Olay Yönetimi Prosedürü

AMAÇ

Bu prosedürün amacı, kurum içerisinde meydana gelebilecek bilgi güvenliği olaylarının tespiti, raporlanması, sınıflandırılması, değerlendirilmesi, kontrol altına alınması, etkilerinin azaltılması ve tekrarının önlenmesine yönelik süreçleri tanımlamaktır.

KAPSAM

Bu prosedür: Tüm çalışanları, Tedarikçileri, taşeronları, Dış hizmet sağlayıcıları, Kurum sistemlerine erişimi olan tüm kullanıcıları, Fiziksel, elektronik ve sözlü bilgi güvenliği olaylarını kapsar.

UYGULAMA

Bilgi Güvenliği Olay İhlalinin Tespiti: Sistem uyarıları (SIEM, DLP, IDS/IPS vb.), Çalışan bildirimi, Log analizleri, Tedarikçi bildirimleri, Otomatik güvenlik yazılımları, Penetrasyon testi sonuçları her olay potansiyel ihlal olarak kabul edilir ve kayıt altına alınır.

Bilgi Güvenliği Olay İhlalinin Olayın Bildirilmesi: Tespit edilen olaylar: Bilgi Güvenliği Olay Bildirim Formu**,** E-posta, telefon veya olay yönetim sistemi üzerinden derhal BGYS Ekibine bildirilir.

Bilgi Güvenliği Olay İhlalinin Olayın Sınıflandırılması

BGYS Ekibi olayları üç seviyede sınıflandırır: Düşük Etki (Sistem kesintisi yok, Veri kaybı yok, Etki minimum), Orta Etki (Sınırlı veri etkisi, Belirli kullanıcı veya sistemlerde kesinti), Yüksek Etki (KRİTİK, Kişisel veri sızıntısı, Sistem durması, Ransomware, Çoklu kullanıcı etkilenmesi, KVKK / hukuksal etki ihtimali) Bu durumda acil durum planı devreye alınır.

Olayın Etki Analizi Etki analizi kapsamında: Hangi sistemler etkilendi? Hangi veriler risk altında? Kesinti süresi nedir? İş süreçleri etkileniyor mu? Kişisel veri var mı? Müşteriler etkileniyor mu? Sorularına yanıt aranır.

Olayın Kontrol Altına Alınması (Containment): Şu adımlar uygulanabilir: Sistemin ağ bağlantısını kesme, Kullanıcı hesabını askıya alma, Zararlı süreçleri sonlandırma, Erişim yetkilerini dondurma, Sistem yedeğine geri dönme, Etkilenen cihazları karantinaya alma, Amaç: Olayın yayılmasını durdurmak.

Delil Toplama (Evidence Collection): Deliller toplanırken: Loglar, sistem kayıtları, güvenlik cihazı çıktıları saklanır. Disk görüntüsü (imaj) alınabilir. Fiziksel deliller korunur. Zaman damgalı kayıt tutulur. Delile müdahale edilmez. Deliller hukuki geçerliliği olacak şekilde saklanır.

Olayın Kök Neden Analizi Yapılır. Olay neden ortaya çıktı? Kullanıcı hatası, Güvenlik açığı, Eksik yama, Zayıf parola, Malware / phishing, Tedarikçi kaynaklı zafiyet, Politikaya uyumsuzluk, Kök neden belirlenir ve kayıt altına alınır.

Düzeltici Faaliyetlerin Uygulanması: Belirlenen kök nedene göre: Yama güncellemesi, Parola sıfırlama, Erişim yetkilerinin revizyonu, Kullanıcı eğitimi, Güvenlik cihazı ayarlarının güçlendirilmesi, Tedarikçi değişikliği, Süreç güncellemesi yapılır.

Olay Yönetimi Prosedürü

Olayın Kapatılması ve Raporlama: Her olay için Olay Kapanış Raporu hazırlanır: Olay özeti, Etki analizi, Yapılan aksiyonlar, Kök neden, Düzeltici faaliyetler, Öğrenilen dersler

Öğrenilen Dersler Toplantısı Kritik olaylar sonrası BGYS ekibi ve ilgili birimler birlikte: Ne yanlış gitti? Ne yapılabilirdi? Süreç nasıl iyileştirilir? Hangi politika/prosedür güncellenmeli? sorularını ele alır.

Süreç İyileştirme: Olay sonrası: BT altyapısı, Politika ve prosedürler, Kullanıcı farkındalığı, Güvenlik cihazı kuralları iyileştirilir. Tüm değişiklikler Değişiklik Yönetimi Prosedürü ile uygulanır.

SORUMLULUKLAR

Tüm Çalışanlar: Olayları derhal bildirmekle yükümlüdür. Delillere müdahale etmeden durumu raporlar.
Bilgi İşlem / Sistem Yönetimi: Teknik analizi yapar. Olayı sınıflandırır ve kontrol altına alır. Delilleri toplar, saklar.
BGYS Ekibi: Olayı değerlendirir. Etki analizini yapar. Düzeltici faaliyetleri başlatır. Yönetimi bilgilendirir.
KVKK Komitesi / Veri Sorumlusu İrtibat Kişisi: Kişisel veri ihlallerini değerlendirir. Gerekirse KVKK Kurumu'na bildirim yapar.
Yönetim: Gerektiğinde dış kaynak, hukuk, iletişim vb. destekleri devreye alır. İyileştirme kararlarını onaylar.

DOKÜMANLAR

Bilgi Güvenliği Olay İhlal Formu
DÖF Formu