T.C
ERCİYES ÜNİVERSİTESİ REKTÖRLÜĞÜ
Bilgi İşlem Daire Başkanlığı

Sayı : 68056880-934.01-
Konu: Teklif Verilmesi Hk.

08/10/2024

Sayın.....

Kurum web sayfalarının siber saldırılara karşı güvenliğini sağlayan test ve benzeri şeyler için sızma testi hizmeti alımı yapılması gerekmektedir. 4734 Sayılı Kamu İhale Kanununun 22/d maddesi gereği (doğrudan temin) satın alınacak olan cihazın/yedek parça/hizmetin tarafınızdan temini mümkün ise **22/10/2024 tarihi saat 12.00'a** kadar Bilgi İşlem Daire Başkanlığı Satın Alma Bürosuna teklif verilmesi konusunda gereğini rica ederim.

Erman ALTAN
Şef

NOT:
1- Zamanında verilmeyen açık adres, vergi no kaşe ve imza olmayan teklifler değerlendirmeye alınmayacaktır.
2- Teklif zarfları kapalı olmalı, teklif konusu ve irtibattaki personelinin ismi zarfın üzerinde yazılı olmalıdır.
3- Teklif edilen ürünlerin markası ve modeli teklif mektubunda yazılmalıdır.
4- Teklif edilen ürünlerin birim fiyatı rakam ve yazı ile yazılacaktır.
5- Teklifler TL cinsinden KDV hariç verilecektir.
6- Teklif mektubunda teslim süresi belirtilecektir.
7- Postadaki ve kargodaki gecikmeler dikkate alınmayacaktır.
8- Teklif mektubunda "şartname hükümlerini kabul ediyorum" ibaresi bulunacak olup teknik şartnamede istenen bilgi ve belgeler varsa ilgili birime teslim edilecektir.
9-Alternatif teklif kabul edilmeyecektir.
10- Elektronik posta yoluyla gönderilen teklifler kabul edilecektir ***.
bidbsatinalma@erciyes.edu.tr adresine gönderilen tekliflerin değerlendirmesi için konusuna söz konusu alım işine verilen teklif olduğu yazılması gerekmektedir.
11-İdare alım yapıp yapmamakta serbesttir.
12-Tedarikçi gizlilik sözleşmesi ürünün üstünüzde kalmanız halinde imzalanıp yollanacaktır.

ADRES: mail:
Erü bilgi işlem daire başkanlığı (araştırma merkezleri ve laboratuvarları binası) eski kmyo Köşk mahallesi Sabahattin Zaim sokak no:4
Tel: +90 352 437 49 35 (0352) 207 66 66 -10222
Teknik şartname ilgili hususlarda;
İrtibat: YASİN BİLİR (yasinbilir@erciyes.edu.tr)

BİRİM FİYAT TEKLİF CETVELİ

İdarenin Adı :Bilgi İşlem Daire Başkanlığı
İşin adı : SIZMA TESTİ HİZMETİ ALIMI

Sıra	İş Kaleminin Adı ve Kısa Açıklaması	Miktar	Birim	Toplam Fiyat (kdv hariç)
1	Sızma testi hizmeti	1	adet	

Adı - SOYADI / Ticaret unvanı

Kaşe ve İmza
Vergi no:

*KDV HARİC FİYAT VERİLECEKTİR.

Köşk Mah. Kutadgu Bilig Sokağı No:6 38030 MELİKGAZİ / KAYSERİ
Tel: +90 352 437 49 35 (0352) 207 66 66 -10200 mail: bidbsatinalma@erciyes.edu.tr

ERCİYES ÜNİVERSİTESİ BİLGİ İŞLEM DAİRE BAŞKANLIĞI
SIZMA TESTİ HİZMET ALIMI
TEKNİK ŞARTNAMESİ

1. GENEL

1.1. İŞİN KONUSU

- Bu şartname Kurum bünyesindeki bilgi sistemlerinin güvenlik açıklarının tespiti amacıyla, mevcut bilgi güvenliği alt yapısının analizi, raporlanması, kullanıcı farkındalığının artırılması çalışmalarını içermektedir.

1.2. AMAÇ

- Sızma testinin hedefi Kurum'un sahip olduğu bilgi işlem altyapısının temel bileşenlerini oluşturan sunucular, ağ cihazları, uygulama sunucuları, veri tabanları gibi standart ekipman ve yazılımlar ile Kurum'a özel geliştirilmiş iş uygulamalarının güvenlik zafiyetlerinin tespit edilmesi, risk düzeylerinin belirlenmesi ve belirlenen risklerin en uygun bir biçimde ortadan kaldırılmasıdır.

1.3. KISALTMALAR

KURUM	Erciyes Üniversitesi Bilgi İşlem Daire Başkanlığı
YÜKLENİCİ	İşi Üstlenen Yüklenici
CISSP	Certified Information Systems Security Professional
CEH	Certified Ethical Hacker
OSCP	Offensive Security Certified Professional
TSE	Türk Standartları Enstitüsü
OSWE	Offensive Security Web Expert

1.4. KAPSAM

1.4.1. Bu şartname kapsamında aşağıdaki başlıklarda yer alan hizmetler alınacaktır:

- Sızma testleri ve raporlaması
- Sosyal Mühendislik (Oltalama) Testi ve raporlaması
- Kontrol testi ve raporlaması

1.4.2. Bu şartnamede tanımlanan hizmetlerin kapsamı, Erciyes Üniversitesi lokasyonlarında yer alan ve ulaşılan sistemlerdir.

1.5. İŞİN SÜRESİ

- Sözleşmenin imzalanmasından itibaren 30(otuz) takvim günüdür. 30 takvim günü içerisinde mevcut durum analizleri gerçekleştirerek envanter durumu, ağ ve sistem topolojileri ile raporlanacaktır.

1.6. YÜKLENİCİ YETKİNLİĞİ

1.6.1. Yüklenici'nin sunacağı hizmete benzer olarak Türkiye'de gerçekleştirdiği en az beş (5) adet referans hizmeti bulunmalıdır. Referans olarak gösterilecek hizmetlerin en az, madde 4'te verilen teknik detaylara denk Kurumlar olması gerekmektedir.

1.6.2. Referans hizmetlerine ilişkin belgeleri, Sızma testi ve Raporlamalar ile ilgili kontak kişisine ait iletişim bilgileri sözleşme aşamasında kuruma sunulmak zorundadır.

1.6.3. Yüklenici'nin tarihi geçerli ve TÜRKAK tarafından akredite edilmiş ISO 27001 Bilgi Güvenliği Yönetim Sistemi belgesi bulunmalıdır.

1.6.4. Yüklenici'nin Türk Standardları Enstitüsü, TS 13638/T2 "Bilgi Teknolojileri - Güvenlik Teknikleri - Sızma testi yapan Yüklenici" belgesi bulunmalı, belge A veya B sınıfı Yüklenici olduğunu göstermelidir. C sınıfı belge kabul edilmeyecektir.

1.6.5. Yüklenici'nin bu şartnamede tanımlanan hizmetler için görevlendireceği ekibi kendi bordrolu personeli olmalıdır. Hizmette görev alacak olan personel bilgilendirmeleri sözleşme aşamasında Yüklenici tarafınca yapılacak, açık kimlik ve sigorta bilgileri Kurum'a teslim edilecektir.

1.6.6. Sızma testi alt yükleniciye yaptırılamaz.

1.6.7. Yüklenici sektörde en az 5 (beş) yıldır faaliyet gösteriyor olmalıdır. Beş yıldır faaliyet gösterdiğini gösteren ilgili belgeyi Kurum'a teslim edecektir.

1.7. Personel Yetkinliği

1.7.1. Yüklenici'nin test ekibi için seçmiş olduğu her bir personelinin bilgi güvenliği ve sızma testi alanında en az 3 yıl tecrübesi bulunması ve bunu sözleşme aşamasında ibraz edebilmesi gereklidir.

1.7.2. Sızma testi yapacak personeller için Türk vatandaşı olma ve kamu hakkından mahrum bulunmama şartları aranır. Yüklenici sözleşme aşamasında bu durumu taahhüt eder.

1.7.3. Sızma testini yapacak Yüklenici'nin iş kapsamında kullanacağı personelinin aşağıda belirtilen sertifikalardan en az iki tanesine sahip olması gerekmektedir.

- OSCP, CISSP, OSWE, CEH ve TSE tarafından verilmiş olan "Kayıtlı Sızma Testi Uzmanı", "Sertifikalı Sızma Testi Uzmanı" ya da "Kıdemli Sızma Testi Uzmanı" sertifikaları.

2. SORUMLULUKLAR

2.1. İşi yapacak Yüklenici ve personelin sorumlulukları

2.1.1. İşbu şartname ile tanımlanan tüm yükümlülükleri yerine getirecektir.

2.1.2. Yapılacak tüm testlerin zamanlarını ve sürelerini Kurum ile belirleyecektir.

2.1.3. Yapılacak tüm testler Kurum ile koordineli bir şekilde gerçekleştirilecektir. Kurum yetkililerine bilgi verilmeden herhangi bir sızma testi çalışması yapılmayacaktır.

2.1.4. İşi yapacak personel taahhütlerini kısmen veya tamamen başkalarına devredemeyecektir.

2.1.5. Proje kapsamında hazırlayacağı ve Kurum'a sunacağı bütün dokümanları Türkçe olarak hazırlayacaktır.

2.1.6. Proje başlangıcında zaman planlaması yapılacak ve belirtilen zaman planına uygun şekilde proje tamamlanacak, zaman planında gecikme olmaması için gerekli önlemleri alacaktır.

2.1.7. Projeye işbu şartnamede belirtilen özelliklerde kaynakları atayacaktır.

2.1.8. Proje kapsamında en az bir proje yöneticisi Yüklenici tarafından atanacaktır.

2.1.9. Proje Yöneticisi, proje boyunca Kurum ile sürekli iletişim içerisinde olarak, gerekli koordinasyonu sağlayacaktır.

2.1.10. Proje Yöneticisi, proje planını, sözleşme imzalandıktan sonra 5 iş günü içinde Kurum'a teslim edecek ve planın Kurum'a teslim edildikten sonra 5 iş günü içinde Kurum'la karşılıklı mutabakat ile güncellenmesini sağlayacak ve Kurum'a onaylatacaktır.

2.1.11. Proje planı, yapılan testlerin hangi günlerde ve hangi saat aralıklarında yapılacağını net olarak içermelidir.

2.1.12. Yüklenici ile yapılacak gizlilik sözleşmesi sonrası süreçler başlatılacak olup, gizlilik sözleşmesi öncesi bilgi paylaşımında bulunulmayacaktır.

2.1.13. Yüklenici yaptığı testler esnasında kişisel bilgilere ulaşması durumunda bu bilgileri Kurum ile paylaşmamalı, sızma testi sonuç raporuna eklememeli ve bir kopyasını kendisine almamalıdır. Sızma test raporunda kullanıcı adı ve parolaları maskelenmelidir.

2.1.14. İşi yapacak personel elde edilen bilgilerin, matbu/elektronik belgelerin gizliliği, saklanması ve güvenliği konusunda gerekli önlemleri alacaktır. İşi yapacak personel, Kurum ile gizlilik sözleşmesi imzalayacaktır.

2.1.15. Yüklenici ve işi yapacak personel, Kurum bünyesinde yürütülmekte olan ISO27001 Bilgi Güvenliği Yönetim Sistemi standartlarına uyacağını taahhüt eder.

3. Sızma Testi Süreci

Sızma testi içeriği aşağıdaki başlıkları içerecektir.

3.1. Web Uygulama Güvenlik Testleri

3.2. Yerel Ağ Güvenlik Testleri

3.3. Kablosuz Ağ Güvenlik Testleri

3.4. Sosyal Mühendislik Testleri

3.5. Doğrulama Testi

3.6. Raporlama

3.1. Web Uygulama Güvenlik Testleri İçeriği

Yapılacak olan WEB uygulamaları güvenlik testleri OWASP-Top10'de yer alan açıklıklar başta olmak üzere aşağıdaki kontrolleri içermelidir.

3.1.1. Veri Kontrolleri

3.1.1.1. Girdi yönetimi

3.1.1.2. Çıktı yönetimi

3.1.1.3. Değiştirilen içeriğin tespiti

3.1.1.4. HTML etiketlerinin filtrelenmesi

3.1.1.5. SQL injection

3.1.1.6. Sunucu taraflı girdi denetimi

3.1.1.7. URL yönlendirmeler

3.1.1.8. XSS

3.1.1.9. HTTP yanıt bölme

3.1.2. Oturum Yönetimi

3.1.2.1. Giriş sonrası oturum bilgisi yenileme, oturum sabitleme

3.1.2.2. Çerezlerin içeriği

3.1.2.3. Oturum sonlandırma

3.1.2.4. Oturum bilgisinin URL içinde taşınması

3.1.2.5. Oturum çalma (Session riding)

3.1.3. CSRF

3.1.4. Kimlik yönetimi, doğrulama ve iş mantığı

- 3.1.4.1. Yetki artırımı-Yetki dışı işlem-Şifre politikaları
- 3.1.4.2. Bilinen hesap/şifre bileşenlerinin denenmesi
- 3.1.4.3. Basit kimlik doğrulama kullanımı
- 3.1.4.4. Kimlik doğrulamanın atlatılması
- 3.1.4.5. Path traversal
- 3.1.4.6. Bypass authorization
- 3.1.4.7. Privilege escalation
- 3.1.4.8. Uygulama mantığı kontrolleri

3.1.5. Web Servis Testleri

- 3.1.5.1. Web servislerin tespiti - Web servisi detay tarama - REST
- 3.1.5.2. SOAP
- 3.1.5.3. Ajax
- 3.1.5.4. Bilgi Sızdırma ve Ayar Yönetim
- 3.1.5.5. Yardım sayfaları -SSL kullanımı -HTML comment -Sunucu bilgisi
- 3.1.5.6. Ayrıntılı hata mesajları
- 3.1.5.7. Dosya uzantıları - Yedek dosyalar - Yönetici ara yüzü
- 3.1.5.8. Desteklenen HTTP metotları ve XST açıklığı
- 3.1.5.9. Sitenin SSL sertifikasının geçerlilik testi
- 3.1.5.10. Metadata kontrolleri

3.2. Yerel Ağ Güvenlik Testleri

3.2.1. Kurum'un yerel alan ağı ve uç noktalar olmak üzere Kurum'da kullanılan tüm ağ yapısı (sunucu, aktif cihaz, ağ anahtarı, uygulama, dns ve veri tabanı sunucuları vb.) için gerçekleştirilecektir.

3.2.2. Testler en az aşağıdaki kontrolleri içerecektir:

- 3.2.2.1. Sunucular üzerindeki erişilebilir servislerin belirlenmesi,
- 3.2.2.2. İşletim sistemi güvenlik açıklıklarının tespiti,
- 3.2.2.3. Uygulamaya özel güvenlik açıklıklarının kontrolü,
- 3.2.2.4. Kullanıcı tahmini ve parola kırma testleri,
- 3.2.2.5. Kritik dosya ve paylaşımların erişilebilirliği ve izinsiz kullanımının kontrolü,
- 3.2.2.6. Dosya sistemi üzerindeki, yönetici veya olması gerekenden yüksek yetkilere sahip servislerin kontrol edilmesi.
- 3.2.2.7. Kapsam dâhilinde yer alan sistemlerde erişilebilir servislerin belirlenmesi,
- 3.2.2.8. İşletim sistemi ve uygulama seviyesi güvenlik zafiyetlerinin kontrolü.

3.2.3. İletişim Altyapısı ve Aktif Cihazlar Sızma Testleri

3.2.3.1. Ağlarda MAC adresi tabanlı filtrelemenin olup olmadığı incelenecektir.

3.2.3.2. Tüm ağ cihazları açıklık bulma araçları ile taranacaktır.

3.2.3.3. Tespit edilen açıkların uygulanabilirlikleri sınanacaktır.

3.2.3.4. Cihazlar üzerinde açık olan Telnet, HTTP, FTP, SNMP, TFTP, SSH servislerine sözlük saldırısı veya kaba güç kullanılarak erişim sağlanmaya çalışılacaktır.

3.2.3.5. Aktif cihazlar için uzak/yerel erişim kontrolü, yönetim, kayıt ve kimlik doğrulama mekanizmaları incelenecektir.

3.2.3.6. Erişim sağlanan cihazlar üzerinden alınan bilgilerle diğer cihazlara erişilmeye çalışılacaktır.

3.2.3.7. Cihazlarda ortak parolanın kullanılıp kullanılmadığı test edilecektir.

3.2.3.8. Yüklenici çalışanları için kullanılan içerik filtreleme sistemleri atlatılmaya çalışılacaktır.

3.2.3.9. Yüklenici dışına açık yönetim ara yüzlerinin varlığı kontrol edilecektir.

3.2.4. E-posta Servisleri Güvenlik Testleri

3.2.4.1. E-posta sunucularının topolojik konumu incelenecektir.

3.2.4.2. Virüs tarayıcı ağ geçitlerinin sürüm bilgisi ve açıklarının tespit edilmesi

3.2.4.3. Relay zafiyetlerinin tespit edilmesi

3.2.4.4. E-posta sunucular üzerinde başka servislerin tespiti

3.2.4.5. E-posta sistemi kimlik doğrulama sisteminin denetimi

3.2.4.6. E-posta sunucusu üzerinde ilgili servislerin kontrolleri (IMAP, POP3)

3.2.4.7. Zafiyet taraması

3.2.4.8. İzin verilen eposta boyutu kontrolü

3.2.4.9. E-posta liste uygulamalarının zafiyet taramaları

3.2.5. Dns Servisleri Güvenlik Testleri

DNS sunucusunun alan yapılandırmasında yer alan kayıtlar ortaya çıkarılmaya çalışılacaktır. Bu kapsamda;

3.2.5.1. Sunucu üzerinden alan transferi (zone transfer) yapılmaya çalışılacaktır.

3.2.5.2. NXT ve NSEC kaynak kayıtları üzerinden bilgi elde edilmeye çalışılacaktır.

3.2.5.3. Netcraft, Google, Whois sorguları yapılarak Yüklenici alanında yer alan sunucular tespit edilmeye çalışılacaktır.

3.2.5.4. Sosyal mühendislik saldırılarında kullanılabilecek özel kodlanmış alan adları tespit edilmeye çalışılacaktır.

3.2.5.5. DNS sunucular için ön bellek zehirlemesi gerçekleştirilmeye çalışılacaktır. DNS sunucular üzerindeki kaynak kayıt girdileri incelenecektir.

3.2.5.6. DNS sunucular üzerindeki ters kaynak kayıt girdileri incelenecektir

3.2.5.7. DNS sunucuların sürüm bilgisi elde edilmeye çalışılacaktır

3.2.5.8. Kurum dışı alan isimleri sorgulanmaya çalışılacaktır

3.2.5.9. Sunucular üzerinde DNS dışında bir servisin çalışıp çalışmadığı incelenecektir

3.2.5.10. Güvenlik duvarında DNS sunucular için izin verilen portlar incelenecektir

3.2.5.11. DNS sunucuları güvenlik taramasına tabi tutulacaktır

3.2.5.12. DNS servisini veren yazılımın açıklıkları araştırılacaktır

3.2.6. Veri tabanı Sistemleri Güvenlik Testleri

3.2.6.1. Yüklenici sistemlerindeki veri tabanı uygulamaları ve bu uygulamaları üzerinde barındıran işletim sistemleri tespit edilerek, tespit edilen sistemlere erişimin açık olup olmadığı denetlenecektir. Erişimin açık olması halinde çeşitli tarama araçlarıyla veri tabanı versiyonu, üretici adı vb. bilgiler ele geçirilmeye çalışılacaktır.

3.2.6.2. Elde edilen veri tabanı sistem bilgileri kullanılarak, bu sistemlere yönelik kullanıcı adı ve parola deneme saldırıları yapılacaktır. Bu saldırılar sırasında, ön tanımlı kullanıcı adı ve parolalar ile birlikte Yüklenici'ye özel olabilecek ve tahmin edilebilir kullanıcı adı ve parolalar da denenecektir.

3.2.6.3. Veri tabanı kullanıcı adı ve parola saldırılarının başarısız olması durumunda, işletim sistemi seviyesinden erişim denemeleri yapılacaktır. Windows, Linux vb. ortamlar üzerinden sistem kullanıcıları ile veri tabanı uygulamasına bağlanılmaya çalışılacaktır

3.2.6.4. Parola deneme saldırılarının başarılı olması durumunda tespit edilen erişim bilgileriyle sistemlere bağlanılacaktır. Bağlanılan sistemlerde hangi hassas verilerin bulunduğu, kullanıcı adı, parola ve parolalara ait karmaşık özet verilerinin bulunup bulunmadığı denetlenecektir.

3.2.6.5. Görüntülenebilen kullanıcı adı ve parola özet bilgileri çeşitli araçlarla tespit edilmeye çalışılarak zayıf olarak belirlenmiş parolalar tespit edilecektir

3.2.6.6. Erişilebilen sistemlerde yama bilgisi kontrol edilecektir. Bilinen açıklıkları içeren ve gerekli güncellemeleri yapılmamış sistemlerde hak yükselme vb. saldırılarla erişim sağlanan kullanıcının hakları genişletilmeye çalışılacaktır.

3.2.6.7. Erişilebilen sistemlerden diğer erişilemeyen sistemlere tanımlanmış bağlantılar varsa bu bağlantılar kullanılarak diğer veri tabanı uygulamalarına geçilmeye çalışılacaktır.

3.2.6.8. Hassas veriler içeren sistemlere erişilmesi halinde yetki seviyesi arttırılmaya çalışılacaktır. Erişim bilgisi elde edilecek sistemlerin sayısı arttıkça, her sistem için yukarda bahsi geçen adımlar tekrarlanır ve mevcut tüm veri tabanlarının güvenliği bu şekilde kontrol edilecektir.

3.3. Kablosuz Ağ Güvenlik Testleri

3.3.1. Kuruluşta buluna kablosuz ağlar taranarak özellikleri keşfedilmeye çalışılacaktır.

3.3.2. Kablosuz ağlarda MAC adresi tabanlı filtrelemenin olup olmadığı incelenecektir.

3.3.3. Kablosuz ağlarda kullanılan şifreleme ayarları incelenecektir.

3.3.4. Tespit edilen ağlarda kablosuz ağ şifresi ele geçirilmeye çalışılacaktır.

3.3.5. Tespit edilen ağlarda trafik dinlenmeye çalışılacaktır.

3.3.6. Kablosuz ağ testlerinde izlenen metodoloji ve denenen yöntemler başarılı ya da başarısız olarak sızma testi raporunda ekran görüntüleri ile birlikte yer alacaktır.

3.4. Sosyal Mühendislik Testleri

3.4.1. Kurum çalışanlarının ilgisini çekebilecek ve Kurum içine sızmaya imkân tanıyacak nitelikte özenle hazırlanmış, Kurum içinden veya dışından gönderilecek e-postalar ile 1100 akademik ve 2400 idari Kurum çalışanına iletilmek üzere, 2 adet senaryo ile 1 adet test uygulanacaktır.

3.4.2. Test kapsamına alınması gereken kullanıcı bilgileri Yüklenici'ye Kurum tarafından verilecektir.

3.4.3. Hizmet kapsamında yürütülecek senaryolar Kurum ile birlikte belirlenecek ve onaylanmasından sonra Kurum tarafından belirtilecek olan gün ve saat aralığında iletilecektir.

3.4.4. Sosyal Mühendislik test sonuçları ayrıca raporlanacak, rapor içerisinde tıklama bilgileri (adet ve tıklayan kullanıcılara ait bilgiler) ile veri girişi yapan kullanıcı bilgileri bulunacaktır. Ayrıca raporda bir Yönetici Özeti hazırlanacak, istatistiksel bilgiler, Kurumun genel farkındalık durumuna yönelik bilgilendirmeler ve önerilere yer verilecektir.

3.4.5. Kullanıcıların yapmış olduğu veri girişlerine ait bilgiler hiçbir şekilde Yüklenici tarafınca saklanmayacak, örnek ekran görüntülerinin rapor içerisinde kullanılması durumunda verilere ait görüntüler maskelenerek rapora eklenecektir.

3.5. Doğrulama Testi

- Penetrasyon (Sızma) Testi Sonuç raporunun teslimi ve sunumunun gerçekleştirilmesinin ardından 6 ay sonra tespit edilen zafiyetlerin giderilip giderilmediğinin kontrol edilmesi maksadıyla bir doğrulama denetimi (kontrol testi) gerçekleştirilecektir.
- Doğrulama denetimi sonucunda yeniden ayrı bir rapor düzenlenmeyecek hangi bulguların kapatıldığı ve hangilerinin devam ettiği bir çizelge halinde Kurum'a teslim edilecektir.

3.6. Raporlama

3.6.1. Raporun gizlilik derecesi GİZLİ olarak belirtilecek ve dijital kopyası şifrelenmiş olarak güvenli bir şekilde paylaşılacaktır.

3.6.2. Şifrelenmiş sonuç raporunu açmak için gerekli olan parola alternatif bir yöntem belirlenerek (SMS vb.) paylaşılacaktır.

3.6.3. Sızma Testi Raporunda sistemde belirlenen güvenlik açıklarının özet açıklaması, bu açıkların taşıdıkları riskler (olası etkiler), risk seviyesi, açıkların giderilmesi için öneriler ve yapılması gerekenlerin detayları, referans kaynaklar tablolar halinde hazırlanacak ve sunulacaktır.

3.6.4. Test sonucunda hazırlanacak olan raporda;

- İncelenen sisteme ilişkin tespit edilen işletim sistemi/çalışan servis ve sürüm bilgileri,
- Tespit edilen güvenlik zafiyetine ait ekran görüntüsü,
- Zafiyetin istismar edilip edilemediğine dair manuel deneme yöntemi ve false-positive bilgilerin belirtilmesi,
- Her bir test adımında uygulanan yöntemler, kullanılan araçların belirtilmesi gerekir.
- Manuel olarak test edilmemiş zafiyetler ve bu zafiyetlerden oluşan raporlar teslim aşamasında kabul edilmeyecek ve testin tekrar gerçekleştirilmesi talep edilecektir. Sadece otomatik tarama araçlarının çıktılarından oluşan Sızma Testi Raporları kabul edilmeyecektir.
- Raporlarda Bulgu Kanıtları ve Saldırı Vektörü açıklamaları yazılacak, manuel olarak gerçekleştirilen işlemler adım adım ekran görüntüleri ile birlikte detaylı olarak açıklanacaktır.
- Sızma Testi Raporlarında sayfa numarası ve İçindekiler Tablosu bulunacaktır.
- Raporlanan bulgular kritiklik seviyelerine göre Kritik – Yüksek – Orta – Düşük bulgular olarak gruplandırılacak ve rapora bu sıra ile eklenecektir.
- Raporda, tespit edilen her güvenlik zafiyetine ait tabloda "Etkilenen Sistemler" kısmı oluşturulacak ve bu zafiyetten etkilenen tüm sistemler aynı zafiyet tablosu ile iletilecektir.
- Raporda, her bir sistem için bulunan zafiyetler o sistem ismi altında listelenecektir.
- Raporda, herhangi bir güvenlik zafiyetinin farklı bir zafiyet nedeniyle ortaya çıktığı tespit edilmişse ilgili zafiyet belirtilecektir.
- Raporlarda, Teknik Rapor kısmının dışında bir de Yönetici Özeti Raporu hazırlanacaktır. Yönetici Özeti raporunda istatistiksel veriler, sistemin mimari yapısına ait bilgilendirme ve genel görüşler, olası zafiyetlere bakılarak alt yapısal iyileştirme önerileri ve tavsiyelere yer verilecektir.
- Raporlamanın teslim edilmesinden sonra Kurumun isteği üzerine bulguların açıklanması ve giderilmesi hususunda online bir toplantı organize edilecektir.

4. Teknik Detaylar

Sızma testi yapılacak sistemlere ait sayısal veriler aşağıdaki gibidir.

- Web sitesi sayısı: 25
- Sunucu sayısı: 2 adet 0/24, 1 adet 0/22
- Dış IP'ler: 0/23
- Ağ alt yapı cihaz sayısı (switch, router, controller vb.): 7 Adet 0/24
- SSID sayısı: 2 Adet
- Sosyal mühendislik testi için kullanıcı sayısı: 3500

5. Diğer Hususlar

5.2. Gerçekleştirilecek çalışmalarda hizmet kesintisine yol açabilecek herhangi bir kontrol/test yapılmayacaktır. Testler sunucu veya uygulamalar üzerinde en az yük oluşturacak ve servis dışı kalmasına mahal vermeyecek şekilde gerçekleştirilecektir.

5.3. Sızma testi, sistemlere herhangi bir zararlı yazılım yüklenmeden yapılacaktır.

5.4. Sızma testi çalışması uzaktan yapılacaktır. Gerekli durumlarda fiziki olarak Erciyes Üniversitesi Bilgi İşlem Daire Başkanlığında yapılabilecektir.

5.5. Sızma testi sürecinde kullanılacak bilgisayarlara ait bilgiler kuruma önceden bildirilecek ve ilgili bilgisayarlar dışında başka bilgisayarlar kullanılmayacaktır.

5.6. Sızma testi sürecinde kullanılan bilgisayarlar üzerine usb bellek, harici hard disk vb. depolama araçları takılmayacaktır. Takılması zorunlu durumlarda Kuruma bilgi verilecek ve Kurumun izni dâhilinde takılacaktır.

5.7. Sızma testi sürecinde kullanılan bilgisayarlara ait hard disklerdeki tüm veriler güvenlik amacı ile iş bitiminde kalıcı olarak silinecektir.

5.8. Sızma testine black box yöntemi ile başlanacak olup black box sonucunda erişilemeyen sistemler için sızma ve zafiyet testlerinde kullanılması gerekecek olan test kullanıcı hesapları ve network izinleri kurum tarafından Yüklenicinin kullanımına verilebilecektir. Söz konusu bilgilerin verilip verilmeyeceğine Kurum karar verecektir.

5.9. Kurum'un onayı ile ilgili çalışmalar yapılacaktır. Yapılacak olan tüm çalışmalar planlı olacaktır.

5.10. İş sonucunda üretilmiş olan raporların tüm telif hakları Kurum'a ait olacaktır.

5.11. İş kapsamında kullanılacak olan bilgisayarlar, yazılım lisansları ve gerekli donanımlar Yüklenici tarafından temin edilecektir.

5.12. İş kapsamında kullanılacak olan işletim sistemi yazılımları, tarama yazılımları, uygulama sunucuları vb. yazılımlar ve lisanslar Yüklenici tarafından temin edilecektir. Kurum lisanslama ile ilgili herhangi bir yükümlülüğe girmeyecektir. Tüm lisans sorumluluğu yükleniciye aittir.

5.13. İş kapsamında sistemler üzerinde Yüklenici tarafından sızma ve zafiyet testleri, hem internet hem intranet üzerinden yapılacaktır. Yüklenici bu iş için ilave ücret talep etmeyecektir.

5.14. Cumhurbaşkanlığı Dijital Dönüşüm Ofisinin Yayınladığı Bilgi ve İletişim Güvenliği Rehberi 3.5.2.2 maddesi kapsamında; Bilgi güvenliği ve SOME personeline, siber olay veya bilgi güvenliği ihlal olayı tespiti ve raporlanması konularında online eğitim verilmelidir.

5.15. Sızma testi teklifler her bir kalem için birim fiyatını belirtecek şekilde verilmelidir.

3. Sızma Testinin Gizliliği

3.2. Yüklenici yaptığı testler sırasında Kurum çalışanlarının kişisel bilgilerine ulaşması durumunda bu bilgileri Kurum ile paylaşmamalı, sızma testi sonuç raporuna eklememeli ve bir kopyasını kendisine almamalıdır. Sızma testi raporunda kullanıcı adı ve parolaları maskelenmelidir.

3.3. Sızma testleri esnasında Yüklenici sadece Kuruma ait içeriklere erişim sağlayabildiğini göstermeli, bunun dışında Kuruma ait içeriklerin tamamına erişim sağlayarak tüm içeriği kopyalamamalı ve üçüncü taraflar ile paylaşmamalıdır. Yüklenicinin içeriklere erişim sağladığını gösterebilmesi için gerekiyorsa örnek olarak birkaç ekran görüntüsü alabilir.

3.4. İş başlangıcında Kurum tarafından Yükleniciye verilen bilgi, dokümanlar vb. ve iş sonunda Yüklenici tarafından hazırlanan raporlar, çıktılar, ekran görüntüleri vb. Kuruma tesliminden sonra Yüklenici tarafından kesinlikle depolanmayacak ve 3. Taraflarla paylaşılmayacaktır. İşlerle ilgili tüm bilgiler (network topolojileri, kullanılan protokol bilgileri, güvenlik zafiyetleri, raporlar vb.) aksi yazılı olarak

belirtilmedikçe 'GİZLİ' olarak kabul edilecektir.

3.5. Sızma testi sonucunda bulunan zafiyetler ve oluşturulan rapor diğer Kurumlara gösterilemez.

3.6. Yüklenici iş ile ilgili olarak elde ettiği her türlü bilgi ile belgeleri özel ve gizli tutacak. Kurumun önceden yazılı izni olmaksızın kurumumuza ait herhangi bir detayı ifşa etmeyecek veya yayınlamayacaktır. Türk yargı mercilerinin kararları saklı kalmak kaydı ile sözleşmenin amaçları doğrultusunda herhangi bir ifşa veya yayınlama gerekliliği konusunda bir uzlaşmazlık ortaya çıkarsa Kurum'un bu konudaki kararı nihai olacaktır. Gizlilik yükümlülüğü, teknik şartnamedeki yükümlülüklerin herhangi bir nedenle sona ermesinden sonra da devam eder.

Muhammed Seyfullah DEMİR
Mühendis

Yasin BİLİR
Mühendis

Mustafa ŞİMŞEK
Bilgisayar İşletmeni

T.C. ERCİYES ÜNİVERSİTESİ
BİLGİ İŞLEM DAİRE BAŞKANLIĞI
SIZMA TESTİ HİZMET SÖZLEŞMESİ

Madde 1- Sözleşmenin Tarafları

Bu sözleşme, bir tarafta Erciyes Üniversitesi Bilgi İşlem Daire Başkanlığı ile diğer tarafta Yetkili Firma arasında aşağıda yazılı şartlar dâhilinde akdedilmiştir.

Madde 2- Tanımlar

İdare: Erciyes Üniversitesi Bilgi İşlem Daire Başkanlığını ifade eder.

Yetkili Firma: İdare tarafından işin ihale edildiği ve sözleşme imzalanan gerçek veya tüzel kişiyi ifade eder.

Madde 3- Taraflara İlişkin Bilgiler

3.1. İdare adresi : Erciyes Üniversitesi Bilgi İşlem Daire Başkanlığı,38039 Kayseri / Türkiye
Tel no : 0352 315 26 00
Faks no : 0352 437 83 81
Elektronik posta adresi :bidb@erciyes.edu.tr

3.2.Yetkili Firma tebligat adresi : .....
Tel no : .....
Faks no : .....
Elektronik posta adresi : ..... dir.

3.3.Her iki taraf madde 3.1. ve 3.2.'de belirtilen adreslerini tebligat adresi olarak kabul etmişlerdir. Adres değişiklikleri usulüne uygun şekilde karşı tarafa tebliğ edilmedikçe en son bildirilen adrese yapılacak tebliğ ilgili tarafa yapılmış sayılır.

3.4. Taraflar, yazılı tebligatı daha sonra süresi içinde yapmak kaydıyla, elden teslim, posta veya posta kuryesi, faks veya elektronik posta gibi diğer yollarla da bildirimde bulunabilirler.

Madde 4- İş Tanımı

4.1. Bilgi İşlem Daire Başkanlığı bünyesinde bulunan bilgi sistemlerinin güvenlik açıklarının tespiti, mevcut bilgi güvenliği alt yapısının analizi, raporlanması, kullanıcı farkındalığının artırılmasını kapsamaktadır.

Madde 5- Yükümlülükler

5.1. Yetkili Firma, bu sözleşme konusu taahhütlerinin yerine getirilmesi için yapılacak faaliyetlerde ve tüm hizmetlerin ifasında yürürlükte bulunan tüm mevzuata, Bilgi İşlem Daire Başkanlığı tarafından kabul edilecek ve Yetkili Firmaya yazılı olarak iletilecek bütün prensiplere, yönergelere ve talimatlara uyacaktır. Yetkili Firmanın, kendisine tebliğ edilecek prensip, yönerge ve talimatlara itiraz etmek hakkı bulunmamaktadır. Yetkili Firma, iş bu sözleşmenin çeşitli maddelerinde yer alan yükümlülüklerine ilave olarak işlere gereken özen ve ihtimamı göstermeyi, sözleşme konusu hizmeti/işi, sözleşme dokümanına göre belirlenen süre, miktar ve bedel dahilinde gerçekleştirmeyi ve oluşabilecek kusurları sözleşme hükümlerine uygun olarak gidermeyi kabul ve taahhüt eder.

5.2. Bu sözleşme ve eklerinde gün olarak anılan tüm süreler takvim günü esasına göredir. Bu sürelerin hesaplanmasında, havanın fen ve tekniğin icaplarına göre çalışmaya uygun olmayan dönemleri ile resmi tatil günleri dikkate alındığından bu nedenlere dayanılarak ayrıca süre uzatımı verilemez.

5.3. Yetkili Firma, sızma testi saldırı simülasyonları sırasında oluşabilecek hizmet aksaklığı, sistem yüklenmeleri gibi olumsuz durumlarda Bilgi İşlem Daire Başkanlığının bildirmesini beklemeden testi durduracak ve Bilgi İşlem Daire Başkanlığına bilgi verecektir.

5.4. Sızma testleri, canlı ortamda yapılacak olup doğabilecek her türlü veri kayıpları/değişikliği vb. olmak üzere zararlardan, Bilgi İşlem Daire Başkanlığı sorumlu değildir.

5.5. Sızma testleri, canlı ortamda yapılması sebebi ile oluşabilecek her türlü aksaklık ve problemlerin giderilmesinde Yetkili Firma, İdareden herhangi bir arıza/ problem bildirilmesi ile derhal testi durdurur ve sorunun giderilmesine ilişkin çözümüne yönelik çalışmaları başlatmayı kabul eder.

5.6. Yetkili Firma, teslim edeceği raporları pdf ve word formatları halinde dijital kopyası şifrelenmiş olarak teslim edecek. Şifrelenmiş sonuç raporunu açmak için gerekli olan parola alternatif bir yöntem belirlenerek (SMS vb.) paylaşılacaktır.

5.7. Sızma testi yapacak personeller için Türk vatandaşı olma ve kamu hakkından mahrum bulunmama şartları aranır. Yüklenici sözleşme aşamasında bu durumu taahhüt eder.

5.8. Yetkili Firma, teknik şartnamede belirtilen tüm şartları eksiksiz olarak yerine getirecektir.

Madde 6- GİZLİLİK

6.1.Tarafların veya çalışanlarının doğrudan veya dolaylı olarak elde ettikleri veya edecekleri, iç işleyişe, çalışanlarla ilgili bilgilere, varlıklara, finansal ve mali yapılarına, stratejilerine, pazarlama planlarına ve projeksiyonlara, taraf oldukları sözleşmelere resmi ve özel kurum ve kuruluşlardaki kayıtlarına ilişkin ilgili tüm teknik verilere ve/veya yürütülen bütün projelere, taşınmazlara, elektronik formattaki her türlü ürün, teknoloji, tasarım, program, buluş, formül, model, derleme, cihaz, yöntem, teknik, süreç, yazılım, marka, patent, öğrenci ve personel verilerine vb. ilişkin tüm yazılı, sözlü ve görsel bilgi ve belge ile Taraflardan birinin şu an için bildiği veya mülkiyetinde olan

veya bundan sonra öğreneceği veya edineceği, genel olarak bilinmemesi ve ifşasından ya da kullanımından ekonomik değer ve imaj kaybı elde edilebilecek başka kişiler tarafından meşru yollarla kolayca ulaşılamaması nedeniyle fiili veya potansiyel ekonomik değere sahip olması veya kuruma özel kalması gereken ve bilinmesi durumunda bilgi güvenliği zafiyetleri oluşabilecek olan her türlü bilgi, belge ve görsel doküman "Gizli Bilgi" olarak kabul edilmektedir.

6.2. Bu kapsamda Yetkili Firma, çalışması esnasında İdare varlıklarının marka, model, adet, hiyerarşik yapılanması, web sayfası ve veri tabanı kayıtları ile tüm İdare altyapı varlıkları, süreçleri vb. İdareye ait Gizli Bilgi olarak kabul eder.

6.3. Yetkili Firma, bu çalışmalar esnasında İdarenin yazılı onayı olmaksızın depolama yapmayacak, üçüncü şahıs, kuruluş ve kişilere yazılı veya sözlü olarak kesinlikle bilgi paylaşımında bulunmayacak, bu verilerin üçüncü kişilerin eline geçmemesi ve ifşa edilmemesi için her türlü tedbiri azami önlemi alacağını kabul, beyan ve taahhüt etmektedir. Paylaşımda bulunduğu takdirde gerekli yasal işlem başlatılacaktır. İdare'nin uğramış olduğu maddi ve manevi zararlar Yetkili Firmadan talep edilecektir.

6.4. Yetkili Firma, tüm hizmetlerini sunarken yönettiği verilerin her türlü güvenliğinden en üst seviyede sorumludur. Hiçbir veri asla izinsiz kullanılamaz, çoğaltılamaz, dağıtılamaz, anonimleştirilemez ve yayınlanamaz. Bu kapsamda Yetkili Firma, bu çalışmalar esnasında edindiği her türlü Gizli Bilgileri; koruyacağını, ticari ilişkinin amaçları dışında kullanmayacağını ve Gizli Bilgiyi bilmeye mutlaka ihtiyacı olan yetkili çalışanlarla sınırlı tutacağını kabul, beyan ve taahhüt etmektedir. Bu hükme aykırı bir durum karşısında İdarenin yasal hakları mahfuzdur.

6.5. Verilen hizmet kapsamında ekran görüntülerinin elektronik ortamlarla (WhatsApp, E-Posta, vb.) 3. kişilerle paylaşılması kesinlikle yasaktır.

6.6. Yetkili Firma, işbu Sözleşme çerçevesinde yükümlülüklerine aykırı davranmaları halinde doğacak zararlardan doğrudan sorumlu olacaklarını peşinen kabul, beyan ve taahhüt etmektedir.

6.7. Yetkili Firma ve sızma testini gerçekleştirecek firma personeli ayrı ayrı işe başladıktan sonra 5 gün içerisinde İdarenin vereceği Gizlilik Sözleşmesini imzalayarak İdare'ye teslim edecektir.

Madde 7- Cezalar ve Kesintiler

7.1. Yetkili Firma hizmeti aksattığı takdirde ve Bilgi İşlem Daire Başkanlığı tarafından yapılan ihtara rağmen 5 takvim gününü aşması halinde gecikilen her takvim günü için sözleşme bedelinin %0,5 (binde 5) oranında gecikme cezası ödemekle yükümlüdür. Bu gecikme cezası, ayrıca protesto çekmeye gerek kalmaksızın, Yetkili Firmaya yapılacak ödemelerden mahsup ya da doğrudan Yetkili Firmadan talep edilebilecektir. Bu cezaların ödenmesi, Yetkili Firma'yı taahhütlerini yerine getirmekten kurtarmaz. KDV, cezalara ayrıca eklenir. Hizmet ve destek yükümlülüğünün yerine getirilmesindeki gecikme, ihtar süresini aşması halinde, ayrıca protesto çekmeye gerek kalmaksızın sözleşme geriye etkili olarak feshedilir. Bilgi İşlem Daire Başkanlığının işbu fesih nedeniyle uğradığı zararı talep etme hakkı saklıdır.

7.2. Yetkili Firma sözleşme süresince sızma testinden doğan majör durumlarda İdare, Yetkili Firmaya arızayı/problemi tebliğ ettiği tarihten itibaren en geç 8 saat içerisinde arızayı Yetkili Firma giderecek veya geçici bir çözüm ile sistemin çalışabilirliğini devam ettirecektir. Alınan sürede Yetkili Firmanın hatası, ihmalinden dolayı meydana gelen hasarlardan, veri kayıplarından vb. Yetkili Firma sorumludur. Verilen sürede problemi çözülmeyen her iş kalemi için Yetkili Firmadan sözleşme bedelinin %0,1 (Binde biri) oranında cezai müeyyide uygulanacaktır.

Madde 8- Kontrol Teşkilatı, Görev ve Yetkileri

8.1. İşin, sözleşme ve teknik şartnamede tespit edilen standartlara (kalite ve özelliklere) uygun yürütülüp yürütülmediği İdare tarafından görevlendirilen kontrol görevlileri aracılığıyla denetlenir.

Madde 9- İşin Yürütülmesine İlişkin Kayıt ve Tutanaklar

9.1. İşin yapıldığına dair Yetkili Firma tarafından düzenlenen sızma testlerinin sonuçlarını, işin süresinin bitimini beklemeden düzenli aralıklarla en az 4 defa İdare'nin görevlendirileceği personellere bilgi mahiyetli online olarak anlatılacaktır.

9.2. Yetkili Firma sızma testlerini 30 gün içerisinde teknik şartnameye uygun ve eksiksiz bir şekilde bitirecektir.

9.3. Yetkili Firma sızma testi raporlarını teknik şartnameye uygun bir şekilde düzenleyip gerekli güvenlik önlemlerini alarak İdareye teslim edecektir.

9.4. Teknik şartnamede İdarenin 3.6 maddesi ile belirtiği sürede Yetkili Firma doğrulama testlerini yapacak ve raporlayacaktır.

Madde 10- Teslim, Muayene ve Kabul İşlemlerine İlişkin Şartlar

10.1. Madde 9 ile belirtilen hükümlerin tamamı eksiksiz bir şekilde yerine getirilecektir.

10.2. İdarenin sızma testi raporlarında raporlama şeklinde değişiklik talebi olması durumunda gerekli değişiklerin yapılacaktır.

10.3. Teknik şartnamede İdarenin 5.7 maddesi ile belirtiği hüküm yerine getirilerek tutanak altına alınarak İdareye iletilecektir.

Madde 11- Sözleşmenin Türü ve Bedeli

11.1. Bu sözleşmenin bedeli .....TL+KDV dir.

Madde 12- İşin Yapılma Yeri, İşyeri Teslim ve İşe Başlama Tarihi

12.1. İşin yapılma yeri: Sızma testi çalışması uzaktan yapılacaktır. Gerekli durumlarda fiziki olarak Erciyes Üniversitesi Bilgi İşlem Daire Başkanlığında yapılabilecektir.

12.2. Uzaktan çalışmalarda teknik şartnamede belirtilen 5.5 ve 5.6 maddeleri ile belirtilen hükümler yerine getirilecektir.

12.3. Bu sözleşmenin konusu olan iş ..... tarihinde başlar ve ..... tarihinde son bulur.

Madde 13- Ödeme Yeri ve Şartları

13.1. Yetkili Firma, gerek sözleşme süresi, gerekse uzatılan süre içinde, sözleşmenin tamamen ifasına kadar, vergi, resim, harç ve benzeri mali yükümlülüklerde artışa gidilmesi veya yeni mali yükümlülüklerin ihdası gibi nedenlerle fiyat farkı verilmesi talebinde bulunamaz.

13.2. Yetkili Firma yapılan işe ilişkin hak ediş ve alacaklarını İdare'nin yazılı izni olmaksızın başkalarına devir veya temlik edemez.

Madde 14- Son Hüküm

14.1. Bu sözleşme on dört (14) maddeden ibaret olup, İdare ve Yetkili Firma tarafından imzalanması ile yürürlüğe girer. ..... tarihinde imza altına alınarak bir (1) nüsha olarak düzenlenmiştir. (Yetkili Firma tarafından istenmesi durumunda, sözleşmenin bir (1) nüsha fotokopisi Yetkili Firma'ya verilecektir.)

Yetkili Firma

İdare
Tayyip ÖZCAN
Bilgi İşlem Daire Başkan V.