T.C.
ANADOLU ÜNİVERSİTESİ REKTÖRLÜĞÜ
DÖNER SERMAYE İŞLETME MÜDÜRLÜĞÜ
Piyasa Fiyat Araştırma Mektubu

Sayı: 97653057/41 Tarih: 01/07/2024

Konu: Piyasa Fiyat Araştırma

Sayın : .....

Kurumumuzun ihtiyacı olan aşağıda cins ve miktarı yazılı 1 kalem malzemeye ve/veya hizmete ilişkin fiyatınızı en geç 05/07/2024 tarih ve saat ...16.00.....'e kadar teslim tarihi ile teklif edilen ürünlere ait bilgiler açıklanmak suretiyle adresimize elden teslim etmenizi, E-posta veya faks göndermenizi rica ederim.

Sertaç BETGÜ
Şef

SNO	MALZEME CİNSİ	MİKTAR	BİRİM	B.FİYAT	TUTAR	MLZ. TESLİM TARİHİ	MARKA
1	Bilişim Sistemi Altyapısına Yönelik Sunucu Ve Veri Merkezi Güvenliği Sızma Testleri Teknik Şartnamede Belirtilmiştir	1	Adet				

TEKNİK ŞARTNAMELERİ EKTEDİR.(TEKNİK ŞARTNAMENİN KAŞELENİP İMZALANARAK GERİ GÖNDERİLMESİ GEREKMEKTEDİR)

MALZEME İSTEK BİRİMİ:	BİLGİSAYAR ARAŞT. VE UYG. MERKEZİ
MALZEME TESLİM YERİ:	A.Ü. Taşınır İşlemleri Şube Müdürlüğü Yunusemre Kampüsü ESKİŞEHİR - 0222 335 05 80 / 1780

Yukarıda cins ve miktarı yazılı malzemeleri ve/veya hizmeti hizalarında belirtilen fiyatlarla vermeyi beyan ediyorum.

Firma Adı/ Kaşe/ İmza

AÇIKLAMA

1- Fiyatlar KDV hariç TL (Türk Lirası olarak belirtilecektir. (Örn:0,00))

2- Alternatif Fiyat Mektubu Değerlendirmeye Alınmayacaktır.

3- Malzeme Teslim Tarihi Önemle Belirtilecektir.

4- Malzemelerin Nakliye Bedeli Firmanıza Aittir.

5- Kargo ile mal gönderilmemesi esastır. Gönderilmesi halinde sorumluluk firmaya aittir.

6- Firmalar malı göndermeden önce Malzeme Muayene Kabul ve Teslim Alma Merkezine bildirimde bulunması ve kabulde firma yetkilisinin bulunması yasa gereğidir.

7- Teklif edilen ürünlere ait varsa TSE marka ve ISO kalite güvence belgeleri teklif ile birlikte sunulmalıdır.

8- Bilgi için telefon numarası: 0 222 335 05 80-1084 -1085 Faks:0 222 3307163

9- Adres: A.Ü. DÖNER SERMAYE İŞLETME MÜDÜRLÜĞÜ YUNUSEMRE KAMPÜSÜ 26470 ESKİŞEHİR

10- E-Posta: donersatinalma@anadolu.edu.tr Web: www.anadolu.edu.tr
Yazılı olan mail adresine cevap veriniz. Bu mail adresi dışındaki adreslere gönderilen teklifleriniz dikkate alınmayacaktır.

11- Üniversitemiz ile ilgili satınalma duyurularımıza [https://www.anadolu.edu.tr/satin-alma-duyurular] adresinden ulaşabilirsiniz.

Bilişim Sistemleri Altyapısına Yönelik Sızma Testleri Hizmet Alımı İşi

Teknik Şartname

1. Konu

Bu teknik şartname Anadolu Üniversitesi'ne ait bilişim sistemleri altyapısına yönelik sunucu ve veri merkezi güvenliği test hizmetleri alımı işine dair genel hükümleri ve teknik özellikleri içermektedir.

2. Genel Hükümler

2.1. Yüklenici, Kurum ile sözleşme imzalamadan önce firma tüzel kişiliği ile "BAUM.SZ.01 Bilgi Güvenliği Yönetim Sistemi Gizlilik Sözleşmesi" ve İdare'ye ait tesislerde görevlendirilecek gerçek kişiler ile "BAUM.TA.02 Kurum Dışı Gizlilik ve Tarafsızlık Taahhütnamesi" formlarını karşılıklı olarak imzalayacaktır.

2.2. Yüklenici tarafından iş sürekliliğinin sağlanması adına Acil Durum Planı hazırlanacaktır.

2.3. Yüklenici tarafından temin edilen yazılımların İdare bünyesinde bulunan sistemlerine her türlü bakım, onarım, güncelleme vb. ihtiyaçlar için uzaktan erişim ihtiyacı bulunması durumunda, ilgili yazılımın ve yazılımın barındırıldığı sunucunun sorumluları gözetiminde, gerektiğinde iş ve işlemlerin kayıt altına alınabildiği Toplantı Çözümü Programları (Webex, GotoMeeting, FastSupport, Zoom, Skype Kurumsal) kullanılacaktır. Bağlantı programı için lisans ihtiyacı oluşması halinde lisans Yüklenici tarafından sağlanacaktır.

2.4. Yüklenici, Bilgi Güvenliği Yönetim Sistemi kapsamında kendisi ya da bir başkası tarafından ihlal gerçekleştiğinde, durumu İdare'ye yazılı olarak bildirecektir.

2.5. Yüklenici ile imzalanan sözleşmenin süresinin dolması ya da fesih edilmesi durumunda yükleniciye atanmış tüm yetkilerin kaldırılması için Yüklenici tarafından İdareye yazılı olarak bilgi verilecektir.

3. Şartlar

3.1. Yüklenicinin TS EN ISO 27001:2013 belgesi bulunacaktır.

3.2. Bu şartnamede tanımlanan hizmetlerin kapsamı, Anadolu Üniversitesi Kampüsü'ndeki tesislerinde yer alan sunucu sistemleridir.

3.3. Bu şartnamede tanımlanan hizmetleri içeren projenin toplam süresi 1 (bir) yıldır.

3.4. Yüklenici ve İdare hizmet başlangıcında bu hizmete özel bir gizlilik sözleşmesi imzalayacaktır.

3.5. Yüklenici, sözleşmenin imzalanmasından itibaren en geç 10 (on) iş günü içerisinde, şartname kapsamında verilecek hizmetler ile ilgili detaylı proje planı hazırlayarak İdare'ye sunacaktır.

3.6. Yüklenici, bu şartname kapsamında verilecek tüm hizmetleri koordine etmek ve projenin planlandığı gibi ilerlemesini kontrol etmek üzere bir proje yöneticisi görevlendirecektir.

3.7. Aşağıdaki sertifikaya sahip personelin CV'leri ve ilgili sertifikaları, teklif dosyasında Kurum'a sunulacaktır.

- En az 1 (bir) adet CEH (Certified Ethical Hacker)
- En az 1 (bir) adet OSCP (Offensive Security Certified Professional) veya GPEN (GIAC Penetration Tester Certification)
- En az 1 (bir) adet TSE Sertifikalı Ağ Sızma Testi Uzmanı (TSE-STU-STF-AĞ)

3.8. Yüklenici, Türk Standartları Enstitüsü tarafından verilen "TS-13638 sızma testi yapan personel ve firmalar için şartlar" standartı kapsamında "A veya B Sınıfı Onaylı Sızma Testi Firması" belgesine sahip olacaktır. Bu belgenin geçerlilik tarihi en az ihalenin yapıldığı yılın sonuna kadar olacaktır. Yüklenici bu belgeyi teklif dosyasında sunacaktır.

4. İnternet Güvenlik Test Hizmeti

4.1. Yüklenici tarafından proje süresi boyunca en az 1 (bir) defa olacak şekilde internet üzerinden güvenlik testleri gerçekleştirilecektir.

4.2. İnternet üzerinden gerçekleştirilecek testler beyaz kutu ve kara kutu şeklinde gerçekleştirilecek olup beyaz kutu testleri İdare tarafından sağlanacak IP adresinde bulunan sunucular için gerçekleştirilecektir.

4.3. İnternet üzerinden yapılacak testler en az aşağıdaki kontrolleri içerecektir.

4.4. Kurum'a ait izlerin toplanması,

- İSS (İnternet Servis Sağlayıcı), alan adı sahibi, IP adresleri, AS (Otonom Sistem) numarası gibi bilgilerin toplanması,
- İnternet üzerinden değişik arama motorları kullanılarak bilgi 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,
- Erişilen sunucu işletim sistemlerinin, yama ve sürümlerinin belirlenmesi,
- Açık portlar üzerinde çalışan uygulamaların belirlenmesi,
- Çalışan servislere ait detaylı bilgiler elde edilmesi.

4.5. DNS sunucu yapılandırma uygunluk kontrolü,

4.6. Dışarıya hizmet veren sunucu kontrolleri,

- İnternet üzerinde servis veren DNS, web, e-posta, FTP vs. gibi sunucuların kontrolü,
- İnternete açık sunucuların üzerindeki erişilebilir servislerin belirlenmesi, uygunsuz/gereksiz olanların tespiti,
- İşletim sistemi güvenlik açıklıklarının kontrolü,
- Uygulamaya (IIS, OWA vb.) özel güvenlik açıklıklarının kontrolü,
- Sunucular üzerinde çalışan kurumsal uygulamaların incelenmesi,
- Kullanıcı tahmini ve parola kırma testleri,
- SMTP, FTP, HTTP, HTTPS, TELNET, ICMP, RPC, NETBIOS, SNMP vb. yaygın kullanılan servisler üzerinden gerçekleştirilebilecek sızmalara karşı detaylı kontroller yapılması, açıklıkların belirlenmesi.

4.7. İnternet üzerinden erişilebilir diğer sistemlerin taranması.

- İnternet üzerinden duyurulmuş sunucuları dışındaki sistemlerinin kontrolü,

- Söz konusu sistemler üzerindeki erişilebilir servislerin belirlenmesi ve güvenlik açıklıklarının kontrolü.

5. Yerel Ağ Güvenlik Test Hizmeti

5.1. Yüklenici, proje süresi boyunca yılda en az 1 (bir) defa olacak şekilde yerel ağ üzerinden güvenlik testleri gerçekleştirecektir.

5.2. Testler en az aşağıdaki kontrolleri içerecektir:

5.3. Genel amaçlı kullanılan sunucu testleri:

- Sunucular üzerindeki erişilebilir servislerin belirlenmesi.
- İşletim sistemi güvenlik açıklıklarının tespiti.
- Uygulamaya özel güvenlik açıklıklarının kontrolü.
- Kullanıcı tahmini ve parola kırma testleri.
- Kritik dosya ve paylaşımların erişilebilirliği ve izinsiz kullanımının kontrolü.
- Dosya sistemi üzerindeki, yönetici veya olması gerekenden yüksek yetkilere sahip servislerin kontrol edilmesi.

5.4. Yerel alan ağında önemli görülen istemcilerin taranması:

- Söz konusu makineler üzerindeki erişilebilir servislerin belirlenmesi.
- İşletim sistemi ve uygulama seviyesi güvenlik problemlerinin kontrolü.

6. Otomatik Servis Dışı Bırakma (DDoS) Test Hizmeti

6.1. Yüklenici, proje süresi boyunca en az 1 (bir) kez otomatik DDOS test aracı sağlayacaktır.

6.2. Proje bazlı test setleri aşağıdaki kriterlere uygun şekilde oluşturulacaktır:

- Bir takvim üzerinden takip edilebilecek.
- Değişik tiplerde ve boyutlarda tatbikatlar önceden programlanıp, vakti geldiğinde hızlı bir şekilde saldırı başlatılabilecek.

6.3. DDOS testleri, en az aşağıdaki saldırı tiplerini içerecektir:

- ICMP Flood,
- TCP Flood,
- UDP Flood,
- DNS Flood,
- Slowloris,
- HTTP/S GET Flood,
- HTTP/S POST Flood,

6.4. Test anında gerçek zamanlı bir şekilde; saldırı boyutu – bant genişliği ve pps bazında izleme yapılabilecektir.

6.5. Test anında gerçek zamanlı bir şekilde hedef sistemin tepki süresi izlenebilecektir.

6.6. Acil durdurma (Emergency stop) mekanizması olacak, bir sıkıntı durumunda DDOS testi tek aşamada durdurulabilecektir.

6.7. DDOS testi sonunda alınacak raporlar aşağıdaki kriterlerde olacaktır:

- Otomatik bir rapor oluşturulabilecek ve bu raporun içeriğinde en az aşağıdaki grafikler yer alacaktır:
  - Saldırı yapılan sistemin sağlık durumu.
  - Gerçekleştirilen saldırının teknik detayları (saldırı türü, boyutu, tarih aralığı, hedef sistem vb.)
- Rapor üzerinde testi gerçekleştiren tarafından yorum eklenebilecek bir alan bulunacaktır.
- Raporlar HTML formatında olacaktır.

7. Raporlama

7.1. Yüklenici tarafından hazırlanacak denetim raporları asgari olarak aşağıdaki hususları kapsayacak ve aşağıda belirtilen formata/içeriğe uygun olacaktır.

7.2. Denetim raporu, sözlü açıklamaya gerek bırakmayacak şekilde açık ve net biçimde yazılacaktır.

7.3. Raporlarda, gizlilik derecesi, denetimin başlangıç-bitiş tarihleri ve rapor teslim tarihi belirtilecektir.

7.4. Risk düzey tanımları belirtilecektir.

7.5. Yapılan zafiyet testlerinin adları ve tanımları ayrıntılı olarak verilecektir.

7.6. Yapılan denetimler sonucunda, zafiyet/açıklık bulunan sistemlerin özet IP bilgisi verilecektir.

7.7. Denetim raporuna ek olarak Yönetici raporu da sağlanacaktır.

7.8. Raporlar, her zafiyet/bulgu için minimum aşağıdaki maddeleri içerecektir:

- Tespit Edilen Zafiyet/bulgu tanımları,
- IP ve/veya FQDN bilgisi,
- Derlenen Veri, zafiyete/bulguya ilişkin kayıtlar ve ekran görüntüleri,
- Zayıflıkların risk düzeyleri ve gerçekleşmeleri durumunda oluşabilecek zararların ölçekleri,
- Zayıflıkların giderilmesine ilişkin ilgili sistem üzerinde çalışan uygulama üreticisinin yayınlamış olduğu ayrıntılı çözüm önerileri ve varsa alternatif çözüm önerileri,
- Tespit edilen zafiyetin çeşitli standartlardaki (PCI, OWASP,vb) kategorisi,
- Zafiyete/bulguya ait varsa CVE, bug-track id,vb ortak zafiyet veri tabanı tanımlayıcı kodları yazılmalıdır.

8. Doğrulama Test Hizmeti

Güvenlik testi tamamlanıp rapor sunulduktan sonra kurum zayıflıkların kapatıldığını belirterek tekrar 2. test olan doğrulama testi talep edecektir. Doğrulama testi güvenlik testi sonuç raporunda tespit edilen zayıflıkların tekrar tespit edilip edilmediğinin doğrulaması için uygulanacaktır.

Ahmet Soner TAN
Öğr. Gör.

Muhammet Nurullah ÇETER
Mühendis

Kemal SAĞLAM
Bilişim Personeli

Dr. Öğr. Üyesi Mesut AYDEMİR
BAUM Müdür Yrd.