Denetci.org

REFERANS İLKELERİ

Uzaktan Erişim Güvenliği İlkeleri

Rİ-KIM-4

Sürüm 1.0 · 11.08.2026

www.denetci.org

Uzaktan Erişim Güvenliği İlkeleri

Uzaktan erişim güvenliği, kullanıcıların ve sistemlerin kuruluşun doğrudan fiziksel veya ağsal kontrolü dışında bulunan ortamlardan kaynaklara erişmesinden doğan güven ilişkilerini ele alır. Amaç belirli bir VPN, uzak masaüstü veya erişim teknolojisi zorunlu kılmak değil; konumun güvenin yerine geçmediği, kullanıcı, cihaz, oturum ve hedef kaynağın birlikte değerlendirildiği bir erişim anlayışı oluşturmaktır.

İlke 1: Uzak veya yerel konum tek başına erişimin güvenilirliğini belirlememelidir.

Bir kullanıcının kurum binasında veya kurumsal ağda bulunması güvenilir olduğunu; dışarıda bulunması da otomatik olarak güvensiz olduğunu göstermez. Erişim, konumdan daha anlamlı kimlik ve yetki unsurlarına dayanmalıdır.

İlke 2: Uzak bağlantı kurabilmek genel sistem erişimi hakkı oluşturmamalıdır.

Bir uzak erişim hizmetine başarıyla bağlanan taraf yalnızca bu nedenle bütün iç ağ veya uygulamalara erişebilmemelidir. Bağlantı sağlamak ile belirli bir kaynağı kullanmaya yetkili olmak ayrı güven kararlarıdır.

İlke 3: Uzaktan erişimin kapsamı gerçek görev ve kaynak ihtiyacını yansıtmalıdır.

Bir kullanıcının belirli bir uygulamaya ihtiyacı varsa bütün ağ alanına erişim verilmesi gerekli olmayabilir. Erişim kapsamı kullanılan teknolojinin kolaylıklarına göre değil gerçek işlev üzerinden belirlenmelidir.

İlke 4: Kullanıcı kimliği ile uzak cihazın güveni birbirinin yerine geçmemelidir.

Doğru kullanıcı kimliği bilinmesine rağmen cihaz ele geçirilmiş veya güvenlik açısından uygun olmayan durumda olabilir. Aynı şekilde güvenilir bir cihaz da onu kullanan kişinin yetkisini kanıtlamaz.

İlke 5: Kuruluş dışındaki cihaz ve çalışma ortamının belirsizliği erişim modeline yansıyabilmelidir.

Uzaktaki cihazın kimler tarafından kullanıldığı, hangi yazılımları çalıştırdığı veya veriyi nasıl sakladığı her zaman bilinmeyebilir. Bu belirsizlik özellikle hassas veri ve yüksek etkili işlemlerde önemsiz kabul edilmemelidir.

İlke 6: Uzaktan erişim bağlantısının korunması erişimin meşruluğunun yerine geçmemelidir.

Şifrelenmiş bir bağlantı veri aktarımını koruyabilir; ancak bağlanan kullanıcının yetkili olduğunu veya hedef kaynağın doğru taraf olduğunu tek başına göstermez. İletişim güvenliği kimlik ve yetki sınırlarını desteklemelidir.

İlke 7: Uzak taraf ve erişim hizmetinin kimliği anlamlı biçimde doğrulanabilmelidir.

Kullanıcı veya istemci, kimlik bilgilerini ve oturumunu gerçekten amaçlanan erişim altyapısına verdiğine güvenebilmelidir. Sahte veya ele geçirilmiş aracılar güven ilişkisini görünmez biçimde devralmamalıdır.

İlke 8: Uzaktan erişim altyapısı taşıdığı geniş güven nedeniyle kritik bir güven alanı olarak görülmelidir.

Uzak erişim geçitleri ve benzeri bileşenler çok sayıda kullanıcıyı iç sistemlere bağlayabilir. Bu altyapının kaybı, tek bir uç sistemin kaybından daha geniş sonuç oluşturabileceği için sıradan bağlantı bileşeni sayılmamalıdır.

İlke 9: Uzaktan erişim hizmetini kullanabilmek onu yönetme yetkisi oluşturmamalıdır.

Kullanıcı trafiği ile erişim altyapısının yönetim düzlemi farklı etki alanlarıdır. Normal uzaktan erişim kullanıcısı aynı yol üzerinden erişim sisteminin güvenlik durumunu değiştirememelidir.

İlke 10: Uzak yönetim olağan kullanıcı erişiminden farklı bir güven düzeyi taşımalıdır.

Sunucu, ağ, güvenlik altyapısı veya başka kritik bileşenleri uzaktan değiştirebilmek olağan uygulama kullanımından daha geniş sonuç oluşturur. Bu erişimin kapsamı ve dayandığı güven de buna göre farklılaşabilmelidir.

İlke 11: Aracı erişim katmanları hedef sistemin kendi güvenlik sınırlarının yerine geçmemelidir.

Kontrollü bir geçit veya yönetim ara sistemi erişimi sınırlandırabilir ve görünürlük sağlayabilir. Bununla birlikte bu katmandan geçmiş olmak hedef sistemde her işlemin yetkili olduğu anlamına gelmemelidir.

İlke 12: Uzaktan erişim oturumu ilk doğrulamanın sonsuz devamı olarak görülmemelidir.

Zaman içinde kullanıcı, cihaz ve risk koşulları değişebilir; oturum ele geçirilebilir veya artık gerekli olmayabilir. Aktif oturumun güveni kendi yaşam süresi boyunca korunmalı ve gerektiğinde yeniden değerlendirilebilmelidir.

İlke 13: Oturumun sona erdirilmesi gerçek erişim yeteneğini sona erdirebilmelidir.

İstemci penceresinin kapanması veya kullanıcının çıkış yapması arka plandaki belirteç ve oturumların hâlâ geçerli olmadığı anlamına gelmelidir. Gerektiğinde kuruluş da riskli aktif oturumları bağımsız biçimde sona erdirebilmelidir.

İlke 14: Uzak erişim ihtiyacı erişimin süresiz olmasını gerektirmemelidir.

Destek, proje, seyahat veya başka geçici ihtiyaçlar için verilen erişim ihtiyaç sona erdiğinde yaşamaya devam etmemelidir. Uzun süredir kullanılmayan erişim de saldırı yüzeyi oluşturmaya devam eder.

İlke 15: Olağan dışı bağlantı özellikleri mutlak karar yerine güven sinyali olarak kullanılmalıdır.

Zaman, coğrafya, cihaz veya eşzamanlı kullanım bazı durumlarda ele geçirilmiş kimliğe işaret edebilir; başka durumlarda tamamen meşru olabilir. Bağlam sinyalleri güven kararını desteklemeli ancak sahte kesinlik üretmemelidir.

İlke 16: Uzaktan çalışma verinin gereksiz biçimde uzak cihaza taşınmasını gerektirmemelidir.

Bir uygulamaya erişebilmek onun verilerini yerel diske, panoya, yazıcıya veya başka ortamlara sınırsız biçimde aktarabilmek anlamına gelmez. Veri hareketi kendi güvenlik etkisine göre sınırlandırılmalıdır.

İlke 17: Uzaktan destek yeteneği kalıcı ve görünmez bir yönetim yoluna dönüşmemelidir.

Geçici destek ihtiyacı geniş yetkili ve sürekli kullanılabilen bir erişimin sessizce cihazda veya sistemde bırakılmasını haklı çıkarmamalıdır. Kalıcı destek gerekiyorsa bu erişim gerçek güven modelinin açık bir parçası olmalıdır.

İlke 18: Acil uzaktan erişim olağan güven modelinin kolay alternatifi olmamalıdır.

Normal kimlik veya bağlantı altyapısı kullanılamadığında bağımsız bir yol gerekli olabilir. Bu yol günlük kullanım için daha kolay bir arka kapıya dönüşmemeli ve normal erişimden farklı güven sonucuna sahip olduğu açık olmalıdır.

İlke 19: Uzaktan erişim görünürlüğü yalnızca bağlantının kurulduğunu göstermekle sınırlı kalmamalıdır.

Önemli durumlarda hangi kimliğin, hangi cihaz ve oturum bağlamında hangi kaynaklara eriştiği anlaşılabilmelidir. Ortak ağ geçitleri veya aracılar gerçek kullanıcı bağlamını tamamen yok etmemelidir.

İlke 20: Uzaktan erişim güvencesi gerçek erişim yolları üzerinden doğrulanabilmelidir.

Bir VPN, erişim portalı veya güvenlik ürünü kullanılması tek başına güvence değildir. Uzaktaki bir tarafın gerçekte hangi sistemlere ulaşabildiği, hangi kimlik ve cihaz güvenine dayanarak eriştiği, hangi veriyi dışarı taşıyabildiği ve erişim sona erdirildiğinde kullanılabilir yolların gerçekten kapandığı gösterilebilmelidir.