KOMENDA GŁÓWNA POLICJI
BIURO FINANSÓW
WYDZIAŁ ZAMÓWIEŃ PUBLICZNYCH
ul. Domaniewska 36/38; 02-672 Warszawa; tel. 22 60 120 44; fax 22 60 118 57
zamowieniakgp@policja.gov.pl

Warszawa, ..14.. 09.2015 r.

L.dz. FZ-6725...../15

Do ubiegających się o udzielenie zamówienia

dot. postępowania pn: Świadczenie usługi ochrony infrastruktury operatora sieci OST112 przed atakami typu DoS i DDoS z sieci Internet przez okres 24 miesięcy – nr sprawy 146/BŁiI/15/TG

Zamawiający informuje, że działając zgodnie z treścią art. 38 ust. 2 i 4 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tj.: Dz. U. z 2013 r. poz. 907 z późn. zm. – ustawa Pzp.) przekazuje treść złożonych pytań oraz udzielonych odpowiedzi:

Pytanie nr 39:
(Doprecyzowanie odpowiedzi na pytanie nr 1 z ww. pisma). Czy zamawiający dopuszcza rozwiązanie, w których ruch przefiltrowany jest tylko do lokalizacji Warszawa, ul. Olszewska 6? Jeśli nie, jakie kryterium rozkładania ruchu na 2 docelowe lokalizacje ma być zastosowane?

Odpowiedź na pytanie nr 39:
Zamawiający informuje, że przypadku niedostępności lokalizacji Olszewska ruch powinien zostać przekierowany do Katowic.

Pytanie nr 40:
(Doprecyzowanie odpowiedzi na pytanie nr 7 z ww. pisma). Czy Zamawiający potwierdza, że w przypadku zestawienia transmisji poprzez PLIX, realizującej łącze do systemu zarządzania, odbierze ją na swoim istniejącym styku z PLIX?

Odpowiedź na pytanie nr 40:
Zamawiający informuje, że w przypadku dostępu do systemu zarządzania realizowanego przez Internet dostęp nie powinien być zależny od łącza do PLIX.

Pytanie nr 41:
(Doprecyzowanie odpowiedzi na pytanie nr 8 z ww. pisma). Czy Zamawiający potwierdza, że w przypadku zestawienia transmisji poprzez PLX, realizującej jednokierunkowe łącze na dosył ruchu przefiltrowanego, odbierze ją na swoim istniejącym styku z PLIX?

Odpowiedź na pytanie nr 41:

Zamawiający informuje, że dosył ruchu nie może być zależny od łącza do PLIX. System powinien umożliwiać dosył ruchu z wykorzystaniem co najmniej dwóch posiadanych łączy przez Zamawiającego.

Pytanie nr 42:

Czy dostęp do statystyk i panelu zarządzania dla klienta może być zrealizowany z wykorzystaniem tunelu IPSec? Jeżeli TAK to czy w obu lokalizacjach (lub innych lokalizacjach, które powinny mieć dostęp do tych informacji) jest możliwość zakończenia takiego tunelu? Moim zdaniem takie rozwiązanie daje wyższy poziom bezpieczeństwa niż https (nawet z WAF).

Odpowiedź na pytanie nr 42:

Zamawiający dopuszcza dostęp do panelu zarządzania i statystyk z wykorzystaniem IPSec.

Pytanie nr 43:

(Doprecyzowanie odpowiedzi na pytanie nr 10 z ww. pisma). Specyfika protokołu BGP nakazuje, aby Zamawiający na czas włączenia ochrony "on demand" w zewnętrznym Scrubbing Center zaprzestał rozgłaszania prefiksów /24 w BGP na swoich łączach podstawowych, inaczej sam ściągnie do siebie ruch pomijając system filtrowania Oferenta. Czy Zamawiający aktywując ochronę jednocześnie dokona rekonfiguracji BGP po swojej stronie w taki sposób, aby w Internecie zniknęły trasy do Zamawiającego inne niż obsługiwana przez Oferenta?

Odpowiedź na pytanie nr 43:

Tak, w opisanym przypadku Zamawiający zaprzestanie rozgłaszania prefiksu.

Pytanie nr 44:

Jakie interfejsy są niezbędne, aby podłączyć urządzenia monitorujące „inline" w sieć dostępową (łącza operatorskie/router Zamawiającego)?

Odpowiedź na pytanie nr 44:

Zamawiający informuje, że łącza T-Mobile zakończone są na routerze zamawiającego stykiem w standardzie 1000BASE-LH, łącze do PLIX zakończone jest stykiem w standardzie 1000BASE-S.

Pytanie nr 45:

Czy usługa ochrony infrastruktury ma przeciwdziałać również atakom aplikacyjnym DDoS?

Odpowiedź na pytanie nr 45:

Zamawiający informuje, że usługa ochrony infrastruktury ma zapobiegać również atakom aplikacyjnym.

Pytanie nr 46:

Czy Zamawiający może kopiować ruch przychodzący na interfejsie od operatora w Katowicach i przesyłać go swoim łączem Katowice-Warszawa na urządzenie Wykonawcy (monitorujące ruch przychodzący na łączach od operatorów w lokalizacji Zamawiającego w Warszawie)?

Odpowiedź na pytanie nr 46:

Zamawiający informuje, że nie będzie kopiował i przesyłał ruchu przychodzącego swoim łączem w relacji Katowice Warszawa, zamawiający może jedynie udostępnić statyki NetFlow z interfejsu na łączu do Internetu.

Jednocześnie Zamawiający informuje, że działając zgodnie z treścią art. 38 ust. 4 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tj.: Dz. U. z 2013 r. poz. 907 z późn. zm. – ustawa Pzp.) dokonuje zmiany treści Rozdziały XII SIWZ, który otrzymuje brzmienie:

„XII.MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT:

1. **<u>Miejsce i termin składania ofert:</u>**

1) Ofertę wraz ze wszystkimi wymaganymi oświadczeniami i dokumentami, należy umieścić w zamkniętej kopercie, zapieczętowanej w sposób gwarantujący zachowanie poufności jej treści oraz zabezpieczającej jej nienaruszalność do terminu otwarcia ofert.

2) Koperta powinna być zaadresowana w następujący sposób:

Komenda Główna Policji, Biuro Finansów
ul. Domaniewska 36/38 02-672 Warszawa
Świadczenie usługi ochrony infrastruktury operatora sieci OST112 przed atakami typu DoS i DDoS z sieci Internet przez okres 24 miesięcy
Przetarg nr 146/BŁiI/15/TG

Nie otwierać przed dniem 20.09.2015 r.

3) Koperta poza oznakowaniem jak wyżej powinna być opatrzona dokładną nazwą i adresem Wykonawcy.

4) Ofertę należy złożyć do **dnia 20.09.2015 r. do godz. 9:30** w Biurze Finansów KGP, 02-672 Warszawa, ul. Domaniewska 36/38, pokój 435, tel. 22 601 32 04, w godz. 8.30 – 15.30 (od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy).

5) Konsekwencje złożenia oferty niezgodnie z ww. opisem (np. potraktowanie oferty jako zwykłej korespondencji i nie dostarczenie jej na miejsce składania ofert w terminie określonym w SIWZ) ponosi Wykonawca.

6) Oferta złożona po terminie zostanie zwrócona Wykonawcy po upływie terminu przewidzianego na wniesienie odwołanie.

2. <u>Miejsce i tryb otwarcia ofert</u>

Publiczna sesja otwarcia ofert odbędzie się w siedzibie Zamawiającego w Warszawie przy ul. Domaniewskiej 36/38, **w dniu 20.09.2015 r. o godz. 10:00.**

3. <u>Zmiana i wycofanie oferty:</u>

1) Wykonawca może wprowadzić zmianę do treści złożonej oferty pod warunkiem, że Zamawiający otrzyma pisemne powiadomienie o wprowadzeniu zmiany przed terminem składania ofert. Zmiana do oferty musi być dokonana według zasad obowiązujących przy składaniu oferty, tj. musi być złożona w zamkniętej kopercie odpowiednio oznakowanej z dopiskiem „ZMIANA".

2) Koperty oznakowane dopiskiem „ZMIANA" zostaną otwarte przy otwieraniu oferty Wykonawcy, który wprowadził zmiany. Po stwierdzeniu poprawności procedury dokonania zmiany zawartość koperty zostanie dołączona do oferty.

3) Wykonawca ma prawo wycofać ofertę pod warunkiem, że Zamawiający otrzyma pisemne powiadomienie (oświadczenie) o wycofaniu oferty przed terminem składania ofert. Wycofanie oferty z postępowania nastąpi poprzez złożenie pisemnego powiadomienia (oświadczenia) w kopercie opatrzonej napisem „WYCOFANIE" - według takich samych zasad, jakie obowiązują przy wprowadzaniu zmian do oferty.

<u>UWAGA:</u>

Do składanego oświadczenia (zmiana lub wycofanie oferty) należy dołączyć stosowny dokument potwierdzający prawo osoby podpisującej oświadczenie do występowania w imieniu Wykonawcy.

Powyższe odpowiedzi oraz zmiany są wiążące dla Stron postępowania.

ZASTĘPCA NACZELNIKA
WYDZIAŁU ZAMÓWIEŃ PUBLICZNYCH
BIURA FINANSÓW
KOMENDY GŁÓWNEJ POLICJI
Anna ŁUCHCIŃSKA

wykonano w 1 egz.
opr./wyk. T.Gugała
tel. 72 119 86