Kurumlarda Bilgi Güvenliği Farkındalığı Önemi ve Oluşturma Yöntemleri

AB Seminer 2009

BANK ASYA

Ender ŞAHİNASLAN

Arzu Kantürk Önder Şahinaslan Emin Borandağ

Eğitimci [Ender Şahinaslan]

2007 – Devam	BANK ASYA - Bilgi Güvenliği – Müdür Yardımcısı
2005 – 2007	BANK ASYA Organizasyon, Kalite ve Sistem Geliştirme Müdürlüğü – II.Müdür
2004 - 2005	BANK ASYA - Yazılım Geliştirme Müdürlüğü – Sistem Analist
2000 - 2004	SABANCI ÜNİVERSİTESİ – Bilgi Teknolojileri - Uygulama Sorumlusu
1999 - 2000	MALTEPE ÜNİVERSİTESİ – Bilgisayar Mühendisliği – Öğretim Görevlisi
1997 - 1999	GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ – Bilgisayar Mühendisliği – Arş.Grv.
1995 - 1996	GAZİ ÜNİVERSİTESİ – Fen Bilimleri Enstitüsü – Araştırma Görevlisi

- **Doktora,** Trakya Üniversitesi – Bilgisayar Mühendisliği – 2008 - Devam
- **Yüksek Lisans,** Gebze Yüksek Teknoloji Enstitüsü – Bilgisayar Mühendisliği – 1998
- **Lisans,** Trakya Üniversitesi – Bilgisayar Mühendisliği – 1995

Gündem

- Temel Bilgi Kavramları
- Bilginin Nitelikleri, Güvenliği ve Tehditler
- BG'de **İnsan Faktörü** ve Farkındalık
- Farkındalık Sınaması – **Temiz Ekran**
- **Farkındalık Oluşturma Yöntemleri**
- Temel Bir BG Farkındalık Eğitiminde …
- **Sonuç - Özet**

Bilgi

Bilgi, bir kurumun önemli değerlerinden biridir ve sürekli korunması gerekir.

ISO 17799:1999

Bilginin Bulunduğu Ortamlar..

" **Bilgi**, bilgi bir çok formlarda bulunabilir-iletilebilir.

Kağıda basılabilir, elektronik olarak depolanabilir, posta veya elektronik yollar ile gönderilebilir, filmler üzerinde gösterilebilir, **sözlü-iletişim yoluyla**.

Bilgi hangi şekilde olursa olsun, her zaman uygun olarak korunmalıdır."

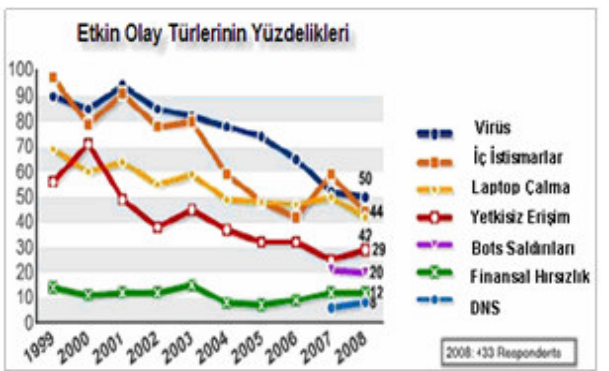
ISO 17799-1:2000

Bilginin Korunacak Nitelikleri

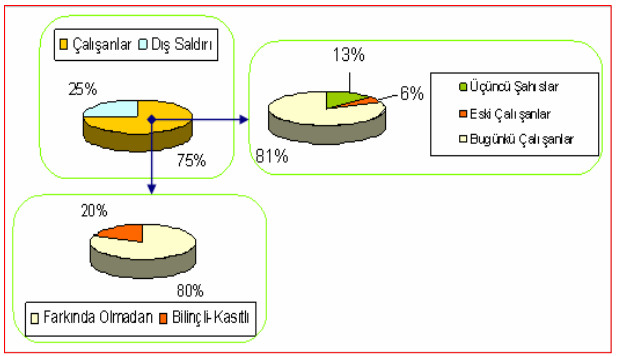
- Gizlilik
  - Bilginin yetkili olmayan kişiler, varlıklar ve süreçler tarafından erişilemez ve ifşa edilemez özelliği
- Doğruluk Bütünlük Özgünlük
  - Bilginin doğruluk, bütünlük ve kendine haz özgünlüğünün korunması
- Kullanılabilirlik
  - Bilginin yetkili kişiler tarafından istenildiğinde ulaşılabilir ve kullanılabilir olma özelliği

Bilgi Güvenliği ve Tehditler

Etkin Bilgi Güvenlik Olay Yüzdeleri



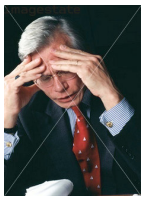
İnsan Faktörü – BG Suçların Dağılımı



İnsan Faktörü

%50

%50



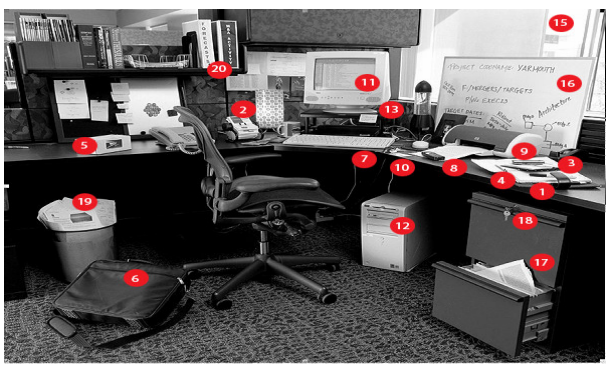
Güvenlikte Teknoloji Faktörü

- 1990'lı yılların sonu ve 2000'in başından itibaren insan faktörü çok fazla önem kazanmıştır.
- Bu durumun **daha artacağı** beklenmektedir.

Temiz Masa! Burada bir yanlışlık var mı?

Temiz Masa!

Sadece Dağınıklık Değil Bilgi Güvenliği Farkındalık Eksikliği ...



Farkındalık Oluşturmanın Ana Yolu

Kurumlarda en üst seviyedeki yönetimden en alt seviyedeki çalışana (hatta tedarikçilere, müşterilere) kadar ilgili gruplar dikkate alınarak **ihtiyaç ve beklentilere göre** farklı eğitim ve farkındalık programları hazırlanarak vermekten geçmektedir.

Farkındalık Oluşturma Yöntemleri

- **Farkındalık eğitimleri** (internet tabanlı interaktif sanal, **sınıf içi eğitimler**),
- Çalışanlara yönelik masaüstü bilgi güvenliği (**el kitabı**) kitapçığı ve **renkli broşürler**, **posterler**,
- Düzenli bilgi güvenlik etkinlikleri, sunular,
- **Animasyonlar**, Film gösterileri, **Tiyatro**
- Bilgi güvenliği **e-posta bülteni**

Farkındalık Oluşturma Yöntemleri

- Ekran koruyucu **mesajlar**, **karikatürler**,
- BG mesajlarını iletmek için **farklı küpler**,
- interaktif **BG oyunları** hazırlanması
- **Güvenliği hatırlatan sisteme giriş mesajları**, **mousepad**, **anahtarlık**, **logo/sloganlar**, **takılar**..
- Çalışanların güvenlik hassasiyetleri **değerlendirilip ödüllendirme**
- Ödüllü **bulmacalar**,**oyun turnuvaları**, **yap bozlar** ..

BG Farkındalık Eğitiminde;

- Eğitimi alacak **gruplara özgü** temel bilgilendirme,
- Bilgi güvenliği **tehdit ve kontrolleri**,
- **Fiziksel güvenlik**,
- **Kötü niyetli yazılımlar**,
- **Şifre kullanımı ve şifre güvenliği**,
- **Yasal düzenlemeler**,
- **Kurum BG politikası**nın ilgili grubu ilgilendiren **çalışan sorumlulukları** üzerine hatırlatmalar(özet),

gibi temel konular örnekleriyle ele alınarak katılımcılara "**farkındalık**" oluşturmak amaçlanır.

Sonuç-Özet

- **Güvenlik kuralları:** bilgiyi korumak amacıyla, çalışan davranışları için yön gösterici bir rehberdir ve **güvenlik tehditlerini bertaraf edebilmek içinde etkili kontrol geliştirilmesinin temel yapı taşıdır.**
- **Etkili güvenlik önlemleri** ise iyi düzenlenmiş kurallar ve süreçlerle **çalışanları eğitmekle mümkün** olacaktır. Bu da ancak **etkili bir çerçevede hazırlanmış farkındalık programları** ile gerçekleştirilebilir.

Sonuç-Özet

- **Bilgi güvenliğinin temini için** sistem üzerinde sadece **teknik açıdan önlem almakla yetinilmemelidir**. Güvenliğin en zayıf unsuru sayılan insan faktörün de dikkate alınması ve **komple bir bütünlük içerisinde farkındalık oluşturulmalıdır**.
- **İnsana/çalışana güvenin esas eğitim ve kontrolün şart** olduğu unutulmamalı.

SORULAR & CEVAPLAR

TEŞEKKÜRLER

BANK ASYA

1997