarak güvenlik süreçlerini atlatma yöntemine dayanan müdahalelere verilen isimdir.

- Kötü niyetli kişi, her konuşmada küçük bilgi parçaları elde etmeye çalışabilir. Konuşmalar daha çok arkadaş sohbeti şeklinde geçer. Bu konuşmalarda önemli kişilerin adları, önemli sunucu bilgisayarlar veya uygulamalar hakkında bilgiler elde edilir.

- Sosyal Mühendislik için en etkin yol telefon ve e-postadır. Telefon haricinde kuruma misafir olarak gelen kötü niyetli kişiler bilgisayarların klavye veya ekran kenarlarına yapıştırılan kullanıcı adı ve şifre kağıtlarını da alabilirler. Çöplerinize kurumsal bilgi içeren kağıtları atmayınız.

GÜVENLİK UZMANLARI TARAFINDAN ÖNERİLEN YÖNTEMLER

- Siber saldırılara karşı mevcutta var olan bütün sistemleri yazılımların güncel olması gerekir.
- Kurum içinde çalışan bütün personelin siber saldırılara karşı bilgi ve yeterlilik düzeyini arttırmak için gerekli eğitimleri almasını sağlayın. Kurum çalışanlarının siber saldırılara karşı bilinç düzeylerinin arttırılması gereklidir.
- Kurum içinde bilgi teknolojileri kısmında çalışan personelin sürekli sistemi denetlemesini sağlayın yapılan her değişiklikten sonra sistemde bir açık olup olmadığı test edilmeli, bu bağlamda bu işlemlerin bir ritüel haline getirilmesi gerekir.
- Geliştirilen tüm sistemleri sürekli denetim altında tutun. Herhangi bir saldırı anında neler yapılması gerektiği ile ilgili yapılması gereken görevleri önceden belirleyin.

- Kurumunuza olası bir saldırı olduğunu ve sistemlerinizin zarar gördüğünü varsayın. Müşterilerinize en kısa sürede geri dönüş yapabilmeniz için sisteminizi tekrar çalışır hale getirmek zorundasınız. Bunu da ancak müşterilerinizden aldığınız verilerin bir kopyasını aldığınız takdirde yapabilirsiniz. Tün verilerin mutlaka kopyasını alın ve bu kopya verileri başka bir alanda muhafaza edin.

- Kurum içinde çalışma yönteminizi gözden geçirin ve sisteminizin saldırılara karşı en zayıf olan yerlerini saptamaya çalışın. Kurum içinde ağ güvenliğini sağlayın.

- Kurumunuzda var olan cihazların yazılımları ve donanımları ile detaylı bilgileri kontrol edin. Temin ettiğiniz firmalar ile sürekli iletişim halinde olun ki cihaz ve yazılım üzerinde ne gibi değişikler yapıldığına dair bilgi sahibi olun ki güvenliğiniz ile alakalı geliştirilen algoritmalardan haberdar olmuş olursunuz.

- Kurum personelleriniz arasında veri güvenliği için mutlaka ayrı personeliniz olması gerekir. Bu personelleriniz verinin güvenliğinin sağlayabilmek için geliştirilen her uygulamadan sonra sistem üzerinde gerekli testleri yapacaktır.

- Sisteminize gelebilecek saldırılara karşı kendi personelinizin yanı sıra ayrı bir güvenlik şirketlerle de çalışabilirsiniz. Büyük saldırı anında size yardımcı olabilecek birilerinin var olması sizi rahatlatacaktır.

- Kurumunuzda bulunan tüm sistemler de yaptığınız işin büyüklüğüne göre karar verebileceğiniz anti virüs programları kullanın.

- Hem kurum içinde hem de uzaktan bağlantı yapmak zorunda kalan personellerinizin sisteme güvenli olan şifreli kanallardan haberleşmesini sağlayın.

Bilgi Güvenliği Politikası Ne İşe Yarar?

- Personele, yaptıkları iş kadar, iş yapış yöntemlerinin ve işledikleri bilginin değerini fark ettirir.
- Kurumu, bilgi kaybı nedeni ile uğrayacağı zarardan korur. Rekabetçi bir avantaj sağlar.
- Riskleri yönetilebilir kılar.
- Toplam kalitenin artmasına fayda sağlar.

KİŞİSEL VERİLERİN KORUNUMU KANUNU HAKKINDA BİLGİLENDİRME

- Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir.

- Kanunda belirtilen ; «Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.» ifadesi kişisel verilerin kullanımı, saklanması veya işlenmesi gibi konularda en temel ifadedir.

- KVKK kapsamında BDDK tarafından finansal sektörlerde hizmet veren kuruluşlar denetlenir. Kanunda belirtilen koşulların yerine getirilmemesi durumunda idari para cezası yaptırımları uygular. Bu cezalardan bazıları şöyledir; aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5.000 Türk lirasından 100.000 Türk lirasına kadar, veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar idari para cezası uygulanır.

- KVKK kapsamında Elekse Ödeme Kuruluşu olarak hem müşterilerimize hem de üye işyerlerimizi kişisel verilerin korunumu kanunu hakkında bilgilendirmek amaçlı dikkat edilmesi gerekenleri belirledik.

KVKK KAPSAMINDA MÜŞTERİLERİMİZE VE BAYİLERİMİZE ÖNERİLERİMİZ

- Kartınızla yapacağınız ödemelerde kart bilgilerinizi kurum çalışanlarımız dahil kimseyle paylaşmayınız.

- Elekse Ödeme Kuruluşu üzerinden yapacağız ödemelerde tek kullanımlık SMS şifresi telefonunuza gelmektedir. Elekse Ödeme Kuruluşu haricinde gelen SMS'leri dikkate almamanızı ve şüpheli durumlarda 0(212) 235 66 00 çağrı merkezimizden bizimle iletişime geçiniz.

- Elekse Ödeme Kuruluşu bayileri olarak müşterilerimizin ödemeleri sonrasında alınan fiş, makbuz gibi muhafaza edilmemesinden, üçüncü taraflara paylaşılmasından dolayı gerçekleşecek olan idari para cezası ödemeyi gerçekleştiren bayinin sorumluluğundadır.

- Elekse Ödeme Kuruluşuna ait bayilerde ödeme esnasında şüpheli durumlarla karşılaşılması halinde (Kart üzerinde ödemelerde ödemeyi gerçekleştiren şahıs ile kart üzerinde ismi yazılı şahsın aynı olmaması gibi) ödemeyi gerçekleştirenden kimlik göstermesi istenilmelidir.

- Elekse Ödeme Kuruluşu bayileri müşterilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel verilerini hiçbir şekilde müşterilerin onayı alınmadın, açık rızası olmadan kullanamaz, paylaşamaz ve işleyemez.

- Elekse Ödeme Kuruluşu bayileri müşterilerinin açık rızası olmadan müşterilerinin kişisel verilerini yurt dışına aktaramaz.

- Belirlenen şifrelerin tahmin edilemeyecek şekilde karmaşık olması, şifrelerin göz önündeki evraklarda bulundurulmaması gerekir.

TEŞEKKÜRLER

elekse®
ÖDEME KURULUŞU A.Ş.