TR CYBERSECURITY ALLIANCE

Ağ Güvenliği ve Siber Dayanıklılık için 10 Temel Adım

GİRİŞ

Karmaşıklaşan dijital altyapılar ve sürekli evrim geçiren tehdit ortamı, kurumların güçlü bir **ağ güvenliği** ve **siber dayanıklılık** stratejisine sahip olmasını zorunlu kılıyor. **TR Cybersecurity Alliance** olarak bu toplantımızda, ağların korunması, hizmet sürekliliğinin sağlanması ve siber tehditlere karşı hızlı toparlanma yetkinliğinin artırılması konularına odaklandık. Bu doğrultuda hazırladığımız bu rehber, kuruluşların güvenlik seviyesini sistematik olarak güçlendirmesi ve siber dayanıklılığını artırması için uygulanabilir 10 temel adımı içermektedir.

1. Ağ Segmentasyonu ile Saldırı Yüzeyini Azaltın

Ağınızı mantıksal olarak farklı segmentlere ayırmak, özellikle hassas sistemlerin diğerlerinden izole edilmesini sağlar. Böylece bir saldırgan ağa sızsa bile, yatay hareket alanı sınırlanır. VLAN'lar, DMZ'ler ve mikro-segmentasyon teknikleri bu amaçla kullanılabilir.

2. Zero Trust Mimarisini Benimseyin

Zero Trust yaklaşımı, hiçbir kullanıcıya veya cihaza otomatik olarak güvenmemeyi esas alır. Erişim izinleri sürekli olarak doğrulanmalı ve cihazların güvenlik durumu izlenmelidir. Bu mimari, kimlik doğrulama, cihaz denetimi ve erişim kontrollerinin merkezde olduğu bir anlayışı benimser.

3. Gelişmiş İzleme ve Günlükleme Sistemlerini Kullanın

Ağ trafiği, kullanıcı davranışları ve sistem olaylarının gerçek zamanlı olarak izlenmesi olası tehditlerin erkenden tespit edilmesini sağlar. SIEM ve NDR (Network Detection and Response) sistemleri, şüpheli aktiviteleri otomatik olarak işaretler ve müdahale sürecini hızlandırır.

4. Ağ Cihazlarını Bilin, Güncel ve Güvenli Tutun

Ağda çalışan tüm cihazlar, bir varlık yönetim sistemi aracılığıyla görünür hale getirilmelidir. Ağ geçitleri, yönlendiriciler, anahtarlar ve güvenlik duvarları gibi donanımlar üzerinde çalışan yazılımların zafiyet analizleri yapılmalı ve düzenli olarak güncellenmelidir. Yazılımlar güncel olsa bile, hatalı konfigürasyonların zafiyete yol açabileceği unutulmamalı ve CIS Benchmark sıkılaştırma kılavuzları baz alınarak güvenli konfigürasyonlar uygulanmalıdır. Bu süreçlerin bir parçası olarak siber hijyen uygulamaları, sistem yöneticilerinin günlük sorumlulukları arasında yer almalıdır.

5. Ağ Dayanıklılığı için Yedeklilik Mekanizmaları Kurun

Kritik servislerde donanım ve bağlantı yedeklemeleri yapılmalı, felaket senaryolarına karşı otomatik geçiş (failover) mekanizmaları devreye alınmalıdır. Bu sayede donanım arızaları, kesintiler veya saldırılar sırasında hizmet sürekliliği sağlanabilir.

6. Yapay Zeka Destekli Tehdit Tespiti Uygulayın

AI ve ML tabanlı ağ güvenlik çözümleri, normal dışı davranışları analiz ederek geleneksel imza tabanlı sistemlerin kaçırabileceği tehditleri tespit edebilir. Özellikle bilinmeyen saldırı tekniklerine ve anomali tabanlı analizlere karşı etkili bir koruma sağlar.

7. Bulut Tabanlı Ağları Ayrı Segmentlerde Yönetin

Bulut altyapılarına erişim, kurum içi ağdan izole edilerek ayrı segmentlerde ele alınmalıdır. Hibrit ortamlarda bu tür izolasyon, bir bulut ihlalinin iç ağa yayılmasını engeller ve erişim kontrolünü merkezi şekilde yönetilebilir hale getirir.

8. Ağ Erişim Politikalarını Mikro Düzeyde Tanımlayın

Her kullanıcıya ve cihaz grubuna sadece ihtiyaç duyduğu kadar erişim izni verilmelidir (Least Privilege). Bu yaklaşım, içeriden kaynaklanabilecek riskleri de azaltır. Network Access Control (NAC) ürünleri ile Role-Based Access Control ve Attribute-Based Access Control politikaları kullanılarak erişim ve erişim denetimleri sıkılaştırılmalıdır.

9. Olay Müdahale ve Kurtarma Planlarını Test Edin

Ağ tabanlı bir ihlal veya hizmet kesintisi durumunda hızlı ve etkili müdahale kritik önemdedir. Bu nedenle, olay müdahale planları belirli aralıklarla test edilmeli ve güncellenmelidir. Masa başı tatbikatlar ve simülasyonlar ile ekibin müdahale refleksleri diri tutulmalıdır.

10. Sürekli Eğitim, Farkındalık ve Siber Hijyen Programları Yürütün

En güçlü teknoloji bile insan hatalarına karşı savunmasızdır. Çalışanlara ağ güvenliği, kimlik avı saldırıları, sosyal mühendislik ve siber hijyen konularında sürekli eğitim verilmeli, güvenlik kültürü kurum genelinde yerleştirilmelidir. Siber hijyenin bir alışkanlık haline gelmesi, günlük dijital davranışlarda daha dikkatli ve güvenli olunmasını sağlar.

SONUÇ

Ağ güvenliği ve siber dayanıklılık yalnızca teknolojik yatırımlarla sağlanamaz. Bunun için doğru yapılandırmalar, sürekli izleme, yetkin insan kaynağı ve güçlü bir siber hijyen kültürü gereklidir. Bu belgede yer alan her adım, kurumların tehditleri erken tespit etmesini ve hızla önlem almasını sağlar. Aynı zamanda olası ihlallere hızlı yanıt verilmesini ve kritik hizmetlerin kesintisiz sürdürülmesini hedefler. TR Cybersecurity Alliance olarak, ülkemizde siber güvenlik bilincini artırmak için çalışıyoruz. En iyi uygulamaların yaygınlaşması adına çabamızı kararlılıkla sürdürüyoruz.

Çalışmaya Katkıda Bulunan Üyelerimiz

Ahmet Özkan
Ali Fuat Türkay
Ali Tursun
Asım Yıldız
Caner Dağlı
Çağrı Güven
Ekrem Kolday
Fatih Özen
Fuat Kılıç
Kadir Çakıcı
Mehmet Üner
Mehtap Kılıç
Merih Önder
Metin Eser
Murat Zaralı
Serkan Akcan
Serkan Kırmızıgül
Yasin Durgaç