Denetci.org

REFERANS İLKELERİ

Dijital Kanıt ve Adli Hazırlık İlkeleri

Rİ-OLY-2

Sürüm 1.0 · 11.08.2026

www.denetci.org

Dijital Kanıt ve Adli Hazırlık İlkeleri

Dijital kanıt ve adli hazırlık, bir güvenlik olayı veya başka önemli teknik durum sonrasında sistemlerde gerçekte ne yaşandığının yeterli güvenle yeniden anlaşılabilmesini ele alır. Amaç mümkün olan her veriyi süresiz saklamak veya her sistemi adli inceleme aracına dönüştürmek değil; gerekli olduğunda olayların kaynağını, sırasını, etkisini ve bağlamını açıklayabilecek güvenilir kanıtın var olmasını sağlamaktır.

İlke 1: Adli hazırlık olay meydana geldikten sonra başlayan bir faaliyet olmamalıdır.

Olay sonrasında gerekli kanıtın geçmişe dönük olarak üretilmesi mümkün olmayabilir. Önemli sistemler, makul olayların sonradan açıklanabilmesine imkân verecek ölçüde baştan kanıt üretmeye ve korumaya elverişli olmalıdır.

İlke 2: Kanıt sistemin gerçek güvenlik davranışını açıklayabilmelidir.

Sistemin çalıştığını gösteren teknik kayıtlar, güvenlik açısından ne yaşandığını her zaman açıklamaz. Kimlik, yetki, erişim, yapılandırma ve benzeri önemli davranışların gerektiğinde olay bağlamında yeniden anlaşılabilmesi gerekir.

İlke 3: Kanıtın değeri yalnızca mevcut olmasına değil güvenilirliğine dayanmalıdır.

Bir kaydın bulunması onun doğru, eksiksiz veya değiştirilmemiş olduğunu göstermez. Kanıtın nasıl üretildiği, hangi bileşenlere dayandığı ve kimler tarafından değiştirilebildiği taşıdığı güveni belirler.

İlke 4: Olayı gerçekleştirebilen taraf kanıt üzerinde sınırsız kontrole sahip olmamalıdır.

Bir taraf yüksek etkili işlem yapabiliyorsa aynı yetkinin kendi faaliyetinin bütün izlerini kolayca yok edebilmesi kanıt değerini zayıflatır. Önemli kanıtların güveni yalnızca incelenen tarafın iyi niyetine bağlı olmamalıdır.

İlke 5: Kanıt ile olayın gerçekleştiği sistem aynı başarısızlığa bütünüyle bağımlı olmamalıdır.

Ele geçirilen veya yok edilen bir sistem üzerinde bulunan kayıtlar da kaybolabilir ya da güvenilirliğini yitirebilir. Önemli kanıtların gerektiğinde olay kaynağından belirli ölçüde bağımsız korunabilmesi olayın açıklanabilirliğini güçlendirir.

İlke 6: Zaman kanıtın bağlamının ayrılmaz bir parçasıdır.

Bir olayın hangi işlemden önce veya sonra gerçekleştiğini bilmeden doğru kayıtlar dahi yanlış yorumlanabilir. Farklı sistemlerin zaman bilgileri olay zincirini anlamlı biçimde kurmaya yeterli olmalıdır.

İlke 7: Kanıt, bağlamından ayrıldığında anlamsız bir teknik değere dönüşmemelidir.

Bir kullanıcı adı, IP adresi, nesne kimliği veya olay kodu tek başına gerçek davranışı açıklamayabilir. Kanıtın hangi sistem, kimlik, işlem ve güven bağlamında oluştuğu gerektiğinde anlaşılabilmelidir.

İlke 8: Kimlik ve yetki geçişleri olay zincirinde korunmalıdır.

Bir taraf başka bir rol kullanabilir, yetki yükseltebilir, ortak hesap üzerinden işlem yapabilir veya otomasyon aracılığıyla faaliyet gösterebilir. Adli görünürlük yalnızca ilk oturum açan kimliği göstermekle yetinmemelidir.

İlke 9: Otomatik faaliyet sorumluluktan bağımsız kabul edilmemelidir.

Betikler, hizmet hesapları ve otomasyon sistemleri önemli değişiklikler gerçekleştirebilir. Bir otomatik işlemin hangi sistem, süreç veya sahip adına gerçekleştiği gerektiğinde ilişkilendirilebilmelidir.

İlke 10: Tek bir kanıt kaynağı olayın tamamını temsil ettiği varsayımına dönüşmemelidir.

Uygulama, işletim sistemi, kimlik altyapısı, ağ, bulut yönetimi ve başka katmanlar aynı olaya ilişkin farklı izler üretebilir. Bir kaynağın eksik veya değiştirilmiş olması diğer bağımsız kanıtların değerini artırabilir.

İlke 11: Farklı kanıt kaynakları gerektiğinde aynı olay zinciri içinde ilişkilendirilebilmelidir.

Dağıtık sistemlerde tek bir işlem birçok bileşene yayılabilir. Kanıt tasarımı bu parçaların ortak olay, kimlik veya zaman bağlamında gerektiğinde bir araya getirilebilmesine imkân vermelidir.

İlke 12: Kanıt toplama olayın kendisini gereksiz biçimde değiştirmemelidir.

İnceleme amacıyla yapılan işlemler sistem durumunu, zaman bilgisini veya başka önemli verileri değiştirebilir. Kanıt elde etme yöntemi oluşturduğu değişikliklerin kanıt değerine etkisini dikkate almalıdır.

İlke 13: Canlı ve kalıcı kanıt aynı özelliklere sahip kabul edilmemelidir.

Bazı bilgiler yalnızca sistem çalışırken mevcut olabilir; bazıları ise kapatma veya müdahale sonrasında korunabilir. Hangi bilginin ne zaman kaybolabileceği olay kararlarının parçası olmalıdır.

İlke 14: Kanıtın korunması her verinin süresiz saklanmasını gerektirmemelidir.

Daha fazla veri her zaman daha güçlü adli hazırlık anlamına gelmez. Saklama süresi, kanıtın olası değeri, olayların keşfedilme süresi ve oluşturulan gizlilik veya güvenlik maliyetiyle birlikte düşünülmelidir.

İlke 15: Kanıtın hassasiyeti adli değerinden bağımsız değildir.

İnceleme verisi kişisel bilgi, sır, güvenlik mimarisi veya başka hassas içerikler taşıyabilir. Kanıt olması bu veriye sınırsız erişim ve kullanım hakkı oluşturmaz.

İlke 16: Kanıt toplama yeni sır kopyaları oluşturmamalıdır.

Bellek, log veya sistem görüntülerinde parolalar, anahtarlar ve belirteçler bulunabilir. Adli hazırlık bu değerlerin gereksiz yere çoğaltılmasına ve yeni yetkisiz erişim yolları oluşturmasına neden olmamalıdır.

İlke 17: Kanıt üzerinde yapılan önemli işlemler kanıtın güvenilirliğini açıklayabilmelidir.

Kanıtın taşınması, dönüştürülmesi veya incelenmesi sırasında değişiklik meydana gelebilir. Orijinal bilgi ile inceleme sırasında üretilen veya değiştirilmiş kopyalar birbirine karıştırılmamalıdır.

İlke 18: Kanıtın kaynağı ve bütünlüğü gerektiğinde savunulabilir olmalıdır.

Bir dosyanın veya kaydın "sistemden geldiği" iddiası tek başına yeterli olmayabilir. Kanıtın hangi kaynaktan elde edildiği ve inceleme sırasında anlamlı biçimde değişip değişmediği değerlendirilebilmelidir.

İlke 19: Dış hizmet kullanılması kanıt ihtiyacını kuruluşun dışına çıkarmaz.

Bulut veya üçüncü taraf hizmetlerinde gerekli kayıt ve sistem verileri kuruluşun doğrudan kontrolünde olmayabilir. Hangi kanıtların üretildiği, ne kadar süre erişilebilir olduğu ve kuruluşun bunları hangi koşullarda elde edebildiği önceden anlaşılabilir olmalıdır.

İlke 20: Kanıtın teknik olarak saklanması yorumlanabilir kalacağını garanti etmemelidir.

Formatlar, yazılımlar, kimlik eşlemeleri ve sistem bağlamı zamanla değişebilir. Kanıt ihtiyaç duyulduğunda artık anlamlandırılamıyorsa yalnızca dosyanın varlığı yeterli koruma sağlamamıştır.

İlke 21: Kanıt eksikliği açıkça bilinmeli ve normal durum kanıtı gibi yorumlanmamalıdır.

Bir olay hakkında kanıt bulunamaması olayın gerçekleşmediğini göstermez. Görünürlük veya saklama eksikliği incelemenin kesinlik sınırının bir parçası olarak ifade edilebilmelidir.

İlke 22: Adli hazırlık yalnızca saldırganın kim olduğunu bulmayı hedeflememelidir.

Bir olayın nasıl mümkün olduğu, hangi sistemlerin etkilendiği, hangi verinin değiştiği ve hangi güven varsayımlarının başarısız olduğu çoğu durumda saldırgan kimliğinden daha önemli olabilir. Kanıt tasarımı bu soruları da desteklemelidir.

İlke 23: Dijital kanıt ve adli hazırlık güvencesi gerçek olayların yeniden açıklanabilirliği üzerinden doğrulanabilmelidir.

Kanıt saklama sistemi, prosedür veya araç bulunması tek başına güvence oluşturmaz. Gerçek veya temsili bir olay sonrasında neyin, ne zaman, hangi kimlik ve sistemler aracılığıyla gerçekleştiğinin; kanıtın güvenilirlik sınırlarıyla birlikte yeterli ölçüde yeniden kurulabilmesi gerekir.