Sahtekarlık ve Dolandırıcılık Önlemleri Eğitimi

Bilgi Güvenliği Sunumu

Temel Bilgi Güvenliği Eğitimi

Sunumun Amacı

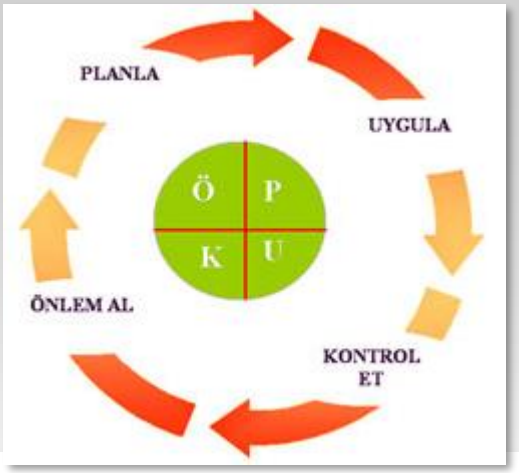
Bilgi güvenliği eğitiminin temel amacı şirketin, temsilcilerinin ve şirketin temsilcileri aracılığı ile oluşturduğu fatura ödeme organizasyonun maruz kalabileceği olumsuz etkileri kabul edilebilir bir seviyeye çekmektir.

Temel Bilgi Güvenliği Kavramları

Temel Kavramlar

... Ödeme Sistemleri Bilgi Güvenliği Yönetim Sistemi

... E-Para ve Ödeme Sistemleri bilgi güvenliğine yönelik çalışmalarını ISO 27001 standardının belirlemiş olduğu Bilgi Güvenliği Yönetim Sistemi ile gerçekleştirmektedir. Bilgi Güvenliği Yönetim Sistemi planla, uygula, kontrol et ve önlem al yaklaşımı ile kurgulanmıştır.



COBIT – Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri

BDDK - Ödeme Kuruluşlari ve Elektronik Para Kuruluşlarinin Bilgi Sistemlerinin Yönetimine ve Denetimine Ilişkin Tebliğ

Uluslararası Bilgi Güvenliği Standardı – ISO 27001

Temel Kavramlar

Bilgi ve Bilgi Varlıkları Ne Demek ?

Bilgi: Yazılı, basılı ya da dijital ortamda bulunan her türlü anlamlandırılmış veridir.

Bilgi Varlığı: Bilginin üretilmesinde, işlenmesinde, paylaşılmasında, saklanmasında, imha edilmesinde kullanılan her türlü varlık bilgi varlığıdır.

Temel Kavramlar

Bilginin Korunması Gereken Özellikleri

- **Gizlilik:** Bilginin yalnızca yetkili ve bilmesi gereken kişiler tarafından erişilebilir olması
- **Bütünlük:** Bilginin doğru ve tam olması
- **Erişilebilirlik:** Bilgiye ihtiyaç duyulan her an erişilebilmesi ve kullanıma hazır olması

Bilgi Güvenliği Tehditleri

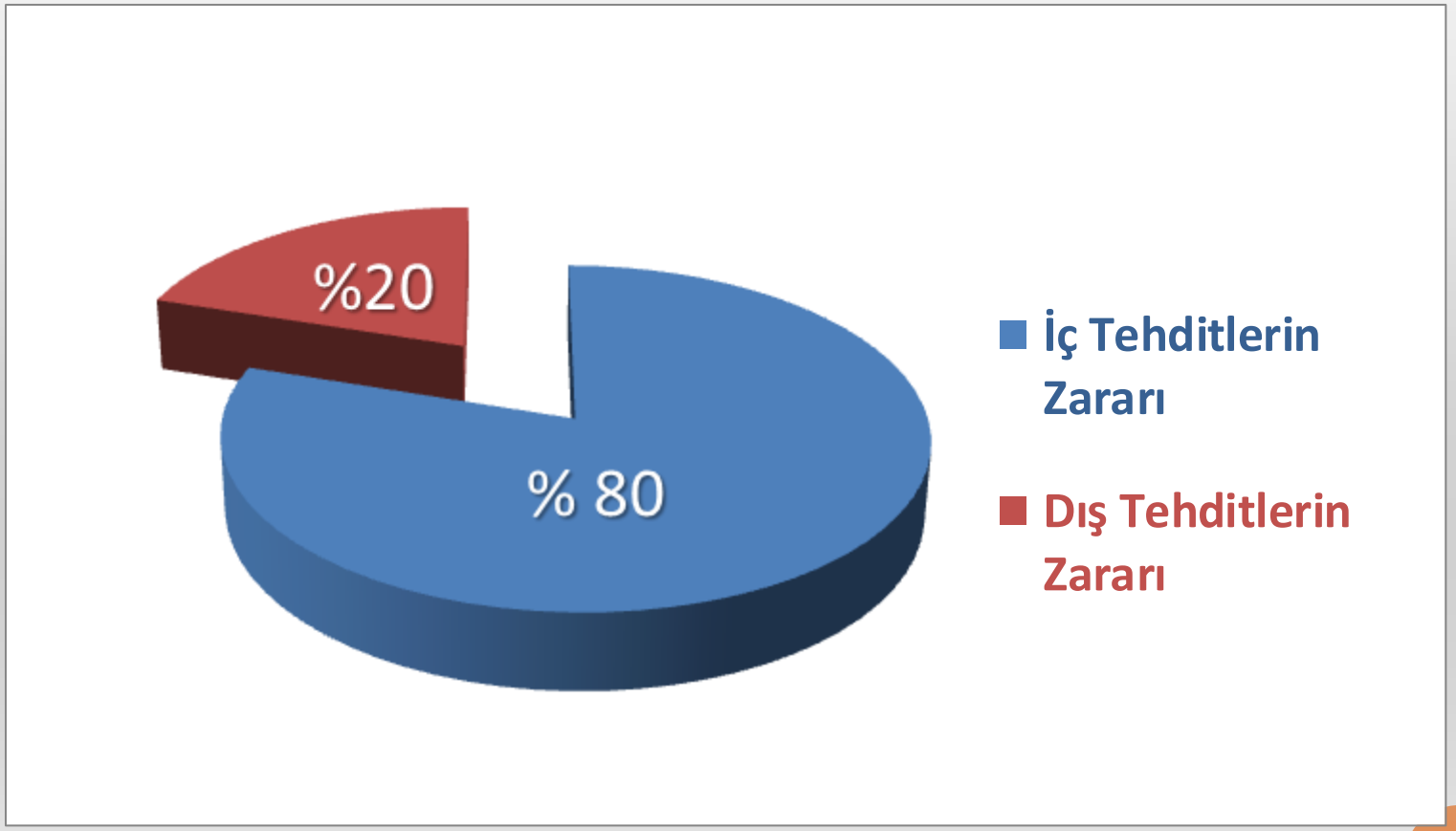
Bilgiye Yönelik Tehditler

İç Tehditler: Elekse Fatura Ödeme Kuruluşu A.Ş nin iş süreçlerinden, kullanılan uygulamalar ve donanımlardan, çalışanlardan kaynaklanan tehditlerdir. Örneğin; yetkisiz işlemler, uygulama ve donanım hataları, farkındalık eksiklikleri…

Dış Tehditler: Firma'nın dışından gelen çevresel tehditlerdir. Örneğin; hırsızlıklar, saldırılar, virüs saldırıları, siber saldırılar…

Doğal ve Fiziksel Tehditler: Deprem, sel, yangın, terör amaçlı saldırılar vb tehditlerdir.

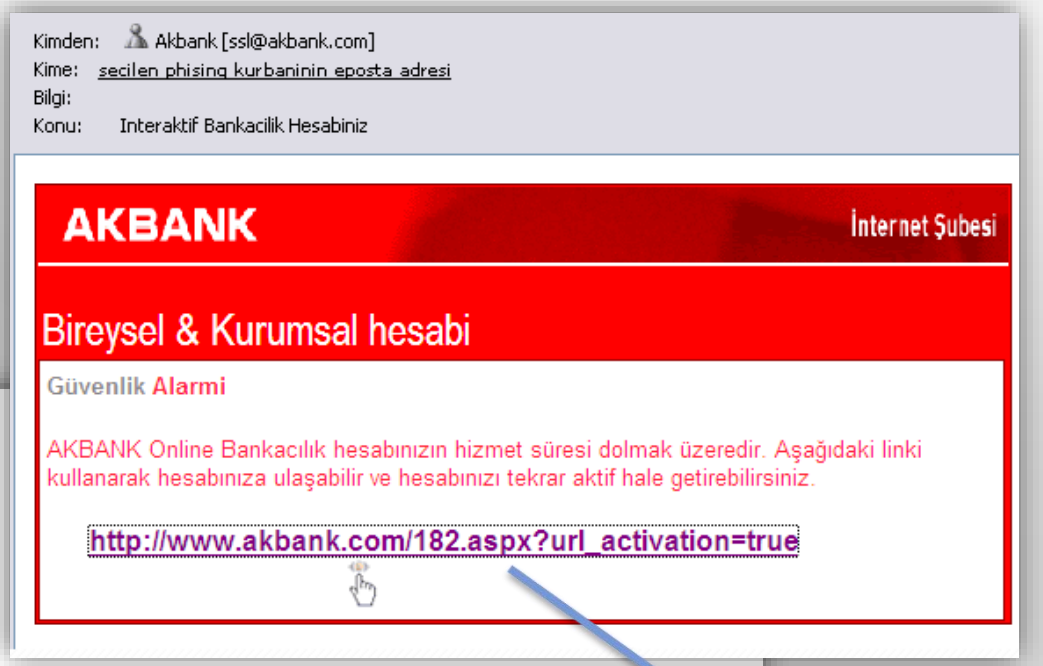
İç ve dış tehditlerin kurumlara verdiği zararların oranları



Sık Rastlanan Bilgi Güvenliği Tehditleri

E-posta Yolu ile Yemleme (Phishing) Saldırıları

Kurumsal tasarımlar kopyalanarak müşteriye aldatıcı içerikte mesajların gönderilmesi ve hesap bilgilerinin ele geçirilmesine yönelik saldırılardır.



Adreste Akbank gözüküyor fakat adres tıklandığında tuzak siteye gidiyor.

E-posta Yolu ile Yemleme (Phishing) Saldırıları

Phishing (Yemleme) nasıl yapılır?

Genellikle bir kurumsal web sitesinin sahte bir kopyası oluşturulur. Kurum çalışanları ya da müşterileri, gönderilen kötü niyetli fakat güvenli bir görünüme sahip e-posta ile sahte web sitesine yönlendirilir. Sahte web sitesi aracılığıyla, kullanıcıların gizli verileri göndermesi ya da bilgisayarlarına zararlı bir yazılımı indirmesi amaçlanır.

Phishing (Yemleme)'den korunmak için nelere dikkat edilmelidir?

- Kullanıcı adı ve parolaları, Firma hesap bilgileri, kart bilgileri gibi gizli bilgiler e-posta ile gönderilmemelidir.
- Kaynağından emin olunmayan e-postalardaki linklere tıklamaktan kaçınılmalıdır.
- E-postaların içine yerleştirilmiş formlar doldurulmamalıdır.
- Web tarayıcıda açılan pop-up ekranlara kişisel bilgiler girilmemelidir.
- Ziyaret edilen sayfaların güvenliğinden emin olmak için internet adresinde "**https://**" ifadesinin yer almasına dikkat edilmelidir.

Türk Ceza Kanununda Bilgi Güvenliği

Madde 135

(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.

(2) Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır.

Madde 136

(1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır.

Madde 137

(1) Yukarıdaki maddelerde tanımlanan suçların;

a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle,

b) **Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle,** İşlenmesi halinde, verilecek ceza yarı oranında artırılır.

Temsilcilerin Karşılaşabileceği Durumlar

Temel Bilgi Güvenliği Eğitimi

Fatura ödeme faaliyeti esnasında temsilcilerin karşılaşabileceği dolandırıcılık ve sahtekarlık işlemleri;

1) Müşteriden alınan paranın sahte para olması

1) Müşteriden alınan paranın sahte olması

- Paranın sahte olduğu nasıl anlaşılır ?

•Dokunma:

Banknotlarda bulunan kimi yazı ve rakam grupları ile motifler parmakla dokunulduğunda kabartma hissi verir.

•Bakma:

Banknotlarda ışığa tutulduğunda her iki yüzden de görülebilen Atatürk portresi ve kupür değerini ortaya koyan rakamdan teşekkül eden filigran ile emniyet şeridi ve bütünleşik görüntü bulunmaktadır.

•Açılı Bakma:

Banknotların ön yüzünde yatay konumda göz hizasında ışığa doğru tutulduğunda görülebilen gizli görüntü ile ayrı açılardan bakıldığında holografik şerit folyo, arka yüzde ise renk değiştiren şerit yer almaktadır.

Temel Bilgi Güvenliği Eğitimi

- Cihaz Yardımıyla Bakma:

  Banknotların kimi özellikleri büyüteç ve ultraviyole ışık veren cihazların yardımı ile görülebilmektedir. En kesin çözüm olarak temsilcilerimize önermekteyiz.

1) Müşteriden alınan paranın sahte olması

Para Sahteyse Neler Yapılır ?

Eğer paranın sahte olduğu anlaşılırsa, kesinlikle ilgili faturanın ödenmesi temsilci tarafından yapılmamalıdır. Şirketimizin şikayet ve itiraz birim müdürü uyum görevlisi olarak şirketimiz tarafından atanmıştır. Temsilci personeli şikayet ve itiraz birim müdürüne konuyla ilgili bilgi vermelidir.

Temsilci tarafından verilen bilgiler ışığında, şirketimiz uyum görevlisi aksiyon uygulamakla yetkilidir.

Temsilcilerde ve Şirketimizde Bilgi Güvenliği

Temiz Masa Temiz Ekran Politi

- Gizli veri içeren, yetkisiz kişilerin eline geçmesi halinde Firmanın zarara uğramasına neden olabilecek nitelikteki her türlü basılı doküman ve bilgi depolayıcı veya taşıyıcı cihazlar masalar üzerinde bırakılmamalı, bu dokümanlarla ilgili çalışmanın tamamlanmasının ardından en kısa sürede
- kilitli dolap veya çekmecelere kaldırılmalıdır.
  Masa üstündeki alanlara yapıştırılan dokümanların gizli bilgi içermemesine
- dikkat edilmelidir.
  Çalışanlar yerlerinden ayrılacağı zaman bilgisayar ekranı kilitlenmeli veya oturumu kapatılmalıdır. Şifreler ve kullanıcı hesap bilgileri masa üzerinde
- yazılı olarak bulundurmamalıdır.
  Bilgisayar ekranları yetkisiz kişilerin ekranları izlemesine izin vermeyecek şekilde konumlandırılmalıdır.

Önemli Kurallar

Dikkat Edilmesi Gerekenler

- Parolalar hiç kimse ile paylaşılmamalıdır.
- Kullanıcı bilgileri ile başkasına işlem yaptırılmamalıdır.
- Toplantı odası vb. ortamlarda bulunan yazı tahtalarında, bilgiler yazılı olarak bırakılmamalı, kullanıldıktan sonra silinmelidir.
- Kapı giriş kartları başkalarına kullandırılmamalıdır.
- Güvenliğinden emin olunamayan ve şüphe duyulan internet siteleri ziyaret edilmemeli bu sitelerden dosya indirilmemelidir.
- Bilgi işlem cihazları üzerinde verilenler haricinde değişiklikler yapılmamalıdır.
- Bilgi güvenliğini tehlikeye atan beklenmedik durumlarla karşılaşıldığında Bilgi Güvenliği yetkilileri bilgilendirilmelidir.
- Firma çalışanlarının eriştiği Genel Ortak alanda sadece “Düşük” ve “Orta” gizlilik seviyesindeki dokümanlar paylaşılabilir. “Düşük” ve “Orta” gizlilik seviyesi dışındaki dokümanlar Genel Ortak alanda paylaşılmamalıdır.
- Kurum e-posta sistemi üzerinden, kişisel kullanım amacıyla (dosyaların yedeklenmesi, evde çalışma vb.) kişisel e-posta adreslerine kurum dosyası gönderimleri yapılmaz.

Çalışanların Sorumlulukla

- Yayınlanmış olan Bilgi Güvenliği politika ve prosedürlerine uygun hareket eder,
- Bilgi Güvenliği farkındalığını artırmak amacıyla gerçekleştirilen eğitim vb. faaliyetlere katılır,
- Bilgi Güvenliği olaylarını Bilgi Güvenliği Olay Yönetim süreci ile bildirir,
- Bilgi Güvenliği Yönetim Sistemi'nin iyileştirilmesi için Bilgi Güvenliği Yetkilisine geri bildirimde bulunur.

Bunları Biliyor musunuz?

- Sadece harflerden oluşan 6 haneli bir parolanın hackerlar tarafından kırılması için gereken süre **1 saniyedir**.
- Harf ve rakam karışımından oluşan 6 haneli bir parolanın hackerlar tarafından kırılması için gereken süre **1 saniyedir**.
- Büyük, küçük harf, rakam ve noktalama işaretlerinden oluşan 6 haneli bir parolanın hacker'lar tarafından kırılması için gereken süre **52 saniyedir**.
- Kırılması saniyeler süren ve dünyada en sık kullanılan parolalar şunlardır: 12345, 123456, abc123, qwerty, 654321, password

Hackerların işlerini zorlaştırmaya var mısınız?

Parolalar

Güçlü Parolaların Özellikleri

- Akılda kalıcı ve hatırlanması kolaydır
- Harf, rakam, noktalama işareti kombinasyonlarını içerir
- Uzundur
- Eski parolalara benzemez

Güçlü Parola Örnekleri

- Mavi Gökyüzü → Mav!G”k100
- Küçük Kızım → k”c”kK1z1m

Parolalar

Zayıf Parolaların Özellikleri

- Akılda kalmayan parolalar
- Ünlülerin, akrabaların, aile fertlerinin isimlerinden oluşan parolalar
- Doğum yeri doğum tarihinden oluşan parolalar
- Harf yada rakam dizileri, QWERTY, 123456, 1Q2W3E

Temel Bilgi Güvenliği Eğitimi

Bilgi Güvenliği Olay Bildirimlerinizi Olay Yönetim Aracı üzerinden kayıt açarak yapabilirsiniz.

Öneri ve katkılarınızı Bilgi Güvenliği Ekibi ile paylaşabilirsiniz. Ancak birlikte başarabiliriz…

Teşekkürler…