KONYA GIDA VE TARIM ÜNİVERSİTESİ

BİLGİ İŞLEM DAİRE BAŞKANLIĞI

SIZMA TESTİ HİZMET ALIMI VE KURUMSAL SOME EĞİTİMİ TEKNİK ŞARTNAMESİ

1. AMAÇ

Bilgi Güvenliği Yönetim faaliyetleri kapsamında; sistem merkezi bünyesinde işletilmekte olan uygulamalar ile diğer bilişim sistemlerinde kişisel veriler ile birlikte ulusal ve uluslararası öneme sahip veriler işlem görmekte, bahsi geçen verilerin güvenliği oldukça önem arz etmektedir. Bu kapsamda güvenlik tarama testleri hizmeti alınması amaçlanmaktadır.

2. KISALTMALAR

İDARE : Konya Gıda ve Tarım Üniversitesi Bilgi İşlem Daire Başkanlığı

YÜKLENİCİ : Teklif veren isteklilerden ihaleyi kazanan ve/veya onun teknik hizmet sağlayıcısı olarak çalışarak hizmetleri gerçekleştirecek firma veya firmalar

BGYS : Bilgi Güvenliği Yönetim Sistemi

3. KAPSAM

3.1 İdarenin bilişim sistemlerinde oluşabilecek güvenlik açıklıklarını veya zafiyetlerini azaltacak gerekli güvenlik taraması testlerinin yürütülmesi,

3.2 Güvenlik Tarama testlerinin kapsamı aşağıdaki şekilde olacaktır.

3.2.1 Sistem ve Network Sızma Testi
3.2.2 Uygulama Sızma Testi
3.2.3 DDOS
3.2.4 Sosyal Mühendislik

4. PROJE SÜRESİ

4.1 Proje imza tarihinden itibaren en fazla 20 (yirmi) iş günüdür. Yüklenici daha önce çalışmalarını tamamlayıp ilgili raporları İdare'ye teslim edebilecektir.

5. GENEL HÜKÜMLER

5.1 Yüklenici, sözleşmenin imzalanmasından sonra projede görevlendireceği kişileri ve görevlerini belirtecektir.

5.2 İdare, tekliflerin değerlendirilmesi sırasında ek açıklama isteme hakkına sahip olacaktır.

5.3 Yüklenici firma, yapılan testler ve rapor işlemlerinde kullanacak bütün donanım, yazılım ve cihazları kendisi temin etmelidir.

5.4 Yüklenici firma, bu teknik şartname kapsamındaki Projenin eksiksiz olarak tamamlanmasından mesuldür.

5.5 Yüklenici, test ve değerlendirme çalışması sonucunda Detaylı Teknik Test Sonuç Raporu'nu hazırlayarak İdare'ye sunacaktır. Teknik rapor yeterince açık ve sözlü açıklamaya gerek bırakmayacak biçimde net olacaktır.

5.6 Test ve inceleme hizmetlerini yürütecek proje lideri projenin yönetilmesinden sorumlu olacaktır.

5.7 Test ve inceleme hizmetlerini yürütecek proje lideri en az lisans mezunu, zafiyet analizi ve sızma testi sahasında en az üç (3) yıllık iş tecrübesine sahip olmalı ve bunu belgelendirebilmelidir.

5.8 Test ve inceleme hizmetlerini yürütecek proje lideri daha önce bilgi güvenliği alanında ISO27001 danışmanlık hizmeti yapmış ve en az 1 proje yönetmiş olmalıdır.

5.9 Detaylı Teknik Test Sonuç Raporunun içeriği en az İç Ağ Testi, Dış Ağ Testi, Kablosuz Ağ Testi, Servis Testi ve DDoS Testi bölümlerinden oluşmalıdır. Sonuç raporu en azından şu konuları kapsamalıdır: Derlenen veriler, tespit edilen zafiyetler, zafiyetlerin risk düzeyleri ve gerçekleşmeleri durumunda oluşabilecek zararların ölçekleri, zafiyetlerin giderilmesine ilişkin (varsa alternatifli) öneriler ve Yüklenicinin diğer notlarından oluşmalıdır.

5.10 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.

5.11 Dış ağ erişim noktaları ve iç ağ topolojisi idare tarafından yüklenici firmaya verilecektir. Bu verilen topolojiye göre ayrıntılı bütün iç ve dış IP numaraları için en az Layer 3 katmanında tarama yapılıp bütün açık port ve sistem topoloji haritası çıkartılacak bu haritaya göre uygun test altyapısı hazırlanıp bu topoloji üzerinden temel metodolojiye karar verilecektir.

5.12 Yapılacak testler en az 4 ana kısım üzerinden yürüyecektir. Bunlar iç ağdan yapılacak testleri, dış ağdan yapılacak testler, servis testleri, DDoS testleri, Sosyal Mühendislik testleri ve varsa diğer testler şeklinde kategorize edilecektir.

5.13 DDoS testleri kurumun en az servis verdiği saatlerde ve sistem yöneticileri ile koordine olarak gerçekleştirilecektir.

5.14 DDoS testleri iç ağ ve dış ağ olmak üzere iki ayrı bölgeden yapılacak olup üniversite bünyesinde hizmet veren bütün Web ve DNS hizmeti veren sunucuları kapsamaktadır.

5.15 İç ağ testleri için yerel ağ altyapısı dikkate alınarak bir erişim noktası belirlenip bu erişim noktası kullanılarak yerel ağa bağlı sistemler test edilecektir.

5.16 Dış ağdan yapılacak testler için farklı erişim noktalarından İdareye ait ve internet üzerinden erişilebilen sistemler test edilecektir.

5.17 Servis testlerinde ise idare bünyesinde çalışmakta bulunan sunucu servislerinin güvenlik açıkları test edilecektir.

5.18 Farklı test kategorilerindeki açıklar ve çözüm önerileri ayrı olarak raporlandırılacaktır.
5.19 Proje yöneticisi olarak bildirilen personelin sağlaması gereken en az özellikler aşağıda belirtilmiştir.
5.19.1 Türk vatandaşı olması ve sabıka kaydının olmaması.
5.19.2 Üniversitelerin 4 (dört) yıllık lisans programlarından mezun olmak.
5.19.3 Aşağıda belirtilen profesyonel sertifikalardan en az birine tanesine sahip olmak;
LPT Master (EC-Council Licensed Penetration Tester)
5.19.3.1 CPTC (Mile2, Certified Penetration Testing Consultant)
5.19.3.2 GPEN (GIAC, Certified Penetration Tester)
5.19.3.3 ECPPT (eLearnsecurity, Certified Professional Penetration Tester)
5.19.3.4 OSCP (Offensive Security Certified Penetration)
5.20 Proje'de görev alacak bütün personellerin sağlaması gereken en az özellikler aşağıda belirtilmiştir:
5.20.1 Türk vatandaşı olması ve sabıka kaydının olmaması.
5.20.2 Aşağıda belirtilen profesyonel sertifikalardan en az birine tanesine sahip olmak;
5.20.2.1 CEH (EC-Council tarafından verilen Certified Ethical Hacker)
5.20.2.2 CPTP (Mile2 tarafından verilen Certified Penetration Tester)
5.20.2.3 CISA (ISACA tarafından verilen Certified Information Systems Auditor)
5.21 Yüklenici, söz konusu personelin sahip olduğu sertifikaları sözleşme imzalandıktan sonra, işe başlamadan önce İdare'ye sunacaktır.
5.22 Teklif veren firmanın TSE Hizmet Yeri Yeterlilik Belgesi, ISO 9001 Kalite Yönetim, ISO 27001 Bilgi Güvenliği Belgesi veya ISO 20000 Bilgi Teknolojileri Hizmet Yönetim Sistemi Kalite Belgeleri bulunmalıdır Bu belgeler kurulum aşamasından önce idareye ibraz edilmelidir.

6. ZAAFİYET ve SIZMA TESTİ ÇALIŞMALARI

6.1 İdarenin BT altyapısı güvenliği, hem internet hem de yerel alan ağı (intranet) üzerinden denetlenecektir.

6.2 İdarenin domain ve subnetlerinde güvenlik açıkları ve bunların yarattığı riskler tespit edilecek, gerekli iyileştirmelere yönelik öneriler raporlanacaktır.

6.3 Yüklenici tarafından gerçekleştirilecek testler kurum bünyesinde çalışan 50 adet sunucu için gerçekleştirilecektir.

6.4 Yapılan analizler sonucunda güvenlik açığı tespit edilirse İdarenin iş akışında ne tür riskler oluşturacağı tespit edilecektir. Sonuçlar gizli bir rapor ile İdareye sunulmalı ve bu açıklara karşı güvenliği arttırmak için iyileştirici öneriler de belirtilecektir.

6.5 Güvenlik Denetiminin sonucunda hazırlanan rapor İdareye bir toplantı ile sunulacaktır. Denetim ve analiz sırasında ortaya çıkan güvenlik konularının karşılıklı olarak görüşülerek hızlıca giderilmesi için öneriler sunulacaktır.

6.6 Yüklenici, denetim testleri sırasında İdarenin internet hizmetlerinin kesintiye uğramamasını sağlamalıdır. Çalışmalar esnasında internet hizmetlerinin kesilmesi gerekli ise, çalışmalar Kurumun resmi mesai saatleri dışında İdarenin izni ile yapılabilecektir.

6.7 Bu şartnamede tanımlanan ve Yüklenici tarafından gerçekleştirilecek güvenlik denetimleri, sonuçları ve ilgili çalışmalar kapsamında elde edilen her türlü bilgi, Yüklenici tarafından gizli tutulacak ve elde edilen hiçbir matbu/elektronik belge kopyalanarak çoğaltılmayacaktır.

7. İç Ağdan Gerçekleştirilecek Temel Sızma Testleri (İç Ağ Testi)

7.1. Yerel ağda bulunan bütün ip bloklarında yer alan bilgisayarlar, sunucu ve cihazlarda tespit edilen açık portlar üzerinden içerik filtreleme, güvenlik duvarı atlatma ve bilgi kaçırma ve sistemlerine giriş testleri gerçekleştirilecektir.

7.2. Üniversite bünyesinde iç ağda bulunan sunucular ve cihazlar üzerinde çalışmakta olan servislere ait kullanıcı adı ve şifreler tahmin edilerek sunuculara erişilmeye çalışılacaktır. Bu işlem için gelişmiş kullanıcı adı ve şifre tahmin etme programları kullanılacaktır.

7.3. Yerel ağ için zafiyet taraması yapılacaktır.

7.4. Kurum yerel ağında araya girme teknikleri ile hassas bilgiler elde edilmeye çalışılacaktır.

7.5. Elde edilen bilgiler ışığında kullanıcı bilgisayarları, sunucu sistemleri ve aktif cihazlara yönelik ele geçirme saldırıları gerçekleştirilecektir.

7.6. Ele geçirilen sunucu ve kullanıcı bilgisayarları üzerinden daha kritik bilgilere ulaşılmaya çalışılacaktır.

7.7. Elde edilen açıklar ve çözüm önerileri İç Ağ Testi raporunda belirtilecektir.

8. İletişim Altyapısı ve Aktif cihazlar Sızma Testleri (İç Ağ testi)

8.1. Kurumda kullanılan ağ cihazlarının genel mimari içindeki yeri incelenecektir.

8.2. Tüm ağ cihazları açıklık bulma araçları ile taratılacaktır.

8.3. Tespit edilen açıkların uygulanabilirlikleri sınanacaktır.

8.4. Ağlarda MAC adresi tabanlı filtrelemenin olup olmadığı incelenecektir.

8.5. Aktif cihaz üzerindeki port güvenliği, VLAN ve trunk yapısı incelenecektir.

8.6. Ağ topolojisi ve segmentasyonu incelenerek kullanıcı-sunucu ağları arasında erişim kontrolünün olup olmadığı denetlenecektir.

8.7. Paket dinlemesi yoluyla ağ üzerinden geçebilecek VoIP paketleri yakalanmaya ve konuşmalar dinlenmeye çalışılacaktır.

8.8. Aktif cihaz üzerinde çalışan servisler incelenecektir.

8.9. Kullanılan servislerin servis dışı bırakılmayla sonuçlanabilecek saldırılara karşı (ARP zehirlemesi, CDP DoS, DHCP DoS, SNMP DoS vb.) durumu incelenecektir.

8.10. Cihazlar üzerinde açık olan Telnet, HTTP, FTP, SNMP, TFTP, SSH servislerine sözlük saldırısı veya kaba güç kullanılarak erişim sağlanmaya çalışılacaktır.

8.11. Erişim sağlanan cihazlar üzerinden alınan bilgilerle diğer cihazlara erişilmeye çalışılacaktır.

8.12. Aktif cihazlar için uzak/yerel erişim kontrolü, yönetim, kayıt ve kimlik doğrulama mekanizmaları incelenecektir.

8.13. Cihazların merkezi şekilde yönetilmesini ve gözetlenmesini sağlayan yönetim sistemlerinin varlığı araştırılıp, bu sistemlere sızma girişimlerinde bulunulacaktır.

8.14. Cihazlarda ortak parolanın kullanılıp kullanılmadığı test edilecektir.

8.15. Kurum çalışanları için kullanılan içerik filtreleme sistemleri atlatılmaya çalışılacaktır.

8.16. Kurum içinden dışarı tünel kurulmasıyla, kurum dışından kurum içine yetkisiz bağlantı gerçekleştirilmeye çalışılacaktır.

8.17. Kurum dışına açık yönetim ara yüzlerinin varlığı kontrol edilecektir.

8.18. Elde edilen açıklar ve çözüm önerileri İç Ağ Testi raporunda belirtilecektir.

9. Dış Ağdan Gerçekleştirilecek Temel Sızma Testleri (Dış Ağ Testi)

9.1. İdare bünyesinde sunucu sistemleri ve cihazlar üzerindeki açık portlar üzerinden içerik filtreleme, güvenlik duvarı atlatma ve bilgi kaçırma testleri gerçekleştirilecektir.

9.2. Üniversite bünyesinde sunucular üzerinde çalışmakta olan servislere ait kullanıcı adı ve şifreleri tahmin edilerek sunuculara erişilmeye çalışılacaktır. Bu işlem için gelişmiş kullanıcı adı ve şifre tahmin etme programları kullanılacaktır.

9.3. Bu sunucular ve cihazlar için dış erişim noktası üzerinden zafiyet taraması yapılacaktır.

9.4. Elde edilen bilgiler ışığında kullanıcı bilgisayarları, sunucu sistemleri ve aktif cihazlara yönelik ele geçirme saldırıları gerçekleştirilecektir.

9.5. Ele geçirilen sunucu ve kullanıcı bilgisayarları üzerinden daha kritik bilgilere ulaşılmaya çalışılacaktır.

9.6. Elde edilen açıklar ve çözüm önerileri Dış Ağ Testi raporunda belirtilecektir.

10. DNS Servisleri Testi (Servis Testi)

10.1. DNS sunucuların topolojik konumu incelenecektir.

10.2. Sunucu üzerinden alan transferi (zone transfer) yapılmaya çalışılacaktır.

10.3. NXT ve NSEC kaynak kayıtları üzerinden bilgi elde edilmeye çalışılacaktır.

10.4. Netcraft, Google, Whois sorguları yapılarak Kurum ağında yer alan sunucular tespit edilmeye çalışılacaktır.

10.5. DNS sunucular için ön bellek zehirlemesi gerçekleştirilmeye çalışılacaktır.

10.6. DNS sunucular üzerindeki kaynak kayıt girdileri incelenecektir.

10.7. DNS sunucular üzerindeki ters kaynak kayıt girdileri incelenecektir.

10.8. DNS sunucuların sürüm bilgisi elde edilmeye çalışılacaktır.

10.9. Kurum dışı alan isimleri sorgulanmaya çalışılacaktır.

10.10. Sunucular üzerinde DNS dışında bir servisin çalışıp çalışmadığı incelenecektir.

10.11. Güvenlik Duvarında DNS sunucular için izin verilen portlar incelenecektir.

10.12. DNS sunucuları güvenlik taramasına tabi tutulacaktır.

10.13. DNS servisini veren yazılımın açıklıkları araştırılacaktır.

10.14. Elde edilen açıklar ve çözüm önerileri Servis Testi raporunda belirtilecektir.

11. Sosyal Mühendislik

11.1 Kurum içi sosyal mühendislik testlerinde asgari olarak aşağıdaki testler gerçekleştirilir:

11.2 Kurum yerel ağından veya dışarıdan gönderilecek e-postalar ile hassas bilgilere ulaşılmaya çalışılacaktır.

11.3 Kurum içinden veya dışarıdan yapılacak telefon görüşmeleri ile hassas bilgilere ulaşılmaya çalışılacaktır.

11.4 Elde edilen şifre ve haklar ile hassas bilgilerin bulunduğu sunucu ve kullanıcı bilgisayarlarına erişim sağlanmasına çalışılır.

12. Kurumsal Some Eğitimi

12.1 1 kişi için ileri seviye Kurumsal Some Eğitimi verilecektir.