# Kurumsal Bilgi Güvenliği Yönetim Süreci

## BİLGİ YÖNETİMİ SEMİNERİ

Prof. Dr. Türksel KAYA BENSGHİR
TODAİE

23 Kasım, 2011

**Prof. Dr. Türksel KAYA BENSGHİR**

**TODAİE eDevlet Merkez Müdürü**

**tkaya@todaie.gov.tr**

**tbensghir@gmail.com**

**0-312-231 73 60/1803**

**0-312-2304285**

# Ele Alınacak Konular

- **Giriş**
- **Siber Güvenlik Kavramları**
- **Ulusal Güvenlik Kavramı**
- **Kurumsal Bilgi Güvenliği ve Yönetimi**
  - **Bilgi Sistemleri Güvenliği Nedir?**
  - **Bilgi Güvenliği Tehdit Unsurları**
  - **Bilgi Güvenliği Sağlama Araçları**
- **Bilgi Güvenliği Yönetim Sistemi (BGYS)**
- **Tartışma**

# Giriş

- Günümüzde bilgiye sürekli erişimi sağlamak ve bu bilginin son kullanıcıya kadar bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden güvenli bir şekilde sunulması zorunluluk haline gelmiştir.
- Siber dünyada barış ve savaş durumunun zaman ve mekan sınırları belirsizleşmiştir.

# GİRİŞ

- Başta A.B.D, Rusya, Çin, İsrail ve Almanya olmak üzere birçok ülke, bilgi savaşlarında kullanılacak silahlar için araştırma-geliştirme faaliyetleri başlatmışlardır.

# Uluslararası bilgi savaşlarında kullanılan yöntemlere örnekler

- **Echelon**
- **SORM** (Rusya),
- **Franchelon** (Fransa)
- **Carnivore**: (E-Postalar İçin Echelon)
- **PGP** (Pretty Good Privacy)

# Echelon

- Soğuk savaş döneminde ABD-İngiltere istihbarat İttifakı tarafından yürürlüğe konulan ECHELON sisteminin temel amacı, SSCB Birliği ve Doğu Blok diplomatik- askeri takip edilmesi.
- Dünyadaki iletişim trafiğinin çoğu eş zamanlı sözcük filitreleriyle izlenmektedir.

# Carnivore

- ABD'de adli Mercilerin izni ile, internet üzerinde gerçekleşebilecek suçları izlemek üzere internet servis sağlayıcısına bağlanarak takibe alınan kişilerin e-posta ve ICQ mesajları takibe alınmaktadır.

# PGP

- Açık anahtarlı kriptografinin özelliklerinden yararlanarak kişlerin e-posta mesajlarının bütünlüğünü, gizliliğini ve mesajın kimin tarafından gönderildiğini teyit eden bir uygulama yazılımıdır.

# Uluslararası bilgi savaşlarında kullanılan yöntemlere örnekler

- **PROMIS** (Prosecutor's Management Information System) PROMIS olgusu, ulusal ya da açık kod yazılımların önemini en çok vurgulayan örneklerden birisidir.
- ABD Adalet Bakanlığına bağlı savcı büroları veritabanlarını birleştirmek amacı ile Inslaw şirketi tarafından 1970'lerin sonunda geliştirilmiştir.
- Girdiği bütün veritabanlarını bir dosya içine toplamasıyla türünün ilk örneği.

# *Bilgi Savaşı Kavramı*

- Politik ve askeri hedefleri desteklemek üzere,

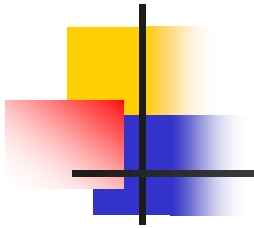
  barış, kriz ve savaş dönemlerinde hasımın sahip olduğu bilgi altyapısı, sistem ve süreçlerinin işlevselliğini engellemek, imha etmek, bozmak ve çıkar sağlamak amacıyla yapılan hareketler ile; düşmanın bu faaliyetlere karşı önlem alarak aldığı benzeri tedbirler ve hareketler bütünüdür.

# Siber–Bilgi Güvenlik Temel Konular-1

- **Güvenlik**
  - AJAX/Web 2.0/Javascript Güvenliği
  - Java & .NET Güvenliği
  - Mobil Cihaz Güvenliği
  - Bilgisayar Güvenliği
  - Mobil İletişim Güvenliği
  - İşletim Sistemi Güvenliği
  - Ağ Güvenliği
  - Algılayıcı Ağ Güvenliği
  - Web Güvenliği
  - E-posta Güvenliği
  - Veritabanı Güvenliği
  - E-ticaret Protokollerinde Güvenlik
  - IPv6 Güvenliği

# Siber–Bilgi Güvenlik Temel Konular-1

- **Gizlilik**
  - Temelleri
  - Geliştirme Teknolojileri
  - Koruma Programlama
  - Politika ve Yasaları
- **Doğal Felaketler/Acil Servisler/Siber terörizm koruma**
- **Risk Analizi, Modelleme ve Yönetimi**
- **Güven**
  - Biçimlendirme ve Modelleme
  - Yönetimi-değerlendirme



# Kurumsal Düzeyde Bilgi Güvenliği

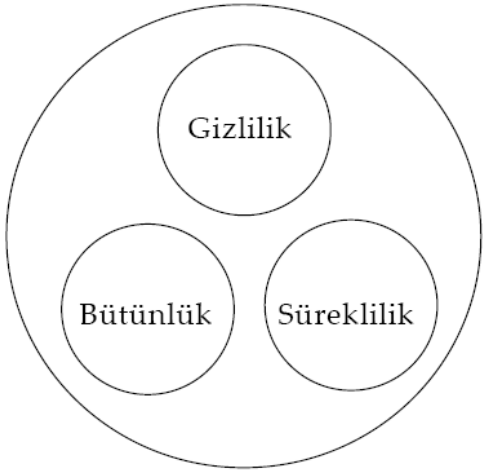
Prof. Dr. Türksel KAYA BENSGHIR-
TODAİE

# Bilgi güvenliği (BG)

- En genel tanımıyla bilginin, üretim ve hizmet sürekliliği sağlamak, parasal kayıpları en aza indirmek üzere tehlike ve tehdit alanlarından korunmasıdır.

# Bilgi Güvenliğinin Temel Amacı;

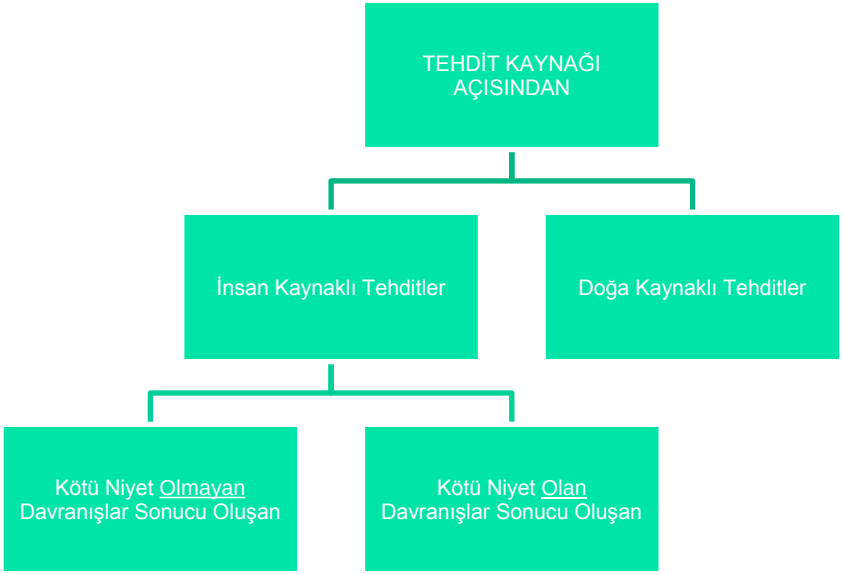
- Veri bütünlüğünün korunması,
- Yetkisiz erişimin engellenmesi,
- Mahremiyet ve gizliliğin korunması
- Sistemin devamlılığının sağlanmasıdır.

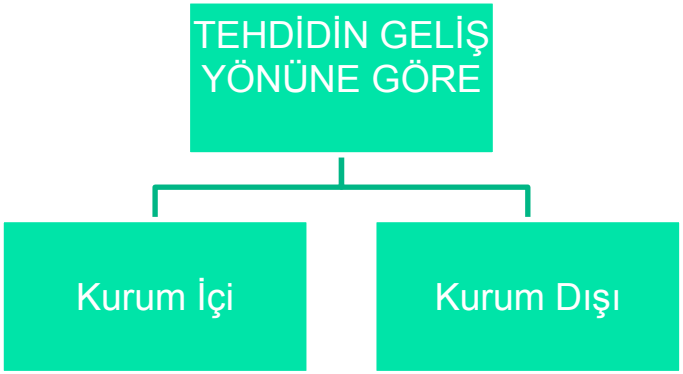


# *Tehdit*

Bir sistemin veya kurumun zarar görmesine neden olan istenmeyen bir olayın arkasındaki gizli neden, olarak tanımlanabilir.

# TEHDİTLER




*Sistemi neye karşı korumalıyım?"*

Prof. Dr. Türksel KAYA BENSGHIR-
TODAİE

# Hedefler

- Yazılım
- Donanım
- Veri
- Depolama Ortamları
- Bilgi Aktarım Ortamları
- İnsanlar

# En Kolay Giriş Prensibi

- Herhangi bir saldırgan, bir bilgisayar sistemine girmek için kullanılabilecek en kolay yolu deneyecektir.

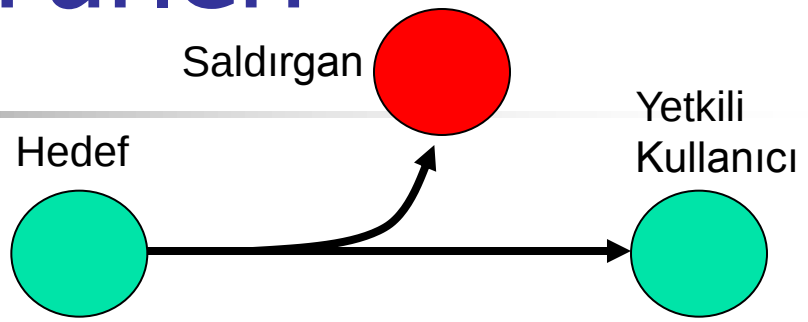
- En kolay yol demek, en belirgin, en çok beklenen, veya saldırılara karşı en çok önlemi alınmış olan yol demek değildir.

# Siber Saldırı Türleri

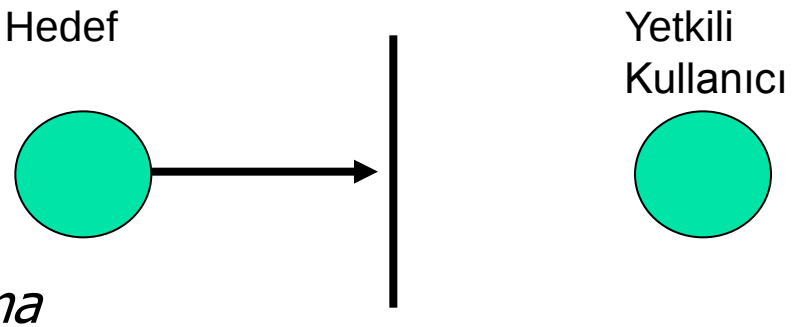
- Program manüplasyonu,
- Sahtekarlık ve taklit,
- Erişim araçlarının çalınması,
- Kimlik çalma,
- Ticari bilgi çalma,
- İstihbarat amaçlı faaliyetler,
- Takip ve gözetleme,
- "Hack" leme,
- Virüsler, Kurtçuklar (worms), Truva atları (Slammer, MsBlaster, Sobig),
- Ajan yazılım (spyware),
- Spam
- Hizmeti durduran saldırılar

# Saldırı Türleri

- İzinsiz Erişim
  - *Kopyalanma*
  - *Dinlenme*

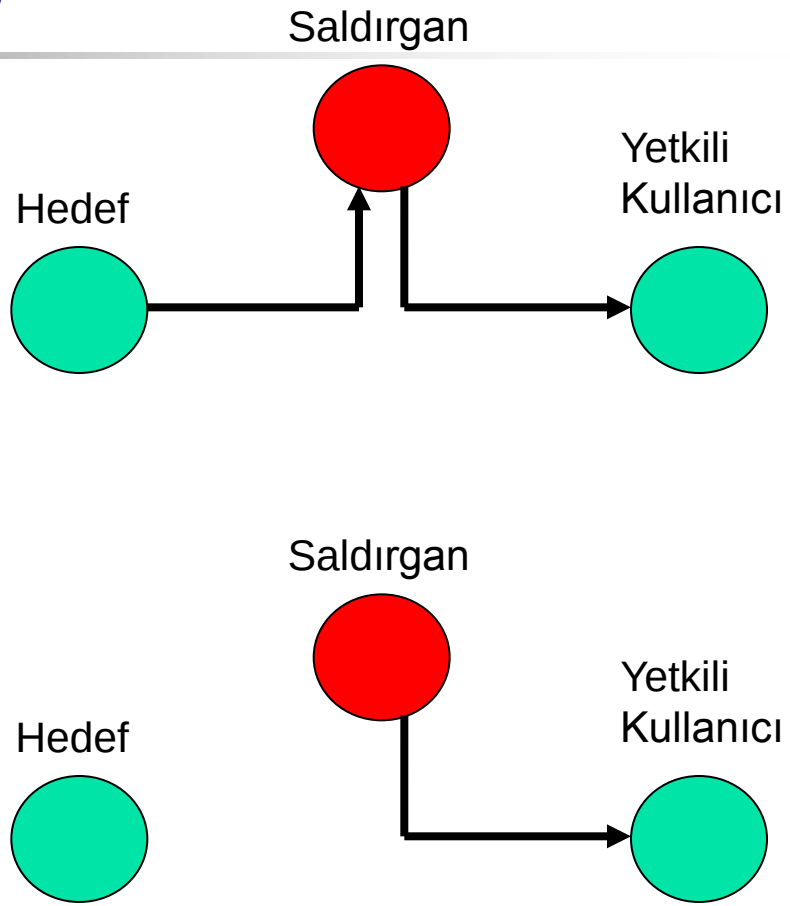



- Zarar Verme (Engelleme)
  - *Kaybolma*
  - *Ulaşılamaz durumda olma*
  - *Kullanılamaz durumda olma*



# Saldırı Türleri /2

- Değişiklik Yapma
  - Program kodları
  - Durgun Veri
  - Aktarılan Veri
- Üretim
  - Veri taklidi
  - Veri ekleme



# Siber saldırıları yolları-1

- Tarama (Scanning) sisteme değişken bilgiler göndererek sisteme giriş için uygun isim ve parolaları bulmak için kullanılır.
- Sırtlama (Piggybacking), yetkili kullanıcı boşluklarından ve hatalarından yararlanarak sisteme girmektir.
- Dinleme (Eavesdropping), iletişim hatlarına saplama yapmaktır.
- Casusluk (Spying), önemli bilginin çalınmasına yönelik aktivitelerdir.
- Yerine geçme (Masquerading), yetkisiz bir kullanıcının yetkili kullanıcı haklarını kullanarak sisteme girmek istemesidir.

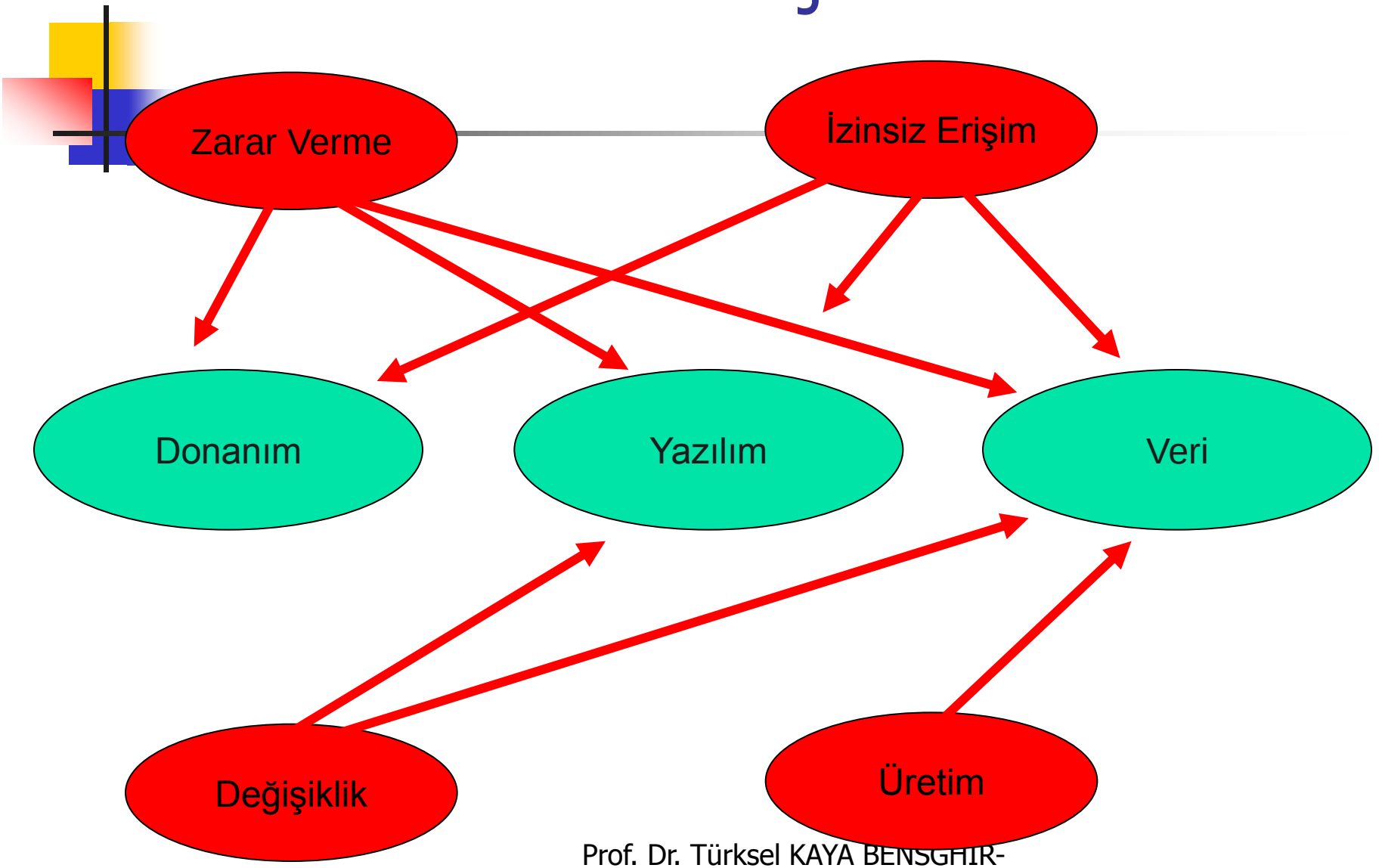
# Siber saldırıları yolları-2

- Çöpleme (Scavenging), gerçekleştirilen işlem sonucu kalan kullanılabilir bilgilerin toplanmasıdır.
- Arkaya takılma (Tailgating), dial-up bağlantı düşmelerinden veya işlemin tamamlanmasından sonra hattı elinde bulundurarak sisteme girmektir.
- Süperzap yöntemi (Superzapping), sistem programının gücünden yararlanarak işlem yapmaktır.
- Truva atı (Trojan Horse),dışarıdan cazibesine kapılarak indirilen veya sisteme kopyalanan programlardır.
- Virüsler, kendi başına çalışamayan, ancak başka programlar aracılığı ile çalışıp kendini taşıyan programlardır.
- Kapanlar (Trap doors), tasarımcıların ve geliştiricilerin sistem bakımında yararlanmak üzere bıraktıkları programlardır. Kötü amaçla kullanılabilirler.

# Siber saldırıları yolları-3

- Kurtçuklar (worms), kendi kendini çalıştırabilen ve kopyalayabilen bir programdır.
- Mantık Bombaları (Logic bomb), önceden belirlenmiş koşullar gerçekleşince harekete geçen programlardır.
- Salami teknikleri (Salami Techniques), dikkati çekmeyecek büyüklükte sistem kaynağı veya kaynakların zimmete geçirilmesi.
- Koklama (Sniffing), ağ üzerindeki paketlerin izlenmesi.
- Aldatma (Spoofing), ağa saplama yapılarak bilgilerin değiştirilmesi adres değişikliği yapılması.
- Kırmak (Cracking), sistem güvenlik önlemlerinin kırılması

# Güvenlik Açıkları



# Güvenlik Açıkları (Donanım)

- Kasıtsız Zarar
  - Yiyecek-içecek
  - Hayvanlar
  - Toz
  - Yıldırım
  - Kaba kullanım
- Kasıtlı Zarar
  - Hırsızlık
  - Fiziksel zararlar (kırma, bozma, parçalama)

# Güvenlik Açıkları (Yazılım)

- Silinme
  - Kasıtsız
  - Kasıtlı
- Değiştirilme
  - Truva Atları
  - Virüsler
  - Arka kapılar
  - Bilgi sızdırma
- Hırsızlık
  - Lisanssız kullanım
  - İzinsiz kopyalama

# Güvenlik Açıkları (Veri)

- Gizliliğin ihlali
  - Dinleme (dinleyiciler, alıcılar, sniffer)
  - Bilgi sızdırma (insanlar yoluyla)
- Engelleme
  - Silme
  - Ulaşılamaz, ya da kullanılamaz hale getirme
- Bütünlüğün bozulması
  - Veri değişikliği
  - Sahte veri

# Gerektiği Kadar Koruma Prensibi

- Değerli şeyler (yazılım, donanım, veri) sadece değerleri geçerli olduğu sürece korunmalı.

- Korumak için harcanan süre, çaba ve para, korunan şeyin değeriyle orantılı olmalı.

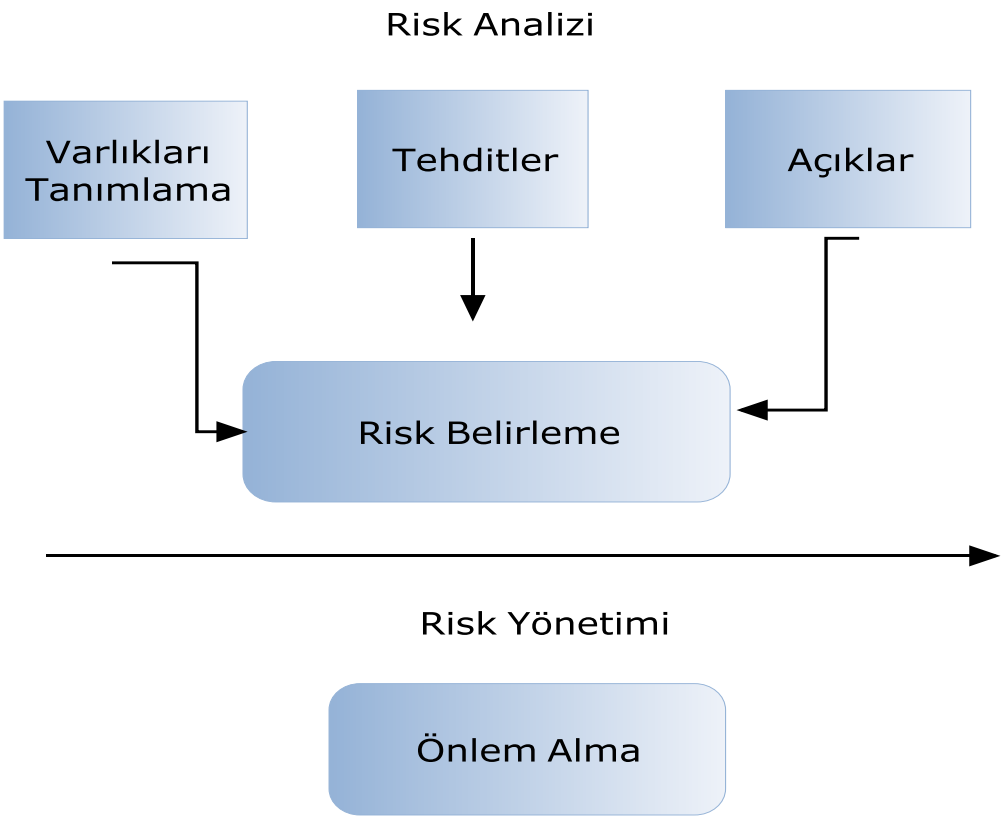
# Saldırgan Grupları

- Amatörler
  - *Kişiler:* Olağan bilgisayar kullanıcıları
  - *Saldırı şekli:* Çoğunlukla bir açığı farketme ve yararlanma şeklinde
- Kırıcılar (Crackers)
  - *Kişiler:* Lise veya üniversite öğrencileri
  - *Saldırı şekli:* Sadece yapmış olmak için, veya yapılabildiğini görme/gösterme için, açık bulmaya çalışma şeklinde
- Profesyonel Suçlular
  - *Kişiler:* Para karşılığı bilgisayar suçları işleyenler
  - *Saldırı şekli:* Saldırının hedefleri önceden belirli, planlı ve organize şekilde

# Bilgi Güvenliği Yönetim Sistemi (BGYS) Nedir?

- Olası risklerin ve tehditlerin belirlenmesi,
- güvenlik politikalarının oluşturulması, denetimlerin ve uygulamaların kontrolü,
- uygun yöntemlerin geliştirilmesi,
- örgütsel yapılar kurulması ve yazılım/donanım fonksiyonlarının sağlanması gibi bir dizi denetim eyleminin birbirini tamamlayacak şekilde gerçekleştirilmesidir.

# Risk Analizi ve Yönetimi



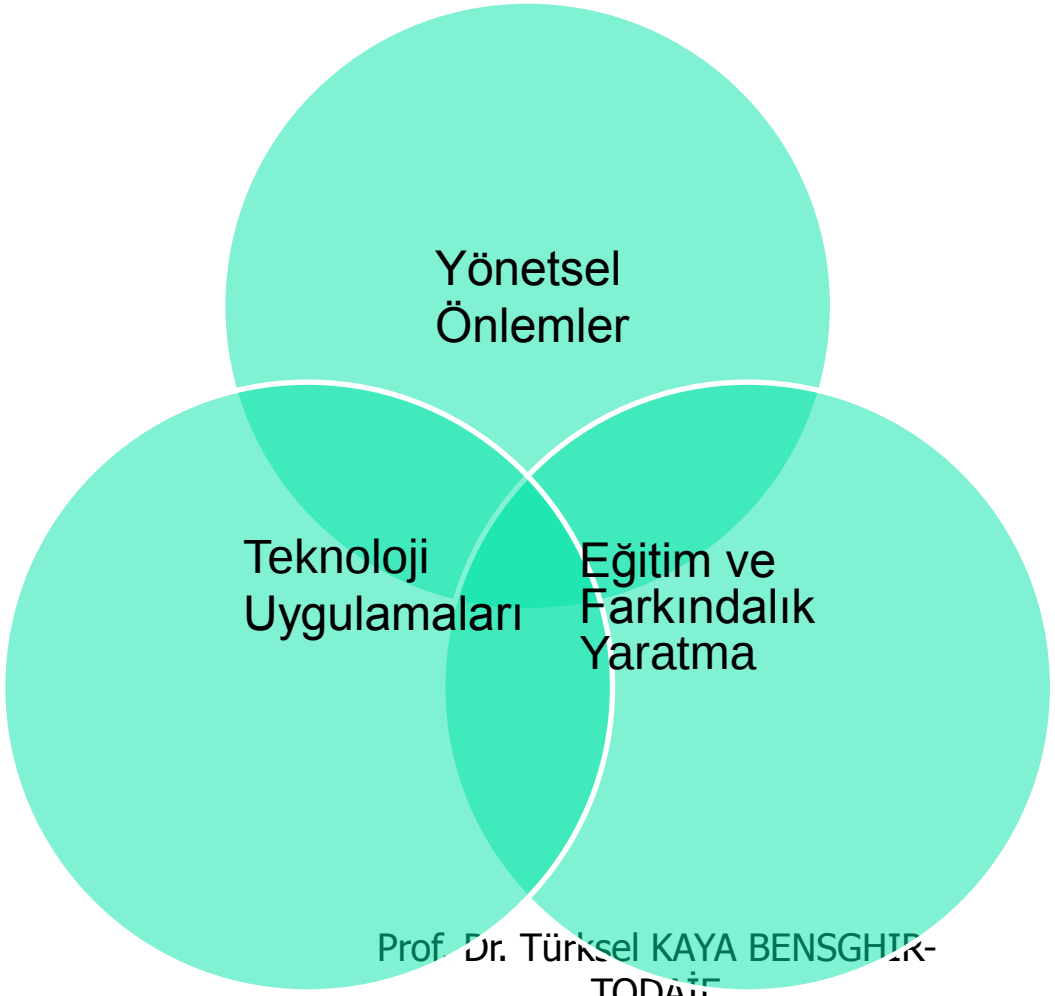
# Güvenlik Risk Analizi

# Risk Yönetimi

- Risk altındaki bilginin değeri
- Risk alma potansiyeli
- Korunması gereken değerlerin ve alınabilecek risklerin belirlenmesi


*Güvenlik, maliyet ve üretkenlik arasında bir dengedir.*

# Bilgi-Bilişim Güvenliği Nasıl Sağlanır?



# Bilgi güvenliğinin sağlanabilmesi için aşağıdaki koşulların sağlanması beklenir:

- Gizlilik (confidentiality)
  - Önemli ve hassas bilgilerin istenmeyen biçimde yetkisiz kişilerin eline geçmesinin önlenmesi ve sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğu garanti altına alınmasıdır.

# Bilgi güvenliğinin sağlanabilmesi için aşağıdaki koşulların sağlanması beklenir:

- Bütünlük (integrity)
  - Bilginin yetkili kişiler dışında değiştirilmesinin ve silinmesinin önlenmesidir.
- Süreklilik (availability)
  - Bilgi veya bilgi sistemlerinin sürekli kullanıma hazır ve kesintisiz çalışır durumda olmasıdır.

# Bilgi Güvenliği Sağlama Araçları

- Fiziksel Güvenlik:
  - Fiziksel önlemlerle (güvenli ortam vb) güvenliğinin sağlanması.
- Kullanıcı Doğrulaması Yöntemleri:
  - Akıllı kart, tek kullanımlı parola, token ve Public Key Certificate gibi araçlar ve RADIUS gibi merkezi kullanıcı doğrulama sunucularının kullanılması.
- Şifreleme:
  - Güvensiz ağlar üzerinden geçen verilerin güvenliği için Virtual Private Network veya şifreleme yapan donanımların kullanılması. Ayrıca web tabanlı güvenli veri transferi için SSL ve Public Key şifrelemenin kullanılması. Donanım tabanlı şifreleme çözümleri de mümkündür.
- E-imza

# Güvenlik Prensipleri

- **Gizlilik(Confidentiality):**
  - Depolanan ve taşınan bilgilere yetkisiz erişimlerin engellenmesi
  - Gizli bilgilerin korunması ve mahremiyetinin sağlanması
- **Güncellik ve Bütünlük (Accuracy & Integrity)**
  - Kullanıcılara bilgilerin en güncel halinin sunulması
  - Yetkisiz değişikliğin ve bozulmanın engellenmesi
- **Süreklilik(Availability)**
  - Sistemin kesintisiz hizmet vermesi
  - Performansın sürekliliği
- **İzlenebilirlik ya da Kayıt Tutma(Accountability)**
  - Kullanıcının parolasını yazarak sisteme girmesi
  - Web sayfasına bağlanmak
  - E-posta almak-göndermek
  - Icq ile mesaj yollamak

# Güvenlik Prensipleri (Devam)

- **Kimlik Sınaması(Authentication)**
  - Alıcı-gönderici doğrulaması
  - Parola doğrulaması
  - Akıllı kart, biyometri doğrulaması
- **Güvenilirlik(Reliability-Consistency)**
  - Sistemden bekleneni eksiksiz ve fazlasız vermesi
  - %100 Tutarlılık
- **İnkâr Edememe(Nonrepudiation)**

# Yönetsel Önlemler-1

- **Güvenlik Politikaları**
  - Kurumsal Güvenlik Politikası
  - Konuya Özel Güvenlik Politikası
  - Sisteme Özel Güvenlik Politikası

- **Standartlar ve Prosedürler**
  - Konfigürasyon Yönetim Prosedürü
  - Yedekleme ve Yedekleme Ortamlarını Saklama Prosedürü
  - Olay Müdahale Prosedürü
  - İş Sürekliliği ve Felaket Kurtarma Prosedürü

# Güvenlik Politikası

- Güvenlik politikası, uygulanacak güvenliğin ne yapması gerektiğini tanımlayan yazılı bir belgedir.
- Aynı zamanda, kurumsal kaynaklara erişim yetkisi olan kurum çalışanlarının uymaları gereken kuralları içeren resmi bir rapor niteliği taşır ve kurumun üst düzey yönetimi tarafından desteklenmelidir.

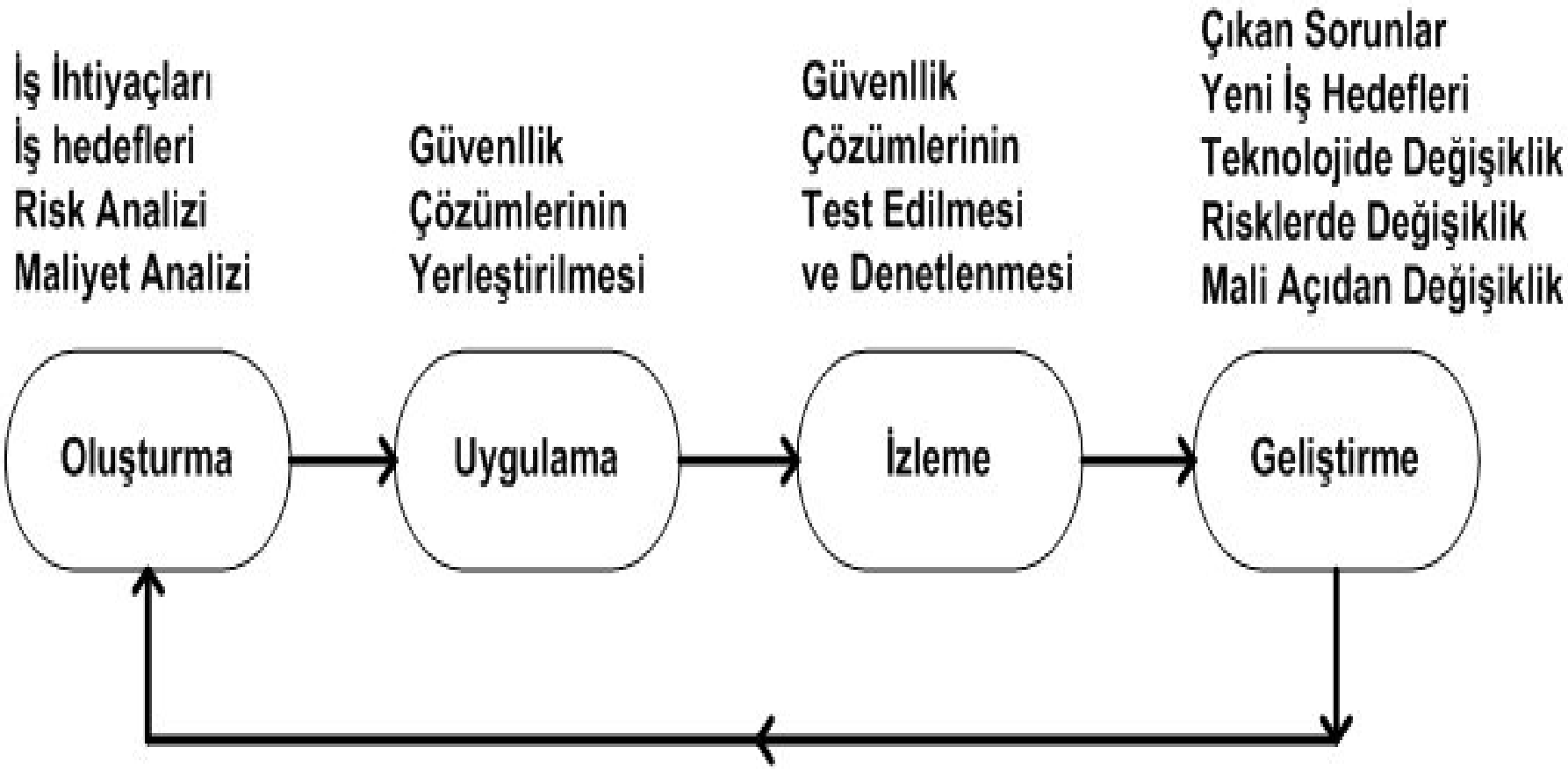
# Güvenlik Politikası/2

- Güvenlik politikası uygulanabilir, kullanılabilir, karşılanabilir ve kolay yönetilebilir olmalı ve kurumun iş ihtiyaçları ve iş hedefleri doğrultusunda belirlenmelidir.

# Güvenlik Bütçesi

- Güvenlik bütçesi oluşturulmadan önce bir risk analizi yapılmalıdır.
- Risk analizi ile kurumun sahip olduğu değerler, bu değerlere karşı potansiyel tehditler, tehdidin sonuç vermesini sağlayan zayıflıklar ve tehdit oluştuğunda kurumun vereceği kayıplar tespit edilmeli, risk analizi sonucunda bir maliyet analizi yapılarak, tüm güvenlik harcamalarının öncelikleri doğru olarak belirlenmeli ve bu harcamaların korunacak sistemlerin değerinden ve onarım maliyetinden yüksek olmamasına dikkat edilmelidir.

# Güvenlik Politikası Döngüsü



# Yönetsel Önlemler-2 (Devam)

- **Güvenlik Yaşam Döngüsü**
  - Sistem Güçlendirme
  - Hazırlık
  - Saldırı / Sorun Tespiti
  - Tespit edilen olaya özgü önlemlerin alınması / kurtarma
  - İyileştirme, tespit edilen olayın tekrarını önleyecek önlemler

- **Minimalist Yaklaşım**
  - Kimseye gerektiğinden fazla erişim hakkı tanımama
  - Kimseye gerektiğinden fazla bilgi vermeme
  - Gerekmeyen hiç bir yazılımı yüklememe
  - Gerekmeyen hiç bir hizmeti sunmama

# Teknoloji Uygulamaları

- Kriptografi
- Sayısal İmza ve PKI
- Ağ Bölümlendirmesi ve Güvenlik Duvarları
- Yedekleme
- Saldırı Tespiti
- Erişim Denetimi
- Anti-Virüs Sistemleri

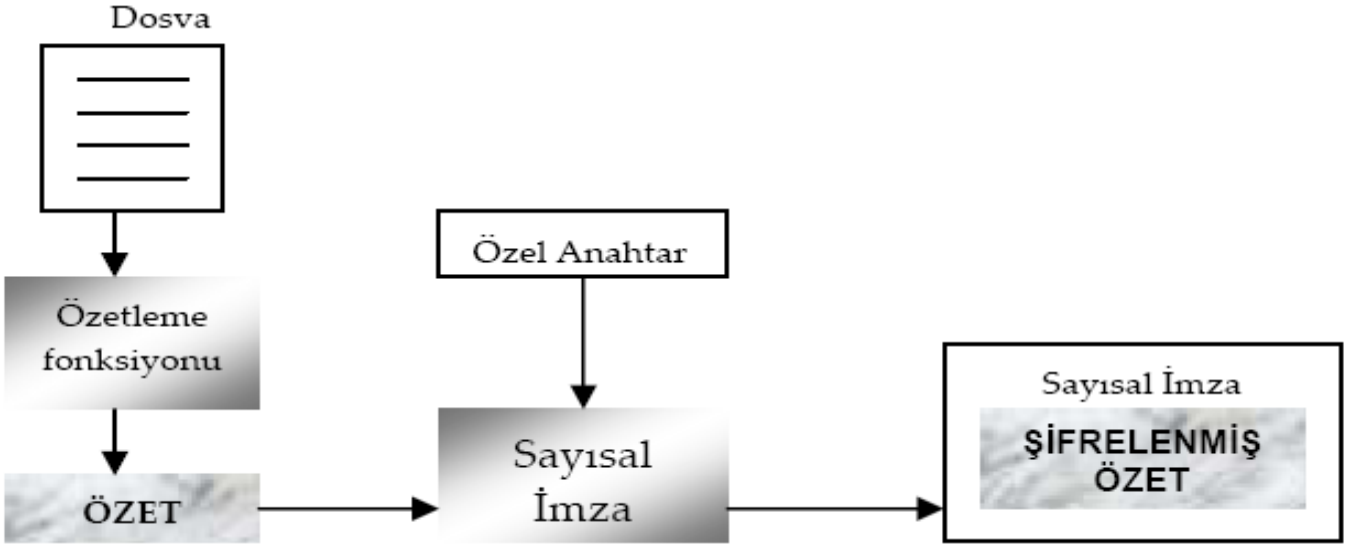
# Kriptografi

- **Simetrik Algoritmalar**
- **Asimetrik Algoritmalar**
- **Özetleme Fonksiyonları**


*Temel Kriptografi Mekanizması*

# Sayısal İmza ve PKI

- **Sayısal sertifikalar**
- **Sertifikasyon Otoriteleri**




*Bir Mesajın Sayısal İmzasının Oluşturulması*

# Güvenlik Duvarları (Firewall)

- Kaynak IP adresi
- Kaynak hizmet noktası (port)
- Hedef IP adresi
- Hedef hizmet noktası
- Bağlantı tipi (TCP, UDP, ICMP, vb.)

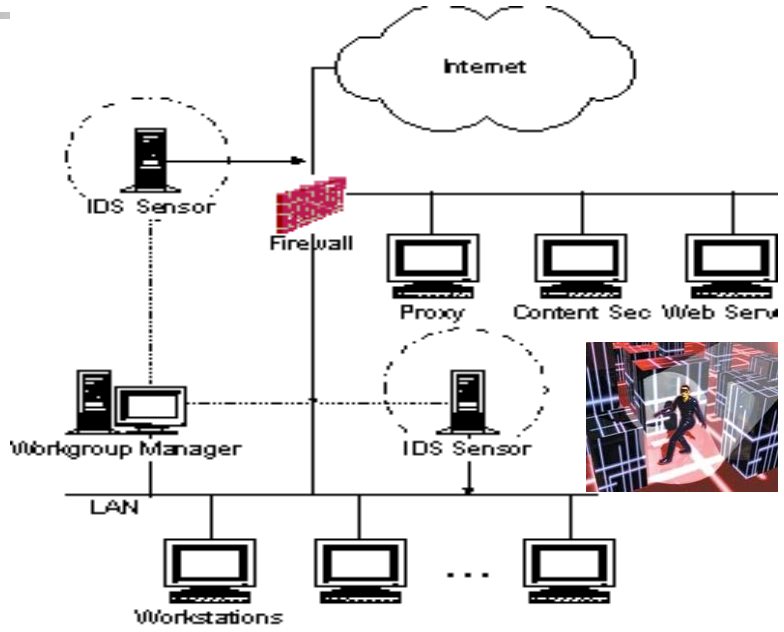
✓ **Tanımlı olmayanlara izin verilmesi**

X **Tanımlı olmayanlara izin verilmemesi**

# Saldırı Tespiti (IDS)

- Saldırı tespit Sistemleri bilgisayarların ve bilgisayar ağlarının faaliyetlerini izlemek, kaydetmek ve olası saldırıları tespit etmek amaçlı olarak tasarlanan sistemlerdir.

- Firewall' girişte kimlik kartı kontrolü yapan bir kapıya benzetirsek, saldırı tespit sistemleri içeriyi gözetleyen güvenlik kameraları gibi çalışırlar.



# Yedekleme

Bir sistemin düzenli olarak yedeğini almak çok zor iştir;
Bu nedenle Kritiklilik/Gereklilik analizi çok iyi yapılmalıdır.

- Verilerin Yedeklenmesi
- İletişim Hatlarının Yedeklenmesi
- Güç Kaynağının Yedeklenmesi
- Cihazların Yedeklenmesi
- Fiziksel Ortamın Yedeklenmesi

} GÜVENLİK-MALİYET ANALİZİ

# Erişim Denetimi

Erişim Denetimi, Kaynaklara kimin nasıl eriştiğini kontrol etmektir. (Access Control)

Erişim denetimi üç aşamalı olarak gerçekleştirilir:

1. Tanımlama (Identification)
   - Kullanıcı Adı
   - Kullanıcı Grubu
2. Kimlik Sınama (Authentication)
   - Parola passwordtester
   - Akıllı Kart,
   - Biyometrik İşaret v.b.
3. Yetkilendirme (Authorization)

# Anti-Virüs Sistemleri

- Bilgisayar virüsleri, "Kötü amaçlı program kodu" olarak tanımlanabilir.
- Anti-virüs yazılımları, bilinen virüsleri tanıyabilen ve temizleyebilen programlardır.
- E-posta yoluyla virüsler, gerçek hayattaki virüslerden farksız bir hızla yayılmaktadırlar.

## Virüs-Solucan(Worm)- Truva Atı(Trojan Horse)

**Nasıl Korunurum?**

1. Anti-virüs yazılımının her zaman güncel tutulması
2. Kullanılan yazılım yamalarının güncel tutulması
3. Yabancı birinden gelen bir e-posta ekini açılmaması
4. Bilinen birinden gelse bile, ne olduğunu bilmedikçe bir e-posta ekteki dosyanın açılmaması

# Eğitim ve Farkındalık Yaratma

- **Üç Farklı Grup İçin Eğitim;**
  - Yöneticiler,
  - Orta Kademe Yöneticiler,
  - Ve Teknik Grup

# Bu yöntemler yeterli mi?

- Ancak bu tür önlemlerin alınması tek başına yeterli değildir.
- Bilgi güvenliği bilgi yönetimi içinde bir süreç olarak görülmelidir.
- Her kurum bir güvenlik politikası oluşturmalı, bunu yazılı olarak raporlayarak, çalışanlarına, paydaşlarına aktarmalıdır.
- BIT Standartları benimsenmeli ve uygulanmalıdır.

# BİT Standartları

- **Yazılım Paketleri Ürün Belgelendirmesi (TS 12119),**
- **Yazılım Süreç Yönetimi Belgelendirmesi (TS 15504),**
- **Bilgi Güvenliği Yönetim Sistemi Belgelendirmesi (TS ISO /IEC 27001)**
- **Ortak Kriterlerler (TS ISO/IEC 15408) Belgelendirmesi**

# TS ISO IEC 27001 'nin kapsamı ve hedefleri

- **Kuruluşun tüm iş riskleri kapsamında yazılı bir BGYS'in oluşturulması, gerçekleştirilmesi, işletilmesi, izlenmesi, gözden geçirilmesi, sürdürülmesi ve geliştirilmesi için gereksinimleri belirtir.**

# 27001 BGY Sürecinde Ana Kontrol Alanları

- Bilgi güvenliği politikası
- BG organizasyonu
- Varlık yönetimi
- Personel güvenliği
- Fiziksel çevre güvenliği
- İletişim ve işletim yönetimi
- Erişim kontrolü
- İhlal olayları yönetme
- İş sürekliliği
- Uyum

# Bilgi güvenliği politikası

- Bir bilgi güvenliği politika dokümanı, yönetim tarafından onaylanmalı, yayınlanmalı ve tüm çalışanlar ve ilgili taraflara bildirilmelidir.
- Bilgi güvenliği politikası, belirli aralıklarla veya önemli değişiklikler ortaya çıktığında sürekli uygunluğunu, doğruluğunu ve etkinliğini sağlamak için gözden geçirilmelidir.

# Varlık Yönetimi

- **Kurumun varlıklarının tümü açıkça tanımlanmalı ve önemli varlıkların bir envanteri hazırlanmalı ve tutulmalıdır.**
- **Bilgi işleme olanakları ile ilişkili tüm bilgi ve varlıklar atanan bir bölüm tarafından sahiplenilmelidir.**
- **Bilgi, değeri, yasal gereksinimleri, hassaslığı ve kuruluş için kritikliğine göre sınıflandırılmalıdır.**

# İnsan Kaynakları Güvenliği

- **Çalışanlar, yükleniciler ve üçüncü taraf kullanıcıların güvenlik rolleri ve sorumlulukları kuruluşun bilgi güvenliği politikasına uygun olarak tanımlanmalı ve dokümante edilmelidir.**
- **Tüm işe alınacak adaylar, yükleniciler ve üçüncü taraf kullanıcıları ilgili yasa, düzenleme ve etik ilkelere göre çalışmaları için uygun doğrulama kontrolleri gerçekleştirilmelidir.**

# Fiziksel ve Çevresel Güvenlik

- **Bilgi ve bilgi işleme olanaklarını içeren alanları korumak için güvenlik önlemleri (duvarlar gibi engeller, kart kontrollü giriş kapıları, görevli bulunan resepsiyon masaları) alınmalıdır.**

- **Veri taşıyan ya da bilgi hizmetlerini destekleyen iletişim ortamları ve araçları, kesilme ya da hasarlardan korunmalıdır.**

# İletişim ve İşletim Yönetimi

- İşletim prosedürleri dokümante edilmeli, sürdürülmeli ve ihtiyacı olan tüm kullanıcıların kullanımına sunulmalıdır.
- Bilgi ve yazılımlara ait yedekleme kopyaları alınmalı ve yedekleme politikasına uygun şekilde düzenli olarak test edilmelidir.

# Erişim Kontrolü

- Erişim için iş ve güvenlik gereksinimlerini temel alan bir erişim kontrol politikası kurulmalı, dokümante edilmeli ve gözden geçirilmelidir.
- Kullanıcılardan, parolaların seçiminde ve kullanımında güvenlik uygulamalarını izlemeleri istenmelidir.
- Ağlarda, bilgi hizmetleri, kullanıcıları ve bilgi sistemleri grupları ayrılmalıdır.
- Etkin olmayan oturumlar tanımlanmış belirli bir hareketsizlik süresinden sonra kapatılmalıdır.

# Bilgi Sistemleri Edinim, Geliştirme ve Bakım

- **Uygulama sistem yazılım güvenliğini sağlamak için gerekli kontrol prosedürleri belirlenmeli ve uygulanmalıdır.**
- **Outsorce edilen yazılımlar kuruluş tarafından denetlenmeli ve izlenmelidir.**
- **Kullanılan bilgi sisteminin teknik açıklıkları hakkında zamanında bilgi elde edilmeli, kuruluşun bu tür açıklıklara maruz kalması değerlendirilmeli ve riskleri hedef alan uygun önlemler alınmalıdır.**

# Bilgi Güvenliği İhlal Olayı Yönetimi

- **Bilgi güvenliği olayları uygun yönetim kanalları aracılığıyla mümkün olduğu kadar hızlı biçimde rapor edilmelidir.**
- **Bilgi sistemleri ve hizmetlerinin tüm çalışanları, yüklenicileri ve üçüncü taraf kullanıcılarından, sistemler ve hizmetlerdeki gözlenen veya şüphelenilen herhangi bir güvenlik zayıflığını dikkat etmeleri ve rapor etmeleri istenmelidir.**
- **Bilgi güvenliği ihlal olaylarının türleri, miktarları ve maliyetlerinin ölçülüp izlenebilmesini sağlayan mekanizmalar bulunmalıdır.**

# İş Sürekliliği Yönetimi

- **Kuruluş genelinde iş sürekliliğini sağlamak bir proses tanımlanmalıdır.**

- **İş sürekliliği planlarının, güncel ve etkili olmalarını sağlamak için, düzenli olarak test edilmeli ve güncelleştirilmelidir.**

# Uyum

- **İlgili tüm yasal düzenleme ve sözleşmeden doğan gereksinimler tanımlanmalı, dokümante edilmeli ve güncel tutulmalıdır.**

# BGYS'nin sağlayacağı faydalar

- Tehdit ve risklerin belirlenerek etkin bir risk yönetiminin sağlanması
- Kurumsal saygınlığın korunması ve artışı
- İş sürekliliğinin sağlanması
- Bilgi kaynaklarına erişimin denetlenmesi
- Personelin ilgili tüm tarafların güvenlik konusunda farkındalık düzeyinin yükseltilmesi ve önemli güvenlik konularında bilgilendirilmesi

| Kriter | Çok İyi | İyi | Kritik | Zayıf | Çok Zayıf |
|---|---|---|---|---|---|
| Bilgi güvenliği politikası | | | | | |
| BG organizasyonu | | | | | |
| Varlık yönetimi | | | | | |
| Personel güvenliği | | | | | |
| Fiziksel çevre güvenliği | | | | | |
| İletişim ve işletim yönetimi | | | | | |
| Erişim kontrolü | | | | | |
| İhlal olayları yönetme | | | | | |
| İş sürekliliği | | | | | |
| Uyum | | | | | |

# BGYS'nin sağlayacağı faydalar-2

- Bilgi varlıklarının bütünlüğünün ve doğruluğunun sağlanması
- Personelin görevlerini yerine getirirken, bilgi sistemleri kaynaklarını kötü amaçlı olarak kullanma ve/veya kaynakları suistimal etmelerinin engellenmesi
- Bilgi varlıklarının gizliliğinin korunması
- Personelin, başkaları tarafından yapılabilecek olan suistimal ve tacizlere karşı zan altında kalmasının engellenmesi

# Sonuç

- Kesin (% 100)  güvenlik ulaşılabilir değildir!
- Kurumsal bilgi güvenliği bir kez gerçekleştirilen bir çalışma olarak değil, bir süreç olarak ele alınmalı ve oluşturulan kurumsal güvenlilik politikalarına uygunluk sürekli denetim altında tutulmalıdır.

- Bilgi ve Sistem Güvenliğine sosyo-teknik sistemle -bütüncül-yaklaşmak gerekir.

# ULUSAL BİLGİ SİSTEMLERİ GÜVENLİK PROGRAMI

Prof. Dr. Türksel KAYA BENSGHIR-
TODAİE

# **BT Stratejisi: 88 numaralı madde:**Ulusal Bilgi Sistemleri Güvenlik Programı

- Ülkemizin bilgisayar olaylarına acil müdahale koordinasyon merkezini kurmak hedeflenmektedir.
- Sorumlu ve İlgili Kuruluşlar:
  - TÜBİTAK-UEKAE (S)
  - Kamu Kurum ve Kuruluşları(İ)
  - Üniversiteler (İ)

# Kamu kurum ve kuruluşları için:

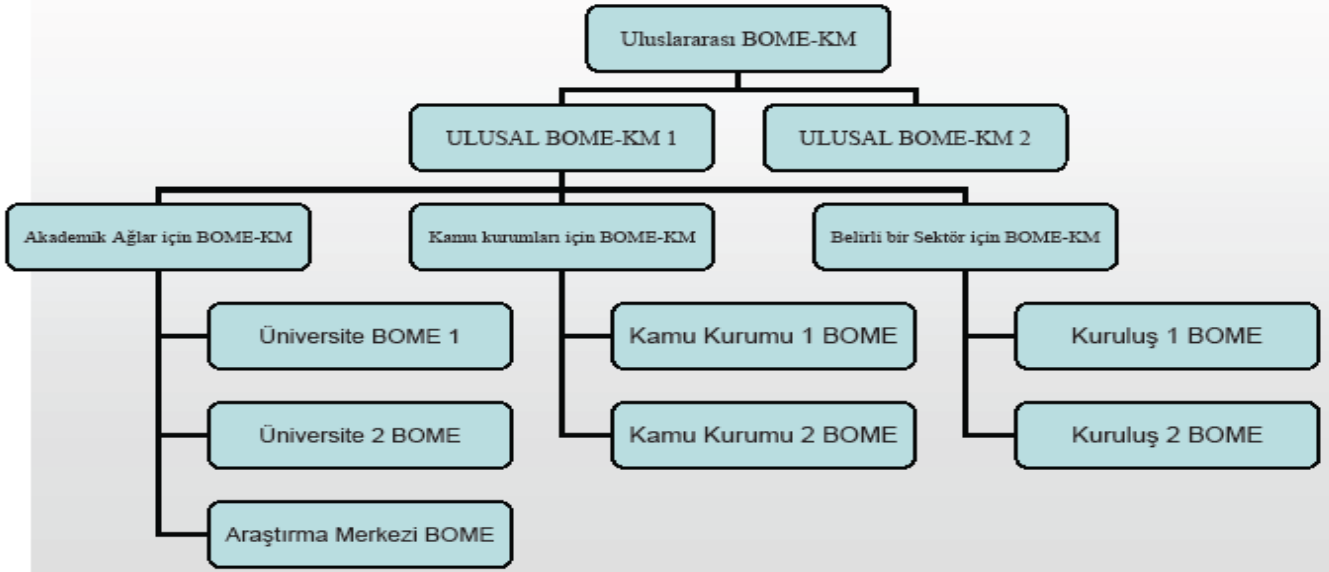
- 1. Minimum güvenlik gereksinimlerini belirlemek
- 2.Bilgi sistem güvenliği ile ilgili tehditleri tespit etmek
- 3. Bilgi sistem güvenliği eksiklikler konusunda önerilerde bulunmak
- 4.Bilgi sistem güvenliği ile ilgili acil uyarılar yapmak
- 5.Bilgi güvenliği yönetim sistemi konusunda pilot kurumlara danışmanlık vermek
- 6.Bilgi sistem güvenliği ile ilgili eğitimler vermek

# Kurumlararası İlişkiler

- Korunmak için işbirliği
- Diğer kurumlarla koordinasyon
- Güven ilişkisi oluşturma
- Ulusal ve uluslararası Olay engelleme
- Acil bilgi güvenlik ikazları oluşturma ve paylaşma

# Bilgisayar Olayları Müdahale Koordinasyon Merkezi

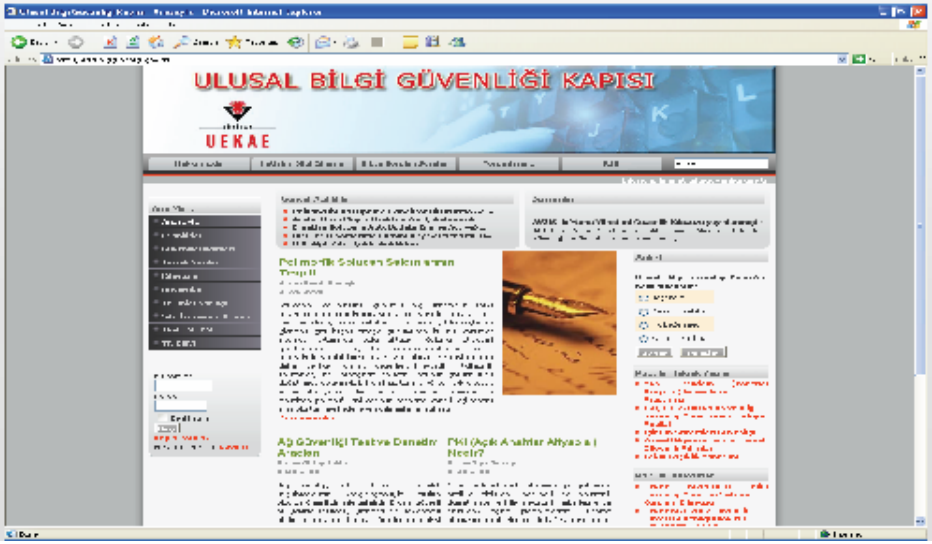
- Bilgisayar olayları müdahale ekipleri koordinasyon merkezleri (BOME-KM) hiyerarşisi




Kaynak:
http://www.bilgiguvenligi.gov.tr/index.php?option=com_content&task=view&id=252&Itemid=6

# Ulusal Bilgi Güvenliği Kapısı Projesi

- www.bilgiguvenligi.gov.tr
- Bilgi güvenliği ile ilgili bilgi kaynağı
- Herkesin katkısına açık
  - Bilgi güvenliği ile ilgili makaleler
  - Yayınlanan dokümanlara yorum verebilme
- Bilgi güvenliği dokümanları




Kaynak:
http://www.bilgiguvenligi.gov.tr/index.php?option=com_content&task=view&id=252&Itemid=6

# Ülkemizde Gerçekleştirilen Siber Güvenlik Tatbikatları

- 1. BOME 2008 Tatbikatı
  - 8 Kamu kuruluşun katıldığı tatbikata TÜBİTAK BİLGEM bünyesinde faaliyet gösteren Türkiye Bilgisayar Olayları Müdahale Ekibi (TR-BOME) tarafından gerçekleştirilmiştir.
- 2. Tatbikat- 2011 (25-28 Ocak)

# 2. Tatbikat- 2011 (25-28 Ocak)

- Tatbikatı amacı,  katılımcı kurumların siber saldırılar karşısındaki teknik kabiliyetleri ve saldırılardan korunma konusunda almaları gereken teknik önlemler kadar siber saldırı durumunda kurum içi ve kurumlar arası koordinasyon ve iletişim yeteneklerinin ölçülmesi hedeflenmiştir.

- Ulusal Siber Güvenlik Tatbikatı 2011'e; enerji, finans, telekom, savunma, sağlık ve sosyal güvenlik gibi 'kritik bilgi-sistem altyapıları'nı oluşturan 41 kamu ve özel sektör kurum/kuruluşu katılmıştır.
- Tatbikat verileriyle, siber olaylarla mücadelede ülkemizin teknik, idari ve hukuki kabiliyetlerinin artırılması için öneriler geliştirilmesi hedeflenmiştir.

# 2. Tatbikat
## (25-28 Ocak 2011)

- Gerçek saldırılar kapsamında;
  - port taraması,
  - dağıtık servis dışı bırakma saldırısı,
  - web sayfası güvenlik denetimi ve
  - kayıt dosyası analizi yapılmıştır.

Yazılı senaryolarda ise;

- elektrik kesintisi,
- kurumiçinden veri sızdırılması,
- web sayfasının ele geçirilmesi,
- sosyal mühendislik saldırıları gibi olası saldırı senaryoları karşısında kurumların verdikleri tepkiler yazılı olarak değerlendirilmiştir.

# 2. Tatbikat (25-28 Ocak 2011)

- Etkinliğin iki günlük kısmında gerçek saldırılar uygulanmış;
- son iki günlük kısmında ise yazılı ortamda olası saldırı senaryoları değerlendirilerek teknik, idari ve hukuki süreçler ele alındı.
- Tatbikatta; 83 gerçek saldırı, 450'nin üzerinde yazılı senaryo değerlendirilmiştir.

# Tatbikatın sonunda düzenleyici kurumların başkanları şu açıklamada bulundular:

- "Tatbikatta Türkiye kazandı.
- Tatbikatta kuruluşlar bazında neler olduğu/yapıldığı/karşılaşıldığı gibi bilgiler herhangi bir şekilde paylaşılmayacak.
- Bu Tatbikat amacına ulaştı ve tüm katılımcı kuruluşlar başarılı bir şekilde tamamladılar. Kendilerini değerlendirdiler."

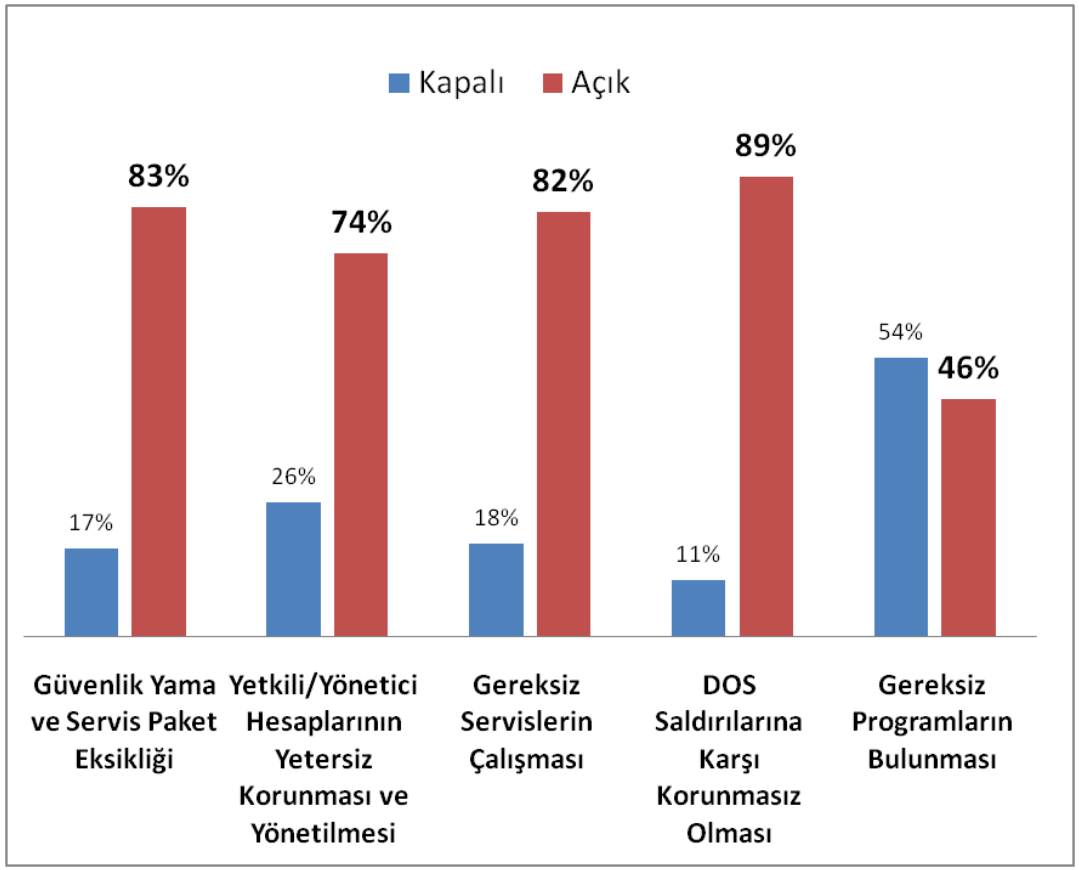
- ilk iki günlük kısmında gerçek saldırılar uygulanırken, son iki günlük kısmında ise yazılı ortamda olası saldırı senaryoları değerlendirilerek teknik, idari ve hukuki süreçler ele alındı. Tatbikatta; 83 gerçek saldırı, 450'nin üzerinde yazılı senaryo değerlendirilmiştir.

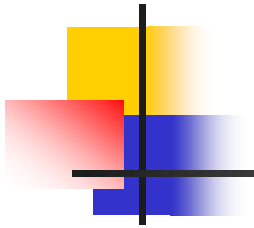
# Kamu kurumlarında yapılan güvenlik testlerinden seçilen bazı açıklıklar;

- Güvenlik Yama ve Servis Paket Eksikliği
- Yetkili/Yönetici Hesaplarının Yetersiz Korunması ve Yönetilmesi
- Gereksiz Servislerin Çalışması
- DOS Saldırılarına Karşı Korunmasız Olması
- Gereksiz Programların Bulunması

# Güvenlik testlerinden seçilen bazı açıklıklar

KAYNAK: *www.tubitak.gov.tr/tubitak_content.../Korkmaz_**Bulut_Bilisim**.ppt*





# Teşekkür ederim...

Prof. Dr. Türksel KAYA BENSGHIR-
TODAİE

# The 2005 Global Security Survey

Global Financial Services Industry Deloitte Touche Tohmatsu

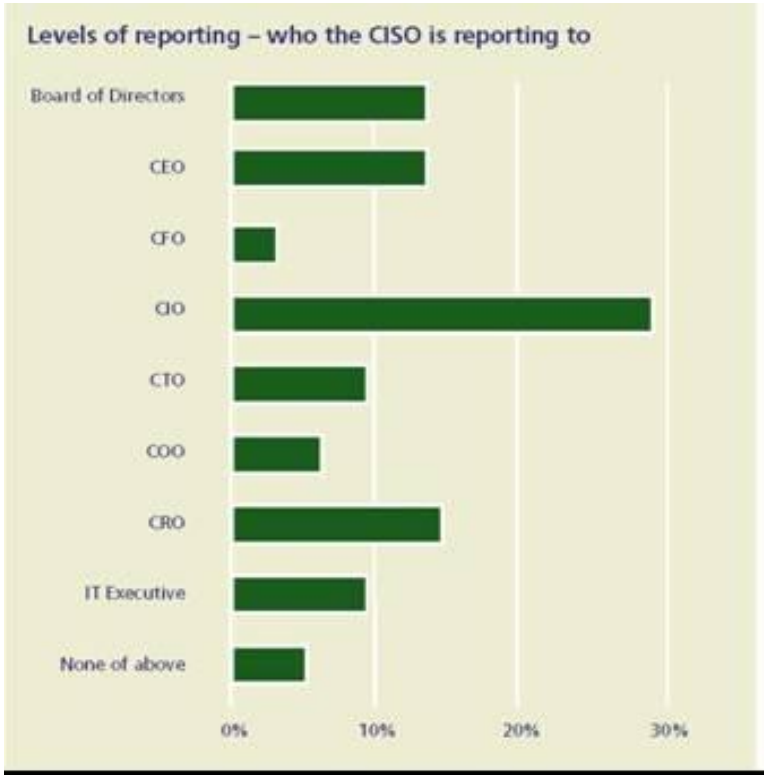
# Küresel Güvenlik Araştırması 2005- The 2005 Global Security Survey

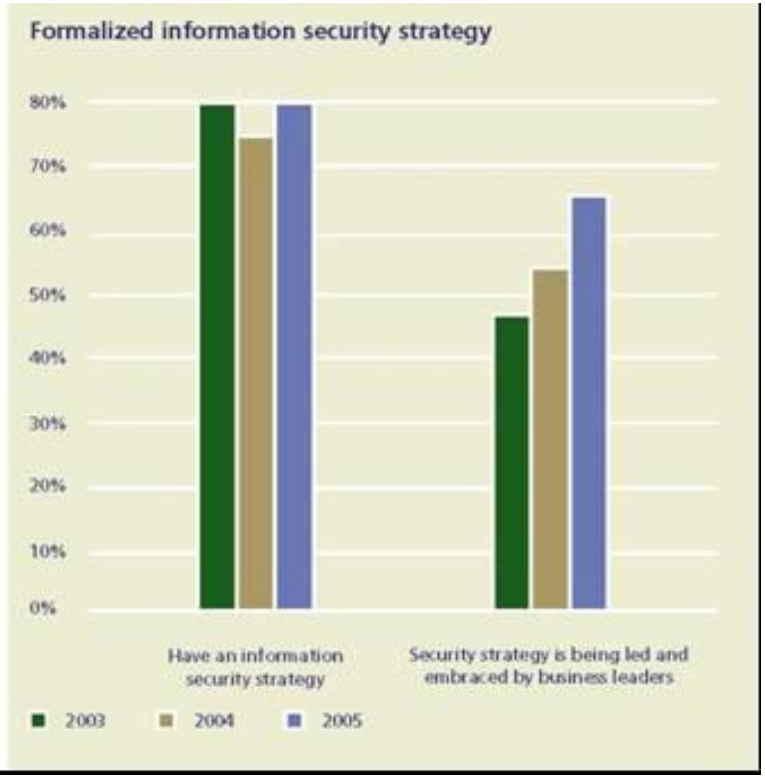
- 180 Finans kuruluşunun (banka, sigorta ve güvenlik şirketleri) güvenlik ve gizlilik konusunda yaklaşımlarını ortaya koymak üzere araştırma yapılmıştır.

# Profil

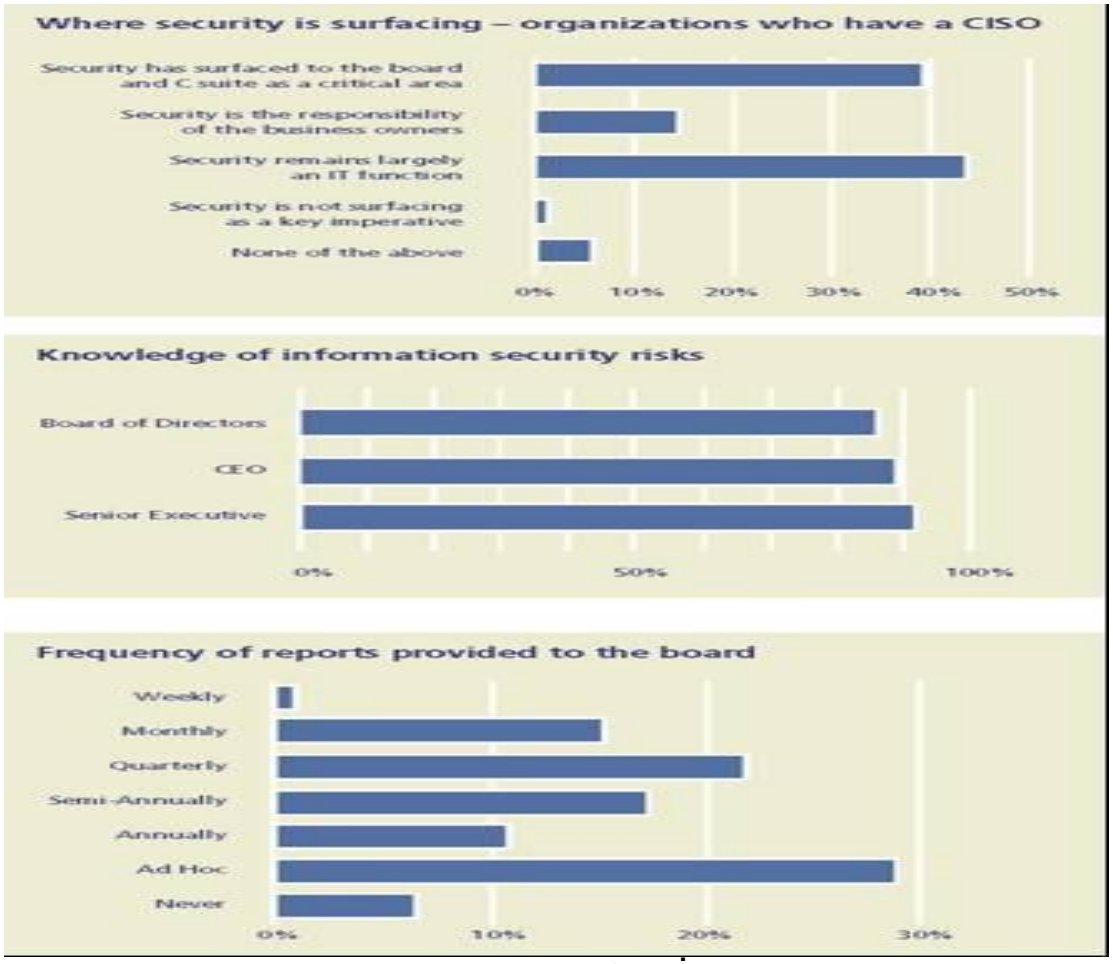
- 120 kuruluşun 26 sı ilk büyük 500 kuruluş arasında yer almaktadır. 28 banka ise 2003 itibarıyla sermaye büyüklüğü açısında ilk sıralarda yer almaktadır.

# CISO-bilgi Güvenlik yöneticisi kime rapor sunmaktadır?
# Resmi bir Bilgi Güvenlik Stratejileri var mı?

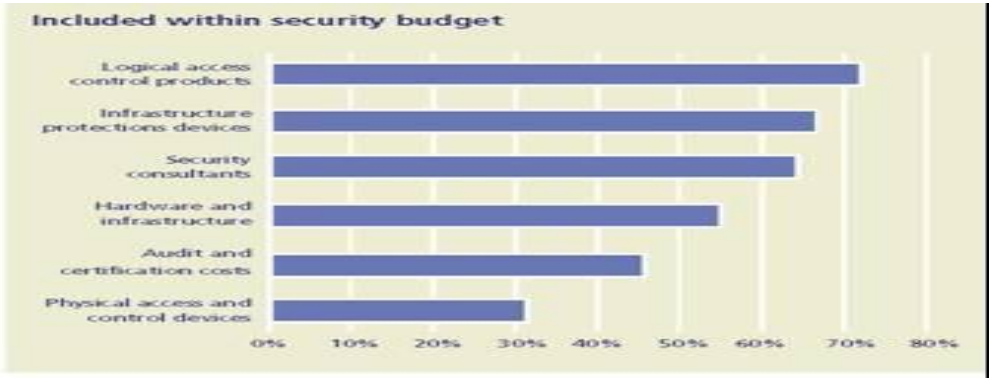


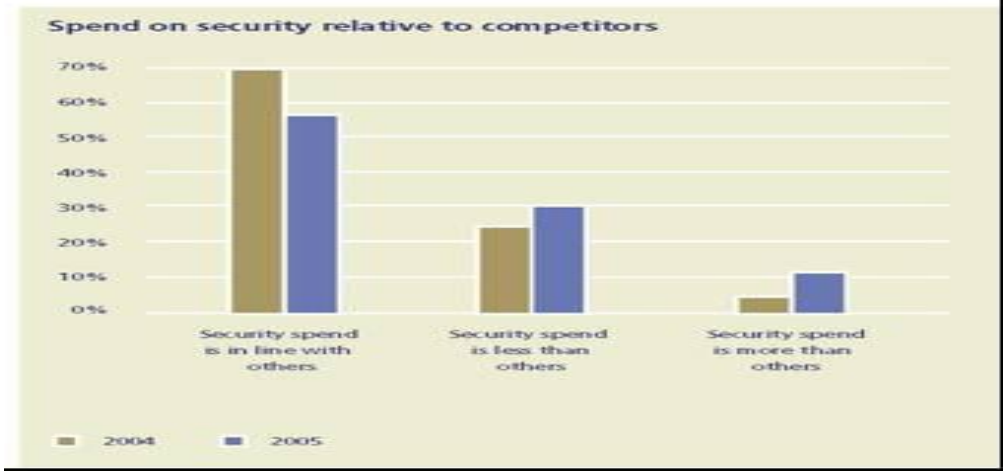



# Güvenlik Riskleri

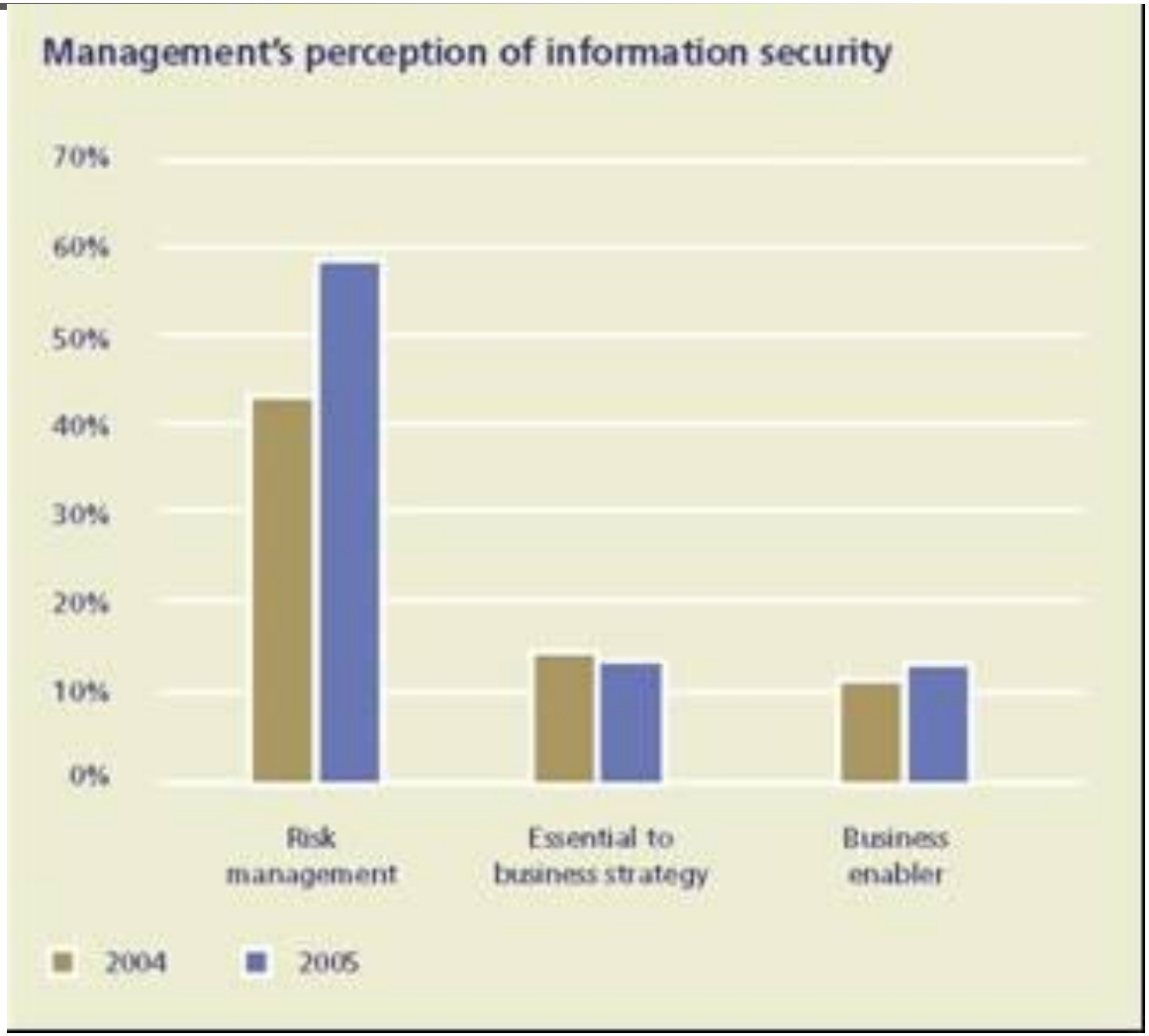


# Güvenlik Bütçesi

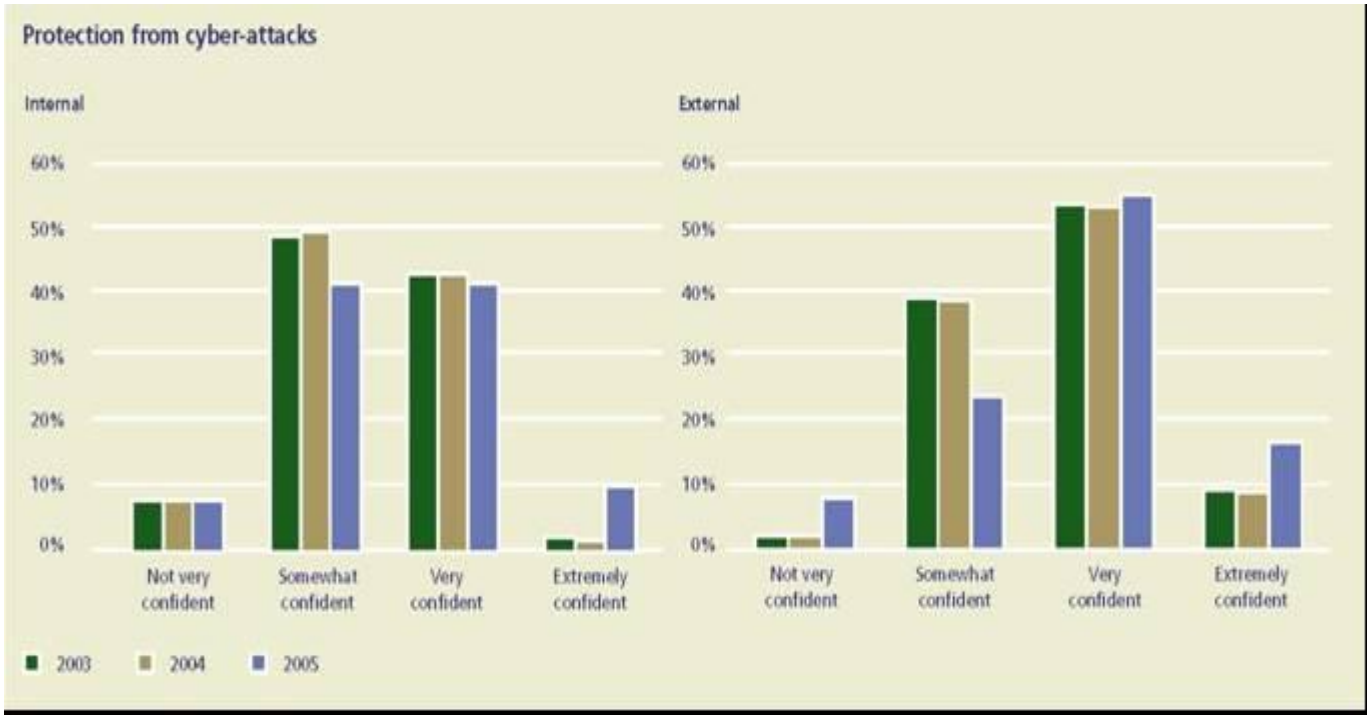


# Yönetim Bilgi Güvenliğini Nasıl Algılıyor?



# Siber Saldırılardan Korunma



# Karşılaşılan Tehditler