

Krasnystaw, 06.12.2012r.

Zmiana w SIWZ

Na podstawie art. 38 ust. 4a ustawy PZP Zamawiający zmienia treść SIWZ w załączniku nr 2 w przetargu nieograniczonym z dnia 04.12.2012 na „ZAKUP SPRZĘTU KOMPUTEROWEGO I OPROGRAMOWANIA” w części „Specyfikacja oprogramowania do audytu sprzętu oraz oprogramowania informatycznego”

Zamawiający wprowadza następujące zmiany w treści SIWZ:

I. Wykrywanie i wizualizacja sieci, ochrona przed awariami – zakup 70 licencji

1. Urządzeń SNMP wspierających SNMP v1/2/3.

Np: switch, routery, drukarki sieciowe, urządzenia VoIP itp.

2. Serwisów TCP/IP, HTTP, POP3, SMTP, FTP i inne.

Możliwość monitorować ich czasu odpowiedzi i procentu utraconych pakietów.

3. Serwerów pocztowych:

- Program powinien monitorować zarówno serwis odbierający, jak i wysyłający pocztę.
- Program powinien mieć możliwość monitorowania stanu systemów i wysyłania powiadomienia, w razie, gdyby przestały one odpowiadać lub wadliwie funkcjonowały (np. gdy ważne parametry znajdą się poza zakresem).
- Program powinien mieć możliwość wykonywania operacji testowych.
- Program musi posiadać możliwość wysłania powiadomienia, jeśli serwer pocztowy nie działa.

4. Monitorowania serwerów WWW i adresów URL

5. Monitoringu routerów i przełączników wg:

- Zmian statusu interfejsów sieciowych
- Ruchu sieciowego
- Podłączonych komputerów
- Generowanego ruchu przez podłączone komputery

6. Serwisów Windows:

Monitor serwisów Windows powinien alarmować w razie gdy serwis przestanie działać oraz pozwalać na jego uruchomienie/zatrzymanie/zrestartowanie.

7. Wydajności systemów Windows:

Obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.

II. Inwentaryzacja, audyt i zarządzanie infrastrukturą IT – odnowienie 50 licencji oraz zakup dodatkowych 20 licencji

W zakresie inwentaryzacji sprzętu program powinien automatycznie gromadzić informacje o sprzęcie i oprogramowaniu urządzeń w sieci oraz:

1. Prezentować szczegóły dotyczące sprzętu: model, CPU, pamięci, płyty głównej, napędów, kart, etc.
2. Audyt sprzętowy powinien obejmować: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dysku, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
3. Informować o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w firmie.
4. Zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranym komputerze: instalacji/deinstalacji aplikacji, zmian adresu IP itd.
5. Posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiegokolwiek zmiany konfiguracji sprzętowej komputera.
6. Umożliwić odczytywanie numeru seryjnego (klucze licencyjne).

Z modułem inwentaryzacji sprzętu program powinien umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie:

- a) przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,
- b) definiowania własnych typów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania powinna istnieć możliwość podawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer i skan faktury zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu i skan gwarancji, termin przeglądu (można podać datę, po której administrator otrzyma powiadomienie o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, inny dowolny plik .DOC, .XLS, skan dokumentu czy też własny komentarz; możliwość importu danych z zewnętrznego źródła (CSV),
- c) możliwości wygenerowania zestawienia wszystkich środków trwałych, w tym urządzeń i zainstalowanego na nich oprogramowania.

Inwentaryzacja oprogramowania powinna zapewnić funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:

1. Skanowanie plików wykonywalnych i multimedialnych na dyskach komputerów oraz skanowanie archiwów.
2. Zarządzanie posiadanymi licencjami; pakietami oprogramowania, licencjami dostępowymi (tzw. CAL'e) itd.
3. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili powinna istnieć możliwość wykonania aktualnych raportów audytowych.
4. Zarządzanie posiadanymi licencjami: raport zgodności licencji
5. Możliwość przypisania do programów numerów seryjnych, wartości itp.

III. Statystyki wykorzystania stacji roboczej – zakup 70 licencji

W zakresie obsługi użytkowników program powinien umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez analizę:

1. Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy).
2. Monitorowanie procesów (każdy proces ma całkowity czas działania oraz czas wykorzystania przez użytkownika)
3. Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona),
4. Informacji o edytowanych przez pracownika dokumentach.
5. Historii pracy (cykliczne zrzuty ekranowe)
6. Listy odwiedzanych stron www (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt)
7. Transferu sieciowego użytkowników (ruch sieciowy lokalny i transfer internetowy wygenerowany przez pracowników)
8. Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, zestawienia pod względem użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukował), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program będzie miał możliwość monitorowania kosztów wydruków.

Program ponadto powinien posiadać możliwość blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla danego użytkownika

z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danej strony.

IV. Ochrona danych przed wyciekiem - kontrola dostępu do pendrive'ów i innych nośników danych – zakup 70 licencji

Kolejny moduł programu powinien posiadać w sobie możliwość ochrony danych przed wyciekiem przez blokowanie portów

Blokowanie portów i nośników danych

Program, ma możliwość zarządza prawami dostępu do wszystkich portów wejścia i wyjścia (przewodowych i bezprzewodowych) oraz urządzeń fizycznych, przez które użytkownik może skopiować pliki z komputera firmowego lub uruchomić na nim program zewnętrzny.

1. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda SD itp., SATA, dyski przenośne, napędy CD/DVD, stacje dyskiety
2. Blokowanie interfejsów bezprzewodowych: WiFi, Bluetooth, IrDA
3. Blokada dotyczy tylko urządzeń do przenoszenia danych - inne urządzenia (drukarka, klawiatura itp.) można podłączyć

Zarządzanie prawami dostępu do portów

1. Definiowanie praw użytkowników/grup do odczytu i kopiowania plików
2. Autoryzowanie urządzeń firmowych: pendrive, dysków HDD, płyty CD i DVD itp. - urządzenia prywatne są blokowane
3. Całkowite zablokowanie określonych typów portów dla wybranych lub komputerów
4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci lub wybranych grup komputerów

Powyższa informacja jest dla wszystkich Wykonawców wiążąca i należy ją uwzględnić w przygotowywanej ofercie.

DYREKTOR

• Janusz Rzepka •

Dyrektor Powiatowego Urzędu Pracy
w Krasnymstawie