MIEJSKI OŚRODEK POMOCY SPOŁECZNEJ

ul. Polskiej Organizacji Wojskowej 2, 42-217 Częstochowa,
Tel.: 34 37 24 200, fax: 34 37 24 250, NIP: 573-23-02-950, REGON: 002741290,
www.mops.czestochowa.um.gov.pl. mops@czestochowa.um.gov.pl

Załącznik nr 1 do SIWZ

SZCZEGÓŁOWY WYKAZ FUNKCJONALNOŚCI PAKIETU ANTYWIRUSOWEGO

1. Stacje Windows:

1) Pełne wsparcie dla systemu Windows 2000/XP/Vista/Windows 7/ Windows 8.
2) Wsparcie dla Windows Security Center (Windows XP SP2).
3) Wsparcie dla 32- i 64-bitowej wersji systemu Windows.
4) Wersja programu dla stacji roboczych Windows dostępna zarówno języku polskim jak i angielskim.
5) Pomoc w programie (help) w języku polskim.
6) Dokumentacja do programu dostępna w języku polskim.
7) Pełna ochrona przed wirusami, trojanami, robakami, adware, spyware, dialer, phishing, narzędziami hakerskich, aplikacjami typu backdoor, itp.,
8) Wbudowana technologia do ochrony przed rootkitami.
9) Skanowanie plików spakowanych i skompresowanych.
10) Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
11) Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
12) Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
13) Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
14) Możliwość skanowania dysków sieciowych i dysków przenośnych.
15) Możliwość definiowania listy rozszerzeń plików, które mają być skanowane wraz z definiowaniem wyłączeń określonych typów plików lub katalogów.
16) Brak konieczności ponownego uruchomienia komputera (restartu) po instalacji programu.
17) Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
18) Pełna integracja skanera z programami MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird i Windows Live Mail.
19) Skanowanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird i Windows Live Mail
20) Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
21) Skanowanie ruchu HTTP na poziomie stacji roboczych z możliwością definiowania

powiadomień dla użytkownika w przypadku zagrożenia.
22) Blokowanie możliwości przeglądania wybranych stron internetowych. Na podstawie nazwy strony lub wybranej frazy występującej w nazwie strony.
23) Automatyczna integracja z dowolną przeglądarką internetową.
24) Skanowanie w oparciu o heurystyczne metody wykrywania zagrożeń.
25) Aktualizacje modułów analizy heurystycznej.
26) Powiadomienia dla użytkownika i/lub administratora poprzez e-mail w przypadku wykrycia zagrożenia.
27) Skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS i POP3S.
28) Transparentne skanowanie HTTPS bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
29) Możliwość zabezpieczenia konfiguracji oraz deinstalacji oprogramowania przy pomocy hasła.
30) Pełna zgodność z technologią CISCO NAC.
31) Kontrola zainstalowanych aktualizacji systemu operacyjnego wraz z powiadomieniami dla użytkownika w przypadku braku aktualizacji wraz z rozróżnieniem na aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie.
32) Możliwość przygotowania płyty CD, DVD lub pamięci USB z pełną aktualizacja baz sygnatur, umożliwiającej uruchomienie komputera w przypadku infekcji i przeskanowania dysku w poszukiwaniu wirusów wraz
33) Blokowanie zewnętrznych nośników danych na stacji z możliwością definiowania wyjątków.
34) Autoochrona aplikacji umożliwiająca monitorowanie i blokowanie plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
35) Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
36) Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej (program antywirusowy z wbudowanym serwerem HTTP).
37) Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
38) Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja).
39) Aktualizacja z sieci lokalnej lub bezpośrednio z Internetu.
40) Jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
41) Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania.

2) Konsola administracyjna

1) Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych Windows.
2) Zdalna instalacja wszystkich wersji programów na stacjach roboczych Windows 2000/XP Professional/ Vista/Windows7/Windows 8.
3) Do instalacji zdalnej i zarządzania zdalnego nie jest wymagany dodatkowy agent.
4) Komunikacja miedzy serwerem a klientami może być zabezpieczona hasłem.
5) Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową zainstalowanymi na stacjach roboczych w sieci korporacyjnej z jednego serwera zarządzającego

6) Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych z opcją wygenerowania raportu ze skanowania i przesłania do konsoli zarządzającej.
7) Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie i skanerów rezydentnych).
8) Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, adresów MAC, wersji systemu operacyjnego oraz domeny, do której dana stacja robocza należy.
9) Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.
10) Możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych.
11) Możliwość tworzenia grup stacji roboczych i definiowania w ramach grupy wspólnych ustawień konfiguracyjnymi dla zarządzanych programów.
12) Możliwość zmiany konfiguracji na stacjach z centralnej konsoli zarządzającej lub lokalnie (lokalnie tylko jeżeli ustawienia programu nie są zabezpieczone hasłem lub użytkownik/administrator zna hasło zabezpieczające ustawienia konfiguracyjne).
13) Serwer centralnej administracji powinien mieć własną wbudowaną bazę (nie jest wymagane zainstalowanie żadnych dodatkowych baz typu MSDE lub MS SQL)
14) Do instalacji serwera centralnej administracji nie jest wymagane zainstalowanie dodatkowych aplikacji takich jak Internet Information Service (IIS) czy Apache.
15) Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) w formacie HTML lub CSV.
16) Możliwość tworzenia hierarchicznej struktury serwerów zarządzających i replikowania informacji pomiędzy nimi w taki sposób, aby nadrzędny serwer miał wgląd w swoje stacje robocze i we wszystkie stacje robocze serwerów podrzędnych (struktura drzewiasta).
17) Serwer centralnej administracji powinien oferować funkcjonalność synchronizacji grup komputerów z drzewem Active Directory. Synchronizacja ta, powinna automatycznie umieszczać komputery należące do zadanych grup w AD do odpowiadających im grup w programie. Funkcjonalność ta nie powinna wymagać instalacji serwera centralnej administracji na komputerze pełniącym funkcję kontrolera domeny.
18) Serwer centralnej administracji powinien być wyposażony w mechanizm informowania administratora o wykryciu nieprawidłowości w funkcjonowaniu oprogramowania zainstalowanego na klientach w tym przynajmniej informowaniu o: wygaśnięciu licencji na oprogramowanie, oraz o tym że zdefiniowany procent z pośród wszystkich stacji podłączonych do serwera ma nieaktywną ochronę.
19) Serwer centralnej administracji powinien być wyposażony w mechanizm zarządzania licencjami.