Denetci.org

REFERANS İLKELERİ

Değişiklik Yönetimi İlkeleri

Rİ-ISL-1

Sürüm 1.0 · 11.08.2026

www.denetci.org

Değişiklik Yönetimi İlkeleri

Değişiklik yönetimi, sistemlerin ihtiyaçlara uyarlanırken mevcut güvenlik özelliklerinin fark edilmeden kaybedilmemesini ve yeni güven ilişkilerinin bilinçli biçimde kurulmasını ele alır. Amaç değişiklikleri yavaşlatan bir onay mekanizması oluşturmak değil; değişikliğin amacı, etkisi ve ortaya çıkardığı yeni durumun anlaşılabilir ve doğrulanabilir olmasını sağlayan bir tasarım anlayışı ortaya koymaktır.

İlke 1: Her değişiklik mevcut güven durumunu değiştirebilecek bir olay olarak görülmelidir.

Kod, yapılandırma, altyapı, veri modeli, bağımlılık veya işletim biçimindeki bir değişiklik daha önce geçerli olan güvenlik varsayımlarını etkileyebilir. Değişikliğin küçük veya rutin görünmesi bu etkinin bulunmadığını göstermez.

İlke 2: Değişikliğin amacı ve beklenen sonucu anlaşılabilir olmalıdır.

Neyin neden değiştirildiği bilinmeden ortaya çıkan yeni durumun doğru olup olmadığı güvenilir biçimde değerlendirilemez. Değişiklik, yalnızca teknik işlemlerden değil gerçekleştirilmek istenen sonuçtan hareketle açıklanabilmelidir.

İlke 3: Değişikliğin kapsamı onu doğuran ihtiyaçla sınırlı olmalıdır.

Belirli bir ihtiyacı karşılamak için yapılan değişiklik ilgisiz sistemleri, yetkileri veya güven sınırlarını gereksiz biçimde etkilememelidir. Değişiklik kolaylığı gereksiz geniş bir etki alanının gerekçesi olmamalıdır.

İlke 4: Değişiklik riski yalnızca değişikliğin büyüklüğüne göre anlaşılmamalıdır.

Tek satırlık bir yapılandırma değişikliği geniş güven sınırlarını kaldırabilir; çok kapsamlı bir değişiklik ise iyi ayrıştırılmış bir alanda sınırlı sonuç oluşturabilir. Önem, değişen unsurun gerçek sistem davranışındaki rolüne dayanmalıdır.

İlke 5: Değişiklik gerçek bağımlılıklarıyla birlikte değerlendirilmelidir.

Bir bileşendeki değişiklik onu kullanan sistemleri, kimlikleri, verileri veya dış hizmetleri etkileyebilir. Görünürde değişmeyen bileşenler bağımlılıkları nedeniyle farklı bir güven durumuna geçebilir.

İlke 6: Değişikliğin başarı ölçütü yalnızca teknik olarak uygulanmış olması olmamalıdır.

Bir dağıtımın tamamlanması veya sistemin çalışmaya devam etmesi beklenen güvenlik sonucunun da oluştuğunu göstermez. Değişiklik, amaçlanan işlev ve güvenlik özelliklerinin birlikte korunması açısından anlam taşımalıdır.

İlke 7: Değişiklik öncesi ve sonrası güvenlik açısından anlamlı durumlar karşılaştırılabilir olmalıdır.

Yeni durumda neyin farklılaştığı bilinmiyorsa istenmeyen sapmaların değişiklikten kaynaklanıp kaynaklanmadığı anlaşılamaz. Özellikle güven sınırları, erişimler ve kritik davranışlardaki değişimler gerektiğinde ayırt edilebilmelidir.

İlke 8: Amaçlanan değişiklik ile fiilen oluşan değişiklik birbirine eşit kabul edilmemelidir.

Bir değişiklik tanımı yalnızca yapılmak isteneni gösterir. Bağımlılıklar, otomasyon, manuel müdahaleler veya beklenmeyen davranışlar sonucunda çalışan sistem farklı bir duruma geçmiş olabilir.

İlke 9: Değişiklik yolları sistemin güven modelini görünmez biçimde aşmamalıdır.

Manuel müdahale, doğrudan üretim erişimi veya başka alternatif yollar değişiklik mekanizmasının dışında kullanılabiliyorsa bunlar gerçek yönetim yüzeyinin parçalarıdır. Resmî yolun güvenli olması alternatif yolların oluşturduğu güven etkisini ortadan kaldırmaz.

İlke 10: Otomasyon değişikliğin doğruluğuna ilişkin bağımsız bir güven kanıtı olmamalıdır.

Otomasyon tutarlılığı artırabilir ve insan hatasını azaltabilir; ancak yanlış bir değişikliği çok daha geniş ve hızlı biçimde uygulayabilir. Değişikliğin otomatik gerçekleştirilmiş olması onun doğru olduğu anlamına gelmez.

İlke 11: Değişiklik yetkisi değiştirilebilen alanın gerçek etkisiyle uyumlu olmalıdır.

Bir sistemde küçük görünen bir değişikliği yapabilen kimlik, gerçekte çok sayıda güvenlik sınırını etkileyebilir. Değişiklik yetkisi işlem adından çok ortaya çıkarabileceği sonuç üzerinden değerlendirilmelidir.

İlke 12: Değişiklik kararı gerçek etkisini anlayabilecek sorumlulukla ilişkilendirilmelidir.

Biçimsel onay, onaylayan taraf değişikliğin amacını veya oluşturabileceği sonucu değerlendiremiyorsa sınırlı güvence sağlar. Karar mekanizması değişikliğin gerçek bağlamından kopmamalıdır.

İlke 13: Değişiklik güvencesi her değişikliği aynı karar ve kontrol yoluna zorlamamalıdır.

Düşük etkili ve iyi sınırlandırılmış değişiklikler ile geniş güven alanlarını etkileyen değişikliklerin aynı süreç yüküne sahip olması gerekmez. Uygulanan güvence değişikliğin gerçek etkisiyle orantılı olmalıdır.

İlke 14: Yüksek etkili değişiklikler tek bir hata veya yanlış karara gereksiz biçimde bağımlı olmamalıdır.

Bir değişikliğin çok geniş ve geri döndürülmesi zor sonuçları varsa tek bir tarafın hatası ölçüsüz bir güven kaybına dönüşmemelidir. Ek güvence ihtiyacı biçimsel rol sayısından değil oluşturulabilecek gerçek etkiden doğmalıdır.

İlke 15: Üretim dışındaki başarı üretimde aynı güvenlik sonucunun oluşacağını garanti etmemelidir.

Test ve benzeri ortamlar üretimden veri, trafik, yapılandırma, bağımlılık veya ölçek açısından farklı olabilir. Değişiklik güvencesi yalnızca başka bir ortamda elde edilen sonuca dayanmamalıdır.

İlke 16: Değişikliğin gerçek sonucu uygulandığı ortamda anlaşılabilir olmalıdır.

Değişiklik sonrası yalnızca hizmetin çalışıp çalışmadığı değil, amaçlanan güvenlik özelliklerinin korunup korunmadığı da gerektiğinde doğrulanabilmelidir. Üretim doğrulaması değişiklikten tamamen ayrı bir düşünce olmamalıdır.

İlke 17: Değişikliğin başarısızlığına karşı geri dönüş yaklaşımı değişikliğin doğasına uygun olmalıdır.

Her değişikliğin kolayca geri alınması mümkün değildir; özellikle veri ve durum değişiklikleri geri dönüş sırasında yeni sorunlar oluşturabilir. Güvence, yalnızca bir "geri al" mekanizmasının varlığına değil güvenilir bir duruma nasıl dönülebileceğinin anlaşılmasına dayanmalıdır.

İlke 18: Değişikliğin etkisi mümkün olduğunda kontrol edilebilir biçimde genişlemelidir.

Bir hatanın bütün kullanıcıları veya sistemleri aynı anda etkilemesi gerekmiyorsa değişikliğin ilk etkisi sınırlandırılabilir olmalıdır. Aşamalı değişim yalnızca operasyonel kolaylık değil belirsizlik altında etkiyi sınırlamanın bir yolu olarak değerlendirilebilir.

İlke 19: Acil ve geçici değişiklikler kalıcı alternatif güven modeli oluşturmamalıdır.

Olağan yaklaşımın dışına çıkmayı gerektiren durumlar olabilir; ancak hız veya geçici ihtiyaç nedeniyle oluşan sapmalar görünmez biçimde sistemin yeni normaline dönüşmemelidir. Onları doğuran koşullar ortadan kalktığında güven ilişkileri de yeniden değerlendirilmelidir.

İlke 20: Dış tarafların yaptığı değişiklikler kuruluş açısından değişiklik olmaktan çıkmaz.

Bulut sağlayıcısı, yazılım tedarikçisi veya başka bir dış taraf sistemin davranışını veya bağımlılıklarını değiştirebilir. Değişikliğin kuruluş tarafından doğrudan yapılmaması onun güvenlik sonuçlarını ortadan kaldırmaz.

İlke 21: Değişiklik yönetiminin güvencesi gerçek sistem dönüşümü üzerinden doğrulanabilmelidir.

Talep, onay veya dağıtım kayıtlarının bulunması tek başına güvence oluşturmaz. Neyin neden değiştiği, çalışan sistemde gerçekte neyin farklılaştığı, önemli güven varsayımlarının nasıl etkilendiği ve beklenen sonuç oluşmadığında güvenilir duruma dönmenin mümkün olup olmadığı gerektiğinde gösterilebilmelidir.