Denetci.org

REFERANS İLKELERİ

Varlık Yönetimi İlkeleri

Rİ-YON-5

Sürüm 1.0 · 11.08.2026

www.denetci.org

Varlık Yönetimi İlkeleri

Varlık yönetimi, kuruluşun güvenlik sonuçlarını etkileyebilecek unsurları ve bunlar arasındaki ilişkileri anlayabilmesini sağlayan temel bir güvence alanıdır. Amaç eksiksiz görünmek için mümkün olan en uzun envanteri oluşturmak değil; güvenlik kararlarının gerçekten var olan sistemler, bilgiler, kimlikler, hizmetler ve bağımlılıklar hakkında yeterli bilgiye dayanmasını sağlamaktır.

İlke 1: Varlık kavramı biçime değil güvenlik etkisine dayanmalıdır.

Donanım, yazılım, veri, kimlik, API, bulut kaynağı veya dış hizmet farklı biçimlerde olsa da kuruluşun güvenliği üzerinde anlamlı etki oluşturabilir. Bir unsurun varlık sayılması satın alınmış, fiziksel veya kalıcı olmasına bağlı olmamalıdır.

İlke 2: Varlık görünümü kuruluşun kayıtlarını değil gerçek ortamını temsil etmelidir.

Satın alma listesi, envanter aracı veya başka bir kayıt sistemi yararlı olabilir; ancak gerçekte kullanılmayan kaynakları içerebilir veya çalışan bazı kaynakları göremeyebilir. Varlık bilgisinin değeri, kuruluşun gerçek çalışma ortamıyla ne kadar uyumlu olduğuyla ölçülmelidir.

İlke 3: Her önemli varlığın amacı ve sorumluluğu anlaşılabilir olmalıdır.

Bir varlığın neden var olduğu, hangi işlevi desteklediği ve onunla ilgili anlamlı kararları kimin verebildiği belirsiz kalmamalıdır. Sahiplik, yalnızca bir ismin kayda yazılması değil gerçek karar ve sorumluluk ilişkisini ifade etmelidir.

İlke 4: Bir varlığın önemi yalnızca kendi doğrudan işlevinden kaynaklanmayabilir.

Basit görünen bir kimlik hizmeti, API, DNS bileşeni veya otomasyon hesabı çok sayıda kritik işlevin bağımlılığı olabilir. Kritiklik, varlığın kendisi kadar kaybının başka hangi sonuçları tetikleyebileceği üzerinden anlaşılmalıdır.

İlke 5: Varlıklar kadar aralarındaki bağımlılıklar da görünür olmalıdır.

Tekil sistemlerin bilinmesi, bir hizmetin nasıl oluştuğunu veya bir başarısızlığın nerelere yayılacağını açıklamak için yeterli olmayabilir. Önemli veri, kimlik, altyapı, hizmet ve üçüncü taraf ilişkileri varlık anlayışının bir parçası olmalıdır.

İlke 6: Geçici ve dinamik kaynaklar güvenlik açısından geçici gerçeklikler olarak görülmemelidir.

Kısa süreli bulut kaynakları, konteynerler, test sistemleri veya otomasyonla oluşturulan bileşenler yaşamları boyunca gerçek veri ve yetki taşıyabilir. Kısa ömürlü olmak, bir kaynağın güvenlik etkisini ortadan kaldırmaz.

İlke 7: Veri ve kimlikler taşıdıkları etki nedeniyle bağımsız varlıklar olarak ele alınabilmelidir.

Bir veri kümesinin değeri yalnızca saklandığı sistemden, bir teknik kimliğin değeri de yalnızca onu kullanan uygulamadan türemez. Gerektiğinde bunların kendi sahipliği, kullanımı, hassasiyeti ve bağımlılıkları ayrı biçimde anlaşılabilmelidir.

İlke 8: Yazılım ve hizmet bileşenleri saldırı yüzeyinin gerçek parçaları olarak görülmelidir.

Uygulamalar, kütüphaneler, API'ler ve dış hizmetler fiziksel bir cihaz olmadan da güvenlik açığı, bağımlılık ve erişim ilişkisi oluşturabilir. Varlık yönetimi yalnızca üzerinde çalıştıkları donanımla sınırlı kalmamalıdır.

İlke 9: Varlığın kimliği, değişebilen teknik göstergelerle karıştırılmamalıdır.

IP adresi, ana bilgisayar adı, etiket veya başka bir teknik özellik zaman içinde değişebilir ya da yeniden kullanılabilir. Varlık bilgisi, gerçek kaynağın sürekliliğini ve bağlamını ayırt edebilecek bir anlayışa dayanmalıdır.

İlke 10: Belirsizlik düşük risk olarak yorumlanmamalıdır.

Sahibi, amacı, veri kullanımı veya kritikliği bilinmeyen bir varlığın önemsiz olduğu sonucuna varılamaz. Bilinmeyen varlık ve eksik bağlam, güvenlik kararını zorlaştıran ayrı bir maruziyet biçimidir.

İlke 11: Varlıkların güven ilişkileri yaşam döngüsüyle birlikte değişmelidir.

Bir varlığın oluşturulması, görev değiştirmesi, başka sisteme taşınması, yeniden kullanılması veya kullanım dışına çıkarılması onun erişimlerini, verilerini ve bağımlılıklarını da etkileyebilir. Varlık ortadan kalkarken ona ait güven ilişkileri görünmez biçimde yaşamaya devam etmemelidir.

İlke 12: Dış hizmetler ve kayıt dışı kullanımlar gerçek varlık görünümünün dışında kalmamalıdır.

Kuruluş tarafından doğrudan sahip olunmayan SaaS hizmetleri, üçüncü taraf API'leri veya kullanıcıların kendi ihtiyaçları için oluşturduğu hizmetler gerçek veri ve erişim ilişkileri doğurabilir. Resmî süreçlerin dışında bulunmak güvenlik etkisini ortadan kaldırmaz.

İlke 13: Varlık bilgisi tek bir kaynağın kusursuz olduğu varsayımına dayanmamalıdır.

Farklı araç ve kayıtlar ortamın farklı bölümlerini görebilir ve birbirleriyle çelişebilir. Bu farklılıklar yalnızca veri kalitesi sorunu olarak değil, görünmeyen veya yanlış anlaşılan varlıkların işareti olarak da değerlendirilebilmelidir.

İlke 14: Varlık bilgisi kayıt tutmak için değil güvenlik kararlarını desteklemek için var olmalıdır.

Kritiklik, sahiplik, maruziyet ve bağımlılık bilgisi erişim, zafiyet, olay müdahalesi ve süreklilik gibi kararların daha doğru verilmesini sağlamalıdır. Hiçbir kararı etkilemeyen ayrıntının güvenlik değeri sınırlıdır.

İlke 15: Varlık bilgisinin kendisi de korunması gereken bir güvenlik varlığıdır.

Sistemlerin konumları, sahipleri, bağlantıları ve önemleri kuruluşun yapısı hakkında değerli bilgi ortaya çıkarabilir. Görünürlük sağlama ihtiyacı, bu bilgilerin gereksiz biçimde açığa çıkarılmasını gerektirmez.

İlke 16: Varlık yönetiminin güvencesi gerçek ortamla olan uyumundan doğmalıdır.

Bir envanter tablosunun, CMDB'nin, etiket standardının veya keşif aracının bulunması tek başına varlıkların bilindiğini göstermez. Güvence; çalışan kaynakların gerçekten tanınabilmesi, önemli sahiplik ve bağımlılıkların anlaşılabilmesi ve varlık bilgisinin kuruluşun gerçek güvenlik kararlarını doğru biçimde desteklemesi üzerinden değerlendirilmelidir.