Denetci.org

REFERANS İLKELERİ

Güvenlik Mimarisi İlkeleri

Rİ-YON-3

Sürüm 1.0 · 11.08.2026

www.denetci.org

Güvenlik Mimarisi İlkeleri

Güvenlik mimarisi, bir sistemin bileşenleri arasındaki güven ilişkilerinin nasıl kurulduğunu, hangi sınırlarla ayrıldığını ve bir güven kaybının ne kadar yayılabileceğini belirleyen tasarım anlayışıdır. Bu ilkelerin amacı belirli bir ağ modeli, ürün veya mimari desen dayatmak değil; sistemlerin güveni nerede oluşturduğunu, nerede sınırlandırdığını ve bu tasarımın gerçek davranış üzerinden nasıl anlaşılabileceğini ortaya koymaktır.

İlke 1: Güven sınırları sistemin gerçek güven ilişkilerini yansıtmalıdır.

Aynı ağda, bulut ortamında, uygulamada veya kuruluş içinde bulunmak bileşenleri kendiliğinden aynı güven alanına getirmemelidir. Bir sınırın anlamı fiziksel veya mantıksal konumdan değil, tarafların birbirleri üzerinde oluşturabildiği gerçek etkiden doğmalıdır.

İlke 2: Her güven ilişkisi bir gereksinime dayanmalı ve bu gereksinimi aşmamalıdır.

Bir kullanıcının, hizmetin veya sistemin başka bir bileşene güvenmesi yalnızca teknik kolaylık veya mevcut bağlantı nedeniyle açıklanmamalıdır. Verilen güven, yerine getirilmek istenen işlev için gereken ilişki ve etki alanıyla sınırlı kalmalıdır.

İlke 3: Bir güven alanının kaybı diğer alanların kaybını kaçınılmaz hale getirmemelidir.

Bir hesap, sistem, ağ bölümü veya hizmet ele geçirildiğinde saldırganın etkisi mimari boyunca sınırsız biçimde ilerlememelidir. Güven sınırları, yalnızca erişimi düzenlemek için değil başarısızlığın yayılmasını sınırlandırmak için de anlam taşımalıdır.

İlke 4: Yüksek etkili yönetim ve kontrol yolları sıradan kullanım yollarından ayrıştırılmalıdır.

Sistemlerin yapılandırmasını, kimliklerini, politikalarını veya çalışma biçimini değiştirebilen yollar normal hizmet kullanımından daha geniş sonuçlar doğurabilir. Mimari, bu geniş etkinin ayrı bir güven alanı olduğunu kabul etmelidir.

İlke 5: Kimlik, konumun veya bağlantının yerine geçen bir güven unsuru olmamalıdır.

Bir tarafın nereden bağlandığı güvenlik kararına katkı sağlayabilir; ancak kim olduğunu ve ne yapmaya yetkili olduğunu tek başına kanıtlamaz. Kullanıcı, cihaz, uygulama ve hizmet kimliklerinin mimari içindeki anlamı açık olmalıdır.

İlke 6: Farklı kimlik türleri taşıdıkları sorumluluğa göre ayrıştırılmalıdır.

İnsan kullanıcılar, uygulamalar, otomasyonlar ve hizmetler farklı kullanım ve hesap verebilirlik özelliklerine sahiptir. Bir kimlik türünün diğerinin yerine kullanılması, sahiplik ve etki sınırlarını görünmez hale getirmemelidir.

İlke 7: Veri hareketi gereksiz yetki hareketi oluşturmamalıdır.

İki sistem arasında veri alışverişi yapılması, bu sistemlerin birbirleri üzerinde yönetim veya geniş erişim yetkisine sahip olmasını gerektirmez. Veri akışı ile kontrol yetkisi mimaride ayrı ilişkiler olarak değerlendirilebilmelidir.

İlke 8: Ortak bağımlılıklar gerçek ortak başarısızlık alanları olarak görülmelidir.

Birbirinden bağımsız görünen sistemler aynı kimlik altyapısına, yönetim hizmetine, sağlayıcıya, ağa veya başka bir temel bileşene dayanabilir. Mimarinin dayanıklılığı, bileşen sayısından çok bu ortak bağımlılıkların ne ölçüde ayrıştırıldığıyla ilgilidir.

İlke 9: Savunma katmanları farklı başarısızlık biçimlerine karşı anlam taşımalıdır.

Aynı varsayıma veya aynı yönetim yoluna dayanan çok sayıda güvenlik mekanizması, tek bir hata karşısında birlikte etkisiz hale gelebilir. Katmanlı tasarımın değeri, bir korumanın kaybından sonra diğer sınırların bağımsız biçimde anlam taşımaya devam edebilmesidir.

İlke 10: Güvenlik sağlayan bileşenlerin kendileri de güven sınırlarının içinde değerlendirilmelidir.

Kimlik hizmetleri, politika motorları, güvenlik cihazları ve benzeri bileşenler yalnızca koruma sağlayan dış unsurlar değildir; kendi saldırı yüzeyleri, yetkileri ve bağımlılıkları vardır. Sağladıkları güvence, kendilerinin güvenilirliğinden bağımsız düşünülemez.

İlke 11: Yoğunlaşmış yetki ve güven bilinçli bir mimari tercih olmalıdır.

Merkezi sistemler yönetimi kolaylaştırabilir; ancak tek noktadan çok geniş etki oluşturabilir. Bir bileşende toplanan güven arttıkça, o bileşenin kaybının oluşturabileceği etki de mimari kararın parçası olmalıdır.

İlke 12: Sırlar ve kriptografik anahtarlar gereksiz güven yolları oluşturmamalıdır.

Bir sırrın çok sayıda sisteme kopyalanması veya farklı güven alanlarında paylaşılması bu alanları görünmez biçimde birbirine bağlayabilir. Kriptografik koruma, uygun kimlik ve yetki sınırlarının yerine değil onların içinde çalışmalıdır.

İlke 13: Dış sistemler ve farklı ortamlar mimarinin dışında kabul edilmemelidir.

Bulut hizmetleri, üçüncü taraflar, federasyonlar, geliştirme ortamları ve diğer dış alanlarla kurulan ilişkiler kuruluşun güven modelini değiştirebilir. Bir ilişkinin kurum sınırının dışında gerçekleşmesi onun mimari etkisini ortadan kaldırmaz.

İlke 14: Olağan dışı ve acil erişim yolları da gerçek mimarinin parçasıdır.

Bakım yolları, kurtarma mekanizmaları, acil erişimler veya normal kontrolleri aşabilen başka yollar seyrek kullanılıyor olmaları nedeniyle güvenlik modelinin dışında tutulmamalıdır. Sistemin gerçekte aşılabildiği bir sınır, mimari olarak mutlak bir sınır değildir.

İlke 15: Hata durumundaki güvenlik davranışı tasarımın bilinçli bir sonucu olmalıdır.

Bir bağımlılık veya güvenlik mekanizması kullanılamaz hale geldiğinde sistemin daha geniş erişime geçmesi ya da korumaları sessizce kaldırması tesadüfi davranış olarak ortaya çıkmamalıdır. Kullanılabilirlik kaybı ile güven kaybı arasındaki tercih mimari düzeyde anlaşılabilir olmalıdır.

İlke 16: Mimari mümkün olduğu ölçüde anlaşılabilir ve gerekçelendirilebilir kalmalıdır.

Gereksiz katmanlar, bağlantılar ve istisnalar sistemin gerçek güven modelinin anlaşılmasını güçleştirir. Karmaşıklık ancak sağladığı işlev veya güvenlik değeri oluşturduğu yeni hata ve yanlış anlama alanını haklı çıkardığında kabul edilmelidir.

İlke 17: Mimari varsayımlar açık olmalı ve değişmez gerçekler gibi ele alınmamalıdır.

Bir tasarım belirli saldırgan yetenekleri, kullanım biçimleri, teknolojiler veya bağımlılıklar hakkında varsayımlara dayanabilir. Bu varsayımlar görünür olmalı ve sistem ya da çevresi değiştikçe geçerlilikleri yeniden sorgulanabilmelidir.

İlke 18: Mimari sapmalar gerçek güven modelini görünmez biçimde değiştirmemelidir.

Geçici bağlantılar, istisnalar ve yerel çözümler zamanla tasarlanmış mimariden daha önemli güven yolları oluşturabilir. Amaçlanan mimari ile fiilî mimari arasındaki fark gerektiğinde anlaşılabilir olmalıdır.

İlke 19: Güvenlik mimarisi doğrulanabilir iddialar ortaya koymalıdır.

“Bu alan diğerinden ayrıdır”, “bu sistem yalnızca şu yoldan yönetilebilir” veya “bu bileşenin kaybı buradan öteye yayılmaz” gibi mimari varsayımlar gerçek sistem davranışıyla sınanabilir nitelikte olmalıdır. Doğrulanamayan bir mimari iddia, güvence açısından yalnızca bir tasarım niyetidir.

İlke 20: Güvence, mimari belgelerden değil gerçek sistem davranışından doğmalıdır.

Diyagramlar, modeller ve tasarım kararları sistemi anlamayı sağlar; ancak sistemin gerçekten bu şekilde çalıştığını tek başına göstermez. Güvenlik mimarisinin güvencesi, amaçlanan güven sınırlarının, bağımlılıkların ve etki alanlarının çalışan ortamda da karşılığının bulunmasıyla oluşmalıdır.