ROMÂNIA
TRIBUNALUL BISTRIŢA-NĂSĂUD
Bistriţa, str. Alba Iulia, nr. 1, tel. 0263-213528, fax. 0263-230491, e-mail trbn@just.ro

Operator de date cu caracter personal nr. 11795
Departamentul ec.financiar şi administrativ
Nr. 307 din 02.02.2018

SOLICITARE DE OFERTĂ

Tribunalul Bistriţa-Năsăud, cu sediul în Bistriţa, Strada Alba Iulia, nr.1, Judeţul Bistriţa-Năsăud, având codul fiscal 4426832, în calitate de autoritate contractantă, intenţionează să **achiziţioneze pe SEAP servicii de protecţie de tip antivirus** conform caietului de sarcini anexat, cu încheierea unui contract pe o perioadă de un an, cu posibilitatea de prelungire conform legislaţiei în vigoare,

sens în care vă invită să depuneţi oferta d-voastră de preţ în data de **07.02.2018**, ora **10.00**.

Modalitatea de achiziţie este **cumpărarea directă**, conform dispoziţiilor **art. 7 alin. 5 din Legea nr. 98/2016** privind achiziţiile publice, cu respectarea cerinţelor tehnice din caietul de sarcini.

Criteriul aplicat în vederea finalizării achiziţiei este **„preţul cel mai scăzut"**. Oferta se va transmite prin fax la nr. 0263/230491 sau pe adresa de email simona.pavelea@just.ro şi va conţine propunerea financiară în care se va evidenţia, punctual şi complet, fiecare cerinţă din caietul de sarcini. Oferta va fi însoţită de certificatul de garanţie şi certificatul de calitate.

Perioada minimă pe parcursul căreia ofertantul trebuie să îşi menţină oferta este de 30 zile.

Data limită până la care se pot solicita clarificări: **07.02.2018, ora 08.00.**

Data limită pentru transmiterea ofertei : **07.02.2018**, ora **10.00**.

Pentru informaţii suplimentare ne puteţi contacta la telefon 0263/213.528 interior 125, persoana de contact : consilier Pavelea Simona.

PREŞEDINTE,
Preda Liliana Elisabeta

MANAGER ECONOMIC,
Andreieş Maria Adriana

ÎNTOCMIT,
Pavelea Simona

ROMÂNIA
TRIBUNALUL BISTRIŢA-NĂSĂUD
Bistriţa, str. Alba Iulia, nr. 1, tel. 0263-213528, fax. 0263-230491, e-mail trbn@just.ro

Biroul IT

Aprobat,

PREŞEDINTE,
jud. dr. PREDA LILIANA ELISABETA

CAIET DE SARCINI

pentru achiziționarea serviciilor de protecție de tip antivirus pentru Tribunalul Bistriţa-Năsăud și Judecătoriile Bistriţa, Năsăud, Beclean

Se dorește achiziționarea de servicii de protecție de tip antivirus cu instalarea produselor antivirus necesare la nivelul Tribunalului Bistriţa-Năsăud și a Judecătoriilor Bistriţa, Năsăud, Beclean, cu licență pentru acces la servicii specifice pentru o perioadă de un an, având componente pentru protecția serverelor de fișiere, componente pentru protecția stațiilor de lucru, componente pentru managementul centralizat (remote) al soluției antivirus servere și stații de lucru, după cum urmează:

- antivirus pentru servere de fișiere: **18 bucăți;**
- antivirus pentru stații de lucru: **215 bucăți;**
- o consolă pentru managementul centralizat al produselor antivirus: **233 clienți** (stații de lucru și servere) din cele 4 instanțe distincte;

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

- dreptul de utilizare a unui produs antivirus care să respecte cerințele de mai jos;
- dreptul de utilizare a consolei 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.

Produsele antivirus, produsele software terțe și consola de management vor fi asigurate de către ofertant, fără costuri suplimentare, urmând ca la finalizarea contractului accesul beneficiarilor la acestea și dreptul de utilizare al acestora să înceteze (software-ul va fi șters de pe calculatoarele și serverele unde se afla instalat).

Serviciile achiziționate vor oferi protecție împotriva malware (viruși, spyware, worms, trojans, rootkit, a mesajelor de tip spam, a tentativelor de fraudare de tip phishing și a altor coduri periculoase) pentru întreaga rețea a Tribunalului Bistriţa-Năsăud și a Judecătoriilor Bistriţa, Năsăud, Beclean.

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

Caracteristici tehnice minimale	
Condiţii generale	Pune la dispoziția beneficiarilor cel puțin următoarele module/servicii: - consolă de management centralizat (asigură funcționalități de administrare); - protecție antivirus, antispam, antispyware, antimalware, antiphishing, antirootkit, firewall pentru stații de lucru, laptop-uri şi servere fizice; - protecţie antivirus, antispam, antispyware, antimalware, antiphishing, antirootkit, firewall pentru staţii şi servere virtualizate; - Servicii de actualizare soluție antivirus;
Cerințe minimale generale ale produsului antivirus pus la dispoziție	
Condiţii generale	Produsul antivirus pus la dispoziție trebuie să fie **certificat VB100**[1] **sau echivalent** în ultimele 12 luni.
	Produsul antivirus pus la dispoziție trebuie să aibă impact minim (sub 10%) asupra performantelor sistemului pe care este instalat. In acest sens furnizorul va prezenta **rezultatele obţinute la testele de performanță** realizate de organizații independente care au ca specific testarea si verificarea software-lui de securitate (ex. **AV-Comparatives, AV-Test.org, Virus Bulletin etc**.),
	Pachetul de instalare trebuie să fie livrat ca o maşină virtuală ce conţine toate rolurile / serviciile necesare sau ca un kit ce permite instalarea rolurilor / serviciilor şi în maşini virtuale.
	Suportă cel puțin următoarele platforme de virtualizare: - Microsoft Hyper-V;
Funcționalități	Soluția îndeplineşte cel puțin următoarele roluri: - Server bază de date; - Server web pentru consola centrală de administrare; - Server pentru comunicarea cu reţeaua de agenţi ce rulează pe terminalele protejate; - Server pentru actualizări.
	Soluția va permite detecţia şi prevenirea intruziunilor (prin funcționalități de tip IDS[2] şi IPS[3]), de blocare a unor port-uri de rețea, de identificare şi blocare a aplicaţiilor malware (atât cele care sunt rulate de pe hard-disk, cât şi cele rezidente în memorie).
Actualizare	Permite actualizarea (automată) de pe Internet a semnăturilor antivirus şi IDS, precum şi offline prin instalarea manuală a unor pachete descărcate.
Instalare și funcționare	Permite scanarea și identificarea aplicațiilor malițioase utilizând o bază de date cu semnături, analiză euristică şi pe bază de reputaţie.
	Permite administrarea de la distanţă şi crearea de roluri de administrare.
	Permite scanarea dispozitivelor amovibile (CD/DVD-uri, dispozitive USB) în momentul imediat conectării acestora, pentru a identifica şi elimina ameninţările în mod proactiv, pentru a bloca scrierea sau transferul unor aplicaţii maliţioase dinspre şi către aceste dispozitive şi pentru blocarea funcţionalităţii de „Autorun".
	Agenţii software instalaţi la nivelul terminalelor (staţii de lucru, laptop-uri, servere) deţin capabilităţi de firewall local cu funcţii de filtrare a pachetelor şi blocare la nivel aplicaţie. Instalarea agenţilor software se realizează în mod centralizat.
	Agenţii software instalaţi la nivelul terminalelor permit scanarea

[1] *VB100* – Certificat acordat de compania *Virus Bulletin*
[2] *IDS* – Intrusion Detection System.
[3] *IPS* – Intrusion Prevention System.

	traficului de e-mail (cel puţin SMTP, POP3, IMAP şi NNTP), web, peer-to-peer (de tip torrent şi DirectConnect), precum şi cel generat de aplicaţii de tipul „Instant Messaging" pentru identificarea aplicaţiilor/codurilor maliţioase.
	Previne execuția automată a aplicațiilor descărcate și previne modificarea fișierelor aferente sistemului de operare.
	Permite scanarea şi sanitizarea resurselor partajate în rețea.
	După identificarea aplicaţiilor malware, soluţia întreprinde următoarele acțiuni: - mutare în carantină; - dezinfecţie sau ştergere. Soluția permite restaurarea fișierelor aflate în carantină.
Inventarierea rețelei	Soluția permite, cel puţin integrarea cu Active Directory şi importă inventarul din această platformă. Pentru integrarea cu Active Directory, se poate defini şi intervalul (în ore) de sincronizare.
	Permite descoperirea stațiilor fizice neintegrate in Active Directory (Workgroup) cu ajutorul operațiunilor de tipul Network discovery.
	Oferă opțiuni de căutare, sortare și filtrare după: - numele sistemului; - tipul sistemului de operare; - după adresa IP.
	Oferă posibilitatea de creare și configurare de sarcini centralizate.
Utilizatori	Permite administrarea pe bază de roluri.
Politici de securitate	Oferă șabloane de politici de securitate, dedicate pentru fiecare serviciu.
Acces consolă	Accesul la consola centrală de management se realizează în mod securizat, prin HTTPS.
Raportare	Permite definirea de rapoarte programabile.
	Rapoartele programabile pot fi trimise către adrese de email.
	Permite implementarea de filtre pentru rapoartele programabile în scopul obținerii de informații relevante pentru fiecare utilizator.
	Permite exportul rapoartelor programabile în formatele PDF şi CSV.
Cerințe minimale pentru consola de management	
Generalități	Consola prezintă un panou de comandă central configurabil (dashboard).
	Consola trebuie să fie compatibilă cel puțin cu următoarele tipuri de browsere web: - Internet Explorer 9+; - Mozilla Firefox 40+; - Google Chrome 40+;
	Panoul central cuprinde o secțiune de analiză, prin intermediul căreia furnizează informații de securitate specifice rețelei.
	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.
Instalare și administrare	Pachetele de instalare aferente serviciilor de securitate pot fi instalate/dezinstalate în mod centralizat, de la distanță.
	Consola oferă informații detaliate privind obiectele, serviciile și administrarea din interiorul rețelei: - 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; - informații despre actualizări.
	Consola oferă posibilitatea de a comanda de la distanță execuția de acțiuni (precum repornirea, scanarea antivirus, ș.a.) pe terminalele protejate.
	Oferă informații detaliate despre fiecare task.
	Permite gestionarea de la distanță a fișierelor aflate în carantină.
Politici de securitate	Consola permite crearea și gestionarea de politici de securitate.
	Oferă posibilitatea de implementare centralizată a politicilor pe mașinile fizice, virtuale şi mobile.
	Consola permite configurarea detaliată a drepturilor administrative, permițând selectarea serviciilor și a obiectelor pentru care un utilizator poate face modificări.
	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.
	Din consolă se trimite o singură politică pentru configurarea integrală a antivirusului de pe stații, servere şi dispozitive mobile.
	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.
Logging și notificări	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: - licențiere; - viruși; - mașini neactualizate.
	Permite înregistrarea (logging) acțiunilor utilizatorilor și oferă informații detaliate pentru fiecare dintre acestea: - logare/delogare; - creare/editare/ştergere rapoarte; - creare/editare/ştergere detalii de autentificare; - creare task-uri; - creare/editare/ştergere/redenumire conturi utilizatori; - ştergere/restaurare fişiere carantină; - creare/editare/ştergere politici de securitate.
	Permite filtrarea acțiunilor utilizatorilor după câmpuri precum: numele utilizatorului și acțiune.
Raportare	Panoul central conține rapoarte pentru toate modulele suportate.
	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).
	Oferă o modalitate de raportare cu privire la securitatea clienților din rețea.
	Consola de management permite raportarea numărului stațiilor de lucru care au instalată soluția de protecție antivirus.
Cerințe minimale 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: - Windows 10; - Windows 8;

	- Windows 7; - Windows Vista; - Windows XP (SP3).
	Permite instalarea pe cel puţin următoarele sisteme de operare pentru servere: - 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: - prin descărcarea directă a pachetului antivirus pe stația pe care se face instalarea; - prin instalarea la distanță, direct din consola web.
	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 maşini virtuale de tip sandbox. Astfel, se realizează protecţia rețelei împotriva virușilor necunoscuți prin detecţia 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 puţin 3 tipuri de detecție bazate pe: - 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 deţine 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 încărca inutil spațiul de stocare.
	Permite mutarea unui fișier din carantină în locația lui originală.
	Carantina permite rescanarea obiectelor după fiecare actualizare de semnături.
Controlul utilizatorului	Consola are integrat un modul dedicat controlului utilizatorilor cu cel puțin următoarele particularități: - 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 înlănțuibile.
	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 serverelor de management a soluției de securizare din fiecare LAN care are conexiune la Internet
Protecția la nivel de medii virtualizate	
Cerințe minimale	Platforme de virtualizare suportate (cel puțin): - Microsoft Hyper-V Server 2012.
	Oferă protecție pentru cel puțin următoarele sisteme de operare: - Windows Server 2012; - Windows Server 2008; - Windows Server 2008 R2; - Windows Server 2003; - Windows Server 2003 R2; - Windows 8; - Windows 7; - Windows Vista; - Windows XP (SP3);
Cerințe minimale pentru serviciile de suport tehnic	
Furnizorul va asigura suport tehnic astfel	- 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 specialiștii Beneficiarului si va acorda

	suport pentru rezolvarea unor probleme deosebite care presupun reconfigurarea sau customizarea soluției antivirus. Serviciile se vor furniza in principal de la distanta. - Procedura de instalare și configurare pentru produsul antivirus, consola de management și ghidul de utilizare a acestora vor fi furnizate in 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). Cel puțin unul din specialiștii producătorului soluției antivirus sau cei ai furnizorului/ofertantului, care vor asigura suport tehnic la implementarea soluției antivirus trebuie să fie certificat în unul din sistemele de operare desktop și unul din sistemele de operare server pe care va rula produsul. Cerința poate fi îndeplinita cumulativ de către doi specialiști, unul certificat în unul din sistemele de operare desktop și un altul certificat in unul din sistemele de operare de tip server, menționate în Caietul de Sarcini.

Serviciul va fi prestat la sediul Tribunalului Bistriţa-Năsăud în maxim o săptămână de la finalizarea achiziţiei pe SEAP.

Termenul de livrare a serviciilor de protecţie de tip antivirus este de o săptămână de la finalizarea achiziţiei pe SEAP.

Cerinţe suplimentare:

- **Ofertele vor evidenţia, punctual şi complet, fiecare cerinţă.**

Manager Economic,
Andreieş Maria Adriana

Întocmit,
Zegrean Gabriel-specialist IT

Pavelea Simona-consilier achiziţii