RG.271.12.2019.EW

Ogłoszenie o wyborze oferty

Na podstawie art. 92 ust. 1 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2018 r. poz. 1986 ze zm.) Zamawiający Gmina Aleksandrów Kujawski z/s ul. Słowackiego 12, 87-700 Aleksandrów Kujawski w postępowaniu prowadzonym w trybie przetargu nieograniczonego na wykonanie zadania pod nazwą: „Dostawę, instalację i uruchomienie sprzętu komputerowego oraz multimedialnego w ramach projektu pn. „Inwestujemy w edukację II" współfinansowanego przez Unię Europejską ze środków Europejskiego Funduszu Społecznego w ramach Regionalnego Programu Województwa Kujawsko-Pomorskiego na lata 2014-2020. Oś priorytetowa 10 Innowacyjna edukacja, Działanie 10.2 Kształcenie ogólne i zawodowe, Poddziałanie 10.2.2 Kształcenie ogólne"zawiadamia o wyborze oferty.

Wybrano ofertę firmy:

- **iCOD. Pl Sp. Z o.o. ul. Grażyñskiego 51, 43-300 Bielsko-Biała**

Uzasadnienie wyboru:

Wykonawca spełnił wszystkie wymogi określone w specyfikacji istotnych warunków zamówienia.

- ilość uzyskanych punktów w kryterium cena – 58,50
- ilość uzyskanych punktów w kryterium gwarancja jakości - 40.
- łączna ilość punktów ustalona na podstawie kryteriów oceny ofert określonych w siwz – 98,80.

Zamówienie nie obejmuje ustanowienia dynamicznego systemu zakupów.

Planowany termin zawarcia umowy: 23.07.2019 r.

W trakcie badania i oceny ofert Zamawiający odrzucił 2 oferty:

Oferty odrzucone

Odrzucono oferty:

Alltech spółka jawna Zdzisław Pająk, Artur Pająk, ul. Spółdzielcza 33, 09-407 Płock – oferta nr 1

Powód odrzucenia:

W dniu 27.06.2019 r. Zamawiający działając na podstawie art. 87 ust. 1 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz.U. z 2018 r. poz. 1986 z ze zm.) wezwał Wykonawcę Alltech spółka jawna Zdzisław Pająk, Artur Pająk, z/s w Płocku do złożenia wyjaśnień, dotyczących treści złożonej oferty w/w postępowaniu o udzielenie zamówienia. W dniu 24.06.2019 r. wpłynęło do Zamawiającego pismo dotyczące złożonych ofert w postępowaniu o udzielenie zamówienia na „Dostawę, instalacja i uruchomienie sprzętu komputerowego oraz multimedialnego w ramach projektu pn. „Inwestujemy w edukację II" (...).

Wezwany wykonawca w wyznaczonym terminie przesłał wyjaśnienia.

W związku z watpliwościami, które pojawiły się na etapie oceny złożonych ofert, Zamawiający zwrócił się do ITD24 Sp. z o.o. z/s Gliwice, jako dystrybutora oprogramowania Seqrite do udzielenia informacji. W dniu 15.07.2019 r. ITD24 Sp. z o.o. z/s Gliwice udzieliła odpowiedzi na zapytanie Zamawaiącego. Z otrzymanej informacji wynika, iż Oprogramowanie Seqrite występuje w różnych wersjach oraz posiada różne pakiety funkcjonalności.

Wersja oprogramowania Seqrite Endpoint Enterprice + DLP + Cloud, zaproponowane przez firmę Alltech spółka jawna Zdzisław Pająk, Artur Pająk **nie spełnia poniższych zapisów** zaznaczonych kolorem, a wymaganych w SIWZ.

System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +. Silnik musi umożliwiać co najmniej:

- wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji,
- wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych,
- stosowanie kwarantanny,
- wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear)
- skanowanie urządzeń USB natychmiast po podłączeniu,
- automatyczne odłączanie zainfekowanej końcówki od sieci,
- skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji.
- Zarządzanie „aktywami" stacji klienckiej, zbierające informacje co najmniej o nazwie komputera, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (proc.,RAM, SN, storage), BIOS, interfejsach sieciowych, dołączonych peryferiach.
- Musi posiadać moduł ochrony IDS/IPS
- Musi posiadać mechanizm wykrywania skanowania portów
- Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów
- Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości

Szyfrowanie danych:

- Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows.
- Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom.

Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.

Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.

Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.

Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.

Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.

Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.

Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware.

Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware

Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:

- Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli

- Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory
- Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux
- Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet.
- Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich
- Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji

Zarządzanie przez Chmurę:

1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach
2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury
3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur
4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy
5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach
6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń
7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej

Centralna konsola do zarządzania i monitorowania. użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach.

Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.

1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer
2. Oprogramowanie klienckie, zarządzane z poziomu serwera.

System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:

- różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie
- funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD
- funkcje regulowania połączeń WiFi i Bluetooth
- funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe
- funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi
- funkcje blokowania dostępu dowolnemu urządzeniu
- możliwość tymczasowego dodania dostępu do urządzenia przez administratora
- zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu
- możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka
- możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora
- możliwość zarządzani urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry

- możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich
- funkcję wirtualnej klawiatury
- możliwość blokowania każdej aplikacji
- możliwość zablokowania aplikacji w oparciu o kategorie
- możliwość dodania własnych aplikacji do listy zablokowanych
- zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze
- dodawanie innych aplikacji
- dodawanie aplikacji w formie portable
- możliwość wyboru pojedynczej aplikacji w konkretnej wersji
- dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB
- kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool
- możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.
- możliwość zablokowania funkcji Printscreen
- funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx
- funkcje monitorowania i kontroli przepływu poufnych informacji
- możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików
- możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj
- możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe
- ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe
- ochrona zawartości schowka systemu
- ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL
- możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych
- ochrona plików zamkniętych w archiwach
- Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem
- możliwość tworzenia profilu DLP dla każdej polityki
- wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania
- ochrona przez wyciekiem plików poprzez programy typu p2p

Monitorowanie zmian w plikach:
- Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.
- Funkcje monitorowania określonych rodzajów plików.
- Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.
- Generator raportów do funkcjonalności monitora zmian w plikach.
- możliwość śledzenia zmian we wszystkich plikach
- możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach
- możliwość definiowana własnych typów plików

Optymalizacja systemu operacyjnego stacji klienckich:
- usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku
- optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem
- możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich
- instruktaż stanowiskowy pracowników Zamawiającego
- dokumentacja techniczna w języku polskim

Wspierane platformy i systemy operacyjne:
1. Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit)
2. Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit)
3. Mac OS X, Mac OS 10
4. Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat

Zgodnie z zapisami art. 89 ust. 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz.U. z 2018 r. poz. 1986 z ze zm.) Zamawiający odrzuca ofertę, gdyż jej treść nie odpowiada zapisom SIWZ.

- **CEZAR Cezary Machnio i Piotr Gębka Sp. z o.o., ul. Wolność 8 lok. 4, 26-600 Radom – oferta nr 2**

  Powód odrzucenia:

  Zgodnie z zapisami SIWZ Wykonawca nie podał nazw w opisie laptopa (pozycja 25) oraz w opisie komputera stacjonarnego (pozycja 18) – Bezpieczeństwo i oprogramowanie dodatkowe, w formularzu oferty wymagane było podanie nazwy oferowanego oprogramowania. Oferent CEZAR Cezary Machnio i Piotr Gębka Sp. z o.o. nie podał nazwy w/w oprogramowania, co oznacza, że złożona oferta przez Wykonawcę jest nie zgodna ze SIWZ.

Zgodnie z zapisami art. 89 ust. 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz.U. z 2018 r. poz. 1986 z ze zm.) Zamawiający odrzuca ofertę, gdyż jej treść nie odpowiada zapisom SIWZ.

Z up. Wójta
mgr Malwina Andrusiak
Zastępca Wójta