EMA SECURITY

Yönetilen İnsan Risk (xHRM) Hizmeti

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

Güvenlik Sıkılaştırma Hizmeti

Hizmet Tanımı

Human Risk Management (İnsan Risk Yönetimi) Hizmeti, organizasyonların insan kaynaklı siber güvenlik risklerini değerlendirmek, çalışanların farkındalığını artırmak ve güvenlik açıklarını minimize etmek için sunulan kapsamlı bir güvenlik yönetim yaklaşımıdır. Teknolojik güvenlik önlemlerinin yanı sıra, insan faktörünün siber tehditler üzerindeki etkisini analiz ederek organizasyonların güvenlik kültürünü geliştirmeyi amaçlar.

Bu hizmet kapsamında, çalışanların güvenlik farkındalık seviyesi ölçümlenir, sosyal mühendislik saldırılarına karşı dayanıklılıkları test edilir ve organizasyonun güvenlik politikalarına uyumluluğu değerlendirilir. Phishing (oltalama) testleri, parola güvenliği analizleri, sosyal mühendislik simülasyonları, bilinçlendirme eğitimleri ve güvenlik politikaları uyumluluk denetimleri gibi yöntemler kullanılarak insan faktörüne dayalı güvenlik açıkları tespit edilir.

Human Risk Management hizmeti, NIST Cybersecurity Framework, ISO 27001, CIS Controls, SANS Security Awareness ve GDPR/KVKK gibi uluslararası güvenlik standartları ve regülasyonlara uygun olarak yürütülmektedir. Çalışanların güvenlik bilincini artırmaya yönelik interaktif eğitimler, simülasyonlar ve sürekli farkındalık kampanyaları ile organizasyonun siber tehditlere karşı direnci artırılır.

Özellikle kimlik avı saldırıları (phishing), iç tehditler, güvenli parola kullanımı, veri sızıntısı, fiziksel güvenlik ihlalleri ve sosyal mühendislik saldırıları gibi insan kaynaklı tehditler ele alınarak, organizasyonların bu risklere karşı önlem alması sağlanır. Gerçekleştirilen risk analizleri sonucunda, organizasyona özel güvenlik farkındalık programları oluşturulur ve uygulanabilir aksiyon planları geliştirilir.

Hizmet, çalışanların bilgi güvenliği farkındalığını sürekli olarak artırmayı hedeflerken, yöneticilere ve güvenlik ekiplerine detaylı analiz ve raporlar sunarak, insan kaynaklı riskleri azaltmaya yönelik stratejik kararlar almalarına yardımcı olur. Organizasyonların daha güvenli bir çalışma ortamı oluşturmasını, güvenlik ihlallerini en aza indirmesini ve yasal uyumluluk gerekliliklerini yerine getirmesini sağlar.

Sonuç olarak, Human Risk Management (İnsan Risk Yönetimi) Hizmeti, siber güvenlikte en zayıf halka olan insan faktörünü güçlendirmeyi, çalışanları tehditlere karşı bilinçlendirmeyi ve organizasyonların insan kaynaklı siber risklere karşı proaktif önlemler almasını sağlayarak, güvenlik kültürünü sürdürülebilir bir şekilde geliştirmelerine katkıda bulunur.

Hizmete Ait Bileşenler

Risk Analizi ve Farkındalık Değerlendirmesi

İnsan Risk Yönetimi hizmeti, organizasyonun insan kaynaklı güvenlik açıklarını belirlemek için kapsamlı bir risk analizi süreciyle başlar. Çalışanların güvenlik farkındalık seviyeleri değerlendirilir, güvenlik politikalarına uyumları analiz edilir ve organizasyon genelinde güvenlik olgunluğu ölçümlenir.

Sosyal Mühendislik Testleri

Çalışanların sosyal mühendislik saldırılarına karşı direncini test etmek amacıyla oltalama (phishing), sahte destek çağrıları, fiziksel erişim testleri ve kimlik avı saldırı simülasyonları gibi yöntemler uygulanır. Bu testler, çalışanların güvenlik tehditlerine karşı farkındalık düzeyini artırmayı ve savunma reflekslerini güçlendirmeyi amaçlar.

Kimlik ve Erişim Güvenliği Değerlendirmesi

Organizasyon içindeki kimlik doğrulama süreçleri, erişim kontrolleri ve parola güvenliği analiz edilerek, insan kaynaklı yetkisiz erişim riskleri değerlendirilir. Zayıf parola kullanımı, çok faktörlü kimlik doğrulama (MFA) eksiklikleri ve yanlış yapılandırılmış erişim yetkilendirmeleri gibi potansiyel güvenlik açıkları tespit edilir.

Güvenlik Farkındalık Eğitimleri

Çalışanların bilinçlendirilmesi amacıyla etkileşimli eğitim programları, simülasyonlar ve siber güvenlik farkındalık atölyeleri düzenlenir. Bu eğitimlerde, kimlik avı saldırılarını tanıma, güvenli parola oluşturma, veri sızıntısını önleme ve sosyal mühendislik taktiklerine karşı korunma konularında bilgi verilir.

İç Tehdit Analizi

Organizasyon içinde kasıtlı veya kasıtsız veri sızıntıları, dikkatsizlik kaynaklı güvenlik ihlalleri ve yetkisiz erişim girişimleri gibi iç tehdit unsurları analiz edilir. Çalışanların güvenlik politikalarına uyumu izlenerek, potansiyel riskler değerlendirilir ve önleyici aksiyonlar geliştirilir.

Fiziksel Güvenlik Testleri

Ofis ortamlarında, veri merkezlerinde ve diğer fiziksel alanlarda yetkisiz giriş testleri, erişim kontrolü denetimleri ve güvenlik prosedürleri değerlendirmeleri gerçekleştirilir. Bu sayede, fiziksel güvenlik zafiyetleri belirlenerek güvenlik önlemlerinin iyileştirilmesi sağlanır.

Olay Müdahale ve Kriz Yönetimi Senaryoları

Gerçek bir siber saldırı durumunda çalışanların nasıl tepki verdiğini ölçmek için acil durum senaryoları, olay müdahale simülasyonları ve siber kriz tatbikatları gerçekleştirilir. Organizasyonun olay yönetim süreçleri test edilerek, iyileştirme önerileri sunulur.

Politika ve Uygunluk Değerlendirmesi

Organizasyonun mevcut güvenlik politikaları, uluslararası standartlar (ISO 27001, GDPR, KVKK, NIST vb.) ve regülasyonlarla uyumluluk açısından değerlendirilir. Güvenlik politikalarının güncellenmesi ve çalışanların bu politikalara daha etkin şekilde uyum sağlaması için öneriler geliştirilir.

İzleme ve Sürekli Gelişim

İnsan Risk Yönetimi hizmeti, düzenli değerlendirme ve takip testleri ile organizasyonun güvenlik farkındalığını sürdürülebilir hale getirmeyi hedefler. Çalışanlara periyodik farkındalık testleri uygulanarak, güvenlik kültürünün gelişimi izlenir ve organizasyonun güvenlik duruşu sürekli olarak iyileştirilir.

Mevcut Durum Analizi

İnsan Risk Yönetimi hizmeti öncesinde, organizasyonun insan kaynaklı güvenlik riskleri kapsamlı bir şekilde analiz edilir. Bu aşamada, çalışanların siber güvenlik farkındalık seviyesi, güvenlik politikalarına uyum düzeyi, sosyal mühendislik saldırılarına karşı duyarlılığı ve iç tehdit unsurları detaylı olarak değerlendirilir.

Mevcut güvenlik kültürü, organizasyon içinde uygulanan kimlik ve erişim yönetimi (IAM) politikaları, veri paylaşım süreçleri, parola yönetim alışkanlıkları ve güvenlik eğitim programları incelenir. Çalışanların yetkilendirme seviyeleri, kritik sistemlere erişim kontrolleri ve güvenlik ihlallerine karşı organizasyonun yanıt mekanizmaları analiz edilir.

Ayrıca, organizasyonun insan kaynaklı güvenlik risklerine karşı aldığı önlemler ve uyguladığı regülasyonlara (ISO 27001, NIST, KVKK, GDPR, HIPAA vb.) uyumluluğu gözden geçirilir. Potansiyel tehdit aktörleri ve organizasyonun maruz kalabileceği saldırı senaryoları belirlenerek risk tabanlı bir yaklaşım benimsenir.

Bu analiz sonucunda, çalışanların güvenlik bilinci artırılmasına yönelik stratejik bir yol haritası oluşturulur ve organizasyonun insan kaynaklı güvenlik zafiyetleri minimize edilerek güvenlik duruşunun güçlendirilmesi hedeflenir.

Strateji ve Yol Haritası Belirleme

İnsan Risk Yönetimi hizmetinde, organizasyonun insan kaynaklı güvenlik riskleri analiz edilerek stratejik bir yol haritası oluşturulur. Çalışan farkındalık eğitimleri, oltalama simülasyonları, erişim kontrollerinin güçlendirilmesi ve parola politikalarının iyileştirilmesi gibi önlemler belirlenir.

Ayrıca, ISO 27001, NIST, KVKK ve GDPR uyumluluğu sağlanarak güvenlik politikaları güncellenir. Sürekli iyileştirme prensibiyle güvenlik farkındalık programları düzenli olarak gözden geçirilir, böylece organizasyonun insan kaynaklı tehditlere karşı dayanıklılığı artırılır.

İnsan Risk Yönetimi Hizmeti Aşamaları

Hizmet, çalışan farkındalık seviyeleri ve sosyal mühendislik zafiyetlerinin analiz edilmesiyle başlar. Oltalama simülasyonları, parola güvenliği testleri ve erişim kontrol denetimleriyle riskler tespit edilir.

Sonrasında, farkındalık eğitimleri ve güvenlik önlemleri uygulanarak insan kaynaklı riskler minimize edilir. Testler tamamlandıktan sonra rapor hazırlanır ve iyileştirme önerileri sunulur. Son aşamada, alınan önlemler tekrar test edilerek etkinliği değerlendirilir.

İnsan Risk Yönetimi Hizmeti Metodolojisi

İnsan Risk Yönetimi (Human Risk Management) hizmeti, organizasyonların insan faktörüne bağlı siber güvenlik risklerini tespit etmek, analiz etmek ve minimize etmek amacıyla geliştirilmiştir. Hizmet, NIST, ISO 27001, CIS Controls ve SANS Security Awareness gibi uluslararası güvenlik çerçeveleri temel alınarak yürütülür. İlk olarak, organizasyonun insan kaynaklı güvenlik riskleri kapsamlı bir şekilde değerlendirilir. Çalışan farkındalık düzeyi, erişim yönetimi politikaları, güvenlik bilinci kültürü ve sosyal mühendislik saldırılarına karşı mevcut savunma mekanizmaları analiz edilir. Bu aşamada, test kapsamı belirlenerek insan faktörüne bağlı potansiyel tehdit alanları tespit edilir ve organizasyonun güvenlik duruşu ölçülür.

Keşif sürecinde, oltalama (phishing) simülasyonları, parola güvenliği testleri, sosyal mühendislik değerlendirmeleri, iç tehdit analizleri ve çalışanların güvenlik farkındalık düzeyini ölçen senaryolar uygulanır. Organizasyon içindeki riskli kullanıcı davranışları analiz edilerek bilinçsiz veri paylaşımı, zayıf parola kullanımı, yetkisiz erişim riskleri ve sosyal mühendislik saldırılarına karşı zafiyetler belirlenir. Bu süreçte, otomatik ve manuel teknikler kullanılarak risk analizi gerçekleştirilir ve organizasyonun insan faktörüne dayalı güvenlik açıklarına nasıl tepki verdiği ölçülür.

Sömürme (exploitation) aşamasında, çalışanların sahte e-postalara verdiği tepkiler, sosyal mühendislik senaryolarına karşı direnç seviyeleri, kimlik avı (phishing) saldırılarına karşı güvenlik farkındalıkları test edilir. Yetkisiz erişim elde etme, bilgi sızdırma ve hassas verilerin ele geçirilmesi gibi olası saldırı senaryoları değerlendirilerek insan kaynaklı güvenlik risklerinin etkileri gözlemlenir.

Test sürecinin sonunda, tespit edilen güvenlik açıkları detaylı bir rapor halinde sunulur ve risk seviyelerine göre sınıflandırılır. Organizasyonun insan kaynaklı riskleri en aza indirmesi için farkındalık artırıcı eğitimler, güvenlik politikalarının güçlendirilmesi, güvenli parola yönetimi, çok faktörlü kimlik doğrulama (MFA) uygulamaları ve teknik önlemler gibi kapsamlı iyileştirme önerileri sunulur. Ayrıca, uygulanan önlemlerin etkinliğini değerlendirmek amacıyla tekrar testler gerçekleştirilerek sürekli iyileştirme sağlanır.

Raporlama ve İyileştirme

İnsan Risk Yönetimi hizmeti kapsamında, çalışanların siber tehditlere duyarlılığı ve güvenlik farkındalık seviyesi analiz edilir. Sosyal mühendislik saldırıları, kimlik avı testleri ve parola güvenliği eksiklikleri değerlendirilerek riskler raporlanır ve önleyici aksiyon planları sunulur.

Olay sonrası analiz ile organizasyonun güvenlik politikalarının etkinliği ölçülür. Eğitimler, erişim kontrolleri ve parola politikaları güçlendirilerek çalışanların siber tehditlere karşı daha bilinçli ve dirençli hale gelmesi sağlanır.

Sıkça Sorulan Sorular (SSS)

İnsan Risk Yönetimi (HRM) nedir?

İnsan Risk Yönetimi, çalışanların siber güvenlik farkındalığını artırmak ve insan kaynaklı güvenlik risklerini azaltmak için geliştirilen bir hizmettir.

HRM neden önemlidir?

Çalışanlar, sosyal mühendislik saldırılarına ve kimlik avı tehditlerine karşı en savunmasız noktadır. HRM, bu riskleri azaltarak organizasyonun genel güvenliğini güçlendirir.

HRM kapsamında hangi testler yapılır?

Kimlik avı (phishing) saldırı simülasyonları, sosyal mühendislik testleri, parola güvenliği analizleri ve güvenlik farkındalık değerlendirmeleri gerçekleştirilir.

Kimlik avı testleri nasıl yapılır?

Gerçek saldırılara benzer şekilde kurgulanan e-posta, mesaj ve sahte giriş sayfaları ile çalışanların saldırılara nasıl tepki verdiği ölçümlenir.

HRM hizmeti kimlere yöneliktir?

Tüm çalışanlar, yöneticiler, BT ekipleri ve özellikle müşteri hizmetleri veya finans departmanı gibi hassas bilgilerle çalışan birimler için uygulanabilir.

HRM hizmeti organizasyonlara nasıl fayda sağlar?

Çalışanların güvenlik farkındalığını artırarak veri ihlallerini önler ve organizasyonun genel siber dirençliliğini güçlendirir.

HRM yasal ve sektörel uyumluluğu destekler mi?

Evet, GDPR, KVKK, ISO 27001, NIST ve benzeri güvenlik standartlarına uyumu güçlendirmek için tasarlanmıştır.

HRM sürekli bir süreç midir?

Evet, tehditler sürekli değiştiği için HRM düzenli eğitimler, testler ve güncellenen politikalar ile devamlı olarak uygulanmalıdır.

HRM hizmeti uzaktan çalışanları kapsar mı?

Evet, uzaktan çalışma politikalarına özel güvenlik farkındalık eğitimleri ve kimlik avı testleri uygulanabilir.