İSTANBUL TİCARET ÜNİVERSİTESİ

İSTANBUL TİCARET ÜNİVERSİTESİ CUMHURBAŞKANLIĞI BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİNE UYUM İÇİN SIZMA TESTİ ve DENETİM HİZMETİ İŞİ

TEKNİK ŞARTNAMESİ

AMAÇ

Bilgi sistemlerinde karşılaşılan güvenlik risklerinin azaltılması, etkisiz kılınması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması amacıyla, kamu kurumları ve kritik altyapı hizmeti veren işletmelerce uyulması gereken Bilgi ve İletişim Güvenliği tedbirlerini içeren, 06.07.2019 tarih ve 30823 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 2019/12 sayılı Cumhurbaşkanlığı Genelgesi yasal düzenleme boyutunda ülke çapında bilgi güvenliği seviyesini artırmaya yönelik önemli bir adım olmuştur.

Bu Teknik Şartname, Üniversite iş süreçlerinde Bilgi ve İletişim Güvenliği tedbirlerine uyumluluğunun sızma ve doğrulama testi hizmeti ve **2023 yılı** denetlenmesi için gerekli hizmetin alımını kapsar.

KONU VE KAPSAM

Üniversite iş süreçlerinde bilgi güvenliği risklerinin daha etkin yönetilmesi amacıyla 2019/12 sayılı Cumhurbaşkanlığı Genelgesi kapsamında oluşturulan Rehberin Bilgi ve İletişim Güvenliği Rehberi Uygulama Süreci kapsamında Üniversite bilişim sistemlerine sızma ve doğrulama testi yapılması ve denetlenmesini hedeflenmektedir.

Sıra No	Ürün Açıklaması	Adet
1	Sızma ve Doğrulama Testi Hizmeti (Ayrı Olarak Fiyatlandırılacak)	Hizmet Alımı
2	Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi Denetimi Hizmeti (Ayrı Olarak Fiyatlandırılacak)	Hizmet Alımı

TANIMLAR

İşbu teknik şartname içinde kullanılan aşağıdaki kelime ve deyimler, içinde geçtiği metin farklı bir anlam vermedikçe aşağıda tarif edildiği gibi anlaşılacaktır.

Kurum/İdare : Üniversite

İstekli : İş bu Şartnameye konu olan işler için teklif veren firma

Yüklenici : Şartnamedeki hizmetleri gerçekleştirmeye hak kazanan firma

Denetçi : TSE Belgelendirme Programı kapsamında yetkilendirilen denetçi

DDO : Cumhurbaşkanlığı Dijital Dönüşüm Ofisi

TSE : Türk Standartları Enstitüsü

Rehber : DDO tarafından yayımlanan Bilgi ve İletişim Güvenliği Rehberi

Firma : Belgelendirme Programı kapsamında yetkilendirilen firma

Proje : İşbu şartname çerçevesinde gerçekleştirilecek tüm faaliyetler

1. GENEL YÜKÜMLÜLÜKLER

Denetim ve sızma testi işi, İdare ve Yüklenicinin birlikte belirleyeceği bir tarihte yapılacak olup denetim tarihinin değişmesinin gerekmesi halinde, Kurum yeni tarihi e-posta/posta/telefon/faks yöntemlerinden herhangi biri ile 10 gün önceden Yüklenici ‘ye bildirecektir.

İdare, Yüklenici tarafından görevlendirilecek personelin ilgili hizmetlere uygun olup olmadığı yönünde değerlendirme yapacaktır. Uygun bulunmayan personelin değiştirilmesi istenebilecektir. Yüklenici, görevlendirilecek hizmet işlerini gerçekleştirecek personelin ayrılması durumunda, görevlendireceği yeni personelini İdare’ ye bildirecek ve İdare’nin yazılı onayını alacaktır.

Tarafların iradesi dışında meydana gelip denetim ve sızma testi hizmetinin yapılmasını olanaksız kılan yangın, fırtına, sel, heyelan, zelzele, salgın hastalık gibi doğal afetler ile grev, lokavt, karantina durumları mücbir hal kabul edilecektir. Mücbir haller, ortaya çıkışını izleyen en geç 3 gün içinde Yüklenici tarafından İdare’ye bildirilecek ve mücbir hali tasdik eden evraklar bilahare İdare’ye ibraz edilecektir. Mücbir hal devamınca yükümlülükler askıya alınacak olup ceza tahakkuk ettirilmeyecektir. Yüklenici bu durumdan kaynaklı herhangi bir maddi ve manevi hak iddia edemeyecektir.

Yüklenici tarafından çalıştırılan personelin bina dâhilinde ve çevresinde kazaya uğramaları, yaralanmaları veya hayatlarını kaybetmeleri halinde, İdare’nin mevzuat uyarınca iş sağlığı ve güvenliği için aldığı önlemler dışında kalan durumlarda sorumluluk Yüklenici ’ye aittir.

Sosyal Sigortalar Mevzuatı ile her türlü işçi ve işveren hakkındaki mevzuattan dolayı personel alınması, personel maaş ve diğer haklarının ödenmesi, personelin işine son verilmesi, kıdem tazminatı vb. konularda tüm sorumluluk Yüklenici ‘ye ait olup, İdare bu konularda sorumlu sayılmayacaktır.

Yüklenici, bu şartnamenin esasları ile ilgili konularda İdare’nin denetimine tabidir. İdare, verilecek denetim hizmeti ile ilgili görülen aksaklıkları, kalite ve verimlilik açısından Yüklenici ‘ye sözlü olarak veya gerektiğinde yazılı olarak bildirir. Bu aksaklıkların tekerrürü veya istemlerin yerine getirilmemesi hallerinde İdare, bu şartnamede bahsedilen esaslar dâhilinde belirtilen kuralları ve ihale mevzuatının ilgili hükümlerini uygular.

Yüklenici, şartnamede belirtilen iş ve işlemleri maliyetlendirebilmek amacıyla Kurum nezaretinde yerinde keşif yapabilir.

Yüklenici personeli sistem üzerinde yapacağı her türlü iş, işlem ve müdahaleyi Kurum personeli gözetim ve denetiminde gerçekleştirecektir. Yüklenici personeli sistemlere ya da sistemlerin bulunduğu mekânlara fiziksel olarak müdahale edebilmek için Kurum’un onayını almak zorundadır.

Proje süresince Rehber'de yapılabilecek güncellemelere göre Yüklenici, proje planında ve projenin uygulanmasında yeni standarda göre Kurum'un onayı ile değişiklik yapabilecek ve Kurum'un talep etmesi durumunda proje yeni standarda göre tamamlanacaktır.

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

1.1. Denetim ve sızma testi Hizmeti kapsamında Kurum ve Yüklenici/denetçi yükümlülükleri aşağıda belirtildiği şekilde olacaktır.

1.1.1. Kurum Yükümlülükleri:

1.1.1.1 Denetim ve sızma testi ekibine denetim kapsamında yer alan süreç, altyapı ve uygulamalara yönelik elektronik ve fiziksel ortamda yapılan tüm çalışmalar hakkında tam ve doğru bilgi vermek; bu çalışmalar doğrultusunda kullanılan tüm dokümantasyon ve ilişkili kayıt, veri/bilgi, belge vb. kaynakları denetime uygun ve hazır hale getirmek.

1.1.1.2 Denetim ve sızma testi ekibine denetim çalışmalarını yürütürken ihtiyaç duyacağı bilgisayar, harici disk vb. ekipmanları mümkün olduğu ölçüde Kurum kaynakları ile sağlamak. Sağlanan ekipmanı; hangi denetçiye, hangi ekipmanın, hangi tarihler arasında teslim edildiği/alındığı gibi bilgileri içerecek şekilde tutanak altına almak.

1.1.1.3. Denetim ve sızma testi süresince, Kurum bünyesinde gerçekleştirilen faaliyetler ile ilgili bilgi aktarımında bulunabilecek personel kaynağını denetim kapsamına ve denetim planına uyumlu olacak şekilde tahsis etmek.

1.1.1.4. Denetim ve sızma testi kapsamında yapılan değerlendirmelerin doğruluğunu olumsuz etkileyebilecek herhangi bir faaliyette bulunmamak.

1.1.2. Yüklenici ve denetçi yükümlülükleri:

1.1.2.1. Denetim ve sızma testi ekibinde, TSE ve DDO Belgelendirme Programı kapsamında yetkilendirilen personel görevlendirmek.
1.1.2.2. Denetim ve sızma testi çalışmaları kapsamında elde ettiği/ürettiği her türlü bilgi, belge ve dokümanın bütünlüğünü korumak ve gizliliğini sağlamak.
1.1.2.3. Denetim ve sızma testi sürecinde elde ettiği/ürettiği elektronik ve/veya basılı formattaki belgeleri Kurum'un yazılı izni olmadan denetim faaliyetlerinin yürütüldüğü fiziksel ortamların dışına çıkarmamak.
1.1.2.4. Denetim ve sızma testi sürecinde; denetim kapsamına yönelik olmayan bilgi, belge veya dokümanları inceleme, denetim kapsamı dışında olan bilgi sistemlerine erişim, denetim faaliyetlerinin yürütüldüğü fiziksel ortamların haricindeki ortamlara erişim gibi denetimin amacı dışında olan taleplerde bulunmamak.
1.1.2.5. Denetim ve sızma testi kapsamında elde ettiği/ürettiği herhangi bir veri/bilgiyi kişisel menfaatler için veya hukuka aykırı olarak Kurum'un ya da üçüncü kişilerin menfaatine veya itibarına zarar verebilecek şekilde kullanmamak.
1.1.2.6. Denetim ve sızma testi kapsamında yapılan değerlendirmelerin tarafsızlığına zarar verebilecek herhangi bir faaliyette bulunmamak.

1.1.2.7. Denetim ve sızma testi faaliyeti sırasında bağımsızlığın veya tarafsızlığın ortadan kalktığı durumlarda bu hususu Kurum'un ilgili birimlerine bildirmek.
1.1.2.8. Denetim ve sızma testi raporunu doğru, tarafsız ve nesnel biçimde hazırlamak.
1.1.2.9. Denetim ve sızma testi süresince oluşturulan tüm çalışma formlarını, bulgu tablosunu, denetim raporunu ve eklerini denetim dosyası haline getirmek.
1.1.2.10. Denetim ve sızma testi dosyasının bütünlüğünün bozulmasını önleyecek yöntemler kullanmak. Denetim dosyasını ve özet (hash) bilgisini Kurum'a elektronik ortamda teslim etmek.

TEKLİF AŞAMASI

Yüklenici, TÜRKAK tarafından akredite edilmiş ve teklif tarihi itibariyle geçerli ISO 9001 ve ISO 27001 belgelerine sahip olacaktır.

Yüklenici, denetim programı kapsamında TSE onaylı Cumhurbaşkanlığı Dijital Dönüşüm Ofisi "Bilgi ve İletişim Güvenliği D1 ve D2 Denetçisi Eğitimi" Sertifikasına sahip olmak ile denetim için yetkilendirilmiş firma olduğunu belgeleyecektir.

Yüklenici, sızma testi hizmeti kapsamında TSE onaylı A veya B Sızma Testi belgesine sahip olduğunu belgelendirecektir.

Yüklenici, sözleşmenin imzalanmasından itibaren en geç 15 (on) iş günü içerisinde, şartname kapsamında verilecek hizmetler ile ilgili detaylı proje planı hazırlayarak İdare'ye sunacaktır.

Yüklenici, bu şartname kapsamında verilecek tüm hizmetleri koordine etmek ve projenin planlandığı gibi ilerlemesini kontrol etmek üzere en az 1 (bir) adet TSE tarafından belgelendirilmiş Baş Denetçi'yi proje yöneticisi olarak görevlendirecektir.

Yüklenici personelinden proje kapsamında çalışacak olanların Yüklenici ile imzaladıkları gizlilik sözleşmeleri İdare'ye sunulacaktır. İdare ile de ayrıca Güvenlik Taahhütnamesi imzalanacaktır.

Yüklenici, proje başlangıcında sunacağı iş planını projenin planlama aşamasında İdare ile birlikte detaylandıracak ve İdare'nin onayına sunacaktır.

Yüklenici, çalıştıracağı her personelin, İdare yetkililerinin iletişim noktası personelin kimler olduğunu, mesai içi ve mesai dışı saatlerde bu kişilere ulaşılabilecek telefon numaraları konusunda bilgilenmesini sağlamaktan sorumlu olacaktır.

İstekli, son 2 yıl içinde kamuda gerçekleştirdiği ihale konusu iş veya benzer işlerle ilgili iş deneyimine ilişkin belgelerini teklifinde verecektir. BGYS kapsamında yapılan işler benzer iş olarak kabul edilecektir.

İstekli, güncel e-posta ve posta adresi ile telefon ve faks numaralarını içeren iletişim bilgilerini teklifinde verecektir.

Teklif değerlendirme aşamasında, İstekli ve denetim ekibi hakkında İdare tarafından güvenlik soruşturması yaptırılabilecektir.

İstekli, teklifini TL cinsinden verecektir.

<u>İstekli Denetim ve Sızma testi aşamalarını ayrı ayrı fiyatlandıracaktır.</u>

SIZMA TESTİ İLE İLGİLİ TEKNİK ŞARTLAR

1. SIZMA VE DOĞRULAMA TESTİ HİZMETİ

1.1.Sızma Testinin Gizliliği ve Yüklenicinin Sorumlulukları

1.1.1. İşbu şartname ile tanımlanan tüm yükümlülükleri yerine getirecektir.

1.1.2. 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 testi raporunda kullanıcı adı ve parolaları maskelenmelidir.

1.1.3. Sızma testleri esnasında Yüklenici, sadece kuruluşa ait içeriklere erişim sağlanabildiğini göstermeli, bunun dışında kuruluşa ait içeriklerin tamamına erişim sağlayarak tüm içeriği kopyalamamalı ve üçüncü taraflar ile paylaşmamalıdır. Yüklenicinin içeriklere erişim sağlandığını gösterebilmesi için gerekiyorsa örnek olarak birkaç kayıt delil sağlamak amacıyla kopyalayabilir.

1.1.4. İş başlangıcında idare tarafından yükleniciye verilen bilgi dokümanlar ve benzeri ve iş sonunda yüklenici tarafından hazırlanan raporlar çıktılar ekran görüntüleri ve benzeri idareye testinden sonra yüklenici tarafından kesinlikle depolayacak ve üçüncü taraflarla paylaşılmayacaktır işlerle ilgili tüm bilgiler Network'te projeleri kullanılan protokol bilgileri güvenlik zafiyetleri raporlar ve benzeri aksi yazılı olarak belirlenmedikçe gizli olarak kabul edilecektir

1.1.5. Raporlar özellikle sunumlarda kullanılmamalı ve örnek mahiyetinde diğer kuruluşlara gösterilmemelidir.

1.2.Sızma testi süreci

Buna testi olarak keşif açık bulma açıklık testi raporlama doğrulama aşamalarından oluşmalıdır sızma testi en az aşağıdaki konuları içermelidir;

1.2.1. İletişim altyapısı ve aktif cihazlar sızma testleri

1.2.1.1.Kurumda kullanılan ağ cihazlarının genel mimari içindeki yeri incelenecektir

1.2.1.2.Cihazların tespiti

1.2.1.3.Tespit edilen cihazların marka modern ve sürüm belirlenmesi

1.2.1.4.Parola ve ayarların kontrolü

1.2.1.5.Üretici yamaları ve uygulanması

1.2.1.6.VLAN güvenlik kontrollerinin yapılması

1.2.1.7.Ele geçirme saldırıları

1.2.1.8.Aktif cihaz üzerinde çalışan servisler incelenecektir

1.2.1.9.MITM (Man in the middle) kontrolleri yapılacaktır

1.2.1.10. Kurum içinde bulunan VOIP hizmetinin testleri

1.2.2. DNS servisleri güvenlik testleri

1.2.2.1.DNS sunucuların topolojik incelenmesi

1.2.2.2.DNS sunucusunun alan yapılandırılmasında yer alan kayıtların ortaya çıkartılması

1.2.2.3.Sunucu üzerinden alan transferi (zone transfer) yapılmaya çalışılacaktır
1.2.2.4.NXT ve NSEC kaynak kayıtları üzerinden bilgiler elde edilmesi
1.2.2.5.Pasif sorgularla bilgi toplanması
1.2.2.6.DNS sunucular için ön bellek zehirlemesi kontrolü
1.2.2.7.DNS sunucular üzerindeki kaynak kayıt girdileri kontrolü
1.2.2.8.DNS sunucuların sürüm bilgisi
1.2.2.9.Kurum dışı alan adı sorguları
1.2.2.10. Sunucular üzerinde DNS dışında bir servisin çalışıp çalışmadığı
1.2.2.11. Güvenlik duvarında DNS sunucular için izin verilen ayarların kontrolü
1.2.2.12. Dns sunucuların zafiyet taraması
1.2.2.13. Dns servisini veren yazılımın açıklıkları araştırılması

1.2.3. Etki alanı ve kullanıcı bilgisayarları güvenlik testleri

1.2.3.1. Etki alanında güvenlik politikaları kontrol edilmesi
1.2.3.2. Etki alanındaki ilgili kullanıcıların ayrıcalıkları ve kullanım şekillerinin kontrolü
1.2.3.3. Yama yönetim politikaları
1.2.3.4. Virüs koruma politikaları
1.2.3.5. Hassas bilgi içeren ve yetkisiz erişime olanak sağlayan paylaşım kontrolleri
1.2.3.6. Aygıtların kullanımıyla ilgili güvenlik ayarları
1.2.3.7. Yerel kullanıcı hesabı ve kullanıcı grupları kontrolleri
1.2.3.8. Bilgisayarların fiziksel saldırılara karşı güvenilirliği a haritalaması

1.2.4. E-posta servisleri güvenlik testleri

1.2.4.1. E-posta sunucularının topolojik konumu
1.2.4.2. Virüs tarayıcı ağ geçitlerinin sürüm bilgisi ve açıklarının tespit edilmesi
1.2.4.3. Relay zafiyetlerinin tespit edilmesi
1.2.4.4. E-posta sunucular üzerinde başka servislerin tespiti
1.2.4.5. E-posta sistemi kimlik doğrulama sisteminin denetimi
1.2.4.6. E-posta sunucusu üzerinde ilgili servislerin kontrolleri (IMAP, POP3)
1.2.4.7. Zafiyet taraması
1.2.4.8. İzin verilen e-posta boyutu kontrolü
1.2.4.9. E-posta listesi uygulamalarının zafiyet taramaları

1.2.5. Veri tabanı sistemleri güvenlik testleri

1.2.5.1. Veri tabanı sunucusunun topolojik konumu
1.2.5.2. Yamaların kontrolü
1.2.5.3. Veri tabanı için önemli olan işletim sistemi dosyalarının erişim izinleri
1.2.5.4. Veri tabanı sunucusunun, güvenlik ayarları
1.2.5.5. Veri tabanı sunucusunun, parola politikası kullanıcı hesapları güvenlik ayarları
1.2.5.6. Veri tabanı sunucusunda, güvenlik açısından önemli olan paketler nesneler roller tablo ve hakların kontrolü
1.2.5.7. Veri tabanı sunucusunda, denetleme mekanizmasının kontrolü

1.2.5.8. Veri tabanı sunucusunun yedekleme ve kurtarma mekanizması
1.2.5.9. Veri tabanının kurulumu ile gelen ve kullanıcılar için atanan varsayılan değerlerin kontrolü
1.2.5.10. Uzaktan erişimin güvenlik kontrolleri

1.2.6. WEB Uygulamaları Güvenlik Testleri

1.2.6.1. veri kontrolleri

1.2.6.1.1. girdi denetime
1.2.6.1.2. çıktı denetime
1.2.6.1.3.değiştirilen içeriğin tespiti
1.2.6.1.4.HTML etiketlerinin filtrelenmesi
1.2.6.1.5.SQL sokuşturma
1.2.6.1.6.Sunucu taraflı girdi denetime
1.2.6.1.7.URL Yönlendirmeler/ Diğer Sokuşturma/XSS
1.2.6.1.8.HTTP yanıt bölme

1.2.6.2. Oturum Yönetimi

1.2.6.2.1. Giriş sonrası oturum bilgisi yenileme, oturum sabitleme
1.2.6.2.2. Çerezlerin içeriği
1.2.6.2.3. Oturum sonlandırma
1.2.6.2.4. Oturum bilgisinin URL içinde taşınması
1.2.6.2.5. Oturum çalma (Session Riding)

1.2.6.3. CSRF

1.2.6.4. İlk yönetimi doğrulama ve iş mantığı

1.2.6.4.1. Yetki artırımı/ yetki dışı işlem/ şifre politikaları
1.2.6.4.2. Bilinen hesap/şifre bileşenlerinin denenmesi
1.2.6.4.3. Basit Kimlik Doğrulama Kullanımı/Kimlik Doğrulamanın Atlatılması/Çıkış İşlevi
1.2.6.4.4. Path traversal
1.2.6.4.5.Bypass Authorization
1.2.6.4.6. Privilege Escalation
1.2.6.4.7.uygulama mantığı kontrolleri

1.2.6.5. WEB SERVİS TESTLERİ

1.2.6.5.1. Web Servislerinin Tespiti/ Web Servisi Detay Tarama/ REST
1.2.6.5.2. SOAP
1.2.6.5.3. Ajax
1.2.6.5.4. Bilgi sızdırma ve Ayar yönetim
1.2.6.5.5. Yardım sayfaları SSL kullanımı/ HTML comment/ sunucu bilgisi
1.2.6.5.6. Ayrıntılı hata mesajları
1.2.6.5.7.Dosya Uzantıları/ Yedek Dosyalar/ Yönetici Ara Yüzü
1.2.6.5.8. Desteklenen HTTP metotları ve XST açıklığı
1.2.6.5.9. Sitelerin SSL Sertifikasının Geçerlilik Testi
1.2.6.5.10. Metadata kontrolleri

1.2.6.6. YEREL TESTLER

1.2.6.6.1. WEB uygulama temelli testler
1.2.6.6.2. XSS ve HTML ekleme (Injection)
1.2.6.6.3. Command Injection
1.2.6.6.4.CSRF
1.2.6.6.5. SQL Injection
1.2.6.6.6. Web Çerezlerinin incelenmesi

1.2.6.7. Kimlik denetimi ve yetkilendirme

1.2.6.7.1.Kimlik doğrulama atlatma
1.2.6.7.2.OTP ve çok faktörlü kimlik doğrulama
1.2.6.7.3.Yerelde saklanan verilerin manipülasyonu

1.2.6.8.Dosya sistemi incelemesi

1.2.6.8.1.Dosya sistemi izinleri
1.2.6.8.2.Ön bellekte veri saklama,
1.2.6.8.3.Cihaz üzerinde şifrelenmiş veri saklama,
1.2.6.8.4.Kullanıcı adı/parola, cihaz ID, kişisel/hassas veri,
1.2.6.8.5.Uygulama yedekleri.
1.2.6.8.6.Silinmiş verilerin geri döndürülmesi

1.2.6.9.Bellek incelemesi

1.2.6.9.1 Bellekte tutulan hassas verilerin kontrolü

1.2.7. Uzak (Remote) Testler

1.2.7.1 Kimlik Denetimi ve Yetkilendirme

1.2.7.1.1 Parola uzunluk ve karmaşıklık gereksinimleri,
1.2.7.1.2. Otomatik saldırılar hesap kitleme,
1.2.7.1.3. Tek noktadan kimlik doğrulama (SSO),
1.2.7.1.4. OTP ve 2 faktörlü kimlik doğrulama,
1.2.7.1.5. Arkadaki sunucu ve servislerine doğrudan/ yetkisiz erişim,
1.2.7.1.6. Yatay ve dikey yetki aşımları

1.2.7.2. Oturum Yönetimi

1.2.7.2.1 Entropi incelemesi
1.2.7.2.2 Cihaz ID bağımlı oturum
1.2.7.2.3 Oturum anahtarlarının yaşam döngüsü ve sonlandırılması
1.2.7.2.4 Yetki aşımı
1.2.7.2.5 Oturum anahtarlarının cihaz üzerinde tutulması

1.2.7.3. İletim katmanı testleri

1.2.7.3.1 Aradaki adam saldırıları
1.2.7.3.2. İzinsiz dinleme
1.2.7.3.3. SSL kontrolleri

1.2.7.4. Sunucu Tarafı Testleri

1.2.7.4.1 SQL injection
1.2.7.4.2. XSS
1.2.7.4.3. Open Redirect
1.2.7.4.4. Tampon bellek taşıması
1.2.7.4.5. XML/ JSON temelli saldırılar
1.2.7.4.6.İşlenmeyen (Unhandled) durumların tespiti
1.2.7.4.7.Kısıtlanmamış dosya yükleme

1.2.8. Kablosuz Ağ Güvenlik Testleri

1.2.8.1. Kurumun tamamında Rouge, merkezi yönetilmeyen gibi erişim noktası tespiti
1.2.8.2. Kurum dahilinde kullanılan kablosuz altyapının kontrolü
1.2.8.3. Kullanılan PSK'lere kırma denemeleri
1.2.8.4. Kablosuz yanıltma saldırıları

1.2.9. Sosyal Mühendislik Testleri

1.2.9.1. Arama motorları, sosyal ağlar ve kurum web siteleri kullanılarak, kurum ve çalışanları hakkında bilgi toplama
1.2.9.2. Google hacking (Google cache'de kuruma ait dosya, veri tabanı, URL, önemli data olup olmadığı) yapılacak
1.2.9.3. Kurum içinden veya dışından Telefon iletişimi ile hassas bilgilerin erişimin denenmesi
1.2.9.4. E-postalar ile kurum içine sızmaya çalışılması

1.3. Sızma Testi Kapsam

Talep Edilen Hizmetler			
Lütfen talep ettiğiniz hizmeti seçiniz.			
İletişim Altyapısı ve Aktif Cihazlar	: ☒	DNS Servisleri	: ☒
Etki Alanı ve Kullanıcı Bilgisayarlar	: ☒	E-posta Servisleri	: ☒
Veri tabanı Sistemleri	: ☒	Web Uygulamaları	: ☒
Mobil Uygulamalar	: ☐	Kablosuz Ağ Sistemleri	: ☒
ATM Sistemleri	: ☒	Dağıtık Servis Dışı Bırakma Testleri	: ☒
Sosyal Mühendislik Testleri	: ☒		

İnternet Üzerinden Güvenlik Denetim Hizmeti			
Test Edilecek Dış IP Listesi	Bir adet /27 – Bir adet /32		
İnternet Üzerinden Test Edilecek Sunucu Bilgileri	Web Sunucu: 14	DNS Sunucu: 3	Firewall/VPN: 1
	Mail Sunucu: 2	FTP Sunucu:	Diğer:

Web Uygulamalarına Yönelik Güvenlik Denetim Hizmeti			
Test Edilecek Web Uygulama ve Sunucu Sayısı			
Test Edilecek Web Uygulamalarına Ait URL'ler	**Uygulama URL'i**	**Teknoloji (.NET,PHP,JAVA, vb.)**	**Test Hesabı Verilecek mi? ***
	23 adet web uygulaması	7 adet .net, 1 adet php	Hayır

Yerel Ağ İçinden Gerçekleştirilecek Güvenlik Denetim Hizmeti Bilgileri				
Yerel Ağ İçinden Test Edilecek Toplam İç IP Sayısı	Sütlüce : Bir adet / 16 Kü çükyalı : Bir adet /16 Veri merkezi : blok 1 : Bir adet /29 blok 2 : Bir adet /27 blok 3 : Bir adet /25 DMZ : Bir adet /24			
Test Edilecek Sunucu Bilgileri	Web Sunucu: 14	DNS Sunucu: 3	Firewall/VPN: 1	
	Mail Sunucu: 2	SFTP Sunucu:	Veri Tabanı:	
	Domain Controller: 3	Router/Switch:93	Diğer:	
Kullanılan Veritabanı Sistemleri	Oracle: x	MSSQL: x	MYSQL: x	Diğer:
Kullanılan İşletim Sistemleri	Windows 7 - Windows 10 – windows 11			
Çalışmanın Gerçekleştirileceği Lokasyon (lar)	Sütlüce ve Küçükyalı kampüsleri			

1.4. Diğer Teknik Hususlar

1.4.1. 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 kuruma sunacaktır.

1.4.2. Test yapılacak sunucu bilgileri Kurum tarafından verilecektir.

1.4.3. 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.) kurum tarafından yükleniciye verilecektir.

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

1.4.5. İş sonucu hazırlanacak olan ilgili raporlarda;

* Tespit edilen güvenlik zafiyetleri, ekran çıktıları

* Bu zafiyetlerin sebep olabileceği zararlar/ sonuçları ve zafiyete ilişkin referans bilgileri

Güvenlik zafiyetleri gidermek için yapılması gerekenler, detaylı şekilde açıklanacaktır.

1.4.6. İş sonucunda oluşturulan raporlar, elektronik ortamda Microsoft Word veya PDF formatında kuruma sunulacaktır.

1.4.7. İş sonucunda üretilmiş olan raporların tüm telif hakları Kurum'a aittir.

1.4.8. İş kapsamında hazırlanan sızma ve zafiyet testi raporunda projeler için tespit edilen zafiyetler raporlanacaktır.

1.4.9. İş kapsamında hazırlanan sızma ve zafiyet testi raporunda tespit edilen güvenlik zafiyetleri kritiklik seviyelerine (kritik, yüksek, normal) göre gruplandırılacak ve sınıflandırmanın nasıl yapıldığı ilgili raporda açıklanacaktır.

1.4.10 İş kapsamında hazırlanan sızma ve zafiyet testi raporunda, tespit edilen bir güvenlik zafiyeti söz konusu zafiyeti bulunduran sistemler bazında gruplandırılır.

1.4.11. İş kapsamında hazırlanan sızma ve zafiyet testi raporunda, tespit edilen her güvenlik zafiyeti için alınması gereken önlem/ önlemler Yüklenici tarafından belirlenmeli ve raporlanmalıdır.

1.4.12 İş kapsamında yapılacak olan sızma ve zafiyet testlerinde şirket iç ağının (intranet) ve/veya sistem ortamlarının kullanılması gerektiği durumda işi yapacak olan Yüklenici personeli, ilgili lokasyona Kurum izni ile girecektir.

1.4.13. İş Kapsamında kullanılacak olan bilgisayar, yazılım lisansları ve gerekli donanımlar Yüklenici tarafından temin edilecektir.

1.4.14 İş kapsamında kullanılacak olan işletim sistemi yazılımları, tarama yazılımları, uygulama sunucu yazılımları vb. yazılımla ve lisansları yüklenici tarafından temin edilecektir. Kurum lisanslama ile ilgili herhangi bir yükümlülüğe girmeyecektir. Tüm lisans sorumluluğu Yükleniciye aittir.

1.4.15. İş kapsamındaki sistemler üzerinde yüklenici tarafından yapılacak sızma ve zafiyet testleri, projenin topolojisine göre hem intranet hem internet üzerinden yapılacaktır. Yüklenici bu iş için ilave ücret talep etmeyecektir.

1.4.16. İş kapsamında yapılacak olan sızma ve zafiyete testlerinde kullanılması gerekebilecek olan test kullanıcı hesapları ve özel kullanıcı bilgileri (credentials) Kurum tarafından Yüklenicinin kullanımına verilebilecektir. Söz konusu bilgilerin verilip /verilmeyeceğine Kurum karar verecektir.

1.4.17. İş kapsamında hazırlanan raporlar, tespit edilen açıklar kullanılarak gerçekleştirilen bir atak bulunması durumunda ekran görüntüleri ve/ veya video çekimlerini içermelidir.

1.4.18. Yüklenici zafiyet raporunu sunduktan sonra, 3 ay içerisinde Kurum'un talebi üzerine tespit edilen bulgular üzerinden yeniden değerlendirme testi yapacaktır.

1.4.19. Yüklenici, sağladığı personelin uzmanlığının yeterli olmadığı durumlarda, çözüm odaklı uzman personel sağlamakla yükümlüdür. Yüklenici sağlamış olduğu uzman personel ile ilgili özgeçmiş bilgilerini önceden İdare ile paylaşacaktır ve İdarenin onayından sonra uzman personel çalışmaya başlayacaktır. Yüklenici, sözleşme süresince sorunlar giderilene kadar teknik uzman hizmeti verecektir.

1.4.20. İdare, Yüklenici personelinin yetersiz bulunduğu veya tutum ve davranışları uygun görülmediği takdirde personelin değiştirilmesi talebinde bulunabilir. İdarenin söz konusu personelin değiştirilmesi isteğini yazılı olarak Yükleniciye bildirdiği tarihten itibaren en geç 15 (onbeş) iş günü içerisinde personel, İdare tarafından uygun görülen kişi ile değiştirilecektir.

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

DENETİM FAALİYETLE İLGİLİ TEKNİK ŞARTLAR

Yüklenici tarafından Rehber yapısının işleyişinin kontrol edilerek, aksayan noktalarını tespit etmek amacıyla bir iç tetkik çalışması yapılacaktır.

İç tetkik raporu tetkikin tamamlanmasından en geç 3 (üç) iş günü içerisinde teslim edilecektir.

Yapılacak denetim faaliyeti Bilgi ve İletişim Güvenliği Denetim Rehberine uygun olarak yapılacaktır.

Denetim hizmetinde Bilgi ve İletişim Güvenliği Denetim Rehberinde belirtilen aşağıdaki formlar yüklenici tarafından hazırlanacaktır.

Ek–A Denetim Ekibi Bilgisi,

Ek–B Varlık Grupları Ve Denetim Kapsamı,

Ek–C Denetim Programı

Ek–D Çalışma Formu

Ek–E Rehber Uygulama Süreci Etkinlik Durumu,

Ek–F Tedbir Etkinlik Durumu

Ek–G Bulgu Tablosu

Ek–H Denetim Görüşü

Denetim hizmeti en az aşağıdaki kontrolleri içerecektir.

Ağ ve sistem güvenliği tedbirlerinin etkinliğinin değerlendirilmesi

Uygulama ve veri güvenliği tedbirlerinin etkinliğinin değerlendirilmesi

Taşınabilir cihaz ve ortam güvenliği tedbirlerinin etkinliğinin değerlendirilmesi

Nesnelerin interneti (IoT) cihazlarının güvenliği tedbirlerinin değerlendirilmesi

Personel güvenliği tedbirlerinin etkinliğinin değerlendirilmesi

Fiziksel mekânların güvenliği tedbirlerinin etkinliğinin değerlendirilmesi

Kişisel verilerin güvenliği tedbirlerinin etkinliğinin değerlendirilmesi

Anlık mesajlaşma güvenliği tedbirlerinin etkinliğinin değerlendirilmesi

Bulut bilişim güvenliği tedbirlerinin etkinliğinin değerlendirilmesi

Kripto uygulamaları güvenliği tedbirlerinin etkinliğinin değerlendirilmesi

Yeni geliştirmeler ve tedarike yönelik güvenlik tedbirlerin etkinliğinin değerlendirilmesi

İşletim sistemi sıkılaştırma tedbirlerinin etkinliğinin değerlendirilmesi

Veri tabanı sıkılaştırma tedbirlerinin etkinliğinin değerlendirilmesi

Sunucu sıkılaştırma tedbirlerinin etkinliğinin değerlendirilmesi

Varlık grupları için yapılan mevcut durum ve boşluk analizlerinin değerlendirilmesi,

Telafi edici kontrollerin değerlendirilmesi,

Rehber uygulama yol haritasının değerlendirilmesi

İŞİN KABULÜ

Yüklenici, çalışmalarını Kurum'a sunduğu Proje Planına uygun olarak yapacaktır.

Yüklenici, hizmetlerini 15 (on) takvim günü içerinde tamamlayacaktır.

Yüklenici, ilgili hizmetleri tamamladıktan sonra kabul için Kurum'a başvurusunu yapacaktır.

Yüklenici, dokümantasyonu kabul sürecinden önce tamamlayacaktır.