Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBIM)
Ulak-CSIRT (Computer Security Incident Response Team)

Network Access Kontrol
Ağ Erişim Kontrolü
(NAC)

Hüsnü Demir
hdemir @ metu.edu.tr
ODTÜ

Hüseyin Yüce
huseyin @ marmara.edu.tr
Marmara Ü.

Gökhan Akın
akingok@itu.edu.tr
İTÜ

NAC Nedir?

- NAC
  - Kullanıcı sistem güvenliğini sağlar.
    - Antivirüs
    - HIPS
    - Zayıflık Taraması
  - Kullanıcı veya sistem yetkilendirmesini sağlar
  - Ağ güvenlik denetlemesi yapar.
- En önemlisi bunların aynı anda sağlanmasını koordine eder.

NAC Amacı Nedir?

- 0-Gün saldırılarını karşılar veya etkisini azaltır.
  - Özellikle solucanlara (worm) karşı.
- Politikaların uygulanmasını sağlar.
  - OS denetlemesi.
- Yetki ve erişim denetimi uygular.
  - Kullanıcı bazlı erişim
  - Cihaz bazlı erişim

NAC

- Ağa erşimden önce veya sonra denetim yapılabilir.
- Agent kullanılabilir veya kullanılmaz.
- Inline veya degil.
  - Arada durabilir.
  - Anahtarlama cihazları sayesinde politikaları uygulayabilir.
- Eğer NAC izin vermez ise;
  - Kullanıcılar duruma göre kapalı bir ağa dahil edilebilir.
  - Kullanıcıların trafiği istenilen işlemlerin yapılabileceği bir ağa yönlendirilir.

Güvenli Erişim

- Bağlantıdan önce, cihaz uyumlu mu?
- Bağlantıdan sonra cihaz kabul edilebilir şekilde davranıyor mu?
- Kim bağlanmış?
- Hangi haklara sahip?
- Eğer bağlanamıyorsa veya uyumsuz ise ne yapılmalı?

Niye Önemli?

- Zararlı kullanıcı/cihazlardan oluşabilecek problemleri engeller
  - Yetkisiz erişimi engeller
  - Zararlı yazılımların ağın içerisine girmesini engeller.
- Güvenlik politikalarının uygulanmasını sağlar.
  - En iyi uygulama metodlarının seçilmesini sağlar.
  - Yönetilebilir/yönetilemez cihazlar
- Önemli kaynaklara erişimi düzenler

NAC Sorunları?

- Pahalı
- Kompleks
- Sorunlu

Zorunlu IEEE 802.1x

Zorunlu DHCP Kullanımı

Zorunlu Agent Kullanımı

Zorunlu Inline Yapılandırma

Ne yapalım?

- Ne amaçla NAC sistemi kurmak istediğimizi bilelim.
  - Çok gerekli mi?
  - Daha iyi alternatif var mı?
- Daha önce denenmiş iyi bir NAC yöntemi seçilmeli.
- Politikalar ve prosedürler iyi hazırlanmalı.
- Sorunlu kullanıcıların/cihazların durumu önceden ele alınmalı.

Önce

- Niye? Amaç?
  - Kurumsal amaçlar
  - İşlevsel/Ticari amaçlar
  - Teknik amaçlar
- Mevcut durum!
- Mevcut uygulamalar ile sizin amaçlarınıza uygun iyi bir çözüm seçimi.
- Başarı için her adım planlanmalı.

Kurumsal Amaçlar

- Kendi kullanım çevrenizi gözlemleyin, araştırın.
- Tüm çalışma koşullarınızın güncellenmiş olduğundan emin olun (yamalar, virus güncellemeleri gibi).
- Misafirleri ve yetkisiz kişileri zarar vermeyecekleri yerlerde tutun.
- Risk koşullarınızı değerlendirin. Ne kadar risk alınabilir?
- Her alan için farklı politiklar geliştirin. Ağın farklı bölgelerini bağımsız bir şekilde koruyun.
- Riskli cihazları karantina altına alın.

İşlevsel Amaçlar

- NAC'ı hangi aşamalarda uygulamak istiyorsunuz?
  - Niçin?
- Kazancınız ne olacak?
- Kurum içirisinde yapınız kaç parçadan oluşacak
- Hangi politikalara ihtiyaç duyacaksınız.
- NAC'ı kim yönetecek? Nasıl yönetilecek?
- İlk önce kim/neresi yapılacak? Örnek!
- Mevcut politikalar uygulanabilir mi?

Teknik Amaçlar

- Yönetim sunucusu nereye konumlanmalı?
- Politika uygulama sunucuları nerelerde olmalı?
- Hangi politikalar uygulanmalı? Politikalar nasıl zorlanmalı?
- Hangi Vlan'lar kullanılmalı?
- Misafirler, bilinmeyen cihazlar, yazıcılar, VOIP cihazları, önemli görevliler ve cihazlar ne olacak?
- Kullanıcı ne kadar deneyimli olmalı?

Uygulama Alanı

- Hangi tip cihazlara izin verilecek?
- Ağa erişen kullanıcı profilleri neler olacak?
  - Bunların kullanım becerileri ne olacak? Nasıl?
- Hangi tip erişim metodlarına izin verilecek?
  - Kablolu, kablosuz vs.
- Şu anda son kullanıcıya nasıl destek veriliyor?
- Mevcut ağ topolojisi?

Son Olarak

- Bu parametrelere cevap bulduktan sonra çözüme ulaşmak sorun olmayacaktır.

- Yönetilebilir ve ölçeklenebilir bir ağ kurulması her zaman için yararlı olacaktır.

TEŞEKKÜRLER

Hüsnü Demir
hdemir @ metu.edu.tr
ODTÜ

Hüseyin Yüce
huseyin @ marmara.edu.tr
Marmara Ü.

Gökhan Akın
akingok@itu.edu.tr
İTÜ