Centrum Informatyki Statystycznej

Znak: CIS-WAZ.2720.18.2020

Warszawa, dnia 14.07.2020 roku

Dotyczy: zapytania ofertowego CIS-WAZ.2720.18.2020 z dnia 08.07.2020 r. na **„Kompleksowe świadczenie usługi dostępu do Internetu wraz z usługą ochrony przed atakami DDos, jako drugi, niezależny operator, na potrzeby sieci korporacyjnej Głównego Urzędu Statystycznego"**.

W dniu 13 lipca 2020 r. do Zamawiającego wpłynęły następujące pytania:

**Pytanie 3**

Ad. Zał.1 OPZ, Pkt I, ppkt. 2.1 Zamawiający wymaga aby ochrona przed atakami DDoS realizowana była w sposób proaktywny na urządzeniach w sieci Wykonawcy bez przekierowywania ruchu poza teren Rzeczypospolitej Polskiej.

Pytanie:

Prosimy o wyjaśnienie przyczyn umieszczenia takiego zapisu. Chcielibyśmy zaznaczyć że Wykonawca będzie odpowiedzialny za świadczenie usługi dostępu do sieci Internet, która z natury jest siecią ogólnoświatową i nieograniczoną. Podczas korzystania z usługi Zamawiający przewiduje możliwość korzystania z zasobów światowych a z drugiej strony w momencie ataku nie dopuszcza możliwości podjęcia działań Wykonawcy w swojej sieci poza granicami kraju.

Biorąc pod uwagę fakt, że znaczna większość ataków DDoS ma swoje źródło poza granicami RP oraz zważając na dobre praktyki podczas realizowania ochrony przed atakami wolumetrycznymi, które nakazują podejmowania działań jak najbliżej źródła ataku (często takie działanie polega na przekierowanie ruchu podczas ataku już z punktów styku Wykonawcy do centrum mitygacyjnego a następnie kierowanie oczyszczonego ruchu w stronę Zamawiającego), pragniemy podkreślić, że w naszej opinii wskazany zapis jest pozbawiony merytorycznego uzasadnienia, a wręcz wyklucza z postępowania dużych operatorów telekomunikacyjnych, posiadających spójną, paneuropejską sieć oraz urządzenia zlokalizowane w największych europejskich punktach wymiany ruchu, jednocześnie preferując lokalnych operatorów mających sieć i urządzenia tylko na terenie RP.

W związku z powyższym – czy Zamawiający dopuszcza zmianę w/w zapisu na:
„2.1 Zamawiający wymaga aby ochrona przed atakami DDoS realizowana była w sposób proaktywny na urządzeniach w sieci Wykonawcy".

**Odpowiedź 3**

Zamawiający dopuszcza zmianę zapisu Ad. Zał.1 OPZ, Pkt I, ppkt. 2.1 Zamawiający wymaga aby ochrona przed atakami DDoS realizowana była w sposób proaktywny na urządzeniach w sieci Wykonawcy bez przekierowywania ruchu poza teren Rzeczypospolitej Polskiej" na następujący „2.1 Zamawiający wymaga aby ochrona przed atakami DDoS realizowana była w sposób proaktywny na urządzeniach w sieci Wykonawcy".

**Pytanie 4**

Ad. Zał.1 OPZ, Pkt. I, ppkt. 3 Zamawiający wymaga świadczenia usługi DNS Secondary

Pytanie:

Bardzo prosimy o podanie ilości domen, dla których miałaby być świadczona usługa DNS Secondary

**Centrum Informatyki Statystycznej**

Aleja Niepodległości 208, 00-925 Warszawa
tel. 22 608 31 44
cissek@stat.gov.pl
cis.stat.gov.pl

**Odpowiedź 4**

W chwili obecnej Zamawiający posiada 8 domen zarejestrowanych w domenie gov.pl i obsługiwanych przez 2 serwery DNS. W przypadku zarejestrowania nowych domen przez Zamawiającego, Wykonawca musi świadczyć usługę secondary DNS również dla nowo zarejestrowanych domen. Zamawiający ma wdrożony protokół DNSSEC

**Pytanie 5**

Odnośnie Państwa wymagań dot. antyDDOsa, czy akceptujecie Państwo fakt, iż nasza usługa w poszczególnych punktach spełnia Państwa wymagania częściowo lub proponujemy inne rozwiązanie.
Poniżej szczegóły dla wymagań, które spełniamy częściowo lub proponujemy alternatywne rozwiązanie:

2.3 Usługa powinna monitorować ruch do sieci Zamawiającego w czasie rzeczywistym oraz zapewniać ochronę przez co najmniej następującymi typami ataków: TCP SYN flood, UDP flood, DNS reflection, DNS flood, http GET flood, http POST flood, ICMP flood.

Nasza usługa częściowo spełnia wymaganie. Dla HTTP GET/POST flood możemy zrobić dynamiczny policer uwzględniający specyfikę Państwa potrzeb.

Może to ograniczyć np. liczbę zapytań HTTP na sekundę spoza Europy per źródłowy adres IP i ścieżkę (URI), ale bez nagłówka "Host".Nie obejmie to również ruchu szyfrowanego. W praktyce filtrowanie HTTP flood po Państwa stronie jest dużo efektywniejsze i prostsze (standardowa funkcjonalność wiodących implementacji serwerów HTTP).

Czy powyższe doprecyzowanie z naszej strony można uznać za spełnienie Państwa wymagań?

**Odpowiedź 5**

Tak, powyższe doprecyzowanie uznajemy za spełnienie wymagań Zamawiającego.

**Pytanie 6**

2.4 System realizujący usługę ma samodzielnie wykrywać anomalie polegające na znaczącym przekroczeniu wolumenu ruchu oraz ataki na usługi Zamawiającego wystawione pod publicznymi adresami IP na podstawie danych historycznych z ruchu sieciowego wyznaczanych w trakcie realizacji usługi.

Nasza usługa nie spełnia wymagania, jednak mamy to zrealizowane w inny sposób.
Jako podejrzany traktujemy ruch powyżej pewnego stałego progu i skutkuje to skierowaniem ruchu na scrubbing.
W przypadku, gdy ten ponadnormatywny ruch nie jest DDoS-em, przejdzie on po prostu przez scrubbing przezroczyście.
Jest również technicznie możliwe skierowanie ruchu na scrubbing na stałe, wówczas odpada problem ew. detekcji i czasu reakcji.

Czy powyższe doprecyzowanie z naszej strony można uznać za spełnienie Państwa wymagań?

**Odpowiedź 6**

Tak, powyższe doprecyzowanie uznajemy za spełnienie wymagań Zamawiającego.

DYREKTOR
Centrum Informatyki Statystycznej
Marcin Piekarek

**Centrum Informatyki Statystycznej**

Aleja Niepodległości 208, 00-925 Warszawa
tel. 22 608 31 44
cissek@stat.gov.pl
cis.stat.gov.pl