Warszawa, dnia 27.04.2018 r.

Nr pisma: NA/370/AZ /124/2018

Do Wykonawców
Strona internetowa Zamawiającego
www.imgw.pl

Dotyczy: postępowania o udzielenie zamówienia publicznego na wykonanie zadania pn.: ***„Dostawa, wdrożenie, migracja z obecnych rozwiązań oraz świadczenie usługi utrzymania w pracy operacyjnej łączy internetowych, routerów brzegowych, systemu zabezpieczeń sieci (Firewall) oraz systemu ochrony przed atakami DDos dla IMGW-PIB”,*** *oznaczenie sprawy* AZ/5/PN/U/AI/um.172,um.173,um.174/18

Wyjaśnienia i zmiany treści
Specyfikacji Istotnych warunków zamówienia

W dniu 19 kwietnia 2018 r. do Zamawiającego wpłynęły drogą elektroniczną wnioski o wyjaśnienie treści Specyfikacji Istotnych Warunków Zamówienia w postępowaniu o udzielenie zamówienia publicznego na wykonanie w/w zadania, zwanej dalej w skrócie SIWZ. W odpowiedzi na otrzymane wnioski, Zamawiający, działając na podstawie art. 38 ust.1 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (tj.: Dz. U. z 2017 r., poz. 1579 ze zm.), zwanej dalej ustawą Pzp, wyjaśnia, co następuje.

Pytanie nr 1
OPZ punkt II i III
Czy urządzenia (routery, firewall-e), które mają być dostarczone w ramach przetargu muszą być fabrycznie nowe?
Odpowiedź:
Zamawiający nie ma w tym zakresie wymagań. Zamawiający dla dostarczonych urządzeń ma wymagania funkcjonalne określone w Opisie przedmiotu zamówienia stanowiącym załącznik nr 1 do SIWZ (dalej OPZ).

Pytanie nr 2
OPZ punkt II i III
Czy urządzenia, które mają być dostarczone w ramach przetargu po zakończeniu umowy pozostają własnością Wykonawcy czy mają być odsprzedane Zamawiającemu?
Odpowiedź:
Po zakończeniu umowy, urządzenia pozostaną własnością Wykonawcy.

Pytanie nr 3
OPZ punkt III, FZ 01-10
Czy zamawiający dopuszcza dostawę systemu do Zarządzania i monitorowania Systemem Zabezpieczeń w formie wirtualnego systemu, jeśli tak to czy zamawiający udostępni odpowiednie zasoby do zainstalowania wirtualnego systemu zarządzania i monitoringu?
Odpowiedź:
Tak, Zamawiający umożliwi instalację systemu do Zarządzania i monitorowania Systemem Zabezpieczeń w środowisku wirtualnym Zamawiającego. Zamawiający udostępni na tą instalację odpowiednie zasoby. Realizacja usługi zgodnie z opisem w pkt III, FZ 01-10 OPZ.

Pytanie nr 4
OPZ punkt I, LI 06
Czy minimalny poziom czystego ruchu chronionego usługą DDoS ma być równy z pasmem łącza internetowego czyli 1 Gb/s ?

INSTYTUT METEOROLOGII I GOSPODARKI WODNEJ
Państwowy Instytut Badawczy
01-673 Warszawa, ul. Podleśna 61, telefon: (+48) 22-56-94-301, fax: (+48) 22-834-18-01, e-mail: imgw@imgw.pl
KONTO: Bank Zachodni WBK S.A. XIV Oddział w Warszawie 54 1090 1014 0000 0000 0301 4206
Regon: 000080507, NIP: 525-000-88-09

Odpowiedź:
Usługa DDoS powinna umożliwiać ochronę czystego ruchu o paśmie do 1Gb/s, zgodnie z opisem w pkt. I, LI01 OPZ.

Pytania dotyczą wyłącznie fragmentu Załącznika nr 1 do SIWZ (strona 2-3 OPZ; LI 06) - czyli poziomu świadczenia usługi ochrony przed atakami DDoS.

Pytanie nr 5
Jaka jest konkretna liczba aplikacji internetowych (stron www), które Zamawiający planuje podłączyć do systemu ochrony przed atakami DDoS wg określonych w OPZ wymagań? Jeśli nie jest możliwe określenie dokładnej liczby aplikacji www ze względu na nieprzewidywalny rozwój organizacji na przestrzeni 4 lat, to uprzejmie proszę o szacunkowe określenie takie jak na przykład: do 10-15 aplikacji www.
Odpowiedź:
Zamawiający planuje, że wszystkich aplikacji www przed zakończeniem umowy nie będzie więcej niż 35-40. Zamawiający zastrzega jednak, że usługą mają być chronione wszystkie aplikacje sieciowe uruchomione na adresacji IP PI Zamawiającego, wskazanej w pkt I, LI 03 OPZ.

Pytanie nr 6
Jaki jest szacowany średni dzienny ruch przychodzący w skali miesiąca na stronach www, które mają być podłączone do systemu ochrony przed atakami DDoS?
Odpowiedź:
Usługa DDoS powinna umożliwiać ochronę czystego ruchu o paśmie do 1Gb/s.

Pytanie nr 7
Zamawiający określił swoje wymaganie "System musi zapewniać możliwość filtrowania ataków o wielkości przynajmniej 10 Gbps". Ochronę jakich maksymalnych ataków DDoS w Gbps ma gwarantować system (np. do 30/40/50 Gbps)? Określenie wyłącznie minimalnego poziomu ataków nie jest wystarczającym parametrem do przygotowania oferty.
Odpowiedź:
W tym zapisie Zamawiający określił maksymalny poziom ataku. Zapis ten należy rozumieć "System musi zapewniać możliwość filtrowania ataków o wielkości przynajmniej do 10 Gbps ....".

Pytanie nr 8
Zamawiający określił czas reakcji na zaistniałe zdarzenie lub zgłoszenie (SLA) na 15 min. Jakiego dokładnego czasu realizacji zgłoszenia lub zdarzenia oczekuje Zamawiający (czyli faktycznego np. usunięcia zgłoszonej awarii, lub błędu)? Pytamy o parametr, który bardzo istotnie wpłynie na poziom świadczenia usługi. Wykonawca może w trakcie świadczenia usługi zareagować na zaistniałe zdarzenie w 15 min zgodnie z obecnym zapisem OPZ, jednak może też potencjalnie wydłużać czas naprawy (przez brak jego określenia w OPZ) ze szkodą dla Zamawiającego.
Odpowiedź:
Zamawiający opisany w tym punkcie czas reakcji rozumie jako maksymalny czas od rozpoznania przez Wykonawcę (jego systemy) lub od zgłoszenia przez Zamawiającego ataku, do jego całkowitego zablokowania. Po czasie tym usługi Zamawiającego dla użytkowników, których zasoby nie biorą udziału w ataku będą dostępne – zgodnie z pkt I, LI 06 OPZ oraz §5 ust 5 wzoru umowy.

Pytanie nr 9
Czy Zamawiający w ramach usługi antyDDoS oczekuje także ochrony przed atakami typu: sql injection, xss, remote file inclusion, local file inclusion, remote code excecution, local code excecution? Są to ataki, które bywają obecnie wykorzystywane równolegle (w tym samym czasie) co zagrożenia wymienione w OPZ, zwiększając prawdopodobieństwo wyrządzenia szkód zaatakowanej organizacji.
Odpowiedź:
Nie.

Pytanie nr 10
Czy w ramach usługi antyDDoS ma być terminowany protokół HTTPS?

Odpowiedź:
Nie.

Pytanie nr 11
Czy Zamawiający oczekuje możliwość modyfikacji regułek w ramach usługi ochrony antyDDOS?
Odpowiedź:
Nie.

Pytanie nr 12
Czy system ochrony przed atakami hakerskimi ma posiadać API?
Odpowiedź:
Nie.

Pytanie nr 13
Czy Zamawiający oczekuje dostępu do interfejsu GUI z monitoringiem incydentów?
Odpowiedź:
Zamawiający wymaga automatycznego tworzenia i przesyłania raportów po każdej mitygacji/obronie dla ataku przekraczającego 100Mbps i zbiorczy raport miesięczny dostarczany Zamawiającemu. Funkcjonalności te mogą być realizowane za pomocą GUI udostępnionego Zamawiającemu przez Wykonawcę. Realizacja usługi zgodnie z opisem w pkt I, LI 06 OPZ.

Pytanie nr 14
Czy Zamawiający oczekuje wyświetlania strony zastępczej w momencie wystąpienia błędów lub niedostępności serwera aplikacji?
Odpowiedź:
Nie.

Pytanie nr 15
SIWZ, Roz. III, OPZ, 2. 1)
SIWZ, Zał.1, OPZ, I LI03
Czy możemy z góry określić maksymalną ilość (pulę) adresów, którą Zamawiający potencjalnie estymuje jako odpowiednią ?
Odpowiedź:
Zamawiający nie widzi potrzeby przydzielania dodatkowych adresów Zamawiającemu, jednak zależy to również od sposobu realizacji połączenia do Internetu. Jeżeli Wykonawca uzna, że będą potrzebne dodatkowe adresy, np. dla sieci połączeniowej, między sieciami Zamawiającego a sieciami Wykonawcy dostarczy niezbędną minimalną pulę takich adresów.

Pytanie nr 16
SIWZ, Roz. III, OPZ, 2. 2)
Czy możemy prosić o nazwy producentów (modele) aktualnie wykorzystywanych routerów ? Chcemy upewnić się iż konfiguracja będzie możliwa do zmigrowania na planowany przez Wykonawcę sprzęt (nie zawsze jest to możliwe z racji specyficznych protokołów stosowanych przez niektórych producentów). Jeśli jest możliwość to prosimy o przesłanie listy uruchomionych/wymaganych funkcjonalności/protokołów.
Odpowiedź:
Zamawiający wykorzystuje obecnie następujące routery

- Warszawa: 2x CISCO - 3925 (C3900-SPE200/K9)
- Kraków: CISCO - 3825 (C3825-SPSERVICESK9-M)
- Gdynia: CISCO - 2821 (C2800NM-ADVSECURITYK9-M)

Pytanie nr 17
SIWZ, Roz. III, OPZ 12. 3)
SIWZ, Zał. 9, Umowa, Par.5, pkt. 8
Czy raport może być dystrybuowany poprzez panel www do którego Zamawiający uzyska bezpieczny dostęp (dedykowany login, hasło) ?

Odpowiedź:
Tak, Zamawiający uzna raport dostarczony w przedstawionej formie – poprzez panel www.

Pytanie nr 18
SIWZ, Zał.1, OPZ, I LI02
Czy Zamawiający dysponuje bezpiecznymi, niezawodnymi połączeniami warstwy Ethernet pomiędzy lokalizacjami Warszawa, Gdynia, Kraków które można wykorzystać celem ustanowienia komunikacji BGP pomiędzy routerami ? Jeśli nie to w jaki inny sposób Zamawiający zamierza utrzymywać komunikację prywatną pomiędzy ww. lokalizacjami ?
Odpowiedź:
Tak. Zamawiający posiada wewnętrzną sieć z routingiem OSPF.

Pytanie nr 19
SIWZ, Zał.1, OPZ, I LI05
„... w zależności od adresu sieci..."Łącząc wymaganie lokalnego wyjścia do Internetu oraz informację o zadysponowaniu publiczną klasą adresową IP /24 (LI03) informujemy iż rynkowo niemożliwe jest lokalne wychodzenie ruchu albowiem jedna rozgłoszona klasa /24 nie jest możliwa do większej granulacji gdyż zwyczajowo Operatorzy „obcinają" podziały klas mniejszych niż /24. Inaczej mówiąc jedyny scenariusz jaki wydaje się możliwy do realizacji to wychodzenie (i powracanie) ruchu z każdej lokalizacji poprzez jedno z łącz na zasadzie „albo-albo" (Warszawa, Gdynia, Kraków) a nie poprzez „balansowanie ruchu" pomiędzy powyższymi lokalizacjami.
Odpowiedź:
Zamawiający zdaje sobie z tego sprawę, że usługi sieciowe dla których adresy będą w sieci Zamawiającego (91.220.17.0/24) mogą być widocznie jedynie na jednym łączu. Zamawiający wykorzystuje do wyjścia użytkowników do Internetu dodatkowe adresacje udostępnione przez poszczególnych dostawców Internetu w Krakowie (Cyfronet) i Gdyni (TASK).

Pytanie nr 20
SIWZ, Zał.1, OPZ, II RO07
HSRP jest właścicielskim protokołem firmy Cisco, prosimy o informację iż ten sprzęt ma być użyty do realizacji zamówienia.
Odpowiedź:
Zamawiający w OPZ umiesił wymaganie RO06 brzmiące: „Routery będą wspierały protokół HSRP i/lub VRRP". Zdaniem Zamawiającego zapis taki nie wymusza zaproponowania urządzeń z obsługą protokołu HSRP, Wykonawca może zaproponować urządzenia obsługujące tylko protokół VRRP. Zamawiający nie wymusza użycia routerów firmy CISCO.

Pytanie nr 21
SIWZ, Zał.1, OPZ, V SI01
Czy słusznym jest domniemanie iż Wykonawca po udanym Wdrożeniu nie będzie odpowiadał za konfigurację routerów i firewalli a na czas kontraktu (48 miesięcy) reagował jedynie na zgłoszenia dot. Awarii sprzętowych ?
Odpowiedź:
Wykonawca nie będzie odpowiadał za konfigurację routerów i firewalli po udanym wdrożeniu natomiast w okresie obowiązywania umowy (48 miesięcy) Wykonawca zobowiązany jest do świadczenia usługi zgodnie z parametrami jakości (SLA) określonymi w OPZ i w § 5 umowy.

Pytanie nr 22
SIWZ, Zał. 9, Umowa, Par.1, pkt. 2,3
Czy Zamawiający dysponuje miejscem w szafach telekomunikacyjnych aby umieścić sprzęt (router + firewall) ? Dla lokalizacji warszawskiej będzie to ok. 6-8U, dla gdyńskiej i krakowskiej będzie to 4-6U. Jakim zasilaniem (AC czy DC) dysponuje w ww. szafach Zamawiający oraz czy istnieje możliwość użycia dwóch niezależnych linii energetycznych ?
Odpowiedź:
Tak. Dodatkowo w każdej lokalizacji istnieją niezależne dwa źródła zasilania AC 230V.

Pytanie nr 23
SIWZ, Zał. 9, Umowa Par.2, pkt. 5.
Prosimy o podanie parametrów (techniczno-konfiguracyjnych) łącz do których ma odnosić się kompatybilność łączy zapasowych.
Odpowiedź:
Zamawiający przez termin kompatybilność w tym zapisie, rozumie spełnienie zapisu LI02 z OPZ, czyli:
„ Wykonawca wspólnie z Zamawiającym uzgodnią w jaki sposób łącza internetowe będą się wzajemnie zastępowały. Zamawiający posiada 2 dodatkowe punkty styku z Internetem w Krakowie i Gdyni, przyznaną przestrzeń adresową Provider Independent (PI) oraz Autonomous System Number (ASN).

W związku z powyższym, Zamawiający, działając na podstawie art. 38 ust. 4 ustawy Pzp, dokonuje poniżej wskazanych zmian treści SIWZ – Wzoru umowy stanowiącego załącznik nr 9 do SIWZ.

W § 4 Wzoru umowy dodaje się ust. 8 o następującym brzmieniu:

„Wykonawca oświadcza, że urządzenia (Routery i Firewall) dostarczone w ramach Umowy są zgodne z wymaganiami funkcjonalnymi zawartymi w OPZ.”.

Zapis zawarty w § 5 ust. 5 Wzoru umowy w dotychczasowym brzmieniu zastępuje się zapisem o następującym brzmieniu:
„Czas reakcji na zgłoszenie dotyczące wykrycia ataku DDos wyniesie 15 min (zgodnie z OPZ).”.

Powyższe wyjaśnienia i zmiany stanowią integralną część SIWZ i są wiążące dla wszystkich Wykonawców. Tym samym, Wykonawcy są zobowiązani uwzględnić je, składając oferty w postępowaniu o udzielenie zamówienia publicznego na wykonanie w/w zadania.

Wzór umowy o treści ujednoliconej w związku z powyższymi zmianami stanowi załącznik do niniejszego pisma.

Pozostałe zapisy SIWZ nie ulegają zmianie. Termin składania ofert nie ulega zmianie.

Zamawiający zwraca się z prośbą o niezwłoczne potwierdzenie faktu otrzymania niniejszego pisma.

Z poważaniem,
ZASTĘPCA DYREKTORA
ds. ORGANIZACYJNYCH
Joanna Szczepańska

Załącznik:
Wzór umowy po zmianie - Załącznik nr 9 do SIWZ