CONSILIUL JUDEŢEAN TIMIŞ
Direcţia Buget-Finanţe, Informatizare
Compartimentul Informatică
Nr. 21689 data: 10.10.2019

CAIET DE SARCINI

Pentru achiziţia unei aplicaţii software de securitate e-mail server pentru 200 de utilizatori cu licenţă pentru 3 ani

I. Obiectul achiziţiei

Achiziţia unei aplicaţii de securitate e-mail server pentru 200 de utilizatori cu licenţă pentru 3 ani.

Este necesară achiziţia unei soluţii informatice de antispam şi filtrare e-mail, detecţie şi blocare antimalware care va fi instalată pe serverul de e-mail şi va asigura protecţia e-mail-urilor pentru un număr de 200 de utilizatori din cadrul sistemului informatic al Consiliului Judeţean Timiş.

1. Caracteristici tehnice minimale pentru – Aplicaţie de securitate e-mai server pentru 200 de utilizatori cu licenţă pentru 3 ani

Nr. Crt.	Specificaţii tehnice impuse prin caietul de sarcini
1.1	Parametrii tehnici şi funcţionali ***Aplicaţie de securitate e-mail server pentru 200 de utilizatori cu licenţă pentru 3 ani***
1.2	Specificaţii de performanţă şi conditii privind siguranţa în exploatare Soluţie dedicată filtrării SPAM, inspecţiei preliminare a conţinutului şi catalogării automate a mesajelor e-mail primite. Topologia logică a sistemului de comunicaţie securizată trebuie să permită instalarea în mod releu, prin care se captează, filtrează şi livrează mesajele către utilizatori. Soluţia va fi instalată în cadrul instituţiei în mediu virtual (ca maşină virtuală), cu specificaţiile descrise mai jos: ➢ **Filtrare mesagerie:** ▪ Solutia impreuna cu aplicatiile sale va avea rol de proxy ce va intercepta mesajele e-mail ale utilizatorilor, va aplica functiile de securitate necesare si va retrimite mesajul catre destinatar, atat timp cat mesajul inspectat nu incalca politicile de securitate. Daca mesajul incalca politicile de securitate, acesta va fi blocat, trecut in carantina si se va putea notifica destinatarul si administratorul de sistem. ➢ **Protecţie împotriva conţinutului rău intenţionat:** ▪ Solutia impreuna cu aplicatiile sale, trebuie sa detina capabilitatea de identificare a atacurilor de tip spoofing si phishing. Se cere sa suporte minim functiile DKIM, SPF si DMARK. Deasemenea se cere capabilitatea de limitare a traficului detectat rau intentionat pentru a nu produce suprasolicitarea Solutiei si a-i permite autoprotejarea. ➢ **Protecţie prin motoare de scanare multivendor:** ▪ Solutia impreuna cu aplicatiile sale va permite instalarea de semnaturi sau de motoare de detectie ale altor vendori, alaturi de semnaturile sau motoarele proprii de scanare, pentru

protectia impotriva mesajelor cu continut rau intentionat sau atasamente infectate. Metodele de scanare anti-phising trebuie sa indeplinesca cel putin functiile de comparatie prin semnaturi, analiza heuristica si reputatie a expeditorului.

- **Suport pentru mesaje semnate:**
  - Solutia impreuna cu aplicatiile sale va permite implementarea serviciilor de securitate, cum sunt descrise in extensiile S/MIME.
- **Protecție Antivirus și Malware:**
  - Solutia va detine capabilitatea de detectie a fisierelor in transit peste protocoalele aflate sub inspectie si va avea capabilitatea de blocare a fisierelor cunoscute ca fiind malitioase. Actualizarea dinamica si constanta a bazei de date cu fisiere malitioase intra in responsabilitatea furnizorului de produs; Pentru protejarea informatiilor cu caracter personal, ce pot face parte din continutul fisierelor, se cere ca Solutia sa verifice starea fisierelor folosind mecanisme de amprentare si anonimizare a acestora prin metode de hashing, spre exemplu SHA256;
- **Protecție multi protocol:**
  - Solutia va permite functionarea in mod stiva IP singulara, doar IPv4, doar IPv6 sau in mod stiva concomitenta IPv4 si IPv6; Toate functionalitatile de mai sus, se aplica la oricare din starile de functionare ale Solutiei, stiva singulara sau stiva concomitenta.
- **Criptarea transmisiilor:**
  - Pentru mentinerea integritatii mesajelor intre expeditor si destinatar se cere ca Solutia sa poata folosi protocolul TLS peste protocolul standard SMTP (secure SMTP over TLS sau STARTTLS)
- **Protecție AntiSPAM:**
  - Solutia va avea capabilitati de detectie antiSPAM cu cel putin un motor de analiza care sa poata asocia mesaje rau intentionate prin analiza imaginilor atasate, sau a reputatiei URL-urilor din continut.
- **Integrare cu ActiveDirectory:**
  - Solutia se va integra si va putea folosi baza de date de utilizatori ce exista in sistemul ActiveDirectory, va avea capabilitati de interoperabilitate prin LDAP sau folosind un alt server SMTP pentru functia de autentificare prin functii SMTP Auth.
- **Raportare centralizată:**
  - Solutia va functiona in mod autonom, sau in mod administrat, in functie de configurarea acestuia. Raportarea se va putea face in mod autonom sau in mod agregat, de la mai multe echipamente proxy catre un singur sistem de administrare.
- **Licențiere:**
  - Licentierea va include initial un minim de 200 casute e-mail pentru o perioadă de 3 ani, pentru functionalitatile specificate mai sus.
- **Funcționalități disponibile opțional:**
  - La cerere, in cadrul Solutiei se va putea implementa ulterior functia de Data Loss Prevention, prin care beneficiarul va urmari cuvinte cheie, documente importante, informatii customizabile pe care doreste sa le trateze in mod particular si nu trebuie sa paraseasca institutia.

	➢ **Servicii instalare si configurare:** ▪ Instalare masina virtuala ▪ Configurare si redirectare trafic e-mail prin noua solutie ▪ Activare filtre ▪ Populare lista exceptii conform cerintelor beneficiarului ▪ Testare solutie antispam ▪ Realizare si prezentare documentatie de proiect: diagrama, conectivitate, planuri adresare, credentiale acces Licențele vor fi individualizate printr-o cheie de activare/serial number unic; Aplicația va beneficia de servicii de actualizare semnături, actualizare versiune aplicație și suport tehnic de la producător pentru o perioadă de 3 ani; **Certificari necesare:** ▪ Minim 2 specialiști certificați de producător
1.3	**Conditii privind conformitatea cu standardele relevante:** Standard de calitate ISO 9001, (sau echivalent) pentru producator
1.4	**Condiţii de livrare:** Aplicația software și licențele aferente vor fi livrate electronic. Aplicația de securitate e-mail server pentru 200 de utilizatori va fi în format „Virtual Appliance" compatibilă cu platforma VMware aflată în funcțiune în rețeua informatică a Consiliului Județean Timiș;

Alte cerinţe:

- Furnizorul trebuie să depună certificările solicitate prin caietul de sarcini pentru aplicația software ofertată;
- Caracteristicile tehnice specificate în caietul de sarcini vor fi minime şi obligatorii;

Garanţia de bună execuţie a contractului.

Furnizorul are obligaţia constituirii garanţiei de bună execuţie a contractului, în favoarea beneficiarului, în cuantum de 10% din valoarea fără T.V.A. a acestuia.

Garanția de bună execuție se constituie prin virament bancar sau printr-un instrument de garantare emis în condițiile legii de o societate bancară sau de o societate de asigurări, în termen de max. 5 zile de la data semnării contractului, înainte de începerea furnizării și instalării aplicației software de securitate e-mail server pentru 200 de utilizatori cu licență pentru 3 ani.

Achizitorul se obligă să restituie garanția de bună execuție, în termen de maxim 14 (patrusprezece) zile de la data întocmirii procesului verbal de recepție, dacă nu a ridicat până la acea dată, pretenții asupra ei.

Pentru Director Executiv,
Direcţia Buget Finanţe, Informatizare

Şef Serviciu Financiar-Contabilitate
Ioana PĂDUREANU

Compartiment Informatică

Viorel IEȘAN – Consilier Superior