ROMÂNIA
MINISTERUL JUSTIŢIEI
TRIBUNALUL CLUJ
Prezentul document este supus reglementărilor aflate sub incidența R.U.E. nr. 2016/679
Nr. 140/DEFA/18.01.2019

SOLICITARE DE OFERTĂ

Tribunalul Cluj cu sediul în municipiul Cluj-Napoca, str. Calea Dorobanților, nr. 2, având cod fiscal 4565300, în calitate de autoritate contractantă, intenţionează să achizitioneze (prin SICAP) în ziua de 22.01.2019 produsele de mai jos, sens în care vă invită să depuneţi oferta dumneavoastră de preţ până la data de 22.01.2019, ora 12,00.

Denumire produs	Cod CPV	UM	Cantitate	Cerințe minimale
Licență software antivirus pentru stații de lucru	48761000-0	Buc	380	Conform Caietului de sarcini nr.136/17.01.2019, cu valabilitate licențe de 12 luni
Licență software antivirus pentru server	48761000-0	Buc	50	

Nota: Tribunalul Cluj își rezerva dreptul de a modifica cantitățile sau de a renunța la unele produse.

Tipul achizitiei este **cumpărarea directă**, conform dispoziţiilor art. 7, alin.5 din Legea nr. 98/2016 privind achizitiile publice, cu etapa prealabila de testare de piata, utilizand catalogul electronic de produse al **SICAP**.

Termenul de livrare este de maxim cinci zile de la finalizarea achiziției.

Termenul de plată este de 30 zile de la data recepției produselor și primirea facturii.

Criteriul utilizat pentru atribuirea contractului : „preţul cel mai scăzut", cu conditia respectarii specificatiilor tehnice solicitate în Caietul de sarcini anexat.

Oferta se va depune la sediul instituţiei în municipiul Cluj- Napoca, str. Calea Dorobanților, nr. 2, camera nr. 82 sau se va transmite prin e-mail la adresa luminita.albu@just.ro şi va conţine propunerea financiară si tehnica.

Data limită până la care se pot solicita clarificări: 22.01.2019, ora 10,00.

Data limită pentru depunerea/transmiterea ofertei: 22.01.2019, ora 12,00.

Locul de livrare: Tribunalul Cluj, Calea Dorobantilor nr.2, parter, Birou Informatic.

Pentru informaţii suplimentare ne puteţi contacta la telefon 0264/596110, int. 140 sau e-mail luminita.albu@just.ro, persoană de contact Luminița ALBU.

Manager economic Tribunalul Cluj

Coța Gabriela Mariana

ROMÂNIA 5 TRIBUNALUL CLUJ

136/17.01.2019

APROBAT,
PREȘEDINTE, Jud. Ana [illegible]

ROMÂNIA 5 TRIBUNALUL CLUJ

AVIZAT,
MANAGER ECONOMIC,
Ec. Gabriela COTA

CAIET DE SARCINI

pentru achiziţionarea serviciilor de protecţie de tip antivirus pentru Tribunalul Cluj

Cluj-Napoca
15-01-2019

Caracteristici tehnice minimale, obligatorii si eliminatorii pentru antivirus stații de lucru, server, dispozitive mobile si consola de administrare

Contents

Caracteristici tehnice minimale, obligatorii si eliminatorii pentru antivirus stații de lucru:

I. Cerinte produs antivirus statii de lucru:

1.1. Suita de securitate sa ruleze pe sisteme de operare Windows 32-bit si 64-bit: Windows 2003/2008/XP-SP3/Vista/7,8,8.1,10;

1.2. Suita de securitate sa ruleze pe sisteme de operare OS X: 10.12 (SIerra), 10.11 (El Capitan) 10.10 (Yosemite), 10.9 (Mavericks), 10.8 (Mountain Lion), 10.7 (Lion), 10.6 (Snow Leopard);

1.3. Suita de securitate sa ruleze pe sisteme de operare Linux 32-bit si 64-bit: Red Hat, Mandriva, SUSE, Debian, UBUNTU, Fedora si pe majoritatea distributiilor care au integrat un manager de distributie software bazat pe technologia RPM sau DEB cu specificatiile: Kernel 2.6 sau mai nou, Libraria de GNU C 2.3 sau mai noua, GTK+ 2.6 sau mai nou si se recomanda ca LSB 3.1 sa fie compatibil.

1.4. Produsul antivirus sa permita importul si exportul tuturor setarilor din toate modulele programului la nivel de client antivirus.

1.5. Produsul antivirus trebuie sa tina cel putin log-uri ale evenimentelor si cererilor de scanare la cerere ;

1.6. Produsul sa permita atentionarea administratorului, daca scanarea la cerere a fost intrerupta de utilizator

1.7. Produsul antivirus sa aiba posibilitatea de a seta perioada de stocare a logurilor

1.8. Sa existe posibilitatea setarii automate sau manuale, pentru optimizarea fisierelor log.

1.9. Sa se poata defini o locatie locala pentru stocarea fisierelor log intr-un alt sistem de fisiere decat cel standard (text,CSV,eveniment)

1.10. Produsul trebuie sa aiba posibilitatea adaugarii automate sau manuale a fisierelor in carantina ;

1.11. Produsul trebuie sa aiba posibilitatea expedierii automate si manuale a fisierelor infectate sau suspecte catre laboratorul de analiza antivirala al producatorului ;

1.12. Produsul antivirus trebuie sa aiba optiuni pentru a crea task-uri programate ;

1.13. Produsul antivirus trebuie sa afiseze informatii despre configuratia statiei pe care este instalat. Vor fi afisate cel putin sistemul de operare, tipul de procesor si capacitatea memoriei RAM instalat pe statia respectiva; cat si informatii cu privire la versiunea de produs instalata, numele calculatorului cat si utilizatorul logat.

1.14. Setarile produsului antivirus trebuie sa poata fi protejate cu o parola pentru a nu fi modificate decat de catre administratorii solutiei ;

1.15. Produsul antivirus trebuie sa poata trimite notificari administratorului solutiei prin SMTP .

1.16. Produsul la nivel de statie, sa nu afiseze mesaje utilizatorului, dar sa informeze administratorul solutiei.

1.17. Produsul antivirus la nivel de statie, sa ofere informatii detaliate despre modulele integrate respectiv: kernel,semnaturi de virusi,euristica,auristica avansata, arhiva,firewall,antispam,WEB filter

1.18. In cazul unei notificari de virus, aplicatia sa avertizeze sonor utilizatorul.Solutia sa permita activarea sau dezactivarea optiunii de avertizare sonora.

1.19. Serviciul antivirus sa ruleze ca serviciu local

1.20. Produsul antivirus sa scaneze in mod automat, orice dispozitiv mobil de stocare la momentul introducerii in portul USB si se vor scana fisierele de tip AUTORUN.INF de pe dispozitivele de stocare.

1.21. Produsul antivirus, sa aiba posibilitatea de a genera din interfata client sau consola de management a unui fisier de tip log detaliiat, cu toate serviciile ce ruleaza pe respectiva statie, pentru identificarea si detalierea fiecarui servicu respectiv fisier cat si nivelul filtrarii in functie de gradul de risc.Fisierul log sa poata fi exportat si trimis catre analiza.

1.22. Produsul de securitate sa aiba posibilitatea,din interfata client de a creea CD/DVD/USB-stick boot-abile, cu versiunea antivirus in vederea devirusarii calculatoarelor in mod "offline".

1.23. Produsul antivirus sa ofere functie de autoprotectie, impotriva dezactivarii sau coruperii solutiei antivirus de catre diferite coduri malware.

1.24. Solutia de securitate sa contina un modul pentru protectia impotriva "exploit-urilor" cum ar fi cititoare PDF, browser-ele WEB, JAVA, clienti-email sau componente MS-OFFICE. Aceasta functie sa poata fi activata sau dezactivata independent

1.25. Clientul antivirus, sa prezinte in interfata de administrare locala vizualizarea activitatii in mod grafic in timp real atat a fisierelor aflate local cat si a activitatii din retea.

1.26. Clientul antivirus sa permita la vizualizarea activitatii din interfata de administrare locala setarea perioadei pe care se doreste vizualizarea raportului.

1.27. Interfata utilizatorului(GUI) sa poata fi setata pe mai multe nivele.

1.28. Sa se poata activa sau dezactiva functia de NAP Network Access Protection

1.29. Utilizatorul din interfata client sa poata vizualiza toate procesele care se executa si sa solicite informatii suplimentare de la producator despre fiecare proces referitor la: nivelul de risc,numar utilizatori, nume aplicatie,detalii despre proces (locatie,dimensiune,descriere,nume companie,versiune fisier,nume produs) si ora la care s-a descoperit.

1.30. La cerere utilizatorul sa poata verifica, reputatia unui fisier oferind informatii despre: nivelul de risc,numar utilizatori, nume aplicatie,detalii despre proces (locatie,dimensiune,descriere,nume companie,versiune fisier,nume produs) si data la care s-a descoperit.

1.31. Clientul antivirus din interfata de administrare locala sa permita o vizualizarea statistica centralizata pentru:

1.32. Protectie antivirus si antispyware

1.33. Protectia in timp real a sistemului de fisiere

1.34. Protectie client email

1.35. Protectie acces WEB

1.36. Solutia de securitate sa poata bloca mesajele de notificare, cand o aplicatie ruleaza in modul FULL SCREEN.De asemenea blocarea notificarilor sa poata fi dezactivata in mod automat dupa un anumit timp definit in minute.

1.37. Dupa prima instalare in mod implicit solutia de securitate sa porneasca o scanare a intregului computer;

1.38. Produsul antivirus sa poata scana computerul cand acesta intra in stare de inactivitate. Detectarea starii de inactivitate se va activa atunci cand computerul se afla in urmatoarele stari: screen saver, blocare computer, deconectare utilizator, fiecare stare se va activa sau dezactiva independent. Functionalitatea scanarii in stare de inactivitate sa poata fi activata sau dezactivata independent.

1.39. Solutia de securitate sa comunice cu server-ul de management prin agent

1.40. Produsul trebuie sa fie lansat in versiune comerciala si sa se prezinte link public din site-ul producatorului

II. Protectie rezidenta:

2.1. Aplicatia sa aiba scanner rezident care sa monitorizeze in timp real aplicatiile care sunt lansate/rulate;

2.2. Scanner-ul rezident sa ofere posibilitatea setarii optiunii de a porni sau nu automat la pornirea sistemului (PC-ului);

2.3. Scanner-ul rezident sa aiba posibilitatea de a fi oprit manual;

2.4. Scanner-ul rezident sa ofere posibilitatea setarii unui mod de scanare optimizat;

2.5. Pentru a putea eficientiza lucrul cu PC-ul, produsul trebuie sa ofere posibilitatea de a seta stadiul in care sa fie scanate fisierele de catre modulul resident, respectiv la deschiderea fisierului, la crearea, respectiv executia lui, oprirea calculatorului.

2.6. Produsul antivirus trebuie sa ofere optiuni de configurare pentru scanarea tuturor tipurilor de fisiere, indiferent de extensie si indiferent daca au sau nu extensie ;

2.7. Scanner-ul rezident al produsului antivirus sa faca cel putin scanarea dupa semnaturi, euristic, spyware, adware si aplicatii ce pot reprezenta potentiale pericole;

2.8. Scanner-ul rezident al produsului antivirus trebuie sa ofere posibilitatea configurarii modulului euristic pe 2 nivele pentru a putea optimiza in functie de caz folosirea resurselor de catre aplicatia antivirus ;

2.9. Modulul rezident sa ofere o protectie rezidenta si pentru amenintarile noi aparute in functie de reputatie.

2.10. Pentru fisierele noi create si modificate acestea sa poata fi scanate cu ajutorul modulelor euristice.

2.11. Configurarea scanner-ului rezident al aplicatiei astfel incat sa fie excluse de la scanare anumite foldere/ fisiere sau extensii specificate si posibilitatea setarii acestei reguli cu caracter permanent;

2.12. Scanner-ul rezident al aplicatiei antivirus trebuie sa faca scanarea: sectoarelor de boot,unitati locale, unitati portabile si a retelei;

2.13. Scanner-ul rezident al aplicatiei trebuie sa ofere posibilitatea mutarii in carantina a fisierului infectat .

2.14. Produsul de securitate sa ofere posibilitatea de a putea defini reguli pentru unitatile portabile(memorii USB), CD/DVD,FireWire,Imaging Device(scaner,camere web),Imprimante USB,Bluetooth Device,Memory Card Reader,Modem,LPT/COM,regulile sa poata fi facute dupa urmatoarele criterii:Tip Dispozitiv,Numar Serie,Producator-Vanzator,Model, si sa se poata aplica drepturi de citire si scriere,sau access refuzat pentru utilizatori definiti locali sau AD

2.15. Din clientul antivirus, utilizatorul sa poata defini limite de scanare a obiectelor in functie de dimensiune fisier si durata maxima de scanare pentru fisierele respective.

2.16. Din setarile clientului antivirus, utilizatorul sa poata defini nivelul de scanare al arhivelor ce contin alte arhive si setarea dimensiunii acestora.

2.17. Produsul antivirus va permite pentru executarea fisierelor activarea functiei de euristica avansata.Aceasta functie se va putea activa independent de setarea generala a produsului antivirus, si va actiona strict numai la executarea fisierelor.

2.18. Produsul antivirus va permite activarea functiei de euristica avansata numai pe unitatii media portabile.Aceasta functie se va putea activa independent de setarea generala a produsului antivirus, si va actiona strict numai la executarea fisierelor de pe unitatii media portabile

2.19. Solutia de securitate sa poata analiza in mod activ comportamentul fisierelor,registrilor, proceselor si sa poata preveni orice modificare fara o notificare.

2.20. Pentru a spori performantele in mediile virtuale, fisierele deja scanate vor trebui indexate si partaje cu fiecare solutie antivirus de la acelasi producator prezenta pe respectivul host.

2.21. Produsul antivirus sa ofere posibilitatea scanarii automate a unui dispozitiv la inserare.

2.22. Produsul antivirus sa ofere protectie impotriva programelor comprimate in pachete sau protectii(Aceste tipuri de protectii sunt adesea exploatate de autorii programelor rau intentionate pentru a evita detectarea). Aceasta functionalitate sa poata fi activata sau dezactivata independent

III. Protectie Internet :

3.1. Aplicatia antivirus trebuie sa aiba cel putin optiuni de scanare a protocoalelor POP3,IMAP , HTTP si HTTPS ;

3.2. Pentru optimizarea resurselor ocupate de solutia antivirus trebuie sa fie posibila setarea scanarii ambelor porturi sau doar a unuia dintre ele (cel folosit), in functie de necesitatile utilizatorului statiei ;

3.3. Produsul antivirus trebuie sa aiba optiune pentru detectarea automata a portului HTTP / HTTPS , setarea manuala a portului in cazul in care nu sunt folosite variante default si posibilitatea de a detecta automat comunicarea HTTP / HTTPS pe alte porturi ;

3.4. Produsul antivirus trebuie sa aiba optiunea de a modifica subiectul e-mail-urilor infectate primite pe statie. Mesajul trebuie sa poata fi modificat conform preferintelor administratorului solutiei antivirus ;

3.5. Produsul antivirus trebuie sa aiba optiuni de a adauga in corpul e-mail-ului a unui mesaj care sa ateste faptul ca e-mail-ul a fost scanat si rezultatul scanarii ;

3.6. Produsul antivirus trebuie sa ofere optiuni de configurare pentru scanarea tuturor tipurilor de fisiere, indiferent de extensie si indiferent daca au sau nu extensie pentru fisierele care sunt scanate pe POP3, IMAP, HTTP si HTTPS;

3.7. Configurarea scanner-ului aplicatiei astfel incat sa fie excluse de la scanarea POP3,IMAP, HTTP si HTTPS anumite extensii specificate ;

3.8. Protectia POP3,IMAP, HTTP si HTTPS a produsului trebuie sa aiba posibilitatea configurarii modulului euristic pe 2 nivele pentru a putea optimiza in functie de caz folosirea resurselor de catre aplicatia antivirus si timpul de scanare a fisierelor ;

3.9. La scanarea POP3,IMAP , HTTP si HTTPS produsul antivirus trebuie sa faca cel putin scanarea dupa semnaturi, euristic, spyware, adware si alte aplicatii ce pot reprezenta potentiale pericole;

3.10. La scanarea HTTP / HTTPS produsul antivirus trebuie sa poata interzice automat descarcarea fisierului infectat ;

3.11. Produsul antivirus trebuie sa aiba posibilitatea configurarii actiunilor care vor fi intreprinse la detectarea codului viral, in functie de tipul obiectelor infectate, la nivel POP3,IMAP , HTTP si HTTPS.

3.12. La scanarea HTTP, sa poata fi adaugate siteuri care sa poata fi excluse de la scanare, sau siteuri care care sa nu fie accesate de utilizatori.

3.13. Produsul antivirus, sa permita scanarea traficului securizat SSL pentru protocolul HTTPS cat si pentru POP3S si IMAPS.

3.14. Produsul de securitate sa ofere protectie Anti-Phishing

IV. Filtrarea continutului WEB:

4.1. Produsul de securitatea sa contina un modul pentru filtrarea automata a continutului WEB.

4.2. Filtrarea continutului sa se poata face pe baza unor categorii predefinite (de exemplu toate web site-urile care au continut despre Violenta, Arme sau Jocuri de noroc).

4.3. Modulul de filtrare sa permita adaugarea de reguli pentru a putea permite / nepermitere accesul la URL-uri ce pot fi in una din categoriile predefinite.

4.4. Modulul de filtrare sa permita crearea unor grupuri de URL-uri.

V. Scanare la cerere :

5.1. Produsul antivirus trebuie sa ofere optiuni de configurare pentru scanarea tuturor tipurilor de fisiere, indiferent de extensie si indiferent daca au sau nu extensie .

5.2. Scanner-ul la cerere al produsului antivirus sa faca cel putin scanarea dupa semnaturi, euristic, euristica avansata si sa verifice reputatia fisierelor in cloud

5.3. Scanner-ul la cerere al produsului antivirus trebuie sa ofere posibilitatea configurarii modulului euristic pe cel putin 2 nivele pentru a putea optimiza in functie de caz folosirea resurselor de catre aplicatia antivirus .

5.4. Pentru scanarea la cerere utilizatorul sa poata defini limite de scanare a obiectelor in functie de dimensiune fisier, durata maxima de scanare, imbricararea arhivelor si setarea dimensiunii unei arhive

5.5. Configurarea scanner-ului la cerere al aplicatiei astfel incat sa fie excluse de la scanare anumite extensii specificate.

5.6. Scanner-ul la cerere sa aiba posibilitatea de a face doar scanare si de a scana si curata .

5.7. Pentru utilizatorii fara experienta, scanarea la cerere sa se faca simplu printr-un singur click.

5.8. Interfata cu utilizatorul, sa aiba o bara de progres cat si date despre ultima scanare si cate alerte de virusi au fost.

5.9. Pentru scanarea la cerere solutia de securitate sa ofere posibilitatea, de a activa sau dezactiva prioritizarea procesului de scanare pentru a nu afecta buna functionate a programelor deja folosite.

VI. Update/Upgrade produs antivirus statie de lucru :

6.1. Solutia antivirus trebuie sa-si poata face update-ul bazei de date cu semnaturi de virusi la intervale de cel putin 1 minut;

6.2. Update-ul trebuie sa poata fi facut de pe Internet/ LAN/ alte medii de stocare ;

6.3. Produsul antivirus trebuie sa poata detecta automat tipul de conexiune la Internet pentru a putea beneficia de fisiere de update adecvate tipului de conexiune ;

6.4. Produsul antivirus trebui sa aiba posibilitatea introducerii unei adrese de Internet/ Intranet de la care sa faca actualizarea componentelor aplicatiei ;

6.5. Updateul/Upgradeul trebuie sa poata fi facute atat automat cat si manual (la cerere);

6.6. Produsul antivirus trebuie sa poata face detectatea automata a Proxy Server-ului daca acesta exista ;

6.7. Produsul antivirus trebuie sa ofere posibilitatea setarii unui utilizator si a unei parole cu care sa se log-eze in LAN pentru a face update-ul (altul decat utilizatorul curent) ;

6.8. Update-ul din LAN trebuie sa se poata face cu ajutorul share-ului de pe sisteme Microsoft sau prin HTTP;

6.9. Produsul antivirus trebuie sa poata fi setat sa dea o notificare inainte de update/upgrade ;

6.10. Produsul antivirus trebuie sa aiba optiuni de configurare astfel incat sa nu fie necesara repornirea PC-ului/ serverului dupa actualizarea componentelor antivirusului;

6.11. Produsul antivirus sa nu necesite repornire a calculatorului la upgrade.

6.12. Solutia antivirus sa permita configurarea varstei maxime permise bazei de semnaturi inainte de a fi considerata invechita;

6.13. Din clientul antivirus sa se poata reveni la o baza de semnaturi anterioara in cazul in care se constata alerte de tip false-positive;

6.14. Produsul antivirus sa permita reluarea descarcarii de unde a ramas in cazul in care conexiunea cu serverul de actualizare este intrerupta.

VII. Firewall

7.1. Modulul FIREWALL al antivirusului sa poata fi setat pe mai multe moduri:automat,interactiv,invatare si bazat pe politici definite de utilizator;

7.2. Sa se poata seta nivele de protectie(Protectie stricta sau Permite partajarea) in special pentru utilizatorii mobili (pentru cei cu laptop), atunci cand se conecteaza la diferite retele;

7.3. Modulul firewall sa poata detecta vulnerabilitati pentru care un patch nu a fost lansat;

7.4. Modulul integrat firewal sa ofere protectie BOTNET

7.5. Modulul FIREWALL sa ofere protectie pentru:

- RPC attack
- DNS attack
- ARP attack
- Port scanning attack(TCP/UDP)
- SMB attack
- Verificare conexiune TCP
- Date ascunse in protocolul ICMP

7.6. Modulul Firewall, sa poata oferi detectarea aplicatiilor daca au fost modificate si vor sa stabileasca o conexiune.

7.7. Modulul Firewall sa ofere optional, facilitatea "Mod de invatare"

7.8. Modulul firewall sa se poata integra cu Microsoft Windows Vista, Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows 8.1, Microsoft Windows 10

7.9. Din interfata client sa se poata crea regului de protectie firewall direct din log sau fereastra de notificari.

7.10. Solutia sa ofere un modul de IDS (Intrusion Detection System) care sa permita configurarea accesului la unele dispozitive din zona de incredere cum ar fi: UpnP, RPC, RDP .

7.11. Modulul IDS sa ofere posibilitatea da a putea verifica pachetele pentru:

- Interzicere a dialectelor SMB vechi (neacceptate)
- Interzicere a deschiderii fişierelor executabile pe un server din afara Zonei de încredere în protocolul SMB
- Interzicere a autentificării NTLM în protocolul SMB pentru conectarea unui server în Zona de încredere
- Verificare stare conexiune TCP
- Detectare suprasolicitare protocol TCP
- Verificare mesaj protocol ICMP
- Detectare date ascunse la protocolul ICMP
- Verificare mesaj protocol ICMP
- Interzicere sesiuni SMB fără securitate extinsă

7.12. Modulul IDS sa ofere posibilitatea de a detecta intruziuni pentru protocoalele: SMB, RPC, RDP cat si diferite atacuri pentru:

- Intoxicare ARP
- Intoxicare DNS
- Detectare atac de tip Scanare port TCP/UDP
- Blocare adresă nesigură după detectarea unui atac

VIII. Antispam

8.1. Produsul va trebui sa ofere protectie antispam, conexiunea sa se realizeze cu o baza de date de semnaturi din internet

8.2. Asigura scanarea atasamentelor si a continutului mesajelor in timp real, fara a incetini traficul e-mail

8.3. Se vor trimite notificari la detectarea unui mail virusat in functie de optiunile alese la administrator, „sender sau receiver"

8.4. Sa importe in mod automat adresele de e-mail din "adress book" si sa le adauge in WHITE LIST pentru a le exclude de la scanarea antispam

8.5. Sa adauge in subiect "[SPAM]" pentru a identifica un mesaj de tip spam mai usor;

8.6. Sa mute mesajele spam intr-un anumit director;

8.7. Produsul antivirus sa afiseze in cifre sau procente cate mesaje a scanat, cate au fost considerate SPAM, cate nu au fost mesaje de tip SPAM.

8.8. Sa afiseze aceleasi detalii de mai sus de cand a fost instalata aplicatia.

8.9. Modulul antispam sa se integreze cu urmatorii clientii de e-mail

- Microsoft Outlook
- Microsoft Outlook Express
- Windows Mail
- Windows Live Mail

IX. Protectie pentru dispozitivele mobile

Caracteristici tehnice minimale, obligatorii si eliminatorii pentru antivirus for Android

9.1. Produsul antivirus sa ruleze pe sisteme de operare Android 4 (Ice Cream Sandwich) şi versiuni ulterioare

9.2. Produsul trebuie sa fie lansat in versiune comerciala si sa se prezinte link public din site-ul producatorului

9.3. Rezoluţie ecran tactil: 480 x 800 pixeli

9.4. CPU: ARM cu setul de instrucţiuni ARMv7, x86 Intel Atom

9.5. Spaţiu de stocare liber: 20 MB

9.6. Conexiune internet

9.7. Aplicatia (APK) sa poata fi descarcata din siteul producatorului sau din magazinul Google Play, pe baza unui cod QR

9.8. Produsul instalat sa poata raporta la o consola de la acelasi producator

9.9. Produsul sa permita scanarea automata a dispozitivului la o oră predefinită

9.10. Produsul sa permita scanarea automata atunci cand dispozitivul este la incarcat.

9.11. Produsul sa permita crearea de loguri dupa fiecare scanare planificata sau declansata manual

9.12. Logurile sa contina :

- data şi ora evenimentului
- durata scanării
- numărul fişierelor scanate
- rezultatele scanării sau erorile întâlnite în timpul scanării

9.13. Produsul sa permita scanarea in timp real a aplicatiilor instalate (APK) si toate fisierele existente pe CARDUL SD dupa instalarea acestuia.

9.14. Produsul sa ofere protectie pentru aplicatii nedorite cum ar fi programe care contin adware ,care instaleaza bare de instrumente,care tin evidenta rezultatelor cautarii sau care au alte obiective neclare

9.15. Produsul sa ofere posibilitatea de monitorizare si blocare a aplicatiilor care permit accesul de la distanta,aplicatiilor pentru stergerea parolelor sau de inregistrare a datelor

9.16. Activarea produsului sa poata fi facut cu o cheie de licenta sau un cont de administrator de Securitate

9.17. Posibilitatea de a configura durata de timp maxima pe care utilizatorul va fi notificat despre necesitatea actualizării solutiei ANTIVIRUS.

9.18. Produsul sa permita oprirea temporara a scanarii

9.19. Produsul sa permita configurarea scanarii in functie de necesitatile utilizatorului pe cel putin 2 nivele

9.20. Produsul sa fie conectat la o baza de semnaturi cloud (de unde sa se pota verifica in mod automat anumite aplicatii/programe)

9.21. Produsul sa permita blocarea SMS,MMS & Apeluri (cu exceptia Android OS 4.4 (KitKat) şi pe dispozitivele pe care Google Hangouts s-a setat ca aplicaţie principală pentru SMS

9.22. Produsul sa poata oferii un istoric al comunicatiilor blocate

9.23. Posibilitatea blocarii comunicatiilor (SMS/MMS/Apeluri) in functie de ora

9.24. Aplicatia de securitate sa contina si un filtru pentru SMS-uri si apeluri in functie de regulile definite de utilizator.

9.25. Produsul sa contina si un modul ANTI-THEFT, pentru a proteja dispozitivul impotriva accesului neautorizat sau in cazul in care dispozitivul este pierdut sau furat.

9.26. In cazul perderii sau furtului si inserarii unui nou card SIM, aplicatia ANTIVIRUS sa poata notifica administratorul si sa blocheze terminalul

9.27. In cazul in care se introduce un alt card SIM mesajul va include numărul de telefon al cartelei SIM introduse în mod curent, numărul IMSI (International Mobile Subscriber Identity) şi numărul IMEI (International Mobile Equipment Identity) al telefonului

9.28. Administratorul sa poata solicita coordonatele GPS ale dispozitivului mobil pierdut si sa poata şterge de la distanţă toate datele stocate pe dispozitiv.

9.29. Aplicatia ANTIVIRUS sa permita cu ajutorul SMS si din consola de administrare: localizarea dispozitivului , blocarea dispozitivului, deblocarea dispozitivului, stergerea datelor de pe dispozitiv, revenirea la setarile din fabrica si sirena.

9.30. Pentru a îmbunătăţi securitatea comenzilor prin SMS, administratorul va primi pe telefonul mobil un cod SMS de verificare unic şi cu limită de timp (la numărul definit în lista contactelor administratorului) atunci când execută o comandă prin SMS. Acest cod de verificare se va utiliza pentru a verifica o anumită comandă.

9.31. Administratorul poate defini informaţiile: nume companie,adresa de email si un mesaj particularizat care se vor afişa atunci când dispozitivul este blocat, cu opţiunea de apelare a unuia dintre contactele predefinite ale administratorului.

9.32. Solutia de Securitate ANTIVIRUS sa contina si control aplicaţiilor care oferă administratorilor opţiunea de a monitoriza aplicaţiile instalate, de a bloca accesul la aplicaţiile definite şi de a reduce riscul expunerii solicitând utilizatorilor să dezinstaleze anumite aplicaţii.

9.33. Administratorul poate selecta una dintre metodele de filtrare a aplicaţiilor:

- Definiţi manual aplicaţiile care trebuie blocate
- Blocare în funcţie de categorie (de exemplu, jocuri sau reţele de socializare)
- Blocare în funcţie de permisiune (de exemplu, aplicaţii care urmăresc locaţia)

- Blocare după sursă (de exemplu, aplicaţii instalate din alte surse decât magazinul Google Play)

9.34. Administratorul sa poata defini regului elementare de securitate pentru dispozitivele mobile cum ar fi:

- complexitatea necesară blocării ecranului(cod PIN,parola,lungimea minima a codului,numarul maxim al incercarilor dupa care dispozitivul sa revina la setarile din fabrica, temporizatorul de blocare a ecranului)
- utilizarea camerei incorporate

9.35. Produsul de securitate sa contina un modul Anti-Phishing si sa se poata integra in toate browserele cunoscute.

X. Protectie pentru serverele de fisiere

Caracteristici tehnice minimale, obligatorii si eliminatorii pentru antivirus file server :

10.1. Produsul antivirus sa ruleze pe urmatoarele sisteme de operare : Windows server 2003 / 2008 32/64-BIT,Windows server 2012 R2, Windows Server 2016

10.2. Produsul trebuie sa fie lansat in versiune comerciala si sa se prezinte link public din site-ul producatorului

10.3. Produsul antivirus sa permita importul si exportul tuturor setarilor din toate modulele programului la nivel de client antivirus

10.4. Produsul antivirus trebuie sa tina cel putin log-uri ale evenimentelor si cererilor de scanare la cerere ;

10.5. Produsul sa permita atentionarea administratorului, daca scanarea la cerere a fost intrerupta de utilizator

10.6. Produsul antivirus sa aiba posibilitatea de a seta perioada de stocare a logurilor

10.7. Sa existe posibilitatea setarii automate sau manuale, pentru optimizarea fisierelor log.

10.8. Produsul trebuie sa aiba posibilitatea adaugarii automate sau manuale a fisierelor in carantina ;

10.9. Produsul trebuie sa aiba posibilitatea expedierii automate si manuale a fisierelor infectate sau suspecte catre laboratorul de analiza antivirala al producatorului ;

10.10. Produsul antivirus trebuie sa aiba optiuni pentru a crea task-uri programate ;

10.11. Produsul antivirus trebuie sa afiseze informatii despre configuratia statiei pe care este instalat. Vor fi afisate cel putin sistemul de operare, tipul de procesor si RAM-ul instalat pe statia respectiva ;

10.12. Setarile produsului antivirus trebuie sa poata fi protejate cu o parola pentru a nu fi modificate decat de catre administratorii solutiei ;

10.13. Produsul antivirus trebuie sa poata trimite notificari administratorului solutiei prin SMTP si mesaje in LAN ;

10.14. Produsul sa nu prezinte optiuni de modificare a interfetei client pentru a nu folosi resurse inutil

10.15. Produsul la nivel de statie, sa nu afiseze mesaje utilizatorului, dar sa informeze administratorul solutiei.

10.16. Produsul antivirus la nivel de statie, sa ofere informatii detaliate despre vesiunea instalata, cat si despre modulele integrate respectiv: kernel,semnaturi de virusi,engines.

10.17. In cazul unei notificari de virus, aplicatia sa avertizeze sonor utilizatorul.Solutia sa permita activarea sau dezactivarea optiunii de avertizare sonora.

10.18. Sa se poata personaliza, pachetele antivirus(client) inainte de instalare in functie de cerintele administratorului la "deployment". Aceasta operatiune, se va efectua in urma unei singure actiuni din partea administratorului si preconfigurarea clientilor antivirus,la momentul deploymentul-ui nu va implica instalarea folosind consola de management.

10.19. Serviciul antivirus sa ruleze ca serviciu local

10.20. Produsul antivirus sa scaneze in mod automat, orice dispozitiv mobil de stocare la momentul introducerii in portul USB si se vor scana fisierele de tip AUTORUN.INF de pe dispozitivele de stocare.

10.21. Produsul antivirus, sa aiba posibilitatea de a genera din interfata client sau consola de management a unui fisier de tip log detaliiat, cu toate serviciile ce ruleaza pe respectiva statie, pentru identificarea si detalierea fiecarui servicu respectiv fisier cat si nivelul filtrarii in functie de gradul de risc.Fisierul log sa poata fi exportat si trimis catre analiza.

10.22. Produsul antivirus sa aiba posibilitatea,din interfata client sau consola de administrare de a genera CD/DVD/USB-stick boot-abile, cu versiunea antivirus la zi in vederea devirusarii calculatoarelor in mod "offline".

10.23. Produsul antivirus sa ofere functie de autoprotectie, impotriva dezactivarii sau coruperii solutiei antivirus de catre diferite coduri malware.

10.24. Clientul antivirus, sa prezinte in interfata de administrare locala vizualizarea activitatii in mod grafic in timp real atat a fisierelor aflate local cat si a activitatii din retea.

10.25. Clientul antivirus sa permita la vizualizarea activitatii din interfata de administrare locala setarea perioadei pe care se doreste vizualizarea raportului.

10.26. Clientul antivirus din interfata de administrare locala sa permita o vizualizarea statistica centralizata pentru:

- Protectie antivirus si antispyware
- Protectia in timp real a sistemului de fisiere
- Protectie client email
- Protectie acces WEB

10.27. Clientul antivirus sa poata fi rulat cel putin pe configuratii de genul:

- Procesor: Intel or AMD x86/x64
- Memorie:48MB
- Spatiu pe disk(descarcare):32
- Spatiu pe disk(instalare):46

10.28. Aplicatia sa aiba scanner rezident care sa monitorizeze in timp real aplicatiile care sunt lansate/rulate;

10.29. Scanner-ul rezident sa ofere posibilitatea setarii optiunii de a porni sau nu automat la pornirea sistemului (PC-ului);

10.30. Produsul sa excluda de la scanare in mod automat fisierele critice;

10.31. Produsul sa contina un instrument de tip Shell (sa permita si folosirea command line)

10.32. Scanner-ul rezident sa aiba posibilitatea de a fi oprit manual;

10.33. Scanner-ul rezident sa ofere posibilitatea setarii unui mod de scanare optimizat;

10.34. Pentru a putea eficientiza lucrul cu PC-ul, produsul trebuie sa ofere posibilitatea de a seta stadiul in care sa fie scanate fisierele de catre modulul resident, respectiv la deschiderea fisierului, la crearea, respectiv executia lui, oprirea calculatorului.

10.35. Produsul antivirus trebuie sa ofere optiuni de configurare pentru scanarea tuturor tipurilor de fisiere, indiferent de extensie si indiferent daca au sau nu extensie ;

10.36. Scanner-ul rezident al produsului antivirus sa faca cel putin scanarea dupa semnaturi, euristic, spyware, adware si aplicatii ce pot reprezenta potentiale pericole;

10.37. Scanner-ul rezident al produsului antivirus trebuie sa ofere posibilitatea configurarii modulului euristic pe 2 nivele pentru a putea optimiza in functie de caz folosirea resurselor de catre aplicatia antivirus ;

10.38. Configurarea scanner-ului rezident al aplicatiei astfel incat sa fie excluse de la scanare anumite foldere/ fisiere sau extensii specificate si posibilitatea setarii acestei reguli cu caracter temporar si / sau permanent;

10.39. Scanner-ul rezident al aplicatiei antivirus trebuie sa faca scanarea: sectoarelor de boot la accesare, a suportilor magentici/optici si a retelei ;

10.40. Scanner-ul rezident al aplicatiei trebuie sa ofere posibilitatea setarii mutarii in carantina a fisierului infectat .

10.41. Produsul antivirus sa aiba posibilitatea de a bloca accesul la unitatii media de stocare portabile cat si posibilitatea de a exclude de la blocare din interfata clientului antivirus sau din consola de administrare a unui sau mai multor porturi USB

10.42. Din clientul antivirus, utilizatorul sa poata defini limite de scanare a obiectelor in functie de dimensiune fisier si durata maxima de scanare pentru fisierele respective.

10.43. Din setarile clientului antivirus, utilizatorul sa poata defini nivelul de scanare al arhivelor ce contin alte arhive si setarea dimensiunii acestora.

10.44. Produsul antivirus va permite pentru executarea fisierelor activarea functiei de euristica avansata.Aceasta functie se va putea activa independent de setarea generala a produsului antivirus, si va actiona strict numai la executarea fisierelor.

10.45. Produsul antivirus va permite activarea functiei de euristica avansata numai pe unitatii media portabile.Aceasta functie se va putea activa independent de setarea generala a produsului antivirus, si va actiona strict numai la executarea fisierelor de pe unitatii media portabile

10.46. Produsul antivirus trebuie sa ofere optiuni de configurare pentru scanarea tuturor tipurilor de fisiere, indiferent de extensie si indiferent daca au sau nu extensie ;

10.47. Scanner-ul la cerere al produsului antivirus sa faca cel putin scanarea dupa semnaturi, euristic, spyware, adware si aplicatii ce pot reprezenta potentiale pericole;

10.48. Scanner-ul la cerere al produsului antivirus trebuie sa ofere posibilitatea configurarii modulului euristic pe cel putin 2 nivele pentru a putea optimiza in functie de caz folosirea resurselor de catre aplicatia antivirus ;

10.49. Configurarea scanner-ului la cerere al aplicatiei astfel incat sa fie excluse de la scanare anumite extensii specificate;

10.50. Scanner-ul la cerere sa aiba posibilitatea de a face doar scanare si de a scana si curata .

10.51. Pentru utilizatorii fara experienta, scanarea la cerere sa se faca simplu printr-un singur click.

10.52. Interfata cu utilizatorul, sa aiba o bara de progres cat si date despre ultima scanare si cate alerte de virusi au fost.

10.53. Solutia antivirus trebuie sa-si poata face update-ul bazei de date cu semnaturi de virusi la intervale de cel putin 1 minut;

10.54. Update-ul trebuie sa poata fi facut de pe Internet/ LAN/ alte medii de stocare ;

10.55. Produsul antivirus trebuie sa poata detecta automat tipul de conexiune la Internet pentru a putea beneficia de fisiere de update adecvate tipului de conexiune ;

10.56. Produsul antivirus trebui sa aiba posibilitatea introducerii unei adrese de Internet/ Intranet de la care sa faca actualizarea componentelor aplicatiei ;

10.57. Updateul/Upgradeul trebuie sa poata fi facute atat automat cat si manual (la cerere);

10.58. Produsul antivirus trebuie sa poata face detectatea automata a Proxy Server-ului daca acesta exista ;

10.59. Produsul antivirus trebuie sa ofere posibilitatea setarii unui utilizator si a unei parole cu care sa se log-eze in LAN pentru a face update-ul (altul decat utilizatorul curent) ;

10.60. Update-ul din LAN trebuie sa se poata face cu ajutorul share-ului de pe sisteme Microsoft sau prin HTTP;

10.61. Produsul antivirus trebuie sa poata fi setat sa dea o notificare inainte de update/upgrade ;

10.62. Produsul antivirus trebuie sa aiba optiuni de configurare astfel incat sa nu fie necesara repornirea PC-ului/ serverului dupa actualizarea componentelor antivirusului.

10.63. Produsul antivirus sa nu necesite repornire a calculatorului la upgrade.

XI. Cerinte producator si furnizor :

11.1. Producatorul trebuie sa fie certificat ISO 9001 pentru dezvoltare de software si consultanta legata de securitatea IT ;

11.2. Producatorul trebuie sa fie certificat ISO 27001 pentru dezvoltare,vanzare,livrare si implementare a serviciilor de securitate;

11.3. Furnizorul trebuie sa fie certficat ca partener al producatorului sau reprezentantului in Romania al producatorului ;

11.4. Furnizorul trebuie sa aiba cel putin 2 oameni specializati si certificati de producator sau de reprezentantului in Romania al producatorului.

11.5. Produsul ofertat va trebui sa prezinte premii si certificari Virus Bulletin 100% Awards;

11.6. Producatorul suitei de securitate trebuie sa detina un numar cat mai mare de validari (distinctii/premii) in testele VB100, Virus Bulletin – numarul premiilor reprezinta un avantaj;

11.7. Producatorul trebuie sa apara in lista Microsoft (List of antivirus software vendors): http://windows.microsoft.com/en-US/windows/antivirus-partners#AVtabs=win7

XII. CONSOLA DE MANAGEMENT

Instalare si configurare

12.1.1. Solutia de management sa poata fi instalata si utilizata pe platforme Windows 32bit si 64bit: Windows Server 2003, Windows Server 2003 R2,Windows Server 2008, Windows Server 2008 R2 Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Vista,Windows 7,Windows 8,Windows 8.1, Windows 10;

12.1.2. Solutia de management sa poata fi instalata si utilizata pe platforme Linux 32bit si 64bit:Ubuntu 12.04, RHEL Server 6, Cent OS6,SLED/SLES11,Open SUSE 13,Debian 7, Fedora 19 si versiunile actualizate ale sistemelor de operare mai sus mentionate

12.1.3. Solutia de management sa poata fi livrata ca un virtual appliance bazat pe sistem de operare linux si sa contina toate serviciile necesare pentru o functionare optima.

12.1.4. Imaginea de tip tamplate sa fie in formatul open virtualization appliance (OWA) si sa fie compatibila cu urmatorii hypervisor-i

12.1.5. VMware- vSphere/Player/Workstation, Oracle VirtualBox 4.3.24 sau mai nou, ESXi 5.0,ESXi 5.1,ESXi 5.5, Microsoft Hyper-V Windows Server 2012, Windows Server 2012 R2, Windows Server 2016

12.1.6. Solutia sa fie scalabila,astfel ca anumite componente (MDM si Proxy) sa ruleze separat pe mai multe masini virtuale

12.1.7. Pentru organizatiile care folosesc medii hibrid sa existe posibilitatea de a folosi solutia de management si pentru Microsoft Azure (necesita licenta pentru Microsoft Azure)

XII.I. Cerinte de sistem

12.2.1. Consola de management sa poata functiona pe urmatoarele specificatii hardware:

Memory	4 GB RAM
Hard Drive	At least 20 GB of free space
Processor	Dual-Core, 2.0 GHz or faster
Network connection	1 Gbit/s

12.2.2. Solutia de management trebuie sa fie compatibila cu urmatoarele baze de date:

Microsoft SQL Server

MySQL(versiunea 5.5 sau mai noi)

Cerintele minime hardware pentru server-ul de baze de date sunt:

Memory	1 GB RAM
Hard Drive	At least 10 GB of free space
Processor Speed	x86 Processor: 1.0 GHz x64 Processor: 1.4 GHz Note: A 2.0 GHz or faster processor is recommended for optimum performance.

Processor Type	x86 Processor: Pentium III-compatible processor or faster x64 Processor: AMD Opteron, AMD Athlon 64, Intel Xeon with Intel EM64T support, Intel Pentium IV with EM64T support

12.2.3. Accesul la consola de mamangement sa fie suportat de cele mai cunoscute browsere (Internet Explore, Mozila Firefox ,Google Chrome , Opera ,Safari ,Microsoft Edge)

XII.II. Caracterisiti Generale

12.3.1. Serverul de management sa permita gestionarea si adaugarea mai multor pachete de licente care nu au fost achizitionate simultan;

12.3.2. Serverul de management sa permita gestionarea licentelor care nu apartin aceluiasi client(valabil pentru integratori);

12.3.3. Solutia de management va putea afisa centralizat rezultate despre numarul de clientii existentii si restul clientilor ce pot fi gestionati cu aceeasi licenta antivirus.

12.3.4. Solutia de management, sa aiba posibilitatea de a genera un fisier de tip log detaliiat, cu serviciile ce ruleaza pe respectiva statie, pentru identificarea si detalierea fiecarui servicu respectiv fisier cat si filtrarea in functie de gradul de risc.Sa se permita si exportul fisierului log .

12.3.5. Produsul de securitate si solutia de management vor avea acelasi producator.

12.3.6. Solutia de management va permite administrarea, tuturor versiunilor antivirus ale producatorului solutiei de management, atat actuale cat si versiunile mai vechi.

12.3.7. Consola de management va avea o structura modulara si usor de folosit, dar va prezenta si o flexibilitate ridicata la nivel de rearanjare vizuala a categoriilor si informatiilor afisate in functie de cerintele administratorului.

12.3.8. Administratrea solutiei antivirus, sa poate permite optional accesul la informatiile despre clientii antivirus din retea, prin interfata WEB de la orice calculator din retea, fara a fi necesara instalarea unei console de aministrare si o conexiune la internet.

12.3.9. In cazul utilizarii, raporartelor prin interfata WEB, utilizatorul sa poata defini categoriile rapoartelor afisate, dar si modul de vizualizare a acestora.

12.3.10. Administratorul sa aibe posibilitatea de a particulariza pachete de instalare care sa contina agent pentru comunicatia ANTIVIRUS > SERVER , certificatul (daca comunicatia ANTIVIRUS > SERVER este securizata), licenta si politica asociata sau configuratia.

12.3.11. Produsul trebuie sa fie lansat in versiune comerciala si sa se prezinte link public din site-ul producatorului

XII.III. Accesare si monitorizare (Dashboard)

12.4.1. Accesarea serverului de management sa fie facuta cu ajutorul unui browser;

12.4.2. Comunicatia cu serverul de management sa fie securizata pe baza unui certificat (HTTPS);

12.4.3. Pentru a sporii securitatea retelei,accesarea serverului de management prin consola web sa poata fi suplinita de un modul integrat de 2-factor authentication (2FA);

12.4.4. Solutia de securitate sa folosesca un agent pentru a putea transmite informatii catre serverul de management;

12.4.5. La instalarea clientilor antivirus solutia de management va avea optiunea de a identifica in reteaua locala calculatoarele neprotejate;

12.4.6. Solutia de management va permite, instalarea si gestionarea tuturor variantelor antivirus de statie ale producatorului respectiv;

12.4.7. Din interfata pricipala (Dashboard) sa poata fi vizualizate statistic eventimente despre incarcarea serverului de management (CPU/ Memorie/ Retea);

12.4.8. Din interfata pricipala (Dashboard) sa poata fi vizualizate statistic eventimente despre protectia antivirus legate de ultimile amenintari,ultima scanare,utilizatorii cu cele mai multe evenimente malware;

12.4.9. Din interfata pricipala (Dashboard) sa poata fi vizualizate toate versiunile antivirusului instalate in reteaua locala de la acelasi producator.

12.4.10. Din interfata principala (Dashboard) sa poata fi vizualizate statistic evenimentele despre proctecita firewall legate de ultimile evenimente, loguri cu privire la tentativele de acces din extern pe clientii protejati.

XII.IV. **Gestionare**

12.5.1. Prin solutia de management administratorul retelei va putea, demara urmatoarele actiuni:

- Scanare la cerere
- Configurare
- Actualizare
- Actualizarea componentelor
- Activarea produsului
- Actualizarea sistemelor de operare Windows, Linux, MAC
- Executarea unei comenzi "command"
- Trimiterea unui mesaj catre un client
- Posibilitaea de a permite instalarea agentului prin GPO, SCCM.

12.5.2. In vederea crearii politicilior diferentiate la nivel de departamente, solutia de management va permite crearea de grupuri in cadrul carora se vor aplica politici dedicate respectivului departament / grup.

12.5.3. Solutia de management va permite administratorului de retea sa monitorizeze activitatea clientului antivirus, la nivel de module ale solutiei de securitate respectiv module activate/dezactivate.

12.5.4. Administratorul de retea, va putea prin intermediul solutiei de management , se colecteze la cerere de pe orice statie din retea un fisier de tip log detaliiat, cu serviciile ce ruleaza pe respectiva statie, pentru identificarea si detalierea fiecarui servicu respectiv fisier cat si filtrarea in functie de gradul de risc.De asemenea, sa se permita si exportul fisierului log.

12.5.5. Administratorul solutiei, va putea prin intermediul solutiei de management sa revina la o baza de semnaturi anterioara, pe orice client antivius din consola de administrare.

12.5.6. Solutia de management va permite gestionarea logurilor primite si efectuarea diferitelor actiuni in functie de datele afisate.

12.5.7. Solutia va avea un modul dedicat ce va monitoriza evenimentele fiecarui client antivirus (log separat de log-ul amenintarilor).

12.5.8. Solutia va un modul dedicat logurilor de scanare la cerere, pentru clientii antivirus.La acest modul, se vor afisa detaliile scanarii pentru oricare dintre clientii antivirus.

12.5.9. Solutia va avea un modul dedicat de vizualizare, a tuturor actiunilor intreprinse de administratorul de retea.

XII.V. **Raportare**

12.6.1. Solutia va avea un modul dedicat raportarii activitatilor din retea.Aceste rapoarte se vor putea personaliza sau se pot folosi rapoarte predefinite (deja existente).

12.6.2. Solutia va oferii rapoarte pentru suita antivirus dupa cum urmeaza: Active Threats, Active threats by IPv4 and IPv6 subnet, Daily summary of threat events in last 30 days, Mobile device last scan, Top active threats, Top computer with active threats, Top users with threat events in last 7 days, Email Server reports, Firewall threats.

12.6.3. Solutia de management va oferi rapoarte din ultimile 6 ore despre serverele de email dupa cum urmeaza:Top spam domains, Top Spam recipients, Top spam senders;

12.6.4. Solutia va oferii rapoarte pentru evenimentele firewall din ultimile 7 zile dupa cum urmeaza:Top computer with firewall events, Top threat blocked, Top users with firewall events;

12.6.5. Raportarea disponibila in solutia de management va putea fi interogata in functie de ora,zi,saptamana, luna si an.De asemenea se vor putea selecta orice perioade intermediare independent de raportarea predefinita.

12.6.6. Solutia va permite planificarea unui program de raportare personalizat sau predefinit ce va putea fi trimis, pe e-mail catre administratorul retelei.

12.6.7. Solutia va permite crearea unor modele de rapoarte ce pot fi salvate si utilizate in mod curent totodata va afisa si un istoric al acestora (modele rapoarte deja create de administratorul solutiei)

12.6.8. Solutia va permite crearea unor raporte de preformata pentru sistemul / serverul pe care a fost instalata, pentru a putea oferi administratorului posibilitatea de a interveni proactiv daca sunt probleme hardware / software.

12.6.9. Solutia va permite exportarea rapoartelor in format **PDF, PS,CSV** atat local cat si transmisibile pe email, totul fiind gestionat la nivel de consola web.

12.6.10. Solutia de management sa ofere suport pentru IBM qRadar, log-urile pot fi exportate in mod nativ in format LEEF recunoscut de IBM qRadar SIEM

XII.VI. **Carantina**

12.7.1. Solutia de management va permite restaurarea fisierelor de carantina in locatia originala

12.7.2. Solutia de management va permite stergerea fisierelor din carantina

12.7.3. Solutia de management va permite incarcarea unui fisier din carantina intr-o locatie definita de administrator

XII.VII. Utilizatori si permisiuni

12.8.1. Administrarea se va face pe baza de roluri

12.8.2. Rolurile sa fie predefinite sau sa existe posibilitatea creari acestora de catre administratorul solutiei de securitate

12.8.3. Utilizatorii sa poata fi importati din active directory, CSV sau sa poata fi definiti local

12.8.4. Sa poate fi configurate detaliat drepturile unui utilizator permitand selectarea actiunilor pentru care un utilizator poate face modificari

12.8.5. Sa se poata defini un interval pentru deconectarea automata a unui utilizator de la consola de management pentru a sporii protectia datelor afisate

Întocmit:

Tămaș Daniel

Specialist IT șef - Tribunalul Cluj