ANEXA nr.1 - Referat de necesitate nr. 9743/14.09.2023

SPECIFICATII TEHNICE

furnizare pachete software protecţie Antivirus

Se solicita o soluţie de securitate centralizata pentru asigurarea unei protecţii împotriva viruşilor, a programelor spion, a mesajelor de tip spam, a tentativelor de fraudare de tip phishing şi a altor coduri periculoase pentru statii de lucru si servere.

Solutia furnizata trebuie:

- sa contina o platforma de management centralizat pentru instalarea şi configurarea de la distanţă a tuturor componentelor pentru staţii de lucru, servere etc din interiorul reţelei, precum şi pentru generarea de rapoarte legate de acestea;
- solutia trebuie sa aiba posibilitatea integrarii cu directoarele utilizate DSP IASI si versiuni mai recente;
- sa ofere administratorilor de reţea posibilitatea identificării rapide a incidentelor legate de prezenţa unor programe periculoase;
- sa poata aplica diverse politici de securitate.

1) Cerinţe minime obligatorii pentru componenta de securitate dedicata staţiilor de lucru :

- Solutie de securitate pentru un numar de minim 100 si maxim 250 statii de lucru.
- Solutia trebuie sa includa:

- tehnologii de detectare, dezinfectare şi trimitere în carantină a viruşilor,
- programelor spion de tip adware/spyware, troienilor şi rootkit-urilor recunoscute
- posibilitatea de a programa scanări imediate sau la cererea utilizatorului pentru a evalua gradul de infectare al sistemului
- trimiterea în carantină a fişierelor suspecte sau infectate, în vederea reducerii riscului de propagare
- protecţie firewall individuală pentru utilizatorii de la distanţă şi ocazionali

  risc redus de infectare prin scanarea în timp real a traficului internet a tuturor staţiilor de lucru
- creşterea productivităţii şi a nivelului de securitate prin blocarea accesului utilizatorilor la anumite site-uri ori prin blocarea posibilităţii de a transmite emailuri conţinând date confidenţiale
- colectarea de date despre ameninţările informatice actuale de la toate staţiile de lucru şi serverele din reţea cu ajutorul interfeţei panoului de control
- management şi configurare de la distanţă, în conformitate cu politica de securitate

- configurarea, evaluarea, instalarea şi îndepărtarea aplicaţiilor la nivel de sistem
- niveluri multiple de protecţie avansată:
    - **Antivirus**
    - **Antispam**
    - **Antispyware**
    - **Antiphishing**
    - **Content Filtering**
    - **Firewall**
- Actualizări automate a bazei de date ce conţine semnături de viruşi

- Solutia trebuie sa poata scana urmatoarele tipuri minime de sisteme: - Procesor compatibil Intel® Pentium 1,6 MHz, Memorie RAM: 1 GB

- Sistem de operare, baze de date si browsere web:

- Windows 7, 8.1, 10
- Servere Windows (2003, 2008, 2012) si mai noi
- Microsoft SQL Server 2005, 2008 sau Microsoft SQL Express Edition
- Microsoft Sharepoint 2010, si mai noi

2) **Cerinte minime obligatorii pentru componenta de securitate dedicata serverelor :**

- Solutie de securitate pentru 10 servere de fisiere MS Windows Server

Soluţia trebuie sa asigure:

- detectare, trimitere în carantină şi dezinfectare a viruşilor la nivel de fişiere şi sistem
- scanarea tuturor tipurilor de fişiere, incluzând fişierele comprimate, pentru a detecta viruşi, programe de tip spyware sau rootkit-uri
- existenţa unor profiluri de scanare antivirus adaptabile, pentru un plus de flexibilitate
- trimiterea în carantină a fişierelor suspecte sau infectate, în vederea reducerii riscului de propagare
- posibilitatea de a retrimite fişierele în locaţia originală, după validarea acestora
- performanţă optimizată şi stabilizată
- declanşarea mai multor sesiuni de scanare în paralel, reducând la minim timpul de procesare şi impact asupra resurselor sistemului
- scanarea optimizată pentru fiecare sesiune reducand astfel impactul asupra resurselor prin scanarea fişierelor o singură dată, până la o accesare viitoare
- integrare în platforma de management pentru administrare centralizată staţiilor de lucru
- panou de control centralizat ce asigură diverse praguri de alertare în legătură progresul procesului de instalare

3) Furnizorul va asigura urmatoarele:

- Actualizarea bazei de semnaturi de virus si a motoarelor de scanare
- Actualizarea versiunii si generatiei de produs
- Suport tehnic prin e-mail si mesagerie scrisa, non stop 24/24 ore, 7/7 zile pe saptamana, inclusiv in weekend si zilele de sarbatoare legale in limba romana asigurat de catre producatorul solutiei.
- Distribuirea unor mesaje de atentionare de urgenta prin e-mail in cazul aparitiei unor noi virusi distructivi sau cu potential de rapandire rapida
- Pentru orice virus pe care producatorul nu il identifica si dezinfecteaza se va livra antidotul in cel mai scurt timp posibil de la trimiterea unei mostre a virusului

Furnizorul va asigura instruirea cu privire la utilizarea si configurarea solutiei si va asigura suport on-site si telefonic la configurarea si instalarea solutiei.

Data: 14.09.2023

Nume, Prenume/Semnatura

Ec. Cristea Florin Septimiu