EMA SECURITY

Yöneticilere Özel Farkındalık Eğitimi

AI-Powered Defense Service

İletişim

www.emasecurity.com

info@emasecurity.com

Bostancı Mah, Ali Nihat Tarhan Cd, Kahraman Sk,
No:2/D:11, Hoffman Plaza, Kadıkoy/İstanbul

+90 (850) 244 49 26

Yöneticilere Özel Farkındalık Eğitimi

Eğitim Açıklaması

Yöneticilere Özel Farkındalık Eğitimi, şirketlerin üst düzey yöneticilerine özel olarak hazırlanmış bir programdır. Eğitim, yöneticilerin bilgi güvenliği politikaları oluşturma, stratejik kararlar alma ve güvenlik tehditlerine karşı proaktif bir yaklaşım benimseme becerilerini geliştirmeyi hedefler. Yöneticiler, siber güvenlik tehditlerine karşı liderlik rolü üstlenebilmek için gerekli olan farkındalığı kazanacaklardır.

Eğitim Yeri

- Online
- Fiziksel

Eğitim Süresi

- 1 Gün

Eğitim Seviyesi

- Herkes

Eğitim Sonunda Katılımcılar Ne Öğrenmiş Olacak?

- Katılımcılar, yöneticiler için kritik siber güvenlik tehditleri, riskler ve yönetim stratejileri hakkında derinlemesine bilgi edinerek, organizasyonel güvenliği sağlama becerisi kazanırlar.

Yöneticilere Özel Farkındalık Eğitimi

Eğitim İçeriği

- Siber Güvenlik Neden Yöneticinin Sorumluluğudur?
- Yöneticinin kararları ile siber risklerin doğrudan ilişkisi
- IT riski = İş riski = Reputasyon riski
- Siber saldırıların üst düzey etkileri: finansal, operasyonel, regülasyonel
- Yönetim Kurulu ve C-level rollerin sorumluluğu
- CEO'ların saldırı sonrası cezai ve hukuki sorumluluğu
- Günümüz Tehditleri ve Trendlere Genel Bakış
- Fidye yazılımları (Ransomware), tedarik zinciri saldırıları, APT grupları
- Siber casusluk ve veri hırsızlığı örnekleri
- E-posta oltalama (phishing), kimlik avı saldırıları
- Tehdit aktörleri: Organize suç grupları, devlet destekli gruplar, içeriden tehditler
- Güncel vaka incelemeleri (Uber, Colonial Pipeline, British Airways vb.)
- Regülasyonlar, Yasal Sorumluluklar ve Uyumluluk
- KVKK, GDPR, ISO 27001, NIS2, DLP politikaları
- Yöneticinin veri koruma sorumluluğu nedir?
- Siber olay bildirimi zorunluluğu
- Denetim süreçlerinde yöneticinin rolü
- Sözleşmelerde siber güvenlik maddeleri
- Siber Riskin Finansal ve İtibari Etkileri
- Veri ihlallerinin ortalama maliyetleri
- Sigorta – neyi kapsar, neyi kapsamaz?
- Reputasyon kaybı örnekleri (müşteri güveni, medya baskısı)
- Güvenlik yatırımı bir maliyet değil, risk azaltma aracıdır
- ROI: Siber güvenlik harcamalarının iş değerine etkisi
- Kurumsal Siber Güvenlik Yapısına Genel Bakış
- CISO ve Bilgi Güvenliği ekibinin sorumlulukları

Yöneticilere Özel Farkındalık Eğitimi

Eğitim İçeriği

- SOC (Security Operations Center) nedir, nasıl işler?
- Olay müdahale ekipleri – kim, ne yapar?
- EDR, SIEM, DLP gibi sistemlerin yönetsel anlamı
- Tedarikçi yönetiminde siber güvenlik kontrolleri
- Kriz Anlarında Yöneticinin Rolü
- Olay anında yapılması / yapılmaması gerekenler
- Basına açıklama, çalışan bilgilendirmesi, paydaş yönetimi
- Olay Müdahale Planı (IRP) içinde yöneticinin pozisyonu
- Hukuk, BT ve üst yönetim koordinasyonu
- “Olay simülasyonu” egzersizlerinin önemi
- Yöneticiler İçin Pratik Siber Güvenlik Önlemleri
- Kişisel cihaz ve hesap güvenliği
- Güçlü parola yönetimi ve çok faktörlü kimlik doğrulama (MFA)
- Sosyal mühendislik saldırılarına karşı korunma
- İş e-postası dolandırıcılığına (BEC) dikkat
- Seyahat ve mobil cihaz güvenliği
- Yönetim Kararlarında Siber Güvenlik Faktörü
- BT projelerinde güvenlik gereksinimlerinin dikkate alınması
- Siber risklerin risk yönetimi ve iş sürekliliği planına entegrasyonu
- Güvenlik bütçelerinin oluşturulması ve doğru kaynak kullanımı
- Güvenlik KPI’ları ile durumu değerlendirme
- Raporlama ve Yönetici Panelleri
- Ne raporlamalıyım, nasıl değerlendirmeliyim?
- Risk temelli raporlama: Teknik değil iş diliyle özet
- Güvenlik skorları, olay istatistikleri, uyumluluk göstergeleri
- “Kırmızı – Sarı – Yeşil” modellemesiyle karar verme