# TEKNİK ŞARTNAME

**İşin çeşidi:** Bilgi Güvenliği Güvenlik Danışmanlık Hizmeti Alımı

**İşin niteliği:** Bilgi Güvenliği çalışmaları kapsamında BT Sistemleri Güvenlik, Sızma ve Doğrulama Testi Hizmeti Alınması

**Alınması planlanan ürünler:**

BT Sistemleri Güvenlik, Sızma ve Doğrulama Testi Hizmeti: 6 set

**Şartnamede;**

İstanbul Bilgi Üniversitesi – BİLGİ,
Bilişim Teknolojileri Departmanı – BT Dept.,
Teklif veren kuruluş – FİRMA,
Satın alınması yapılacak donanım/yazılım/hizmet – ÜRÜN/HİZMET
olarak anılacaktır.

## ÖN KOŞULLAR

- İşbu şartname, BİLGİ'nin kendi lokasyonunda konuşlandırdığı, hizmet aldığı firmalarda barındırdığı sistemler ile veri iletişim ağları üzerinde, BT Güvenlik, Sızma ve Doğrulama Testi hizmetinin konusunda bilgi birikimine sahip olan FİRMA' dan yapılmasını kapsamaktadır.

- Bu kapsamda BİLGİ'nin BT sistemlerine mümkün olabilecek her yolun denenerek sızılmanın test edilmesi, güvenlik açıklarının bulunması ile birlikte açığın değerlendirilip sistemlere erişimlerin test edilmesi, hizmet durdurmaya yönelik testlerin yapılarak zafiyetlerin belirlenmesi, test sonuçlarına göre yapılan iyileştirmelerin doğrulanması için yıllık 6 set, BİLGİ ihtiyaç duyduğu taktirde ek set halinde hizmet alımı yapılacaktır.

- HİZMET'in alım yeri, BİLGİ'nin Santral (Merkez), Kuştepe ve Dolapdere kampüsleridir.

- HİZMET ifa süresi, sözleşmenin imzalandığı tarihten itibaren 1 (bir) yıldır. Ancak kanunlarda belirtilen mücbir sebeplerden dolayı veya set aralıklarının geniş tutulmasından dolayı ifa süresinin uzaması durumunda taraflar yeni tarih belirleyecektir. BİLGİ, 1 yıl içinde karşılanmasını talep ettiği set sayısını, sözleşme süresini 6 ay aşabilecek sürede alma hakkını saklı tutar. Set aralıklarını 1 aydan uzun tutup toplam hizmeti en fazla 1,5 yılda alabilir. BİLGİ, test talebinde bulunmasına rağmen FİRMA'dan kaynaklı 1 haftadan fazla gecikme olursa mücbir sebep halleri dışındaki gecikmeler, cezaya tabidir.

- FİRMA, detayları ve koşulları işbu şartnamede belirtilen "BT Sistemleri Güvenlik Sızma ve Doğrulama Testi Hizmeti" ni sağlamakla yükümlüdür.

- HİZMET kapsamında sözleşme süresi içinde 6 (altı) "BT Sistemleri Güvenlik, Sızma ve Doğrulama Testi" hizmeti alınacaktır. Testlerin uygulanma tarihleri BİLGİ tarafından belirlenecektir. Bir sonraki set, önceki setten en az 1 ay sonra, yine BİLGİ'nin onaylayacağı tarih/saat aralığında yapılacaktır. Test tarihleri BİLGİ ve FİRMA ortak kararı ile belirlenecektir.

- HİZMET'in belirtilen sürede ifa edilememesi veya teklif edilen ve onaylanan HİZMET' ten farklı sunulması durumunda, oluşacak zarardan dolayı BİLGİ'nin uğrayacağı maddi ve manevi tazminatlar FİRMA tarafından kayıtsız şartsız kabul edilecektir.

## GENEL İSTEK ve ÖZELLİKLER

- HİZMET, FİRMA'nın bordrolu ve şartnamede belirtilen yetkinliklere sahip personeli tarafından sağlanacaktır.
- Sızma testini yapacak FİRMA'nın bu sözleşme kapsamında istihdam edeceği personel, konusunda uzman, benzer projelerde bulunmuş, bu konularda en az 2 yıl tecrübe kazanmış olmalıdır.
- Sızma testini yapacak FİRMA' nın %100 Yerli ve Türk Sermayesi ile kurulu olması tercih edilmektedir.
- Sızma testini yapacak FİRMA gerçekleştirecek olduğu Sızma Testi hizmetinde herbir testin manuel veya otomatik olacağını belirtmeli, test aşamasında BİLGİ den uygunluğu ile ilgili onay almalıdır.
- Sızma testini yapacak FİRMA bu özelliklere sahip personellerinin sözleşme aşamasında çalıştığını gösteren SGK bildirgelerini, özgeçmişini, sertifikalarını ve diplomalarını sözleşme aşamasında BİLGİ'ye sunacaktır.
- FİRMA'nın sektörde en az 5 (beş) yıldır faaliyet gösteriyor olmalıdır. Sürenin görüldüğü faaliyet belgesini ihale evraklarına eklemelidir.
- FİRMA, sunacağı hizmete benzer olarak Türkiye'de gerçekleştirdiği en az üç (3) adet referans projeyi (işlem hacmi, IP sayısı marka değeri vb. kriterlere göre BİLGİ ölçeğinde) sunacaktır. FİRMA tarafından bu referans projelere ilişkin kontak kişi ve iletişim bilgileri teklif ekinde sunulacaktır.
- Sızma testini yapacak FİRMA, bu sözleşme kapsamında görevlendirilen teknik personelinden memnun kalınmaması durumunda, BİLGİ'den gelecek değişiklik talebini en az aynı vasıfta başka bir personel istihdam ederek karşılayacaktır.

## TEKNİK KOŞULLAR

### 1. TANIMLAR

- **Zafiyet:** Bir sistemde sistemin olası saldırılara karşı dayanma gücünü en aza indirecek hastalıklı/zayıf nokta, açık kapı.
- **Uyumluluk Testleri:** PCI-DSS ya da ISO 27001 standartlarına uygunluğun ölçüldüğü testlerdir.
- **PCI-DSS (Payment Card lndustry Data Security Standard):** Kartlı ödeme sistemlerinde veri güvenliğini sağlamak amacıyla, American Express, Mastercard Worldwide, Visa Inc., JCB lnternational, Discover Financial Services gibi uluslararası ödeme markaları tarafından desteklenen PCI Güvenlik Standartları Kurulu (PCI Security Standards Council) tarafından oluşturulan PCI-DSS olarak bilinen Ödeme Kartı Sektörü Veri Güvenliği standardıdır.
- **Penetrasyon (Sızma) Testi:** Kontrollü şekilde yapılan 'hacking' saldırı simülasyonudur.
- **Exploit:** Programların zayıflık veya hatalarını kullanan programcıklar, sistemlerin zafiyetlerini kullanabilen özel scriptler ya da programlardır.
- **Test:** Uyumluluk testleri ve penetrasyon (sızma) testleri için işbu şartnamede kullanılan genel ifade.

## 2. AMAÇ

- Gerçek bir saldırganın kullandığı yöntemlerin ve bakış açısının kullanılması ve bu sayede rutin kontrollerde tespit edilemeyen güvenlik zafiyetlerinin belirlenmesi ve teknoloji bağımsız çözümler tavsiye edilmesi hedeflenmektedir.

- Ayrıca PCI-DSS standardının 11.3 maddesinde belirtilen altyapı ve uygulamalardaki değişikliklerden sonra penetrasyon testi (bilgi güvenliği zafiyet testi) yapılmasının karşılanması hedeflenmektedir.

## 3. GENEL KAPSAM

BİLGİ tarafından, talep edilecek her bir çalışmanın öncesinde bildirilecek sistemler ya da uygulamalar için iş bu şartnamenin "Teknik Kapsam" bölümünde belirtilen işlerin tamamı kapsamda olacaktır.

### 3.1. Değerlendirme

- FİRMA işbu şartnamede belirtilen hususlara madde sırasını belirterek, ayrı ayrı cevap verecektir. Şartname maddelerinde istenilen şartların sağlanıp sağlanmadığı hiçbir yoruma olanak vermeyecek şekilde belirtilecektir. Cevaplanmayan maddeler 'anlaşılmış ve kabul edilmiş' olarak değerlendirilecektir.

- BİLGİ tarafından aşağıda belirtilen değerlendirme kriterlerine göre teknik değerlendirme yapılacaktır.

    - Hizmeti teklif eden FİRMA'nın ilgili konuda gerçekleştirdiği projeler (ölçek ve miktar yazılı olarak beyan edilecektir, FİRMA bilgileri istenildiğinde sözlü olarak iletilecektir.)

    - Madde 5.1'de belirtilen asgari yeterlilik kriterlerinin sağlanma seviyesi (ilave yeterlilikler artı puan olarak değerlendirilecektir)

    - Madde 5.2'de belirtilen asgari yeterlilik kriterlerinin sağlanma seviyesi (ilave yeterlilikler artı puan olarak değerlendirilecektir).

### 3.2. Proje Planı:

- İşbu şartnamede belirtilen tüm işlemler FİRMA tarafından gerekli hallerde BİLGİ lokasyonunda, BİLGİ yetkili personeli ile birlikte gerçekleştirilecektir. İşin gereği zorunlu olarak farklı bir lokasyonda yapılması gereken çalışma yine BİLGİ yetkili personeli ile iletişim kurularak gerçekleştirilecektir.

- İşbu şartnamede belirtilen hükümlerin yorumlanmasında BİLGİ'nin görüşü esas kabul edilecektir.

- Hizmetin ifası esnasında FİRMA ve BİLGİ arasında hizmetin şekli, yapılışı, usul ve esasları, teknikleri vb. dair olabilecek anlaşmazlıklarda BİLGİ'nin görüşü esas kabul edilecektir.

- FİRMA belirtilen tüm işlemleri bizzat gerçekleştirecektir. BİLGİ yalnızca ihtiyaç duyulacak koordinasyonu sağlamaktan sorumlu olacaktır.

### 3.3. Teklif Değerlendirme Kriterleri:

FİRMA iş bu şartnamede belirtilen hizmet kalemleri için talep edilen hizmetlerin toplamı bazında fiyat teklifi iletecektir.

### 3.4. Proje Süresi:

- FİRMA işbu şartnamede tariflenen hizmetleri gerçekleştirmeye, BİLGİ'nin talep ettiği süreden itibaren en fazla 15 (onbeş) gün içerisinde başlayabilir durumda olmalıdır.

- Şartname kapsamında yapılan testler Sızma Testi (Pentest) ve Doğrulama Testi olmak üzere iki aşamadan oluşan 1 set şeklinde olacaktır. Sızma Testi için hizmetin öğrenme, denetim ve test aşaması 30 iş gününü geçmeyecektir. Bu süre net olmamakla birlikte, BİLGİ tarafından verilecek çalışma desteğine bağlı olarak artabilir.

- FİRMA, Pentest hizmetini ifasından sonra üreteceği raporunu en geç hizmetin tamamlanmasını takip eden 15 iş günü içerisinde BİLGİ'ye teslim etmelidir.

- BİLGİ, Pentest raporunu inceledikten sonra raporda belirtilen açıklara karşı tedbirlerini gerek görürse FİRMA danışmanlığında alacak ve FİRMA'ya geribildirim verecektir.

- BİLGİ geribildirim yaptıktan sonra, FİRMA en geç 10 iş günü içinde raporda belirtilen tüm konularda denetim ve test işlemlerini kontrol amaçlı tekrarlayacaktır (Doğrulama Testi). Ayrıca, BİLGİ gerek görürse alınan tedbirler nedeniyle etkilenen sistemler için FİRMA'dan ek denetim ve test talep edebilecektir.

- FİRMA, Doğrulama raporunu, BİLGİ'nin kontrolleri ve gerekli iyileştirmeleri yaptığını bildirmesinden sonraki 15 iş günü içerisinde BİLGİ'ye teslim etmelidir.

## 4. TEKNİK KAPSAM:

### 4.1. Sızma (Penetration) Testi:

#### 4.1.1. Kapsam ve Genel Hükümler:

- FİRMA, aşağıda tariflenen tüm hizmetler için vereceği teklifini, toplamda 6 set Sızma Testi ve Doğrulama Testi hizmetlerini sağlayacak şekilde düzenleyecektir.

- Sızma testi BİLGİ'nin talebine göre internet ortamından ve BİLGİ kurumsal networkünden gerçekleştirilecektir.

- * FİRMA, sızma testine (İnternet, Yerel Ağ ve Kablosuz Ağ dahil) Kara Kutu yöntemi ile önceden bir veri ve yetki verilmeden başlayacaktır. Bu testin ara raporları sunulduktan sonra Beyaz kutu yöntemine dönülecek ve kapsam için verilen ya da eksik kalan hedefler bu yöntem ile tekrar test edilecektir.

- * Siyah kutu ve beyaz kutu sızma testi işlemleri raporlarda ayrıca bildirilecektir.

- * BİLGİ' ye ait tüm web uygulamaları sızma testi kapsamına dahildir. En az 200 site ve alt site, 50 wordpress site)

- Öğrenci Bilgi Sistemi (SIS) uygulama ve veriyabanı sunucuları ile kod güvenliği

- Test kapsamına dahil olacak cihazlar, uygulamalar, IP numaraları, uygulanacak testler, internet ya

da BİLGİ networkünden yapılacağı gibi bilgiler her bir test talebinde BİLGİ tarafından FİRMA'ya bildirilecektir.

- FİRMA her bir test talebi için BİLGİ ile kullanacağı insan kaynağı ve zaman bilgisinin de yer aldığı test planlarını yazılı olarak paylaşacak ve BİLGİ'nin yazılı onayı ile mutabık kalınan plana uygun şekilde testlere başlayacaktır.

- FİRMA, BİLGİ sistemlerinde hizmet kesintisine ya da zarara neden olabilecek test türleri için BİLGİ'ye özellikle bildirimde bulunacak ve onay alacaktır.

- FİRMA, test planında mutabık kalınan zaman planına azami ölçüde uyacak, istisnai durumlarda detaylı bilgilendirme ile birlikte BİLGİ'den onay alacaktır. FİRMA kaynaklı gecikmelerin sorumluluğu FİRMA'da olacak, bunlar için ek bedel ödenmeyecektir.

- FİRMA, onaylı plana göre gerçekleştirdiği test hizmeti sonucunda, ödeme planına uygun şekilde hizmetini faturalandıracaktır.

- FİRMA test işlemleri için 7x24 esası ile çalışabilecektir.

- FİRMA testleri en az senior yetkinlik seviyesindeki personeli ile (işbu şartnamenin 5.1 maddesinde belirtilmiştir) gerçekleştirecektir.

- FİRMA testlerde kullanacağı ve referans alacağı metodolojiyi (OSSTMM (Open Source Security Testing Methodology Manual), OWASP (Open Web Application Security Project) ve NIST 800-42 (National lnstitute of Standards and Technology- Guideline on Network Security Testing)) gibi açık bir şekilde tarifleyen belgelerini teklifi ile iletecektir.

- BİLGİ, testlerin belirli IP'lerden yapılması ile ilgili Sızma Testi aşamasında IP sınırlaması getirmeyecektir. FİRMA test uyguladığı IP'leri raporunda belirtecektir. BİLGİ, gerektiğinde Doğrulama Testi aşamasında bizzat test edilmesini istediği IP'leri FİRMA ile paylaşacaktır.

- Test kapsamında yapılan çalışmaları, hazırlanan raporları, tespit edilen açıkları ve bu açıkları giderme yöntemlerini görüşmek üzere yapılacak tüm toplantılara BİLGİ talep etmesi halinde FİRMA katılım sağlayacaktır. FİRMA bu işler için ayrıca ücret talep etmeyecektir.

- FİRMA kullanacağı tüm araçları temin etmekten, bu araçlara ait yasal sorumluluklarından ve olası maliyetlerinden bizzat sorumludur.

- Sızma Testi ve Doğrulama Testi ile ilgili raporlama ve tüm kayıtlar, FİRMA tarafından, her bir test hizmeti süresi sonunda, BİLGİ'ye teslimini müteakip geri döndürülemez şekilde yok edilecek, herhangi bir kopyası tutulmayacak ve BİLGİ'ye bu işlemin tamamlandığına dair bildirimde bulunacaktır.

- FİRMA, gerçekleştirdiği bu hizmete dair BİLGİ'nin yazılı izni olmadan kurumsal ismini, logosunu yazılı ya da sözlü hiçbir şekilde kullanmayacaktır.

- Test kapsamında FİRMA tarafından yapılacak işlerin tamamı ya da bir kısmında BİLGİ'nin belirleyeceği BİLGİ personeli/personelleri gözlemci olarak bulunabileceklerdir. FİRMA gözlemciye işbaşı eğitimi vermekle ve bilgilerini paylaşmakla yükümlüdür.

### 4.1.2. Hizmet:

- Sızma Testi temel olarak keşif, açık bulma, açıklık testi, raporlama, doğrulama aşamalarından oluşmalıdır.

- Sızma Testi en az aşağıdaki konuları içermelidir:

**BİLGİ'ye ait verilerin toplanması, keşif;**

- ✓ Servis sağlayıcı bilgilerinin belirlenmesi
- ✓ Kullanılan IP adreslerinin ve etki alanlarının belirlenmesi
- ✓ BİLGİ'ye ait veri detaylarının ve ilgili kişilerin doğruluğunun kontrol edilmesi
- ✓ Tanımlanmış DNS bilgileri ve BİLGİ internet sunucularının hakkında bilgi alınması
- ✓ Benzer alan adları ile kaydedilmiş, yanıltıcı olabilecek alan adlarının belirlenmesi
- ✓ Erişilebilirlik süresi ve oranlarının belirlenmesi
- ✓ Yerel IP adreslerinin belirlenmesi
- ✓ Yapıda var olan güvenlik cihazları ve güvenlik uygulamalarının belirlenmesi
- ✓ BİLGİ internet sunucuları ve Tanımlanmış DNS bilgileri hakkında bilgi alınması. DNS sunucularının konfigürasyon ve uygunluk kontrolünün yapılması
- ✓ DNS Poisoning, Recursive DNS Query vb. karşı güvenlik kontrollerinin ve sızma testlerinin yapılması
- ✓ Ağdaki farklı erişim tipleri, güvenli bölge ve sunucuların yerlerinin, hassas verilerin akış şemasının belirlenmesi
- ✓ DMZ bölgeleri, extranet, portal, web uygulamaları, yönetim arabirimlerini vb. içeren ağ topolojisinin belirlenmesi
- ✓ IP yönlendirme testleri
- ✓ Port taramaları
- ✓ Güvenlik duvarı ardında kalan tüm aktif IP adreslerinin, bu adresleri kullanan sistemlerin marka/model, işletim sistemi markaları ve sürümlerinin belirlenmesi

**Internet yönlendiricisinin (Router) kontrolleri;**

- ✓ BİLGİ'nin internet yönlendiricisinden alınabilecek yönlendirme ve ağ bilgilerinin belirlenmesi, yönlendirmeye ilişkin güvenlik sorunlarının kontrol edilmesi
- ✓ Paket filtreleme güvenlik kontrolünün yapılması
- ✓ Yönlendirici üzerindeki servislerin belirlenmesi ve güvenlik kontrolleri

**Güvenlik duvarı(firewall) kontrolleri;**

- ✓ Servis yetki kontrollerinin yapılması
- ✓ Yönlendirmeye ilişkin güvenlik sorunlarının kontrol edilmesi
- ✓ Paket filtrelemeye ilişkin güvenlik sorunlarının kontrol edilmesi
- ✓ İşletim sistemine ilişkin güvenlik sorunlarının kontrol edilmesi
- ✓ Firewall güvenlik kurallarının kontrol edilmesi, sorunların ve zayıflıkların belirlenmesi, tasarım, ek bileşen ve güvenlik sıkılaştırması için önerilerde bulunulması
- ✓ NAT kuralları tablosunun gözden geçirilmesi ve tasarım sorunlarının belirlenmesi, önerilerde bulunulması
- ✓ VPN ayar kontrolleri
- ✓ Güvenlik duvarı konfigürasyon kontrolleri
- ✓ Zayıflık ve sızma testleri

- ✓ Ön tanımlı parola, kullanıcı, grup vb. belirlenmesi
- ✓ Uygulama seviyesi geçitlerin kullanımı ve kurallarındaki problemlerin belirlenmesi
- ✓ Firewall üzerinden yoğun/çok fazla paket gönderilmesine karşılık loglama mekanizmasının test edilmesi
- ✓ Endpoint cihazlar için ağ taraması (zararlı içerik alma riskleri)
- ✓ Firewall, Load Balancer ve waf taraması ve güvenliği

**Sunucu kontrolleri;**

- ✓ Sunucuların üzerindeki erişilebilir servislerin belirlenmesi ve güvenlik açıklarının kontrol edilmesi
- ✓ Sunucuların kernel, yama, sürüm bilgilerinin elde edilmesi
- ✓ İşletim sistemine ilişkin güvenlik sorunlarının ve ağ zayıflıklarının kontrol edilmesi
- ✓ Kullanıcı tahmini ve parola kırma testleri
- ✓ Kullanıcı ve servislerde uygunsuz/aşırı yetkilendirmelerin ve zayıflığa yol açabilecek yapılandırmaların belirlenmesi
- ✓ Yapılandırma problemlerinin belirlenmesi
- ✓ Paket filtreleme kurallarına ilişkin problemlerin belirlenmesi
- ✓ Sunucu yazılımlarının güncelliğinin kontrolü
- ✓ Sunucu yazılım yapılandırma ve yetkilendirmelerinin kontrolü
- ✓ Uygulamalara yönelik güvenlik sorunlarının kontrol edilmesi
- ✓ SMTP, FTP, HTIP, HTIPS, TELN ET, ICMP, HPC, NETBIOS, SNMP vb. yaygın kullanılan servisler üzerinden gerçekleştirilebilecek sızmalara karşı detaylı kontroller yapılması, sorunların belirlenmesi
- ✓ Veritabanı ve SAP BO güvenliği
- ✓ Network switch lerin güvenliği
- ✓ İçeriden erişilen uygulamaların güvenliği (Active Roles, İK Oracle, SAP BO, Bott)
- ✓ Admin şifre güvenliği

**Web Uygulamaları Denetimi;**

- ✓ Mevcut uygulamalara sıradan bir kullanıcı gibi giriş yapılarak, yazılım açıklarının kötü kullanıma açıklığının kontrol edilmesi
  - ➢ Oturum yönetimi testleri
  - ➢ Girdi doğrulama testleri
  - ➢ Kimlik doğrulama testleri
  - ➢ Uygulama artığı testleri
  - ➢ Girdi/çıktı yönetimi testleri
  - ➢ Diğer sistemler le iletişim ve veri aktarımı güvenliği testleri
  - ➢ Brute-force parola testi
  - ➢ Yetkilendirme mekanizmasını devre dışı bırakma testleri
  - ➢ Erişime açık olmayan bilgilerin ve dokümanları erişilebilirlik kontrolü
  - ➢ Debug mode denetimleri
  - ➢ Veritabanı servisleri denetimi
  - ➢ Veritabanı yetkisiz erişim denetimleri
  - ➢ Uygulama sunucusu servisleri denetimi
  - ➢ Kullanıcı ve sistem yönetici hakları ayrımı
  - ➢ Kod güvenliği (SIS) sistemi (Güvenli yazılım geliştirme) denetimi

- ✓ Web uygulamalarının otomatik zayıflık testleri
  - ➢ Web sunucu konfigürasyonu
  - ➢ HTIP header manipülasyonu
  - ➢ HTIP form manipülasyonu
  - ➢ UHL manipülasyonu, cross-site scripting testleri
  - ➢ Command injection (OS, SSI, LDAP, XPATH vb. komutları) testleri
  - ➢ SQL sokuşturma (SQL-Injection)
  - ➢ Blind lnjection
  - ➢ Back-end memory, session hijacking, buffer overflow kontrolleri
  - ➢ Çerez (cookie) manipülasyonu
  - ➢ Oturum (session) bilgilerinin manipülasyonu
  - ➢ Cross-frame scripting, cross-site request forgery, CGI script
  - ➢ Erişim izni ve yetkilendirme kontrolleri (authorization & authentication)
  - ➢ Hataların ele alınmaması (error handling)
  - ➢ İstisnaların ele alınmaması (exception handling)
  - ➢ Siteler arası kod çalıştırma (cross-site scripting)
  - ➢ UHL bazlı veri girdisi (UHL validation)
  - ➢ Uygunsuz SSL kullanımı (improper use of SSL certificates)
  - ➢ Zayıf şifre yapıları (weak passwords)
  - ➢ Uygunsuz dosya erişimi (veri kaybı) (improper use of access control)
  - ➢ Diğer uygulama zayıflık testleri

- o FİRMA, internet üzerinden erişilebilen sistemlerde tarama yapacaktır. Asgari olarak yapılacak tarama tipleri aşağıdaki gibidir;
  - ✓ Çalışan sistem taraması (Live System Scanning)
  - ✓ Açık port taraması (Open port scanning)
  - ✓ Güvenlik açıklıkları taraması (Vulnerability Scanning)

- o FİRMA, ilgili sistemlere atak yapacaktır. Yapılacak atak tipleri en az aşağıdaki gibidir;
  - ✓ İşletim sistemi seviyesi (Operating System level attacks)
  - ✓ Uygulama seviyesi (Application level attacks)
  - ✓ Sunucu konfigürasyon hatalarına yönelik ataklar (Misconfiguration attacks)
  - ✓ Yetki seviyesinin yükseltilmesi (Elevating of privileges)

- o Yukarıda listelenen işlemlerin dışında herhangi bir güvenlik açığı bulunup bulunmadığına dair kontrol işlemler yapılmalıdır.

- o Testlerin yalnızca otomatik araçlarla gerçekleştirilmesi yeterli kabul edilmeyecektir. Ek olarak ağ cihazlarının/sunucuların ve özellikle uygulamaların manuel olarak test edilmesi gerekmektedir.

- o Sızma testi raporlarının BİLGİ'ye sunulmasını müteakip güvenlik açıkları BİLGİ tarafından giderildikten sonra, FİRMA bu açıkların giderilip giderilemediğini doğrulama testi ile kontrol edecek ve raporlayacaktır.

**Kaynak Kod Static Kod Analizi**

- o * BİLGİ'nin istemiş olduğu tüm yazılım geliştirme kaynak kodları, limit uygulanmaksızın Statik Kod Analizine tabi tutulacaktır.

- * Tüm bu işlemler BİLGİ'nin temin ettiği bilgisayarlarda kaynak kod dışarıya çıkarılmadan ofline olarak yapılacaktır.

- Firma ve işlemi yapan personelin, kaynak kodların dışarıya çıkarılamayacağına dair test öncesi ceza yaptırımları da olan taahhütname imzalayacaktır.

- * Sızma testi sonrası güvenli yazılım geliştirme için ihtiyaç duyulan uygulamaların istenilmesi halinde "Community edition" versiyonları firma tarafından kurulup, temel eğitimi verilecektir.

**Kablosuz Ağların Testleri**

- BİLGİ'de kullanılan kablosuz ağ cihazlarının genel mimari içindeki yeri incelenecektir.

- BİLGİ'de bulunan kablosuz ağlar taranarak özellikleri keşfedilmeye çalışılacaktır. Kablosuz ağlarda MAC adresi tabanlı filtrelemenin olup olmadığı incelenecek varsa kırılmaya çalışılacaktır.

- Kablosuz ağlarda kullanılan şifreleme ayarları incelenecektir. WEP ve WPA/WPA2 vb. şifreleme kullanılan ağlarda kablosuz ağ şifresi ele geçirilmeye çalışılacaktır.

- Sahte kablosuz ağ erişim noktaları oluşturularak BİLGİ'de bulunan istemciler ele geçirilmeye çalışılacaktır.

- Kablosuz ağ taraması yapılarak, BİLGİ etrafında bulunan diğer kablosuz ağlar keşfedilmeye çalışılacaktır.

**Veritabanı Sızma Testleri**

- Kurum sistemlerindeki Veritabanı uygulamaları ve bu uygulamaları üzerinde barındıran işletim sistemleri tespit edilerek, tespit edilen sistemlere erişimin açık olup olmadığı denetlenecektir. Erişimin açık olması halinde çeşitli tarama çeşitli tarama araçlarıyla Veritabanı versiyonu, üretici adı vb. bilgiler elde edilmeye çalışılacaktır.

- * Elde edilen Veritabanı sistem bilgileri kullanılarak, bu sistemlere yönelik kullanıcı adı ve parola deneme saldırıları yapılacaktır. Bu saldırılar sırasında, ön tanımlı kullanıcı adı ve parolalar ile giriş testleri yapılacaktır.

- *Veritabanı kullanıcı adı ve parola saldırılarının başarısız olması durumunda, işletim sistemi seviyesinden erişim denemeleri yapılacaktır. Windows, Linux vb. ortamlar üzerinden sistem kullanıcıları ile Veritabanı uygulamasına bağlanılmaya çalışılacaktır.

- *Parola deneme saldırılarının başarılı olması durumunda tespit edilen erişim bilgileriyle sistemlere bağlanacaktır. Bağlanılan sistemlerde hassas verilerin bulunduğu, kullanıcı adı, parola ve parolalara ait karmaşık 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 edilecektir. Bilinen açıklıkları içeren ve gerekli güncellemeleri yapılmamış sistemlerde hak yükselme vb. saldırılarla erişim sağlanan kullanıcıların hakları genişletilmeye çalışacaktır.

- * Erişilen sistemlerden diğer erişilemeyen sistemlere tanımlanmış bağlantılar varsa bu bağlantılar kullanılarak diğer Veritabanı uygulamalarına geçilmeye çalışılacaktır.

**Sosyal Mühendislik Testleri**

- Arama motorları, sosyal ağlar ve Kuruma ait web siteleri kullanılarak çalışanları hakkında bilgi elde edilmeye çalışılacaktır.
- Google Hacking (Google Cache'de kuruma ait dosya, Veritabanı, URL, önemli data olup olmadığı) kontrol edilecektir.
- Kurum çalışanlarının ilgisini çekebilecek ve içine sızmaya olanak tanıyacak nitelikte özenle hazırlanmış içinden veya dışından gönderilecek e-postalar ile kullanıcıların bilgileri alınmaya çalışılacaktır.

**Mobil Uygulama Testi**

- BİLGİ' nin sahip olduğu Android ve IOS mobil uygulamaları ayrıntılı şekilde incelenecektir.
- Mobil uygulamaların statik ve dinamik analizleri yapılacaktır.
- Mobil uygulamaların aktivite erişim kontrolleri yapılacaktır.
- Mobil uygulamaların oluşturduğu web trafiği analiz edilecektir.
- Mobil uygulamalardan yerel ağa ve internete yapılan web istekleri analiz edilecek ve güvenlik testleri yapılacaktır.
- Lokal network ve internet üzerinden Mobil uygulama yapılan web istekleri analiz edilecek ve güvenlik testleri yapılacaktır.

### 4.1.3. Raporlama:

- Sızma testi raporunda sistemde belirlenen güvenlik açıkları, bu açıkların taşıdıkları riskler itibariyle öncelikleri ve giderilmesi için yapılması gereken işlemler detaylı ve anlaşılır bir şekilde tarif edilmelidir.
- Test sonucunda hazırlanacak olan ilgili raporlarda;
  - ✓ İncelenen sistemlere ilişkin tespit edilen işletim sistemi/çalışan servis ve sürümleri gibi bilgileri
  - ✓ Tespit edilen güvenlik zafiyetleri, ekran çıktıları ve/veya video görüntüleri
  - ✓ Bu zafiyetlerin sebep olabileceği zararlar/sonuçları ve zafiyete ilişkin referans bilgileri
  - ✓ Güvenlik zafiyetlerini gidermek için yapılması gerekenler
  - ✓ Her bir test adımında uygulanan yöntemler ve kullanılan araçlar, detaylı şekilde açıklanacaktır.
- Test sonucunda oluşturulan tüm raporların içeriği sistematik olarak oluşturulmalı ve her raporda, rapor içeriğine kolay erişilebilirliği sağlamak amacı ile indeks yapısı bulunmalıdır.
- Test sonucunda hazırlanan penetrasyon testi raporunda, tespit edilen güvenlik zafiyetleri kritiklik seviyelerine (kritik, yüksek, orta, düşük) göre gruplandırılacak ve sınıflandırmanın nasıl yapıldığı

ilgili raporda açıklanacaktır.

- Test sonucunda hazırlanan Sızma testi raporunda, tespit edilen bir güvenlik zafiyeti, söz konusu zafiyeti bulunduran sistemler bazında gruplandırılmalıdır.
- Test sonucunda hazırlanan Sızma testi raporunda, tespit edilen her güvenlik zafiyeti için alınması gereken alternatifli önlem/önlemler FİRMA tarafından belirlenmeli ve raporlanmalıdır.
- Test sonucunda hazırlanan Sızma testi raporunda, herhangi bir güvenlik zafiyeti başka bir güvenlik zafiyeti veya zafiyetlerinden faydalanılarak tespit edildiyse, bu zafiyet belirlenmelidir.
- Test sonucunda oluşturulan raporlar, elektronik ortamda Microsoft Word ve Adobe PDF formatında şifreli olarak BİLGİ'ye sunulacaktır. Ek olarak, her iş sonucunda oluşan raporun bir özeti Microsoft PowerPoint sunusu halinde FİRMA tarafından verilecektir.
- Test sonucunda üretilmiş olan raporlar BİLGİ logolu olarak ve FİRMA onaylı formatta sunulacaktır.
- Hizmete ait raporlamalar, ayrıntılı teknik içerikten oluşan "Teknik Rapor" ve istatistiksel özet niteliği taşıyan "Yönetimsel Rapor" şeklinde oluşturulacak ve iletilecektir.
- FİRMA oluşturacağı raporda, zafiyetlerin giderilmesi ve olası zafiyetlerin tekrarlanmaması için genel tasarım ve altyapısal iyileştirmelere tavsiye niteliğinde yer verecektir.

## 5. YETERLİLİKLER:

### 5.1. Test Ekibi Yeterlilikleri:

- FİRMA, teklifinde bu hizmeti gerçekleştireceği personellerini açık kimlikleriyle birlikte tanıtmalı ve bununla ilgili belgeleri (sigorta evrakları, bordro vb.) teklif dosyasına eklemelidir.
- FİRMA bildirdiği ve BİLGİ tarafından kabul edilen personeli dışında hizmetin ifasında başkaca hiçbir personeli BİLGİ'nin özel izni olmadan kullanamaz.
- FİRMA test ekibindeki personel, bu şartnamenin hükümleri saklı kalmak kaydı ile BİLGİ gizlilik sözleşmesini okuyup anladığına ve hükümlerine uyacağına dair, FİRMA ise müteselsil kefil olarak imzalayacaktır. FİRMA imzalanan gizlilik sözleşmelerini, ihaleyi kazanması durumunda yapılacak iş sözleşmesinin imzası ile birlikte teslim edecektir.
- Test ekibi asgari aşağıdaki şartlara sahip olmalı, ekip üyelerinin özgeçmişleri ve ilgili sertifikalarının 'aslı gibidir' onaylı fotokopileri teklif dosyasına eklenmelidir.
- FİRMA'nın test ekibi üyeleri bilgi güvenliğiyle ilgili projelerde en az 10 yıl tecrübeli olmalıdır. Tecrübe süresi SGK kaydı ve sertifikalarıyla ispatlanmalıdır.
- * Sızma testini yapacak olan saha personelinde geçerli TSE Kıdemli Sızma Testi Uzmanı Sertifikası olmalıdır.

### 5.2. FİRMA Yetkinlikleri:

- Sızma testini yapacak FİRMA güncel ISO27001 sertifikasına sahip olmalıdır.
- Sızma testini yapacak FİRMA'nın ihale konusu hizmet kapsamında görevlendireceği en az bir

personeli, uluslararası sertifikalarından (OSCP, OSCE, CISSP, CISA, CEH) en az birine sahip olmalıdır.

- * Sızma testini yapacak FİRMA mevcutta çalışan bir SOC (Security Operations Center) ve NOC (Network Operations Center) yapısına sahip olmalıdır.
- * Sızma testini yapacak FİRMA test ile birlikte bir yıl boyunca DIGITAL CYBER THREAT INTELLIGENCE hizmetini de vermelidir. Bu konuda mevcut çalışan bir ürün ve hizmet yapısına sahip olmalıdır.

## TEST KAPSAMINDAKİ SİSTEMLER-ALTYAPILAR:

**Internet üzerinden tarama için;**

- Üniversite IP Blokları (1xx.xxx.xxx.0/24)(Sözleşmenin imzalanmasından sonra bildirilecektir.)
- Internetten ulaşılabilen bilgi.edu.tr uzantılı siteler. (~200 adet alt site için yüzesel tarama, 50 adet site için derin tarama talep edilmektedir.)

**Lokal tarama için;**

- DMZ ve sunucuların lokal IP blokları verilerek, yerel ağa dahil olan bir client ve test tarayıcı sistemi üzerinden atak denemeleri yapılması zafiyetlerin araştırılması talep edilmektedir. (~200 sanal sunucu) (Sunuculara erişim, güvenlik açıklarının tespiti, çözümü, kontrolü gibi..)

| **KURUM** | **FİRMA** |
|---|---|
| İSTANBUL BİLGİ ÜNİVERSİTESİ | |