

# I. Bilgi Güvenliğine Giriş

## I.I Tanımlar

### Güvenlik

Güvenlik terimi çeşitli değerlerin tehditlere ve saldırılara karşı korunmasını ifade eder. Güvenlik soyut bir kavram olmamakla birlikte, her gün karşımıza çıkan bir konudur. Örnek vermek için, bir üniversite öğrencisi olan Ali'nin sabah yaptığı işlere göz gezdirelim, ve güvenlikle ilgili etkinliklerini inceleyelim:

1. Ali evi terketmeden önce kapısını kilitler.
2. Güvenlik personeli kampüs nizamiyesinde Ali'nin öğrenci kimliğini kontrol eder.
3. Ali banka kartından para çekmek için bir ATM makinesine gider.
4. Son olarak, Ali ders notlarını okumaya başlamadan önce bilgisayarını parolası ile açar.

Ali gibi, günlük telaşımız içerisinde, pek çok güvenlik ile alakalı karar veriyoruz. Pek çoğumuz bunlar hakkında pek düşünmüyor bile. Bu kararlar gerçekten gerekli mi? Yeterli önlem alıyor muyuz? Bu ders güvenlik hakkında eleştirel bir bakış açısı getirecek olsa da, kapsamı bir altalan ile sınırlıdır.

Kabaca, güvenlik ile alakalı iki ana konu belirleyebiliriz:

1. Fiziksel Güvenlik
2. Dijital Güvenlik

Fiziksel güvenlik "somut" değerleri korumak içindir. Son zamanlarda gelişmiş bir ihtiyaç değildir, insanlığın başından bu yana vardır. Fiziksel güvenlik hakkında fazlaca tartışmayacağız, fakat iki güvenlik alanındaki bazı temel prensiplerin ortak olduğunu ve güvenlik amaçlarımıza ulaşabilmek için iki alandan da faydalanmamız gerekebileceğini göreceğiz.

### Bilgi Güvenliği

Dersin adından da anlaşılacağı üzere, ana odağımız bilginin dijital formatta olduğu bilgi güvenliği olacak. Bilgi ve iletişim teknolojilerindeki gelişmeler ile, "bilgi" sahip olduğumuz en önemli değer oldu. Değeri arttıkça, artan saldırılar ve tehditler ile "bilgi güvenliği" konusuna olan ilgi de arttı.

Tartışmalarımız şunları kapsayacak

1. bilginin kapalı bilgisayar sistemlerindeki işlenmesi ve saklanması (bilgisayar güvenliği)
2. bilginin bağlı sistemler üzerinden transferi (ağ güvenliği)

İnternetin uluslararası bağlantılılığının getirdikleri sayesinde, bu iki durumun birbirine karıştığını ve ayrımlarının net yapılamadığını da unutmamak gerekmektedir.

## Güvenlik ve Emniyet

Güvenlik ve emniyet kavramları arasında ince fakat önemli bir fark vardır. Güvenlikte, odak bilinçli olarak yapılan saldırıların üzerindeyken, istatistiksel hatalar veya kaza eseri meydana gelen davranışlar emniyet ile alakalıdır (veya hata toleransı).

## Güvenlik Neden Zordur?

Farklı görüş açılarından bakarak, bu önemli soruya detaylı bir cevap verebiliriz:

1. Bilgi teknolojilerinin çoğunluğu istenilen davranışı elde etmekle uğraşır. Diğer taraftan, güvenlik istenilmeyen davranışı engellemek ister. Bir şeyin ne yaptığını belirtmek ne yapmadığını belirtmekten çok daha kolaydır. Fonksiyonellik açısından, istenilmeyen bir fonksiyonellikte bir problem yoktur, fakat konu güvenlik olduğunda bu ciddi bir problemdir, zira saldırı yapanlara kötü şeyler yapabilmeleri için açık kapı bırakmaktadır.
2. Eğer bunu emniyetin diğer kolları ile karşılaştırırsak, güvenlik ile ilgili sağlam bir tanımımız olmadığı açığa anlaşılacaktır. Diğer taraftan, olasılık emniyet konularında formalizm sağlayan, güvenli bir temeli bulunan bir araçtır. Mesela bir uçağı düşünün, havada kalmak için bir motora ihtiyaç duyar. Bir motorun bozulma ihtimalini, ve uçak için izin verilen en yüksek hata payını göz önünde bulundurursak, bir uçakta kaç motora ihtiyacımız olduğunu hesaplayabiliriz. Güvenlik için benzer bir hesaplama yapabilir miyiz? Artıklık güvenlik için uygun bir teknik midir? Olasılık modellemesi mümkün müdür? Bu soruların hepsinin ucu açıktır.
3. Diğer mühendislik dalları gibi, gereklilik analizi güvenlik için en fazla öneme sahiptir. Fakat güvenlik gereksinimleri belirlemek kolay bir iş değildir, zira kullanıcıların çoğunlukla güvenlik tecrübesi olmadığından veya güvenlik nedir bilmediklerinden güvenlik gereksinimleri de belirli değildir.
4. Bir sistem birleşik bir tümü içeren birbiriyle ilgili elemanların toplamıdır. Sistemler tekil makinelerden ayırt edilebilmektedirler, örn. makara bir makinedir, fakat bir asansör makaraları da içeren pek çok bileşeni içeren bir sistemdir. Bir bilgi sistemi genel olarak bilgi akışını sağlamak üzere bağlanmış bileşenlerden oluşur. Sistemlerin güvenlik tasarımcılarının işini zorlaştıran iki özellikleri vardır:
  1. Karmaşıklık: Sistemler büyüydükleri gibi, başka sistemlerle de birleşerek karmaşıklığı artırırlar. İnsan yapımı en karmaşık sistem muhtemelen Internettir. Başka bir karmaşık sistem bilgisayarların işletim sistemleri olabilir, milyonlarca satır koddan oluşan MS Windows gibi. MS Windows daha büyük oldukça, yeni güvenlik açıklarının ortaya çıkma ihtimalleri artmaktadır, ve bu açıkları insanlar kapatabilme ihtimalleri de düşmektedir.
  2. Meydana çıkma: Bir sistemin karmaşık davranışları veya özellikleri sistemin sadece bir bileşeninin veya alt sisteminin özelliği değildir, bu yüzden davranışların alt seviyelerde tahmin edilmeleri veya sebeplerinin bulunmaları zordur.

**Soru:** Karmaşıklık ve boyut aynı şeyler midir? Daha büyük sistemlerin daha karmaşık olduğu doğru mudur?

## Bilgi Güvenliği Neden Özellikle Zordur?

Bilgi güvenliği için işleri daha zor yapmak üzere, siberuzayın şu karakteristikleri vardır:

1. Otomasyon: Bilgisayarlar ile, önceden mümkün olmayan veya planlanması imkansız olan saldırılar bile ana birer tehdit olmuştur.
2. Uzaktan müdahale: Saldırganların hedeflerinin yakınlarında olması gerekmemektedir.
3. Teknik iletimi: Saldırı araçları Internet üzerinden yayılabilmektedir.

## Ana Güvenlik Ölçüleri

Üç ana güvenlik ölçümüz vardır:

1. Engelleme
2. Tespit Etme
3. Tepki verme

Örnek olarak, kapınızdaki bir kilidi ve alarmı düşünün. Kilit engelleme sağlarken, kapıdaki alarm sadece bir saldırı olduğunda bunu tespit edebilir. Polisi aramak ise bir tepki verme eylemidir. Unutmayın ki tepki vermek olmaksızın tespit anlamsızdır, ve tepki verme sadece bu iki ölçünün birbirine bağlanması ile alakalı bir durum tespit ettiğinizde anlamlıdır. Ayrıca unutmayın ki engelleme bazı, zararın telafi edilemez olduğu durumlarda tek şansımızdır.

Tespit etme ile alakalı bir diğer önemli konu yanlış alarmlardır. Eğer bir alarm varsa, fakat saldırı yoksa, buna bir yanlış pozitif deriz. Ve fakat, eğer bir saldırı varsa, fakat alarm etkinleşmedi ise, bu duruma bir yanlış negatif deriz. Elbette ki ana hedef hem yanlış pozitiflerin hem de yanlış negatiflerin durumunu minimumda tutmaktır.

**Soru:** Yanlış negatiflerin yanlış pozitiflerden daha ciddi olduğunu söyleyebilir miyiz?