



MINISTERUL SĂNĂTĂȚII
DIRECȚIA DE SĂNĂTATE PUBLICĂ IASI
Str. Vasile Conta nr. 2-4 , Telefon - centrala : 0232 / 210900 ; secretariat : 0232 / 271687; fax : 0232 / 241963
Email:- dsp99@dspiiasi.ro, site – www.dspiiasi.ro
OPERATOR DATE CU CARACTER PERSONAL Nr. 11730



Nr. 28013/ 13.11.2019

Invitatie de participare

AUTORITATE CONTRACTANTA:

Directia de Sanatate Publica Iasi, cu sediul in Iasi, strada Vasile Conta nr.2-4, telefon/fax 023227228, CP: 700106, Romania, e-mail: achizitii@dspiiasi.ro, adresa internet (URL): www.dspiiasi.ro.

DETALII ANUNT:

1. Achizitie directa de furnizare produse, ce se realizeaza in conformitate cu prevederile art 7, alin. 5 din Legea nr. 98/2016 privind achizițiile publice.

2. Obiectul achiziției publice: “Pachet Soft protectie Antivirus”.

Cantitate = 50 pachete a cate 3 licente.

3. Cod CPV: 48761000-0 Pachete software antivirus.

4. Valoare totala estimata: 7563 lei, fara TVA.

5. Ofertele se vor transmite /depune la sediul Directiei de Sanatate Publica Iasi, strada Vasile Conta nr.2-4, cod postal 700106, secretariatul institutiei, sau prin intermediul postei electronice la adresa de e-mail: achizitii@dspiiasi.ro.

Oferta va cuprinde pretul unitar in lei, fara TVA precum si pretul total exprimat in lei fara TVA si cu TVA.

Perioada de valabilitate a ofertei este de 90 de zile.

6. Criteriul de atribuire: Pretul cel mai scazut . Operatorul economic declarat castigator va publica in 2 zile lucratoare in catalogul electronic SEAP oferta financiara conform documentatiei depuse.

7. Termen limita de depunere a ofertelor: 18.11.2019, ora 14:00.

Persoana de contact: Consilier achizitii, ing. Liliana Cucu, tel 0232.278228.

8. Informatii suplimentare: Pachetul antivirus trebuie sa asigure protectia bazelor de date impotriva amenintarii aplicatiilor de tip virus si a atacurilor de tip RANSOMWARE. Antivirusul detecteaza si blocheaza amenintarile cibernetice inclusiv mesajele email si atasamentele respective.



Director Executiv,
Dr. Liviu Stafie

Intocmit,
Compartiment Achizitii
ing. Liliana Cucu

ANEXA NR. 1.



APROBAT,
Director Executiv
Dr. Liviu Stafie

SPECIFICATIE TEHNICA pentru achiziție - furnizare pachete soft protecție anti-virus

Caracteristici generale minimale

- protecție completă pentru Windows cu multiple niveluri de securitate, împotriva amenințărilor noi sau existente.
- producătorul soluției anti-virus trebuie fie certificat de Microsoft.
- se solicită autorizare de distribuție în original din partea producătorului pentru revînzător.
- certificări internaționale obținute cel târziu în intervalul 2007 - 2011 (ICSA Labs, Checkmark, Virus Bulletin etc); Se vor prezenta certificate emise de organizații europene pentru produsele anti-virus livrate.

Privind produsele anti-virus

- Posibilitatea de update centralizat a soluției anti-virus atât pentru stații cât și pentru servere în mod automat/programat la un interval de maxim 1 ora.
- Existenta unui singur motor de scanare a anti-virusului de stație, pentru a nu se încărca suplimentar memoria sistemelor de calcul.
- Din considerentele unei soluții complete cu management centralizat, întreaga soluție va apartine aceluiași producător.
- Asigurarea și garantarea actualizării semnăturilor de virus și 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 și/sau server de mail să fie livrat un kit de instalare și certificat de licență pentru produsul nou fără costuri suplimentare.
- Soluțiile anti-virus trebuie să aibă opțiunea de scanare automată a fișierelor, a memoriei și a cheilor de registre Windows înainte de instalarea pe sisteme.
- Pentru reducerea la minim a consumului de resurse, soluțiile anti-virus trebuie să permită instalarea customizată a modulelor deținute (de exemplu, să permită instalarea soluțiilor software fără modulul antispam sau modulul firewall).
- Soluțiile software trebuie să aibă interfață și documentația în limba română.

Privind serviciile si echipa de suport tehnic:

- Avertizări prin e-mail asupra apariției noilor viruși
 - Mesaje de alertă în cazul apariției unor noi viruși distructivi sau cu potențial mare de răspândire rapidă.
 - Posibilitatea de a trimite aceste avertizări și 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 virușilor în termen de 24 ore prin intervenție în locațiile beneficiarului fizic/sau de la distanță folosind o aplicație cu următoarele particularități (pe sistemele Windows):
 - Intervenție real-time securizată, bazată pe un ticket cu durată limitată de valabilitate.
 - Contact continuu între inginerul suport tehnic și client prin intermediul unei aplicații de chat inclusă în sesiunea remote.
 - Vizibilitate totală asupra acțiunilor întreprinse prin aplicația remote.
 - Posibilitatea clientului de a prelua controlul în orice moment.
 - Conectare via plug-in web care nu necesită configurații suplimentare în firewall-ul sau serverele clienților.
 - Nu necesită dezvăluirea parolelor de administrator de pe serverele clienților.

- Antidot pentru orice virus nou semnalat de către beneficiar.
- Suport tehnic, telefonic, e-mail și chat non-stop, 24/24 în limba română oferit de producător. În oferta tehnică și comercială furnizorul va prezenta numerele de telefon și adresele de email la care beneficiarul poate accesa serviciile de suport tehnic.
- Instruire pentru utilizarea/configurarea și administrarea soluției de securizare LAN/WAN și probleme generale legate de virusologia IT. Instruirea se va efectua la locația beneficiarului.
- Personalul care va asigura intervențiile periodice și la cerere trebuie să fie certificat de producătorul soluției software.
- Soluția trebuie să fie disponibilă pentru livrare în cel mult 48 de ore de la semnarea contractului.
- Produsele software anti-virus furnizate trebuie să fie însotite de certificate de calitate.
- Constatarea de deficiențe sau neconcordanțe între caracteristicile tehnice și funcționale ale produsului livrat și instalat și cerințele tehnice atrage după sine înlocuirea produsului software anti-virus sau actualizarea acestuia, în termen de 48 ore de la constatarea deficiențelor.
- Nu se admit neconcordanțe între performanțele, caracteristicile produselor software anti-virus livrate/installate și caracteristicile din specificația tehnică.

Termenul de livrare

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

Cerințe minime pentru produsele anti-virus:

Anti-virus pentru stații de lucru cu management centralizat

Caracteristici generale:

- Termenul de valabilitate a soluției de securitate - minimum 1 an cu posibilitatea de prelungire ulterioară.
- Metode de detecție a virușilor, a programelor spion, a rootkit-urilor, a mesajelor de tip spam, a tentativelor de fraudare de tip phising și a altor programe cu potențial malicioas, backup fișiere.
- Interfață grafică în limba română.
- Soluția de securitate pentru stații va fi livrată împreună cu manualul de utilizare în limba română.

Caracteristici și funcționalități principale ale modulului anti-virus și antispyware :

- Scanarea automata “on acces” (în timp real) a fișierelor care se copiază de pe suport extern și din LAN sau WAN.
- Scanarea automata “on acces” (în timp real) a fișierelor va putea fi setată să scaneze numai anumite tipuri de fișiere, definite de administrator.
- Scanarea automata “on acces” (în timp real) a fișierelor va putea fi setată să nu scaneze arhive mai mari de « x » Kb, mărimea fișierelor putând fi definită de administratorul soluției.
- Clienții anti-virus pentru workstation să permită scanarea transferurilor de fișiere la comunicații P2P (instant messaging).
- Scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de viruși necunoscuți prin detectarea codurilor periculoase a căror semnătură nu a fost lansată încă.
- Scanarea la cerere și la acces a oricărui suport de stocare a informației (FDD, HDD, CD-ROM, USB Flash Memory).
- Scanarea în următoarele arhive și efectuarea dezinfecției 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 automată a e-mailurilor la nivelul stației de lucru indiferent de clientul de e-mail folosit la nivelul POP3.
- La scanarea la cerere vor fi scanate și arhivele e-mail.
- Posibilitatea selectării tipului principal și secundar de acțiune 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 fișiere.
- Clienții anti-virus pentru workstation să permită excluderea de la scanarea “on-access” (în timp real) a fișierelor de anumite dimensiuni, cu posibilitatea definirii dimensiunilor respective.
- Clienții anti-virus pentru workstation să permită definirea unor liste de excludere de la scanarea “on-access” și “on demand” (în timp real și la cerere) a anumitor directoare, discuri, fișiere sau extensii.
- Clienții anti-virus pentru workstation trebuie să conțină opțiunea de pauza și reluare a scanărilor.
- Clienții anti-virus pentru workstation să permită monitorizarea activă a regisrelor afișând mesaje de atenționare a utilizatorului în momentul în care o aplicație încearcă să modifice cheile regisrelor.
- Cu ajutorul unei baze de date complete cu semnături de spyware și a euristicii de detecție a acestui tip de programe, produsul va trebui să ofere protecție anti-spyware și să permită prevenirea furtului de date confidențiale.
- Clientul anti-virus pentru worstation trebuie să funcționeze atât în cadrul rețelei interacționând cu consola de management cat și în mod standalone cu posibilitatea de actualizare atât din LAN cît și de pe serverul producătorului soluției fără ca utilizatorul să intervină asupra setărilor.
- Pentru a nu încărca resursele sistemului produsul anti-virus trebuie să conțină un singur motor de scanare și să poată rula scanările programate cu prioritate redusă.
- Mod de vizualizare grafică a procesului de scanare la acces precum și a activității în Internet, afișată permanent la nivelul stației de lucru.
- Pentru o mai mare protecție, soluția anti-virus trebuie să aibă 3 tipuri de detecție: bazată pe semnături, bazată de comportamentul fișierelor și bazată pe monitorizarea proceselor.

Protectie:

- Protectie completa în timp real a datelor - pentru a combate toate tipurile de amenințări electronice, de la viruși, viermi și troieni la ransomware, exploatare de tip ziua zero, rootkit-uri și programe spion.
- Prevenire amenintari retea – capacitate de a detectata și respinge toate amenințările online, de a analiza și identifica activitățile suspecte la nivel de rețea și sa fie posibil a se bloca exploatarele, programele malware și atacurile informaticce care utilizează bootnet-uri, precum și atacurile prin forță brută. Datele și confidențialitatea beneficiarului trebuie să fie în siguranță.
- Monitorizare îndeaproape a aplicațiilelor active; în momentul în care se va detecta ceva suspect, acesta va lua măsuri imediat pentru a preveni infectările.
- Abordarea pe mai multe niveluri împotriva amenințărilor ransomware și protejarea fișierelor importante împotriva criptării de către programele ransomware.
- Blocharea linkurilor infectate cunoscute, protectie anti-phising, antifraudă, antispam, protectie fisiere.
- Soluția de securitate trebuie să reacționeze imediat la amenințările malware fără a compromite performanța sistemului beneficiarului.
- Tehnologia propusa trebuie să se adapteze la configurația hardware și software specifică sistemului beneficiarului pentru a economisi resurse și pentru a îmbunătăți viteza și performanța sistemului.

Firewall:

- Firewall protecție a datelor și filtrarea traficului la intrare și la ieșire, controlând fișierele de tip cookie, blocând scripturile malicioase și programele de tipul „XXX-dialer”.
- Predefinirea setului de reguli ce urmează a fi aplicate în mod automat.
- Controlul fișierelor de tip script și cookie.
- Posibilitatea de a stabili tipul de lucru „invizibil” la nivelul rețelei locale sau Internet.
- Definirea perioadei de timp în care o regulă poate fi activă sau inactivă.
- Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului.

- **Antispam:**
- Tehnologiile antispam să permită adaptarea la noile tehnici de lansare a spam-ului, analizând și memorând preferințele utilizatorului, reducând 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 să poată recunoaște noile mesaje de acest tip prin identificarea asemănărilor cu cele pe care le-a examinat deja.
- Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului.

Carantina:

- Produsul anti-virus să permită trimiterea manuală și automată a fișierului din carantină către laboratorul anti-virus.
- Trimiterea conținutului carantinei va putea fi expediată în mod automat, la un număr de minute definit de administrator.
- Produsul anti-virus să permită ștergerea automata a fișierelor duplicate sau a celor din carantină mai vechi de o anumita perioadă, pentru a nu încărca inutil spațiul de stocare.
- Posibilitatea de a muta un fișier din carantină în locația lui originală.

Administrare și instalare remote:

- Posibilitatea de a avea o consola centrală care la rândul ei să poată avea subordonate mai multe console care pot îndeplini aceleasi funcții.
- Consola de management va putea raporta numărul stațiilor de lucru care au instalată și neinstalată soluția de protecție anti-virus.
- Posibilitatea consolei de a raporta dacă modulul anti-virus este sau nu este activ la nivelul stației de lucru.
- În cazul în care clientul anti-virus pentru stație nu a fost actualizat sau a fost actualizat corespunzător, consola de management va trebui să poată raporta acest aspect.
- Consola de management va trebui să gestioneze numărul licențelor active și va putea raporta numărul licențelor utilizate.
- Posibilitatea de instalare a clienților 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 și pe 64-bit.
- Detectare automată a stațiilor nou intrate în rețea cu posibilitatea de instalare automată a protecției anti-virus pe acestea.
- Deteția stațiilor de lucru fără protecție după numele acestora și după plaja de adrese IP.
- Clienții anti-virus pentru workstation să permită scanarea programată, respectiv verificarea, periodică sau numai la anumite momente, a sistemului fără intervenția utilizatorului.
- Protejarea prin parolă a accesului la consola de management a soluției anti-virus.
- Asigură respectarea politicilor de securitate ale companiei de către utilizatorii stațiilor de lucru mobile, chiar și atunci când acestea nu sunt conectate la rețea.
- Produsul trebuie să fie compatibil și integrabil cu Microsoft Active Directory.

- Consola de management a soluției anti-virus va avea suport integrat pentru scripturi WMI cu următoarele particularități:
 - minim 30 de sarcini de rețea predefinite, pentru o cât mai bună administrare a rețelei;
 - Instalarea/dezinstalarea programelor (instalate cu MSI installer) de pe stațiile client ;
 - Posibilitatea de a colecta informații legate de componentele stațiilor de lucru: cantitate memorie RAM, spațiu existent pe harddisk, procesor, sistem operare și procesele care rulează la nivelul sistemului de operare;
 - Blocare porturi USB;
 - Trimitere mesaje către utilizatorii stațiilor de lucru;
 - Oprire și restartare sistem operare;
 - Oprirea anumitor procese la nivelul stațiilor de lucru pe care rulează clientul anti-virus;
- Consola va avea integrat un modul dedicat controlului utilizator cu următoarele particularități :
 - Blocarea accesului la Internet pentru anumiți utilizatori sau grupuri de utilizatori;
 - Blocarea accesului la Internet pentru anumite aplicații;
 - Blocarea accesului la Internet pentru anumite perioade de timp;
 - Blocare pagini web care conțin anumite cuvinte cheie;
 - Permitere acces numai la anumite pagini web specificate de administrator;
 - Blocarea accesului la aplicații;
- Permite stabilirea a două tipuri de utilizatori – clienții autorizați, cu acces nelimitat la interfața și setările produs și clienții restricționați, cu acces limitat, fără acces la setările produsului.
- Posibilitatea de notificare a administratorului în cazul în care clienții de workstation au fost inactivi un număr de zile predefinit.
- Integrare cu soluțiile de securitate pentru servere ale aceluiași producător.
- Consola va putea grupa și gestiona grupările clienților anti-virus pentru stații sau servere conform următoarelor criterii:
 - Gruparea clienților după numărul stațiilor sau serverelor care au sau nu au protecția instalată.
 - Gruparea clienților după numărul stațiilor care au fost excluse de la instalarea protecției.
 - Gruparea clienților după numărul stațiilor care au clientul anti-virus restricționat și nerestricționat.
- Sincronizare zilnică cu Active Directory.
- Politicile și sarcinile de rețea pot fi aplicate nu numai la nivel de stație, ci și la nivel de user.

Audit REȚEA

- Soluția anti-virus trebuie să aibă un colector configurabil și automat al informațiilor hardware și software ale stațiilor, care să permită colectarea automată la un anumit interval de timp și pentru anumite caracteristici.
- Datele colectate în vederea auditului trebuie să poată fi arhivate automat prin intermediul unui arhivator programabil (perioada, locație, cu parolă).
- Existenta unor multiple şabloane de raportare în vederea auditului (rapoarte customizate, rapoarte de tip istoric și 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 soluției anti-virus pe stațiile din rețea.

Backup

- Posibilitatea realizării unor copii de rezervă a datelor importante la nivel local, pe stațiile de lucru sau direct pe medii de stocare externe: CD, DVD, Usb-flash.
- Posibilitatea consolei de management de realiza o copie de siguranță a setărilor efectuate de administrator la nivelul soluției 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 silențios (fără avertizare).

- Posibilitatea de a aștepta 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, fișierele de update vor fi semnate de producător.

Anti-virus pentru servere de fișiere pe platforma Windows :

- Protecție anti-virus, antispyware și antirootkit.
- Actualizarea anti-virus să poată fi făcută automat la un interval de maxim 1 ora, on demand.
- Scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de virusii necunoscuți prin detectarea codurilor periculoase a căror semnătura nu a fost lansată încă.
- Marcarea „read only” a fișierelor scanate în cadrul aceleiași sesiuni și rescanarea acestora numai în cazul unei noi sesiuni, update sau infecție în cadrul sistemului.
- Scanare în timp real a fișierelor ce trec prin server, atât la deschiderea acestora cât și la închidere; posibilitatea scanării la cerere și a serverului pe care este instalat.
- Cu ajutorul unei baze de date complete cu semnături de spyware și a euristicii de detecție a acestui tip de programe, produsul va trebui să ofere protecție anti-spyware și să permită prevenirea furtului de date confidențiale.
- Administrarea să poată fi făcută centralizată din cadrul consolei de management globale sau independent.
- Posibilitatea scanării la alegere doar a fișierelor având extensiile specificate de administrator precum și opțiunea de scanare numai a fișierelor de o dimensiune mai mică decât o limită stabilită de administrator.
- Posibilitatea de definire a proceselor care să fie excluse de la scanare.
- Posibilități de acțiuni multiple la detecția unui virus (disinfect, delete, mutare în carantina).
- Posibilitatea de a seta locația de carantină unde vor fi stocate mailurile virusate – în funcție de opțiunea administratorului.
- Produsul va trebui să ofere rapoarte și statistici detaliate referitoare la scanarea anti-virus.
- Update configurabil de pe internet cu setări specifice unui proxy (user și password) sau din cadrul rețelei de pe un server de update propriu. Se vor trimite notificări la detectarea unui mail virusat în funcție de opțiunile alese la administrator.
- Posibilitatea de notificare prin mail a existenței unei versiuni noi a produsului instalat.
- Posibilitatea de export a setărilor produsului pentru a putea fi importante la o instalare ulterioară sau pe un alt server de fișiere.
- Să se poată integra în consola de administrare Windows MMC.
- Produsul se va integra în cadrul consolei de management unitar al soluției anti-virus.
- Soluția trebuie să permită rescanarea fișierelor din carantină.
- Soluția trebuie să permită scanarea contextuală.

Intocmit,
Avadanei Ovidiu Neculai