Aprobare,
Manager
Anca-Cristina Râpeanu

CAIET DE SARCINI
privind achiziţia publică de servicii de de actualizare program antivirus

Forma documentului	Iniţială: 10.11.2017
Elemente ale revizuirii:	n/a

OBIECTIVUL ACHIZIŢIEI:

Autoritatea contractantă solicită servicii de servicii de actualizare pentru programul antivirus Kaspersky Anti-virus utilizat pentru protecţia echipamentelor IT din cadrul Bibliotecii Metropolitane Bucureşti, începând din 23.12.2017.

CONDIŢII PRIVIND LIVRAREA:

Livrarea se va face prin poşta electronică pe adresele biblioteca@bibmet.ro si ovidiu.dragulinescu@bibmet.ro

TERMEN DE LIVRARE: 2 zile de la data comenzii

LOCUL LIVRĂRII:

Livrarea se va face prin poşta electronică.

CONDIŢII PRIVIND GARANTIA: 12 luni

SPECIFICAŢII TEHNICE MINIMALE:

Sunt necesare servicii de actualizare program antivirus pentru protecţia:
- mai multor tipuri de sisteme de operare pentru staţii de lucru (Windows şi MacOS X)
- mai multor tipuri de sisteme de operare pentru servere (cu Windows server 2012, Windows Server 2008, Linux)

1. S.O. staţii de lucru Windows:
Microsoft Windows 10 Pro x86 / x64
Microsoft Windows 8.1 Pro x86 / x64
Microsoft Windows 7 Professional x86 / x64 SP1 şi ulterior
Microsoft Windows 7 Ultimate x86 / x64 SP1 şi ulterior
Microsoft Windows Vista x86 / x64 SP2 şi ulterior
Microsoft Windows XP Professional x86 SP3

Produsul trebuie sa aibă următoarele caracteristici:
- are doar un singur motor de scanare care include toate componentele de protecţie, pentru un consum mai eficient de resurse.
- să permită ca instalarea să fie efectuată pe un computer local sau de la distanţă.
- instalarea locala a produsului trebuie sa poată fi realizata in doua moduri: interactiv sau fără interacţiunea cu utilizatorul
- instalarea de la distanta a produsului trebuie sa fie permisa prin intermediul unei

soluții de administrare centralizata de la același producător sau prin politicile de domeniu Microsoft Group

- metodele de instalare de la distanta trebuie sa permită administratorului selectarea componentelor produsului
- trebuie sa fie permisa realizarea upgrade-ului de la versiuni mai vechi
- trebuie sa includă componente care pornesc împreună cu sistemul de operare, rămân in permanenta in memoria RAM a computerului si scanează toate fișierele care sunt deschise, salvate sau rulate pe computer si pe toate dispozitivele atașate la acesta, pentru a detecta prezenta virușilor si a altor amenințări.
- pentru a creste nivelul de protecție, produsul trebuie sa utilizeze analiza euristica, pe parcursul căreia componentele analizează activitatea obiectelor in sistem.
- sa detecteze si sa înlăture programele periculoase de tip rootkit
- sa includă tehnologii care sa optimizeze viteza de scanare a fișierelor prin excluderea acelor fișiere care nu au fost modificate de la ultima scanare.
- sa includă componente care scanează mesajele primite sau trimise prin intermediul protocoalelor POP3, SMTP, IMAP pentru a detecta virușii si alte amenințări.
- sa includă module de extensie sau "plug-in-uri" care permit ca setările scanărilor de e-mail sa fie ajustate pentru clienții de mail Microsoft Office Outlook
- sa permită configurarea filtrării atachementelor e-mailurilor in funcție de tipul acestora, prin care fișiere de un anumit tip sunt redenumite sau șterse automat.
- sa permită activarea sau dezactivarea scanării arhivelor atașate la e-mail si sa limiteze dimensiunea atasamentelor care vor fi scanate, precum si durata maxima de scanare pentru aceste arhive.
- sa includă componente de protecție a datelor trimise si primite de la si pe un computer prin protocoalele HTTP/HTTPS si FTP de verificare a URL-urilor in lista de adrese web suspecte sau de phishing
- sa permită optimizarea performantei de scanare a traficului web trimis si primit prin protocoale HTTP/HTTPS si FTP, prin limitarea timpului de memorare in cache si crearea unei liste cu URL-uri de încredere.
- sa includă componente care scanează traficul clienților de mesagerie instant
- sa includă componente care monitorizează activitatea unui program in sistem si daca programul este considerat periculos, activitatea sa este blocata sau este trecuta in carantina.
- tiparele comportamentale ale programelor utilizate de componenta care monitorizează activitatea programelor trebuie sa fie incluse in actualizările de produs
- componentele care monitorizează activitatea programelor trebuie sa poată restaura sistemul la starea de dinaintea acțiunii programelor periculoase
- sa includă protecție împotriva programelor care exploatează vulnerabilitățile, inclusiv împotriva celor care folosesc așa numitele vulnerabilități zero-day, dar si amenințări care nu au fost înregistrate încă in baza de date cu semnături
- sa includă componente de firewall care permit crearea de reguli pe doua nivele: pachete pentru rețea si la nivel de aplicație.
- componentele firewall ale produsului trebuie sa permită crearea de reguli bazate pe reputația aplicațiilor
- să includă o componentă care scanează traficul de intrare pentru activități tipice atacurilor de rețea si să blocheze activitatea din rețea care provine de la computerul care inițiază atacul.
- sa permită administratorului posibilitatea stabilirii unei liste a porturilor de rețea si o lista a aplicațiilor care necesita permisiune de acces in rețea, care vor fi analizate de componentele produsului atunci când monitorizează traficul de rețea
- sa includă sistem bazat pe tehnologii cloud care sa monitorizeze si sa răspundă rapid la amenințări. Furnizează o infrastructura de servicii online care permit accesul la:
- informații pentru reacții rapide la fișiere si URL-uri periculoase

- informații despre reputația fișierelor si categoriile acestora.

- sa aibă abilitatea sa interacționeze cu sistemele cloud fără acces direct la Internet, prin intermediul sistemului de administrare centralizata

- sa permită actualizarea bazelor de date de semnături si a modulelor aplicației

- pe parcursul procesului de actualizare, produsul trebuie sa realizeze o copie de rezerva a bazei de date si a modulelor aplicației existente, permițând administratorului sa restaureze bazele de date si aplicațiile modulelor la starea inițiala, daca este necesar.

- după o actualizare produsul trebuie sa realizare o scanare automata fișierelor aflate in carantina

- pentru o protecție optimizata, actualizările trebuie lansate de către producător la fiecare ora

- sa permită administratorului sa realizeze diferite tipuri de scanare, predefinite (scanare completa, rapida, personalizata)

- sa înregistreze informații despre fișiere in care a detectat o amenințare activa si care a rămas neprocesata

- sa aibă un depozit de rezerva pentru copiile de rezerva ale fișierelor care au fost șterse sau modificate pe parcursul procesului de înlăturare a amenințărilor.

- sa permită crearea unei liste definite de administrator, cu obiecte si aplicații care nu sunt monitorizate

- sa poată crea un set de excluziuni de la protecție pentru fișiere de un anumit format, fișiere selectate printr-o masca, cu un anumit scop (cum ar fi un folder sau o aplicație), procese ale aplicațiilor, obiecte clasificate

- sa includă un mecanism de auto-protecție care sa prevină distrugerea sau ștergerea fișierelor aplicației de pe hard disc, proceselor de memorie si intrările in sistemul de regiștrii.

- sa permită administratorului accesul restricționat la aplicații prin setarea unei parole si prin specificarea operațiunilor pentru care aplicația trebuie sa solicite utilizatorului o parola

- sa permită administratorului sa identifice toate încercările utilizatorului de pornire a aplicației si sa reglementeze lansarea aplicațiilor prin intermediul regulilor de control pentru pornirea aplicațiilor

- sa permită administratorului sa creeze reguli pentru pornirea aplicațiilor, stabilind multiple condiții cum ar fi:

- calea către folderul ce conține fișierul executabil al aplicației

- metadate (denumirea originala a fișierului executabil al unei aplicații, numele fișierului executabil al unei aplicații aflate pe un dispozitiv drive, versiunea fișierului executabil al aplicației, numele aplicației si producătorul aplicației)

- aplicația aparține unei categorii predefinite, care este actualizată constant de producător

- sa permită implementarea politicilor negare implicite pentru pornirea aplicațiilor

- sa ofere administratorului posibilitatea de împiedicare a acțiunilor periculoase pentru sistem ale aplicațiilor si sa asigure controlul accesului la resursele sistemului de operare si la datele confidențiale.

- sa permită administratorului sa creeze reguli pentru restricționarea accesului utilizatorilor la dispozitive instalate pe computer sau conectate la acesta la nivel de magistrala, tip si dispozitiv.

- sa permită administratorului sa creeze reguli pentru accesarea dispozitivelor pe baza unui set de parametri care definesc cel puțin următoarele funcții:

- permit selectarea utilizatorilor si/sau grupurilor de utilizatori pentru a accesa tipuri specifice de dispozitive in anumite perioade de timp;

- setarea dreptului de vizualizarea a arborelui de foldere in dispozitivele de memorie;

- setarea dreptului de citire a conținutului dispozitivelor de memorie;

- setarea dreptului de editarea a conținutului dispozitivelor de memorie.

- sa permită identificarea dispozitivelor bazate pe un număr sau serie de identificare unice

- sa permită administratorului sa permită accesul temporar la un dispozitiv blocat

- sa permită administratorului sa creeze reguli care asigura control asupra acțiunilor utilizatorilor indiferent de locația stației de lucru in interiorul sau in exteriorul LAN-ului): restricționând sau blocând accesul la resursele web

- sa permită administratorului sa creeze reguli pentru accesarea resurselor web in funcție de:

  - conținutul si tipul datelor

  - adresa resurselor web (o masca de adresa pentru o resursa web trebuie utilizata pentru a înlocui un număr mare de adrese web).

  - după nume sau grupuri de utilizatori

- sa permită administratorului sa afişeze mesaje utilizatorului, atunci când acesta încearcă sa acceseze resurse web care sunt restricționate

- sa permită administratorului crearea de reguli in funcție de utilizator din infrastructura LDAP sau Active directory

- a asigure suport pentru crearea regulilor pentru aplicații in funcție de imaginile diferitelor sisteme de operare (Windows XP, Vista, 7, 8, 10).

- produsul trebuie sa permită detectarea automata a vulnerabilităților din sistemul de operare

2. S.O. server Windows (Windows Server 2008, Windows Server 2012):

Produsul trebuie sa aibă următoarele caracteristici:

- sa fie optimizat pentru sistemele de operare de tip Microsoft Server pentru o scanare rapida si un consum scăzut de resurse

- sa permită actualizări ale motorului de scanare, detecția si a modulelor fără reinstalarea produsului sau restartul sistemului de operare

- sa includă tehnologii de detecție proactiva a malware-ului necunoscut

- sa permită administratorului sa specifice zonele ce urmează a fi scanate cat si zonele de încredere ce vor fi excluse de la scanare

- sa permită administratorului sa adauge ca obiecte de încredere fişiere, directoare sau tipuri de fişiere

- produsul trebuie sa permită administratorului sa creeze activităţi dedicate care pot fi pornite pentru scanarea celor mai vulnerabile zone, fişiere autorun sau fişiere de sistem

- produsul trebuie sa ofere setări flexibile pentru scanare cu posibilitatea de a

  - exclude anumite procese de la scanare

  - specifica care fişiere trebuie scanate mereu si care trebuie excluse de la scanare

  - efectua răspunsuri presetate la detecția obiectelor suspecte sau infectate

- sa permită administratorului sa inițieze scanări atât manuale cat si programate

- sa permită salvarea setărilor de securitate ca si template-uri ce ulterior pot fi utilizate ca punct de plecare pentru configurare

- sa salveze obiectele identificate ca fiind suspecte in carantina sau intr-un director dedicat in format criptat

- sa salveze intr-o locație de back-up, o copie a fişierului original cu toate atributele atunci când un obiect este detectat ca fiind infectat si curăţat sau şters.

- sa ofere posibilitatea de restaurare a obiectelor din locația de back-up

- sa permită scanarea si alte acțiuni, după nevoie, asupra arhivelor împachetate pe mai multe niveluri

- sa blocheze executarea scripturilor periculoase

- sa ofere suport pentru administrarea centralizata prin aceeaşi soluție ca si produsul de protecție al stațiilor de lucru si prin consola de administrare dedicata

- produsul trebuie sa ofere suport pentru administrarea din linie de comanda

- sa ofere posibilitatea administratorului de trimitere de notificări prin serviciul de mesagerie sau e-mail

- sa ofere suport pentru Simple Network Management Protocol (SNMP) si Microsoft Operations Manager (MOM)

- sa includă utilitar pentru urmărirea performanţelor acestuia pe timpul funcţionarii

- sa includă suport pentru roluri de administrare cu drepturi diferite pentru fiecare administrator

- sa ofere posibilitatea de a seta exact timpii de pornire si oprire a activităţilor de scanare

- sa includă tehnologii de balansare a consumului de resurse intre sistemul de protecţie si aplicaţiile ce rulează

- sa ofere posibilitatea de rulare a acţiunilor de scanare in fundal

- sa includă tehnologii de optimizare a scanării astfel încât fişierele care nu au fost modificate de la ultima scanare sa nu fie rescanate.

- produsul trebuie sa ofere suport pentru instalarea pe cluster-e de servere cu mod de lucru Active / Active si Active / Passive.

- produsul trebuie sa ofere suport pentru instalare si eliminarea fără restartarea sistemului de operare

- produsul trebuie sa fie compatibil atât cu sistemele fizice cat si cu cele virtualizare

- sa fie compatibil cu o gama variata de aplicaţii software pentru server incluzând soluţii de back-up

- sa ofere suport pentru scanarea fişierelor offline

- sa ofere protecţie utilizatorilor de terminal ce lucrează in modurile desktop/application publishing

- sa ofere posibilitatea de notificare a utilizatorilor de sesiuni terminal folosind utilitarele de terminal

- sa ofere posibilitatea de audit a acţiunilor efectuate cu fişierele si scripturile utilizatorilor terminal

- sa fie compatibil si sa ofere protecţie pentru sistemele de stocare

- sa ofere detectarea virusilor care criptează documentele permiţând blocarea accesului la resursa partajata a gazdei infectate.

- sa ofere blocarea accesului la o resursa partajata in cazul in care un utilizator încearcă sa încarce un document infectat.

- sa permită administratorului sa definească timpul de blocare a accesului utilizatorilor la resursa partajata.

3. S. O. server Linux (Red Hat, CentOS):

Produsul trebuie sa aibă următoarele caracteristici:

- sa asigure protecţie împotriva tuturor tipurilor de ameninţări nu doar cele dedicate sistemelor de operare Linux

- sa includă tehnologii euristice de analiza si detecţie împreuna cu metode tradiţionale de detecţie in baza semnăturilor malware

- nu trebuie sa necesite restart la actualizarea modulelor de detecţie malware si reparare sau a motorului antivirus

- trebuie sa permită efectuarea scanărilor la cerere a anumitor locaţii din sistem

- setările pentru scanarea fişierelor trebuie sa permită cel puţin:

- selectarea obiectelor prin intermediul măştilor sau a expresiilor alfanumerice, incluzând caractere de tip wildcard

- setări diferite pentru fiecare utilizator la accesarea obiectelor protejate de pe serverul de fişiere

- o varietate a posibilităţii de configurare a excepţiilor de la scanare

- ajustarea nivelului de protecţie

- efectuarea scanărilor conform unui program prestabilit
- curăţarea sau ştergerea obiectelor arhivate

- sa stocheze obiectele suspecte detectate in carantina in format criptat
- sa stocheze o copie a obiectelor infectate detectate, care au fost curăţate sau şterse, incluzând toate atributele fişierului original pentru restaurare
- sa includă o consola web dedicata, ce poate fi accesata independent de browser sau sistem de operare, si care sa ofere cel puţin următoarele funcţionalitatea:
  - configurarea trimiterii de notificări
  - urmărirea statusului protecţiei si a acţiunilor programului
  - vizualizarea informaţiilor despre evenimentele de sistem
  - crearea de rapoarte grafice ce pot fi salvate in cel puţin următoarele formate: PDF, XLS
- produsul trebuie sa permită administrarea centralizata prin intermediul aceluiaşi software de management utilizat pentru administrarea produselor de securitate dedicate staţiilor de lucru si serverelor cu sistem de operare Microsoft Windows.
- produsul trebuie sa permită administrarea din linie de comanda a acţiunilor si primirea de rapoarte despre activitatea produsului si a componentelor acestuia
- sa permită exportul din linie de comanda a rapoartelor in cel puţin următoarele formate: HTML si CSV
- sa permită trimiterea de notificări către administrator prin servicii de mesagerie sau prin e-mail pentru o lista extinsa de evenimente
- sa ofere suport pentru pornirea si finalizarea activităţilor de scanare la momente exacte in timp
- sa permită administratorului stabilirea exacta a momentelor când se efectuează actualizările
- sa includă tehnologii de echilibrare a utilizării resurselor sistemului intre aplicaţii si produsul de securitate
- sa permită efectuarea scanărilor in fundal
- sa ofere suport pentru selectarea automata a surselor de actualizare din cele disponibile in funcţie de încărcarea de pe sistemul sursa
- sa ofere suport pentru instalare si actualizare fără restartul sistemului
- sa ofere integrare cu Samba Server

4. Sistem de management centralizat:

Produsul trebuie să:

- permită instalarea dintr-un singur kit de instalare care sa includă toate pachetele necesare pentru implementare
- ofere suport pentru implementarea si administrarea de la distanta a sistemelor client independent de structura si dimensiunea reţelei
- ofere multiple moduri de instalare in funcţie de dimensiunea reţelei
- permită instalarea si înlăturarea de la distanta a aplicaţiilor instalate pe staţiile client
- permită setarea diferitor tipuri de permisiuni ale administratorilor pentru accesul la funcţiile aplicaţiei, modificarea drepturilor de acces, editarea setărilor de logare si notificare, instalare de la distanta a aplicaţiilor, editarea ierarhiei de servere de administrare, salvarea conţinutului listelor de sisteme detectate in reţea si crearea de tunele de comunicare.
- ofere suport pentru multiple roluri si drepturi administrative
- includă posibilitatea de logare a tuturor operaţiunilor efectuate de administratorii care au acces la consola de administrare
- permită administrarea de la distanta a aplicaţiilor de securitate pentru diverse sisteme de operare (Windows, Mac, Linux) din aceeaşi consola
- permită crearea unei ierarhii de servere de administrare astfel încât secţiunile din reţea independente sau izolate sa poată fi controlate prin intermediul unor servere de administrare

diferite controlate la rândul lor de un server de tip master, in vederea:

- scăderii încărcării pe serverul de administrare (comparat cu scenariul in care exista un singur server)
- scăderii traficului pe internet si simplificării lucrului cu locaţiile remote
- distribuţiei de responsabilităţi mai eficiente intre administratori.

- permită crearea unei ierarhii de servere de administrare pe doua niveluri pe un singur sistem fizic:
  - server de administrare master – gazda şi server de administrare virtual slave – virtual (virtualizarea este realizata in interiorul produsului de administrare centralizata si nu necesita utilitare de virtualizare adiţionale)
- ofere suport pentru Windows Failover Clustering, ce oferă disponibilitate si stabilitate sistemului
- permită configurarea unui set minim de setări necesare pentru construirea unui sistem de protecţie endpoint cu management centralizat folosind utilitar de tip "Wizard". Acest lucru permite administratorului de pornească procesul de instalare de la distanta pe staţiile client imediat după implementarea sistemului de management centralizat
- ofere posibilitatea de creare automata a pachetelor de instalare a soluţiei de securitate pentru clienţi astfel încât aceasta sa poată fi instalata de la distanta.
- ofere posibilitatea de generare automata a activităţilor de scanare, actualizare si a politicilor aplicaţiei de securitate
- permită distribuţia automata a licenţelor pe sisteme administrate
- permită administratorului sa trimită notificări de tip e-mail si NET SEND in legătura cu evenimentele înregistrare la oprirea serverului de administrare a aplicaţiilor administrate
- permită împărţirea sistemelor administrate in grupuri cu posibilitatea de creare a unei structuri ierarhice de grupuri
- îi permită administratorului sa efectueze căutarea de noi sisteme in reţea efectuând scanarea reţelei Windows, structurii Active Directory sau pe baza IP-ului
- ofere posibilitatea de creare a structurii de grupuri administrative bazata pe grupurile de lucru din Microsoft Windows Network sau a structurii Active Directory
- ofere posibilitatea de creare a structurii de grupuri administrative in urma importului din fişier text
- ofere un sistem de autentificare si schimb de date cu sistemele client bazata pe certificat de securitate
- permită administratorului sa actualizeze bazele de date si modulele din pachetele de instalare înainte de pornirea efectiva a procesului de instalare
- ofere posibilitatea administratorului de a accesa centralizat cel puţin următoarele:
  - pachete de instalare
  - director de actualizare pentru sistemele client
  - licenţe
  - fişierele stocate in carantina pe staţiile client
  - fişierele stocate in locaţia de back-up pe staţiile client
  - fişierele neprocesate pe staţiile client
- ofere suport pentru back-up-ul automat al datelor serverului de administrare si posibilitatea de restaurare a acestora
- ofere o consola web ce permite administratorului sa efectueze acţiuni de monitorizare si administrare
- permită administratorului instalarea de la distanta a produselor de securitate, configurarea parametrilor aplicaţiilor, actualizarea programata a produselor, monitorizarea sistemelor si efectuarea de acţiuni rapide in caz de urgenta dintr-un singur punct
- permită administratorului sa configureze setările aplicaţiilor de securitate de pe staţiile client in mod centralizat prin definirea unor politici sau similar şi pornirea programata a sistemelor folosind tehnologia Wake-on-lan

- permită definirea unor setări separate pentru sistemele client de tip mobile (care se deplasează in afara rețelei administrate), ce vor fi aplicate imediat ce sistemul client este deconectat de la serverul de administrare

- permită definirea unor setări separate ce vor fi aplicate in cazul unei epidemii de viruși

- permită administratorului sa definească sisteme din rețeaua administrată care vor deservi ca puncte intermediare de distribuție pentru actualizări si pachete de instalare

- permită administratorului sa implementeze o procedura de testare a actualizărilor pe anumite sisteme selectate, cu scopul de a efectua o verificare preliminara a calității actualizărilor înainte de distribuția lor pe toate sistemele client

- includă posibilitatea de scanare pentru detecția vulnerabilităților aplicațiilor si sistemelor de operare

- permită crearea de rapoarte la detectarea vulnerabilităților cu posibilitatea de grupare a sistemelor conform vulnerabilităților detectate

- permită administratorului sa salveze obiectele infectate sau suspecte direct pe stația de la care lucrează de pe sistemele client pe care acestea au fost detectate, pentru a le putea trimite către analiza

- ofere suport pentru monitorizarea parametrilor antivirus prin SNMP

- ofere un panou de informare ce prezintă in timp real informații despre starea securității pe sistemele administrat si alte informații suplimentare despre sistemele client

- ofere funcționalitate extinsa de monitorizare a soluției de securitate de pe sisteme prin salvarea de loguri la nivelul serverului de administrare

- permită administratorului sa primească rapoarte despre starea sistemului de protecție anti-malware, pe baza informațiilor stocate la nivelul serverului de administrare

- permită administratorului sa creeze selecții de sisteme client bazate pe starea protecție de pe acestea sau in funcție de alte criterii, cum ar fi sistemul de operare de pe acestea

- permită administratorului exportul de rapoarte in cel puțin următoarele formate: HTML, XML si PDF

- permită administratorului vizualizarea centralizată a tuturor aplicațiilor instalate pe sistemele client

- permită administratorului vizualizarea centralizată a informațiilor despre hardware-ul sistemelor client

- ofere administratorului posibilitatea de a se conecta de la distanta la stațiile client cu probleme in vederea efectuării acțiunilor de analiza si soluționare a problemelor (posibilitatea de extragere de pe sistemele client a informațiilor de sistem, event logs sau rularea de utilitare)

- includă tehnologii de detecție a sistemelor virtualizate administrate

- soluția va permite crearea unei politici dedicate sau configurații care pot fi lansate în mod automat fără intervenția administratorului în cazul în care numărul de incidente malware depășește un prag definit (de exemplu, in timpul unui " atac de virus ").

Șerbănescu Elisabeta
Șef birou