Denetci.org

REFERANS İLKELERİ

Ağ Güvenliği İlkeleri

Rİ-ALT-2

Sürüm 1.0 · 11.08.2026

www.denetci.org

Ağ Güvenliği İlkeleri

Ağ güvenliği, sistemler arasındaki iletişimin hangi güven sınırları içinde gerçekleşebileceğini ve bir ağ üzerindeki erişimin ne ölçüde etki oluşturabileceğini ele alır. Amaç belirli bir ağ mimarisi, segmentasyon modeli veya güvenlik ürünü öngörmek değil; bağlantının güven anlamına gelmediği ve ağın sistemler arasındaki güven ilişkilerini bilinçli biçimde sınırlandırdığı bir tasarım anlayışı ortaya koymaktır.

İlke 1: Ağ üzerindeki konum tek başına güven kaynağı olmamalıdır.

Bir kullanıcının veya sistemin belirli bir kurum ağına, yerel ağa, veri merkezine ya da bulut ortamına bağlanabilmesi kimliğinin, amacının veya erişim hakkının kendiliğinden güvenilir olduğu anlamına gelmez. Ağ konumu güvenlik kararına katkı sağlayabilir; ancak başka güven unsurlarının yerine geçmemelidir.

İlke 2: Ağ sınırları gerçek güven ve etki farklarını yansıtmalıdır.

Ağların bölünmesi yalnızca teknik veya idari düzen amacı taşımamalıdır. Farklı güven düzeyleri, işlevler veya olası etkiler arasında anlamlı ayrım varsa ağ mimarisi de bu ayrımı mümkün olduğu ölçüde desteklemelidir.

İlke 3: Bağlantı kurabilmek genel bir erişim hakkına dönüşmemelidir.

Bir sistemin başka bir sisteme ağ üzerinden ulaşabilmesi, hedefin bütün servis ve işlevlerine erişebilmesi anlamına gelmemelidir. İletişim imkânı, gerekli taraflar ve gerekli etkileşimlerle sınırlı bir güven ilişkisi olarak ele alınmalıdır.

İlke 4: Ağdaki bir güven kaybının yayılabileceği alan sınırlı olmalıdır.

Bir uç noktanın, sunucunun veya ağ alanının ele geçirilmesi ilgisiz sistemlere sınırsız biçimde ilerleme imkânı vermemelidir. Ağ tasarımı yalnızca saldırının girişini engellemeyi değil, giriş başarılı olduğunda etkinin ne kadar ilerleyebileceğini de dikkate almalıdır.

İlke 5: Yönetim iletişimi olağan iletişimden farklı bir güven ilişkisi olarak görülmelidir.

Bir sistemi yönetebilen trafik, o sistemi yalnızca kullanan trafikten daha geniş etki oluşturabilir. Yönetim yollarının sıradan erişimin doğal uzantısı haline gelmesi, bir kullanıcı veya sistemin kaybını daha geniş bir güven kaybına dönüştürmemelidir.

İlke 6: Ağın kontrolünü sağlayan bileşenler taşıdıkları güvene göre değerlendirilmelidir.

Yönlendirme, ad çözümleme, uzaktan erişim, ağ politikası veya benzeri işlevleri sağlayan bileşenler çok sayıda sistem arasındaki iletişimi etkileyebilir. Bu bileşenlerin önemi yalnızca üzerlerinden geçen veriden değil, ağın davranışını değiştirebilme güçlerinden kaynaklanır.

İlke 7: İletişimin hedefi yalnızca ağ adresine duyulan güvene dayanmamalıdır.

Adresler, isimler ve ağ yolları değiştirilebilir, yeniden kullanılabilir veya yanıltıcı hale gelebilir. Güven gerektiren iletişimlerde hedefin gerçekten amaçlanan taraf olduğuna ilişkin güven, yalnızca paketin doğru adrese gitmesine indirgenmemelidir.

İlke 8: İletişimin gizliliği, iletişimin meşru olduğu anlamına gelmemelidir.

Şifrelenmiş bir bağlantı içeriğin korunmasını sağlayabilir; ancak hangi tarafların konuştuğunu, iletişimin gerekli olup olmadığını veya aktarılan işlemin yetkili olduğunu tek başına açıklamaz. İletişimin korunması ile iletişime güvenilmesi aynı şey değildir.

İlke 9: Güvenli ağ, güvensiz uç sistemleri güvenilir hale getirmemelidir.

Ağ üzerindeki korumalar uç sistemlerin kimlik, yetki, yapılandırma ve güvenlik ihtiyaçlarının yerine geçmez. Bir sistemin yalnızca korunan bir ağ içinde bulunması kendi güvenlik özelliklerinin zayıf bırakılmasının gerekçesi olmamalıdır.

İlke 10: İçeri ve dışarı yönlü iletişim aynı güven modelinin parçalarıdır.

Güvenlik yalnızca dışarıdan gelen bağlantıları sınırlandırmakla kurulamaz. Ele geçirilmiş veya hatalı çalışan bir sistemin dışarıya hangi taraflarla ve hangi amaçlarla iletişim kurabildiği de ortaya çıkabilecek etkinin bir parçasıdır.

İlke 11: Dış ağlarla kurulan ilişkiler güven sınırını görünmez biçimde genişletmemelidir.

İnternet, iş ortakları, bulut hizmetleri, uzak kullanıcılar veya başka ağlarla kurulan bağlantılar farklı güven alanlarını birbirine bağlar. Bir bağlantının operasyonel olarak gerekli olması, iki tarafın aynı güven düzeyinde kabul edilmesini gerektirmez.

İlke 12: Ağ sınırının fiziksel olması güvenlik açısından zorunlu değildir.

Sanal ağlar, bulut ağları, yazılım tanımlı politikalar ve benzeri mantıksal sınırlar gerçek güven ayrımları oluşturabilir. Güvence, sınırın fiziksel cihazlardan oluşmasına değil fiilen hangi iletişimi ve etkiyi ayırabildiğine dayanmalıdır.

İlke 13: Ağ değişiklikleri mevcut güven ilişkilerini fark edilmeden değiştirmemelidir.

Yeni bağlantılar, yönlendirmeler, servisler veya geçici çözümler daha önce birbirinden ayrılmış alanlar arasında yeni yollar oluşturabilir. Ağdaki bir değişiklik, yalnızca bağlantı değişikliği değil güven modelini değiştirebilen bir olay olarak görülmelidir.

İlke 14: Geçici bağlantılar kalıcı ve gerekçesiz güven yollarına dönüşmemelidir.

Bakım, taşıma, destek veya olağanüstü ihtiyaç nedeniyle oluşturulan ağ erişimleri zamanla normal mimarinin parçası haline gelebilir. Bir bağlantının geçmişte gerekli olması, gelecekte de aynı güven ilişkisinin korunması için yeterli gerekçe değildir.

İlke 15: Ağ güvenliği tek bir koruma noktasının kusursuzluğuna bağlı olmamalıdır.

Tek bir güvenlik duvarı, geçit, ağ politikası veya başka bir mekanizmanın varlığı bütün ağın güvenli olduğunu göstermez. Kritik güven sınırları, tek bir bileşenin hatası veya ele geçirilmesiyle bütünüyle anlamsız hale gelmemelidir.

İlke 16: Ağın kullanılabilirliği ile güvenliği birbirinden kopuk tasarlanmamalıdır.

Bir güvenlik mekanizmasının kaybı sırasında iletişimin nasıl devam edeceği önemli bir güven kararıdır. Kullanılabilirliği korumak adına ağ sınırlarının fark edilmeden kaldırılması veya bütün erişimin genişletilmesi sistemin doğal hata davranışı olmamalıdır.

İlke 17: Görülemeyen ağ davranışı güvenli davranış olarak kabul edilmemelidir.

Şifreleme, yeni protokoller, bulut hizmetleri veya teknik sınırlamalar bazı iletişimlerin içeriğini ya da bağlamını görünmez hale getirebilir. Görünürlüğün bulunmaması, bu trafiğin meşru veya düşük riskli olduğunun kanıtı değildir.

İlke 18: Ağ güvenliği gerçek iletişim davranışı üzerinden doğrulanabilmelidir.

Ağ diyagramları, kurallar veya segment isimleri tek başına güven sınırlarının gerçekten çalıştığını göstermez. Güvence; hangi tarafların fiilen iletişim kurabildiği, bu iletişimin hangi sınırlar içinde gerçekleştiği ve bir güven kaybının ağ üzerinden ne kadar ilerleyebildiği üzerinden değerlendirilebilmelidir.