ROMÂNIA

MINISTERUL AFACERILOR INTERNE
INSTITUŢIA PREFECTULUI - JUDEŢUL BISTRIŢA-NĂSĂUD
Nr. I/C/342 din 09.01.2020

APROB:
PREFECT
Nechita-Stelian DOLHA

CAIET DE SARCINI

1. AUTORITATEA CONTRACTANTĂ

- Instituţia Prefectului - Judeţul Bistriţa-Năsăud, cu sediul în municipiul Bistriţa, Piaţa Petru Rareş, nr. 1, judeţul Bistriţa-Năsăud.

2. OBIECTUL ACHIZIŢIEI îl reprezintă:

- "Pachete software de protecţie antivirus" - cod CPV 48761000-0.

3. INTRODUCERE

3.1. Obiectul prezentului caiet de sarcini este achiziţionarea serviciilor de asigurare a protecţiei antivirus, anti-malware, anti-spam, anti-spyware, anti-phising și anti-ransomware pentru infrastructura IT din cadrul Instituției Prefectului - Județul Bistrița-Năsăud (denumită în continuare IPBN), respectiv pentru un număr de 57 stații de lucru și 2 servere.

3.2. Achiziţionarea serviciilor este necesară pentru protejarea împotriva viruşilor informatici şi software-ului de tip *malware, spyware, spam* şi de altă natură, în măsură să afecteze securitatea şi disponibilitatea reţelei de calculatoare a IPBN şi echipamentelor de calcul individuale neconectate în reţea.

3.3. Serviciile au ca scop asigurarea protecţiei infrastructurii informatice împotriva atacurilor informatice generale şi particulare; soluţia trebuie să minimizeze riscul contaminării cu viruşi informatici sau alte programe maliţioase şi să asigure protecţia eficientă împotriva vulnerabilităţilor cunoscute.

3.4. Pentru asigurarea serviciilor, licenţele software proprii sau terţe vor fi asigurate de către prestator în concordanţă cu necesităţile operaţionale, fără costuri suplimentare din partea beneficiarului.

3.5. Produsele care asigură îndeplinirea serviciilor ofertate, la momentul depunerii ofertei, trebuie să nu fie *end-of-life;* în situaţia în care independent de voinţa prestatorului un produs al unui terţ ajunge *end-of-life* pe timpul derulării contractului, înlocuirea acestuia se face pe cheltuiala prestatorului, cu un produs având cel puţin specificaţiile şi performanţele celui ofertat.

3.6. Cerinţele prezentului Caiet de Sarcini sunt minimale şi obligatorii.

Bistriţa, Piaţa Petru Rareş, nr. 1, 420080, Telefon: 0263/216150, Fax: 0263/214235
e-mail: inform_publice@prefecturabn.ro, website: https://bn.prefectura.mai.gov.ro

4. SPECIFICAŢII GENERALE

4.1. Specificaţii privind oferta

Oferta este compusă din servicii de protecţie informatică antivirus, anti-malware, anti-spam, anti-spyware, anti-phising și anti-ransomware, prevăzute la punctul 7.5, pentru reţeaua de calculatoare a IPBN şi echipamentele de calcul individuale neconectate în reţea.

Cantităţile sunt: 57 stații de lucru și 2 servere.

Oferta financiară pentru fiecare tip de serviciu descris la punctul 7.5 trebuie să cuprindă câte un preţ per serviciu.

4.2. Specificaţii generale ale soluţiei tehnice

Prestatorul trebuie să asigure, pe toată durata contractului, serviciile de actualizare a semnăturilor de virus, de upgrade la cele mai recente versiuni ale motoarelor de scanare şi ale tuturor serviciilor livrate, precum şi serviciile de suport tehnic, fără costuri suplimentare din partea achizitorului.

În situaţia constatării de deficienţe sau neconcordanţe între caracteristicile tehnico-funcţionale ale unui serviciu prestat şi prevederile caietului de sarcini, prestatorul trebuie să înlocuiască serviciul sau actualizarea acestuia în termen de cel mult **48 de ore** de la primirea notificării din partea beneficiarului.

Ofertantul trebuie să livreze beneficiarului kit-urile de instalare şi documentaţiile necesare.

4.3. Specificaţii generale ale serviciilor de protecţie informatică antivirus

- Serviciile de protecţie informatică antivirus prestate trebuie să fie însoţite de certificatele de calitate.
- Odată cu oferta tehnică, pentru serviciile antivirus livrate, prestatorul va prezenta cel puţin 1 certificat emis de una dintre organizaţiile internaţionale de profil *ICSA Labs, Checkmark, Virus Bulletin.*
- Actualizarea semnăturilor de virus şi a versiunilor atât pentru staţii de lucru, cât şi pentru servere trebuie să se poată efectua periodic în mod automat şi/sau manual.
- Pentru evitarea încărcării suplimentare a sistemelor de calcul protejate, funcţiile de protecţie trebuie să fie asigurate printr-un singur motor de scanare instalat şi să poată rula scanările programate cu prioritate redusă *(background).*
- Serviciile antivirus trebuie să aibă opţiunea de scanare automată a fişierelor înainte de copierea/instalarea acestora.
- Serviciile antivirus trebuie să permită instalarea/activarea personalizată a modulelor componente, în funcţie de nevoi.
- Serviciile antivirus trebuie să fie compatibile cu sistemele de operare în funcţie de tehnologia pe care este instalat sistemul de operare (32/64 biţi) pentru: *Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10, VMWare* şi reţea.
- Serviciile trebuie să fie livrate cu şabloane de raportări predefinite, atât despre starea produselor, cât şi despre evenimente *malware.*
- Caracteristicile jurnalelor funcţionale sunt următoarele:

a) format: XML, syslog sau alt format standardizat;

b) conţinut: evenimente relevante ale funcţionării fiecărui modul structură (minimală, dar nu restrictivă): (1) moment de timp, (2) identificator sursă, (3) descriere eveniment, (4) rezultat.

4.4. Specificaţii generale ale serviciilor de suport

Serviciile livrate trebuie să includă servicii de suport şi mentenanţă *on-site* valabile pe toată durata contractului.

Bistriţa, Piaţa Petru Rareş, nr. 1, 420080, Telefon: 0263/216150, Fax: 0263/214235
e-mail: inform_publice@prefecturabn.ro, website: https://bn.prefectura.mai.gov.ro

Orice noi informaţii privind posibile ameninţări trebuie să fie puse la dispoziţia beneficiarului cu maximă urgenţă prin mesaje electronice de alertă în cazul unor noi viruşi distructivi sau cu potenţial mare de răspândire.

La solicitarea beneficiarului, prestatorul trebuie să fie în măsură să răspundă la incidentele provocate de atacuri ale virusilor sau software-ului malitios în termen de 24 ore prin deplasarea şi intervenţia în locaţia fizică a beneficiarului.

Prestatorul trebuie să fie în măsură să ofere un antidot pentru orice nou cod malitios semnalat de beneficiar în termen de cel mult 72 ore de la notificare.

Prestatorul trebuie să pună la dispoziţie servicii de suport tehnic de instalare, configurare, diagnoză şi remediere exclusiv în limba română, în regim 24/7, atât telefonic, cât şi prin mijloace electronice (web, e-mail); oferta tehnică va cuprinde datele de contact relevante.

La solicitarea beneficiarului, prestatorul va întreprinde vizită *in-site* în scopul verificării funcţionării serviciilor prestate şi remedierii eventualelor disfuncţionalităţi; concluziile vizitei vor fi consemnate într-un proces-verbal întocmit în două exemplare, câte unul pentru fiecare parte, şi care se va ataşa la documentele care se întocmesc pentru efectuarea plăţii lunare a serviciilor.

5. CARACTERISTICI TEHNICE

5.1. Caracteristici tehnice ale componentei *antivirus, anti-malware, anti-spam, anti-spyware, anti-phising, anti-ransomware* pentru servere şi staţii de lucru

• Asigură minimum 3 tipuri de detecţie:

a) bazată pe semnături;

b) bazată pe comportament (euristic);

c) bazată pe monitorizarea proceselor.

• Asigură scanarea automată *"on acces"* (în timp real) şi *"on demand"* (la cerere) pentru:

a) suporţii de stocare a informaţiei: FDD, HDD, CD-ROM, USB Flash Memory, SSD, cititoare de card;

b) fişierele care se copiază de pe suport extern şi din reţeaua de date;

c) arhive .arj, .ace, .cab, .zip, .rar, .tar, .gz;

d) arhivele de mesagerie electronică (e-mail);

e) transferurile de fişiere în comunicaţii P2P (instant messaging);

f) anumite tipuri de fişiere (listă configurabilă) sau pentru toate fişierele;

g) anumite dimensiuni de arhive (dimensiune maximă configurabilă);

h) anumite căi (listă configurabilă).

• În funcţie de nevoi, opţiunile şi listele de scanare sunt configurabile de către administrator; configurările "la cerere" *("on demand")* sunt accesibile şi la nivelul utilizatorului obişnuit.

• Administratorul poate gestiona liste de excludere de la scanarea anumitor directoare, suporţi de stocare, fişiere sau extensii, precum şi fişiere cu anumite dimensiuni, configurabile.

• Permite afişarea de mesaje pe ecran sub formă de fereastră *pop-up* în momentul detectării unei cod malitios.

• Permite opţiunea de pauză şi reluare a sarcinilor de scanare.

• Asigură monitorizarea activă a regiştrilor sistemului de operare afişând mesaje de atenţionare în momentul în care o aplicaţie încearcă să îi modifice.

Bistriţa, Piaţa Petru Rareş, nr. 1, 420080, Telefon: 0263/216150, Fax: 0263/214235
e-mail: inform_publice@prefecturabn.ro, website: https://bn.prefectura.mai.gov.ro

• Asigură protecţie *anti-spyware.*

• Asigură protecție *anti-malware*, și anume:

a) protecția în timp real contra website-urilor malițioase;

b) protecția completă contra vulnerabilităților de sistem și software, astfel încât să nu fie exploatate de către un program malițios;

c) existența unor straturi multiple de protecție *anti-ransomware* cu rol de prevenire, detecție și remediere;

d) monitorizarea proceselor în timp real.

• Asigură protecție *anti-phising* prin blocarea automată a accesului la pagini web de tip phising, detectarea traficului web și de rețea suspecte.

• Permite funcţionarea clientului antivirus în oricare dintre următoarele moduri:

a) **în reţea**, în interacţiune cu software-ul de management şi actualizare;

b) **standalone** (cu sau fără suport de reţea).

• Actualizarea bazei de date locale cu semnături antivirus şi anti-spyware a clientului se face fără intervenţia utilizatorului, de regulă de pe server-ul special destinat, însă la nevoie poate fi configurată şi o altă locaţie de reţea. Atât clienţii cu management, cât şi clienţii instalaţi *standalone* trebuie sa aibă opţiunea de actualizare manuală.

5.2. Caracteristici tehnice ale modulului *firewall* pentru servere și stații de lucru

Modulul *firewall* trebuie să asigure îndeplinirea următoarelor funcţii:

• Asigură protecţia datelor şi filtrarea traficului la intrare şi la ieşire, controlând fişierele de tip cookie, blocând scripturile maliţioase şi programele de tipul *"XX-dialer".*

• Asigură predefinirea setului de reguli ce urmează a fi aplicate în mod automat.

• Permite opţiunea de instalare/dezinstalare şi activare/dezactivare în funcţie de necesităţi.

5.3. Caracteristici tehnice ale modulului *anti-spam* pentru staţii de lucru și servere

Modulul *anti-spam* trebuie să asigure îndeplinirea următoarelor funcţii:

• Adaptarea la noile tehnici de lansare a spam-ului, analizând şi memorând preferinţele utilizatorului, reducând astfel la minimum numărul mesajelor legitime etichetate în mod eronat ca *spam.*

• Filtrarea mesajelor *spam* de tip imagine.

• Blocarea mesajelor e-mail scrise cu caractere diferite de cele europene (de ex. chirilice sau chinezeşti).

• Utilizarea filtrului antispam *"antrenat"* pe baza unei serii de mesaje *spam* astfel încât acesta să poată recunoaşte noile mesaje de acest tip prin identificarea asemănărilor cu cele pe care le-a examinat deja.

• Permite opţiunea de instalare/dezinstalare în funcţie de necesităţi.

5.4. Caracteristici tehnice ale modulului *carantină* pentru staţii de lucru și servere

Modulul *carantină* trebuie să asigure îndeplinirea următoarelor funcţii:

• Restaurarea fişierelor din carantină în locaţiile lor originale.

• Trimiterea manuală sau automată a fişierelor din carantină către *laboratorul antivirus.*

5.5. Caracteristici tehnice ale modulului *administrare şi instalare remote* pentru staţii de lucru și servere

Modulul *administrare şi instalare remote* trebuie să asigure îndeplinirea următoarelor funcţii:

Bistrița, Piața Petru Rareș, nr. 1, 420080, Telefon: 0263/216150, Fax: 0263/214235
e-mail: inform_publice@prefecturabn.ro, website: https://bn.prefectura.mai.gov.ro

• Console centrale de management ce vor facilita administrarea şi instalarea agenţilor. După caz, soluţia de virtualizare poate necesita una sau mai multe console pentru instalarea, configurarea, monitorizarea şi raportarea stării de securitate a staţiilor de lucru şi a serverelor.

• Consola de management trebuie să îndeplinească următoarele funcţii minimale:

a) identificarea echipamentelor accesibile în reţea gruparea şi gestionarea grupărilor de clienţi antivirus pentru echipamentele din reţea;

b) identificarea stării echipamentelor din punctul de vedere al instalării soluţiei antivirus;

c) identificarea stării de activare globală şi individuală a funcţiilor (activ/inactiv) şi schimbarea acesteia în funcţie de necesităţi;

d) identificarea stării de actualizare şi forţarea actualizării la nevoie;

e) gestionarea licenţelor;

f) crearea kit-ului de instalare personalizat destinat atât sistemelor de operare de 32 biţi, cât şi celor de 64 biţi;

h) crearea şabloanelor de raportări suplimentare faţă de cele predefinite.

• Consola trebuie să aibă integrat un modul dedicat controlului activităţii utilizatorilor, cu următoarele funcţii minimale:

a) restricţionarea accesului la internet pentru anumiţi clienţi sau grupuri de clienţi;

b) restricţionarea accesului la internet pentru anumite aplicaţii;

c) restricţionarea accesului la internet pentru anumite perioade de timp;

d) blocarea paginilor web care conţin anumite cuvinte cheie.

• Accesul la consola de management în urma introducerii credenţialelor de acces (username şi parolă).

• Prestatorul trebuie să asigure compatibilitatea şi integrabilitatea soluţiei de management centralizat cu *Microsoft® Active Directory* din sistemele de operare *Windows Server* suportate.

5.6. Caracteristici tehnice ale modulului *rapoarte, grafice şi alerte* pentru staţii de lucru şi servere

Modulul *rapoarte, grafice şi alerte* trebuie să asigure îndeplinirea următoarelor funcţii:

• Crearea de rapoarte pe baza şabloanelor definite în consola de management.

• Generarea de rapoarte complete privind rezultatele scanării şi infecţiilor detectate dar şi a tuturor obiectelor scanate, inclusiv la nivelul clienţilor.

• Generarea în mod automat, în cazul detecţiei unui eveniment, a unui mesaj de alertă către una sau mai multe adrese de *e-mail* prin intermediul componentei centralizate.

• Generarea rapoartelor în mod programat şi expedierea lor în mod automat prin e-mail către administrator.

• Generarea rapoartelor într-un format standardizat (ex.: html, pdf, etc.).

5.7. Caracteristici tehnice ale modulului *audit reţea* pentru staţii de lucru şi servere

Modulul *audit reţea* trebuie să asigure îndeplinirea următoarelor funcţii:

• Arhivarea automată a datelor de audit, pe termen lung, prin intermediul unui modul de arhivare.

• Realizarea raportării de audit pe baza şabloanelor de raportare predefinite sau personalizate.

• Trimiterea rapoartelor, prin e-mail.

Bistriţa, Piaţa Petru Rareş, nr. 1, 420080, Telefon: 0263/216150, Fax: 0263/214235
e-mail: inform_publice@prefecturabn.ro, website: https://bn.prefectura.mai.gov.ro

5.8. Caracteristici tehnice ale modulului *actualizare* pentru staţii de lucru şi servere

Modulul *actualizare* trebuie să asigure îndeplinirea următoarelor funcţii:

- Actualizarea în mod automat a semnăturilor de antivirus și anti-spyware la intervale de timp configurabile sau la cerere.
- Posibilitatea configurării intervalului de verificare automată a disponibilităţii unei noi actualizări.
- Posibilitatea actualizării semnăturilor de virus la nivelul staţiei de lucru atât la cerere, cât şi automat, fără intervenţia utilizatorului, în mod silenţios *(unattended).*
- Posibilitatea administratorului de a configura automat sau cu confirmare din partea utilizatorului, în situaţia în care este necesară repornirea echipamentului după încheierea unei actualizări.
- Securizarea sistemului de actualizare a semnăturilor de virus şi a motorului de scanare, prin mecanisme de semnare a fişierelor de către producător.
- Upgrade la noile versiuni ale produsului pe perioada contractului.

6. CERINŢE PRIVIND OPERAȚIONALIZAREA SERVICIILOR

6.1. Instalarea serviciilor

Soluţia trebuie să fie instalată pe toate echipamentele specificate în contract: st i de lucru și servere.

În procesul de instalare şi configurare a componentelor software prevalează limitările şi regulile de securitate impuse de beneficiar.

Politica de actualizare a semnăturilor de virus trebuie să nu producă blocaje, iar activarea ulterioară a licenţelor contractate trebuie să se facă fără cheltuieli suplimentare din partea beneficiarului.

6.2. Asistenţa tehnică

Prestatorul trebuie să asigure asistenţă tehnică pe toată durata contractului exclusiv în limba română, în regim 24/7. În acest sens, oferta tehnică trebuie să cuprindă datele de contact relevante pentru toate modalităţile de contact (telefon, fax, e-mail, sms).

Elementele fluxului de tratare a evenimentelor sunt următoarele:

a) evenimentul de securitate informatică detectat de beneficiar în perioada de derulare a contractului se notifică prestatorului prin e-mail/site web/telefonic, solicitându-i-se intervenţia; notificarea conţine obligatoriu o descriere detaliată a problemei;

b) orice solicitare de intervenţie transmisă de beneficiar trebuie confirmată de către prestatorul serviciilor, în limitele timpului de răspuns, prin numărul unic al tichetului deschis, comunicat de regulă, dar nu restrictiv, pe aceeaşi cale pe care a fost recepţionată solicitarea de intervenţie;

c) numărul tichetului serveşte ca referinţă unică pentru urmărirea de către beneficiar a stadiului rezolvării, până la închiderea tichetului;

d) închiderea unui tichet deschis de beneficiar trebuie confirmată de către acesta;

e) prestatorul trebuie să pună la dispoziţia beneficiarului instrumente de verificare *on-line* a tichetelor proprii din evidenţa acestuia, indiferent dacă acestea sunt active sau nu; în acest sens, în contract vor fi precizate toate detaliile necesare

Timpul de răspuns al prestatorului (considerat faţă de momentul înregistrării solicitării de intervenţie):

a) în cazul evenimentelor critice: **răspuns în cel mult 2 ore,** rezolvare în cel mult 24 ore.

Bistriţa, Piaţa Petru Rareş, nr. 1, 420080, Telefon: 0263/216150, Fax: 0263/214235
e-mail: inform_publice@prefecturabn.ro, website: https://bn.prefectura.mai.gov.ro

b) în cazul evenimentelor obişnuite: răspuns în cel mult 12 ore, rezolvare în cel mult 72 ore.

7. CONDIŢII DE LIVRARE, INSTALARE ŞI ACCEPTANŢĂ

7.1. Instalarea şi configurarea serviciilor trebuie să înceapă cât mai curând posibil, dar nu mai târziu de 7 zile calendaristice de la semnarea contractului şi se va finaliza în termenul de instalare ce se va menţiona în contract.

7.2. Acceptanţa la beneficiar a instalării şi configurării serviciilor va avea loc după încheierea tuturor procedurilor de instalare şi configurare şi întocmirea procesului verbal de acceptanţă.

7.3. În cazul în care, din vina sa exclusivă, prestatorul depăşeşte termenul de instalare şi configurare, prevăzut în contract, beneficiarul are dreptul de a solicita şi încasa ca penalităţi o sumă echivalentă cu o cotă procentuală reprezentând 0,1% din valoarea întregului contract, pentru fiecare zi calendaristică de întârziere, până la îndeplinirea efectivă a obligaţiilor.

7.4. Prestatorul va pune la dispoziţia beneficiarului pe suport optic/electronic toate kit-urile necesare, precum şi documentaţia tehnică pentru instalarea, configurarea, administrarea şi mentenanţa serviciilor livrate.

7.5. Detalierea serviciilor de protecţie informatică antivirus este următoarea:

a) serviciu de protecţie informatică antivirus, anti-malware, anti-spam, anti-spyware, anti-phising și anti-ransomware pentru staţii de lucru;

b) serviciu de protecţie informatică antivirus, anti-malware, anti-spam, anti-spyware, anti-phising și anti-ransomware pentru servere.

8. DISPOZIŢII FINALE

8.1. Prestatorul va prezenta lunar şi ori de câte ori intervine o modificare, către beneficiar, următoarele date, într-o formă structurată:

- Beneficiarul contractului, numărul, data, valoarea şi perioada de valabilitate a contractului.
- Tipul şi valoarea serviciilor care fac obiectul contractului (ex.: Protecţie informatică pentru staţii de lucru - număr de staţii protejate - valoare totală serviciu, protecţie informatică pentru servere - număr de servere protejate - valoare totală serviciu, etc.).
- Numărul, data şi valoarea facturilor emise, contractul în baza căruia se emite factura, valoarea şi data plăţilor, precum şi numărul, valoarea şi motivul valoarea penalităţilor emise sau primite, dacă este cazul.
- Raportul va fi transmis către beneficiar, atât pe hârtie, cât şi în format electronic.

8.2. Prestatorul va informa beneficiarul cu privire la finalizarea contractului, dar nu mai târziu de 7 zile de la data finalizării acestuia.

ŞEF SERVICIU
TEODORA DANA ROMAN

Întocmit,
Cons. II DANIELA BILIBOACĂ

Bistriţa, Piaţa Petru Rareş, nr. 1, 420080, Telefon: 0263/216150, Fax: 0263/214235
e-mail: inform_publice@prefecturabn.ro, website: https://bn.prefectura.mai.gov.ro