EMA SECURITY

Sızma Testleri Hizmeti

AI-Powered Offensive Services

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

Hizmet Tanımı

Sızma testleri (Penetration Testing), organizasyonların dijital varlıklarını olası saldırılara karşı korumak için sistematik olarak gerçekleştirilen, kontrollü saldırı simülasyonlarıdır. Bu hizmet kapsamında, kurumların ağları, sistemleri, uygulamaları ve fiziksel güvenlik önlemleri, saldırgan bakış açısıyla test edilerek güvenlik açıkları tespit edilir ve bu zafiyetlerin nasıl istismar edilebileceği değerlendirilir. Sızma testleri, yalnızca güvenlik açıklarını belirlemekle kalmaz, aynı zamanda kurumların güvenlik duruşunu geliştirmek için öneriler sunar.

Sızma testleri hizmeti, saldırı yüzeyini analiz etmek, zafiyetleri belirlemek, sömürme (exploitation) tekniklerini test etmek ve saldırının etkisini değerlendirmek gibi aşamalardan oluşur. NIST SP 800-115, OSSTMM, OWASP, PTES ve MITRE ATT&CK gibi uluslararası standartlara uygun olarak gerçekleştirilen testlerde, yetkisiz erişim girişimleri, ayrıcalık yükseltme, veri sızdırma, hizmet dışı bırakma (DoS) saldırıları ve yanlamasına hareket (lateral movement) gibi saldırı teknikleri kullanılır.

Bu hizmet kapsamında ağ, web ve mobil uygulamalar, kablosuz ağlar, veri tabanları, bulut sistemleri, IoT cihazları ve endüstriyel kontrol sistemleri (ICS/SCADA) gibi bileşenler test edilir. Beyaz kutu, gri kutu ve siyah kutu testleri gibi farklı yöntemler kullanılarak, iç ve dış tehdit senaryoları modellenir. Gerçekleştirilen testler sonucunda, organizasyonların güvenlik açıklarını kapatmaları ve tehditlere karşı daha dayanıklı bir siber güvenlik altyapısı oluşturmaları için detaylı teknik raporlar sunulur.

Sızma testleri, düzenli olarak gerçekleştirilmesi gereken bir güvenlik önlemidir. Siber tehditlerin giderek gelişmesi ve saldırganların yeni teknikler kullanması nedeniyle, organizasyonların güvenlik açıklarını sürekli olarak değerlendirmesi ve risklerini minimize etmesi gerekmektedir. Bu kapsamda, yasal ve sektörel uyumluluk gereksinimlerine (KVKK, ISO 27001, PCI DSS, GDPR, NIST) uygun şekilde gerçekleştirilen sızma testleri, güvenlik politikalarının güçlendirilmesine katkı sağlar.

Sonuç olarak, sızma testleri hizmeti, kurumların güvenlik açıklarını gerçek saldırganlardan önce tespit etmesini, savunma mekanizmalarını güçlendirmesini ve siber güvenlik stratejilerini sürekli olarak geliştirmesini sağlayarak, tehditlere karşı daha dayanıklı bir altyapı oluşturmasına yardımcı olur.

Hizmete Ait Bileşenler

Keşif ve Zafiyet Analizi

Sızma testleri hizmeti, hedef sistemlerin saldırı yüzeyini belirlemek için keşif süreciyle başlar. Açık kaynak istihbaratı (OSINT) teknikleri kullanılarak bilgi toplanır ve otomatik/manual taramalarla güvenlik açıkları tespit edilir.

Ağ ve Sistem Sızma Testleri

Kurumsal ağlar, sunucular ve güvenlik cihazları analiz edilerek güvenlik duvarlarının ve IDS/IPS sistemlerinin etkinliği test edilir. Yetkisiz erişim ve ağ içi yatay hareket (lateral movement) teknikleri uygulanarak saldırgan senaryoları simüle edilir.

Web ve Mobil Uygulama Güvenlik Testleri

OWASP Top 10 çerçevesinde gerçekleştirilen bu testlerde, SQL Injection, XSS, güvenli kimlik doğrulama açıkları gibi yaygın güvenlik zafiyetleri incelenir ve uygulamaların saldırılara karşı dayanıklılığı test edilir.

Kablosuz Ağ Güvenlik Testleri

Yetkisiz erişim girişimleri, WPA/WPA2/WPA3 şifreleme kırma, sahte erişim noktaları oluşturma (Evil Twin Attack) ve MITM (Man-in-the-Middle) saldırıları gerçekleştirilerek kablosuz ağ güvenliği değerlendirilir.

Sosyal Mühendislik Testleri

Çalışan farkındalığını ölçmek ve insan odaklı güvenlik açıklarını değerlendirmek amacıyla oltalama (phishing), telefon dolandırıcılığı (vishing) ve fiziksel güvenlik testleri yapılır. Çalışanların hassas verilere nasıl tepki verdiği analiz edilerek güvenlik farkındalığı artırıcı öneriler sunulur.

Zafiyet Sömürme (Exploitation) ve Yetki Yükseltme

Tespit edilen güvenlik açıkları istismar edilerek sistemlerde yetki yükseltme (privilege escalation) işlemleri gerçekleştirilir. Kurumsal ağ içerisinde yatay hareket edilerek hassas verilere erişim sağlanmaya çalışılır.

ICS/SCADA ve IoT Güvenlik Testleri

Test sonuçları teknik ve yönetimsel detaylarıyla birlikte raporlanır. Güvenlik açıklarının nasıl giderileceğine dair iyileştirme önerileri sunularak organizasyonun güvenlik duruşu güçlendirilir.

Raporlama ve Güvenlik İyileştirme Önerileri

Endüstriyel kontrol sistemleri (ICS/SCADA) ve IoT cihazları için özel güvenlik testleri uygulanarak kritik altyapılar ve bağlı cihazların güvenliği değerlendirilir. Siber saldırılara karşı dayanıklılığı artırıcı güvenlik önerileri geliştirilir.

Regülasyon ve Uyumluluk Değerlendirmesi

ISO 27001, PCI DSS, KVKK, GDPR, NIST ve COBIT gibi standartlar doğrultusunda güvenlik kontrolleri değerlendirilir. Uyumluluk açıkları belirlenerek yasal gereksinimlere uygunluk sağlanması için öneriler geliştirilir.

Doğrulama Testi ve Farkındalık Eğitimi

Zafiyetlerin giderildiğini doğrulamak için tekrar testler gerçekleştirilir. Çalışanlara yönelik güvenlik farkındalığı eğitimleri düzenlenerek organizasyonun uzun vadeli siber güvenlik stratejisi desteklenir.

Mevcut Durum Analizi

Sızma testleri hizmeti öncesinde, organizasyonun mevcut güvenlik durumu kapsamlı bir şekilde analiz edilir. Bu aşamada, ağ altyapısı, sistem mimarisi, güvenlik politikaları, erişim kontrolleri ve mevcut güvenlik çözümleri (firewall, IDS/IPS, antivirüs, SIEM vb.) değerlendirilerek potansiyel güvenlik açıkları belirlenir. Ayrıca, organizasyonun sektörel regülasyonlara (ISO 27001, PCI DSS, KVKK, GDPR vb.) uyumluluğu gözden geçirilir. Mevcut tehdit ortamı analiz edilerek, organizasyonun maruz kalabileceği saldırı vektörleri belirlenir ve risk tabanlı bir yaklaşım benimsenerek test kapsamı oluşturulur.

Strateji ve Yol Haritası Belirleme

Sızma testleri sürecinin etkili bir şekilde yürütülmesi için organizasyonun ihtiyaçlarına ve tehdit modeline uygun bir strateji geliştirilir. Testlerin kapsamı belirlenirken, kritik sistemler, veri varlıkları, iç ve dış tehdit unsurları göz önünde bulundurularak, siyah kutu (black box), gri kutu (grey box) veya beyaz kutu (white box) test yöntemlerinden en uygun olanı seçilir. Kullanılacak test araçları ve teknikleri belirlenerek, testin müşteri organizasyonuna zarar vermeden güvenli bir şekilde yürütülmesini sağlamak adına gerekli önlemler alınır. Ayrıca, test süreci boyunca raporlama ve iletişim planı oluşturularak, organizasyonun her aşamada bilgilendirilmesi sağlanır.

Sızma Testleri Hizmeti Uygulama Aşamaları

Sızma testleri hizmeti, belirlenen metodolojiye uygun olarak aşağıdaki aşamalar doğrultusunda gerçekleştirilir: İlk olarak, keşif ve bilgi toplama süreciyle organizasyonun sistemleri, ağ yapısı ve potansiyel açık noktaları analiz edilir. Daha sonra, zafiyet analizi yapılarak tespit edilen güvenlik açıkları, manuel ve otomatik araçlarla doğrulanır. Tespit edilen zafiyetlerin sömürülmesi (exploitation) aşamasında, saldırgan perspektifinden hareket edilerek yetkisiz erişim elde edilmeye çalışılır. Yetki yükseltme ve yatay hareket (lateral movement) teknikleri kullanılarak sistem içindeki diğer kaynaklara erişim sağlanmaya çalışılır. Test sürecinin ardından, tüm bulgular detaylı olarak raporlanır ve organizasyonun güvenlik açıklarını gidermesi için öneriler sunulur. Son aşamada ise, giderilen zafiyetlerin doğrulanması amacıyla tekrar testler gerçekleştirilerek güvenlik önlemlerinin etkinliği değerlendirilir.

Sızma Testleri Hizmeti Metodolojisi

Sızma testleri hizmetlerinin etkin bir şekilde yürütülebilmesi için OWASP Testing Guide, NIST 800-115 Teknik Güvenlik Testi Metodolojisi ve OSSTMM (Open Source Security Testing Methodology Manual) gibi uluslararası kabul görmüş standartlar temel alınarak kapsamlı bir metodoloji uygulanır. İlk olarak, organizasyonun mevcut güvenlik durumu analiz edilerek sistem mimarisi, ağ yapısı, güvenlik politikaları ve kimlik doğrulama mekanizmaları değerlendirilir. Bu aşamada, test kapsamı belirlenerek iç ve dış saldırı yüzeyi analiz edilir, kritik sistemler ve potansiyel zafiyetler tespit edilir.

Sızma testleri sırasında, pasif ve aktif keşif teknikleri kullanılarak bilgi toplama süreci yürütülür ve hedef sistemlerin zafiyetleri analiz edilir. Ardından, tespit edilen güvenlik açıklarının istismar edilebilirliği (exploitability) değerlendirilerek yetkisiz erişim elde etme, ayrıcalık yükseltme (privilege escalation), sistemler arası yatay hareket (lateral movement) ve veri sızdırma (data exfiltration) gibi saldırı senaryoları uygulanır. Manuel ve otomatik test araçları kullanılarak gerçekleştirilen bu aşamalar sayesinde, organizasyonun güvenlik önlemlerinin saldırganlara karşı ne kadar dayanıklı olduğu ölçülür.

Test sürecinin sonunda, tespit edilen güvenlik açıkları teknik detaylarıyla birlikte raporlanır ve risk seviyelerine göre sınıflandırılır. Organizasyonun güvenlik kontrollerini güçlendirmesi için zafiyetleri gidermeye yönelik teknik ve operasyonel öneriler sunulur. Ayrıca, güvenlik açıklarının doğrulama testleri gerçekleştirilerek alınan önlemlerin etkinliği değerlendirilir. Sızma testleri hizmeti, düzenli olarak tekrarlanarak organizasyonun siber tehditlere karşı savunma yeteneklerini geliştirmesine ve güvenlik duruşunu sürekli olarak iyileştirmesine katkı sağlar.

Raporlama ve İyileştirme

Sızma testleri hizmeti kapsamında gerçekleştirilen test süreçleri, tespit edilen güvenlik açıkları ve istismar edilen zafiyetler detaylı olarak raporlanır. Elde edilen bulgular, saldırı vektörleri, risk seviyeleri ve organizasyonun güvenlik kontrollerine verdiği tepkiler teknik ve yönetsel perspektiften analiz edilir. Test sonuçlarına dayanarak, güvenlik açıklarının giderilmesi için düzeltici ve önleyici aksiyon planları oluşturulur ve organizasyonun güvenlik seviyesini artırmaya yönelik öneriler sunulur.

Olay sonrası analiz çalışmaları ile, gerçekleştirilen testler sırasında organizasyonun güvenlik mekanizmalarının tehditlere nasıl tepki verdiği değerlendirilir. Elde edilen veriler doğrultusunda, güvenlik politikaları ve erişim kontrolleri güncellenerek benzer saldırıların tekrarlanmasının önüne geçilir. Sürekli iyileştirme yaklaşımıyla, organizasyonun güvenlik duruşu güçlendirilir ve gelecek tehditlere karşı daha dirençli hale gelmesi sağlanır.

Sıkça Sorulan Sorular (SSS)

Sızma Testi (Penetrasyon Testi) nedir?

Sızma testi, bir organizasyonun sistemlerini, ağlarını ve uygulamalarını güvenlik açıkları açısından değerlendirmek amacıyla yapılan kontrollü saldırı simülasyonudur. Güvenlik açıklarının istismar edilme potansiyeli test edilerek, olası risklerin minimize edilmesi hedeflenir.

Sızma Testi neden gereklidir?

Siber tehditler sürekli gelişmekte ve saldırganlar yeni zafiyetleri keşfetmektedir. Sızma testleri, güvenlik açıklarını proaktif olarak tespit edip kapatarak, organizasyonun saldırılara karşı korunmasını sağlar ve uyumluluk gereksinimlerini karşılamaya yardımcı olur.

Sızma Testleri hangi sistemleri kapsar?

Sızma testleri; ağ altyapıları, web ve mobil uygulamalar, bulut ortamları, kablosuz ağlar, IoT cihazları, veri tabanları ve iç sistemler gibi birçok farklı bileşeni kapsayacak şekilde gerçekleştirilebilir.

Sızma Testleri ne sıklıkla yapılmalıdır?

En iyi uygulamalara göre, organizasyonlar yılda en az bir kez sızma testi yaptırmalıdır. Ancak, büyük altyapı değişiklikleri, yeni sistemler veya uygulamalar devreye alındığında, siber tehdit ortamında önemli değişiklikler yaşandığında ek testler yapılması önerilir.

Sızma Testleri hangi güvenlik standartlarına uygun olarak yapılır?

Sızma testleri, OWASP, NIST, OSSTMM, PTES ve ISO 27001 gibi uluslararası güvenlik standartlarına uygun olarak gerçekleştirilir. Bu sayede, organizasyonların güvenlik politikaları en iyi uygulamalara göre değerlendirilir.

Sızma Testi sonrasında ne yapılmalıdır?

Sızma testi raporunda belirtilen güvenlik açıkları ve öneriler doğrultusunda düzeltici aksiyonlar alınmalı, sistemler güncellenmeli ve güvenlik politikaları iyileştirilmelidir. Ayrıca, tespit edilen risklere karşı sürekli izleme ve iyileştirme süreçleri uygulanmalıdır.