Kielce: DOSTAWA I INSTALACJA OPROPGRAMOWANIA ANTYWIRUSOWEGO DLA POTRZEB ŚWIĘTOKRZYSKIEGO BIURA ROZWOJU REGIONALNEGO W KIELCACH

OGŁOSZENIE O ZAMÓWIENIU - dostawy

Zamieszczanie ogłoszenia: obowiązkowe.

Ogłoszenie dotyczy: zamówienia publicznego.

SEKCJA I: ZAMAWIAJĄCY

I. 1) NAZWA I ADRES: Świętokrzyskie Biuro Rozwoju Regionalnego, ul. Targowa 18, 25-520 Kielce, woj. świętokrzyskie, tel. 041 3350502, faks 041 3350607.

Adres strony internetowej zamawiającego: www.sbrr.pl

I. 2) RODZAJ ZAMAWIAJĄCEGO: Administracja samorządowa.

SEKCJA II: PRZEDMIOT ZAMÓWIENIA

II.1) OKREŚLENIE PRZEDMIOTU ZAMÓWIENIA

II.1.1) Nazwa nadana zamówieniu przez zamawiającego: DOSTAWA I INSTALACJA OPROPGRAMOWANIA ANTYWIRUSOWEGO DLA POTRZEB ŚWIĘTOKRZYSKIEGO BIURA ROZWOJU REGIONALNEGO W KIELCACH.

II.1.2) Rodzaj zamówienia: dostawy.

II.1.3) Określenie przedmiotu oraz wielkości lub zakresu zamówienia: Wymagania dla ochrony serwerów - 8 licencji Lp. Parametry wymagane 1. Program musi działać poprawnie na serwerach pracujących pod kontrolą systemów operacyjnych Windows Server 2008 SP1 lub wyższy 32/64 bit. 2. Program musi posiadać mechanizm umożliwiający skanowanie tylko nowych i zmienionych plików. 3. Program powinien mieć możliwość zmiany poziomu użycia zasobów systemowych. 4. Podczas pracy komputera program musi automatycznie skanować wszystkie pliki: - uruchamiane lub otwierane, - kopiowane lub przenoszone, - tworzone lub modyfikowane. 5. W przypadku wykrycia wirusa program musi posiadać możliwość automatycznego: - podejmowania zalecanych działań, czyli próbowania leczenia, a jeżeli nie jest to możliwe to usunięcia obiektu, - rejestrowania w pliku raportu informacji o wykryciu wirusa, - powiadamiania administratora (oraz ewentualnie użytkownika) przy użyciu poczty elektronicznej, - utworzenia kopii zapasowej przed podjęciem próby leczenia lub usunięcia zainfekowanego pliku, - poddawania kwarantannie podejrzanych obiektów. 6. Program musi mieć możliwość zabezpieczenia hasłem dostępu do ustawień, uruchamiania/zatrzymywania ochrony i zakończenia działania programu. 7. Program musi mieć możliwość zarządzania ustawieniami z poziomu jego lokalnego interfejsu zainstalowanego na serwerze (zapisywanie, przywracanie, resetowanie ustawień). 8. Program musi mieć możliwość zarządzania oprogramowaniem z wiersza poleceń. 9. Program musi pozwalać na planowanie zadań, w tym także terminów automatycznej

modułem zarządzania, a programem zainstalowanym na serwerach powinna być szyfrowana. 11. Program powinien udostępniać interfejs lokalny. 12. Interfejs konsoli programu powinien być polskojęzyczny dla systemów operacyjnych w polskiej wersji językowej. 13. Program powinien mieć możliwość definiowania sposobu powiadamiania administratora o zdarzeniach. 2. Wymagania dla ochrony stacji roboczych - 218 licencji Lp. Parametry wymagane 1. Program musi zapewniać ochronę antywirusową na jednakowym poziomie dla stacji roboczych pracujących pod kontrolą następujących systemów operacyjnych: - Windows XP (wszystkie SP) architektura 32 bit, - Windows Vista (wszystkie SP) architektura 32/64 bit, - Windows 7 (wszystkie SP) architektura 32/64 bit. 2. Interfejs konsoli programu powinien być polskojęzyczny dla systemów operacyjnych w polskiej wersji językowej. 3. Program musi posiadać możliwość utworzenia płyty ratunkowej w oparciu o pliki instalacyjne systemu Windows, umożliwiającej przeskanowanie dysków komputera bez uruchamiania systemu operacyjnego zainstalowanego na dysku komputera. 4. Program musi umożliwiać obsługę protokołów POP3, SMTP, (także szyfrowane z wykorzystaniem SSL/TLS). 5. Program musi posiadać możliwość skanowania w czasie rzeczywistym ruchu HTTP (także ruch szyfrowany z wykorzystaniem SSL/TLS). 6. Program musi posiadać funkcję informowania użytkownika i administratora o przestarzałych definicjach szczepionek na stacjach roboczych. 7. Program musi posiadać możliwość zablokowania dostępu do ustawień programu dla użytkowników nieposiadających uprawnień administracyjnych. 8. Program musi posiadać funkcję, która uniemożliwia użytkownikowi komputera możliwości wyłączenia działania monitora antywirusowego, jeżeli nie posiada uprawnień administratora. 9. Program musi posiadać funkcję wykonania instalacji oprogramowania antywirusowego na stacjach roboczych w oparciu o konto i hasło administratora stacji roboczej. 10. Komunikacja pomiędzy serwerem zarządzającym a agentami sieciowymi na stacjach roboczych powinna być szyfrowana. 11. Program musi posiadać możliwość skanowania dowolnego zasobu podłączonego do stacji roboczej np.: dyski zewnętrzne, pamięci USB. 12. Program musi posiadać ochronę przed phishingiem. 13. Program musi posiadać moduł zapory ogniowej, która może być włączana opcjonalnie przez administratora systemu. - moduł zapory ogniowej musi posiadać możliwość ustawienia predefiniowanych poziomów ochrony, w tym poziomu zapewniającego interakcję z użytkownikiem po wykryciu nowego połączenia (tryb uczenia zapory), - moduł zapory ogniowej musi umożliwiać ręczne tworzenie i modyfikację reguł dostępu dla zainstalowanych aplikacji, - moduł zapory ogniowej musi posiadać możliwość zdefiniowania reguł zezwalających na komunikację na określonym porcie niezależnie od reguł dla aplikacji, - moduł zapory ogniowej musi posiadać możliwość zdefiniowania zaufanych podsieci, - moduł zapory ogniowej musi chronić przed atakami sieciowymi i mieć możliwość ukrywania obecności komputera w sieci lokalnej. 14. Program musi posiadać możliwość skanowania protokołów POP3, SMTP. Moduł antyspamowy musi posiadać technologie wykrywania spamu poprzez analizę nagłówków. 15. Program musi posiadać funkcję aktualizacji baz definicji wirusów jak i oprogramowania z wewnętrznego repozytorium umieszczonego na serwerze zarządzającym. 16. Program musi posiadać funkcję aktualizacji baz definicji wirusów jak i oprogramowania z poziomu stacji mających dostęp do Internetu bezpośrednio z serwerów aktualizacji producenta lub z wewnętrznego repozytorium serwera zarządzającego w tej sieci. 17. Program musi zapewniać możliwość ręcznej aktualizacji baz definicji antywirusowych bez dostępu

do serwerów aktualizacji producenta Programu przez siec Internet. 18. Program musi zapewniać centralne zbieranie, przetwarzanie alarmów w czasie rzeczywistym oraz ich prezentację administratorom. 19. Program musi mieć funkcję planowania zadań, w tym planowania terminów automatycznej aktualizacji baz sygnatur antywirusowych. 20. W przypadku wykrycia wirusa Program musi posiadać możliwość automatycznego: - podejmowania zalecanych działań, czyli próbowania leczenia, a jeżeli nie jest to możliwe to usunięcia obiektu, - rejestrowania w pliku raportu informacji o wykryciu wirusa i podjętych działaniach, - powiadamiania administratora przy użyciu poczty elektronicznej, - poddawania kwarantannie podejrzanych obiektów. 21. Program musi posiadać wbudowany mechanizm obsługi kwarantanny zainfekowanych i/lub podejrzanych obiektów oraz obiektów nie przetworzonych na stacjach. 3. Wymagania wspólne dla ochrony serwerów i stacji roboczych Lp. Parametry wymagane 1. Program musi zapewniać ochronę przed różnymi typami wirusów, robaków i koni trojańskich, przed zagrożeniami z Internetu i poczty elektronicznej, a także złośliwym kodem (napisanym w Java i ActiveX). 2. Program musi posiadać możliwość wykrywania oprogramowania szpiegowskiego, pobierającego reklamy, programów podwyższonego ryzyka oraz narzędzi hakerskich. 3. Program powinien umożliwiać leczenie z archiwów plików przynajmniej następującego formatu: ZIP. 4. Program musi być uruchamiany automatycznie w momencie startu systemu operacyjnego serwera/stacji roboczej i działać nieprzerwanie do momentu zamknięcia systemu operacyjnego. 5. Podczas startu systemu operacyjnego monitor antywirusowy musi skanować przynajmniej: - główny sektor rozruchowy (MBR), - sektory rozruchowe wszystkich dysków twardych i dyskietek (jeżeli obecne), - pamięć operacyjną komputera oraz aplikacje uruchamiane podczas ładowania systemu operacyjnego. 6. Program antywirusowy musi posiadać możliwość skanowania archiwów i plików spakowanych niezależnie od poziomu ich zagnieżdżenia. 7. Program musi obsługiwać w pełni protokoły IP v4 i IP v6. 8. Program musi pozwalać na pobieranie uaktualnień w trybie przyrostowym (np. po zerwaniu połączenia, bez konieczności retransmitowania już pobranych fragmentów definicji antywirusowych lub uaktualnień komponentów modułów aplikacji). 9. Program oprócz standardowego wyszukiwania, opartego o sygnatury znanych wirusów, musi posiadać także opcję wyszukiwania heurystycznego bazującego na analizie kodu potencjalnego wirusa. 4. Wymagania dla konsoli centralnej administracji Lp. Parametry wymagane 1. Moduł zarządzający musi poprawnie funkcjonować na stacjach pracujących pod kontrolą następujących systemów operacyjnych: - Windows Server 2008 SP1 lub wyższy 32/64 bit, - Windows XP (wszystkie SP) architektura 32 bit, - Windows 7 (wszystkie SP) architektura 32/64 bit. 2. Moduł zarządzania musi mieć możliwość informowania administratorów o wykryciu wirusa. 3. Moduł zarządzania musi posiadać możliwość automatycznej reakcji na wystąpienie wirusa. 4. Moduł zarządzania powinien mieć funkcję wykonania instalacji oprogramowania antywirusowego na stacjach roboczych i serwerach. 5. Moduł zarządzania musi posiadać mechanizm dystrybucji oprogramowania oraz zdefiniowanych polityk antywirusowych do wskazanych komputerów, grup komputerów w zdefiniowanych sieciach. 6. Moduł zarządzający musi mieć możliwość integracji z Active Directory. 7. Moduł zarządzający powinien mieć funkcję automatycznego procesu wykrywania sieci lub ręcznego definiowania sieci i automatycznego odnajdywania znajdujących się w nich komputerów. 8. Moduł zarządzający musi posiadać funkcję wykrywania nowych nieobjętych ochroną antywirusową komputerów

przyłączonych do sieci. 9. Moduł zarządzający musi posiadać szeroką gamę wbudowanych raportów dotyczących stanu ochrony antywirusowej sieci, a także umożliwiać administratorom tworzenie własnych raportów. 10. Moduł zarządzający musi umożliwiać tworzenie i eksport pakietu instalacyjnego na dowolną stację roboczą oraz możliwość instalacji innego oprogramowania. 11. Moduł zarządzający musi mieć możliwość aktualizacji repozytorium baz antywirusowych serwera zarządzającego za pomocą dedykowanego serwera. 12. Moduł zarządzający musi umożliwiać eksportowanie raportów do plików. 13. Moduł zarządzający powinien posiadać możliwość tworzenia grup komputerów w oparciu o Active Directory. 14. Moduł zarządzający musi pozwalać na centralną dystrybucję i instalację aktualizacji bibliotek sygnatur wirusów, która umożliwia automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowej wersji biblioteki. 15. Moduł zarządzający musi zapewniać centralne zbieranie i przetwarzanie alarmów z oprogramowania antywirusowego serwerów w czasie rzeczywistym. 16. Moduł zarządzający musi posiadać możliwość zdalnego inicjowania skanowania antywirusowego na serwerach i stacjach roboczych włączonych do sieci. 17. Moduł zarządzający musi posiadać funkcję tworzenia i konfiguracji pakietów instalacyjnych oprogramowania antywirusowego i jego zdalną dystrybucję na klientów. 18. Moduł zarządzający powinien mieć funkcję wykonania instalacji oprogramowania antywirusowego na stacjach roboczych i serwerach w oparciu o konto administratora lokalnego komputera. 19. Moduł zarządzający powinien posiadać funkcję ręcznego uruchamiania zadań przypisanych do komputerów. 20. Moduł zarządzający powinien posiadać funkcję tworzenia zadań, które będą wykonywane cyklicznie. 21. Program powinien przechowywać wszelkie informacje w relacyjnej bazie danych np. Microsoft SQL Server 2005/2008 lub SQL Express. 4. Wymagania dodatkowe Lp. Parametry wymagane 1. Aktualizacja baz i programów antywirusowych - min. 12 miesięcy. 2. Prace związane z deinstalacją oprogramowania użytkowanego przez Zamawiającego, instalacją nowego oprogramowania oraz uruchomieniem konsoli administracyjnych będą wykonane przez Oferenta w dwóch lokalizacjach ŚBRR na terenie Kielc: ul. Targowa 18 (6 serwerów i 107 komputerów) i ul. Jagiellońska 70 (2 serwery i 111 komputerów). 3. Oferent zapewni szkolenie pracowników Zamawiającego z obsługi i administracji dostarczonego oprogramowania antywirusowego. 4. Dostarczone oprogramowanie antywirusowe musi posiadać telefoniczne wsparcie techniczne w języku polskim dostępne w dni robocze od godziny 9:00 do 15:00 zapewnione przez producenta oprogramowania lub Oferenta..

II.1.4) Czy przewiduje się udzielenie zamówień uzupełniających: nie.

II.1.5) Wspólny Słownik Zamówień (CPV): 48.76.10.00-0.

II.1.6) Czy dopuszcza się złożenie oferty częściowej: nie.

II.1.7) Czy dopuszcza się złożenie oferty wariantowej: nie.

II.2) CZAS TRWANIA ZAMÓWIENIA LUB TERMIN WYKONANIA: Okres w dniach: 4.

SEKCJA III: INFORMACJE O CHARAKTERZE PRAWNYM, EKONOMICZNYM, FINANSOWYM I TECHNICZNYM

III.1) WADIUM

III.2) ZALICZKI

Czy przewiduje się udzielenie zaliczek na poczet wykonania zamówienia: nie

III.4) INFORMACJA O OŚWIADCZENIACH LUB DOKUMENTACH, JAKIE MAJĄ DOSTARCZYĆ WYKONAWCY W CELU POTWIERDZENIA SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU ORAZ NIEPODLEGANIA WYKLUCZENIU NA PODSTAWIE ART. 24 UST. 1 USTAWY

III.4.1) W zakresie wykazania spełniania przez wykonawcę warunków, o których mowa w art. 22 ust. 1 ustawy, oprócz oświadczenia o spełnieniu warunków udziału w postępowaniu, należy przedłożyć:

III.4.2) W zakresie potwierdzenia niepodlegania wykluczeniu na podstawie art. 24 ust. 1 ustawy, należy przedłożyć:

- oświadczenie o braku podstaw do wykluczenia

III.5) INFORMACJA O DOKUMENTACH POTWIERDZAJĄCYCH, ŻE OFEROWANE DOSTAWY , USŁUGI LUB ROBOTY BUDOWLANE ODPOWIADAJĄ OKREŚLONYM WYMAGANIOM

W zakresie potwierdzenia, że oferowane dostawy, usługi lub roboty budowlane odpowiadają określonym wymaganiom należy przedłożyć:

- inne dokumenty

  Do oferty należy załączyć opis oferowanego oprogramowania antywirusowego. W opisie należy podać dostawcę, Producenta lub dystrybutora na Polskę oraz symbol produktu.

III.6) INNE DOKUMENTY

Inne dokumenty niewymienione w pkt III.4) albo w pkt III.5)

podpisane oświadczenie Wykonawcy z art. 22 ust. 1 ustawy o spełnieniu warunków podmiotowych oraz braku podstaw do wykluczenia z postępowania o udzielenie zamówienia w okolicznościach, o których mowa w art. 24 ust. 1 i ust. 2 pkt. 1 ustawy. (Załącznik do SIWZ.).

III.7) Czy ogranicza się możliwość ubiegania się o zamówienie publiczne tylko dla wykonawców, u których ponad 50 % pracowników stanowią osoby niepełnosprawne: nie

SEKCJA IV: PROCEDURA

IV.1) TRYB UDZIELENIA ZAMÓWIENIA

IV.1.1) Tryb udzielenia zamówienia: przetarg nieograniczony.

IV.2) KRYTERIA OCENY OFERT

IV.2.1) Kryteria oceny ofert: najniższa cena.

IV.2.2) Czy przeprowadzona będzie aukcja elektroniczna nie.

IV.3) ZMIANA UMOWY

Czy przewiduje się istotne zmiany postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru wykonawcy: tak

Dopuszczalne zmiany postanowień umowy oraz określenie warunków zmian

Zmiany terminu przewidzianego na zakończenie dostawy w przypadku wstrzymania dostawy przez Zamawiającego; Zmiana zaoferowanego produktu na produkt o parametrach tożsamych lub lepszych od przyjętych w ofercie w przypadku wycofania z rynku oferowanego produktu lub zaprzestania produkcji lub wstrzymania produkcji/dostaw do końca roku 2012. Wymagane jest oświadczenie producenta zaoferowanego produktu.

IV.4) INFORMACJE ADMINISTRACYJNE

IV.4.1) Adres strony internetowej, na której jest dostępna specyfikacja istotnych warunków zamówienia: www.sbrr.pl

Specyfikację istotnych warunków zamówienia można uzyskać pod adresem: Świętokrzyskie Biuro Rozwoju Regionalnego w Kielcach, ul. Targowa 18 pok. 316, piętro III, (sekretariat).

IV.4.4) Termin składania wniosków o dopuszczenie do udziału w postępowaniu lub ofert: 09.10.2012 godzina 10:00, miejsce: Świętokrzyskie Biuro Rozwoju Regionalnego w Kielcach, ul. Targowa 18 pok. 316, piętro III, (sekretariat).

IV.4.5) Termin związania ofertą: okres w dniach: 30 (od ostatecznego terminu składania ofert).

IV.4.16) Informacje dodatkowe, w tym dotyczące finansowania projektu/programu ze środków Unii Europejskiej: .

IV.4.17) Czy przewiduje się unieważnienie postępowania o udzielenie zamówienia, w przypadku nieprzyznania środków pochodzących z budżetu Unii Europejskiej oraz niepodlegających zwrotowi środków z pomocy udzielonej przez państwa członkowskie Europejskiego Porozumienia o Wolnym Handlu (EFTA), które miały być przeznaczone na sfinansowanie całości lub części zamówienia: nie

DYREKTOR
mgr inż. Krzysztof Domagała