Denetci.org

REFERANS İLKELERİ

Yapılandırma Güvenliği İlkeleri

Rİ-ALT-1

Sürüm 1.0 · 11.08.2026

www.denetci.org

Yapılandırma Güvenliği İlkeleri

Yapılandırma güvenliği, bir sistemin hangi özellikleriyle ve hangi güven sınırları içinde çalışacağını belirleyen ayarların güvenilir biçimde tasarlanmasını ele alır. Amaç bütün teknolojiler için tek bir sertleştirme listesi oluşturmak değil; sistemlerin başlangıç durumundan çalışma zamanına kadar gereksiz güven, yetki ve maruziyet üretmemesini sağlayan ortak tasarım anlayışını ortaya koymaktır.

İlke 1: Başlangıç durumu gereksiz güven, yetki veya maruziyet üretmemelidir.

Yeni kurulan veya oluşturulan bir sistem, ek güvenlik adımları tamamlanmadığı için kendiliğinden geniş erişime açık hale gelmemelidir. Güvenli durum, sürekli sonradan kısıtlama yapılmasını gerektiren bir istisna değil tasarımın doğal başlangıç noktası olmalıdır.

İlke 2: Üretici veya platform varsayımları güvenlik gerekçesinin yerine geçmemelidir.

Bir ayarın ürünle birlikte gelmesi onun kuruluşun kullanım amacı için güvenli olduğu anlamına gelmez. Yapılandırmanın uygunluğu, kaynağından çok sistemin gerçek rolü, maruziyeti ve güven ilişkileri üzerinden anlaşılmalıdır.

İlke 3: Yapılandırma sistemin gerçek işlevine göre şekillenmelidir.

Farklı görevler ve güven alanları farklı güvenlik ihtiyaçları doğurabilir. Tek bir ayar kümesini bütün sistemlere uygulamak kadar, her sistemi tamamen özel ve karşılaştırılamaz hale getirmek de güvenilir bir yapılandırma yaklaşımı değildir.

İlke 4: Kullanılmayan yetenekler güvenlik açısından nötr kabul edilmemelidir.

Gereksiz servisler, erişim yolları, hesaplar ve özellikler kullanılmasalar bile hata ve saldırı alanı oluşturabilir. Sistem, amaçlanan işlevi yerine getirmek için ihtiyaç duyduğu yeteneklerle sınırlı kalmalıdır.

İlke 5: Yönetim yeteneği taşıdığı etkiyle orantılı biçimde sınırlandırılmalıdır.

Bir sistemi değiştirebilen yönetim yolları normal kullanıcı işlevlerinden daha geniş sonuçlar doğurabilir. Yapılandırma, yönetim imkânlarının gereksiz kişi, ağ veya sistemlere açılmasını doğal durum haline getirmemelidir.

İlke 6: Yapılandırmanın gerçek etkisi tek bir görünen değerden ibaret kabul edilmemelidir.

Bir ayarın sonucu başka ayarlar, varsayımlar, kalıtım, politika öncelikleri veya çalışma zamanı davranışları tarafından değiştirilebilir. Güvence, yalnızca bir arayüzde veya dosyada görünen değere değil sistemin fiilen uyguladığı davranışa dayanmalıdır.

İlke 7: Bir ayarın hangi kaynaktan ve hangi öncelikle oluştuğu belirsiz olmamalıdır.

Aynı davranışın farklı dosya, araç, politika veya otomasyon tarafından belirlenmesi amaçlanan durum ile çalışan durum arasında fark yaratabilir. Yapılandırma modeli, bir güvenlik kararının gerçekte nereden geldiğinin anlaşılabilmesine izin vermelidir.

İlke 8: Yapılandırma üretim davranışını değiştirebildiği ölçüde kritik bir sistem girdisidir.

Kod değiştirilmeden yalnızca yapılandırmayla erişim, veri akışı, kimlik doğrulama veya güvenlik kontrolleri değiştirilebilir. Bu nedenle yapılandırmanın bütünlüğü ve kaynağı, üretilen yazılımın bütünlüğünden bağımsız veya daha önemsiz görülmemelidir.

İlke 9: Sırlar ile yapılandırma gereksiz biçimde birbirine bağlanmamalıdır.

Bir sistemin nasıl çalışacağını tarif eden yapılandırmanın paylaşılması veya çoğaltılması, beraberinde parolaların, anahtarların ve diğer sırların da yayılmasına neden olmamalıdır. Yapılandırma kolaylığı, güven unsurlarının gereksiz kopyalarını oluşturmamalıdır.

İlke 10: Ortak şablonlar güvenli başlangıç sağlamalı, bilinçli farklılıkları ortadan kaldırmamalıdır.

Şablonlar ve temel yapılandırmalar tekrar eden güvenlik kararlarının güvenilir biçimde uygulanmasını sağlayabilir. Bununla birlikte farklı bir ihtiyaca dayanan sapma sırf standarttan farklı olduğu için yanlış sayılmamalı; güvenlik açısından anlamı açıklanabilir olmalıdır.

İlke 11: Sapma ve istisnalar amaçlanan güvenlik durumunu görünmez biçimde değiştirmemelidir.

Yerel değişiklikler, geçici gevşetmeler ve uyumluluk ihtiyaçları zamanla sistemin fiilî yapılandırmasını başlangıç tasarımından uzaklaştırabilir. Bu farklılıklar kalıcı ve açıklanamayan yeni varsayımlara dönüşmemelidir.

İlke 12: Yapılandırma değişikliği güvenlik davranışını değiştirebilen bir tasarım olayıdır.

Bir ayarın değiştirilmesi kod değişikliği kadar önemli güvenlik sonuçları doğurabilir. Değişikliğin kaynağı, oluşturduğu etki ve ortaya çıkan yeni durum gerektiğinde anlaşılabilir olmalıdır.

İlke 13: Amaçlanan yapılandırma ile çalışan yapılandırma birbirinden ayrılabilmelidir.

Bir depoda, yönetim aracında veya şablonda doğru görünen ayar çalışan sisteme hiç uygulanmamış ya da sonradan değiştirilmiş olabilir. Güvenli olduğu düşünülen durum ile sistemin gerçekten kullandığı durum arasındaki fark görünmez kalmamalıdır.

İlke 14: Otomasyon güvenli kararın yerine değil, uygulanmasına hizmet etmelidir.

Otomasyon doğru yapılandırmayı tutarlı biçimde yayabilir; ancak hatalı bir kararı da çok daha hızlı ve geniş ölçekte çoğaltabilir. Otomatik oluşturma veya düzeltme yapılması, ortaya çıkan durumun doğru olduğu konusunda tek başına güvence oluşturmamalıdır.

İlke 15: Merkezi yapılandırma yeteneği bir güven yoğunlaşması olarak görülmelidir.

Tek bir platform veya kimlik çok sayıda sistemin davranışını değiştirebiliyorsa onun kaybı aynı ölçüde geniş sonuç doğurabilir. Merkezi yönetimin sağladığı kolaylık, oluşturduğu ortak etki alanını görünmez hale getirmemelidir.

İlke 16: Geçici güvenlik gevşemeleri kalıcı çalışma biçimine dönüşmemelidir.

Hata giderme, geliştirme, geriye dönük uyumluluk veya başka geçici ihtiyaçlar normalden daha açık bir yapılandırmayı gerektirebilir. İhtiyaç sona erdiğinde daha zayıf durumun kendi kendine süresiz devam etmesi tasarımın kabul edilmiş sonucu olmamalıdır.

İlke 17: Yapılandırmanın güvenlik anlamı teknoloji ve çalışma bağlamından bağımsız değildir.

Aynı ayar farklı sürümlerde, platformlarda veya dağıtım biçimlerinde farklı sonuçlar oluşturabilir. Bir yapılandırmanın geçmişte güvenli kabul edilmiş olması yeni teknoloji veya kullanım koşullarında aynı sonucu garanti etmez.

İlke 18: Güvenlik ürünlerinin yapılandırmaları da aynı güvence anlayışına tabi olmalıdır.

Bir güvenlik aracının kurulmuş olması onun amaçlanan korumayı gerçekten sağladığını göstermez. Güvenlik sağlayan sistemler de yanlış ayar, gereksiz yetki ve gerçek durumdan sapma bakımından diğer sistemler gibi değerlendirilebilmelidir.

İlke 19: Yapılandırma güvenliği uyum oranına indirgenmemelidir.

Çok sayıda düşük etkili ayarın beklenen değerde olması, tek bir kritik yapılandırma hatasının oluşturduğu riski ortadan kaldırmaz. Değerlendirme, kaç ayarın doğru olduğundan çok hangi güvenlik davranışlarının ortaya çıktığına dayanmalıdır.

İlke 20: Yapılandırma güvencesi sistemin gerçek çalışma davranışıyla doğrulanabilmelidir.

Bir sertleştirme standardının, şablonun, otomasyon aracının veya yapılandırma raporunun bulunması tek başına güvenli bir sistem oluşturmaz. Güvence; amaçlanan ayarların gerçekten uygulandığı, kritik güvenlik özelliklerinin beklenen sonucu verdiği ve fiilî durumun dayandığı güvenlik varsayımlarının açıklanabildiği ölçüde oluşmalıdır.