GMINA CZERNICA
ul. Kolejowa nr 3
55-003 CZERNICA

Czernica, dnia 21.09.2017r.

GKil.271.2.20.2017.KM

WYJAŚNIENIA
TREŚCI SPECYFIKACJI ISTOTNYCH WARUNKÓW ZAMÓWIENIA

Dotyczy przetargu nieograniczonego pn.: Dostawa niezbędnego sprzętu i infrastruktury sieciowej aktywnej i pasywnej na potrzeby realizacji e-usług w ramach projektu pod nazwą „Zwiększenie dostępności i jakości elektronicznych usług publicznych dla mieszkańców i podmiotów gospodarczych Powiatu Wrocławskiego oraz 8 Gmin: Czernicy, Długołęki, Jordanowa Śląskiego, Kątów Wrocławskich, Kobierzyc, Mietkowa, Siechnic i Żórawiny – usługi wdrożenia oprogramowania"

Działając na podstawie art. 38 ust. 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tj. Dz. U. z 2017 r., poz. 1579 ze zm., dalej jako ustawa Pzp), Zamawiający udziela odpowiedzi na pytania Wykonawców:

Pytanie nr 1:
ZAŁĄCZNIK NR 10, Szczegółowy opis przedmiotu zamówienia.pdf , 2.3 Część I – Firewall:
ochrona przed wirusami – antywirus [AV] co najmniej dla protokołów SMTP, SMTPS, POP3, POP3S, IMAPS, HTTP, FTP, HTTPS. System AV musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) oraz powinien umożliwiać skanowanie archiwów typu zip, rar,
- Czy zamawiający dopuszcza rozwiązanie, które wykonuje analizę AV dla wszystkich protokołów z wyjątkiem IMAPS?
Odpowiedź:
Zamawiający wymaga aby antywirus [AV] skanował szyfrowany protokół IMAPS.

Pytanie nr 2:
ZAŁĄCZNIK NR 10, Szczegółowy opis przedmiotu zamówienia.pdf , 2.3 Część I – Firewall:
identyfikacja i kontrola aplikacji (rozpoznawanie min. 1500 aplikacji) bez względu na port oraz protokół w tym rozpoznawanie ruchu P2P,
- czy zamawiający dopuszcza rozwiązanie gdzie kontrola aplikacji odbywa się za pomocą głębokiej analizy pakietów i wykrywania typu komunikacji i protokołu bez określenia dokładnej aplikacji? W takiej analizie pojedyncza sygnatura pozwala na wykrycie określonej rodziny aplikacji i kontrolę ruchu przez nie generowanego a więc umożliwia kontrolę wielu aplikacji za pomocą jednej sygnatury.
Odpowiedź:
Zamawiający dopuszcza takie rozwiązanie.

Pytanie nr 3:
Warunki gwarancji - Świadczenie gwarancji w systemie „door to door" - polegającej na odbiorze uszkodzonego sprzętu od Zamawiającego a następnie dostarczenie sprawnego sprzętu. Wykonawca na własny koszt zapewni transport urządzeń do i z serwisu. Maksymalny czas skutecznej naprawy - 10 dni roboczych od momentu zgłoszenia.
- warunki gwarancji mówią:
W przypadku wystąpienia awarii urządzenia Odbiorca powinien zgłosić tą okoliczność Sprzedawcy od poniedziałku do piątku (dni robocze). Jeśli potwierdzenie wymiany nastąpi do godziny 15:00 od poniedziałku do piątku to urządzenie zastępcze zostanie wysłane jeszcze w tym samym dniu.
Jeśli zgłoszenie zostanie wysłane w dzień wolny od pracy lub po godzinie 15:00, nowe urządzenie zostanie wysłane w najbliższy dzień roboczy.
W ramach gwarancji Next Business Day Odbiorca otrzyma nieodpłatnie urządzenie zastępcze w ciągu kolejnego dnia roboczego następującego po dniu w którym odbiorca dokonał zgłoszenia.
Odbiorca ma obowiązek odesłać uszkodzone urządzenie przesyłką kurierską ubezpieczoną na swój koszt na adres wskazany przez Sprzedawcę w ciągu 7 dni od dnia otrzymania urządzenia zastępczego.
W przypadku nieodesłania uszkodzonego urządzenia w podanym terminie Odbiorca zobowiązuje się do przyjęcia faktury na kwotę równą wartości nowo otrzymanego urządzenia.
Urządzenie dostarczone w ramach serwisu Next Business Day może być nowe lub używane ale o parametrach technicznych nie gorszych niż pierwotnie dostarczone urządzenie.
Dostarczone urządzenie zastępcze w ramach serwisu Next Business Day jest traktowane jako docelowe urządzenie dla klienta (klient nie może zażądać np. naprawy i odesłania pierwotnie używanego urządzenia).

Wszystkie pierwotnie uruchomione serwisy zostają przeniesione i kontynuowane na urządzeniu wymienionym w ramach usługi NBD.
Czy zamawiający dopuszcza taki rodzaj świadczenia gwarancji ?
Odpowiedź:
Zamawiający podtrzymuje zapis w SIWZ. Zamawiający nie zgadza się na odesłanie uszkodzonego urządzenia na swój koszt.

Pytanie nr 4:

Dotyczy: Załącznik nr 10; SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA; 2.4 Część I - Firewall – 1 szt.; Funkcje Bezpieczeństwa;

„ochrona przed wirusami – antywirus [AV] co najmniej dla protokołów SMTP, SMTPS, POP3, POP3S, IMAPS, HTTP, FTP, HTTPS. System AV musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) oraz powinien umożliwiać skanowanie archiwów typu zip, rar,"

Pytanie: Czy Zamawiający dopuszcza rozwiązanie, które wykonuje analizę AV dla wszystkich protokołów z wyjątkiem IMAPS?

Odpowiedź:
Zamawiający wymaga aby antywirus [AV] skanował szyfrowany protokół IMAPS.

Pytanie nr 5:

Dotyczy: Załącznik nr 10; SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA; 2.4 Część I - Firewall – 1 szt.; Funkcje Bezpieczeństwa;

„identyfikacja i kontrola aplikacji (rozpoznawanie min. 1500 aplikacji) bez względu na port oraz protokół w tym rozpoznawanie ruchu P2P,"

Pytanie: Czy Zamawiający dopuszcza rozwiązanie gdzie kontrola aplikacji odbywa się za pomocą głębokiej analizy pakietów i wykrywania typu komunikacji i protokołu bez określenia dokładnej aplikacji? W takiej analizie pojedyncza sygnatura pozwala na wykrycie określonej rodziny aplikacji i kontrolę ruchu przez nie generowanego, a więc umożliwia kontrolę wielu aplikacji za pomocą jednej sygnatury.

Odpowiedź:
Zamawiający dopuszcza takie rozwiązanie.

Zastępca Wójta
Andrzej Czech