Denetci.org

REFERANS İLKELERİ

Temel İlkeler

Rİ-GEN-1

Sürüm 1.0 · 11.08.2026

www.denetci.org

Temel İlkeler

Temel İlkeler, sistemlerin, hizmetlerin, süreçlerin ve güvenlik yapılarının hangi güven anlayışıyla tasarlanması gerektiğine ilişkin ortak zemini tanımlar. Belirli bir teknolojiye, ürüne veya kontrol setine bağlı değildir. Amaç hangi önlemlerin uygulanacağını tek tek belirlemek değil; güvenin nasıl kurulacağı, sınırlandırılacağı, korunacağı ve doğrulanacağı konusunda kalıcı bir tasarım anlayışı ortaya koymaktır.

İlke 1: Güven bir gerekçeye ve sınıra dayanmalıdır.

Bir kullanıcıya, sisteme, cihaza, hizmete veya başka bir tarafa duyulan güvenin neden gerekli olduğu ve nerede sona erdiği açıklanabilir olmalıdır. Geçmiş alışkanlık, organizasyonel yakınlık veya sistem içindeki konum tek başına sınırsız güven gerekçesi oluşturmamalıdır.

İlke 2: Güven kalıcı bir özellik olarak kabul edilmemelidir.

Güven; kimlik, rol, yapılandırma, sahiplik, ortam ve kullanım bağlamı gibi koşullara bağlıdır. Bu koşullar değiştiğinde daha önce verilmiş bir güven kararının geçerliliği de değişebilmelidir.

İlke 3: Belirsizlik güven lehine yorumlanmamalıdır.

Bir kimliğin, isteğin, işlemin veya sistem durumunun güvenilirliği yeterince anlaşılamıyorsa bu belirsizlik daha geniş erişim veya daha büyük etki üretmemelidir. Güven gerektiren sonuçlar, onları destekleyen yeterli gerekçe bulunduğu ölçüde mümkün olmalıdır.

İlke 4: Varsayılan durum gereksiz güven ve yetki üretmemelidir.

Yeni bir kullanıcı, sistem, bağlantı, özellik veya entegrasyon yalnızca var olduğu için başka kaynaklara erişim kazanmamalıdır. Güvenli durumun oluşması sürekli ek kısıtlama ve sonradan düzeltme gerektirmemelidir.

İlke 5: Yetki, ihtiyaç duyulan etkiyle sınırlı olmalıdır.

Bir tarafın yapabilecekleri, yerine getirdiği işlev için gereken kaynak, işlem ve etki alanını aşmamalıdır. Olası bir hata veya kötüye kullanımın sonucu, gereksiz geniş yetkiler nedeniyle büyümemelidir.

İlke 6: Tek bir güven kaybının etkisi mümkün olduğu ölçüde sınırlanmalıdır.

Bir hesabın, cihazın, uygulamanın, hizmetin veya başka bir bileşenin kaybedilmesi bütün sistemin güveninin kaybedilmesi anlamına gelmemelidir. Tasarım, bir başarısızlığın ne kadar ileri yayılabileceğini bilinçli olarak sınırlandırmalıdır.

İlke 7: Kritik güvence tek bir bileşenin kusursuz kalmasına bağlı olmamalıdır.

İnsanlar, yazılımlar, güvenlik ürünleri, altyapılar ve hizmet sağlayıcılar hata yapabilir veya ele geçirilebilir. Kritik bir güvenlik özelliği, tek bir unsur başarısız olduğunda bütünüyle ortadan kalkacak şekilde kurulmamış olmalıdır.

İlke 8: Savunma katmanları aynı başarısızlığa bağımlı olmamalıdır.

Birden fazla mekanizmanın bulunması tek başına savunma derinliği oluşturmaz. Katmanlar, aynı kimliğin, aynı yönetim yolunun veya aynı varsayımın kaybıyla birlikte etkisiz hale geliyorsa sağladıkları ek güvence sınırlıdır.

İlke 9: Karmaşıklık güvenceyi etkileyen bir tasarım maliyetidir.

Her ek bileşen, istisna, entegrasyon ve özel durum sistemin anlaşılmasını ve doğru işletilmesini zorlaştırabilir. Ek karmaşıklık, sağladığı fayda bu yeni hata ve yanlış anlama alanını haklı çıkardığı ölçüde kabul edilmelidir.

İlke 10: Güvenlik, tasarımın gizli kalmasına bağımlı olmamalıdır.

Bir mekanizmanın nasıl çalıştığının öğrenilmesi, tek başına onun koruduğu sınırları geçersiz hale getirmemelidir. Güvence, bilinmezliğe değil dayanıklı ve doğrulanabilir güvenlik özelliklerine dayanmalıdır.

İlke 11: Saldırı ve etkileşim yüzeyi gerçek ihtiyaçla sınırlı tutulmalıdır.

Her servis, hesap, özellik, protokol ve entegrasyon sisteme yeni bir etkileşim yolu ekler. Kullanılmayan veya artık anlamlı bir ihtiyaca hizmet etmeyen yüzeyler güvenlik açısından nötr kabul edilmemelidir.

İlke 12: Kimlik, yetki ve işlem birbirinden ayrılmalı ancak ilişkilendirilebilir kalmalıdır.

Bir tarafın kim olduğunun bilinmesi, yapacağı işlemin uygun olduğu anlamına gelmez. Önemli işlemlerde kimliğin, verilen yetkinin ve ortaya çıkan eylemin ilişkisi gerektiğinde anlaşılabilir olmalıdır.

İlke 13: İnsan hatası beklenmeyen bir istisna olarak görülmemelidir.

Güvenilir tasarım, insanların zaman zaman yanlış seçim yapacağını, bir uyarıyı gözden kaçıracağını veya bir süreci hatalı uygulayacağını kabul etmelidir. Makul bir insan hatasının ölçüsüz bir güvenlik sonucuna dönüşmesi mümkün olduğu ölçüde engellenmelidir.

İlke 14: Güvenli yol, gerçek kullanım içinde uygulanabilir olmalıdır.

Bir güvenlik mekanizması işi sürekli olarak gereksiz biçimde zorlaştırıyorsa kullanıcıları ve işletmecileri onu aşan yollar oluşturmaya teşvik edebilir. Güvenlik, yalnızca teorik olarak doğru değil, amaçlanan çalışma biçimi içinde sürdürülebilir de olmalıdır.

İlke 15: Veri üzerindeki güven, verinin bütün yaşamı boyunca korunmalıdır.

Veri gereğinden fazla toplanmamalı, açığa çıkarılmamalı veya kullanım amacı ortadan kalktıktan sonra sınırsız biçimde varlığını sürdürmemelidir. Verinin güvenliği; oluşturulması, kullanılması, aktarılması, saklanması ve yaşamının sona ermesiyle birlikte düşünülmelidir.

İlke 16: Yoğunlaşmış güven unsurları taşıdıkları etkiye göre korunmalıdır.

Sırlar, kriptografik anahtarlar, ayrıcalıklı kimlikler ve benzeri unsurlar çok sayıda güvenlik sınırını tek noktadan etkileyebilir. Bunların değeri yalnızca kendi içeriklerinden değil, ele geçirilmeleri halinde açabilecekleri güven yollarından kaynaklanır.

İlke 17: Güvenlik, başarısızlığın hiç yaşanmayacağı varsayımına dayanmamalıdır.

Bazı önlemler bozulabilir, bazı saldırılar başarılı olabilir ve bazı hizmetler kullanılamaz hale gelebilir. Tasarım, böyle bir durumda etkinin sınırlandırılmasını ve güvenilir bir duruma yeniden ulaşılabilmesini de güvenliğin parçası olarak görmelidir.

İlke 18: Değişiklik, güven durumunu değiştirebilen temel bir olaydır.

Bir sistem aynı adla çalışmaya devam etse bile yazılımı, yapılandırması, bağımlılıkları, verisi veya kullanım biçimi değiştiğinde güvenlik varsayımları da değişebilir. Daha önce geçerli olan güvence, önemli değişikliklerden bağımsız ve süresiz kabul edilmemelidir.

İlke 19: Dış bağımlılıklar güven sınırının dışında kabul edilmemelidir.

Bir işlevin üçüncü tarafa, bulut hizmetine, tedarikçiye veya başka bir dış sisteme bırakılması kuruluş üzerindeki etkisini ortadan kaldırmaz. Kuruluşun güvencesi, kendi sonuçlarını etkileyen bağımlılıkların güvenilirliğini de hesaba katmalıdır.

İlke 20: Güvence, amaçlanan tasarım ile gerçek davranışın uyumuna dayanmalıdır.

Bir kontrolün tanımlanmış, bir ürünün kurulmuş veya bir testin geçmiş olması tek başına güvence oluşturmaz. Güven iddiaları, sistemin gerçekte nasıl davrandığını gösteren ve sınırları bilinen kanıtlarla desteklenebilmelidir.