Denetci.org

REFERANS İLKELERİ

Bilgi Sistemleri İşletim Güvencesi İlkeleri

Rİ-ISL-6

Sürüm 1.0 · 11.08.2026

www.denetci.org

Bilgi Sistemleri İşletim Güvencesi İlkeleri

Bilgi sistemleri işletim güvencesi, tasarlanmış ve kurulmuş güvenlik özelliklerinin sistem günlük olarak çalıştırılırken korunmasını ele alır. Amaç işletim prosedürlerinin ayrıntısını belirlemek değil; üretim sistemlerinin gerçek durumunun anlaşılabildiği, işletim yetkilerinin sınırlandırıldığı ve hata, bakım veya olağan dışı koşullarda güvenilir davranışın sürdürülebildiği bir çalışma anlayışı oluşturmaktır.

İlke 1: İşletim, sistemin tasarımında kurulan güven sınırlarını zaman içinde korumalıdır.

Bir sistem başlangıçta güvenli tasarlanmış olsa da günlük müdahaleler, geçici çözümler ve değişen ihtiyaçlar bu sınırları aşındırabilir. Güvenlik, kurulum anında elde edilip daha sonra kendiliğinden devam eden bir özellik olarak görülmemelidir.

İlke 2: Üretim ortamı taşıdığı gerçek etkiye uygun ayrı bir güven alanı olmalıdır.

Geliştirme, test ve günlük kullanıcı faaliyetleri üretim sistemlerini değiştirme veya üretim verisine erişme gücünü doğal olarak taşımamalıdır. Ortam ayrımı yalnızca isim veya altyapı etiketi değil gerçek yetki ve etki sınırı oluşturmalıdır.

İlke 3: Üretim üzerinde değişiklik yapma gücü genel kullanım yetkisinin doğal uzantısı olmamalıdır.

Bir kişinin sistemi kullanması veya geliştirmesi onu doğrudan üretim davranışını değiştirmeye yetkili hale getirmemelidir. İşletim yetkileri oluşturabilecekleri sonuçlara göre ayrıca sınırlandırılmalıdır.

İlke 4: İşletim güvenilirliği tek tek kişilerin hafızasına ve sürekli varlığına bağlı olmamalıdır.

Kritik sistem bilgisi yalnızca belirli kişilerin bildiği komutlara, istisnalara veya çalışma alışkanlıklarına dayanıyorsa sistem o kişilerin hata veya yokluğuna gereksiz biçimde bağımlıdır. İşletimin önemli varsayımları kurumsal olarak anlaşılabilir olmalıdır.

İlke 5: İşletim otomasyonu kararı görünmez hale getirmemelidir.

Otomasyon tutarlı ve hızlı çalışma sağlayabilir; ancak hangi sistemde neyi ve hangi yetkiyle değiştirdiği anlaşılmaz hale gelmemelidir. Otomatik çalışma, geniş yetkinin kaynağını veya sonucunu belirsizleştirmemelidir.

İlke 6: Otomatik uygulama ile insan muhakemesi birbirinin yerine geçmemelidir.

Tekrarlanabilir işlemler otomatikleştirilebilir; ancak bağlam veya risk değerlendirmesi gerektiren bir karar sırf otomasyon mümkün olduğu için makineye aktarılmamalıdır. Aynı şekilde insan onayı da otomatik doğrulamanın sağlayabileceği tutarlılığın yerine geçmemelidir.

İlke 7: İşletim araçları etkileyebildikleri sistemler kadar önemli güven unsurlarıdır.

Orkestrasyon, uzaktan yönetim, güncelleme veya başka işletim platformları çok sayıda sisteme yüksek yetkiyle erişebilir. Bu araçların kaybı geniş bir güven kaybına dönüşebileceği için yardımcı araçlar olarak güven modelinin dışında tutulmamalıdır.

İlke 8: Merkezi işletim yeteneği gereksiz ortak başarısızlık alanı oluşturmamalıdır.

Tek bir yönetim kimliği veya platformun kaybı bütün sistemleri aynı anda değiştirme imkânı veriyorsa operasyonel kolaylığın yanında ciddi bir güven yoğunlaşması da oluşur. İşletim mimarisi bu ortak etkiyi bilinçli biçimde ele almalıdır.

İlke 9: Sistemin gerçek durumu planlanan veya kayıtlı durumla eşit kabul edilmemelidir.

Şablonlar, yapılandırma depoları ve işletim kayıtları amaçlanan durumu gösterebilir; ancak çalışan sistem manuel müdahale, hata veya başka nedenlerle farklılaşmış olabilir. İşletim güvencesi fiilî durumu da anlayabilmelidir.

İlke 10: Geçici işletim çözümleri görünmez kalıcı mimariye dönüşmemelidir.

Sorun giderme veya acil ihtiyaç sırasında eklenen hesaplar, bağlantılar, servisler veya yapılandırmalar daha sonra kullanılmaya devam edebilir. Geçici çözümün varlığı ve sona ermesi sistemin gerçek güven modelinin bir parçası olmalıdır.

İlke 11: Güncel olmak ile güvenli olmak aynı şey olarak kabul edilmemelidir.

Güncellemeler güvenlik sorunlarını giderebilir ancak yeni davranış, bağımlılık veya uyumsuzluk da oluşturabilir. Bir güncellemenin güvenlik değeri yalnızca daha yeni bir sürüm olmasından değil sistemin gerçek durumunu nasıl değiştirdiğinden doğmalıdır.

İlke 12: Güncellenemeyen ve desteklenmeyen sistemler olağan güven varsayımları altında görünmez biçimde yaşamamalıdır.

Teknik veya iş nedenleriyle bazı sistemler mevcut güvenlik beklentilerini karşılayamayabilir. Böyle bir durum, sistemin diğer sistemlerle aynı güven seviyesinde kabul edilmesinin sessiz gerekçesi olmamalıdır.

İlke 13: Bakım erişimi sistemin normal güven sınırlarını anlamsız hale getirmemelidir.

Sorun giderme ve destek faaliyetleri yüksek yetki veya alternatif erişim yolları gerektirebilir. Seyrek kullanılmaları bu yolların gerçek saldırı ve güven yüzeyi olmadığı anlamına gelmez.

İlke 14: İşletim sırasında oluşan önemli müdahaleler sonradan açıklanabilir olmalıdır.

Bir sistemin durumu manuel veya otomatik bir müdahaleyle değiştiğinde gerektiğinde bu değişikliğin kaynağı ve sonucu anlaşılabilmelidir. Bu, her işlemin ayrıntılı biçimde bürokratik kayda dönüştürülmesini değil önemli davranışın tamamen izsiz kalmamasını gerektirir.

İlke 15: Kapasite ve kaynak sınırları güvenlikten bağımsız işletim konuları olarak görülmemelidir.

Kaynak tükenmesi hizmetin kullanılamamasına, güvenlik mekanizmalarının çalışmamasına veya başka beklenmeyen davranışlara yol açabilir. Sistem, makul bir yük veya hata altında güven sınırlarını koruyamayacak biçimde işletilmemelidir.

İlke 16: Hata durumundaki sistem davranışı bilinçli bir güvenlik tercihini yansıtmalıdır.

Bir bağımlılık, güvenlik ürünü veya temel hizmet kullanılamadığında sistemin daha geniş erişime geçmesi ya da kritik kontrolleri kaldırması tesadüfi sonuç olmamalıdır. Güvenlik ve kullanılabilirlik arasındaki davranış anlaşılabilir olmalıdır.

İlke 17: Tek bir işletim arızası gereksiz ölçüde geniş hizmet veya güven kaybına dönüşmemelidir.

Bir bileşenin veya operasyonel hatanın diğer bağımsız hizmetleri de kaybettirmesi ortak bağımlılığın göstergesi olabilir. Dayanıklılık yalnızca yedek bileşen sayısıyla değil gerçek başarısızlık alanlarının sınırlandırılmasıyla oluşur.

İlke 18: Olay sırasında yapılan müdahaleler korunan sistemden daha büyük zarar oluşturmamalıdır.

Acil durumda hız gerekebilir; ancak sorunu çözmek amacıyla güvenlik sınırlarının geniş biçimde kaldırılması, kanıtların yok edilmesi veya geri dönüş imkanının kaybedilmesi yeni riskler doğurabilir. Müdahalenin kendisi de güvenlik etkisi olan bir işletim faaliyetidir.

İlke 19: Sistemin yeniden çalışması güvenin tamamen geri kurulduğu anlamına gelmemelidir.

Bir olay veya arıza sonrasında hizmet kullanılabilir hale gelebilirken kimlikler, yapılandırmalar, veri bütünlüğü veya başka güven unsurları hâlâ şüpheli olabilir. Kurtarma, yalnızca teknik çalışırlığın değil güvenilir durumun yeniden kurulmasını hedeflemelidir.

İlke 20: Dış işletim hizmetleri kuruluşun sistemleri üzerindeki gerçek etkisini görünür tutmalıdır.

Bir sağlayıcının sistemleri yönetmesi kuruluşun bu sistemlerdeki güvenlik sonuçlarıyla ilişkisini ortadan kaldırmaz. Hangi tarafın neyi değiştirebildiği ve hangi alanlarda görünürlük sağladığı anlaşılabilir olmalıdır.

İlke 21: Kullanılmayan sistemler ve işletim yolları güvenlik açısından nötr sayılmamalıdır.

Artık gerçek bir işlevi bulunmayan servisler, hesaplar, yönetim araçları ve sistemler saldırı ve bakım yüzeyi oluşturmaya devam edebilir. Kullanım ihtiyacı sona erdiğinde buna bağlı güven ilişkilerinin de devam etmesi varsayılan durum olmamalıdır.

İlke 22: Bir sistemin devreden çıkarılması güven ilişkilerinin de sona erdirilmesini kapsamalıdır.

Sistemin kapatılması sonrasında kimlikler, sırlar, ağ yolları, veriler, yedekler veya dış entegrasyonlar yaşamaya devam edebilir. İşletim yaşam döngüsünün sonu yalnızca cihazın veya hizmetin kapatılmasıyla tamamlanmış sayılmamalıdır.

İlke 23: İşletim güvencesi sistemin gerçek çalışma biçimi üzerinden doğrulanabilmelidir.

İşletim prosedürleri, otomasyon platformları, güncelleme raporları veya destek sözleşmeleri tek başına güvence oluşturmaz. Çalışan sistemlerin amaçlanan güven durumunu koruyup korumadığı, kimlerin ve hangi araçların onları değiştirebildiği, olağan dışı koşullarda nasıl davrandıkları ve güvenilir duruma gerçekten geri döndürülebildikleri gerektiğinde gösterilebilmelidir.