Denetci.org

REFERANS İLKELERİ

Güvenlik Olayı Müdahalesi İlkeleri

Rİ-OLY-1

Sürüm 1.0 · 11.08.2026

www.denetci.org

Güvenlik Olayı Müdahalesi İlkeleri

Güvenlik olayı müdahalesi, bir güven kaybı ihtimalinin fark edilmesinden zararın sınırlandırılmasına ve sistemlerin güvenilir bir duruma yeniden ulaştırılmasına kadar alınan kararları ele alır. Amaç bütün olayları aynı adımlarla yöneten bir prosedür oluşturmak değil; belirsizlik altında etkili karar verilebildiği, kanıtın gereksiz yere kaybedilmediği ve yalnızca hizmetin değil güvenin de yeniden kurulabildiği bir müdahale anlayışı ortaya koymaktır.

İlke 1: Müdahale tam kesinlik oluşana kadar ertelenmemelidir.

Bir olay ilk fark edildiğinde kapsamı, nedeni ve etkisi tam olarak bilinmeyebilir. Ciddi sonuç ihtimali bulunan durumlarda bilgi eksikliği gerekli koruyucu kararların anlamsız biçimde geciktirilmesine neden olmamalıdır.

İlke 2: Belirsizlik karar sürecinde görünür kalmalıdır.

İlk bulgular yanlış, eksik veya sonradan değişebilir. Bilinenler, güçlü şüpheler ve varsayımlar birbirine karıştırılmamalı; kararların hangi bilgi düzeyinde alındığı anlaşılabilir olmalıdır.

İlke 3: Olayın önemi teknik belirtiden çok oluşturabileceği sonuçla anlaşılmalıdır.

Aynı zararlı yazılım, hesap ele geçirme veya hizmet kesintisi farklı sistemlerde farklı sonuçlar doğurabilir. Öncelik etkilenen veri, kimlik, hizmet, güven sınırı ve kuruluş üzerindeki gerçek etkiyle ilişkilendirilmelidir.

İlke 4: İlk görülen belirti olayın gerçek sınırı olarak kabul edilmemelidir.

Bir saldırı tek bir hesapta veya sistemde fark edilmiş olsa da başka alanlara daha önce yayılmış olabilir. Müdahale, gözlemlenen başlangıç noktasını olayın tamamı olarak varsaymamalıdır.

İlke 5: Sınırlandırma yalnızca mevcut zararı durdurmayı değil yayılmayı önlemeyi de amaçlamalıdır.

Ele geçirilmiş bir kimlik veya sistem başka güven alanlarına ulaşabiliyorsa olayın etkisi devam ediyor olabilir. Müdahale, zarar alanının gereksiz biçimde genişlemesini engellemeye çalışmalıdır.

İlke 6: Hız ile kontrolsüz müdahale aynı şey olmamalıdır.

Olay anında zaman önemli olabilir; ancak aceleyle yapılan değişiklikler hizmeti bozabilir, saldırganı uyarabilir veya önemli kanıtları yok edebilir. Müdahalenin hızı kararların etkisini tamamen görünmez hale getirmemelidir.

İlke 7: Sistemi kapatmak veya bağlantıyı kesmek varsayılan doğru cevap olmamalıdır.

Bazı olaylarda izolasyon zararı sınırlar; başka durumlarda ise kanıt kaybı, veri kaybı veya daha geniş hizmet etkisi oluşturabilir. Kullanılan müdahale olayın gerçek bağlamına dayanmalıdır.

İlke 8: Zararı sınırlandırmak ile olayın açıklanabilirliğini korumak birlikte düşünülmelidir.

Bir sistemi silmek, hesabı kapatmak veya ortamı değiştirmek saldırganın faaliyetini durdurabilirken olayın nasıl gerçekleştiğine ilişkin bilgiyi de ortadan kaldırabilir. Mümkün olduğu ölçüde koruma ve kanıt ihtiyacı birlikte değerlendirilmelidir.

İlke 9: Müdahale sahipliği ve kritik karar yetkileri belirsiz kalmamalıdır.

Birden fazla teknik ve kurumsal tarafın katılması sorumluluğun hiç kimseye ait olmadığı bir durum oluşturmamalıdır. Olayı kimin koordine ettiği ve hangi tür kararların kimler tarafından verilebildiği gerektiğinde anlaşılabilir olmalıdır.

İlke 10: Teknik yetki ile iş sonucu hakkında karar verme yetkisi birbirine karıştırılmamalıdır.

Bir sistemi izole etmenin teknik gerekliliğini değerlendiren taraf ile kritik hizmetin durdurulmasının kurumsal sonucunu taşıyan taraf farklı olabilir. Müdahale yaklaşımı bu kararları birbirinden koparmadan uygun sorumluluklarla ilişkilendirmelidir.

İlke 11: Müdahale tek bir güvenlik ekibinin sınırları içinde düşünülmemelidir.

Yüksek etkili olaylar teknoloji kadar hukuk, iletişim, iş sürekliliği, veri sahipliği, yönetim ve dış ilişkileri de etkileyebilir. Gerekli uzmanlık ve karar sahipleri olayın gerçek sonucuna göre sürece dahil olabilmelidir.

İlke 12: Kimlik olayları yalnızca ilk ele geçirilen hesapla sınırlı değerlendirilmemelidir.

Bir saldırgan oturumlara, belirteçlere, teknik hesaplara, anahtarlara veya başka kimlik unsurlarına erişmiş olabilir. Tek bir parolanın değiştirilmesi gerçek erişimin sona erdiği anlamına gelmemelidir.

İlke 13: Bir erişimin kaldırılması fiilî saldırgan yeteneğini sona erdirebilmelidir.

Hesap kapatılmış veya rol kaldırılmış görünse bile aktif oturumlar, sırlar veya başka erişim yolları çalışmaya devam edebilir. Müdahale kayıt durumundan çok kullanılabilir gerçek yetkiye odaklanmalıdır.

İlke 14: Bir sistemde saldırı belirtisinin kalmaması güvenin geri kazanıldığı anlamına gelmemelidir.

Saldırganın kalıcılık oluşturup oluşturmadığı, yapılandırmayı değiştirip değiştirmediği veya başka kimlikler elde edip etmediği bilinmeyebilir. “Temiz görünmek” ile güvenilir duruma dönmek ayrıştırılmalıdır.

İlke 15: Yeniden kurulum veya geri yükleme tek başına kök nedeni ortadan kaldırmış sayılmamalıdır.

Aynı zafiyet, kimlik bilgisi veya yanlış güven ilişkisi devam ediyorsa yeni kurulmuş sistem yeniden ele geçirilebilir. Kurtarma, yalnızca sistemin teknik durumunu değil olayın mümkün olmasını sağlayan koşulları da dikkate almalıdır.

İlke 16: Olay sırasında açılan geçici güven yolları olay sonrasında yaşamaya devam etmemelidir.

Acil erişimler, geçici hesaplar, ağ bağlantıları ve devre dışı bırakılmış kontroller müdahaleyi kolaylaştırabilir. Olay bittiğinde bunların görünmez biçimde yeni normal güven modeline dönüşmesi engellenmelidir.

İlke 17: Kanıt toplama müdahalenin dışında daha sonra yapılacak ayrı bir faaliyet olarak görülmemelidir.

İlk müdahaleler olay izlerini değiştirebilir veya yok edebilir. Kanıt ihtiyacı, gerekli müdahaleyi engellemeden alınan teknik kararların doğal bir parçası olmalıdır.

İlke 18: Olay sırasında oluşturulan bilgi izlenebilir ancak kesinlik sınırları bilinen bir kayıt oluşturmalıdır.

Kararlar, önemli gözlemler ve değişen olay anlayışı sonradan yeniden kurulabilmelidir. Bunun amacı bürokratik kayıt üretmek değil, uzun veya karmaşık olaylarda ortak ve güvenilir bir durum anlayışını korumaktır.

İlke 19: Olay iletişiminde hız doğruluğun yerine geçmemelidir.

Eksik bilgi altında iletişim gerekebilir; ancak varsayımlar doğrulanmış gerçek gibi sunulmamalıdır. Teknik ayrıntı, karar vericilerin gerçek etkiyi anlamasını zorlaştıracak biçimde iletişimin merkezine yerleşmemelidir.

İlke 20: Dış iletişim ve bildirim kararları olayın teknik yönünden ayrı fakat kopuk olmayan güven kararlarıdır.

Müşteriler, düzenleyiciler, iş ortakları veya kamuya yapılabilecek bildirimlerin zamanlaması ve içeriği teknik ekibin tek başına kararı olmayabilir. Bununla birlikte karar sahiplerinin yeterli ve güvenilir teknik bilgiye ulaşabilmesi gerekir.

İlke 21: Üçüncü tarafta gerçekleşen olay kuruluş açısından dış olay sayılmamalıdır.

Bir sağlayıcının veya iş ortağının güvenlik kaybı kuruluşun verisini, hizmetini veya kimlik ilişkilerini etkileyebilir. Müdahalenin başka kuruluş tarafından yürütülmesi kendi etkisini anlamak ve sınırlamak konusundaki sorumluluğu ortadan kaldırmaz.

İlke 22: Kurtarma hizmeti çalıştırmanın yanında güven ilişkilerini yeniden kurmalıdır.

Sistem yeniden erişilebilir olsa bile kimliklerin, verinin, yapılandırmanın veya güvenlik altyapısının güvenilirliği henüz doğrulanmamış olabilir. Olayın sona ermesi yalnızca kullanılabilirliğin dönmesine dayanmamalıdır.

İlke 23: Kurtarma sırası teknik kolaylıktan çok bağımlılık ve etkiye dayanmalıdır.

Bazı kimlik, güvenlik veya temel altyapı hizmetleri diğer sistemlerin güvenilir biçimde çalışmasının ön koşulu olabilir. Hızlı açılabilen sistemleri önce çalıştırmak her zaman güvenli bir kurtarma sırası oluşturmaz.

İlke 24: Olaydan öğrenme yalnızca kullanılan saldırı yolunu kapatmakla sınırlı kalmamalıdır.

Bir olay daha temel bir mimari zayıflığı, aşırı yetkiyi, görünürlük eksikliğini veya yanlış güven varsayımını ortaya çıkarabilir. İyileştirme yalnızca saldırganın kullandığı tek tek tekniği engellemeye odaklanmamalıdır.

İlke 25: Güvenlik olayı müdahalesi gerçek zarar sınırlama ve güvenin yeniden kurulması üzerinden doğrulanabilmelidir.

Müdahale planı, olay kayıtları veya olayın kapatılmış olması tek başına güvence oluşturmaz. Kuruluşun belirsizlik altında olayı anlamlandırabildiği, etkisini sınırlandırabildiği, gerçek erişim yollarını sona erdirebildiği ve sistemlerini güvenilir duruma geri getirebildiği gerektiğinde gösterilebilmelidir.