E-POSTA GÜVENLİK ÇÖZÜMÜ (ANTISPAM) TEKNİK ŞARTNAMESİ

Teklif edilecek e-posta ağ geçidi güvenlik yazılımı aşağıdaki özelliklere sahip olacaktır.

1- Teklif edilecek E-Posta Güvenlik Yazılımı, SMTP ağ geçidi ürünü olacaktır.
2- Teklif edilecek program, sanal sunucular üzerinde ya da daha önceden uyumluluğu üretici tarafından belgelendirilmiş sunucu donanımları üzerinde çalışabilmelidir. Aşağıda belirtilen sanal platform sistemlerinin en az ikisi desteklenmelidir.
    - Microsoft Hyper-V Server 2012- 2012 R2
    - VMware ESXi 6.0 ve üzeri
    - Citrix Xenserver 6.5
3- Teklif edilecek program istenmeyen elektronik postalara (spam), virüslere ve zararlı yazılımlara karsı ağ geçidi olarak koruma sağlayacaktır.
4- Teklif edilecek program, LDAP sorgulaması ile alıcı adresi doğrulaması yapabilecektir ve alıcısı dizinde var olmayan gelen ve giden e-postaları reddedecektir.
5- Teklif edilecek program aşağıda belirtilen LDAP dizin sistemlerini desteklemelidir. LDAP sunucuları ile yapılan bağlantı SSL protokolü üzerinden gerçekleşmelidir (LDAP over SSL).
    - IBM Lotus Domino
    - Microsoft Active Directory
    - Microsoft AD Global Catalog
    - OpenLDAP
    - Sun iPlanet Directory
6- Teklif edilecek program, gönderici alan adı için DNS sorgusu yaparak DNS kaydı olmayan epostaları engelleyebilecektir.
7- Teklif edilecek program, gönderici IP adresi için PTR sorgusu yapabilecektir ve PTR kaydı olmayan epostaları engelleyebilecektir.
8- Teklif edilecek program, izin verdiği epostaları, yük dengeleme ve önceliklendirme yöntemleri ile birden fazla eposta sunucusuna yönlendirebilecektir.
9- Teklif edilecek program, TLS destekleyecektir. Gelen bağlantılarda TLS protokolünü hem opsiyonel hem zorunlu olarak kullanabilecektir.
10- Teklif edilecek program Anti Spam ve Anti virüs özelliği ile teklif edilecektir.
11- Teklif edilecek program gelen ve giden tüm trafiği tek bir sanal sunucu üzerinde tarayabilmelidir.
12- Teklif edilecek program “0” gün virüs koruması ile şüpheli bulunan mesaj ekleri virüs karantinasına gönderilebilmelidir.
13- Teklif edilecek program ile Pazarlama, Sosyal Medya siteleri gibi yerlerden gelen e-postalar için ayrı bir filtreleme mekanizması bulunmalıdır. Bu mekanizmaya uygun şekilde kurallar yazılarak aksiyonlar alınması sağlanabilmelidir.
14- Teklif edilecek program üreticisi tarafından sunulan eposta saygınlık sistemi veri tabanına göre e-postaların spam olup olmadığını sorgulayacak ve bu duruma göre aksiyonlar alınmasını sağlayabilecektir.
15- Teklif edilecek program oltalama saldırılarına karşı Sosyal Mühendislik saldırılarından koruma yeteneğine sahip olmalıdır. Teklif edilecek program Spyware, adware tipinde zararlılara karşı koruma sağlamalıdır.
16- Teklif edilecek program, giden e-postalar için DKIM imzalama metodunu (DomainKeys Identified Mail Signing) desteklemelidir.
17- Teklif edilecek program, SPF(Sender Policy Framework) doğrulaması yapabilecektir. Bu doğrulama sonucuna göre reddetme, karantinaya alma ve benzeri aksiyonlar alabilecektir.

18- Teklif edilecek program uyumlu bir Internet tarayıcısı ile yönetilebilecek HTTPS tabanlı bir web yönetim arayüzüne sahip olmalıdır. Yönetim arayüzü üzerinde; sistem bileşenlerinin güncellik derecesi, anlık olarak işlemci, hafıza, disk kullanımı, sistem tarafından denetlenen ve yakalanan zararlı mail istatistikleri gibi bilgiler görülebilmelidir.
19- Teklif edilecek program gelen e-posta içerisinde bulunan linkleri gerçek zamanlı bir reputasyon filtresinden geçirerek zararlı linkler bulunduran e-postaları engelleyebilmeli, karantina altına alabilmelidir.
20- Teklif edilecek program, e-posta içerisinde geçen URL adresleri o anda veritabanında zararlı olarak işaretlenmemiş olsa dahi ilerde zararlı olarak veritabanına eklenmesi ihtimaline karşı URL adresinin hedefini değiştirerek izin verebilmelidir. Böylece kullanıcının ileri bir tarihte URL adresine gidişini engelleyebilmelidir.
21- Teklif edilecek program gelen ve giden e-postalara boyut ve gönderici sayısı sınırlamaları uygulayabilmelidir.
22- Teklif edilecek program, aşağıda belirtilen son kullanıcı karantina özelliklerini sağlamalıdır.
    - Son Kullanıcı Karantina Sistemi (EUQ), doğrulama sistemi içermelidir. Doğrulama sistemi, LDAP dizin sistemini ve SMTP doğrulama sistemini desteklemelidir.
    - Son Kullanıcı Karantina Sistemi (EUQ), günlük olarak kullanıcılara karantina bilgilendirme e-postası iletebilmelidir.
    - Son Kullanıcı Karantina Sistemi (EUQ), kullanıcılara web tabanlı bir arayüz üzerinden karantinaya alınan e-postaların yönetimini desteklemelidir.
    - Son Kullanıcı Karantina Sistemi (EUQ) üzerinden gönderilen bilgilendirme e-postaları içerisinde karantinaya alınmış e-postalar için silme ya da karantinadan çıkarma aksiyonlarına dair linkler bulunmalıdır.
23- Teklif edilecek program istendiğinde internette ön filtreleme yaparak sisteme gereksiz e-posta gelmesini önleyebilir özellikte olmalıdır. İnternette yapılacak ön filtreleme ayarları SMTP ağ geçidi üzerinden tanımlanmalıdır. Bu özellik isteğe bağlı olarak açılıp kapatılabilmelidir. Teklif edilecek program görünen dosya uzantısından bağımsız olarak gerçek dosya tipini algılayarak silme, karantinaya alma, değiştirme gibi aksiyonlar alabilmelidir.
24- Teklif edilecek program üzerinde şifre korumalı taranamayan ekler için özel politika tanımlanabilmelidir.
25- Teklif edilecek program şifre korumalı sıkıştırılmış ZIP dosyalarının içindeki dosyaları algılayarak bu dosyalar için isim ve uzantıya göre bloklama politikası uygulayabilmelidir. Teklif edilecek program, sıkıştırılmış dosyalarda (ZIP, ARJ, LZH, RAR,TAR, CAB,TD0,7Z, BZ2, VBX) zararlı denetimi yapabilecektir.
26- Teklif edilecek program, kendi üzerinde bulunan olay kayıtlarını syslog entegrasyonu ile birden çok kaynağa iletebilmelidir.
27- Teklif edilecek program, sıkıştırılmış dosyalarda birden fazla iç içe katman olarak sıkıştırılmış dosyaları açabilecek ve denetim yapabilecektir.
28- Teklif edilecek program, mail bombardımanlarını algılayıp engelleme yapabilecektir.
29- Teklif edilecek program, göndericinin mail adresi ya da IP adresine göre izin verilen ya da engellenen liste kurallarını uygulayabilmelidir.
30- Teklif edilecek program, e-posta başlığına, içeriğine ve eklentisine göre filtre tanımlanmasına imkan tanımalıdır.
31- Teklif edilecek program, anti-spoofing özelliği barındırmalıdır.
32- Teklif edilecek program, kelime tabanlı gövde filtreleme (body filter) desteği olmalıdır.
33- Teklif edilecek program, anahtar sözcük bazında e-postanın ekinin içeriği kontrol edilebilmelidir.
34- Teklif edilecek program, e-posta içindeki kötü niyetli URL'lere karsı koruma sağlamalıdır.

35- Teklif edilecek program, e-posta eklerini spam ve virüs içeriğe karşı kontrol edebilmelidir.
36- Teklif edilecek program, spam olarak tespit edilen e-postaları silebilmeli, başka bir adrese gönderebilmeli, karantinada tutabilmeli, konu kısmına, e-posta bölümüne özel bir mesaj ekleyebilmelidir.
37- Teklif edilecek program, belirli bir ip adresinden gelen bağlantı sayısı önceden tanımlanmış maksimum bağlantı değerini aştığında, kaynak ip adresini bloklamayı desteklemelidir.
38- Teklif edilecek program, belirli bir e-posta adresinden gelen eposta sayısı önceden tanımlanmış maksimum eposta değerini aştığında, kaynak eposta adresini bloklamayı desteklemelidir.
39- Teklif edilecek program, Gelişmiş Saldırılar için Detaylı Analiz Sistemi ile entegre olabilecek, gelen e-postaları analiz amacı ile bu sisteme iletebilecektir.
40- Teklif edilecek program, Gelişmiş Saldırılar için harici bir Detaylı Analiz Sistemi ile entegrasyonu ile zararlı içerik bulunduran e-postaları Detaylı Analiz Sistemi bulgularına uygun şekilde karantinaya alabilecektir.
41- Teklif edilecek program, Kullanıcı ve Alan Adı Bazında Giden E-posta Limiti sağlayabilmelidir.
42- Teklif edilecek E-Posta Güvenlik Çözümü 900 kullanıcı mailbox ve 50 distribution grup dahil olacak şekilde hesaplanarak 1 ve 3 yıl olarak lisanslanmalıdır.
43- Teklif veren firma teklif edilen programı, yerinde ve kurumun istediği şekilde kurup yapılandırarak personele yerinde eğitim verecektir.