24.10.2017

CAIET DE SARCINI

pentru achiziție Servicii de inchiriere licente software antivirus si antimalware la Biblioteca Universitatii Politehnica Timisoara

Obiectul prezentei proceduri de achiziție publică este reprezentat de achiziția de servicii de inchiriere licente software antivirus si antimalware la **Biblioteca Universitatii Politehnica Timișoara**, pentru o perioadă de 12 luni.

1. Serviciile care fac obiectul prezentei proceduri includ :

Servicii de inchiriere licente software antivirus si antimalware pentru protectia datelor de pe statiile de lucru, masinilor virtuale si a serverelor impotriva atacurilor informatice de tip virus si malware utilizand motoare de scanare distincte pentru diferite tipuri de fisiere si programe periculoase, verificarea obiectului scanat si eliminarea programului considerat periculos.

2. Caracteristici tehnice generale ale serviciilor :

Produsul este necesar a fi o platforma integrata pentru managementul securitatii, realizata ca solutie modulara. Produsul sa contina urmatoarele module:

- o consola de management care asigura functionalitati de administrare.
- protectie statii si servere fizice/virtuale.

3. Cerințe tehnice minimale generale, obligatorii :

3.1. Instalare si configurare:

1. Pachetul de instalare va fi livrat ca o masina virtuala bazata pe sistem de operare Linux securizat care contine toate rolurile sau serviciile necesare. Consola nu va necesita o licenta suplimentara pentru sistemul de operare. Imaginea de tip template se va putea importa in :
    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 livreaza cu o baza de date inclusa care este de tip non-relationala, pentru o functionare cat mai rapida, fara a fi nevoie de licente aditionale.
3. Solutia va fi scalabila, astfel ca oricare dintre roluri sau servicii pot fi instalate separat pe mai multe masini virtuale sau pe aceeasi masina virtuala.
4. Masinile de scanare pentru mediile virtuale VMware si Citrix se insteaza la distanta prin task din consola de management, iar pentru alte platforme se descarca separat din interfata web a produsului.
5. Rolurile principale trebuie sa fie cel putin similare cu: Server cu baza de date, Server de comunicatie, Server de actualizare, Server de Web.
6. Solutia va include aditional si un modul de balansare (load balancer) pentru cazurile in care mai multe masini virtuale ale componentei de management sunt instalate cu acelasi rol (pentru Load Balancing si performanta/redundanta).
7. Solutia va include un mecanism de configurare a disponibilitatii pentru Serverul cu baze de date (clustering pentru redundanta). Astfel, baza de date se va putea instala de mai multe ori, pe mai multe masini virtuale.

3.2. Cerinte generale:

1. Interfata consolei de management va fi in limba romana.
2. Interfata clientului de securitate, care se instaleaza pe statii si servere, va fi in limba romana.
3. Manualul de instalare a produsului va fi in limba romana.
4. Manualul de administrare a produsului va fi in limba romana.
5. Solutia va include un modul de update server prin care se asigura actualizarea de produs si a semnaturilor.
6. Solutia va pemite activarea/dezactivarea actualizarilor de produs/semnaturi.
7. Solutia permite stabilirea actualizarii automate a consolei de management prin stabilirea recurentei zilnice, saptamanale sau lunare, dar si prin stabilirea intervalului orar in care acesta se va actualiza. De asemenea, permite si trimiterea unei alerte de nefunctionalitate, cu 30 de minute inainte de actualizare.
8. Pentru o mai buna urmarire a actualizarilor consolei de management, solutia va permite vizualizarea unui jurnal de modificari in care sunt precizate istoric:
    a. versiunea consolei de management

b. data versiunii
c. functii noi si imbunatatiri
d. probleme rezolvate
e. probleme cunoscute

9. Notificarile – prezente in interfata, notificarile necitite sunt evidentiate, trimise catre una sau mai multe adrese de email, alerteaza administratorul in cazul unor probleme majore: licentiere, detectie virusi, actualizari de produs disponibile).
10. Solutia va permite integrarea cu un server Syslog pentru raportarea evenimentelor antimalware.
11. Solutia va permite instalarea serviciului de SMNP prin care se pot raporta statusul masinilor din cadrul componentei de management.
12. Solutia va permite crearea unei copii de siguranta a bazei de date a consolei de administrare, la cerere sau programata, putand fi stocata local, pe un server FTP sau in retea.

3.3 Panou de monitorizare si raportare (Dashboard):

1. Rapoartele din panoul de monitorizare vor putea fi configurate specificand numele raportului, tipul raportului, tinta raportului, optiuni specifice pentru orice tip de raport (de exemplu pentru raportul de actualizare - care este intervalul dupa care o statie este considerata neactualizata).
2. Panoul central contine rapoarte pentru toate modulele suportate.
3. Rapoartele din panoul central de comanda permit: adaugarea altor rapoarte, stergerea lor si rearanjarea.

3.4. Inventarierea retelei – managementul securitatii:

1. Solutia se va integra cu domenii Active Directory multiple, VMware vCenter, Citrix Xen si importa inventarul acestor platforme.
2. Pentru integrarea cu Active Directory, se va putea defini si intervalul (in ore) de sincronizare si forta sincronizarea.
3. Sa permita descoperirea masinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM.
4. Sa permita descoperirea statiilor statii fizice neintegrate in Active Directory (Workgroup) cu ajutorul Network discovery.
5. Solutia va oferi optiuni de cautare, sortare si filtrare dupa numele sistemului, sistem de operare si adresa IP.
6. Solutia sa permita instalarea la distanta sau manual a clientilor antimalware pe masini fizice/virtuale.

7. Solutia va permite selectarea modulelor componente atunci cand se creaza pachetul clientului care se instalează pe mașinile fizice/virtuale.
8. Solutia va permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanta pentru clientul antimalware.
9. Solutia va oferi posibilitatea de repornire a masinilor fizice de la distanta.
10. Solutia va oferi informatii detaliate despre fiecare task si se fiseaza daca task-ul s-a finalizat sau nu cu succes.
11. Solutia va permite configurarea centralizata a clientilor antimalware prin intermediul politicilor
12. Se vor oferi in consola de management informatii detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuita, Ultimele actualizare, Versiunea produsului, Versiunea de semnaturi.
13. Solutia permite descoperirea tuturor aplicatiilor instalate pe toate statiile si serverele din reatea, prin rularea unui task din consola de administrare.

3.5. Politici:

1. Solutia va permite configurarea setarilor clientului antimalware prin intermediul unei singure politici ce contine setari pentru toate module
2. Politica va contine optiuni specifice de activare/dezactivare si configurarea functionalitatilor precum scanarea antimalware la cerere, firewall, controlul accesului la Internet, controlul aplicatiilor, scanarea traficului web,controlul dispozitivelor, power user.
3. Solutia permite aplicarea politicilor pe masini client, grupuri de masini, pool-uri de resurse (VMware), domeniu, unitati organizationale sau useri de active directoy.
4. Politica sa poate fi schimbata automat in functie de:
   a. User-ul logat pe statie
   b. IP sau clasa de IP al statiei
   c. Gateway-ul alocat
   d. DNS serverul alocat
   e. Clientul este/nu este in acceasi retea cu infrastructura de management
   f. Tipul retelei (lan, wireless)

3.6. Rapoarte:

1. Solutia va contine rapoarte care prezinta statusul masinilor clientil din punct de vedere al actualizarilor, fisierelor malware detectate, aplicatiile blocate, site-urilor web blocate.

2. Rapoartele programate pot fi trimise catre un numar nelimitat de adrese de email (nu este nevoie sa aiba un cont in consola de management).
3. Solutia va permite vizualizarea rapoartelor curente programate de administrator.
4. Solutia va permite exportarea rapoartelor in format .pdf si detaliile ca format .csv.
5. Solutia sa includa un generator de rapoarte care sa ofere posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, mentinand informatiile concise si ordonate corespunzator. Astfel, solutia e necesar a include interogari precum: starea terminalului, evenimente terminal, evenimente Exchange.
6. Interogarea legata de starea terminalului sa includa informatii precum :
    a. tip masina
    b. infrastructura retelei careia ii apartine terminalul
    c. datele agentului de securitate
    d. starea modulelor de protectie
    e. rolurile terminalelor.
7. Interogarea legata de evenimente terminal sa includa informatii precum :
    a. calculatorul tinta pe care a avut loc evenimentul
    b. tipul starea si configuratia agentului de securitate instalat
    c. starea modulelor si rolurilor de protectie instalate pe agentul de securitate
    d. denumirea si alocarea politicii
    e. utilizatorul autentificat in timpul evenimentului
    f. evenimente (site-uri blocate, aplicatii blocate, detectiile etc)
8. Interogarea legata de evenimente Exchange sa includa informatii precum :
    a. Directia traficului e-mail
    b. Evenimente de securitate (detectarea programelor de tip malware sau a fisierelor atasate)
    c. Masurile implementate in fiecare situatie (curatarea, stergerea, inlocuirea sau carantinarea fisierului, stergerea sau respingerea e-mail-ului)

3.7. Carantina :

1. Solutia sa permita restaurarea fisierelor carantinate in locatia originala sau intr-o cale configurabila.
2. Carantina va fi locala, pe fiecare statia administrata si va fi administrata, fie local, fie din consola de magement
3. Sa permita descarcarea fisierelor carantinate doar pentru masinile virtuale protejate prin modulul mediilor virtuale integrat cu VMware vShield.

3.8. Utilizatori:

1. Administrarea se se poata realiza pe baza de roluri.
2. Roluri multiple predefinite: Administrator retea sau rol personalizat.
   a. Administrator retea: administreaza serviciile de securitate;
3. Utilizatorii sa poata fi importati din Microsoft Active Directory sau creati in consola de management.
4. Se permita configurarea detaliata a drepturilor administrative cu selectarea serviciilor si obiectelor pentru care un utilizator poate face modificari.
5. Sa permita deconectarea automata a oricarui tip de utilizator dupa un anumit timp pentru o protectie sporita a datelor afisate in consola de administrare. Acest interval sa se poata personaliza de administratorul solutiei.

3.9. Log-uri:

1. Inregistrarea actiunilor utilizatorilor.
2. Sa ofere informatii detaliate pentru fiecare actiune a unui utilizator.
3. Sa permita filtrarea actiunilor utilizator dupa numele utilizatorului, actiune.

3.10. Actualizare:

1. Sa permita definirea de locatii de actualizare multiple.
2. Sa permita activarea/dezactivarea actualizarilor de produs si semnaturi.
3. Sa permita actualizarea produsului intr-o retea fara acces la Internet.
4. Orice client antivirus sa poata fi configurat sa livreze update-urile catre alt client antivirus
5. Solutia oferita sa contina un server de actualizare (update) al prestatorului care face posibila stabilirea componentelor ce vor fi descarcate automat de pe internet, fara interventia administratorului. Astfel, administratorul sa poata descarca pachetele pentru protectia statiilor si serverelor pe care ruleaza sistemul de operare Windows, Linux, Mac sau sa poata descarca pachetele pentru modul de scanare centralizata in mediile de virtualizare VMware, Hyper-V sau Citrix.
6. In cadrul serverului de actualizare, pentru o mai buna urmarire a actualizarilor pachetele, protectia statiilor si serverelor sau a pachetelor pentru modul de scanare centralizata, sa se poata vizualiza un jurnal de modificari in care sa fie precizate istoric:
   a. versiunea pachetului
   b. data versiunii
   c. functii noi si imbunatatiri
   d. probleme rezolvate
   e. probleme cunoscute

7. Solutia sa permita testarea noilor versiuni de pachete de instalare ale clientului antimalware, inainte de a fi instalate pe toate statiile si serverele din retea, evitand posibile probleme ce pot afecta serverele sau statiile critice. Astfel, serverul de actualizaresa includa minim 2 tipuri de actualizari de produs:
   a. Ciclu rapid, pentru un mediu de test in cadrul retelei
   b. Ciclu lent, pentru restul retelei (servere critice)
8. Solutia sa permita stabilirea zonelor de test si critice din cadrul retelei prin intermediul politicilor din consola de management.

3.11. Certificate:

1. Accesul la consola de management sa se faca doar prin HTTPS.
2. Serverul web, din consola centrala de management trebuie sa permita importarea de certificate digitale eliberate de o autoritate de certificare autorizata sau proprie organizatiei.
3. Solutia sa permita afisarea in consola de management informatii despre certificate: nume, autoritatea emitenta, data eliberarii si data expirarii certificatelor eliberate.

4. Caracteristici generale minimale :

4.1 Protectie statiilor si serverelor fizice/virtuale

1. Reducerea la minim a consumului de resurse : solutia antimalware trebuie sa permita instalarea personalizata a modulelor detinute (de ex.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 sa includa o componenta de tip anti-ransomware. Aceasta componenta sa asigure protectia impotriva tuturor amenintarilor cunoscute de tip ransomware, prin imunizarea statiilor si serverelor, chiar daca sunt infectate si prin blocarea procesului de criptare.
3. Componenta anti-ransomware sa primeasca actualizari de la producator, odata cu actualizarea semnaturilor produsului Antimalware.
4. Pentru o mai buna protectie a statiilor si serverelor, solutia sa includa protectie impotriva atacurilor zero-day de tip exploit (atacuri directionate).

4.2. 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)

4.3. Administrare si instalare remote:

1. Inainte de instalare, administratorul sa poata particulariza pachetele de instalare cu modulele dorite: firewall, content control, device control, power user.
2. Instalarea sa se poata 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 sa se poata realiza prin intermediul unui alt client antivirus existent in locatiile necesare 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 sa se poata trimite o singura politica pentru configurarea integrala a clientului de pe statii/servere.
6. Consola sa includa 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 sa poata crea grupuri sau chiar subgrupuri, unde va putea muta statiile/serverele din retea pentru cele care nu sunt integrate domeniu.
11. Sa permita selectarea clientului care va realiza descoperirea statiilor din retea, altele decat cele integrate in domeniu.

4.4 Caracteristici si functionalitati principale ale modulului antimalware:

1. Solutia sa permita 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 o anumita valoare MB, marimea fisierelor se va defini 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 de o anumita valoare in 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 a 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 sa 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, sa includa 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.

4.5. 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.

4.6. 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.

4.7. Protectia datelor:

1. Produsul sa permita blocarea datelor confidentiale transmise prin HTTP sau SMTP prin crearea unor reguli specifice.

4.8. 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).

4.9. Controlul aplicatiilor:

1. Pentru o mai buna inventariere si administrare, solutia sa includa o sectiune in consola de administrare unde sa se regaseasca toate aplicatiile descoperite in retea, grupate dupa: nume, versiune, descoperit la, gasit pe.
2. Pentru o mai buna inventariere si administrare, solutia sa includa 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

4.10. 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.

4.11. Power User:

1. Modulul sa poata fi instalat/dezinstalat in functie de preferinta administratorului.
2. Modulul sa permita 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 sa poata suprascrie din consola setarile aplicate de utilizatorii Power User.

4.12. 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.

4. Cantitati

Cantitatile ce fac obiectul prezentei achizitii sunt :

Specificatii serviciu	Cantitati (buc.)
Licente software antivirus si antimalware	
Licente pentru statii virtuale	*340*
Licente pentru servere	*15*
Licente pentru statii desktop, laptop	*7*

Întocmit,

Serviciul de Comunicații și Informatizare