SPITALUL CLINIC JUDEȚEAN DE URGENȚĂ „PIUS BRÎNZEU" TIMIȘOARA

• Bulevardul Liviu Rebreanu, Nr. 156Timișoara, jud. Timis, Cod Postal 300723
• Cod fiscal 4663448 • Telefon +4 0356 433111 • Fax +4 0256 486936
• e-mail: judetean@hosptm.ro • www.hosptm.ro

Sursa de Finantare Venituri Proprii
Nr 9282 13 .02.2023

INVITAȚIE DE PARTICIPARE

1. Autoritate contractantă: **Spital Clinic Județean de Urgență "Pius Brînzeu" Timișoara, Bv. Liviu Rebreanu, nr.156, Cod fiscal 4663448,Tel. 0356/433.127 Fax. 0356/433.114**

2. Tipul si durata contractului pentru care este solicitată ofertă: **Contract de furnizare , valabilitate pana la data de 31.12.2023.**

3. Procedura aplicată pentru atribuirea contractului de furnizare produse: **Achizitie directe**

4. Locul de executie : **Spital Clinic Județean de Urgență "Pius Brînzeu" Timișoara**

4.Natura achiziției, codul CPV, valoarea estimată a contractului:

Licenta Antivirus Bitdefender GravityZone Business Security Enterprise (950 Licenta Antivirus Bitdefender GravityZone Business Security Enterprise)

cod CPV 48760000-3

Valoare estimată, exclusiv TVA: 80,750,00 lei exclusiv TVA

5. Oferta va conține:

Ofertanții,tertii susținatori și subcontractanții nu trebuie să se regăsească în situațiile prevăzute la art 164,165,167 din legea nr 98/2016.Modalitatea prin care poate fi demonstrate indeplinirea cerinței .

Se va complecta o declarație pe propria raspundere de către operatorii economici participanți la procedura de atribuire cu informaiile aferente situației lor

Propunerea tehnică va respecta cerințele caietului de sarcini. Nr 5343.27.01.2023

- **Propunerea financiară (va fi exprimată în lei, fără TVA, cu două zecimale)**

6. Durata de realizare a contractului 15..**02.2023- 31.12.2023.**

7. Se interzice depunerea de oferte alternative.

8. Termenul limită de primire a ofertelor:. **15.02.2023 , ora 08^{00},**

9. Limba în care trebuie redactate oferetele: **romană**

10. Data, ora, locul deschiderii ofertelor **15.02. 2023, ora 08^{00}, ofertele se depun pe adresa de e-mail florin.ambru@hosptm.ro , urmand ca oferta castigatoare va urcara oferta in catalogul electronic de achiziții publice SICAP.**

Sursa de Finantare Venituri Proprii

In cazul in care se constată două sau mai multe oferte clasate pe primul loc cu același preț, la solicitarea comisiei de evaluare se va depune o noua ofertă online la o dată stabilită de catre comisie. Prețurile noi ofertate nu pot depași valoarea ofertată anterior.

Pentru ofertanții care nu vor prezenta o nouă ofertă de preț respectiv, nu vor transmite oferta finală până la datele stabilite de către comisia de evaluare se va lua in considerare valoarea din oferta anterioară, respectiv oferta inițiala. Procesul de reofertare se va desfasura intr-o singură etapă.

11. Modalități principale de finanțare și de plată și/sau referirile la prevederile care le reglementează: **Sursa de Finantare Venituri Proprii**

12. Termenul de plată al facturilor este de 30 de zile de la data primirii facturii de către Achizitor.

13. Perioada pentru care ofertantul trebuie să își mențină oferta valabilă: **90 de zile de la data de deschidere a ofertelor.**

14. Alăturat vă transmitem:

- **Caietul de sarcini nr 5343.27.01.2023**

Prof. Univ. Dr. Sande

Manager

Șef Bi

Ing Petr

Șef Biro

Vasile Ma

Întocmit Referent,
Ec Florin Ambru

SPECIFICAȚII TEHNICE – PROGRAM ANTIVIRUS

CARACTERISTICI GENERALE ALE PRODUSULUI

Produsul reprezinta o platforma integrata pentru managementul securitatii, gandita ca o solutie modulara. Produsul contine urmatoarele module:

A. O consola de management care asigura functionalitati de administrare.
B. Protectie antimalware pentru statii fizice/virtuale, laptop-uri si servere
C. Protectie si securitate pentru serverele email Microsoft Exchange

A. CONSOLA DE MANAGEMENT

1. Instalare si configurare:

1. Masinile de scanare (pentru tipul de scanare centralizata) pentru mediile virtuale se descarca din interfata web a produsului.

2. Cerinte generale:

1. Interfata consolei de management va fi in limba romana.
2. Interfata clientului de securitate, care se instaleaza pe statii si servere, va fi in limba romana.
3. Manualul de instalare a produsului va fi in limba romana.
4. Manualul de administrare a produsului va fi in limba romana.
5. Solutia va pemite activarea/dezactivarea actualizarilor de produs/semnaturi.
6. Actualizari automate a consolei de management facute de catre producatorul solutiei, fara interventia utilizatorului.
7. Notificarile – prezente in interfata, notificarile necitite sunt evidentiate, trimise catre una sau mai multe adrese de email, alerteaza administratorul in cazul unor probleme majore: licentiere, detectie virusi, actualizari de produs disponibile).
8. Consola de management este accesibila de oriunde in lume (solutie de tip Cloud), fara a fi nevoie de setari suplimentare din partea utilizatorului.
9. Consola de management este accesibila atat de pe statii de lucru cat si de pe dispozitive mobile (smartphone, tableta).

3. Panou de monitorizare si raportare (Dashboard):

1. Rapoartele din panoul de monitorizare vor putea fi configurate specificand numele raportului, tipul raportului, tinta raportului, optiuni specifice pentru orice tip de raport (de exemplu pentru raportul de actualizare - care este intervalul dupa care o statie este considerata neactualizata).
2. Panoul central contine rapoarte pentru toate modulele suportate.
3. Rapoartele din panoul central de comanda permit: adaugarea altor rapoarte, stergerea lor si rearanjarea.

4. Inventarierea retelei – managementul securitatii:

1. Solutia se va integra cu domeniul Active Directory si va putea importa inventarul.

2. Se permite descoperirea statiilor fizice neintegrate in Active Directory (Workgroup) cu ajutorul Network discovery.
3. Solutia va oferi optiuni de cautare, sortare si filtrare dupa numele sistemului, sistem de operare, adresa IP, politica aplicata, ultima data cand s-a conectat (online si/sau offline) si FQDN.
4. Solutia va permite crearea unui pachet unic pentru toate sistemele de operare, de statii sau servere. Astfel, administratorul va putea descarca pachetele pentru protectia statiilor si serverelor pe care ruleaza sistemul de operare Windows, Linux, Mac.
5. Solutia va permite instalarea la distanta sau manual a clientilor antimalware pe masini fizice/virtuale.
6. Solutia va permite selectarea modulelor componente atunci cand se creaza pachetul clientului care se instalează pe mașinile fizice/virtuale.
7. Solutia va permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanta pentru clientul antimalware.
8. Solutia va oferi posibilitatea de repornire a masinilor fizice de la distanta.
9. Solutia va oferi informatii detaliate despre fiecare task si se fiseaza daca task-ul s-a finalizat sau nu cu succes.
10. Solutia va permite configurarea centralizata a clientilor antimalware prin intermediul politicilor
11. Se vor oferi in consola de management informatii detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuita, Ultimele actualizare, Versiunea produsului, Versiunea de semnaturi.

5. Politici:

1. Solutia va permite configurarea setarilor clientului antimalware prin intermediul unei singure politici ce contine setari pentru toate module
2. Politica va contine optiuni specifice de activare/dezactivare si configurarea functionalitatilor precum scanarea antimalware la cerere, firewall, controlul accesului la Internet, controlul aplicatiilor, scanarea traficului web,controlul dispozitivelor, power user.
3. Solutia permite aplicarea politicilor pe masini client, grupuri de masini, domeniu, unitati organizationale.
4. Politica sa poate fi schimbata automat in functie de:
   a. IP sau clasa de IP al statiei
   b. Gateway-ul alocat
   c. DNS serverul alocat
   d. WINS serverul alocat
   e. Sufix DNS pentru conexiunea dhcp
   f. Clientul este/nu este in aceasi retea cu infrastructura de management (statia de lucru poate solutiona implicit numele gazdei)
   g. Tipul retelei (lan, wireless)

6. Rapoarte:

1. Solutia va contine rapoarte care prezinta statusul masinilor clientilor din punct de vedere al actualizarilor, fisierelor malware detectate, aplicatiile blocate, site-urilor web blocate.

2. Rapoartele programate pot fi trimise catre un numar nelimitat de adrese de email (nu este nevoie sa aiba un cont in consola de management).
3. Solutia va permite vizualizarea rapoartelor curente programate de administrator.
4. Solutia va permite exportarea rapoartelor in format .pdf si detaliile ca format .csv. sau arhiva.
5. Solutia include un generator de rapoarte care ofera posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, mentinand informatiile concise si ordonate corespunzator. Astfel, solutia include interogari precum: starea terminalului, evenimente terminal, evenimente Exchange.
6. Interogarea legata de starea terminalului include informatii precum:
    a. tip masina
    b. infrastructura retelei careia ii apartine terminalul
    c. datele agentului de securitate
    d. starea modulelor de protectie
    e. rolurile terminalelor.
7. Interogarea legata de evenimente terminal include informatii precum:
    a. calculatorul tinta pe care a avut loc evenimentul
    b. tipul starea si configuratia agentului de securitate instalat
    c. starea modulelor si rolurilor de protectie instalate pe agentul de securitate
    d. denunmirea si alocarea politicii
    e. utilizatorul autentificat in timpul evenimentului
    f. evenimente (site-uri blocate, aplicatii blocate, detectiile etc)
8. Interogarea legata de evenimente Exchange include informatii precum:
    a. Directia traficului e-mail
    b. Evenimente de securitate (detectarea programelor de tip malware sau a fisierelor atasate)
    c. Masurile implementate in fiecare situatie (curatarea, stergerea, inlocuirea sau carantinarea fisierului, stergerea sau respingerea e-mail-ului)

7. Carantina:

1. Solutia va permite restaurarea fisierelor carantinate in locatia originala sau intr-o cale configurabila.
2. Carantina va fi locala, pe fiecare statie administrata si va fi administrata, fie local, fie din consola de management.

8. Utilizatori:

1. Administrarea se va putea face pe baza de roluri.
2. Roluri multiple predefinite: Administrator companie, Administrator retea, Reporter sau rol personalizat.
    a. Administrator companie: administreaza arhitectura consolei de management;
    b. Administrator retea: administreaza serviciile de securitate;
    c. Reporter: monitorizeaza si genereaza rapoarte.

3. Utilizatorii pot fi importati din Microsoft Active Directory sau creati in consola de management.
4. Se va permite configurarea detaliata a drepturilor administrative, permitand selectarea serviciilor si obiectelor pentru care un utilizator poate face modificari.
5. Se va permite deconectarea automata a oricarui tip de utilizator dupa un anumit timp pentru o protectie sporita a datelor afisate in consola de administrare. Acest interval se poate personaliza de administratorul solutiei.

9. Log-uri:

1. Inregistrarea actiunilor utilizatorilor.
2. Se vor oferi informatii detaliate pentru fiecare actiune a unui utilizator.
3. Se va permite filtrarea actiunilor utilizator dupa numele utilizatorului, actiune.

10. Actualizare:

1. Se permite definirea de locatii de actualizare multiple.
2. Se permite activarea/dezactivarea actualizarilor de produs si semnaturi.
3. Orice client antivirus sa poata fi configurat sa livreze update-urile catre alt client antivirus
4. Solutia permite testarea noilor versiuni de pachete de instalare ale clientului antimalware, inainte de a fi instalate pe toate statiile si serverele din retea, evitand posibile probleme ce pot afecta serverele sau statiile critice. Astfel, serverul de actualizare include 2 tipuri de actualizari de produs:
   a. Ciclu rapid, gandit pentru un mediu de test in cadrul retelei
   b. Ciclu lent, gandit pentru restul retelei (productie, servere critice etc)
5. Solutia permite stabilirea zonelor de test si critice din cadrul retelei prin intermediul politicilor din consola de management.

B. PROTECTIE STATII SI SERVERE FIZICE/VIRTUALE

1. Caracteristici generale minimale si eliminatorii:

1. Pentru reducerea la minim a consumului de resurse, solutia antimalware trebuie sa permita instalarea personalizata a modulelor detinute (de exemplu, sa permita instalarea solutiei antimalware fara modulul de control al accesului web, modul de control al dispozitivilelor sau modulul firewall).
2. Pentru o mai buna protectie a statiilor si serverelor, solutia include un vaccin anti-ransomware. Acest vaccin asigura protectia impotriva tuturor amenintarilor cunoscute de tip ransomware, prin imunizarea statiilor si serverelor, chiar daca sunt infectate si prin blocarea procesului de criptare.
3. Vaccinul anti-ransomware primeste actualizari de la producator, odata cu actualizarea semnaturilor produsului Antimalware.
4. Pentru o mai buna protectie a statiilor si serverelor, solutia include protectie impotriva atacurilor zero-day de tip exploit avansate (atacuri directionate) bazata pe tehnologii de invatare automata (machine learning).
5. Pentru o mai buna protectie a a statiilor si serverelor, solutia include un modul integrat de tip ERA (Endpoint Risk Analytics – Analiza de risc a endpoint-ului) capabil sa identifice si remedieze in mod automatizat sau manual un numar

mare de riscuri existente la nivel de retea sau sistem de operare ce pot afecta functionalitatea si nivelul de securizare al endpoint-ului

6. Pentru o mai buna protectie a statiilor si serverelor, solutia include un modul avansat de securitate – HyperDetect, bazat pe tehnologii de tip „machine learning tunabil" proiectat special pentru a detecta atacuri avansate si activitati suspecte in faza pre-executie.
7. Acest modul avansat de securitate va proteja impotriva: atacurilor directionate (Targeted Attack - APT), fisierelor suspecte si traficului la nivel de retea suspect, exploit-urilor, ransomware si grayware. Fiecarui tip de amenintare mentionat, i se vor putea stabili, independent, un nivel de protectie dorit: permisiv, normal, agresiv.
8. Modulul avansat de securitate are posibilitatea de a raporta, bloca accesul, dezinfecta, sterge sau muta in carantina pentru fiecare din categoriile descrise. Astfel, administratorul va putea decide daca doreste intai monitorizare sau doreste si blocarea amenintarilor. Aceste actiuni mentionate, vor putea fi stabilite independent, pentru fisiere sau pentru traficul din retea, cu posibilitatea extinderii nivelului de raportare pentru a include nivelurile superioare (vor putea fi raportate amenintarile care ar fi fost detectate daca nivelul de protectie era stabilit mai agresiv).
9. Pentru a oferi un nivel aditional de protectie a statiilor si serverelor, solutia include un sandbox in cloud-ul public al producatorului acesteia.
10. Modulul de Sandbox va putea trimite automat fisiere in Sandbox-ul din cloud-ul producatorului unde vor putea fi „detonate" pentru o analiza in profunzime.
11. Modulul de Sandbox include doua variante de analiza: doar monitorizare sau blocare. In modul monitorizare utilizatorul va putea accesa fisierul dorit, pe cand in modul blocare, utilizatorului i se va bloca rularea fisierului pana cand Sandbox-ul din cloud-ul producatorului va da verdictul.
12. Modulul de Sandbox include doua tipuri de actiuni remediere: implicita si de siguranta. Pentru actiunea implicita se va putea stabili: doar raportare, dezinfectie, stergere si carantinare. Pentru actiunea de siguranta se va putea stabili: stergere sau carantinare.
13. Modulul de Sandbox include si posibilitatea de trimitere manuala a fisierelor in Sandbox-ul din cloud-ul producatorului. Astfel, daca administratorul suspecteaza un fisier ca fiind malitios, il poate trimite manual in Sandbox pentru a fi „detonat" si a afla verdictul. Va putea trimite mai multe fisiere de odata, cu posibilitate de a specifica daca vor fi „detonate" individual sau toate in acelasi timp.
14. Modulul de Sandbox poate suporta „detonarea" urmatoarelor tipuri de fisiere: Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (executable), PDF, PEF (executable), PIF (executable), RTF, SCR, URL (binary), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.
15. Fisierele mentionate anterior, vor putea fi detectate corect chiar daca sunt incluse in arhive de tipul: : 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ.

16. Modul de detectare, corelare si raspuns la evenimente de tip EDR („endpoint detection and response") capabil sa identifice amenintari avansate sau atacuri in curs de desasurare.
17. Acest modul cuprinde colectare de date si evenimente despre hardware si software aferent fiecarei statii de lucru aducand informatii detaliate referitoare la incidentele detectate, o harta detaliata a acestora precum si actiuni de remediere automate si integrare cu modulele de Sandbox si modulul avansat de securitate - – HyperDetect. Din punct de vedere functional modulul EDR cuprinde 2 componente distincte: senzorul ce colecteaza si proceseaza datele respectiv partea de analiza de securitate care are ca obiect interpretarea acestora.
18. Modulul EDR are capacitatea de a evalua activitatea tipica a unui endpoint din perspectiva securitatii acestuia conform tehnicilor de atac MITRE („baselining") si poate raporta orice deviatie de la acest comportament sub forma unui incident
19. Modulul EDR permite filtrarea incidentelor din interfata grafica in functie intervalul de timp, pe baza unui scor de incredere („confidence score"), indicatori de atac, tehnici de atac (ATT&CK) respectiv sistem de operare afectat cat si dupa IP, nume fisier, nume static.
20. Modulul permite vizualizarea detaliata a incidentelor incluzand detalii specifice fiecarui nod afectat dupa cum urmeaza: tabul „rezumat" genereaza o harta de principiu a incidentului, tabul „timeline" detaliaza incidentul in functie de amprenta de timp a fiecarei actiuni aferente incidentului, respectiv butonul „actioneaza" care poate genera un set de masuri specifice fiecarui element din harta incidentului (kill, carantina – la nivel de nod, investigati - virus total, sandbox, google – la nivel de fisier, adaugare in lista de blocare – la nivel de retea sau instalare patch – la nivel de nod).
21. Modulul poate bloca fisiere si/sau procese folosind valori hash de tip MD5/SHA256 direct din pagina aferenta incidentului sau importate folosind un fisier CSV.
22. Modulul poate excepta fisiere non-malitioase de la actiunea de investigare sau poate genera/adauga un set de fisiere malitioase intr-o lista neagra pentru a preveni miscarea laterala a fisierelor/proceselor malitioase.
23. Modulul permite deschiderea unei conexiuni remote catre un endpoint potential infectat pentru a permite o investigare rapida a gazdei, colecta date despre atac respectiv remedia in timp real brese de securitate eliminand astfel posibile incertitudini privitoare la comportamentul potential malitios al unor fisiere/procese, reducand timpul de remediere (downtime) in cazul in care un atac a avut succes si statia tinta trebuie reconfigurata/reinstalata, permite executarea unor comenzi in linia de comanda care se executa cu privilegii de kernel ce permit eliminarea in timp real a unor amenintari sau colectarea de date privitoare la atacul in desfasurare.
24. Pentru o mai buna protectie, produsul va permite vizualizarea incidentelor extinse din cadrul tehnologiei XDR (Extended Incidents), care se vor crea prin corelarea evenimentelor de pe mai multe statii din reteaua clientului.

2. Cerinte de sistem:

- Sisteme de operare pentru statii de lucru: **Windows11, Windows 10, Windows 8/8.1, Windows 7, Mac OS Monterey 12.x, macOS BIG SUR 11.x, macOS Catalina 10.15, Mac OS X Mojave (10.14), Mac OS High Sierra (10.13), Mac OS Sierra (10.12),**
- Sisteme de operare embedded: **Windows 10 IOT Enterprise, Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded Standard 7,Windows Embedded POS Ready 7 Windows Embedded POSReady 7, Windows Embedded Enterprise 7**
- Sisteme de operare pentru servere: **Windows Server 2022, Windows Server 2019, Windows Server 2019 CORE, Windows Server 2016 , Windows Server 2016 (Core), Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, , Windows Server 2008 R2,**
- Sisteme de operare Linux: Red Hat Enterprise Linux 7.x, 8.x,9.x, CentOS 7.x, 8.x, Ubuntu 16.04 sau mai recent, SUSE Linux Enterprise Server 12SP4,5, SUSE LINUX Exnterprise15 SP2,SP3, OpenSUSE LEAP 15-2-15.3., Fedora 31 sau mai recent, AWS Bottlerocket 2020.03, Amazon Linux v2, Google COS Milestones 77,81,85, Azure Mariner 2, AlmaLinux 8,9.x, Rocky Linux 8.x, Cloud Linux 7,8.x, Pardus 21, Linux Mint 20.3, Miracle 8.4.

3. Administrare si instalare remote:

1. Inainte de instalare, administratorul va putea particulariza pachetele de instalare cu modulele dorite: firewall, content control, device control, power user.
2. Instalarea se va putea face in mai multe moduri:
    a. prin descarcarea directa a pachetului pe statia pe care se va face instalarea;
    b. prin instalarea la distanta, direct din consola de management
    c. trimiterea pe email (oricate adrese) a linkului cu pachetul de instalare pentru Windows, Linux, Mac.
3. Instalarea clientilor la distanta in alte locatii decat cele in care este instalata consola de management se va face prin intermediul unui alt client antivirus existent in locatiile respective pentru a minimiza traficul in WAN.
4. In consola vor fi disponibile informatii despre fiecare statie: numele statiei, IP, sistem de operare, module instalate, politica aplicata, informatii despre actualizari etc.
5. Din consola se va putea trimite o singura politica pentru configurarea integrala a clientului de pe statii/servere.
6. Consola va include o sectiune, „Audit", unde se vor mentiona toate actiunile intreprinse fie de administratori fie de reporteri, cu informatii detaliate: logare, editare, creare, delogare, mutare etc.
7. Posibilitatea crearii unui singur pachet de instalare, utilizabil atat pentru sistemele de operare pe 32 de biti cat si pentru cele pe 64 de biti.
8. Posibilitatea creari unui singur pachet de instalare, utilizabil pentru statii (fizice si/sau virtuale), servere (fizice si/sau virtuale), exchange.

9. Posibilitatea de a crea pachetele de instalare de tip web installer sau kit full.
10. Administratorul va putea crea grupuri sau chiar subgrupuri, unde va putea muta statiile/serverele din retea pentru cele care nu sunt integrate domeniu.
11. Permite selectarea clientului care va realiza descoperirea statiilor din retea, altele decat cele integrate in domeniu.

4. Caracteristici si functionalitati principale ale modulului antimalware:

1. Solutia permite administratorului sa stabileasca actiunea luata de produsul Antimalware la detectarea unei amenintari noi. Astfel administratorul va putea alege intre urmatoarele actiuni:
   a. Actiune imiplicita pentru fisiere infectate:
      - interzice accesul
      - dezinfecteaza
      - stergere
      - muta fisierele in carantina
      - nicio actiune
   b. Actiune alternativa pentru fisierele infectate:
      - interzice accesul
      - dezinfecteaza
      - stergere
      - muta fisierele in carantina
   c. Actiune imiplicita pentru fisierele suspecte:
      - interzice accesul
      - stergere
      - muta fisierele in carantina
      - nicio actiune
   d. Actiune alternativa pentru fisierele suspecte:
      - interzice accesul
      - stergere
      - muta fisierele in carantina
2. Scanarea automata in timp real va putea fi setata sa nu scaneze arhive sau fisiere mai mari de « x » MB, marimea fisierelor putand fi definita de administratorul solutiei,
3. Definirea pana la 16 nivele de profunzime pentru scanarea in arhive.
4. Scanarea euristica comportamentala prin simularea unui calculator virtual in interiorul caruia sunt rulate aplicatii cu potential periculos protejand sistemul de virusii necunoscuti prin detectarea codurilor periculoase a caror semnatura nu a fost lansata inca.
5. Scanarea oricarui suport de stocare a informatiei (CD-uri, harduri externe, unitati partajate etc). De asemenea, se va putea anula scanarea in cazul in care sunt detectate unitati care au informatii stocate mai mult de « x » MB.
6. Scanarea automata a emailurilor la nivelul statiei de lucru pentru POP3 (incoming)/SMTP(outgoing).
7. Configurarea cailor ce urmeaza a fi scanate la cerere.
8. Clientii antimalware pentru workstation sa permita definirea unor liste de excludere de la scanarea in timp real si la cerere a anumitor directoare, discuri, fisiere, extensii sau procese.

9. Cu ajutorul unei baze de date complete cu semnaturi de spyware si a euristicii de detectie a acestui tip de programe, produsul va trebui sa ofere protectie anti-spyware.
10. Abilitatea de a detecta atacuri fără fișiere, inclusiv cele care folosesc instrumente legitime ale sistemului de operare, cum ar fi Powershell sau interpreții de script. Soluția nu va bloca global scripturile pentru a realiza acest lucru.
11. Ofera tehnologia Anti-Ransomware.
12. Posibilitatea de configura scanarile programate sa se execute cu prioritate redusa
13. Produsul antimalware poate fi configurat sa foloseasca scanarea in cloud, si partial scanarea locala. Pentru statiile ce nu au suficiente resurse hardware, scanarea se poate face cu o masina de scanare instalata in retea (scanare centralizata).
14. 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 nicio 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)
15. Pentru o protectie sporita, solutia antimalware trebuie sa aiba 3 tipuri de detectie: bazata pe semnaturi, bazata de comportamentul fisierelor si bazata pe monitorizarea proceselor.
16. Pentru o protectie sporita, solutia antimalware trebuie sa poata scana paginile HTTP.
17. Pentru o mai buna gestionare a antimalware instalat pe statii, produsul va include optiunea de setare a unei parole pentru protectia la dezinstalare.
18. Pentru siguranta utilizatorului, clientul va include un modul de antiphishing.
19. Solutia ofera protectie in timp real pe masinile cu sistem de operare Linux in conformitate cu versiunea de kernel instalata.

5. Anti-Exploit-Avansat:

1. Posibilitatea de a opri atacurile avansate de tip „zero-day" efectuate prin intermediul unor exploit-uri evazive
2. Depistarea in timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare.

3. Protejarea aplicatiilor utilizate frecvent si a celor de tip „sistem" cum ar fi browserele, aplicatiile de tip office sau reader, procesele critice aferente sistemelor de operare.

6. Firewall:

1. Posibilitatea de a configura reguli de firewall pentru aplicatii sau conectivitate.
2. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului.
3. Posibilitatea de a defini retele de incredere pentru masina destinatie.
4. Abilitatea de a detecta scanarea de porturi.
5. Posibilitatea de a seta diferite profiluri de rețea ((Home/Office, Trusted, Public, Untrusted sau Let the Windows decide)
6. Abilitatea de a crea reguli personalizate bazate pe aplicație și/sau conexiune

7. Carantina:

1. Produsul antimalware sa permita trimiterea automata a fisierelor din carantina catre laboratoarele antimalware ale producatorului.
2. Trimiterea continutului carantinei va putea fi expediat in mod automat, la un interval definit de administrator.
3. Produsul antimalware sa permita stergerea automata a fisierelor carantinate mai vechi de o anumita perioada, pentru a nu incarca inutil spatiul de stocare.
4. Posibilitatea de a restaura un fisier din carantina in locatia lui originala.
5. Modulul de carantina va permite rescanarea obiectelor dupa fiecare actualizare de semnaturi.

8. Protectia datelor:

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

9. Controlul continutului:

1. Consola va avea integrat un modul dedicat controlului accesului la Internet cu urmatoarele particularitati:
   a. Permite blocarea accesului la Internet pentru anumite masini client sau grupuri de masini.
   b. Permite blocarea accesului la Internet pe intervale orare.
   c. Permite blocarea paginilor de internet care contin anumite cuvinte cheie.
   d. Permite controlul accesului numai la anumite pagini de internet specificate de administrator;
   e. Permite blocarea accesului la anumite aplicatii definite de administrator;
   f. Permite restrictionarea accesului pe anumite pagini de internet dupa anumite categorii prestabilite (ex: online dating, violenta, pornografie etc).

10. Controlul dispozitivelor:

1. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului.
2. Modulul va permite controlul urmatoarelor 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 Raid
m. Printers
n. Network Adapters
o. Wireless Network Adapters
p. Internal and External Storage

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

11. Power User:

1. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului.
2. Modulul permite posibilitatea de a acorda utilizatorilor drepturi de Power User. Utilizatorii vor putea accesa si modifica setarile clientului antimalware dintr-o consola disponibila local pe masina client.
3. Modificarile efectuate din modulul Power User vor fi active local, pe masina pe care s-au facut respectivele modificari.
4. Administratorul va putea suprascrie din consola setarile aplicate de utilizatorii Power User.

12. Actualizare:

1. Posibilitatea efectuarii actualizarii la nivel de statie in mod silentios (fara avertizare).
2. Sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate).
3. Actualizarea pentru locatiile remote prin intermediul unui client antimalware care are si rol de server de actualizare.
4. Abilitatea de a împiedica punctele finale să iasă pe internet pentru a descărca actualizări.

C. PROTECTIE SI SECURITATE PENTRU SERVERELE EMAIL MICROSOFT EXCHANGE

Cerinte minime de sistem:

- Exchange server 2019, 2016, 2013 cu rol de Edge Transport sau Mailbox
- Exchange server 2010 cu rold de Edge Transport, Hub Transport sau Mailbox

1. Produsul va oferi protectie antimalware, antispam (inclusiv antiphishing), precum si filtrare de atasamente si continut, prin integrarea cu serverul Microsoft Exchange. De asemenea, va permite scanarea antimalware la cerere a bazelor de date Exchange.
2. Produsul va asigura scanarea atasamentelor si a continutului mesajelor in timp real, fara a afecta vizibil performanta serverului de mail.
3. Actualizarea antimalware trebuie sa poata fi facuta automat la un interval de maxim 1 ora, precum si la cerere.
4. In afara de detectia pe baza de semnaturi, modulul de protectie antimalware va trebui sa includa si scanare euristica comportamentala, prin simularea unui calculator virtual in interiorul caruia sunt rulate si analizate aplicatii cu potential periculos, pentru a proteja sistemul de virusii necunoscuti prin detectarea codurilor periculoase a caror semnatura nu a fost lansata inca.
5. Produsul va oferi optiuni multiple de actiune la identificarea unui atasament virusat (dezinfectare, stergere, mutare in carantina).
6. Cu ajutorul unei baze de date complete cu semnaturi de spyware si a euristicii de detectie a acestui tip de programe, produsul va oferi protectie anti-spyware pentru a preveni furtul de date confidentiale.
7. Produsul va oferi protectie antispam, cu o baza de semnaturi actualizabila prin internet.
8. Modulul antispam va trebui sa includa un filtru URL cu o baza de adrese URL cunoscute a fi folosite in mesaje spam, precum si un filtru de caractere pentru detectarea automata a mesajelor scrise cu caractere chirilice sau asiatice.
9. Produsul va trebui sa ofere filtru RBL care sa identifice spam-ul prin sincronizarea cu anumite baze de date online care contin liste de servere de mail cunoscute ca fiind la originea acestui tip de mesaje.
10. Produsul va trebui sa ofere un serviciu/filtru online pentru imbunatatirea protectiei impotriva valurilor de spam nou aparute.
11. Produsul va oferi posibilitatea de a defini politici de filtrare antimalware, antispam, a continutului sau atasamentelor pentru diferite grupuri sau utilizatori.
12. Actualizarea produsului va fi configurabila si se va putea realiza de pe internet, direct sau printr-un proxy, sau din cadrul retelei de pe un server de actualizare propriu.

13. Produsul va trebui sa ofere statistici atat referitoare la scanarea antivirus cat si la scanarea antispam.
14. Produsul se va integra in cadrul consolei de management unitar al solutiei antivirus. Pentru usurinta accesului la setarile produsului din diferite medii de operare, produsul va avea consola de administrare web.

Întocmit,
Ing. Lucian Boșneag

Dr.ing. Mariana Mog
Șef Serviciu Inform.