Denetci.org

REFERANS İLKELERİ

Tedarik Zinciri Güvenliği İlkeleri

Rİ-TED-2

Sürüm 1.0 · 11.08.2026

www.denetci.org

Tedarik Zinciri Güvenliği İlkeleri

Tedarik zinciri güvenliği, kuruluşun kullandığı dış yazılım, donanım, hizmet, geliştirme aracı ve diğer bağımlılıkların kendi güvenlik sonuçlarına nasıl etki ettiğini ele alır. Amaç dış bağımlılıkları ortadan kaldırmak veya tedarikçileri koşulsuz biçimde güvenilir ya da güvensiz saymak değil; dışarıya verilen güvenin nerede başladığını, ne kadar etki oluşturduğunu ve bu güven kaybedildiğinde sonucun ne ölçüde sınırlandırılabildiğini anlamaktır.

İlke 1: Her dış bağımlılık bir güven ilişkisi olarak görülmelidir.

Bir yazılım paketi, hizmet, API, donanım veya başka dış unsur kuruluş sistemlerine kod, veri veya yetki taşıyabilir. Satın alma ya da entegrasyon kararı, beraberinde hangi güvenin kabul edildiğini görünmez bırakmamalıdır.

İlke 2: Tedarikçinin önemi ticari büyüklüğünden değil oluşturabileceği etkiden doğmalıdır.

Düşük maliyetli küçük bir bileşen kritik bir sistem içinde yüksek yetkiyle çalışabilir; büyük bir sağlayıcı ise sınırlı bir işlev sunabilir. Tedarik zinciri riski sözleşme değerine değil gerçek teknik ve iş etkisine dayanmalıdır.

İlke 3: Doğrudan görünmeyen bağımlılıklar güven modelinin dışında kalmamalıdır.

Tedarikçiler kendi alt yüklenicilerini, yazılım bağımlılıklarını veya altyapı sağlayıcılarını kullanabilir. Kuruluşun doğrudan sözleşme yapmadığı bir taraf da sonuçları üzerinde önemli etki oluşturabilir.

İlke 4: Dış bileşenin yaygın kullanılması güvenilirliğinin tek gerekçesi olmamalıdır.

Yaygın yazılım ve hizmetler daha fazla inceleme görebilir; ancak aynı zamanda geniş saldırı değeri ve ortak başarısızlık alanı oluşturabilir. Popülerlik kendi başına güven kanıtı değildir.

İlke 5: Bileşenin kaynağı gerektiğinde doğrulanabilir olmalıdır.

Bir yazılımın, güncellemenin veya cihaz yazılımının amaçlanan üreticiden ya da dağıtım yolundan geldiğine ilişkin güven bulunmalıdır. İçeriğin nereden geldiğinin bilinmemesi tedarik zincirinin önemli bir bölümünü belirsiz bırakır.

İlke 6: Güvenilir kaynaktan gelmek içeriğin güvenli olduğunu garanti etmemelidir.

Yetkili bir tedarikçi hatalı veya ele geçirilmiş bir bileşen yayımlayabilir. Kaynağın doğrulanması, içeriğin güvenlik etkisinin ayrıca değerlendirilmesi ihtiyacını ortadan kaldırmamalıdır.

İlke 7: Bileşen bütünlüğü yalnızca üretildiği noktada değil teslimat boyunca korunmalıdır.

Bir yazılım veya donanım doğru üretilmiş olsa bile dağıtım, depolama veya güncelleme yollarında değiştirilebilir. Güven zinciri yalnızca üreticinin başlangıç iddiasına dayanmamalıdır.

İlke 8: Güncelleme mekanizması kritik bir kod ve güven dağıtım yolu olarak görülmelidir.

Güncelleme yetkisi çok sayıda sisteme yeni davranış taşıyabilir. Bu mekanizmanın kaybı, tek tek sistemlere saldırmaktan daha geniş etki oluşturabileceği için sıradan işletim kolaylığı olarak değerlendirilmemelidir.

İlke 9: Otomatik güncelleme sağladığı güvenlik faydası ile oluşturduğu ortak etkiyi birlikte taşımalıdır.

Hızlı güncelleme bilinen zayıflıkların süresini azaltabilir; ancak hatalı veya ele geçirilmiş güncellemenin de hızla yayılmasına neden olabilir. Otomasyon güncellemenin kaynağı ve sonucuna ilişkin bütün muhakemeyi ortadan kaldırmamalıdır.

İlke 10: Dış bileşenlerin gerçek kullanımı anlaşılabilir olmalıdır.

Bir paketin veya hizmetin kuruluşta bulunması hangi sistemler tarafından ve ne ölçüde kullanıldığını açıklamaz. Tedarik zinciri olayında veya zayıflığında gerçek etkilenme ancak kullanım ilişkileri bilindiği ölçüde anlaşılabilir.

İlke 11: Bileşen bilgisi yalnızca isim ve sürüm listesinden ibaret olmamalıdır.

Aynı bağımlılık farklı uygulamalarda farklı işlev ve yetkilerle kullanılabilir. Güvenlik açısından önemli olan yalnızca bileşenin bulunması değil, sistem içinde ne yapabildiği ve hangi sonuçlara katkı sağladığıdır.

İlke 12: Kullanılmayan dış bağımlılıklar güvenlik açısından nötr kabul edilmemelidir.

Artık işlev üretmeyen bir bileşen zafiyet, güncelleme ve tedarik zinciri riski taşımaya devam edebilir. Bir bağımlılığın geçmişte gerekli olması onu süresiz biçimde sistemin parçası yapmamalıdır.

İlke 13: Yeni bağımlılık eklemek kalıcı ve maliyetsiz bir karar olarak görülmemelidir.

Her yeni bileşen yeni güven varsayımları, bakım ihtiyacı ve olası saldırı yolları oluşturur. Sağladığı değer, oluşturduğu uzun vadeli bağımlılığı haklı çıkarabilmelidir.

İlke 14: Kritik dış bağımlılıktan çıkabilme imkânı güvenlik tasarımının parçası olmalıdır.

Bir sağlayıcı veya bileşen artık güvenilir, desteklenebilir veya kullanılabilir olmadığında kuruluşun tamamen hareketsiz kalması gerekmemelidir. Değiştirme veya kaldırma maliyeti, bağımlılığın oluşturduğu gerçek güven yoğunlaşmasının bir parçasıdır.

İlke 15: Tedarikçiye verilen erişim tedarik ürününden ayrı bir güven ilişkisi olarak ele alınmalıdır.

Bir hizmet veya ürün satın alınması, sağlayıcının kuruluş sistemlerine geniş teknik erişimini otomatik olarak gerektirmez. Destek ve yönetim erişimleri gerçek görev ve etki ihtiyacına göre ayrıca sınırlandırılmalıdır.

İlke 16: Tedarikçinin yönettiği kimlik, sır ve anahtarlar kuruluşun güven modelinin parçasıdır.

Bu unsurlar başka tarafta tutuluyor olsa bile kuruluşun sistemlerine veya verisine erişim sağlayabilir. Yönetimin dışarıda olması güvenlik etkisini kuruluşun dışına çıkarmaz.

İlke 17: Tedarikçiyle veri paylaşılması yalnızca veri aktarımı olarak görülmemelidir.

Veri dış tarafa geçtiğinde yeni saklama, erişim, yedekleme ve alt işleme alanları oluşabilir. Güvenlik modeli yalnızca ilk teslim noktasına değil verinin tedarikçi ortamındaki gerçek yaşamına da dayanmalıdır.

İlke 18: Bir tedarikçinin güvenlik beyanları yararlı kanıt olmalı fakat güvenin kendisi haline gelmemelidir.

Sertifikalar, denetim raporları ve güvenlik açıklamaları belirsizliği azaltabilir; ancak kuruluşun gerçek kullanım biçimini veya bütün gelecekteki davranışları garanti etmez. Kanıtın kapsamı ve desteklediği iddia bilinmelidir.

İlke 19: Tedarik zinciri güvenliği yalnızca ilişkinin başlangıcında değerlendirilmemelidir.

Tedarikçinin sahipliği, altyapısı, güvenlik durumu, alt bağımlılıkları veya sağladığı ürün zaman içinde değişebilir. Geçmiş değerlendirme değişmiş bir güven ilişkisi için süresiz güvence sağlamamalıdır.

İlke 20: Tedarikçi güvenlik olayı kuruluş için dışarıda gerçekleşen bağımsız bir olay sayılmamalıdır.

Bir dış tarafın ele geçirilmesi kuruluşun verisini, yazılımını, kimliklerini veya sistemlerini etkileyebilir. Sağlayıcının kendi müdahalesini yürütmesi kuruluşun kendi etkisini anlamak ve sınırlandırmak ihtiyacını ortadan kaldırmaz.

İlke 21: Tedarik zinciri olayında etki yalnızca tedarikçinin bildirdiği alanla sınırlı varsayılmamalıdır.

Kuruluşun bileşeni nasıl kullandığı tedarikçinin bilmediği ek etkiler oluşturabilir. Olay kapsamı, dış bildirim ile kuruluşun kendi bağımlılık ve erişim bilgisi birlikte kullanılarak anlaşılmalıdır.

İlke 22: Tedarik zincirindeki güven kaybı gerektiğinde gerçek sistem davranışında sınırlandırılabilmelidir.

Bir sağlayıcıya, güncellemeye, sertifikaya veya bileşene artık güvenilmediğinde yalnızca idari karar almak yeterli değildir. İlgili kod, bağlantı, kimlik veya veri ilişkisinin etkisi teknik olarak da sona erdirilebilmelidir.

İlke 23: Birden fazla sağlayıcının bulunması tek başına bağımsızlık oluşturmaz.

Alternatifler aynı altyapıya, teknolojiye veya alt sağlayıcıya dayanabilir; ayrıca gerçek geçiş yeteneği bulunmayabilir. Tedarik çeşitliliği, ortak başarısızlık alanlarını gerçekten azaltabildiği ölçüde güvence sağlar.

İlke 24: Tedarik zinciri güvencesi gerçek bağımlılık ve etki ilişkileri üzerinden doğrulanabilmelidir.

Tedarikçi listeleri, anketler, sözleşmeler veya sertifikasyonlar tek başına güvence oluşturmaz. Kuruluşun hangi dış unsurlara neden güvendiği, bunların hangi sistem ve verileri etkileyebildiği, güven kaybının ne kadar yayılabileceği ve gerektiğinde bu ilişkinin gerçekten sona erdirilip erdirilemediği gösterilebilmelidir.