

## CAIET DE SARCINI

Acord cadru pentru servicii lunare de  
protecție informatică antivirus și antimalware  
la nivelul Ministerului Afacerilor Interne

### 1. INTRODUCERE

- 1.1. Obiectul prezentului caiet de sarcini este achiziționarea serviciilor de asigurare a protecției antivirus, antispam și antimalware pentru infrastructura IT a Aparatului Central al Ministerului Afacerilor Interne (denumit în continuare MAI), precum și pentru infrastructurile IT aflate la nivelul ordonatorilor de credite din subordinea MAI, prevăzuți în anexa nr. 1 la modelul de acord cadru.
- 1.2. Achiziționarea serviciilor este necesară pentru protejarea împotriva virusilor informatici și software-ului de tip *malware*, *spyware*, *spam* și de altă natură, în măsură să afecteze securitatea și disponibilitatea rețelei de calculatoare a MAI și echipamentelor de calcul individuale neconectate în rețea, inclusiv a dispozitivelor portabile.
- 1.3. Serviciile au ca scop asigurarea protecției infrastructurii informatice (stații de lucru, thin clients, servere fizice și virtualizate și dispozitive mobile) împotriva atacurilor informatice generale și particulare; soluția trebuie să minimizeze riscul contaminării cu virusi informatici sau alte programe malițioase și să asigure protecția eficientă împotriva vulnerabilităților cunoscute.
- 1.4. Pentru asigurarea serviciilor, licențele software proprii sau terțe vor fi asigurate de către prestator în concordanță cu necesitățile operaționale, fără costuri suplimentare din partea beneficiarului.
- 1.5. Produsele care asigură îndeplinirea serviciilor oferite, la momentul depunerii ofertei, trebuie să nu fie *end-of-life*; în situația în care independent de voința prestatorului un produs al unui terț ajunge *end-of-life* pe timpul derulării contractului subsecvent la acordul cadru, înlocuirea acestuia se face pe cheltuiala prestatorului, cu un produs având cel puțin specificațiile și performanțele celui oferit.
- 1.6. În funcție de necesitățile operaționale și disponibilitatea alocării fondurilor bugetare, fiecare ordonator de credite din structura MAI prevăzut în anexa nr. 1 la modelul de acord cadru, poate încheia în condițiile specificate la punctele 2.1.1 - 2.1.11, contracte subsecvente la acordul cadru, cu unul din promitenții-prestatori declarați câștigători, în urma derulării procesului de reluare a competiției, în condițiile dispozițiilor art. 150 din O.U.G nr. 34/2006, cu modificările și completările ulterioare.
- 1.7. Cerințele prezentului Caiet de Sarcini sunt minimale și obligatorii.

## 2. SPECIFICAȚII GENERALE

### 2.1. Specificații privind oferta

- 2.1.1.** Atribuirea contractelor subsecvente în baza acordului cadru se va face prin reluarea competiției în conformitate cu specificațiile din capitolul 4 al prezentului caiet de sarcini, aplicând criteriul de atribuire „prețul cel mai scăzut”.
- 2.1.2.** Atât în acordul cadru cât și cu ocazia reluării competiției, fiecare promitent-prestator este obligat să prezinte câte o ofertă și numai una pentru fiecare dintre serviciile precizate la punctul 5.8 al prezentului caiet de sarcini, să aparțină aceluiași producător (excepție face componenta antivirus pentru dispozitivele portabile, cap. 3.2, ce poate aparține unui alt producător); nu sunt admise oferte alternative pentru același 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 aceeași 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, desfășurată în conformitate cu prevederile subcapitolului 4.2.
- 2.1.6.** În procesul de reluare a competiției, în vederea atribuirii unui contract subsecvent, achizitorul va solicita promitenților–prestatori semnături ai acordului cadru oferte pentru servicii de protecție informatică antivirus și antimalware descrise la punctul 5.8.
- 2.1.7.** Cantitățile minime și 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 preț per serviciu.
- 2.1.9.** Prin contractul subsecvent, fiecare autoritate contractantă achiziționează doar acele servicii prevăzute la punctul 5.8, în cantitățile necesare, în funcție de nevoile operaționale și fondurile bugetare alocate, fără a avea obligația de a achiziționa toate serviciile care fac obiectul acordului cadru.
- 2.1.10.** În cadrul procedurii de reluare a competiției la nivelul ordonatorilor de credite din MAI, prețurile per serviciu individual oferite de semnatarul acordului-cadru, se pot modifica doar în sensul îmbunătățirii acestora față de oferta inițială din acordul cadru, în conformitate cu prevederile art. 69 alin. (3) din HG 925/2006, cu modificările și completările ulterioare. Adjudecarea se va face pe oferta totală a serviciilor oferite.
- 2.1.11.** În cadrul procesului de reluare a competiției, în cazul în care, în urma reoferțării, autoritatea contractantă nu obține îmbunătățiri ale elementelor/ condițiilor care fac obiectul reluării competiției, aceasta are obligația de a atribui contractul ofertantului clasat pe primul loc în cadrul procedurii aplicate pentru încheierea acordului-cadru,

prin luarea în considerare a condițiilor și elementelor prevăzute în oferta inițială 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 competiției, la care au obligația să participe și să depună ofertă toți promitenții-prestatori semnatari ai acordului cadru.

## 2.2. Specificații generale ale soluției 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 și ale tuturor serviciilor livrate, precum și serviciile de suport tehnic, fără costuri suplimentare din partea achizitorului.
- 2.2.2. În situația constatării de deficiențe sau neconcordanțe între caracteristicile tehnico-funcționale ale unui serviciu prestat și 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 și documentațiile necesare, fiecărei structuri a MAI care încheie un contract subsecvent.

## 2.3. Specificații generale ale serviciilor de protecție informatică antivirus

- 2.3.1. Serviciile de protecție informatică antivirus prestate trebuie să fie însoțite de certificatele de calitate.
- 2.3.2. Odată cu oferta tehnică, pentru serviciile antivirus livrate, prestatorul va prezenta cel puțin 1 certificat emis de una dintre organizațiile internaționale de profil *ICSA Labs, Checkmark, Virus Bulletin*.
- 2.3.3. Actualizarea semnăturilor de virus și a versiunilor atât pentru stații de lucru, servere cât și pentru serviciile de virtualizare trebuie să se poată efectua periodic în mod automat și/sau manual, în funcție de opțiunea 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, funcțiile de protecție trebuie să fie asigurate printr-un singur motor de scanare instalat și să poată rula scanările programate cu prioritate redusă (*background*).
- 2.3.5. Serviciile antivirus trebuie să aibă opțiunea de scanare automată a fișierelor înainte de copierea/instalarea acestora.
- 2.3.6. Serviciile antivirus trebuie să permită instalarea/activarea personalizată a modulelor componente, în funcție de nevoi.
- 2.3.7. Interfețele și documentațiile componentelor de servicii trebuie să fie în limba română.
- 2.3.8. Serviciile antivirus trebuie să fie compatibile cu sistemele de operare în funcție de tehnologia pe care este instalat sistemul de operare (32/64 biți) pentru: *Windows Server 2003, Windows Server 2008 R2, Windows Server 2012, Windows XP, Windows Vista, Windows 7, Windows 8, VMWare* și rețeaua TCP/IP.



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

2.3.10. Caracteristicile jurnalelor funcționale sunt următoarele:

- (a) format: XML, syslog sau alt format standardizat
- (b) conținut: evenimente relevante ale funcționării fiecărui modul structură (minimală, dar nu restrictivă): (1) moment de timp, (2) identificator sursă, (3) descriere eveniment, (4) rezultat.

## 2.4. Specificații generale ale serviciilor de suport

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

2.4.2. Orice noi informații privind posibile amenințări trebuie să fie puse la dispoziția beneficiarului cu maximă urgență prin mesaje electronice de alertă în cazul unor noi viruși distructivi sau cu potențial mare de răspândire.

2.4.3. La solicitarea beneficiarului, prestatorul trebuie să fie în măsură să răspundă la incidentele provocate de atacuri ale virușilor sau software-ului malițios în termen de 24 ore prin deplasarea și intervenția în locațiile fizice ale beneficiarului.

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

2.4.5. Prestatorul trebuie să pună la dispoziție servicii de suport tehnic de instalare, configurare, diagnoză și remediere exclusiv în limba română, în regim 24/7, atât telefonic cât și 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 puțin o dată pe lună) *in-site* în scopul verificării funcționării serviciilor prestate și remedierii eventualelor disfuncționalități; concluziile vizitei vor fi consemnate într-un proces verbal întocmit în două exemplare, câte unul pentru fiecare parte, și care se va atașa la documentele care se întocmesc pentru efectuarea plății lunare a serviciilor.

## 3. CARACTERISTICI TEHNICE

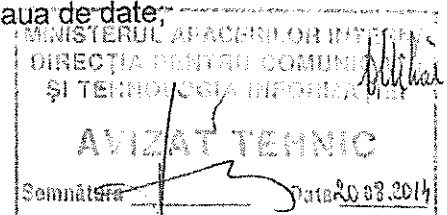
### 3.1. Caracteristici tehnice ale componentei antivirus și antispyware pentru servere, stații de lucru și thin clients

3.1.1. Asigură minimum 3 tipuri de detecție:

- (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) și "on demand" (la cerere) pentru:

- (a) suportii de stocare a informației: FDD, HDD, CD-ROM, USB Flash Memory, SSD, cititoare de card;
- (b) fișierele care se copiază de pe suport extern și din rețeaua de date;
- (c) arhive ARJ, ACE, CAB, ZIP, RAR, TAR, GZ;



- (d) arhivele de mesagerie electronică (e-mail);
- (e) transferurile de fișiere în comunicații P2P (instant messaging);
- (f) anumite tipuri de fișiere (listă configurabilă) sau pentru toate fișierele;
- (g) anumite dimensiuni de arhive (dimensiune maximă configurabilă);
- (h) anumite căi (listă configurabilă).

3.1.3. În funcție de nevoi, opțiunile și listele de scanare de la pct. 3.1.2. sunt configurabile de către administrator; configurările "la cerere" („on demand”) sunt accesibile și la nivelul utilizatorului obișnuit.

3.1.4. Administratorul poate gestiona liste de excludere de la scanarea anumitor directoare, suporturi de stocare, fișiere sau extensii, precum și fișiere cu anumite dimensiuni, configurabile.

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

3.1.6. Permite opțiunea de pauză și reluare a sarcinilor de scanare.

3.1.7. Asigură monitorizarea activă a regiștrilor sistemului de operare afișând mesaje de atenționare în momentul în care o aplicație încearcă să îi modifice.

3.1.8. Asigură protecție *spyware*.

3.1.9. Permite funcționarea clientului antivirus în oricare dintre următoarele moduri:

- (a) în rețea, în interacțiune cu software-ul de management și actualizare
- (b) *standalone* (cu sau fără suport de rețea).

3.1.10. Actualizarea bazei de date locale cu semnături antivirus și antispyware a clientului se face fără intervenția utilizatorului, de regulă de pe serverul special destinat, însă la nevoie poate fi configurată și o altă locație de rețea. Atât clienții cu management cât și clienții instalați *standalone* trebuie să aibă opțiunea 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:

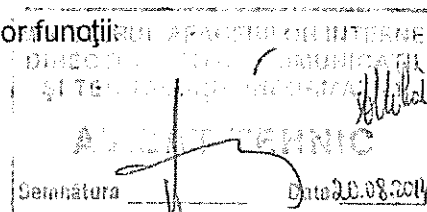
- (a) Windows 7, Windows 8
- (b) Google Android (începând cu versiunea 2.3)
- (c) iOS (începând cu versiunea 7)

3.2.2. Componenta antivirus instalată pe dispozitivele portabile trebuie să asigure cel puțin următoarele funcții de protecție:

- (a) protecția *animalware* și *antiphishing*;
- (b) scanarea cardurilor SD (*Secure Digital*);
- (c) protecția datelor stocate pe dispozitivul portabil.

### 3.3. Caracteristici tehnice ale modulului firewall pentru servere

Modulul *firewall* trebuie să asigure îndeplinirea următoarelor funcții:



- 3.3.1. Asigură protecția datelor și filtrarea traficului la intrare și la ieșire, controlând fișierele de tip cookie, blocând scripturile malițioase și 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 opțiunea de instalare/dezinstalare și activare/dezactivare în funcție de necesități.

#### 3.4. Caracteristici tehnice ale modulului *antispam* pentru servere, stații de lucru și thin clients

Modulul *antispam* trebuie să asigure îndeplinirea următoarelor funcții:

- 3.4.1. Adaptarea la noile tehnici de lansare a *spam*-ului, analizând și memorând preferințele 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 chinezești).
- 3.4.4. Utilizarea filtrului *antispam* „*antrena*” pe baza unei serii de mesaje *spam* astfel încât acesta să poată recunoaște noile mesaje de acest tip prin identificarea asemănărilor cu cele pe care le-a examinat deja.
- 3.4.5. Permite opțiunea de instalare/dezinstalare în funcție de necesități.
- 3.4.6. Pentru serverele de e-mail, componenta antimalware și *antispam* trebuie să includă suport pentru sistemul de operare GNU/Linux, distribuțiile *RedHat*, *Suse* și *Debian* cât și kernelurile versiunile 2.4, 2.6 și 3. De asemenea, trebuie să fie de tip modular și integrabil cu MTA-urile existente: *CommuniGate*, *Postfix*, *Sendmail*.

#### 3.5. Caracteristici tehnice ale modulului *carantină* pentru stații de lucru, servere, thin clients și virtualizare

Modulul *carantină* trebuie să asigure îndeplinirea următoarelor funcții:

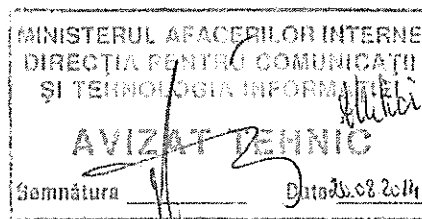
- 3.5.1. Restaurarea fișierelor din *carantină* în locațiile lor originale.
- 3.5.2. Trimiterea manuală sau automată a fișierelor din *carantină* către *laboratorul antivirus*.

#### 3.6. Caracteristici tehnice ale modulului „*administrare și instalare remote*” pentru stații de lucru, servere și virtualizare

Modulul *administrare și instalare remote* trebuie să asigure îndeplinirea următoarelor funcții:

- 3.6.1. Console centrale de management ce vor facilita administrarea și instalarea agenților. După caz, soluția de virtualizare poate necesita una sau mai multe console pentru instalarea, configurarea, monitorizarea și raportarea stării de securitate a stațiilor de lucru și a serverelor virtualizate.
- 3.6.2. Consola de management trebuie să îndeplinească următoarele funcții minimale:

- (a) identificarea echipamentelor accesibile în rețea



- (b) gruparea și gestionarea grupărilor de clienți antivirus pentru echipamentele din rețea
- (c) identificarea stării echipamentelor din punctul de vedere al instalării soluției antivirus
- (d) identificarea stării de activare globală și individuală a funcțiilor (activ/inactiv) și schimbarea acestora în funcție de necesități
- (e) identificarea stării de actualizare și forțarea actualizării la nevoie
- (f) gestionarea licențelor
- (g) crearea kit-ului de instalare personalizat destinat atât sistemelor de operare de 32 biți cât și celor de 64 biți
- (h) crearea șabloanelor de raportări suplimentare față de cele predefinite

**3.6.3.** Consola trebuie să aibă integrat un modul dedicat controlului activității utilizatorilor, cu următoarele funcții minimale:

- (a) restricționarea accesului la *Internet* pentru anumiți clienți sau grupuri de clienți
- (b) restricționarea accesului la *Internet* pentru anumite aplicații
- (c) restricționarea accesului la *Internet* pentru anumite perioade de timp
- (d) blocarea paginilor *web* care conțin anumite cuvinte cheie

**3.6.4.** Accesul la consola de management în urma introducerii credențialelor de acces (username și parolă)

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

### **3.7. Caracteristici tehnice ale modulului *rapoarte, grafice și alerte* pentru stații de lucru, servere, thin clients și virtualizare**

Modulul *rapoarte, grafice și alerte* trebuie să asigure îndeplinirea următoarelor funcții:

**3.7.1.** Crearea de rapoarte pe baza șabloanelor definite în consola de management.

**3.7.2.** Generarea de rapoarte complete privind rezultatele scanării și infecțiilor detectate dar și a tuturor obiectelor scanate, inclusiv la nivelul clienților.

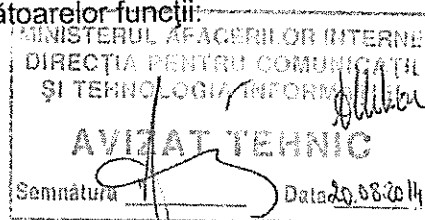
**3.7.3.** Generarea în mod automat, în cazul detecției unui eveniment, a unui mesaj de alertă către una sau mai multe adrese de *e-mail* prin intermediul componentei centralizate

**3.7.4.** Generarea rapoartelor în mod programat și 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 rețea* pentru stații de lucru, thin client, servere și virtualizare**

Modulul *audit rețea* trebuie să asigure îndeplinirea următoarelor funcții:



- 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 șabloanelor de raportare predefinite sau personalizate
- 3.8.3. Trimiterea rapoartelor, prin e-mail

### 3.9. Caracteristici tehnice ale modulului „actualizare” pentru stații de lucru, servere, thin clients și virtualizare

Modulul *actualizare* trebuie să asigure îndeplinirea următoarelor funcții:

- 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 disponibilității unei noi actualizări.
- 3.9.3. Posibilitatea actualizării semnăturilor de virus la nivelul stației de lucru atât la cerere, cât și automat, fără intervenția utilizatorului, în mod silențios (*unattended*).
- 3.9.4. Posibilitatea administratorului de a configura automat sau cu confirmare din partea utilizatorului, în situația în care este necesară repornirea echipamentului după încheierea unei actualizări
- 3.9.5. Securizarea sistemului de actualizare a semnăturilor de virus și a motorului de scanare, prin mecanisme de semnare a fișierelor de către producător.

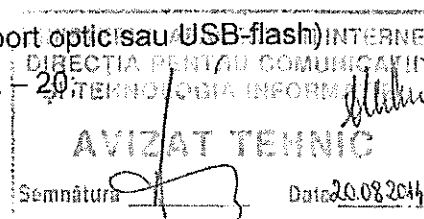
## 4. CERINȚE PRIVIND OPERAȚIONALIZAREA SERVICIILOR

### 4.1. Instalarea serviciilor

- 4.1.1. Soluția trebuie să fie instalată pe toate echipamentele specificate în contractul subsecvent: servere fizice și virtuale, stații de lucru, thin clients și dispozitive mobile.
- 4.1.2. În procesul de instalare și configurare a componentelor software prevalează limitările și regulile de securitate impuse de achizitor.
- 4.1.3. Politica de actualizare a semnăturilor de virus trebuie să nu producă blocaje la nivelul locațiilor, iar activarea ulterioară a licențelor 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) locația de instruire: într-o locație adecvată procesului de instruire
  - (c) instruirile pot fi realizate prin cumularea cererilor de la mai multe autorități contractante
  - (d) suportul de curs: asigurat de prestator
  - (e) materialul didactic: în format fizic cât și electronic (pe suport optic sau USB-flash)
  - (f) numărul cursanților pentru fiecare contract subsecvent: 2 – 20





- (g) numărul grupelor pentru fiecare contract subsecvent: 1 – 3;
- (h) durata cursului: cel puțin 5 zile pentru fiecare serie

**4.2.2.** Organizarea instruirii trebuie să țină cont cel puțin de următoarele cerințe:

- (a) procesul de instruire trebuie asigurat de prestator în cadrul fiecărui contract subsecvent.
- (b) numărul exact al cursanților și numărul grupelor în care vor fi distribuiți trebuie stabilit la fiecare contract subsecvent în limitele precizate la lit. (a), în funcție de necesitățile operaționale ale achizitorului.
- (c) o grupă de instruire poate cuprinde cursanți ai mai multor achizitori, astfel încât să fie completat în mod eficient numărul locurilor disponibile.

**4.2.3.** Instruirea trebuie să abordeze cel puțin următoarele subiecte:

- (a) problematica generală și specifică a virusilor IT
- (b) utilizarea, configurarea și administrarea serviciilor contractate
- (c) curs de analiză *malware* și *spyware* ce trebuie să includă:
  - fundamentele analizei *malware*
  - analiza codului malițios
  - analiza *malware* în detaliu
  - analiza coduri *malware* cu protecție la detectare
  - dezasamblare cod
  - analiza memoriei RAM și a documentelor malițioase (ex.: pdf, docx, xls sau similar etc.)
  - analiza infecțiilor tip root kit

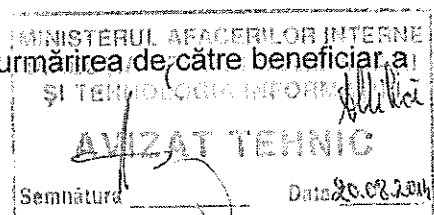
Cursul de analiză *malware* și *spyware* menționat la litera (c), va fi organizat numai dacă se achiziționează serviciile menționate la punctul 5.8, literele (b) și (d).

**4.3. Asistența tehnică**

**4.3.1.** Prestatorul trebuie să asigure asistență tehnică pe toată durata acordului cadru și 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 modalitățile de contact (telefon, fax, e-mail, sms).

**4.3.2.** Elementele fluxului de tratare a evenimentelor sunt următoarele:

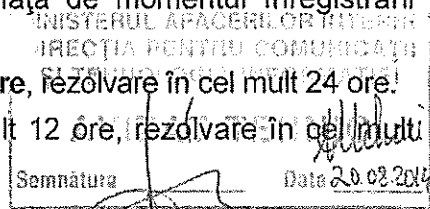
- (a) evenimentul de securitate informatică detectat de beneficiar în perioada de derulare a contractului subsecvent se notifică prestatorului prin e-mail/site web/telefonice, solicitându-i-se intervenția; notificarea conține obligatoriu o descriere detaliată a problemei, precum și încadrarea în nivelul de criticitate definit la 4.3.3, apreciat de beneficiar.
- (b) orice solicitare de intervenție 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 aceeași cale pe care a fost recepționată solicitarea de intervenție
- (c) numărul tichetului servește ca referință 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 dispoziția beneficiarului instrumente de verificare *on-line* a tichetelor proprii din evidența 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 față de momentul înregistrării solicitării de intervenție):

- (a) în cazul evenimentelor critice: **răspuns în cel mult 2 ore, rezolvare în cel mult 24 ore!**
- (b) în cazul evenimentelor obișnuite: răspuns în cel mult 12 ore, rezolvare în cel mult 72 ore.



## 5. CONDIȚII DE LIVRARE, INSTALARE ȘI ACCEPTANȚĂ

- 5.1. În cadrul fiecărui contract subsecvent, instalarea și configurarea serviciilor trebuie să înceapă cât mai curând posibil, dar nu mai târziu de 10 zile calendaristice de la semnarea contractului subsecvent și se va finaliza în termenul de instalare ce se va menționa 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 penalități 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 obligațiilor.
- 5.4. În cadrul fiecărui contract subsecvent, prestatorul va pune la dispoziția achizitorului pe suport optic toate kit-urile necesare precum și documentația tehnică pentru instalarea, configurarea, administrarea și mentenanța serviciilor livrate; oferta tehnică trebuie să includă inventarul livrabilelor.
- 5.5. Conținutul procedurii de testare, propusă de fiecare promitent-prestator, în vederea acceptanței la beneficiar, trebuie avizat de către structura centrală cu atribuții de coordonare a activității IT din MAI.
- 5.6. Procedura de testare în vederea acceptanței la beneficiar avizată de structura centrală a beneficiarului devine obligatorie pentru fiecare promitent-prestator și va fi parte a contractelor subsecvente.
- 5.7. În cadrul implementării contractelor subsecvente, procedura de testare în vederea acceptanței la beneficiar trebuie să înceapă cât mai curând posibil după încheierea procedurilor de instalare și configurare, consemnată prin proces verbal de recepție 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 protecție informatică antivirus și antimalware pentru stații de lucru
  - (b) serviciu de protecție informatică antivirus și antimalware pentru servere

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

**5.9.** Pentru stabilirea clasamentului în cadrul se va aplica în mod exclusiv criteriul „prețul cel mai scăzut”. Sunt declarate câștigătoare ofertele admisibile clasate pe primele patru locuri, în caz contrar se aplică prevederile art. 148<sup>1</sup> din O.U.G. nr. 34/2006 și vor participa după caz la procesul de reluare a competiției pentru adjudecarea contractelor subsecvente.

**5.10.** În contractele subsecvente, clasamentul promitenților–prestatori se întocmește în ordinea crescătoare a prețurilor totale ale ofertelor configurate în conformitate cu necesitățile operaționale de servicii formulate de fiecare promitent–achizitor în conformitate cu prevederile prezentului caiet de sarcini; este declarată câștigătoare oferta cu prețul 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.

## Denumirea serviciilor, cantitățile și 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)	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 protecție informatică antivirus și antimalware pentru stații 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 protecție informatică antivirus și 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 protecție informatică antivirus și 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 protecție informatică antivirus și 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 protecție informatică antivirus și 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
<b>Valoare totala estimata</b>								<b>7.975,52</b>	<b>1.754,92</b>	<b>49.387.603,84</b>	<b>10.867.269,84</b>	<b>1.993,88</b>	<b>438,73</b>	<b>5.506.598,85</b>	<b>1.211.674,00</b>

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