Załącznik do Zapytania o wycenę szacunkową

Szczegółowy opis przedmiotu zamówienia

Świadczenie usługi dostępu do sieci Internet i usługi AntyDDoS

1. Definicje:

Określenia użyte w niniejszym dokumencie mają następujące znaczenie:

1) **Usługa** – usługa dostępu do sieci Internet wraz z usługą AntyDDoS świadczona w danej Lokalizacji;
2) **Aktywacja** – data uruchomienia Usługi w danej Lokalizacji, potwierdzona protokołem odbioru;
3) **Awaria** – powstałe z przyczyn nie leżących po stronie Zamawiającego uszkodzenie lub przerwa w transmisji w sieci Wykonawcy, uniemożliwiające korzystanie przez Zamawiającego z usługi w pełnym zakresie i z zachowaniem wymaganej przepustowości;
4) **Lokalizacja I** – ul. Chmielna 69, 00-801 Warszawa, siedziba Narodowego Centrum Badań i Rozwoju (NCBR);
5) **Lokalizacja II** – ul. Szlachecka 49, 03-259 Warszawa, Data Center T-Mobile;
6) **Łącze** – łącze światłowodowe symetryczne o gwarantowanej przepustowości nie mniejszej niż 1 Gbps/1 Gbps;
7) **Dni robocze** – dni od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy na terenie Rzeczypospolitej Polskiej.

2. Przedmiot zamówienia:

1) **Część I -** świadczenie usługi dostępu do sieci Internet i usługi AntyDDoS w Lokalizacji I dla Zamawiającego, przez okres 36 miesięcy od dnia Aktywacji;
2) **Część II -** świadczenie usługi dostępu do sieci Internet i usługi AntyDDoS w Lokalizacji II dla Zamawiającego, przez okres 36 miesięcy od dnia Aktywacji.

3. Wymagania szczegółowe dla Usługi, o której mowa w ust. 2 pkt 1 (Część I):

1) Łącze o minimalnej gwarantowanej przepustowości 1 Gbps/1 Gbps.
2) Łącze musi być doprowadzone do szafy dystrybucyjnej w serwerowni Zamawiającego na poziomie 03.
3) Zamawiający wymaga łącza z 16-adresową podsiecią publicznie dostępnych adresów IPv4 (maska CIDR /28).
4) Łącze musi być zakończone wtykiem typu RJ45 pracującym w technologii Gigabit Ethernet - 1000Base-T lub światłowodowej wraz z odpowiednim konwerterem Gigabit Ethernet doprowadzonym bezpośrednio do szafy dystrybucyjnej znajdującej się w serwerowni Zamawiającego.

5) Oferowana usługa musi zapewniać nielimitowany transfer danych, nielimitowaną ilość otwartych sesji, brak blokowania usług i protokołów w Internecie (w szczególności, możliwa obustronna komunikacja na wszystkie porty TCP/UDP) oraz możliwość użytkowania dowolnej liczby urządzeń w przypadku zastosowania przez Zamawiającego translacji adresów (NAT).
6) Możliwość użytkowania przyznanych adresów IP na urządzeniach Zamawiającego bez konieczności zgłaszania adresów MAC urządzeń Zamawiającego do Wykonawcy lub rejestrowania ich w systemach informatycznych Wykonawcy.
7) Gwarantowany poziom usług:
   a) Wykonawca zapewni dla łącza SLA, obejmujące maksymalnie 6 (sześcio) godzinny czas usunięcia Awarii z gotowością służb technicznych Wykonawcy do usunięcia Awarii przez 24 (dwadzieścia cztery) godziny na dobę we wszystkie dni w miesiącu kalendarzowym do:
      – przyjęcia zgłoszenia Awarii,
      – przyjęcia informacji o tym, że nadal nie jest możliwe korzystanie z usługi w pełnym zakresie i z zachowaniem wymaganej przepustowości łącza,
      – przekazanie Zamawiającemu zawiadomienia o wykryciu Awarii,
      – usunięcia Awarii,
      – przekazania Zamawiającemu informacji o usunięciu Awarii.
   b) Wykonawca w ramach SLA gwarantuje dostępność usługi na poziomie 99,9 % (maksymalny łączny czas Awarii nie może przekroczyć 8 godz., 45 min., 36 s w skali roku i 43 min., 48 s. w skali miesiąca);
   c) czas reakcji na awarie w świadczonej usłudze dostępu do sieci Internet w czasie nieprzekraczającym 4 godziny od chwili jej zgłoszenia przez Zamawiającego;
   d) Czas trwania Awarii liczony jest od momentu, w którym Zamawiający zgłosi Wykonawcy Awarię lub Wykonawca zawiadomi Zamawiającego o wykryciu Awarii. Awarię uznaje się za usuniętą po poinformowaniu o tym Zamawiającego, o ile Zamawiający nie poinformuje Wykonawcy, że nadal nie jest możliwe korzystanie z usługi w pełnym zakresie i z zachowaniem wymaganej przepustowości łącza;
   e) Zgłoszenia Awarii oraz informacje o tym, że nadal nie jest możliwe korzystanie z usługi w pełnym zakresie i z zachowaniem wymaganej przepustowości łącza, a także potwierdzenie przyjęcia zawiadomienia o wykryciu Awarii oraz potwierdzenia przyjęcia informacji o usunięciu Awarii przyjmowane będą przez Wykonawcę: telefonicznie lub drogą mailową;
   f) Następnie Wykonawca potwierdzi Zamawiającemu, pocztą elektroniczną, przyjęcie zgłoszenia Awarii oraz przyjęcie informacji o tym, że nadal nie jest możliwe korzystanie z usługi w pełnym zakresie i z zachowaniem wymaganej przepustowości łącza;
   g) Potwierdzenie przyjęcia zgłoszenia Awarii, potwierdzenie przyjęcia informacji o tym, że nadal nie jest możliwe korzystanie z usługi w pełnym zakresie i z zachowaniem wymaganej przepustowości

łącza, a także zawiadomienie o wykryciu Awarii oraz informacje o usunięciu Awarii przyjmowane będą przez Zamawiającego drogą mailową;

h) Potwierdzenie przez Wykonawcę przyjęcia zgłoszenia Awarii, potwierdzenie przyjęcia informacji o tym, że nadal nie jest możliwe korzystanie z usługi w pełnym zakresie i z zachowaniem wymaganej przepustowości łącza, a także zawiadomienie o wykryciu Awarii oraz informacja o usunięciu Awarii, nastąpi niezwłocznie, jednak nie później niż w ciągu 15 (piętnastu) minut odpowiednio od zgłoszenia, przyjęcia informacji, wykrycia lub usunięcia Awarii;

i) Do czasu Awarii nie wlicza się czasu planowanych prac konserwacyjnych, których przeprowadzenie Wykonawca potwierdzi pocztą elektroniczną z Zamawiającym z wyprzedzeniem co najmniej 7 dni. Planowane prace konserwacyjne będą prowadzone w godzinach 18:00 do 7:00 rano oraz w dni wolne od pracy.

8) Możliwość ustawienia na zgłoszenie Zamawiającego rekordów Reverse DNS w ciągu maksymalnie 1 dnia roboczego.

9) Ochrona przed atakami Distributed Denial of Service (DDoS) dla całej udostępnionej przepustowości oferowanego łącza i dla całej adresacji IP Zamawiającego obejmująca:

a) monitorowanie ruchu sieciowego kierowanego do sieci Zamawiającego pod kątem prób ataków DDoS na udostępnione usługi w trybie 24/7/365. Monitoring odbywa się wyłącznie na urządzeniach Wykonawcy bez przekierowywania ruchu poza teren UE;

b) ochrona, co najmniej przed następującymi typami ataków: TCP SYN flood, UDP flood HTTP GET flood, HTTP POST flood, ICMP flood, IGMP flood, invalid packets, IP fragments, IP NULL, DNS flood, SIP request flood, SSL negotiation;

c) powiadamianie Zamawiającego (poprzez ustalone kanały komunikacji) w ciągu 30 minut od pojawienia się zagrożeń wskazujących na wystąpienie ataku DDoS;

d) przekierowywanie ruchu w przypadku podejrzenia wystąpienia ataku do dedykowanych do tego celu zasobów wewnętrznych Wykonawcy, zlokalizowanych na terytorium UE, w ciągu 30 minut od zgłoszenia przez Zamawiającego;

e) filtrowanie ruchu przy możliwie jak najmniejszym wpływie na ruch uprawniony oraz przekierowywanie odfiltrowanego ruchu do Zamawiającego;

f) przygotowanie dla Zamawiającego raportu po zakończeniu oczyszczania ruchu po zaistniałym ataku DDoS;

g) dostęp do panelu użytkownika usługi udostępniającego statystyki i raporty dla 5 pracowników Zamawiającego.

10) Wykonawca jest odpowiedzialny za doprowadzenie, uruchomienie i obsługę łącza, samodzielnie uzyska pozwolenia, o ile będą wymagane oraz dokona niezbędnych ustaleń technicznych w celu świadczenia usługi.

11) Wykonawca zapewni Zamawiającemu możliwość korzystania z aplikacji monitorującej w czasie rzeczywistym aktualny poziom wykorzystywania łącza w Mbps. Aplikacja powinna mieć możliwość gromadzenia i dostępu do danych historycznych z całego okresu trwania umowy. Dostęp do aplikacji przez przeglądarkę internetową z protokołem https SSL/TLS.

Aktywacja Usługi musi nastąpić w dniu 1.08.2025 r.

W przypadku wyboru oferty jako najkorzystniejszej, złożonej przez wykonawcę, który dotychczas świadczy dla Zamawiającego usługę dostępu do sieci Internet i usługę AntyDDoS, Aktywacja Usługi musi nastąpić w dniu 17.08.2025 r. o godz. 00:00.

4. Wymagania szczegółowe dla Usługi, o której mowa w ust. 2 pkt 2 (Część II):

1) **Z uwagi na zapewnienie redundancji łączy, Zamawiający wymaga łącza od Wykonawcy, który nie świadczy usługi Data Center dla Zamawiającego. Na terenie DC dopuszczalne jest korzystanie z infrastruktury T-Mobile.**
2) Łącze o minimalnej gwarantowanej przepustowości 1 Gbps/1 Gbps.
3) Zamawiający wymaga łącza z 32-adresową podsiecią publicznie dostępnych adresów IPv4 (maska CIDR /27).
4) Łącze musi być zakończone wtykiem typu RJ45 pracującym w technologii Gigabit Ethernet - 1000Base-T lub światłowodowej wraz z odpowiednim konwerterem Gigabit Ethernet doprowadzonym bezpośrednio do szafy dystrybucyjnej znajdującej się w serwerowni Zamawiającego.
5) Oferowana usługa musi zapewniać nielimitowany transfer danych, nielimitowaną ilość otwartych sesji, brak blokowania usług i protokołów w Internecie (w szczególności, możliwa obustronna komunikacja na wszystkie porty TCP/UDP) oraz możliwość użytkowania dowolnej liczby urządzeń w przypadku zastosowania przez Zamawiającego translacji adresów (NAT).
6) Możliwość użytkowania przyznanych adresów IP na urządzeniach Zamawiającego bez konieczności zgłaszania adresów MAC urządzeń Zamawiającego do Wykonawcy lub rejestrowania ich w systemach informatycznych Wykonawcy.
7) Gwarantowany poziom usług:
   a) Wykonawca zapewni dla łącza SLA, obejmujące maksymalnie 6 (sześcio) godzinny czas usunięcia Awarii z gotowością służb technicznych Wykonawcy do usunięcia Awarii przez 24 (dwadzieścia cztery) godziny na dobę we wszystkie dni w miesiącu kalendarzowym do:
      – przyjęcia zgłoszenia Awarii;
      – przyjęcia informacji o tym, że nadal nie jest możliwe korzystanie z usługi w pełnym zakresie i z zachowaniem wymaganej przepustowości łącza;
      – przekazanie Zamawiającemu zawiadomienia o wykryciu Awarii;

– usunięcia Awarii;
– przekazania Zamawiającemu informacji o usunięciu Awarii.

b) Wykonawca w ramach SLA gwarantuje dostępność usługi na poziomie 99,9 % (maksymalny łączny czas Awarii nie może przekroczyć 8 godz., 45 min., 36 s w skali roku i 43 min., 48 s. w skali miesiąca);

c) czas reakcji na awarie w świadczonej usłudze dostępu do sieci Internet w czasie nieprzekraczającym 4 godziny od chwili jej zgłoszenia przez Zamawiającego;

d) Czas trwania Awarii liczony jest od momentu, w którym Zamawiający zgłosi Wykonawcy Awarię lub Wykonawca zawiadomi Zamawiającego o wykryciu Awarii. Awarię uznaje się za usuniętą po poinformowaniu o tym Zamawiającego, o ile Zamawiający nie poinformuje Wykonawcy, że nadal nie jest możliwe korzystanie z usługi w pełnym zakresie i z zachowaniem wymaganej przepustowości łącza;

e) Zgłoszenia Awarii oraz informacje o tym, że nadal nie jest możliwe korzystanie z usługi w pełnym zakresie i z zachowaniem wymaganej przepustowości łącza, a także potwierdzenie przyjęcia zawiadomienia o wykryciu Awarii oraz potwierdzenia przyjęcia informacji o usunięciu Awarii przyjmowane będą przez Wykonawcę: telefonicznie lub drogą mailową;

f) Następnie Wykonawca potwierdzi Zamawiającemu, pocztą elektroniczną, przyjęcie zgłoszenia Awarii oraz przyjęcie informacji o tym, że nadal nie jest możliwe korzystanie z usługi w pełnym zakresie i z zachowaniem wymaganej przepustowości łącza;

g) Potwierdzenie przyjęcia zgłoszenia Awarii, potwierdzenie przyjęcia informacji o tym, że nadal nie jest możliwe korzystanie z usługi w pełnym zakresie i z zachowaniem wymaganej przepustowości łącza, a także zawiadomienie o wykryciu Awarii oraz informacje o usunięciu Awarii przyjmowane będą przez Zamawiającego drogą mailową;

h) Potwierdzenie przez Wykonawcę przyjęcia zgłoszenia Awarii, potwierdzenie przyjęcia informacji o tym, że nadal nie jest możliwe korzystanie z usługi w pełnym zakresie i z zachowaniem wymaganej przepustowości łącza, a także zawiadomienie o wykryciu Awarii oraz informacja o usunięciu Awarii, nastąpi niezwłocznie, jednak nie później niż w ciągu 15 (piętnastu) minut odpowiednio od zgłoszenia, przyjęcia informacji, wykrycia lub usunięcia Awarii;

i) Do czasu Awarii nie wlicza się czasu planowanych prac konserwacyjnych, których przeprowadzenie Wykonawca potwierdzi pocztą elektroniczną z Zamawiającym z wyprzedzeniem co najmniej 7 dni. Planowane prace konserwacyjne będą prowadzone w godzinach 18:00 do 7:00 rano oraz w dni wolne od pracy.

8) Możliwość ustawienia na zgłoszenie Zamawiającego rekordów Reverse DNS w ciągu maksymalnie 1 dnia roboczego.

9) Ochrona przed atakami Distributed Denial of Service (DDoS) dla całej udostępnionej przepustowości oferowanego łącza i dla całej adresacji IP Zamawiającego obejmująca:

a) monitorowanie ruchu sieciowego kierowanego do sieci Zamawiającego pod kątem prób ataków DDoS na udostępnione usługi w trybie 24/7/365. Monitoring odbywa się wyłącznie na urządzeniach Wykonawcy bez przekierowywania ruchu poza teren UE;
b) ochrona, co najmniej przed następującymi typami ataków: TCP SYN flood, UDP flood HTTP GET flood, HTTP POST flood, ICMP flood, IGMP flood, invalid packets, IP fragments, IP NULL, DNS flood, SIP request flood, SSL negotiation;
c) powiadamianie Zamawiającego (poprzez ustalone kanały komunikacji) w ciągu 30 minut od pojawienia się zagrożeń wskazujących na wystąpienie ataku DDoS;
d) przekierowywanie ruchu w przypadku podejrzenia wystąpienia ataku do dedykowanych do tego celu zasobów wewnętrznych Wykonawcy, zlokalizowanych na terytorium UE, w ciągu 30 minut od zgłoszenia przez Zamawiającego;
e) filtrowanie ruchu przy możliwie jak najmniejszym wpływie na ruch uprawniony oraz przekierowywanie odfiltrowanego ruchu do Zamawiającego;
f) przygotowanie dla Zamawiającego raportu po zakończeniu oczyszczania ruchu po zaistniałym ataku DDoS;
g) dostęp do panelu użytkownika usługi udostępniającego statystyki i raporty dla 5 pracowników Zamawiającego.

10) Wykonawca jest odpowiedzialny za doprowadzenie, uruchomienie i obsługę łącza, samodzielnie uzyska pozwolenia, o ile będą wymagane oraz dokona niezbędnych ustaleń technicznych w celu świadczenia usługi.
11) Wykonawca zapewni Zamawiającemu możliwość korzystania z aplikacji monitorującej w czasie rzeczywistym aktualny poziom wykorzystywania łącza w Mbps. Aplikacja powinna mieć możliwość gromadzenia i dostępu do danych historycznych z całego okresu trwania umowy. Dostęp do aplikacji przez przeglądarkę internetową z protokołem https SSL/TLS.

Aktywacja Usługi musi nastąpić w dniu 1 września 2025 r.

W przypadku wyboru oferty jako najkorzystniejszej, złożonej przez wykonawcę, który dotychczas świadczy dla Zamawiającego usługę dostępu do sieci Internet i usługę AntyDDoS, Aktywacja Usługi musi nastąpić w dniu 15.09.2025 r. o godz. 00:00.