Denetci.org

REFERANS İLKELERİ

Sır Yönetimi İlkeleri

Rİ-KRP-1

Sürüm 1.0 · 11.08.2026

www.denetci.org

Sır Yönetimi İlkeleri

Sırlar; ele geçirilmesi halinde bir sistem, hizmet, veri veya başka bir güven ilişkisi üzerinde yetki sağlayabilen gizli değerlerdir. API anahtarları, erişim belirteçleri, teknik hesap bilgileri ve benzeri değerler bu kapsamda değerlendirilebilir. Amaç belirli bir sır kasası veya rotasyon yöntemi dayatmak değil; sırların oluşturdukları gerçek erişim kadar kritik görüldüğü ve yaşamları boyunca gereksiz yere yayılmadığı bir tasarım anlayışı ortaya koymaktır.

İlke 1: Bir sırın güvenlik değeri gizli kalmasına ve sağladığı yetkiye dayanmalıdır.

Bir değer ele geçirildiğinde artık güven sağlamıyorsa onun güvenliği yalnızca nerede saklandığıyla değil kimlerin onu öğrenebildiği ve onunla ne yapabildiğiyle değerlendirilmelidir. Sır kavramı, dosya türüne veya ürün sınıfına değil gerçek güven etkisine dayanmalıdır.

İlke 2: Her sır açıklanabilir bir amaca sahip olmalıdır.

Neden var olduğu veya hangi erişimi sağladığı bilinmeyen sırlar güvenilir biçimde korunamaz ve gerektiğinde kaldırılamaz. Sır oluşturmak teknik kolaylık uğruna varsayılan ve kalıcı erişim mekanizması haline gelmemelidir.

İlke 3: Sırrın kapsamı onu doğuran ihtiyaçla sınırlı olmalıdır.

Bir sır yalnızca belirli bir sisteme, işleve veya kaynağa erişim için gerekiyorsa ilgisiz alanlarda da aynı yetkiyi sağlamamalıdır. Tek bir sırrın ele geçirilmesi gereksiz ölçüde geniş bir güven kaybına dönüşmemelidir.

İlke 4: Aynı sırrın paylaşılması bağımsız güven alanlarını birbirine bağlamamalıdır.

Bir sırrın birden fazla sistem, ortam veya taraf arasında kullanılması bu alanlardan herhangi birinin kaybını diğerlerine taşıyabilir. Ortak sır kullanımı, yönetim kolaylığının görünmeyen ortak risk oluşturduğu durumları dikkate almalıdır.

İlke 5: İnsan ve makine sırları aynı kullanım modeline zorlanmamalıdır.

İnsanların hatırladığı veya doğrudan kullandığı sırlarla uygulamaların otomatik biçimde kullandığı sırların ihtiyaçları farklıdır. Makine kimlikleri gereksiz biçimde insan hafızasına, manuel kopyalamaya veya insanlara yönelik parola alışkanlıklarına bağımlı olmamalıdır.

İlke 6: Sırlar kendilerine ihtiyaç olmayan kalıcı ortamlara yerleşmemelidir.

Kaynak kodu, imajlar, yapılandırmalar, kullanıcı cihazları ve başka dağıtılabilir alanlar bir sırrın çok sayıda kontrolsüz kopyasını oluşturabilir. Bir sırrın daha sonra görünür konumdan kaldırılması, geçmiş kopyalarının ve dağıtımlarının oluşturduğu güven kaybını kendiliğinden ortadan kaldırmaz.

İlke 7: Sır saklama mekanizması güvenin kendisi olarak görülmemelidir.

Merkezi bir sır deposu veya başka özel bir teknoloji sırların yönetimini güçlendirebilir; ancak sırları otomatik olarak doğru kapsamda veya güvenli hale getirmez. Güvence, ürünün varlığından çok sırların kimler tarafından hangi koşullarda kullanılabildiğine dayanmalıdır.

İlke 8: Bir sırrı kullanabilmek ile onu öğrenebilmek gerektiğinde ayrıştırılabilmelidir.

Bazı işlevlerin bir sırrın sağladığı yetkiye ihtiyaç duyması, insanın veya uygulamanın sır değerinin kendisini görmesini gerektirmeyebilir. Tasarım, kullanım ihtiyacını gereksiz açıklama ve kopyalama ihtiyacına dönüştürmemelidir.

İlke 9: Sırlar mümkün olduğu ölçüde ihtiyaç anına ve kullanım alanına yakın tutulmalıdır.

Bir sırrın çok daha önce dağıtılması veya uzun süre erişilebilir halde beklemesi ele geçirilme alanını büyütür. Sırların yaşamı, kullanılacakları bağlamdan gereksiz biçimde daha geniş olmamalıdır.

İlke 10: Sırların aktarılması yeni ve kontrolsüz kopyalar oluşturmamalıdır.

E-posta, mesajlaşma, destek çıktıları, pano veya benzeri genel amaçlı kanallar sırların daha sonra bulunamayacak kopyalarını üretebilir. İlk teslim ve sonraki paylaşım, sırrın yaşam döngüsünün dışında kabul edilmemelidir.

İlke 11: Üretim ve üretim dışı ortamlar sırlar aracılığıyla birbirine bağlanmamalıdır.

Aynı sırrın farklı güven düzeyindeki ortamlarda kullanılması daha zayıf ortamın kaybını daha güçlü ortama taşıyabilir. Ortam ayrımı yalnızca altyapı düzeyinde değil kimlik ve sır düzeyinde de gerçek olmalıdır.

İlke 12: Bir sırrın geçerlilik süresi oluşturabileceği etkiyle uyumlu olmalıdır.

Süresiz geçerlilik, ele geçirilmiş bir sırrın etkisini de süresiz hale getirebilir. Bununla birlikte kısa ömür tek başına güvence değildir; sır yenilenirken veya tekrar elde edilirken aynı zayıf güven ilişkisi devam edebilir.

İlke 13: Sır değişikliği takvimsel bir amaç değil güven ilişkisinin yenilenmesi olmalıdır.

Rotasyon yalnızca yeni bir değer üretmekten ibaret değildir. Değişiklik sonrasında eski sırrın gerçek erişim sağlayıp sağlamadığı ve yeni sırrın aynı gereksiz riskleri sürdürüp sürdürmediği önem taşır.

İlke 14: Güveni kaybolan sır olağan yaşam döngüsünün tamamlanmasını beklememelidir.

Bir sırrın açığa çıktığına veya güvenilirliğini kaybettiğine ilişkin yeterli neden varsa takvimsel değişim zamanı güvenin sürmesi için gerekçe değildir. Güven kaybı gerçek erişim yeteneğine yansıtılabilmelidir.

İlke 15: Sırrın kaldırılması kayıt durumundan çok gerçek erişimi sona erdirmelidir.

Bir envanterde “iptal edildi” olarak işaretlenen sır çalışan sistemlerde hâlâ geçerliyse güven ilişkisi sona ermemiştir. Sır yaşam döngüsü, kayıtların değil fiilen kullanılabilen yetkinin durumunu yansıtmalıdır.

İlke 16: Üçüncü tarafla paylaşılan sır kuruluşun güven sınırını o tarafa genişletir.

Bir sağlayıcıya veya iş ortağına sır verilmesi, o tarafın güvenliği ile kuruluşun ilgili erişimi arasında doğrudan ilişki oluşturabilir. Dış tarafın ihtiyacı sona erdiğinde bu güven ilişkisinin de fiilen sona erdirilebilmesi gerekir.

İlke 17: Sırrın kopyaları asıl kullanım alanının dışında da yaşamaya devam edebilir.

Yedekler, arşivler, tanılama verileri ve geçmiş dağıtımlar aktif sistemden kaldırılmış bir sırrı içermeye devam edebilir. Yaşam döngüsü değerlendirilirken görünmeyen kopyaların oluşturduğu güven etkisi göz ardı edilmemelidir.

İlke 18: Sır yönetiminin güvencesi gerçek erişim ve yaşam döngüsü üzerinden doğrulanabilmelidir.

Sır envanteri, tarama aracı veya merkezi yönetim sistemi bulunması tek başına güvence oluşturmaz. Hangi sırların gerçekte kullanılabildiği, hangi erişimi sağladığı, kimlere ve hangi sistemlere yayıldığı, güven kaybında etkisiz hale gelip gelmediği ve artık gerekli olmadığında gerçek erişimin sona erip ermediği gerektiğinde gösterilebilmelidir.