T.C.

ULAŞTIRMA VE ALTYAPI BAKANLIĞI

TÜRASAŞ GENEL MÜDÜRLÜĞÜ

Bilişim Teknolojileri Sistemleri Güvenlik, Sızma ve Doğrulama Test Hizmetleri

Teknik Şartnamesi

2024, Ankara

İçindekiler Tablosu

1. Konu ve Kapsam..... 3
2. Tanımlar ve Kısaltmalar..... 3
3. Çalışmanın Amacı..... 5
4. Genel Hususlar..... 5
5. İnternet Üzerinde Gerçekleştirilecek Sızma Testleri..... 8
6. Web Uygulamalarına Yönelik Sızma Testleri..... 10
7. Kurum Yerel Ağı İçinden Gerçekleştirilecek Sızma Testleri..... 12
8. DOS/DDOS Testleri..... 14
9. Sosyal Mühendislik Testleri..... 15
10. Kablosuz Ağ Güvenlik Testleri..... 16
11. Raporlama ve Kabul..... 17

1. KONU VE KAPSAM

İşbu şartnamenin konusu, T.C. Ulaştırma Ve Altyapı Bakanlığı TÜRASAŞ Genel Müdürlüğü(Ankara) bünyesinde ve 3 adet Bölge Müdürlüğünde(Eskişehir-Sakarya-Sivas) bulunan varlıklara yönelik açıkların ve zafiyet oluşturabilecek hususların tespiti için yerinden ve uzaktan Güvenlik, Sızma ve Doğrulama hizmeti sağlanmasıdır. Bu hizmet kapsamında KURUM tarafından talep edilen hizmetler aşağıda listelenmiştir.

- Internet Üzerinden Sızma Testleri
- Web Uygulama Sızma Testleri
- Kurum Yerel Ağı İçinden Gerçekleştirilecek Sızma Testleri
- DOS/DDOS Testleri
- Sosyal Mühendislik Testleri
- Kablosuz Ağ Güvenlik Testleri

2. TANIMLAR VE KISALTMALAR

YÜKLENİCİ	Teklif sahibi FİRMA veya FİRMA lar
KURUM	TÜRASAŞ GENEL MÜDÜRLÜĞÜ
KURUM Personeli	KURUM çalışanları ve/ya dış kaynakları
Ticketing Sistemleri	Proje yönetiminde gerçekleştirilecek aksiyon planlarının düzenlenmesi ve kayıtların aktarılması amacıyla kullanılan yazılım
Bulgu	Güvenlik Araçları ve Sızma Testi çalışmalarında tespit edilen güvenlik açıkları
CEH	Certified Ethical Hacker
LPT	Licenced Penetration Tester
OSCP	Offensive Security Certified Professional

OSEP	Offensive Security Experienced Penetration Tester
OSWE	Offensive Security Web Expert
OSCE	Offensive Security Certified Expert
CRTO	Certified Red Team Operator
CRTE	Certified Red Team Expert
OSWP	Offensive Security Wireless Professional
TSE	Türk Standartları Enstitüsü
BT	Bilgi Teknolojileri
OT	Operasyonel Teknolojiler
SDLC	Yazılım Geliştirme Yaşam Döngüsü
CI/CD	Sürekli Entegrasyon/Sürekli dağıtım
False/Positive	Hatalı Üretilmiş Sonuçlar

3. ÇALIŞMANIN AMACI

KURUM sistemlerinin sızma testlerine tabi tutularak zafiyetlerin, yapılandırma hatalarının ve temel eksikliklerin ortaya çıkartılması, alınacak tedbirler ile bunların giderilerek KURUM siber güvenlik direncinin artırılmasıdır. Bunu sağlamak amacıyla aşağıda detayları verilen faaliyetlerin gerçekleştirilmesi beklenmektedir.

4. GENEL HUSUSLAR

4.1. Gerçekleştirilecek tüm hizmet kalemlerinde 6698 sayılı Kişisel Verileri Koruma Kanunu kapsamından tanımlanmış olan kişisel verilerin, gizlilik, bütünlük ve erişilebilirliğinin sağlanması hususlarına uygun hareket edildiği kontrol edilmelidir.

4.2. YÜKLENİCİ ile hizmet başlangıcında bu hizmete özel bir gizlilik sözleşmesi imzalanacaktır.

4.3. İşin süresi yer teslimi yapıldıktan sonra 30(otuz) gündür.

4.4. YÜKLENİCİ, şartnameye bütün olarak teklif verecek olup parçalı teklifler kabul edilmeyecektir.

4.5. YÜKLENİCİ, bu şartname kapsamında verilecek tüm hizmetlere koordine etmek ve projenin planlandığı gibi ilerlemesini kontrol etmek üzere en az 1(bir) adet PMP (Project Management Professional) sahip bir proje yöneticisi görevlendirilecektir. Bu belgeyi sözleşme aşamasında KURUM' a sunacaktır.

4.6. YÜKLENİCİ, proje kapsamında çalışacak olan personelleri ile YÜKLENİCİ arasında imzaladıkları gizlilik sözleşmeleri KURUM' a sunulacaktır. YÜKLENİCİ ile KURUM arasında da ayrıca Güvenlik Taahhütnamesi imzalanacaktır.

4.7. YÜKLENİCİ, tarafından proje kapsamında elde edilen, öğrenilen bütün bilgiler "GİZLİ" statüsünde olup; söz konusu testler, KURUM altyapısı, yürütülen işler ve sonuçların içeriği hakkında üçüncü kişilere yazılı veya sözlü bilgi vermeyecektir, referans göstermeyecektir. YÜKLENİCİ, elde edilen bilgilerin gizliliği, saklanması

ve güvenliği konusunda gerekli önlemleri alacak ve gizlilik taahhütnamesini imzalayacaktır.

4.8. İşbu şartnamede belirtilen hükümlerin yorumlanmasında KURUM' un görüşü esas kabul edilecektir. Hizmetin ifası esnasında YÜKLENİCİ ve KURUM arasında hizmetin şekli, yapılışı, usul ve esasları, teknikleri vb. dair olabilecek anlaşmazlıklarda KURUM' un görüşü esas kabul edilecektir.

4.9. Yapılacak tüm faaliyetler KURUM ile birlikte koordineli bir şekilde gerçekleştirilecektir. KURUM yetkililerine bilgi verilmeden herhangi bir test çalışması yapılmayacaktır. Yapılacak tüm testlerin zamanları KURUM ile birlikte belirlenecektir.

4.10. YÜKLENİCİ firma taahhütlerini kısmen veya tamamen başkalarına devredemeyecektir.

4.11. YÜKLENİCİ proje kapsamında hizmetlerini yerine getirmek için gerekli tüm kullanıcı cihazları ve/veya yazılımlarını beraberinde getirecek, KURUM' dan bu konuda herhangi bir talepte bulunmayacaktır.

4.12. Gerçekleştirilecek çalışmalar süresince, KURUM' un bilgi güvenliğini sağlamak için kullandığı teknoloji uygulamaları (içerik filtreleri, güvenlik duvarları, saldırı tespit sistemleri vb.) olağan biçimde çalıştırılmaya devam edilecek; YÜKLENİCİ' nin işini kolaylaştıracak ya da zorlaştıracak herhangi bir yeni düzenleme yapılmayacaktır.

4.13. Denetim çalışması kapsamında gerçekleştirilecek saldırı simülasyonları, yalnızca saldırıların gerçekleştirilebilirliğinin gösterilmesi amacıyla düzenlenmektedir. YÜKLENİCİ' nin sızmayı, diğer bir deyişle uzaktan kumanda etmeyi başardığı durumda, KURUM sistemleri üzerinde yer alan hiçbir veriyi (dosya, veri tabanı vb.) okumaması, kopyalamaması ve değiştirmemesi gerekmektedir. Aykırı durumların tespiti, KURUM tarafından sözleşmenin ihlali olarak değerlendirilecektir.

4.14. Gerçekleştirilecek çalışmalarda hizmet kesintisine yol açabilecek herhangi bir kontrol yapılmamalıdır. Testler, sunucu veya uygulamalar üzerinde en az yük oluşturacak ve servis dışı kalmasına mahal vermeyecek şekilde gerçekleştirilmelidir. Sistemleri kesintiye uğratması muhtemel testler öncesinde KURUM' a bilgi verilecek ve KURUM' un onayı ile KURUM tarafından belirlenecek zaman dilimleri içinde gerçekleştirilebilecektir. Yukarıda ifade edilenlerin aksi halinde doğabilecek tüm zararlardan YÜKLENİCİ sorumlu olacaktır.

4.15. YÜKLENİCİ tarafından verilecek tüm hizmetlerde, testler nedeniyle çıkabilecek sorunlara müdahale edebilmek için 7/24 (yedi gün yirmi dört saat) esasına uygun olarak telefon ile ulaşılabilecek bir YÜKLENİCİ personeli olacak ve bu personelin iletişim bilgileri Kurum'a testler öncesinde bildirilecektir.

4.16. Gerçekleştirilecek çalışmalar kapsamında YÜKLENİCİ tarafından yapılacak işlerin tamamı ya da bir kısmında KURUM' un belirleyeceği uzmanlar gözlemci olarak bulunabileceklerdir.

4.17. YÜKLENİCİ uzmanları problemin giderilmesi ile birlikte gerekli doğrulama çalışmalarını yapacaktır.

4.18. YÜKLENİCİ, BT teknolojileri özelinde KURUM' dan iletilebilecek güvenli mimari tasarım gibi konularda gerekli tasarım desteğini verecek, gerekli durumlarda KURUM tarafından talep edilecek toplantılara katılım sağlayacaktır.

4.19. Testler sırasında belirlenen, kritik risk taşıyan problemler anlık olarak KURUM yetkililerine iletilmeli, bu tip problemlerin iletimi için çalışmaların sonuçlanması beklenmemelidir.

4.20. YÜKLENİCİ, teklif edilen hizmetlerle ilgili, dünyadaki ve Türkiye'deki belli başlı referanslar ve gerektiğinde görüşme yapılabilecek kişilerin ad, unvan, telefon ve varsa e-posta adreslerini belirtecektir.

4.21. YÜKLENİCİ firma ISO2000, ISO22301, ISO27001 ve ISO9001 sertifikalarına sahip olmalı ve bunu sözleşme sırasında KURUM' a ibraz etmelidir.

4.22. YÜKLENİCİ, Türk Standartları Enstitüsü tarafından verilen"TS-13638 sızma testi yapan personel ve firmalar için şartlar" standardı kapsamında "TSE A Sınıfı Onaylı Sızma Testi Firması" belgesine sahip olmalı ve bu belgeyi sözleşme sırasında KURUM' a ibraz etmelidir.

4.23. YÜKLENİCİ, uluslararası yetkinliğin bir göstergesi olarak CREST tarafından onaylanmış sızma testleri firması belgesine sahip olmalıdır.

4.24. YÜKLENİCİ'nin Siber Güvenlik risk sigortası bulunmalıdır.

4.25. Yapılan çalışmalar sırasında KURUM hakkında edinilebilecek bilgilerin önemi ve gizliliği nedeniyle söz konusu hizmeti gerçekleştirecek YÜKLENİCİ firmanın yerli

sermayeye sahip olması, bu işlevi T.C. vatandaşlarından oluşan bir ekip ile Türkiye sınırları dâhilinde gerçekleştirmesi gerekmektedir.

4.26. Çalışmaları gerçekleştirecek ekipte CEH, LPT, OSCP, OSEP, OSWE, OSCE, CRTO, CRTE, OSWP ve TSE kıdemli sızma testi uzmanı sertifikalarına sahip, en az 5 uzman yer almalıdır.

4.27. Çalışma kapsamında ifa edilecek tüm faaliyetler Bilgi Güvenliği ve Sızma Testleri konularında en az 5 yıllık tecrübesi bulunan uzmanlar tarafından gerçekleştirilmelidir. Projede çalışacak uzmanların CV'leri KURUM ile paylaşılmalıdır.

4.28. YÜKLENİCİ, son 2 sene içinde kuruma sızma testi hizmeti vermemiş olmalıdır.

4.29. Teklifler bir proje planı içermelidir. Denetim çalışmasının hangi adımının hangi tarihler arasında ve ne şekilde gerçekleştirileceği ayrıntılı bir biçimde açıklanacaktır.

4.30. Çalışmalar neticesinde KURUM' un tabi olduğu regülasyonlara uygun olarak ihtiyaç duyulabilecek tüm raporlar üretilecektir.

4.31. KURUM tarafından talep edilecek tüm doğrulama çalışmaları YÜKLENİCİ tarafından gerçekleştirilecek ve sonuçları iletilecektir.

4.32. YÜKLENİCİ Proje kapsamında hazırlayacağı ve KURUM yetkililerine sunacağı bütün dokümanları Türkçe ve talep edilmesi durumunda İngilizce olarak hazırlayacaktır.

4.33. Yerinde gerçekleştirilecek olan test hizmetleri en az 2 günü kapsamalıdır.

5. INTERNET ÜZERİNDE GERÇEKLEŞTİRİLECEK SIZMA TESTLERİ

KURUM için öncelikli olarak risk oluşturabilecek Internet üzerinden erişilebilir durumdaki tüm sistemlerin keşfi ve test edilmesi, gerekli sızma testlerinin yapılması sağlanacaktır.

5.1. Bu kapsamda aşağıda belirtilen hizmetlerin sözleşme süresi boyunca en az 1 defa yapılması beklenmektedir.

5.2. Çalışmanın yapılacağı kapsama ilişkin detaylar sözleşme aşamasında YÜKLENİCİ ile paylaşılacaktır. Ancak KURUM'a ait Internet üzerinden erişilebilir tüm sistemler ve web/mobil uygulamalar çalışma kapsamında kontrol edilecektir.

5.3. KURUM'a ait Internet üzerinden erişilebilir durumda bulunan tüm sistemler, ağ blokları ve etki alanları için aktif ve pasif keşif çalışmaları gerçekleştirilecektir.

5.4. Internet üzerinden gerçekleştirilen tüm testler YÜKLENİCİ kontrolündeki IP adreslerinden düzenlenecek testlerin yapılacağı IP adresleri çalışma öncesinde KURUM ile paylaşılacaktır. İletilen ve mutabık kalınan IP adresleri haricindeki herhangi bir sistemden onay alınmadan test faaliyetleri düzenlenmeyecektir.

5.5. Sunuculara ait DNS kayıtları, hostname bilgileri, yerel ağ IP adresleri gibi açığa çıkan tüm bilgiler toplanacaktır.

5.6. Keşif aşamasında veri sızıntısı gibi problemler için OSINT (tehdit istihbarat) çalışmaları da gerçekleştirilecektir. Arama motorları tarafından kayıt altına alınan Kurum ile ilişkili veriler incelenecek ve risk oluşturan bilgiler raporlanacaktır.

5.7. Keşif çalışması neticesinde Internet üzerinden erişilebilir varlık envanteri çıkartılacak, işletim sistemi, üzerinde çalışan bileşenler ve servisler belirlenerek raporda yer verilecektir.

5.8. Erişilebilen sunuculara yönelik port ve servis taramaları ile sunucular üzerinde çalışan servisler ortaya çıkartılacaktır.

5.9. Belirlenen servisler ve işletim sistemleri için zafiyet araştırmaları gerçekleştirilecektir.

5.10. Internet erişimine açık sunucuların üzerindeki erişilebilir servislerin analizi ve uygunsuz/gereksiz olanların tespiti gerçekleştirilecektir.

5.11. İşletim sistemlerinin, bu sistemler üzerinde çalışan servislerin sürüm bilgilerinin belirlenmesi, belirlenen sürümlerin güncelliğinin kontrol edilmesi sağlanacaktır.

5.12. Ağ haritası çıkartılacaktır.

5.13. DNS ve E-Posta sunucu ayarları muhtemel yapılandırma hatalarına karşı kontrol edilecektir.

5.14. SMTP, DNS, FTP, SCP, SSH, HTTP, HTTPS, ICMP, NTP, SIP gibi Internet üzerinden yaygın olarak erişilebilen ve keşif çalışmaları sırasında belirlenen tüm servislere yönelik detaylı sızma testleri düzenlenecektir.

5.15. Kurum tarafından kullanılan ağ yönlendiricileri üzerinde bulunabilecek muhtemel zafiyetler ortaya çıkartılacaktır.

5.16. Firewall kurallarının ortaya çıkartılması, hatalı kuralların, gereksiz yere erişim izni veren kuralların belirlenmesine yönelik testler gerçekleştirilecektir.

5.17. Kullanıcı tahmini ve basit parolalara yönelik parola kırma testleri gerçekleştirilecektir.

5.18. Keşfedilen tüm sistemler, cihazlar, web ve mobil uygulamalar, ticari ağ ve web uygulama zafiyet tarama araçları ile zafiyet taramasına tabi tutulacaktır. Zafiyet taramasında kullanılacak ticari araçların listesi ayrıca KURUM' a sunulacaktır.

5.19. Zafiyet taramalarının yanı sıra tüm sistemler sızma testi uzmanları tarafından kontrol edilecek ve detaylı sızma testleri gerçekleştirilecektir.

5.20. Acil ve Kritik risk taşıyan problemler için sızma testi çalışmalarının tamamlanması beklenmeden, ilgili sorumlulara hemen aktarılacaktır.

5.21. Söz konusu hizmet kapsamında gerçekleştirilecek çalışmaların nasıl bir yöntem kullanılarak gerçekleştirileceği adımları ile birlikte detaylı olarak açıklanmalıdır. Bu adımların gerçekleştirilmesinde kullanılan metot ve araçlar açıkça tarif edilmelidir. Sadece otomatik güvenlik tarama yazılım araçlarıyla gerçekleştirilen, otomatik ve bir yazılıma dayalı güvenlik tarama işlemleri teknik olarak yeterli sayılmayacaktır.

6. WEB UYGULAMALARINA YÖNELİK SIZMA TESTLERİ

Gerçekleştirilecek güvenlik denetim hizmetleri kapsamında Kurum'a ait web uygulamaları kontrol edilecektir. Kontrol edilecek uygulamaların listesi yüklenici firma ile ayrıca paylaşılacaktır. Web uygulamalarına yönelik gerçekleştirilecek denetimler en az aşağıda belirtilen hususlar göz önünde bulundurularak gerçekleştirilmelidir;

6.1. Bu test hizmeti yerinde ve uzaktan (karma) gerçekleştirilecektir.

6.2. Gerçekleştirilecek testler kabul görmüş (OSSTMM, OWASP gibi) standart ve metodolojilere göre yapılacak bir web ve uygulama güvenliği testidir.

6.3. Uygulama, farklı profiller içeriyorsa testler farklı kullanıcı profillerini içermeli ve profiller arasında yetki aşımı yapılıp yapılamadığı test edilmelidir.

6.4. Arama motorları ve otomatik tarama araçları kullanılarak site haritası çıkarılacaktır.

6.5. Kullanılan uygulama ve sunucu bileşenleri bilinen zafiyetlere yönelik kontrol edilecektir.

6.6. Uygulama veya web sunucusundan kaynaklı bilgi sızıntıları tespit edilecektir.

6.7. Uygulamada alınan güvenlik tedbirlerinin yeterliliğine veya mevcut önlemlerin nasıl aşılabileceğine ilişkin detaylı kontroller gerçekleştirilecektir.

6.8. Tüm testler anonim kullanıcı hakları ile gerçekleştirilecektir. Ancak test edilen web uygulama hesap açılmasına imkân tanıyor ise, açılacak hesaplar ile testlere devam edilecektir.

6.9. Sunucu ve uygulama kaynaklı yapılandırma hataları belirlenecektir.

6.10. Oturum yönetimine ilişkin güvenlik kontrolleri gerçekleştirilecektir.

6.11. Uygulama kimlik doğrulama mekanizması yetkisiz erişim, zayıf parola kullanımı, yetkilendirme mekanizmasını atlatma gibi sorunlara karşı kontrol edilecektir.

6.12. Yetki aşımı ve hak yükseltme problemlerine ilişkin kontroller düzenlenecektir.

6.13. Uygulamalara ve kullanıcı verilerine yetkisiz erişime (IDOR) neden olabilecek sorunlara yönelik kontroller gerçekleştirilecektir.

6.14. SQL, LDAP, XPATH, XML, OS Command Injection gibi önemli sorunları belirlemeye yönelik kontroller gerçekleştirilecektir.

6.15. XXE, SSRF güvenlik problemlerine yönelik kontroller gerçekleştirilecektir.

6.16. Deserialization güvenlik problemlerine yönelik kontroller gerçekleştirilecektir.

6.17. Kod enjekte etme güvenlik problemlerine ilişkin kontroller gerçekleştirilecektir.

6.18. İşletim sistemi üzerinde komut çalıştırmaya neden olabilecek sorunlara yönelik kontroller gerçekleştirilecektir.

6.19. Cross Site Scripting (XSS) ve Cross Site Request Forgery (XSRF) problemlerine yönelik kontroller gerçekleştirilecektir.

6.20. Veri iletim güvenliğine ilişkin olarak uygulama ve sunucu ayarları kontrol edilecektir.

6.21. API ve Web servis güvenliğine ilişkin kontroller düzenlenecektir.

6.22. Dizin atlatma yöntemi ile işletim sistemi üzerindeki dosyalara erişim kontrolleri gerçekleştirilecektir.

6.23. Uzak veya yerel dosya kaynak kodu ekleme kontrolleri (RFI, LFI) gerçekleştirilecektir.

6.24. Hizmet kesintisine yol açabilecek sorunlara ilişkin kontroller gerçekleştirilecektir.

6.25. Uygulama işlevine bağlı olarak muhtemel mantıksal iş akış problemlerini belirlemeye yönelik kontroller düzenlenecektir.

6.26. Güvenlik Testleri Raporunda, yapılan testler ve kullanılan yöntemler, yönetici özeti, tespit edilen açıklıklar, bu açıklıklara yönelik tehditler ve açıklıkların giderilmesi için çözüm önerileri detaylı bir şekilde tarif edilecektir.

7. KURUM YEREL AĞI İÇİNDEN GERÇEKLEŞTİRİLECEK SIZMA TESTLERİ

Çalışma kapsamında KURUM yerel ağına değişik profillerde bağlantı sağlanarak, KURUM içinden sızma testleri gerçekleştirilecektir. Kurum yerel ağı içinde bulunan sistemler (genel amaçlı sunucu, aktif cihaz, uygulama ve veri tabanı sunucuları, sanallaştırma sistemleri vb.) için sızma testleri gerçekleştirilecektir. Kontrol edilecek sistemlerin listesi gerçekleştirilecek çalışma öncesi YÜKLENİCİ firmaya bildirilecektir. Yerel ağ içinden gerçekleştirilecek testler en az aşağıdaki kontrolleri içerecektir.

7.1. Bu test hizmeti yerinde gerçekleştirilecektir.

7.2. Bu kapsamda aşağıda belirtilen hizmetlerin sözleşme süresi boyunca en az 1 defa yapılması beklenmektedir.

7.3. Kurum yerel ağı içinde bulunan sistemlere yönelik otomatik zafiyet taramaları gerçekleştirilecektir.

7.4. ICMP, SNMP, TCP, UDP ile genel ağ taraması, port ve servis taramaları ile sunucuların belirlenmesi, ağ haritasının çıkartılması, yerel ağ içinden keşif çalışmaları gerçekleştirilecektir.

7.5. Mac filtreleri, port güvenliği ve VLAN yapıları incelenerek tespit edilen problemler raporlanacaktır.

7.6. Mevcut ağ topolojisi incelenecek muhtemel hatalar ortaya çıkartılacaktır.

7.7. DNS / WINS / DHCP / LDAP / AD sunucuların kontrolü, bu sunucular aracılığı ile bilgi toplama ve yapılandırma hatalarını belirleme çalışmaları gerçekleştirilecektir.

7.8. Aktif dizin sistemi ile ilgili mevcut güvenlik politikalarının ve erişim haklarının incelenmesi, muhtemel eksikliklerin ortaya çıkartılması sağlanacaktır.

7.9. Sunucular üzerindeki erişilebilir servisler belirlenerek, sürüm ve yama bilgileri ortaya çıkartılacak, sistemlerin etkilenebileceği zafiyetler raporlanacaktır.

7.10. Kurum yerel ağında kullanılabilecek VOIP altyapısına yönelik güvenlik testleri gerçekleştirilecektir.

7.11. Belirlenen zafiyetler veya hesaplar üzerinden hak yükseltme denemeleri gerçekleştirilecektir.

7.12. Sistemler üzerindeki HTTP, FTP, SSH, RDP, SNMP, RLOGIN, TELNET gibi açık olabilecek servislere yönelik kullanıcı tahmini ve basit parola kırma testleri düzenlenecektir.

7.13. Kurum bünyesinde kullanılan anti-virüs, EDR, DLP, URL Filtreleme teknolojilerinin sağladıkları kontrolleri atlatmaya yönelik çalışmalar gerçekleştirilecektir.

7.14. Kurum yerel ağı içindeki önemli kaynaklara ve paylaşımlara yönelik yetkisiz erişim testleri düzenlenecektir.

7.15. Erişim yapılabilen dosya paylaşımları parola, uygulama kodları, loglar gibi hassas veriler için kontrol edilecektir.

7.16. Yerel ağ içinden kullanılan çevresel güvenlik kontrollerinin etkinliğini ölçmeye yönelik kontroller gerçekleştirilecektir.

7.17. Yerel ağ içinden önemli görülen en az 10 adet istemcinin güvenlik denetimine tabi tutulması sağlanacaktır.

7.18. Kullanıcı bilgisayarlarının açılış ayarları, şifreleme gibi konularda kontrolleri ve yerel yönetici haklarına sahip olmaya yönelik kontroller gerçekleştirilecektir.

7.19. Kurum yerel ağı içinde kullanılan kablosuz ağ alt yapısına yönelik güvenlik kontrolleri ve zafiyet taramaları gerçekleştirilecektir.

8. DOS/DDOS TESTLERİ

Kurum sistemlerine İnternet üzerinden servis dışı bırakma (DoS) ve dağıtık servis dışı bırakma (DDoS) saldırıları gerçekleştirilerek, Kurum altyapısının söz konusu saldırılara karşı durumu tespit edilecek ve mevcut koruma sistemlerinin etkinliği gözlemlenecektir. Bu bağlamda istenilen hizmet detayları aşağıda listelenmiştir.

8.1. Bu test hizmeti uzaktan gerçekleştirilebilecektir.

8.2. Bu hizmet yılda 1 defa sağlanacaktır.

8.3. Testler KURUM tarafından belirlenecek zamanda başlayıp, belirlenmiş zamanı aşmayacak şekilde ve KURUM' un talep ettiği zaman durdurulabilecek şekilde gerçekleştirilecektir.

8.4. Testler kontrolü tamamen YÜKLENİCİ' ye ait olan Türkiye içindeki lokasyonlardan gerçekleştirilecek, yasal olmayan botnet kiralama yöntemi ile saldırı gerçekleştirme gibi işlemler kesinlikle kabul edilmeyecektir.

8.5. Testlerde uygulama ve network katmanı saldırılarının simule edilmesi beklenmektedir.

8.6. Testler, kapsam formunda bildirimi yapılan bant genişliklerini dolduracak sayıda farklı IP adresleri üzerinden gerçekleştirilecektir.

8.7. DDos ve DoS testlerinde uygulanacak olan saldırı çeşitleri ve senaryoları Kurum personeli ile birlikte belirlenecektir. Bununla birlikte ağ ve uygulama katmanında en az aşağıdaki saldırıların yapılması beklenmektedir.

- TCP SYN Flood Saldırıları
- ICMP Flood
- UDP Flood Saldırıları
- DNS Flood Saldırıları
- HTTP GET/ POST Flood saldırıları
- HTTPS GET / POST Flood saldırıları
- RST Flood saldırıları

8.8. TCP ve UDP protokollerine yönelik ağ katmanı saldırılarında değişik paket büyüklüklerinde veya farklı TCP bayrakları işaretlenerek saldırılar düzenlenebilecektir.

8.9. Ağ katmanından yapılan tüm saldırılarda IP Spoofing (Kaynak IP Adreslerinin Rastgele Üretilmesi) tekniği kullanılacaktır. Testler sırasında IP Spoofing işleminin gerçekleştirildiğinin gösterilmesi için örnek trafik kaydı istenecektir.

8.10. Uygulama katmanında gerçekleştirilecek GET/POST Flood saldırıları en az 1000 farklı IP adresi üzerinden gerçekleştirilmeli, bu işlem için nasıl bir yapı kullanıldığı açıklanmalıdır. Testler öncesinde bu IP adresleri kurum ile paylaşılmalıdır.

8.11. Testler esnasında KURUM personelinin canlı olarak yapılan saldırıları izleyebileceği bir arayüz test ekibi tarafından sağlanacaktır.

9. SOSYAL MÜHENDİSLİK TESTLERİ

Kurum çalışanlarından kaynaklanabilecek güvenlik risklerini belirlemek amacıyla Sosyal Mühendislik testleri gerçekleştirilecektir. Bu testler aşağıda belirtilen hususlara uygun olarak düzenlenmelidir.

9.1. Sosyal mühendislik testlerinin uygulanacağı hedef kitle arama motorları, sosyal ağlar ve Kuruma ait sistemler/uygulamalar üzerinden toplanacak bilgiler kullanılarak belirlenecektir.

9.2. Arama motorları tarafından kayıt altına alınmış Kuruma ait hassas bilgiler araştırılacaktır.

9.3. Elde edilen bilgiler ışığında belirlenen hedef listesi Kurum yetkililerinin onayına sunulacak ve Sosyal Mühendislik testleri Kurum tarafından onaylanmış liste baz alınarak gerçekleştirilecektir.

9.4. Test kapsamında aşağıda listelenen 2 farklı senaryonun değişik zaman dilimlerinde uygulanması beklenmektedir.

- Özel hazırlanmış e-posta içerikleri ile phishing saldırıları
- Fiziksel sosyal mühendislik testleri

9.5. E-Posta aracılığı ile yapılacak saldırılar 3500 adet kullanıcı için gerçekleştirilecektir.

9.6. E-Posta ile düzenlenecek phishing saldırıları için hazırlanacak ortam sadece test süresince aktif durumda bulunmalı, testler tamamlandıktan sonra bu ortama erişimler kapatılmalıdır. Elde edilen hassas verilerin yetkisiz kişilerin eline geçmesini engelleyecek güvenlik tedbirleri alınmalıdır.

9.7. Fiziksel sosyal mühendislik testlerinde uygulanacak senaryo Kurum yetkilileri ile birlikte yapılacak görüşmeler neticesinde belirlenecektir. Yüklenici bu kapsamda ne gibi testler yapabileceğini, şartname cevaplarında iletmelidir.

9.8. Gerçekleştirilen test sonucunda elde edilen bulgular detaylı olarak raporlanacaktır.

10.KABLOSUZ AĞ GÜVENLİK TESTLERİ

KURUM bilgi sistemleri alt yapısı içinde bulunan kablosuz ağ alt yapısı en az aşağıda belirtilen kontroller uygulanarak test edilecektir.

10.1. Bu test hizmeti yerinde gerçekleştirilecektir.

10.2. Kablosuz ağ mimarisi çıkarılarak, Kuruma ait diğer ağlar ile ilişkisi belirlenecektir.

10.3. Kurum misafir ağından, Kurum yerel ağına erişim denemeleri yapılacaktır.

10.4. Kurum içinde bulunan kablosuz ağlar taranarak yetkilendirme ve şifreleme özellikleri belirlenecektir.

10.5. Kablosuz ağ erişiminde kullanılan şifreleme ve kimlik denetimi yöntemleri incelenerek ağ şifresi ele geçirilmeye çalışılacak ya da kimlik doğrulama yöntemi atlatılmaya çalışılacaktır.

10.6. Kablosuz ağ yapısı içinde bulunabilecek hotspot, erişim noktası gibi sistemlere doğru sızma testleri ve zafiyet taramaları gerçekleştirilecektir.

10.7. Kablosuz ağ erişimi için kullanılabilecek sabit parolalara yönelik, parola kırma testleri düzenlenecektir.

10.8. Sahte kablosuz ağ erişim noktaları oluşturularak Kurumda bulunan istemciler ele geçirilmeye çalışılacaktır.

10.9. İstemciler üzerinden kablosuz ağ taraması yapılarak, Kurum etrafında bulunan diğer kablosuz ağlar keşfedilmeye çalışılacaktır.

10.10. İstemciler üzerinden kablosuz ağ kullanılarak, Kurum dışına bağlantı yapılıp yapılamayacağı incelenecektir.

11.RAPORLAMA VE KABUL

11.1. YÜKLENİCİ, yapılan testlerin sonuçlarını raporlayıp testlerin bitişinden itibaren en geç 7(yedi) gün içerisinde KURUM' a teslim edecektir.

11.2. YÜKLENİCİ, ilgili hizmetleri tamamladıktan sonra Kabul için KURUM 'un onayına başvuracaktır.

Rukiye KILIÇ
Mühendis

Filiz ARAL
Şube Müdür V.

Bilgi İşlem Daire Başkanı

Testi talep eden kurum/kuruluş/ organizasyon adı	TÜRASAŞ GENEL MÜDÜRLÜĞÜ

Açıklama: Gerçekleştirilecek güvenlik testlerinin tiplerini ve kapsamlarını belirlemek maksadıyla kullanılır.

Güvenlik Testi için Talep Edilen Hizmetler
☒ İnternet Güvenlik Test Hizmeti
☒ Web Uygulama Güvenlik Test Hizmeti
☐ Mobil Uygulama Güvenlik Test Hizmeti
☐ Web Servisi/API Güvenlik Test Hizmeti
☒ Yerel Ağ Güvenlik Test Hizmeti
☐ VoIP Güvenlik Test Hizmeti
☒ Kablosuz Ağ Güvenlik Test Hizmeti
☒ Sosyal Mühendislik Test Hizmeti
☒ Dağıtık Hizmet Dışı Bırakma (DDOS) Test Hizmeti
☐ Yazılım Kaynak Kod Analizi Hizmeti
☐ Sürekli Zafiyet Analizi Hizmeti
☐ Web Uygulama Yük Testi Hizmeti
☐ Kırmızı Takım (Red Team) Hizmeti

Testlerin Yapılacağı Lokasyon Bilgisi

Testlerin Yapılacağı Lokasyon Bilgisi	
Test Yapılması Planlanan Lokasyon Sayısı	4 Adet
1. Lokasyon adresi	Oğuzlar Mahallesi Ceyhun Atuf Kansu Caddesi No:61/1 Balgat/ Çankaya/ ANKARA/TÜRKİYE
2. Lokasyon adresi	Ahmet Kanatlı Cad. 26 490 Eskişehir / Türkiye
3. Lokasyon adresi	Milli Egemenlik Cad. Mithatpaşa Mah. No:131 54100 Adapazarı / Sakarya / Türkiye
4. Lokasyon adresi	Kadıburhanettin Mah. Fabrika Cad. No: 12 Sivas/Türkiye

İnternet Güvenlik Test Hizmeti

Kurum/Kuruluş veya Firmanın İnternetten erişilebilen kapsam dâhilindeki bilgi sistem bileşenlerinin; zafiyetlerinin tespiti, manuel yöntemlerle denenmesi, analiz edilmesi, bulgu/çözüm önerilerinin raporlanması

ve hizmet kapsamında talep edildiğinde doğrulanması faaliyetlerini de içeren güvenlik test hizmetidir. Kara Kutu; güvenlik sistemlerinden izin verilmeden ve sistemler hakkında kapsam haricinde detay bilgi verilmeden gerçekleştirilen testlerdir. Beyaz kutu; güvenlik sistemleri üzerinden test yapacak IP adreslerine izin verilerek ve sistemler hakkında detaylı bilgi sağlanarak gerçekleştirilecek testleri ifade etmektedir. Gri kutu; bu tür testler kara kutu ve beyaz kutu karışımı testleri ifade eder, daha çok kısıtlı yetkiye sahip kullanıcıların sistem üzerinde yapabilecekleri tespit edilmeye çalışılır.

İnternet Güvenlik Test Hizmeti			
Test Edilecek **İnternete Açık** IP Sayısı		9 Adet	
Test Edilecek İnternete Açık IP'ler veya IP aralığı			
Test Edilecek Sunucu Bilgileri	Web Sunucu: Adet	DNS Sunucu: ... Adet	FW/VPN: 4 Adet
	Mail Sunucu: 1 Adet	FTP Sunucu : ... Adet	Diğer : ... Adet
Test Tipi	☐Kara Kutu (Black Box)	☐ Beyaz Kutu (White Box)	☒ Gri Kutu (Gray Box)

Web Uygulama Güvenlik Test Hizmeti

Kurum/Kuruluş veya Firmanın kapsam dâhilindeki web uygulamalarının farklı kullanıcı profilleriyle zafiyetlerin tespiti, manuel yöntemlerle denenmesi, analiz edilmesi, bulgu/çözüm önerilerinin raporlanması ve hizmet kapsamında talep edildiğinde doğrulanması faaliyetlerini de içeren güvenlik test hizmetidir. Aşağıda Test yapılacak kullanıcı profil sayısı verilmez ise kara kutu (Black Box) test gerçekleştirilecektir.

Web Uygulama Güvenlik Test Hizmeti			
Web Uygulama	Sayısı: 1 Adet		
	Uygulama Adres Bilgisi	**Test Yapılacak Kullanıcı Profil Sayısı (Anonim, 1,2, vb.)**	**İnternet Üzerinden Erişiliyor mu?**
			☒ Evet ☐ Hayır
			☐ Evet ☐ Hayır
			☐ Evet ☐ Hayır
			☐ Evet ☐ Hayır
İnternet Üzerinden Erişilmeyen Uygulamalar için VPN Erişimi Verilecek mi?	☒ Evet ☐ Hayır		

Web Servisi/API Güvenlik Test Hizmeti

Kurum/Kuruluş veya Firmanın kapsam dahilindeki web servislerinin veya uygulamalara ait API'lerin farklı kullanıcı profilleriyle zafiyetlerin tespiti, manuel yöntemlerle denenmesi, analiz edilmesi, bulgu/çözüm önerilerinin raporlanması ve hizmet kapsamında talep edildiğinde doğrulanması faaliyetlerini de içeren güvenlik test hizmetidir.

Web Servisi/API Güvenlik Test Hizmeti		
Test Edilecek Web Servis/API Bilgileri	... Adet	
	Web Servisi/API Adres Bilgisi	**Test Yapılacak Kullanıcı Profil Sayısı (Anonim, 1,2, vb.)**
	<Gerektiği kadar satır ilave ediniz>	

Yerel Ağ Güvenlik Test Hizmeti

Kurum/Kuruluş veya Firmanın Yerel Ağlarında bulunan kapsam dâhilindeki bilgi sistem bileşenlerinin; zafiyetlerinin tespiti, manuel yöntemlerle denenmesi, analiz edilmesi, bulgu/çözüm önerilerinin raporlanması ve hizmet kapsamında talep edildiğinde doğrulanması faaliyetlerini de içeren güvenlik test hizmetidir. Test yapılacak lokasyon sayısı kadar 3. lokasyon bilgileri tablosunun altına tablo eklemesi yapılabilir. Kara Kutu güvenlik sistemlerinden izin verilmeden, beyaz kutu ise güvenlik sistemleri üzerinden test yapacak IP adreslerine izin verilerek gerçekleştirilecek testleri ifade etmektedir.

Yerel Ağ Güvenlik Test Hizmeti (Ankara)			
Test Edilecek Toplam Sunucu Sayısı (Fiziksel + Sanal Sunucu)	81 Adet (1+80)		
Test Edilecek Client Sayısı	175 Adet		
Test Tipi	☐ Kara Kutu (Black Box)/Anonim Kullanıcı Profili	☐ Beyaz Kutu (White Box)/ Yetkili kullanıcı Profili	☒ Gri Kutu (Gray Box)/Kurum Personeli Profili

Yerel Ağ Güvenlik Test Hizmeti (Sivas)			
Test Edilecek Toplam Sunucu Sayısı (Fiziksel + Sanal Sunucu)	60 Adet		
Test Edilecek Client Sayısı	400 Adet		
Test Tipi	☐ Kara Kutu (Black Box)/Anonim Kullanıcı Profili	☐ Beyaz Kutu (White Box)/ Yetkili kullanıcı Profili	☒ Gri Kutu (Gray Box)/Kurum Personeli Profili

Yerel Ağ Güvenlik Test Hizmeti (Eskişehir)			
Test Edilecek Toplam Sunucu Sayısı (Fiziksel + Sanal Sunucu)	75 Adet [3+72)		
Test Edilecek Client Sayısı	700 Adet		
Test Tipi	☐ Kara Kutu (Black Box)/Anonim Kullanıcı Profili	☐ Beyaz Kutu (White Box)/ Yetkili kullanıcı Profili	☒ Gri Kutu (Gray Box)/Kurum Personeli Profili

Yerel Ağ Güvenlik Test Hizmeti Sakarya)			
Test Edilecek Toplam Sunucu Sayısı (Fiziksel + Sanal Sunucu)	42 Adet [2+40)		
Test Edilecek Client Sayısı	650 Adet		
Test Tipi	☐ Kara Kutu (Black Box)/Anonim Kullanıcı Profili	☐ Beyaz Kutu (White Box)/ Yetkili kullanıcı Profili	☒ Gri Kutu (Gray Box)/Kurum Personeli Profili

VoIP Güvenlik Test Hizmeti

Kurum/Kuruluş veya Firmanın Yerel kapsam dahilindeki VoIP sistem bileşenlerinin; zafiyetlerinin tespiti, manuel yöntemlerle denenmesi, analiz edilmesi, bulgu/çözüm önerilerinin raporlanması ve hizmet kapsamında talep edildiğinde doğrulanması faaliyetlerini de içeren güvenlik test hizmetidir.

VoIP Güvenlik Test Hizmeti	
Kaç farklı tipte Video Konferans veya Telefon Sistemi test edilecek?	... Adet
VoIP sistemi testi gerçekleştirilecek lokasyon sayısı?	... Adet

Kablosuz Ağ Güvenlik Test Hizmeti

Kurum/Kuruluş veya Firmanın ağlarına bağlı kapsam dâhilindeki kablosuz ağların, erişim kontrollerinin, yapılandırmalarının ve kullanıcılarının davranışlarının değerlendirilmesi, parola kırma testleri, erişim sağlanan kablosuz ağlar üzerinden kurum ağına gerçekleştirilebilecek saldırıların test edilmesi, bulgu/çözüm önerilerinin raporlanması ve hizmet kapsamı dâhilinde talep edildiğinde doğrulanması faaliyetlerini içeren güvenlik test hizmetidir.

Kablosuz Ağ Güvenlik Test Hizmeti		
Test Edilecek SSID sayısı	Ankara 3 Adet Sivas 2 Adet Eskişehir 5 adet Sakarya 2	
Test yapılacak lokasyon sayısı	4 Adet	
Birden çok lokasyon varsa lokasyonlar birbirine yakın mıdır? (Yakınsa aynı gün içinde 2-3 SSID'nin testleri bitirilebilmektedir)	☐ Evet	☒ Hayır
	Açıklama:	

Sosyal Mühendislik Test Hizmeti

Kurum/Kuruluş veya Firmanın çalışanlarının tamamına ya da örnekleme usulü seçilen bir kısmına yönelik gerçekleştirilen ve çeşitli aldatma teknikleri kullanarak personelin bilgi güvenliği konusundaki bilinç seviyesini ölçmeyi hedefleyen test hizmetidir. **Doğrulaması yapılmamaktadır, testin tekrarı gerekir.**

Sosyal Mühendislik Test Hizmeti		
İstenen Sosyal Mühendislik Testi	☒E-Posta (Oltalama)	☐ Telefon (Bilgi Alma)
E-posta gönderilecek kullanıcı Sayısı	3500 Adet	
Oltalama Saldırısında Hassas Bilgilerin (Kullanıcı parolaları vb) Test Sırasında kayıt edilmesi isteniyor mu?	☐ Evet ☒ Hayır	
Telefonla aranacak kullanıcı sayısı	... Adet	
Varsa, talep edilen senaryolar ve ilave bilgi	*<Testler ile ilgili özel istekler belirtilmelidir>*	

Dağıtık Hizmet Dışı Bırakma (DDoS) Test Hizmeti

Kurum/Kuruluş veya Firmanın Dağıtık Servis Dışı bırakma (DDoS) Saldırılarına yönelik aldığı önlemlerin etkinliği ve gerçek hayat senaryoları karşısındaki durumunu test etmeye yönelik LoDDos ürünü ile gerçekleştirilen bir test hizmetidir. **Doğrulaması yapılmamaktadır, testin tekrarı gerekir.**

Dağıtık Hizmet Dışı Bırakma (DDoS) Test Hizmeti				
Test yapılacak varlık sayısı	3 Adet			
Test yapılacak servis sağlayıcı sayısı	☒ 1 ☐ 2 ☐ 3			
Mevcut Bant genişliği	600 Mbit/s veya ... Gbit/s			
Test Tipi	**İstenen Testleri Seçiniz**	**İstenen Max Bant Genişliği**	**Max. User**	**IP: port/FQDN**
HTTP(S) Get Flood	☒			
HTTP(S) Post Flood	☒			
TCP SYN Flood	☒		N/A	
TCP SYNACK Flood	☒		N/A	
TCP ACKFIN Flood	☒		N/A	
DNS Query Flood	☐		N/A	
UDP Flood	☒		N/A	
ICMP Flood	☒		N/A	
Diğer (.....)	☐			

Raporlama

Raporlama Dili	☒ Türkçe ☐ İngilizce ☐ ..... ☐ .....
Rapor Teslimi İçin İstenen Tarih	
Test raporu testlerden sonra tarafımıza gönderilecek ve YÜKLENİCİ tarafında imha edilecektir. Doğrulama testi yapılırken ilgili test raporu tarafımızdan talep edildiğinde Yüklenici'ye gönderilecektir.	
Raporlama ile ilgili ilave istekler var ise bu bölümde belirtilebilir.	