Denetci.org

REFERANS İLKELERİ

Güvenlik Tatbikatı İlkeleri

Rİ-OLY-3

Sürüm 1.0 · 11.08.2026

www.denetci.org

Güvenlik Tatbikatı İlkeleri

Güvenlik tatbikatı, kuruluşun güvenlik olayları ve diğer yüksek etkili durumlar karşısında sahip olduğunu düşündüğü hazırlığın kontrollü koşullarda sınanmasını ele alır. Amaç bir senaryoyu başarıyla tamamlamak veya prosedür bilgisini göstermek değil; insanların, sistemlerin, karar mekanizmalarının ve bağımlılıkların belirsizlik altında gerçekte nasıl davrandığını ortaya çıkarmaktır.

İlke 1: Her tatbikat açık bir güvence iddiasını sınamalıdır.

Bir tatbikatın yalnızca gerçekleştirilmiş olması hazırlık hakkında anlamlı bilgi vermez. Çalışmanın hangi yeteneğin gerçekten var olup olmadığını göstermek istediği açık olmalıdır.

İlke 2: Tatbikat kuruluşun gerçek güvenlik bağlamına dayanmalıdır.

Senaryolar, kuruluşun gerçek sistemlerini, hizmetlerini, verilerini, kimliklerini ve bağımlılıklarını anlamlı ölçüde temsil etmelidir. İlgi çekici ancak kuruluşun gerçek maruziyetleriyle ilgisiz senaryolar sınırlı güvence sağlar.

İlke 3: Tatbikat önceden bilinen doğru cevabın tekrarı olmamalıdır.

Gerçek olaylarda bilgi eksik, yanlış veya değişken olabilir. Tatbikat, yalnızca prosedürü hatırlama becerisini değil belirsizlik altında doğru muhakeme ve uyum sağlama kapasitesini de sınayabilmelidir.

İlke 4: Senaryonun gelişimi katılımcının kararlarından bağımsız sabit bir gösteriye dönüşmemelidir.

Gerçek bir olay alınan kararlar nedeniyle farklı yönlere ilerleyebilir. Tatbikat mümkün olduğu ölçüde katılımcıların davranışlarının oluşturduğu sonuçları yansıtmalıdır.

İlke 5: Tatbikat başarıyı göstermekten çok hazırlığın sınırlarını ortaya çıkarmalıdır.

Hiç sorun yaşanmayan bir çalışma her zaman güçlü hazırlığın göstergesi değildir. Tatbikatın değeri, gerçek olaydan önce zayıf varsayımları ve eksik kabiliyetleri güvenli koşullarda görünür hale getirebilmesindedir.

İlke 6: Katılımcı hatası tatbikatın başarısızlığı olarak görülmemelidir.

Yanlış karar veya gecikme gerçek çalışma biçimindeki bir zayıflığı ortaya çıkarabilir. Amaç bireyleri hatasız davranmaya yöneltmek değil, sistemin insan hatasını nasıl karşıladığını anlamaktır.

İlke 7: Tatbikat bireylerin yanında organizasyonun çalışma biçimini de sınamalıdır.

Hazırlık yalnızca uzmanların bilgisine bağlı değildir. Yetkiler, bilgi akışı, araçlar, ekipler arası ilişkiler ve kurumsal bağımlılıklar da gerçek müdahale kapasitesinin parçalarıdır.

İlke 8: Kritik kabiliyet tek bir kişinin varlığına bağlıysa bu bağımlılık görünür hale gelmelidir.

Bir görevin yalnızca belirli bir kişi tarafından gerçekleştirilebilmesi gerçek olayda önemli bir süreklilik riski oluşturabilir. Tatbikat bu tür tekil insan bağımlılıklarını saklamamalıdır.

İlke 9: Karar yetkileri yalnızca belgelerde değil tatbikat davranışında da anlam taşımalıdır.

Kimin sistemi izole edebileceği, iş hizmetini durdurabileceği veya başka yüksek etkili kararları verebileceği gerçek olayda belirsiz kalmamalıdır. Biçimsel sorumluluk ile fiilî karar kapasitesi arasındaki fark tatbikatta ortaya çıkabilmelidir.

İlke 10: İletişim kabiliyeti normal iletişim araçlarının çalışacağı varsayımına bağlı olmamalıdır.

Güvenlik olayı kimlik, e-posta, mesajlaşma veya başka kurumsal iletişim sistemlerini de etkileyebilir. Koordinasyon ihtiyacı, tek bir iletişim kanalının güvenilirliğine bütünüyle bağlı kalmamalıdır.

İlke 11: Tatbikat gerçek olayda gerekli olacak tarafları gerektiği ölçüde kapsamalıdır.

Teknik ekipler, iş sahipleri, yönetim, hukuk, iletişim ve dış taraflar aynı olayda farklı kararlar taşıyabilir. Tatbikatın kapsamı organizasyon şemasından çok gerçek olayın gerektireceği işbirliğine dayanmalıdır.

İlke 12: Üçüncü taraflar ideal davranacakları varsayımıyla temsil edilmemelidir.

Sağlayıcılar gecikebilir, ulaşılamayabilir veya sınırlı bilgi sunabilir. Kuruluşun hazırlığı dış tarafların her zaman beklenen zamanda ve biçimde yardımcı olacağı varsayımına bağlı olmamalıdır.

İlke 13: Teknik tatbikat gerçek güvenlik sınırlarını anlamsız biçimde çevresinden dolaşmamalıdır.

Bir saldırı veya müdahale yolunun sürekli olarak simüle edilmesi, korunması gereken gerçek kontrollerin çalışıp çalışmadığını göstermeyebilir. Tatbikat güvenli koşulları korurken sınamak istediği güvenlik mekanizmasını da mümkün olduğu ölçüde gerçekten kullanmalıdır.

İlke 14: Tatbikatın kendisi gereksiz yeni bir güvenlik riski oluşturmamalıdır.

Tatbikat erişimleri, hesapları, araçları ve verileri üretim sistemlerini etkileyebilir. Hazırlığı sınamak amacı, kalıcı saldırı yüzeyi, gereksiz hassas veri kullanımı veya kontrolsüz sistem etkisi oluşturmayı haklı çıkarmamalıdır.

İlke 15: Tatbikat olayın yalnızca ilk anına odaklanmamalıdır.

Gerçek güvenlik olayları tespit, karar, sınırlandırma, uzun süreli çalışma, kurtarma ve normale dönüş gibi farklı aşamalar içerir. Hazırlık yalnızca ilk bildirime ne kadar hızlı cevap verildiğiyle ölçülmemelidir.

İlke 16: Uzun süreli olayların insan ve organizasyon üzerindeki etkisi dikkate alınmalıdır.

Bir müdahale planı kısa bir tatbikatta uygulanabilir görünürken saatler veya günler süren gerçek olayda sürdürülemeyebilir. Hazırlık, dikkat, vardiya, bilgi devri ve karar yorgunluğu gibi gerçek insan sınırlarını hesaba katmalıdır.

İlke 17: Tespit ile müdahale arasındaki bağ tatbikatta gerçek bir kabiliyet olarak sınanmalıdır.

Bir güvenlik sinyalinin üretilmesi tek başına olayın doğru taraflarca anlaşılacağı ve eyleme dönüşeceği anlamına gelmez. Bilginin fark edilmesi, anlamlandırılması ve karar sahibine ulaşması birlikte çalışabilmelidir.

İlke 18: Kurtarma, hizmeti yeniden açmaktan daha geniş bir tatbikat alanı olmalıdır.

Bir sistemin çalışmaya başlaması kimliklerin, verinin veya yapılandırmanın yeniden güvenilir olduğu anlamına gelmez. Tatbikat gerektiğinde güvenilir duruma dönüşün gerçekten mümkün olup olmadığını da sınamalıdır.

İlke 19: Tatbikat olayın sonradan açıklanabilme kapasitesini de sınayabilmelidir.

Müdahale sırasında önemli kanıtların korunması ve olayın ne şekilde geliştiğinin yeniden kurulabilmesi gerçek güvenlik kapasitesinin bir parçasıdır. Tatbikat yalnızca saldırıyı durdurmaya odaklanarak bu yeteneği görünmez bırakmamalıdır.

İlke 20: Tatbikat sonucu tek bir süre, puan veya başarı sınıfına indirgenmemelidir.

Hız, teknik doğruluk, karar kalitesi, iletişim, kanıt koruma ve kurtarma gibi yetenekler farklı sonuçlar gösterebilir. Tek bir sayının bu farklı güvence alanlarını olduğundan daha kesin göstermesine izin verilmemelidir.

İlke 21: Tatbikat değerlendirmesi yalnızca katılımcıların kendi algısına bağlı olmamalıdır.

Katılımcılar olay sırasında bazı bağımlılıkları veya hataları fark etmeyebilir. Değerlendirme, gerçek davranışa ve gerektiğinde bağımsız gözleme dayanabilmelidir; ancak gözlem de tatbikatın doğal davranışını gereksiz biçimde yönlendirmemelidir.

İlke 22: Tatbikatta bulunan zayıflık gerçek iyileştirmeye dönüşebilmelidir.

Aynı sorun tekrar tekrar görülüyor ancak sistemde, yetkilerde veya çalışma biçiminde hiçbir değişiklik oluşturmuyorsa tatbikat yalnızca tekrar eden bir etkinliğe dönüşür. Öğrenmenin değeri gerçek hazırlık durumunu değiştirebilmesindedir.

İlke 23: Tatbikat ihtiyacı yalnızca takvime bağlı olmamalıdır.

Önemli mimari değişiklikler, yeni hizmetler, değişen bağımlılıklar veya gerçek olaylar yeni varsayımların sınanmasını gerektirebilir. Geçmişte yapılan bir tatbikat değişmiş bir sistem için süresiz güvence sağlamamalıdır.

İlke 24: Güvenlik tatbikatı güvencesi gerçek davranış ve öğrenme üzerinden doğrulanabilmelidir.

Tatbikat planları, katılım kayıtları veya tamamlanmış senaryolar tek başına hazırlık kanıtı değildir. Kuruluşun belirsizlik altında tespit, karar, koordinasyon, müdahale ve kurtarma yeteneklerini gerçekten gösterebilmesi ve ortaya çıkan eksikliklerden öğrenebilmesi güvence oluşturmalıdır.