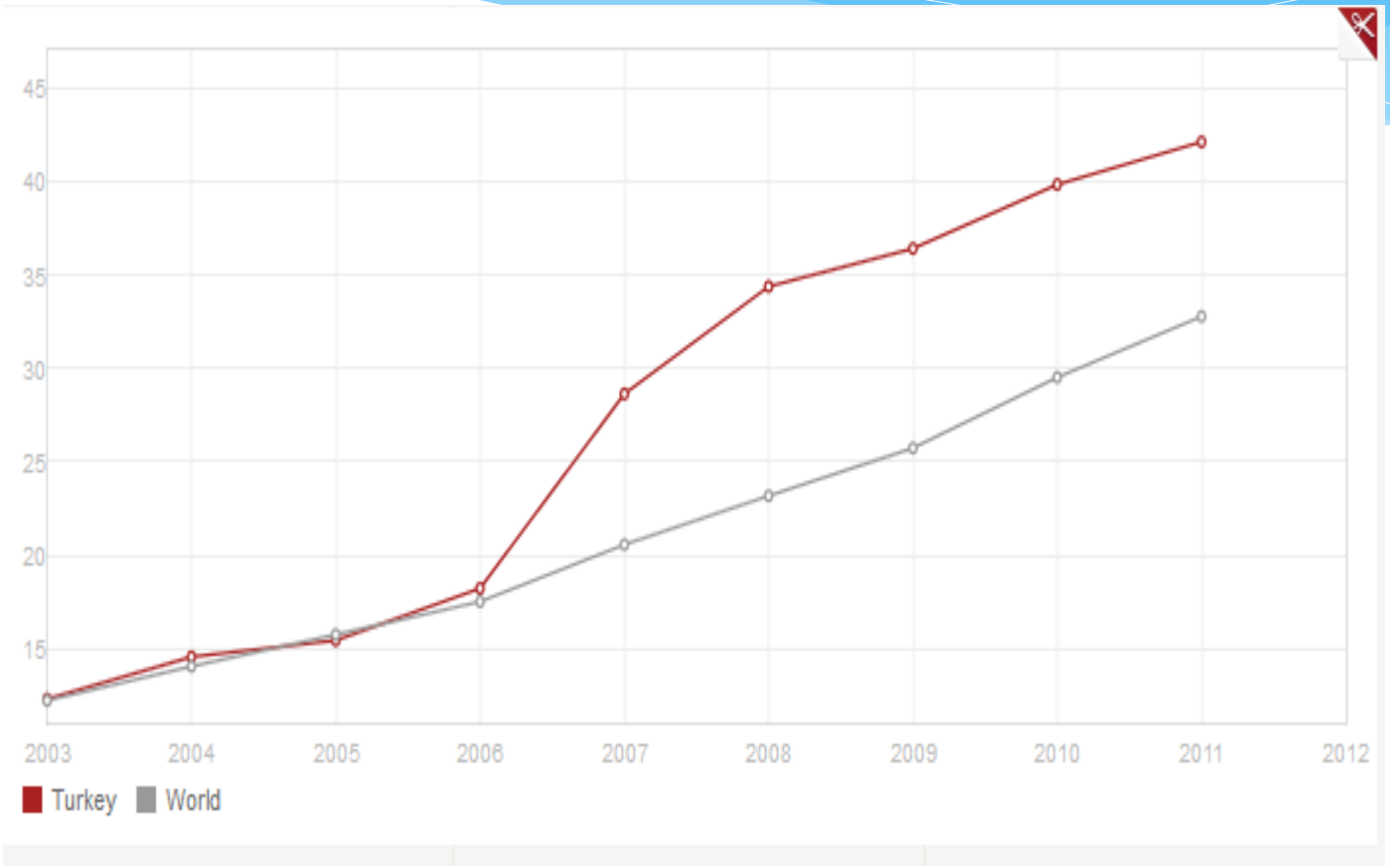
BİLGİ GÜVENLİĞİ

İnternet Kullanımı



Bilgi Güvenliği Kavramı

- Bilişim ürünleri/cihazları ile bu cihazlarda işlenmekte olan verilerin gizliliğini, bütünlüğünü ve sürekliliğini korumayı amaçlayan çalışma alanıdır.

Dahili Tehdit Unsurları

- Bilgisiz ve Bilinçsiz Kullanım
  - Temizlik görevlisinin sunucunun fişini çekmesi
  - Eğitilmemiş çalışanın veri tabanını silmesi
- Kötü Niyetli Hareketler
  - İşten çıkarılan çalışanın, kuruma ait Web sitesini değiştirmesi
  - Bir çalışanının, ağda sniffer çalıştırarak e-postaları okuması
  - Bir yöneticinin, geliştirilen yeni bir ürünün bilgilerini rakip firmalara satması

Harici Tehdit Unsurları

Hedefe Yönelmiş Saldırılar

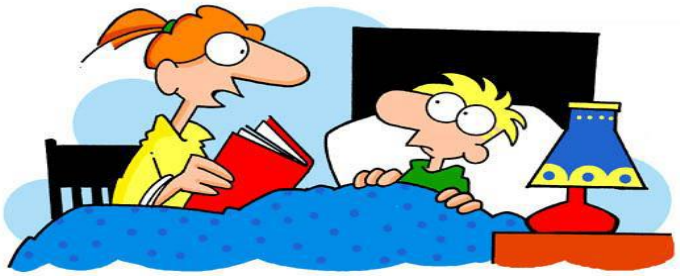
- Bir saldırganın kurumun web sitesini değiştirmesi
- Bir saldırganın kurumun korunan bilgisini çalması
- Birçok saldırganın kurum web sunucusunu servis dışı bırakma saldırısı yapması

Geleceğin Hackerleri

- Bilgisayar kullanım yaşı düştü, geleceğin hackerleri hacker okullarında (Internet Kafelerde) yetişiyor.

BT'nin Kötüye Kullanımı Sonucu Oluşan Zararlar

- Bilginiz başkalarının eline geçebilir
- Kurumun toplumdaki imajı zarar görebilir (en kötü durum)
- Donanım, yazılım, veri ve kurum çalışanları zarar görebilir
- Önemli veriye zamanında erişememek
- Parasal kayıplar
- Vakit kayıpları



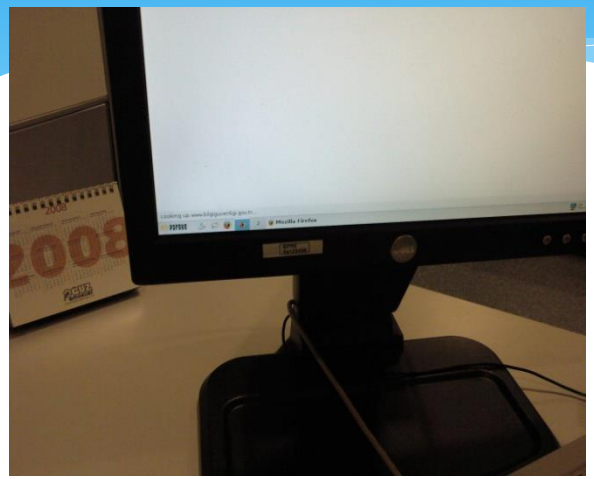
Romeo ve Juliet bir chat odasında buluşmuşlar ama beraberlikleri trajik bir sonla noktalanmış.

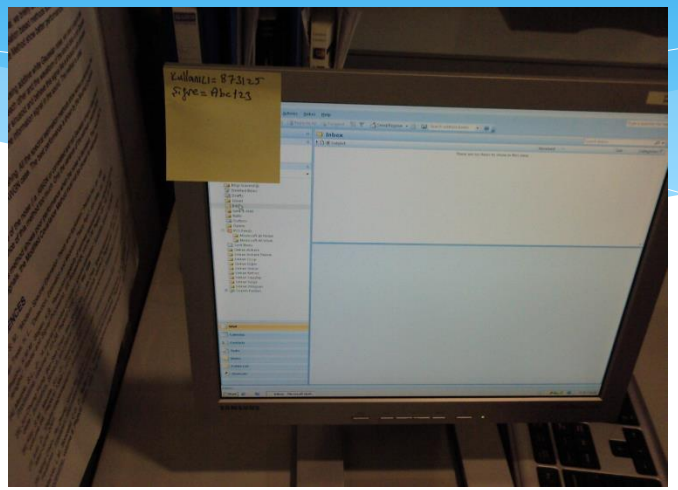
Kullanıcı Bilincinin Önemi

- Bilgi güvenliğinin en önemli parçası kullanıcı güvenlik bilincidir.
- Oluşan güvenlik açıklıklarının büyük kısmı kullanıcı hatasından kaynaklanmaktadır.
- Saldırganlar (Hacker) çoğunlukla kullanıcı hatalarını kullanmaktadır.

- Bir kullanıcının güvenlik ihlali tüm sistemi etkileyebilir
- Teknik önlemler kullanıcı hatalarını önlemede yetersiz kalmaktadır
- Kullanıcılar tarafından dikkat edilmesi gereken kurallar sistemlerin güvenliğinin sağlanmasında kritik bir öneme sahiptir.

Şifreler Güvenli Muhafaza Edilmeli





Şifre Güvenliği- 1

- En önemli kişisel bilgi şifrenizdir
- Hiç kimseyle herhangi bir şekilde paylaşılmamalıdır
- Mümkünse bir yere yazılmamalıdır. Yazılması gerekiyorsa güvenli bir yerde muhafaza edilmelidir
- Güvenli olmadığını düşündüğünüz mekanlarda kurumsal şifrelerinizi kullanmanızı gerektirecek uygulamaları kullanmayınız

Şifre Güvenliği-2

- En az sekiz karakterli olmalıdır.
- Rakam ve özel karakterler (?, !, @ vs) içermelidir.
- Büyük ve küçük harf karakteri kullanılmalıdır.
- Kişisel bilgilerle ilişkili olmamalıdır (doğum tarihi, öğrenci numaranız, vb.)
- Örnek: Güçlü bir şifre: Ag6486kt!

Kötü Şifre Örnekleri

- 12345
- abcdef
- 1978
- 11111
- 13579
- aaaaa
- bbbbbbb
- 123123 …

- deniz
- deniz1998
- Deniz123

Yazılım Yükleme- Güncelleme

- Kurum tarafından belirlenmiş yazılımların dışında bilgisayarlarda program bulunmamalıdır. Her bir programın açıklık oluşturma ihtimali vardır.
- Güvenilir olmayan sitelerden yazılımlar indirilmemeli ve kullanılmamalıdır

* Bir USB bellek, 1 milyon adet kağıtta yer alan bilgi kadar veri içerebilir.

Dizüstü Bilgisayar Kullanımı

- Çalınmalara karşı fiziksel güvenlik sağlanmalıdır.
- Şifre güvenliği sağlanmış olmalıdır.
- İçinde kurumsal veri olmamalıdır.
- Eğer veri şifreleme sistemi kurumda kullanılıyor ise gizli bilgiler şifrelenmelidir.

Zararlı Programlar- Virüsler

- Tüm bilgisayarlarda virüs koruma programı çalıştırılmalı ve güncellemesi yapılmalıdır.
- Anti virüs programı kapatılmamalıdır.
- Dosyalar virüs taramasından geçirilmelidir.

E-posta Güvenliği

- Virüslerin en fazla yayıldığı ortam e-postalardır.
- Kaynağı tanınmayan e-postalar kesinlikle açılmamalıdır.
- Güvenilmeyen eklentiler açılmamalıdır.
- Gizli bilgi şifrelenmedikçe e-postalarla gönderilmemelidir.
- Spam e-postalara cevap verilmemelidir.
- E-posta adres bilgisi güvenilir kaynaklara verilmelidir.

TEŞEKKÜRLER