Denetci.org

REFERANS İLKELERİ

Loglama İlkeleri

Rİ-ISL-3

Sürüm 1.0 · 11.08.2026

www.denetci.org

Loglama İlkeleri

Loglama, sistemlerde gerçekleşen güvenlik açısından anlamlı davranışların sonradan anlaşılabilmesini sağlayan kanıt üretme yeteneğidir. Amaç mümkün olan en fazla veriyi toplamak veya her işlemi kaydetmek değil; önemli olayların ne olduğunu, hangi bağlamda gerçekleştiğini ve ne sonuç doğurduğunu güvenilir biçimde açıklayabilecek yeterli kayıt oluşturmaktır.

İlke 1: Loglama hangi güvenlik sorularının cevaplanması gerektiğinden başlamalıdır.

Kayıt üretmek kendi başına güvenlik hedefi değildir. Hangi olayların sonradan açıklanması, ilişkilendirilmesi veya incelenmesi gerektiği loglama tasarımına yön vermelidir.

İlke 2: Her olayın kaydedilmesi gerektiği varsayılmamalıdır.

Aşırı kayıt gereksiz veri maruziyeti ve gürültü oluşturabilir; yetersiz kayıt ise önemli olayları görünmez bırakabilir. Loglama, miktarı değil anlamlı açıklanabilirliği hedeflemelidir.

İlke 3: Güvenlik açısından önemli durum ve güven değişiklikleri görünmez kalmamalıdır.

Kimlik, yetki, güvenlik yapılandırması veya başka kritik durumlarda meydana gelen değişiklikler sistemin güven modelini etkileyebilir. Bu olayların gerektiğinde sonradan anlaşılabilir olması önem taşır.

İlke 4: Başarılı ve başarısız davranışlar güvenlik açısından ayrı anlam taşıyabilir.

Yalnızca hataları veya reddedilen işlemleri kaydetmek, ele geçirilmiş geçerli bir kimliğin başarılı faaliyetlerini görünmez bırakabilir. Hangi başarılı işlemlerin güvenlik açısından anlamlı olduğu da sistem bağlamında değerlendirilmelidir.

İlke 5: Bir kayıt olayın ne olduğunu ve sonucunu anlaşılabilir kılmalıdır.

Bir isteğin geldiğini bilmek her zaman yeterli değildir; önemli durumlarda neyin yapılmaya çalışıldığı ve hangi sonucun oluştuğu da gerekli olabilir. Log, teknik bir mesaj üretmekten çok olay hakkında kullanılabilir kanıt sağlamalıdır.

İlke 6: Olay gerektiğinde anlamlı bir kaynağa ilişkilendirilebilmelidir.

Kullanıcı, hizmet, cihaz, süreç veya başka bir tarafın gerçekleştirdiği önemli bir faaliyet tamamen anonim teknik kayıtlar arasında kaybolmamalıdır. Kimlik ilişkisinin gerekli olmadığı olaylarda ise gereksiz kişisel veri oluşturulmamalıdır.

İlke 7: Kimlik geçişleri kayıtların anlamını bozmamalıdır.

Bir kişi başka bir hesapla, yükseltilmiş yetkiyle veya aracılı bir sistem üzerinden işlem yaptığında yalnızca son teknik hesabın görünmesi gerçek sorumluluğu saklayabilir. Önemli güven geçişleri gerektiğinde olay zinciri içinde anlaşılabilmelidir.

İlke 8: Otomasyon da açıklanabilir bir kaynak olarak ele alınmalıdır.

Bir işlemin insan tarafından yapılmamış olması onun kaynağının önemsiz olduğu anlamına gelmez. Otomatik faaliyetler hangi sistem, işlev veya güven ilişkisi adına gerçekleştikleriyle ilişkilendirilebilmelidir.

İlke 9: Zaman bilgisi olay kanıtının temel bir parçasıdır.

Bir olayın başka olaylarla ilişkisini kurabilmek için ne zaman gerçekleştiğinin anlamlı biçimde bilinmesi gerekir. Belirsiz veya birbirleriyle karşılaştırılamayan zaman bilgileri olay zincirinin yanlış yorumlanmasına yol açabilir.

İlke 10: Farklı sistemlerdeki olaylar gerektiğinde ilişkilendirilebilir olmalıdır.

Dağıtık bir işlem tek bir sistemde başlamayıp farklı uygulama ve hizmetlerden geçebilir. Yeterli bağlam bulunduğunda aynı olay veya işlem zincirinin parçalarının birbirine bağlanabilmesi mümkün olmalıdır.

İlke 11: Kullanıcıya gösterilen bilgi ile güvenlik kanıtında gereken bilgi aynı olmak zorunda değildir.

Dışarıya verilen hata bilgisi saldırgan için gereksiz ayrıntı oluşturmamalı; iç kayıt ise olayın araştırılmasını imkânsız kılacak kadar yetersiz olmamalıdır. İki ihtiyacın farklı güven sınırları olduğu kabul edilmelidir.

İlke 12: Loglama yeni bir sır ve hassas veri deposu oluşturmamalıdır.

Parolalar, erişim belirteçleri, özel anahtarlar ve benzeri güven unsurları loglarda yer aldığında log erişimi doğrudan sistem erişimine dönüşebilir. Kayıt amacı bu değerlerin gereksiz kopyalarını oluşturmayı haklı çıkarmamalıdır.

İlke 13: Hassas veri yalnızca olayın açıklanması için gerekli olduğu ölçüde kaydedilmelidir.

Loglama amacıyla toplanan veri de açığa çıkabilir, kötüye kullanılabilir veya gereğinden uzun süre saklanabilir. Kanıt değeri ile oluşturulan yeni veri maruziyeti birlikte değerlendirilmelidir.

İlke 14: Log verisinin kendisi korunan bir güvenlik varlığıdır.

Kayıtlar kullanıcı davranışı, sistem yapısı, güvenlik olayları ve başka hassas bilgiler içerebilir. Görünürlük sağlama ihtiyacı logların gereksiz taraflara açık olmasını gerektirmez.

İlke 15: Olayı gerçekleştirebilen taraf kendi faaliyetinin kanıtını sınırsız biçimde değiştirememelidir.

Özellikle yüksek yetkili kullanıcı veya ele geçirilmiş sistem, yaptığı işlemleri aynı yetkiyle kolayca silebiliyor veya değiştirebiliyorsa kayıtların kanıt değeri azalır. Log bütünlüğü yalnızca normal kullanıcıların kayıtlarla ilgilenmeyeceği varsayımına dayanmamalıdır.

İlke 16: Merkezi loglama kaynak sistemden bağımsızlık sağlarken yeni bir ortak kayıp alanı oluşturmamalıdır.

Kayıtların kaynak sistem dışında tutulması sistemin ele geçirilmesi veya kaybı karşısında kanıtı koruyabilir. Buna karşılık merkezi yapı çok sayıda hassas kaydı tek bir yerde topladığı için kendisi yüksek etkili bir güven unsuruna dönüşür.

İlke 17: Log üretimi veya aktarımındaki kayıp olay yokluğu gibi görünmemelidir.

Kayıt gelmemesi sistemde hiçbir olay yaşanmadığı anlamına gelmeyebilir. Log üretiminin, iletiminin veya alınmasının durması gerektiğinde kendi başına anlaşılabilir bir durum olmalıdır.

İlke 18: Logların yaşam süresi gerçek kanıt ihtiyacıyla uyumlu olmalıdır.

Çok kısa saklama olayların araştırılmasını imkânsız hale getirebilir; gereksiz uzun saklama ise maliyet ve veri maruziyetini artırır. Farklı kayıtların değeri ve ihtiyaç süresi aynı olmak zorunda değildir.

İlke 19: Saklanan kayıtlar zaman içinde anlamlarını kaybetmemelidir.

Bir kayıt yıllar sonra hâlâ mevcut olsa bile formatı, alanlarının anlamı veya ilişkilendirme bilgisi artık anlaşılamıyorsa kanıt değeri sınırlıdır. Log yaşam döngüsü yalnızca dosyanın korunmasını değil gerektiğinde yorumlanabilmesini de kapsamalıdır.

İlke 20: Loglama hacmi önemli olayların bulunabilirliğini ortadan kaldırmamalıdır.

Daha fazla kayıt her zaman daha fazla görünürlük sağlamaz. Kritik davranışlar gereksiz ayrıntı içinde kayboluyorsa loglama güvenlik açısından amaçlanan değeri üretmeyebilir.

İlke 21: Geçici ayrıntılı loglama kalıcı yeni güvenlik maruziyetine dönüşmemelidir.

Sorun giderme sırasında normalden daha ayrıntılı kayıt gerekebilir. Bu durum hassas verinin veya yüksek hacimli kayıtların ihtiyaç sona erdikten sonra da süresiz biçimde üretilmesini doğal hale getirmemelidir.

İlke 22: Loglama sistem değiştikçe güvenlik anlamını koruyabilmelidir.

Yeni işlevler, kimlik modelleri, entegrasyonlar ve mimari değişiklikler farklı olayları önemli hale getirebilir. Bir zamanlar yeterli olan kayıt tasarımı sistem değişmesine rağmen otomatik olarak yeterli sayılmamalıdır.

İlke 23: Loglama güvencesi gerçek olayların açıklanabilirliği üzerinden doğrulanabilmelidir.

Log ürününün kurulmuş olması, belirli kayıt türlerinin etkin görünmesi veya çok miktarda veri saklanması tek başına güvence oluşturmaz. Gerçek bir önemli olayın ne olduğu, kim veya hangi sistemle ilişkili olduğu, ne zaman gerçekleştiği ve ne sonuç oluşturduğu yeterli güvenle yeniden açıklanabiliyorsa loglama amacına hizmet ediyor demektir.