2389 / 10.02.2017

CAIET DE SARCINI

Servicii de furnizare abonament software antivirus

1. Prezentare generală

Prezentul caiet de sarcini cuprinde datele necesare prezentării ofertei şi efectuării serviciilor prezentate în continuare, precum şi precizări privind condiţiile suplimentare, altele decât cele cuprinse în normele specifice în vigoare.

Datele prezentate sunt obligatorii pentru Prestator, dar nu exclud obligativitatea respectării prescripţiilor cuprinse în normativele republicane sau departamentale, standarde de stat.

În prezentul caiet de sarcini nu este specificată totalitatea prescripţiilor generale cuprinse în norme, dar a căror aplicativitate este obligatorie pentru beneficiar şi prestator.

Nu se vor efectua modificări ale prezentului Caiet de sarcini, după demararea procedurilor de achiziţie publică.

Caietul de sarcini face parte integrantă din documentaţia de atribuire şi constituie ansamblul cerinţelor pe baza cărora se elaborează de către fiecare ofertant propunerea tehnică.

Cerinţele impuse vor fi considerate ca fiind minimale. În acest sens orice ofertă prezentată, care se abate de la prevederile Caietului de sarcini, va fi luată în considerare, dar numai în măsura în care propunerea tehnică presupune asigurarea unui nivel calitativ superior cerinţelor minimale din Caietul de sarcini.

Ofertarea de servicii inferioare celor cerute prin Caietul de sarcini va atrage anularea ofertei.

2. Obiectul serviciilor

Serviciile de furnizare abonament software antivirus, din cadrul Universităţii de Vest constă în furnizarea unei soluţii antivirus pentru protecţia serverelor şi a calculatoarelor din patrimoniul UVT.

MR970/02.03.2017

B-dul Vasile Pârvan, Nr. 4, 300223 Timişoara, România
Tel.: +4 0256-592.305, E-mail: support@e-uvt.ro, **www.dict.uvt.ro**
DSICD

3. Cerințele tehnice minimale

Prestatorul va furniza serviciile solicitate pe o perioadă de **3 ani** cu următoarele caracteristici tehnice minimale, printr-o platformă integrată pentru managementul securității:

- protecție pentru minim 1100 stații de lucru (calculatoare desktop - soluție centralizată prin consolă de management, instalată la beneficiar);
- protecție pentru minim 100 stații de lucru mobile (laptopuri - pentru utilizatori individuali, cu funcții antispam, firewall, asistență parentală, antifurt, protecție MAC);
- protecție pentru minim 20 servere fizice;
- protecție pentru minim 50 mașini virtuale;
- protecție pentru minim 30 terminale thin client.
- protecție pentru minim 30 telefoane mobile de tip smartphone cu sistem de operare iOS sau Android.

Platforma antivirus va include:

- o consola de management ce va asigura funcționalități de administrare;
- protecție pentru stații și servere fizice și virtuale;
- protecție și securitate pentru telefoanele mobile de tip smartphone cu sistem de operare iOS sau Android.

3.1. Consola de management

3.1.1. Instalare si configurare

1. Pachetul de instalare va fi livrat ca o mașina virtuala bazată pe sistem de operare Linux securizat care va conține toate rolurile sau serviciile necesare. Consola nu va necesita o licență suplimentară pentru sistemul de operare. Imaginea de tip template se va putea importa în minim următoarele variante:
   a. VMware vSphere;
   b. Citrix XenServer;
   c. Microsoft Hyper-V;
   d. Red Hat Enterprise Virtualization;
   e. KVM;
   f. Oracle VM.
2. Consola de management se va livra cu o bază de date inclusă care va fi de tip non-relațională, pentru o funcționare cât mai rapidă, fără a fi nevoie de licențe adiționale.
3. Soluția va fi scalabilă, astfel ca oricare dintre roluri sau servicii vor putea fi instalate separat pe mai multe mașini virtuale sau pe aceeași mașină virtuală.
4. Mașinile de scanare pentru mediile virtuale VMware si Citrix se vor putea fi instalate de la distanță prin task din consola de management, iar pentru alte platforme se va putea descărca separat din interfața web a produsului.

B-dul Vasile Pârvan, Nr. 4, 300223 Timișoara, România
Tel.: +4 0256-592.305, E-mail: support@e-uvt.ro, **www.dict.uvt.ro**
DSICD

5. Rolurile principale vor trebui să fie cel puțin similare cu: Server cu bază de date, Server de comunicație, Server de actualizare, Server de Web.

6. Soluția va include și un modul de balansare (load balancer) pentru cazurile în care mai multe mașini virtuale ale componentei de management sunt instalate cu același rol (pentru Load Balancing și performanță/redundantă).

7. Soluția va include un mecanism de configurare a disponibilității pentru Serverul cu baze de date (clustering pentru redundanta). Astfel, baza de date se va putea instala de mai multe ori, pe mai multe mașini virtuale.

3.1.2. Cerințe generale pentru consola de management

1. Interfața consolei de management va fi în limba română.
2. Interfața clientului de securitate, care se instalează pe stații și servere, va fi în limba română.
3. Manualul de instalare a produsului va fi in limba romana.
4. Manualul de administrare a produsului va fi in limba romana.
5. Soluția va include un modul de update server prin care se asigura actualizarea de produs și a semnăturilor.
6. Soluția va permite activarea/dezactivarea actualizărilor de produs/semnături.
7. Soluția va permite stabilirea actualizării automate a consolei de management prin stabilirea recurenței zilnice, săptămânale sau lunare, dar și prin stabilirea intervalului orar în care acesta se va actualiza. De asemenea, va permite și trimiterea unei alerte de nefuncționalitate, cu minim 30 de minute înainte de actualizare.
8. Pentru o mai bună urmărire a actualizărilor consolei de management, soluția va permite vizualizarea unui jurnal de modificări în care vor fi precizate istoric:
   a. versiunea consolei de management;
   b. data versiunii;
   c. funcții noi și îmbunătățiri:
   d. probleme rezolvate;
   e. probleme cunoscute;
9. Soluția va permite integrarea cu un server Syslog pentru raportarea evenimentelor antimalware.
10. Soluția va permite instalarea serviciului de SMNP prin care se pot raporta statusul mașinilor din cadrul componentei de management.
11. Soluția va permite creare unei copii de siguranța a bazei de date a consolei de administrare, la cerere sau programată, putând fi stocată local, pe un server FTP sau în rețea.

3.1.3. Panou de monitorizare și raportare

1. Rapoartele din panoul de monitorizare vor putea fi configurate specificând numele raportului, tipul raportului, ținta raportului, opțiuni specifice pentru orice tip de raport (de

B-dul Vasile Pârvan, Nr. 4, 300223 Timişoara, România
Tel.: +4 0256-592.305, E-mail: support@e-uvt.ro, **www.dict.uvt.ro**
DSICD

exemplu pentru raportul de actualizare - care este intervalul după care o stație este considerată neactualizată).

2. Panoul central va conține rapoarte pentru toate modulele suportate.

3. Rapoartele din panoul central de comandă ce permit: adăugarea altor rapoarte, ștergerea lor și rearanjarea.

3.1.4. Inventarierea rețelei, managementul securității

1. Soluția se va integra cu domenii Active Directory multiple, VMware vCenter, Citrix Xen și va importa inventarul acestor platforme.
2. Pentru integrarea cu Active Directory, se va putea defini și intervalul (în ore) de sincronizare.
3. Va suporta și descoperirea mașinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM.
4. Va suporta și descoperirea stațiilor fizice neintegrate in Active Directory (Workgroup) cu ajutorul Network discovery.
5. Soluția va oferi opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare și adresa IP.
6. Soluția va permite instalarea la distanță sau manual a clientilor antimalware pe mașini fizice/virtuale.
7. Soluția va permite selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale.
8. Soluția va permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanta pentru clientul antimalware.
9. Soluția va oferi posibilitatea de repornire a mașinilor fizice de la distanță.
10. Soluția va oferi informații detaliate despre fiecare task și se afișează dacă task-ul s-a finalizat, sau nu, cu succes.
11. Soluția va permite configurarea centralizată a clienților antimalware prin intermediul politicilor.
12. Se vor oferi în consola de management informații detaliate ale obiectelor din consolă: Nume, IP, Sistem de operare, Grup, Politica atribuita, Ultimele actualizări, Versiunea produsului, Versiunea de semnături.
13. Soluția va permite descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea, prin rularea unui task din consola de administrare.

3.1.5. Politici

1. Soluția va permite configurarea setărilor clientului antimalware prin intermediul unei singure politici ce conține setări pentru toate modulele.

2. Politica va conține opțiuni specifice de activare/dezactivare și configurarea funcționalităților precum scanarea antimalware la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web,controlul dispozitivelor, power user.

B-dul Vasile Pârvan, Nr. 4, 300223 Timişoara, România
Tel.: +4 0256-592.305, E-mail: support@e-uvt.ro, **www.dict.uvt.ro**
DSICD

3. Soluția va permite aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resourse (VMware), domeniu, unități organizaționale sau useri de active directoy.
4. Politica sa poate fi schimbată automat în funcție de:
    a. User-ul logat pe stație
    b. IP sau clasa de IP al stației
    c. Gateway-ul alocat
    d. DNS serverul alocat
    e. Clientul este/nu este în aceeași rețea cu infrastructura de management
    f. Tipul rețelei (lan, wireless)

3.1.6. Rapoarte

1. Soluția va include un generator de rapoarte care oferă posibilitatea de a investiga o problemă de securitate pe baza mai multor criterii, menținând informațiile concise și ordonate corespunzător. Astfel, soluția include interogări precum: starea terminalului, evenimente terminal, evenimente Exchange.
2. Interogarea legată de starea terminalului va include informații precum:
    a. tip mașina
    b. infrastructura rețelei căreia îi aparține terminalul
    c. datele agentului de securitate
    d. starea modulelor de protecție
    e. rolurile terminalelor.
3. Interogarea legată de evenimente terminal va include informații precum:
    a. calculatorul țintă pe care a avut loc evenimentul
    b. tipul, starea și configurația agentului de securitate instalat
    c. starea modulelor și a rolurilor de protecție instalate pe agentul de securitate
    d. denumirea și alocarea politicii
    e. utilizatorul autentificat în timpul evenimentului
    f. evenimente (site-uri blocate, aplicații blocate, detecțiile etc)

3.1.7. Carantină

1. Soluția va permite restaurarea fișierelor carantinate în locația originală sau într-o cale configurabilă.
2. Carantina va fi locală, pe fiecare stația administrată și va fi administrată, fie local, fie din consola de management
3. Va permite descărcarea fișierelor carantinate doar pentru mașinile virtuale protejate prin modulul mediilor virtuale integrat cu VMware vShield.

3.1.8. Utilizatori

1. Administrarea se va putea face pe baza de roluri.

B-dul Vasile Pârvan, Nr. 4, 300223 Timişoara, România
Tel.: +4 0256-592.305, E-mail: support@e-uvt.ro, **www.dict.uvt.ro**
DSICD

2. Roluri multiple predefinite: Administrator companie, Administrator retea, Reporter sau rol personalizat.
    a. Administrator companie: administrează arhitectura consolei de management;
    b. Administrator rețea: administrează serviciile de securitate;
    c. Reporter: monitorizează și generează rapoarte.
3. Utilizatorii vor putea fi importați din Microsoft Active Directory sau creați în consola de management.
4. Se va permite configurarea detaliata a drepturilor administrative, permițând selectarea serviciilor și obiectelor pentru care un utilizator poate face modificări.
5. Se va permite deconectarea automată a oricărui tip de utilizator după un anumit timp, pentru o protecție sporită a datelor afișate în consola de administrare. Acest interval se va putea personaliza de administratorul soluției.

3.1.9. Log-uri

1. Înregistrarea acțiunilor utilizatorilor.
2. Se vor oferi informații detaliate pentru fiecare acțiune a unui utilizator.
3. Se va permite filtrarea acțiunilor utilizator după numele utilizatorului.

3.1.10. Actualizare

1. Soluția va dispune un server de actualizare (update) care face posibilă stabilirea componentelor ce vor fi descărcate automat de pe internet, fără intervenția administratorului. Astfel, administratorul va putea descărca pachetele pentru protecția stațiilor și a serverelor pe care rulează sistemul de operare Windows, Linux, Mac sau, poate descărca pachetele pentru modul de scanare centralizată în mediile de virtualizare VMware, Hyper-V sau Citrix.

2. În cadrul serverului de actualizare, pentru o mai buna urmărire a actualizărilor, pachetele pentru protecția stațiilor și a serverelor, sau a pachetelor pentru modul de scanare centralizată, se va putea vizualiza un jurnal de modificări în care sunt precizate istoric:
    a. versiunea pachetului
    b. data versiunii
    c. funcții noi și îmbunătățiri
    d. probleme rezolvate
    e. probleme cunoscute

3. Soluția va permite testarea noilor versiuni de pachete de instalare ale clientului antimalware, înainte de a fi instalate pe toate stațiile și serverele din rețea, evitând posibile probleme ce pot afecta serverele sau stațiile critice. Astfel, serverul de actualizare va include minim 2 tipuri de actualizări de produs:
    a. Ciclu rapid, gândit pentru un mediu de test în cadrul rețelei
    b. Ciclu lent, gândit pentru restul rețelei (producție, servere critice etc)

4. Soluția va permite stabilirea zonelor de test și critice din cadrul rețelei prin intermediul politicilor din consola de management.

B-dul Vasile Pârvan, Nr. 4, 300223 Timişoara, România
Tel.: +4 0256-592.305, E-mail: support@e-uvt.ro, **www.dict.uvt.ro**
DSICD

3.2. Protecția stațiilor și a serverelor fizice/virtuale

3.2.1. Caracteristici tehnice minimale

1. Pentru protecția stațiilor și a serverelor, soluția va include un vaccin anti-ransomware. Acest vaccin va asigura protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și a serverelor, chiar dacă sunt infectate și prin blocarea procesului de criptare.
2. Vaccinul anti-ransomware va primi actualizări de la producător, odată cu actualizarea semnăturilor produsului Antimalware.
3. Solutia va include protecție împotriva atacurilor zero-day de tip exploit (atacuri direcționate).

3.2.2. Caracteristici tehnice minimale

1. Posibilitatea creării unui singur pachet de instalare, utilizabil pentru stații (fizice și/sau virtuale), servere (fizice și/sau virtuale), exchange.

3.2.3. Caracteristici și funcționalități minimale pentru modulul antimalware

1. Soluția va permite administratorului să stabilească acțiunea luată de produsul Antimalware la detectarea unei amenințări noi, astfel ca administratorul să poată alege între următoarele acțiuni:
    a. Acțiune implicită pentru fișiere infectate:
        - interzice accesul
        - dezinfectează
        - ștergere
        - mută fișierele în carantină
        - nici o acțiune
    b. Acțiune alternativă pentru fișierele infectate:
        - interzice accesul
        - dezinfectează
        - ștergere
        - mută fișierele în carantină
    c. Acțiune implicită pentru fișierele suspecte:
        - interzice accesul
        - ștergere
        - mută fișierele în carantină
        - nici o acțiune

B-dul Vasile Pârvan, Nr. 4, 300223 Timișoara, România
Tel.: +4 0256-592.305, E-mail: support@e-uvt.ro, **www.dict.uvt.ro**
DSICD

d. Acțiune alternativă pentru fișierele suspecte:
   - interzice accesul
   - ștergere
   - mută fișierele în carantină

2. Definirea până la 16 nivele de profunzime pentru scanarea în arhive.
3. Produsul antimalware va putea fi configurat să folosească scanarea în cloud, și parțial scanarea locală. Pentru stațiile ce nu au suficiente resurse hardware, scanarea se va putea face cu o mașină de scanare instalată în rețea.
4. Administratorul va putea 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 nici o 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)

5. Soluția va oferi protecție în timp real pe mașinile cu sistem de operare Linux în
6. Pe mașinile virtuale parte a unui pool, instalarea clientului antimalware se va face doar pe mașina de tip template, după care se va recompune pool-ul de mașini virtuale.

3.2.4. Firewall

1. Posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate.
2. Modulul va putea fi instalat/dezinstalat în funcție de preferința administratorului.
3. Posibilitatea de a defini rețele de încredere pentru mașina destinație.

3.2.5. Carantina

1. Produsul antimalware va putea să permită trimiterea automată a fișierelor din carantină către laboratoarele antimalware ale producătorului.
2. Trimiterea conținutului carantinei va putea fi expediat în mod automat, la un interval definit de administrator.
3. Produsul antimalware va putea să permită ștergerea automată a fișierelor carantinate mai vechi de o anumită perioadă, pentru a nu încărca inutil spațiul de stocare.

B-dul Vasile Pârvan, Nr. 4, 300223 Timişoara, România
Tel.: +4 0256-592.305, E-mail: support@e-uvt.ro, **www.dict.uvt.ro**
DSICD

4. Posibilitatea de a restaura un fişier din carantină în locaţia lui originală.
5. Modulul de carantină va permite rescanarea obiectelor după fiecare actualizare de semnături.

3.2.6. Controlul aplicaţiilor

1. Pentru o mai bună inventariere şi administrare, soluţia va include o secţiune în consola de administrare unde se vor regăsi toate aplicaţiile descoperite în reţea, grupate după: nume, versiune, descoperit la, găsit pe, etc.
2. Pentru o mai bună inventariere şi administrare, soluţia va include o secţiune în consola de administrare unde se vor regăsi toate procesele negrupate descoperite în reţea, grupate după: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, găsit pe, etc.
3. Pentru prevenirea infectării staţiilor şi serverelor dar şi pentru a permite aplicaţiilor descoperite în reţea să se poată actualiza, soluţia va permite definirea unor programe de actualizare (Updater) care vor fi lăsate să actualizeze diferite aplicaţii instalate pe staţii sau servere.
4. Soluţia va include opţiunea de a permite sau a bloca rularea anumitor aplicaţii sau procese definite de administrator (inclusiv subprocese) după:
   a. Cale fişier: local, CD-ROM, portabil sau reţea
   b. Hash
   c. Certificat

4. Alte condiţii contractuale

În cazul în care soluţia propusă de prestator diferă de cea existentă la beneficiar, prestatorul va asigura în cadrul acestui contract, prin resurse proprii, fără costuri suplimentare, instalarea consolei de management pe un server virtual pus la dispoziţie de către beneficiar, respectiv instalarea produsului antivirus solicitat pe toate staţiile de lucru, servere fizice şi virtuale, menţionate în Capitolul 3.

Perioada de implementare de la data semnării contractului, va fi de maxim 5 zile lucrătoare.

Director IT
Dr. Marinel IORDAN

Şef birou adm. reţele IT
Dr. Ing. Robert SZABO

B-dul Vasile Pârvan, Nr. 4, 300223 Timişoara, România
Tel.: +4 0256-592.305, E-mail: support@e-uvt.ro, **www.dict.uvt.ro**
DSICD