ROMÂNIA
Tribunalul Sălaj

DEPARTAMENTUL ECONOMICO FINANCIAR ŞI ADMINISTRATIV

Nr. 217 din 14 ianuarie 2019

PREŞEDINTE
JUDECĂTOR HODIŞ IOANA DIANA

SOLICITARE DE OFERTĂ

Tribunalul Sălaj, cu sediul în municipiul Zalău, strada T.Vladimirescu, nr.10, având codul fiscal 4792205, în calitate de autoritate contractantă, intenţionează să achiziţioneze, în ziua de 17 ianuarie 2019, **servicii de protecţie de tip antivirus pentru Tribunalul Sălaj şi instanţele arondate acestuia, Cod CPV:48761000-0 "Pachete software antivirus", conform Caietului de sarcini anexat.**

Documentele care însoţesc produsul :

- certificat de calitate;
- certificat de garanţie;
- documente care certifică conformitatea cu cerinţele din Caietul de sarcini.

Procedura de achiziţie aplicată este cumpărarea directă, conform dispoziţiilor art.7 alin.5 din Legea.nr.98/2016, privind achiziţiile publice.

Achizitorul va achita contravaloarea serviciilor achiziţionate în termen de maxim 30 zile de la recepţia acestora.

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

Criteriul utilizat pentru atribuirea contractului: **„ preţul cel mai scăzut",** cu respectarea cerinţelor din Caietul de sarcini.

Oferta se va transmite prin fax la nr.0260-611085 sau prin adresa de e-mail anuta.petre@just.ro şi va conţine propunerea financiară şi propunere tehnică. Ofertanţii vor fi înscrişi obligatoriu în SEAP.

Data limită până la care se pot solicita clarificări: **16.01.2019, ora 16^{00}.**

Data limită pentru transmiterea ofertei: **17.01.2019, ora 10^{00}.**

Pentru informaţii suplimentare ne puteţi contacta la telefon 0260-611085, persoană de contact Petre Anuţa, consilier achiziţii publice.

MANAGER ECONOMIC,
ŞTIRB ILEANA

CONSILIER SUPERIOR,
PETRE ANUŢA

TRIBUNALUL SĂLAJ

Zalău, str. Tudor Vladimirescu, nr. 10, judeţul Sălaj,
telefon/fax 0260611085, e-mail:trsj@just.ro

APROBAT:

PREŞEDINTE,
HODIŞ IOANA DIANA

ROMANIA MINISTERUL JUSTIŢIEI TRIBUNALUL SĂLAJ

CAIET DE SARCINI

pentru achiziţionarea serviciilor de protecţie de tip antivirus pentru instanţele de judecată : Tribunalul Sălaj, Judecătoria Zalău, Judecătoria Şimleu SIlvaniei şi Judecătoria Jibou

Se doreşte achiziţionarea de servicii de protectie de tip antivirus cu instalarea produselor antivirus necesare la nivelul instanţele de judecată din judeţul Sălaj, cu licenţă pentru acces la servicii specifice până la sfârşitul anului 2019, având componente pentru protecţia serverelor de fişiere, componente pentru protecţia staţiilor de lucru, componente pentru managementul centralizat (remote) al soluţiei antivirus servere şi staţii de lucru, după cum urmează:

- antivirus pentru servere de fişiere: **12 bucăţi;**
- antivirus pentru staţii de lucru: 135 **bucăţi;**
- consola pentru managementul centralizat al produselor antivirus: 147 **clienţi** (staţii de lucru şi servere) administraţi prin intermediul unei (1) console;

Serviciile achiziţionate vor fi ofertate sub forma unui pachet care include:
- dreptul de utilizare a unui produs antivirus care să respecte cerinţele de mai jos;
- dreptul de utilizare a unei console de management centralizat pentru administrarea clienţilor;
- servicii de actualizare a semnăturilor produsului antivirus pus la dispoziţie;
- servicii de suport tehnic pentru instalarea, configurarea, depanarea şi devirusarea în caz de nevoie.

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

Serviciile achizitionate vor oferi protectie împotriva malware (viruşi, spyware, worms, tojans, rootkit, a mesajelor de tip spam, a tentativelor de fraudare de tip phishing şi a altor coduri periculoase) pentru întreaga reţea a Ministerului Justiţiei şi a instantelor de judecata.

Ofertantul va furniza servicii de protecţie de tip antivirus cu management centralizat pentru servere şi staţii de lucru, respectând următoarele cerinţe tehnice minimale:

Caracteristici tehnice minimale	
Condiţii generale	Pune la dispoziţia beneficiarilor cel puţin următoarele module/servicii: - consolă de management centralizat (asigură funcţionalităţi de administrare); - protecţie antivirus, antispam, antispyware, antimalware, antiphishing, antirootkit, firewall pentru staţii 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	
Condiții generale	Produsul antivirus pus la dispoziție trebuie să fie **certificat VB100[1] sau echivalent** în ultimele 12 luni.
	Produsul antivirus pus la dispoziție trbuie să aibă impact minim (sub 10%) asupra performantelor sistemului pe care este instalat. In acest sens furnizorul va prezenta **rezultatele obtinute 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 mașină virtuală ce conține toate rolurile / serviciile necesare sau ca un kit ce permite instalarea rolurilor / serviciilor și în mașini virtuale.
	Suportă cel puțin următoarele platforme de virtualizare: - Microsoft Hyper-V; - VMware vSphere;
Funcționalități	Soluția trebuie să fie scalabilă, astfel încât oricare dintre roluri sau servicii să poată fi instalate separat pe mai multe mașini (inclusiv virtuale), sau pe aceeași mașină (inclusiv virtuală).
	Soluția îndeplinește cel puțin următoarele roluri: - 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.
	Soluția va permite detecția și prevenirea intruziunilor (prin funcționalități de tip IDS[2] și IPS[3]), 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).
Actualizare	Permite actualizarea (automată) de pe Internet a semnăturilor antivirus și IDS, precum și 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 și pe bază de reputație.
	Permite administrarea de la distanță și crearea de roluri de administrare.
	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".
	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.
	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.
	Previne execuția automată a aplicațiilor descărcate și previne modificarea fișierelor aferente sistemului de operare.

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

	Permite scanarea și sanitizarea resurselor partajate în rețea.
	După identificarea aplicațiilor malware, soluția întreprinde următoarele acțiuni: - mutare în carantină; - dezinfecție sau ștergere. Soluția permite restaurarea fișierelor aflate în carantină.
Inventarierea rețelei	Soluția permite,cel puțin, integrarea cu Active Directory și importă inventarul din această platformă. Pentru integrarea cu Active Directory, se poate defini și 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.
	Permite roluri multiple predefinite (cel puțin): - *administrator global*: administrează întreaga soluție de protecție la nivel „end-point"; - *administrator*: administrează serviciile de securitate; - *dispecer*: 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	Oferă șabloane de politici de securitate, dedicate pentru fiecare serviciu.
	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.
Certificate	Accesul la consola centrală de management se realizează în mod securizat, prin HTTPS.
	Serverul web, din consola centrală de management, permite importul de certificate digitale eliberate de o autoritate de certificare autorizată sau proprie organizației.
	Certificatele digitale, odată importate, oferă posibilitatea înlocuirii acestora în caz de expirare sau de revocare.
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.
	Oferă posibilitatea de arhivare a acestor rapoarte.
	Permite exportul rapoartelor programabile în formatele PDF și 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 20+; - Google Chrome 20+;
	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.
	Oferă informații legate de certificate: - nume; - autoritatea emitentă; - data eliberării certificatelor; - data expirării certificatelor eliberate.
Politici de securitate	Consola permite crearea și gestionarea de politici de securitate.
	Oferă posibilitatea de implementare centralizată a politicilor pe mașinile fizice, virtuale și 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 și 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/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.
	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 puțin 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 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 virușilor 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: - 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 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 semnaturi 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
Protecția la nivel de medii virtualizate	
Cerințe minimale	Platforme de virtualizare suportate (cel puțin): - VMware vSphere 4.1+ (cu VMware vCenter Server 4.1+); - Microsoft Hyper-V Server 2008 R2; - 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); - Open SUSE 12+; - Cent OS 5.6+; - Red Hat Enterprise Linux; - Ubuntu 10.04+; - SUSE Linux Enterprise Server 11; - Open SUSE 11+; - Fedora 16+.
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 catre specialistii 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 doua saptamani 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 exceptionale (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 putin 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.

La livrarea soluției ofertate, furnizorul va oferi suport tehnic pentru integrarea acesteia cu sistemul SIEM (Security Information and Event Management) HP Arcsight instalat la Ministerul Justiției, făcând astfel posibilă colectarea și interpretarea datelor jurnalizate de către soluția antivirus. Serviciul va fi prestat la sediul Ministerului Justiției în maxim o luna de la semnarea contractului.

Termenul de livrare a serviciilor de protective de tip antivirus este de 2 săptămâni de la semnarea contractului.

Întocmit,

Cotor Călin-Petru

Specialist IT, Tribunalul Sălaj

Zalău, 14 ianuarie 2019