SIZMA TESTİ HİZMETİ POLİTİKASI

1. AMAÇ VE KAPSAM

Bu politika, bilgi güvenliğini sağlamak amacıyla kurumların bilgi sistemleri üzerinde gerçekleştirilecek sızma testleri için temel prensipleri ve standartları belirlemek amacıyla oluşturulmuştur. Politika, TSE tarafından yayımlanan TS13638, TS ISO/IEC 27001, TS ISO/IEC 27002 ve TS ISO/IEC 27017 gibi bilgi güvenliği standartlarına uygun şekilde düzenlenmiştir.
Bu politika, aşağıdaki alanlarda gerçekleştirilecek sızma testlerini kapsar:
Ağ altyapıları

- Web ve mobil uygulamalar
- Veri tabanları
- Kablosuz ağlar
- Sosyal mühendislik
- Kaynak Kod Analizi
- Donanım ve IoT cihazları

2. İLKE VE ESASLAR

Yetkilendirme ve Onay:

- Sızma testi faaliyetleri, yalnızca yasal yetkilendirme ve hedef sistem sahibinin onayı ile gerçekleştirilir.
- Tüm süreç, test yapılan kurum ile imzalanan **Hizmet Sözleşmesi** ve **Gizlilik Anlaşması** çerçevesinde yürütülür.
- TS 13638 ile uyumlu prosedürler ve ilgili yasal düzenlemeler (KVKK, 5651 Sayılı Kanun) doğrultusunda hareket edilir.

Gizlilik ve Etik:

- Test sırasında elde edilen veriler ve bilgiler, yalnızca test amacıyla kullanılır ve hiçbir koşulda üçüncü şahıslarla paylaşılmaz.
- Gizlilik Anlaşması (Non-Disclosure Agreement - NDA) imzalanarak tarafların veri koruma yükümlülükleri netleştirilir.

Standardizasyon ve Kalite:

- Test metodolojileri, uluslararası standartlarla (OWASP, OSSTMM, PTES) uyumlu olacak şekilde planlanır ve uygulanır.
- Sızma testi süreçlerinde TSE tarafından önerilen güvenlik değerlendirme prosedürleri dikkate alınır.
- Test, yalnızca tanımlanan kapsam ve hedeflerle sınırlıdır.
- Sistemlerin iş sürekliliğine zarar vermemek için testler kontrollü bir şekilde gerçekleştirilir.

Risk Yönetimi:

- Test sırasında, sistemin işletim süreçlerine zarar verilmemesi için gerekli önlemler alınır.
- Elde edilen bulguların, kurumun iş sürekliliği üzerindeki etkisi değerlendirilir ve risk derecelerine göre sınıflandırılır.

3. SIZMA TESTİ SÜRECİNDE FİRMA TARAFINDAN GERÇEKLEŞTİRİLEN ADIMLAR

İlk Temas ve İhtiyaç Analizi

- **Müşteri ile İletişim:**
  Müşterinin sızma testi talebi alınır ve genel ihtiyaçları öğrenilir.
- **Bilgi Toplama:**
  Test yapılacak sistemin türü (web uygulaması, ağ altyapısı, mobil uygulama vb.), kapsamı ve genel durumu hakkında bilgi toplanır.

Teklif Hazırlama ve Sunma

- **Kapsamın Belirlenmesi:**
  Hangi sistemlerin/test türlerinin kapsam dahilinde olacağı netleştirilir.
  Testin derinliği (siyah kutu, gri kutu, beyaz kutu) ve süresi belirlenir.
- **Teklif Hazırlığı:**
  Müşterinin ihtiyaçlarına uygun bir fiyat teklifi hazırlanır ve testin kapsamı, zaman çizelgesi, kullanılacak metodoloji teklif dosyasında açıklanır.
- **Teklifin Onayı:**
  Müşteri teklifi inceler ve kabul ederse süreç bir sonraki adıma geçer.

Sözleşme ve Gizlilik Anlaşması

- **Hizmet Sözleşmesi İmzalanması:**
  Firma ile müşteri arasında yasal bağlayıcılığı olan bir hizmet sözleşmesi imzalanır. Bu sözleşmede:
  - Test kapsamı
  - Sorumluluklar
  - Hizmet bedeli gibi detaylar yer alır.
- **Gizlilik Anlaşması (NDA):**
  Test sırasında elde edilen tüm bilgilerin gizliliği için bir **Gizlilik Anlaşması** (Non-Disclosure Agreement) imzalanır.

Planlama ve Test Hazırlığı

- **Ekip Görevlendirme:**
  Testi gerçekleştirecek ekip üyeleri belirlenir (genellikle CEH, OSWE, TSE gibi sertifikalı uzmanlar).
- **Zaman Çizelgesi Hazırlama:**
  Testin başlangıç ve bitiş tarihleri müşteriyle mutabık kalınarak planlanır.
- **Erişim Bilgileri Talebi:**
  Müşteriden test için gerekli izinler ve erişim bilgileri talep edilir.
- **Test Planının Hazırlanması:**
  Testin hangi metodolojiye göre yapılacağı, kullanılacak araçlar ve hedefler içeren detaylı bir plan hazırlanır.

Sızma Testinin Gerçekleştirilmesi

- **Bilgi Toplama:**
  Hedef sistemin pasif ve aktif bilgi toplama yöntemleriyle incelenmesi.
- **Zafiyet Analizi:**
  Tarama araçları ve manuel analiz yöntemleriyle sistemdeki açıkların belirlenmesi.
- **İstismar:**

Tespit edilen zafiyetlerin kontrollü bir şekilde istismar edilmesi ve elde edilen sonuçların analiz edilmesi.

- **Etkilerin Analizi:**
  İstismar işleminin sistem üzerindeki etkileri değerlendirilir.

Raporlama ve Çözüm Önerileri

- **Rapor Hazırlama:**
  Test sırasında elde edilen bulgular, risk dereceleriyle birlikte detaylı bir şekilde belgelenir. Rapor, şu bölümleri içerir:
  - Genel test özeti
  - Tespit edilen zafiyetler ve bunların iş süreçlerine etkisi
  - İstismar yöntemleri
  - Önerilen çözüm adımları
- **Müşteri ile Paylaşım:**
  Hazırlanan rapor müşteriye teslim edilir ve gerekirse raporun sunumu yapılır.
- **Soru-Cevap:**
  Müşterinin rapor hakkında soruları yanıtlanır ve çözüm önerileri detaylandırılır.

Test Sonrası Destek

- **Düzeltme Çalışmalarının Takibi:**
  Müşteri tarafından uygulanan düzeltici önlemler izlenir.
- **Yeniden Test:**
  Müşteri talebi doğrultusunda düzeltmelerin etkinliği test edilir ve gerekirse rapor güncellenir.

Faturalandırma ve Sürecin Sonlandırılması

- **Fatura Kesimi:**
  Hizmet tamamlandıktan sonra belirlenen bedel üzerinden müşteriye fatura düzenlenir.
- **Hizmet Değerlendirmesi:**
  Müşteri memnuniyeti ölçülür ve süreç iç değerlendirme için analiz edilir.
- **Arşivleme:**
  Sözleşmeler, raporlar ve test sonuçları şirket prosedürlerine uygun şekilde arşivlenir.

4. SORUMLULUKLAR

- **Test Ekibi:**
  Testi gerçekleştiren uzmanlar, gerekli sertifikalara (TSE, CEH, OSWE, vb.) sahip ve yetkin olmalıdır.
- **Müşteri:**
  Test kapsamında sağlanacak sistem bilgilerini eksiksiz olarak paylaşmalıdır. Ayrıca test sırasında belirlenen zaman diliminde sistemin izlenmesine yönelik gerekli erişimleri sağlamalıdır.
- **Hizmet Sağlayıcı (Firma):**
  Tüm test süreçlerinde tarafsızlığı ve profesyonelliği sağlamakla yükümlüdür. Tespit edilen zafiyetlerin ve diğer bilgilerin gizliliğini korur. Sızma testi ile ilgili gerek kuruluş tarafından doldurulan anket, form vb. dokümanlar gerekse firma tarafından üretilen sızma testi sonuç raporu vb. dokümanlar gizlilik dereceli dokümanlardır. Bu dokümanlara gizlilik derecesini belirten işaret konmalı ve bu tür dokümanlar üretim, kullanım ve saklama aşamalarında hassasiyetleele alınmalı ve çalınma, yetkisiz erişim, kaybolma vb. risklere karşı korunmalıdır.

5. İLGİLİ STANDARTLAR VE YASAL DAYANAKLAR

- TS 13638: Bilgi Teknolojileri - Güvenlik Yönetim Sistemi - Sızma Testi Hizmetleri
- TS ISO/IEC 27001 - Bilgi Güvenliği Yönetim Sistemi
- TS ISO/IEC 27002 - Bilgi Güvenliği Kontrolleri
- TS ISO/IEC 27017 - Bulut Güvenliği Standartları
- 5651 Sayılı Kanun - İnternet Ortamında Yapılan Yayınların Düzenlenmesi
- Kişisel Verilerin Korunması Kanunu (KVKK)