Warszawa, 14.08.2014

Wydział Zamówień Publicznych
Komendy Stołecznej Policji
WZP -2964/14/2646/14

Dotyczy: postępowania prowadzonego w trybie przetargu nieograniczonego na „Świadczenie usług dostępu do Internetu" WZP – 2646/14/78/Ł

Wydział Zamówień Publicznych KSP, działając w imieniu Zamawiającego, zgodnie z art. 38 ust. 2 i ust. 4 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t.j. Dz. U. z 2013 r. , poz. 907 ze zm.), uprzejmie informuje o treści pytań zadanych przez Wykonawców i udzielonych przez Zamawiającego odpowiedziach oraz dokonanych zmianach w SIWZ:

Pytanie 1:
Zamawiający w pkt III ppkt 3 SIWZ wskazał, że wykonawca, na żądanie Zamawiającego, ma zapewnić świadczenie dodatkowej usługi w zakresie zabezpieczenie łącza Internetowego przed atakami DDOS i że będzie ona świadczona na podstawie odrębnej umowy. Prosimy o odpowiedź czy świadczenie w/w usługi w odrębnej umowie będzie odbywać się za wynagrodzeniem, które będzie niezależne od wynagrodzenia za świadczenie usługi dostępu do Internetu.

Pytanie nr 2:
Zgodnie z wymaganiem ujętym w rozdziale II, pkt. 3, wykonawca zobowiązany jest, na żądanie Zamawiającego do świadczenia dodatkowej usługi w zakresie zabezpieczenia łącza internetowego użytkownika przed atakami DDoS, czy cena oferty składanej w niniejszym postępowaniu, powinna uwzględniać również świadczenie dodatkowej usługi ochrony łącza przed atakami DDoS? Jeśli nie, czy Zamawiający przewiduje inne ograniczenie ceny usługi dodatkowej?

Odpowiedź na pytanie 1 i 2:
Zamawiający dokonuje zamiany zapisu SIWZ w:

1. Rozdziale II. PRZEDMIOT, TERMIN I MIEJSCE WYKONANIA ZAMÓWIENIA: pkt 3 otrzymuje brzmienie: *„Zamawiający zastrzega sobie możliwość skorzystania w okresie obowiązywania umowy z prawa opcji w zakresie usługi zabezpieczenia łącza internetowego użytkownika przed atakami DDoS. Skorzystanie przez Zamawiającego z prawa opcji odbędzie się poprzez złożenie Wykonawcy jednostronnego oświadczenia w formie zlecenia. Świadczenie usługi winno nastąpić w terminie nie przekraczającym 7 dni roboczych od dnia przesłania zlecenia. Zamawiający wymaga aby:*
   - *Rozwiązane powinno monitorować ruch w sposób ciągły (24/7/365), z ukierunkowaniem na wykrycie anomalii mogących skutkować wysyceniem łącza i w efekcie utratą ciągłości procesów biznesowych.*
   - *w trakcie mitygacji pakiety nie mogą być przekierowane poza teren Polski*
   - *usługa powinna zapewniać ochronę przed atakami o wolumenie*
   - *Monitoringiem i obsługą incydentów związanych z atakami DDoS musi zajmować się wyspecjalizowana jednostka organizacyjna działająca w trybie 24/7/365*
   - *Monitorowanie ruchu powinno być przeprowadzane przy wykorzystaniu technologii bazujących na przeplywach pakietów IP (ang.IP flow) takich jak np. NetFlow czy sFlow.*
   - *Informacje o wszystkich połączeniach do systemów usługowych Zamawiającego poprzez wykorzystanie protokołu typu NetFlow lub podobne*

- *usługa powinna zapewniać comiesięczny raport obejmujący: wykres ilustrujący wolumen ruchu do i z chronionej podsieci, lista alarmów, lista mityzacji*

- *system realizujący usługę powinien na podstawie danych historycznych wyznaczać oczekiwaną wartość ruchu do i od chronionej podsieci o danej porze dnia w danym dniu tygodnia.*

- *usługa powinna zapewniać odrzucanie lub przepuszczanie na bazie zdefiniowanych dla każdego z klientów filtrów operujących na informacjach w nagłówka warstwy 3-ciej i 4-tej modelu OSI*

- *Przełączanie ruchu Zamawiającego w przypadku ataku powinno być realizowane za pomocą protokołu BGP.*

- *Rozwiązanie powinno umożliwiać stosowanie szeregu technik w celu mityzacji ataków DDoS, takich jak co najmniej:*

    - *Blokada niedozwolonych zapytań http przy wykorzystaniu wyrażeń regularnych;*

    - *Blokada niedozwolonych zapytań DNS przy wykorzystaniu wyrażeń regularnych;*

    - *Wykrywanie i blokada ataków typu TCP SYN, TCP RST, TCP Null, ICMP, IP Null, IP Fragmented flood, ataków na protokoły poprzez eliminację źródeł które przekroczą zdefiniowany próg (bps, pps);*

    - *Geolokalizacja adresów IP, umożliwiająca blokadę ruchu pochodzącego z danego kraju bądź regionu geograficznego;*

    - *Dopuszczanie, blokada, lub ograniczenie pasma (policing) dla ruchu pochodzącego z krajów z którymi w normalnych warunkach Zamawiający nie utrzymuje stosunków handlowych;*

    - *Listy przepuszczające ruch z krytycznych serwisów i lokacji, lub blokujące spoofowane adresy oraz ruch obserwowany na niewłaściwych portach;*

    - *Listy przepuszczające ruch pochodzący ze znanych i zaakceptowanych lokalizacji, oraz blokujące ruch pochodzący od zainfekowanych hostów i serwerów będących pod kontrolą botnetów;*

    - *Monitorowanie podsieci i protokołów w celu identyfikacji ruchu o parametrach wyższych niż zdefiniowane;*

    - *Inspekcja ruchu w celu identyfikacji ataków przeprowadzanych na podatności payload;*

    - *Ochrona przed przepełnieniem tablicy stanu dla serwerów, firewall i urządzeń równoważących obciążenie;*

    - *Ochrona serwerów przed atakiem polegającym na podtrzymywaniu bezpodstawnie długiej sesji;*

    - *Ochrona przed atakami typu flash crowd poprzez ograniczenie ruchu do poziomu pozwalającego na normalne funkcjonowanie chronionego hosta;*

    - *Ochrona serwerów SIP poprzez przepuszczanie zapytań zgodnych z RFC oraz pochodzących z właściwych źródeł;*

    - *Ochrona serwerów web poprzez przepuszczanie zapytań http zgodnych z RFC oraz pochodzących z właściwych źródeł;*

- *Ochrona serwerów DNS przed atakami typu DNS reflection atack, cache poisoning, resource exhausion poprzez przepuszczanie zapytań DNS zgodnych z RFC oraz pochodzących z właściwych źródeł;*

- *Powinna istnieć możliwość zastosowania dodatkowych narzędzi (np. blackholing, niezależne blokowanie ruchu z adresów IP z zagranicy do atakowanego adresu) zwiększających pewność znacznego ograniczenia lub usunięcia wpływu ataku na usługi Zamawiającego,*

- *Rozwiązanie musi zapewniać dostęp do statystyk i panelu zarządzania dla klienta, w trybie do odczytu , w szczególności musi zapewniać:*

- *Dostęp do statystyk ruchu na podstawie Netflow, Jflow itd.*

- *Dostęp do raportów generowanych przez system*

- *Dostęp do listy wykrytych ataków*

- *Dostęp do listy akcji wykonanych w celu ograniczenia wpływu ataków - tryb oczyszczania*

- *Możliwość zapisywania raportów w formie PDF/XML z poziomy konsoli WebUl Dostęp do zarządzania powinien odbywać się szyfrowanym kanałem (np. HTTPS).*

- *Urządzenie zarządzające po stronie operatora musi być chronione rozwiązaniem typu WAF (Web Application Firewall).*

- *W ramach usługi konieczne jest zapewnienie całodobowej gotowości do podjęcia reakcji w 15 minut od wykrycia ataku.*

- *Konieczne jest niezwłoczne informowanie oraz raportowanie do Zamawiającego po każdym wykrytym ataku DDoS oraz ścisła współpraca pomiędzy zespołem Zamawiającego i scrubbing center.*

- *Należy dostarczać okresowe raporty na temat monitorowanego ruchu oraz ilości ataków DDoS przeprowadzonych na infrastrukturę.*

- *Usługa powinna być dostępna na poziomie SLA co najmniej 99.5% (downtime roczny: 3dni, miesięczny: 7h).*

- *Rozwiązanie musi zapewniać blokowania/ograniczanie ruchu na poziomie styku z operatorem - łącze do klienta musi być ograniczone lub oczyszczone z ruchu spowodowanego atakiem Dos*

- *Rozwiązanie powinno mieć możliwość integracji z urządzeniami ochrony DDoS po stronie klienta, zainstalowanym bezpośrednio na zakończeniu łącza po stronie klienta, w szczególności:*

- *Przekazywanie informacji o atakach wykrytych po stronie klienta*

- *o możliwość włączania trybu oczyszczania z poziomu konsoli zarządzającej urządzeniem po stronie klienta WebUl*

- *o możliwość automatycznego wymuszania trybu czyszczenia na podstawie informacji o ruchu i atakach wykrytych przez urządzenie klienta*

- *Ruch nie powinien wychodzić poza granice Polski*

- *Wielkości ruchu podlegającego ochronie DDOS na poziomie 50 Mbps."*

2. Rozdziale XII. MIEJSCE I TERMIN OTWARCIA OFERT:
   Pkt 3 otrzymuje brzmienie: *„Przed otwarciem ofert Zamawiający poda łączną kwotę, jaką zamierza przeznaczyć na sfinansowanie zamówienia w tym kwotę na zamówienie podstawowe i zamówienie w prawie opcji"*
3. Rozdziale XIV. OPIS KRYTERIÓW OCENY OFERT ORAZ SPOSOBU WYLICZENIA CENY:
Zamawiający dokonuje zmiany treści pkt 2 na następujący:

Cena oferty brutto w PLN stanowić będzie wartość wyliczoną wg. poniższego wzoru:

Co = (Czp x 0,8) + (Cpo x 0,2) gdzie:

Co – cena oferty.

Czp – cena zamówienia podstawowego stanowiąca sumę wartości wynikających z iloczynu zaoferowanej przez Wykonawcę miesięcznej opłaty za usługę dostępu do Internetu brutto w PLN (Podstawy Rozliczenia SLA) wskazanej w tabeli formularza ofertowego w poz. 1 w kol. 3 oraz ilości miesięcy świadczenia usługi wskazanej przez Zamawiającego w tabeli Formularza Ofertowego w kol. 4

Cpo – cena zamówienia w prawie opcji stanowić będzie wartość wynikającą z iloczynu zaoferowanej przez Wykonawcę miesięcznej opłaty za usługę zabezpieczenia łącza internetowego przed atakami DDOS w PLN wskazanej w poz. 2 w kolumnie 3 oraz ilości miesięcy świadczenia usługi wskazanej przez Zamawiającego w tabeli Formularza ofertowego w kol. 4.

Dodaje pkt 2a) który otrzymuje brzmienie: *Wykonawca ubiegający się o udzielenie niniejszego zamówienia może zaoferować opłatę miesięczną za usługę dostępu do Internetu nie wyższą niż 50% opłaty miesięcznej za usługę zabezpieczenia łącza internetowego przed atakami DDoS. W przypadku zaoferowania opłaty miesięcznej wyższej niż wskazana w zdaniu pierwszym, Zamawiający odrzuci ofertę na podstawie art. 89 ust. 1 pkt 2) ustawy „Zamawiający odrzuca ofertę, jeżeli jej treść nie odpowiada treści specyfikacji istotnych warunków zamówienia...."*

Pkt 3 otrzymuje brzmienie: *„W miesięcznej opłacie abonamentowej za usługę dostępu do Internetu Wykonawca uwzględni koszt:*

a) wykonania usługi, o której mowa w Rozdziale II pkt 2 SIWZ,

b) pozostałe koszty związane z wykonanie zamówienia w tym podatek VAT.

W miesięcznej opłacie abonamentowej za usługę zabezpieczenia łącza internetowego użytkownika przed atakami DDoS Wykonawca uwzględni koszt:

a) wykonania usługi, o której mowa w Rozdziale II pkt 3 SIWZ,

b) pozostałe koszty związane z wykonanie zamówienia w tym podatek VAT."

Pkt 4 otrzymuje brzmienie: *„Wskazana przez Wykonawcę miesięczna opłata abonamentowa brutto w PLN oraz wartość brutto usługi w PLN uwzględniająca stawkę podatku VAT, musi być podana w PLN cyfrowo z dokładnością do dwóch miejsc po przecinku."*

4. w Rozdziale XVII OGOLNE WARUNKI UMOWY:

§ 1 zmienia zapis ust. 5, który otrzymuje brzmienie: *Zamawiający zastrzega sobie możliwość skorzystania okresie obowiązywania umowy z prawa opcji w zakresie usługi zabezpieczenia łącza internetowego użytkownika przed atakami DDoS. Świadczenie usługi winno nastąpić w terminie nie przekraczającym 7 dni roboczych od dnia przesłania przez Zamawiającego jednostronnego pisemnego (dopuszczalna droga faksowa lub e-mail) oświadczenia woli w formie zleceń na numer faksu/adresu e-mail Wykonawcy wskazanego w § 3 ust. 2.*

§ 2 ust. 1 otrzymuje brzmienie:

„Strony ustalają:

a) wartość umowy w zamówieniu podstawowym na kwotę nie wyższą niż ..... brutto w PLN (zgodnie z ofertą Wykonawcy)

b) niezmienną w okresie obowiązywania umowy miesięczną opłatę abonamentową (podstawa Rozliczenia SLA) w wysokości .... brutto w PLN (zgodnie z ofertą Wykonawcy),

c) wartość umowy w prawie opcji nie wyższa niż .... brutto w PLN (zgodnie z ofertą Wykonawcy) oraz niezmienna w okresie obowiązywania umowy miesięczną opłatę abonamentową za usługę zabezpieczenia łącza internetowego użytkownika przez atakami DDoS w wysokości ..... brutto w PLN (zgodnie z ofertą Wykonawcy)."

§ 2 ust. 3 otrzymuje brzmienie:

Podstawą do wystawienia przez Wykonawcę faktury będzie:

a) sporządzony przez Wykonawcę i podpisany przez Strony Raport SLA za dany miesięczny okres rozliczeniowy (wzór Raportu SLA sanowi załącznik nr 3 do umowy),

b) sporządzony przez Wykonawcę i podpisany przez Strony protokół odbioru usługi zabezpieczenia łącza internetowego użytkownika przed atakami DDoS za miesięczny okres rozliczeniowy (wzór protokołu stanowi załącznik nr 5 do umowy)."

Do § 4 dodaje się ust. 3 w brzmieniu:

„Wykonawca gwarantuje, że usługa zabezpieczenia łącza internetowego przed atakami DDoS spełni nw. Warunki:

- *Rozwiązane powinno monitorować ruch w sposób ciągły (24/7/365), z ukierunkowaniem na wykrycie anomalii mogących skutkować wysyceniem łącza i w efekcie utratą ciągłości procesów biznesowych.*
- *w trakcie mitygacji pakiety nie mogą być przekierowane poza teren Polski*
- *usługa powinna zapewniać ochronę przed atakami o wolumenie*
- *Monitoringiem i obsługą incydentów związanych z atakami DDoS musi zajmować się wyspecjalizowana jednostka organizacyjna działająca w trybie 24/7/365*
- *Monitorowanie ruchu powinno być przeprowadzane przy wykorzystaniu technologii bazujących na przepływach pakietów IP (ang.IP flow) takich jak np. NetFlow czy sFlow.*
- *Informacje o wszystkich połączeniach do systemów usługowych Zamawiającego poprzez wykorzystanie protokołu typu NetFlow lub podobne*
- *usługa powinna zapewniać comiesięczny raport obejmujący: wykres ilustrujący wolumen ruchu do i z chronionej podsieci, lista alarmów, lista mitygacji*
- *system realizujący usługę powinien na podstawie danych historycznych wyznaczać oczekiwaną wartość ruchu do i od chronionej podsieci o danej porze dnia w danym dniu tygodnia.*
- *usługa powinna zapewniać odrzucanie lub przepuszczanie na bazie zdefiniowanych dla każdego z klientów filtrów operujących na informacjach w nagłówka warstwy 3-ciej i 4-tej modelu OSI*
- *Przełączanie ruchu Zamawiającego w przypadku ataku powinno być realizowane za pomocą protokołu BGP.*
- *Rozwiązanie powinno umożliwiać stosowanie szeregu technik w celu mityzacji ataków DDoS, takich jak co najmniej:*
  - *Blokada niedozwolonych zapytań http przy wykorzystaniu wyrażeń regularnych;*
  - *Blokada niedozwolonych zapytań DNS przy wykorzystaniu wyrażeń regularnych;*
  - *Wykrywanie i blokada ataków typu TCP SYN, TCP RST, TCP Null, ICMP, IP Null, IP Fragmented flood, ataków na protokoły poprzez eliminację źródeł które przekroczą zdefiniowany próg (bps, pps);*
  - *Geolokalizacja adresów IP, umożliwiająca blokadę ruchu pochodzącego z danego kraju bądź regionu geograficznego;*

- *Dopuszczanie, blokada, lub ograniczenie pasma (policing) dla ruchu pochodzącego z krajów z którymi w normalnych warunkach Zamawiający nie utrzymuje stosunków handlowych;*
- *Listy przepuszczające ruch z krytycznych serwisów i lokacji, lub blokujące spoofowane adresy oraz ruch obserwowany na niewłaściwych portach;*
- *Listy przepuszczające ruch pochodzący ze znanych i zaakceptowanych lokalizacji, oraz blokujące ruch pochodzący od zainfekowanych hostów i serwerów będących pod kontrolą botnetów;*
- *Monitorowanie podsieci i protokołów w celu identyfikacji ruchu o parametrach wyższych niż zdefiniowane;*
- *Inspekcja ruchu w celu identyfikacji ataków przeprowadzanych na podatności payload;*
- *Ochrona przed przepełnieniem tablicy stanu dla serwerów, firewall i urządzeń równoważących obciążenie;*
- *Ochrona serwerów przed atakiem polegającym na podtrzymywaniu bezpodstawnie długiej sesji;*
- *Ochrona przed atakami typu flash crowd poprzez ograniczenie ruchu do poziomu pozwalającego na normalne funkcjonowanie chronionego hosta;* ,
- *Ochrona serwerów SIP poprzez przepuszczanie zapytań zgodnych z RFC oraz pochodzących z właściwych źródeł;*
- *Ochrona serwerów web poprzez przepuszczanie zapytań http zgodnych z RFC oraz pochodzących z właściwych źródeł;*
- *Ochrona serwerów DNS przed atakami typu DNS reflection atack, cache poisoning, resource exhausion poprzez przepuszczanie zapytań DNS zgodnych z RFC oraz pochodzących z właściwych źródeł;*
- *Powinna istnieć możliwość zastosowania dodatkowych narzędzi (np. blackholing, niezależne blokowanie ruchu z adresów IP z zagranicy do atakowanego adresu) zwiększających pewność znacznego ograniczenia lub usunięcia wpływu ataku na usługi Zamawiającego,*
- *Rozwiązanie musi zapewniać dostęp do statystyk i panelu zarządzania dla klienta, w trybie do odczytu , w szczególności musi zapewniać:*
- *Dostęp do statystyk ruchu na podstawie Netflow, Jflow itd.*
- *Dostęp do raportów generowanych przez system*
- *Dostęp do listy wykrytych ataków*
- *Dostęp do listy akcji wykonanych w celu ograniczenia wpływu ataków - tryb oczyszczania*
- *Możliwość zapisywania raportów w formie PDF/XML z poziomy konsoli WebUl*
  Dostęp do zarządzania powinien odbywać się szyfrowanym kanałem (np. HTTPS).
- *Urządzenie zarządzające po stronie operatora musi być chronione rozwiązaniem typu WAF (Web Application Firewall).*

- *W ramach usługi konieczne jest zapewnienie całodobowej gotowości do podjęcia reakcji w 15 minut od wykrycia ataku.*
- *Konieczne jest niezwłoczne informowanie oraz raportowanie do Zamawiającego po każdym wykrytym ataku DDoS oraz ścisła współpraca pomiędzy zespołem Zamawiającego i scrubbing center.*
- *Należy dostarczać okresowe raporty na temat monitorowanego ruchu oraz ilości ataków DDoS przeprowadzonych na infrastrukturę.*

- *Usługa powinna być dostępna na poziomie SLA co najmniej 99.5% (downtime roczny: 3dni, miesięczny: 7h).*
  - *Rozwiązanie musi zapewniać blokowania/ograniczanie ruchu na poziomie styku z operatorem - łącze do klienta musi być ograniczone lub oczyszczone z ruchu spowodowanego atakiem DDoS*
  - *Rozwiązanie powinno mieć możliwość integracji z urządzeniami ochrony DDoS po stronie klienta, zainstalowanym bezpośrednio na zakończeniu łącza po stronie klienta, w szczególności:*
- *Przekazywanie informacji o atakach wykrytych po stronie klienta*
  - *o możliwość włączania trybu oczyszczania z poziomu konsoli zarządzającej urządzeniem po stronie klienta WebUI*
  - *o możliwość automatycznego wymuszania trybu czyszczenia na podstawie informacji o ruchu i atakach wykrytych przez urządzenie klienta*
  - *Ruch nie powinien wychodzić poza granice Polski*
  - *wielkości ruchu podlegającego ochronie DDoS na poziomie 50 Mbps."*

Do § 5 ust. 1 dodaje się lit. i) w brzmieniu:
1/30 miesięcznej opłaty abonamentowej, o której mowa w § 2 ust. 1 lit. c) za każdy dzień opóźnienia w dotrzymaniu terminu, o którym mowa w § 1 ust. 5.
Zmianie ulega § 5 ust. 2 , który otrzymuje brzmienie:
„Zapłata kary, o której mowa w ust. 1 lit. c) - i) nie zwalnia Wykonawcy z obowiązku wykonania umowy."
§ 8 ust. 5 lit. a) otrzymuje brzmienie:
„zmiany miesięcznej opłaty abonamentowej wskazanej w § 2 ust. 1 lit. b) i lit. c) w przypadku ustawowej zmiany podatku VAT, która wynosi (zgodnie z ofertą Wykonawcy),"
Zmianie ulega Wzór załącznik nr 1 do SIWZ, którego zmieniona wersja stanowi załącznik do niniejszego pisma.

Pytanie nr 3:
Zamawiający w wymaganiach w rozdziale II punkt 2 lit. i, określił poziom gwarancji SLA, czy Zamawiający określając parametry oczekuje ich spełnienia w ramach sieci wykonawcy?

Odpowiedź na pytanie nr 3:
Zamawiający oczekuje spełnienia warunków SLA w sieci wykonawcy – do połączenia pomiędzy interfejsem (interfejsami) Wykonawcy, udostępnionymi Zamawiającemu i interfejsem (interfejsami) urządzenia Zamawiającego.

Pytanie nr 4:
Zamawiający w rozdziale II pkt. 2 lit. b wskazał, iż oczekuje zapewnienia puli minimum 16 adresów IP z klasy publicznej. Adresy publiczne IP, które może zapewnić Wykonawca pochodzą z jego puli adresów PA. Jednocześnie w pkt. 2 lit. k Zamawiający wskazał, iż oczekuje wykreowania dla Zamawiającego routingu BGP. Wymagania te wzajemnie się wykluczają, czy Zamawiający może wyjaśnić wskazane wymagania? Czy Zamawiający dysponuje adresacją PI, która może zostać wykorzystana do routingu BGP?

Odpowiedź na pytanie nr 4:
Zamawiający dokonuje zmiany zapisu SIWZ w Rozdziale XVII Ogólne warunki umowy § 1 ust. 4 lit. k) oraz Rozdz. II Przedmiot, termin i miejsce wykonywania zamówienia pkt 2 lit. k) które otrzymują brzmienie: *„możliwość wykreowania dla Zamawiającego routingu BGP (w przypadku dysponowania przez Zamawiającego własną pulą adresową), co da możliwość Zamawiającemu zarządzania i tworzenia scenariuszy zarządzania ruchem IP na różnych dostępach do Internetu."*

Pytanie nr 5:
Zamawiający określając obowiązek uruchomienia dodatkowej usługi w zakresie zabezpieczenia łącza internetowego przed atakami DDoS nie określił oczekiwanych parametrów jakie będzie musiała spełnić ta usługa,

- czy usługa powinna monitorować ruch do i od chronionej podsieci w czasie rzeczywistym?
- czy usługa powinna zapewniać wykrywanie anomalii polegających na przekroczeniu wartości uważanych za normalne w ruchu Internetowym w szczególności pakietów TCP SYN, TCP RST, TCP Null, ICMP, IP Null, IP Fragmented, DNS?
- czy system realizujący usługę powinien na podstawie danych historycznych wyznaczać oczekiwaną wartość ruchu do i od chronionej podsieci o danej porze dnia w danym dniu tygodnia?
- czy usługa powinna zapewniać wykrywanie anomalii polegających na znaczącym przekroczeniu wolumenu ruchu w stosunku do wcześniej wyznaczonych wartości oczekiwanych ruchu?
- czy usługa powinna zapewniać ochronę przed atakami o wolumenie co najmniej 10Gb/sek?
- czy w trakcie mitygacji pakiety nie mogą być przekierowane poza teren Polski?
- czy usługa powinna zapewniać odrzucanie lub przepuszczanie na bazie zdefiniowanych dla każdego z klientów filtrów operujących na informacjach w nagłówka wartwy 3-ciej i 4-tej modelu OSI?
- czy usługa powinna chronić przed atakami ze „spoofowanymi" (udawanymi) adresami źródłowymi IP poprzez autentykację sesji TCP, zapytań DNS oraz zapytań HTTP?
- czy usługa powinna chronić przed atakami pochodzącym od sieci botnetowych (komputerów zainfekowanych w sposób umożliwiające zdalne sterowanie przez hackerów) poprzez filtrowanie na podstawie na bieżąco aktualizowanych sygnatur zawierających listę adresów IP?
- czy usługa powinna zapewniać comiesięczny raport obejmujący: wykres ilustrujący wolumen ruchu do i z chronionej podsieci, lista alarmów, lista mitygacji?

Odpowiedź na pytanie nr 5:
Zamawiający udzielił odpowiedzi na powyższe pytanie odpowiadając na pytanie nr 1 i nr 2.

Pytanie nr 6:
Czy Zamawiający przewiduje przeprowadzenie przed podpisaniem umowy na świadczenie usługi łącza internetowego, testów funkcjonalności usługi dodatkowej ochrony łącza internetowego przed atakami DDoS?

Odpowiedź na pytanie nr 6:
Zamawiający nie przewiduje przeprowadzenie przed podpisaniem umowy na świadczenie usługi łącza internetowego, testów funkcjonalności usługi dodatkowej ochrony łącza internetowego przed atakami DDoS

Pytanie nr 7:
Wykonawca zwraca się o potwierdzenie, że w przypadku wyboru oferty Wykonawcy prowadzącego działalność gospodarczą w formie spółki akcyjnej, część komparycyjna Umów poświęcona Wykonawcy będzie obejmować wszelkie dane wymagane przez art. 374 § 1 KSH.

Odpowiedź na pytanie nr 7:
Tak, Zamawiający potwierdza, że w przypadku wyboru oferty Wykonawcy prowadzącego działalność gospodarczą w formie spółki akcyjnej, część komparycyjna umowy poświęcona Wykonawcy będzie obejmować wszelkie dane wymagane przez art. 374 § 1 KSH.

Pytanie nr 8:
Zgodnie z treścią § 2 ust, 6 Umowy „Zamawiający dokona zapłaty za świadczona w danym miesiącu usługę w terminie 30 dni, licząc od daty otrzymania od Wykonawcy faktury. Za dzień zapłaty uznaje się datę obciążenia rachunku Zamawiającego."
Zauważyć należy, iż takie określenie terminu płatności nie pozwala ustalić daty w jakiej Zamawiający będzie zobowiązany do zapłaty należnej Wykonawcy kwoty za świadczone usługi telekomunikacyjne. W takim stanie rzeczy takie ukształtowanie warunków umowy naraża Wykonawcę na istotne niebezpieczeństwo błędnego określenia terminów, co w konsekwencji doprowadzić może do nieprawidłowego wyliczenia kwot należnych podatków. Wobec powyższego rozwiązaniem takiej sytuacji może być wyłącznie uzależnienie terminu płatności od daty wystawienie faktury VAT (z punktu widzenia Wykonawcy jest to data pewna), nie zaś od daty otrzymania przez Zamawiającego. W związku z powyższym zwracam się z pytaniem, czy Zamawiający dopuszcza możliwość modyfikacji treści § 2 ust. 6 Umowy poprzez zastąpienie wyrazu „otrzymania" wyrazem „wystawienia"?

Odpowiedź na pytanie nr 8:
Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 9:
Wykonawca zwraca z pytaniem czy Zamawiający wyraża zgodę na umieszczenie w § 5 Umowy zapisu, zgodnie z którym:
a) „Całkowita suma kar umownych naliczonych na podstawie § 5 ust. 1 pkt c, d, e, f ,g ,h Umowy nie przekroczy 15% wartości łącznego wynagrodzenia brutto określonego w § 2 ust. 1 Umowy"?
b) Łączna suma kar umownych, bonifikat, odszkodowań naliczonych w danym miesiącu na podstawie § 5 ust.1 pkt c ,d ,e ,f ,g ,h Umowy nie przekroczy sumy opłat należnych Wykonawcy za świadczenie usług w danym miesiącu"?
Na wypadek, gdyby Zamawiający nie uwzględnił ograniczenia całkowitej wysokości kar umownych do 15% kwoty wartości umowy, Wykonawca wraca się o rozważenie innej wartości procentowej, gdyż wskazanie maksymalnej wysokości kar umownych umożliwi oszacowanie ryzyka kontraktowego związanego z karami i uwzględnienie go w treści oferty.

Odpowiedź na pytanie nr 9:
Zamawiający podtrzymuje zapisy SIWZ

Pytanie nr 10:
W treści § 5 ust. 5 Umowy Zamawiający przewidział dla siebie prawo potrącenia kar umownych z wynagrodzenia (faktury), Niczym nieograniczone jednostronne prawo naliczenia kar umownych i potrącenia ich przez Zamawiającego z należnego Wykonawcy wynagrodzenia godzi nie tylko w interes Wykonawcy ale także uniemożliwia mu podjęcie próby zbadania, czy naliczona kara umowna potrącona została naliczona prawidłowo i w odpowiedniej wysokości. Nadto, stwarzając możliwość pozbawienia Wykonawcy efektywnego wynagrodzenia za spełnione świadczenie bez żadnej kontroli czy to Wykonawcy czy sądu, może ono być uznane za nadużycie prawa skutkujące nieważność tegoż postanowienia na podstawie art. 58 § 2 k, c, w zw. z art. 139 ust. 1 p.z.p.
W związku z powyższym, z uwagi na nierówne ukształtowanie praw stron umowy, prosimy o wyjaśnienie czy Zamawiający dopuszcza możliwość zmodyfikowania zapisów Umowy poprzez

modyfikację zapisu poprzez dodanie do treści § 5 ust. 5 Umowy słów *„po przeprowadzeniu postępowania potwierdzającego zasadność naliczenia kar umownych "*?

Odpowiedź na pytanie nr 10:
Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 11:
Czy Zamawiający wyraża zgodę aby Regulamin świadczenia usług stanowił załącznik do umowy i obowiązywał w zakresie niesprzecznym i nieuregulowanym w umowie?

Odpowiedź na pytanie nr 11:
Zamawiający wyraża zgodę aby regulamin świadczenia usług stanowił załącznik do umowy. W związku z powyższym Zamawiający zmienia zapisy SIWZ:

1) W Rozdziale XV INFORMACJE O FORMALNOSCIACH JAKIE POWINNY ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY:
   dodaje się pkt 4 w brzmieniu: *„Przed podpisaniem umowy Wykonawca dostarczy Regulamin świadczenia usług, który będzie stanowił załącznik nr 6 do umowy."*
2) Rozdział XVII OGÓLNE WARUNKI UMOWY:
   § 9 ust. 3 otrzymuje brzmienie: *W sprawach nieuregulowanych niniejszą umową stosuje się przepisy: ustawy Prawo zamówień publicznych, Kodeksu cywilnego, Prawa telekomunikacyjnego oraz zapisy Regulaminu świadczenia usług, stanowiącego Załącznik Nr 6 • do umowy, w zakresie nieuregulowanym w umowie oraz powołanymi wcześniej aktami i dokumentami. W przypadku rozbieżności pomiędzy zapisami Regulaminu, a zapisami umowy pierwszeństwo maja zapisy zawarte w umowie. "*

Ponadto Zamawiający zmienia zapis:

1) Rozdz. X pkt 2, który otrzymuje brzmienie: **„Termin składania ofert upływa w dniu 21.08.2014r. godz. 12:00"**,
2) Rozdz. XII pkt 1, który otrzymuje brzmienie: **„Otwarcie złożonych ofert nastąpi w dniu 21.08.2014r. godz. 13:00 w siedzibie Zamawiającego – Komenda Stołeczna Policji, ul. Nowolipie 2, 00-150 Warszawa"**

Zmiany do SIWZ należy traktować wiążąco dla Stron.

NACZELNIK
Wydziału Zamówień Publicznych
Komendy Stołecznej Policji
kom. Halina ZONKO

Opr. Alicja Wielęgowska – Niepostyn (tel. 226036543)

Wzór – Załącznik nr 1 do SIWZ

OFERTA WYKONAWCY

Pełna nazwaWykonawcy:_____

Adres:_____

Nr telefonu i faksu, adres e-mail_____

Osoba/osoby uprawnione do reprezentacji, w tym do podpisania umowy _____

Przystępując do postępowania o udzielenie zamówienia prowadzonego w trybie przetargu nieograniczonego na zestawienie, uruchomienie i obsługę przewodowego łącza dostępowego do sieci Internet (Numer sprawy: WZP- 2646/14/78/Ł)

I. Oferujemy wykonanie przedmiotu zamówienia, za:

L.p.	Rodzaj usługi	Miesięczna opłata *	Okres świadczenia usługi (w miesiącach)	Wartość brutto usługi * (kol. 3x kol.4)
1	2	3	4	5
1	dostęp do Internetu (podstawa rozliczenia SLA)		**12**	
2	Zabezpieczenie łącza internetowego przed atakami DDOS		**12**	

Stawka podatku VAT wynosi .....%**

II. Oświadczamy, że:

1. Dysponujemy urządzeniami końcowymi, które zainstalujemy w Komendzie Stołecznej Policji, ul. Nowolipie 2, 00-150 Warszawa i mediami transmisyjnych, w oparciu o które będziemy świadczyć usługę objętą niniejszym postępowaniem, wskazanymi przez nas w załączniku nr .....** do oferty.

2. Zobowiązujemy się do wykonania zamówienia w zakresie:

   a) zestawienia i uruchomienia łącza dostępowego - w terminie do dnia **12.09.2014r.**
   b) obsługi i serwisowania łącza dostępowego – przez okres **12 miesięcy od** daty podpisania protokołu odbioru zestawienia i uruchomienia łącza dostępowego do Internetu,
   c) na zlecenie Zamawiającego w terminie do 7 dni roboczych uruchomić usługę zabezpieczenia łącza internetowego użytkownika przed atakami DDOS.

3. Zapewnimy możliwość całodobowego (7 dni w tygodniu) zgłaszania awarii i nieprawidłowości w funkcjonowaniu łącza dostępowego oraz całodobowy (7 dni w tygodniu) dostęp telefoniczny i e-mail do Biura Obsługi Klienta.
4. Zapoznaliśmy się z postanowieniami zawartymi w SIWZ i nie wnosimy do nich zastrzeżeń oraz z dobyliśmy konieczne informacje potrzebne do właściwego przygotowania oferty.
5. Zawarte w Rozdziale XVII SIWZ Ogólne warunki umowy zostały przez nas zaakceptowane i w przypadku wyboru naszej oferty zobowiązujemy się do zawarcia umowy na warunkach tam określonych w miejscu i terminie wskazanym przez Zamawiającego.

6. Uważamy się za związanych niniejsza ofertą na czas wskazany w SIWZ tj. 30 dni od upływu terminu składania ofert.
7. Zobowiązujemy się do zapewnienia możliwości odbierania wszelkiej korespondencji związanej z prowadzonym postępowaniem przez całą dobę na numer faksu/e-maila wskazanych w pkt III ppkt1. **W przypadku braku możliwości przekazania korespondencji - Zamawiający ma prawo uznać, iż powzięliśmy wiadomość o okolicznościach opisanych w tej korespondencji w dniu zamieszczenia jej treści na stronie internetowej Zamawiającego.**
8. Będziemy niezwłocznie potwierdzać fakt otrzymania wszelkiej korespondencji od Zamawiającego na nr faksu wskazany w pkt 5 Rozdz. I SIWZ. W przypadku braku potwierdzenia faktu otrzymania korespondencji Zamawiający uzna, iż Wykonawca zapoznał się z treścią dokumentu w dniu jego przesłania przez Zamawiającego.

III. Informujemy, że:

1. Awarie i nieprawidłowości w funkcjonowaniu łącza dostępowego/zlecenia należy zgłaszać na adres:
   .....**
   nr faksu: .....**, nr telefonu .....**, e-mail ....., lub do Biura Obsługi Klienta, nr tel. .....** nr faksu .....** e- mail ..... **
2. Osoba odpowiedzialna za realizację umowy .....** tel. .....**
3. Usługa wykonana będzie własnymi siłami/z pomocą Podwykonawcy***, który wykonywać będzie część zamówienia obejmującą .....

DATA: **PODPIS I PIECZĘĆ WYKONAWCY**

Uwaga:

* należy z dokładnością do dwóch miejsc po przecinku

** należy wpisać

*** niepotrzebne skreślić - jeżeli Wykonawca nie dokona skreślenia i nie wypełni pkt III ppkt. 2, Zamawiający uzna, że Wykonawca nie zamierza powierzyć części zamówienia Podwykonawcom