Łomża, 21.02.2020 r.

Znak sprawy: KZp.2730.3.20

Uczestnicy postępowania

Dotyczy: postępowania o udzielenie zamówienia publicznego na „**Dostawę aktualizacji oprogramowania antywirusowego**" (Znak sprawy: KZp.2730.3.20)
Ogłoszenie o zamówieniu zostało opublikowane w Biuletynie Zamówień Publicznych pod numerem 513485-N-2020 z dnia 18.02.2020 r.

Na podstawie art. 38 ust.2 ustawy z dnia 29 stycznia 2004r Prawo zamówień publicznych (t.j. Dz. U. z 2018 r., poz. 1986 ze zmianami), Państwowa Wyższa Szkoła Informatyki i Przedsiębiorczości w Łomży zawiadamia, że w dniu 18.02.2020 r. wpłynął wniosek o wyjaśnienie treści Specyfikacji Istotnych Warunków Zamówienia, wobec powyższego Zamawiający wyjaśnia jak poniżej:

Pytanie 1

Czy dopuszczają Państwa, aby oprogramowanie antywirusowe nie spełniało lub spełniało w inny sposób następujące wymagania:

- możliwość przenoszenia zainfekowanych plików do kwarantanny,
- automatyczna rejestracja nieautoryzowanych prób zmian rejestrów dokonywanych przez użytkownika,
- umożliwiać blokowanie dostępu do pliku autorun.inf na dyskach wymiennych oraz sieciowych,
- [...] Musi istnieć możliwość dodania własnego komunikatu,
- możliwość definiowania różnych działań automatycznej ochrony w odpowiedzi na różne zagrożenia dotyczące systemu plików oraz poczty elektronicznej (czyszczenie, kwarantanna, usunięcie zagrożenia),
- możliwość włączania i wyłączania zapory wbudowanej w systemach Windows.
- możliwość definiowania własnych sygnatur zagrożeń,
- możliwość blokowania dostępu do urządzeń typu [...], urządzenia HID, interfejsy sieciowe [...],
- możliwość blokowania dostępu do plików systemowych i skryptów (np. autorun.ini, blokada modyfikacji pliku hosts i innych plików systemowych),
- zarządzanie zdalne zagrożeniami przeniesionych do kwarantanny

- przywracanie pliku do pierwotnej lokalizacji, ponowne skanowanie i usuwanie z kwarantanny.

Wyjaśnienie:

Zamawiający wymienia funkcjonalności, które muszą być realizowane przez oprogramowanie, ale nie określa sposobu realizacji tych funkcjonalności.

Jednocześnie działając na podstawie art. 38 ust. 4 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t.j. Dz. U. z 2018 r., poz. 1986 ze zmianami). Zamawiający informuje, że wprowadza następujące zmiany w treści SIWZ:

1) w załączniku nr 2 do SIWZ opis przedmiotu zamówienia i załączniku nr 6 do SIWZ formularz jakościowy, pkt 3 tabeli – oprogramowanie alternatywne:

było:

Zamawiający dopuści rozwiązanie równoważne do eksploatowanego oprogramowania Symantec Endpoint Protection, pod warunkiem że będzie dostarczona nowa licencja ze wsparciem producenta na co najmniej 1 rok. Oferowane wsparcie powinno obejmować dostęp do najnowszych sygnatur dla poszczególnych modułów zabezpieczeń, aktualizacji składników oprogramowania oraz możliwość konsultacji telefonicznych z inżynierem producenta w standardowych godzinach pracy.

Licencja musi pozwalać na instalację na co najmniej 20 systemach serwerowych.

Oprogramowanie musi posiadać następujące funkcjonalności:

2. Ochrona antywirusowa:

- ochrona przed wirusami i programami typu spyware
- ochronę przed nieznanymi zagrożeniami i atakami na nieznane luki w zabezpieczeniach
- prewencyjne skanowania w poszukiwaniu aktywnych procesów wykazujących cechy destrukcyjne.
- automatyczne skanowanie plików do których użytkownik ma dostęp oraz otwieranych, zapisywanych, kopiowanych, przenoszonych i wykonywanych,
- możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według zaplanowanego harmonogramu,
- możliwość uruchamiania skanowania pliku lub folderu z menu kontekstowego,
- możliwość definiowania wielu zadań skanowania z różnymi ustawieniami,
- możliwość blokowania dostępu użytkownika do ustawień automatycznej ochrony,
- możliwość definiowania wyjątków skanowania dla plików, folderów, rozszerzeń plików

oraz skanowania prewencyjnego,

- możliwość przenoszenia zainfekowanych plików do kwarantanny,
- możliwość podejmowania odpowiednich czynności przez użytkownika oraz administratora z poziomu konsoli systemu zarządzającego,
- możliwość skanowania wychodzącej i przychodzącej poczty elektronicznej - SMTP, POP3, IMAP,
- automatyczna integracja z klientami poczty MS Outlook, Windows Mail, Mozilla Thunderbird bez konieczności zamian w ich konfiguracji,
- rejestracja zdarzeń związanych z infekcjami wirusowymi i spayware, potencjalnymi zagrożeniami oraz z zagrożeniami sieciowymi,
- automatyczna rejestracja nieautoryzowanych prób zmian rejestrów dokonywanych przez użytkownika,
- umożliwiać blokowanie dostępu do pliku autorun.inf na dyskach wymiennych oraz sieciowych,
- opóźnianie skanowania zaplanowanego w sytuacji komputer przenośny jest zasilany z baterii,

3. Zapora sieciowa:

- zabezpieczenie stacji klienckich przed atakami hakerów oraz nieautoryzowanymi próbami dostępu do komputerów i skanowaniem portów,
- konfiguracja reguł zapory lokalnej w oparciu o protokoły ICMP,UDP, TCP, Ethernet,
- konfiguracja zezwalanego i zabronionego ruchu w oparciu o takie informacje jak: interfejs sieciowy, protokół, stacja źródłowa / docelowa, aplikacja,
- możliwość konfigurowania zapory sieciowej w taki sposób by możliwe było powiadamianie użytkownika o zablokowanych aplikacjach. Musi istnieć możliwość dodania własnego komunikatu,
- możliwość definiowania różnych działań automatycznej ochrony w odpowiedzi na różne zagrożenia dotyczące systemu plików oraz poczty elektronicznej (czyszczenie, kwarantanna, usunięcie zagrożenia),
- możliwość ograniczania dostępu do sieci dla poszczególnych aplikacji,
- wykrywanie skanowania portów i ataków typu DoS oraz automatyczne blokowanie adresu IP atakującego na określony czas,
- możliwość włączania i wyłączania zapory wbudowanej w systemach Windows.

4. Zapobieganie włamaniom

- ochrona przed zagrożeniami sieciowymi poprzez konfigurowaną dwukierunkową zaporę

sieciową oraz mechanizm IPS,

- automatyczna aktualizacja sygnatur zagrożeń sieciowych udostępnianych przez producenta oprogramowania,
- możliwość definiowania własnych sygnatur zagrożeń,

5. Kontrola urządzeń i aplikacji:

- kontrolę dostępu do nośników wymiennych USB, CD/DVD z możliwością blokowania,
- możliwość blokowania dostępu do urządzeń typu drukarka skaner, czytniki kart, urządzenia HID, interfejsy sieciowe i bluetooth,
- możliwość blokowania uruchamiania programów z nośników wymiennych,
- możliwość rejestrowania lub blokowania zapisu na nośnikach USB,
- możliwość blokowania dostępu do plików systemowych i skryptów (np. autorun.ini, blokada modyfikacji pliku hosts i innych plików systemowych),

6. Obsługiwane systemy operacyjne operacyjnych i metody instalacji:

- obsługa 32 i 64 bitowych systemów Windows 7, 8, 10, Serwer 2008R2/2019, Linux oraz macOS,
- możliwość instalacji starszych wersji oprogramowania antywirusowego w systemach Windows XP i Vista,
- Interfejs użytkownika oraz pomoc w języku polskim (co najmniej dla instalacji w systemach Windows),
- instalację zarządzaną oraz nie zarządzaną,
- instalacja centralnego modułu zarządzania stacjami klienckimi musi być możliwa w tym samym systemie operacyjnym co moduł zarządzania oprogramowania Symantec Endpoint Ptotection Manager i nie może ograniczać jego funkcjonalności,
- automatyczną aktualizację sygnatur udostępnianych przez producenta za pomocą Internetu,
- możliwość aktualizacji sygnatur „offline" na komputerach nie posiadających połączenia z Internetem,

7. Funkcjonalności centralnego zarządzania systemem antywirusowym:

- w ramach licencji musi być dostępne oprogramowanie do centralnego zarządzania oprogramowaniem antywirusowym do instalacji w środowisku Windows, Linux lub maszyny wirtualnej do instalacji w środowisku VMWare
- zdalna instalacja oprogramowania antywirusowego w postaci instalacji „wypychanej" oraz instalacji użytkownika (na żądanie),
- współpracę z kontrolerem domeny ActiveDirectory,

- wykrywanie komputerów bez zainstalowanego oprogramowania antywirusowego, z oprogramowaniem nie zarządzanym lub z nieaktualnymi sygnaturami, w różnych segmentach sieci,
- zdalne konfigurowanie wszystkich parametrów oprogramowania antywirusowego,
- możliwość definiowania parametrów dla pojedynczych komputerów oraz grup komputerów,
- centralną rejestrację wszystkich zdarzeń występujących na komputerach zarządzanych,
- podgląd szczegółów zarejestrowanego incydentu, który wystąpił na dowolnym z zarządzanych komputerów,
- generowanie zastawień i statystyk dotyczących występujących zdarzeń, zagrożeń, ilości komputerów i stanu zainstalowanego na nich oprogramowania antywirusowego,
- informowanie o zagrożeniach, które nie zostały usunięte, wyczyszczone,
- automatyczną i na żądanie aktualizację zasad bezpieczeństwa na chronionych komputerach,
- sprawdzenie aktualności zasad bezpieczeństwa na komputerach z zainstalowanym oprogramowaniem antywirusowym,
- automatyczne lub na żądanie włączenie automatycznej ochrony w przypadku kiedy użytkownik ją wyłączył,
- automatyczne wymuszanie pobierania nowych definicji zagrożeń na komputerach klienckich,
- konfigurację powiadomień email dla administratora przy wystąpieniu poszczególnych zagrożeń,
- zarządzanie zdalne zagrożeniami przeniesionych do kwarantanny – przywracanie pliku do pierwotnej lokalizacji, ponowne skanowanie i usuwanie z kwarantanny,
- przesyłanie potencjalnie zainfekowanych plików do laboratorium producenta w celu poddania ich analizie,
- możliwość generowania wiadomości email do administratorów w przypadku wystąpienia zagrożeń i innych zdarzeń systemowych.

Ponadto

Dostawca rozwiązania równoważnego zobowiązany jest do przeprowadzenia szkoleń co najmniej 2 administratorów Zamawiającego, w zakresie instalacji i konfiguracji wszystkich wyżej opisanych funkcjonalności oprogramowania wymaganych przez Zamawiającego lub zgodnie z programem szkoleniowym producenta oprogramowania. Szkolenie może być przeprowadzone przez Wykonawcę lub inny wskazany podmiot metodą stacjonarną lub

zdalną, przy czym środowisko dydaktyczne zapewnia podmiot szkolący. Szkolenie metodą zdalną powinno odbywać się w sesjach nie dłuższych niż 4 godziny dziennie.

Osoba przeprowadzająca szkolenia powinna legitymować się certyfikatem ukończenia kursu autoryzowanego przez producenta oprogramowania antywirusowego.

Instruktor będzie udzielał wsparcia osobom szkolonym przez co najmniej 14 dni po zakończeniu kursu.

winno być:

Zamawiający dopuści rozwiązanie równoważne do eksploatowanego oprogramowania Symantec Endpoint Protection, pod warunkiem że będzie dostarczona nowa licencja ze wsparciem producenta na co najmniej 1 rok. Oferowane wsparcie powinno obejmować dostęp do najnowszych sygnatur dla poszczególnych modułów zabezpieczeń, aktualizacji składników oprogramowania oraz możliwość konsultacji telefonicznych z inżynierem producenta w standardowych godzinach pracy.

Licencja musi pozwalać na instalację na co najmniej 20 systemach serwerowych.

Oprogramowanie musi posiadać następujące funkcjonalności:

1. Ochrona antywirusowa:

- ochrona przed wirusami i programami typu spyware
- ochronę przed nieznanymi zagrożeniami i atakami na nieznane luki w zabezpieczeniach
- prewencyjne skanowania w poszukiwaniu aktywnych procesów wykazujących cechy destrukcyjne.
- automatyczne skanowanie plików do których użytkownik ma dostęp oraz otwieranych, zapisywanych, kopiowanych, przenoszonych i wykonywanych
- możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według zaplanowanego harmonogramu,
- możliwość uruchamiania skanowania pliku lub folderu z menu kontekstowego,
- możliwość definiowania wielu zadań skanowania z różnymi ustawieniami,
- możliwość blokowania dostępu użytkownika do ustawień automatycznej ochrony,
- możliwość definiowania wyjątków skanowania dla plików, folderów, rozszerzeń plików oraz skanowania prewencyjnego,
- automatyczne przenoszenie do kwarantanny zainfekowanych plików do kwarantanny z możliwością wykonania ponownej kontroli antywirusowej oraz przywrócenia do pierwotnej lokalizacji,
- możliwość podejmowania odpowiednich czynności przez użytkownika oraz administratora z poziomu konsoli systemu zarządzającego,

- możliwość skanowania wychodzącej i przychodzącej poczty elektronicznej - SMTP, POP3, IMAP,
- automatyczna integracja z klientami poczty MS Outlook, Windows Mail, Mozilla Thunderbird bez konieczności zamian w ich konfiguracji,
- rejestracja zdarzeń związanych z infekcjami wirusowymi i spayware, potencjalnymi zagrożeniami oraz z zagrożeniami sieciowymi,
- rejestracja nieautoryzowanych prób zmian w rejestrach systemowych na chronionych urządzeniach,
- opóźnianie skanowania zaplanowanego w sytuacji komputer przenośny jest zasilany z baterii,

2. Zapora sieciowa:

- zabezpieczenie stacji klienckich przed atakami hakerów oraz nieautoryzowanymi próbami dostępu do komputerów i skanowaniem portów,
- konfiguracja reguł zapory lokalnej w oparciu o protokoły ICMP,UDP, TCP, Ethernet,
- konfiguracja zezwalanego i zabronionego ruchu w oparciu o takie informacje jak: interfejs sieciowy, protokół, stacja źródłowa / docelowa, aplikacja,
- możliwość konfigurowania zapory sieciowej w taki sposób by możliwe było powiadamianie użytkownika o zablokowanych aplikacjach lub komunikacji sieciowej,
- możliwość ograniczania dostępu do sieci dla poszczególnych aplikacji,
- wykrywanie skanowania portów i ataków typu DoS oraz automatyczne blokowanie adresu IP atakującego na określony czas,
- możliwość włączania i wyłączania zapory wbudowanej w systemach Windows.

3. Zapobieganie włamaniom

- ochrona przed zagrożeniami sieciowymi poprzez konfigurowaną dwukierunkową zaporę sieciową oraz mechanizm IPS,
- automatyczna aktualizacja sygnatur zagrożeń sieciowych udostępnianych przez producenta oprogramowania,
- możliwość definiowania własnych zasad reakcji na zagrożenia,

4. Kontrola urządzeń i aplikacji:

- kontrolę dostępu do nośników wymiennych USB, CD/DVD z możliwością blokowania,
- możliwość blokowania dostępu do urządzeń typu czytniki kart, urządzenia typu HID,
- możliwość blokowania uruchamiania programów z nośników wymiennych,
- możliwość rejestrowania lub blokowania zapisu na nośnikach USB,
- zapobieganie modyfikacji plików systemowych (np. blokowanie modyfikacji hosts)

i uruchamiania skryptów (np. blokowanie przetwarzania autorun.ini),

5. Obsługiwane systemy operacyjne operacyjnych i metody instalacji:

- obsługa 32 i 64 bitowych systemów Windows 7, 8, 10, Serwer 2008R2/2019, Linux oraz macOS,
- możliwość instalacji starszych wersji oprogramowania antywirusowego w systemach Windows XP i Vista,
- Interfejs użytkownika oraz pomoc w języku polskim (co najmniej dla instalacji w systemach Windows),
- instalację zarządzaną oraz nie zarządzaną,
- instalacja centralnego modułu zarządzania stacjami klienckimi musi być możliwa w tym samym systemie operacyjnym co moduł zarządzania oprogramowania Symantec Endpoint Ptotection Manager i nie może ograniczać jego funkcjonalności,
- automatyczną aktualizację sygnatur udostępnianych przez producenta za pomocą Internetu,
- możliwość aktualizacji sygnatur „offline" na komputerach nie posiadających połączenia z Internetem,

6. Funkcjonalności centralnego zarządzania systemem antywirusowym:

- w ramach licencji musi być dostępne oprogramowanie do centralnego zarządzania oprogramowaniem antywirusowym do instalacji w środowisku Windows, Linux lub maszyny wirtualnej do instalacji w środowisku VMWare
- zdalna instalacja oprogramowania antywirusowego w postaci instalacji „wypychanej" oraz instalacji użytkownika (na żądanie),
- współpracę z kontrolerem domeny ActiveDirectory,
- wykrywanie komputerów bez zainstalowanego oprogramowania antywirusowego, z oprogramowaniem nie zarządzanym lub z nieaktualnymi sygnaturami, w różnych segmentach sieci,
- zdalne konfigurowanie wszystkich parametrów oprogramowania antywirusowego,
- możliwość definiowania parametrów dla pojedynczych komputerów oraz grup komputerów,
- możliwość definiowania różnych działań automatycznej ochrony w odpowiedzi na różne zagrożenia dotyczące ochrony antywirusowej, kontroli aplikacji i urządzeń oraz zapory sieciowej (np. czyszczenie, kwarantanna, rejestrowanie, usunięcie zagrożenia, blokowanie dostępu),
- centralną rejestrację wszystkich zdarzeń występujących na zarządzanych komputerach,

- podgląd szczegółów zarejestrowanego incydentu, który wystąpił na dowolnym z zarządzanych komputerów,
- generowanie zastawień i statystyk dotyczących występujących zdarzeń, zagrożeń, ilości komputerów i stanu zainstalowanego na nich oprogramowania antywirusowego,
- informowanie o zagrożeniach, które nie zostały usunięte, wyczyszczone,
- automatyczną i na żądanie aktualizację zasad bezpieczeństwa na chronionych komputerach,
- sprawdzenie aktualności zasad bezpieczeństwa na komputerach z zainstalowanym oprogramowaniem antywirusowym,
- automatyczne lub na żądanie włączenie automatycznej ochrony w przypadku kiedy użytkownik ją wyłączył,
- automatyczne wymuszanie pobierania nowych definicji zagrożeń na komputerach klienckich,
- generowanie raportów związanych ze stanem ochrony na poszczególnych urządzeniach, rodzajów występujących zagrożeń, przeprowadzonych zadań skanowania i zdarzeń systemowych,
- monitorowanie zdalne zagrożeń przeniesionych do kwarantanny,
- przesyłanie potencjalnie zainfekowanych plików do laboratorium producenta w celu poddania ich analizie,
- możliwość generowania wiadomości email do administratorów w przypadku wystąpienia zagrożeń i innych zdarzeń systemowych.

Ponadto

Dostawca rozwiązania równoważnego zobowiązany jest do przeprowadzenia szkoleń co najmniej 2 administratorów Zamawiającego, w zakresie instalacji i konfiguracji wszystkich wyżej opisanych funkcjonalności oprogramowania wymaganych przez Zamawiającego lub zgodnie z programem szkoleniowym producenta oprogramowania. Szkolenie może być przeprowadzone przez Wykonawcę lub inny wskazany podmiot metodą stacjonarną lub zdalną, przy czym środowisko dydaktyczne zapewnia podmiot szkolący. Szkolenie metodą zdalną powinno odbywać się w sesjach nie dłuższych niż 4 godziny dziennie.

Osoba przeprowadzająca szkolenia powinna legitymować się certyfikatem ukończenia kursu autoryzowanego przez producenta oprogramowania antywirusowego.

Instruktor będzie udzielał wsparcia osobom szkolonym przez co najmniej 14 dni po zakończeniu kursu.

2) **<u>w SIWZ w dziale XII Miejsce i termin składania i otwarcia ofert, zmianie ulega pkt. 1 i 3:</u>**

było:

1. Oferty należy składać do dnia: 26.02.2020 r. do godz. 12:00 w siedzibie Zamawiającego:
   Państwowa Wyższa Szkoła Informatyki i Przedsiębiorczości w Łomży
   ul. Akademicka 14, 18-400 Łomża, po
   kój nr 124 I piętro (sekretariat)
3. Oferty zostaną otwarte dnia 26.02.2020 r. o godz. 12:30 w siedzibie Zamawiającego:
   Państwowa Wyższa Szkoła Informatyki i Przedsiębiorczości w Łomży
   ul. Akademicka 14, 18-400 Łomża, pokój nr 16 parter

winno być:

1. **Oferty należy składać do dnia: 28.02.2020 r. do godz. 12:00** w siedzibie Zamawiającego:
   Państwowa Wyższa Szkoła Informatyki i Przedsiębiorczości w Łomży
   ul. Akademicka 14, 18-400 Łomża, pokój nr 124 I piętro (sekretariat)
3. **Oferty zostaną otwarte dnia: 28.02.2020 r. o godz. 12:30** w siedzibie Zamawiającego:
   Państwowa Wyższa Szkoła Informatyki i Przedsiębiorczości w Łomży
   ul. Akademicka 14, 18-400 Łomża, pokój nr 16 parter

Pozostałe zapisy specyfikacji istotnych warunków zamówienia pozostają bez zmian.

Ponadto działając na podstawie art. 12a ust. 3 ustawy z dnia 29 stycznia 2004r Prawo zamówień publicznych (t.j. Dz. U. z 2018 r., poz. 1986 ze zmianami), Zamawiający informuje, że w związku ze zmianą Specyfikacji Istotnych Warunków Zamówienia zmianie ulega treść ogłoszenia o zmówieniu w przedmiotowym zakresie. Zmianę ogłoszenia zamieszczono w Biuletynie Zamówień Publicznych w dniu dzisiejszym.

W imieniu Zamawiającego:

dr hab. Dariusz Sukowik, prof. PWSIiP

Załączniki:

1. *Opis przedmiotu zamówienia (Załącznik nr 2 do SIWZ) po zmianach*
2. *Formularz jakościowy (Załącznik nr 6 do SIWZ) po zmianach*