Denetci.org

REFERANS İLKELERİ

Kimlik ve Erişim Yönetimi İlkeleri

Rİ-KIM-1

Sürüm 1.0 · 11.08.2026

www.denetci.org

Kimlik ve Erişim Yönetimi İlkeleri

Kimlik ve erişim yönetimi, bir kişi, sistem veya başka bir tarafın kim olduğuna ilişkin güven ile hangi kaynaklar üzerinde ne yapmasına izin verildiği arasındaki ilişkiyi ele alır. Amaç hesap açma, parola belirleme veya erişim onaylama süreçlerini tarif etmek değil; erişimin açıklanabilir bir kimliğe, gerçek ihtiyaca ve sınırlandırılmış yetkiye dayanmasını sağlayan ortak tasarım anlayışını ortaya koymaktır.

İlke 1: Kimlik, erişim kararının açık ve anlamlı bir dayanağı olmalıdır.

Bir erişimin hangi kişi, sistem, hizmet veya başka bir taraf adına kullanıldığı gerektiğinde anlaşılabilmelidir. Erişim, gerçek sorumluluğu belirsiz hale getiren teknik hesapların veya bağlantıların arkasında görünmez hale gelmemelidir.

İlke 2: Kimlik ile hesap aynı şey olarak kabul edilmemelidir.

Bir kişi veya sistem birden fazla hesap kullanabilir, bir hesap farklı teknik bağlamlarda kullanılabilir veya kimlik çeşitli sistemlerde farklı biçimlerde temsil edilebilir. Güven ilişkisi yalnızca hesap adına değil, hesabın hangi gerçek kimliği ve amacı temsil ettiğine dayanmalıdır.

İlke 3: Her önemli kimlik açıklanabilir bir amaca ve sorumluluğa sahip olmalıdır.

Bir kimliğin neden var olduğu ve onun adına verilen erişimlerden kimin veya hangi sistemin sorumlu olduğu belirsiz kalmamalıdır. Sahibi veya amacı bilinmeyen bir kimlik, güvenilir biçimde yetkilendirilemez.

İlke 4: Kimliğin varlığı erişim hakkı doğurmamalıdır.

Bir kullanıcı, cihaz, uygulama veya hizmet için kimlik oluşturulması onun kaynaklara genel erişime sahip olması anlamına gelmemelidir. Erişim, kimlikten ayrı ve açık bir ihtiyaç üzerinden verilmelidir.

İlke 5: Yetki gerçek görev ve amaçla sınırlı olmalıdır.

Bir tarafın erişebileceği kaynaklar, gerçekleştirebileceği işlemler ve etkileyebileceği veriler yerine getirdiği işlev için gereken sınırı aşmamalıdır. Kolaylık veya geçmiş kullanım, gereksiz geniş yetkinin kalıcı gerekçesi haline gelmemelidir.

İlke 6: Kimlik doğrulama ile yetkilendirme birbirinin yerine geçmemelidir.

Bir tarafın kimliğinin güvenilir biçimde doğrulanmış olması, istediği işlemi yapmaya yetkili olduğunu göstermez. Kim olduğu ile ne yapabileceği ayrı güven kararları olarak ele alınmalıdır.

İlke 7: Kimlik doğrulama gücü erişimin oluşturabileceği etkiyle uyumlu olmalıdır.

Bütün erişimler aynı güven düzeyini gerektirmeyebilir. Daha geniş etki veya daha hassas kaynaklara erişim, kimlik hakkında daha güçlü güven gerektirebilir.

İlke 8: Kimlik doğrulamanın değeri yöntem adından değil gerçek saldırı dayanıklılığından doğmalıdır.

Bir yöntemin çok faktörlü, sertifikalı veya başka bir teknik tanıma sahip olması tek başına yeterli güvence oluşturmaz. Kimlik avı, kimlik bilgisi devri, oturum ele geçirme ve benzeri gerçek saldırı yolları karşısındaki davranışı dikkate alınmalıdır.

İlke 9: Kimliği geri kazanma yolu normal doğrulamanın gizli ve daha zayıf alternatifi olmamalıdır.

Parola sıfırlama, hesap kurtarma veya başka destek yolları bir kimlik üzerindeki kontrolü yeniden kurabilir. Normal erişimden daha geniş bir güven sonucu üreten bu yollar, daha düşük güvenle aynı kimliği devralmayı mümkün kılmamalıdır.

İlke 10: Oturum, ilk kimlik doğrulamasından sonra bağımsız bir güven unsuru haline gelir.

Bir kullanıcının başlangıçta doğru biçimde doğrulanmış olması aktif oturumun daha sonra başka bir tarafça ele geçirilemeyeceği anlamına gelmez. Erişim güvencesi yalnızca giriş anına değil, kimlik ile aktif kullanım arasındaki bağın devamına dayanmalıdır.

İlke 11: Güven koşulları değiştiğinde erişim kararı da değişebilmelidir.

Görev, cihaz, konum, ilişki, risk veya başka anlamlı koşullar değiştiğinde geçmişte verilmiş erişimin sınırsız biçimde devam etmesi gerekmemelidir. Dinamik bağlam güven kararının parçasıysa bu bağlamın değişmesi de anlam taşımalıdır.

İlke 12: Kullanıcı, cihaz ve hizmet kimlikleri birbirinin yerine geçmemelidir.

Güvenilir bir cihaz üzerinde bulunmak kullanıcının güvenilir olduğunu; doğrulanmış bir kullanıcı da kullanılan cihazın güvenilir olduğunu tek başına göstermez. Farklı kimlik türleri gerektiğinde ayrı güven unsurları olarak değerlendirilebilmelidir.

İlke 13: İnsan olmayan kimlikler kendi kullanım biçimlerine uygun olarak ele alınmalıdır.

Uygulamalar, otomasyonlar, cihazlar ve hizmetler insan kullanıcılarla aynı yaşam döngüsüne veya kimlik doğrulama biçimine sahip değildir. Teknik kimliklerin uzun ömürlü, görünmez veya otomatik olması onların daha geniş ve belirsiz yetki taşımasını haklı çıkarmamalıdır.

İlke 14: Paylaşılan erişim sorumluluğu belirsiz hale getirmemelidir.

Bazı ortak veya teknik erişim biçimleri gerekli olabilir; ancak bunların kullanımı yapılan işlemin gerçek sorumlusunun kaybolmasına yol açmamalıdır. Ortak çalışma ihtiyacı, kişisel kimliklerin paylaşılmasını veya hesap verebilirliğin ortadan kalkmasını gerektirmez.

İlke 15: Yetkilendirme modeli gerçek erişimi anlaşılır kılmalıdır.

Roller, gruplar, nitelikler ve politikalar erişim yönetimini kolaylaştırabilir; ancak çok katmanlı kalıtım ve karmaşık ilişkiler fiilî erişimi görünmez hale getirmemelidir. Bir tarafın neden belirli bir yetkiye sahip olduğu gerektiğinde açıklanabilmelidir.

İlke 16: Ayrı ayrı makul görünen yetkilerin birleşik etkisi dikkate alınmalıdır.

Birden fazla rol, grup veya erişim birlikte kullanıldığında tek tek hiçbirinde bulunmayan daha geniş bir güç ortaya çıkabilir. Yetkilendirme, yalnızca izinlerin ayrı ayrı uygunluğuna değil anlamlı birleşimlerinin oluşturduğu etkiye de dayanmalıdır.

İlke 17: Görev ayrımı gerçek etkiyi sınırlandırmalıdır.

Farklı rollerin veya onay adımlarının bulunması tek başına görev ayrımı oluşturmaz. Tek bir taraf kritik bir işlemin bütün aşamalarını fiilen kontrol edebiliyorsa kâğıt üzerindeki ayrım güvenlik açısından anlamını kaybedebilir.

İlke 18: Erişim, onu doğuran ihtiyaçtan daha uzun yaşamamalıdır.

Geçici görevler, rol değişiklikleri, dış ilişkiler ve işten ayrılma gibi durumlar mevcut güven ilişkilerinin anlamını değiştirebilir. Bir erişimin geçmişte gerekli olması gelecekte de gerekli olduğu anlamına gelmemelidir.

İlke 19: Bir kimliğin kapatılması gerçek erişimin sona erdiği anlamına gelmelidir.

Merkezi bir hesabın devre dışı bırakılması sonrasında aktif oturumlar, yerel hesaplar, anahtarlar, belirteçler veya dış hizmetlerdeki kimlik ilişkileri erişim sağlamaya devam edebilir. Kimlik yaşam döngüsü kayıt durumundan çok fiilen kullanılabilen erişim üzerinden anlaşılmalıdır.

İlke 20: Dış ve federatif kimlikler açık bir güven ilişkisine dayanmalıdır.

Başka bir kuruluşun veya kimlik sağlayıcının doğruladığı bir kimliğin kabul edilmesi, o tarafın bazı güven kararlarının da kabul edilmesi anlamına gelir. Hangi kimliklere, hangi özelliklere ve hangi güven düzeyine dayanıldığı sınırlandırılabilir ve anlaşılabilir olmalıdır.

İlke 21: Erişim kararı gerçek karar sahibinin muhakemesini yansıtmalıdır.

Bir erişimin gerekli olup olmadığını veya oluşturacağı etkiyi anlayamayan tarafın biçimsel onayı güvence oluşturmaz. Yetki kararı, işlevi ve riski değerlendirebilen sorumlulukla ilişkilendirilmelidir.

İlke 22: Erişimin geçmişte onaylanmış olması gelecekteki ihtiyacın kanıtı olmamalıdır.

Bir yetkinin uzun süredir kullanılması veya daha önce gözden geçirilmiş olması onun mevcut görevle hâlâ uyumlu olduğunu göstermez. Güven ilişkileri içinde bulundukları güncel bağlama dayanmalıdır.

İlke 23: Olağanüstü erişim normal erişim modelinin gizli alternatifi olmamalıdır.

Acil durumlarda normal kimlik altyapısından bağımsız erişim yolları gerekli olabilir. Bu yollar günlük kolaylık amacıyla kullanılmamalı ve varlıkları normal erişim sınırlarını anlamsız hale getirmemelidir.

İlke 24: Kimlik ve erişim güvencesi fiilî erişim üzerinden doğrulanabilmelidir.

Hesap listeleri, rol matrisleri, onay kayıtları veya gözden geçirme sonuçları tek başına güvence oluşturmaz. Bir tarafın gerçekte hangi kaynaklara erişebildiği, bu erişimin hangi kimlik ve yetki ilişkilerinden doğduğu ve koşullar değiştiğinde erişimin gerçekten sona erip ermediği gerektiğinde gösterilebilmelidir.