



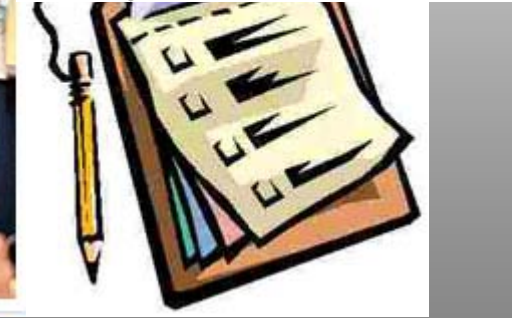
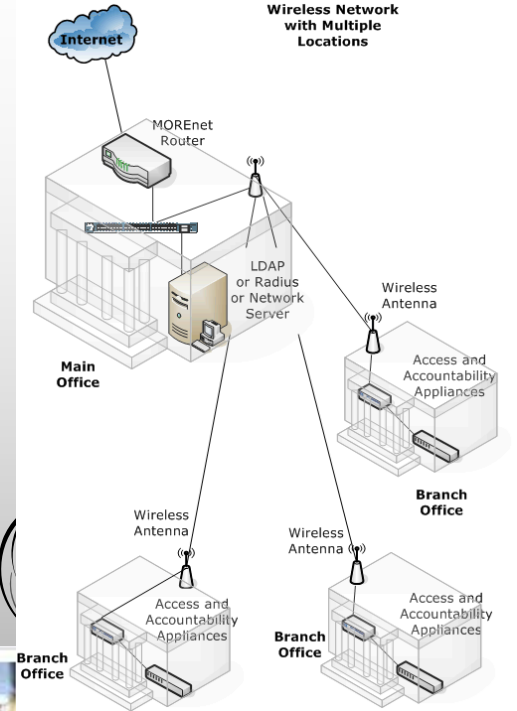
# KABLOSUZ AĞ GÜVENLİĞİNE KURUMSAL BAKIŞ

Battal ÖZDEMİR  
Uzman Araştırmacı

15 Mart 2007, İstanbul

# Sunum İeriđi

- Kablosuz Ađlar
- Tehditler Riskler
- Kurumsal Yaklařım



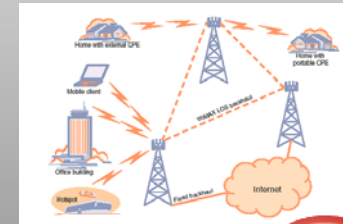
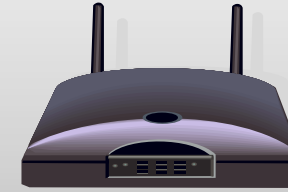
# Neden Kablosuz

- Esneklik
  - Mobil Veri Erişimi
- Maliyet
  - Düşük altyapı maliyeti
- İş Gereksinimleri
  - PDA ile eposta erişimi
- Yüksek Verimlilik
  - Zaman kaybının önlenmesi



# Engel Olmak Neredeyse İmkansız!!!

- Laptop/PDA/Bluetooth/  
Infrared/Cep Telefonları
- Kablosuz Modemler
- Yakında Wimax
- Geleneksel Sınır Güvenliği  
Yaklaşımı Geçersiz



## Güvenilir Kılmak İmkansız Deęil !!!

- Gelişmiş Kimlik Doğrulama/Şifreleme Protokolleri
- Merkezi Yönetim
- 24/7 İzleme/Saldırı Tespit Yazılımları
- Bağımsız Denetleme/Penetrasyon Testleri



# Tehditler

- Dinleme
- Yetkisiz Eriřim
- Yabancı EN'larına Bağlanma
- Servis Dıřı Bırakma
- Veri Bütünlüğünün Bozulması
- Kaynağın Tespit Edilememesi

# Saldırı Senaryoları

## 1. Basit Dinleme:

- Güvenlik önlemi alınmamış veya WEP kullanılmış
- İnternette ücretsiz yazılım + 15 dk'lık bir sunum
- Kablosuz ağ trafiği dinlenir,
- Ziyaret edilen web sayfaları takip edilebilir,
- Eposta trafiği izlenebilir.

## 2. İstemci Üzerinden İç Ağa Erişim:

- Sisteme bağlı EN yok
- Çalışan laptopunu hem evde hem işyerinde kullanıyor,
- “Home” ismiyle güvenlik önlemi olmayan Kablosuz ADSL bağlantısı mevcut,
- Saldırgan “Home” isimli bir sahte EN oluşturuyor ve çalışanın laptopuna bağlanıyor
- Laptopa yükleyeceği casus yazılımlarla kurum ağındaki trafiği dinleyebiliyor.

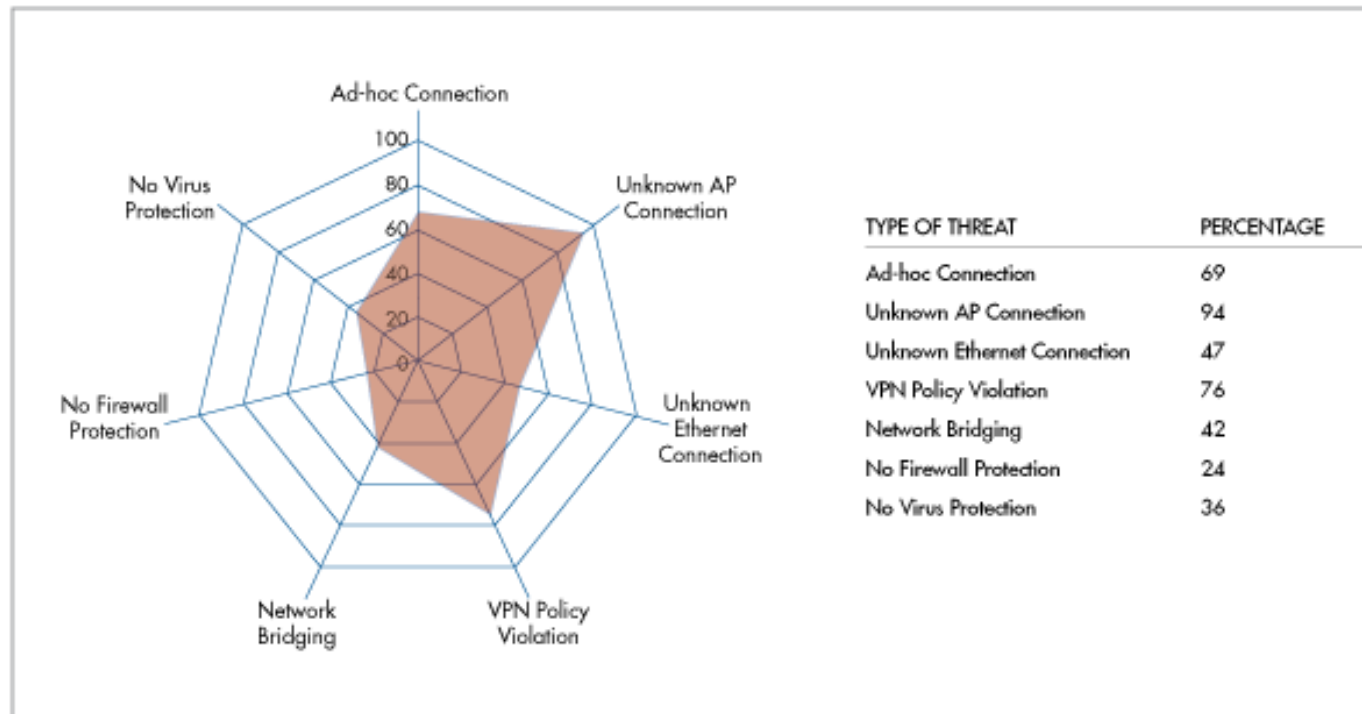
## 3. İç Ağa Direk erişim

- İç ağa giriş için uç bulunmayan labda çalışan mühendisler, masalarına bir EN kuruyor ve laptoplarıyla dosya sunumcuya/internete bağlanıyorlar
- Yetersiz güvenlik önlemini farkedenden saldırgan, EN'yi kullanarak iç ağa erişiyor,
- Güvenlik Duvarı kurallarına hiç takılmadan iç ağa erişim.

# İş Riskleri

- Ağ/Sistem Devre dışı
- Veri Kaybı/Çalınması
- Güvenilirlik/İmaj Kaybı
- Tazminat/Ceza Nedeniyle Maddi Kayıp



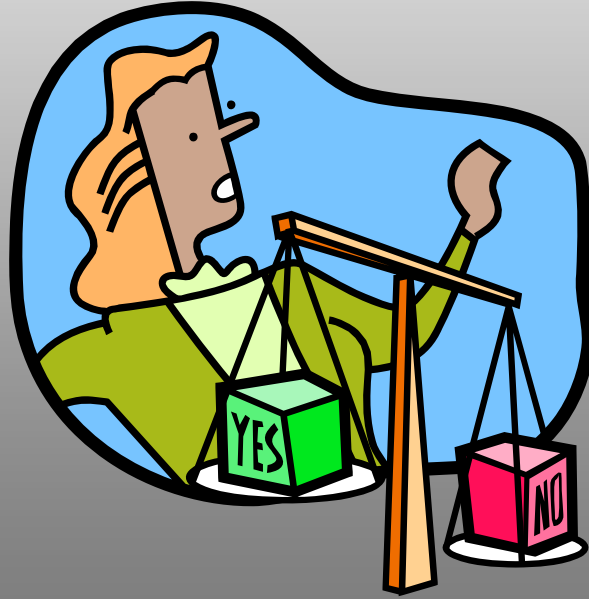


Threat Index: <http://www.networkchemistry.com/labs/threatindex.php>

- Mayıs 2006 – Aralık 2006 karşılaştırması:
  - VPN politikası ihlalleri %11.8 arttı,
  - AdHoc bağlantılar %9.5 arttı,
  - Bilinmeyen EN'lere bağlantı %8 arttı,



# Ne Yapmalı ?





Kablosuz Ağ'a HAYIR!!!

# Kablosuz Ağ'a HAYIR



- HAYIR cevabı güvenliğimiz için yeterli mi?
  - Switch'lere bağlanan Access Pointler!!!
  - Kurum Çevresinde bulunan Access Pointler!!!
  - Ad Hoc Bağlantı kuran Laptop/PDA'ler!!!
  - Bluetooth Cihazlar!!!

# Kablosuz Ağ'a HAYIR

- Ne Yapmalı?

- 24/7 Denetleme

- Kablosuz Bağlantıların Engellenmesi

- Penetrasyon Testleri

- Raporlama/Uygunluğun Belgelendirilmesi





Kablosuz Ağ'a EVET!!!

# Aşama 1 - Gereksinimlerin Belirlenmesi

- İş ve Fonksiyonel gereksinimlerin belirlenmesi
  - Konferans salonunda e-posta, web erişimi
  - Toplantı salonlarında dosya sunumcuya erişim
  - Çalışanlara laptop/PDA tahsisi ve kablosuz erişim
- Risk Analizi
  - Tehditler, Gerçekleşme Olasılıkları, Varlıklara Etkisi => Risk Değeri
- Kullanım politikası
  - Çalışanlar, İş ortakları, Müşteriler, Misafirler
  - Bilgi kaynaklarına erişimde kısıtlamalar
    - Örnek: Misafir kullanıcı internet erişimine sahip olsun, ama veritabanlarına ulaşmasın
  - İstemcilerin dış ağlara bağlanması üzerindeki kısıtlamalar
    - Ev, Otel, Restoran



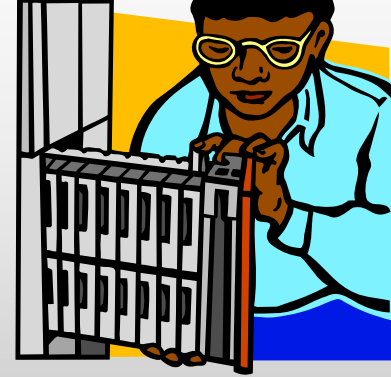
## Aşama 2 – Tasarım / Satın Alma

- Güvenlik Yapısının Tasarımı
  - EAP methodu, PKI altyapısı, VLAN yapısı vb.
  - Firewall Kuralları
  - Antivirus, Firewall, OS güncellemeleri vb.
- Kapsama Alanı Analizi
  - Hangi noktalara / Kaç tane EN
- Güvenlik Denetleme Yöntemleri,
- Kablosuz Ağ Bileşenlerinin Özellik ve Sayılarının Belirlenmesi,
- Satın Alma

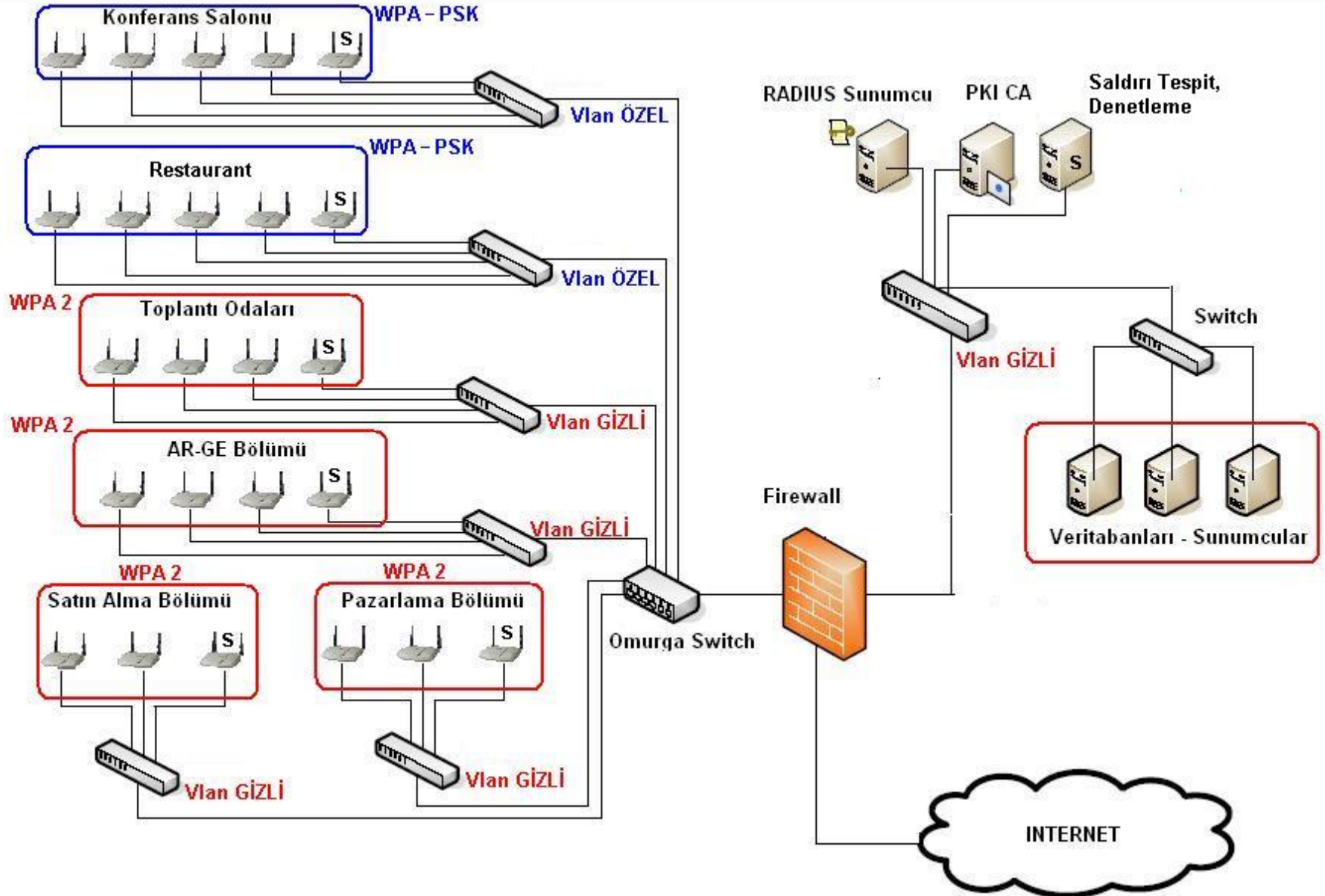


## Ařama 3 - Kurulum

- VLAN yapısı, Güvenlik Duvarı Kuralları
- PKI Yapısı
- Bileřenlerin Konfigürasyonu
- İstemci, Sunumcu Sıkılařtırmaları
- 24/7 Saldırı Tespit / Denetleme Sistemi Kurulumu

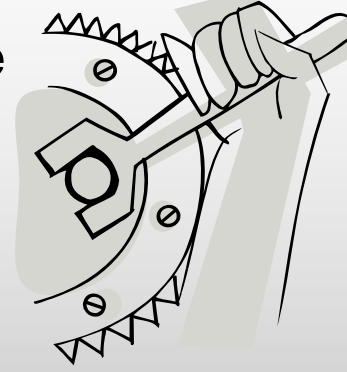


# Örnek Tasarım

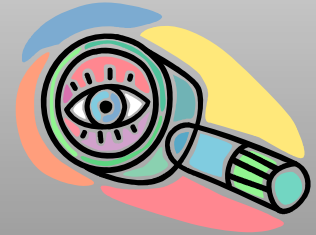


## Aşama 4 - İşletme ve Bakım

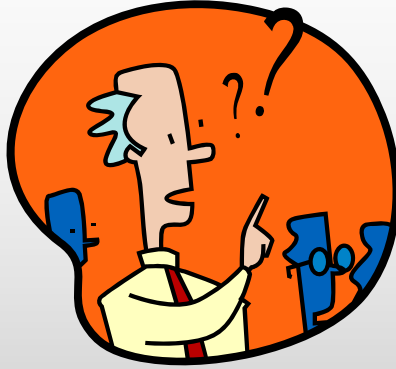
- Düzenli Yazılım, Bellenim Güncelleme
- Düzenli Şifre Değişiklikleri
- Sıfırlanmış En Konfigürasyonunun Yenilenmesi
- Kayıtlı En Ve İstemci Listesinin Güncellenmesi
- Erişim Kontrol Listesinin Denetlenmesi
- Güvenlik Kayıtlarının İncelenmesi



- 24/7 Saldırıları Tespit / Önleme,
- Penetrasyon Testleri
- Düzeltici/ Sıkılaştırıcı İşlemler



# Sorular



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