**Denetci.org**

**REFERANS İLKELERİ**

# Veritabanı Güvenliği İlkeleri

**Rİ-VER-3**

Sürüm 1.0 · 11.08.2026

www.denetci.org

# Veritabanı Güvenliği İlkeleri

Veritabanı güvenliği, verinin saklandığı teknoloji kadar o veriye kimlerin, hangi sistemlerin ve hangi yolların erişebildiğini; verinin nasıl değiştirilebildiğini ve kayıp halinde nasıl geri kazanılabildiğini ele alır. Amaç belirli bir veritabanı ürünü, sorgu yöntemi veya şifreleme teknolojisi belirlemek değil; veritabanının taşıdığı veri ve yetkinin açık güven sınırları içinde tutulmasını sağlayan tasarım anlayışını ortaya koymaktır.

**İlke 1: Veritabanının güvenliği yalnızca veritabanı sisteminin güvenliğinden ibaret değildir.**

Uygulamalar, yönetim araçları, kimlik altyapıları, yedekler, replikalar ve bulut yönetim katmanları veriye ulaşmanın farklı yollarını oluşturabilir. Verinin gerçek güvenliği, erişilebildiği bütün anlamlı yollar birlikte ele alınarak değerlendirilmelidir.

**İlke 2: Veritabanına erişim açıklanabilir bir kimlik ve ihtiyaca dayanmalıdır.**

Bir kişinin, uygulamanın veya hizmetin veritabanına neden eriştiği ve bu erişimin hangi işlev adına kullanıldığı anlaşılabilir olmalıdır. Teknik bağlantı ihtiyacı, belirsiz veya gereksiz geniş veri erişiminin gerekçesi haline gelmemelidir.

**İlke 3: Uygulama erişimi ile veritabanını yönetme yetkisi birbirine dönüşmemelidir.**

Bir uygulamanın veriyi okuyabilmesi veya değiştirebilmesi, veritabanının güvenlik ayarlarını, kullanıcılarını veya yapısını yönetebilmesini gerektirmez. Veriyi kullanmak ile veri ortamının güven sınırlarını değiştirmek ayrı etki alanlarıdır.

**İlke 4: Erişim, gerekli veri ve işlem kapsamıyla sınırlı olmalıdır.**

Bir tarafın belirli bir veri kümesini kullanması gerekiyorsa bu ihtiyaç ilgisiz verileri okuma, değiştirme, silme veya veri yapısını değiştirme yetkisi doğurmamalıdır. Yetki, veritabanının tamamına değil yerine getirilen gerçek işleve dayanmalıdır.

**İlke 5: Farklı veri işlemleri farklı güvenlik etkileri olarak ele alınmalıdır.**

Okuma, değiştirme, silme, toplu dışa aktarma ve veri yapısını değiştirme aynı sonucu doğurmaz. Bir işlev için gerekli olan yetki diğer yüksek etkili işlemleri kendiliğinden beraberinde getirmemelidir.

**İlke 6: Veritabanı bağlantısının teknik kimliği gerçek sorumluluğu görünmez hale getirmemelidir.**

Ortak veya aracılı hesaplar bazı mimarilerde gerekli olabilir; ancak önemli işlemlerin hangi uygulama, hizmet veya insan faaliyeti sonucunda gerçekleştiği tamamen kaybolmamalıdır. Bağlantı havuzu veya ortak hesap kullanımı hesap verebilirliğin sona ermesi anlamına gelmemelidir.

**İlke 7: Veritabanına ulaşabilmek veriye güvenilir erişim hakkı oluşturmamalıdır.**

Aynı ağda bulunmak, bağlantı noktasına erişebilmek veya bağlantı bilgisini bilmek tek başına yeterli güven oluşturmamalıdır. Ağ erişimi ile veri yetkisi ayrı güven sınırları olarak korunmalıdır.

**İlke 8: Uygulamanın veri erişim sınırları doğrudan veritabanı yollarıyla aşılmamalıdır.**

Bir uygulamanın kullanıcılar için uyguladığı iş kuralları ve erişim sınırları, yaygın doğrudan erişim yollarıyla kolayca etkisiz hale geliyorsa gerçek veri güvenliği daha zayıf olan bu yolla belirlenir. Bakım veya destek erişimi de gerçek güven modelinin parçasıdır.

**İlke 9: Üretim verisi daha düşük güvenli ortamlara taşındığında aynı veri olarak değerlendirilmelidir.**

Verinin geliştirme, test, analiz veya destek ortamına kopyalanması hassasiyetini ortadan kaldırmaz. Ortamın amacı değiştiğinde verinin gerekli olup olmadığı ve yeni erişim alanının oluşturduğu sonuç yeniden değerlendirilmelidir.

**İlke 10: Verinin yalnızca gerekli bölümü görünür ve kullanılabilir olmalıdır.**

Bir işlem verinin tamamına ihtiyaç duymuyorsa teknik olarak aynı kayıtta bulunduğu için bütün değerlerin açığa çıkarılması gerekmemelidir. Görüntüleme, sorgulama ve dışa aktarma davranışı gerçek kullanım ihtiyacıyla sınırlı kalmalıdır.

**İlke 11: Verinin şifrelenmesi gereksiz erişimi güvenli hale getirmemelidir.**

Şifreleme depolama ortamının veya belirli altyapı katmanlarının kaybına karşı koruma sağlayabilir; ancak veriyi çözebilen aşırı yetkili uygulama veya kullanıcıların oluşturduğu riski ortadan kaldırmaz. Kriptografik koruma erişim modelinin yerine geçmemelidir.

**İlke 12: Şifreleme anahtarları korudukları veriyle aynı kayıp alanına gereksiz biçimde bağlanmamalıdır.**

Veri ile onu çözebilecek anahtar aynı yetki, aynı sistem veya aynı yedek içerisinde birlikte ele geçirilebiliyorsa şifrelemenin sağladığı bağımsız koruma azalır. Anahtarın güven sınırı koruduğu veriyle olan gerçek ilişkiye göre tasarlanmalıdır.

**İlke 13: Veritabanına gönderilen veri ve sorgu amacı birbirine karışmamalıdır.**

Dışarıdan gelen bir değer, veritabanına hangi işlemin yaptırılacağını veya sorgunun yapısını sınırsız biçimde belirleyememelidir. Veri olarak alınan içerik, uygulamanın veritabanı üzerindeki daha geniş yetkisini saldırgana aktaracak bir komuta dönüşmemelidir.

**İlke 14: Veritabanı içindeki programlanabilir davranış da uygulamanın güvenlik yüzeyinin parçasıdır.**

Saklı yordamlar, tetikleyiciler, fonksiyonlar ve benzeri veritabanı içi mantık veri üzerinde önemli işlemler gerçekleştirebilir. Bu davranışların veritabanında bulunması onları normal yazılım güvenliği ve yetkilendirme anlayışının dışında bırakmamalıdır.

**İlke 15: Veri kopyaları üretim verisinden daha düşük değerde kabul edilmemelidir.**

Yedekler, snapshot'lar, klonlar ve replikalar aynı veya benzer veriyi farklı erişim yollarında barındırabilir. Birincil sistemin güçlü biçimde korunması, kopyalarının daha geniş erişilebilir olmasını güvenli hale getirmez.

**İlke 16: Kurtarma yeteneği onu gerekli kılacak olaydan mümkün olduğu ölçüde bağımsız olmalıdır.**

Üretim verisini bozabilen veya silebilen aynı hata, kimlik veya saldırının bütün geri dönüş kopyalarını da ortadan kaldırabilmesi veri güvencesini zayıflatır. Çoğaltma, erişilebilirlik sağlayabilir; ancak bozulan durumun aynı anda çoğaltılması kurtarılabilirlik anlamına gelmez.

**İlke 17: Veritabanındaki önemli değişiklikler yalnızca veri değişikliği olarak görülmemelidir.**

Şema, erişim modeli, veri ilişkileri veya kritik yapılandırmalar değiştiğinde uygulamanın güvenlik varsayımları da değişebilir. Teknik değişikliğin veri bütünlüğü ve erişim sınırları üzerindeki etkisi anlaşılabilir olmalıdır.

**İlke 18: Yönetilen veritabanı hizmeti kullanılması güvenlik sorumluluğunu bütünüyle başka tarafa taşımaz.**

Sağlayıcı altyapının bazı katmanlarını yönetebilir; ancak kuruluşun kimlere erişim verdiği, hangi veriyi tuttuğu ve hizmeti nasıl yapılandırdığı gibi güven kararları devam eder. Bulut veya dış hizmet kullanımı gerçek sorumluluk sınırlarını görünür kılmalıdır.

**İlke 19: Veritabanı güvencesi gerçek veri erişimi ve değişim davranışı üzerinden doğrulanabilmelidir.**

Rol listeleri, şifreleme ayarları, yedeklerin varlığı veya veritabanı güvenlik ürünleri tek başına güvence oluşturmaz. Gerçekte hangi kimliklerin hangi veriler üzerinde hangi işlemleri yapabildiği, doğrudan ve dolaylı erişim yollarının neler olduğu, önemli değişikliklerin nasıl ortaya çıktığı ve verinin gerektiğinde güvenilir biçimde geri kazanılıp kazanılamadığı gösterilebilmelidir.