|  |  |  |
| --- | --- | --- |
|  | **Satınalan Birim** | Bilgi İşlem Daire Başkanlığı |
| **Talep Eden Birim** | BİLGİ İŞLEM DAİRE BAŞKANLIĞI |
| **Talep Eden Birim** **Sorumlusu** |  |  |
| **Dosya Numarası** | 2018-3 |
| **Satınalma Usulü** | Yaklaşık maliyet esas olmak üzere piyasa fiyat araştırması |
| **Satınalma Memuru** | Zafer CAN | **Tel** : 0224 294 28 23-24 |
| **Fax**: 0224 294 05 01 |
| **E-mail**:zafercan@uludag.edu.tr |

|  |  |  |  |
| --- | --- | --- | --- |
| **Sıra No** | **Mal/Hizmet Cinsi** | **Mal/Hizmet Özellikleri** | **Miktarı** |
| **Donanım** |
| **1-** | Ağ/Teknoloji Ürünleri ve Bileşenlerine Sızma Testleri Yapılması, | Teknik Şartname | 1 |
| **2-** |  |  |  |
| **3-** |  |  |  |
| **4-** |  |  |  |
| **5-** |  |  |  |
| **6-** |  |  |  |
| **7-** |  |  |  |
| **8-** |  |  |  |
| **9-** |  |  |  |

Üniversitemiz Bilgi İşlem Daire Başkanlığı Kurum bünyesinde yer alan uygulamalar, ağ/teknoloji ürünleri ve bileşenlerine sızma testleri yapılması, bilgi güvenliği farkındalık eğitimleri ve danışmanlık hizmetinin gerçekleştirilmesi alımı için teklifler 15/10/2018 tarih ve saat 17:00 ye kadar U.Ü. Rektörlüğü Bilgi İşlem Daire Başkanlığına elden teslim edileceği gibi posta yoluyla da gönderilebilir. **(Not: Fax ile gönderilen teklifler geçerli sayılmayacaktır.)**

1. Teklif mektubu imzalı ve kaşeli olmalıdır.
2. Teklifin hangi tarihe kadar geçerli olduğu belirtilmelidir.
3. Sipariş sonrasında mal/hizmetin kaç günde teslim edileceği belirtilmelidir.
4. Teklif mektubuna dosya numarası yazılmalıdır.
5. Kısmi teklif verilmeyecektir.
6. Mal/Hizmetle ilgili her türlü giderler (Montaj, nakliye, sigorta, vergi, vb.) tedarikçiye aittir.
7. Teklifler **KDV hariç** olarak **TL** cinsinden verilmelidir. (TL cinsinden verilmeyen teklifler değerlendirmeye alınmayacaktır.)
8. Mal/Hizmet ile ilgili Garanti verilmelidir. (4077 sayılı Tüketici Korunması hakkında kanun ve ilgili mevzuat gereği)
9. Teklifler sıra numaralarına göre verilecektir.
10. Sipariş edilen mal/hizmetin teklifte belirtilen tarihe kadar teslim edilmesi , belirtilen tarihten sonra teslim edilmek istenilmesi halinde idare tarafından mal/hizmetin kabulü yapılmayacaktır.
11. **Aşağıda idare tarafından standart hale getirilen teklif mektubu eksiksiz doldurulup gönderilmesi halinde geçerli sayılacaktır.**

**Adres: Uludağ Üniversitesi Rektörlüğü – Bilgi İşlem Daire Başkanlığı Görükle Kampusü 16059 Nilüfer / BURSA**

 **Tel : (0224) 294 05 00 Fax : (0224) 294 05 01**

**TEKLİF MEKTUBU**

**ULUDAĞ ÜNİVERSİTESİ REKTÖRLÜĞÜ**

**BİLGİ İŞLEM DAİRE BAŞKANLIĞINA**

 **Tarih: …./…./2018**

|  |
| --- |
| **Teklif Vermeye Yetkili Kişinin;** |
| **Adı ve Soyadı** |  |
| **Firma Adı** |  |
| **Açık Tebligat Adresi** |  |
| **Vergi Dairesi ve Vergi Numarası** |  |
| **Telefon ve Fax Numarası** |  |
| **Elektronik Posta Adresi**  |  |

|  |
| --- |
| **Teklife İlişkin Kurum Dosya Numarası:** |
| **Sıra No** | **Mal/Hizmet Cinsi** | **Miktarı** | **Birim Fiyatı** | **Toplam** |
| **1-** |  |  |  |  |
| **2-** |  |  |  |  |
| **3-** |  |  |  |  |
| **4-** |  |  |  |  |
| **5-** |  |  |  |  |
| **6-** |  |  |  |  |
| **KDV’siz Genel Toplam (TL)** |  |

**1-** Yukarıda belirtilen **( …… Kalem )** mal/hizmet alımına ait teklifimizi **KDV** **hariç** ……………….. **TL** bedel karşılığında vermeyi kabul ve taahhüt ediyorum/ediyoruz.

**2-**Teklifimiz **…./…./2018**  tarihine kadar geçerlidir.

**3-**Söz konusu mal/hizmet idarece tarafımıza sipariş verilmesinden sonra **……………. takvim günü içerisinde** teslim edilecektir.

**4-** 4077 Sayılı Tüketici Koruması hakkında kanun ve ilgili mevzuat hükümlerini kabul ediyor, mal/hizmet için ……. (gün/ay/yıl) garanti taahhüt ediyorum.

**5-** Teklifimizin kabul edilmesi halinde sipariş yazısının, yukarıda yer alan; 🟋

**🞎** Elektronik posta adresime veya faks numarama tebligat yapılmasını kabul ediyorum.

**🞎** Elektronik posta adresime veya faks numarama tebligat yapılmasını kabul etmiyorum.

 🟋**Teklif veren istekli kabul ettiği seçeneği yazacaktır.**

 **Teklif Vermeye Yetkili Kişinin;**

 **Adı ve Soyadı:**

 **İmzası:**

 **Firma Kaşe**

**ULUDAĞ ÜNİVERSİTESİ**

**BİLGİ İŞLEM DAİRE BAŞKANLIĞI**

**SIZMA TESTİ HİZMET ALIMI**

**(Eğitim Dâhil)**

 **TEKNİK ŞARTNAMESİ**

# KONU

Kurum bünyesinde yer alan uygulamalar, ağ/teknoloji ürünleri ve bileşenlerine sızma testleri yapılması, bilgi güvenliği farkındalık eğitimleri ve danışmanlık hizmetinin gerçekleştirilmesidir.

# AMAÇ

Kurumun mevcut bilgi güvenliği yatırımlarının analizi ile internet üzerinden ve yerel alan ağından sızma testlerini gerçekleştirerek kurumun bilgi varlıklarının güvenilirliğini üst seviyede tutmak.

Kurumun kritik sunucu ve altyapısına yönelik yapılacak olan sızma testi ile bilgi sızıntılarına karşı önlem almak.

Yapılan testlerin ardından ortaya çıkması muhtemel zafiyetlerin, yenilenen ve sürekli güncellenen yazılımsal ve donanımsal teknolojilerin uygulama süreçlerinde ön fikir algısı oluşturmak.

Mevcut bilgi güvenliği yatırımlarının işlevselliğini kontrol ederek, teknoloji yatırımlarının güvenilirliğini ve güncel süreçlerini kontrol etmek.

Bilgi sistemlerinde yetkisiz erişim elde edilmesine veya hassas bilgilere ulaşılmasına neden olabilecek güvenlik açıklarının istismar edilmeden önce tespit edilmesi ve düzeltilmesi.

# TANIMLAR

## Kurum: Uludağ Üniversitesi

## Yüklenici: Sızma testi, eğitim ve danışmanlık hizmetini sağlayacak firmadır.

## Sistem: Kurum bünyesindeki uygulamalar, ağ/teknoloji ürünleri ve bileşenlerinin tümüdür.

## Taraflar: Kurum ve Yükleniciyi belirtir.

## Taraf: Kurum veya Yükleniciden birini belirtir.

## Proje: Sızma Testi Projesi'dir.

# GENEL HUSUSLAR

## Teknik Güvenlik Denetimleri Kurum tarafından yürütülen iş süreçleri, uygulamalar ve fiziksel olarak merkez binası ile sınırlı olacaktır.

## Yüklenici, bu teknik şartname kapsamındaki projenin eksiksiz olarak tamamlanmasından sorumlu olacaktır.

## Sızma testi sonucunda tespit edilen açıklıkların Kurum tarafından kapatılmasının ardından Yüklenici kontrol denetimi yapacaktır.

## Projede görev alacak tüm uzmanlar Türkiye Cumhuriyeti vatandaşı olacak ve hizmet tümüyle Türkiye Cumhuriyeti sınırları içerisinde verilecektir.

## Test ve inceleme hizmetlerini yürütecek personel/personeller güncel olan CEH, ECSA/LPT, OSCP, GPEN, IRCA onaylı ISO 27001 BGYS denetçiliği, TSE Sızma Testi Uzmanı sertifikalarından en az birine sahip olacak ve personel/personeller Yüklenicinin çalışanı olacaktır.

## Yüklenici yapılacak tüm testlerin zamanlarını ve sürelerini Kurum ile birlikte belirleyecektir.

## Yüklenici yapılacak tüm testler Kurum ile birlikte koordineli bir şekilde gerçekleştirilecektir. Kurum yetkililerine bilgi verilmeden herhangi bir denetim çalışması yapılmayacaktır.

## Yüklenici taahhütlerini kısmen veya tamamen başkalarına devredemeyecektir.

## Yükleniciden daha önce yaptığı testlerle ilgili örnek raporlar istenebilecektir.

## Testler belirli ip adreslerinden yapılacak ve bu ip adresleri Kurum’a bildirilecektir.

## Yüklenici test için kullandıkları standartları Kurum’a bildirecektir.

## Yüklenici tarafından Kurum’a verilecek raporlar okunabilir ve anlaşılır olacaktır.

## Yüklenici proje kapsamında hazırlayacağı ve Kurum'a sunacağı bütün dokümanları Türkçe olarak hazırlayacaktır.

## Yüklenici Kurumun talep etmesi durumunda proje ile ilgili periyodik olarak iki haftada bir ara raporları ve sunumları hazırlayacaktır.

## Yüklenici projeyi belirtilen zaman planına uygun şekilde tamamlayacak, zaman planında gecikme olmaması için gerekli önlemleri alacaktır.

## Yüklenici proje kapsamında en az bir proje yöneticisi atayacaktır.

## Proje yöneticisi proje boyunca Kurum ile sürekli ilişki içerisinde olarak, gerekli koordinasyonu sağlayacaktır.

## İçeride yapılacak testlerde kullanılacak (dizüstü bilgisayar, masaüstü bilgisayar vb.) cihazlar Yüklenici tarafından temin edilecektir.

## Yapılacak tüm sızma testleri (özellikle DDOS testleri), çalışmakta olan sistemleri kesintiye uğratmayacak şekilde gerçekleştirilecektir.

## Yüklenici proje sonunda çıkabilecek açıklarla ve siber güvenlikle ilgili Kurumun belirlediği en az 5 kişiye Kurumun göstereceği yerde 5 günlük eğitim verecektir. Bu eğitimler USOM’un Kurumsal SOME Kurulum ve Yönetim Rehberi’nde SOME personelinin alması tavsiye edilen eğitimlerinden aşağıda belirtilen eğitimler olacaktır.

###  Zafiyet Analizi

* + 1. Güvenli Yapılandırma Denetimi
		2. Sızma Testleri Eğitimi
		3. Saldırı Teknikleri Eğitimi

### Kayıt Yönetimi

* + 1. Saldırı Tespit ve Kayıt Yönetimi Eğitimi
		2. Merkezi Güvenlik İzleme ve Olay Yönetimi

# SIZMA TESTLERİ VE TEKNİK GÜVENLİK DENETİMLERİ

## BİLGİLERİN TOPLANMASI VE GENEL TESTLER

### ISS (Internet Servis Sağlayıcı), alan adı sahibi, IP adresleri gibi bilgilerin toplanması,

### Sunuculara ait DNS kayıtları, hostname bilgilerinin elde edilmesi, erişilebilir sunucuların ve erişim yöntemlerinin tespit edilmesi,

### Açık, kapalı ve filtrelenmiş portların tespit edilmesi,

### Kullanılan IP adreslerinin belirlenmesi, IP adreslerinin yönlendirme kontrollerinin yapılması,

### Çeşitli yöntemlerle güvenlik kuralları aşılarak bilgi toplanması,

### Kullanılan güvenlik cihazlarının ve güvenlik uygulamalarının tespit edilmesi,

### Açık portlar üzerinde çalışan uygulamaların belirlenmesi,

### Çalışan servislere ait detaylı bilgiler elde edilmesi,

### Dışarıya hizmet veren sunucu kontrolleri,

### Ağ topolojisi ve segmentasyonu incelenerek kullanıcı-sunucu ağları arasında erişim kontrolünün olup olmadığının kontrol edilmesi,

### Yönlendirici, güvenlik duvarı ve anahtarların paket filtreleme güvenlik problemlerinin kontrolü,

### Yönlendirici, güvenlik duvarı ve anahtarlar tarafından verilen servislerin belirlenmesi ve güvenlik problemi yaratabilecek servislerin kontrolü, sunucu tabanlı yönlendiriciler için işletim sistemine ilişkin güvenlik problemlerinin kontrolü,

### Anabilgisayar tabanlı yönlendiriciler için işletim sistemine ilişkin güvenlik problemlerinin kontrolü,

### Ağ geçitleri hassas yetkili servisleri kontrolü,

### Ağ geçidi yönlendirme güvenlik problemlerinin kontrolü,

### Ağ geçidi paket filtreleme güvenlik problemlerinin kontrolü,

### Ağ geçidi işletim sisteminin güvenlik problemlerinin kontrolü,

### Network aktif cihaz üzerindeki port güvenliği, VLAN ve trunk yapısı kontrollü,

### Cihazların merkezi şekilde yönetilmesini ve gözetlenmesini sağlayan yönetim sistemlerinin varlığı araştırılması ve bu sistemlere sızma girişimleri,

### Tüm ağ cihazlarının açıklıklarının kontrolü,

### Kurum içinden dışarı tünel kurulmasıyla, kurum dışından kurum içine yetkisiz bağlantı gerçekleştirilmeye çalışılması,

### Kurum dışına açık yönetim ara yüzlerinin varlığı kontrolü ve sızma testleri,

### Sanallaştırma yönetim sunucuları üzerinde çalışan veri tabanı ve uygulama sunucuları denetlenecektir.

### Sanallaştırma yönetim yazılımı üzerinde kullanıcı ve grupların yapılandırmaları denetlenecektir.

### Sanallaştırma sisteminde yapılan kullanıcı ve rol tabanlı yetkilendirmeler denetlenecektir.

### Sanallaştırma sistemi bileşenleri genel açıklık tarama yazılımları ile taranacaktır,

### Web servis testleri (SOAP, Ajax testi vb.)

### İnternete açık sunucuların üzerindeki erişilebilir servislerin analizi ve uygunsuz/gereksiz olanların tespiti,

### İşletim sistemi güvenlik açıklıklarının kontrolü,

### Uygulamaya (IIS, OWA vb.) özel güvenlik açıklıklarının kontrolü,

### SMTP, FTP, HTTP, HTTPS, TELNET, ICMP, RPC, NETBIOS, SNMP vb. yaygın kullanılan servisler üzerinden gerçekleştirilebilecek sızmalara karşı detaylı kontroller yapılması, açıklıkların belirlenmesi,

### Hatalı sonuçların ayıklanması ve tespit edilen güvenlik açıklarının sömürülmeye çalışılması.

## WEB TESTLERİ

### Veri Denetimi

1. Girdi Denetimi,
2. Çıktı Denetimi,
3. XSS Enjeksiyonu (XSS Injection),
4. SQL Enjeksiyonu (SQL Injection),
5. Diğer Enjeksiyonlar (XPATH, LDAP vb.),
6. HTTP Yanıt Bölme (HTTP Response Splitting),
7. URL Yönlendirmeleri,
8. Diğer sistemlerle iletişim ve veri aktarımı güvenliği testleri,
9. Erişime açık olmayan bilgilerin ve dokümanların erişilebilirlik kontrolü,
10. Uygulama sunucusu servisleri denetimi,
11. Veri tabanı servisleri denetimi,
12. Veri tabanı yetkisiz erişim denetimleri,

## Oturum Yönetimi

1. Oturum Sabitleme (Session Fixation),
2. Çerez içeriği,
3. Oturum Sonlandırma Fonksiyonu,
4. Oturum Bilgisinin URL İçinde Taşınması,
5. Oturum Çalma,
6. Siteler Arası istek Sahteciliği (Cross-Site Request Forgery, CSRF),
7. Oturum (Session) ve Çerezler (Cookie) ile taşınan verinin güvenlik denetimi

##  Kimlik Doğrulama ve Yetkilendirme

1. Yetki Artırımı, Yetkilendirmenin Atlatılması,
2. Eksik Hesap/Parola Yönetimi ve Yetersiz Parola Politikası,
3. Kimlik Doğrulamanın Atlatılması,
4. Tersine Yol (Path Traversal),
5. Uygulama Mantığı Kontrolleri (Application LogicFlaw, Business LogicFlaw)

## Bilgi Sızdırma ve Ayar Yönetimi

1. Minimum Bilgi Prensibine Aykırı Yardım Sayfaları, HTML Yorumları, Hata Mesajları, Hata Sayfaları ve Durumlar,
2. Veri İletiminde SSL Kullanılmaması,
3. Güçsüz veya Geçersiz SSL Sertifikası Kullanılması,
4. Sunucu Bilgisinin Kısıtlanması,
5. Yedeklenmiş ve Unutulmuş Dosyaların Varlığı,
6. Yönetici Ara yüzüne Erişim,
7. JavaScript, CSS, AngularJS ..v.b. web arayüz zafiyetlerinin araştırılması.

## Web Servislerin Testleri

1. Web Servis Metotların Tespit Edilmesi
2. Web Servis Metotlarına Yetki Dışı Erişim ve Veri Güncellemesi Kontrolü

## Web Sayfası Kaynak Kod Analizi

Kurumun belirleyeceği 3 adet web uygulamasının kaynak kod analizi yapılmalı, bu analiz neticesinde risk profili çıkarılmalı, güvenlik açıklarının tespiti için kapsamlı bir çalışma ve raporlama yapılmalıdır. Bu kapsamda;

* + - * 1. Web uygulamasının fonksiyonel olarak incelenmesi
				2. Güvenlik açıklarının taranması
				3. Konfigürasyon hatalarının incelenmesi
				4. Uygulamanın çalıştığı alt yapının uygulama üzerindeki etkilerinin değerlendirilmesi
				5. Gereksiz hizmet sunucu bileşenlerinin çalışır durumda olup olmadığı
				6. Bilgi sızdırılabilmesine imkân veren zafiyetlerin varlığı,
				7. Ön-tanımlı parola, topluluk adı vb. bilgilerin var olup olmadığı
				8. Uygulama seviyesi geçitlerin kullanımına ve kurallarına ilişkin problemlerin varlığı,
				9. Çeşitli uygulama giriş noktalarının, sistem konfigürasyon yazılımlarının giriş sayfalarının ve diğer kıymetli veri barındıran URL’lerin tespiti yapılmalıdır
				10. Web taraması ile hedef web sunucular üzerinde normal kullanıcılardan saklanmış dizin/dosyaların tespiti yapılmalıdır
				11. Uygulamayı oluşturan tüm HTML ara yüzlerine ait kaynak kodları incelenerek açıklama, gizli form alanı gibi kıymetli bilgiler, gizli girdi noktaları Yüklenici uzmanları tarafından yazılmış betikler ve elle yapılmalıdır.
				12. Girdi işleme ve görüntüleme kodlarının cross-site scripting (XSS) saldırılarına dayanıklılığının test edilerek XSS zafiyetlerinin varlığı tespit edilecektir. Bu adım araç ve elle yapılmalıdır.
				13. Erişim denetimi mekanizmaları atlatılmaya çalışılarak Erişim Kontrolleri Uygulamalarının yeterli erişim kontrollerini doğru yapıp yapmadığının denetimi elle yapılmalıdır.
				14. Uygulamaların almış olduğu girdiler kontrol edilerek sistem üzerinde erişim hakkı olmayan dosyaların okunup okunamadığı veya komut çalıştırılıp çalıştırılamadığı, Girdi denetimlerinin doğru ve eksiksiz bir biçimde gerçekleştirilip gerçekleştirilmediği tespit edilmelidir (SQL injection, command injection, LDAP injection, buffer overflow vb.). Bu adım elle gerçekleştirilmelidir.
				15. Erişim gerçekleştirilen uygulamalardan uygun olanları için parola kırma testleri yapılmalıdır. Bu testler araç ile kaba kuvvet ve/veya ön tanımlı parolaların denenmesi şeklinde yapılmalıdır. Uygulamalara özel parola girdileri ise araç ile kontrol edilmelidir.
				16. Oturum Güvenliği Denetimi için kurulan mekanizmanın, bu doğrultuda çerez, web parametreleri ve gizli form elemanlarının kullanımının testi yapılmalıdır. Bu adımda çerez güvenliği, XSRF zafiyetleri, oturum sabitleme gibi konular test edilmelidir. Bu denetimler elle ve araç aracılığı ile yapılmalıdır.
				17. Kod akışı değiştirme testleri yapılmalıdır.

## MOBİL UYGULAMA TESTLERİ

1. Android ve iPhone Mobil Uygulama Güvenlik Analizi
2. Mobil Uygulamaların Web Servislere Güvenli Erişim Kontrolü
3. Mobil Uygulamalarda Tutulan Yerel Verinin Güvenliği
4. Yetki Artırımı, Yetkilendirmenin Atlatılması

## DNS SERVİSLERİNİN TESTLERİ

* 1. DNS sunucuların topolojik konumu incelenecektir.
	2. DNS Sunucusunun alan yapılandırmasında yer alan kayıtlar ortaya çıkarılmaya çalışılacaktır.
	3. Sunucu üzerinden alan transferi (zone transfer) yapılmaya çalışılacaktır.
	4. Netcraft, Google, Whois sorguları yapılarak Kurum alanında yer alan sunucular tespit edilmeye çalışılacaktır.
	5. DNS sunucular için ön bellek zehirlemesi gerçekleştirilmeye çalışılacaktır.
	6. DNS sunucular üzerindeki kaynak kayıt girdileri incelenecektir.
	7. DNS sunucuların sürüm bilgisi elde edilmeye çalışılacaktır.
	8. Sunucular üzerinde DNS dışında bir servisin çalışıp çalışmadığı incelenecektir.
	9. Güvenlik Duvarında DNS sunucular için izin verilen portlar incelenecektir.
	10. DNS sunucular güvenlik taramasına tabi tutulacaktır.

## DAĞITIK SERVİS DIŞI BIRAKMA TESTLERİ

* 1. DNS sunucularına yönelik dağıtık aşırı paket gönderimi ile trafiğin üzerinden
	geçtiği güvenlik duvarı gibi aktif cihazlara yönelik yük testi gerçekleştirilecek.
	2. Web sunucularına yönelik dağıtık aşırı paket gönderimi ile trafiğin üzerinden
	geçtiği güvenlik duvarı gibi aktif cihazlara yönelik yük testi gerçekleştirilecek.
	3. Herkese hizmet veren servisler tespit edilerek, bu servislere yönelik dağıtık aşırı paket gönderimi ile trafiğin üzerinden geçtiği güvenlik duvarı gibi aktif cihazlara yönelik yük testi gerçekleştirilecek.
	4. DNS sunucularına yönelik rastgele istek gönderimi ile DNS sunucu yük testi gerçekleştirilecek.
	5. Web sunucularına yönelik aşırı paket gönderimi ile web sunucu yük testi gerçekleştirilecek.
	6. Uygulama seviyesinde gerçekleştirilecek DDOS saldırıları o DNS sunucularına
	yönelik rastgele istek gönderimi ile DNS sunucu yük testi gerçekleştirilecektir.

## KABLOSUZ AĞLARIN TESTLERİ

* 1. Kurumda kullanılan kablosuz ağ cihazlarının genel mimari içindeki yeri incelenecektir.
	2. Kurumda bulunan kablosuz ağlar taranarak özellikleri keşfedilmeye çalışılacaktır.
	3. Kablosuz ağlarda MAC adresi tabanlı filtrelemenin olup olmadığı incelenecek varsa kırılmaya çalışılacaktır.
	4. Kablosuz ağlarda kullanılan şifreleme ayarları incelenecektir.
	5. WEP ve WPA/WPA2 vb. şifreleme kullanılan ağlarda kablosuz ağ şifresi ele geçirilmeye çalışılacaktır.
	6. Sahte kablosuz ağ erişim noktaları oluşturularak kurumda bulunan istemciler ele geçirilmeye çalışılacaktır.
	7. Kablosuz ağ taraması yapılarak, kurum etrafında bulunan diğer kablosuz ağlar keşfedilmeye çalışılacaktır.

## SOSYAL MÜHENDİSLİK TESTLERİ

* 1. Yetkisiz mail yollama
	2. Konuşma esnasında bilgi edinme
	3. Çalışanları gözleme (Shoulder Surfing)
	4. Yetkili bir kişinin giriş izni olduğu sitem odasına yetkili kişinin arkasından izinsiz girme (Tailgating)
	5. Telefonla yetkili bilgi işlem çalışanı adına arayarak şifre ve bilgi isteme
	6. Spam dağıtım ve etkileri
	7. Phishing e-mail dağıtımı ve etkileri
	8. ikna etme veya aldatma yoluyla bilgi elde edilmeye çalışılması

## SAĞLAMLAŞTIRMA VE DOĞRULAMA ANALİZİ

### Belirtilen güvenlik açıkları KURUM tarafından giderildikten sonra YÜKLENİCİ, bu açıkların giderilip giderilemediğini ve kapatılan açıklıkların yeni açıklıklara neden olup olmadığını gerçekleştirilecek bir seferlik yeni bir doğrulama testi ile kontrol edecektir.

# YÖNTEM VE RAPORLAR

## Sızma Testi için kurum mevcut ağ yapısı değiştirilmeyecek, hizmet kesintisine neden olunmayacak, istemci ve sunuculara bir yazılım bileşeni kurulmayacak veya çalıştırılmayacaktır.

## Sızma Testi için gerekli her türlü yazılım ve donanım sistemleri Yüklenici tarafından sağlanacaktır.

## Sızma Testi raporu sözleşmenin imzalanması itibari ile 2 ay içerisinde hazırlanacak ve test tamamlanacaktır.

## 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. Raporlar Türkçe olacaktır.

# GİZLİLİK

## Bu Proje kapsamında yapılacak her türlü iş ve işlemlerle ilgili olarak manyetik ortamda ve/veya yazılı ve/veya sözlü olarak birbirlerine iletilmiş ya da iletilecek olan Taraflardan birine ya da kullanıcı veya personeline ilişkin ve/veya kurum bilgilerine dair her türlü bilgi ve belge gizli tutulacak, hangi amaçla olursa olsun hiçbir şekilde üçüncü kişi ve kuruluşlara aktarılmayacak ve üçüncü kişilerin bu bilgi ve belgelere ulaşma olanağı kesin surette engellenecek olup, işbu yükümlülüğe aykırılık Kurum açısından sözleşmenin tek taraflı kesin fesih nedenidir.

## Taraflar, hangi sebep ve surette olursa olsun bu Proje sona erse dahi, bu madde kapsamındaki sorumluklarının ve yükümlülüklerinin aynı şartlarla süresiz olarak devam edeceğini, kanunen açıkça yetkili makam ve merciler dışında kalan kişilere gizli bilgileri ifşa etmemekle süresiz olarak yükümlü olduklarını kabul ve taahhüt ederler.

## Projenin herhangi bir sebeple sona ermesi halinde dahi bu madde gereği Taraflar birbirlerine ve kullanıcı ile sistemlerine ait sırlan, bilgi ve belgeleri 3. kişilere ifşa etmemek ve kendilerinde bulunmakta olan her türlü bilgi ve belgeleri ait olduğu Tarafa iade etmekle, iadenin mümkün olmadığı hallerde imha etmekle yükümlü olduklarını Taraflar kabul, beyan ve taahhüt eder.

## Yukarıda belirtilen kurallara uyulmaması ve/veya gizli bilgilerin amacı dışında kullanılması, gizliliğin herhangi bir biçimde ihlal edilmesi halinde, kuralı ihlal eden taraf diğer tarafın uğrayacağı maddi, manevi zararı ödemeyi beyan ve taahhüt eder.

## Taraflar, bu Proje devamı süresince diğer Tarafa ait olan bilgisayar programları, tasarımlar, kavramlar, teknikler, işlemler, yöntemler, sistemler, devreler, deneyici çalışmalar, gelişme aşamasındaki çalışmalar, yazılımların kaynak kodları, yazılım geliştirme bilgilerini ilgili mevzuatın ve yasaların gerektirdiği zorunlu bildirimler dışında üçüncü kişiler karşısında tamamen gizli tutulması için gerekli önlemleri almayı kabul ve taahhüt eder.

## Projenin başlangıcında Yüklenici ile Kurumun arasında şartname dışında gizlilik sözleşmesi imzalanacaktır.

# GARANTİ

Proje sözleşme imzalama tarihinden itibaren 6 ay garanti kapsamındadır.