CAIET DE SARCINI

Acord cadru pentru servicii lunare de
protecţie informatică antivirus şi antimalware
la nivelul Ministerului Afacerilor Interne

1. INTRODUCERE

1.1. Obiectul prezentului caiet de sarcini este achiziţionarea serviciilor de asigurare a protecţiei antivirus, antispam şi antimalware pentru infrastructura IT a Aparatului Central al Ministerului Afacerilor Interne (denumit în continuare MAI), precum şi pentru infrastructurile IT aflate la nivelul ordonatorilor de credite din subordinea MAI, prevăzuţi în anexa nr. 1 la modelul de acord cadru.

1.2. 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 MAI şi echipamentelor de calcul individuale neconectate în reţea, inclusiv a dispozitivelor portabile.

1.3. Serviciile au ca scop asigurarea protecţiei infrastructurii informatice (staţii de lucru, thin clients, servere fizice şi virtualizate şi dispozitive mobile) 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.

1.4. 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.

1.5. 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 subsecvent la acordul cadru, înlocuirea acestuia se face pe cheltuiala prestatorului, cu un produs având cel puţin specificaţiile şi performanţele celui ofertat.

1.6. În funcţie de necesităţile operaţionale şi disponibilitatea alocării fondurilor bugetare, fiecare ordonator de credite din structura MAI prevăzut în anexa nr. 1 la modelul de acord cadru, poate încheia în condiţiile specificate la punctele 2.1.1 - 2.1.11, contracte subsecvente la acordul cadru, cu unul din promitenţii-prestatori declaraţi câştigători, în urma derulării procesului de reluare a competiţiei, în condiţiile dispoziţiilor art.150 din O.U.G nr. 34/2006, cu modificările şi completările ulterioare.

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

2. SPECIFICAŢII GENERALE

2.1. Specificaţii privind oferta

2.1.1. Atribuirea contractelor subsecvente în baza acordului cadru se va face prin reluarea competiţiei în conformitate cu specificaţiile din capitolul 4 al prezentului caiet de sarcini, aplicând criteriul de atribuire *„preţul cel mai scăzut"*.

2.1.2. Atât în acordul cadru cât şi cu ocazia reluării competiţiei, fiecare promitent-prestator este obligat să prezinte câte o ofertă şi numai una pentru fiecare dintre serviciile precizate la punctul 5.8 al prezentului caiet de sarcini, să aparţină aceluiaşi producător (excepţie face componenta antivirus pentru dispozitivele portabile, cap. 3.2, ce poate aparţine unui alt producător); nu sunt admise oferte alternative pentru acelaşi tip de serviciu.

2.1.3. Ofertantul trebuie să ofere servicii de protecție informatică la peste 200 de locații ale beneficiarului. În contextul în care calitatea serviciilor trebuie să fie de aceiași manieră, în toate locațiile beneficiarului, ofertantul trebuie să prezinte modalitatea în care va asigura serviciile pe întregul teritoriu al României, în mod eficient și operativ.

2.1.4. Oferta pentru acordul cadru este compusă din servicii de protecție informatică antivirus și antimalware, prevăzute la punctul 5.8.

2.1.5. Serviciile cuprind în mod obligatoriu instruirea personalului achizitorului, desfăşurată în conformitate cu prevederile subcapitolului 4.2.

2.1.6. În procesul de reluare a competiţiei, în vederea atribuirii unui contract subsecvent, achizitorul va solicita promitenţilor–prestatori semnatari ai acordului cadru oferte pentru servicii de protecție informatică antivirus și antimalware descrise la punctul 5.8.

2.1.7. Cantităţile minime şi maxime estimate pentru acordul cadru sunt prezentate în anexa nr. 1 la prezentul Caiet de Sarcini.

2.1.8. Oferta financiară pentru fiecare tip de serviciu descris la punctul 5.8 trebuie să cuprindă câte un preţ per serviciu.

2.1.9. Prin contractul subsecvent, fiecare autoritate contractantă achiziționează doar acele servicii prevăzute la punctul 5.8, în cantităţile necesare, în funcţie de nevoile operaţionale şi fondurile bugetare alocate, fără a avea obligaţia de a achiziţiona toate serviciile care fac obiectul acordului cadru.

2.1.10. În cadrul procedurii de reluare a competiţiei la nivelul ordonatorilor de credite din MAI, preţurile per serviciu individual ofertate de semnatarii acordului-cadru, se pot modifica doar in sensul îmbunătăţirii acestora faţă de oferta iniţială din acordul cadru, în conformitate cu prevederile art. 69 alin. (3) din HG 925/2006, cu modificările si completările ulterioare. Adjudecarea se va face pe oferta totală a serviciilor ofertate.

2.1.11. În cadrul procesului de reluare a competiţiei, In cazul în care, în urma reofertării, autoritatea contractantă nu obţine îmbunătăţiri ale elementelor/ condiţiilor care fac obiectul reluării competiţiei, aceasta are obligaţia de a atribui contractul ofertantului clasat pe primul loc în cadrul procedurii aplicate pentru încheierea acordului-cadru,

prin luarea în considerare a condiţiilor şi elementelor prevăzute în oferta iniţială a acestuia, conform prevederilor art. 69 alin. (6) din HG 925/2006. .

2.1.12. La finalizarea unui contract subsecvent sau ori de câte ori este necesar, asigurarea serviciilor se poate face exclusiv prin reluarea competiţiei, la care au obligaţia să participe şi să depună ofertă toţi promitenţii–prestatori semnatari ai acordului cadru.

2.2. Specificaţii generale ale soluţiei tehnice

2.2.1. Prestatorul trebuie să asigure pe toată durata contractului subsecvent 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.

2.2.2. 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 achizitorului.

2.2.3. Ofertantul trebuie să livreze kiturile de instalare şi documentaţiile necesare, fiecărei structuri a MAI care încheie un contract subsecvent.

2.3. Specificaţii generale ale serviciilor de protecţie informatică antivirus

2.3.1. Serviciile de protecţie informatică antivirus prestate trebuie să fie însoţite de certificatele de calitate.

2.3.2. 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*.

2.3.3. Actualizarea semnăturilor de virus şi a versiunilor atât pentru staţii de lucru, servere cât şi pentru serviciile de virtualizare trebuie să se poată efectua periodic în mod automat şi/sau manual, în funcţie de opţiunea administratorului desemnat de ordonatorul de credite din cadrul MAI care a încheiat contractul subsecvent.

2.3.4. 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*).

2.3.5. Serviciile antivirus trebuie să aibă opţiunea de scanare automată a fişierelor înainte de copierea/instalarea acestora.

2.3.6. Serviciile antivirus trebuie să permită instalarea/activarea personalizată a modulelor componente, în funcţie de nevoi.

2.3.7. Interfeţele şi documentaţiile componentelor de servicii trebuie să fie în limba română.

2.3.8. 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 R2*, *Windows Server 2012*, *Windows XP*, *Windows Vista*, *Windows 7*, *Windows 8*, *VMWare* şi reţea TCP/IP.

MINISTERUL AFACERILOR INTERNE
DIRECŢIA PENTRU COMUNICAŢII ŞI TEHNOLOGIA INFORMAŢIEI
AVIZAT TEHNIC
Semnătura _____ Data 20.08.2014

2.3.9. Serviciile trebuie să fie livrate cu şabloane de raportări predefinite, atât despre starea produselor, cât şi despre evenimente *malware*.

2.3.10. 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.

2.4. Specificaţii generale ale serviciilor de suport

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

2.4.2. 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.

2.4.3. La solicitarea beneficiarului, prestatorul trebuie să fie în măsură să răspundă la incidentele provocate de atacuri ale viruşilor sau software-ului maliţios în termen de 24 ore prin deplasarea şi intervenţia în locaţiile fizice ale beneficiarului.

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

2.4.5. 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, email); oferta tehnică va cuprinde datele de contact relevante.

2.4.6. La solicitarea beneficiarului prestatorul va întreprinde câte o vizită (cel puţin o dată pe lună) *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 atașa la documentele care se întocmesc pentru efectuarea plăţii lunare a serviciilor.

3. CARACTERISTICI TEHNICE

3.1. Caracteristici tehnice ale componentei antivirus şi antispyware pentru servere, staţii de lucru şi thin clients

3.1.1. Asigură minimum 3 tipuri de detecţie:

(a) bazată pe semnături;

(b) bazată pe comportament (euristic);

(c) bazată pe monitorizarea proceselor.

3.1.2. 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;

MINISTERUL AFACERILOR INTERNE
DIRECŢIA PENTRU COMUNICAŢII ŞI TEHNOLOGIA INFORMAŢIEI
AVIZAT TEHNIC
Semnătura _____ Data 20.03.2014

(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).

3.1.3. În funcţie de nevoi, opţiunile şi listele de scanare de la pct. 3.1.2. sunt configurabile de către administrator; configurările *"la cerere"* (*„on demand"*) sunt accesibile şi la nivelul utilizatorului obişnuit.

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

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

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

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

3.1.8. Asigură protecţie *spyware*.

3.1.9. 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).*

3.1.10. Actualizarea bazei de date locale cu semnături antivirus şi antispyware a clientului se face fără intervenţia utilizatorului, de regulă de pe serverul 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.

3.2. Caracteristici tehnice ale componentei antivirus pentru dispozitivele portabile

3.2.1. Trebuie asigurate servicii pentru următoarele sisteme de operare instalate pe dispozitivele portabile tip telefon, tabletă sau similar:

(a) Windows 7, Windows 8

(b) Google Android (începând cu versiunea 2.3)

(c)iOS (începând cu versiunea 7)

3.2.2. Componenta antivirus instalată pe dispozitivele portabile trebuie să asigure cel puţin următoarele funcţii de protecţie:

(a) protecţia *animalware* şi *antiphishing;*

(b) scanarea cardurilor SD (*Secure Digital*);

(c) protecţia datelor stocate pe dispozitivul portabil.

3.3. Caracteristici tehnice ale modulului firewall pentru servere

Modulul *firewall* trebuie să asigure îndeplinirea următoarelor funcţii:

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

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

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

3.4. Caracteristici tehnice ale modulului *antispam* pentru servere, staţii de lucru şi thin clients

Modulul *antispam* trebuie să asigure îndeplinirea următoarelor funcţii:

3.4.1. 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*.

3.4.2. Filtrarea mesajelor *spam* de tip imagine.

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

3.4.4. 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.

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

3.4.6. Pentru serverele de e-mail, componenta antimalware și antispam trebuie să includă suport pentru sistemul de operare GNU/Linux, distribuţiile *RedHat*, *Suse* şi *Debian* cât şi kernele versiunile 2.4, 2.6 şi 3. De asemenea, trebuie să fie de tip modular şi integrabil cu MTA-urile existente: *Communigate*, *Postfix*, *Sendmail*.

3.5. Caracteristici tehnice ale modulului *carantină* pentru staţii de lucru, servere, thin clients şi virtualizare

Modulul *carantină* trebuie să asigure îndeplinirea următoarelor funcţii:

3.5.1. Restaurarea fişierelor din carantină în locaţiile lor originale.

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

3.6. Caracteristici tehnice ale modulului „*administrare şi instalare remote*" pentru staţii de lucru, servere şi virtualizare

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

3.6.1. 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 virtualizate.

3.6.2. Consola de management trebuie să îndeplinească următoarele funcţii minimale:

(a) identificarea echipamentelor accesibile în reţea

MINISTERUL AFACERILOR INTERNE
DIRECŢIA PENTRU COMUNICAŢII
ŞI TEHNOLOGIA INFORMAŢIEI
AVIZAT TEHNIC
Semnătura _____ Data 30.08.2019

(b) gruparea şi gestionarea grupărilor de clienţi antivirus pentru echipamentele din reţea

(c) identificarea stării echipamentelor din punctul de vedere al instalării soluţiei antivirus

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

(e) identificarea stării de actualizare şi forţarea actualizării la nevoie

(f) gestionarea licenţelor

(g) 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

3.6.3. 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

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

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

3.7. Caracteristici tehnice ale modulului *rapoarte, grafice şi alerte* pentru staţii de lucru, servere, thin clients şi virtualizare

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

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

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

3.7.3. 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

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

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

3.8. Caracteristici tehnice ale modulului *"audit reţea"* pentru staţii de lucru, thin client, servere şi virtualizare

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

MINISTERUL AFACERILOR INTERNE
DIRECŢIA PENTRU COMUNICAŢII ŞI TEHNOLOGIA INFORMAŢIEI
AVIZAT TEHNIC
Semnătura ____ Data 20.08.2014

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

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

3.8.3. Trimiterea rapoartelor, prin e-mail

3.9. Caracteristici tehnice ale modulului *„actualizare"* pentru staţii de lucru, servere, thin clients şi virtualizare

Modulul *actualizare* trebuie să asigure îndeplinirea următoarelor funcţii:

3.9.1. Actualizarea în mod automat a semnăturilor de virus la intervale de timp configurabile sau la cerere.

3.9.2. Posibilitatea configurării intervalului de verificare automată a disponibilităţii unei noi actualizări.

3.9.3. Posibilitatea actualizării semnăturilor de virus la nivelul staţiei de lucru atât la cerere, cât şi automat, fără intervenţia utilizatorului, în mod silenţios (*unattended*).

3.9.4. Posibilitatea administratorului de a configura automat sau cu confirmare din partea utilizatorului, în situaţia în care este necesară repornirea echipamentului după încheierea unei actualizări

3.9.5. Securizarea sistemului de actualizare a semnăturilor de virus şi a motorului de scanare, prin mecanisme de semnare a fişierelor de către producător.

4. CERINŢE PRIVIND OPERAŢIONALIZAREA SERVICIILOR

4.1. Instalarea serviciilor

4.1.1. Soluţia trebuie să fie instalată pe toate echipamentele specificate în contractul subsecvent: servere fizice şi virtuale, staţii de lucru, thin clients şi dispozitive mobile.

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

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

4.2. Instruirea personalului achizitorului

4.2.1. Prestatorul, pe cheltuiala sa, trebuie să asigure achizitorului instruire de specialitate sub formă de cursuri, pentru serviciile prestate astfel:

(a) instruirea: în maximum 90 de zile de la semnarea contractului subsecvent

(b) locaţia de instruire: într-o locaţie adecvată procesului de instruire

(c) instruirile pot fi realizate prin cumularea cererilor de la mai multe autorităţi contractante

(d) suportul de curs: asigurat de prestator

(e) materialul didactic: în format fizic cât şi electronic (pe suport optic sau USB-flash)

(f) numărul cursanţilor pentru fiecare contract subsecvent: 2 – 20

(g) numărul grupelor pentru fiecare contract subsecvent: 1 – 3;

(h) durata cursului: cel puţin 5 zile pentru fiecare serie

4.2.2. Organizarea instruirii trebuie să ţină cont cel puţin de următoarele cerinţe:

(a) procesul de instruire trebuie asigurat de prestator în cadrul fiecărui contract subsecvent.

(b) numărul exact al cursanţilor şi numărul grupelor în care vor fi distribuiţi trebuie stabilit la fiecare contract subsecvent în limitele precizate la lit. (a), în funcţie de necesităţile operaţionale ale achizitorului.

(c) o grupă de instruire poate cuprinde cursanţi ai mai multor achizitori, astfel încât să fie completat în mod eficient numărul locurilor disponibile.

4.2.3. Instruirea trebuie să abordeze cel puţin următoarele subiecte:

(a) problematica generală şi specifică a virusilor IT

(b) utilizarea, configurarea şi administrarea serviciilor contractate

(c) curs de analiză *malware* şi *spyware* ce trebuie să includă:

- fundamentele analizei *malware*
- analiza codului maliţios
- analiza *malware* în detaliu
- analiza coduri *malware* cu protecţie la detectare
- dezasamblare cod
- analiza memoriei RAM şi a documentelor maliţioase (ex.: pdf, docx, xls sau similar etc.)
- analiza infecţiilor tip root kit

Cursul de analiză malware și spyware menționat la litera (c), va fi organizat numai dacă se achiziționează serviciile menționate la punctul 5.8, literele (b) și (d).

4.3. Asistenţa tehnică

4.3.1. Prestatorul trebuie să asigure asistenţă tehnică pe toată durata acordului cadru şi a contractelor subsecvente 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).

4.3.2. Elementele fluxului de tratare a evenimentelor sunt următoarele:

(a) evenimentul de securitate informatică detectat de beneficiar în perioada de derulare a contractului subsecvent se notifică prestatorului prin e-mail/site web/telefonic, solicitându-i-se intervenţia; notificarea conţine obligatoriu o descriere detaliată a problemei, precum şi încadrarea în nivelul de criticitate definit la 4.3.3, apreciat de beneficiar.

(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

MINISTERUL AFACERILOR INTERNE
ŞI TEHNOLOGIA INFORMAȚIEI
AVIZAT TEHNIC
Semnătura _____ Data 20.02.2014

(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 contractul subsecvent vor fi precizate toate detaliile necesare

4.3.3. 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.

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

MINISTERUL APĂRĂRII NAȚIONALE
DIRECȚIA PENTRU COMUNICAȚII ȘI SISTEME INFORMATICE
Semnătura Data 20.02.2020

5. CONDIŢII DE LIVRARE, INSTALARE ŞI ACCEPTANŢĂ

5.1. În cadrul fiecărui contract subsecvent, instalarea şi configurarea serviciilor trebuie să înceapă cât mai curând posibil, dar nu mai târziu de 10 zile calendaristice de la semnarea contractului subsecvent şi se va finaliza în termenul de instalare ce se va menţiona în contractul subsecvent.

5.2. Acceptanța la beneficiar a instalării și configurării serviciilor va avea loc, după încheierea tuturor procedurilor de instalare și configurare și întocmirea procesului verbal de acceptanță.

5.3. În cazul în care, din vina sa exclusivă, prestatorul depășește termenul de instalare și configurare, prevăzut în contractul subsecvent, achizitorul are dreptul de a solicita și 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.

5.4. În cadrul fiecărui contract subsecvent, prestatorul va pune la dispoziţia achizitorului pe suport optic toate kit-urile necesare precum şi documentaţia tehnică pentru instalarea, configurarea, administrarea şi mentenanţa serviciilor livrate; oferta tehnică trebuie să includă inventarul livrabilelor.

5.5. Conţinutul procedurii de testare, propusă de fiecare promitent-prestator, în vederea acceptanţei la beneficiar, trebuie avizat de către structura centrală cu atribuții de coordonare a activităţii IT din MAI.

5.6. Procedura de testare în vederea acceptanţei la beneficiar avizată de structura centrală a beneficiarului devine obligatorie pentru fiecare promitent–prestator şi va fi parte a contractelor subsecvente.

5.7. În cadrul implementării contractelor subsecvente, procedura de testare în vederea acceptanţei la beneficiar trebuie să înceapă cât mai curând posibil după încheierea procedurilor de instalare şi configurare, consemnată prin proces verbal de recepţie a livrabilelor, dar nu mai târziu de 3 zile lucrătoare de la data încheierii acestor proceduri.

5.8. Detalierea serviciilor de protecție informatică antivirus și antimalware, este următoarea:

(a) serviciu de protecţie informatică antivirus și antimalware pentru stații de lucru

(b) serviciu de protecţie informatică antivirus și antimalware pentru servere

(a) serviciu de protecţie informatică antivirus și antimalware pentru stații de lucru
(b) serviciu de protecţie informatică antivirus și antimalware pentru servere
(c) serviciu de protecţie informatică antivirus și antimalware pentru dispozitive portabile
(d) serviciu de protecţie informatică antivirus și antimalware pentru soluții de virtualizare
(e) serviciu de protecţie informatică antivirus și antimalware pentru thin clients

5.9. Pentru stabilirea clasamentului în acordul cadru se va aplica în mod exclusiv criteriul „preţul cel mai scăzut". Sunt declarate câştigătoare ofertele admisibile clasate pe primele patru locuri, în caz contrar se aplică prevederile art. 148^1 din O.U.G. nr. 34/2006 şi vor participa după caz la procesul de reluare a competiţiei pentru adjudecarea contractelor subsecvente.

5.10. În contractele subsecvente, clasamentul promitenţilor–prestatori se întocmeşte în ordinea crescătoare a preţurilor totale ale ofertelor configurate în conformitate cu necesităţile operaţionale de servicii formulate de fiecare promitent–achizitor în conformitate cu prevederile prezentului caiet de sarcini; este declarată câştigătoare oferta cu preţul total cel mai scăzut.

6. DISPOZIȚII FINALE

6.1. Promitentul-prestator care a încheiat cel puțin un contract subsecvent, va prezenta lunar și ori de câte ori intervine o modificare, către autoritatea contractantă, următoarele date, într-o formă structurată:

- Beneficiarul contractului subsecvent, numărul, data, valoarea și perioada de valabilitate a contractului subsecvent.
- Tipul și valoarea serviciilor care fac obiectul contractului (ex.: Protecție informatică pentru stații de lucru – număr de stații protejate – valoare totală serviciu, protecție informatică pentru servere – număr de servere protejate – valoare totală serviciu, etc).
- Numărul, data și valoarea facturilor emise, contractul subsecvent în baza căruia se emite factura, valoarea și data plăților, precum și numărul, valoarea și motivul valoarea penalităților emise sau primite, dacă este cazul.
- Raportul va fi transmis către autoritatea contractantă, atât pe hârtie cât și în format electronic.

6.2. Promitentul-prestator care a încheiat cel puțin un contract subsecvent, va informa autoritatea contractantă cu privire la finalizarea contractului subsecvent, nu mai târziu de 10 zile de la data finalizării acestuia.

Anexa nr. 1

Denumirea serviciilor, cantităţile şi valorile estimate ale acestora

TIP SERVICIU	U.M	Pret unitar estimat (lei fara TVA)	Pret unitar estimat (euro fara TVA)	Cant. AC (pentru 4 ani)		Cant. CS (pentru 1 an)		Valoare AC (pentru 4 ani)				Valoare CS (pentru 1 an)			
				min	max	min	max	valoarea minimă (lei/euro fără TVA)		valoarea maximă (lei/euro fără TVA)		valoarea minimă (lei/euro fără TVA)		valoarea maximă (lei/euro fără TVA)	
servicii de protectie informatica antivirus si antimalware pentru statii de lucru	buc	169,06	37,20	1	65.586	1	30.000	676,24	148,80	44.351.876,64	9.759.196,80	169,06	37,20	5.071.800,00	1.116.000,00
servicii de protectie informatica antivirus si antimalware pentru servere	buc	209,82	46,17	1	3.458	1	1.000	839,28	184,68	2.902.230,24	638.623,44	209,82	46,17	209.820,00	46.170,00
servicii de protectie informatica antivirus si antimalware pentru dispozitive portabile	buc	82,53	18,16	1	495	1	400	330,12	72,64	163.409,40	35.956,80	82,53	18,16	33.012,00	7.264,00
servicii de protectie informatica antivirus si antimalware pentru solutii de virtualizare	buc	1.363,41	300,00	1	283	1	85	5.453,64	1.200,00	1.543.380,12	339.600,00	1.363,41	300,00	115.889,85	25.500,00
servicii de protectie informatica antivirus si antimalware pentru thin clients	buc	169,06	37,20	1	631	1	450	676,24	148,80	426.707,44	93.892,80	169,06	37,20	76.077,00	16.740,00
Valoare totala estimata								**7.975,52**	**1.754,92**	**49.387.603,84**	**10.867.269,84**	**1.993,88**	**438,73**	**5.506.598,85**	**1.211.674,00**

S-a avut în vedere cursul euro BNR din data de 10.01.2014, 1 euro = 4,5447 lei