SZPZLO
WARSZAWA-TARGÓWEK

Samodzielny Zespół Publicznych Zakładów
Lecznictwa Otwartego Warszawa-Targówek

SZPZLO W-T 366/2016

Warszawa, dn. 29.11.2016 r.

Samodzielny Zespół Publicznych Zakładów Lecznictwa Otwartego Warszawa-Targówek zaprasza do składania ofert na **Dzierżawę łącz światłowodowych oraz zapewnienie dostępu do Internetu dla SZPZLO Warszawa-Targówek** o wartości poniżej 30 000 EUR.

Informacje niezbędne do sporządzenia oferty:

1. Połączenie światłowodem „ciemnym włóknem" o przepustowości 10 Gbit/s oddziałów:
   - ul. Balkonowa 2
   - ul. Balkonowa 4
   - ul. Łojewska 6
   - ul. Poborzańska 6
   - ul. Rembielińska 8
   - ul. Remiszewska 14

   z serwerownią na ul. Tykocińskiej 34 w Warszawie
2. Dostarczenie do serwerowni przy ul. Tykocińskiej Internetu światłowodem min. 200 Mbit/200 Mbit symetrycznie z min. 16 publicznymi adresami IP oraz podziału go na odziały. Backupowy Internet min. 20 Mbit za pomocą sieci LTE.
3. Dostarczenie routera dostępowego w Centrali (Tykocińska 34) oraz 7 szt. switchy dostępowych w oddziałach:
   - ul. Balkonowa 2
   - ul. Balkonowa 4
   - ul. Łojewska 6
   - ul. Poborzańska 6
   - ul. Rembielińska 8
   - ul. Remiszewska 14
   - ul. Tykocińska 34
4. Zamawiający wymaga połączenia pomiędzy oddziałami a centralą za pomocą „ciemnego włókna" /bez urządzeń aktywnych pośredniczących do transmisji danych (sieć LAN)/ o przepustowości 10Gbit/s.

ul. Tykocińska 34, 03-545 Warszawa
Sekretariat tel. 22 518 26 41, fax 22 518 26 44
e-mail: sekretariat@zoztargowek.waw.pl, www.zoztargowek.waw.pl
NIP 524-27-48-756, Regon: 145950090, konto: PEKAO S.A. 33 1240 6074 1111 0010 4364 7094

5. Operator dostarczy następujące urządzenia: router, switche, wkładki, media konwertery itd. do centrali oraz oddziałów niezbędne do uruchomienia świadczenia usługi oraz skonfiguruje sprzęt według potrzeb Zamawiającego.
   W ofercie należy podać zaproponowane modele oraz specyfikację dostarczonych urządzeń.
   Minimalne warunki dla routera w centrali:
   - 8x SFP+ port
   - taktowanie procesora - 1 GHz
   - ilość rdzeni – 72
   - RAM 16GB

   Minimalne wymagania switchy:
   - 2x SFP+ port
   - 24 10/100/1000 Ethernet ports
6. Zamawiający wymaga przeszkolenia personelu z obsługi dostarczonych urządzeń min. 100 h w siedzibie zamawiającego w 2 pierwszych miesiącach świadczenia usługi.
7. Zamawiający wymaga suportu (wsparcie IT 24/dobę) w ramach umowy.
8. Sprzęt używany do transmisji danych (routery, switche) wraz z kompletem wkładek lub media konwerterów po okresie umowy przechodzi na własność Zamawiającego.
9. Zamawiający wymaga ochrony DDOS dla łącza światłowodowego do Internetu. Opis wymagań ochrony DDoS stanowi załącznik numer 1.
10. Okres umowy od 01.01.2017 r. do 31.01.2018 r.
11. Oferty należy składać w siedzibie Zamawiającego,
    Samodzielny Zespół Publicznych Zakładów Lecznictwa Otwartego Warszawa-Targówek, ul. Tykocińska 34, 03-545 Warszawa
    w sekretariacie do godziny 10:00 do dnia 05.12.2016 r.
    lub drogą elektroniczną na adres: dyrektor@zoztargowek.waw.pl
12. Termin składania ofert upływa dnia 05.12.2016 r. o godz. 10.00.

DYREKTOR
Marcin Jakubowski

Opis wymagań ochrony DDoS – załącznik nr 1 do zapytania ofertowego

1. **Łącze dostępu do Internetu**
   1) Zamawiający wymaga zapewnienia usługi ochrony przed atakami DDoS realizowanej jako usługi powiązanej z symetrycznym łączem dostępu do Internetu dostarczanym w ramach zamówienia dla całej udostępnionej przepustowości łącza. Usługa będzie świadczona dla całej adresacji IP Zamawiającego na dostarczanym łączu internetowym.
   2) W ramach realizacji usługi ochrony przed atakami DDoS, Zamawiający wymaga zapewnienia co najmniej:
      a) analizy ruchu w celu identyfikacji typu i natury ataku,
      b) powiadamianie Zamawiającego o podejrzeniu wystąpienia ataku,
      c) rozpoczęcie usuwania ataku w porozumieniu z Zamawiającym (możliwe jest automatyczne uruchamianie obrony dla alarmów o wysokim poziomie zagrożenia),
      d) modyfikację zestawu użytych mechanizmów przeciwdziałania tak, by uzyskać maksymalny poziom filtracji ruchu niepożądanego przy minimalnym wpływie na ruch prawidłowy,
      e) klasyfikację alarmów typu DDoS jako:
         - zweryfikowany atak,
         - fałszywy alarm,
         - nagły ruch – znaczący wzrost ruchu spowodowany inną przyczyną niż atak na daną usługę Zamawiającego.

2. **Wykrywanie zagrożeń**
   1) Zamawiający wymaga zapewnienia efektywnej identyfikacji potencjalnych ataków DDoS z wykorzystaniem co najmniej poniższych mechanizmów detekcji:
      a) Sygnatury,
      b) przekroczenie progów dla określonych typów pakietów i protokołów,
      c) oparte na analizie profilu ruchu Zamawiającego wykrywanie nieoczekiwanych zmian ruchu w odniesieniu do tego profilu.
   2) Usługa monitoruje ruch do i od chronionej podsieci w czasie rzeczywistym, w tym w odniesieniu do poszczególnych usług Zamawiającego. Lista usług Zamawiającego realizowanych na udostępnionym łączu, zgłoszonych przez Zamawiającego w terminie uruchomienia łącza i ochrony przed atakami DDoS, jest listą otwartą i może się zmieniać z dnia na dzień w okresie realizacji Umowy, w zależności od uruchamianych / kasowanych usług Zamawiającego.
   3) Usługa zapewnia wykrywanie anomalii polegających na przekroczeniu wartości uważanych za normalne w ruchu Internetowym, w szczególności pakietów TCP SYN, TCP RST, TCP Null, ICMP, IP Null, IP Fragmented, DNS, IP Private, UDP.
   4) System realizujący usługę na podstawie danych historycznych wyznacza oczekiwaną wartość ruchu do i od chronionej podsieci o danej porze dnia w danym dniu tygodnia, w odniesieniu do poszczególnych usług Zamawiającego.
   5) Usługa zapewnia wykrywanie anomalii polegających na znaczącym przekroczeniu wolumenu ruchu oraz wykrywanie potencjalnych ataków w warstwie aplikacyjnej dla poszczególnych usług Zamawiającego w stosunku do wcześniej wyznaczonych wartości oczekiwanych ruchu.

3. **Mitygacja – oczyszczanie ruchu**
   1) Zamawiający wymaga zapewnienia usługi ochrony przed atakami DDoS polegającej na usuwaniu ataku przy możliwie jak najmniejszym wpływie na ruch uprawniony. Efektywne działanie powinno obejmować trzy procedury:
      a) Procedura uruchamiana w przypadku podejrzenia wystąpienia ataku, ruch przekierowany zostanie do dedykowanych do tego celu zasobów wewnętrznych Wykonawcy,
      b) Procedura filtrowania oparta o wielowarstwową analizę ruchu i mechanizmy przeciwdziałania,
      c) Procedura oparta o kierowanie odfiltrowanego ruchu z powrotem do Klienta.
   2) Zamawiający wymaga ochrony co najmniej przed następującymi typami ataków:
      - TCP SYN flood
      - UDP flood (w tym DNS reflection)
      - HTTP GET flood
      - HTTP POST flood
      - ICMP flood
      - IGMP flood
      - invalid packets
      - IP fragments
      - IP NULL
      - DNS flood
      - SIP request flood
      - SSL negotiation

4. **Poziom SLA dotyczący powiadomienia o ataku**
   1) **Czas Reakcji na Atak (CRA)**:
      a) przez CRA rozumie się czas, jaki upłynie od wykrycia Ataku DDoS do rozpoczęcia skutecznego telefonicznego poinformowania Zamawiającego, przez ustalone kanały komunikacji,
      b) przez skuteczny kontakt z Zamawiającym rozumie się: rozmowę z Zamawiającym oraz jego poprawną autoryzację,
      c) czas CRA liczony jest od momentu zaraportowania na platformie ataku do czasu zarejestrowania w systemie teleinformatycznym Wykonawcy czasu dokonania pierwszej czynności mającej na celu poinformowanie Zamawiającego (czas wykonania rozmowy telefonicznej, wysłania SMS-a, wysłania e-maila),
      d) CRA liczone jest w następujący sposób: kontakt Wykonawcy z Zamawiającym – czas mierzony jest od momentu wykrycia ataku przez system Wykonawcy do momentu próby wykonania pierwszego telefonicznego kontaktu z Zamawiającym (zgodnie z listą osób/numerów i priorytetami wskazanym przez Zamawiającego). Każda próba kontaktu będzie wykonywana przez Wykonawcę co dwie minuty w maksymalnym czasie łącznym CRA. Jeśli nie dojdzie do skutecznego kontaktu w pierwszej próbie Wykonawca zobowiązany jest do wykonania następnej próby do kolejno wskazanych osób/numerów
      z listy kontaktów. W przypadku niemożności uzyskania połączenia z Zamawiającym w czasie CRA we wszystkich próbach kontaktu, Wykonawca wysyła SMS do grupy adresowej z informacją o zanotowanym ataku,

e) w przypadku ochrony na żądanie ochrona nie będzie włączona do momentu skutecznego kontaktu z Zamawiającym i potwierdzenia decyzji o włączeniu lub nie ochrony,
f) wartość parametru CRA wynosi 15 minut.

2) **Czas Reakcji na Zlecenie oczyszczania ruchu (CRZ)**:
   a) przez CRZ rozumie się czas, jaki upłynie od przyjęcia Zlecenia od Zamawiającego z żądaniem włączenia lub wyłączenia oczyszczania po zarejestrowanym Ataku.
   b) wartość parametru CRZ wynosi 15 minut.

5. Raporty miesięczne

Zamawiający wymaga umieszczania w comiesięcznych protokołach odbioru usługi w punkcie dotyczącym ochrony przed atakami DDoS, informacji zawierających co najmniej następujące statystyki:

a) uśredniony poziom ruchu wchodzącego i wychodzącego
b) maksymalne poziomy ruchu
c) liczba zarejestrowanych ataków
d) liczba usuniętych ataków.

6. Raport z incydentu

Zamawiający wymaga każdorazowo po zakończeniu operacji oczyszczania ruchu po zaistniałym ataku sporządzenia raportu z incydentu. Sposób inicjowania oraz zakończenia procedury zostanie uzgodniony z Zamawiającym. Informacja w raporcie o incydencie zawierać będzie co najmniej następujące statystyki:

a) rozmiar ataku, liczniki pakietów, Gb/s oraz procent całości ruchu
b) czas trwania ataku
c) główne źródła ataku
d) typ i natura ataku
e) wdrożone metody eliminacji ataku
f) geograficzna lokalizacja źródeł ataku
g) wielkość oczyszczonego ruchu
h) czasy – w szczególności: początek ataku, powiadomienie, wdrożenie procedur obronnych, zakończenie ataku, przywrócenie normalnej pracy sieci.

7. Obszar działania usługi

Zamawiający wymaga aby ruch w sieci Zamawiającego przekierowany do oczyszczania był wysyłany wyłącznie na obszar znajdujący się pod bezpośrednim nadzorem służb technicznych Wykonawcy na terenie Polski.

8. Czas świadczenia usługi

Zamawiający wymaga świadczenia usługi ochrony przed DDoS w trybie 24/7/365.

9. Procedura przerwania mitygacji – Fall-back Procedure

Jeśli uruchomiona procedura eliminacji DDoS ma negatywny wpływ na chronione zasoby lub usługi, Zamawiający ma możliwość zlecenia jej przerwania, co następuje w ciągu 15 minut od momentu zlecenia przez Zamawiającego (godzina, minuta). Pomimo przerwania akcji, ruch Klienta cały czas podlega monitorowaniu i istnieje możliwość przywrócenia procedur obronnych w odpowiednio dostosowanym zakresie i analogicznym czasie wdrożenia.

10. Alarmy i sposób powiadamiania Klienta:

Wykryte w ramach realizacji usługi zdarzenia zostaną przyporządkowane do jednej z niżej opisanych przykładowych grup alarmów:

Kategoria alarmu	*Opis*	*Akcja / Czas reakcji*	*Przykład*
KRYTYCZNA (Servity High)	Alarm o największym stopniu zagrożenia dla Zamawiającego.	Automatycznie rozpoczęcie akcji oczyszczania w sytuacjach uzgodnionych z Zamawiającym. Przystąpienie do rozwiązywania problemu przez Wykonawcę. Do Zamawiającego zostanie wysłane powiadomienie o zaistnieniu potencjalnego ataku DDoS w czasie zdefiniowanym przez SLA.	Alarmy w tej kategorii zawierają m. in.: • potencjalne ataki DDoS • utrata komunikacji z monitorowanymi zasobami. • inne alarmy na podstawie ustaleń z Zamawiającym.
WAŻNA (Servity Medium)	Alarm, który w późniejszym czasie może wymagać akcji ze strony Wykonawcy lub Zamawiającego.	Podjęcie działań, jeśli to konieczne, ze strony Wykonawcy lub Zamawiającego. Informowanie Zamawiającego o zaistniałej sytuacji.	Informacje na temat ruchu nie związane z wystąpieniem nieprawidłowości.
INFORMACYJNA (Servity Low)	Zapis informacji o ataku.	Brak działania. Brak konieczności informowania Zamawiającego.	Zdarzenia związane z działaniami systemu lub jego rekonfiguracją np. planowy update sygnatur.

Kryteria definiujące wystąpienie zdarzeń oraz poziom, jaki zostanie przyporządkowany dla poszczególnych zdarzeń zostaną uzgodnione z Zamawiającym.

11. Implementacja usługi

1) **Projekt wykonawczy**

Po podpisaniu Umowy na świadczenie usługi, przy współpracy z Zamawiającym, Wykonawca utworzy Projekt wykonawczy. Dokument zawierać będzie m. in.:

a) opis techniczny integracji usługi z siecią Zamawiającego,
b) opis procedur powiadamiania i eskalacji,
c) testy akceptacyjne,
d) opis procedur obsługi zgłoszeń i raportowania,
e) jednocześnie Wykonawca przeprowadzi w siedzibie Zamawiającego dla pracowników Komórki IT (3 osoby), szkolenie w zakresie działania usługi, obsługi zgłoszeń i raportowania, a w szczególności aspektów dotyczących ochrony przed atakami DDoS.

2) **Implementacja**

Implementacja obejmuje rekonfigurację urządzeń Zamawiającego oraz Wykonawcy pod kątem monitorowania ruchu oraz uruchomienia usługi przeciwdziałania atakom DDoS.

3) **Testy akceptacyjne**
   a) Po zakończeniu Implementacji Zamawiający wraz z Wykonawcą przeprowadzą Testy akceptacyjne zgodnie z uzgodnionym Projektem wykonawczym
   i stanowiące test funkcjonalny platformy ochrony przeciwko atakom DDoS. Testy uwzględnią weryfikację poprawności wdrożonej konfiguracji.
   b) Przed wdrożeniem pełnej funkcjonalności usługi DDoS Zamawiający wymaga przeprowadzenia, w okresie pełnego miesiąca kalendarzowego od terminu uruchomienia usługi, Procesu analizy ruchu Abonenta, proces w którym ruch zdefiniowany w ramach danego obiektu kierowany jest do platformy ochrony przed atakami DDoS Wykonawcy. Ruch podczas tego procesu nie podlega żadnym filtracjom i w sposób niezmieniony kierowany jest do sieci użytkownika. Platforma podczas przedmiotowego procesu nauczania zbiera statystyki, na których podstawie jest w stanie określić parametry algorytmów mitygacji (countremeasures) tak, aby w trakcie ataku zachować ruch użytkowników, a odfiltrować ruch ataku. Ze względu na specyfikę poszczególnych usług Zamawiającego realizowanych na udostępnionym łączu, dla wybranych usług Zamawiającego termin wdrożenia pełnej funkcjonalności usługi DDoS może być przedłużony w porozumienie Zamawiającego z Wykonawcą.

12. Dostęp do infrastruktury Klienta

W uzasadnionych przypadkach, świadczenie usługi może być powiązane z dostępem do urządzeń aktywnych zarządzanych przez Zamawiającego, w celu uzyskania statystyk ruchu otrzymywanego oraz wysyłanego do sieci Wykonawcy.