



**TR-BOME KM**  
**(Türkiye Bilgisayar Olayları Müdahale**  
**Ekibi - Koordinasyon Merkezi)**

**Mehmet ERİŞ**

[eris@uekae.tubitak.gov.tr](mailto:eris@uekae.tubitak.gov.tr)

**6 HAZİRAN 2008**

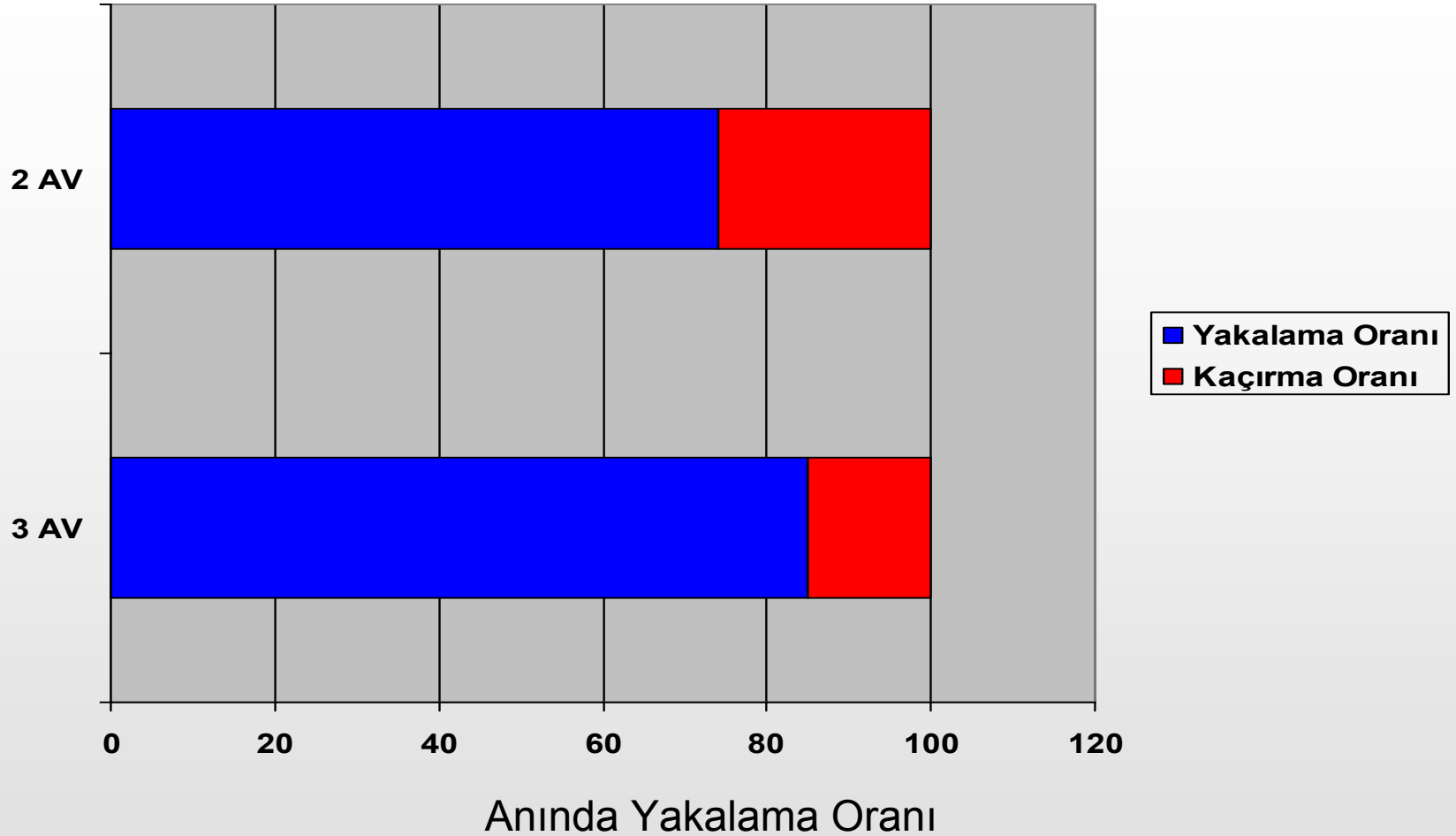
- Bilgisayar Güvenlik Olaylarının Tespiti
- Saldırgan – Güvenlik Çalışanı Yarışı
- TR-BOME KM Çalışmaları

# Bilgisayar Güvenlik Olaylarının Tespiti

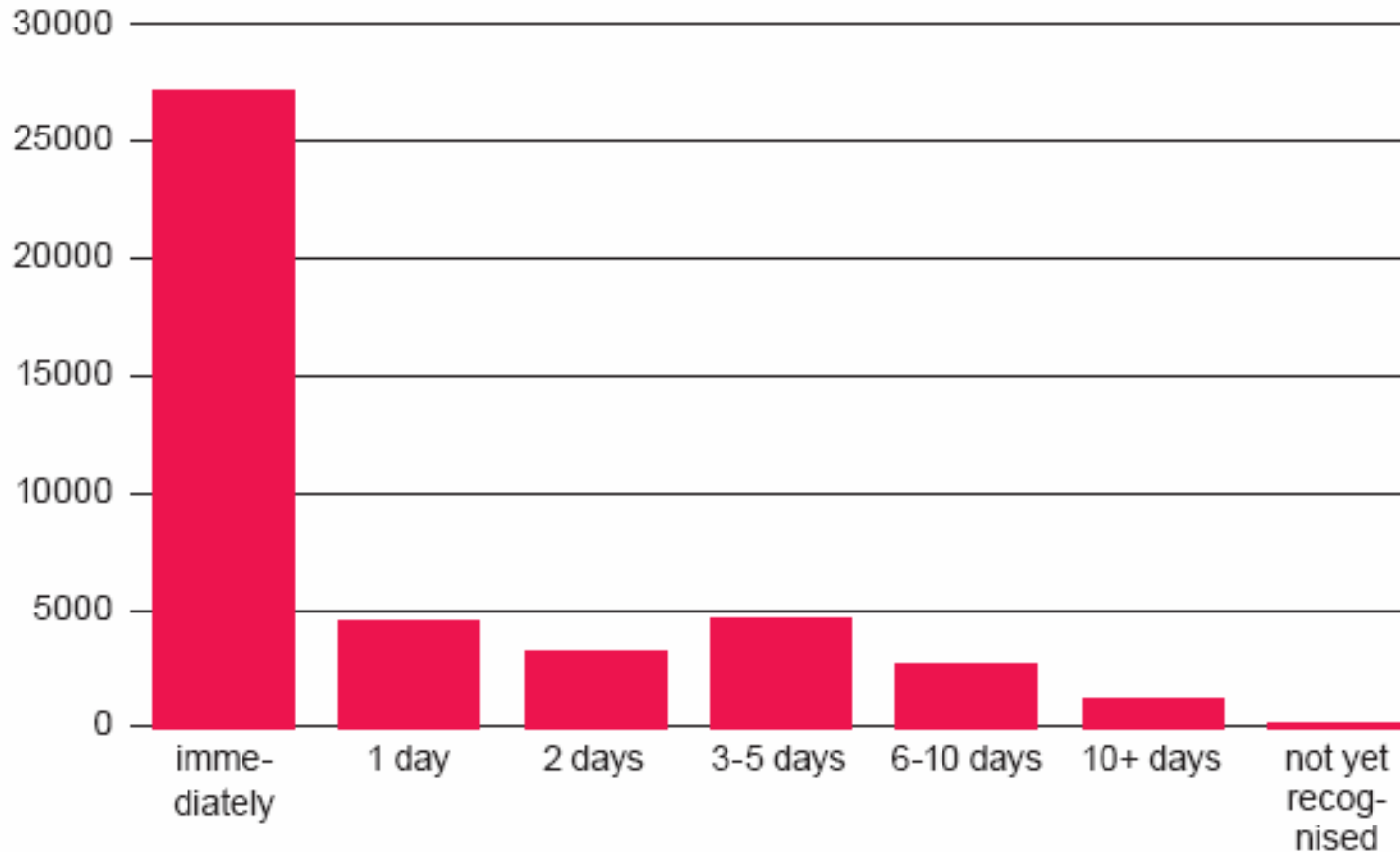
- Güvenlik Olayı Yaşadık mı?
- Gerçekten “hack” edilip edilmediğimizden ne kadar eminiz?
- Bir kere daha düşünelim.

# Ciddi Bir Olay Sonucunda Neler Olurdu?

- Bilgilerimiz çalınırdı.
  - Tespit edebilir miydik?
  - Bilgilerimiz ortaya çıktığında
- Ağ trafiğimizde anormallikler olurdu.
  - Ağ trafiğimizi gözlüyor muyuz?
- Güvenlik duvarı kayıtlarından görürdük.
  - Güvenlik duvarı kayıtlarından hangi saldırılar anlaşılabilir.
  - Güvenlik duvarı kayıtlarına bakıyor muyuz?
- AV sistemimiz görürdü.
  - Emin misiniz?
- Saldırı tespit sistemimiz var. Kesin farkederdik.
  - Saldırı tespit sistemi kayıtlarınıza bakıyor musunuz?
- Sistemlerimiz çalışmazdı.
  - Evet servis dışı bırakma saldırıları çok kolay farkedilen bir olaydır.



- GovCERT-NL (Hollanda - Kamu BOME)  
2007 Yılı Trend Raporu



- GovCERT-NL (Hollanda - Kamu BOME) 2007 Yılı Trend Raporu, n=44112

- Zararlı Yazılımlar (Virüs, Solucan, Reklam Yazılımları, ...)
  - Ne kadar zarar verici
  - Ne kadar sizi hedeflemiş saldırılar
- Tespit Edilen Saldırıları
  - Rastgele saldırılar (merak veya solucanlar)
- Web Sayfası Değişikliği
  - Saldıranlar kim
  - Ne kadar ciddi bir olay



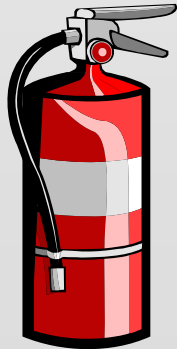
**Güvenlik olaylarına yüzde yüz tespit edebiliyor olsaydık.**

**Ve yüzde yüz doğrulukla bugüne kadar hiç güvenlik olayı yaşamadık diyebilseydik...**

- Çok azımızın başına gelmiştir.

- “Hiç yangın yaşamadık.”

- “O halde neden yangın için hazırlık yapıyoruz?”





# Güvenlik Olayı Yaşamadığımızdan Nasıl Emin Olabiliriz?

Dosya Düzen Görünüm Geçmiş Yer İmleri Araçlar Yardım

http://www.██████████.com.tr/

İlk Adım Haberler


Adobe - Adobe Reader download than... ██████████ TEKSTİL



English

- Hakkımızda
- Ürünlerimiz
- Üretim
- Organizasyon
- Kalite
- Araçlar
- Bayilerimiz
- Haberler
- İnsan Kaynakları
- İletişim Formu
- İletişim Bilgileri

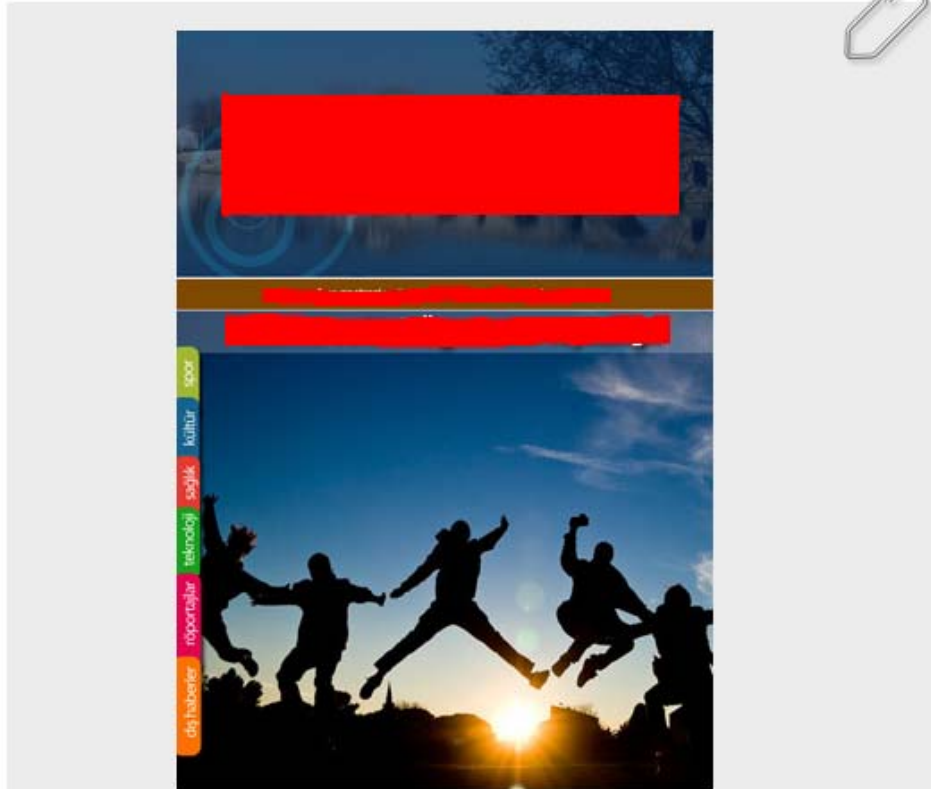
Tam zamanında, yüksek kalitede üretmek...





Bulduğunuz yer: Anasayfa

## Duyuru



Dergimizin 2. sayısı çıktı!

Sizde yeni sayımızı okumak istiyorsanız BÜLTEN sayfamızı ziyaret ediniz..

Kullanıcı Adı

Parola

Beni hatırla

Giriş

[Kayıp Parola?](#)

Hesabımız yok mu? [Kayıt Ol](#)

### EN SON EKLENENLER

- [Eğitim Fakültesi Dekanı Hilmi İBAR Röportajı](#)
- [2007-2008 Bahar Döneminde Dernek-Topluluğumuzda Yapılacak Etkinlik-Faaliyetler](#)
- [İFTAR YEMEĞİ](#)
- [İSTANBUL ve BURSA TARİHSEL GEZİSİ](#)
- [II.GELENEKSEL UFUK TOPLANTISI](#)

### HAVA DURUMU

### WIKIPEDIA YENİUFUK



Arama...

Git

Arama

### > ANKET KÖŞESİ

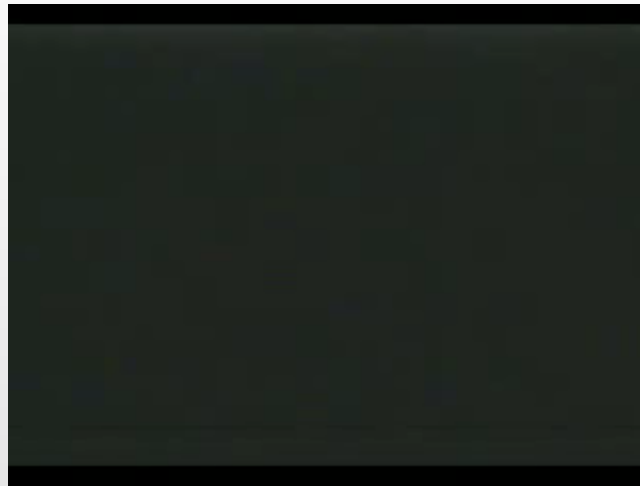
**Köprü Dergisinin ikinci sayısı hakkında düşünceniz nedir?**

- Kesinlikle olmamış!
- Çok basit kaçmış :(
- Tasarım hoş ama içerik bol!
- Beklediğim gibi değil!
- Biraz daha farklı alanlara dikkat çekilmeli!
- İlk sayı için oldukça güzel
- Mükemmel! devamını merakla bekliyorum

Oy Ver

Sonuçlar

SAYGAC



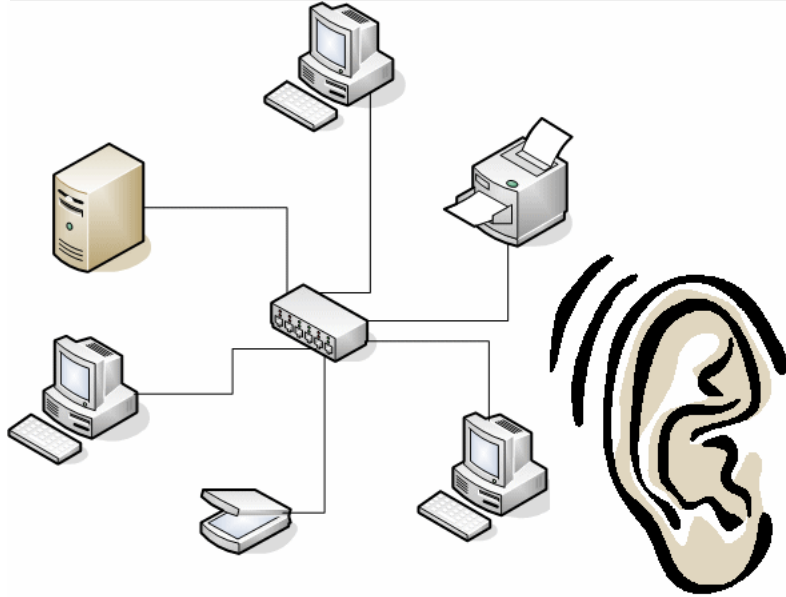


# **Saldırganların Kendilerini Gizleme Yöntemleri**

**Saldırgan - Güvenlik Çalışanı Yarışı**

# Başlangıç

- Saldırgan bilgisayarda hak sahibi olduğunda o bilgisayarın yer aldığı yerel alan ağını dinlemek ister.
- Bunu gerçekleştirmek için bilgisayara dinleyici (sniffer) yerleştirir.



Dinleyicinin çalışabilmesi içinse ethernet kartının rastgele (promiscuous) modunda olması gerekir.

Bu bilgileri verdikten sonra konu ile ilgili tarihsel gelişime bakalım...

- Durum: Güvenlik Bilgi Seviyesi Düşük.
- Dinleyici yazılımından ve rastgele modundan iyi tarafta bulunan kişilerin çoğunun haberi yok.
- Bu nedenle saldırganın da tespit edilmek gibi bir kaygısı yok.

```
mehmet : bash
File Edit View Scrollback Bookmarks Settings Help
root@Mehmet:
root@Mehmet:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:1b:38:8b:2c:48
          UP BROADCAST PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:195 errors:0 dropped:0 overruns:0 frame:0
          TX packets:98 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:20097 (19.6 KB)  TX bytes:12321 (12.0 KB)
          Base address:0x5040 Memory:d8520000-d8540000

root@Mehmet:~# █
```

- Bu bilgiyi öğreniyoruz. Artık sistemimizde bir makinadan şüphelendiğimizde “ifconfig” yazıyoruz.
- Bakıyoruz çıkan sonuçta “promisc” var anlıyoruz ki, sistemimizde sniffer çalışıyor.

- Durum: Dinleyiciler tespit edilebiliyor.
- Saldırgan sisteme müdahale eder. Ethernet kartı rastgele’de olmasına rağmen “*ifconfig*” dediğimizde “*promisc*” ifadesini göremeyeceğiz.

```
mehmet@Mehmet: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

mehmet@Mehmet:~$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:1b:38:8b:2c:48
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Base address:0x5040 Memory:d8520000-d8540000

mehmet@Mehmet:~$ █
```

- Saldırgan tekrar güvende.

- Durum: “ifconfig” komutu bize yalan söylüyor. Saldırganın bu yönteminden haberdar oluyoruz.
- Karşı önlem geliştiriyoruz:
  - Eternet kartımızı kontrol ediyoruz. “Promisc” gözüküyor.
  - Eternet kartını kendimiz rastgele moduna alıyoruz. Bakıyoruz hala “promisc” gözüküyor.
- Sistemimizde dinleyici olduğunu anlıyoruz.

- Durum: Saldırgan yeniden tespit edilebiliyor.
- Saldırgan gizlenme yöntemini geliştiriyor:
- Eternet kartını biz rastgele moduna aldığımızda “ifconfig” komutu promisc gösteriyor.
- ...

# **TR-BOME KM**

## **Bilgisayar Güvenlik Olayları Müdahale**

### **Çalışmaları**

- DPT Bilgi Toplumu Dairesi Bilgi Toplumu Stratejisi Ek'i 88 no'lu Eylem Maddesi
- Altı proje
  - TR-BOME KM
  - Bilgi Güvenliđi Dokümanları
  - Bilgi Güvenliđi Portalı
  - Merkezi Tehdit Gözetleme Sistemi
  - Bilgi Güvenliđi Eđitimleri
  - Pilot Bilgi Güvenliđi Yönetim Sistemleri

- Saldırganlar Organizeler.
- **Biz Neden Organize Değiliz?**

- Olay Müdahale Koordinasyonu
- BOME Destek
- Bilgi ve Tecrübe Paylaşımı
- Zararlı Yazılım Araştırma

- Bilgisayar Güvenlik Olaylarına Müdahale birden çok kurum ve kuruluşu ilgilendirmektedir:
  - Diğer BOME'ler
  - Internet Servis Sağlayıcı
  - Barındırma Hizmeti Veren Şirketler
  - Saldırganın Aracı Olarak Kullandığı Diğer Mağdurlar
  - Adli Makamlar
  - BT Üreticileri
  - Basın
  - ....
- Bu kurum ve kuruluşlar çoğunlukla birden fazla ülkeye yayılmış durumdadırlar.

- TR-BOME yasal zorunlulukların dışında olay raporları ile bilgileri ilgili kurumun onayı dışında herhangi bir kurum veya kişi ile paylaşmayacaktır.
- TR-BOME, olay raporlarını ve her türlü bilgiyi güvenlik politikasına uygun bir şekilde korumaktadır.

- Eğitim
  - BOME Kurulum ve Yönetim (3 gün)
  - Bilgisayar Olaylarına Müdahale – Giriş (3 gün)
  - Bilgisayar Olaylarına Müdahale – İleri (5 gün)
- Danışmanlık
- Olay Müdahale Tatbikatı

- Planlanan Tarih:
  - Eylül 2008
- Kapsam
  - Güvenli Haberleşme
  - Olay Müdahale Sürecinin Test Edilmesi
  - Süprizler
- Katılımcı Kurumlar
  - BOME Çalışma Grupları

- Kamu BOME Çalışma Grupları

## I. Çalışma Grubu

- Başbakanlık
- Adalet Bakanlığı,
- Sayıştay Başkanlığı
- Muhasebat Gn. Md.lüğü,
- SPK

## II. Çalışma Grubu

- Merkez Bankası,
- Dış Ticaret Müsteşarlığı,
- Hazine Müsteşarlığı,
- Tapu ve Kadastro Gn. Md.lüğü

- Güvenilir BOME Forumu

- BOME Etiği
- Güvenlik olayları ile ilgili bilgilerin güvenilir bir ortamda paylaşılması

- Çalışma grubunda sırasıyla aşağıdaki çalışmalar gerçekleştirilecektir:
  - BOME Çerçevesi
  - Servis ve Kalite Çerçevesi
    - BOME Servisleri
    - Bilgi Akışı
    - Kalite Güvence
    - Politikalar
  - Olay Müdahale Araçlarının kullanılması
  - Olay Müdahale Sürecinin geliştirilmesi



- Güvenilir Bilgi Paylaşım Platformu
- BOME Etiği
  - Bilgisayar güvenlik olayı müdahale koordinasyonu çerçevesinde kendisine bildirilen güvenlik raporlarının gizli tutulması
  - Bilgisayar güvenlik olayları ile ilgili kayıtların güvenli şekilde korunması ve kurum içerisinde bilmesi gereken prensibine göre paylaşılması
  - Diğer kurum ve kuruluşların bilgisayar güvenliğini tehdit eden bilgilerin TR-BOME'den gizli tutulmaması
  - BOME temas noktalarının güncel tutulması
- Dünyadaki Örnekleri:
  - FIRST
  - TF-CSIRT
  - European Government CERTs

Saldırganların bilişim sistemlerine girmek, kalmak, bilgileri çalmak veya değiştirmek, diğer sistemlere saldırmak için kullandıkları araçların incelenmesi

- Virüs
- Solucan
- Arka kapı
- Truva atı
- Rootkit
- ...

- Bilgisayar güvenlik olaylarına hazırlıklı olmalıyız.
- Yaşadığımız tecrübeleri paylaşmalıyız.



**İlginiz İçin Teşekkürler**

**Sorular ve Cevaplar**