FastNAC

ACİL DURUM YÖNETİMİ

İçindekiler;

1. Operasyonel ve Siber Güvenlik Risk Senaryoları

FastNAC servislerinin durması durumunda karşılaşılabilecek temel riskler şunlardır:

1.1. Ağ Cihazlarının Erişimi Kaybetmesi

En büyük risk, ağ yönetim cihazlarının (switch/access point, vb.) FastNAC sunucusuna ulaşamadığında takınacağı tavırdır:

Risk: Ağa bağlanan her cihaz (yetkisiz veya zararlı olsa dahi) doğrudan ağa kabul edilir. Bu, ağın tamamen korumasız kalması demektir.

1.2. Hibrit Çalışma Yapısındaki Riskler

FastNAC, hibrit çalışma yapısını desteklediği için (hem Yeni Nesil hem de Radius tabanlı) oluşabilecek kesintiler aşağıda listelenmiştir:

RADIUS Kesintisi: 802.1X kimlik doğrulaması yapan kurumsal cihazların hepsi ağa giremez. Cihazlar bağlantı kesintisi yaşayabilir.

Yeni Nesil NAC Kesintisi: Politika/Profil sistemi devre dışı kalır . Yeni bağlanan cihazlar, herhangi bir politika sorgusu yapılamadığı için karantinaya alınamaz. Doğrudan ağa kabul edilir. Herhangi bir bağlantı kesintisi yaşanmaz.

1.3. Görünürlük Kaybı ve Yanıt Süreleri

Risk: FastNAC devre dışıyken ağa hangi cihazın, nereden ve ne zaman bağlandığına dair log üretilemez. Bir siber saldırı gerçekleşirse "Adli Bilişim" (Forensics) süreci imkansız hale gelir.

2. Olası Yalnış Kullanım Senaryoları

FastNAC üzerinde yapılabilecek hatalı bir profilleme veya politika, cihazların ağa bağlanmasını engelleyebilir.

2.1. Profilleme Hatası

Hatalı tanımlanan profiller, cihazın ilgili profile takılamamasını sağlar ve cihaz karantina ağına gidebilir.

2.2. Politika Hatası

Cihazlar için tanımlanan politikaların aksiyonu yalnış bir VLAN tanımı girilirse, ilgili cihaz yalnış girilen VLAN numarasına atabilir.

3. Müdahele ve Riski Azaltma

Kritik Müdahale Tablosu

Senaryo	Etki	Acil Aksiyon Planı
RADIUS Servis Durması	Kimlik doğrulama yapılamaz.	Switch üzerinde critical vlan veya auth-fail vlan yapılandırmasının aktif olduğundan emin olun.
SNMP İletişim Hatası	Cihaz profilleme ve port yönetimi durur.	Ağ cihazlarındaki SNMP topluluk (community) dizelerini ve ACL listelerini kontrol edin.
Tam Sistem Kesintisi	Tüm NAC fonksiyonları durur.	Yedekli (High Availability - HA) yapının devreye girip girmediğini kontrol edin.

4. Güvenli Yapılandırma Önerileri

High Availability (HA): FastNAC Cluster olarak kurulmalıdır.

Kritik VLAN Yapılandırması: Ağ cihazlarında Radius tipi kullanılıyorsa "Radius sunucuya ulaşılamazsa kullanıcıyı sınırlı bir VLAN'a (Guest/Quarantine) at" kuralı tanımlanmalıdır.

Log İzleme: FastNAC servislerinin durumu bir SIEM veya SNMP Monitoring aracı ile 7/24 izlenmeli, kesinti anında BT ekibine anlık alarm (SMS/E-posta) gitmelidir.

Düzenli Yedekleme: FastNAC sunucusunun yedekleri felaket kurtarma senaryoları için düzenli olarak alınmalıdır.