Denetci.org

REFERANS İLKELERİ

Uç Nokta Güvenliği İlkeleri

Rİ-ALT-3

Sürüm 1.0 · 11.08.2026

www.denetci.org

Uç Nokta Güvenliği İlkeleri

Uç nokta güvenliği, kullanıcıların ve iş yüklerinin kuruluş sistemleriyle etkileştiği cihazların taşıdığı güveni ve oluşturabileceği etkiyi ele alır. Uç noktalar masaüstü ve dizüstü bilgisayarları, mobil cihazları, iş istasyonlarını ve benzeri istemci sistemlerini kapsayabilir. Amaç belirli bir işletim sistemi veya güvenlik ürünü zorunlu kılmak değil; cihazın ele geçirilebileceği, kaybolabileceği ve kullanıcı hatasına maruz kalabileceği kabulü altında oluşturabileceği güven kaybını sınırlandırmaktır.

İlke 1: Uç nokta güvenilir kabul edilen bir araç değil bağımsız bir güven alanı olarak görülmelidir.

Bir cihaz kuruluş tarafından sağlanmış veya yönetiliyor olsa bile hata yapabilir, ele geçirilebilir veya yanlış kullanılabilir. Üzerinde bulunan güven ilişkileri bu olasılığı dikkate almalıdır.

İlke 2: Uç noktanın güven düzeyi taşıdığı veri ve erişimle ilişkili olmalıdır.

Bütün cihazlar aynı işlevi ve etkiyi oluşturmaz. Kritik yönetim yetkileri veya hassas veriler taşıyan cihazların güvenlik gereksinimleri daha düşük etkili kullanım cihazlarından farklı olabilir.

İlke 3: Bir kullanıcının yetkileri gereksiz biçimde cihazın bütünlüğüne bağlanmamalıdır.

Kullanıcı hesabının geniş yetkileri ele geçirilmiş bir uç noktadan kullanılabiliyorsa cihaz kaybı doğrudan daha büyük bir güven kaybına dönüşebilir. Kimlik ve cihaz güveni birlikte değerlendirilebilmeli ancak biri diğerinin yerini almamalıdır.

İlke 4: Olağan kullanıcı faaliyeti gereksiz yönetim yetkisi gerektirmemelidir.

Bir kullanıcının günlük işlerini yerine getirmesi cihazın güvenlik ayarlarını veya sistem genelindeki davranışı sınırsız biçimde değiştirebilmesini gerektirmez. Yönetim gücü olağan kullanımın doğal uzantısı olmamalıdır.

İlke 5: Yerel yönetim yetkisi taşıdığı gerçek etkiye göre sınırlandırılmalıdır.

Cihaz üzerindeki yüksek yetki güvenlik mekanizmalarını değiştirebilir, diğer kullanıcıların verisine erişebilir veya kalıcı yazılım çalıştırabilir. Bu güç yalnızca “yerel” olduğu için düşük riskli kabul edilmemelidir.

İlke 6: Uç noktanın başlangıç durumu gereksiz hizmet, yazılım ve yetki üretmemelidir.

Kullanılmayan özellik ve bileşenler saldırı ve bakım yüzeyi oluşturmaya devam eder. Cihazın işlevi için gerekli olmayan yetenekler doğal ve kalıcı çalışma durumunun parçası olmamalıdır.

İlke 7: Uç noktadaki güvenlik yapılandırması kullanıcı kolaylığıyla sessizce aşınmamalıdır.

Günlük sorunları çözmek için yapılan yerel istisnalar veya geçici değişiklikler zamanla cihazın gerçek güvenlik durumunu değiştirebilir. Amaçlanan yapılandırma ile çalışan durum arasındaki fark görünmez kalmamalıdır.

İlke 8: Uç noktanın gerçek güvenlik durumu merkezi kayıtlardan farklı olabilir.

Bir yönetim sistemi cihazı uyumlu veya güncel gösterirken cihaz üzerindeki gerçek davranış farklılaşmış olabilir. Güvence yalnızca yönetim aracında görünen duruma değil cihazın fiilî özelliklerine dayanmalıdır.

İlke 9: Desteklenen ve güvenilir biçimde güncellenebilen yazılım uç nokta güveninin parçasıdır.

İşletim sistemi, uygulamalar ve cihaz yazılımları zaman içinde yeni zayıflıklar taşıyabilir. Güncellik yalnızca sürüm numarası değil güvenlik düzeltmelerinin güvenilir biçimde uygulanabilir olması açısından anlam taşımalıdır.

İlke 10: Güncelleme mekanizması cihaz üzerinde geniş kod çalıştırma gücü taşıyan bir güven yolu olarak görülmelidir.

Güncellemeler yüksek ayrıcalıkla yeni yazılım taşıyabilir. Bu yolun kaybı çok sayıda cihazın aynı anda ele geçirilmesine neden olabileceği için sıradan bakım mekanizması olarak değerlendirilmemelidir.

İlke 11: Uç nokta üzerinde çalışan yazılım ihtiyaç duyduğu yetkiyle sınırlı olmalıdır.

Bir uygulamanın çalışması cihazın tamamını veya diğer kullanıcıların verilerini kontrol etmesini gerektirmeyebilir. Yazılımın sahip olduğu yetki, işlevinin gerçek ihtiyacını aşmamalıdır.

İlke 12: Uç noktaya kurulan üçüncü taraf yazılımı kuruluşun güven modelinin parçasıdır.

Eklentiler, yardımcı araçlar ve başka yazılımlar kullanıcı adına veri okuyabilir veya sistem üzerinde işlem yapabilir. Kullanıcı tarafından edinilmiş veya dışarıdan sağlanmış olması bu yazılımın güvenlik etkisini ortadan kaldırmaz.

İlke 13: Uç noktadaki hassas veri yalnızca gerçek ihtiyaç kadar bulunmalıdır.

Yerel kopyalar cihaz kaybı, kötü amaçlı yazılım veya başka kullanıcıların erişimi halinde yeni bir veri kaybı alanı oluşturabilir. Kullanım için gerekli olmayan hassas verinin cihazda kalıcılaşması varsayılan davranış olmamalıdır.

İlke 14: Veri koruması yalnızca cihaz açık değilken oluşabilecek kayıplara odaklanmamalıdır.

Depolama şifrelemesi kapalı veya kayıp cihazdaki veriyi koruyabilir; ancak oturum açıkken çalışan zararlı yazılım veya yetkili kullanıcı veriye erişebilir. Uç nokta veri güvenliği farklı kullanım durumlarını birlikte ele almalıdır.

İlke 15: Sırlar ve kimlik bilgileri cihaz üzerinde gereksiz biçimde kalıcılaşmamalıdır.

Parolalar, belirteçler, anahtarlar ve oturum bilgileri cihaz ele geçirildiğinde başka sistemlere erişim sağlayabilir. Uç nokta kaybının etkisi, cihazın kendisinden daha geniş güven alanlarına yayılmamalıdır.

İlke 16: Tarayıcı ve kullanıcı oturumu önemli güven unsurları olarak görülmelidir.

Çok sayıda kurumsal uygulamanın erişimi tarayıcı oturumları veya benzeri istemci durumları üzerinden taşınabilir. Cihazı kullanan başka bir tarafın bu aktif güveni kolayca devralabilmesi ölçüsüz sonuç oluşturmamalıdır.

İlke 17: Harici veri ve cihazlar güvenilir kaynaktan geliyor varsayımıyla işlenmemelidir.

Dosyalar, taşınabilir ortamlar ve bağlı çevre birimleri kullanıcı niyeti dışında kod, veri veya yeni güven ilişkileri taşıyabilir. Fiziksel olarak cihaza bağlanabilmek sınırsız güven oluşturmamalıdır.

İlke 18: Güvenlik araçları cihazın geri kalanından bağımsız ve kusursuz kabul edilmemelidir.

Koruma, izleme veya yönetim yazılımları da hata yapabilir, devre dışı bırakılabilir veya ele geçirilebilir. Bir güvenlik ürününün kurulu olması uç noktanın güvenilir olduğuna ilişkin nihai kanıt olmamalıdır.

İlke 19: Güvenlik görünürlüğünün kaybı cihazın güvenilir olduğu şeklinde yorumlanmamalıdır.

Bir uç noktadan beklenen güvenlik sinyallerinin gelmemesi cihazda sorun olmadığı anlamına gelmeyebilir. Görünürlük kaybı güven düzeyini etkileyen ayrı bir belirsizlik olarak değerlendirilebilmelidir.

İlke 20: Cihaz kaybı veya ele geçirilmesi bağlı güven ilişkilerinin yeniden değerlendirilmesini tetikleyebilmelidir.

Bir cihazın kaybolması yalnızca donanım kaybı değildir; üzerinde bulunan oturumlar, anahtarlar ve erişimler de etkilenmiş olabilir. Cihaza bağlı güven başka sistemlerde de gerektiğinde sona erdirilebilmelidir.

İlke 21: Bir uç noktanın kullanım dışına çıkarılması verinin ve güven unsurlarının yaşamını sona erdirebilmelidir.

Cihazın kullanıcıdan alınması veya envanterden çıkarılması üzerinde bulunan verinin, kimlik bilgisinin ve erişim ilişkilerinin gerçekten ortadan kalktığını tek başına göstermez. Yaşam döngüsünün sonu gerçek kullanılabilir güven üzerinden değerlendirilmelidir.

İlke 22: Uç nokta güvencesi cihazın gerçek davranışı üzerinden doğrulanabilmelidir.

Envanter kaydı, güvenlik ajanı, şifreleme durumu veya uyum raporu tek başına güvence oluşturmaz. Cihazın gerçekte hangi yetkilere ve verilere sahip olduğu, güvenlik sınırlarının kullanıcı veya yazılım tarafından ne ölçüde değiştirilebildiği ve cihaz kaybedildiğinde bağlı güvenin gerçekten sınırlandırılabildiği gösterilebilmelidir.