Załącznik nr 1

**Wymagania dla łącza internetowego w lokalizacji Wspólna 30**

1. Przedmiotem Zamówienia będzie zakup usług telekomunikacyjnych polegających na zestawieniu, uruchomieniu i udostępnianiu przez całą dobę (24 godz.) przez wszystkie dni roku w okresie od 31 lipca 2024 r. do 30 marca 2026 r. symetrycznych łączy dostępowych zapewniających dostęp do Internetu w lokalizacji: Główny Inspektorat Ochrony Roślin i Nasiennictwa, gmach budynku Ministerstwa Rolnictwa i Rozwoju Wsi, ul. Wspólna 30, 00-930 Warszawa, 4 piętro (nie ostatnie piętro), do pokoju nr 445/447.

2. Oferowane łącze z dostępem do wszystkich usług i serwisów krajowych i zagranicznych oraz z nielimitowaną ilością sesji oraz przesyłanych danych.

3. Zamawiający informuje, że nie jest właścicielem budynku, a więc w przypadku konieczności wykonania prac budowlanych i instalacyjnych konieczne będzie uzyskanie stosownej zgody od zarządcy budynku. Zamawiający informuje, że budynek jest objęty ochroną konserwatorską.

4. Dostęp do Internetu musi być oparty na dwóch niezależnych łączach dostępowych – głównym i zapasowym.

5. W/w łącza muszą mieć przepustowość minimum 300 Mbp/s łącze główne, 100 Mbp/s łącze zapasowe, każde (CIR=EIR).

6. Łącze główne oraz łącze zapasowe muszą zapewniać dostęp do Internetu przez dwie oddzielne lokalizacje – węzły jednego lub dwóch dostawców internetowych.

7. Wykonawca podłączy Zamawiającemu dostęp do sieci Internet poprzez łącze w standardzie Ethernet.

8. Łącze zapasowe ma działać w sytuacji kiedy nie będzie działać łącze główne.

9. Dopuszcza się instalację dostępu do Internetu na łączy zapasowym z wykorzystaniem łącza radiowego.

10. W przypadku awarii łącza głównego łącze zapasowe musi przejąć cały ruch. Przełączanie między łączami z głównego na zapasowe oraz z zapasowego na główne nie może trwać dłużej niż 2 minuty.

11. Zasoby Zamawiającego muszą być dostępne cały czas pod tymi samymi numerami IP/nazwami domen bez względu na to, które z dwóch łącz jest aktualnie wykorzystywane. Łącze musi być dostępne 24 godziny na dobę przez 7 dni w tygodniu,

12. Zamawiającemu zostanie przydzielona pula dwóch podsieci stałych, realnych adresów IP – pierwsza podsieć co najmniej 6 adresów IP, druga co najmniej 14 adresów IP (utrzymanie obecnie przydzielonej adresacji).

13. Zamawiającemu zostanie przydzielona podsieć połączeniowa między urządzeniem końcowym Wykonawcy a urządzeniem „firewall" Zamawiającego.

14. Wykonawca zapewni możliwość monitorowania łącza głównego w zakresie co najmniej: wielkości ruchu wejściowego i wyjściowego.

15. Wykonawca zapewni możliwość modyfikacji wpisów revDNS.

16. W ramach oferowanej usługi dostawca zapewni ochronę DDoS:

    a. usługa dla całej przepustowości oferowanego łącza
    b. monitorowanie ruchu sieciowego kierowanego do sieci Zamawiającego
    c. zapewnienie ciągłego dyżuru pełniącego monitoring ochrony przed atakami DDoS
    d. ochronę przed wolumetrycznymi atakami DDoS

e. ochronę 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
f. zapobieganie atakom do przepływowości do 10 Gbps, bez limitu czasu trwania ataku
g. zawiadamianie Zamawiającego poprzez ustalone kanały komunikacji w ciągu 15 minut od pojawienia się zagrożeń wskazujących na wystąpienie ataku DDoS
h. zastosowanie filtrowania ruchu za pomocą „block list" oraz „safe list" w czasie nie dłuższym niż 2 godziny od wykrycia incydentu
i. dostęp dla Zamawiającego do panelu administracyjnego usług DDoS, umożliwiający m.in. monitoring i rekonfigurację parametrów usługi.

17. Wykonawca dostarczy, zainstaluje i skonfiguruje wszystkie urządzenia i oprogramowanie niezbędne do realizacji będącej przedmiotem zamówienia.

18. Zamawiający zapewni miejsce w szafie i zasilanie dla urządzeń Wykonawcy.

19. Urządzenia i oprogramowanie o których mowa w pkt. 17
    a. pozostają własnością Wykonawcy
    b. koszty ich użytkowania, obsługi, konfiguracji, konserwacji i napraw ponosi Wykonawca
    c. koszt transportu urządzeń ponosi Wykonawca

20. Wymagany poziom gwarancji jakości świadczonej usługi:
    a. poziom dostępności łącza co najmniej 99.5 % (w skali miesiąca)
    b. czas reakcji na zgłoszoną awarię nie może być dłuższy niż 4 godziny (24 godziny na dobę przez 7 dni w tygodniu).
    c. czas usunięcia usterki maksymalnie 12 godzin od momentu przyjęcia zgłoszenia
    d. w przypadku niedotrzymania warunków gwarancji jakości świadczonej usługi Wykonawca zapłaci Zamawiającemu rekompensatę naliczoną jako czas niedostępności łącza [%] * wysokość miesięcznego abonamentu.
    e. wymagania dotyczą łącza rozumianego jako całość tj. łącza głównego i zapasowego.

21. Wykonawca posiada certyfikaty ISO 9001 w zakresie świadczenia usług telekomunikacyjnych oraz usług bezpieczeństwa teleinformatycznego oraz ISO 27001 w zakresie usług z zakresu cyberbezpieczeństwa.

Załącznik nr 2

**Wymagania dla łącza internetowego w lokalizacji CL Toruń**

1. Przedmiotem Zamówienia będzie zakup usług telekomunikacyjnych polegających na zestawieniu, uruchomieniu i udostępnianiu przez całą dobę (24 godz.) przez wszystkie dni roku w okresie od 20 sierpnia 2024 r. do 30 marca 2026 r. symetrycznych łączy dostępowych zapewniających dostęp do Internetu w lokalizacji: Centralne Laboratorium GIORiN, ul. Żwirki i Wigury 73, 87-100 Toruń.

2. Zamawiający informuje, że jest właścicielem budynku. Zamawiający informuje, że budynek nie jest objęty ochroną konserwatorską.

3. Łącze musi mieć przepustowość minimum 100 Mbp/s (CIR=EIR).

4. Wykonawca podłączy Zamawiającemu dostęp do sieci Internet poprzez łącze w standardzie Ethernet.

5. Zamawiającemu zostanie przydzielona pula stałych, realnych adresów IP co najmniej 6 adresów IP (utrzymanie obecnie przydzielonej adresacji).

6. Wykonawca zapewni możliwość monitorowania łącza głównego w zakresie co najmniej: wielkości ruchu wejściowego i wyjściowego.

7. Wykonawca zapewni możliwość modyfikacji wpisów revDNS.

8. W ramach oferowanej usługi dostawca zapewni ochronę DDoS:

    a. usługa dla całej przepustowości oferowanego łącza
    b. monitorowanie ruchu sieciowego kierowanego do sieci Zamawiającego
    c. zapewnienie ciągłego dyżuru pełniącego monitoring ochrony przed atakami DDoS
    d. ochronę przed wolumetrycznymi atakami DDoS
    e. ochronę 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
    f. zapobieganie atakom do przepływowości do 10 Gbps, bez limitu czasu trwania ataku
    g. zawiadamianie Zamawiającego poprzez ustalone kanały komunikacji w ciągu 15 minut od pojawienia się zagrożeń wskazujących na wystąpienie ataku DDoS
    h. zastosowanie filtrowania ruchu za pomocą „block list" oraz „safe list" w czasie nie dłuższym niż 2 godziny od wykrycia incydentu
    i. dostęp dla Zamawiającego do panelu administracyjnego usług DDoS, umożliwiający m.in. monitoring i rekonfigurację parametrów usługi.

9. Wykonawca dostarczy, zainstaluje i skonfiguruje wszystkie urządzenia i oprogramowanie niezbędne do realizacji będącej przedmiotem zamówienia.

10. Zamawiający zapewni miejsce w szafie i zasilanie dla urządzeń Wykonawcy.

11. Urządzenia i oprogramowanie o których mowa w pkt. 9
    a. pozostają własnością Wykonawcy
    b. koszty ich użytkowania, obsługi, konfiguracji, konserwacji i napraw ponosi Wykonawca
    c. koszt transportu urządzeń ponosi Wykonawca

12. Wymagany poziom gwarancji jakości świadczonej usługi:
    a. poziom dostępności łącza co najmniej 99.5 % (w skali miesiąca)
    b. czas reakcji na zgłoszoną awarię nie może być dłuższy niż 4 godziny (24 godziny na dobę przez 7 dni w tygodniu).
    c. czas usunięcia usterki maksymalnie 12 godzin od momentu przyjęcia zgłoszenia

d. w przypadku niedotrzymania warunków gwarancji jakości świadczonej usługi Wykonawca zapłaci Zamawiającemu rekompensatę naliczoną jako czas niedostępności łącza [%] * wysokość miesięcznego abonamentu.

13. Wykonawca posiada certyfikaty ISO 9001 w zakresie świadczenia usług telekomunikacyjnych oraz usług bezpieczeństwa teleinformatycznego oraz ISO 27001 w zakresie usług z zakresu cyberbezpieczeństwa.

Marcin Gajewski

Elektronicznie podpisany przez Marcin Gajewski
Data: 2024.06.14 11:37:55 +02'00'