

# **Bilgisayar Güvenliğine Giriş**

Yrd. Doç. Dr. Özgü Can

# İçerik

- Temel Kavramlar
- Tehditler (Threats)
- Politika ve Düzenek (Policy and Mechanism)
- Varsayım ve Güven (Assumption and Trust)
- Güvence (Assurance)
- İşlemsel Sorunlar (Operational Issues)
- İnsan Sorunları (Human Issues)

# Temel Kavramlar

- CIA
  - **C**onfidentiality (Gizlilik)
  - **I**ntegrity (Bütünlük)
  - **A**vailability (Kullanılabilirlik)



# Gizlilik

## (Confidentiality)

- Bilginin ya da kaynağın gizlenmesidir.
  - Duyarlı (sensitive) alanlarda bilginin saklanmasına duyulan ihtiyaç → Hükümet, askeriye, endüstri vs.
- “Bilmeye ihtiyaç” (need to know) prensibi → erişimin kontrol edilmesi
  - ÖR: Tescilli ürünlerin güvenliği

# **Gizlilik**

## **(Confidentiality)**

- Erişim denetim düzenekleri (Access control mechanisms) gizliliği desteklemektedir.
  - Kriptografi
    - Veriyi anlaşılmaz bir hale getirmek için karıştırmak
    - Gelir vergisi dokümanının şifrelenmesi (encipher)

# **Gizlilik**

## **(Confidentiality)**

- Sistem-bağımlı (System-dependent) düzenekler, bilgiye yasadışı erişimden işlemleri (process) engelleyebilmektedir.
  - Kriptografiden daha fazla verinin gizliliğini koruyabilirler.
  - Ancak, denetim başarısız olduğunda ya da atlandığında, sadece bu denetleme ile korunan veriler okunabilir bir duruma gelmektedir.

# **Gizlilik**

## **(Confidentiality)**

- Gizlilik, verinin varlığına (existence of data) da uygulanabilir.
  - ÖR: Güven oylaması sonuçları
- Bazı durumlara, erişim denetim düzenekleri korunması gereken başka bir bilginin ortaya çıkmasını önlemek için verinin varlığını saklamaktadır.

# Gizlilik (Confidentiality)

- Kaynağın gizlenmesi (Resource hiding)
  - Kaynağın saklanması gizliliğin bir diğer önemli unsurudur.
  - Kurumlar belirli donanımların diğerleri tarafından bilinmesini istemeyebilirler.
    - ÖR: Bir servis sağlayıcıdan hizmet alan bir şirket kullandığı kaynakların diğerleri tarafından bilinmesini istemeyebilirler.



**Erişim Denetim  
Düzenekleri**




**Yetkilendirilmemiş erişimler**



# Bütünlük (Integrity)

- Verinin ya da kaynağın güvenirliği
- Yetkilendirilmemiş ya da uygunsuz değişimin önlenmesi
- Bütünlük:
  - Veri bütünlüğü (Data integrity)
    - Bilginin içeriği
  - Köken bütünlüğü (Origin integrity)
    - Verinin kaynağı (aslıyla aynılığını kanıtlama olan ***authentication*** olarak da adlandırılmaktadır)

# Bütünlük (Integrity)

- Verinin kaynağı:
  - Doğruluk (Accuracy)
  - Güvenirlik (Credibility)
  - Güven (Trust)
- ÖR: Gazete haberi & Haber kaynağı
  - Veri bütünlüğü 
  - Kaynak  → Köken bütünlüğü 

# Bütünlük (Integrity)

- Bütünlük düzenekleri:
  - Önleme/Engelleme düzenekleri (Prevention mechanisms)
  - Tespit düzenekleri (Detection mechanisms)

# Önleme Düzenekleri

- Verinin bütünlüğünü;
    - veriyi değiştirmek isteyen yetkilendirilmemiş teşebbüsleri
    - ya da
    - veriyi yetkilendirilmemiş bir şekilde değiştirmek isteyen teşebbüsleri bloklayarak sağlamaktadır.
- Kullanıcının veriyi değiştirme hakkı bulunmadığı bir durumda veriyi değiştirmeye çalışması
- Veri üzerinde belirli değişiklikleri yapmaya hakkı olan bir kullanıcının değişikliği farklı yollar ile yapmaya çalışması

# Önleme Düzenekleri

- ÖR: Muhasebe sistemi
  - Sistemi kırıp veri üzerinde değişiklik yapmak:  
Yetkilendirilmemiş bir kullanıcı muhasebe veritabanının **bütünlüğünü** bozmaya çalışmaktadır.
  - Şirkette çalışan muhasebeci, zimmetine para geçiriyor & bunun için banka işlemlerini saklıyor:  
Muhasebeci muhasebe verisini **yetkilendirilmemiş** bir şekilde değiştirmeye çalışıyordur.

# Tespit Düzenekleri

- Bütünlük ihlallerini önlemeye çalışmaz.
- Verinin bütünlüğünün artık güvenilir (trustworthy) olmadığını bildirir.
- Problemleri tespit etmek için sistem olaylarını ya da verinin kendisini analiz eder.
- Bütünlük ihlaline neden olan gerçek nedeni (bir dosyanın belirli bir kısmının değiştiğini) ya da basitçe dosyanın artık bozulduğunu bildirir.

# Gizlilik vs Bütünlük

- Gizlilik → Verinin gizliliğinin ihlal edilip edilmediğini belirtir.
- Bütünlük → Verinin hem doğruluğunu (correctness) hem de güvenirliliğini (trustworthiness) içerir.
- Veri bütünlüğünün değerlendirilmesi:
  - Verinin kökeni
  - Verinin mevcut makineye gelmeden önce ne kadar iyi korunmuş olduğu
  - Verinin mevcut makine içerisinde ne kadar iyi korunduğu

# Gizlilik vs Bütünlük

- Bütünlüğün değerlendirilmesi çoğunlukla zordur.
- Bütünlük
  - Verinin kaynağı ile ilgili varsayımlara (assumption)
  - Kaynak ile ilgili güvene (trust) dayanmaktadır.



# Kullanılabilirlik (Availability)

- İstenen bilginin ya da kaynağın kullanılabilmesi durumudur.
- Güvenilirliğin (reliability) önemli bir unsurudur.
  - Kullanılamaz bir sistem mevcut olmayan bir sistem kadar kötüdür.
- Güvenlikte kullanılabilirlik:
  - Kişinin veriye veya sisteme erişimin kasten reddini ayarlayarak kullanılamaz bir hale getirmesidir.

# Kullanılabilirlik (Availability)

- ÖR: Bir banka sunucusunun gizliliğinin ihlal edilmesi sonucu saldırganın bütün ödemelerinin onaylanması.
- Servisin reddi (Denial of service, DoS) → Kullanılabilirliği engellemeye yönelik girişimler

# Tehditler (Threats)

- Güvenliğin ihlal edilmesidir.
- Tehdit olması için ihlalin gerçekten meydana gelmiş olması gerekmemektedir.
- İhlalin oluşabilecek olması → Buna neden olacak eylemlerin meydana gelmesine karşı hazırlıklı olmaktır.
  - Eylemler → **Saldırı** (Attack )
  - Eylemleri gerçekleştiren ya da olmasına neden olan → **Saldırgan** (Attacker)
- Tehditlere karşı korunma:
  - CIA

# Tehditler (Threats)

[Shirey] :

1. Açığa çıkarmak (disclosure) ya da bilgiye yetkilendirilmemiş erişim (unauthorized access)
2. Aldatma (deception) ya da hatalı verinin kabulü (acceptance of false data)
3. Bozulma (disruption) ya da kesme (interruption) ya da doğru işlemin engellenmesi (prevention of correct operation)
4. Gasp etme (usurpation) ya da bir sistemin bazı kısımlarında yetkilendirilmemiş denetim (unauthorized control of some part of a system)

# Tehditler (Threats)

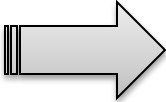
- Dinleme (Snooping)
  - Bilginin yetkilendirilmemiş bir şekilde ele geçirilmesidir.
  - Pasif
  - Bazı varlıkların iletişimi dinlediğini/okuduğunu ya da dosyalar arasında gezindiğini veya sistem bilgisini okuduğunu belirtir.
- Hatta girme/Hattı dinleme (Wiretapping)
  - Ağ izleme (Network monitoring)

**Confidentiality**

# Tehditler (Threats)

- Değişiklik (Modification/Alteration)
    - Bilginin yetkilendirilmemiş bir şekilde değiştirilmesidir.
    - 3 tehdit:
      - Aldatma (Deception) → Bazı durumlarda saldırgan değişikliğe uğramış verinin durumuna göre davranışı belirler.
      - Bozulma (Disruption)
      - Gasp etme (Usurpation)
- Değiştirilmiş veri sistemin işleyişini kontrol ediyorsa

# Tehditler (Threats)

- *Değişiklik (Modification/Alteration)*
  - Aktif  Saldırganın veriyi değiştirmesi
  - Aktif hat dinleme (Active wiretapping)
    - Man-in-the-middle attack → İzinsiz giren kişi (intruder), göndericinin gönderdiği mesajı okur ve alıcıya mesajın bir versiyonunu gönderir.

**Integrity**

# Tehditler (Threats)

- Taklit etme (Spoofing) / Maskeleye (Masquerading)
  - Bir varlığın diğer bir varlık tarafından taklit edilmesidir (impersonation).
  - Mağdur olan kişinin farklı bir varlık ile iletişimde olduğuna inanmasına neden olur.
  - ÖR:
    - İstenilenden farklı bir bilgisayara bağlanma
    - Farklı bir dosyaya yönlendirilme





# Tehditler (Threats)

- *Taklit etme (Spoofing) / Maskeleye (Masquerading)*
- Aktif → Saldırgan yetkili yönetici gibi hareket ederek bir sistemin denetimini gasp etmeye (usurpation) çalışmaktadır.

**Integrity**

# Tehditler (Threats)

- *Taklit etme (Spoofing) / Maskeleye (Masquerading)*
- Bazı maskeleye biçimlerine izin verilmektedir.
  - Yetkilendirme (Delegation)
    - Bütün taraflar yetkilendirmeden haberdardır.
- Güvenlik ihlali:
  - Maskeleye 
  - Yetkilendirme 

# Tehditler (Threats)

- Kökenin inkar edilmesi (Repudiation of origin)
  - Varlığın yarattığı ya da gönderdiği mesajın reddinin doğru olmamasıdır.
  - Aldatma (Deception) biçimidir.

# Tehditler (Threats)

- *Kökenin inkar edilmesi (Repudiation of origin)*
  1. Müşteri satıcıya bir ürün için yüklü miktarda para göndereceğine dair bir mesaj gönderir.
  2. Satıcı ürünü sipariş eder ve ödemeyi ister.
  3. Müşteri ürünü sipariş ettiğini inkar eder & ürün için ödeme yapmayı reddeder.
    - Müşteri mesajın kökenini inkar etmektedir.
    - Satıcı mesajın müşteriden geldiğini ispatlayamazsa → **saldırı başarılı**
- Bu saldırının bir başka biçimi, belirli bir bilgiyi ya da dosyayı yaratan kişinin bunu inkar etmesidir.

**Integrity**

# Tehditler (Threats)

- Alındının reddedilmesi (Denial of receipt)
  - Varlığın aldığı bilgiyi ya da mesajı aldığını reddetmesidir.
  - Aldatma (Deception) biçimidir.

# Tehditler (Threats)

- *Alındının reddedilmesi (Denial of receipt)*
  1. Müşteri pahalı bir ürünü sipariş eder.
  2. Satıcı ödemeyi ürünün sevkinden önce ister.
  3. Müşteri ödemeyi yapar ve satıcı ürünü gönderir.
  4. Müşteri satıcıya ürünün eline ne zaman geçeceğini sorar.
    - Ürün müşterinin eline zaten geçtiyse → Alındının reddedilmesi saldırısı

**Integrity & Availability**

# Tehditler (Threats)

- Gecikme (Delay)
  - Bir mesajın ya da servisin iletim süresinin ( $t$ ) geciktirilmesidir.
    - $t \uparrow \rightarrow$  *Saldırı başarılı*
  - Gasp etme (Usurpation) biçimidir, ancak aldatmayı da (Deception) destekler.

**Availability**

# Tehditler (Threats)

- Servis reddi (Denial of service)
  - Servisin uzun bir süre engellenmesidir.
  - Gasp etme (Usurpation) biçimidir.
  - Farklı düzenekler ile birlikte kullanılabilir.



# Tehditler (Threats)

- *Servis reddi (Denial of service)*
- Saldırgan sunucunun bir servisi sunmasına engel olur.
- Reddedilme:
  - Kaynakta (Source) → Sunucunun fonksiyonları
  - Hedefte (Destination) → Sunucudan gelen iletişimler
  - Yol (Path) üzerinde → İstemciden, sunucudan ya da her ikisinden gelen mesajlarda meydana gelebilir.

**Availability**

# Tehditler (Threats)

- *Denial of service* ya da *delay* doğrudan saldırılar sonucunda ya da güvenlik-dışı problemlerden meydana gelebilir.
- Etki-sonuç önemlidir.
  - Sistem güvenliğini tehlikeye düşürüyorsa ya da bir sistemi tehlikeye düşürecek olaylar zincirinin bir parçasıysa → Sistem güvenliğine yönelik bir teşebbüs/girişim
  - Kasten değilse → Saldırı yerine çevresel/ortamsal özelliklerin bir ürünü

# **Politika & Düzenek**

## **(Policy & Mechanism)**

- **Güvenlik Politikası (Security Policy)**
  - Neye izin verildiği neye izin verilmediği ile ilgili durumdur.
- **Güvenlik Düzenegi (Security Mechanism)**
  - Bir güvenlik politikasını uygulayan bir yöntem (method), araç (tool) ya da yordamdır (procedure).

# **Politika & Düzenek**

## **(Policy & Mechanism)**

- Düzenek teknik olmayabilir.
  - Şifre değiştirmeden önce kimlik doğrulaması yapmak
- Politikalar yordamsal düzeneklere ihtiyaç duymaktadır.
  - İzin verilenler (güvenli) ve izin verilmeyenler (güvenli olmayan) şeklinde temsil edilir.

# **Politika & Düzenek**

## **(Policy & Mechanism)**

- Üniversitenin bilgisayar lab'ında öğrencilerin birbirlerinin ödev dosyalarını kopyalamasını yasaklama → Politika
- Düzenek → Bir kullanıcının dosyalarının diğerleri tarafından okunmasını engelleyebilir.



# Politika & Düzenek (Policy & Mechanism)

Kişi ödevi kopyalamasa, fakat ödevi okumuş  
olsa bu bir güvenlik ihlali midir?

**Cevap, kurallara, yönetmeliklere ve  
kanunlara göre zamanla değişmektedir.**

# **Politika & Düzenek**

## **(Policy & Mechanism)**

- İki farklı taraf iletişim kuruyorsa ya da işbirliği yapıyorsa, onların meydana getirdiği varlık her ikisinin de güvenlik politikalarını temel alacaktır.
  - Bu politikalar tutarsız (inconsistent) → Taraflar oluşturdukları ürün için güvenlik politikasının ne olacağına karar vermelidir.

# Politika & Düzenek (Policy & Mechanism)

- Tescilli dokümanlarını üniversiteye veren bir kurumun politikası bir çok üniversitenin açık politikaları nedeni ile çelişki yaratacaktır.
  - Üniversite ve kurumun, tutarlı bir politikaya sahip olması için, ihtiyaçları doğrultusunda ortak bir güvenlik politikası belirlemesi gerekmektedir.
  - Üçüncü bir parti ile iletişim → Durumun karmaşıklığı daha hızlı artacaktır.



# Güvenlik Amaçları

- Güvenlik düzenekleri:

- Saldırıyı önleyebilir (prevent)
- Saldırıyı tespit edebilir (detect)
- Saldırıdan kurtarabilir (recover)



**Birlikte ya da  
ayrı ayrı  
kullanılabilir.**

# Güvenlik Amaçları

- Önleme (Prevention)
  - Saldırının başarısız olması
    1. Saldırgan bir makineye (host) saldırmak ister
    2. Makinenin internet bağlantısı yok
      - Saldırı önlenmiş olacaktır.
  - Doğru bir şekilde gerçekleştirilmiş ve değiştirilemez olan güvenilir düzenekler kullanıcılar tarafından değiştirilemez. → Saldırgan tarafından da değiştirilemez.

# Güvenlik Amaçları

- *Önleme (Prevention)*
- Kullanışsızdır
  - Sistem kullanımına engel olarak sistemin normal kullanımını aksatırlar.
- Basit önleme düzenekleri kabul görür
  - Yetkilendirilmemiş kullanıcıların sisteme erişimini engellemeyi amaçlayan şifreler

# Güvenlik Amaçları

- *Önleme (Prevention)*
- Sistemin riskli kısımlarını koruyabilir.
- Teoride, düzenek tarafından korunan kaynağın güvenlik problemleri nedeni ile izlenmesine (monitoring) gerek yoktur.

# Güvenlik Amaçları

- Tespit etme (Detection)
  - Saldırı önlenemediğinde kullanışlıdır.
  - Bir saldırının gerçekleşeceğini kabul etmektedir.
  - Amaç;
    - Saldırının devam etmekte olduğunu  
ya da
    - Bir saldırı olduğunu belirtmek  
ve bunu raporlamaktır.

# Güvenlik Amaçları

- *Tespit etme (Detection)*
- Sistemi izler, eylemleri ve saldırı niteliğindeki bilgiyi inceler.
  - ÖR: Sisteme üç defa yanlış şifre giren kullanıcı durumunda uyarı veren düzenektir.
    - Login işlemi devam edebilir, ancak sistem log'u fazla sayıda hatalı şifre girişi ile ilgili bir hata mesajı raporlar.

# Güvenlik Amaçları

- *Tespit etme (Detection)*
- Sistemin riskli kısımlarını korumaz.
- Tespit etme düzeneği tarafından korunan kaynak, güvenlik problemlerine karşı devamlı ya da periodik olarak izlenmektedir (monitored).

# Güvenlik Amaçları

- Kurtarma (Recovery)
  1. Saldıyı durdurmak ve saldırı nedeni ile meydana gelmiş zararları onarmak
  2. Saldırı sürerken sistem düzgün bir şekilde çalışmaya devam eder.



# Güvenlik Amaçları

- *Saldırıyı durdurmak ve saldırı nedeni ile meydana gelmiş zararları onarmak*
- ÖR: Saldırgan bir dosyayı silerse, kurtarma düzeneği dosyayı yedekleme ünitelerinden (backup tapes) geri yükleyebilir (restore).

# Güvenlik Amaçları

- *Saldırıyı durdurmak ve saldırı nedeni ile meydana gelmiş zararları onarmak*
- Sistemin çalışması saldırı tarafından engellenmiştir.
  - Kurtarma doğru işlemin sürdürülmesine/işlemin düzgün bir şekilde sürdürülmesine ihtiyaç duyar. (Sistemin tekrar ayaklanması)

# Güvenlik Amaçları

- *Saldırıyı durdurmak ve saldırı nedeni ile meydana gelmiş zararları onarmak*
- Pratikte, saldırıların özgün (unique) yapısından dolayı:
  - Kurtarma daha karmaşıktır.
    - Herhangi bir zararın türünü ve boyutunu/büyükliğini tamamen tanımlamak zordur.
    - Saldırgan geri dönebilir
      - Sisteme girmek için kullanılan savunmasız noktaların onarılmasını gerekir.

# Güvenlik Amaçları

- *Saldırıyı durdurmak ve saldırı nedeni ile meydana gelmiş zararları onarmak*
  - Bazı durumlarda;
    - misilleme (retailation) → saldırganın sistemine saldırma ya da saldırganı sorumlu tutmak için yasal adımlar atma
- kurtarmanın bir parçası olabilir.

# Güvenlik Amaçları

- *Saldırı sürerken sistem düzgün bir şekilde çalışmaya devam eder.*
- Bilgisayar sistemlerinin karmaşıklığı nedeni ile zordur.
- Güvenliği kritik sistemler (safety-critical system) için olan **fault-tolerance** teknikleri ve güvenlik teknikleri gerektirir.

# Güvenlik Amaçları

- *Saldırı sürerken sistem düzgün bir şekilde çalışmaya devam eder.*
- Birinci maddedeki kurtarma biçiminden farklıdır.
  - **Hiçbir aşamasında sistem hatalı bir şekilde çalışmaz.**
  - Gereksiz fonksiyonelliği (functionality) hizmet dışı bırakabilir.
    - Sistem düzgün olmayan işleyiş tespit ettiğinde ve daha sonra hatayı düzelttiğinde ya da düzeltmeye teşebbüs ettiğinde, çoğunlukla daha zayıf bir biçimde uygulanmaktadır.

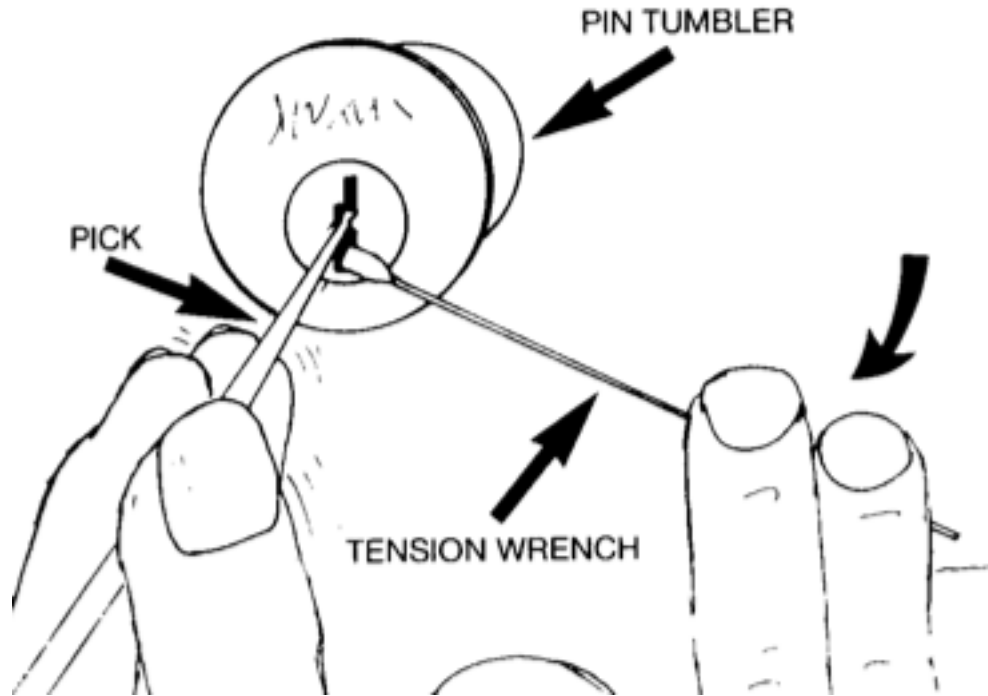
# **Varsayım & Güven**

## **(Assumption & Trust)**

- Politikanın istenilen güvenlik düzeyini ve türünü doğru bir şekilde tanımladığını nasıl belirleyebiliriz?
- Güvenlik, ihtiyaç duyulan güvenlik türüne özel varsayımlara ve güvenliğin uygulanacağı ortama dayanmaktadır.

# Varsayım & Güven (Assumption & Trust)



- Kapı kilidi → Anahtar



Varsayım: **Kilidin kırılmaya karşı güvende olduğu**



# Varsayım & Güven (Assumption & Trust)

- Anahtarı açacak olan güvenilir
  - Yetki verilmediği sürece kilidi açmaz.
  - Varsayım geçerli 
- Anahtarı açacak olan güvenilir değil
  - Varsayım geçersiz 

Varsayım: **Kilidin kırılmaya karşı güvende olduğu**

# Varsayım & Güven (Assumption & Trust)

- Güven, arka kapının (backdoor) kullanılmayacağı inancına dayanır.
- Arka kapı kullanılırsa;
  - Güven yanlış kullanılmış olacak
  - Güvenlik düzeneği **[kilit]** herhangi bir güvenlik sağlamayacak

# Varsayım & Güven (Assumption & Trust)

- Politika uygulanabilir bir aksiyom kümesinden oluşur.

– İki varsayım:

1. Politika doğru ve belirli bir şekilde sistem durumları kümesini “güvenli (secure)” ve “güvensiz (nonsecure)” durumlarına ayırır.
2. Güvenlik düzenekleri, sistemin “güvensiz” duruma girmesini önler.



**Sistem güvensiz!**

# **Varsayım & Güven**

## **(Assumption & Trust)**

- Her iki varsayım birbirinden farklıdır.
- ÖR: Banka çalışanları hesaplar arası para değişimi yapmaya yetkilidir.

Banka çalışanı hesabına \$100.000 aktarırsa,  
banka güvenliği ihlal edilmiş olur mu?



# Varsayım & Güven

## (Assumption & Trust)

- *Politika doğru ve belirli bir şekilde sistem durumları kümesini “güvenli (secure)” ve “güvensiz (nonsecure)” durumlarına ayırır.*
  - Politikanın, güvenli bir sistemi belirtenlerin doğru bir tanımı olduğunu belirtir.
- *Güvenlik düzenekleri, sistemin “güvensiz” duruma girmesini önler.*
  - Güvenlik politikasının güvenlik düzenekleri tarafından uygulanabileceğini belirtmektedir.

# **Varsayım & Güven**

## **(Assumption & Trust)**

- Çalışan düzeneğe güvenilmesi için varsayımlar:
  1. Her bir düzenek, güvenlik politikasının bir ya da daha fazla kısmını gerçekleştirmek (implement) için tasarlanmaktadır.
  2. Düzeneklerin birleşimi, güvenlik politikasının bütün yönlerini (aspects) gerçekleştirir.
  3. Düzenekler doğru bir şekilde gerçekleştirilmektedir.
  4. Düzenekler doğru bir şekilde kurulmuş (installed) ve yönetilmektedir (administrated).

# Güvence (Assurance)

- Güven tam olarak ölçülemez.
- Bir sisteme ne kadar güvenileceği → Sistem tanımı, tasarım ve uygulama



Güvence



Kişinin sisteme ne kadar güveneceği

# Güvence (Assurance)

- Mühürlenmiş ilaçlara olan güvenin temelleri:
  1. **Sertifikasyon:** FDA (Food and Drug Administration) tarafından verilen ilacın testi ve sertifikasyonu
  2. **Üretici Standartları:** Firmanın üretim standartları ve ilacın bozulmadığını ya da kirlenmediğini garantileyen önlemler
  3. **Güvenlik Mührü:** Kutunun üzerindeki güvenlik mührü



# Güvence (Assurance)

- Güvence dünya genelinde benzerdir.
- Bilgisayarın doğru bir şekilde işlediğini garantileyen adımlara ihtiyaç duyulur:
  1. İstenilen veya istenmeyen davranışın ayrıntılılandırılmış belirtimi (specification)
  2. Donanım ve yazılım tasarımının analizi, ve sistemin belirtilen belirtimi ihlal etmeyeceğini gösteren diğer bileşenler
  3. Uygulamanın, çalışma yordamlarının ve bakım yordamlarının istenilen davranışı ortaya koyacağını belirten argümanlar ve kanıtlar

# Güvence (Assurance)

- Eğer belirtim (specification) doğru bir şekilde sistemin nasıl çalışacağını belirtiyorsa, o zaman bir sistemin belirtimi yerine getirdiği söylenebilir.



Belirtimi yerine getiren tasarım ve uygulamaya da uygulanmaktadır.

# Belirtim (Specification)

- Sistemin istenilen işlevinin **formal**
    - Matematiksel
    - Bu amaç için geliştirilmiş diller
  - ya da **informal**
    - Belirli durumlarda sistemin ne yapması gerektiğini belirten açıklama (İngilizce , Türkçe, vs..)
- durum**udur.


# Belirtim (Specification)

- Tanımlama, sistemin neyi yapabileceği ya da neyin yapılmasına izin verilmediği ile ilgili durumun belirtimidir.
  - Yeni bir bilgisayar alan firmanın informal açıklaması:
    - *“Sisteme internet üzerinden saldırılamaz.”*

# Belirtim (Specification)

- Belirtilimler sadece güvenlik için değil, aynı zamanda güvenlik için tasarlanmış sistemlerde de kullanılmaktadır.
  - Medikal teknolojiler
  - Trafik ışıkları
    - “Aynı anda **kırmızı** ve **yeşil** yanamaz.”

# Tasarım (Design)

- Belirtilimleri onları gerçekleştirecek olan bileşenlere dönüştürmektedir.
  - Tasarım, eğer bütün ilgili durumlar altında, **sistemin belirtilimleri ihlal etmesine izin vermiyorsa**; bu durumda **tasarım belirtilimleri sağlıyor** denmektedir.
    - Modem
    - Ağ kartı
-  ***Sisteme internet üzerinden saldırılamaz.***

# Tasarım (Design)

- Analist, tasarımın belirtileri sağlayıp sağlamadığını belirleyebilir:
  - Belirtiler ve tasarım matematiksel ifadeler ile açıklanmış → analist tasarım formüllerinin belirtiler ile tutarlı olduğunu mutlaka göstermelidir.
  - Belirtiler ve tasarım matematik kullanmıyor → ikna edici ve zorlayıcı argümanların yapılmış olması gerekir.

# Gerçekleştirim (Implementation)

- Verilen tasarımı sağlayan/karşılayan bir sistem yaratır.
- **Tasarım belirtileri sağlıyor** → geçişlilik (transitivity) özelliğine göre aynı zamanda **gerçekleştirim de belirtileri sağlamaktadır.**
- Problem → Bir programın tasarımı ve belirtileri doğru bir şekilde gerçekleştirdiğinin kanıtlanmasının karmaşıklığı.





# Gerçekleştirim (Implementation)



- Bir programın gerçekleştirimi belirtilen şekilde uygulanıyorsa bu program doğrudur.
- Doğruluğun kanıtı → Kaynak kodun her bir satırının matematiksel doğruluğunun kontrol edilmesidir.
  - Her bir satır → Bir fonksiyon
  - Fonksiyonların bileşimi → Yordam (Routine)
  - Yordamların bileşimi → Program

**Sistemin  
doğruluğu**

# Gerçekleştirim (Implementation)

- Süreçteki zorluklar:
  1. Programların karmaşıklığı → Matematiksel olarak doğrulamayı zorlaştırmaktadır.
  2. Programın doğruluğunun kanıtlanması, programların doğru bir şekilde derlendiğini, yüklendiğini ve yürütüldüğünü kabul eder.
    - Donanımsal hataları, koddaki bugları ve diğer araçların neden olabileceği hatalar girdileri (inputs) geçersiz kılabilir.
  3. Eğer doğrulama, girdinin koşulunu (condition) temel alıyorsa, program koşulları sağlamayan girdileri geri çevirmelidir.

# Gerçekleştirim (Implementation)

- Doğruluk kanıtlama → zaman alıcı 
- Test 
  - Test yordamları
  - Dokümantasyon
- Programı ya da programın bir parçasını veri üzerinde yürütme:
  - Çıktının olması gereken olup olmadığı
  - Programın bir hata içermesinin ne kadar muhtemel olduğunu anlamak

# Gerçekleştirim (Implementation)

- Test teknikleri:
  - Girdileri verilmiş bütün yürütme yollarının **programda oluşabilecek hatalara karşı test edildiğinin kontrol edilmesi** ve belirtileri sağlayan **çıktıları nasıl etkiledikleri**
  - Programın **belirtileri sağlayıp sağlamadığının** test edilmesi
- Biçimsel metotlarla aynı derecede güvence sağlamamaktadır.
  - Güvence teknikleri güvenliği ya da doğruluğu **garantilemese de**, kişinin sistemin **güvenilir olduğuna güvenmesi** için bir temel sağlar.

# İşlemsel Sorunlar (Operational Issues)

- Politika ve düzenek, korunmanın faydalarını; tasarım, gerçekleştirim ve düzeneğin kullanım maliyetine karşı dengelemelidir.
- Bu denge;
  - Güvenlik ihlalinin risklerinin analizi
  - Güvenlik ihlalinin gerçekleşmesi ihtimali ile belirlenebilir.
- Böyle bir analiz sübjektiftir.
  - Riskler, sadece **çok az** durumda **kesin olarak ölçülebilir**.

# Maliyet-Fayda Analizi (Cost-Benefit Analysis)

- Bilgisayar güvenliğinin faydaları toplam maliyete göre değerlendirilmektedir.
  - Sistemin **gizliliği ihlal edilirse meydana gelecek ek maliyet** de buna dahildir.

# Maliyet-Fayda Analizi

## (Cost-Benefit Analysis)

- Eğer veri ya da kaynakların maliyeti korunmalarından daha az maliyetli ise;
  - Güvenlik düzeneklerinin ve yordamlarının eklenmesi **uygun maliyetli** (cost-effective) olmayacaktır.

Çünkü

Veri ya da kaynak korunmanın maliyetinden **daha ucuz** bir şekilde yeniden düzenlenebilir.

# Maliyet-Fayda Analizi (Cost-Benefit Analysis)

- Maaş bilgilerini tutan veritabanında değişiklik yapılması.
  - Şirketin finansal kaybı
  - Maliyet-Fayda analizi



**Integrity**



# Maliyet-Fayda Analizi (Cost-Benefit Analysis)



# Maliyet-Fayda Analizi (Cost-Benefit Analysis)

- Analiz **her zaman** kesin olmayabilir.
- Veritabanında gizliliğin ihlali:
  - Maaş bilgilerinin ortaya çıkması
- Şirketin finansal kaybı:
  - Davalar
  - Politikalar, yordamlar ve personelde değişiklik
  - Gelecek iş hayatına olan etkiler

# Maliyet-Fayda Analizi

## (Cost-Benefit Analysis)

- Birbiri ile örtüşen faydalar da dikkate alınmalıdır.
- ÖR: Bütünlük düzenekleri, gizliliğin sağlanması için kolaylıkla ve ucuz bir şekilde arttırılabiliyorsa:
  - Gizliliğin sağlanmasının maliyeti düşecektir.
- Belirli bir güvenlik servisinin maliyeti
  - seçilen düzeneğeve
  - diğer güvenlik servislerini gerçekleştirecek düzenekleregöre değerlendirildiğini göstermektedir.

# Maliyet-Fayda Analizi

## (Cost-Benefit Analysis)

- Maliyet-fayda analizi, olabildiğince çok düzeneği göz önünde bulundurmalıdır.
- Mevcut bir sisteme güvenlik düzeneklerinin eklenmesi, çoğunlukla sistem ilk tasarlanırken eklenmesine göre **daha pahalı** ve **daha az etkili** olmaktadır.

# Risk Analizi (Risk Analysis)

- Bir varlığın korunup korunmayacağının belirlenmesi
- Hangi derecede korunacağının belirlenmesi



Olası tehditlerin analizini gerektirir.

# Risk Analizi

## (Risk Analysis)

- Korumanın derecesi:
  - saldırının **gerçekleşmesinin olasılığı**ve
  - bu saldırının **başarılı olmasının etkilerinin** bir fonksiyonudur.

# Risk Analizi

## (Risk Analysis)

- Saldırının **gerçekleşmesi olasılığı düşükse**;
  - Bu saldırıya karşı **korunmanın önceliği**, gerçekleşme olasılığı yüksek olan bir saldırıya göre **daha düşüktür**.

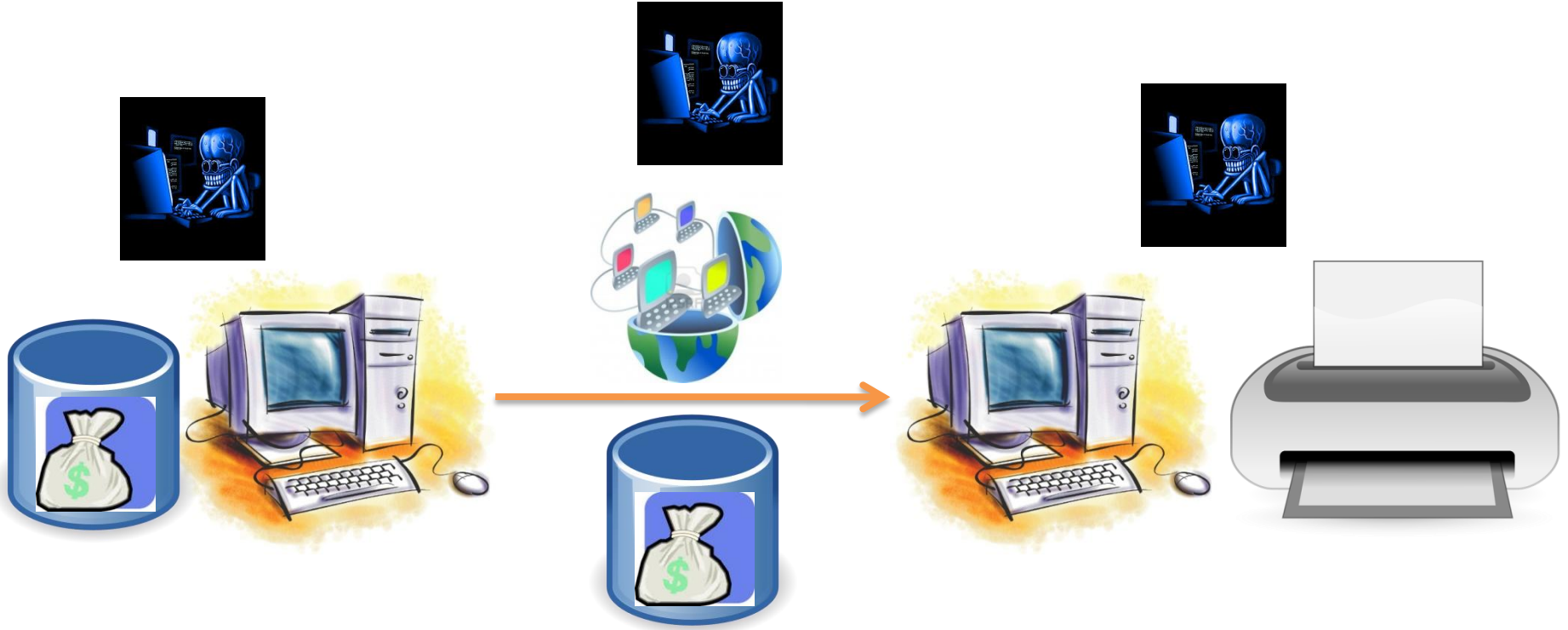
# Risk Analizi

## (Risk Analysis)

- Gerçekleşme olasılığı düşük olan saldırı, şirketin üretiminde gecikmeye neden olacaksa ve gerçekleşmesi ihtimali daha yüksek olan saldırının bir zararı olmayacaksa;
  - Gerçekleşme ihtimali düşük olan saldırının önlenmesine daha çok çalışılmalıdır.



# Risk Analizi (Risk Analysis)



- Ağ şirket içinde yerel bir ağ → Güvenilir olmayan şirket personeli
- Ağın internet bağlantısı var → Dışarıdan gelecek saldırı riski dikkate alınmalıdır.

# Risk Analizi

## (Risk Analysis)

- **Risk ortamın bir fonksiyonudur.**
- Şirketin işlerlik gösterdiği ortamda ortaya çıkmaktadır.
  - Bilgisayarın internet bağlantısı olmadığında → Dış dünyadaki saldırganlar şirket için bir tehdit olmayacaktır.
    - Eğer dış dünyadaki saldırganlar sisteme girmek isterlerse fiziksel olarak şirkete girmek zorundadırlar → Yerel
  - Bilgisayar internete bağlıysa → Dış dünyadaki saldırganlar artık bir tehdittir.
    - İnternet üzerinden saldırabilirler.
  - Şirket içerisinde ki bağlılık
    - Ödenmeyen maaşlar → Çalışanlar → Davalar → Yatırımcılar

# Risk Analizi

## (Risk Analysis)

- **Risk zamanla değişir.**
- Şirket ağı internete bağlı değil → İnternetteki diğer sistemlerden saldırı konusunda herhangi bir risk görünmemektedir.
  - Ancak, politikaların tersine, herhangi biri modem aracılığı ile internete bağlanabilir. → **Risk analizi geçerli değildir.**
  - Politikalar ile modem bağlantısı yasaklanabilir.
    - Modem ile böyle bir bağlantı gerçekleştirilemeyeceği garantilenmediği sürece **risk değişebilir.**

# Risk Analizi

## (Risk Analysis)

- **Bir çok risk uzak olsa bile mevcuttur.**
- Şirket internet bağlantısı riskini azaltmayı deneyebilir.
- Risk *mümkündür* ancak *yok değildir*.

# **Risk Analizi**

## **(Risk Analysis)**

- Analizin felç olması (Analysis paralysis)
  1. Şirket bir risk analizi gerçekleştirir.
  2. Yöneticiler bütün risklerin tespit edildiğinden emin değillerdir.
  3. Birinciyi doğrulayacak ikinci bir çalışma talep ederler.
  4. Bu çalışmaları karşılaştırıp, bu analizler üzerine eyleme geçmek için beklerler.
  5. Bu sırada, güvenlik kısmında çalışanlar işyerindeki durumların artık orijinal risk analizinin yapıldığı durumlardan farklı olduğunu belirtirler.
  6. Analiz tekrar edilir.
  7. Şirket, riskleri nasıl iyileştireceğine karar veremez ve bir eylem planı gerçekleştirilene kadar bekler.
  8. Süreç devam eder.

# Kanunlar (Laws)

- Kanunlar;
  - Teknolojinin kullanımını ve kullanılabilirliğini kısıtlamaktadır.
  - Yordamsal kontrolleri etkilemektedir.
- Bu nedenle, herhangi bir politika ve düzenek yasal faktörleri dikkate almalıdır.

# Kanunlar (Laws)

- 2000'li yıllara kadar A.B.D şifrelenmiş donanım ve yazılımın ihracatını kontrol etmiştir.
- **ÖR:** Bir Amerikan şirketi Londra'daki bir bilgisayar üreticisi ile çalışıyorsa, bu üreticiye şifrelenmiş yazılım gönderememektedir.
  - Amerikan şirketi öncelikle yazılımın ihraç edilmesi için gerekli lisansa sahip olmalıdır.
- Günümüzde, bu kanun esnetilmiş ve bazı ufak kısıtlamalar getirilmiştir.

# Kanunlar (Laws)

- 1990'larda, Fransa'daki kanun → Şifrelenmiş veri gönderilirken, şifre anahtarının hükümete kaydettirilmesini talep etmektedir.
- Fransa'da ki şirkete şifrelenmiş dosya gönderecek farklı bir ülkede bulunan şirketin bu durumu göz önüne alması gerekmektedir.
- Google → Export controls on encryption



# Kanunlar (Laws)

- Kullanıcının izini olmadan dosyasının okunmasını yasaklayan bir kanunda:
  1. Saldırgan sistemi kırar ve kullanıcının dosyalarını indirir.
  2. Sistem yöneticisi bunu fark eder ve saldırganın dosyayı okuduğunu gözlemler → Kişinin dosyalarını izini olmadan okumuş ve kanunları ihlal etmiş olacak.

# Kanunlar (Laws)

- Bir çok site, kullanıcılarının sistem yöneticilerinin dosyalarını okumalarına izin vermelerini talep eder.
- Bazı durumlarda;
  - servis kalitesinin korunması
  - sisteme herhangi bir zarar verilmesinin önlenmesi için sistem yöneticilerinin sistemdeki bilgiye erişimine açık bir şekilde izin verilmektedir.

# Kanunlar (Laws)

- Politikalar ve düzeneklerdeki tek kısıt kanunlar değildir.
- Toplumlarda da genel kuralları olabilir:
  - Yasal ve kabul edilebilir uygulamalar arasında ayırım yapılabilir.
  - **ÖR:**  
DNA örneği alımı  
Şifre → Kimlik numarası

Yasal 

Toplum tarafından kabul edilemez.

# Kanunlar (Laws)

- Kanunlar ve gelenekler psikolojik bir kabul edilebilirlik oluşturmaktadır.
- Kullanıcıları ve sistem yöneticilerini yasal risklerle karşı karşıya bırakan bir güvenlik düzeneği, bu kişiler üzerine sorumluluk yüklemektedir.

# İnsan Sorunları (Human Issues)

- Bilgisayar güvenliği kontrollerinin geliştirimi karmaşıktır.
- Büyük bir organizasyon içinde yordamsal kontroller çoğunlukla **belirsiz** ya da **kullanışsız** olabilmektedir.
- Teknik kontrollere bakılmaksızın, **teknik olmayan faktörler** güvenlik kontrollerinin geliştirimini ve kullanımını etkiler.
  - Bunun güvenliğe etkisi ciddi olabilir.

# İnsan Sorunları (Human Issues)

- Konfigürasyon ya da kullanım doğru şekilde gerçekleştirilmezse;
    - en iyi güvenlik kontrolü
      - en iyi ihtimalle **yararsız**
      - en kötü ihtimalle **tehlikeli**
- olacaktır.

# İnsan Sorunları (Human Issues)

- Güvenlik kontrollerini;
  - tasarlayanlar (designers)
  - geliştiriciler (implementers)
  - bakımını gerçekleştirenler (maintainers)

bu kontrollerin doğru bir şekilde işleyebilmesi için en temel gereksinimlerdir.

# Organizasyon Problemleri (Organizational Problems)

- Güvenlik:
  - Kullanıcıya direkt bir finansal ödül sağlamaz.
  - Kayıpları kısıtlar.
  - Kaynaklar için ek masraflara ihtiyaç duyar.




# Organizasyon Problemleri (Organizational Problems)

- Organizasyonlar;
  - Kayıplar meydana gelene kadar güvenlik ile ilgili **boşa harcama** yaptıklarına inanırlar.
  - Güvenlik kontrollerin **değerleri kayıptan sonra takdir edilir.**



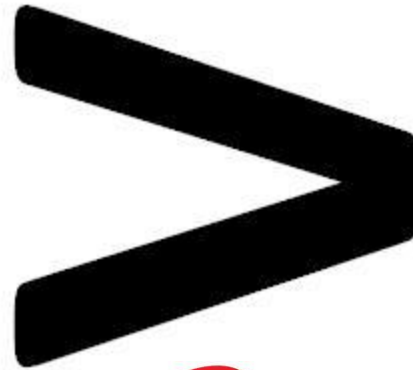
# Organizasyon Problemleri (Organizational Problems)

- Güvenlik kontrolleri çoğunlukla basit olan işlemlere karmaşıklık kazandırmaktadır.
  - **ÖR:** Stok kontrolü
    - Güvenlik kontrolsüz → 2 dk.
    - Güvenlik kontrolü ile → 3 dk.
- 
- 50%  
Verimlilik  
kaybı

# Organizasyon Problemleri (Organizational Problems)

- Güvenlik uygulanırken **kayıplar** yaşanacaktır.
  - Bu kayıpların güvenlik düzenekleri olmadığından yaşanacak kayıplardan az olması beklenir.

Güvenlik uygulanırken  
yaşanan kayıp  
+  
Verimlilikte meydana  
gelen kayıp



Güvenli olmayan  
işlemin finansal  
kayıbı



# Organizasyon Problemleri (Organizational Problems)



Şirketlerde bilgisayar sorunlarından kim sorumludur?

**Gerçekleştirim *gücü* sorumlu olan  
kişide olmalıdır.**



Sorumluluksuz Güç = Güçsüz Sorumluluk

**Problem**

# Organizasyon Problemleri (Organizational Problems)

- Problemler:
  1. Bilgisayar güvenliği alanında **eğitim almış kişilerin eksikliği**
  2. Güvenlik konusunda eğitilmiş kişilerin **iş yükünün fazlalığı**
  3. Güvenlik yöneticisinin sistem yönetimi, yazılım geliştirim ve diğer **ikincil işlevlerde de görev alması**
    - İşin güvenlik boyutunun ikincil olarak görülmesi

# Organizasyon Problemleri (Organizational Problems)

- Güvenlik problemleri çoğunlukla belirgin değildir.
- Güvenlik problemlerini fark etmek:

– Zaman

ve

– Beceri

gerektirir.



# Organizasyon Problemleri (Organizational Problems)

Güvenliđi ikincil iş olarak görmek

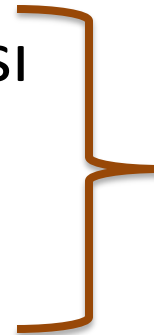


Beklenen işin başarısız olması



# Organizasyon Problemleri (Organizational Problems)

- Kaynak yetersizliği
  - Sistemin güvenilirliğinin sağlanması için kaynağa gerek duyulmaktadır.
- **Zaman ihtiyacı**
  - Konfigürasyonun tasarlanması
  - Gerçekleştirim
  - Sistemin yönetilebilmesi





# Organizasyon Problemleri (Organizational Problems)

- **Para ihtiyacı**

- Güvenlik sistemlerinin kurulması için gerekli olan ürünlerin alımı
- Tasarım için belirli bir ücret ödenmesi
- Güvenlik ölçümlerinin gerçekleştirimi



# Organizasyon Problemleri (Organizational Problems)

- **Bilgisayar kaynakları ihtiyacı**
  - Güvenlik düzeneklerinin  
ve
  - Yordamlarının  
gerçekleştirimi ve yürütülmesi



# Organizasyon Problemleri (Organizational Problems)

- **Eğitim ihtiyacı**
- Personelin eğitimi:
  - Güvenlik araçlarının kullanımı
  - Sonuçların değerlendirilmesi
  - Güvenlik politikalarının gerçekleştirimi



# İnsan Kaynaklı Problemler

- İnsanlar → Güvenlik sistemlerinin kalbi
- Bilgisayar güvenliğinde → Teknolojik kontroller
- ÖR:
  - Yetkilendirilmiş kullanıcı → Kullanıcının şifre ile sisteme girmesi
  - Kullanıcının şifresini yetkilendirilmemiş birine vermesi → Masquerading

# İnsan Kaynaklı Problemler

- Yabancı (Outsider) → Bir kuruma saldırımayı düşünen ve kurumun sistemini kullanmaya yetkisi olmayan kişi
  - Sistem için ciddi bir tehdit oluşturur.
- Daha büyük tehlike:
  - Kurumun hoşnutsuz elemanlarından
  - Sistemi kullanmaya yetkisi olan kurum içindeki diğer kişilerden (intruders) gelir.



# İnsan Kaynaklı Problemler

- Insider:
  - Şirket sistemlerinin **organizasyonunu**
  - Kullanıcıların ve operatörlerin hangi **yordamları** takip ettiğini
  - Dışarıdan gelecek saldırıyı tespit edecek güvenlik kontrollerini geçmek için gerekli **şifreleri** bilmektedirler.
- Şirket içi elemanlardan kaynaklanan **yetkilendirmenin yanlış kullanımı** çözümü zor bir problemdir.

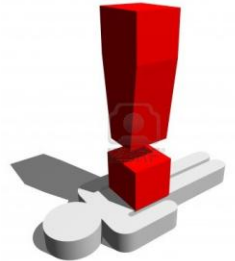


# İnsan Kaynaklı Problemler

- Sistem güvenliği için tehdit → Eğitilmemiş personel
- ÖR: Yedekleme ünitelerinin (backup tapes) saklanmadan önce doğrulanması gerektiğini bilmeyen bir operatör.
  1. Sistem saldırıya uğrar
  2. Dosyalar silinir



Yedekleme  
üniteleri  
okunamaz



# İnsan Kaynaklı Problemler

- Güvenliği zayıflatan unsurlar:
  1. Güvenlik düzeneklerinin **çıktılarını yanlış okuyan ya da analiz edemeyen** güvenlik yöneticisi
  2. Sistemin güvenlik ile ilgili özelliklerini **yanlış yapılandıran** sistem yöneticisi
  3. Güvenlik düzeneklerini **yanlış kullanan** kullanıcılar

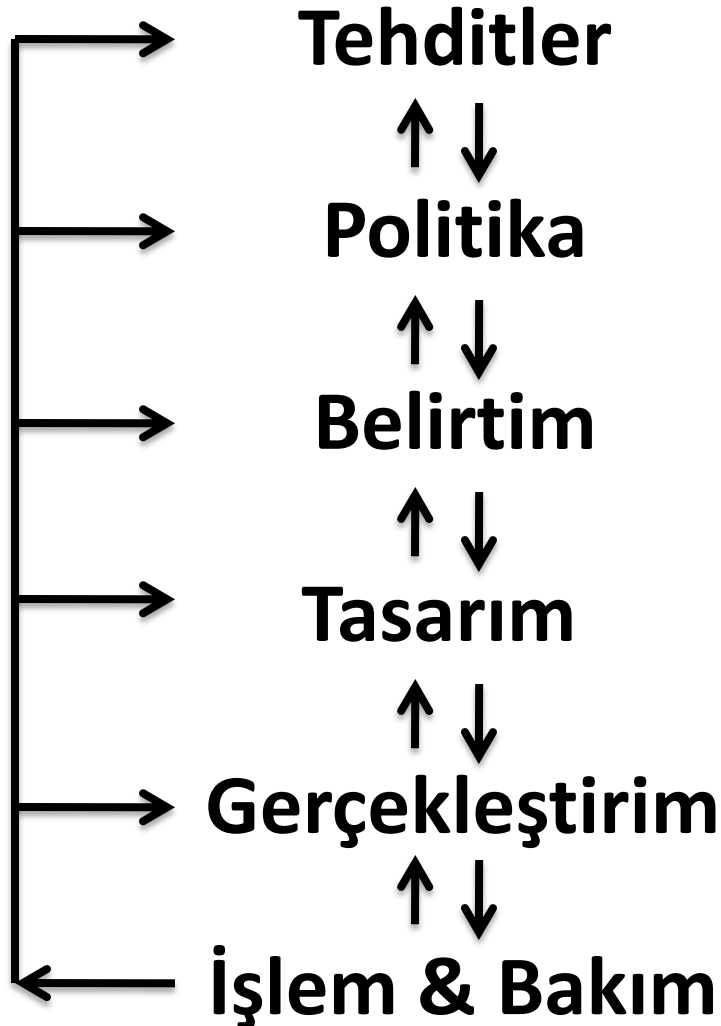


# İnsan Kaynaklı Problemler

- Saldırılar her zaman teknik değildir → Toplum Mühendisliği (Social Engineering) saldırıları
  - Önemli ölçüde başarılı & tahrip edici
- ÖR: Operatörün telefonda şifre değiştirmesi



# Güvenlik Yaşam Döngüsü



- Her bir aşama önceki ve bu aşama boyunca bütün önceki aşamalara bir geribildirim sağlar.
- Geribildirim için Denetleme (Auditing) kullanılır.
  - Sistemin işleyişi ve analizi kaydedilir. → Analist problemleri belirler.