İSTANBUL TİCARET ÜNİVERSİTESİ

BİLGİ SİSTEMLERİ GÜVENLİĞİ KAPSAMINDA

TEKNİK AÇIKLIK TESTLERİ

VE

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBER UYUM DENETİMİ

HİZMETLERİ ALIMI TEKNİK ŞARTNAMESİ

1. GİRİŞ

1.2. İşin Tanımı

İstanbul Ticaret Üniversitesi bünyesinde kurulu bulunan bilgi işlem altyapısı kapsamında,

i) Teknik Açıklık Testlerinin gerçekleştirilmesi
ii) Bilgi ve İletişim Güvenliği Rehberi'ne uyum Denetiminin Yapılması

Hizmetlerinin verilmesini kapsamaktadır.

1.2. Tanımlar ve Kısaltmalar

İDARE / Kurum	Ticaret Üniversitesi
BİDB	Ticaret Üniversitesi Bilgi Teknolojileri Daire Başkanlığı
YÜKLENİCİ	İDARE ile sözleşme imzalayan firma
BTHYS	Bilgi Teknolojileri Hizmet Yönetim Sistemi
BT	Bilgi Teknolojileri
TÜRKAK	Türk Akreditasyon Kurumu
TSE	Türk Standartları Enstitüsü
CISSP	Certified Information Systems Security Professional
PMP	Project Management Professional
CEH	Certified Ethical Hacker
CCEE	Common Criteria Expert Evaluator
ISECOM	The Institute for Security and Open Methodologies
OSSTMM	The Open Source Security Testing Methodology Manual
OPST	OSSTMM Professional Security Tester Accredited Certification
DOS	Denial of Service
ISO	International Organization for Standardization
BGYS	Bilgi Güvenliği Yönetim Sistemi
SOME	Siber Olaylara Müdahale Ekibi

2. AMAÇ

Bu teknik şartname kapsamında alınacak hizmet ile aşağıdaki çalışmaların tamamlanması hedeflenmektedir:

- Bilişim ortamlarındaki teknik açıklık testlerinin (sızma testi) gerçekleştirilmesi, zafiyet içeren alanların belirlenerek raporlanması ve bunların giderilmesi için gerekli yönlendirmelerin yapılması.

- Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yayınlanan Bilgi ve İletişim Güvenliği Rehberi Uyum denetimi yapılması.

3. TEKNİK AÇIKLIK TESTLERİ

3.1 YÜKLENİCİ, Sızma testi ve güvenlik denetimi süresince, kurumun domain ve subdomain'lerinde ve internet üzerinden erişilebilirliği olan IP adres aralığında çalışan sunucularındaki güvenlik açıklarını tarayacak, güvenlik açıkları ve riskleri tespit edecektir.

3.2 Güvenlik denetimi sırasında İDARE hakkında edinilebilecek bilgiler nedeniyle söz konusu denetimi gerçekleştirecek YÜKLENİCİ'nin, bu işlevi T.C. vatandaşı olan bir ekip ile Türkiye sınırları dâhilinden gerçekleştirmesi zorunludur. Yurtdışından gerçekleştirilecek güvenlik denetimi işlemleri kabul edilmeyecektir.

3.3 YÜKLENİCİ, denetimi gerçekleştirecek uzman/uzmanların açık özgeçmişleri ve projede alacakları görevleriyle birlikte tanıtacaktır.

3.4 Denetimi gerçekleştirecek uzmanda/uzmanlarda, başarılı olarak sonuçlandırılmış en az 1 (bir) adet Üniversite Teknik Açıklık Testi Projesi gerçekleştirmiş olma şartı aranacaktır.

3.5 YÜKLENİCİ işe başlamadan önce, söz konusu güvenlik denetimini nasıl bir metodoloji kullanarak gerçekleştireceğini, adımları ile detaylı olarak açıklamalıdır. Bu metodoloji adımlarının gerçekleştirilmesinde kullanılan metot ve araçlar açıkça tarif edilmelidir. Sadece otomatik güvenlik tarama araçlarıyla gerçekleştirilen güvenlik tarama işlemleri kabul edilmeyecektir.

3.6 Güvenlik Denetimi çalışmasının tamamlanmasını izleyen 15 (onbeş) iş günü içerisinde YÜKLENİCİ, denetim raporunu İDARE'ye iletecek ve takip eden 10 (on) iş günü içerisinde İDARE tarafından uygun görülecek zamanda sunumunu gerçekleştirecektir.

3.7 Denetim çalışması kapsamında mesai saatleri içinde hizmet kesintisi (DoS/DDoS-Denial of Service vb.) saldırıları gerçekleştirilmeyecektir. YÜKLENİCİ, istenmeden neden olunabilecek hizmet kesintileri durumunda İDARE'yi en kısa sürede bilgilendirecektir.

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

3.9 Test aşağıda belirtilen kapsamda gerçekleştirilecektir:

- İletişim Altyapısı ve Aktif Cihazlar
- DNS Servisleri
- Etki Alanı ve Kullanıcı Bilgisayarları
- E-Posta Servisleri
- Veri tabanı Sistemleri
- Web Uygulamaları
- Kablosuz Ağ Sistemleri
- Dağıtık Servis Dışı Bırakma Testleri
- Sosyal Mühendislik Testleri
- Sanallaştırma Sistemleri

3.10 Testler, ihtiyaç halinde testin türüne göre aşağıdaki kullanıcı tipleri ile yapılacaktır:

- İnternet Kullanıcısı Profili: İnternet üzerinde İDARE'nin internet servislerine erişebilen ve internet uygulamasına giriş yetkilerine sahip olmayan kullanıcıyı temsil eder. İDARE'ye ait internet uygulamasına giriş yetkilerine sahip olmayan kullanıcıların sistem için oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılacaktır.

- Misafir Profili: İDARE personeli dışında, İDARE'nin kablolu ve kablosuz ağını kullanarak kurumun bilişim hizmetlerinden yararlanacak kullanıcı profili üzerinden test edilecektir.

- Uygulama Kullanıcısı Profili: İnternet üzerinde İDARE'nin internet servislerine erişebilen ve internet uygulamasına giriş yetkilerine sahip olan kullanıcıyı temsil eder. İDARE'ye ait internet uygulamasına giriş yetkilerine sahip olan kullanıcıların sistem için oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılacaktır.

- E-posta Kullanıcısı Profili: Gerek internet gerekse iç ağdan e-posta servislerini kullanabilen kullanıcıları temsil eder. Bu yetkiye sahip kullanıcıların sistem için oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılacaktır.

- İDARE Personeli Profili: Personelin çalışma ortamını kullanarak sahip olduğu yetkiler ile sistemde oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılacaktır. Bu profil ile gerçekleştirilecek testlerde, kurum

çapında en yaygın olarak kullanılan çalışan profilinin seçilmesinin yanında, yerel yönetici (local admin) yetkisine sahip çalışan profilleri ile de sızma testleri gerçekleştirilecektir. Testi yapan kişi/kuruluşa idare tarafından tanımlanan erişim yetkileri ve verilen izinler raporda açıkça ifade edilecektir.

- Diğer kullanıcı profilleri: Sızma testlerinin, yukarıda tanımlanan diğer kullanıcı profiline uymayan bir kullanıcı profili ile gerçekleştirilmesi durumunda, kullanılan her bir profil için tanımlanan hak ve yetkiler bu başlık altında açıkça ifade edilir.

3.11 Testler, aşağıdaki erişim noktaları üzerinden gerçekleştirilecektir:

- Kurum Dışı Ağı: Kurumun internet üzerinden erişilebilen tüm sunucu ve servislerine internet üzerinden erişilerek sızma testleri gerçekleştirilir.
-
- Kurum İç Ağı: Kurumun iç ağında yer alan ve test kapsamında ele alınan sunuculara Kurum iç ağı üzerinden erişilerek sızına testleri gerçekleştirilir. Ağ ve ağ trafiği üzerinde gerçekleştirilecek testler için de bu ağ kullanılır ve testi gerçekleştirecek şahıslara kullanımı en yaygın olan çalışan bilgisayarı profilinde bilgisayarlar sağlanır.

- Sunucu Konsolu: Bazı testler için sunucu konsolundan erişim ihtiyacı oluşması durumunda, sistem yöneticilerinin kontrolünde ve gözetiminde erişim sağlanarak testler gerçekleştirilecektir.

3.12 Test Metodolojisi aşağıda tanımlandığı şekilde uygulanacaktır:

- Sızma testleri, yukarıda detaylandırılan kullanıcı profilleri ile tanımlanan erişim noktalarından gerçekleştirilecek temel sızma testleri ve detaylı sızma testlerinden oluşacaktır.
- Temel sızma testleri sistem tespiti, servis tespiti ve açıklık taraması/araştırması adımları ile başlayacak ve her bir erişim noktası kapsamında uygulanacak adımlar ile devam edecektir.
- Temel sızına testleri sonrası saptanan açıklık ve bulgular, detaylı sızma testlerinin gerçekleştirilmesi suretiyle ayrıntılı olarak incelenerek raporlanacaktır.
- Temel sızına testi, bilgi toplama, zafiyet taraması, ağ haritası tespiti, envanter tespiti vb. adımlardan oluşmaktadır.
- Detaylı sızma testi, temel sızına testinde elde edilen bilgiler ışığında otomatik ve manuel araçlar kullanılarak sistemlere sızma çalışmalarının gerçekleştirilmesidir.

- Sızma testleri gerçekleştirilirken her bir test başlığı kapsamında saptanan açıklık ve bulgular, ayrı ayrı değerlendirilmenin yanında, bir araya geldiklerinde oluşturabilecekleri riskler ve açıklıklar açısından da değerlendirilecek ve bu birlikte değerlendirme sonucu ortaya çıkan yeni açıklık ve bulgular da raporlanacaktır.
- Sızma testleri gerçekleştirilirken, İDARE faaliyetlerinin aksamamasına ve hizmet kesintisine yol açmayacak yöntemler kullanılmasına dikkat edilecektir. Hizmet kesintisine yol açabilecek tüm testler İDARE ile koordineli bir şekilde planlanarak gerçekleştirilecektir.

3.13 Teknik açıklık testleri kapsamında en az aşağıdaki alanlarda testler gerçekleştirilecektir:

3.13.1 İDARE'nin ağ altyapısı ve aktif ağ cihazlarına yönelik asgari olarak aşağıdaki testler gerçekleştirilecektir.

- İDARE'de kullanılan ağ cihazlarının genel mimari içindeki yeri incelenecektir.
- Tüm ağ cihazları açıklık bulma araçları ile taranacaktır.
- Tespit edilen açıkların uygulanabilirlikleri sınanacaktır.
- Ağlarda MAC adresi tabanlı filtrelemenin olup olmadığı incelenecektir.
- Aktif cihaz üzerindeki port güvenliği, VLAN ve trunk yapısı incelenecektir.
- Ağ topolojisi ve alt bölümleri incelenerek kullanıcı-sunucu ağları arasında erişim kontrolünün olup olmadığı kontrol edilecektir.
- Paket dinlemesi yoluyla ağ üzerinden geçebilecek VolP paketleri yakalanmaya ve konuşmalar dinlenmeye çalışılacaktır.
- Aktif cihaz üzerinde çalışan servisler incelenecektir.
- Kullanılan servislerin servis dışı bırakılmayla sonuçlanabilecek saldırılara karşı (ARP zehirlemesi, CDP DOS, DHCP DOS, SNMP Dos vb.) durumu incelenecektir.
- Cihazlar üzerinde açık olan Telnet, HTTP, FTP, SNMP, TFTP, SSH vb. servislerine sözlük saldırısı veya kaba güç kullanılarak erişim sağlanmaya çalışılacaktır.
- Erişim sağlanan cihazlar üzerinden alınan bilgilerle diğer cihazlara erişilmeye çalışılacaktır.
- Aktif cihazlar için uzak/yerel erişim kontrolü, yönetim, kayıt ve kimlik doğrulama mekanizmaları incelenecektir.
- Cihazların merkezi şekilde yönetilmesini ve gözetlenmesini sağlayan yönetim sistemlerinin varlığı araştırılacak, bu sistemlere sızma girişimlerinde bulunulacaktır.
- Cihazlarda ortak parolanın kullanılıp kullanılmadığı test edilecektir.

- İDARE çalışanları için kullanılan içerik filtreleme sistemleri atlatılmaya çalışılacaktır.
- Kurum içinden dışarı tünel kurulmasıyla, kurum dışından kurum içine yetkisiz bağlantı gerçekleştirilmeye çalışılacaktır.
- Kurum dışına açık yönetim ara yüzlerinin varlığı kontrol edilecektir.

3.13.2 Kurumun DNS servislerine yönelik asgari olarak aşağıdaki testler gerçekleştirilecektir:

- DNS sunucuların topolojik konumu incelenecektir.
- DNS Sunucusunun alan yapılandırmasında yer alan kayıtlar ortaya çıkarılmaya çalışılacaktır.
- Sunucu üzerinden alan transferi (zone transfer) yapılmaya çalışılacaktır.
- NXT ve NSEC kaynak kayıtları üzerinden bilgi elde edilmeye çalışılacaktır.
- Netcraft, Google, Whois sorguları yapılarak Kurum alanında yer alan sunucular tespit edilmeye çalışılacaktır.
- DNS sunucular için ön bellek zehirlemesi gerçekleştirilmeye çalışılacaktır.
- DNS sunucular üzerindeki kaynak kayıt girdileri incelenecektir.
- DNS sunucular üzerindeki ters kaynak kayıt girdileri incelenecektir.
- DNS sunucuların sürüm bilgisi elde edilmeye çalışılacaktır.
- Kurum dışı alan isimleri sorgulanmaya çalışılacaktır.
- Sunucular üzerinde DNS dışında bir servisin çalışıp çalışmadığı incelenecektir.
- Güvenlik Duvarında DNS sunucular için izin verilen portlar incelenecektir.
- DNS sunucuları güvenlik taramasına tabi tutulacaktır.
- DNS servisini veren yazılımın açıklıkları araştırılacaktır.

3.13.3 Kurum etki alanı (domain) sisteminde ve kullanıcı bilgisayarlarında asgari olarak aşağıdaki testler gerçekleştirilecektir:

- Kullanıcı bilgisayarlarının açılış ayarlarındaki eksiklikler tespit edilip, yerel yönetici hakları elde edilmeye çalışılacaktır.
- Yerel yöneticilerin kullanımındaki zafiyetler ile hak yükseltme saldırıları gerçekleştirilecektir.
- Etki alanındaki şifre politikası ve şifre saklama politikasındaki zafiyetler tespit edilip, kullanıcı hesaplarının şifreleri ele geçirilmeye çalışılacaktır.

- Yama yönetimindeki zafiyetler ve desteği kaldırılmış eski sistemler tespit edilip, uzaktan kod çalıştırma ve hak yükseltme saldırıları gerçekleştirilecektir.
- Yetkisiz erişime imkân tanıyan dosya paylaşımları tespit edilerek, bu paylaşımlar ve paylaşımlardaki hassas veriler yoluyla hak yükseltme saldırıları gerçekleştirilecektir.
- Hak yükseltme saldırıları ile etki alanı kullanıcılarının hesapları ele geçirilmeye çalışılacaktır.
- Etki alanında yönetici haklarına sahip kullanıcı hesapları ve kullanıcı hesabı gruplarının kullanımındaki zafiyetler kullanılarak hak yükseltme saldırıları gerçekleştirilecektir.
- Elde edilen şifre ve haklar ile hassas bilgilerin bulunduğu sunucu ve kullanıcı bilgisayarlarına erişim sağlanmasına çalışılacaktır.

3.13.4 Kurumun e-posta servislerinde asgari olarak aşağıdaki testler gerçekleştirilecektir:

- E-posta sunucularının topolojik konumu incelenecektir.
- Virüs tarayıcı ağ geçitlerinin sürüm bilgileri elde edilmeye çalışılarak bu sürümlerin bilinen açıklıkları araştırılacaktır.
- Sunucular üzerindeki yönlendirme (relaying) zafiyetlerini incelemek üzere bir dizi e-posta gönderilecektir.
- Anti-spam ağ geçitlerinin kurum dışı sahte e-postalara karşı davranışı incelenecektir.
- Sunucular üzerinde e-posta dışında bir servisin çalışıp çalışmadığı incelenecektir.
- E-posta sunucusu üzerinde kimlik doğrulamanın aktif olup olmadığını incelenecektir.
- E-posta sunucusu üzerinde POP3, IMAP gibi istemci servislerinin erişime açık olup olmadığı kontrol edilecektir.
- E-posta sunucuları güvenlik taramasına tabi tutulacaktır.
- Sistemlerde kullanılan e-posta içerik kontrolcüleri, anti-virüs ağ geçitleri, spam filtrelerinin kullanıldığı kütüphanelerde var olabilecek muhtemel açıklıklar incelenecektir.
- E-posta servisini veren yazılımların bilinen diğer açıklıkları araştırılacaktır.
- E-posta servislerinin gönderilen e-postaların boyutlarını sınırlayıp sınırlamadığını kontrol etmek amacı ile boyutu büyük e-postalar gönderilecektir.
- Kullanılması muhtemel e-posta listesi yazılımlarının açıklıkları tespit edilmeye çalışılacaktır.

3.13.5 Veritabanı sistemlerine yönelik asgari olarak aşağıdaki testler gerçekleştirilecektir:

- Sistemdeki veritabanı uygulamaları ve bu uygulamaları üzerinde barındıran işletim sistemleri tespit edilerek, tespit edilen bu sistemlere erişimin açık olup olmadığı denetlenecek ve erişimin açık olması halinde çeşitli tarama araçlarıyla veritabanı versiyonu, üretici adı vb. bilgiler ele geçirilmeye çalışılacaktır.
- Elde edilen veritabanı sistem bilgileri kullanılarak, bu sistemlere yönelik kullanıcı adı ve parola deneme saldırıları yapılır. Bu saldırılar sırasında, ön tanımlı kullanıcı adı ve parolaların denenmesinin yanında, Kuruma özel olabilecek ve tahmin edilebilir kullanıcı adı ve parolalar da denenecektir.
- Veritabanı kullanıcı adı ve parola saldırılarının başarısız olması durumunda, işletim sistemi seviyesinden erişim denemeleri yapılır. Windows, Linux vb. ortamlar üzerinden sistem kullanıcıları ile veritabanı uygulamasına bağlanılmaya çalışılacaktır.
- Parola deneme saldırılarının başarılı olması durumunda tespit edilen erişim bilgileriyle sistemlere bağlanılır. Bağlanılan sistemlerde hangi hassas verilerin bulunduğu, kullanıcı adı, parola ve parolalara ait karmaşıklaştırılmış özet verilerinin bulunup bulunmadığı denetlenecektir.
- Görüntülenebilen kullanıcı adı ve parola özet bilgileri çeşitli araçlarla tespit edilmeye çalışılarak zayıf olarak belirlenmiş parolalar tespit edilecektir.
- Erişilebilen sistemlerde yama bilgisi kontrol edilir. Bilinen açıklıkları içeren ve gerekli güncellemeleri yapılmamış sistemlerde hak yükselme vb. saldırılarla erişim sağlanan kullanıcının hakları genişletilmeye çalışılacaktır.
- Erişilebilen sistemlerden diğer erişilemeyen sistemlere tanımlanmış bağlantılar varsa bu bağlantılar kullanılarak diğer veritabanı uygulamalarına geçilmeye çalışılacaktır.
- Hassas verileri ihtiva eden sistemlere erişilebilmesi 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.

3.13.6 YÜKLENİCİ, Kurumun bildireceği web uygulamalarına aşağıdaki testleri uygulayacaktır:

- Girdi Denetimi
- Çıktı Denetimi

- Değiştirilen İçeriğin Tespiti
- HTML Etiketlerinin Filtrelenmesi
- SQL Enjeksiyonu
- URL Yönlendirmeler
- XSS Enjeksiyonu (XSS ınjection)
- Oturum Yönetimi
- Giriş Sonrası Oturum Bilgisi Yenileme, Oturum Sabitleme,
- Çerezlerin İçeriği,
- Oturum Sonlandırma,
- Oturum Çalma (Session Riding),
- Yetki Artırımı,
- Yetki Dışı İşlem,
- Şifre Politikaları,
- Bilenen Hesap/Şifre Bileşenlerinin Denenmesi,
- Basit Kimlik Doğrulama Kullanımı,
- Kimlik Doğrulamanın Atlatılması,
- Çıkış (Logout) İşlevi,
- Tersine Yol (Path Traversal),
- Yetki Atlatma (Bypass Authorization),
- Web Servis Testleri,
- Yetki Artırımı (Privilege escalation),
- SSL Kullanımı,
- HTML Yorumları
- Sunucu Bilgisinin Kısıtlanması,
- Hata Sayfalarının Gösterimi,
- Yönetici Arayüzü Erişim Testi,
- Güvenlik Resmi (Captcha) Kullanımı,
- HTTP Yanıt Bölme (HTTP Response Spliüing)
- Siteler Arası İstek Sahteciliği (Cross-Site Request Forgery, CSRF)

3.13.7 Kablosuz ağlara yönelik asgari olarak aşağıdaki testler gerçekleştirilecektir:

- Kurumda kullanılan kablosuz ağ cihazlarının genel mimari içindeki yeri incelenecektir. Kablosuz ağlardan kurum içi ağlara erişim olup olmadığı incelenecek ve kablosuz ağlardan kurum ağına sızılmaya çalışılacaktır.
- İstemcilerin kablosuz ağ yapılandırmaları incelenecektir.
- Kurumda bulunan kablosuz ağlar taranarak özellikleri keşfedilmeye çalışılacaktır.
- Kablosuz ağlarda MAC adresi tabanlı filtrelemenin olup olmadığı incelenecektir.
- Kablosuz ağlarda kullanılan şifreleme ayarları incelenecektir.

- Kablosuz ağ erişiminde kullanılan şifreleme ve kimlik denetimi yöntemleri incelenerek ağ şifresi ele geçirilmeye çalışılacak ya da kimlik doğrulama yöntemi atlatılmaya çalışılacaktır.
- Sahte kablosuz ağ erişim noktaları oluşturularak kurumda bulunan istemciler ele geçirilmeye çalışılacaktır.
- İstemciler üzerinden kablosuz ağ taraması yapılarak, kurum etrafında bulunan diğer kablosuz ağlar keşfedilmeye çalışılacaktır.
- İstemciler üzerinden kablosuz ağ kullanılarak kurum dışına bağlantı yapılıp yapılamayacağı incelenecektir.

DDOS testleri, Kurumun verdiği servisin en az yoğun olduğu saatlerde ve sistem yöneticileri ile koordine olarak gerçekleştirilir. Bu kapsamda asgari olarak aşağıdaki testler gerçekleştirilecektir:

• IP seviyesinde DDOS testleri gerçekleştirilecektir.
• DNS sunucularına yönelik dağıtık aşırı paket gönderimi ile trafiğin üzerinden geçtiği güvenlik duvarı gibi aktif cihazlara yönelik yük testi gerçekleştirilecektir.
• Web sunucularına yönelik dağıtık aşırı paket gönderimi ile trafiğin üzerinden geçtiği güvenlik duvarı gibi aktif cihazlara yönelik yük testi gerçekleştirilecektir.
• Web sunucularına yönelik aşırı paket gönderimi ile web sunucu testi gerçekleştirilecektir.

3.13.8 İDARE çalışanlarının bilgi güvenliği farkındalıklarının sınanması amacıyla asgari olarak aşağıdaki sosyal mühendislik testleri gerçekleştirilecektir:

- Kurum çalışanlarının ilgisini çekebilecek ve kurum içine sızmaya imkân tanıyacak nitelikte özenle hazırlanmış, İDARE içinden veya dışından gönderilecek epostalar ile kullanıcı bilgisayarlarına sızma denemesi gerçekleştirilecektir.

3.13.9 Sanallaştırma sistemleri üzerindeki sanal sunucular ve bu sunucularda çalışan servislerle ilgili bilgiler toplanacaktır. Sistemler açıklık bulma araçları ile taranacak ve tespit edilen açıkların uygulanabilirlikleri sınanacaktır.

3.14 Gerçekleştirilen testler sonucunda aşağıdaki gereklilikleri karşılayacak şekilde raporlama yapılacaktır:

3.14.1 YÜKLENİCİ, test ve değerlendirme çalışması sonucunda Detaylı Teknik Test Sonuç Raporu ile Yönetici Test Sonuç Raporu'nu hazırlayarak İDARE'ye sunacaktır. Teknik rapor yeterince açık ve sözlü açıklamaya gerek bırakmayacak biçimde net olacaktır.

3.14.2 Yapılan testler sonucunda oluşturulacak rapor, testin bitiminden sonra en geç 15 (onbeş) iş günü içerisinde İDARE'ye teslim edilmelidir.

3.14.3 Denetim raporu asgari şu konuları kapsamalıdır: Derlenen veriler, tespit edilen zafiyetler, zafiyetlerin risk düzeyleri ve gerçekleşmeleri durumunda oluşabilecek zararların ölçekleri, zafiyetlerin giderilmesine ilişkin (varsa alternatifli) öneriler ve YÜKLENİCİ'nin diğer notları.

3.14.4 Dokümanda ayrıca testlerde elde edilen bulgular ve yapılmış olan belirlemeler ışığında, Kurum bilişim ağı yapılanmasına ilişkin geliştirme ve değişiklik önerilerine yer verilecek bir strateji belgesi üretilerek İDARE'ye sunulacaktır.

3.14.5 Denetim ve analiz sırasında ortaya çıkan kritik güvenlik konularının karşılıklı olarak görüşülerek, hızlıca giderilmesi için öneriler sunulacaktır. Bu açıklıklar için raporlama beklenmeyecektir.

3.14.6 İDARE, sözleşme süreleri içerisinde kalmak koşulu ile, belirlendikten sonra giderilen açıklıkların güncel bir testini talep edebilecektir. Bu testler için ilave ücret talep edilemeyecektir.

4. BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ DENETİMİ

Denetim Hizmetleri Cumhurbaşkanlığı Dijital Dönüşüm Ofisince hazırlanan Bilgi ve İletişim Güvenliği Denetim Rehberine uygun olarak yapılacaktır.

4.1 Denetim en az aşağıdaki başlıklarda yürütülecektir;

- Donanım Varlıklarının Envanter Yönetimi
- Yazılım Varlıklarının Envanter Yönetimi
- Tehdit ve Zafiyet Yönetimi
- E-Posta Sunucusu ve İstemcisi Güvenliği
- Zararlı Yazılımlardan Korunma
- Ağ Güvenliği
- Veri Sızıntısı Önleme
- İz ve Denetim Kayıtlarının Tutulması ve İzlenmesi
- Sanallaştırma Güvenliği
- Siber Güvenlik Olay Yönetimi
- Sızma Testleri ve Güvenlik Denetimleri
- Kimlik Doğrulama ve Erişim Yönetimi
- Felaket Kurtarma ve İş Sürekliliği Yönetimi

- Uzaktan Çalışma
- Kimlik Doğrulama
- Oturum Yönetimi
- Yetkilendirme
- Dosyaların ve Kaynakların Güvenliği
- Güvenli Kurulum ve Yapılandırma
- Güvenli Yazılım Geliştirme
- Veri Tabanı ve Kayıt Yönetimi
- Hata Ele Alma ve Kayıt Yönetimi
- İletişim Güvenliği
- Kötücül İşlemleri Engelleme
- Dış Sistem Entegrasyonlarının Güvenliği
- Akıllı Telefon ve Tablet Güvenliği
- Taşınabilir Bilgisayar Güvenliği
- Taşınabilir Ortam Güvenliği (CD/DVD, Taşınabilir Bellek Ortamları)
- Ağ Servisleri ve İletişimi
- Dâhili Veri Depolama
- Kimlik Doğrulama ve Yetkilendirme
- API ve Bağlantı Güvenliği
- Diğer Güvenlik Tedbirleri
- Genel Güvenlik Tedbirleri
- Eğitim ve Farkındalık Faaliyetleri
- Tedarikçi İlişkileri Güvenliği
- Genel Güvenlik Tedbirleri
- Sistem Odası/Veri Merkezine Yönelik Güvenlik Tedbirleri
- Elektromanyetik Bilgi Kaçaklarından Korunma Yöntemleri (TEMPEST)
- Kayıt Yönetimi
- Erişim Kayıtları Yönetimi
- Yetkilendirme
- Şifreleme
- Yedekleme, Silme, Yok Etme ve Anonim Hale Getirme
- Aydınlatma Yönetimi
- Açık Rıza Yönetimi

- Kişisel Veri Yönetim Sürecinin İşletilmesi
- Anlık mesajlaşma güvenliği
- Bulut bilişim güvenliği
- Kripto uygulamaları güvenliği
- Enerji sektörü özelinde güvenlik tedbirleri
- Genel Sıkılaştırma Tedbirleri
- Linux İşletim Sistemi Sıkılaştırma Tedbirleri
- Windows İşletim Sistemi Sıkılaştırma Tedbirleri
- Veri Tabanı Sıkılaştırma Tedbirleri
- Web Sunucusu Sıkılaştırma Tedbirleri
- Sanallaştırma Sunucusu Sıkılaştırma Tedbirleri

4.2 Denetim hizmetinde rehberde 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

4.3 Denetim raporu Türkçe olarak hazırlanacaktır.

4.4 Denetim raporu Rehber'de belirtilen format ve özelliklere uygun olarak hazırlanacaktır.

4.5 Denetim çalışmalarını yürütecek personelde en az aşağıdaki sertifikalar bulunacaktır:

- Türk Standardları Enstitüsü tarafından verilmiş "Bilgi ve İletişim Güvenliği Rehberi Uyum Denetimi" D1 veya D2 Baş denetçi sertifikası,

5. YÖNTEM

5.1 İşin başlangıcında bir çalışma planı yapılacak ve taraflarca onaylanacaktır.

5.2 Çalışmaların durumu ve gereklerine göre uzaktan bağlantı, telekonferans, yüz yüze çalışma veya saha ziyareti yöntemleri kullanılacaktır.

5.3 Her çalışma için yöntem birlikte kararlaştırılacaktır.

5.4 Denetçi; çalışma programına uygun olarak bir proje takip platformu üzerinden bir denetim panosu oluşturacak ve denetimde görev alacak kişiler bu çalışma ortamına, rolleri dahilinde, eklenecektir.

5.5 denetimin ilerlemesi bu platformu üzerinden anlık olarak izlenecektir.

5.6 Dosya paylaşımı için bu platform kullanılmayacaktır.

5.7 Her çalışmanın sonunda denetim takip formu oluşturulacak ve karşılıklı olarak imza (e-imza) ile kayıt altına alınacaktır.

5.8 Denetim süresince aylık ilerleme raporları hazırlanacak ve kuruma sunulacaktır.

5.9 Çalışmalarda ihtiyaç duyulduğunda teknik uzmanlar da görevlendirilecektir. Kurum veya danışmanın teknik uzmanları da aynı gizlilik ilkelerine bağlı olarak çalışacaktır.

5.10 Eğer öngörülemeyen şartlardan dolayı planlanmış uzaktan veya yüz yüze çalışmanın yapılamaması söz konusu olursa bu bilgi geç kalınmadan karşı tarafa bildirilecek ve alternatif çalışma zamanı kararlaştırılacaktır.

5.12 Proje takvimine uyumda sorun veya olası tıkanıklıklar tespit edildiğinde taraflar için uygun olan en kısa sürede değerlendirme toplantısı yapılacak ve çözüm yöntemi tespit edilecektir. Toplantı kararları karşılıklı olarak ıslak imza veya e-imza ile kayıt altına alınacaktır.

6. GENEL HUSUSLAR

6.1 YÜKLENİCİ, sözleşme aşamasında projede görevlendireceği personelin bilgilerini İDARE ile paylaşacak ve işin sonuna kadar proje personelinin teminini sağlayacaktır.

6.2 YÜKLENİCİ, sağladığı personelin uzmanlığının yeterli olmadığı durumlarda, muadil uzman personel sağlamakla yükümlüdür.

6.3 YÜKLENİCİ, sağlamış olduğu uzman personel ile ilgili özgeçmiş bilgilerini önceden İDARE ile paylaşacaktır ve İDARE'nin onayından sonra uzman personel çalışmaya başlayacaktır.

6.4 İDARE, YÜKLENİCİ personelinin yetersiz bulunduğu veya tutum ve davranışlarını uygun görülmediği takdirde, personelin değiştirilmesi talebinde bulunabilir.

6.5 İDARE'nin söz konusu personelin değiştirilmesi talebini yazılı olarak YÜKLENİCİ'ye bildirdiği tarihten itibaren en geç 15 (onbeş) iş günü içerisinde personel, YÜKLENİCİ tarafından uygun görülen kişi ile değiştirilecektir.

6.6 Proje ekibinde en az 4 (dört) kişi yer alacaktır.

6.7 Teknik açıklık testlerini gerçekleştirecek uzman veya uzmanlar ile aynı kişi olmamak üzere YÜKLENİCİ tarafından; 1 (bir) Proje Koordinatörü görevlendirilecektir. Proje koordinatörü; projenin yönetilmesinden sorumlu olacak, sözleşme süresi boyunca proje ile ilgili olarak İDARE tarafından muhatap kabul edilecek, genel olarak projenin takibinden, üretilen çıktıların doğruluğu ve kalitesinin kontrolünden sorumlu olacaktır.

6.8 Projede görev alacak danışman personel bireysel olarak aşağıda listelenen şartlardan en az birini ve danışmanlık ekibinin (kümülatif olarak) tümünü sağlaması gerekmektedir:

6.9.1 En az bir ISO 27001 BGYS Baş Denetçi belgeli kişi
6.9.2 En az bir ISO 27701 KVYS Baş Denetçi belgeli kişi
6.9.3 En az bir CISSP belgeli kişi
6.9.4 Bilgi Teknolojileri, Bilgi Güvenliği ve ilgili sektörlerde veya projelerde en az 10 (on) yıl tecrübeye sahip olmak
6.9.5 Kamu veya kritik altyapı şirketlerinde Bilgi Teknolojileri, Bilgi Güvenliği veya İş Sürekliliği yöneticiliği yapmış olmak
6.9.6 TSE tarafından verilen Bilgi ve İletişmi Güvenliği Uyum Denetçisi Eğitim Sertifikasına sahip olmak
6.9.7 TSE onaylı Cumhurbaşkanlığı Dijital Dönüşüm Ofisi "Bilgi ve İletişim Güvenliği D1 ve D2 Denetçisi Eğitimi" Sertifikasına sahip olmak
6.9.8 En az 1 (bir) üniversitede başarılı bir Bilgi ve İletişim Güvenliği Uyum Danışmanlığı projesini tamamlamış olmak

6.9 Proje Koordinatörünün sahip olması ve sözleşme aşamasında belgelendirmesi gereken özellikler şunlardır:

6.10.1 Proje koordinatörü YÜKLENİCİ firmanın çalışanı olmalıdır.
6.10.2 Sızma testi personelinin sahip olması ve sözleşme aşamasında belgelendirmesi gereken özellikler şunlardır:
6.10.2.1 Sızma testi uzmanı YÜKLENİCİ veya ALTYÜKLENİCİ firmanın çalışanı olmalıdır.

6.10.2.2 Bilgi güvenliği alanında CISA, LPT, CISSP, OSCP, OSWE, OSWP, CCEE, TSE Kıdemli Sızma Test Uzmanı, TSE Sızma Testi Uzmanı sertifikalarından en az birine sahip olmalıdır.

6.10.2.3 Denetimi gerçekleştirecek uzmanın/uzmanların başarılı olarak sonuçlandırılmış en az 2 (iki) üniversitede teknik açıklık testi projeleri gerçekleştirmiş olması gerekmektedir.

6.10 YÜKLENİCİ firmada aranan ve sözleşme aşamasında belgelendirmesi gereken belgeler aşağıda verilmiştir:

6.10.2.4 Kamu Bilişim Yetki Belgesine sahip olmak
6.10.2.5 ISO27001:2013 sertifikasına sahip olmak
6.10.2.6 TSE onaylı A veya B Sızma Testi belgesine sahip olmak

6.11 YÜKLENİCİ, bu teknik şartname kapsamındaki Projenin eksiksiz olarak tamamlanmasından sorumlu olacaktır.

6.12 YÜKLENİCİ, projede görev alacak personelin nüfus cüzdanı fotokopilerini, adli sicil kayıtlarını, iş deneyimlerini ve sertifikalarım sözleşme dosyasına ekleyecektir.

6.13 YÜKLENİCİ, şartnamede tanımlanan aşamalara ait işlerle ilgili hiçbir bilgiyi İDARE personelinden saklamayacak, belirlenen güvenlik seviyesine sahip personele tüm bilgileri istenildiği zaman verecektir.

6.14 YÜKLENİCİ ve projede görev alacak personel, İDARE ile ilgili veya işin kapsamına giren, öğrendiği hiçbir bilgiyi üçüncü şahıslar ile paylaşmayacağını taahhüt edecek ve İDARE ile gizlilik sözleşmesi imzalayacaktır.

6.15 YÜKLENİCİ, bu teknik şartname maddeleri aşamalarına uygun şekilde, sözleşmenin imzalandığı tarihten en geç 10 (on) iş günü içerisinde proje süresince kullanacağı kaynakları, iş kalemlerini ve bu iş kalemleri için öngördüğü süreleri içeren detaylı bir "Proje Planı”nı İDARE'nin onayına sunacaktır.

6.16 İDARE’ye sunulan Proje Planı, İDARE tarafından en geç 5 (beş) takvim günü içerisinde onaylanacaktır. İDARE’nin planla ilgili herhangi bir değişiklik talebi olması durumunda en geç 5 (beş) taktim günü içinde YÜKLENİCİ’ye bu talebini iletecektir.

6.17 YÜKLENİCİ, bu şartname kapsamında yürüttüğü iş ve işlemler sırasında, İDARE’nin bilişim sistemlerine bilerek veya bilmeyerek vereceği tüm zararı karşılayacaktır.