Denetci.org

REFERANS İLKELERİ

Güvenlik Açığı Yönetimi İlkeleri

Rİ-ISL-2

Sürüm 1.0 · 11.08.2026

www.denetci.org

Güvenlik Açığı Yönetimi İlkeleri

Güvenlik açığı yönetimi, sistemlerde ve bağımlılıklarda bulunan zayıflıkların kuruluşun gerçek güvenliği üzerindeki etkisinin anlaşılmasını ve azaltılmasını ele alır. Amaç mümkün olan en fazla bulguyu üretmek veya bütün açıkları aynı biçimde kapatmak değil; hangi zayıflıkların gerçek saldırı yolları oluşturduğunu, bunların hangi güven sınırlarını etkilediğini ve alınan kararların riski gerçekten azaltıp azaltmadığını anlayabilmektir.

İlke 1: Güvenlik açığı ile risk aynı şey olarak görülmemelidir.

Aynı teknik zayıflık farklı sistemlerde çok farklı sonuçlar doğurabilir. Bir açığın önemi yalnızca teknik özelliğinden değil; erişilebilirliğinden, etkileyebileceği varlıklardan, mevcut güven sınırlarından ve saldırganın onunla oluşturabileceği gerçek sonuçtan doğmalıdır.

İlke 2: Güvenlik açığı yönetimi bulgu sayısını değil gerçek maruziyeti azaltmayı hedeflemelidir.

Çok sayıda bulgunun bulunması veya kapatılması sistemin daha güvenli hale geldiğini tek başına göstermez. Çalışma, kuruluşun önemli saldırı yollarını ve güven kaybı ihtimalini ne ölçüde azalttığı üzerinden anlam taşımalıdır.

İlke 3: Öncelik tek bir teknik puana indirgenmemelidir.

Standart puanlar ortak karşılaştırma sağlayabilir; ancak sistemin kuruluş içindeki rolünü, gerçek erişilebilirliğini veya diğer zayıflıklarla birleştiğinde oluşacak etkiyi bütünüyle temsil etmeyebilir. Öncelik teknik bilgi ile sistem bağlamını birlikte yansıtmalıdır.

İlke 4: İstismar edilebilirlik gerçek çalışma koşullarında değerlendirilmelidir.

Bir açığın teorik olarak istismar edilebilir olması kuruluş ortamında aynı saldırı yolunun mevcut olduğunu göstermeyebilir. Bunun tersi de geçerlidir: düşük önem verilen bir zayıflık gerçek mimari içinde saldırgana kritik bir geçiş sağlayabilir.

İlke 5: Güncel saldırı bilgisi mevcut öncelikleri değiştirebilmelidir.

Bir zayıflığın aktif olarak kullanıldığına veya yeni bir istismar yolunun ortaya çıktığına ilişkin güvenilir bilgi, geçmişte yapılmış değerlendirmeyi geçersiz kılabilir. Önceliklendirme bir kez verilip değişmez hale gelen bir karar olmamalıdır.

İlke 6: Varlığın güvenlik açısından önemi açığın değerlendirilmesine yansımalıdır.

Aynı zayıflık sıradan bir sistemde ve kritik kimlik ya da yönetim altyapısında aynı sonucu doğurmaz. Güvenlik açığı, bulunduğu bileşenin gerçek yetkileri ve bağımlılıklarıyla birlikte anlaşılmalıdır.

İlke 7: Maruziyet değiştiğinde aynı açığın riski de değişebilmelidir.

Daha önce yalnızca sınırlı bir alandan erişilebilen sistem yeni bağlantı, entegrasyon veya yapılandırma nedeniyle farklı saldırganlara açılabilir. Zafiyet değerlendirmesi sistemin geçmiş durumuna süresiz biçimde bağlı kalmamalıdır.

İlke 8: Birden fazla zayıflığın birleşik etkisi tek tek değerlendirmelerin toplamından farklı olabilir.

Ayrı ayrı sınırlı görünen zayıflıklar bir saldırı zinciri içinde kimlik doğrulama, yetki veya güven sınırlarını aşan daha ciddi bir sonuç oluşturabilir. Değerlendirme yalnızca bağımsız bulgu listesine indirgenmemelidir.

İlke 9: Tekrarlanan zayıflıklar yalnızca tekrarlanan tekil hatalar olarak görülmemelidir.

Aynı tür sorun farklı sistemlerde veya sürümlerde sürekli ortaya çıkıyorsa bunun altında ortak mimari, geliştirme, yapılandırma veya işletim nedeni bulunabilir. Yönetim, her örneği ayrı ayrı kapatmakla yetinmeyip zayıflığı üreten koşulu da anlayabilmelidir.

İlke 10: Görünürlük tek bir tespit yöntemine bağlı olmamalıdır.

Tarama araçları, üretici bildirimleri, güvenlik testleri, araştırmacılar ve gerçek olaylar farklı zayıflıkları ortaya çıkarabilir. Bir yöntemin hiçbir bulgu üretmemesi sistemde anlamlı zayıflık bulunmadığının kanıtı olmamalıdır.

İlke 11: Tespit kapsamı kuruluşun gerçek saldırı yüzeyini temsil etmelidir.

İncelenmeyen, taranamayan veya teknik olarak zor sistemler güvenlik açığı yönetiminin dışında kalmış sayılmamalıdır. Hakkında bilgi üretilemeyen alanlar düşük riskli değil, daha yüksek belirsizlik taşıyan alanlardır.

İlke 12: Bir bulgunun kaynağı doğruluğunun tek kanıtı olmamalıdır.

Otomatik araç, üretici, araştırmacı veya başka güvenilir kaynaklar hatalı ya da eksik değerlendirme yapabilir. Önemli kararlar, bulgunun gerçek sistemde ne ifade ettiğinin anlaşılmasına dayanmalıdır.

İlke 13: Yanlış sonuç ihtimali iki yönde de kabul edilmelidir.

Bir tespit gerçekte bulunmayan bir sorunu gösterebilir; aynı zamanda hiçbir bulgu görülmeyen bir sistemde zayıflık bulunabilir. Güvence yalnızca araç çıktısının doğruluğuna duyulan varsayıma dayanmamalıdır.

İlke 14: Giderme belirli bir teknik yönteme eşitlenmemelidir.

Yama uygulamak, yapılandırmayı değiştirmek, özelliği kaldırmak, mimari sınırı güçlendirmek veya başka bir yöntem aynı zayıflık için farklı koşullarda anlamlı olabilir. Esas olan kullanılan yöntemin gerçek saldırı yolunu veya etkisini anlamlı biçimde azaltmasıdır.

İlke 15: Giderme yeni ve daha büyük bir güvenlik sorunu oluşturmamalıdır.

Bir güvenlik açığını kapatmak için yapılan değişiklik yeni uyumsuzluk, yetki, karmaşıklık veya kullanılabilirlik kaybı oluşturabilir. Çözümün değeri yalnızca eski bulgunun artık görünmemesi üzerinden anlaşılmamalıdır.

İlke 16: Doğrudan giderilemeyen zayıflık görünmez biçimde kabul edilmiş sayılmamalıdır.

Teknik, iş veya başka nedenlerle bazı zayıflıklar hemen ortadan kaldırılamayabilir. Bu durum, maruziyetin ortadan kalktığı anlamına gelmez; kalan risk ve onu sınırlandıran koşullar görünür kalmalıdır.

İlke 17: Telafi edici koruma zayıflığın adını değil gerçek istismar yolunu etkilemelidir.

Bir ek kontrol yalnızca kayıt üzerinde "önlem var" sonucunu üretmemelidir. Saldırganın zayıflığa ulaşmasını, kullanmasını veya etkisini gerçekten sınırlandırdığı ölçüde güvenlik değeri taşır.

İlke 18: Risk kabulü güvenlik açığını ortadan kaldırılmış hale getirmemelidir.

Bir zayıflığın belirli koşullarda kabul edilmesi teknik gerçeği değiştirmez. Kabulü mümkün kılan koşullar değiştiğinde aynı kararın geçerliliği de yeniden değerlendirilmelidir.

İlke 19: Geçici istisnalar kalıcı ve görünmez güvenlik borcuna dönüşmemelidir.

Bir zayıflığın belirli süre veya koşullarda ertelenmesi gerekli olabilir. Ancak geçmişte verilen istisna, açığın süresiz biçimde önemini kaybetmesinin gerekçesi olmamalıdır.

İlke 20: Giderildiği düşünülen zayıflığın gerçek saldırı yolu sona ermiş olmalıdır.

Bir paketin güncellenmesi veya bir bulgunun sistemde görünmemesi tek başına yeterli değildir. Aynı zayıflık başka bileşende, yapılandırmada veya alternatif erişim yolunda etkisini sürdürüyorsa risk fiilen giderilmemiş olabilir.

İlke 21: Bağımlılıklardaki zayıflıklar uygulamanın dışında kabul edilmemelidir.

Kütüphaneler, işletim bileşenleri, cihaz yazılımları ve dış hizmetler kuruluş kodu tarafından geliştirilmemiş olsa da gerçek sistemin parçasıdır. Bir zayıflığın başka tarafın ürününde bulunması onun oluşturabileceği etkiyi kuruluşun güven modelinden çıkarmaz.

İlke 22: Destek dışı sistemler sıradan bir güvenlik açığı istisnasına dönüşmemelidir.

Artık güvenlik düzeltmesi üretilemeyen bir teknoloji, bilinen zayıflıkların yanında gelecekte ortaya çıkacak zayıflıklara da farklı biçimde maruz kalır. Böyle sistemler güncel sistemlerle aynı güven varsayımları altında görünmez biçimde yaşamamalıdır.

İlke 23: Güvenlik açığı bilgisi kendisi de korunması gereken bir güvenlik varlığıdır.

Ayrıntılı bulgular sistemlerin zayıf noktalarını, mimarisini ve saldırı yollarını gösterebilir. Giderme için gerekli paylaşım sağlanırken bu bilginin gereksiz biçimde yeni saldırı kolaylığı oluşturması engellenmelidir.

İlke 24: Güvenlik açığı yönetiminin güvencesi gerçek risk azalması üzerinden doğrulanabilmelidir.

Tarama sıklığı, kapatılan bulgu sayısı veya hedef sürelere uyum tek başına güvence oluşturmaz. Önemli zayıflıkların gerçek ortamda tanınabildiği, doğru bağlamda önceliklendirildiği ve alınan önlemlerin saldırı yolunu veya etkisini gerçekten azalttığı gösterilebilmelidir.