Dyrektor
Sądu Rejonowego
w Puławach

Puławy, dnia 20 listopada 2018r.

D - 231 - 80/18

WYKONAWCY

WSZYSCY

Działając w imieniu i na rzecz Sądu Rejonowego w Puławach, uprzejmie proszę o przygotowanie i złożenie oferty cenowej na zakup oprogramowania antywirusowego, zgodnie ze specyfikacją techniczną.

Dodatkowe informacje:

1. Obecnie Sąd Rejonowy w Puławach korzysta z oprogramowania antywirusowego Bitdefender GravityZone Advanced Business Security. Zakup dotyczył będzie przedłużenia posiadanego lub zakupu nowego oprogramowania antywirusowego z przeznaczeniem na urządzenia końcowe – stacje robocze i serwery, opcjonalnie z konsolą zarządzającą – w ilości 21 szt. (17 szt. na stacje + 1 szt. na serwer fizyczny + 3 szt. na serwery wirtualne) na okres 12 miesięcy.

Licencja dotycząca wyżej wymienionego programu antywirusowy wygasa z dniem 27.12.2018r.; oprogramowanie jest niezbędne do ochrony komputerów użytkowanych w V Wydziale Ksiąg Wieczystych.

Oferta musi zawierać w szczególności:

- ceny jednostkowe i wartości netto i brutto;

- nazwę i wersję zaproponowanego produktu;

- imię i nazwisko, telefon, adres e – mail do osoby uprawnionej do kontaktu w sprawie niniejszego zapytania.

Ofertę proszę przygotować do dnia 28 listopada 2018r. do godz. 12,00. Ofertę można złożyć osobiście, przesłać faksem, pocztą lub pocztą elektroniczna na podane niżej adresy;

Zamawiający zastrzega sobie możliwość unieważnienie postępowania w każdym momencie bez podania przyczyny.

Osobami uprawnionymi do kontaktu w sprawie niniejszej są:

- Jacek Mogielnicki oraz Arkadiusz Illek: e - mail: jacek.mogielnicki@pulawy.sr.gov.pl, arkadiusz.illek@pulawy.sr.gov.pl

Sąd Rejonowy w Puławach, ul. Lubelska 7 pok. 114, 24 - 100 Puławy, tel./fax 81 88 67 555

IW/jm

DYREKTOR
Sądu Rejonowego w Puławach

Specyfikacja techniczna

Zamawiający wymaga dostarczenia programu antywirusowego lub innego równoważnego oprogramowania spełniającego kryteria poniższej specyfikacji:

1) Usuwanie wirusów, makro – wirusów, robaków internetowych oraz koni trojańskich (oraz wirusów i robaków z plików skompresowanych oraz samorozpakowujących się) lub kasowanie zainfekowanych plików; ochrona przed oprogramowaniem typu „spyware" i „adware", włącznie z usuwaniem zmian wprowadzonych do systemu przez to oprogramowanie tego typu,
2) Wykrywanie wirusów, makro-wirusów, robaków internetowych, koni trojańskich, spyware, adware i dialerów ma być realizowane w pojedynczym systemie skanującym,
3) Określanie obciążenia CPU dla zadań skanowania zaplanowanego oraz skanowania na żądanie,
4) Skanowanie plików pobranych z Internetu wraz ze skryptami umieszczonymi w sieci internet oraz plików skompresowanych,
5) Zapewnienie stałej ochrony wszystkich zapisywanych, odczytywanych, a także uruchamianych plików przez mechanizm skanujący pracujący w tle wraz z metodą heurystyczną wyszukiwania wirusów (na życzenie); pliki te mogą być skanowane:
a) na dyskach twardych
b) w boot sektorach
c) na pendrive'ach
d) na płytach CD/DVD
6) Możliwość samodzielnego pobierania aktualizacji z Internetu do stacji roboczej
7) Możliwość zablokowania funkcji zmiany konfiguracji klienta lub ukrycie interfejsu użytkownika klienta,
8) Scentralizowana obsługa wirusów polegającą na przekazywaniu nieodwracalnie zainfekowanych plików do bezpiecznego miejsca w postaci centralnej kwarantanny na centralnym serwerze, w celu przeprowadzenia dalszych badań
9) Wbudowana w oprogramowanie funkcja do wysyłania podejrzanych lub zainfekowanych nowymi wirusami plików do producenta w celu uzyskania szczepionek
10) Wyszukiwanie i usuwanie wirusów w plikach skompresowanych (także zagnieżdżonych wewnątrz innych plików skompresowanych) w szczególności z plikach typu ZIP, GNU, LZH/LHA, BinHex, HTTP, ARJ, RAR, MIME/UU, TAR, kontenery CAB,UUE, Rich text format, ArcManager, MS-TNEF, 7z.
11) Aktualizacja definicji wirusów nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie – serwerze czy stacji roboczej
12) Mikrodefinicje wirusów - przyrostowe, scentralizowane aktualizowanie klientów jedynie o nowe definicje wirusów i mechanizmy skanujące
13) Możliwość cofnięcia procesu aktualizacji definicji wirusów i mechanizmów skanujących – powrót do poprzedniego zastawu definicji wirusów bez konieczności reinstalacji oprogramowania czy też restartu komputerów
14) Możliwość natychmiastowego „wypchnięcia" definicji wirusów do stacji klienckich
15) Aktualizacja bazy definicji wirusów oraz mechanizmów skanujących co najmniej 1 raz dziennie
16) Heurystyczna technologia do wykrywania nowych, nieznanych wirusów
17) Moduł analizy zachowań aplikacji do wykrywania nowych, nieznanych zagrożeń typu robak internetowy, koń trojański, keylogger.
18) Automatyczna rejestracja w dzienniku zdarzeń wszelkich nieautoryzowanych prób zmian rejestru dokonywanych przez użytkownika.
19) Automatyczne ponowne uruchomianie skanowania w czasie rzeczywistym, jeśli zostało wyłączone przez użytkownika mającego odpowiednie uprawnienia na z góry określony czas.
20) Automatyczne wymuszanie na kliencie programu pobrania zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe
22) Aktualizacje definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione

Ochrona systemu operacyjnego

- Produkt ma umożliwiać uruchamianie i blokowanie wskazanych aplikacji
- Produkt ma umożliwiać ładownie modułów lub bibliotek DLL

• Produkt ma umożliwiać kontrolę odczytywania i zapisywania na systemie plików przez wskazane aplikacje
• Aplikacje powinny być rozróżniane poprzez nazwę i sygnaturę cyfrową
• Produkt ma umożliwiać blokowanie wskazanego typu urządzeń przed dostępem użytkownika – urządzenia muszą być identyfikowane po ich numerze seryjnym
• Produkt ma kontrolować dostęp do rejestru systemowego
• Produkt ma umożliwiać logowanie plików wgrywanych na urządzenia zewnętrzne
• Polityki ochrony mają mieć możliwość pracy w dwóch trybach, testowym i produkcyjnym. W trybie testowym aplikacje i urządzenia nie są blokowane, ale jest tworzony wpis w logu.

Moduł centralnego zarządzania:
• Centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie oprogramowaniem z pojedynczej konsoli
• Centralna aktualizacja ochrony antywirusowej, zapory ogniowej i systemu wykrywania włamań przez administratora sieci,
• Produkt ma wykrywać i raportować nieautoryzowane zmiany w konfiguracji produktu na stacji roboczej. Ma istnieć możliwość blokowania takich zmian.
• Produkt powinien zapewniać zarządzanie poprzez konsolę. Dostęp do konsoli ma być możliwy po wcześniejszej weryfikacji użytkownika. Produkt ma mieć możliwość definiowania wielu kont administracyjnych i niezależną konfigurację uprawnień.
• Możliwość definiowania wielu niezależnych organizacji na jednym serwerze zarządzającym – informacje dostarczone do serwera zarządzającego nie będą dostępne pomiędzy organizacjami
• Integracja z Microsoft ActiveDirectory w celu importu użytkowników, listy maszyn, struktury jednostek organizacyjnych.
• Konta administracyjne mają być tworzone na poziomie serwerów zarządzających i na poziomie organizacji definiowanych na serwerze.
• Uprawnienia administratorów mają być ustawiane niezależnie dla każdego kontenera wewnątrz organizacji.
• Możliwość utworzenia administratorów z uprawnieniami tylko do odczytu.
• Konfiguracja agentów ma mieć strukturę drzewa, z mechanizmami dziedziczenia.
• Uwierzytelnianie administratorów ma się odbywać w oparciu o wewnętrzną bazę danych lub z użyciem Microsoft ActiveDirectory. Produkt ma mieć możliwość wykorzystania wieloelementowego uwierzytelniania (np. z wykorzystaniem tokenów, certyfikatów itp.)
• Dostęp do interfejsu produktu i listy funkcji dostępnych dla użytkownika ma być konfigurowany z poziomu centralnej konsoli zarządzającej.
• Konfiguracja aktywna na stacji ma rozróżniać lokalizację agenta i według tego kryterium określać stosowany zestaw reguł dla agenta.
• Lokalizacja ma być określana według: typu interfejsu sieciowego, numeru MAC domyślnej bramki, adresu IP, zakresu podsieci, możliwości komunikacji z wybranymi serwerami, wartości kluczy w rejestrze, serwera zarządzającego, nazwy domeny, adresów serwerów WINS, DNS, DHCP, wyniku zapytania do serwera DNS.
• Opis lokalizacji powinien zawierać możliwość tworzenia połączeń logicznych „I" oraz „LUB" na powyżej wymienionych elementach.
• Paczki instalacyjne produktu mają pozwalać na dodanie własnej konfiguracji

• Pełna funkcjonalność ma być zawarta w jednym pliku instalacyjnym
• Produkt ma zapewniać graficzne raportowanie,
• Wbudowane raporty mają pokazywać:
a) stan dystrybucji sygnatur antywirusowych oraz IDS/IPS
b) wersje zainstalowanych klientów
c) inwentaryzacje stacji roboczych
d) wykrytych wirusów, zdarzeń sieciowych, integralności komputerów
• Moduł raportowania ma pokazywać stan wykonywanych poleceń na komputerach
• Możliwość zaplanowanego tworzenia raportów i przesyłania ich do danych kont pocztowych
• Możliwość zdefiniowania alertów administracyjnych zawierających zdarzenia:
a) błędnej autoryzacji do systemu zarządzania
b) dostępności nowego oprogramowania
c) pojawienia się nowego komputera

d) zdarzeń powiązanych z infekcjami wirusów
e) stanu serwerów zarządzających
• Pełna polska wersja językowa oprogramowania dla systemu zarządzania i stacji klienckich wraz z dokumentacją.

Platforma:
• Oprogramowanie musi działać na systemach Windows 2000 Professional i Server, Windows XP 32/64-bit, Windows Vista 32/64-bit, Windows 2003 32/64-bit, Windows 2008 32/64-bit, Windows 7 32/64-bit, Windows 2008R2, Windows 2012, Windows 2012R2.
• Oprogramowanie musi posiadać wersję dedykowaną do ochrony stacji roboczych oraz serwerów, w tym serwerów plików.
• Komponenty rozwiązania takie jak: firewall, zapobieganie włamaniom i kontrola integralności komputera muszą działać na wszystkich powyższych platformach 32/64-bitowych.
• Serwer zarządzający musi działać na systemach, Windows 2008 32/64-bit, Windows 2008 R2, Windows 2012, Windows 2012R2.

Opracował:
Grzegorz Ląd
Informatyk