EMA SECURITY

Bilgi Güvenliği 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

Bilgi Güvenliği Farkındalık Eğitimi

Eğitim Açıklaması

Saldırı Tespit ve Analiz Eğitimi, siber saldırıları erken tespit etme ve analiz etme becerisini kazandırmayı hedefleyen bir eğitim programıdır. Katılımcılar, siber tehditleri tanıma, log analizleri yapma ve saldırıların kökenini belirleme konusunda yetkinlik kazanacaklardır. Bu eğitim, siber güvenlik profesyonellerinin olayları hızlıca tespit etmelerini ve etkin bir şekilde analiz etmelerini sağlar. Ayrıca, saldırı türlerine göre doğru analiz yöntemlerini kullanmayı öğretir.

Eğitim Yeri

- Online
- Fiziksel

Eğitim Süresi

- 1 Gün

Eğitim Seviyesi

- Başlangıç

Bilgi Güvenliği Farkındalık Eğitimi

Eğitim İçeriği

- Bilgi Güvenliği Nedir?
- Bilginin tanımı: Gizlilik, bütünlük ve erişilebilirlik prensipleri
- Bilgi türleri: Kişisel veri, müşteri bilgisi, ticari sır, fikri mülkiyet
- Dijital ve fiziksel bilgi güvenliği ayrımı
- Neden önemlidir?
- Gerçek vaka: Basit bir şifrenin kuruma maliyeti
- En Sık Karşılaşılan Tehditler
- Sosyal Mühendislik: Telefonla parola isteme, sahte IT destekleri
- Phishing (Oltalama): Sahte e-postalar ve link tuzakları
- USB ve Taşınabilir Medya Tehlikeleri
- Zayıf Parola Kullanımı
- Fidye Yazılımları (Ransomware)
- Gizli Bilgi Sızdırma / Yanlış Paylaşım
- Günlük hayatla bağlantılı örnek senaryolar
- Parola Güvenliği
- Parola oluşturma kuralları
- Kurumsal ve kişisel hesaplar için farklı parola kullanımı
- Çok Faktörlü Kimlik Doğrulama (MFA)
- Parola yöneticisi kullanımı
- Şifreleri paylaşmamak neden bu kadar önemli?
- E-Posta ve İnternet Kullanımında Güvenlik
- E-posta ekleri ve linklere dikkat
- Şirket dışı paylaşım riskleri
- Kişisel e-posta hesabını işte kullanma riski
- Güvenli internet kullanımı: HTTPS, VPN, güvenilir siteler
- Wi-Fi güvenliği ve halka açık ağlarda dikkat edilmesi gerekenler
-

Eğitim İçeriği

- Cihaz Güvenliği
- İş bilgisayarı ve mobil cihazların fiziksel korunması
- Ekran kilidi ve otomatik kilit ayarları
- USB cihaz takarken nelere dikkat edilmeli?
- Yazılım ve güncelleme politikaları
- Güvnlik yazılımlarının önemini kavrama
- Olay Bildirimi ve Sorumluluk
- Şüpheli bir e-posta, dosya veya davranışla karşılaşıldığında ne yapılmalı?
- Bildirim yolları: Kime, ne zaman, nasıl?
- Bildirmemek de risktir: Geciken bildirimlerin sonuçları
- Çalışanların yasal ve kurumsal sorumlulukları
- Kurumsal Politikalar ve Uyum
- Bilgi güvenliği politikası nedir, ne işe yarar?
- Gizlilik sözleşmeleri ve KVKK kapsamındaki yükümlülükler
- İşten ayrılırken veri/devlet cihaz politikaları
- Güvenli uzaktan çalışma kuralları
- Dosya ve belge paylaşım politikaları
- Gerçek Hayattan Olaylar ve Dersler
- Örnek 1: Sahte e-posta ile yapılan ödeme dolandırıcılığı
- Örnek 2: USB cihaz ile sistemin ele geçirilmesi
- Örnek 3: Sosyal mühendislik ile parola ele geçirilmesi
- Örnek 4: Yanlış gönderilen dosya ile KVKK ihlali
- Tartışmalı senaryolar ve grup egzersizleri
- Güvenli Alışkanlıklar Kazanmak
- Güvenlik kültürü: “Benim başıma gelmez” düşüncesinden uzaklaşmak
- Sadece IT’nin değil, herkesin sorumluluğu
- Günlük küçük alışkanlıkların büyük fark yaratması
- Şüphe duy – sorgula – bildir: Güvenlik refleksi oluşturma
-