# Yerleşke Ağ Güvenliği Ve Yönetimi

ODTÜ BİLGİ İŞLEM DAİRE BAŞKANLIĞI, ***2007***

ccnet@metu.edu.tr

# İŞİNİ BİLEN

# TEKNİK

# ELEMAN

# GÜVENLİK

- Güvenliğin amacı:
  - CIA (confidentiality, integrity, and availability).
    - Confidentiality: Bilgilerin gizliliği ve mahremiyet.
    - Integrity: Bilgilerin doğruluğu. Yani bilgilerin taşınırken veya saklanırken değiştirilmemesidir (MD5SUM gibi).
    - Availability: Erişilebilirlik. Yani bir kullanıcı istediği bilgiye ulaşabilir olmalıdır.
- Riziko: Bir tehditin gerçekleşme olasılığıdır. Üç eleman ile;
  - Varlıklar: Maddi veya manevi değerli şeylerdir.
  - Tehdit: Varlıklara zarar verebilecek kişi veya durumlardır.
  - Zayıflıklar: Bunlar ise sistemlerin hassas noktalarıdır. Bu noktalar doğru uygulamalar ile azaltılabilir.

# POLİTİKA

- POLİTİKA METNİ
  - Hiç yazılmamış bir politika metninin anlamı “**herşeye izin ver**”
  - Politika metni olmayan ağların güvenliklerinin sağlanması zordur.
  - Yeterli derecede duyurusu yapılmayan metnin uygulanabilirliği azalır.
  - Ağ, güvenlik, sistem kullanım politikaları ayrı ayrı veya birlikte yazılmalıdır.
  - Bu politika metni yetkili makamlarca onaylanmalıdır. Onaylanmayan uygulamaların yaptırımı hiç yoktur veya azdır.

# KAMPÜS GÜVENLİĞİ

- Sınır güvenliği
  - Nasıl her ülkenin güvenliği sınırda başlarsa ağ güvenliği de sınırda başlar.
  - Sınırların belirlenmesi önemlidir.
    - İnternet bağlantıları
    - Dış kampüs bağlantıları
      - Burada her dış kampüsü de ayrı birer kampüs olarak tasarlamak gerekir.
    - Modem hatları
    - GPRS bağlantıları
    - Kablosuz iletişim hatları
    - Son olarak, dışarıdan gelen tüm taşınabilir cihazlar.

# KAMPÜS GÜVENLİĞİ

- Sistem Güvenliği
  - Kampüs ağ güvenliği bir bütündür.
  - Ağ güvenliği için tüm sistemlerin güvenliği sağlanmalıdır.
  - Güvenlik duvarı ve virus koruma uygulamaları zorunlu olmalıdır.
  - Pekçok ticari şirket bu konuda çözüm sunmaktadır. Ayrıca açık kaynaklar da bu konuda yardımcı olmaktadır (snort gibi).
- ICMP (Internet Control Message Protocol)
  - IP haberleşmesinde genelde hata mesajları için kullanılır.
  - Tamamen kısıtlanması iyi değildir. (Echo Reply, Destination Unreachable, Echo Request gibi tipleri hala kullanılmaktadır.)
  - QoS ile şekillendirilmesi yararlı olur.

# KAMPÜS GÜVENLİĞİ

- IPv4 dışında kalanlar eğer kullanılmıyorsa kapatılmalıdır.
- Mümkün olduğu zamanlarda “**herşeyi engelle gerekli olanlara izin ver**” güvenlik kuralı uygulanmalıdır.
- Multicast eğer kullanılmıyorsa engellenmeli veya kontrol altında tutulmalıdır.

# KAMPÜS GÜVENLİĞİ

- Saldırı çeşitleri
  - Uygulama tabanlı saldırılar – E-posta saldırısı gibi
  - Servis engelleme (Denial of Service, DoS) saldırıları.
  - IP Spoofing
  - Şifre saldırısı

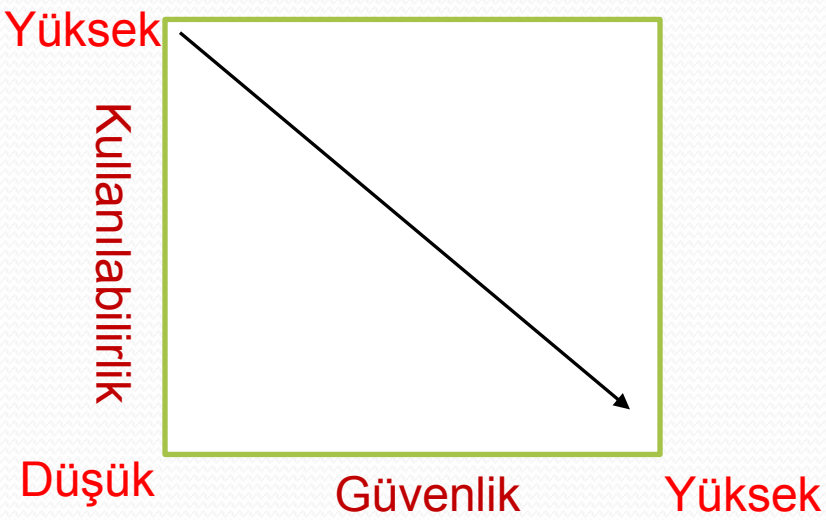
# KAMPÜS GÜVENLİĞİ

ÖNEMLİ BİR NOKTA

**Güvenlik nedeni ile sınırlandırılan**
**TÜM kullanıcılar**
**(IP, MAC veya kullanıcı kodu bazında)**
**mutlak surette**
**bilgilendirilmelidirler.**

# KAMPÜS GÜVENLİĞİ

- Ağ güvenliği parasal bir sorundur.
- **Ne kadar maddi kaynak o kadar güvenlik.**
- Ağa erişim ağ güvenliğinin önüne geçmemelidir. Hiç kimsenin kullanamadığı paronayak bir ağ kurmak **kaynakların anlamsız bir şekilde harcanması** demektir.
- Ağ kullanımı ile güvenlik arasında düzgün bir orantı kurulmalıdır.



# SINIR YÖNLENDİRİCİ

- Akıllı olmalıdır.
  - 3. seviye IPv4 yönlendirme yapması zorunludur.
  - Filtreleme yapabilir olmalıdır. En azından 4. seviye olmalıdır. İstenen 7. seviye filtreleme yapabilmesidir.
  - Politika metnine uygun yapılandırılmalıdır.
  - Para/güvenlik
  - Birden fazla İnternet bağlantısı sahibi olanların BGP kullanması gereklidir.
  - Her zamanki gibi işini bilen bir teknik elemana ihtiyaç vardır. Özellikle açık kaynak kodlu bir yapılandırma için bu gereklidir.
  - INLINE cihazlar performans kaybına neden olmaktadır.
  - Güvenlik duvarı olması iyi bir özelliktir.
    - İçeriden dışarıya başlatılan bağlantılara izin ver ama dışarıdan içeriye bağlantı kurulmasına izin verme?

# BLACKHOLE – Kara Delik

- Başıboş bir şekilde içeride dolaşan paketleri yakalamanızı sağlar.
- İstenmeyen trafiklerin (adaware, spyware gibi) yoğunluğunu ölçmenizi sağlar.
- Bu cihaz özel hazırlanmış bir PC tabanlı sunucu olabilir.
- Yönlendirilmesi olmayan IP'ler bu cihaza yönlendirilir. Mümkünse bu cihaz IDS olarak konumlandırılmalıdır.
- Cihaza gelen bilgiler değerlendirilmeli ve gerekli tedbirler alınmalıdır. Mesela; bir kaynaktan toplam 5dk içerisinde gelen paketler sayılıp port taraması yapan cihazların otomatik erişimi kısıtlanabilir.
- Eğer varsayılan yönlendirme kullanılıyorsa olmayan IP blokları bu cihaza yönlendirilebilir.
  - http://www.iana.org/assignments/ipv4-address-space Reserved Networks
- Ayrıca genelde virüsler tarafından kullanılan Microsoft portları (135-139, 445 gibi) bu cihaza yönlendirilebilir.
  - Mesela herkesin bildiği bir yöntem:

    **# tcpdump –i eth0 –n 'port 135 or port 445'**

    Bu komutun çıktısı size tarama yapan virüslü bilgisayarların IPlerini verecektir.
- Son olarak http://www.bleedingsnort.com/blackhole-dns/ adresinde benzer bir yöntem kullanılarak DNS kara deliği mekanizması kurulabilir.

# KABLOSUZ AĞLAR

- Esasen kablosuz ağların kendisinin bir güvenlik sorunu olmasının dışında bu teknolojiye sahip cihazlarda aynı güvenlik sorunlarına neden olmaktadır.
- Taşınabilir tüm cihazlar yanlarında güvenlik tehditlerini de taşımaktadırlar.
- Bu ağdan gelen bağlantılar kampüs dışı bağlantı olarak algılanmalıdır.
- Bu ağa girişler düzgün bir şekilde yapılanmalıdır.
- Mümkünse IEEE 802.1X kullanılmalıdır.
- IEEE 802.1X yapısı RADIUS, LDAP ile merkezi yapılabilir.
- WPA veya daha iyi WPA2 (IEEE 802.11i) kullanılması sağlanmalıdır.
- Kullanıcılar ağ kullanımı hakkında bilinçlendirilmelidir.

# P2P – Paylaşım Uygulamaları

- Ağ kullanım yoğunluğu artmaktadır.
- Mümkünse engellenmelidir. Engelleme işlem daha çok idari bir süreçte yapılmalıdır.
- Para/Güvenlik
- P2P aynı zamanda önemli bir güvenlik açığıdır.
  - Güvenli ağlarda kesinlikle izin verilmemelidir.
  - Gerekli durumlarda P2P için özel ağlarda kullanımına izin verilebilir.
  - Güvenlik açıklarının yanında, kullanıcıların indirdiği uygulamaların çalıştırılması ile oluşan güvenlik açıkları.
  - Önemli bir BOTNET kaynağıdır.
- Aynı zamanda iyi işler içinde kullanılabilir.
  - IPHONE
  - Linux, BSD sürümleri
  - Oyun, OS güncellemleri gibi.
- En azından QoS ile yönetilmelidir.

# SALDIRI KAYNAĞI MIYIZ?

- Saldırılar bize geliyor.
- Peki bizden saldırı gidiyor mu?
- Güvenlik çift taraflıdır.
  - Bize gelen saldırılar.
  - Bizden giden saldırılar.
- Her iki taraf içinde tedbir alınmalıdır.
  - Kullanıcılarımız uyarılmalıdır.
  - Bilinçsiz yapılan işlemler kullanıcıyı saldırı kaynağı yapabilir.
    - Açık bırakılan bir kablosuz bağlantı kullanılarak hiç tanımadığımız biri hiç tanımadığımız birinin hesabını boşaltabilir.
    - Bağlantı sahibi bu hırsızlıktan sorumlu(mudur?).

# HONEYPOTS – HONEYNET

- Saldırıları çekmek için kurulan sisteme honeypot (bal kübü), bu sistemlerden oluşan ağa ise honeynet denir.
- Düzgün kurulmalıdır. Yanlış yapılandırma tüm sistemin ele geçirilmesini sağlar.
- IDS tabanlı olmalıdır.
- Ana amaç sistemde yalancı açıklar gösterip saldırganı ve yöntemlerini öğrenmek ve karşı politika oluşturmaktır.
- Tarpit (http://labrea.sourceforge.net/)
- KFsensor (http://www.keyfocus.net/kfsensor/) – Windows
- Honeyd (http://www.honeyd.org/)
- Tüm loglama mekanizmasının merkezi olması ve cihazlar üzerinde tutulmaması sistemin ele geçirilmesinin anlaşılmasında yardımcı olacaktır.
- 2. Seviye veya 3. seviye olarak yapılandırılabilirler.
  - 2. Seviye cihazların bulunması daha zor olduğu için bu sistemler daha güvenlidir.

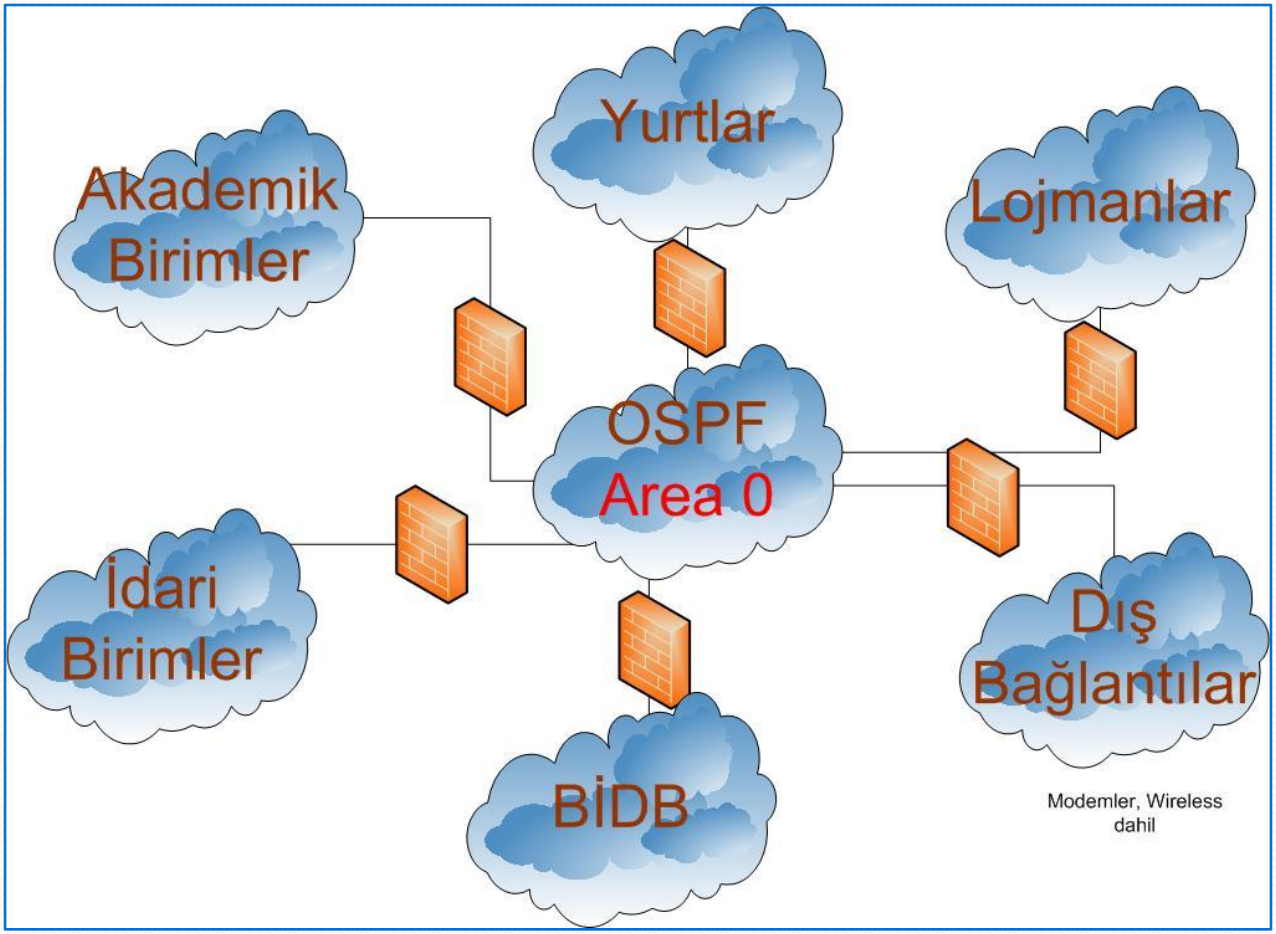
# GRAFİKLER

- Tüm cihazların kullanım grafikleri çizilmelidir.
  - Bunun için MRTG, RRDTOOL veya CACTI kullanılabilir. CACTI kullanımı son zamanlarda artmıştır.
  - Grafik arayüzünden trafikte oluşabilecek anomali rahatlıkla görülebilmektedir.
- Aynı zamanda mümkünse cihazların CPU, Bellek gibi değerlerinin grafikleri de hazırlanmalıdır.
- Kullanıcı sayılarını ve bağlantıları gösteren grafiklerde yararlı olacaktır.
- Bu grafikler aynı zamanda raporlamalarda da çok işe yarayacaktır.

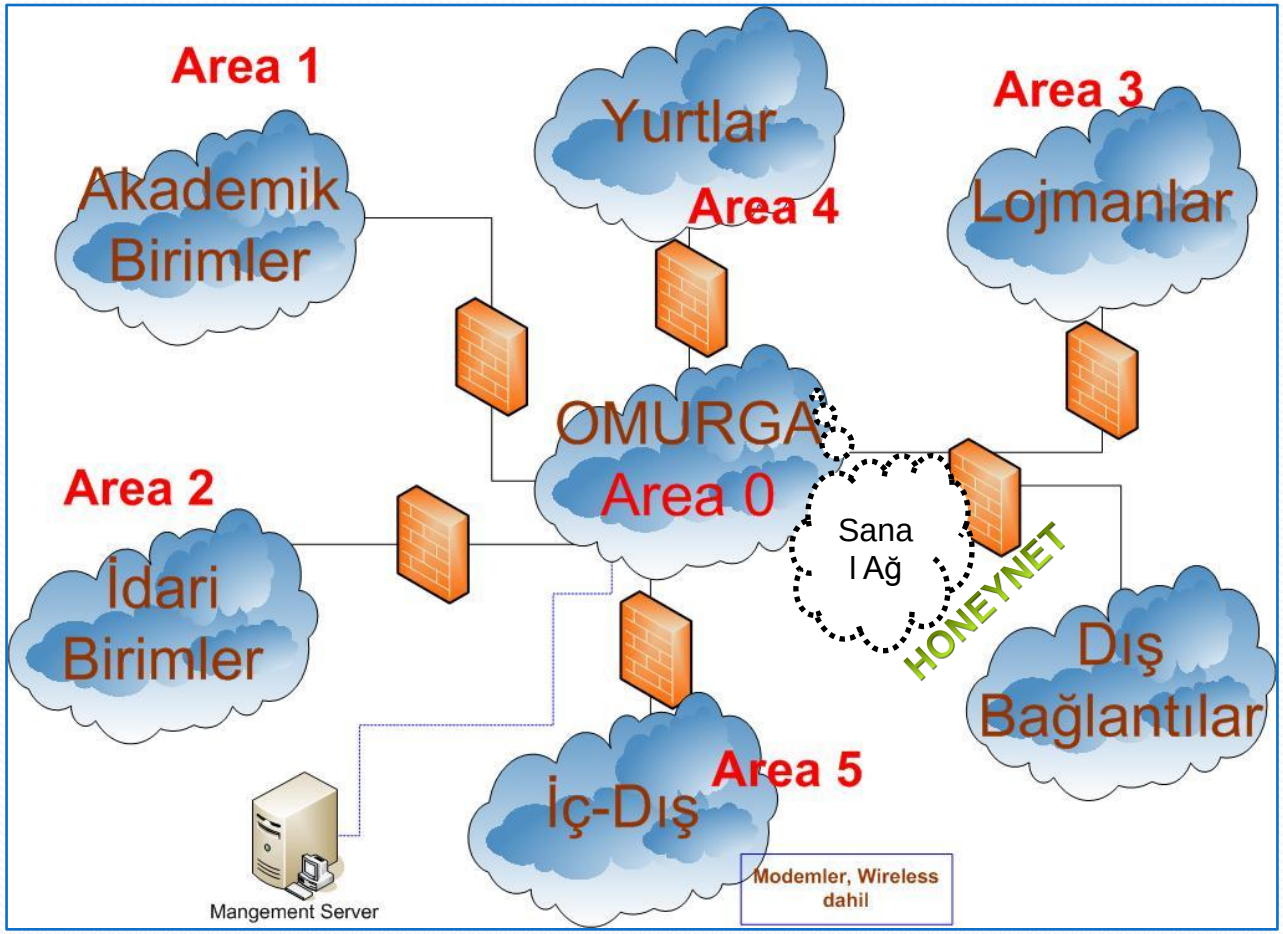
# MERKEZİ LOG SİSTEMİ

- LOG tutma işlemi mümkünse merkezi olmalıdır.
- Tutulan loglar günlük olarak kontrol edilmeli veya otomatik sistemler kurulmalıdır.
- Bağlantı izlerinin logları da tutulmalı ve uzun süreli kaydedilmelidir.
- Sisteme giriş yapan tüm kullanıcı logları tutulmalıdır.
- Sistemde bulunan tüm arp kayıtları gün ve yer bilgisi ile beraber arşivlenmelidir.

# Örnek 1


Yurtlar
Akademik Birimler
Lojmanlar
OSPF Area 0
İdari Birimler
Dış Bağlantılar
BİDB
Modemler, Wireless dahil

# Örnek 2


Area 1
Akademik Birimler
Yurtlar
Area 4
Area 3
Lojmanlar
OMURGA
Area 0
Area 2
İdari Birimler
Sana l Ağ
HONEYNET
Dış Bağlantılar
İç-Dış
Area 5
Mangement Server
Modemler, Wireless dahil

# TEŞEKKÜR EDERİZ

ccnet@metu.edu.tr