



## Ağ Güvenliği Politikalarında Giriş Seviyesinde Geliştirme ve Uygulama Planı

Mehrdad A. Mizani / Serkan Kenar  
Sistem ve Yazılım Uzmanları  
Labris Teknoloji

Kapsam: Bu doküman **orta ve altı büyüklükteki kurumlar** için Ağ Güvenliği Politikası geliştirmek ve uygulamak için eskiz halinde bir zaman planı sunmaktadır. Bu planın gelişmiş sürümleri ve çevresindeki tüm ek dokümanlar Labris Teknoloji'nin Profesyonel Güvenlik Servis Hizmetlerinin bazıını oluşturmaktadır.

Planda 5 bölüm vardır. Bunlar;

- o Kapsam Analizi (1-2 gün)
- o Ağ Analizi (4-5 gün)
- o Risk Analizi (2-3 gün)
- o Politika Geliştirme (en az 1 hafta)
- o Uygulama (yaklaşık bir hafta)

### Kapsam Analizi (KA)

Nelerin üzerine gidileceği ve nelerin üretileceğini belirler. Ağın sahip olduğu değerlerden hangilerinin bu AGP ile korunacağını belirler. Kapsam analizi aşağıdaki soruların yanıtları ile uğraşır:

- o Bu AGP personel sorumluluklarını içeriyor mu?
- o AGP fiziksel sınırlamaları içeriyor mu? (bina koruması, sistem odası koruması, iş istasyonu koruması...)
- o AGP bir Güvenlik Ekibi oluşturup rolleri tanımlıyor mu?
- o AGP yeni ekipman alımı içerebilir mi?
- o AGP uygulama ve eğitim içeriyor mu?
- o AGP yedekleme politikası içeriyor mu?

Bu bölüm yukarıda verilen cevaplar ile belirlenmiştir. Ayrıntılar iş başlangıcı ardından netleşecektir.

### Ağ Analizi (AA)

Derinlemesine ağ topolojisi belirlenmesi ve ağdaki varlıkların listesi bu bölümün çıktısıdır. Yazılım güvenliği için girdiler, yazılım sürümleri ile belirlenecektir.

- o Gerçek ağ topolojisinin belirlenmesi
- o Fiziksel makinelerin ve ağ cihazlarının, model ve yazılım sürümlerinin bulunması ve kimliklendirilmesi (işletim sistemi surumu, Web server surumu)
- o Ağ cihazlarının yapılandırılmaları (VLAN, erişim listeleri vb.)
- o Başarım ve yük testleri

- o Ekipmanların fiziksel analizi

Bu bölüm KA tarafından çerçevelenmiştir ve yaklaşık 4-5 gün alır. Müşterinin işbirliği çok önemlidir.

### Risk Analizi (RA)

Varlıkların değerlendirilmesi, önceliklendirilmesi bu bölümün çıktısıdır.

- o Varlıkları önceliklendir (tüm ağ birimleri)
- o Varlıklara tehditleri belirle
- o Risklerin ve tehditlerin önceliklendirilmiş varlıklar ile değerlendirilmesi

Bu bölüm 2-3 gün alacaktır. Müşteri işbirliği gereklidir.

### Politika Belirlenmesi (PB)

Kullanıcıların rollerinin belirleneceği bir politika bu bölümün çıktısıdır. Politika tüm önceki bölümlerdeki çıktılara göre oluşturulacaktır.

- o yeni ağ topolojisinin oluşturulması
- o Düşük, orta ve yüksek risk için politikalar oluşturulması:
  1. erişim kontrolü
  2. yetkilendirme
  3. fiziksel güvenlik
  4. anahtar güvenliği (yetkilendirme)
  5. denetleme
  6. izleme
  7. gözden geçirme
- o farklı tip olaylar için politika kontrol listeleri (ağa yeni makine eklenmesi, yeni kullanıcı eklenmesi, şifre doğrulamalar...)
- o oluşan olaylarda hareketler ve felaket kotası planları
- o kullanıcı eğitim planları
- o kabul edilebilir kullanım politikası
- o doğrulama ve yetkilendirme politikası
- o internet erişim politikası
- o iç ağ erişim politikası
- o uzaktan erişim politikası (dial-up, VPN,...)

Bu bölüm topolojiye bağlı olarak 5-6 gün alacaktır.

### Uygulama (DE)

Uygulanması bu AGP'nin kapsamında olmamakla beraber bir önceki bölümde çıkarılan politikaya istinaden ağın hangi birimlerinde neler yapılması gerektiği ile ilgili ayrıntı işler çıkarılacaktır.

- o Yeni ağ politikasının oluşturulması
- o Yazılım güvenlik arttırmaları (Güncellemeler,

yamalar...)

- o Anahtar güçlendirme
- o Personel eğitimi

Bu bölüm politikaya bağlı olarak yaklaşık 1 hafta olacaktır.