



Invitatie de participare

Achizitia de : soft protecție antivirus Bitdefender Internet Security 2021

1. Denumirea contractantului: Directia de Sanatate Publica a Judetului Iasi.

Adresa: Iasi, Str. V. Conta nr.2-4, tel: 0232/278228, fax: 0232/241.963, e -mail: secretariat@dspiiasi.ro.

2. Obiectul caietului de sarcini: DSP IASI doreste sa achizitioneze un produs care asigura protectia impotriva amenințărilor cibernetice a echipamentelor de calcul - Pachete soft protecție antivirus Bitdefender Internet Security 2021; cantitate – 40 pachete a cate 3 licente.

3. Procedura aplicata : – Achizitia directa se realizeaza in conformitate cu prevederile art.7, alin.5 din Legea nr. 98/2016, privind achizitiile publice.

4. Cod CPV: 487610000-0 Pachete software antivirus

5. Sursa de finantare : Buget de stat/ Venituri proprii

6. Criteriul de atribuire : cel mai scazut pret.

7. Specificatii tehnice: conform Caietului de sarcini anexat.

8. Durata contractului de achiziție publică: de la data semnarii contractului de furnizare, de catre ambele parti, pana la 31.12.2021.

9. Valoarea estimata a contractului: 6720,00 lei, fara TVA.

10. Conditii de participare. Ofertantii vor prezenta urmatoarele documente:

- Declaratie pe propria raspundere privind neincadrarea in dispozitiile art. 164 din legea nr. 98/2016;
- Declaratie pe propria raspundere privind neincadrarea in dispozitiile art. 165 si 167 din legea nr. 98/2016;
- Declaratie pe propria raspundere privind neincadrarea in dispozitiile art. 59 si 60 din legea nr. 98/2016;
- Cod Unic de Identificare Fiscala.

11. Perioada de valabilitate a ofertelor: 30 de zile de la data depunerii.

12. Pretul va fi exprimat in lei, fara TVA.

13. Prezentarea ofertei: La oferta de baza nu sunt acceptate oferte parțiale si oferte alternative.

a) Perioada de valabilitate a ofertelor: 30 de zile de la data deschiderii ofertelor. Pretul va fi ferm pe intreaga perioada de derulare a contractului.

b) Modul de prezentare a ofertei tehnice trebuie sa asigure o corespondenta intre aceasta si cerintele impuse prin specificatiile tehnice solicitate de autoritatea contractanta.

c) Modul de prezentare a propunerii financiare – oferta va cuprinde pretul exprimat in lei/pachet, fara TVA si in lei, cu TVA. Preturile unitare in lei, fara TVA din oferta sunt ferme si nu pot fi modificate pe toata durata contractului.

14. Conditii de plata - Plata se va efectua conform Legii nr. 72/2013 privind măsurile pentru combaterea întârzierii în executarea obligațiilor de plată a unor sume de bani rezultând din contracte încheiate între profesioniști și între aceștia și autorități contractante. Nu se accepta plati in avans.

15. Depunerea ofertei - Oferta insotita de documentele solicitate se vor transmite pe email la adresa: achizitii@dspiiasi.ro, pana la data de 08.11.2021, ora 12:00.

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 revinzător.
- 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 aparține aceluiași producător.
- Asigurarea și garantarea actualizării semnăturilor de virus și upgrade la noi versiuni pe întreaga perioadă 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
 - o Mesaje de alerta în cazul apariției unor noi viruși distructivi sau cu potențial mare de răspândire rapidă.
 - o 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):
 - o Intervenție real-time securizată, bazată pe un ticket cu durată limitată de valabilitate.
 - o Contact continuu între inginerul suport tehnic și client prin intermediul unei aplicații de chat inclusă în sesiunea remote.
 - o Vizibilitate totală asupra acțiunilor întreprinse prin aplicația remote.
 - o Posibilitatea clientului de a prelua controlul în orice moment.
 - o Conectare via plug-in web care nu necesită configurări suplimentare în firewall-ul sau serverele clienților.
 - o Nu necesită dezvăluirea parolilor 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 însoțite de certificatele 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/instalate 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 ani cu posibilitatea de prelungire ulterioară.
- Metode de detecție a virusurilor, a programelor spion, a rootkit-urilor, a mesajelor de tip spam, a tentativelor de fraudare de tip phishing și a altor programe cu potențial malițios, 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 automată "on acces" (în timp real) a fișierelor care se copiază de pe suport extern și din LAN sau WAN.
- Scanarea automată "on acces" (în timp real) a fișierelor va putea fi setată să scaneze numai anumite tipuri de fișiere, definite de administrator.
- Scanarea automată "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 virusi 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 dezinfectării într-o serie de formate uzuale (arj, ace, cab, dbx, docfile, zip, 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 pauză și reluare a scanărilor.
- Clienții anti-virus pentru workstation să permită monitorizarea activă a registrelor afișând mesaje de atenționare a utilizatorului în momentul în care o aplicație încearcă să modifice cheile registrelor.
- 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 workstation trebuie să funcționeze atât în cadrul rețelei interacționând cu consola de management cât și în mod standalone cu posibilitatea de actualizare atât din LAN cât 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.

Protecție:

- Protecție completă în timp real a datelor - pentru a combate toate tipurile de amenințări electronice, de la virusi, viermi și troieni la ransomware, exploatarea de tip ziua zero, rootkit-uri și programe spion.
- Prevenire amenințări rețea - capacitate de a detecta și respinge toate amenințările online, de a analiza și identifica activitățile suspecte la nivel de rețea și să fie posibil să se bloca exploatarea, programele malware și atacurile informatice care

utilizează bootnet-uri, precum și atacurile prin forță brută. Datele și confidențialitatea beneficiarului trebuie să fie în siguranță.

- Monitorizare îndeaproape a aplicațiilor 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.
- Blocarea linkurilor infectate cunoscute, protecție anti-phishing, antifrauda, antispam, protecție fișiere.
- Soluția de securitate trebuie să reacționeze imediat la amenințările malware fără a compromite performanța sistemului beneficiarului.
- Tehnologia propusă 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 malițioase 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 memorînd preferințele 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 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 expedit în mod automat, la un număr de minute definit de administrator.
- Produsul anti-virus să permită ștergerea automată a fișierelor duplicate sau a celor din carantină mai vechi de o anumită perioadă, pentru a nu încălca 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 aceleași 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 antiphishing).
- 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.
- Detectia 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:
 - o minim 30 de sarcini de rețea predefinite, pentru o cât mai bună administrare a rețelei;
 - o Instalarea/dezinstalarea programelor (instalate cu MSI installer) de pe stațiile client ;
 - o 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;
 - o Blocare porturi USB;
 - o Trimitere mesaje către utilizatorii stațiilor de lucru;
 - o Oprire și restartare sistem operare;
 - o 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 :
 - o Blocarea accesului la Internet pentru anumiți utilizatori sau grupuri de utilizatori;
 - o Blocarea accesului la Internet pentru anumite aplicații;
 - o Blocarea accesului la Internet pentru anumite perioade de timp;
 - o Blocare pagini web care conțin anumite cuvinte cheie;
 - o Permite acces numai la anumite pagini web specificate de administrator;
 - o Blocarea accesului la aplicații;
- Permite stabilirea a doua tipuri de utilizatori – clienții autorizați, cu acces nelimitat la interfața și setări de 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:
 - o Gruparea clienților după numărul stațiilor sau serverelor care au sau nu au protecția instalată.
 - o Gruparea clienților după numărul stațiilor care au fost excluse de la instalarea protecției.
 - o 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).
- Existența unor multiple șabloane de raportare în vederea auditului (rapoarte personalizate, 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 euristica comportamentala prin simularea unui calculator virtual in interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de viruși necunoscuți prin detectarea codurilor periculoase a căror semnătura nu a fost lansata încă.
- Marcarea „read only” a fișierelor scanate în cadrul aceleiași sesiuni și rescannerarea acestora numai în cazul unei noi sesiuni, update sau infecție în cadrul sistemului.
- Scanare in 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 centralizat 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 mica decât o limita stabilita 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 in 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 ulterioara 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 rescannerarea fișierelor din carantină.
- Soluția trebuie să permită scanarea contextuală.

Intocmit,

Ec. Cristea Florin Septimiu