*Załącznik nr 1 do Rozeznania cenowego rynku*

**OPIS PRZEDMIOTU ZAMÓWIENIA**

# Słownik pojęć:

## IP – publiczny adres IP w wersji 4;

## Awaria – rozumiana jako przerwa w działaniu Usługi, z wyłączeniem następujących sytuacji:

### awarii z przyczyn leżących po stronie Zamawiającego,

### braku zasilania, za które winy nie ponosi Wykonawca,

### siły wyższej (zdarzenie o charakterze nadzwyczajnym, niemożliwym wcześniej do przewidzenia. Ciężar wskazania zaistniałych okoliczności spoczywa na Wykonawcy),

### planowanej konserwacji sieci uzgodnionej z wyprzedzeniem z Zamawiającym,

### braku dostępu do urządzeń i okablowania znajdujących się na powierzchni, do których dostęp zapewnia Zamawiający, do których Wykonawca musi otrzymać dostęp w celu wyeliminowania wadliwego ich działania,

### przyczyn leżących po stronie sprzętu i okablowania sieci Zamawiającego nieobjętych Usługą, a także warunków środowiskowych w siedzibie Zamawiającego.

# **Lokalizacja** przyłącza:

## Stałe symetryczne łącze dostępowe we wskazanym przez Zamawiającego pomieszczeniu, w lokalizacji wskazanej w tabeli poniżej:

| **Miasto** | **Adres siedziby zamawiającego** |
| --- | --- |
| Warszawa | Centrum Egzaminowania i Monitorowania MaszynistówAl. Jerozolimskie 211, 02-222 Warszawa |

# Parametry techniczne oraz zakres Usługi:

## zapewnienie przepustowości gwarantowanej dla łącza 500 Mb/s,

## przyłączenie po stronie Zamawiającego do routerów dostępowych będących w posiadaniu Zamawiającego, za pośrednictwem interfejsów FC, zainstalowanych w urządzeniach StormShield SN2100 pracujących w konfiguracji HA. W związku z tym Wykonawca dostarczy przyłącza w takiej formie, by możliwe było wykorzystanie łącza poprzez dowolne z dwóch urządzeń,

## cały sprzęt niezbędny do realizacji Usługi dostarczony przez Wykonawcę i zamontowany we wskazanym przez Zamawiającego pomieszczeniu,

## dostęp do wszystkich usług i serwisów internetowych krajowych i zagranicznych,

## nielimitowana ilość sesji oraz przesyłanych danych, z zastrzeżeniem, że wymaganie to nie dotyczy blokowania ruchu związanego ze zidentyfikowanymi przez Wykonawcę atakami skierowanymi na infrastrukturę Zamawiającego lub blokowania adresacji IP pojedynczych adresów IP bądź całych sieci internetowych (ograniczonych maską – dowolną) przekazanej przez Zamawiającego,

## obsługa adresów IP używanych przez Zamawiającego, przydzielonych przez Wykonawcę w ramach świadczenia Usługi,

## obsługa zgłoszeń w zakresie problemów eksploatacyjnych przez 24 godziny na dobę przez wszystkie dni w roku,

## świadczenie usługi wsparcia technicznego na rzecz wszystkich upoważnionych administratorów Zamawiającego (do 6 osób),

## przydzielenie minimum 30 publicznych adresów IPv4 (maska /27), nie występujących na ogólnodostępnych w sieci Internet czarnych listach (IP Address Blacklist),

## blokowanie adresacji IP przekazanej przez Zamawiającego. Wymóg blokowania na wskazanych przez Zamawiającego łączach internetowych adresów IP bądź całych sieci internetowych (ograniczonych maską – dowolną) na wyraźne każdorazowe (bez limitów czasowych, ilościowych) żądanie Zamawiającego. Blokowanie realizowane na urządzeniach dostępowych Wykonawcy, gdzie czas realizacji zgłoszenia nie może przekroczyć 1 godziny od zgłoszenia przez Zamawiającego,

## umożliwienie Zamawiającemu przez Wykonawcę ustawienia reverse DNS dla poszczególnych adresów IP nazw domen, dla których Zamawiający jest subskrybentem,

## zagwarantowanie przez Wykonawcę rocznej dostępności dla Usługi na poziomie minimum 99,5%. Czas usunięcia Awarii od momentu zgłoszenia nie może być dłuższy niż 4 godziny.

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

### monitorowanie ruchu sieciowego kierowanego do sieci Zamawiającego pod kątem prób ataków DDoS na udostępnioną Usługę w trybie 24/7/365 z ukierunkowaniem na wykrycie anomalii mogących skutkować wysyceniem łącza i utratą ciągłości procesów biznesowych,

### monitoring odbywający się wyłącznie na urządzeniach Wykonawcy bez przekierowywania ruchu poza teren (granice) Rzeczpospolitej Polskiej. Monitoringiem i obsługą incydentów związanych z atakami musi zajmować się wyspecjalizowana jednostka realizująca funkcję wyłącznie nadzoru pracująca w sposób ciągły (24/7/365),

### linię wsparcia, która będzie pełnić funkcję monitoringu i operacyjnej ochrony przed atakami oraz prowadzić ciągły dyżur,

### linię wsparcia (niezależną od linii wymienionej w punkcie poprzednim), która będzie realizowała funkcję poszukiwania i wdrażania niestandardowych rozwiązań związanych z obsługą incydentów bezpieczeństwa,

### ochronę przed wolumetrycznymi atakami DDoS,

### 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 negotiation,

### zapobieganie atakom do przepływności 10 Gbps,

### powiadamianie Zamawiającego (poprzez ustalone kanały komunikacji) w ciągu 15 minut od pojawienia się zagrożeń wskazujących na wystąpienie ataku DDoS,

### przekierowywanie ruchu w przypadku podejrzenia wystąpienia ataku do dedykowanych do tego celu zasobów wewnętrznych Wykonawcy, zlokalizowanych na terytorium Rzeczpospolitej Polskiej, w ciągu 20 minut od zgłoszenia przez Zamawiającego. Brak przekierowania ruchu po upływie ww. 20 minut będzie traktowane jako Awaria,

### zastosowanie filtrowania ruchu za pomocą „blacklist” oraz „whitelist” w czasie nie dłuższym niż 2 godziny od wykrycia incydentu,

### filtrowanie ruchu sieciowego (odrzucanie pakietów pochodzących ze źródeł ataku, zanim właściwy ruch zostanie przekazany do Zamawiającego) przy możliwie jak najmniejszym wpływie na ruch uprawniony oraz przekierowywanie odfiltrowanego ruchu do Zamawiającego,

### dostęp dla Zamawiającego do panelu usługi DDoS, za pośrednictwem którego będzie możliwość pełnego monitoring systemu ochrony DDoS,

### przyjmowanie wnioskowanych przez Zamawiającego zmian parametrów usługi systemu ochrony DDoS oraz ich implementację po wcześniejszym skonsultowaniu ze specjalistami Zamawiającego, że wdrażane zmiany nie spowodują negatywnych skutków dla funkcjonowania łącza internetowego Zamawiającego,

### przygotowanie dla Zamawiającego raportu po zakończeniu oczyszczania ruchu po zaistniałym ataku DDoS.