KATEGORİ 4 · SIZMA TESTLERİ

TS 13638 Standartlarında Kapsamlı Sızma Testi (Penetrasyon Testi) Hizmeti

TS 13638 Belgeli

TSE TS 13638 Sızma Testi Firma Belgesi'ne sahip, CEH/OSCP/CISSP sertifikalı kadroyla yürütülen; 8 aşamalı resmî metodolojiyle web, mobil, API, ağ, kablosuz ve SCADA katmanlarını kapsayan bağımsız teknik güvence.

sızma testi · penetrasyon testi · TS 13638 · OWASP · web uygulama güvenlik testi · API güvenlik testi

KATEGORİ
Sızma Testleri

TİPİK SÜRE
Kapsama göre 1–6 hafta · Ücretsiz doğrulama (re-test) dâhil

KİMLER İÇİN
İnternete açık uygulama ve servis işleten tüm kurumlar; BİGR/SGYM denetimine hazırlanan kamu ve kritik altyapı kuruluşları; PCI-DSS, ISO 27001 veya müşteri sözleşmeleri gereği periyodik test yükümlülüğü bulunan şirketler.

1 Hizmetin Tanımı

Bu hizmet; kurumunuzun bilişim sistemlerinin, ağ altyapısının, uygulamalarının ve verilerinin güvenliğini sağlamak, zafiyetleri teknik analizlerle tespit etmek ve bu zafiyetlerin giderildiğini doğrulamak amacıyla gerçekleştirilen bağımsız bir güvenlik denetimi faaliyetidir. TSE tarafından TS 13638 Sızma Testi Firma Belgesi'ne sahip ve uluslararası geçerliliği olan (CEH, OSCP, CISSP vb.) sertifikalı uzman kadromuz tarafından yürütülen bu denetim; kurumsal yönetişim, risk ve uyum süreçlerinize makul güvence sunar. MSSP operasyonlarıyla tam entegre çalışabilecek bir vizyonla tasarlanan süreç, güvenlik kontrollerinizin yalnızca tasarımda değil işletim seviyesinde de etkinliğini kanıtlamayı amaçlar.

2 Neden Gereklidir?

Güncel siber tehditlerin kurum ağlarına ve kritik altyapılara verebileceği potansiyel zararın, derinlemesine savunma (defense in depth) prensibine sadık kalınarak bağımsız bir gözle incelenmesi operasyonel süreklilik için zorunludur. Belirli bir sıralamada kullanılan düşük riskli açıklıkların kombinasyonundan kaynaklanan yüksek riskli istismar yollarının tespit edilmesi, ağ koruma cihazlarının olaylara karşılık verme kabiliyetlerinin ölçülmesi ve güvenlik yatırımlarının üst yönetime raporlanabilmesi adına bu testler kritik öneme sahiptir.

YAPTIRIM VE RİSK EŞİĞİ

Zafiyet ve olayların tespit edilip bildirilmemesi 7545 sayılı Kanun kapsamında 1.000.000 ₺ – 10.000.000 ₺ idari para cezasına konudur. Ayrıca BİGR ve SGYM denetimlerinde sızma testi bulguları zorunlu kanıt kalemi olarak aranır.

3 Yasal ve Normatif Dayanak

- TS 13638 Sızma Testi standardı
- 7545 sayılı Siber Güvenlik Kanunu
- Bilgi ve İletişim Güvenliği Rehberi
- EPDK EKS Güvenlik Usul ve Esasları
- ISO/IEC 27001 A.8.8
- 6698 sayılı KVKK m. 12
- OWASP metodolojileri

4 Sağladığı Katma Değer

Resmî metodoloji ile tam uyum

TS 13638 standardının zorunlu tuttuğu 8 aşamalı süreç (Ön İrtibat, Bilgi Toplama, Zafiyet Analizi, Tehdit Modelleme, Sızma, Sızma Sonrası, Raporlama ve Doğrulama) harfiyen işletilir.

Çok katmanlı saldırgan simülasyonu

Güvenlik duvarı dışındaki anonim bir saldırgandan (Siyah Kutu), iç ağa sızmış yetkisiz bir kullanıcıya (Gri Kutu) ve tam bilgiye sahip bir sistem yöneticisine (Beyaz Kutu) kadar tüm kullanıcı profilleri simüle edilerek riskler her yönüyle değerlendirilir.

Kanıta dayalı teknik raporlama

Sadece otomatik tarama araçlarına bağlı kalınmaz; uluslararası uzmanlıklara sahip denetçilerin manuel derinlemesine analizleri ile güvenlik mimarisindeki iş mantığı hataları sahada doğrulanır.

5 Hizmet Kapsamı ve Metodoloji

Genel bakış: 01 Ön İrtibat 02 Bilgi Toplama 03 Zafiyet Analizi 04 Tehdit Modelleme 05 Sızma 06 Sızma Sonrası 07 Raporlama 08 Doğrulama

KATMAN 1

Ağ ve Sistem Altyapısı Sızma Testleri

Dış ağ (İnternet/DMZ) ve yerel ağ (İntranet) üzerinde yanal hareket (lateral movement), yetki yükseltme ve zayıf yapılandırma testleri.

KATMAN 2

Uygulama Güvenlik Testleri

OWASP metodolojisine uygun olarak web, mobil, API / web servis ve opsiyonel olarak masaüstü uygulamalarının denetimi.

KATMAN 3

SCADA / Endüstriyel Kontrol Sistemleri Testleri

EPDK usul ve esaslarına tam uyumlu, operasyonel sürekliliği riske atmayacak özel metodolojilerle kritik altyapı cihazlarının incelenmesi.

KATMAN 4

Kablosuz Ağ ve İletişim Testleri

Kurumsal kimlik doğrulama, izolasyon zafiyetleri ve sahte erişim noktası (Rogue AP) analizleri.

KATMAN 5

DDoS ve Sosyal Mühendislik Testleri

Sistemlerin aşırı yük altındaki davranışlarının ölçülmesi ve personel farkındalığını hedef alan oltalama (phishing) simülasyonları.

6 Teslimatlar, Çıktılar ve Başarı Kriterleri

TESLİMATLAR VE ÇIKTILAR

- ✓ Sızma Testi Sonuç Raporu — TS 13638 formatına uygun; yönetici özeti, kapsam/IP bilgileri, risk derecelendirme tablosu (Acil'den Düşük'e 5 seviye) ve istismar kanıtlarını içeren detaylı teknik bölüm
- ✓ Doğrulama Testi (Re-Test) Raporu — bulguların giderilmesini takiben yapılan ücretsiz kontrol testi sonuç raporu

HEDEFLENEN ÇIKTI / BAŞARI KRİTERİ

- ✓ Siber güvenlik yatırım stratejileri, salt risk teorileri üzerinden değil; bizzat teknolojik sahada istismar edilmiş somut veriler üzerinden şekillendirilebilir.
- ✓ Tespit edilen zafiyetlerin risk ağırlıklarına göre önceliklendirildiği net bir Düzeltici ve Önleyici Faaliyet (DÖF) eylem planına sahip olunur.
- ✓ Regülatif kurumların (TSE, EPDK vb.) beklediği bağımsız güvenlik denetim gereksinimleri akredite bir hizmet aracılığıyla karşılanmış olur.

- ✓ Operasyonel Yönetim Belgeleri — TSE standartları gereği zorunlu kapsam belirleme formu, gizlilik taahhütnameleri, görev yazıları ve müşteri feragatnamesi
- ✓ Tüm çıktılar veri güvenliği standartlarına uygun olarak şifreli formda teslim edilir

7 Sık Sorulan Sorular

Test sırasında sistemlerimiz zarar görür mü?

Kapsam belirleme formunda kırılganlık eşikleri, test pencereleri ve durdurma kriterleri yazılı olarak mutabık kalınır. Üretim etkisi olabilecek testler (DDoS, EKS) yalnızca planlı pencerelerde ve yazılı onayla yürütülür.

Doğrulama testi ücretli mi?

Hayır. Tespit edilen bulguların kurum tarafından giderilmesini takiben yapılan re-test hizmet kapsamındadır ve güncellenmiş durum raporu teslim edilir.

Otomatik tarama ile sızma testi arasındaki fark nedir?

Otomatik tarama bilinen imzaları listeler; sızma testi bu bulguları zincirleyerek gerçek istismar yollarını ve iş mantığı hatalarını kanıtla ortaya koyar. Regülatif denetimlerde kabul edilen, ikincisidir.

8 Etiketler

sızma testi · penetrasyon testi · TS 13638 · OWASP · web uygulama güvenlik testi · API güvenlik testi · SCADA sızma testi · kablosuz ağ testi · oltalama simülasyonu · black box grey box

Bu hizmet, tam hizmet kataloğunun bir parçasıdır. Diğer 11 hizmet ve bütüncül paketler hakkında bilgi için Genel Broşür'e başvurabilirsiniz. Bu doküman bilgilendirme amaçlıdır; hukuki mütalaa veya taahhüt niteliği taşımaz.