Denetci.org

REFERANS İLKELERİ

Veri Aktarımı İlkeleri

Rİ-VER-2

Sürüm 1.0 · 11.08.2026

www.denetci.org

Veri Aktarımı İlkeleri

Veri aktarımı, verinin bir sistemden, güven alanından veya sorumluluk alanından başka birine taşındığı süreçte oluşan güven ilişkilerini ele alır. Amaç belirli bir protokol, dosya aktarım ürünü veya iletişim kanalı belirlemek değil; aktarılan verinin doğru tarafa, gerekli kapsamda, beklenen bütünlükle ve açıklanabilir bir güven ilişkisi içinde ulaşmasını sağlayan tasarım anlayışını ortaya koymaktır.

İlke 1: Her veri aktarımı kaynak, hedef ve amaç bakımından açıklanabilir olmalıdır.

Bir veri akışının neden var olduğu, hangi taraftan hangi tarafa gerçekleştiği ve hangi ihtiyacı karşıladığı bilinmelidir. Sahibi ve amacı bilinmeyen veri akışları zamanla gereksiz ve görünmez güven ilişkilerine dönüşebilir.

İlke 2: Veri yalnızca gerçek aktarım ihtiyacı kadar paylaşılmalıdır.

Hedef tarafın bir işlev için veriye ihtiyaç duyması kaynak sistemde bulunan bütün verinin aktarılmasını gerektirmez. Aktarım kapsamı, amaç için gerekli veri ve işlemle sınırlı olmalıdır.

İlke 3: Veri aktarımı bir güven sınırının geçilmesi olarak değerlendirilebilmelidir.

Kaynak ve hedef aynı kuruluşta veya aynı ağda bulunsa bile farklı kullanıcıları, sistemleri ve güven varsayımlarını temsil edebilir. Bir aktarımın “içeride” gerçekleşmesi onun güvenlik açısından önemsiz olduğu anlamına gelmez.

İlke 4: Kaynak ve hedef kimlikleri gerçek taraflarla güvenilir biçimde ilişkilendirilmelidir.

Bir adres, ağ konumu veya bağlantının kurulabilmiş olması gönderenin veya alıcının amaçlanan taraf olduğunu tek başına kanıtlamaz. Önemli veri akışlarında iletişimin hangi gerçek taraflar arasında kurulduğuna ilişkin yeterli güven bulunmalıdır.

İlke 5: Bağlantı kurabilmek veri alma veya gönderme yetkisi oluşturmamalıdır.

Bir tarafın iletişim kanalına erişebilmesi ilgili veriyi gönderme, alma veya değiştirme hakkına sahip olduğu anlamına gelmez. Aktarım yetkisi veri, işlem ve amaç bakımından sınırlandırılmalıdır.

İlke 6: Aktarımın gizliliği, doğru aktarım yapıldığı anlamına gelmemelidir.

Şifrelenmiş bir kanal veriyi gözlemden koruyabilir; ancak yanlış alıcıya gönderilen, gereğinden fazla paylaşılan veya yetkisiz biçimde kullanılan veriyi güvenli hale getirmez. Gizlilik, aktarım güvencesinin yalnızca bir bölümüdür.

İlke 7: Aktarımın bütünlüğü yalnızca verinin bozulmamış görünmesine indirgenmemelidir.

Verinin kaynağı, içeriği, sırası veya bütünlüğü aktarım sırasında değiştirilebilir. Hedef taraf gerektiğinde aldığı verinin beklenen kaynaktan ve beklenen biçimde geldiğine güvenebilmelidir.

İlke 8: Güvenli protokol adı tek başına güvenli aktarım kanıtı olmamalıdır.

Güçlü bir protokol yanlış kimlik doğrulaması, hatalı sertifika doğrulaması veya gereksiz geniş yetkilerle kullanıldığında beklenen güvenceyi sağlamayabilir. Değerlendirme kullanılan teknoloji etiketinden çok gerçek bağlantı davranışına dayanmalıdır.

İlke 9: Güçlü bir aktarım yöntemi başarısız olduğunda daha zayıf güvene sessizce geçilmemelidir.

Uyumluluk veya kullanılabilirlik amacıyla daha zayıf bir iletişim biçimine geçiş yapılabiliyorsa bu sistemin gerçek güvenlik davranışının parçasıdır. Hata durumunda hangi güven düzeyinin kabul edildiği açık ve bilinçli olmalıdır.

İlke 10: Aktarımda kullanılan kimlik bilgileri aktarabildikleri veri kadar kritik kabul edilmelidir.

Bir servis hesabı, belirteç, anahtar veya sertifika ele geçirildiğinde saldırgan veri akışını taklit edebilir veya kullanabilir. Bu güven unsurlarının kapsamı aktarımın gerçek ihtiyacını aşmamalıdır.

İlke 11: Ara sistemler veri yolunun gerçek parçaları olarak görülmelidir.

Geçitler, proxy'ler, mesajlaşma sistemleri, entegrasyon platformları ve dönüşüm hizmetleri aktarım sırasında veriyi görebilir, değiştirebilir veya saklayabilir. Güvence yalnızca kaynak ve hedef uçların korunmasına dayanmamalıdır.

İlke 12: Geçici taşıma noktaları gereksiz kalıcı veri depolarına dönüşmemelidir.

Aktarım sırasında veri bazı ara sistemlerde tutulabilir; ancak taşıma ihtiyacının sona ermesi bu kopyaların süresiz yaşamasını gerektirmez. Ara depolama da verinin gerçek yaşam döngüsünün bir parçasıdır.

İlke 13: Veri dönüşümü aktarım bütünlüğünün parçasıdır.

Biçim, kodlama, alan eşleme veya başka dönüşümler verinin anlamını değiştirebilir. Hedefe teknik olarak ulaşmış bir veri, beklenen anlamı taşımıyorsa aktarım güvenilir biçimde tamamlanmış sayılmamalıdır.

İlke 14: Güvenilir kaynaktan gelen veri güvenilir içerik varsayımına dönüşmemelidir.

Yetkili bir sistem hatalı, bozuk veya saldırgan tarafından etkilenmiş veri üretebilir. Hedef sistem, gelen veriyi kaynağın kimliğinden bağımsız olarak kendi güvenlik sınırları içinde değerlendirebilmelidir.

İlke 15: Tekrar ve sıralama anlam taşıyorsa aktarım tasarımında korunmalıdır.

Geçerli bir mesajın yeniden gönderilmesi veya mesajların farklı sırada ulaşması bazı işlemlerde farklı ve zararlı sonuçlar oluşturabilir. Aktarımın güveni, uygulamanın bu davranışlara ilişkin varsayımlarını dikkate almalıdır.

İlke 16: Teknik gönderim ile başarılı iş sonucu aynı şey değildir.

Kaynak tarafın veriyi göndermiş olması hedefin onu eksiksiz aldığını, doğruladığını veya işleyebildiğini göstermez. Önemli aktarımlarda başarı, beklenen sonucun gerçekten oluşmasıyla ilişkilendirilebilmelidir.

İlke 17: Kısmi ve yinelenen aktarım güvenilir tam aktarım gibi işlenmemelidir.

Bağlantı kesintileri ve yeniden denemeler eksik veya tekrar eden veriler oluşturabilir. Hata davranışı, veri bütünlüğünü ve işlemin gerçek anlamını koruyacak şekilde tasarlanmalıdır.

İlke 18: Toplu veri aktarımı daha geniş bir güvenlik etkisi olarak görülmelidir.

Bir veri akışının olağan olması, çok büyük hacimde veya alışılmadık kapsamda gerçekleşmesinin de aynı güvenlik anlamına geldiği anlamına gelmez. Tek bir aktarımın oluşturabileceği toplam etki tasarımın parçası olmalıdır.

İlke 19: Aktarım kanalı değiştiğinde veri güvenlik varsayımları yeniden değerlendirilmelidir.

E-posta, API, dosya paylaşımı, mesajlaşma veya fiziksel taşıma gibi farklı kanallar farklı kopyalama, yönlendirme ve erişim özellikleri oluşturabilir. Veri güvenliği kanaldan bağımsız ilkeler taşısa da kanalın gerçek davranışı göz ardı edilmemelidir.

İlke 20: Üçüncü tarafa aktarım verinin yaşam döngüsünü sona erdirmez.

Veri başka kuruluşa geçtiğinde orada saklanabilir, yedeklenebilir veya başka hizmetlere aktarılabilir. Kaynak kuruluş açısından güvenlik değerlendirmesi yalnızca ilk teslim noktasında bitmemelidir.

İlke 21: Gerçek veri yolu dolaylı alıcıları da içermelidir.

Bir aktarımın doğrudan hedefi başka sağlayıcıları, alt yüklenicileri veya farklı işleme alanlarını kullanabilir. Verinin güven modeli yalnızca ilk alıcının adıyla sınırlandırılmamalıdır.

İlke 22: Aktarım ilişkisi sona erdiğinde gerçek veri akışı da sona erebilmelidir.

Bir entegrasyonun, iş ilişkisinin veya ihtiyacın sona ermesi sonrasında otomatik veri akışları, erişim bilgileri veya eski aktarım uçları çalışmaya devam etmemelidir. İdari sona erme teknik davranışta karşılık bulmalıdır.

İlke 23: Aktarımın izlenebilirliği veri içeriğinin gereksiz kopyalarını oluşturmamalıdır.

Hangi taraflar arasında hangi aktarımın gerçekleştiğini anlamak önemli olabilir; ancak bunun için hassas verinin tamamını loglara veya tanılama sistemlerine taşımak gerekmeyebilir. Görünürlük, yeni bir veri maruziyeti yaratmadan sağlanmalıdır.

İlke 24: Önemli veri aktarımları sonradan açıklanabilir olmalıdır.

Gerektiğinde hangi verinin veya veri kümesinin, hangi kaynaktan, hangi hedefe ve hangi sonuçla hareket ettiği anlaşılabilmelidir. Bu açıklanabilirlik her aktarımın bütün içeriğinin

kaydedilmesini değil, güven ilişkisini ve sonucu gösterebilecek yeterli kanıtın bulunmasını gerektirir.

İlke 25: Veri aktarımı güvencesi gerçek veri akışı üzerinden doğrulanabilmelidir.

Bir entegrasyon belgesi, şifreli protokol veya veri aktarım ürününün varlığı tek başına güvence oluşturmaz. Gerçekte hangi verinin hangi taraflara gittiği, aktarım sırasında hangi ara sistemlerden geçtiği, hangi kapsam ve yetkiyle kullanıldığı, bütünlüğünün korunup korunmadığı ve ilişki sona erdiğinde akışın gerçekten durdurulabildiği gerektiğinde gösterilebilmelidir.