KURUMSAL BİLGİ GÜVENLİĞİ

Prof.Dr. Şeref SAĞIROĞLU
Gazi Üniversitesi
Mühendislik Fakültesi
Bilgisayar Mühendisliği Bölümü
Maltepe/Ankara

SS@gazi.edu.tr
http://w3.gazi.edu.tr/~ss

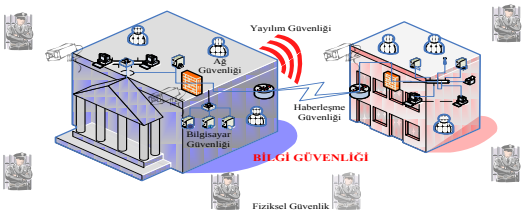
Bilgi Güvenliği

Bilgiye sürekli olarak erişilebilirliğin sağlandığı bir ortamda,

- bilginin göndericisinden alıcısına kadar gizlilik içerisinde,
- bozulmadan,
- değişikliğe uğramadan ve
- başkaları tarafından ele geçirilmeden
- bütünlüğünün sağlanması ve
- güvenli bir şekilde iletilmesi süreci

Bilgi güvenliğini sağlama unsurları

Bilgi Güvenliği



Bilgi güvenliğini sağlama unsurları

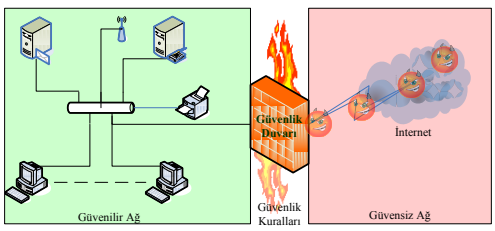
Güvenliğin Sınıflandırılması

- Fiziksel Güvenlik: Çit, kameralar, duvarlar, özel güvenlik görevlileri, şifreli oda girişleri vb.
- Haberleşme Güvenliği: Steganografi
- Yayılım Güvenliği: TEMPEST
- Bilgisayar Güvenliği: Güvenli Bilgisayar Sistemi Değerlendirme Kriterleri (TCSEC-Trusted Computer System Evaluation Criteria)
- Ağ Güvenliği: Kablolu, Kablosuz Ağlar, GD, IDS, IPS
- Bilgi Güvenliği : Kriptografi

Güvenlik duvarı yapılandırmasına bir örnek

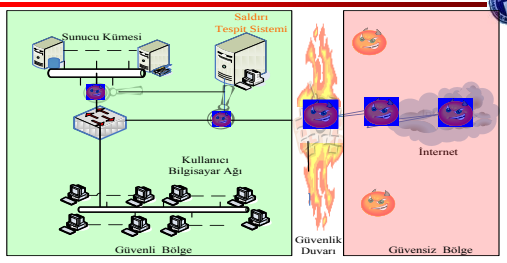
Saldırı tespit sistemine bir örnek

Güvenliğin Sınıflandırılması



Güvenlik duvarı yapılandırmasına bir örnek

Güvenliğin Sınıflandırılması



Saldırı tespit sistemine bir örnek

Bilgi Güvenliği Tehditleri

- Doğal afetler ve teknik arızalarla ilgili tehditler
  - Deprem, yangın, su baskını, sel, ani sıcaklık değişimleri, toprak kayması, kasırgalar, fırtınalar ve çığ düşmesi,yazılım veya donanım arızaları,Havalandırma sistemi arızaları
- Prosedürel eksiklere dayalı tehditler
  - İdari Prosedür Eksiklikleri
    - Personel işe alma ve işe son vermede güvenlik prosedürlerinin olmaması
    - Güvenlikle ilgili görev ve sorumlulukların verilmesinde eksiklikler
  - Teknik Prosedür Eksiklikleri
    - Bilgi yedekleme prosedürlerinin olmaması
    - Bilgi envanterinin tutulmaması ve güncelliğini sağlayacak mekanizmanın olmaması
    - Ağ hizmetleri (e-posta, internet, dosya paylaşımı, vb.) kullanım prosedürlerinin olmaması

Bilgi Güvenliği Tehditleri

- İnsan faktöründen kaynaklanan tehditler
  - İstem dışı olarak yapılan davranışlar
  - Bilinçli olarak yapılan davranışlar
- Kötücül Yazılımlar
  - Virüsler, Solucanlar,
  - Truva Atları,
  - Casus Yazılım
  - Arka Kapılar,
  - Mantıksal Bombalar,
  - Sazan Avlama

- Kişisel güvenlik
- Sertifikalandırma, Akreditasyon, ve Güvenlik Tespitleri
- Giriş Kontrol Mekanizmaları
- Tanıma ve Yetkilendirme Mekanizmaları (Biometrics, tokens, passwords)
- Denetim Mekanizmaları
- Şifreleme mekanizmaları
- Güvenlik duvarları ve ağ güvenlik mekanizmaları
- Saldırı tespit sistemleri
- Risk analizi
- Güvenlik Planlama
- Güvenlik politikaları ve prosedürleri
- Olay karşı koyma planlama
- Güvenlik bilinci ve eğitim
- Fiziksel güvenlik
- Güvenlik Konfigürasyon Kurulumları
- Anti-viral yazılımlar
- Akıllı kartlar

Bilgisayar Güvenliği Farkındalığı?

... Erişilen ve saklanan veriler ile bilgisayar sistemlerinin korunması.

Masaüstü PC	Kurumsal Bilgiler
Dizüstü	Sınırlı Bilgiler
Sunucular	Kişisel bilgiler
El Bilgisayarları	Arşivler
Taşınabilir bellekler	Veri tabanları

Kişisel olarak neden bilgisayar güvenliğini almak zorundayız?

Bu bir BİT problemi değil mi?

Herkes sorumlu..
Bilgisayarını ve bilgisini korumak zorunda..

İyi bir güvenlik için pratik olarak "90/10" Kuralı

- Güvenlik koruma sistemleri (10% teknik)
- kullanıcılara veya sistem yöneticilerine bağlı (90% diğer)

Güvenliği zayıflatan unsurlar?

- Sürekli kendini ve hizmet aldığı birime suç bulmak
- Kaybolan verileri tekrar elde ederim düşüncesi
- Kimlik hırsızlıkları
- Verilerin bozulması veya kaybolması
- Sabırsızlık, İşveren ve herkese güven
- Rahatsızlıklar
- Zafiyetler
- Farkındalık eksikliği
- …

"Korumada Top 10 Kural"

Bilgisayar Güvenliği Uygulamaları

"Kural 1"

Gizli bilgileri taşınabilir ortamlarda bulundurma..

- Kayıp olabilir.
- Çalınabilir.
- Düşürülebilir.
- Kopyası kolaylıkla çıkarılabilir.
- Zarar görebilir.
- ….

"Kural 2"

Verini Yedekle..

- Düzenli bir plan çerçevesinde veriyi yedekle. İdeali günde bir kez…
- Yedeklemeyi silinebilir ortamlarda tut taşınabilir HD, CD, ve DVD sürücüleri veya USB bellek.
- Yedekleme ünitelerinizi güvenli ortamlarda tutunuz. PC'den farklı bir ortamda tutmanız önerilir..

"Kural 2"

Verini Yedekle..

- Eposta adresleriniz, yazdıklarınız, çizdikleriniz, hazırladığınız tablolar, kayıp olursa ne kadar verimli olabilirsiniz?
- Bu kadar veriyi tekrar geri elde etmek ne kadar zaman alır?
- …

"Kural 3"

- Şifrelerini koru..
- Şifrelerini belirli sürelerde değiştir.
- Kolaylıkla tahmin edilmeyen şifreler kullan..
- Şehitler Ölmez Vatan Bölünmez! ŞeÖlVaBö!
- Şifrelerinizi görünebilir bir yere yazm
- Hiçbir kimseyle paylaşma..
- ..

"Kural 4"

- Anti-viral çözümler
  - anti-virüs,
  - anti-casus,
  - anti-spam,
- Güvenlik duvarı,
- Güncel yamalar kullan..

"Kural 5"

- Bilmediğiniz yazılım kullanmayınız.
- Lisansız yazılım kullanmayınız.
- ...

"Kural 6"

- Güvenli E-posta kullanınız.
- Bilmediğiniz dosyaları açmayınız, yönlendirmeyiniz
- Şüpheli e-postalara cevap vermeyiniz.
- E-posta eklerini açmayınız.
- E-postalarda gelen web adreslerine tıklamayınız.
- Spamları siliniz.
- GüPosta, SAYcrypt, ..
- Kendiniz geliştiriniz..
- Kişisel bilgilerinizi UCSF'in güvenli posta sistemini kullanarak gönderiniz.
- Subject: Secure:_ (http://its.ucsf.edu/information/applications/exchange/secure_email.jsp)

"Test 1"

"Bilgi Güvenliği" başlıklı bir mesaj aldınız ve mesajın ekini açmanız isteniliyor..

Ne yapardınız?

a) Açılım adımlarını takip ederdim.
b) Ekini açardım.
c) Mesaja cevap verir ve "beni listeden çıkarın" mesajı atardım.
d) Mesajı silerdim.
e) BİM'e başvururdum.

"Test 2"

"Ders Hocanız" size bir screensaver gönderdi..

Ne yapardınız?

a) Mesajı ve ekini sevdiğim arkadaşlarıma gönderirim.
b) Eki bilgisayarıma indirir ve kurardım.
c) Mesaja cevap verir "bilgisayarıma yüklediğimi belirtir ve kendisine teşekkür mesajı" atardım.
d) Mesajı silerdim.
e) Bilen bir arkadaş nezaretinde bilgisayarıma yükletirdim.

"Kural 7"

Güvenli internet kullanımı için

- İnternet ortamında erişilen herhangi bir web sitesinden erişilen bilgisayarın adı ve yerine ulaşılabilmektedir.
- Şüpheli veya soru işareti olabilecek sitelere erişme; spam, virüs ve casus yazılımın bilgisayarınıza indirilmesini sağlayabilir.
- Bilinmeyen programları bilgisayara indirme
- Lisansız yazılımları kullanmaya hefeslenme

"Kural 8 ve 9"

Kullanım alanını ve verilerini fiziksel olarak koru

- Dosyalarını ve taşınabilir cihazlarını koru, Örn: memory sticks.
- Laptoplarınızı kilitli ortamlarda ve kilitlenebilir şekilde koruyunuz.
- ID'lerinizi, giriş şifrelerinizi, kartlarınızı, veya anahtar gibi kullanılan cihazlarınızı hiçbir kimseyle paylaşmayınız.

"Kural 10"

Ekran koruyucu kullanınız..

- For a PC ~
  - <ctrl> <alt> <delete> <enter> OR
  - <⊞> <L>
- For a MAC ~
  - Ekran koruyucuya şifre koyunuz.
  - Ekran koruyucuyu çalıştırmak için bir kısayol oluşturunuz.
- Bilgisayarın açılışına veya uyanması esnasında şifre koyunuz.

"Test 3"

İş istasyonu güvenlik araçlarından hangisi devam etmek ve/veya korunmak için gereklidir?

a) Kullanıcı ID
b) Şifre
c) Log-off programları
d) Ofis veya çalışma ortamının kilitlenmesi (kapılar, pencereler)
e) Hepsi

"Test 4"

Bilgisayar ekranınızda fare kendi kendine hareket etmeye ve masaüstünüzde bazı uygulamalara kiliklemektedir. Ne yapardınız?

a) Arkadaşlarıma veya hocalarıma gösterirdim.
b) Bilgisayar internet kablo bağlantısını çekerdim.
c) Fareni bağlantısını çıkarırdım.
d) BİM e bildirirdim.
e) Bilgisayarı kapatırım.
f) anti-virüs yazılımı aktif hale getirir tarama yaparım.
g) Hepsi

"Test 5"

Saldırgan bilgisayarınıza eriştiğinde ne yapabilir?

a) Büyük miktarda istenilmeyen trafik oluştururlar ve sistemi yavaşlatırlar.
b) Atak yapılan programları saklar.
c) Bilgisayarınızdan illegal olarak yazılım ve dokümanları dağıtırlar.
d) Gizli bilgilere erişebilirler (örn: kimlik hırsızlığı)
e) Tuş basım bilgilerinizin tamamını alabilirler.
f) Tuş basım bilgilerinden Şifreleri elde edebilirler.
g) Ekran görüntülerini saklayabilirler.
h) Erişilen web adreslerini elde edebilirler.

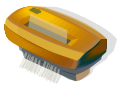
"Test 6"

Aşağıdakilerden hangisi gizli bilgilerdir?

- Ad ve soyad
- Sağlık karnesi bilgileri
- Emeklilik sandığı, SSK bilgileri, Kurum Kimlik bilgileri
- Etnik bilgiler
- Doğum tarihi
- Kredi kart bilgileri, Banka hesap no
- Tez adı
- Öğrenci numarası, Enstitü no,
- Ev adresi,Tel no,..
- Derslerden aldığı notlar..

"Gizli Bilgilerin Yönetimi ve Korunması"

- Verilerin nerede saklı olduğunun bilinmesi
- İhtiyaç duyulmayan bilgileri yok ediniz.
  - atmadan önce yok ediniz.
  - gerekirse fiziksel olarak ta yok ediniz.
- Tutulan gizli bilgileri koru
  - Belirli aralıklarla yedekleme al.

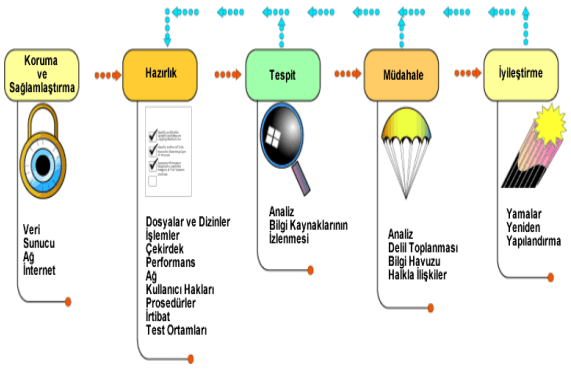


NE YAPILMALI ?

- Bilgi üretmeli.
- Bilgiye önem verilmeli ve korumayı bilmeli,
- Bilginin geleceğimizin anahtarı olduğu unutulmamalı
- Ulusal stratejiler geliştirilmeli,
- Üniversitelerde eğitimler verilmeli,
- Bu konuda ar-ge çalışmaları yapılmalı,
- E-imzayı kullanmalıyız..

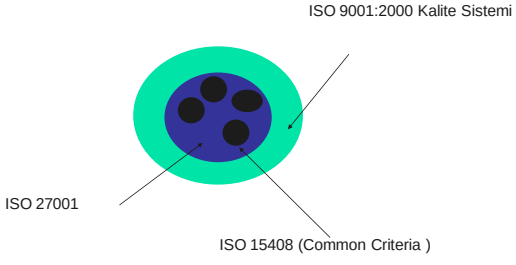
NELER YAPILMALI ?

- Çalışmayan bir sistem hiçbir zaman güvenli olamaz.
- Gerçekçi yaklaşım kendine güvendir.
- Gereği kadar koruma yapılmalıdır.
- **%100 güvenlik olmadığı her zaman hatırda tutulmalıdır.**



CERT/CC Güvenlik Yaşam Döngüsü

Büyük KBG Bakış Modeli?



SORU-CEVAP
KATKILAR