Regionalne Centrum
Krwiodawstwa i Krwiolecznictwa
w Zielonej Górze

Zielona Góra, 9-01-2017 r.

Dotyczy: dostawy urządzeń komputerowych i oprogramowania.

Zamawiający informuje o zmianie wymagań w zadaniu 2 pozycja 1 **Program antywirusowy dla 90 użytkowników + konsola administracyjna** na następujące:

Zadanie 2

1. Program antywirusowy dla 90 użytkowników + konsola administracyjna

Ochrona antywirusowa dla systemów z rodziny Microsoft Windows od wersji XP SP3 wzwyż systemów 32 i 64 bit., wzwyż od Microsoft Windows Server w wersji 2003 systemów 32 i 64 bit. Przyrostowe aktualizacje baz sygnatur dla chronionych końcówek roboczych z centralnego serwera zarządzającego oraz dowolnych serwerów HTTP lub zasobów lokalnych lub mapowanych dysków wskazanych w konfiguracji systemu. Ochrona przed wirusami, spyware, adware oraz phishingiem, kontrola w czasie rzeczywistym wszystkich otwieranych, uruchamianych i zapisywanych zbiorów, plików pobieranych z Internetu oraz poczty elektronicznej. Ochrona przed rootkitami. Skaner uruchamiany na żądanie lub według harmonogramu. Analiza heurystyczna, analiza algorytmiczna, sygnatury generyczne. Rozpoznawanie zbiorów już raz sprawdzonych – skanowanie ich w przypadku, gdy zbiór został zmieniony lub została zaktualizowana baza sygnatur wirusów.

Skanowanie przychodzącej poczta elektroniczna wraz z załącznikami "w locie" i w razie potrzeby automatycznie oczyszczana. Monitorowanie w czasie rzeczywistym przeglądanych stron WWW (ruch HTTP) oraz wszystkich pobieranych z Internetu zbiorów. Współpraca z każdym typem przeglądarki internetowej oraz z dowolnym programem pocztowym obsługującym protokół POP3. Do każdej przeskanowanej wiadomości automatyczne dopisywanie informacja, że została ona sprawdzona i jest bezpieczna. Bezpieczne przechowywanie zainfekowanych zbiorów w kwarantannie, szyfrowanie niebezpiecznych programów zabezpieczające przed ich przypadkowym uruchomieniem. Definiowanie wielu profili użytkownika. Ochrona aktualnej konfiguracji programu antywirusowego hasłem, które uniemożliwi odinstalowanie programu. Możliwość aktualizowania przez Internet, z dowolne stacji roboczej lub serwera w sieci lokalnej. Możliwość zdefiniowania alternatywnego źródła aktualizacji.

Obsługa dzienników zdarzeń z informacją o wynikach skanowania, wykrytych wirusach i wrogich programach oraz o aktualizacjach systemu. Możliwość wysłania powiadomień za pośrednictwem poczty elektronicznej w przypadku zaistnienia określonych zdarzeń jak np. wykrycie wirusa czy błąd przy próbie aktualizacji baz sygnatur.

Centralna instalacja, administracja, konfiguracja oraz monitorowanie całego systemu ochrony antywirusowej stacji roboczych i serwerów. Zdalna konsola umożliwiająca skanowanie wybranych stacji roboczych lub serwerów na żądanie lub według ustalonego harmonogramu, wymuszenie aktualizacji bazy sygnatur wirusów, wyszukanie w sieci stacji roboczych i serwerów niezabezpieczonych programem. Tworzenie szczegółowych raportów i statystyk dotyczących wszelkich przypadków aktywności wirusów, aktualizacji

65-046 Zielona Góra, ul. Zyty 21 • tel. +48 68 329 83 60 • fax +48 68 329 83 99 • GSM +48 603 952 755
KRS 0000037792 • NIP 973-05-89-613 • REGON 000291931
www.rckik.zgora.pl • e-mail: dyrekcja@rckik.zgora.pl

programu antywirusowego oraz wyników skanowania. Zarządzanie hostami z wykorzystaniem Active Directory: import, synchronizacja kont komputerów, jednostek organizacyjnych, zarządzanie zadaniami, harmonogramami, politykami z uwzględnieniem grup komputerów i użytkowników, określanie dostępu do konsoli i poziomu dostępnej administracji i zarządzania, zdalnej instalacji i deinstalacji ochrony na podłączonych komputerach. Szyfrowanie komunikacji między serwerem zarządzającym a klientami (SSL). Możliwość przygotowania pakietów instalacyjnych oprogramowania. Możliwość zdalnej instalacji przygotowanych pakietów oprogramowania na pojedyncze stacje robocze i /lub grupy stacji roboczych. Konfigurowanie wszystkich modułów systemu antywirusowego zainstalowanych na stacjach klienckich. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania). Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej i/lub Internetu, w zależności od zdefiniowanych zasad bezpieczeństwa na serwerze zarządzającym. Możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych. Możliwość zmiany konfiguracji na stacjach i serwerach z centralnej konsoli zarządzającej lub lokalnie (lokalnie tylko jeżeli ustawienia programu nie są zabezpieczone hasłem lub użytkownik/administrator zna hasło zabezpieczające ustawienia konfiguracyjne). Możliwość generowania raportów.

Kontrola portów USB – blokowanie portów lub nieautoryzowanych urządzeń, powiadamianie użytkownika o wykryciu naruszenia polityki korzystania z komputerów, przekazywanie alertów o incydentach do centralnego systemu zarządzania. Moduł ma wykrywać i blokować urządzenia takie jak pendrive, kamera cyfrowa, odtwarzacze MP3, drukarki i inne oraz umożliwiać zmianę dostępu do urządzeń posiadających system plików na tryb „tylko do odczytu".

Zatwierdzam

GŁÓWNY KSIĘGOWY
Małgorzata Kesicka-Gonia