

SPECIFICAȚIA TEHNICĂ

Nr. crt	Denumirea bunurilor	Cod CPV	Cantitat ea (licențe)	Prețul MD (incl. TVA)	Suma totală MD (inclusiv TVA)
1.	Procurarea programului antivirus (Pachetul software antivirus pentru 12 computere + 2 servere), vezi componentele sistemului antivirus solicitate.	48761000 - 0	12 + 2 = 14		
	TOTAL				

I. Componentele sistemului antivirus:

A. Protecție

1. Controlul programelor active

* Încredere față de programele care au o semnătură digitală

Pentru programe necunoscute:

* Introducerea automată într-un grup (restricții slabe, restricții puternice, nesigur)

* Utilizare analiza euristică pentru a determina grupul

* Eliminarea regulilor de control ale programului care nu au accesat mai mult de un anumit număr de zile.

2. File Anti-Virus

* Nivel de securitate (scăzut, recomandat, ridicat)

* Acțiune când se detectează o amenințare (solicitați acțiune, blocați accesul (dezinfecțai / ștergeți dacă dezinfecția nu reușește))

* Tipuri de fișiere (toate fișierele, fișierele scanate după format, fișierele scanate prin extensie)

* Localizare (toate unitățile detașabile, toate unitățile hard disk, toate unitățile de rețea)

* Analiza semnăturii

* Analiza euristică (suprafață, medie, profundă)

* Optimizarea verificării

- Scanarea numai a fișierelor noi și modificate

* Verificarea fișierelor compuse:

- Scanare arhive

- Verificare pachetele de instalare

- Verificare obiecte OLE imbricate

- Verificare obișnuită - opțională (despachetați fișierele compuse în fundal / despachetați fișiere compozite de dimensiuni mari)

* Modul de testare (inteligent, la accesarea și schimbarea, la accesare, în timpul execuției)

* Tehnologii de scanare (iSwift, iChecker)

* Suspendarea sarcinii (conform programului, la începutul programelor) este opțională

3. Firewall

* Reguli pentru programe

* Reguli pentru pachete

* Zone (rețele disponibile)

* Sistem de detectare a intruziunilor

-blocați computerul atacat pentru un anumit număr de minute

4. Antivirusul poștal

* Nivel de securitate (scăzut, recomandat, ridicat)

* Zonă de protecție (numai mesaje primite și trimise / mesaje primite)

* Integrarea în sistem (POP3 trafic / SMTP / NNTP / IMAP, ICQ / MSN, MS Office Outlook plug-in, plug-in The Bat)

* Metodele de verificare (a verifica link-urile pe baza Web-link-uri suspecte, verificare link-urile pe baza fishing Web-link-uri)

* Analiza euristică (suprafață, medie, profundă)

* Verificarea fișierelor compuse:

- Posibilitatea de scanați ori ne scanare arhivele

- Posibilitatea de scanați ori ne scanare obiecte cu un anumit volum

* Filtru atașament (după formatul fișierului)

5. Web-antivirus

* Metode de verificare (verificați linkurile către baza de date a adreselor Web suspecte, verificați linkurile către baza de date a adreselor Web de fishing)

* Limitați timpul cache al fragmentelor în câteva secunde.

* adrese de încredere (add / change / delete / export / import)

* Acțiune (cerere / bloc / permite)

6. Protecție pro activă

- * Analiza activității proceselor
- * Monitorizarea sistemului de registru

7. Anti-hacker

- * Reguli pentru programe
- * Reguli pentru pachete
- * Zone (rețele disponibile)
- * Sistem de detectare a intruziunilor
Blocați computerul atacat pentru un anumit număr de mine.

8. Anti-Spy

- * Anti-banner (lista neagră, lista albă)
- * Anti-apelare (adrese de încredere)

9. Anti-Spam

- * Nivelul de agresivitate (scăzut, recomandat, ridicat, blocați tot)
- * Integrarea în sistem (POP3 trafic / SMTP / NNTP / IMAP, ICQ / MSN, MS Office Outlook plug-in, plug-in The Bat)
- * Metodele de verificare (a verifica link-urile pe baza Web-link-uri suspecte, verificați link-urile pe baza phishing Web-link-uri)
- * Algoritmi pentru recunoaștere (analiza expresii lor pe baza de date Resent Terms, utilizarea unei baze de date extinse, analiza anteturilor și mesajelor PDB, recunoaștere a imaginii GSG, algoritmul de auto-învățare Bayes pentru analiza textului)
- * Lista albă
- * Lista neagră
- *Instruire (prezența maestrului de formare)

10. Controlul accesului

- * Lista dispozitivelor blocate
- * Auto start (dezactivați autor un pentru toate dispozitivele, dezactivați autorun.inf)

II. Scanare

Tipuri:

1. Scanare completă

2. Scanare rapidă

Specificarea:

- * Nivel de securitate (scăzut, recomandat, ridicat)
- * Acțiune când se detectează o amenințare (cereți la sfârșitul scanării, cereți în timpul scanării, nu întrebați: tratați, ștergeți dacă tratamentul nu este posibil)
- * Modul de lansare (în fiecare zi, în fiecare zi lucrătoare, la fiecare oră, în fiecare zi a lunii)
- * Domeniul de aplicare (toate fișierele, fișierele scanate după format, fișierele scanate prin extensie)
- * Verificarea fișierelor compuse:
 - Scanare arhive
 - Verificare pachetele de instalare
 - Verificare obiecte OLE imbricate
 - Scanare fișierelor de format e-mail
 - Scanare arhive protejate prin parolă
- * Analiza euristică (suprafață, medie, profundă)
- * Tehnologii de scanare (iSwift, iChecker)
- * Căutare Rootkit
- * Modul de lansare: executare sarcina cu drepturi de cont (nume de utilizator, parolă)

III. Actualizare

- * Mod de pornire: automat, după o anumită perioadă, manual

- * Setări proxy
- * Actualizare sursă (servere de actualizare firmei-producătorului. Servere de administrare, surse adăugătoare)
- * Modul de pornire:
 - executare sarcina cu drepturi de cont (nume de utilizator, parolă)
- * Distribuirea actualizărilor:
 - Copiați actualizările într-un dosar (adresa dosarului)

IV. Mai multe opțiuni

- * Auto-apărare a programului
 - * Dezactivare controlul extern al programului
 - * Protecția prin parolă
 - * Nu executați sarcini programate atunci când rulează pe baterie
 - * Carantină și spațiu de stocare de rezervă (nu mai mult de un anumit număr de zile de stocare a obiectelor, dimensiunea obiectelor, verificarea fișierelor în carantină după actualizare)
 - * Posibilitatea de controlate porturi (Control toate porturile / porturile selectate)
 - * Protecție antivirus pentru nodurile principale ale unei rețele: stații de lucru, laptopuri, servere de fișiere;
 - * Producătorul trebuie să facă parte din grupul liderilor ori a vizionarilor în ceea ce privește protecția pentru *end point* așa cum este definit de Gartner 2018.
- * Produsul trebuie să salveze obiectele identificate ca fiind suspecte în carantină sau într-un director dedicat în format criptat.
- * Produsul trebuie să permită ca instalarea să fie efectuată pe un computer local sau la distanță. Produsul trebuie să ofere suport pentru sisteme de operare Windows.
- * Consola de administrare a produsului trebuie să fie instalată on-permis (nu se accepta consola web).
- * Produsul trebuie să permită instalarea dintr-un singur kit de instalare care să includă toate pachetele necesare pentru implementare.
- * Produsul trebuie să ofere administratorului posibilitatea de împiedicare a acțiunilor periculoase pentru sistemul de operare ale aplicațiilor, și să asigure controlul accesului la resursele sistemului de operare și la datele confidențiale.
- * Produsul trebuie să permită crearea, păstrarea și implementarea imaginilor a sistemului de operare, cu ajutorul consolei de administrare dedicată.
 - * Produsul trebuie să permită detectarea automată a vulnerabilităților din sistemul de operare și a aplicațiilor instalate.
 - * Produsul trebuie să permită administratorului să identifice toate încercările utilizatorului de pornirea aplicației și să reglementeze lansarea aplicațiilor prin intermediul regulilor de control pentru pornirea aplicațiilor.

II. Cerințe față de Furnizorul de program antivirus licențiat:

- * Prezentarea de către Prestator a unui document de parteneriat confirmativ și MAF parvenit de la compania producător/filiala companiei producător.
- * Furnizorul trebuie să ofere instruiți gratuite pentru administratori de fiecare dată când apare o versiune nouă a soluției.