Załącznik 1 do Umowy WI1.374.43.2023.MC

# Opis przedmiotu Zamówienia - Świadczenie usług dostępu do Internetu na łączu symetrycznym

Przedmiotem zamówienia jest świadczenie przez Wykonawcę usług telekomunikacyjnych zapewnienia dostępu do Internetu wraz z usługami ochrony przed atakami DDoS.

## Informacje Ogólne

1. Obecna umowa na świadczenie dostępu do sieci Internet na łączu symetrycznym wraz z usługami ochrony przed atakami DDoS jest zawarta na czas określony do 30.09.2023r.
2. Termin realizacji zamówienia – 01.10.2023 – 30.09.2025.
3. Zamawiający nie ponosi odpowiedzialności za szkody wyrządzone przez Wykonawcę podczas wykonywania przedmiotu Zamówienia.
4. Wykonawca odpowiada ze ewentualne uzyskanie wszystkich niezbędnych pozwoleń niezbędnych do realizacji przedmiotu zamówienia.

## Usługa telekomunikacyjna zapewnienia dostępu do sieci Internet.

1. Zestawianie, uruchomienie i utrzymywanie przez cały okres trwania umowy, symetrycznego łącza dostępowego o przepustowości gwarantowanej wynoszącej 600Mbps.
   1. Gwarantowana prędkość połączenia pomiędzy Wykonawcą, a Zamawiającym wynosi 600Mbps (słownie: sześćset megabitów na sekundę).
   2. Gwarantowana prędkość połączenia pomiędzy Zamawiającym, a Wykonawcą wynosi 600Mbps (słownie: sześćset megabitów na sekundę).
   3. Miejscem instalacji łącza jest budynek Urzędu Morskiego w Gdyni, ul. Chrzanowskiego 10, 81-338 Gdynia.
   4. Zakończenie sieciowe po stronie zamawiającego musi być zgodne ze standardem Ethernet pracujące na portach miedzianych RJ45 1000 Base-TX lub optycznych 1000 Base-LX/LH.
   5. Wykonawca musi zapewnić obsługę ruchu generowanego przez Zamawiającego przy pomocy protokołu routingu BGP w wersji 4.
   6. Wykonawca musi zapewnić obsługę klasy adresów IPv4 o charakterze (Provider Independent) należących do Zamawiającego posiadającego własny numer AS.
   7. Wykonawca musi zapewnić dostęp do wszystkich usług i serwisów internetowych krajowych i zagranicznych.
   8. Ilość generowanego ruchu przez Zamawiającego nie może być w żaden sposób limitowana oraz ograniczana funkcjonalnie.
   9. Wszystkie urządzenia instalowane w serwerowni w budynku Urzędu Morskiego w Gdyni przy ulicy Chrzanowskiego 10 w Gdyni muszą być fabrycznie przystosowane do montażu i zamontowane w szafach RACK 19 cali.
   10. Dostępność świadczonej usługi nie może być niższa niż 99,5% w skali roku.
   11. Gwarantowany czas usunięcia awarii na łączu nie może być wyższy niż 8 godzin.
   12. Wykonawca musi zapewnić 24 godzinny serwis zgłoszeń awarii technicznych łącza.
2. Utrzymanie na życzenie Zamawiającego serwera secondary DNS dla strefy: umgdy.gov.pl
3. Usługi muszą mieć charakter powszechny oraz muszą być świadczone zgodnie z powszechnie obowiązującymi przepisami tj. ustawą z dnia 16 lipca 2004r – Prawo telekomunikacyjne (Jednolity tekst Dz.U. 2022 poz. 1648).
4. Świadczenie usługi może realizować Wykonawca, który został wpisany do rejestru przedsiębiorców telekomunikacyjnych prowadzonego przez Prezesa Urzędu Komunikacji Elektronicznej, zgodnie z ustawą z dnia 16 lipca 2004 roku Prawo telekomunikacyjne (Jednolity tekst Dz.U. 2022 poz. 1648). W celu potwierdzenia spełnienia niniejszego warunku Wykonawca zobowiązany jest przedłożyć aktualne zaświadczenie o wpisie do rejestru przedsiębiorców telekomunikacyjnych wydane przez Prezesa Urzędu Komunikacji Elektronicznej.

## Usługa ochrony przed atakami DDoS.

### Informacje ogólne.

* 1. Usługa musi być świadczona przez Wykonawcę w trybie całodobowym, siedem dni w tygodniu.

### Monitorowanie ruchu.

* 1. Usługa musi obejmować monitorowanie ruchu sieciowego kierowanego do sieci Zamawiającego pod kątem prób ataków DDoS na udostępnione przez Zamawiającego w sieci Internet treści i usługi.
  2. Usługa monitorowania ruchu musi opierać się na monitorowaniu urządzeń aktywnych Wykonawcy, które wykorzystuje on w realizacji usług dostępu do Internetu dla Zamawiającego.
  3. Dane zgromadzone w procesie monitoringu muszą być podstawą do sporządzania statystyk ruchu.
  4. Monitorowanie ruchu na chronionym łączu Zamawiającego musi odbywać się w na zasadzie próbkowania w trybie ciągłym w czasie rzeczywistym.

### Wykrywanie zagrożeń.

* 1. Wykrywanie zagrożeń w ruchu sieciowym musi odbywać się co najmniej na podstawie następujących mechanizmów detekcji:
     1. Sygnatury.
     2. Przekroczenie wartości progowych dla określonych typów pakietów i protokołów.
     3. Wykrywanie anomalii ruchu sieciowego w stosunku do profilu ruchu sieciowego Zamawiającego.
  2. W ramach usługi Wykonawca monitoruje ruch do i od chronionej podsieci w czasie rzeczywistym.
  3. Wykonawca musi zapewniać wykrywanie anomalii ruchu sieciowym, co najmniej dla: TCP SYN, TCP RST, TCP Null, ICMP, IP Null, IP Fragmented, DNS.
  4. W oparciu o dane historyczne system musi określać oczekiwaną wartość ruchu od i do Zamawiającego w danym czasie.
  5. Wykonawca musi zapewnić wykrywanie anomalii ruchu sieciowego polegających na znacznym przekroczeniu wolumenu ruchu w stosunku do wcześniej wyznaczonych wartości oczekiwanego ruchu dla Zamawiającego.
  6. Wykonawca musi klasyfikować ruch sieciowy co najmniej na następujące kategorie:
     1. Zweryfikowany atak.
     2. Fałszywy alarm.
     3. Nagły ruch, tj. wzrost woluminu ruchu sieciowego spowodowany inną przyczyną niż atak.
  7. Wykonawca musi powiadamiać Zamawiającego o pojawieniu się zagrożeń wskazujących na wystąpienie ataku (alarmów krytycznych) w terminie nie dłuższym niż 15 minut od momentu ich identyfikacji.
  8. Wykonawca musi powiadamiać Zamawiającego o pojawieniu się alarmów krytycznych, obejmujących co najmniej taki zdarzenia, jak:
     1. Potencjalne ataki DDoS.
     2. Utrata komunikacji z monitorowanymi zasobami.
     3. Inne alarmy wynikające z ustaleń z Zamawiającym.
  9. Kryteria definiujące wystąpienie zdarzeń oraz poziom, jaki zostanie przyporządkowany dla poszczególnych zdarzeń musi zostać uzgodniony z Zamawiającym na etapie wdrożenia usługi.

### Oczyszczanie ruchu - mitygacja.

* 1. Mechanizmy oczyszczania ruchu sieciowego muszą w maksymalnym stopniu filtrować ruch niepożądany, a jednocześnie nie mogą w znaczący sposób oddziaływać (ograniczać, blokować itp.) na ruch uprawniony.
  2. W ramach oczyszczania ruchu Wykonawca musi zapewnić automatyczną mitygację zdarzenia, polegającą na przekierowywaniu zidentyfikowanego złośliwego ruchu DDoS do centrum analizy ruchu Wykonawcy, przefiltrowaniu i oczyszczeniu go z niepożądanej aktywności, a następnie przekierowaniu go do Zamawiającego.
  3. Centrum analizy ruchu Wykonawcy nie może znajdować się poza terenem Rzeczypospolitej Polskiej.
  4. W trakcie mitygacji ruch sieciowy nie może być przekierowany poza teren Rzeczypospolitej Polskiej.
  5. Ruch w sieci Zamawiającego przekierowany do oczyszczania nie może być wysyłany poza obszar i infrastrukturę, która nie znajduje się pod bezpośrednim nadzorem Wykonawcy.
  6. Wykonawca musi poddawać ciągłej analizie ruch sieciowy i konfigurację mechanizmów filtracji i w porozumieniu z Zamawiającym dokonywać modyfikacji, aby realizować założenia opisane w punkcie 4.1.
  7. Wykonawca w ramach świadczonej usługi oczyszczania ruchu musi zapewniać:
     1. Ochronę przed atakami wolumetrycznymi o wolumenie do 50 Gb/sek.
     2. Filtrowanie ruchu z błędnymi nagłówkami IP, TCP, UDP.
     3. Filtrowanie ruchu na określonych portach TCP i UDP na podstawie zawartości pola danych w oparciu o wyrażenia regularne.
     4. Odrzucanie lub przepuszczanie ruchu sieciowego na podstawie zdefiniowanych – we współpracy z Zamawiającym – filtrów, operujących na informacjach w nagłówkach.
     5. Ochronę przed atakami ze spoofowanymi adresami źródłowymi IP poprzez autentykację sesji TCP, zapytań DNS oraz zapytań http.
     6. Filtrowanie nieprawidłowych zapytań DNS.
     7. Ograniczenia zapytań DNS do zadanej wartości zapytań na sek.
     8. Co najmniej 5 filtrów opartych o wyrażenia regularne, definiujące zakres stosowania autentykacji DNS oraz ograniczania liczby zapytań DNS.
     9. Filtrowanie nieprawidłowych zapytań http.
     10. Blokowanie ruchu od stacji końcowych przekraczających progi dla operacji HTTP na sekundę per serwer lub per URL.
     11. Co najmniej 5 filtrów opartych o wyrażenia regularne, definiujących zakres stosowania autentykacji HTTP lub ograniczania liczby zapytań http.
     12. Filtrowanie ruchu w oparciu o wyrażenia regularne dotyczące nagłówków http.
     13. Ochronę przez atakami typu slow Lories, poprzez resetowanie połączeń, które pozostają nieaktywne przez zadany okres czasu.
     14. Ochronę przez atakami typu slow Lories, poprzez resetowanie sesji TCP, której aktywność jest poniżej zadanej liczby bajtów przesyłanej w zadanym okresie czasu.
     15. Wykrywanie ruchu kierowanego z serwerów CDN proxy i stosowanie algorytmów filtrowania na podstawie oryginalnego źródła ruchu
     16. Wykrywanie i filtrowanie pakietów z nieprawidłowymi nagłówkami SSL/TLS lub nagłówkami SSL/TLS, które są poza sekwencją.
     17. Blokowanie sesji, jeżeli podczas negocjacji SSL/TLS klient zażąda nadmiernej ilości metod kryptograficznych lub rozszerzeń użytkownika - próg dla tych wartości musi być konfigurowalny.
     18. Wykrywanie i rozłączanie sesji, jeżeli negocjacja SSL/TLS nie zakończy się w zadanym czasie.
     19. Blokowanie ruchu ze stacji, dla których występuje nadmierna liczba nieprawidłowych, nadmiarowych lub niekompletnych sesji SSL.
     20. Monitorowanie negocjacji SSL dla wszystkich portów, na których mogą być stosowane aplikacje zabezpieczone protokołem TLS: HTTPS, SMTP, IMAP4, POP, LDAP, IRC, NNTP, TELNET, FTP i SIP.
     21. Ochronę przed atakami pochodzącym od sieci botnetowych poprzez filtrowanie dzięki na bieżąco aktualizowanym sygnaturom zawierającym listę adresów IP.
     22. Ochronę przed atakami pochodzącymi z sieci botnetowych poprzez wykrywanie źródeł ataku o wolumenie przekraczającym zadane wartości.
     23. Uruchamianie mitygacji w celu nauczenia się systemu wartości typowych ruchu, które następnie mogą być wykorzystywania do właściwego ustawiania progów dla algorytmów mitygacji.
  8. Czas uruchomienia automitygacji nie może być dłuższy niż 5 minut od momentu przekroczenia parametrów detekcji złośliwego ruchu.
  9. Ruch sieciowy musi być oczyszczany do momentu ustania ataku.
  10. W przypadku, gdy uruchomiana procedura eliminacji DDoS ma negatywny wpływ na zasoby lub usługi, Zamawiający ma możliwość jej przerwania, co następuje w czasie nie dłuższym niż 15 minut od momentu zgłoszenia takiej potrzeby przez Zamawiającego.

### Raportowanie.

* 1. Wykonawca musi sporządzać i przesyłać w formie elektronicznej do Zamawiającego raporty ze zdarzeń zaistniałych w ramach realizacji niniejszej usługi. Raport musi obejmować co najmniej:
     1. Wielkość ruchu przychodzącego i wychodzącego.
     2. Maksymalne wartości ruchu.
     3. Listę zarejestrowanych ataków.
     4. Listę usuniętych ataków.

### Dostęp do panelu użytkownika.

* 1. Wykonawca musi przydzielić Zamawiającemu dostęp do serwisu www dla usługi.
  2. Zamawiający musi mieć możliwość realizacji dostępu do serwisu poprzez sieć Internet.
  3. W ramach korzystania z usługi Zamawiający musi mieć nadane co najmniej uprawnienia do odczytu.
  4. Dostęp do serwisu musi być zabezpieczony w oparciu o technologię IPsec.
  5. W ramach funkcjonalności serwisu Zamawiający będzie mógł co najmniej:
     1. Tworzyć raporty i przeglądać statystyki z analizy ruchu sieciowego.
     2. Generować i pobierać raporty w formacie pdf i xml.
     3. Wysyłać raporty na wskazany adres email.

### Wdrożenie usługi.

* 1. W ramach Projektu Wykonawczego Wykonawca we współpracy z Zamawiającym uzgodni co najmniej następujące szczegóły techniczne:
     1. Opis techniczny integracji usługi z siecią Klienta,
     2. Opis procedur powiadamiania i eskalacji,
     3. Testy akceptacyjne,
     4. Opis procedur obsługi zgłoszeń i raportowania.
  2. Proces tworzenia dokumentu zostaje zakończony z chwilą akceptacji przez Zamawiającego.
  3. W ramach implementacji usługi Wykonawca dokona rekonfiguracji swoich urządzeń sieciowych oraz skonfiguruje usługę przeciwdziałania atakom DDoS zgodnie z wymaganiami Zamawiającego określonymi Projektem Wykonawczym.
  4. Po zakończeniu implementacji usługi – w celu potwierdzenia, że dotychczasowa funkcjonalność sieci Zamawiającego nie została utracona – Wykonawca z udziałem Zamawiającego przeprowadzą testy funkcjonalne usługi przeciwdziałania atakom DDoS (testy akceptacyjne).
  5. W ramach testów akceptacyjnych musi zostać sprawdzona:
     1. Poprawność routingu z i do Wykonawcy.
     2. Poprawność re-routingu BGP.
     3. Działanie mechanizmów BGP Flowspec.
  6. Po zakończeniu testów akceptacyjnych. Wykonawca przedstawia Zamawiającemu do akceptacji dokumentację, zawierającą, co najmniej:
     1. Procedury operacyjne odnoszące się do inicjalizacji i zakończenia obsługi incydentu ataku DDoS.
     2. Szczegóły techniczne chronionych sieci i usług Klienta.
     3. Udokumentowaną procedurę wdrażania zmian funkcjonalnych w zakresie sieci i usług Klienta, które mają wpływ na szczegółową konfigurację usługi.