Evrak Tarih ve Sayısı: 28.05.2024-E.435182

T.C.
GAZİOSMANPAŞA ÜNİVERSİTESİ REKTÖRLÜĞÜ
Bilgi İşlem Daire Başkanlığı

Konu : Teklife Davet

Üniversitemiz Bilgi İşlem Daire Başkanlığı kurumsal bilgi sistemlerinin güvenliğini artırmaya yönelik, mevcut bilgi güvenliği alt yapısının analizi, raporlanması ve iyileştirilmesi çalışmaları için gerekli olan sızma testi hizmeti alımı işi, 4734 Sayılı Kamu İhale Kanunu'nun 22. maddesinin (d) fıkrası uyarınca (**DOĞRUDAN TEMİN USULÜ**) satın alınacaktır. İlgilendiğiniz takdirde **K.D.V. hariç** fiyat teklifi göndermenizi, teklifinizde teslimat süresinin de bildirilmesini rica ederim.

Rafet DAYAN
Daire Başkanı

Ek: Teknik Şartname

Son Başvuru Tarih ve Saati : **31.05.2024 – 12:00**

Teklif Başvuru Yeri : Rektörlük Binası İdari ve Mali İşler Daire Başkanlığı
1.zemin kat 110 nolu oda - Taşlıçiftlik Kampüsü TOKAT

Teslimat Yeri : TOGOÜ Bilgi İşlem D.B. Taşlıçiftlik Kampüsü /TOKAT
Teklif Türü : İşin tamamı

İHTİYAÇ LİSTESİ

S.N.	Malzemenin Adı	MİKTARI	KDV HARİÇ BİRİM FİYAT	KDV HARİÇ TOPLAM FİYAT
1	KURUMSAL BİLGİ SİSTEMLERİNİN GÜVENLİĞİNİ ARTIRMAYA YÖNELİK, MEVCUT BİLGİ GÜVENLİĞİ ALT YAPISININ ANALİZİ, RAPORLANMASI VE İYİLEŞTİRİLMESİ ÇALIŞMALARI İÇİN GEREKLİ OLAN SIZMA TESTİ HİZMETİ ALIMI	1 adet		
			KDV HARİÇ TOPLAM	

Yukarıda cinsi ve miktarı yazılı malzemelerin TAMAMI KDV HARİÇ (RAKAMLA).....(YAZI İLE)..... TL karşılığında vermeyi / yapmayı taahhüt ederim.

Teslimat Süresi : .....
KDV Oranı : .....
Diğer Açıklamalar:

FİRMA KAŞE
ADI SOYADI İMZA

NOT:

1- Talep Edilen mallara ilişkin ödeme, Maliye Bakanlığı'nın ödenekleri serbest bırakma oran ve ilkeleri doğrultusunda yapılacaktır.
2- Teklifler kapalı zarf içerisinde elden teslim edilebilir veya posta, kargo, faks yoluyla da gönderilebilir.
3- Teklif isteme yazımızda mal/malzeme/iş verilecek TOPLAM FİYAT üzerinden değerlendirmeye alınacaktır.
4- Şartlı teklifler ve Türk Lirası haricinde verilen fiyat teklifleri değerlendirilmeye alınmayacaktır.
5- Teslimat süresi değerlendirmede tercih nedeni olabilecektir.
6- Ulaşım, nakliye, kargo vb. giderler yüklenici firmaya aittir.

Taşlıçiftlik Kampüsü – TOKAT
Telefon (0 356) 252 15 80 Faks: (0 356) 252 16 05
e- posta: idarimali@gop.edu.tr
web: www.gop.edu.tr

TOKAT GAZİOSMANPAŞA ÜNİVERSİTESİ SIZMA TESTİ HİZMETİ (PENETRASYON) TEKNİK ŞARTNAMESİ - 2024

1. İŞİN KONUSU

Bu şartname **Tokat Gaziosmanpaşa Üniversitesi Bilgi İşlem Daire Başkanlığı** kurumsal bilgi sistemlerinin güvenliğini artırmaya yönelik, mevcut bilgi güvenliği alt yapısının analizi, raporlanması ve iyileştirilmesi çalışmalarını içermektedir. Sızma testinin hedefi kuruluşun sahip olduğu bilgi işlem altyapısının temel bileşenlerini oluşturan sunucular, ağ aktif cihazları, uygulama sunucuları, veri tabanları gibi standart ekipman ve yazılımlar ile kuruluşa özel geliştirilmiş, iş uygulamalara yetkisiz erişim elde edilmesine veya hassas bilgilere ulaşılmasına neden olabilecek güvenlik açıklarının istismar edilmeden önce tespit edilmesi, risk düzeylerinin belirlenmesi hizmetidir.

2. TANIMLAR

İş bu teknik şartnamede kullanılan kelime ve deyimler, içinde geçtiği metin farklı bir anlam vermedikçe aşağıda tarif edildiği gibi anlaşılacaktır.

2.1. İDARE: Tokat Gaziosmanpaşa Üniversitesi
2.2. İŞ GÜNÜ: Resmî tatiller haricinde haftanın pazartesi, salı, çarşamba, perşembe, cuma günleridir.
2.3. SİSTEM: Tokat Gaziosmanpaşa Üniversitesi Bilgi İşlem Daire Başkanlığı tarafından geliştirilen uygulamalar ve kurumun yerel ağı.
2.4. TARAFLAR: İDARE ve YÜKLENİCİ 'yi belirtir.
2.5. YÜKLENİCİ: İhaleyi kazanan, İDARE ile sözleşme yaptıktan sonra ihale konusu işi yapmaya yetkili ve aynı zamanda idari ve teknik açıdan sorumlu firma.
2.6. Doğrulama Testi: Sızma Testi sonuç raporunda yer alan güvenlik açıklarının giderilip giderilmediğini kontrol etmek amacıyla yapılan testleri ifade etmektedir.
2.7. Sızma Testi Hizmeti Kapsam Listesi: İçerisinde sızma testi yapılacak olan web uygulamalarının ve alt ağların listelerinin olduğu dokümandır.

3. KISALTMALAR

3.1. DNS : Domain Name System
3.2. FTP : File Transfer Protocol
3.3. HTTP : Hyper Text Transfer Protocol
3.4. HTTPS : Secure Hyper Text Transfer Protocol
3.5. ICMP : Internet Control Message Protocol
3.6. IP : Internet Protocol
3.7. LPT : Licensed Penetration Tester
3.8. NETBIOS: Network Basic Input/Output System
3.9. RPC : Remote Procedure Call

artırmaya yönelik tüm açıklıkları, zafiyetleri ve iyileştirilmesi gereken alanları tespit etmekten ve bunların kapatılması ve iyileştirilmesi amacıyla önerilerle birlikte raporlanmasından sorumludur.

5.9. Dış ağ erişim noktaları ve iç ağ topolojisi idare tarafından yüklenici firmaya verilecektir. Bu verilen topolojiye göre ayrıntılı bütün iç ve dış IP numaraları için en az Layer 3 katmanında tarama yapılıp bütün açık port ve network topoloji haritası çıkartılacak bu haritaya göre uygun test altyapısı hazırlanıp bu topoloji üzerinden temel metodolojiye karar verilecektir.

5.10. Yapılacak testler en az 4 ana kısım üzerinden yürüyecektir. Bunlar iç ağdan yapılacak testler, dış ağdan yapılacak testler, servis testleri ve varsa diğer testler şeklinde kategorize edilecektir.

5.11. İç ağ testleri için yerel ağ altyapısı dikkate alınarak her bir VLAN için bir erişim noktası belirlenip bu erişim noktası kullanılarak yerel ağa bağlı sistemler test edilecektir.

5.12. Dış ağdan yapılacak testler için farklı erişim noktalarından İdareye ait ve internet üzerinden erişilebilen sistemler test edilecektir.

5.13. Servis testlerinde ise idare bünyesinde çalışmakta bulunan sunucu servislerinin güvenlik açıkları test edilecektir.

5.14. Farklı test kategorilerindeki açıklar ve çözüm önerileri ayrı olarak raporlandırılacaktır.

5.15. İDARE'nin talep etmesi durumunda sözleşme sürecinde alınan tedbirler nedeniyle güvenlikten etkilenen veya envantere eklenen web ve mobil uygulamalar için ek ücret talep edilmeksizin kapsamın %10'u kadar uygulama, test edilmesi için Sızma Testi Hizmeti Kapsam Listesi(EK-1)'ne eklenebilecektir.

5.16. YÜKLENİCİ Proje kapsamında hazırlayacağı ve İDARE'ye sunacağı bütün dokümanları Türkçe olarak hazırlayacaktır. Teknik detaylar için İngilizce terimler kullanıldığı durumlarda parantez içinde Türkçesi yazılacaktır.

6. SIZMA TESTİNİN GİZLİLİĞİ VE YÜKLENİCİNİN SORUMLULUKLARI

6.1. İş bu şartname ile tanımlanan tüm yükümlülükleri yerine getirecektir.

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

6.3. Testler yasadışı araçları veya yöntemleri içermemelidir. Testler esnasında kuruluş ile sözleşmede veya teknik şartnamede belirlenmiş olan kapsam dışına kuruluşun yazılı izni olmadan çıkılmamalıdır.

6.4. Bu şartnamede tanımlanan ve Yüklenici tarafından gerçekleştirilecek güvenlik denetimleri, sonuçları ve ilgili çalışmalar kapsamında elde edilen her türlü bilgi, Yüklenici tarafından gizli tutulacak ve elde edilen hiçbir matbu/elektronik belge kopyalanarak çoğaltılmayacaktır ve üçüncü taraflar ile paylaşmayacaktır. Sadece yüklenicinin içeriklere erişim sağlandığını gösterebilmesi için gerekiyorsa örnek olarak birkaç kayıt delil sağlamak amacıyla kopyalanabilecektir.

6.5. Yüklenici yasal olarak faaliyetlerine son vermesi durumunda, kendisinde bulunan

7.8. Çalışmalar neticesinde hazırlanacak raporun dili Türkçe olacaktır. Raporlarda tespit edilen zafiyetlerle ilgili yeterli seviyede detay bilgi verilecek, zafiyetin giderilmesi konusunda yapılması gerekli düzenlemelere ilişkin öneriler net biçimde yer alacaktır. Raporda yer alacak önerilerin uygulanması durumunda ortaya çıkacak olası etkiler belirtilecektir.

7.9. Yüklenicinin raporda belirteceği bütün bulgular elle kontrol edilmiş ve zafiyetin gerçekliği teyit edilmiş olmalıdır.

8. SIZMA TESTİ SÜRECİ

8.1. YÜKLENİCİ, sistemlerin güvenlik seviyesinin analizi için, kurum bünyesinde aşağıdaki çalışmaları gerçekleştirecektir.

8.2. İç Ağdan Gerçekleştirilecek Temel Sızma Testleri

8.2.1. Yerel ağda bulunan bütün ip bloklarında yer alan bilgisayarlar, sunucu ve cihazlarda tespit edilen açık portlar üzerinden içerik filtreleme, güvenlik duvarı atlatma, bilgi kaçırma ve sistemlerine giriş testleri gerçekleştirilecektir.

8.2.2. Kurum bünyesinde iç ağda bulunan sunucular ve cihazlar üzerinde çalışmakta olan servislere ait kullanıcı adı ve şifreler tahmin edilerek sunuculara erişilmeye çalışılacaktır. Bu işlem için gelişmiş kullanıcı adı ve şifre tahmin etme programları kullanılacaktır.

8.2.3. Yerel ağ için zafiyet taraması yapılacaktır.

8.2.4. Kurum yerel ağında araya girme teknikleri ile hassas bilgiler elde edilmeye çalışılacaktır.

8.2.5. Elde edilen bilgiler ışığında kullanıcı bilgisayarları, sunucu sistemleri ve aktif cihazlara yönelik ele geçirme saldırıları gerçekleştirilecektir.

8.2.6. Ele geçirilen sunucu ve kullanıcı bilgisayarları üzerinden daha kritik bilgilere ulaşılmaya çalışılacaktır.

8.3. Dış ağdan Gerçekleştirilecek Temel Sızma Testleri

8.3.1. İdareye ait internet erişimi için Ek-1 de yer alan dış IP adresleri için testler yapılacaktır.

8.3.2. İdareye ait dışarıya açık Ek-1 de yer alan normal web uygulamaları için sızma testi araçları ile otomatik testler yapılacaktır.

8.3.3. İdareye ait dışarıya açık Ek-1 de yer alan kritik web uygulamaları için sızma testi araçları ile otomatik testler, detaylı analizler için de elle taramalar yapılacaktır.

8.3.4. İdareye ait dışarıya kapalı Ek-1 de yer alan normal web uygulamaları için sızma testi araçları ile otomatik testler yapılacaktır.

8.3.5. İdareye ait dışarıya kapalı Ek-1 de yer alan kritik web uygulamaları için sızma testi araçları ile otomatik testler, detaylı analizler için de elle taramalar yapılacaktır.

8.3.6. İnternet güvenliği testlerinde Whitebox, Graybox, Blackbox metotlarından uygun olanı İdare ile birlikte belirlenip uygulanacaktır.

8.3.27. Uygulamanın kullandığı veri tabanına sızılmaya çalışılacaktır.

8.3.28. SSL/TLS varsa versiyon, algoritma ve sertifika geçerlilik testleri yapılacaktır.

8.3.29. Hassas bilgilerin şifreli / şifresiz kanallardan aktarılıp aktarılmadığı kontrol edilecektir.

8.3.30. Hedef site üzerinde varsa tanımlı kullanıcılar belirlenecek, kullanıcı adı belirleme/doğrulama çalışmaları, kimlik doğrulama aşamasını atlatma denemeleri yapılarak, parola hatırlatma ve parola sıfırlama özellikleri test edilerek yetkili kullanıcılara yönelik brute force parola denemeleri yapılacaktır.

8.3.31. Oturum yönetimi zayıflıkları, oturum yönetimi bypass testleri ve detaylı cookie güvenlik testleri gerçekleştirilecektir.

8.3.32. Oturum Sabitleme (Session Fixation) testleri, oturum değerleri tahmin saldırıları, CSRF (Cross Side Request Forgery) testleri, dizin atlatma/gezme (Directory Traversal) testleri, yetkilendirme atlatma/yetkilendirme geçiş testleri ve yetki yükseltimi testleri yapılacaktır.

8.3.33. Uygulamanın işleyişinin belirlenmesini takiben uygulamanın işleyişine yönelik teknik olmayan iş mantığı atakları yapılacaktır.

8.3.34. Yansıtılan/depolanmış/DOM tabanlı XSS testleri yapılacaktır.

8.3.35. SQL enjeksiyon / kod enjeksiyon testleri yapılacaktır.

8.3.36. İşletim sistemi komut enjeksiyon testleri, bellek taşması (buffer overflow) testleri, HTTP Response Splitting testleri ve hesap kilitleme politikasının testleri gerçekleştirilecektir.

8.3.37. Web servisi bilgi toplama çalışmaları, WSDL testleri, XML yapı testleri ve genel Ajax testleri yapılacaktır.

8.3.38. Web uygulama güvenlik duvarı keşif testleri ve network IPS keşif testleri tamamlandıktan sonra IPS / web uygulama güvenlik duvarı atlatma testleri gerçekleştirilecektir.

8.3.39. Yapılan analizlerin sonucunda Güvenlik Denetim Raporu hazırlanarak, bulunan güvenlik açıklarının ne gibi risklere sebep olduğu belirtilecektir. Raporda, bulunan açıklara karşı alınacak önlemler ile güvenliği arttırmak için gerekli iyileştirici öneriler yer alacak, sistemde tespit edilen güvenlik açıklarının taşıdıkları riskler itibariyle öncelikleri ve giderilmesi için yapılması gereken işlemler detaylı ve anlaşılır bir şekilde tarif edilecektir.

8.3.40. Raporlar bir toplantı ile sunulacak, teker teker açıklar üzerinden geçilecek, çözümü kimin yapacağı not alınacak ve rapor ilgili kişilere göre bölünerek ayrı ayrı tekrar verilecektir.

8.3.41. İdare bünyesinde dış IP üzerinden iç IP yönlendirilmesi yapılan sunucu sistemleri ve cihazlar üzerindeki açık portlar üzerinden içerik filtreleme, güvenlik duvarı atlatma ve bilgi kaçırma testlerinin gerçekleştirilecektir.

8.3.42. Üniversite bünyesinde dış IP üzerinden iç IP yönlendirilmesi yapılan sunucu üzerinde çalışmakta olan servislere ait kullanıcı adı ve şifreleri tahmin edilerek sunuculara erişilmeye çalışılacaktır. Bu işlem için gelişmiş kullanıcı adı ve şifre tahmin etme programları kullanılacaktır.

8.5. DNS Servisleri Güvenlik Testleri

8.5.1. DNS sunucuların topolojik incelenmesi yapılacaktır.
8.5.2. DNS Sunucusunun alan yapılandırmasında yer alan kayıtların ortaya çıkartılması
8.5.3. Sunucu üzerinden alan transferi (zone transfer) yapılmaya çalışılacaktır.
8.5.4. NXT ve NSEC kaynak kayıtları üzerinden bilgiler elde edilmeye çalışılacaktır.
8.5.5. Pasif sorgularla bilgi toplanacaktır.
8.5.6. DNS sunucular için ön bellek zehirlemesi kontrolü yapılacaktır.
8.5.7. DNS sunucular üzerindeki kaynak kayıt girdileri kontrolü yapılacaktır.
8.5.8. DNS sunucuların sürüm bilgisi incelenecektir.
8.5.9. Kurum dışı alan adı sorgularının kontrolü yapılacaktır.
8.5.10. Sunucular üzerinde DNS dışında bir servisin çalışıp çalışmadığının kontrolü yapılacaktır.
8.5.11. Güvenlik Duvarında DNS sunucular için izin verilen ayarların kontrolü yapılacaktır.
8.5.12. DNS sunucuların zafiyet taraması yapılacaktır.
8.5.13. DNS servisini veren yazılımın açıklıkları araştırılacaktır.
8.5.14. DNS sunucuların topolojik konumu incelenecektir.
8.5.15. Netcraft, Google, Whois sorguları yapılarak Kurum ağında yer alan sunucular tespit edilmeye çalışılacaktır.
8.5.16. DNS sunucular üzerindeki ters kaynak kayıt girdileri incelenecektir.
8.5.17. Elde edilen açıklar ve çözüm önerileri Servis Testi raporunda belirtilecektir.

8.6. Etki alanı ve Kullanıcı Bilgisayarları Güvenlik Testleri

8.6.1. Kullanıcı bilgisayarlarının açılış ayarlarındaki eksiklikler tespit edilip, yerel yönetici hakları elde edilmeye çalışılacaktır.
8.6.2. Yerel yöneticilerin kullanımındaki zafiyetler ile hak yükseltme saldırıları gerçekleştirilecektir.
8.6.3. Etki alanındaki şifre politikası ve şifre saklama politikasındaki zafiyetler tespit edilip, kullanıcı hesaplarının şifreleri ele geçirilmeye çalışılacaktır.
8.6.4. Yama yönetimindeki zafiyetler ve desteği kaldırılmış eski sistemler tespit edilip, uzaktan kod çalıştırma ve hak yükseltme saldırıları gerçekleştirilecektir.
8.6.5. Yetkisiz erişime imkân tanıyan dosya paylaşımları tespit edilerek, bu paylaşımlar ve paylaşımlardaki hassas veriler yoluyla hak yükseltme saldırıları gerçekleştirilecektir.
8.6.6. Hak yükseltme saldırıları ile etki alanı kullanıcılarının hesapları ele geçirilmeye çalışılacaktır.
8.6.7. Etki alanında yönetici haklarına sahip kullanıcı hesapları ve kullanıcı hesabı gruplarının kullanımındaki zafiyetler kullanılarak hak yükseltme saldırıları gerçekleştirilecektir.
8.6.8. Elde edilen şifre ve haklar ile hassas bilgilerin bulunduğu sunucu ve kullanıcı bilgisayarlarına erişim sağlanmasına çalışılacaktır.
8.6.9. Etki alanında güvenlik politikaları kontrol edilecektir.
8.6.10. Etki alanındaki yetkili kullanıcıların ayrıcalıkları ve kullanım şekilleri

bulunduğu, kullanıcı adı, parola ve parolalara ait karmaşıklaştırılmış özet verilerinin bulunup bulunmadığı denetlenecektir.

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

8.8.6. Erişilebilen sistemlerde yama bilgisi kontrol edilir. Bilinen açıklıkları içeren ve gerekli güncellemeleri yapılmamış sistemlerde hak yükselme gibi saldırılarla erişim sağlanan kullanıcının hakları genişletilmeye çalışılacaktır.

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

8.8.8. Hassas verileri ihtiva eden sistemlere erişilmesi halinde yetki seviyesi arttırılmaya çalışılır. 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.

8.8.9. Veri tabanı sunucusunun topolojik konumu incelenecektir.

8.8.10. Yamaları kontrol edilecektir.

8.8.11. Veri tabanı için önemli olan işletim sistemi dosyalarının erişim izinlerinin incelenecektir.

8.8.12. Veri tabanı sunucusunun güvenlik ayarları kontrol edilecektir.

8.8.13. Veri tabanı sunucusunun parola politikası, kullanıcı hesapları güvenlik ayarları kontrol edilecektir.

8.8.14. Veri tabanı sunucusunda, güvenlik açısından önemli olan paketler, nesneler, roller, tablo ve hakların kontrolü sağlanacaktır.

8.8.15. Veri tabanı sunucusunda, denetleme mekanizmasının kontrolü sağlanacaktır.

8.8.16. Veri tabanı sunucusunun yedekleme ve kurtarma mekanizması kontrol edilecektir.

8.8.17. Veri tabanının kurulumu ile birlikte gelen ve kullanıcılar için atanan varsayılan değerlerin kontrolünü yapılacaktır.

8.8.18. Uzaktan erişimin güvenlik kontrolleri yapılacaktır.

8.9. Web Uygulamaları Güvenlik Testleri

Aşağıdaki maddeler kontrol edilecektir.

8.9.1. Veri Kontrolleri

- 8.9.1.1. Girdi denetimi
- 8.9.1.2. Çıktı denetimi
- 8.9.1.3. Değiştirilen içeriğin tespiti
- 8.9.1.4. HTML etiketlerinin filtrelenmesi
- 8.9.1.5. SQL injection
- 8.9.1.6. Sunucu taraflı girdi denetimi
- 8.9.1.7. URL yönlendirmeler
- 8.9.1.8. Diğer injection
- 8.9.1.9. XSS
- 8.9.1.10. HTTP yanıt bölme
- 8.9.1.11. HTTP başlık değiştirme
- 8.9.1.12. HTTP form değiştirme
- 8.9.1.13. Bellek taşma

8.9.5.2. Web Server hizmet dışı bırakma saldırısı
8.9.5.3. İstemci talebine uyarınca bellekte nesne oluşturmak (User specified object allocation)
8.9.5.4. Fazla veri döndüren işlemler

9. TEKNİK HUSUSLAR

9.1. Sızma testini yapacak Yüklenici; iş bu şartnamede işin kapsamında belirtilen her proje için tanımlanan işleri (bundan sonra tümü "iş" olarak ifade edilecektir) gerçekleştirecek ve iş sonunda Sızma ve Zafiyet Testi raporlarını hazırlayarak İdareye sunacaktır.

9.2. Sızma testini yapacak Yüklenici; iş bu şartnamede işin kapsamında belirtilen her proje için tanımlanan işleri ve çalışacak personeli Proje Planında belirtecek ve yazılı/e-posta ile İdareye bildirecektir. İdarenin yazılı bildirimi veya e-posta cevabı olmadan iş kapsamında herhangi bir çalışma yapılamaz, İdare'nin onay vermediği kişi/kişiler çalıştırılamaz veya mevcut kişi/kişiler değiştirilemez.

9.3. Test yapılacak sunucu bilgileri İdare tarafından verilecektir.

9.4. Sızma ve zafiyet testi yapılacak olan sunucular için, işin yapılmasında ihtiyaç duyulan bilgi ve dokümanlar (network topolojisi, kullanılan IP bilgileri, proje iç işleyiş bilgileri vb.) İdare tarafından Yükleniciye verilecektir.

9.5. İdare, Sızma testlerinde, whitebox, blackbox, graybox yöntemlerinden bir veya birkaçının kullanılmasını isteyebilecektir.

9.6. İş kapsamında yapılacak olan Sızma ve Zafiyet testlerinin hedefi olacak bilgi sistemleri üzerinde oluşabilecek olası hizmet kesintileri ve/veya sistemlere verilebilecek zararlar, testler yapılmadan en az 2 (iki) gün önce İdareye yazılı/e-posta olarak bildirilecektir. İdarenin onayı ile ilgili çalışmalar yapılacaktır. Yapılacak olan tüm çalışmalar planlı olacaktır.

9.7. İş kapsamında yapılacak olan Sızma ve Zafiyet testlerinde sistem kesintilerini en aza indirgeyebilmek için kullanılan tarama araçlarında "health check" seçeceği aktif edilerek taramalar yapılacaktır.

9.8. İş sonucunda hazırlanacak olan ilgili raporlarda;

Tespit edilen güvenlik zafiyetleri, ekran çıktıları ve/veya video görüntüleri,
Bu zafiyetlerin sebep olabileceği zararlar/sonuçlan ve zafiyete ilişkin referans bilgileri, Güvenlik zafiyetlerini gidermek için yapılması gerekenler,

detaylı şekilde açıklanacaktır.

9.9. İş sonucunda oluşturulan raporlar hem basılı hem de elektronik ortamda Microsoft Word ve Pdf formatında İdare'ye sunulacaktır.

9.10. İş sonucunda üretilmiş olan raporların tüm telif hakları İdareye ait olacaktır. Raporlar, İdareye özelleştirilmiş, İdare logolu ve Yüklenici logolu olarak iki ayrı formda sunulacaktır.

9.11. İş kapsamında Yüklenici tarafından yapılacak işlerin tamamı ya da bir kısmında İdare'nin belirleyeceği İdare personeli/personelleri gözlemci olarak

10. DİĞER HUSUSLAR

10.1. Sızma testini yapacak Yükleniciden istenen sertifikalar, bu sözleşme kapsamında tek bir personelde toplanamaz.

10.2. Sızma testini yapacak Yüklenici bu özelliklere sahip personellerinin sözleşme aşamasında çalıştığını gösteren SGK bildirgelerini, özgeçmişini, sertifikalarını ve diplomalarını sözleşme aşamasında kuruma sunacaktır.

10.3. Tüm proje bilgileri elektronik formatta belgelenerek İdare'ye teslim edilecektir.

10.4. Belgeler şifreli bir şekilde teslim edilecek, şifre ayrı olarak gönderilecektir.

10.5. Belgeler teslim edildikten sonra detaylı bir toplantı ile tüm maddeler anlatılacaktır.

Sızma Testi Hizmeti Kapsam Listesi(EK-1)

Sunucu Sayısı	150 adet
İç IP Adresleri Sayısı	**5000 adet**
Domain adı	gop.edu.tr
Çalışma Lokasyonu	Tokat Gaziosmanpaşa Üniversitesi Taşlıçiftlik Kampüsü
Dış IP Adresleri	**193.140.180.0/24 193.140.182.0/24**
Sosyal Mühendislik (e-posta ile)	3700 adet e-posta adresi için uygulanacaktır.
Web Sunucu Sayısı	10 adet
Web Uygulama Sayısı	12 adet
URL Adresleri	12 adet adres uygulama aşamasında verilecektir.
Active Directory Sayısı	2 adet
DNS Sayısı	2 adet
Mail Sunucu	1 adet
DHCP Sunucu	1 adet

Engin TÜRK
Öğretim Görevlisi

Şakire YÜCE
Tekniker

Mustafa KAPLAN
Mühendis