

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

dotyczące przedmiotu zamówienia, w związku z art. 2 ust. 1 pkt 1 *a contrario* – ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2023 r., poz. 1605 t.j. z dnia 14.09.2023) na:

wykonanie dwóch niezależnych łącz internetowych oraz świadczenie z ich wykorzystaniem usługi dostępu do Internetu dla Górnośląsko-Zagłębiowskiej Metropolii..

1. Specyfikacja głównych wymagań.

1.1. Łącze symetryczne medium transmisyjne: światłowód (1 szt.):

- a) Wykonanie instalacji wraz z urządzeniami niezbędnymi do odbioru sygnału i możliwością wpięcia do infrastruktury Zamawiającego. Miejsce montażu urządzeń końcowych to pomieszczenie nr 118 na pierwszym piętrze budynku zlokalizowanego w Katowicach przy ul. Barbary 21A (właścicielem budynku jest Zamawiający),
- b) świadczenie usługi dostępu do Internetu,
- c) przepustowość łącza min. 1 GBit/s,
- d) poziom jakości usług (SLA) – nie więcej niż 4 godziny niesprawności łącza na miesiąc licząc od momentu zgłoszenia niesprawności przez Zamawiającego,
- e) świadczenie usługi dostępu do Internetu z wykorzystaniem dotychczasowych adresów IP. Obecna przestrzeń adresowa:

77.252.189.160/28

213.216.92.140/30

81.219.66.128/25

81.219.66.32/27

- f) Wykonawca, w celu nawiązania transmisji danych pomiędzy ruterem brzegowym a siedzibą Zamawiającego może wykorzystać istniejące łącze światłowodowe w porozumieniu z obecnym właścicielem (Netia S.A. lub 3S-Śląskie Sieci Światłowodowe) lub wykonać nowe połączenie. Wszelkie formalności związane z uzyskaniem pozwoleń na wykonanie nowego połączenia pozostają w gestii Wykonawcy. Właścicielem wykonanego połączenia pozostaje Wykonawca.
- g) Wykonawca, w ramach odbioru połączenia, zobowiązany jest przedstawić wyniki pomiaru parametrów łącza.

1.2. Łącze symetryczne medium transmisyjne: fale radiowe (1 szt.):

- a) wykonanie instalacji wraz z urządzeniami niezbędnymi do odbioru sygnału i możliwości wpięcia do infrastruktury Zamawiającego. Miejsce montażu urządzeń końcowych to pomieszczenie nr 116 na pierwszym piętrze budynku zlokalizowanego w Katowicach przy ul. Barbary 21A (właścicielem budynku jest Zamawiający),
- b) świadczenie usługi dostępu do Internetu,
- c) przepustowość łącza min. **100 Mbit/s**,

- d) poziom jakości usług (SLA) – nie więcej niż 4 godziny niesprawności łącza na miesiąc licząc od momentu zgłoszenia,
- e) świadczenie usługi dostępu do Internetu z wykorzystaniem dotychczasowych adresów IP. Obecna przestrzeń adresowa:

78.9.15.224/28

89.25.195.208/28

1.3. Świadczenie usługi dostępu do Internetu przez okres 24 miesięcy, w rozliczeniu miesięcznym:

- a) Zamawiający wymaga, aby czas reakcji Wykonawcy na zgłoszone telefonicznie lub mailem usterki łącza wynosił maksymalnie 1 godzinę od chwili zgłoszenia, zaś maksymalny czas naprawy – zgodnie z formularzem ofertowym (max.10 godzin),
- b) Usługi telekomunikacyjne świadczone będą zgodnie z ustawą z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U.2022.1648 t.j. z dnia 2022.08.05), dalej „Ustawa”,
- c) Wykonawca nie może powierzyć wykonania zamówienia osobom trzecim, **za wyjątkiem prac, o których mowa w pkt. 1.1 lit. a), pkt. 1.2 lit. a),**
- d) Wykonawca zapewnia, że przez cały okres trwania Umowy i świadczenia usług, z wyłączeniem okresów Awarii i Planowanych Prac, zapewni jakość usług umożliwiającą nieprzerwane prowadzenie działalności przez Zamawiającego,
- e) Zamawiający oświadcza, że posiada prawo do dysponowania lokalem, w tym do wykonania w nim podłączenia, objętego przedmiotem Umowy.
- f) Wykonawca oświadcza, że:
 - przedstawiony przez niego formularz ofertowy (**Załącznik nr 1 do umowy**) sporządzony został zgodnie z IWUZ i obejmuje wszystkie koszty związane z realizacją Umowy,
 - otrzymał pełną i wyczerpującą informację od Zamawiającego, pozwalającą określić wszystkie koszty przygotowania, wykonania i odbioru przedmiotu Umowy,
 - jest przedsiębiorcą telekomunikacyjnym w rozumieniu Ustawy i posiada wszelkie uprawnienia niezbędne do wykonania przedmiotu Umowy,
 - zapoznał się z warunkami technicznymi podłączeń linii telekomunikacyjnych w budynku ZTM przy ul. Barbary 21A w Katowicach i nie wnosi żadnych zastrzeżeń dotyczących możliwości technicznych podłączenia nowego medium teletransmisyjnego,
 - w przypadku konieczności wykonania Planowanych Prac Wykonawca zawiadomi pisemnie Zamawiającego, co najmniej na 7 dni przed ich rozpoczęciem. Planowane Prace powinny być w miarę możliwości wykonywane w soboty, niedziele i inne dni ustawowo wolne od pracy. Planowane Prace nie mogą powodować przerwy w świadczeniu usług w wykonaniu przedmiotu Umowy, dłuższych niż 12 godzin.

1.4. Usługa ochrony przed Atakami DDoS:

a) Informacje ogólne:

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

b) Monitorowanie ruchu:

- 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.
- Usługa monitorowania ruchu musi opierać się na monitorowaniu urządzeń aktywnych Wykonawcy, które wykorzystuje on w realizacji usług dostępu do Internetu dla Zamawiającego.
- Dane zgromadzone w procesie monitoringu muszą być podstawą do sporządzania statystyk ruchu.
- Monitorowanie ruchu na chronionym łączu Zamawiającego musi odbywać się na zasadzie próbkowania w trybie ciągłym w czasie rzeczywistym.

c) Wykrywanie zagrożeń:

- Wykrywanie zagrożeń w ruchu sieciowym musi odbywać się co najmniej na podstawie następujących mechanizmów detekcji:
 - Sygnatury.
 - Przekroczenie wartości progowych dla określonych typów pakietów i protokołów.
 - Wykrywanie anomalii ruchu sieciowego w stosunku do profilu ruchu sieciowego Zamawiającego.
- W ramach usługi Wykonawca monitoruje ruch do i od chronionej podsieci w czasie rzeczywistym.
- Wykonawca musi zapewniać wykrywanie anomalii ruchu sieciowym, co najmniej dla: TCP SYN, TCP RST, TCP Null, ICMP, IP Null, IP Fragmented, DNS.
- W oparciu o dane historyczne system musi określać oczekiwaną wartość ruchu od i do Zamawiającego w danym czasie.
- Wykonawca musi zapewnić wykrywanie anomalii ruchu sieciowego polegających na znacznym przekroczeniu wolumenu ruchu w stosunku do wcześniej wyznaczonych wartości oczekiwanego ruchu dla Zamawiającego.
- Wykonawca musi klasyfikować ruch sieciowy co najmniej na następujące kategorie:
 - Zweryfikowany atak.
 - Fałszywy alarm.
 - Nagły ruch, tj. wzrost woluminu ruchu sieciowego spowodowany inną przyczyną niż atak.
- 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.
- Wykonawca musi powiadamiać Zamawiającego o pojawieniu się alarmów krytycznych, obejmujących co najmniej takie zdarzenia, jak:
 - Potencjalne ataki DDoS.
 - Utrata komunikacji z monitorowanymi zasobami.
 - Inne alarmy wynikające z ustaleń z Zamawiającym.
- Kryteria definiujące wystąpienie zdarzeń oraz poziom, jaki zostanie

przyporządkowany dla poszczególnych zdarzeń musi zostać uzgodniony z Zamawiającym na etapie wdrożenia usługi.

d) Oczyszczanie ruchu - mitygacja.

- 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.
- 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 niepożądanego aktywności, a następnie przekierowaniu go do Zamawiającego.
- Centrum analizy ruchu Wykonawcy nie może znajdować się poza terenem Rzeczypospolitej Polskiej.
- W trakcie mitygacji ruch sieciowy nie może być przekierowany poza teren Rzeczypospolitej Polskiej.
- Ruch w sieci Zamawiającego przekierowany do oczyszczania nie może być wysyłany poza obszar i infrastrukturę, która nie znajduje się pod bezpośrednim nadzorem Wykonawcy.
- Wykonawca musi poddawać ciągłej analizie ruch sieciowy i konfigurację mechanizmów filtracji i w porozumieniu z Zamawiającym dokonywać modyfikacji,
- Wykonawca w ramach świadczonej usługi oczyszczania ruchu musi zapewniać:
 - Ochronę przed atakami wolumetrycznymi o wolumenie do 50 Gb/sek.
 - Filtrowanie ruchu z błędnymi nagłówkami IP, TCP, UDP.
 - Filtrowanie ruchu na określonych portach TCP i UDP na podstawie zawartości pola danych w oparciu o wyrażenia regularne.
 - Odrzucanie lub przepuszczanie ruchu sieciowego na podstawie zdefiniowanych – we współpracy z Zamawiającym – filtrów, operujących na informacjach w nagłówkach.
 - Ochronę przed atakami ze spoofowanymi adresami źródłowymi IP poprzez autentykację sesji TCP, zapytań DNS oraz zapytań http.
 - Filtrowanie nieprawidłowych zapytań DNS.
 - Ograniczenia zapytań DNS do zadanej wartości zapytań na sek.
 - Co najmniej 5 filtrów opartych o wyrażenia regularne, definiujące zakres stosowania autentykacji DNS oraz ograniczania liczby zapytań DNS.
 - Filtrowanie nieprawidłowych zapytań http.
 - Blokowanie ruchu od stacji końcowych przekraczających progi dla operacji HTTP na sekundę per serwer lub per URL.
 - Co najmniej 5 filtrów opartych o wyrażenia regularne, definiujących zakres stosowania autentykacji HTTP lub ograniczania liczby zapytań http.
 - Filtrowanie ruchu w oparciu o wyrażenia regularne dotyczące nagłówków http.
 - Ochronę przed atakami typu slow Lories, poprzez resetowanie połączeń, które pozostają nieaktywne przez zadany okres czasu.
 - Ochronę przed atakami typu slow Lories, poprzez resetowanie sesji TCP, której aktywność jest poniżej zadanej liczby bajtów przesyłanej w zadanym okresie czasu.
 - Wykrywanie ruchu kierowanego z serwerów CDN proxy i stosowanie algorytmów filtrowania na podstawie oryginalnego źródła ruchu
 - Wykrywanie i filtrowanie pakietów z nieprawidłowymi nagłówkami SSL/TLS lub nagłówkami SSL/TLS, które są poza sekwencją.

- Blokowanie sesji, jeżeli podczas negocjacji SSL/TLS klient zażąda nadmiernej ilości metod kryptograficznych lub rozszerzeń użytkownika - próg dla tych wartości musi być konfigurowalny.
 - Wykrywanie i rozłączanie sesji, jeżeli negocjacja SSL/TLS nie zakończy się w zadanym czasie.
 - Blokowanie ruchu ze stacji, dla których występuje nadmierna liczba nieprawidłowych, nadmiarowych lub niekompletnych sesji SSL.
 - 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.
 - Ochronę przed atakami pochodzącym od sieci botnetowych poprzez filtrowanie dzięki na bieżąco aktualizowanym sygnaturom zawierającym listę adresów IP.
 - Ochronę przed atakami pochodzącymi z sieci botnetowych poprzez wykrywanie źródeł ataku o wolumenie przekraczającym zadane wartości.
 - Uruchamianie mitygacji w celu nauczenia się systemu wartości typowych ruchu, które następnie mogą być wykorzystywane do właściwego ustawiania progów dla algorytmów mitygacji.
- Czas uruchomienia automitygacji nie może być dłuższy niż 5 minut od momentu przekroczenia parametrów detekcji złośliwego ruchu.
 - Ruch sieciowy musi być oczyszczany do momentu ustania ataku.
 - 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.

e) Raportowanie.

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

f) Dostęp do panelu użytkownika.

- Wykonawca musi przydzielić Zamawiającemu dostęp do serwisu www dla usługi.
- Zamawiający musi mieć możliwość realizacji dostępu do serwisu poprzez sieć Internet.
- W ramach korzystania z usługi Zamawiający musi mieć nadane co najmniej uprawnienia do odczytu.
- Dostęp do serwisu musi być zabezpieczony w oparciu o technologię IPsec.

- W ramach funkcjonalności serwisu Zamawiający będzie mógł co najmniej:
 - Tworzyć raporty i przeglądać statystyki z analizy ruchu sieciowego.
 - Generować i pobierać raporty w formacie pdf i xml.
 - Wysyłać raporty na wskazany adres email.

g) Wdrożenie usługi.

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

2. **Termin wykonania zamówienia.**

1. Wykonawca dokona uruchomienia usługi w dniu **01.11.2023** r.
2. Zamawiający udostępni Wykonawcy lokal do przeprowadzenia koniecznych prac pod nadzorem pracownika Zamawiającego.
3. Po wykonaniu podłączenia, Zamawiający dokona sprawdzenia prawidłowości jego wykonania oraz protokolarnego odbioru wykonania tej części przedmiotu Umowy.
4. Umowa zostanie zawarta na okres pełnych 24 miesięcy rozliczeniowych.
5. Wykonawca jest związany ofertą 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.