Denetci.org

REFERANS İLKELERİ

Ayrıcalıklı Erişim İlkeleri

Rİ-KIM-2

Sürüm 1.0 · 11.08.2026

www.denetci.org

Ayrıcalıklı Erişim İlkeleri

Ayrıcalıklı erişim, bir sistemin yapılandırmasını, güvenlik durumunu, kimliklerini, verisini veya çalışmasını olağan erişimden daha geniş ölçüde etkileyebilen yetkileri ifade eder. Amaç belirli bir ayrıcalıklı erişim ürünü veya yönetim süreci tarif etmek değil; yüksek etkili yetkinin olağan erişimden farklı bir güven ilişkisi olarak ele alınmasını ve bu gücün gereksiz biçimde yoğunlaşmamasını sağlayan tasarım anlayışını ortaya koymaktır.

İlke 1: Ayrıcalıklı erişim olağan erişimden ayrı bir güven durumu olmalıdır.

Bir kişi veya sistem günlük faaliyetlerini yerine getirirken sürekli olarak yüksek yetki taşımamalıdır. Ayrıcalık gerektirmeyen kullanım ile sistemi geniş ölçüde değiştirebilen kullanım arasındaki fark gerçek erişim modelinde anlam taşımalıdır.

İlke 2: Ayrıcalığın kapsamı oluşturabileceği etkiyle birlikte sınırlandırılmalıdır.

Belirli bir görev yalnızca bir sistem veya işlev üzerinde yüksek yetki gerektiriyorsa bu ihtiyaç ilgisiz sistemlerde aynı gücün verilmesini gerektirmez. Ayrıcalığın değeri sahip olduğu unvandan değil, fiilen neyi değiştirebildiğinden anlaşılmalıdır.

İlke 3: Ayrıcalığın süresi onu doğuran ihtiyaçtan daha uzun olmamalıdır.

Kısa süreli bir ihtiyaç için sürekli yüksek yetki taşınması doğal durum haline gelmemelidir. Kalıcı ayrıcalık gerçekten gerekli olduğunda bunun geçici erişimden daha geniş ve bilinçli bir güven kararı olduğu kabul edilmelidir.

İlke 4: Ayrıcalıklı faaliyet açıklanabilir bir kimlik ve sorumlulukla ilişkilendirilebilmelidir.

Yüksek etkili bir işlemin kim tarafından, hangi sistem adına veya hangi otomasyon aracılığıyla gerçekleştirildiği belirsiz kalmamalıdır. Ortak teknik hesap veya aracılı erişim kullanılması gerçek sorumluluğun kaybolmasını gerektirmez.

İlke 5: Ayrıcalıklı erişim taşıdığı etkiye uygun güven koşullarına dayanmalıdır.

Olağan kullanım için yeterli olan kimlik, cihaz veya erişim koşulları daha geniş etki oluşturabilen işlemler için her zaman yeterli olmayabilir. Ayrıcalık arttıkça ona dayanak oluşturan güvenin de anlamlı biçimde güçlü olması gerekir.

İlke 6: Ayrıcalıklı erişim yolu koruduğu sistemin güven sınırının bir parçasıdır.

Bir sistem güçlü biçimde korunurken onu yönetebilen cihaz, oturum, ağ yolu veya yönetim hizmeti daha zayıf bırakılırsa sistemin gerçek güvenliği bu zayıf yol tarafından belirlenebilir. Yönetim yolu hedef sistemden bağımsız bir yardımcı unsur olarak görülmemelidir.

İlke 7: Olağan kullanıcı ortamının kaybı doğrudan ayrıcalığın kaybına dönüşmemelidir.

Günlük kullanım için kullanılan hesap, cihaz veya oturumun ele geçirilmesi mümkün olduğu ölçüde bütün yönetim yetkilerinin de ele geçirilmesi anlamına gelmemelidir. Olağan kullanım ile yüksek etkili kullanım arasındaki ayrım saldırı yolları bakımından da gerçek olmalıdır.

İlke 8: Tek bir ayrıcalığın kaybı sınırsız bir yönetim alanı açmamalıdır.

Bir ayrıcalıklı hesabın, kimlik bilgisinin veya oturumun ele geçirilmesi ilgisiz bütün sistem ve güven alanlarında aynı gücü sağlamamalıdır. Yüksek yetkinin yayılabileceği alan, görevin gerektirdiği kapsamla sınırlı tutulmalıdır.

İlke 9: Ayrıcalığın sistemler arasında taşınması açık bir güven ilişkisi olmalıdır.

Bir sistemde kazanılan yönetim gücünün başka sistemlerde de geçerli hale gelmesi mimarinin görünmez sonucu olmamalıdır. Özellikle farklı güven ve önem düzeyleri arasında ayrıcalığın zincirleme ilerlemesi bilinçli bir tasarım kararı olmalıdır.

İlke 10: Ayrıcalıklı kimlik bilgileri sağlayabildikleri gerçek erişim kadar kritik kabul edilmelidir.

Parola, anahtar, sertifika veya belirtecin önemi biçiminden değil, ele geçirildiğinde oluşturabileceği etkiden doğar. Yüksek yetki sağlayan kimlik bilgileri gereksiz taraflara, sistemlere veya kullanım alanlarına yayılmamalıdır.

İlke 11: Ayrıcalıklı oturum, kimlik doğrulamasından sonra da korunması gereken bir güven unsurudur.

Başlangıçta güçlü biçimde doğrulanmış bir kullanıcının oturumu sonradan ele geçirilebilir veya başka bir tarafça kullanılabilir. Ayrıcalık güvencesi yalnızca giriş anındaki doğrulamaya bağlı kalmamalıdır.

İlke 12: Yetki yükseltme açık ve sınırlı bir güven geçişi olmalıdır.

Bir kullanıcı veya sistem daha yüksek yetkiye geçtiğinde bu değişiklik sıradan bir işlemin görünmez yan etkisi olmamalıdır. Ayrıcalığın ne zaman ve hangi kapsamda kazanıldığı anlaşılabilir olmalıdır.

İlke 13: Devredilen veya otomatik kullanılan ayrıcalık kendi sınırlarını korumalıdır.

Bir yönetici başka bir tarafa yetki devredebilir veya bir otomasyon yüksek yetkiyle çalışabilir; ancak bu durum kaynaktaki bütün gücün sınırsız biçimde aktarılmasını gerektirmez. İnsan olmayan kullanım da açıklanabilir amaç, kapsam ve etkiye sahip olmalıdır.

İlke 14: Ayrıcalık güvenlik sınırlarını değiştirebildiğinde bu ek güç ayrıca dikkate alınmalıdır.

Bazı ayrıcalıklar yalnızca sistem üzerinde işlem yapmaz; erişim kontrollerini, kayıtları veya başka güvenlik mekanizmalarını da değiştirebilir. Korumanın kendisini etkileyebilen yetki, yalnızca korunan kaynağı kullanan yetkiden daha geniş bir güven sonucu oluşturur.

İlke 15: Ayrıcalıklı taraf kendi faaliyetinin bütün kanıtını tek başına kontrol etmemelidir.

Yüksek yetkili bir kullanıcının veya sistemin gerçekleştirdiği önemli işlemler gerektiğinde sonradan anlaşılabilir olmalıdır. Ayrıcalığın kapsamı, aynı tarafın kendi faaliyetini bütünüyle görünmez hale getirebilmesini doğal ve denetlenemez bir sonuç haline getirmemelidir.

İlke 16: Üçüncü taraf ayrıcalığı gerçek dış ihtiyaçla sınırlı olmalıdır.

Destek sağlayıcı, yüklenici veya başka bir dış tarafın yönetim erişimine ihtiyaç duyması kuruluş içindeki bütün ayrıcalıkların aynısını taşımasını gerektirmez. Dış erişim, ilişkinin amacı ve oluşturabileceği etkiyle sınırlandırılmış ayrı bir güven ilişkisi olarak görülmelidir.

İlke 17: Olağanüstü ayrıcalık olağan yönetimin gizli alternatifi olmamalıdır.

Normal kimlik veya yönetim yollarının kullanılamadığı durumlar için bağımsız bir erişim gerekli olabilir. Bu erişimin varlığı günlük kullanımda normal güvenlik sınırlarını aşan sürekli bir arka kapıya dönüşmemeli ve kullanıldığında olağan davranıştan ayırt edilebilmelidir.

İlke 18: Ayrıcalığın kaldırılması gerçek etki yeteneğini sona erdirebilmelidir.

Rolün veya hesabın kaldırılması sonrasında aktif oturumlar, anahtarlar, belirteçler veya başka yönetim yolları çalışmaya devam ediyorsa ayrıcalık fiilen sona ermemiştir. Ayrıcalığın yaşam döngüsü kayıt durumundan çok gerçek kullanılabilir güç üzerinden değerlendirilmelidir.

İlke 19: Ayrıcalıklı erişim hiçbir yöneticinin hata yapmayacağı varsayımına dayanmamalıdır.

Yetkili kullanıcılar yanlış işlem yapabilir, hesaplar ele geçirilebilir ve otomasyonlar hatalı davranabilir. Tasarım, ayrıcalıklı bir tarafın hata veya kötüye kullanımının ölçüsüz ve geri döndürülemez sonuçlara dönüşmesini mümkün olduğu ölçüde sınırlandırmalıdır.

İlke 20: Ayrıcalıklı erişim güvencesi gerçek yönetim yeteneği üzerinden doğrulanabilmelidir.

Ayrıcalıklı hesap listeleri, yönetici rolleri veya erişim araçlarının bulunması tek başına güvence oluşturmaz. Gerçekte kimlerin hangi sistemleri ne ölçüde değiştirebildiği, bu gücün nereden geldiği, hangi alanlara taşınabildiği ve kaldırıldığında gerçekten sona erip ermediği gerektiğinde gösterilebilmelidir.