Denetci.org

REFERANS İLKELERİ

Veri Güvenliği İlkeleri

Rİ-VER-1

Sürüm 1.0 · 11.08.2026

www.denetci.org

Veri Güvenliği İlkeleri

Veri güvenliği, verinin oluşturulmasından kullanımına ve yaşamının sona ermesine kadar taşıdığı değerin, bütünlüğün, erişilebilirliğin ve kullanım sınırlarının korunmasını ele alır. Amaç belirli sınıflandırma seviyeleri, şifreleme yöntemleri veya veri kaybı önleme ürünleri belirlemek değil; verinin gerçek değeri, kullanım amacı, kopyaları ve bağımlılıkları üzerinden korunmasını sağlayan kalıcı bir tasarım anlayışı oluşturmaktır.

İlke 1: Verinin korunma düzeyi gerçek kayıp ve kötüye kullanım etkisine dayanmalıdır.

Bütün veriler aynı güvenlik sonucunu doğurmaz. Açığa çıkma, değiştirilme, yok olma veya kullanılamama halinde ortaya çıkabilecek gerçek sonuçlar verinin nasıl korunacağına yön vermelidir.

İlke 2: Veri sınıflandırması yalnızca isimlendirme değil güvenlik kararlarını etkileyen bir anlam taşımalıdır.

Bir veriye verilen etiket, erişim, paylaşım, saklama veya başka davranışlarda hiçbir fark oluşturmuyorsa sınıflandırmanın güvenlik değeri sınırlıdır. Sınıflandırma, verinin nasıl ele alınacağı konusunda açıklanabilir sonuçlar doğurmalıdır.

İlke 3: Verinin değeri yalnızca tekil parçalarından anlaşılmayabilir.

Tek başına düşük hassasiyetli görünen bilgiler bir araya geldiğinde yeni ve daha hassas bir anlam oluşturabilir. Veri güvenliği, birleşimlerin ve çıkarımların yaratabileceği güvenlik etkisini de dikkate almalıdır.

İlke 4: Önemli verinin amacı ve sorumluluğu anlaşılabilir olmalıdır.

Bir verinin neden tutulduğu, hangi işlevi desteklediği ve onun kullanımı hakkında anlamlı kararları kimin verebildiği belirsiz kalmamalıdır. Sahipsiz veya amacı bilinmeyen veri zamanla gereksiz ve kontrolsüz bir maruziyete dönüşebilir.

İlke 5: Veri erişimi, işlev için gereken veri ve işlem kapsamıyla sınırlı olmalıdır.

Bir sisteme erişebilmek onun içerdiği bütün veriyi görme, değiştirme, silme veya dışarı çıkarma hakkı doğurmamalıdır. Erişimin genişliği kullanıcının veya sistemin gerçek ihtiyacıyla uyumlu olmalıdır.

İlke 6: Farklı veri işlemleri farklı güven sonuçları olarak ele alınmalıdır.

Veriyi görüntülemek, değiştirmek, silmek, çoğaltmak veya toplu biçimde dışarı aktarmak aynı etkiyi oluşturmaz. Bir işlem için verilen yetki gereksiz biçimde diğer işlem yetkilerini beraberinde getirmemelidir.

İlke 7: Toplu erişim, tekil erişimin yalnızca daha hızlı biçimi değildir.

Çok sayıda kayda aynı anda erişebilmek veya bunları dışarı aktarabilmek tek tek kayıtlarla çalışmaktan çok daha geniş bir kayıp alanı oluşturabilir. Yetkilendirme ve koruma, erişimin hacmini ve birikimli etkisini dikkate almalıdır.

İlke 8: Yetkili erişim her kullanımın uygun olduğu anlamına gelmemelidir.

Bir tarafın veriye erişmeye yetkili olması veriyi her amaçla kullanabileceği anlamına gelmez. Veri güvenliği, mümkün olduğu ölçüde erişimin yanında kullanımın amaç ve bağlamını da korumalıdır.

İlke 9: Verinin güvenliği ana sisteminin sınırlarıyla sona ermemelidir.

Veri uygulamalarda, yedeklerde, analiz ortamlarında, dışa aktarımlarda, loglarda veya dış hizmetlerde kopyalanabilir. Güvenlik anlayışı, verinin bilinen bütün anlamlı kopyalarını ve kullanım alanlarını kapsamalıdır.

İlke 10: Veri kopyalarının çoğalması güvenlik açısından bir maliyettir.

Her yeni kopya yeni bir erişim ve kayıp alanı oluşturabilir. Veri, gerçek bir ihtiyaç olmadan çoğaltılmamalı ve ihtiyacı sona eren kopyalar varsayılan olarak süresiz yaşamamalıdır.

İlke 11: Geçici veri güvenlik yaşam döngüsünün dışında değildir.

Önbellekler, kuyruklar, geçici dosyalar, bellek dökümleri ve işlem ara çıktıları kısa ömürlü olsalar da hassas bilgi taşıyabilir. Verinin ne kadar süre kaldığı kadar bu süre boyunca kimler tarafından görülebildiği de önemlidir.

İlke 12: Daha düşük güvenli ortamlara veri taşınması açık bir güven kararı olmalıdır.

Test, geliştirme, destek veya analiz ihtiyacı üretim verisinin otomatik olarak başka ortamlara kopyalanmasını gerektirmez. Ortam değiştiğinde verinin erişim alanı ve koruma varsayımları da yeniden değerlendirilmelidir.

İlke 13: Verinin tanımlanamaz olduğu iddiası gerçek yeniden ilişkilendirme imkânına dayanmalıdır.

Bir adın veya doğrudan tanımlayıcının kaldırılması, veri başka bilgilerle yeniden ilişkilendirilebiliyorsa anonimlik oluşturmaz. Maskeleme, takma adlandırma ve benzeri yöntemlerin güvencesi gerçek yeniden tanımlama ihtimaline göre değerlendirilmelidir.

İlke 14: Kriptografik koruma doğru veri erişiminin yerine geçmemelidir.

Şifreleme veriyi önemli tehditlere karşı koruyabilir; ancak gereksiz kişilere verilen çözme yetkisini veya yanlış paylaşımı düzeltmez. Kriptografi, veri üzerindeki kimlik ve yetki sınırlarını desteklemelidir.

İlke 15: Veri farklı yaşam durumlarında farklı biçimde açığa çıkabilir.

Aktarım sırasında korunan veri depolanırken, işlenirken veya kullanıcıya gösterilirken farklı güven sınırlarına girebilir. Veri güvenliği yalnızca durağan veya yalnızca hareket halindeki veri üzerinden tasarlanmamalıdır.

İlke 16: Verinin bütünlüğü, yalnızca mevcut değerin doğru görünmesi değildir.

Veri yanlışlıkla veya kasıtlı biçimde değiştirilebilir, kaynağı taklit edilebilir veya önemli bölümleri kaldırılabilir. Kritik kullanımda verinin kaynağı ve değişim geçmişi gerektiğinde güvenilir biçimde anlaşılabilmelidir.

İlke 17: Veriyi yok etme gücü de bir güvenlik yetkisidir.

Silme veya bozma, bazı durumlarda veriyi okumaktan daha büyük etki oluşturabilir. Veri güvenliği gizliliğin yanında bütünlük, kullanılabilirlik ve geri dönüş imkânını da dikkate almalıdır.

İlke 18: Kurtarılabilirlik verinin korunmasının bir parçasıdır.

Bir veri hata, saldırı veya başka bir olay sonrasında güvenilir duruma döndürülemiyorsa yalnızca yetkisiz erişimin engellenmiş olması yeterli güvence oluşturmaz. Kurtarma yeteneği, korunması gereken veri ve sonuçlarla uyumlu olmalıdır.

İlke 19: Kurtarma kopyaları aynı güven kaybına bütünüyle bağımlı olmamalıdır.

Üretim verisini değiştirebilen veya yok edebilen aynı kimlik, hata veya saldırının bütün geri dönüş imkânlarını da ortadan kaldırabilmesi veri güvencesini zayıflatır. Kurtarılabilirlik, mümkün olduğu ölçüde onu gerekli kılacak olaydan bağımsızlık taşımalıdır.

İlke 20: Veri yalnızca gerekli olduğu süre boyunca güven ilişkisi oluşturmaya devam etmelidir.

Geçmişte ihtiyaç duyulmuş bir verinin süresiz saklanması yeni değer üretmeden güvenlik etkisini sürdürebilir. Saklama, veri değerinin ve gerçek yükümlülüklerin devam ettiği süreyle anlamlı biçimde ilişkili olmalıdır.

İlke 21: Verinin yaşamının sona ermesi yalnızca ana kopyanın silinmesiyle gerçekleşmiş sayılmamalıdır.

Yedekler, arşivler, dışa aktarımlar ve üçüncü taraf sistemler aynı veriyi taşımaya devam edebilir. Bir verinin artık tutulmadığı veya erişilemediği iddiası gerçek kopyaların durumuyla uyumlu olmalıdır.

İlke 22: Veri başka tarafa geçtiğinde yeni güven ilişkileri doğduğu kabul edilmelidir.

Üçüncü taraflar, dış hizmetler veya başka sistemler verinin yeni kopyalarını, erişim yollarını ve bağımlılıklarını oluşturabilir. Verinin kaynak sistemden çıkması kuruluş açısından güvenlik etkisinin sona erdiği anlamına gelmemelidir.

İlke 23: Teknik yönetim yetkisi gereksiz veri kullanım yetkisine dönüşmemelidir.

Bir sistemin altyapısını yönetmek, içindeki bütün verinin içeriğine ihtiyaç olduğu anlamına gelmez. Mümkün olduğu ölçüde sistemi yönetebilme gücü ile veriyi kullanabilme gücü birbirinden ayrılmalıdır.

İlke 24: Veri güvenliği insan hatasının makul biçimde gerçekleşeceğini kabul etmelidir.

Yanlış alıcı, yanlış paylaşım, yanlış dışa aktarım veya yanlış silme tamamen ortadan kaldırılamayabilir. Tasarım, tek bir olağan hatanın gereksiz ölçüde büyük veri kaybına veya açıklamaya dönüşmesini sınırlandırmalıdır.

İlke 25: Güvenlik görünürlüğü yeni veri maruziyeti oluşturmamalıdır.

Loglama, izleme, tanılama ve güvenlik araçları veriyi korumaya yardımcı olurken hassas içeriğin yeni kopyalarını da oluşturabilir. Güvence amacıyla toplanan bilgi, korunan veriden daha geniş ve kontrolsüz bir maruziyet alanına dönüşmemelidir.

İlke 26: Veri güvenliği değişen kullanım biçimleriyle birlikte yeniden anlamlandırılmalıdır.

Yeni entegrasyonlar, analiz biçimleri, yapay zekâ kullanımları veya başka teknolojik değişiklikler aynı verinin erişim ve kullanım alanını değiştirebilir. Geçmişte uygun kabul edilen koruma modeli yeni kullanım bağlamında otomatik olarak yeterli sayılmamalıdır.

İlke 27: Veri güvenliği gerçek veri davranışı üzerinden doğrulanabilmelidir.

Sınıflandırma şeması, şifreleme ürünü, DLP sistemi veya erişim matrisi tek başına güvence oluşturmaz. Hassas verinin gerçekte nerelerde bulunduğu, hangi tarafların hangi işlemleri yapabildiği, hangi kopyaların oluştuğu ve veri yaşamının sona erdirilmesinin veya kurtarılmasının fiilen mümkün olup olmadığı gerektiğinde gösterilebilmelidir.