



Bilgi Güvenliği Farkındalık Eğitim Örneği AB Seminer 2009



Ender ŞAHİNASLAN



Dr. Rembiye KANDEMİR

Önder ŞAHİNASLAN

Ender ŞAHİNASLAN

11-13 Şubat 2009

Gündem

- 00:00 – 00:05 Tanışma / Takdim
- 00:05 – 00:08 Temel Bilgi Kavramları
- 00:08 – 00:20 Bilgi Nereelerde Bulunur?
- 00:20 – 00:25 Temiz Masa
- 00:25 – 00:32 Bilginin Korunacak Nitelikleri
- 00:32 – 00:40 Bilgi Güvenliği ve Tehditler
- 00:40 – 00:43 Saldırıların Yönü
- 00:43 – 00:46 İnsan Faktörü
- 00:46 – 00:50 Şifre Güvenliği
- 00:50 – 00:53 Yasal Düzenlemeler
- 00:53 – 00:57 Temel bir BG Farkındalık Eğitiminde ...
- 00:57 – 01:00 Soru-Cevap



2

Ender ŞAHİNASLAN

11-13 Şubat 2009

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

3

Ender ŞAHİNASLAN

11-13 Şubat 2009

Veri / Bilgi Nedir?

Veri(Data), sayısal veya mantıksal her değer bir veridir.

Veri denildiğinde akla önce sayılar mı geliyor? Doğal olarak Finans sektöründe çalışıyoruz 📊. Oysa sözcükler, sesler, görüntüler de veri olabilir. Bu çerçevede veriyi, “**Karar vermeye yarayan soyut simge dizileri**” olarak tanımlamak daha uygun olacaktır.

Bilgi(Information), verinin işlenmiş, anlamlı hale gelmiş şekline bilgi denir.

4

Ender ŞAHİNASLAN

11-13 Şubat 2009

Bilginin Değeri

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

ISO 17799:1999

5

Ender ŞAHİNASLAN

11-13 Şubat 2009

ISO-Bilgi Güvenliği Standardı Der ki :

“ **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

6

Ender ŞAHİNASLAN

11-13 Şubat 2009

Bilgi Nerelerde Bulunur?

➤ Fiziksel Ortamlarda

- Kağıt, Tahta, Pano, Yazıcı, Fax, Çöp/Kağıt Kutusu, Dolaplar vb.

➤ Elektronik Ortamlarda

- Bilgisayarlar, Mobil İletişim cihazları, E-posta, USB, CD vb Manyetik ortamlar

➤ Sosyal Ortamlar

- Yemek araları, Telefon görüşmeleri, Muhabbetler vb sosyal aktivitelerde

➤ Tanıtım Ortamları

- Web siteleri, broşürler, reklamlar, sunularımız, eğitimler, video vb.

7

Ender ŞAHİNASLAN

11-13 Şubat 2009

Temiz Masa! Burada bir yanlışlık var mı?



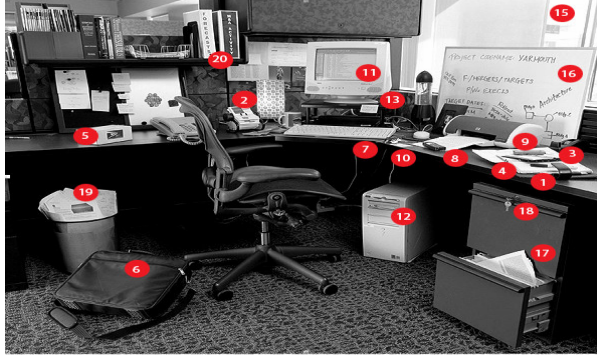
8

Ender ŞAHİNASLAN

11-13 Şubat 2009

Temiz Masa!

Sadece Dağınıklık Değil Bilgi Güvenliği Farkındalık Eksikliği ...



9

Ender ŞAHİNASLAN

11-13 Şubat 2009

Bilginin Korunması

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

ISO 17799:1999

10

Ender ŞAHİNASLAN

11-13 Şubat 2009

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

11

Ender ŞAHİNASLAN

11-13 Şubat 2009

Bilgi Güvenliği ve Tehditler

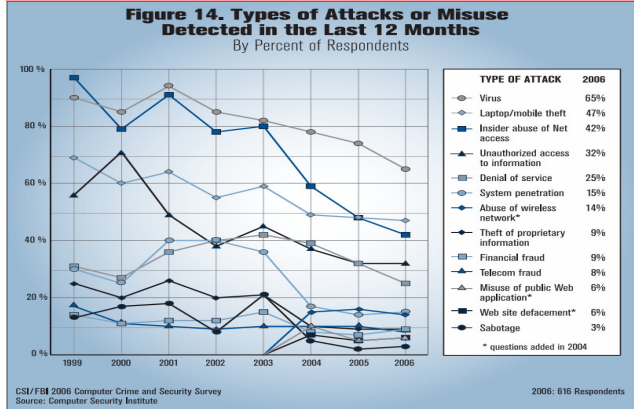


12

Ender ŞAHİNASLAN

11-13 Şubat 2009

Saldırıların Yönü!



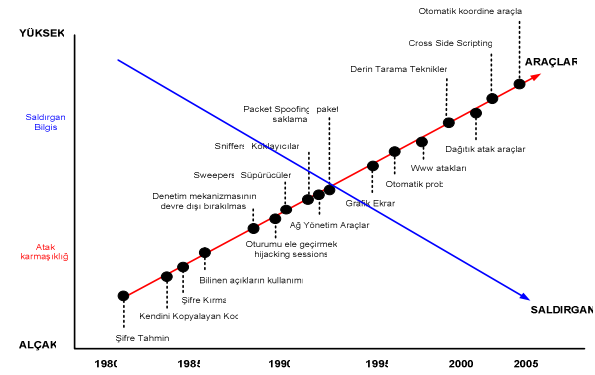
Kaynak:CS/FBI 2006

Ender ŞAHİNASLAN

11-13 Şubat 2009

13

Saldırgan Bilgisi & Saldırıların Yönü!



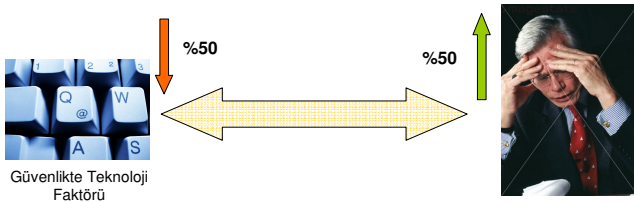
Kaynak: CERT 2006

Ender ŞAHİNASLAN

11-13 Şubat 2009

14

İnsan Faktörü



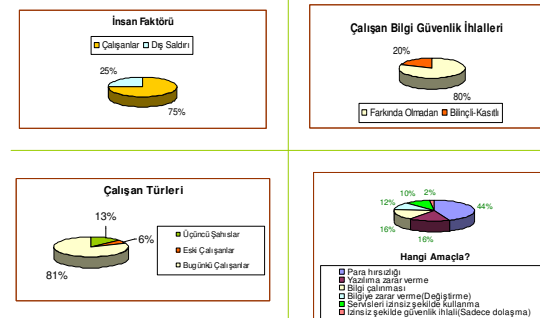
- 1990'lı yılların sonu ve 2000'in başından itibaren insan faktörü çok fazla önem kazanmıştır.
- Bu durumun **daha artacağı** beklenmektedir.

Ender ŞAHİNASLAN

11-13 Şubat 2009

15

İnsan Faktörü – BG Suçların Dağılımı



Ender ŞAHİNASLAN

11-13 Şubat 2009

16

Şifre Güvenliğini Sağlamak

- ❖ Şifrele kullanıcılar tarafından, **tahmin edilmesi ve bulunması zor olan**, kullanıcı hakkında **bilgileri içermeyen şifreler** seçilmelidir.
- ❖ Şifreler **kağıt üzerine yazılmamalı**, kayıt amaçlı saklanması gerekiyorsa şifrenin bulunduğu belge güvenliği sağlanmış sadece yetkili kişilerin erişebilecekleri bir ortamda saklanmalıdır;
- ❖ En temel kullanıcı sorumluluğu yetkisiz kullanıcı erişiminin engellenmesidir. Kullanıcılar, **kişisel şifrelerini gizli tutmalı** ve çalışma grubu şifrelerini sadece grup üyeleri kullanmalıdır;
- ❖ Şifreler **paylaşılmalı** veya otomatik sistem girişleri sırasında **kaydedilmemelidir**;
- ❖ Şifreler en fazla üç ayda düzenli olarak değiştirilmeli.
- ❖ **Şifre güvenliği tehlikeye düştüğü durumlarda** şifre kullanıcı tarafından derhal **değiştirilmelidir**;

17

Ender ŞAHİNASLAN

11-13 Şubat 2009

Yasal Düzenlemeler

- 1951 tarih ve 5846 sayılı **Fikir ve Sanat Hakları Kanunu**,
- 2004 tarih ve 5237 sayılı **Bilişim Suçları Kanunu**; Her türlü Bilgi teknolojisi kullanılarak yapılan **kanun ve ahlak dışı** tüm eylemler.
- Kurumların bağlı olduğu düzenleyici kurumların (**BDDK, YÖK, Bakanlıklar, Sayıştay vb**) getirdiği yükümlülükler.
- **5651** sayılı 'İnternet üzerinden yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun'

18

Ender ŞAHİNASLAN

11-13 Şubat 2009

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 politikasının ilgili grubu ilgilendiren **çalışan sorumlulukları** üzerine hatırlatmalar(özet),

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

19

Ender ŞAHİNASLAN

11-13 Şubat 2009



SORULAR & CEVAPLAR TEŞEKKÜRLER

