Załącznik nr 1
do ogłoszenia o udzielanym
zamówieniu nr ZZ/308/009/D/2023

OPIS PRZEDMIOTU ZAMÓWIENIA

Oprogramowanie do inspekcji ruchu użytkownika końcowego sieci 5G oraz zabezpieczenia płaszczyzny sterowania rdzenia sieci 5G – 1 szt.

Gwarancja: min. 12 miesięcy

Wymagania ogólne

1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Dostawa licencji na komercyjne oprogramowanie pozwalające na inspekcję ruchu użytkownika końcowego sieci 5G oraz zwiększenie ochrony płaszczyzny sterowania rdzenia sieci 5G. Dopuszcza się rozwiązanie realizowane jako oprogramowanie modułowe. Oprogramowanie lub poszczególne elementy wchodzące w skład systemu powinny umożliwiać uruchomienie w postaci wirtualnej maszyny w środowisku wirtualnym – VMware.

System musi zostać dostarczony w modelu, w którym niewykupienie odnowienia licencji dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu, a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania i dostępu do baz funkcji ochronnych.

Dostarczone rozwiązanie musi być objęte serwisem gwarancyjnym producenta przez okres 12 miesięcy. W ramach tego serwisu zapewniony zostanie dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. Licencje upoważniające do korzystania w okresie 12 miesięcy z aktualnych baz funkcji ochronnych obejmują przynajmniej aktualizację:

a) dla funkcjonalności inspekcji ruchu użytkowników końcowych sieci 5G:

- baz sygnatur rozpoznających aplikacje
- baz GeoIP
- baz Zaufanych Certyfikatów
- baz usług SaaS

b) dla funkcjonalności zabezpieczenia płaszczyzny sterowania sieci 5G:

- baz sygnatur ochrony aplikacji web
- baz GeoIP
- baz sygnatur malware
- baz reputacji adresów IP

Specyfikacja funkcjonalna w zakresie inspekcji ruchu użytkowników końcowych sieci 5G

Oprogramowanie powinno zapewniać możliwość inspekcji ruchu użytkownika końcowego przenoszonego przynajmniej przez protokoły GTP wykorzystywanego w systemach 5G. Powinno ono oferować funkcjonalność w zakresie mechanizmów bezpieczeństwa usług VoIP, firewalla SCTP, inspekcji ruchu GTP zgodnie z poniższymi wymaganiami.

Mechanizmy bezpieczeństwa usługi VoIP przynamniej w zakresie:

- firewall stanowy dla protokołu SIP
- praca w trybie SIP Transparent
- praca w trybie Rewrite SIP Header
- śledzenie sesji SIP poprzez Session Lifespan
- obsługa mechanizmów HA w postaci SIP Session Failover
- możliwość ograniczenia intensywności ruchu protokołu SIP
- mechanizmy ukrywania topologii
- statystyka połączeń SIP
- możliwość wykrywania anomalii w ruchu VoIP

Mechanizmy bezpieczeństwa w zakresie analizy ruchu GTP:

- możliwość inspekcji ruchu przenoszonego przez tunele GTP
- możliwość filtrowania ruchu z wykorzystaniem przynajmniej następujących parametrów:
- MNC/MCC, typ wiadomości, typ sieci RAT, lokalizacja, IMEI, MSISDN
- Obsługa interfejsu n9 zdefiniowanego w architekturze systemu 5G
- Obsługa interfejsów S11 I S5/S8 w architekturze systemu LTE
- Mechanizmy zabezpieczenia przed atakiem typu Session Hijacking

Możliwość wykorzystania przynajmniej baz z poniższej listy:

- baz sygnatur rozpoznających aplikacje
- baz GeoIP
- baz Zaufanych Certyfikatów
- baz usług SaaS

Specyfikacja funkcjonalna w zakresie ochrony płaszczyzny sterowania rdzenia 5G

Oprogramowanie powinno zapewniać możliwość ochrony komunikacji realizowanej w płaszczyźnie sterowania rdzenia sieci 5G poprzez oferowane mechanizmy poprawiające bezpieczeństwo wymiany danych realizowanej z wykorzystaniem protokołu http/2.

Parametry funkcjonalne:

- Obsługa dysków twardych o rozmiarze większym niż 40GB
- Możliwość obsługi minimum 10 interfejsów sieciowych
- Obsługa mechanizmów HA
- Obsługa ruchu http o przepustowości mnie mniszej niż 25 Mbps
- Zarządzanie przynajmniej przez interfejs webowy oraz wiersz poleceń
- Natywne wsparcie dla protokołu http/2
- Weryfikacja zgodności XML oraz JSON
- Możliwość integracji z rozwiązaniami CI/DI
- Mechanizmy wykrywania botów
- Obsługa łączności IPv6

Ochrona przed atakami warstwy aplikacji przynajmniej w zakresie zastępujących typów ataków:

- Cross Site Scripting
- SQL Injection
- Cross Site Request Forgery
- Session Hijacking

Możliwość wdrażania przynajmniej w zakresie następujących trybów:

- Odwrócone proxy
- Transparentne proxy
- Analiza offline

Realizacja ochrony komunikacji przynajmniej w zakresie zastępujących mechanizmów:

- Możliwość wprowadzenie dodatkowego poziomu zabezpieczającego realizującego funkcje virtual patching
- Wykrywania zagrożeń typu malware
- Ochrona przed atakami typu brute-force
- Ocena istotności wykrytych zagrożeń
- Wykrywanie ataków SQL injection
- Wykrywanie ataków XSS
- Mechanizmy zabezpieczenia nagłówków HTTP
- Stanowy firewall pracujący w warstwie transportowej
- Ochrona przed atakami DoS
- Mechanizmy ochrony przed wyciekiem danych
- Ochrona przed atakami MITB

Obsługa mechanizmów http przynajmniej w zakresie:

- serwer load balancing
- URL Rewriting
- HTTPS/SSL Offloading
- HTTP Compression

- Caching

Możliwość wykorzystania przynajmniej baz z poniższej listy:

- baza sygnatur ochrony aplikacji web
- baza GeoIP
- baza sygnatur malware
- baza reputacji adresów IP