Denetci.org

REFERANS İLKELERİ

Bilgi Güvenliği Yönetişimi İlkeleri

Rİ-YON-1

Sürüm 1.0 · 11.08.2026

www.denetci.org

Bilgi Güvenliği Yönetişimi İlkeleri

Bilgi güvenliği yönetişimi, kuruluşun güvenlikle ilgili kararları nasıl sahiplendiğini, hangi esaslara göre verdiğini ve bu kararların iş hedefleriyle nasıl ilişkilendirildiğini ele alır. Amaç güvenliği ayrı bir idari katmana dönüştürmek değil; güvenliği etkileyen kararların doğru sorumluluk, yetki ve bilgiyle alınmasını sağlayan bir yönetim anlayışı oluşturmaktır.

İlke 1: Bilgi güvenliği kuruluşun amaçlarından ayrı yönetilmemelidir.

Güvenlik, korunmaya çalışılan hizmetler, bilgiler, insanlar ve iş sonuçları bilinmeden kendi başına anlamlı bir hedef haline gelemez. Güvenlik kararlarının değeri, kuruluşun önemli gördüğü sonuçları ne ölçüde koruduğuyla anlaşılmalıdır.

İlke 2: Güvenlik sorumluluğu, güvenliği etkileyen kararların bulunduğu yerde paylaşılmalıdır.

Güvenlik ekibi uzmanlık ve bağımsız görüş sağlayabilir; ancak sistemler, hizmetler, süreçler ve veriler hakkında karar veren tarafların güvenlik üzerindeki sorumluluğunu bütünüyle devralamaz. Riski değiştirebilen bir kararın güvenlik sonucu, karar sürecinin dışında bırakılmamalıdır.

İlke 3: Sorumluluk ile karar yetkisi birbirinden kopmamalıdır.

Bir sonuçtan sorumlu tutulan tarafın o sonucu etkileyebilecek kararlar üzerinde gerçek bir etkisi bulunmalıdır. Yetkisi olmayan bir tarafa sorumluluk vermek veya yetki sahibini sonuçlardan ayırmak gerçek hesap verebilirlik oluşturmaz.

İlke 4: Güvenlik yönetişimi belge ve yapıların varlığıyla eş anlamlı değildir.

Politikalar, komiteler, roller ve raporlar yönetişimi destekleyebilir; ancak bunların varlığı güvenlik kararlarının doğru alındığını göstermez. Güvence, bu yapıların kuruluşun gerçek kararlarına ve davranışlarına nasıl yansıdığı üzerinden değerlendirilmelidir.

İlke 5: İlkeler karar vermenin yerini değil, dayanağını oluşturmalıdır.

Her yeni durumun önceden kurala bağlanması mümkün değildir. Yönetişim, tanımlanmamış veya çatışmalı durumlarda da tutarlı karar verilebilmesini sağlayacak ortak bir güvenlik anlayışı sunmalıdır.

İlke 6: Teknik güvenlik sonuçları iş sonuçlarıyla ilişkilendirilebilmelidir.

Bir zafiyetin, kontrol eksikliğinin veya mimari kararın önemi yalnızca teknik özelliklerinden anlaşılmayabilir. Güvenlik yönetişimi, teknik gerçekler ile hizmet, veri, yükümlülük, süreklilik ve diğer kurumsal sonuçlar arasındaki ilişkiyi görünür tutmalıdır.

İlke 7: Öncelikler görünürlüğe değil gerçek etkiye dayanmalıdır.

Yeni, dikkat çekici veya kolay ölçülebilen sorunlar daha temel risklerin önüne otomatik olarak geçmemelidir. Kaynaklar, kuruluşun maruz kaldığı gerçek risk ve korunmak istenen sonuçlarla orantılı biçimde yönlendirilmelidir.

İlke 8: Risk kabulü gerçek bir yönetim kararı olmalıdır.

Bir riskin giderilmemesine karar verilmesi teknik bir kaydın kapatılmasıyla eş anlamlı değildir. Riskin sonuçlarını taşıyabilecek ve gerekli tercihleri yapabilecek taraf, neyin kabul edildiğini ve hangi varsayımlara dayanıldığını anlayabilmelidir.

İlke 9: İstisnalar ve güvenlik borcu görünmez bir yönetişim alanı oluşturmamalıdır.

Geçici çözümler, ertelenmiş iyileştirmeler ve genel yaklaşımdan sapmalar zamanla normal çalışma biçimine dönüşebilir. Bu durumlar güvenlik modelinin dışında değil, onun gerçek durumunu etkileyen kararlar olarak ele alınmalıdır.

İlke 10: Önemli değişiklikler ve dış bağımlılıklar yönetişim sınırlarını aşmamalıdır.

Kuruluşun sistemlerini veya riskini önemli ölçüde değiştiren bir karar, yalnızca başka bir ekipte veya başka bir kuruluşta alındığı için güvenlik yönetişiminin dışında kalmamalıdır. Güvenliği etkileyen karar yolları organizasyon şemasından daha geniş olabilir.

İlke 11: Yönetişim, güvenli karar vermeyi gereksiz yere zorlaştırmamalıdır.

Aşırı yavaş, karmaşık veya gerçek çalışma biçiminden kopuk yapılar zamanla resmi süreçlerin çevresinden dolaşılmasına yol açabilir. Yönetişim, gerekli değerlendirmeyi korurken kararların ihtiyaç duyulan zamanda alınabilmesini desteklemelidir.

İlke 12: Olumsuz bilgi yönetimden uzaklaştırılmamalıdır.

Güvenlik sorunlarının görünür hale gelmesi veya üst seviyeye taşınması kendi başına başarısızlık değildir. Yönetişim, karar vericilerin kötü haberleri gecikmeden görebildiği ve sorunları saklamayı teşvik etmeyen bir yapı oluşturmalıdır.

İlke 13: Ölçüm, yönetim muhakemesinin yerine geçmemelidir.

Sayılar, puanlar ve göstergeler karar vermeyi destekleyebilir; ancak temsil ettikleri gerçeklikten daha kesin kabul edilmemelidir. Kolay ölçülebilen sonuçlar, önemli fakat daha zor ölçülen güvenlik özelliklerini görünmez hale getirmemelidir.

İlke 14: Yönetişim kendi sonuçlarından öğrenebilmelidir.

Daha önce alınmış bir karar, geçmişte doğru kabul edildiği için süresiz biçimde korunmamalıdır. Değişen koşullar, yaşanan olaylar ve kararların gerçek sonuçları yönetişim anlayışının yeniden değerlendirilmesine imkân vermelidir.

İlke 15: Yönetişimin güvencesi kuruluşun gerçek davranışında görülmelidir.

Bir kuruluşun güvenlikle ilgili beyanları ile bütçe, öncelik, risk kabulü, değişiklik ve günlük kararları arasında sürekli bir çelişki bulunuyorsa tanımlanmış yönetişim gerçekte işlemiyor olabilir. Güvenlik yönetişimi, kuruluşun fiili kararları üzerinden doğrulanabilir olmalıdır.