



ROMÂNIA
TRIBUNALUL MARAMUREȘ

B-dul Republicii nr.2A, Baia Mare, jud. Maramureș, cod poștal: 430264
C.U.I.: 3695026, Tel.: 0262/218235, Fax: 0262/218209

DEPARTAMENTUL ECONOMICO FINANCIAR
Nr. 134 / 16.01.2018

SOLICITARE DE OFERTĂ

Tribunalul Maramureș, cu sediul în Baia Mare, Bd. Republicii nr.2A, județul Maramureș, având codul fiscal 3695026, în calitate de autoritate contractantă, intenționează să achiziționeze antivirus pentru stații de lucru :249 bucati si consola pentru managementul centralizat al produselor antivirus:249 clienti (stații de lucru) administrati din 1 consola, conform caietului de sarcini atasat.

Cod CPV- 48761000- Pachete software antivirus

Documente ce însoțesc produsul:

- certificat de calitate;
- certificat de garanție;
- documente care certifică conformitatea cu cerințele din caietul de sarcini.

Licențele își vor începe perioada de valabilitate după ce expira perioada de valabilitate ale licențelor existente în acest moment instalate pe echipamente.

Procedura de achiziție aplicată este cumpărarea directă, conform dispozițiilor art. 7. alin.5 din Legea 98/2016, privind achizițiile publice, potrivit căreia „ **Autoritatea contractantă are dreptul de a achiziționa direct produse sau servicii în cazul în care valoarea estimată a achiziției, fără TVA, este mai mică decât 132.519 lei**”.

Criteriul utilizat pentru atribuirea contractului: „**prețul cel mai scăzut**”.

Oferta se va transmite prin fax la nr. 0262/218.209 sau pe adresa de email:

aniela.molcsan@just.ro și va conține **propunerea financiară și propunerea tehnică**.

Perioada minimă pe parcursul căreia ofertantul trebuie să își mențină oferta este de 30 zile.

Achizitorul va achita contravaloarea produselor achiziționate, în termen de maximum 30 zile de la recepție.

Oferta se va transmite prin fax la nr. 0262/218.209 sau pe adresa de email:

Aniela.molcsan@just.ro și va conține **propunerea financiară și propunerea tehnică. Ofertanții vor fi înscriși obligatoriu în sistemul SEAP.**

Data limită până la care se pot solicita clarificări: 18.01.2018, ora 1200.

Data limită pentru transmiterea ofertei: 18.01.2018, ora 1500.

Pentru informații suplimentare ne puteți contacta la telefon:

0262/218235 int 212 sau 0744643351, persoană de contact: consilier Aniela Molcsan.

PREȘEDINTE

Cristina Laura Lihet

MANAGER ECONOMIC

Monica Indre



Caiet de sarcini

pentru achiziționarea serviciilor de protecție de tip antivirus Bitdefender Gravityzone
pentru
Tribunalul Maramureș și instanțele de judecată arondate acestuia

Se dorește achiziționarea de servicii de protecție de tip antivirus cu instalarea produselor antivirus necesare la nivelul Tribunalului Maramureș precum și în instanțele subordonate, respectiv Judecătoria Baia Mare, Judecătoria Sighetu Marmăției, Judecătoria Vișeu de Sus, Judecătoria Dragomirești și Judecătoria Târgu Lăpuș, cu licență pentru acces la servicii specifice până la sfârșitul anului 2018, având, componente pentru protecția stațiilor de lucru, componente pentru managementul centralizat (remote) al soluției antivirus stațiilor de lucru, după cum urmează:

- antivirus pentru stații de lucru: **249 bucăți**;
- consola pentru managementul centralizat al produselor antivirus: **249 clienți** (stații de lucru) administrați din 1 consola;

Serviciile achiziționate vor fi oferite sub forma unui pachet care include:

- dreptul de utilizare a unui produs antivirus care să respecte cerințele de mai jos;
- dreptul de utilizare a 1 consola de management centralizat pentru administrarea clienților;
- servicii de actualizare a semnăturilor produsului antivirus pus la dispoziție;
- servicii de suport tehnic pentru instalarea, configurarea, depanarea și devirusarea în caz de nevoie.

Serviciile achiziționate vor oferi protecție împotriva malware (virusi, spyware, worms, tojans, rootkit, a mesajelor de tip spam, a tentativelor de fraudare de tip phishing și a altor coduri periculoase) pentru întreaga rețea a Tribunalului Maramureș și a instanțelor de judecată.

Ofertantul va furniza servicii de protecție de tip antivirus cu management centralizat pentru servere și stații de lucru, respectând următoarele cerințe tehnice minime:

| Caracteristici tehnice minime | |
|---|--|
| Condiții generale | Pune la dispoziția beneficiarilor cel puțin următoarele module/servicii: <ul style="list-style-type: none">- consolă de management centralizat (asigură funcționalități de administrare);- protecție antivirus, antispam, antispayware, antimalware, antiphishing, antirootkit, firewall pentru stații de lucru, laptop-uri;- Servicii de actualizare soluție antivirus; |
| Cerințe minime generale ale produsului antivirus pus la dispoziție | |
| Condiții generale | Produsul antivirus pus la dispoziție trebuie să fie certificat VB100¹ sau echivalent în ultimele 12 luni. |
| | Produsul antivirus pus la dispoziție trebuie să aibă impact minim (sub 10%) asupra performanțelor sistemului pe care este |

¹ VB100 – Certificat acordat de compania *Virus Bulletin*

| | |
|---------------------------------|--|
| | <p>instalat. In acest sens furnizorul va prezenta rezultatele obținute la testele de performanță realizate de organizații independente care au ca specific testarea și verificarea software-ului de securitate (ex. AV-Comparatives, AV-Test.org, Virus Bulletin etc.),</p> |
| Funcționalități | <p>Soluția îndeplinește cel puțin următoarele roluri:</p> <ul style="list-style-type: none"> - Server bază de date; - Server web pentru consola centrală de administrare; - Server pentru comunicarea cu rețeaua de agenți ce rulează pe terminalele protejate; - Server pentru actualizări. |
| | <p>Soluția va permite detecția și prevenirea intruziunilor (prin funcționalități de tip IDS² și IPS³), de blocare a unor port-uri de rețea, de identificare și blocare a aplicațiilor malware (atât cele care sunt rulate de pe hard-disk, cât și cele rezidente în memorie).</p> |
| Actualizare | <p>Permite actualizarea (automată) de pe Internet a semnăturilor antivirus și IDS, precum și offline prin instalarea manuală a unor pachete descărcate.</p> |
| Instalare și funcționare | <p>Permite scanarea și identificarea aplicațiilor malițioase utilizând o bază de date cu semnături, analiză euristică și pe bază de reputație.</p> <p>Permite administrarea de la distanță și crearea de roluri de administrare.</p> <p>Permite scanarea dispozitivelor amovibile (CD/DVD-uri, dispozitive USB) în momentul imediat conectării acestora, pentru a identifica și elimina amenințările în mod proactiv, pentru a bloca scrierea sau transferul unor aplicații malițioase dinspre și către aceste dispozitive și pentru blocarea funcționalității de „Autorun”.</p> <p>Agenții software instalați la nivelul terminalelor (stații de lucru, laptop-uri, servere) dețin capabilități de firewall local cu funcții de filtrare a pachetelor și blocare la nivel aplicație. Instalarea agenților software se realizează în mod centralizat.</p> <p>Agenții software instalați la nivelul terminalelor permit scanarea traficului de e-mail (cel puțin SMTP, POP3, IMAP și NNTP), web, peer-to-peer (de tip torrent și DirectConnect), precum și cel generat de aplicații de tipul „Instant Messaging” pentru identificarea aplicațiilor/codurilor malițioase.</p> <p>Previne execuția automată a aplicațiilor descărcate și previne modificarea fișierelor aferente sistemului de operare.</p> <p>Permite scanarea și sanitizarea resurselor partajate în rețea.</p> <p>După identificarea aplicațiilor malware, soluția întreprinde următoarele acțiuni:</p> <ul style="list-style-type: none"> - mutare în carantină; - dezinfecție sau ștergere. <p>Soluția permite restaurarea fișierelor aflate în carantină.</p> |
| Utilizatori | <p>Permite administrarea pe bază de roluri.</p> <p>Permite roluri multiple predefinite (cel puțin):</p> <ul style="list-style-type: none"> - <i>administrator global</i>: administrează întreaga soluție de protecție la nivel „end-point”; - <i>administrator</i>: administrează serviciile de securitate; |

² IDS – Intrusion Detection System.

³ IPS – Intrusion Prevention System.

| | |
|--|---|
| | <ul style="list-style-type: none"> - <i>dispecer</i>: rol de tip read-only care monitorizează statusul de securitate și analizează rapoarte; - roluri personalizate pentru care se pot defini un anumit set de drepturi. |
| | Permite importul utilizatorilor din Microsoft Active Directory. |
| Politici de securitate | <p>Oferă șabloane de politici de securitate, dedicate pentru fiecare serviciu.</p> <p>Fiecare serviciu de securitate conține un șablon propriu cu opțiuni specifice de activare/dezactivare și configurarea funcționalităților precum scanarea antivirus, firewall cu opțiunea de prevenire a intruziunilor, accesul controlat la rețea, controlul aplicațiilor, accesul la Internet, criptare, localizarea dispozitivelor, forțarea autentificării și acțiuni ce pot fi întreprinse în cazul unor viruși sau a unor dispozitive neconforme detectate, precum blocarea de la distanță, deblocarea, ștergerea definitivă a datelor etc.</p> |
| CertIFICATE | <p>Accesul la consola centrală de management se realizează în mod securizat, prin HTTPS.</p> <p>Serverul web, din consola centrală de management, permite importul de certificate digitale eliberate de o autoritate de certificare autorizată sau proprie organizației.</p> <p>Certificatele digitale, odată importate, oferă posibilitatea înlocuirii acestora în caz de expirare sau de revocare.</p> |
| Raportare | <p>Permite definirea de rapoarte programabile.</p> <p>Rapoartele programabile pot fi trimise către adrese de email.</p> <p>Permite implementarea de filtre pentru rapoartele programabile în scopul obținerii de informații relevante pentru fiecare utilizator.</p> <p>Oferă posibilitatea de arhivare a acestor rapoarte.</p> <p>Permite exportul rapoartelor programabile în formatele PDF și CSV.</p> |
| Cerințe minime pentru consola de management | |
| Generalități | <p>Consola prezintă un panou de comandă central configurabil (dashboard).</p> <p>Consola trebuie să fie compatibilă cel puțin cu următoarele tipuri de browsere web:</p> <ul style="list-style-type: none"> - Internet Explorer 9+; - Mozilla Firefox 20+; - Google Chrome 20+; <p>Panoul central cuprinde o secțiune de analiză, prin intermediul căreia furnizează informații de securitate specifice rețelei.</p> <p>La nivel de rețea, consola permite instalarea de module de protecție, implementarea de politici privind setările de securitate, rularea de task-uri de la distanță, crearea, adăugarea și ștergerea de rapoarte.</p> |
| Instalare și administrare | <p>Pachetele de instalare aferente serviciilor de securitate pot fi instalate/dezinstalate în mod centralizat, de la distanță.</p> <p>Consola oferă informații detaliate privind obiectele, serviciile și administrarea din interiorul rețelei:</p> <ul style="list-style-type: none"> - numele stațiilor sau ale terminalelor; - adresă IP; - sistem de operare; - grup; - politica de securitate aplicată; - module instalate; - ultimele informații despre viruși; - ultimele rapoarte de scanare; |

| | |
|-------------------------------|---|
| | <p>- informații despre actualizări.</p> <p>Consola oferă posibilitatea de a comanda de la distanță execuția de acțiuni (precum repornirea, scanarea antivirus, ș.a.) pe terminalele protejate.</p> <p>Oferă informații detaliate despre fiecare task.</p> <p>Permite gestionarea de la distanță a fișierelor aflate în carantină.</p> <p>Oferă informații legate de certificate:</p> <ul style="list-style-type: none"> - nume; - autoritatea emitentă; - data eliberării certificatelor; - data expirării certificatelor eliberate. |
| Politici de securitate | <p>Consola permite crearea și gestionarea de politici de securitate.</p> <p>Consola permite configurarea detaliată a drepturilor administrative, permițând selectarea serviciilor și a obiectelor pentru care un utilizator poate face modificări.</p> <p>Soluția permite deconectarea automată a oricărui tip de utilizator după o perioadă de timp specifică, pentru o protecție sporită a datelor afișate în consola de administrare.</p> <p>Din consolă se trimite o singură politică pentru configurarea integrală a antivirusului de pe stații, servere și dispozitive mobile.</p> <p>În funcție de rolul îndeplinit de către utilizator, fiecărui cont i se indică pentru ce grupuri de utilizatori din consolă se dețin drepturi de modificare a setărilor sau de generare a rapoartelor.</p> |
| Logging și notificări | <p>Oferă un serviciu de notificări care permite transmiterea acestora către una sau mai multe adrese de email, evidențierea notificărilor necitite, alertarea administratorului în cazul unor probleme majore:</p> <ul style="list-style-type: none"> - licențiere; - viruși; - mașini neactualizate. <p>Permite înregistrarea (logging) acțiunilor utilizatorilor și oferă informații detaliate pentru fiecare dintre acestea:</p> <ul style="list-style-type: none"> - logare/delogare; - creare/editare/ștergere rapoarte; - creare/editare/ștergere detalii de autentificare; - creare task-uri; - creare/editare/ștergere/redenumire conturi utilizatori; - ștergere/restaurare fișiere carantină; - creare/editare/ștergere politici de securitate. <p>Permite filtrarea acțiunilor utilizatorilor după câmpuri precum: numele utilizatorului și acțiune.</p> |
| Raportare | <p>Panoul central conține rapoarte pentru toate modulele suportate.</p> <p>Rapoartele din panoul de monitorizare pot fi configurate specificând numele, tipul de raport, ținta raportului, opțiuni specifice pentru orice tip de raport (de exemplu pentru raportul de actualizare - care este intervalul după care o stație este considerată neactualizată).</p> <p>Oferă o modalitate de raportare cu privire la securitatea clienților din rețea.</p> <p>Consola de management permite raportarea numărului stațiilor de lucru care au instalată soluția de protecție antivirus.</p> |

| Cerințe minime pentru protecția la nivel de stații fizice, laptop-uri și servere | |
|--|--|
| Caracteristici generale | Soluția antivirus permite instalarea personalizată a modulelor deținute (de ex: să permită instalarea antivirus fără modulul de control al accesului web sau modulul firewall). |
| Cerințe minime privind sistemele de operare suportate | Permite instalarea pe cel puțin următoarele sisteme de operare pentru stații: <ul style="list-style-type: none"> - Windows 10; - Windows 8; - Windows 7; - Windows Vista; - Windows XP (SP3). |
| | Permite instalarea pe cel puțin următoarele sisteme de operare pentru servere: <ul style="list-style-type: none"> - Windows Server 2012; - Windows Server 2008; - Windows Server 2008 R2; - Windows Server 2003; - |
| Administrare și instalare remote | Oferă posibilitatea de particularizare a pachetelor de instalare cu modulele dorite: firewall, content control. |
| | Instalarea poate fi realizată cel puțin prin următoarele moduri: <ul style="list-style-type: none"> - prin descărcarea directă a pachetului antivirus pe stația pe care se face instalarea; - prin instalarea la distanță, direct din consola web. |
| | Posibilitatea creării unui singur pachet de instalare compatibil atât pentru sistemele de operare pe 32 de biți cât și pentru cele pe 64 de biți. |
| | Posibilitatea de a crea grupuri (sau subgrupuri), unde administratorul poate muta stațiile sau serverele din rețea. |
| Caracteristici și funcționalități principale ale modulului antivirus și antispyware | Scanarea automată în timp real poate fi setată să nu scaneze arhive sau fișiere mai mari de „x” MB, mărimea fișierelor putând fi definită de administratorul soluției. |
| | Oferă posibilitatea de definire a unor nivele de profunzime pentru scanarea în arhive. |
| | Oferă posibilitatea scanării euristice comportamentale prin rularea aplicațiilor cu potențial periculos în interiorul unei mașini virtuale de tip sandbox. Astfel, se realizează protecția rețelei împotriva virusilor necunoscuți prin detecția codurilor periculoase a căror semnătură nu a fost publicată încă. |
| | Oferă posibilitatea de scanare la cerere și în momentul accesării oricărui suport de stocare a informației (CD-uri, harduri externe, unități partajate etc.). |
| | Permite configurarea căilor ce urmează a fi scanate, inclusiv la nivel de fișiere. |
| | Clienții antivirus pentru stații trebuie să permită definirea unor liste de excludere de la scanarea în timp real și, la cerere, a anumitor directoare, discuri, fișiere, extensii sau procese. |
| | Protecția anti-spyware trebuie să fie asigurată cu ajutorul euristicii de detecție și a unei baze de date cu semnături de spyware. |
| | Oferă posibilitatea de rulare a scanărilor programate cu prioritate redusă și cu posibilitatea de oprire automată a stației după terminarea scanării. |
| | Conține cel puțin 3 tipuri de detecție bazate pe: |

| | |
|--|---|
| | <ul style="list-style-type: none"> - semnături; - comportamentul fișierelor; - monitorizarea proceselor. |
| | Permite scanarea traficului HTTP/HTTPS. |
| | Include opțiunea de setare a unei parole pentru protecția la dezinstalare, pentru o mai bună gestionare a antivirusului instalat pe stații. |
| | Include un modul de antiphishing care deține și opțiunea de verificare a link-urilor rezultate din motoarele de căutare. |
| Firewall | Permite tipul de lucru „invizibil” la nivelul rețelei locale sau Internet. |
| | Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului. |
| | Modulul include opțiunea de Intrusion Detection System (IDS) configurabil pe nivele multiple. |
| Protecția datelor | Permite blocarea datelor confidențiale (pin-ul cardului, cont bancar etc.) transmise prin HTTP sau SMTP, prin crearea unor reguli specifice. |
| Carantină | Permite utilizatorului să decidă dacă se transmit fișierele aflate în carantină către laboratoarele antivirus ale producătorului. |
| | Trimiterea conținutului carantinei poate fi realizată în mod automat, la un interval de timp definit de administrator sau poate fi inhibată permanent. |
| | Permite ștergerea automată a fișierelor din carantină care sunt mai vechi de o perioadă specificată, pentru a nu încălca inutil spațiul de stocare. |
| | Permite mutarea unui fișier din carantină în locația lui originală. |
| | Carantina permite rescannerarea obiectelor după fiecare actualizare de semnături. |
| Controlul utilizatorului | <p>Consola are integrat un modul dedicat controlului utilizatorilor cu cel puțin următoarele particularități:</p> <ul style="list-style-type: none"> - blocarea accesului la Internet pentru anumiți clienți sau grupuri de clienți; - blocarea accesului la Internet pentru anumite perioade de timp; - blocarea paginilor de Internet care conțin anumite cuvinte cheie; - permiterea accesului numai la anumite pagini web specificate de administrator; - blocarea accesului la anumite aplicații definite de administrator; - restricționarea accesului la anumite pagini web după anumite categorii prestabilite (ex: online dating, violence). |
| Cerințe minimale pentru serviciile de actualizare a semnăturilor produsului antivirus pus la dispoziție | |
| Actualizare | Posibilitatea actualizării la nivel de stație în mod transparent (fără avertizare). |
| | Sistem de actualizare folosind mai multe servere înlanțuibile. |
| | Actualizarea locațiilor remote, prin intermediul altor clienți ce pot avea rol și de server de update. |
| | Antidot sub forma de semnături sau aplicație separată pentru orice nou produs malware în maxim 24 de ore de la infectare |
| | Actualizare zilnică a semnăturilor de virus, prin Internet, automata sau comandată, a stațiilor și a server-elor de |

| | |
|--|---|
| | management a soluției de securizare din fiecare LAN care are conexiune la Internet |
| Cerințe minimale pentru serviciile de suport tehnic | |
| Furnizorul va asigura suport tehnic astfel | <ul style="list-style-type: none"> - va pune la dispoziția achizitorului procedura de instalare și configurare pentru produsul antivirus, consola de management și ghidul de utilizare a acestora, pentru instalarea și configurarea produsului antivirus și a consolei de management de către specialistii Beneficiarului și va acorda suport pentru rezolvarea unor probleme deosebite care presupun reconfigurarea sau customizarea soluției antivirus. Serviciile se vor furniza în principal de la distanță. - Procedura de instalare și configurare pentru produsul antivirus, consola de management și ghidul de utilizare a acestora vor fi furnizate în maxim o săptămână de la semnarea contractului. - telefonic, e-mail sau Internet - 24/24. În oferta tehnică și comercială furnizorul va prezenta numerele de telefon, adresele de email sau adresa de Internet la care beneficiarul poate accesa serviciile de suport tehnic - Echipă de suport tehnic specializată pentru situații excepționale (aceasta va interveni doar atunci când pentru rezolvarea unor probleme deosebite se impune reconfigurarea sau customizarea soluției antivirus de către dezvoltator sau personal acreditat de către producătorul soluției). |

Serviciul va fi prestat la sediul Tribunalului Maramures în maxim o săptămână de la semnarea contractului.

Termenul de livrare a licențelor este de 1 săptămână de la semnarea contractului.

Saitos Felicia

Specialist IT șef

