

REHBER

Olay Müdahale Planı Hazırlama Rehberi

Bir güvenlik olayı yaşandığında ne yapılacağını önceden belirleyen bir olay müdahale planının nasıl hazırlanacağını anlatan pratik bir rehber hazırladık.



REHBER

YAKLAŞIK 6 DK OKUMA

OLAY MÜDAHALE

BU REHBERDE

1. Neden plan gerekli?
2. Olay müdahalenin aşamaları
3. Roller ve sorumluluklar
4. Olayları sınıflandırmak
5. İlk 60 dakika kontrol listesi
6. Playbook ve tatbikat

01 Neden plan gerekli?

Bir olay anında en pahalı şey zamandır. Kimin karar vereceği, kimin ne yapacağı ve kime haber verileceği o anda tartışılırsa kayıplar büyür. İyi bir plan, kriz anında düşünme yükünü azaltır ve herkesin aynı sayfada olmasını sağlar.

02 Olay müdahalenin aşamaları

1

Hazırlık

Plan, roller, araçlar, eğitim

2

Tespit ve analiz

Olayı fark et, sınıflandır, kapsamını anla

3

Sınırlama

Yayılmayı durdur

4

Temizleme ve kurtarma

Kök nedeni gider, sistemleri güvenle geri getir

5

Olay sonrası

Kök neden analizi ve dersler

03

Roller ve sorumluluklar**Olay yöneticisi**

Süreci yönetir, karar verir, durumu raporlar.

Teknik ekip

Analiz, sınırlama ve kurtarma işlemlerini yürütür.

Hukuk / KVKK

Bildirim yükümlülüklerini ve delil bütünlüğünü değerlendirir.

İletişim

İç ve dış paydaşlarla tutarlı iletişim kurar.

Yönetim

Kaynak ve öncelik kararlarını verir.

Dış destek

Adli bilişim veya müdahale uzmanları, gerekirse.

04

Olayları sınıflandırmak

Her olay aynı seviyede ele alınmaz. Önceden tanımlı bir ölçek, doğru kişilere doğru hızda ulaşmayı sağlar:

- Düşük: sınırlı etki, rutin ekip kapasitesiyle çözülebilir
- Orta: bir iş sürecini veya birden çok kullanıcıyı etkiliyor, yönetim bilgilendirilir
- Yüksek: kritik sistem veya kişisel veri etkileniyor, kriz ekibi toplanır ve bildirim yükümlülükleri değerlendirilir

05

İlk 60 dakika kontrol listesi

- | | |
|---|---|
| ☐ Olayı kayda geç: ne zaman, kim fark etti, neyi gördü | ☐ Etkilenen sistemleri ağdan izole et, ancak delili bozma (gerekmedikçe kapatma) |
| ☐ Olay yöneticisini ve kriz ekibini topla | ☐ Logları ve ilgili delilleri koru |
| ☐ İletişimi güvenli bir kanaldan yürüt (e-posta ele geçirilmiş olabilir) | ☐ Hukuk/KVKK sorumlusunu bilgilendir |



Sınıflandırmayı yap ve yönetimi
bilgilendir

06

Playbook ve tatbikat

Sık görülen senaryolar için adım adım playbook'lar hazırlayın: fide yazılımı, hesap ele geçirme, veri sızıntısı, hizmet engelleme. Playbook'ları yılda en az bir kez masabaşı tatbikatla deneyin; tatbikat plandaki boşlukları gerçek olay yaşanmadan gösterir.

Önemli: Planı yazıp rafa kaldırmayın. İletişim bilgileri, roller ve araçlar değiştikçe güncelleyin.

Olay müdahale hazırlığınızı birlikte kuralım Planınızı, rollerinizi ve tatbikatlarınızı birlikte oluşturalım.

// İLETİŞİM

Bize ulaşın

İhtiyacınızı ve mevcut durumunuzu paylaşın; size uygun kapsamı ve yol haritasını birlikte belirleyelim. Bilgi formumuzu doldurabilir veya doğrudan bize ulaşabilirsiniz.

Troy Bilgi Teknolojileri Ticaret Limited Şirketi

Atatürk Mah. Vedat Günyol Cad. 44M/2

Ataşehir / İstanbul

T 0-216-575 5222 **E** info@troybilgiteknolojileri.com



Hizmet sayfası ve bilgi formu
için QR kodu okutun