29883/ 24.09.2020

CAIETUL DE SARCINI

pentru achiziţia:

Licenta antivirus in mediul fizic/virtual + licenta antivirus pentru solutia de e-mail

INTRODUCERE

Caietul de sarcini conţine indicaţii privind regulile de bază care trebuie respectate astfel încât potenţialii ofertanţi să elaboreze propunerea tehnică corespunzător cu necesităţile autorităţii contractante.

SCURTĂ DESCRIERE, context si beneficii:

Impactul infectării cu viruși afectează eficiența operațională a companiei și poate duce la scăderea productivității în rândul angajaților. Această pierdere de productivitate poate afecta grav compania, împiedicând functionarea si creșterea acesteia. Răspunsul la scurgerile de informații și pierderile de productivitate este protecția proactivă împotriva programelor dăunătoare.
Romgaz are nevoie de o solutie care sa poata proteja în mod eficient posta electronica (e-mail), stațiile de lucru ale clienților și serverele importante, împotriva atacurilor, de a asigura respectarea politicilor de securitate ale companiei și de a le administra, utilizând cât mai puține resurse IT.

Datorita faptului ca Licenta de antivirus in mediul fizic/virtual expira pe data de 20.11.2020 iar Licenta antivirus pentru solutia de email expira pe data de 01.12.2020, este necesara reinnoirea acestora pentru a se asigura continuitate in actualizarea antivirusului.

Actualizarea antivirusului este destinata desfasurarii în bune condiţii a activităţilor specifice din cadrul SNGN ROMGAZ SA.

Cerinţele din caietul de sarcini vor fi considerate ca fiind minimale si obligatorii.

Locatia unde se va face livrarea (adrese/persoane) de contact:

- Sediul Romgaz: Str. Constantin Motas, nr. 4, Mediaş. Iosif FAZAKAS: 0749331297

Documentele care insotesc livrarea

- certificat de calitate,
- certificat de garantie - trebuie sa acopere intreaga perioada pentru care sunt activate licentele;
- declaratie de conformitate.
- Certificat de licentiere.
- Proces verbal de predare/primire si activare licente semnat de ambele parti.

Receptia

- Se va face in baza certificatului de licentiere transmis beneficiarului si va fi consemată în proces verbal de predare/primire si activare licente si servicii aferente licentelor, semnate de ambele părţi

Plata

- Se va face pe baza procesului verbal de predare/primire si activare licente si servicii aferente licentelor.

Cerinte privind oferta tehnica:

- Oferta tehnica va contine obligatoriu fiecare specificatie tehnica ceruta cu confirmarea / neconfirmarea indeplinirii cerintei.
- Ofertantul isi asuma intreaga responsibilitate a conformitatii cerintelor tehnice obligatorii cerute cu cele ofertate.
- Preţurile unitare de achiziţie prevăzute în ofertă, au caracter ferm şi nu se modifică pe durata valabilităţii contractului.

Cantitatile necesare

Achizitia se realizeaza pentru "GravityZone Enterprise Security" (pentru 2200 clienti, servere, statii fizice sau virtuale).

CANTITATILE NECESARE

Tabelul 1.

POZ PAS 2020	CodCPV	Denumire	Cantitate	Valoare (Lei)
811.1	48760000-3	Licenta antivirus in mediul fizic/virtual + Licenta antivirus pentru solutia de e-mail	1	134000

SPECIFICATII TEHNICE antivirus in mediul fizic/virtual (poz 811.1)

1. Caracteristici generale minimale si eliminatorii:

1. Pentru reducerea la minim a consumului de resurse, solutia antimalware trebuie sa permita instalarea personalizata a modulelor detinute (de exemplu, sa permita instalarea solutiei antimalware fara modulul de control al accesului web, modul de control al dispozitivilelor sau modulul firewall).
2. Pentru o mai buna protectie a statiilor si serverelor, solutia include un vaccin anti-ransomware. Acest vaccin asigura protectia impotriva tuturor amenintarilor cunoscute de tip ransomware, prin imunizarea statiilor si serverelor, chiar daca sunt infectate si prin blocarea procesului de criptare.
3. Vaccinul anti-ransomware primeste actualizari de la producator, odata cu actualizarea semnaturilor produsului Antimalware.
4. Pentru o mai buna protectie a statiilor si serverelor, solutia include protectie impotriva atacurilor zero-day de tip exploit (atacuri directionate).
5. Pentru o mai buna protectie a statiilor si serverelor, solutia include un modul avansat de securitate, proiectat special pentru a detecta atacuri avansate si activitati suspecte in faza pre-executie.
6. Acest modul avansat de securitate va proteja impotriva: atacurilor directionate (Targeted Attack - APT), fisierelor suspecte si traficului la nivel de retea suspect, exploit-urilor, ransomware si grayware. Fiecarui tip de amenintare mentionat, i se vor putea stabili, independent, un nivel de protectie dorit: permisiv, normal, agresiv.
7. Modulul avansat de securitate are posibilitate doar de raportare sau si blocare. Astfel, administratorul va putea decide daca doreste intai monitorizare sau doreste si blocarea amenintarilor. Aceste doua actiuni mentionate, vor putea fi stabilite independent, pentru fisiere sau pentru traficul din retea, cu posibilitatea extinderii nivelului de raportare pentru a include nivelurile superioare (vor putea fi raportate amenintarile care ar fi fost detectate daca nivelul de protectie era stabilit mai agresiv).
8. Pentru o mai buna protectie a statiilor si serverelor, solutia include si un sandbox in cloud-ul producatorului, unul local fiind foarte mare consumator de resurse.
9. Modulul de Sandbox va putea trimite automat fisiere in Sandbox-ul din cloud-ul producatorului unde vor putea fi „detonate" pentru o analiza in profunzime.
10. Modulul de Sandbox include doua variante de analiza: doar monitorizare sau blocare. In modul monitorizare utilizatorul va putea accesa fisierul dorit, pe cand in modul blocare, utilizatorului i se va bloca rularea fisierului pana cand Sandbox-ul din cloud-ul producatorului va da verdictul.
11. Modulul de Sandbox include doua tipuri de actiuni remediere: implicita si de siguranta. Pentru actiunea implicita se va putea stabili: doar raportare, dezinfectie, stergere si carantinare. Pentru actiunea de siguranta se va putea stabili: stergere sau carantinare.
12. Modulul de Sandbox include si posibilitatea de trimitere manuala a fisierelor in Sandbox-ul din cloud-ul producatorului. Astfel, daca administratorul suspecteaza un fisier ca fiind malitios, il poate trimite manual in Sandbox pentru a fi „detonat" si a afla verdictul. Va putea trimite mai multe fisiere de odata, cu posibilitate de a specifica daca vor fi „detonate" individual sau toate in acelasi timp.

13. Modulul de Sandbox poate suporta „detonarea" urmatoarelor tipuri de fisiere: Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (executable), PDF, PEF (executable), PIF (executable), RTF, SCR, URL (binary), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.
14. Fisierele mentionate anterior, vor putea fi detectate corect chiar daca sunt incluse in arhive de tipul: : 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ.

2. Cerinte de sistem:

- Sisteme de operare pentru statii de lucru: Windows 10, Windows 8, Windows 7, Windows Vista (SP1), Windows XP (SP3), Mac OS X Sierra (10.12.x), Mac OS X El Capitan (10.11.x), Mac OS X Yosemite (10.10.5), Mac OS X Mavericks (10.9.5), Mac OS X Mountain Lion (10.8.5)
- Sisteme de operare embedded: Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded Standard 7, Windows Embedded POSReady 7, Windows Embedded Enterprise 7, Windows Embedded POSReady 2009, Windows Embedded Standard 2009, Windows XP Embedded with Service Pack 2, Windows XP Tablet PC Edition
- Sisteme de operare pentru servere: Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Small Business Server (SBS) 2008, Windows Server 2008 R2, Windows Server 2008, Windows Small Business Server (SBS) 2003, Windows Server 2003 R2, Windows Server 2003 with Service Pack 1, Windows Home Server
- Sisteme de operare Linux: Red Hat Enterprise Linux / CentOS 5.6 sau mai recent, Ubuntu 10.04 LTS sau mai recent, SUSE Linux Enterprise Server 11 sau mai recent, OpenSUSE 11 sau mai recent, Fedora 15 sau mai actual and Debian 5.0 sau mai recent.
- Sisteme de operare MAC: Mac OS X El Capitan (10.11.x), Mac OS X Yosemite (10.10.5), Mac OS X Mavericks (10.9.5), Mac OS X Mountain Lion (10.8.5)

3. Administrare si instalare remote:

1. Inainte de instalare, administratorul va putea particulariza pachetele de instalare cu modulele dorite: firewall, content control, device control, power user.
2. Instalarea se va putea face in mai multe moduri:
    a. prin descarcarea directa a pachetului pe statia pe care se va face instalarea;
    b. prin instalarea la distanta, direct din consola de management
3. Instalarea clientilor la distanta in alte locatii decat cele in care este instalata consola de management se va face prin intermediul unui alt client antivirus existent in locatiile respective pentru a minimiza traficul in WAN.
4. In consola vor fi disponibile informatii despre fiecare statie: numele statiei, IP, sistem de operare, module instalate, politica aplicata, informatii despre actualizari etc.
5. Din consola se va putea trimite o singura politica pentru configurarea integrala a clientului de pe statii/servere.
6. Consola va include o sectiune, „Audit", unde se vor mentiona toate actiunile intreprinse fie de administratori fie de reporteri, cu informatii detaliate: logare, editare, creare, delogare, mutare etc.
7. Posibilitatea creari unui singur pachet de instalare, utilizabil atat pentru sistemele de operare pe 32 de biti cat si pentru cele pe 64 de biti.
8. Posibilitatea creari unui singur pachet de instalare, utilizabil pentru statii (fizice si/sau virtuale), servere (fizice si/sau virtuale), exchange.
9. Posibilitatea de a crea pachetele de instalare de tip web installer sau kit full.
10. Administratorul va putea crea grupuri sau chiar subgrupuri, unde va putea muta statiile/serverele din retea pentru cele care nu sunt integrate domeniu.
11. Permite selectarea clientului care va realiza descoperirea statiilor din retea, altele decat cele integrate in domeniu.

4. Caracteristici si functionalitati principale ale modulului antimalware:

1. Solutia permite administratorului sa stabileasca actiunea luata de produsul Antimalware la detectarea unei amenintari noi. Astfel administratorul va putea alege intre urmatoarele actiuni:
    a. Actiune imiplicita pentru fisiere infectate:

- interzice accesul
- dezinfecteaza
- stergere
- muta fisierele in carantina
- nicio actiune

b. Actiune alternativa pentru fisierele infectate:
   - interzice accesul
   - dezinfecteaza
   - stergere
   - muta fisierele in carantina

c. Actiune imiplicita pentru fisierele suspecte:
   - interzice accesul
   - stergere
   - muta fisierele in carantina
   - nicio actiune

d. Actiune alternativa pentru fisierele suspecte:
   - interzice accesul
   - stergere
   - muta fisierele in carantina

2. Scanarea automata in timp real va putea fi setata sa nu scaneze arhive sau fisiere mai mari de « x » MB, marimea fisierelor putand fi definita de administratorul solutiei,
3. Definirea pana la 16 nivele de profunzime pentru scanarea in arhive.
4. Scanarea euristica comportamentala prin simularea unui calculator virtual in interiorul caruia sunt rulate aplicatii cu potential periculos protejand sistemul de virusii necunoscuti prin detectarea codurilor periculoase a caror semnatura nu a fost lansata inca.
5. Scanarea oricarui suport de stocare a informatiei (CD-uri, harduri externe, unitati partajate etc). De asemenea, se va putea anula scanarea in cazul in care sunt detectate unitati care au informatii stocate mai mult de « x » MB.
6. Scanarea automata a emailurilor la nivelul statiei de lucru pentru POP3/SMTP.
7. Configurarea cailor ce urmeaza a fi scanate la cerere.
8. Clientii antimalware pentru workstation sa permita definirea unor liste de excludere de la scanarea in timp real si la cerere a anumitor directoare, discuri, fisiere, extensii sau procese.
9. Cu ajutorul unei baze de date complete cu semnaturi de spyware si a euristicii de detectie a acestui tip de programe, produsul va trebui sa ofere protectie anti-spyware.
10. Posibilitatea de configura scanarile programate sa se execute cu prioritate redusa
11. Produsul antimalware poate fi configurat sa foloseasca scanarea in cloud, si partial scanarea locala. Pentru statiile ce nu au suficiente resurse hardware, scanarea se poate face cu o masina de scanare instalata in retea.
12. Administratorul poate personaliza și motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare:
    - Scanare locală, când scanarea se efectuează pe stația de lucru locală. Modul de scanare locală este potrivit pentru mașinile puternice, având toate semnăturile și motoarele stocate local.
    - Scanarea hibrid cu motoare light (Cloud public), cu o amprentă medie, folosind scanarea în cloud și, parțial, semnături locale. Acest mod de scanare oferă avantajul unui consum mai bun de resurse, fără să implice scanarea locală.
    - Scanarea centralizată în Cloud-ul privat, cu o amprentă redusă, necesitând un server de securitate pentru scanare. În acest caz, nu se stochează local nicio semnătură, iar scanarea este transferată către serverul de securitate.
    - Scanare centralizată (Scanare în cloud privat cu server de securitate) cu fallback* pe Scanare locală (motoare full)
    - Scanare centralizată (Scanare în cloud privat cu server de securitate) cu fallback* pe Scanare hibrid (cloud public cu motoare light)
13. Pentru o protectie sporita, solutia antimalware trebuie sa aiba 3 tipuri de detectie: bazata pe semnaturi, bazata de comportamentul fisierelor si bazata pe monitorizarea proceselor.
14. Pentru o protectie sporita, solutia antimalware trebuie sa poata scana paginile HTTP.
15. Pentru o mai buna gestionare a antimalware instalat pe statii, produsul va include optiunea de setare a unei parole pentru protectia la dezinstalare.
16. Pentru siguranta utilizatorului, clientul va include un modul de antiphishing.

17. Solutia ofera protectie in timp real pe masinile cu sistem de operare Linux in conformitate cu versiunea de kernel instalata.
18. Pe masinile virtuale parte a unui pool instalarea clientului antimalware se face doar pe masina de tip template, dupa care se recompune pool-ul de masini virtuale.

5. Firewall:

1. Posibilitatea de a configura reguli de firewall pentru aplicatii sau conectivitate.
2. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului.
3. Posibilitatea de a defini retele de incredere pentru masina destinatie.

6. Carantina:

1. Produsul antimalware sa permita trimiterea automata a fisierelor din carantina catre laboratoarele antimalware ale producatorului.
2. Trimiterea continutului carantinei va putea fi expediat in mod automat, la un interval definit de administrator.
3. Produsul antimalware sa permita stergerea automata a fisierelor carantinate mai vechi de o anumita perioada, pentru a nu incarca inutil spatiul de stocare.
4. Posibilitatea de a restaura un fisier din carantina in locatia lui originala.
5. Modulul de carantina va permite rescanarea obiectelor dupa fiecare actualizare de semnaturi.

7. Protectia datelor:

1. Produsul permite blocarea datelor confidentiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice.

8. Controlul continutului:

1. Consola va avea integrat un modul dedicat controlului accesului la Internet cu urmatoarele particularitati:
   a. Permite blocarea accesului la Internet pentru anumite masini client sau grupuri de masini.
   b. Permite blocarea accesului la Internet pe intervale orare.
   c. Permite blocarea paginilor de internet care contin anumite cuvinte cheie.
   d. Permite controlul accesului numai la anumite pagini de internet specificate de administrator;
   e. Permite blocarea accesului la anumite aplicatii definite de administrator;
   f. Permite restrictionarea accesului pe anumite pagini de internet dupa anumite categorii prestabilite (ex: online dating, violenta, pornografie etc).

9. Controlul aplicatiilor:

1. Pentru o mai buna inventariere si administrare, solutia va include o sectiune in consola de administrare unde se vor regasi toate aplicatiile descoperite in retea, grupate dupa: nume, versiune, descoperit la, gasit pe.
2. Pentru o mai buna inventariere si administrare, solutia va include o sectiune in consola de administrare unde se vor regasi toate procesele negrupate descoperite in retea, grupate dupa: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, gasit pe.
3. Pentru prevenirea infectarii statiilor si serverelor dar si pentru a permite aplicatiilor descoperite in retea sa se poata actualiza, solutia permite definirea unor programe de actualizare (Updater) care vor fi lasate sa actualizeze diferite aplicatii instalate pe statii sau servere.
4. Solutia include optiunea de a permite sau a bloca rularea anumitor aplicatii sau procese definite de administrator (inclusiv subprocese) dupa:
   a. Cale fisier: local, CD-ROM, portabil sau retea
   b. Hash
   c. Certificat

10. Controlul dispozitivelor:

1. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului.
2. Modulul va permite controlul urmatoarelor tipuri de dispozitive:
   a. Bluetooth Devices
   b. CDROM Devices
   c. Floppy Disk Drives

d. Security Policies 153
e. IEEE 1284.4
f. IEEE 1394
g. Imaging Devices
h. Modems
i. Tape Drives
j. Windows Portable
k. COM/LPT Ports
l. SCSI Raid
m. Printers
n. Network Adapters
o. Wireless Network Adapters
p. Internal and External Storage

3. Modulul va permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la masina client.
4. Modulul va permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli.

10. Power User:

1. Modulul poate fi instalat / dezinstalat in functie de preferinta administratorului.
2. Modulul permite posibilitatea de a acorda utilizatorilor drepturi de Power User. Utilizatorii vor putea accesa si modifica setarile clientului antimalware dintr-o consola dispobibila local pe masina client.
3. Administratorul va putea suprascrie din consola setarile aplicate de utilizatorii Power User.

11. Actualizare:

1. Posibilitatea efectuarii actualizarii la nivel de statie in mod silentios (fara avertizare).
2. Sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate).
3. Actualizarea pentru locatiile remote prin intermediul unui client antimalware care are si rol de server de actualizare.

Durata contractului: 1 an (de la 21.11.2020 pana la 20.11.2021)

Data de activare licente si servicii aferente: 21.11.2020

SPECIFICATII TEHNICE antivirus solutia de e-mail (poz 811.1)

Achizitia se va face pe baza cerintelor minime de mai jos:

1. Produsul va oferi protectie antimalware, antispam (inclusiv antiphishing), precum si filtrare de atasamente si continut, prin integrarea cu serverul Microsoft Exchange. De asemenea, va permite scanarea antimalware la cerere a bazelor de date Exchange.
2. Produsul va asigura scanarea atasamentelor si a continutului mesajelor in timp real, fara a afecta vizibil performanta serverului de mail.
3. Actualizarea antimalware trebuie sa poata fi facuta automat la un interval de maxim 1 ora, precum si la cerere.
4. In afara de detectia pe baza de semnaturi, modulul de protectie antimalware va trebui sa includa si scanare euristica comportamentala, prin simularea unui calculator virtual in interiorul caruia sunt rulate si analizate aplicatii cu potential periculos, pentru a proteja sistemul de virusii necunoscuti prin detectarea codurilor periculoase a caror semnatura nu a fost lansata inca.

5. Produsul va oferi optiuni multiple de actiune la identificarea unui atasament virusat (dezinfectare, stergere, mutare in carantina).
6. Cu ajutorul unei baze de date complete cu semnaturi de spyware si a euristicii de detectie a acestui tip de programe, produsul va oferi protectie anti-spyware pentru a preveni furtul de date confidentiale.
7. Produsul va oferi protectie antispam, cu o baza de semnaturi actualizabila prin internet.
8. Modulul antispam va trebui sa includa un filtru URL cu o baza de adrese URL cunoscute a fi folosite in mesaje spam, precum si un filtru de caractere pentru detectarea automata a mesajelor scrise cu caractere chirilice sau asiatice.
9. Produsul va trebui sa ofere filtru RBL care sa identifice spam-ul prin sincronizarea cu anumite baze de date online care contin liste de servere de mail cunoscute ca fiind la originea acestui tip de mesaje.
10. Produsul va trebui sa ofere un serviciu / filtru online pentru imbunatatirea protectiei impotriva valurilor de spam nou aparute.
11. Produsul va oferi posibilitatea de a defini politici de filtrare antimalware, antispam, a continutului sau atasamentelor pentru diferite grupuri sau utilizatori.
12. Actualizarea produsului va fi configurabila si se va putea realiza de pe internet, direct sau printr-un proxy, sau din cadrul retelei de pe un server de actualizare propriu.
13. Produsul va trebui sa ofere statistici atat referitoare la scanarea antivirus cat si la scana antispam.
14. Produsul se va integra in cadrul consolei de management unitar al solutiei antivirus. Pentru usurinta accesului la setarile produsului din diferite medii de operare, produsul va avea consola de administrare web.

Durata contractului: 1 an (01.12.2020 → 01.12.2021)

Data de activare licente si servicii aferente: 01.12.2020

Cerinţe de protecţia mediului

1. **Documente obligatorii în faza de adjudecare** .
   - Nu este cazul

2. **Documente obligatorii a fi prezentate ulterior declarării câştigătorului şi cu minim 4 zile înainte de data semnării contractului**
   - Nu este cazul

3. **Cerinţe de protecţia mediului asociate aspectelor de mediu potenţiale**
   - Nu este cazul

Director T.I.
Adrian BOIARCIUC
.....

Sef Birou T.B.D.
Stefan STOICOVICI
.....

Intocmit
Iosif FAZAKAS
.....