INSPECȚIA MUNCII

Nr.519 /C.A.P./16.04.2018

ANUNT

Inspectia Muncii, cu sediul in Bucuresti, str. Matei Voievod, nr 14, sector 2, in calitate de autoritate contractanta, organizează o achizitie directă pentru:

1. Extindere valabilitate pachet licențe antivirus Bitdefender pentru un an.
2. servicii de asistență tehnică informatică pentru instalarea și configurarea noilor versiuni și verificarea și asigurarea securității informatice la nivelul rețelei locale Inspecției Muncii și inspectoratelor teritoriale de muncă.

în conformitate cu prevederile art. 7, alin (5) din Legea nr 98/2016 privind achizitiile publice si ale art. 43-46 din HG nr. 395/2016 pentru aprobarea Normelor metodologice de aplicare a prevederilor referitoare la atribuirea contractului de achizitie publice /acordul-cadru din Legea nr. 98/2016 privind achizitiile publice, achizitie ce se va finaliza cu incheierea unui contract de servicii.

Obiectul achizitiei: extindere valabilitate pachet licențe antivirus Bitdefender pentru un an și servicii de asistență tehnică informatică pentru instalarea și configurarea noilor versiuni și verificarea și asigurarea securității informatice la nivelul rețelei locale Inspecției Muncii și inspectoratelor teritoriale de muncă.

1. Cod CPV: 48760000-3 – Pachet software de protecție antivirus
2. Cod CPV: 72611000-6 - Servicii de asistență tehnică informatică

Durata contractului : pentru extindere valabilitate pachet licențe antivirus Bitdefender un an de la data semnarii contractului,

pentru servicii de asistență tehnică informatică pentru instalarea și configurarea noilor versiuni și verificarea și asigurarea securității informatice la nivelul rețelei locale Inspecției Muncii și inspectoratelor teritoriale de muncă până la data de 31.12.2018 cu posibilitatea prelungirii pentru 4 luni conform prevederilor art.165 din HG 395/2016 cu completările și modificările ulterioare.

Str. Matei Voievod, nr. 14, Sector 2, București
Tel.: +4 021 302 70 31; fax: +4 021 252 00 97
comunicare@inspectiamuncii.ro
www.inspectiamuncii.ro

3. Valoarea estimata:

- pentru extindere valabilitate pachet licențe antivirus Bitdefender pentru un an pentru un număr de 2250 licențe : 92.200 lei fără TVA
- pentru servicii de asistență tehnică informatică pentru instalarea și configurarea noilor versiuni și verificarea și asigurarea securității informatice la nivelul rețelei locale Inspecției Muncii și inspectoratelor teritoriale de muncă: 18.400 lei fără TVA sau 27.600 lei în cazul prelungirii contractului pentru 4 luni conform prevederilor art.165 din HG 395/2016 cu completările și modificările ulterioare

4. Sursa de finantare : bugetul de stat
5. Criteriul de atribuire: pretul cel mai scazut.
6. Modul de elaborare a ofertei: conform caietului de sarcini anexat. Ofertele care nu indeplinesc in totalitate cerintele cuprinse in caietul de sarcini sau valoarea totala depaseste valoarea estimata a achizitiei, vor fi respinse.

   Pretul ofertei este ferm, nu se accepta actualizarea pretului.

   Limba de redactare a ofertei: romana
7. Perioada de valabilitate a ofertei: 30 zile de la termenul limita de depunere a ofertei.
8. Modul de transmitere a ofertelor:
   - la adresa autoritatii contractante amintita mai sus, cu adresa de inaintare sau,
   - la adresa de e-mail : cristian.tache@inspectiamuncii.ro sau
   - postare in catalogul de produse si servicii disponibil in SEAP, la adresa www.e-licitatie.ro si confirmarea postarii la adresa de email de mai sus.
9. Data limita pentru depunerea ofertelor : 23.04.2018, ora 14,00 . Ofertele depuse dupa aceasta data nu se iau in considerare.
10. Informatii suplimentare pot fi solicitate de la Cristian Tache , telefon 0755. 037.377, e-mail : cristian.tache@inspectiamuncii.ro

INSPECȚIA MUNCII

CAIET DE SARCINI

PRECIZĂRI INTRODUCTIVE

Inspecția Muncii deține un pachet de licențe pentru produsul(soluția) antivirus Bitdefender a cărei valabilitate a expirat.

Se dorește:

1. extinderea valabilității pachetului de licențe antivirus Bitdefender deținut de Inspecția Muncii pentru o perioadă de un an.

2. achiziționarea de servicii de asistență tehnică informatică pentru instalarea și configurarea noilor versiuni și verificarea și asigurarea securității informatice la nivelul rețelei locale Inspecției Muncii și inspectoratelor teritoriale de muncă.

I. OBIECTIVE GENERALE

Extinderea valabilității pachetului de licență antivirus trebuie să asigure protecția împotriva atacurilor virușilor informatici și a altor categorii de programe de aceeași natură (troieni, malware, ransomware, spyware, etc.), pentru toate resursele din rețeaua locală a Inspecției Muncii și inspectoratelor teritoriale de muncă, în conformitate cu Anexa 1 și cantitățile de mai jos.

Oferta va fi întocmită pentru protejarea a:

- 2.100 stații de lucru și conturile de e-mail echivalente;

- 1 mediu virtual și 150 servere de fișiere sau echivalente.

Autoritatea contractantă își rezervă dreptul de a modifica pe durata contractului în plus sau în minus, în cuantum de 10%, valorile de mai sus.

Extinderea valabilității pachetului de licență antivirus și serviciile antivirus ofertate, vor acoperi toate componentele rețelei IM și ITM și vor răspunde integral cerințelor exprimate în prezentul caiet de sarcini.

II. EXTINDEREA VALABILITĂȚII PACHETULUI DE LICENȚĂ ANTIVIRUS

Extinderea valabilității pachetului de licență antivirus va asigura funcționarea pe o perioadă de 12 luni a soluției existente descrisă mai jos :

CARACTERISTICI GENERALE

Produsul este o platformă integrată pentru managementul securității, gândită ca o soluție modulară.
Produsul conține următoarele module:

Str. Matei Voievod, nr. 14, Sector 2, București
Tel.: +4 021 302 70 31; fax: +4 021 252 00 97
comunicare@inspectiamuncii.ro
www.inspectiamuncii.ro

A. O consolă de management care asigură funcționalități de administrare.
B. Protecție antimalware pentru stații fizice, laptop-uri și servere si medii virtualizate
C. Controlul dispozitivelor, controlul accesului la Internet, filtrarea traficului prin modul de tip firewall pentru mașinile fizice și virtuale.
D. Protecție și securitate pentru serverele email.

A. CONSOLA DE MANAGEMENT

1. Instalare și configurare:

1. Pachetul de instalare este o mașină virtuală bazată pe sistem de operare Linux (ce nu necesită licențe adiționale) securizat care conține toate rolurile sau serviciile necesare. Imaginea de tip template se poate importa în:
   a. VMware vSphere
   b. Citrix XenServer
   c. Microsoft Hyper-V
   d. Red Hat Enterprise Virtualization
   e. KVM

2. Consola de management este instalată cu o bază de date inclusă.
3. Soluția este scalabilă, astfel ca oricare dintre roluri sau servicii pot fi instalate separat pe mai multe mașini virtuale sau pe aceeași mașină virtuală.
4. Mașinile de scanare pentru mediile virtuale VMware și Citrix se instalează la distanță prin task din consola de management, iar pentru alte platforme se descarcă separat din interfața web a produsului.
5. Rolurile principale sunt: Server cu bază de date, Server de comunicație, Server de actualizare, Server de Web.
6. Soluția include adițional și un modul de balansare (load balancer) pentru cazurile în care mai multe mașini virtuale ale componentei de management sunt instalate cu același rol (pentru Load Balancing și performanță).
7. Soluția include un mecanism de configurare a disponibilității pentru Serverul cu baze de date (clustering pentru redundanță). Astfel, baza de date se poate instala de mai multe ori, pe mai multe mașini virtuale.

2. Caracteristici generale:

1. Interfața consolei de management este și în limba română.
2. Interfața clientului de securitate, care se instalează pe stații și servere, este și în limba română.
3. Manualul de instalare a produsului este și în limba română.
4. Manualul de administrare a produsului este și în limba română.
5. Soluția include un modul de update server prin care se asigură actualizarea de produs și a semnăturilor.
6. Soluția permite activarea/dezactivarea actualizărilor de produs/semnături.
7. Soluția permite stabilirea actualizării automate a consolei de management prin stabilirea recurenței zilnice, săptămânale sau lunare, dar și prin stabilirea intervalului orar în care

acesta se va actualiza. De asemenea, soluția permite și trimiterea unei alerte de ne-funcționalitate, cu 30 de minute înainte de actualizare.

8. Pentru o mai bună urmărire a actualizărilor consolei de management, soluția permite vizualizarea unui jurnal de modificări în care sunt precizate istoric:
    a. versiunea consolei de management
    b. data versiunii
    c. funcții noi și îmbunătățiri
    d. probleme rezolvate
    e. probleme cunoscute
9. Notificările – prezente în interfața, notificările necitite sunt evidențiate, trimise către una sau mai multe adrese de email, alertează administratorul în cazul unor probleme majore: licențiere, detecție viruși, actualizări de produs disponibile).
10. Soluția permite integrarea cu un server Syslog pentru raportarea evenimentelor antimalware.
11. Soluția permite instalarea serviciului de SMNP prin care se pot raporta stările de funcționare a mașinilor din cadrul componentei de management.

3. Panou de monitorizare și raportare (Dashboard):

1. Rapoartele din panoul de monitorizare pot fi configurate specificând numele raportului, tipul raportului și opțiuni specifice pentru orice tip de raport (de exemplu pentru raportul de actualizare - care este intervalul după care o stație de lucru este considerată neactualizată).
2. Panoul central conține rapoarte pentru toate modulele suportate.
3. Rapoartele din panoul central de comanda permit: adăugarea altor rapoarte, ștergerea lor și rearanjarea.

4. Inventarierea rețelei – managementul securității:

1. Soluția se integreaza cu domenii Active Directory multiple, VMware vCenter și importă inventarul acestor platforme.
2. Pentru integrarea cu Active Directory, se poate defini și intervalul de timp de sincronizare și efectuează sincronizarea.
3. Se permite descoperirea mașinilor din Microsoft Hyper-V, Red Hat VM, KVM.
4. Se permite descoperirea stațiilor stații fizice neintegrate în Active Directory/ Workgroup cu ajutorul Network Discovery.
5. Soluția oferă opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare și adresa IP.
6. Soluția permite instalarea la distanță sau manual a clienților antimalware pe mașini fizice și virtuale.
7. Soluția permite selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice și virtuale.
8. Soluția permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanță pentru clientul antimalware.
9. Soluția oferă posibilitatea de repornire a mașinilor fizice de la distanță.
10. Soluția oferă informații detaliate despre fiecare task și se sesizează daca task-ul s-a finalizat sau nu cu succes.

11. Soluția permite configurarea centralizată a clienților antimalware prin intermediul politicilor
12. Politicile se pot aplica per Active Directory, user, computere și în funcție de locația fizică a acestora.
13. Se oferă în consola de management informații detaliate ale obiectelor din consolă: Nume, IP, Sistem de operare, Grup, Politica atribuită, Ultimele actualizare, Versiunea produsului, Versiunea de semnături.
14. Clientul antivirus este capabil să facă actualizări din locații diferite, în funcție de rețeaua din care face parte (rețeaua poate fi identificată prin: DNS, Gateway, MAC, IP, etc.)
15. Soluția permite descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea, prin rularea unui task din consola de administrare.

5. Politici:

1. Soluția permite configurarea setărilor antimalware prin intermediul politicilor din consola de management.
2. Politica conține opțiuni specifice de activare/dezactivare și configurare a funcționalităților precum scanarea antimalware la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web,controlul dispozitivelor, power user.
3. Soluția permite aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resurse (VMware), domeniu, unități organizaționale.
4. Clientul antivirus poate fi configurat de la distanță prin aplicarea unei singure politici ce include setări pentru toate modulele.
5. Posibilitatea ca politica să poată fi schimbată automat în funcție de:

a. User-ul logat pe stație
b. IP sau clasa de IP a stației
c. Gateway-ul alocat
d. DNS serverul alocat
e. Clientul este/nu este în aceeași rețea cu infrastructura de management
f. Tipul rețelei (LAN, wireless).

6. Rapoarte:

1. Soluția conține rapoarte care prezintă statusul mașinilor client din punct de vedere al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate.
2. Rapoartele programate pot fi trimise către un număr nelimitat de adrese de email (nu este nevoie să aibă un cont în consola de management).
3. Soluția permite vizualizarea rapoartelor curente programate de administrator.
4. Soluția permite exportarea rapoartelor în format .pdf și detaliile ca format .csv.

7. Carantina:

1. Soluția permite restaurarea fișierelor aflate in carantină în locația originala sau într-o cale sau locație configurabilă.
2. Permite descărcarea fișierelor aflate in carantină doar pentru mașinile virtuale protejate prin modulul mediilor virtuale integrate cu VMware vShield.
3. Carantina este locală, pe fiecare stație administrată și este administrată, fie local, fie din consola de management.

8. Utilizatori:

1. Administrarea se poate face pe bază de roluri.
2. Roluri multiple predefinite: Administrator companie, Administrator rețea, Reporter sau rol personalizat.
a. Administrator companie: administrează arhitectura consolei de management;
b. Administrator rețea: administrează serviciile de securitate;
c. Reporter: monitorizează și generează rapoarte.
3. Utilizatorii pot fi importați din Microsoft Active Directory sau creați în consola de management.
4. Se permite configurarea detaliată a drepturilor administrative, permițând selectarea serviciilor și obiectelor pentru care un utilizator poate face modificări.
5. Se permite deconectarea automată a oricărui tip de utilizator după un anumit timp pentru o protecție sporită a datelor afișate în consola de administrare. Acest interval se poate personaliza de administratorul soluției.

9. Log-uri:

1. Înregistrarea acțiunilor utilizatorilor.
2. Se vor oferi informații detaliate pentru fiecare acțiune a unui utilizator.
3. Se permite filtrarea acțiunilor utilizator după numele utilizatorului, acțiune.

10. Actualizare:

1. Se permite definirea de locații de actualizare multiple.
2. Se permite activarea/dezactivarea actualizărilor de produs și semnături.
3. Se permite actualizarea produsului într-o rețea fără acces la Internet.
4. Orice client antivirus să poată fi configurat să livreze update-urile către alt client antivirus
5. Soluția să dispună de un server de actualizare (update) care face posibilă stabilirea componentelor ce vor fi descărcate automat de pe internet, fără intervenția administratorului. Astfel, administratorul poate descărca pachetele pentru protecția stațiilor și serverelor pe care rulează sistemul de operare Windows, Linux, Mac sau, poate descarcă pachetele pentru modul de scanare centralizată în mediile de virtualizare VMware, Hyper-V sau Citrix.
6. În cadrul serverului de actualizare, pentru o mai bună urmărire a actualizărilor pachetele pentru protecția stațiilor și serverelor sau a pachetelor pentru modul de scanare centralizată, să fie posibilă vizualizarea unui jurnal de modificări în care sunt precizate istoric:
a. versiunea pachetului
b. data versiunii
c. funcții noi și îmbunătățiri
d. probleme rezolvate
e. probleme cunoscute
7. Soluția permite testarea noilor versiuni de pachete de instalare ale clientului antimalware, înainte de a fi instalate pe toate stațiile și serverele din rețea, evitând posibile probleme ce pot afecta serverele sau stațiile critice. Astfel, serverul de actualizareinclude 2 tipuri de actualizări de produs:
a. Ciclu rapid, gândit pentru un mediu de test în cadrul rețelei
b. Ciclu lent, gândit pentru restul rețelei (producție, servere critice etc.)

8. Soluția permite stabilirea zonelor de test și critice din cadrul rețelei prin intermediul politicilor din consola de management.

11. Certificate:

1. Accesul la consola de management sa se facă prin HTTPS.
2. Serverul web, din consola centrală de management permite importarea de certificate digitale eliberate de o autoritate de certificare autorizată sau proprie organizației.
3. Soluția permite afișarea în consola de management a informațiilor despre certificatele instalate: nume, autoritatea emitenta, data eliberării și data expirării certificatelor eliberate.

B. PROTECȚIE STAȚII ȘI SERVERE FIZICE/VIRTUALE

1. Caracteristici generale minimale și eliminatorii:

1. Pentru reducerea la minimum a consumului de resurse, soluția antimalware permite instalarea personalizată a modulelor deținute (de exemplu, să permită instalarea soluției antimalware fără modulul de control al accesului web, modul de control al dispozitivilelor sau modulul firewall).
2. Pentru o mai bună protecție a stațiilor și serverelor, soluția include un vaccin anti-ransomware. Acest vaccin asigură protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor de lucru și serverelor, chiar dacă sunt infectate și prin blocarea procesului de criptare.
3. Vaccinul anti-ransomware primește actualizări de la producător, odată cu actualizarea semnăturilor produsului Antimalware.
4. Pentru o mai bună protecție a stațiilor de lucru și serverelor, soluția include protecție împotriva atacurilor zero-day de tip exploit (atacuri direcționate).

2. Cerințe de sistem:

- Sisteme de operare pentru stații de lucru: Windows 10, Windows 8, Windows 7, Windows Vista (SP1), Windows XP (SP3).
- Sisteme de operare pentru servere: Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, Windows Server 2003 R2, Windows Server 2003 with Service Pack 1.
- Sisteme de operare Linux: Red Hat Enterprise Linux / CentOS 5.6 sau mai recent, Ubuntu 10.04 LTS sau mai recent, SUSE Linux Enterprise Server 11 sau mai recent, OpenSUSE 11 sau mai recent, Fedora 15 sau mai recent, Debian 5.0 sau mai recent.

3. Administrare și instalare la distanță (remote):

1. Înainte de instalare, administratorul poate particulariza pachetele de instalare cu modulele dorite: firewall, content control, device control, power user.
2. Instalarea se poate face în mai multe moduri:
a. prin descărcarea directă a pachetului pe stația pe care se va face instalarea;
b. prin instalarea la distanță, direct din consola de management

3. Instalarea clienților la distanță în alte locații decât cele în care este instalată consola de management se va face prin intermediul unui client existent în locațiile respective de tip relay pentru a minimiza traficul în WAN.
4. În consolă vor fi disponibile informații despre fiecare stație de lucru: numele stației, IP, sistem de operare, module instalate, politica aplicată, informații despre actualizări etc.
5. Din consolă se poate trimite o singură politică pentru configurarea integrală a clientului de pe stații/servere.
6. Consola include o secțiune, „Audit", unde se vor menționa toate acțiunile întreprinse fie de administratori fie de reporteri, cu informații detaliate: logare, editare, creare, delogare, mutare etc.
7. Posibilitatea creării unui singur pachet de instalare, utilizabil atât pentru sistemele de operare pe 32 de biți cat și pentru cele pe 64 de biți.
8. Posibilitatea creării unui singur pachet de instalare, utilizabil pentru stații (fizice și/sau virtuale), servere (fizice și/sau virtuale).
9. Posibilitatea de a crea pachetele de instalare de tip web installer sau kit full.
10. Administratorul poate crea grupuri sau chiar subgrupuri, unde poate muta stațiile/serverele din rețea pentru cele care nu sunt integrate in domeniu.
11. Permite selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decât cele integrate în domeniu.

4. Caracteristici și funcționalități principale ale modulului antimalware:

1. Soluția permite administratorului să stabilească acțiunea luată de produsul Antimalware la detectarea unei amenințări noi. Astfel administratorul poate alege între următoarele acțiuni:

1. Acțiune implicită pentru fișiere infectate:
    i. interzice accesul
    ii. dezinfectează
    iii. ștergere
    iv. mută fișierele în carantină
    v. nici o acțiune
2. Acțiune alternativă pentru fișierele infectate:
    i. interzice accesul
    ii. dezinfectează
    iii. ștergere
    iv. mută fișierele în carantină
3. Acțiune implicită pentru fișierele suspecte:
    i. interzice accesul
    ii. ștergere
    iii. mută fișierele în carantină
    iv. nici o acțiune
4. Acțiune alternativă pentru fișierele suspecte:
    i. interzice accesul
    ii. ștergere
    iii. mută fișierele în carantină

2. Scanarea automată în timp real poate fi setată să nu scaneze arhive sau fișiere mai mari de o anumită dimensiune, mărimea fișierelor putând fi definită de administratorul soluției,
3. Definirea până la 16 nivele de profunzime pentru scanarea în arhive.

4. Scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătură nu a fost lansată încă.
5. Scanarea oricărui suport de stocare a informației (CD-uri, hard disk-uri externe, unități partajate etc.). De asemenea, se poate anula scanarea în cazul în care sunt detectate unități care au informații stocate mai mari de o anumită dimensiune configurabilă.
6. Scanarea automată a emailurilor la nivelul stației de lucru pentru POP3/SMTP.
7. Configurarea căilor ce urmează a fi scanate la cerere.
8. Clienții antimalware pentru workstation să permită definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese.
9. Posibilitatea de a testa semnăturile și update-urile de produs înainte de a fi lansate în producție (stageing)
10. Cu ajutorul unei baze de date complete cu semnături de spyware și a euristicii de detecție a acestui tip de programe, produsul va trebui să ofere protecție anti-spyware.
11. Posibilitatea de a configura scanările programate astfel încât să se execute cu prioritate redusă
12. Produsul antimalware poate fi configurat să folosească scanarea în cloud, și parțial scanarea locală. Pentru stațiile ce nu au suficiente resurse hardware, scanarea se poate face cu o mașină de scanare instalată în rețea.
13. Administratorul poate personaliza și motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare:

- Scanare locală, când scanarea se efectuează pe stația de lucru locală. Modul de scanare locală este potrivit pentru mașinile puternice, având toate semnăturile și motoarele stocate local.
- Scanarea hibrid cu motoare light (Cloud public), cu o amprentă medie, folosind scanarea în cloud și, parțial, semnături locale. Acest mod de scanare oferă avantajul unui consum mai bun de resurse, fără să implice scanarea locală.
- Scanarea centralizată în Cloud-ul privat, cu o amprentă redusă, necesitând un server de securitate pentru scanare. În acest caz, nu se stochează local nici o semnătură, iar scanarea este transferată către serverul de securitate.
- Scanare centralizată (Scanare în cloud privat cu server de securitate) cu fallback* pe Scanare locală (motoare full)
- Scanare centralizată (Scanare în cloud privat cu server de securitate) cu fallback* pe Scanare hibrid (cloud public cu motoare light)

14. Pentru o protecție sporită, soluția antimalware trebuie sa aibă 3 tipuri de detecție: bazată pe semnături, bazată pe comportamentul fișierelor și bazată pe monitorizarea proceselor.
15. Pentru o protecție sporită, soluția antimalware trebuie sa poată scana paginile HTTPS.
16. Pentru o mai bună gestionare a antimalware instalat pe stații, produsul include opțiunea de setare a unei parole pentru protecția la dezinstalare.
17. Pentru siguranța utilizatorului, clientul include un modul de antiphishing.
18. Soluția oferă protecție în timp real pe mașinile cu sistem de operare Linux în conformitate cu versiunea de kernel înstalată.
19. Pe mașinile virtuale parte a unui pool instalarea clientului antimalware se face doar pe mașină de tip template, dupa care se recompune pool-ul de mașini virtuale.

5. Firewall:

1. Posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate.
2. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului.
3. Posibilitatea de a defini rețele de încredere pentru mașina destinație.
4. Să existe predefinite minim 10 seturi de reguli.

6. Carantina:

1. Produsul antimalware să permită trimiterea automată a fișierelor din carantină către laboratoarele antimalware ale producatorului.
2. Trimiterea continutului carantinei poate fi expediat în mod automat, la un interval definit de administrator.
3. Produsul antimalware să permită ștergerea automată a fișierelor aflate în carantină mai vechi de o anumită perioadă, pentru a nu încărca inutil spațiul de stocare.
4. Posibilitatea de a restaura un fișier din carantină în locația lui originală.
5. Modulul de carantină permite rescanarea obiectelor după fiecare actualizare de semnături.

7. Protecția datelor:

1. Produsul permite blocarea datelor confidențiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice.

8. Controlul conținutului:

1. Consola are integrat un modul dedicat controlului accesului la Internet cu urmatoarele particularități:

a. Permite blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini.
b. Permite blocarea accesului la Internet pe intervale orare.
c. Permite blocarea paginilor de internet care conțin anumite cuvinte cheie.
d. Permite controlul accesului numai la anumite pagini de internet specificate de administrator;
e. Permite blocarea accesului la anumite aplicații definite de administrator;
f. Permite restricționarea accesului pe anumite pagini de internet după anumite categorii prestabilite (ex: online dating, violență, pornografie, etc.).

9. Controlul dispozitivelor:

1. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului.
2. Modulul permite controlul următoarelor tipuri de dispozitive:

a. Bluetooth Devices
b. CDROM Devices
c. Floppy Disk Drives
d. Security Policies 153
e. IEEE 1284.4
f. IEEE 1394
g. Imaging Devices
h. Modems
i. Tape Drives
j. Windows Portable
k. COM/LPT Ports
l. SCSI/SAS RAID

m. Printers
n. Network Adapters
o. Wireless Network Adapters
p. Internal and External Storage

3. Modulul permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client.
4. Modulul permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli.

10. Power User:

1. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului.
2. Modulul permite posibilitatea de a acorda utilizatorilor drepturi de Power User. Utilizatorii pot accesa și modifica setările clientului antimalware dintr-o consolă disponibilă local pe mașina client.
3. Administratorul poate suprascrie din consolă setările aplicate de utilizatorii Power User.

11. Actualizare:

1. Posibilitatea efectuării actualizării la nivel de stație în mod silențios (fără avertizare).
2. Sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate).
3. Actualizarea pentru locațiile remote prin intermediul unui client antimalware care are și rol de server de actualizare.

C. PROTECȚIE ȘI SECURITATE PENTRU SERVERELE EMAIL AXIGEN

1. Produsul oferă protecție antimalware, antispam (inclusiv antiphishing), precum și filtrare de atașamente și conținut, prin integrarea cu serverul de e-mail Axigen. De asemenea, permite scanarea antimalware la cerere a bazelor de date Microsoft Outlook.
2. Produsul va asigură scanarea atașamentelor și a conținutului mesajelor în timp real, fără a afecta vizibil performanța serverului de mail.
3. Actualizarea antimalware trebuie să poată fi făcută automat la un interval de maxim 1 ora, precum și la cerere.
4. În afară de detecția pe bază de semnături, modulul de protecție antimalware va trebui să includă și scanare euristică comportamentală, prin simularea unui calculator virtual în interiorul căruia sunt rulate și analizate aplicații cu potențial periculos, pentru a proteja sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnatură nu a fost lansată încă.
5. Produsul oferă opțiuni multiple de acțiune la identificarea unui atașament virusat (dezinfectare, ștergere, mutare în carantină).
6. Cu ajutorul unei baze de date complete cu semnături de spyware și a euristicii de detecție a acestui tip de programe, produsul oferă protecție anti-spyware pentru a preveni furtul de date confidențiale.
7. Produsul oferă protecție antispam, cu o bază de semnaturi actualizabilă prin internet.

8. Modulul antispam va trebui să includă un filtru URL cu o bază de adrese URL cunoscute a fi folosite în mesaje spam, precum și un filtru de caractere pentru detectarea automată a mesajelor scrise cu caractere chirilice sau asiatice.
9. Produsul va trebui să ofere filtru RBL care să identifice spam-ul prin sincronizarea cu anumite baze de date online care conțin liste de servere de mail cunoscute ca fiind la originea acestui tip de mesaje.
10. Produsul va trebui să ofere un serviciu/filtru online pentru îmbunătățirea protecției împotriva valurilor de spam nou apărute.
11. Produsul oferă posibilitatea de a defini politici de filtrare antimalware, antispam, a conținutului sau atașamentelor pentru diferite grupuri sau utilizatori.
12. Actualizarea produsului este configurabilă și se poate realiza de pe internet, direct sau printr-un proxy, sau din cadrul rețelei de pe un server de actualizare propriu.
13. Produsul oferă statistici atât referitoare la scanarea antivirus cât și la scanarea antispam.
14. Produsul se integreaza în cadrul consolei de management unitar al soluției antivirus. Pentru ușurință accesului la setările produsului din diferite medii de operare, produsul are consola de administrare web.

D. ANTIMALWARE, ANTISPAM ȘI FILTRARE DE CONTINUT PENTRU SERVERE EMAIL LINUX

15. Produsul oferă protecție antimalware, antispam și antiphishing, precum și filtrare de atașamente și conținut.
16. Actualizarea motoarelor și semnăturilor antimalware trebuie să poată fi făcută automat la un interval de maxim 1 ora, precum și la cerere.
17. Administratorul poate defini o acțiune secundară (ștergere sau plasare în carantină) pentru cazul în care dezinfectarea unui mesaj eșuează.
18. În afara de detecția pe bază de semnături, modulul de protecție antimalware include și scanare euristică comportamentală, prin simularea unui calculator virtual în interiorul căruia sunt rulate și analizate aplicații cu potențial periculos, pentru a proteja sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătură nu a fost lansată încă.
19. Modulul antimalware permite configurarea de acțiuni separate pentru fișierele suspecte.
20. Produsul oferă protecție anti-phishing, care să detecteze tentativele de copiere a infățișării și conținutului mesajelor autentice în vederea păcălirii destinatarului acestora pentru obținerea ilegală de date confidențiale.
21. Produsul oferă protecție antispam, cu o bază de semnaturi actualizabila prin internet.
22. Modulul antispam include un filtru URL cu o bază de adrese URL cunoscute a fi folosite în mesaje spam sau phishing, precum și un filtru de caractere pentru detectarea automată a mesajelor scrise cu caractere chirilice sau asiatice.
23. Modulul antispam include un filtru euristic și un serviciu/filtru online pentru imbunătățirea protecției împotriva valurilor de spam nou apărute.
24. Produsul oferă opțiuni multiple de acțiune la identificarea unui mesaj spam: ștergere, plasarea în carantina sau marcarea subiectului ca spam.
25. Produsul permite configurarea unei liste de adrese sau domenii email considerate sigure, ale căror emailuri vor fi permise automat de către modulul antispam. Produsul permite configurarea unei liste de adrese sau domenii email cunoscute pentru trimiterea de mesaje spam, care vor fi detectate în mod automat de către modulul antispam.

26. Produsul permite configurarea de reguli de filtrare de conținut pe bază de cuvinte cheie și expresii regulate, precum și configurarea de reguli de filtrare a atașamentelor email în funcție de tip, nume și mărime.
27. Produsul oferă acțiuni specifice pentru mesajele de conțin obiecte protejate prin parola (ignorare, ștergere sau plasare în carantină).
28. Produsul permite configurarea de reguli de filtrare specifice pentru anumite grupuri de utilizatori.
29. Pentru ușurința accesului la setări, produsul are consola de administrare web. Consola web permite crearea de conturi de administrator diferite.
30. Produsul înregistrează evenimentele privind funcționarea și activitatea de scanare în fișiere log
31. Produsul permite configurarea dimensiunii fișierelor log și ștergerea automată a logurilor mai vechi de un număr de zile definit de administrator
32. Produsul permite trimiterea de alerte pe mail către administrator în cazul detecțiilor de viruși, spam și conținut
33. Produsul notifică administratorul în momentul în care detectează o actualizare disponibilă pe serverele producătorului antivirus.
34. Produsul oferă statistici și grafice privind activitatea de scanare (inclusiv numărul de mesaje scanate și detecții de viruși și spam)
35. Oferă suport SNMP pentru trimiterea mesajelor de tip alertă
36. Produsul este certificat VBSpam/VBSpam+ în fiecare dintre ultimele 12 teste VBSpam, cu o rată medie de detecție de peste 99.8%”

III.SERVICII

Servicii prestate pe durata contractului

Sistemul antivirus este în mod obligatoriu însoţit de următoarele servicii pentru perioada contractată:

1. Instalarea și configurarea în întreaga rețea a Inspecției Muncii a celor mai recente versiuni ale produselor ofertate şi a cheilor de licenţă aferente acestora.

2. Posibilitatea prestatorului de a răspunde unor solicitări cu privire la incidente provocate de către atacurile virușilor în termen de 24 ore prin intervenție în locațiile beneficiarului fizic sau de la distanță.

3. Ofertantul trebuie să asigure intervenţii periodice, on site la sediul central al Inspecţiei Muncii cu frecvenţă săptămânală pentru verificarea şi dezinfecţia reţelei locale de calculatoare.

4. Ofertantul trebuie să asigure intervenţii periodice, remote la sediul inspectoratelor teritoriale de muncă cuprinse în anexa nr. 1, cu frecvenţă lunară, pentru verificarea și dezinfecţia reţelei locale de calculatoare.

5. Ofertantul trebuie să asigure intervenţii la cerere, în situaţii critice, on site, la sediul Inspecţiei Muncii şi ITM Bucureşti pentru evenimente critice în maximum 4 ore de la primirea solicitării.

6. Ofertantul trebuie să asigure intervenţii la cerere, în situaţii critice, on site, la sediul celorlalte inspectorate teritoriale de muncă cuprinse în anexa nr.1 pentru evenimente critice în maximum

8 ore de la primirea solicitării. Intervențiile la cerere vor fi în limita de o intervenție/lună calendaristică.

7. Fiecare intervenție periodică din orice locație IM și ITM se va finaliza prin completarea unei fișe de intervenție în care vor fi consemnate activitățile efectuate. Fișa de intervenție este semnata de către persoana care a efectuat intervenția și de către un reprezentant desemnat al beneficiarului. Fișele de intervenție vor certifica prestarea serviciilor și vor condiționa plata lunara a acestora. Modelul fișei de intervenție precum și procedura de solicitare a intervențiilor la cerere vor fi stabilite de comun acord între beneficiarul și prestatorul serviciilor, în momentul contractării.

8. Ofertantul trebuie să asigure asistență și suport tehnic în limba română prin telefon, e-mail și chat non-stop 24h/zi, 7 zile/săptămână, pentru perioada de derulare a contractului. Modalitatea de asigurare a asistenței și a suportului tehnic pentru diagnoza și rezolvarea problemelor va fi on line sau telefonic, după caz.

LIVRABILE: Serviciile vor fi implementate în rețeaua IM și ITM pentru o perioadă cuprinsă între data încheierii contractului și 31.12.2018, facturabile lunar, cu posibilitatea de prelungire a contractului cu o perioadă de maxim 4 luni conform prevederilor art.165 din HG.395/2016 alin.(1), cu condiția existenței resurselor financiare alocate cu această destinație;

- kit-urile de instalare ale produselor cu interfața în limba româna,
- certificate de licență,
- documentația produsului în limba română.

IV.CERINȚE MINIME OBLIGATORII PENTRU OFERTANȚI

Ofertanții trebuie să răspundă la toate cerințele cuprinse în caietul de sarcini și să detalieze în propunerea tehnică modalitatea în care produsul antivirus îndeplinește această cerință. În cazul în care soluția prezentată nu oferă informații complete sau nu îndeplinește cerințele solicitate, comisia de evaluare are dreptul să declare soluția ca fiind necorespunzătoare.
Producătorul aplicațiilor software antivirus trebuie să fie certificat tehnic conform grupei de standarde ISO 9001:2001 pentru producție de software și vor fi prezentate certificate doveditoare. Acestea trebuie să fie emise de către o autoritate competentă din țara de origine a producătorului.

Prestatorul serviciilor de protecție antivirus trebuie să fie certificat tehnic conform grupei de standarde ISO 9001:2001 și ISO 27001:2013 și vor fi prezentate certificate doveditoare.

Ofertanții trebuie să fie certificați și autorizați de către producătorul aplicațiilor software antivirus ce vor fi utilizate pentru prestarea serviciilor ce fac obiectul prezentului caiet de sarcini și vor prezenta documente doveditoare.

Soluțiile și aplicațiile software ale produsului antivirus folosite de prestatorul de servicii pentru protecția stațiilor de lucru și a serverelor fizice și virtuale trebuie sa fie parte integranta a unei soluții de administrare centralizata, în vederea monitorizării facile de care beneficiar.

Ofertanții vor include în ofertă de servicii toate cheltuielile: transport la sediul beneficiarului a personalului de intervenție, manoperele aferente, taxele și orice alte cheltuieli legate de prestarea serviciilor și de configurarea echipamentelor prevăzute în prezenta cerere de ofertă.

INSPECȚIA MUNCII

Soluțiile și aplicațiile antivirus pentru produsul de securitate a datelor trebuie sa fie disponibila pentru livrare și instalare de către furnizor pe toate sistemele beneficiarului în 5 zile de la semnarea contractului, pentru a nu exista perioade lungi de timp în care sistemele și serverele nu sunt protejate împotriva amenințărilor.

Str. Matei Voievod, nr. 14, Sector 2, București
Tel.: +4 021 302 70 31; fax: +4 021 252 00 97
comunicare@inspectiamuncii.ro
www.inspectiamuncii.ro