Załącznik nr 5 do umowy _____

PROCEDURA WSPÓŁPRACY I DZIAŁANIA W PRZYPADKU WYSTĄPIENIA ATAKU TYPU DDOS

Klient ma możliwość zablokowania niepożądanego ruchu, generowanego w obrębie sieci Internet i kierowanego poprzez sieć szkieletową operatora [nazwa operatora] do jego własnych zasobów, za pomocą mechanizmu „black-hole". Mechanizm „Black-hole", powoduje że niepożądany ruch zamiast być kierowanym do sieci klienta, zostaje dropowany. Dropowaniu podlegają wszystkie pakiety kierowane na docelowy adres IP z podsieci użytkowanych przez klienta. Decyzję o tym jaki adres IP z podsieci klienta będzie podlegał blokowaniu podejmuje klient który informuje operatora za pomocą poniższej procedury.

1. Podstawowa procedura działań gwarantuje wykonanie analizy i uzgodnionych działań w przeciągu [zgodnie z ofertą Wykonawcy] godzin. W ramach usługi ochrony DDoS, operator [nazwa operatora] gwarantuje terminowe wykonanie procedur ochronnych i dostęp do inżynierów sieciowych, oraz dołoży wszelkich starań, aby ograniczyć skutki ataku DDoS, w jak najkrótszym czasie.
2. Klient nawiązuje kontakt poprzez wysłanie e-maila na adres: _____ lub numer telefonu: _____.
3. E-mail lub zgłoszenie telefoniczne muszą zawierać:
   1) dane identyfikujące usługę w temacie wiadomości email Pomoc przy ataku DDOS Centrum Usług Infromatycznych
   2) adresację sieci połączeniowej dla sesji BGP;
   3) czas wystąpienia zdarzenia;
   4) zlecenie zablokowania ataku z podaniem konkretnych adresów IP lub całych prefiksów w stronę wskazanych przez Klienta adresów;
   5) opcjonalnie dodatkowe informacje zebrane przez Klienta na temat anomalii występujących w ruchu do Klienta mogące pomoc w podjęciu decyzji o ewentualnym blokowaniu ruchu i wyeliminowaniu ataku DDoS przez operatora [nazwa operatora]
4. Email lub zgłoszenie telefoniczne zostanie zarejestrowane w systemie operatora [nazwa operatora] i przekazane do diagnozy i podjęcia działań prewencyjnych.
5. Zgłoszenie od klienta drogą mailową lub telefoniczną zostanie potwierdzone e-mailem zwrotnym z informacją o odebraniu zgłoszenia nie później niż w ciągu [zgodnie z ofertą Wykonawcy] godzin od jego otrzymania.
6. Wszelkie informacje zwrotne ze strony operatora [nazwa operatora], będą przesyłane na adres: dmstd@cui.wroclaw.pl oraz przekazane telefonicznie na numery wskazane w umowie.

7. Operator [nazwa operatora] rozpoczyna analizę i identyfikację zdarzenia. W ciągu [zgodnie z ofertą Wykonawcy] godzinach od otrzymania zgłoszenia, pracownik operatora [nazwa operatora] powiadamia klienta telefonicznie lub e-mailem na temat propozycji działań ochronnych wraz z informacjami kontaktowymi takimi jak numer telefonu oraz e-mail do Inżyniera wsparcia, który będzie odpowiedzialny za prowadzenie ochrony sieci Klienta. Klient może zostać poproszony o przedstawienie krótkiego opisu problemu oraz potwierdzenia że zdarzenie może mieć charakter ataku DDoS. Następnie Inżynier wsparcia blokuje atak DDoS na wskazany przez Klienta adres.
8. Operator [nazwa operatora] po wykonaniu procedury ochrony, przed zamknięciem zgłoszenia, przekaże informacje o wielkości generowanego ruchu na zablokowany adres, oraz listę źródłowych adresów IP generujących ruch na zablokowany adres.
9. Zamknięcie zgłoszenia przez operatora [nazwa operatora] możliwe jest tylko po potwierdzonym przez klienta fakcie zadziałania procedur ochronnych.
10. Klient po zamknięciu zgłoszenia, aby odblokować adresy IP musi poinformować operatora [nazwa operatora]za pomocą emaila. W treści emaila muszą zostać uwzględnione wszystkie adresy lub prefixy do odblokowania.
11. Technika ochrony Klienta: Blackholing - skutecznie chroni usługobiorcę przed atakiem, ale wyklucza pojedynczy adres lub cały prefiks z ruchu przez skierowanie go do "czarnej dziury". Zyskiem jest ochrona sieci klienta, kosztem zablokowanego hosta lub grupy hostów.