Anexa Nr. 3

SPECIFICATIE TEHNICA
pentru achiziţie servicii protecţie anti-virus

Caracteristici generale minimale

- Producătorul soluţiilor software anti-virus ce vor fi utilizate pentru prestarea serviciilor trebuie să fie certificat tehnic conform grupei de standarde ISO 9001:2001 pentru producţie de software şi vor fi prezentate certificate doveditoare. Acestea trebuie să fie emise de către o autoritate competentă din ţara de origine a producătorului.
- producătorul soluţiei anti-virus trebuie fie certificat de Microsoft ca si partener Gold.
- se solicită autorizare de distribuţie în original din partea producătorului pentru revînzător.
- certificări internaţionale obţinute cel târziu în intervalul 2007 - 2011 (ICSA Labs, Checkmark, Virus Bulletin etc); Se vor prezenta cel puţin 10 certificate emise de organizaţii europene pentru produsele anti-virus livrate.

Privind produsele anti-virus

- Posibilitatea de update centralizat a soluţiei anti-virus atît pentru staţii cît şi pentru servere în mod automat/programat la un interval de maxim 1 ora.
- Existenta unui singur motor de scanare a anti-virusului de staţie, pentru a nu se încărca suplimentar memoria sistemelor de calcul.
- Din considerentele unei soluţii complete cu management centralizat, întreaga soluţie va aparţine aceluiaşi producător.
- Asigurarea şi garantarea actualizării semnăturilor de virus şi upgrade la noi versiuni pe întreaga perioada care se va contracta, cu posibilitatea de prelungire.
- Să existe posibilitatea ca în cazul trecerii la alt sistem de operare şi/sau server de mail să fie livrat un kit de instalare şi certificat de licenţă pentru produsul nou fără costuri suplimentare.
- Soluţiile anti-virus trebuie să aibă opţiunea de scanare automată a fişierelor, a memoriei şi a cheilor de registre Windows înainte de instalarea pe sisteme.
- Pentru reducerea la minim a consumului de resurse, soluţiile anti-virus trebuie să permită instalarea customizată a modulelor deţinute (de exemplu, să permită instalarea soluţiilor software fără modulul antispam sau modulul firewall).
- Soluţiile software trebuie să aibă interfaţă şi documentaţia în limba română.

Privind serviciile si echipa de suport tehnic:

- Avertizări prin e-mail asupra apariţiei noilor viruşi
    - Mesaje de alerta în cazul apariţiei unor noi viruşi distructivi sau cu potenţial mare de răspândire rapidă.
    - Posibilitatea de a trimite aceste avertizări şi la partenerii Beneficiarului pe baza unor adrese de e-mail furnizate de acesta.
- Posibilitatea furnizorului/producătorului de a răspunde unor solicitări cu privire la incidente provocate de către atacurile virusilor în termen de 24 ore prin intervenţie în locaţiile beneficiarului fizic/sau de la distanta folosind o aplicaţie cu următoarele particularităţi (pe sistemele Windows):
    - Intervenţie real-time securizată, bazată pe un ticket cu durata limitată de valabilitate.
    - Contact continuu între inginerul suport tehnic şi client prin intermediul unei aplicaţii de chat inclusă în sesiunea remote.
    - Vizibilitate totală asupra acţiunilor întreprinse prin aplicaţia remote.
    - Posibilitatea clientului de a prelua controlul în orice moment.
    - Conectare via plug-in web care nu necesită configurări suplimentare în firewall-ul sau serverele clienţilor.

- Nu necesită dezvăluirea parolelor de administrator de pe serverele clienţilor.
- Antidot pentru orice virus nou semnalat de către beneficiar.
- Suport tehnic, telefonic, e-mail si chat non-stop, 24/24 în limba română oferit de producător. În oferta tehnică şi comercială furnizorul va prezenta numerele de telefon şi adresele de email la care beneficiarul poate accesa serviciile de suport tehnic.
- Cel puţin 4 dintre specialiştii de suport tehnic ai producătorului soluţiei anti-virus vor avea certificări Microsoft Certified Professional sau Microsoft Certified Technology Specialist.
- Training pentru utilizarea/configurarea şi administrarea soluţiei de securizare LAN/WAN şi probleme generale legate de virusologia IT. Training-ul se va efectua la locaţia furnizorului de produse anti-virus sau la locaţia beneficiarului.
- Asistenta tehnică telefonică şi remote la configurarea produselor pentru locaţiile din Chişinău şi din teritoriu.
- Personalul care va asigura intervenţiile periodice şi la cerere trebuie să fie certificat de producătorul soluţiei software (se vor prezenta documente justificative pentru cel puţin 3 ingineri).

- Soluţia trebuie să fie disponibilă pentru livrare în cel mult 48 de ore de la semnarea contractului.
- Produsele software anti-virus furnizate trebuie să fie însoţite de certificatele de calitate.
- Constatarea de deficienţe sau neconcordanţe între caracteristicile tehnice şi funcţionale ale produsului livrat şi instalat şi cerinţele tehnice din caietul de sarcini atrage după sine înlocuirea produsului software anti-virus sau actualizarea acestuia, în termen de 48 ore de la constatarea deficienţelor.
- Nu se admit neconcordanţe între performanţele, caracteristicile produselor software anti-virus livrate/instalate şi caracteristicile din specificaţia tehnică a Caietului de sarcini.

Termenul de livrare

Livrarea produselor se va face in 2 zile de la data semnării contractului.

<u>Cerinţe minime pentru produsele anti-virus:</u>

Anti-virus pentru staţii de lucru (mobile sau fixe) cu management centralizat

Caracteristici generale:

- Termenul de valabilitate a soluţiei de securitate - minimum 2 ani cu posibilitatea de prelungire ulterioară.
- Numărul de staţii client în reţea este de circa 750 (şapte sute cinci zeci).
- Metode de detecţie a virusilor, a programelor spion, a rootkit-urilor, a mesajelor de tip spam, a tentativelor de fraudare de tip phising şi a altor programe cu potenţial malitios, backup fişiere.
- Interfaţă grafică în limba română.
- Soluţia de securitate pentru staţii va fi livrată împreună cu manualul de utilizare în limba română.

Caracteristici şi funcţionalităţi principale ale modulului anti-virus şi antispyware :

- Scanarea automata “on acces” (în timp real) a fişierelor care se copiază de pe suport extern şi din LAN sau WAN.

- Scanarea automata “on acces” (în timp real) a fişierelor va putea fi setată sa scaneze numai anumite tipuri de fişiere, definite de administrator.
- Scanarea automata “on acces” (în timp real) a fişierelor va putea fi setată să nu scaneze arhive mai mari de « x » Kb, mărimea fişierelor putând fi definită de administratorul soluţiei.
- Clienţii anti-virus pentru workstation să permită scanarea transferurilor de fişiere la comunicaţii P2P (instant messaging).
- Scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicaţii cu potenţial periculos protejând sistemul de viruşi necunoscuţi prin detectarea codurilor periculoase a căror semnătură nu a fost lansată încă.
- Scanarea la cerere şi la acces a oricărui suport de stocare a informaţiei (FDD , HDD, CD-ROM, USB Flash Memory).
- Scanarea în următoarele arhive şi efectuarea dezinfectării într-o serie de formate uzuale (arj, ace, cab, dbx, docfile, gzip, lha, mbx, mime, pdf, pst, rar, rpm, rtf, sfx, tar, zip, thebat).
- Scanarea automata a e-mailurilor la nivelul staţiei de lucru indiferent de clientul de e-mail folosit la nivelul POP3.
- La scanarea la cerere vor fi scanate şi arhivele e-mail.
- Posibilitatea selectării tipului principal şi secundar de acţiune la detectarea unui mesaj infectat.
- Mesaje pe ecran sub formă de fereastră pop-up în momentul detectării unui e-mail infectat.
- Configurarea căilor ce urmează a fi scanate, inclusiv la nivel de fişiere.
- Clienţii anti-virus pentru workstation să permită excluderea de la scanarea “on-access” (în timp real) a fişierelor de anumite dimensiuni, cu posibilitatea definirii dimensiunilor respective.
- Clienţii anti-virus pentru workstation să permită definirea unor liste de excludere de la scanarea “on-access” şi “on demand” (în timp real şi la cerere) a anumitor directoare, discuri, fişiere sau extensii.
- Clienţii anti-virus pentru workstation trebuie să conţină opţiunea de pauza şi reluare a scanărilor.
- Clienţii anti-virus pentru workstation să permită monitorizarea activă a registrelor afişând mesaje de atenţionare a utilizatorului în momentul în care o aplicaţie încearcă să modifice cheile registrelor.
- Cu ajutorul unei baze de date complete cu semnături de spyware şi a euristicii de detecţie a acestui tip de programe, produsul va trebui să ofere protecţie anti-spyware şi să permită prevenirea furtului de date confidenţiale.
- Clientul anti-virus pentru worstation trebuie să funcţioneze atât în cadrul reţelei interacţionând cu consola de management cat şi în mod standalone cu posibilitatea de actualizare atât din LAN cît şi de pe serverul producătorului soluţiei fără ca utilizatorul să intervină asupra setărilor.
- Pentru a nu încărca resursele sistemului produsul anti-virus trebuie să conţină un singur motor de scanare şi să poată rula scanările programate cu prioritate redusă.
- Mod de vizualizare grafică a procesului de scanare la acces precum şi a activităţii în Internet, afişată permanent la nivelul staţiei de lucru.
- Pentru o mai mare protecţie, soluţia anti-virus trebuie sa aibă 3 tipuri de detecţie: bazată pe semnături, bazata de comportamentul fişierelor şi bazată pe monitorizarea proceselor.

Firewall:

- Firewall protecţie a datelor şi filtrarea traficului la intrare şi la ieşire, controlând fişierele de tip cookie, blocând scripturile maliţioase şi programele de tipul „XXX-dialer”.
- Predefinirea setului de reguli ce urmează a fi aplicate în mod automat.
- Controlul fişierelor de tip script şi cookie.
- Posibilitatea de a stabili tipul de lucru „invizibil” la nivelul reţelei locale sau Internet.
- Definirea perioadei de timp în care o regulă poate fi activă sau inactivă.
- Modulul poate fi instalat/dezinstalat în funcţie de preferinţa administratorului.

Antispam:

- Tehnologiile antispam să permită adaptarea la noile tehnici de lansare a spam-ului, analizînd şi memorînd preferinţele utilizatorului, reducînd astfel la minim numărul mesajelor legitime etichetate ca spam.
- Filtrul antispam să poată fi antrenat de către utilizator, prin simpla clasificare a câtorva e-mail-uri ca spam sau legitime.
- Filtrare a mesajelor Spam de tip imagine.
- Posibilitatea blocării mesajelor e-mail cu caractere Cyrilice.
- Folosirea filtrului antispam "antrenat" pe baza unei serii de mesaje spam astfel încât acesta sa poată recunoaşte noile mesaje de acest tip prin identificarea asemănărilor cu cele pe care le-a examinat deja.
- Modulul poate fi instalat/dezinstalat în funcţie de preferinţa administratorului.

Carantina:

- Produsul anti-virus să permită trimiterea manuală şi automată a fişierului din carantină către laboratorul anti-virus.
- Trimiterea conţinutului carantinei va putea fi expediat în mod automat, la un număr de minute definit de administrator.
- Produsul anti-virus să permită ştergerea automata a fişierelor duplicate sau a celor din carantină mai vechi de o anumita perioadă, pentru a nu încărca inutil spaţiul de stocare.
- Posibilitatea de a muta un fişier din carantină în locaţia lui originală.

Administrare şi instalare remote:

- Posibilitatea de a avea o consola centrala care la rândul ei să poată avea subordonate mai multe console care pot îndeplini aceleaşi funcţii.
- Consola de management va putea raporta numărul staţiilor de lucru care au instalată şi neinstalată soluţia de protecţie anti-virus.
- Posibilitatea consolei de a raporta dacă modulul anti-virus este sau nu este activ la nivelul staţiei de lucru.
- În cazul în care clientul anti-virus pentru staţie nu a fost actualizat sau a fost actualizat corespunzător, consola de management va trebui să poată raporta acest aspect.
- Consola de management va trebui sa gestioneze numărul licenţelor active şi va putea raporta numărul licenţelor utilizate.
- Posibilitatea de instalare a clienţilor anti-virus doar cu anumite module (ex: fără antiphising).
- Posibilitatea creării unui singur kit de instalare, utilizabil atât pentru sistemele de operare 32-bit cât şi pe 64-bit.
- Detectare automată a staţiilor nou intrate în reţea cu posibilitatea de instalare automată a protecţiei anti-virus pe acestea.
- Detecţia staţiilor de lucru fără protecţie după numele acestora şi după plaja de adrese IP
- Clienţii anti-virus pentru workstation să permită scanarea programată, respectiv verificarea, periodică sau numai la anumite momente, a sistemului fără intervenţia utilizatorului
- Protejarea prin parolă a accesului la consola de management a soluţiei anti-virus
- Asigură respectarea politicilor de securitate ale companiei de către utilizatorii staţiilor de lucru mobile, chiar şi atunci când acestea nu sunt conectate la reţea
- Produsul trebuie să fie compatibil şi integrabil cu Microsoft Active Directory

- Consola de management a soluţiei anti-virus va avea suport integrat pentru scripturi WMI cu următoarele particularităţi:
    - minim 30 de sarcini de rețea predefinite, pentru o cât mai bună administrare a rețelei
    - Instalarea/dezinstalarea programelor (instalate cu MSI installer) de pe staţiile client
    - Posibilitatea de a colecta informaţii legate de componentele staţiilor de lucru: cantitate memorie RAM, spaţiu existent pe harddisk, procesor, sistem operare şi procesele care rulează la nivelul sistemului de operare
    - Blocare porturi USB
    - Trimitere mesaje către utilizatorii staţiilor de lucru
    - Oprire şi restartare sistem operare
    - Oprirea anumitor procese la nivelul staţiilor de lucru pe care rulează clientul anti-virus
- Consola va avea integrat un modul dedicat controlului utilizator cu următoarele particularităţi :
    - Blocarea accesului la Internet pentru anumiţi utilizatori sau grupuri de utilizatori
    - Blocarea accesului la Internet pentru anumite aplicaţii
    - Blocarea accesului la Internet pentru anumite perioade de timp
    - Blocare pagini web care conţin anumite cuvinte cheie
    - Permitere acces numai la anumite pagini web specificate de administrator
    - Blocarea accesului la aplicaţii
    - Restricţionare acces internet între anumite intervale orare
- Permite stabilirea a doua tipuri de utilizatori – clienţii autorizaţi, cu acces nelimitat la interfaţa şi setări de produs şi clienţii restricţionaţi, cu acces limitat, fără acces la setările produsului
- Posibilitatea de notificare a administratorului în cazul în care clienţii de workstation au fost inactivi un număr de zile predefinit.
- Integrare cu soluţiile de securitate pentru servere ale aceluiaşi producător.
- Consola va putea grupa şi gestiona grupările clienţilor anti-virus pentru staţii sau servere conform următoarelor criterii:
    - Gruparea clienţilor după numărul staţiilor sau serverelor care au sau nu au protecţia instalată.
    - Gruparea clienţilor după numărul staţiilor care au fost excluse de la instalarea protecţiei.
    - Gruparea clienţilor după numărul staţiilor care au clientul anti-virus restricţionat şi nerestricţionat.
- Sincronizare zilnica cu Active Directory.
- Politicile şi sarcinile de rețea pot fi aplicate nu numai la nivel de staţie, ci şi la nivel de user.

Rapoarte, grafice şi alerte:

- Posibilitatea de a crea rapoarte pe baza unor şabloane de rapoarte definite în consola de management.
- Clienţii anti-virus pentru workstation să permită generarea de rapoarte complete privind rezultatele scanării şi infecţiilor detectate dar şi a tuturor obiectelor scanate.
- Posibilitatea trimiterii de mesaje alertă în mod automat către adresa de e-mail a administratorului în caz de detecţie a unui mesaj infectat.
- Posibilitatea setării dimensiunii mesajului de alertă. Livrarea mesajelor se va face indiferent de dimensiunea stabilită de administrator, dimensiunea mesajului.
- Generarea rapoartelor în mod programat şi expedierea lor în mod automat către administratorul soluţiei
- Rapoartele vor putea fi exportate în vederea vizualizării/imprimării în următoarele formate: HTML şi PDF
- Existenta a minim 20 de şabloane de rapoarte predefinit, atât despre starea produselor, cât şi despre evenimente malware

Audit REȚEA

- Soluţia anti-virus trebuie să aibă un colector configurabil şi automat al informaţiilor hardware şi software ale staţiilor, care să permită colectarea automată la un anumit interval de timp şi pentru anumite caracteristici.
- Datele colectate în vederea auditului trebuie să poată fi arhivate automat prin intermediul unui arhivator programabil (perioada, locaţie, cu parolă)
- Existenta unor multiple şabloane de raportare în vederea auditului (rapoarte customizate, rapoarte de tip istoric şi de tip comparative).
- Modulul de audit trebuie să permită transmiterea rapoartelor prin mail, la adresa stabilită de administrator, la intervalul de timp stabilit de acesta.
- Auditul se va putea efectua în mod independent de instalarea soluţiei anti-virus pe staţiile din reţea.

Backup

- Posibilitatea realizării unor copii de rezervă a datelor importante la nivel local, pe staţiile de lucru sau direct pe medii de stocare externe: CD, DVD, Usb-flash.
- Posibilitatea consolei de management de realiza o copie de siguranţă a setărilor efectuate de administrator la nivelul soluţiei anti-virus.

Actualizare:

- Actualizarea anti-virus să poată fi făcută automat la un interval de maxim 1 ora, on demand.
- Posibilitatea efectuării update-ului la nivel de client de workstation în mod silenţios (fără avertizare).
- Posibilitatea de a aştepta restartarea calculatorului după efectuarea actualizării fără a notifica utilizatorul.
- Posibilitatea stabilirii intervalului de descărcare a actualizărilor.
- Sistem de actualizare cascadat.
- În vederea securizării sistemului de update, fişierele de update vor fi semnate de producător.

Anti-virus pentru servere de fişiere pe platforma Windows :

- Protecţie anti-virus, antispyware şi antirootkit.
- Actualizarea anti-virus să poată fi făcută automat la un interval de maxim 1 ora, on demand.
- Scanarea euristica comportamentala prin simularea unui calculator virtual in interiorul căruia sunt rulate aplicaţii cu potenţial periculos protejând sistemul de viruşii necunoscuţi prin detectarea codurilor periculoase a căror semnătura nu a fost lansata încă.
- Marcarea „read only" a fişierelor scanate în cadrul aceleiaşi sesiuni şi rescanarea acestora numai în cazul unei noi sesiuni, update sau infecţie în cadrul sistemului.
- Scanare in timp real a fişierelor ce trec prin server, atât la deschiderea acestora cât şi la închidere; posibilitatea scanării la cerere şi a serverului pe care este instalat.
- Cu ajutorul unei baze de date complete cu semnături de spyware şi a euristicii de detecţie a acestui tip de programe, produsul va trebui să ofere protecţie anti-spyware şi să permită prevenirea furtului de date confidenţiale.
- Administrarea să poată fi făcută centralizat din cadrul consolei de management globale sau independent.
- Posibilitatea scanării la alegere doar a fişierelor având extensiile specificate de administrator precum şi opţiunea de scanare numai a fişierelor de o dimensiune mai mica decât o limita stabilita de administrator.
- Posibilitatea de definire a proceselor care să fie excluse de la scanare.
- Posibilităţi de acţiuni multiple la detecţia unui virus (disinfect, delete, mutare in carantina).

- Posibilitatea de a seta locaţia de carantină unde vor fi stocate mailurile virusate – în funcţie de opţiunea administratorului.
- Produsul va trebui să ofere rapoarte şi statistici detaliate referitoare la scanarea anti-virus.
- Update configurabil de pe internet cu setări specifice unui proxy (user şi password) sau din cadrul reţelei de pe un server de update propriu. Se vor trimite notificări la detectarea unui mail virusat în funcţie de opţiunile alese la administrator.
- Posibilitatea de notificare prin mail a existentei unei versiuni noi a produsului instalat.
- Posibilitatea de export a setărilor produsului pentru a putea fi importante la o instalare ulterioara sau pe un alt server de fişiere.
- Să se poată integra în consola de administrare Windows MMC.
- Produsul se va integra în cadrul consolei de management unitar al soluţiei anti-virus.
- Soluţia trebuie să permită rescanarea fişierelor din carantină.
- Soluţia trebuie să permită scanarea contextuală.