	PROSEDÜR	Sayfa	:	1/2
		Doküman No	:	PR.08
		Revizyon No	:	00
		Revizyon Tarihi	:	-
		Yayın Tarihi	:	08.02.2021
KONU: SIZMA TESTİ PROSEDÜRÜ				

1. **AMAÇ**

Erzurum Teknik Üniversitesi Bilgi İşlem Daire Başkanlığı'nın domainindeki sunucu ve uygulamaların (web sunucular, e-posta sunucu, ftp sunucular, internet firewall vb.) düzenli olarak iç kaynaklar veya hizmet alımı ile sızma testlerinden geçirilmesi, testler sonucunda bulunan açıkların sistemlerden sorumlu Bilgi İşlem Daire Başkanlığı tarafından giderilmesini sağlamaktır.

2. **KAPSAM**

Erzurum Teknik Üniversitesi Bilgi İşlem Daire Başkanlığı'nın domain yapısındaki servis ve uygulamaları, sorumlu tüm Bilgi İşlem Daire Başkanlığı personellerini kapsar.

3. TANIMLAR

3.1. Servis/Uygulama: Kurum dışından veya içinden erişilen uygulamalardır.
3.2. Varlık Sahibi: Uygulama veya sunucunun sahibidir.
3.3. Tedarikçi (Firma): Sızma testini yapacak yetkili firmadır.
3.4. Sızma Testi (Pentest, Penetration Test): Sızma Testi sistem ve ağ güvenliğini sağlamak için mevcut güvenlik mekanizmalarının analiz edilmesi ve atlatılması çalışmalarını kapsar. Varlık sahibi ile birlikte organizasyonun ihtiyaçlarına göre kapsamı belirlenir.
3.5. Dış Ağ Sızma Testi: Organizasyonun internete bakan ara yüzleri test edilir. Bunlar genellikle web sayfaları, web uygulama sunucuları, ağ iletişim cihazları, güvenlik duvarı vb. gibi sistemlerdir.
3.6. İç Ağ Sızma Testi: İç ağdan gerçekleştirilen bu test iç ağa erişebilen saldırgan bakış açısı ile gerçekleştirilir.

4. **UYGULAMA**
4.1. Bilgi sistemleri ve uygulamaları, düzenli olarak sızma testinden geçirilir.
4.2. Periyodik dış penetrasyon testleri 1 yılı aşmayacak şekilde tekrarlanır.
4.3. Periyodik olmayan test istekleri Bilgi İşlem Daire Başkanlığı'na iletilerek başlatılabilir.
4.4. Bu testler aşağıdaki alanları kapsar ancak bunlarla sınırlı değildir. Kurumun/Uygulamanın yapısına göre riskler ve alanlar değişiklik gösterebilir.

- Web Uygulaması
- DNS Servisi
- DoS/DDoS
- Kablosuz Ağ cihazları
- Mobil Cihaz Güvenliği
- Sosyal Mühendislik
- Sunucu ve Servis Güvenliği
- Ağ ve İletişim Cihazları Testleri
- Firewall ve IDS/IPS Cihazları
- Sanallaştırma Ortamı Güvenlik Testleri
- Domain ve PC Güvenliği
- Veri tabanı Güvenlik Testleri

4.5. Sızma testi, Bilgi İşlem Daire Başkanlığı' nın onay verdiği kendi personeli ve/veya

yetkilendirdiği firmalar tarafından yapılır.

4.6. Çalışmayı yapacak personel veya firma ile test kapsamı üzerinde mutabakata varılmalıdır.

4.7. İhtiyaç varsa çalışma sırasında, personel veya firmaya gereken yetkiler verilir ve denetim sonunda kaldırılır.

4.8. Sızma testinin uygulamanın işleyişine zarar vermemesi için gerekli önlemler alınır ve zamanlaması ona göre seçilir.

4.9. Personel veya firma testi gerçekleştirir ve raporu Bilgi İşlem Daire Başkanlığı'na iletir, Bilgi İşlem Daire Başkanlığı raporu inceledikten sonra düzeltme aksiyonları için Düzeltici Faaliyet başlatır ve Üst yönetim bilgilendirilir.

4.10. Sızma testleri sonucunda oluşturulan raporlar sadece ilgili kişilerin erişimine açıktır.

4.11. Mevcut bilişim sistem ve uygulamaları üzerinde yeni risk oluşturma ihtimali olan bir değişiklik veya yeni bir entegrasyon yapıldı ise canlı sisteme aktarılmadan önce mutlaka teste tabi tutulur.

4.12. Sızma testi raporundaki bulgular, Bilgi İşlem Daire Başkanlığı'nın takibi altında giderilir ve yapılan iyileştirmeler firma üzerinden tekrar test edilerek doğrulanır.

4.13. Bulguların kapatılamadığı durumlarda ilgili açıklar Bilgi İşlem Daire Başkanlığı tarafından düzeltici faaliyetler tekrar planlanır, takibe alınır ve Üst Yönetim bilgilendirilir.

4.14. Düzeltici Faaliyet uygulandıktan sonra ilgili düzeltici faaliyet formu BGYS Yönetim Temsilcisine iletilir. BGYS Yönetim Temsilci yapılan faaliyeti yeterli gördüğü taktirde Düzeltici Faaliyet kapatır.

	HAZIRLAYAN	ONAYLAYAN
ÜNVANI	BGYS YÖNETİM TEMSİLCİSİ (DAİRE BAŞKANI)	GENEL SEKRETER
ADI SOYADI	Dr. Naci BAYRAK	Prof.Dr. Ahmet DUMLU
İMZA		