Katowice, 25.07.2022 r.

Zgodnie z art. 284 ust. 2 i 6 ustawy – Prawo zamówień publicznych z 11 września 2019 r. (Dz. U. z 2021 r., poz. 1129 ze zm.), Zamawiający udziela wyjaśnień treści Specyfikacji Warunków Zamówienia dot. postępowania prowadzonego w trybie podstawowym pn.: **„Dostawa sprzętu IT dla Wojewódzkiego Ośrodka Ruchu Drogowego w Katowicach – etap II”.**

**Treść pytań:**

Proszę o informację, czy dopuszczają Państwo udział w przetargu rozwiązania, które nie spełnia poniższych wymogów lub spełnia je częściowo/w inny sposób zgodnie z poniższym (w nawiasie komentarze jeśli spełniamy, częściowo.

Brak nawiasu = rozwiązanie nie spełnia wymogu):

1. Program musi umożliwić działanie na sprzęcie o minimalnych parametrach sprzętowych: • Procesor 1 GHz lub szybszy (wymagana jest obsługa SSE2). • Pamięć RAM: ▪ 1 GB dla 32-bitowych systemów operacyjnych. ▪ 2 GB dla 64-bitowych systemów operacyjnych. • 2 GB wolnej przestrzeni na dysku twardym. {Minimalne wymagania naszego rozwiązania to 2GHz (2.4GHz dla serwerów)}

**Odpowiedź 1:**

**Zamawiający wyraża zgodę na podniesienie minimalnych parametrów sprzętowych opisanych w punkcie I.2 zastępując treść: „Procesor 1 GHz lub szybszy (wymagana jest obsługa SSE2)” następująco:   
„Procesor 2 GHz lub szybszy” oraz w punkcie II.2 zastępując treść: „Procesor 1 GHz lub szybszy (wymagana jest obsługa SSE2)” następująco: „Procesor 2,4 GHz lub szybszy”.**

2. Mechanizm który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji.

**Odpowiedź 2:**

**Zamawiający modyfikuje treść punktu I.8 oraz II.8 zastępując treść: „Mechanizm który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji” następująco: „Mechanizm który wspiera powrót do ostatnich działającej wersji sygnatur w przypadku wdrożenia wadliwej aktualizacji. Za wsparcie jest uważana również możliwość wczytania z zewnętrznego źródła wcześniejszej poprawnej wersji sygnatur”.**

3. Możliwość tworzenia reguł blokujących/zezwalających na korzystanie z danego urządzenia w zależności od konta, na którym pracuje użytkownik.

**Odpowiedź 3:**

**Zamawiający modyfikuje treść Przedmiotu zamówienia poprzez usunięcie pkt. I.9.1.**

4. Wbudowany moduł skanujący i oczyszczający protokoły POP3, SMTP, IMAP niezależnie od klienta pocztowego. {oprócz IMAP, jeśli mówimy o ochronie na poziomie protokołu, jeśli na poziomie klienta pocztowego to rozwiązanie spełnia}

**Odpowiedź 4:**

**Zamawiający modyfikuje treść punktu I.14 zastępując treść: „Wbudowany moduł skanujący i oczyszczający protokoły POP3, SMTP, IMAP niezależnie od klienta pocztowego” następująco: „Aplikacja winna skanować i oczyszczać komunikację dowolnego klienta pocztowego z serwerem, prowadzoną z użyciem protokołów POP3, SMTP, IMAP”.**

5. System antywirusowy ma posiadać możliwość skanowania archiwów i plików spakowanych niezależnie od poziomu ich zagnieżdżenia. {16 razy może być zagnieżdżony plik}

**Odpowiedź 5:**

**Zamawiający modyfikuje treść punktu I.24, II.16, II.29 zastępując treść „niezależnie od poziomu ich zagnieżdżenia” następująco: „minimum do 12 krotnego zagnieżdżenia”.**

6.Skanowanie w czasie rzeczywistym: • Pobieranej i wysyłanej z Internetu poczty elektronicznej (wraz z załącznikami) po protokołach POP3, SMTP, IMAP niezależnie od klienta pocztowego. • Poczty elektronicznej przetwarzanej przez program MS Outlook niezależnie od wykorzystywanego protokołu pocztowego. {oprócz IMAP, jeśli mówimy o ochronie na poziomie protokołu, jeśli na poziomie klienta pocztowego to rozwiązanie spełnia}

**Odpowiedź 6:**

**Zamawiający modyfikuje treść punktu I.31 podpunkt drugi zastępując treść „Pobieranej i wysyłanej z Internetu poczty elektronicznej (wraz z załącznikami) po protokołach POP3, SMTP, IMAP niezależnie od klienta pocztowego” następująco: „Komunikacji dowolnego klienta pocztowego z serwerem, prowadzoną z użyciem protokołów POP3, SMTP, IMAP wraz ze skanowaniem załączników”.**

7. W przypadku wykrycia wirusa monitor antywirusowy winien automatycznie: • Podejmować zalecane działanie czyli próbować leczyć, a jeżeli nie jest to możliwe usuwać obiekt.

Przed usunięciem zainfekowanego obiektu monitor antywirusowy powinien przenieść go w bezpieczny obszar dysku – kwarantanna, plik w kwarantannie powinien być zaszyfrowany. {Po niedanej próbie leczenia jeśli plik w całości jest uznany za niebezpieczny to jest usuwany i nie trafi do kwarantanny. Jeśli jego fragment jest złośliwy i nie uda się go wyleczyć to może trafić do kwarantanny}

**Odpowiedź 7:**

**Zamawiający modyfikuje treść punktu I.32 oraz II.27 podpunkt pierwszy zastępując treść: „Przed usunięciem zainfekowanego obiektu monitor antywirusowy powinien przenieść go w bezpieczny obszar dysku – kwarantanna, plik w kwarantannie powinien być zaszyfrowany” następująco: „Przed usunięciem zainfekowanego obiektu, jeżeli jego fragment jest złośliwy, monitor antywirusowy powinien przenieść go w bezpieczny obszar dysku – kwarantanna, plik w kwarantannie powinien być zaszyfrowany Jeśli plik w całości jest uznany za niebezpieczny to przeniesienie do kwarantanny nie jest wymagane”.**

8. Predefiniowane zestawy reguł monitorowania dla typowych aplikacji serwerowych np. Serwer MSSQL, mySQL, IIS itp.

**Odpowiedź 8:**

**Zamawiający modyfikuje treść Przedmiotu zamówienia poprzez usunięcie pkt. II.22**

9. Możliwość dynamicznej zmiany użycia zasobów systemowych w zależności od obciążenia systemu przez aplikacje użytkownika.

**Odpowiedź 9:**

**Zamawiający modyfikuje treść Przedmiotu zamówienia poprzez usunięcie pkt. II.23**

10. System scentralizowanego zarządzania powinien przechowywać ustawienia w bazie danych. Silnik bazy danych winien być dostarczony wraz z systemem lub też powinien być dostępny na darmowej licencji dla użytkowników biznesowych np. Microsoft SQL Server Express 64-bitowy.

**Odpowiedź 10:**

**Zamawiający podtrzymuje wymaganie.**

11. System zdalnego zarządzania powinien umożliwiać automatyczne umieszczenie komputerów w grupach administracyjnych. {Przy synchronizacji z Active Directory będzie struktura jak w Active Directory; bez Active Directory nie ma grup dynamicznych}

**Odpowiedź 11:**

**Zamawiający modyfikuje treść Przedmiotu zamówienia poprzez usunięcie pkt. IV.8**

12. Zarządzanie aplikacjami odbywa się przy użyciu profili aplikacji oraz zadań.

**Odpowiedź 12:**

**Zamawiający modyfikuje treść punktu IV.11 zastępując treść „Zarządzanie aplikacjami odbywa się przy użyciu profili aplikacji oraz zadań” następująco: „Zarządzanie aplikacją antywirusową na stacjach roboczych odbywa się przy użyciu profili aplikacji oraz zadań”.**

13. 26. System zdalnego zarządzania powinien mieć możliwość zbierania informacji o sprzęcie zainstalowanym na komputerach klienckich.

**Odpowiedź 13:**

**Zamawiający modyfikuje treść Przedmiotu zamówienia poprzez usunięcie pkt. IV.26**

14. Program powinien mieć możliwość dezinstalacji aplikacji niekompatybilnych.

**Odpowiedź 14:**

**Zamawiający modyfikuje treść Przedmiotu zamówienia poprzez usunięcie pkt. IV.27**

15. System zdalnego zarządzania powinien umożliwić wysyłanie powiadomień do wybranych użytkowników przy użyciu min. poczty elektronicznej.

**Odpowiedź 15:**

**Zamawiający modyfikuje treść punktu IV.34 zastępując treść „umożliwić wysyłanie powiadomień do wybranych użytkowników przy użyciu min. poczty elektronicznej” następująco: „umożliwić wysyłania powiadomień o wybranych zdarzeniach związanych z systemem antywirusowym do wybranych użytkowników (administratorów) zdefiniowanych w tym systemie przy użyciu min. poczty elektronicznej**

16. System zdalnego zarządzania powinien tworzyć repozytorium sprzętu min. komputerów i nośników wymiennych.

**Odpowiedź 16:**

**Zamawiający modyfikuje treść punktu IV.35 zastępując treść „komputerów i nośników wymiennych” na „Napędów CD-ROM/DVD/BR oraz pamięci masowe np. pendrive, dysk przenośny itp.”**

17. System winien zawierać aplikację przygotowującą repozytorium do przeniesienia. {Aktualizacje ręczne są pobierane przez Internet ze strony producenta, nie przez aplikację}

**Odpowiedź 17:**

**Zamawiający modyfikuje treść punktu IV.38 pkt. 1 dodając po końcowej kropce treść „Jeżeli aktualizacje aplikacji i baz wirusów są przygotowywane przez producenta i udostępniane na jego stronie internetowej jako pojedyncze archiwa, odrębna aplikacja przygotowująca repozytorium do przeniesienia nie jest wymagana”.**

18. Tylko pojedyncze stacje w podsieciach majce dostęp do internetu w celu pobierania uaktualnień i udostępniające je stacjom z tej samej podsieci. Na stacjach tych nie może być zainstalowane oprogramowanie antywirusowe. System musi umożliwiać ograniczenie pasma sieciowego wykorzystywanego do pobierania uaktualnień.

**Odpowiedź 18:**

**Zamawiający modyfikuje treść punktu IV.38 pkt. 2 dodając po końcowej kropce treść: „Za ograniczenia pasma sieciowego będzie uważane również rozwiązanie pobierające uaktualnienia w zdefiniowanym przez zamawiającego przedziale czasowym.**

**Ponadto Zamawiający dokonuje modyfikacji ostatniego zdania przedmiotu zamówienia zastępując treść „Wraz z produktem wykonawca jest zobowiązany dostarczyć w języku polskim opis instalacji i konfiguracji systemu dla wymagań opisanych w pkt. 40” następująco: „Wraz z produktem wykonawca jest zobowiązany dostarczyć w języku polskim opis instalacji i konfiguracji systemu dla wymagań opisanych w pkt. 38”.**

W oryginale podpis:

Dyrektor Word – Janusz Freitag