



**ZASTĘPCA DYREKTORA
BIURA FINANSÓW
KOMENDY GŁÓWNEJ STRAŻY
GRANICZNEJ**

ul. Podchorążych 38, 00- 463 Warszawa

KG-BF-ZP.3710.40.2019

Warszawa, dn. 24.07.2019r.

Strona internetowa

Dotyczy: postępowania o udzielenie zamówienia publicznego pn.: „Rozbudowa i utrzymanie systemu KORUND” – sprawa nr 40/BF/BŁil/19

Szanowni Państwo,

na podstawie art. 38 ust. 2 ustawy z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (Dz. U. z 2018 r. poz. 1986 ze zm.) informuję, że Zamawiający udziela następujących odpowiedzi na pytania złożone do treści Specyfikacji Istotnych Warunków Zamówienia (SIWZ):

Pytanie nr 1: Pytanie dotyczy kwalifikacji technicznych (pkt III.2.3) w związku z opisem zamówienia (pkt II.3. ppkt 1 - krótki opis dla części nr 1):

Zdefiniowany w pkt III.2.3 ogłoszenia warunek udziału dotyczy „dostawy obejmującej swym zakresem dostarczenie i instalację urządzeń bezpieczeństwa będących przedmiotem zamówienia”. Przy czym, przedmiot zamówienia w pkt II.3. ppkt 1 (krótki opis dla części nr 1) zdefiniowany został bardzo ogólnie jako „dostawa licencji na system zaawansowanej ochrony stacji końcowych wraz niezbędnymi urządzeniami umożliwiającymi obsługę użytkowników”.

W związku z powyższym prosimy o doprecyzowanie jakie cechy musi posiadać system zaawansowanej ochrony stacji końcowych.

Biorąc pod uwagę specyfikę Zamawiającego jako bardzo ważnej instytucji dbającej o względy bezpieczeństwa i obronności kraju, prosimy o potwierdzenie niżej wymienionych minimalnych cech, jakie musi spełnić „dostawa obejmująca swym zakresem dostarczenie i instalację urządzeń bezpieczeństwa będących przedmiotem zamówienia”, aby spełniała warunek udziału w postępowaniu i była oceniona pozytywnie.

Dla bezpieczeństwa Zamawiającego, zgodnie z naszą profesjonalną wiedzą zaawansowane systemy ochrony stacji końcowych muszą posiadać co najmniej następujące cechy:

* zakres ochrony zapewnianej przez system: ochrona przed szkodliwymi plikami, plikami wykonywalnymi, dokumentami, URL (szkodliwe domeny), nieznanymi zagrożeniami poprzez dynamiczną i statyczną analizę plików i URL w środowisku typu sandbox,

* ochrona w postaci agentowej instalowana na stacjach końcowych i serwerach co najmniej Windows i Linux,

* zakres ochrony obejmującej urządzenia także poza siecią np. laptop,

* system ochrony w pełni zarządzalny, tj. administrowanie i raportowanie, przy pomocy centralnej konsoli zainstalowanej na serwerze,

* system nie może działać przy wykorzystaniu mechanizmów skanowa

Odpowiedź: System do zaawansowanej ochrony stacji końcowych musi posiadać co najmniej następujące cechy:

- ochrona w postaci agentów instalowanych na stacjach końcowych i serwerach,
- ochrona obejmująca urządzenia mobilne również poza siecią Straży Granicznej np. laptop,
- zakres ochrony zapewnianej przez system: ochrona przed szkodliwymi plikami, plikami wykonywalnymi, dokumentami, URL (szkodliwe domeny), nieznanymi zagrożeniami poprzez statyczną a dynamiczną analizę plików i URL w środowisku typu sandbox,
- możliwość pełnego zarządzania systemem ochrony, tzn. administrowanie i raportowanie przy pomocy centralnej konsoli zarządzającej zainstalowanej na serwerze zlokalizowanym w obiekcie Zamawiającego,

- system ochrony nie może działać przy wykorzystaniu mechanizmów skanowania i analizy ruchu sieciowego.

Pytanie nr 2: Pytanie dotyczy kwalifikacji technicznych (pkt III.2.3):

Zgodnie z treścią ogłoszenia przewidywane są dwie części zamówienia, natomiast został określony tylko jeden warunek. Czy powyższe oznacza, że dla każdej z części zamówienia ten warunek ma być spełniony osobno

Odpowiedź: Nie jest jeden łączny warunek dla obu części.

Odpowiedzi udzielone przez Zamawiającego stanowią integralną część Ogłoszenia o Zamówieniu i należy je uwzględnić podczas przygotowywania wniosku o dopuszczeniu do udziału w postępowaniu.

Z poważaniem

Liz RADCA
Zespołu Stanowisk Samodzielnych
Biura Finansów
Komendy Głównej Straży Granicznej
ppłk SG Marcin WOJCIECHOWSKI