



## Bilgi Güvenliđi

**Murat Balaban**

EnderUNIX Yazılım Geliřtirme Takımı  
Kurucu Üyesi

[murat@enderunix.org](mailto:murat@enderunix.org)

<http://www.enderunix.org/murat/>

**Metin Kaya**

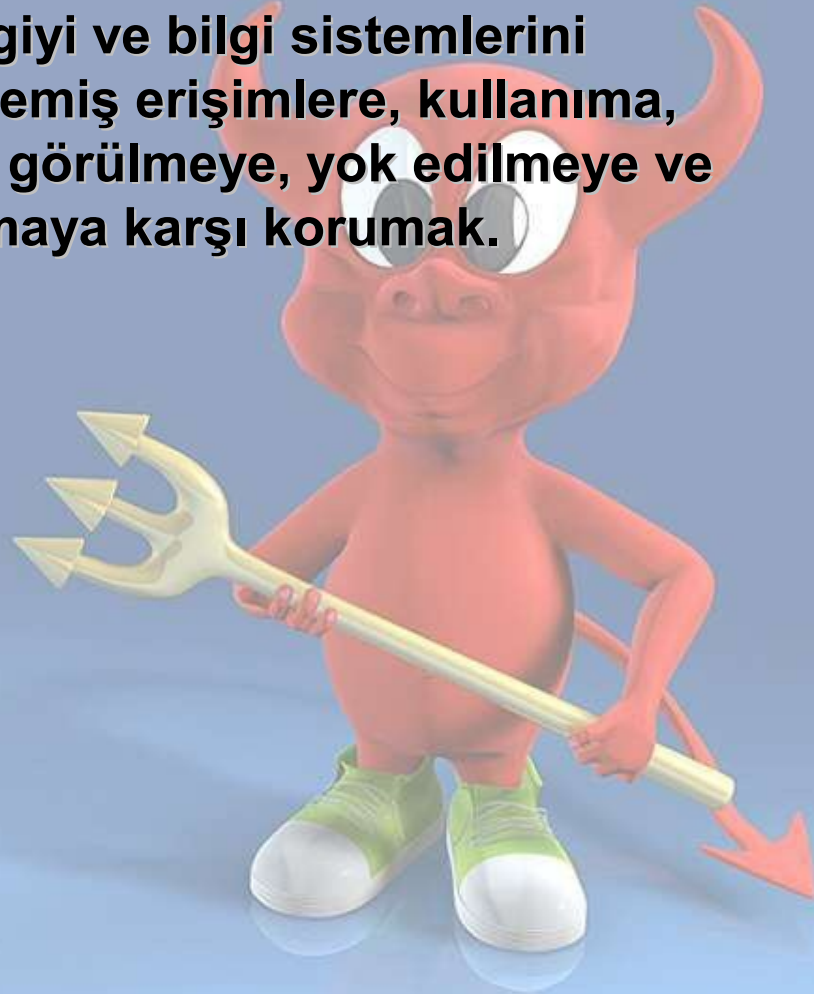
EnderUNIX Yazılım Geliřtirme Takımı  
Üyesi

[metin@enderunix.org](mailto:metin@enderunix.org)

<http://www.enderunix.org/metin/>

# Bilgi Güvenliđi: Özet

**Amaç; bilgiyi ve bilgi sistemlerini yetkilendirilmemiş erişimlere, kullanıma, deđiştirilmeye, görülmeye, yok edilmeye ve bozulmaya karşı korumak.**



# CIA

**Confidentiality - Gizlilik**

**Integrity - Bütünlük**

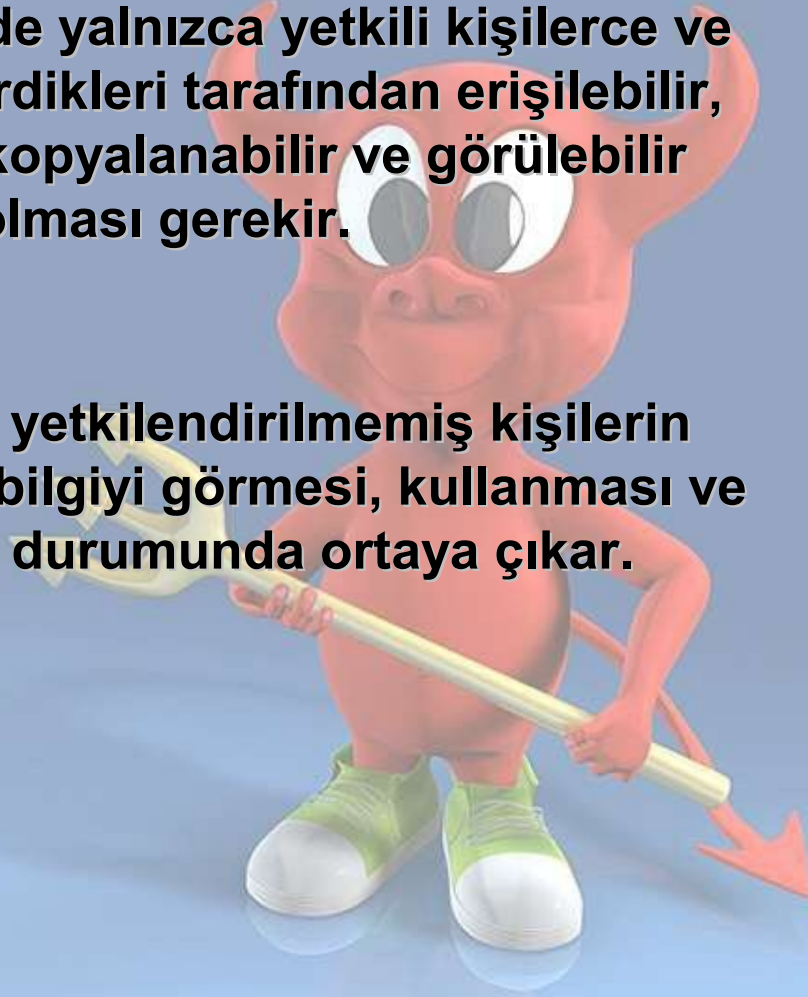
**Availability - Erişilebilirlik**



# Gizlilik

Bilginin normalde yalnızca yetkili kişilerce ve bunların izin verdikleri tarafından erişilebilir, kullanılabilir, kopyalanabilir ve görülebilir olması gerekir.

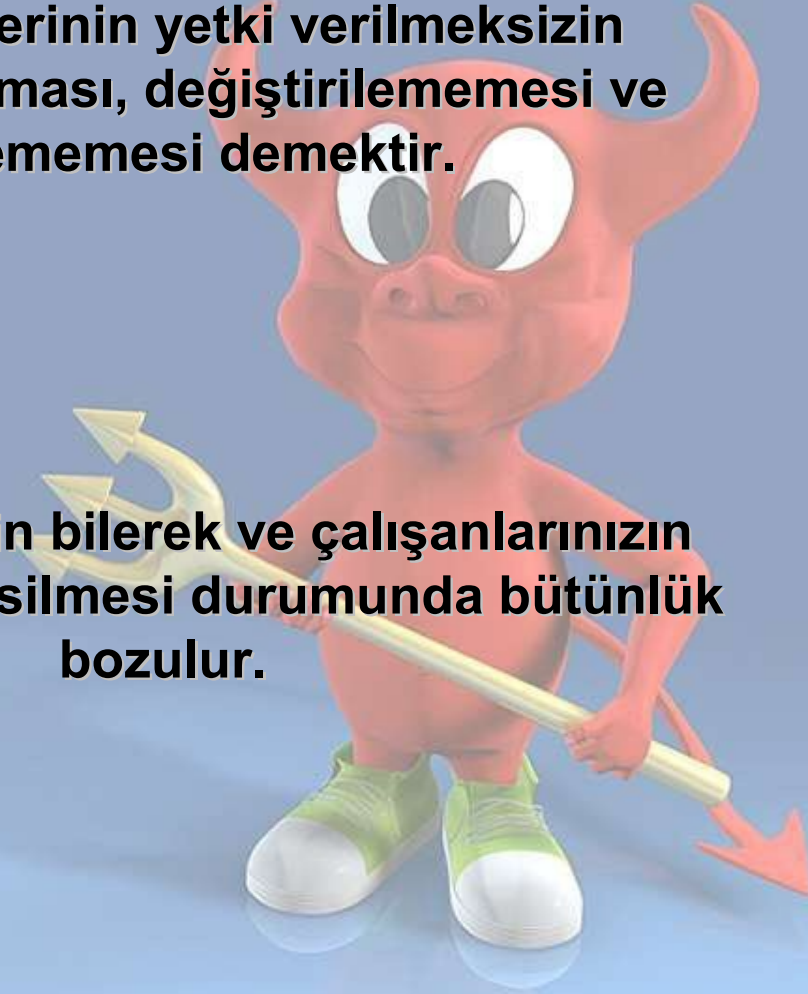
Gizliliğin ihlali; yetkilendirilmemiş kişilerin bilgiye erişmesi, bilgiyi görmesi, kullanması ve kopyalaması durumunda ortaya çıkar.



# Bütünlük

**Bütünlük; verinin yetki verilmeksizin oluşturulamaması, değiştirilememesi ve silinememesi demektir.**

**Kötü niyetlilerin bilerek ve çalışanlarınızın kazayla verileri silmesi durumunda bütünlük bozulur.**



# Eriřilebilirlik

Bilgi ve bilgisayar sistemleri verileri iřler ve gvenlik; eriřebilir ve dzgn alıřan verileri gerektiđinde korur.

Servisleri Engelleme (Denial of Service - DoS)  
Saldırıları

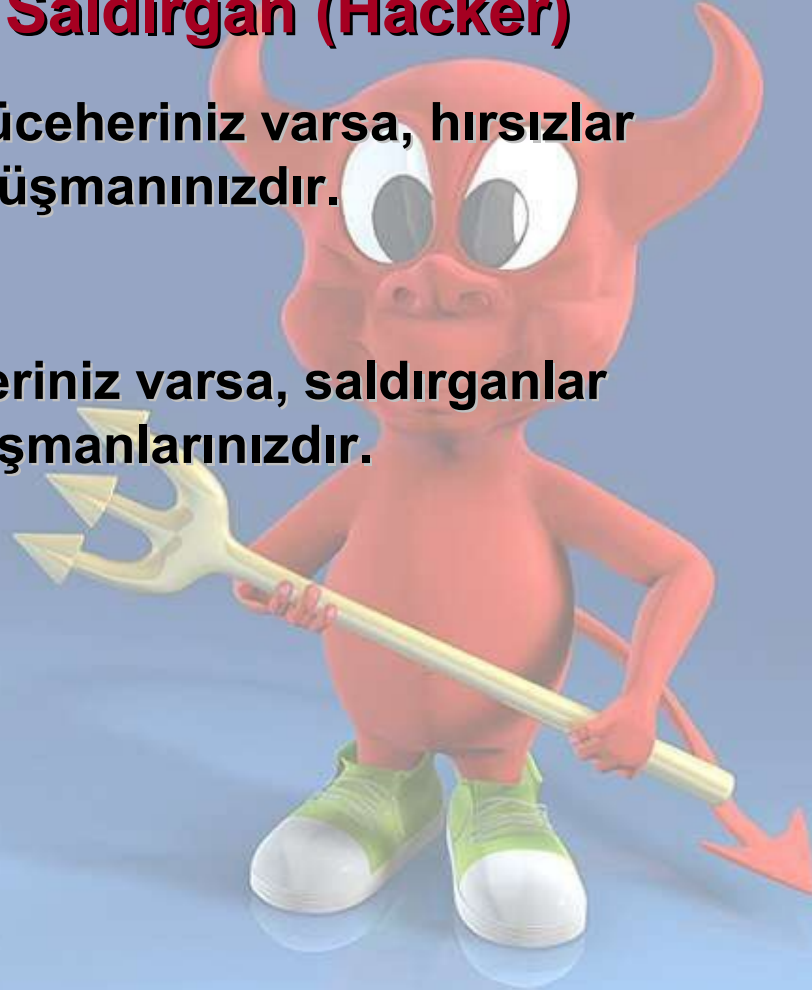


**Mücevher ~ Hırsız**

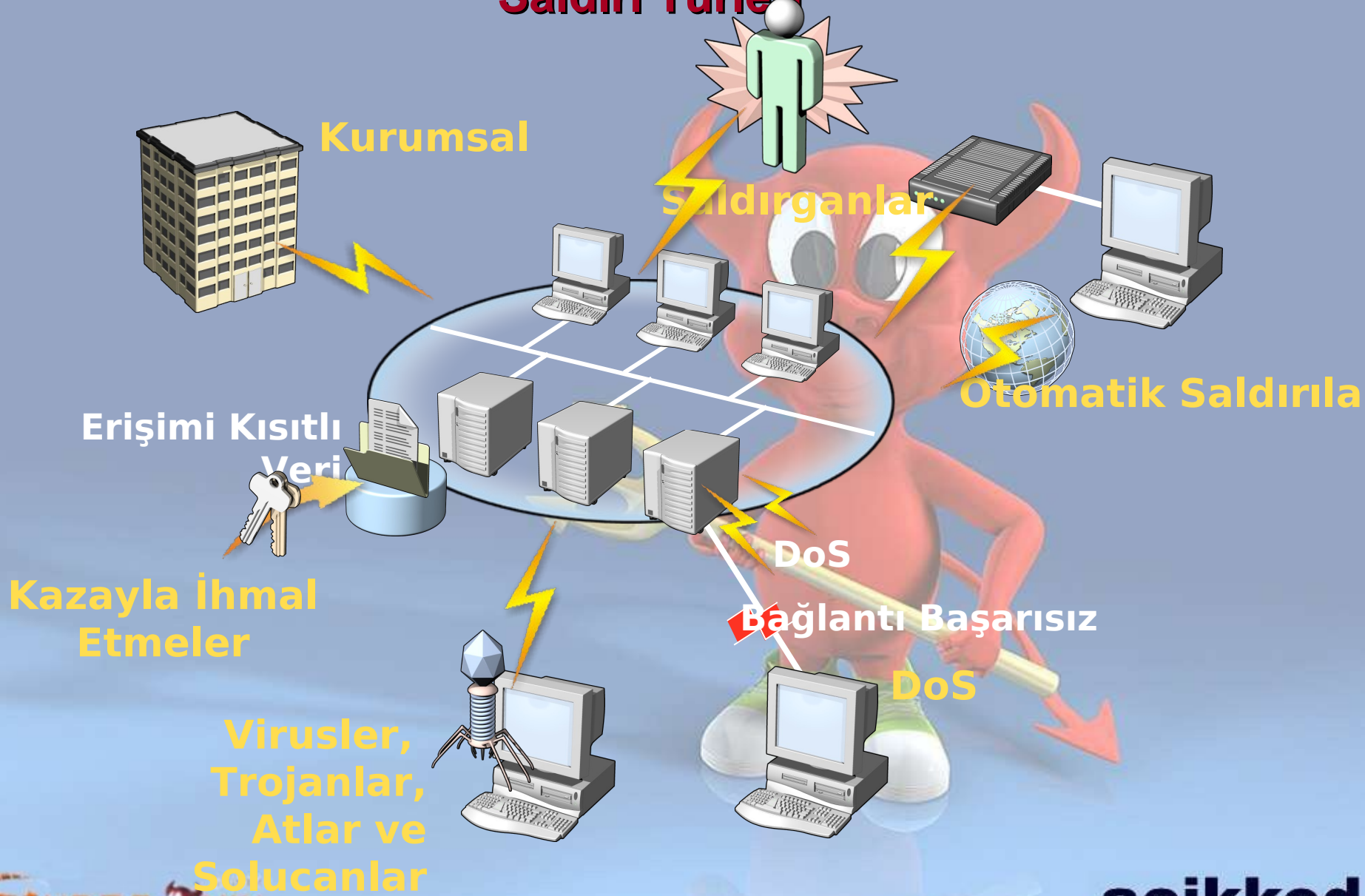
**Bilgi ~ Saldırgan (Hacker)**

**Paralellik: Mücevheriniz varsa, hırsızlar düşmanınızdır.**

**Dijital bilgileriniz varsa, saldırganlar düşmanlarınızdır.**



# Saldırı Türleri



# Gizliliğe Karşı Yapılan Saldırıları

En çok bilineni: Sniffing  
Karşı Tedbir: Kriptoloji



# Bütünlüğe Karşı Yapılan Saldırıları

```
1 /tcp      open      hosts2-ns
3 [mobile]
1 Starting nmap U. 2.54BETA25
1 Insufficient responses for TCP sequencing (3), OS detection may be less
3 accurate
3 Interesting ports on 10.2.2.2:
3 (The 1539 ports scanned but not shown below are in state: closed)
4 Port      State      Service
4 22/tcp    open      ssh
1
1 No exact OS matches for host
8
8 Nmap run completed -- 1 IP address (1 host up) scanned
8 # sshnuke 10.2.2.2 -rootpw="Z10N0101"
4 Connecting to 10.2.2.2:ssh ... successful.
0 Attempting to exploit SSHv1 CRC32 ... successful.
  Reseting root password to "Z10N0101".
  System open: Access Level <9>
  # ssh 10.2.2.2 -l root
  root@10.2.2.2's password:
7
PRE-CONTROL> disable grid nodes 21 - 48
```

# Erişilebilirliğe Karşı Saldırılar

**DoS**

**Engellenmesi en zor saldırı**

**Bot Net Saldırıları**



# Neler Yapılabilir?

Her zaman ve her yerde “güvenliđi” aklınızdan çıkarmayın.

Verilerinizi Őfreleyin.

“Sađlıklı” yazılımlar kullanın.

Dijital dünyadan bahsediyorsanız “güvenilir” sözcüğünü unutun.

Asla unutmayın: hiç bir Őey görüldüğü gibi değildir!

Sistemlerinizi güncel tutun.



**Daha fazla bilgi**

- <http://www.enderunix.org/docs/>





-- Teşekkürler --

Sorular

