Ogłoszenie powiązane:

Ogłoszenie nr 168049-2014 z dnia 2014-08-04 r. Ogłoszenie o zamówieniu - Warszawa

1. Przedmiotem zamówienia jest usługa zestawienia, uruchomienia i obsługi przewodowego łącza dostępowego do sieci Internet. 2. Przedmiot zamówienia obejmuje zestawienie, uruchomienie i obsługę stałego, symetrycznego, przewodowego...

Termin składania ofert: 2014-08-12

Numer ogłoszenia: 176527 - 2014; data zamieszczenia: 14.08.2014

OGŁOSZENIE O ZMIANIE OGŁOSZENIA

Ogłoszenie dotyczy: Ogłoszenia o zamówieniu.

Informacje o zmienianym ogłoszeniu: 168049 - 2014 data 04.08.2014 r.

SEKCJA I: ZAMAWIAJĄCY

Komendant Stołeczny Policji, ul. Nowolipie 2, 00-150 Warszawa, woj. mazowieckie, tel. 22 6038608. 6037691, fax. 22 6037642.

SEKCJA II: ZMIANY W OGŁOSZENIU

II.1) Tekst, który należy zmienić:

Miejsce, w którym znajduje się zmieniany tekst: II.1.4).

W ogłoszeniu jest: 2. lit. k) wykreowanie dla Zamawiającego routingu BGP, co da możliwość Zamawiającemu zarządzania i tworzenia scenariuszy zarządzania ruchem IP na różnych dostępach do Internetu. 3. Wykonawca zapewni - na żądanie Zamawiającego - świadczenie dodatkowej usługi w zakresie zabezpieczenia internetowego użytkownika przed atakami DDoS. Świadczenie usługi winno nastąpić w terminie nie przekraczającym 7 dni licząc od dnia podpisania odrębnej umowy w tym zakresie..

W ogłoszeniu powinno być: 2. lit. k) możliwość wykreowania dla Zamawiającego routingu BGP (w przypadku dysponowania przez Zamawiającego własną pulą adresową), co da możliwość Zamawiającemu zarządzania i tworzenia scenariuszy zarządzania ruchem IP na różnych dostępach do Internetu. 3. Zamawiający zastrzega sobie możliwość skorzystania w okresie obowiązywania umowy z prawa opcji w zakresie usługi zabezpieczenia łącza internetowego użytkownika przed atakami DDoS. Skorzystanie przez Zamawiającego z prawa opcji odbędzie się poprzez złożenie Wykonawcy jednostronnego oświadczenia w formie zlecenia. Świadczenie usługi winno nastąpić w terminie nie przekraczającym 7 dni roboczych od dnia przesłania zlecenia. Zamawiający wymaga aby: + Rozwiązane powinno monitorować ruch w sposób ciągły (24/7/365), z ukierunkowaniem na wykrycie anomalii mogących skutkować wysyceniem łącza i w efekcie utratą ciągłości procesów biznesowych. + w trakcie mitygacji pakiety nie mogą być przekierowane poza teren Polski + usługa powinna zapewniać ochronę przed atakami o wolumenie + Monitoringiem i obsługą incydentów związanych z atakami DDoS musi zajmować się wyspecjalizowana jednostka organizacyjna działająca w trybie 24/7/365 + Monitorowanie ruchu powinno być przeprowadzane przy wykorzystaniu technologii bazujących na przepływach pakietów IP (ang.IP flow) takich jak np. NetFlow czy sFlow. + Informacje o wszystkich połączeniach do systemów usługowych Zamawiającego poprzez wykorzystanie protokołu typu NetFlow lub podobne + usługa powinna zapewniać comiesięczny raport obejmujący: wykres ilustrujący wolumen ruchu do i z chronionej podsieci, lista alarmów, lista mityzacji + system realizujący usługę powinien na podstawie danych historycznych wyznaczać oczekiwaną wartość ruchu do i od chronionej podsieci o danej porze dnia w danym dniu tygodnia. + usługa powinna

zapewniać odrzucanie lub przepuszczanie na bazie zdefiniowanych dla każdego z klientów filtrów operujących na informacjach w nagłówka warstwy 3-ciej i 4-tej modelu OSI + Przełączanie ruchu Zamawiającego w przypadku ataku powinno być realizowane za pomocą protokołu BGP. + Rozwiązanie powinno umożliwiać stosowanie szeregu technik w celu mityzacji ataków DDoS, takich jak co najmniej: - Blokada niedozwolonych zapytań http przy wykorzystaniu wyrażeń regularnych; - Blokada niedozwolonych zapytań DNS przy wykorzystaniu wyrażeń regularnych; - Wykrywanie i blokada ataków typu TCP SYN, TCP RST, TCP Null, ICMP, IP Null, IP Fragmented flood, ataków na protokoły poprzez eliminację źródeł które przekroczą zdefiniowany próg (bps, pps); - Geolokalizacja adresów IP, umożliwiająca blokadę ruchu pochodzącego z danego kraju bądź regionu geograficznego; - Dopuszczanie, blokada, lub ograniczenie pasma (policing) dla ruchu pochodzącego z krajów z którymi w normalnych warunkach Zamawiający nie utrzymuje stosunków handlowych; - Listy przepuszczające ruch z krytycznych serwisów i lokacji, lub blokujące spoofowane adresy oraz ruch obserwowany na niewłaściwych portach; - Listy przepuszczające ruch pochodzący ze znanych i zaakceptowanych lokalizacji, oraz blokujące ruch pochodzący od zainfekowanych hostów i serwerów będących pod kontrolą botnetów; - Monitorowanie podsieci i protokołów w celu identyfikacji ruchu o parametrach wyższych niż zdefiniowane; - Inspekcja ruchu w celu identyfikacji ataków przeprowadzanych na podatności payload; - Ochrona przed przepełnieniem tablicy stanu dla serwerów, firewall i urządzeń równoważących obciążenie; - Ochrona serwerów przed atakiem polegającym na podtrzymywaniu bezpodstawnie długiej sesji; - Ochrona przed atakami typu flash crowd poprzez ograniczenie ruchu do poziomu pozwalającego na normalne funkcjonowanie chronionego hosta; - Ochrona serwerów SIP poprzez przepuszczanie zapytań zgodnych z RFC oraz pochodzących z właściwych źródeł; - Ochrona serwerów web poprzez przepuszczanie zapytań http zgodnych z RFC oraz pochodzących z właściwych źródeł; - Ochrona serwerów DNS przed atakami typu DNS reflection atack, cache poisoning, resource exhausion poprzez przepuszczanie zapytań DNS zgodnych z RFC oraz pochodzących z właściwych źródeł; - Powinna istnieć możliwość zastosowania dodatkowych narzędzi (np. blackholing, niezależne blokowanie ruchu z adresów IP z zagranicy do atakowanego adresu) zwiększających pewność znacznego ograniczenia lub usunięcia wpływu ataku na usługi Zamawiającego, - Rozwiązanie musi zapewniać dostęp do statystyk i panelu zarządzania dla klienta, w trybie do odczytu , w szczególności musi zapewniać: - Dostęp do statystyk ruchu na podstawie Netflow, Jflow itd. - Dostęp do raportów generowanych przez system - Dostęp do listy wykrytych ataków - Dostęp do listy akcji wykonanych w celu ograniczenia wpływu ataków - tryb oczyszczania - Możliwość zapisywania raportów w formie PDF/XML z poziomy konsoli WebUl - Dostęp do zarządzania powinien odbywać się szyfrowanym kanałem (np. HTTPS). - Urządzenie zarządzające po stronie operatora musi być chronione rozwiązaniem typu WAF (Web Application Firewall). - W ramach usługi konieczne jest zapewnienie całodobowej gotowości do podjęcia reakcji w 15 minut od wykrycia ataku. - Konieczne jest niezwłoczne informowanie oraz raportowanie do Zamawiającego po każdym wykrytym ataku DDoS oraz ścisła współpraca pomiędzy zespołem Zamawiającego i scrubbing center. - Należy dostarczać okresowe raporty na temat monitorowanego ruchu oraz ilości ataków DDoS przeprowadzonych na infrastrukturę. + Usługa powinna być dostępna na poziomie SLA co najmniej 99.5% (downtime roczny: 3dni, miesięczny: 7h). - Rozwiązanie musi zapewniać blokowania/ograniczanie ruchu na poziomie styku z operatorem - łącze do klienta musi być ograniczone lub oczyszczone z ruchu spowodowanego atakiem Dos - Rozwiązanie powinno mieć możliwość integracji z urządzeniami ochrony DDoS po stronie klienta, zainstalowanym bezpośrednio na zakończeniu łącza po stronie klienta, w szczególności: - Przekazywanie informacji o atakach wykrytych po stronie klienta - o możliwość włączania trybu oczyszczania z poziomu konsoli zarządzającej urządzeniem po stronie klienta WebUl - o możliwość automatycznego wymuszania trybu czyszczenia na podstawie informacji o ruchu i atakach wykrytych przez urządzenie klienta - Ruch nie powinien wychodzić poza granice Polski - Wielkości ruchu podlegającego ochronie DDOS na poziomie 50 Mbps.

Miejsce, w którym znajduje się zmieniany tekst: IV.4.4).

W ogłoszeniu jest: Termin składania ofert : 18.08.2014 godzina 11:00.

W ogłoszeniu powinno być: Termin składania ofert: 21.08.2014 godzina 12:00.