Denetci.org

REFERANS İLKELERİ

Bilgi Güvenliği Risk Yönetimi İlkeleri

Rİ-YON-2

Sürüm 1.0 · 11.08.2026

www.denetci.org

Bilgi Güvenliği Risk Yönetimi İlkeleri

Bilgi güvenliği risk yönetimi, belirsizlik altında hangi güvenlik sonuçlarının kuruluş için önemli olduğunu ve bu sonuçlarla ilgili hangi tercihlerin yapılacağını ele alır. Amaç bütün riskleri tek bir puana indirgemek veya eksiksiz bir tehdit listesi oluşturmak değil; maruziyetin gerçek niteliğini anlamak ve alınan güvenlik kararlarının hangi risk anlayışına dayandığını görünür kılmaktır.

İlke 1: Risk, gerçek bir bağlam içindeki olası kayıp üzerinden anlaşılmalıdır.

Bir tehdit veya zafiyet yalnızca var olduğu için aynı derecede önemli değildir. Risk, neyin etkilenebileceği, bu etkinin kuruluş açısından ne anlama geldiği ve olayın hangi koşullarda ortaya çıkabileceği birlikte düşünülerek anlam kazanır.

İlke 2: Risk değerlendirmesi korunmaya değer olan şeylerden ve onların bağımlılıklarından başlamalıdır.

Bir sistemin riski yalnızca kendisine doğrudan yönelen tehditlerden oluşmaz. Hizmetler, veriler, insanlar, altyapılar ve dış bağımlılıklar arasındaki ilişkiler gerçek maruziyetin bir parçasıdır.

İlke 3: Mevcut kontrollerin varlığı etkin olduklarının kanıtı olarak kabul edilmemelidir.

Bir kontrolün tanımlanmış veya uygulanmış olması riski beklenen ölçüde azalttığını göstermeyebilir. Risk değerlendirmesi, güvenlik önlemlerinin amaçlanan etkiyi gerçekten sağladığına ilişkin güven düzeyini de hesaba katmalıdır.

İlke 4: Olasılık, etki ve belirsizlik birbirinden kopuk değerlendirilmemelidir.

Risk yalnızca gerçekleşme ihtimalinden veya yalnızca olası zararın büyüklüğünden oluşmaz. Bu unsurların hangi bilgiye dayandığı ve ne kadar belirsizlik taşıdığı da verilen kararın parçası olmalıdır.

İlke 5: Düşük olasılık, ağır sonuçları kendiliğinden önemsiz hale getirmemelidir.

Nadir gerçekleşmesi beklenen ancak kuruluşun devamlılığı veya temel yükümlülükleri üzerinde çok büyük etkisi olabilecek olaylar sırf olasılıkları düşük görüldüğü için göz ardı edilmemelidir. Risk anlayışı olağan durumların yanında uç sonuçları da taşıyabilmelidir.

İlke 6: Riskler birbirinden bağımsızmış gibi ele alınmamalıdır.

Aynı teknolojiye, kimliğe, sağlayıcıya, fiziksel ortama veya başka bir ortak bağımlılığa dayanan riskler birlikte gerçekleşebilir. Ayrı ayrı kabul edilebilir görünen maruziyetler birleştiğinde farklı bir risk oluşturabilir.

İlke 7: Risk yalnızca amaçlanan kullanım biçimine göre değerlendirilmemelidir.

Sistemler yanlış kullanılabilir, hatalı yapılandırılabilir, beklenmedik koşullarla karşılaşabilir veya saldırganlar tarafından tasarım amacının dışında kullanılabilir. Makul biçimde öngörülebilen hata ve kötüye kullanım yolları risk anlayışının dışında bırakılmamalıdır.

İlke 8: Risk sahipliği, riski etkileyebilecek gerçek karar yetkisiyle ilişkili olmalıdır.

Bir riskin sahibi yalnızca onu kayıt altına alan veya teknik olarak gözlemleyen taraf olmamalıdır. Sahiplik, riskin sonuçlarını anlayabilecek ve kabul, değişiklik veya kaynak kullanımı konusunda anlamlı karar verebilecek bir konumla ilişkilendirilmelidir.

İlke 9: Riskin azaltılması kontrol sayısını artırmakla eş anlamlı değildir.

Eklenen her mekanizma riski azaltmayabilir; bazıları yeni bağımlılık veya karmaşıklık da oluşturabilir. Risk yaklaşımı, sorunun kaynağını ve gerçekleşme yolunu değiştiren çözümlerin gerçek etkisine dayanmalıdır.

İlke 10: Bir güvenlik önleminin oluşturduğu yeni risk de değerlendirilmelidir.

Bir kontrolün maliyeti yalnızca para veya işletme yükü değildir. Ek karmaşıklık, yeni ayrıcalıklar, ortak hata noktaları veya süreklilik üzerindeki etkiler azaltılmak istenen riskin yanında dikkate alınmalıdır.

İlke 11: Riskin başka bir tarafa aktarılması kuruluşun sonuçla ilişkisini ortadan kaldırmaz.

Sigorta, sözleşme, hizmet sağlayıcı veya başka bir taraf bazı sonuçları paylaşabilir; ancak kuruluşun müşterileri, hizmetleri veya yükümlülükleri üzerindeki etkiler devam edebilir. Risk transferi, hangi sorumluluğun gerçekten değiştiği üzerinden değerlendirilmelidir.

İlke 12: Risk kabulü sınırsız ve geri alınamaz bir güven kararı olmamalıdır.

Bir risk belirli koşullarda kabul edilebilirken bu koşullar değiştiğinde aynı karar geçerliliğini yitirebilir. Kabul, riskin ortadan kalktığı varsayımı değil, bilinen maruziyet altında yapılmış bilinçli bir tercih olarak görülmelidir.

İlke 13: Risk puanları karar vermeyi desteklemeli, riskin kendisi haline gelmemelidir.

Sayısal yöntemler farklı riskleri karşılaştırmayı kolaylaştırabilir; ancak benzer puanlar farklı sonuçlar ve farklı belirsizlikler barındırabilir. Karar, hesaplanan değerin arkasındaki gerçek senaryodan kopmamalıdır.

İlke 14: Risk anlayışı değişiklikler ve gerçek olaylarla sınanabilmelidir.

Yeni mimariler, kullanım biçimleri, tehditler, güvenlik olayları ve beklenmeyen sonuçlar daha önceki varsayımların geçerliliğini değiştirebilir. Risk yönetimi, geçmiş değerlendirmeyi korumak yerine yeni gerçekliği yansıtabilmelidir.

İlke 15: Risk görünümü kuruluşun fiilen kabul ettiği güvenlik durumunu yansıtmalıdır.

Resmî kayıtlardaki riskler ile kuruluşun gerçekte maruz kaldığı ve bilerek sürdürdüğü durumlar birbirinden kopmamalıdır. Risk yönetiminin değeri, kayıtların eksiksiz görünmesinden çok karar vericilere gerçek maruziyeti gösterebilmesinde yatar.