Opis techniczny przedmiotu zamówienia

Zakup i dostawa urządzenia klasy UTM w ramach realizacji projektu „Wzmocnienie zdolności do przeciwdziałania zagrożeniom informatycznym i reakcji na te zagrożenia w Gminie Miejskiej Legionowo. Program Fundusze Europejskie na Rozwój Cyfrowy (FERC) Priorytet – II. Zaawansowane usługi cyfrowe Działanie - 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa - nr wniosku FERC.02.02-CS.01-001/23/1713 - nr naboru FERC.02.02-CS.01-001/23.”

Informacje o zamawiającym i przedmiocie zakupu.

Przedmiot zamówienia:

1 Klaster dwóch urządzeń klasy UTM/NGFW o parametrach nie słabszych niż:

1.1 Zapewnienie ochrony sieci dla ok. 1 000 stacji roboczych przy łączu 1 Gb/s symetrycznym.

1.2 Obudowa przystosowana do montażu w szafie rack 19-calowej;

1.3 Pełna inspekcja SSL/TLS (w tym TLS 1.3, HTTP/2, HTTP/3/QUIC, DoH/DoQ).

1.4 Klaster 2× UTM/NGFW w trybie active-active, z równoważeniem obciążenia i synchronizacją stanów sesji (stateful).

1.5 Automatyczne przełączenie przy awarii (failover): max. 5 s.

1.6 Przepustowość UTM+SSL (IMIX/real traffic): min. 1,0 Gb/s.

1.7 Przepustowość samej inspekcji SSL/TLS: min. 1,2 Gb/s.

1.8 Nowe sesje na sekundę: ≥ 25 000; sesje równoczesne: min. 1 000 000.

1.9 Wymagane interfejsy sieciowe (per urządzenie wchodzące w skład klastra): Min. 2×10 GbE (SFP+) i 6×1 GbE,

1.10 dedykowany port do pracy w klastrze (HA) oraz dedykowany port zarządzający,

1.11 Redundantne zasilacze (hot-swap), akceleracja strumieni/SSL w sprzęcie.

1.12 Stateful firewall L3–L7; IPS; Anti-Malware; Anti-Bot/C2; URL Filtering; App Control; DNS Security.

1.13 Sandbox (chmura lub on-prem); polityki deszyfracji oddzielone od polityk bezpieczeństwa.

1.14 VPN IPsec/IKEv2 oraz SSL-VPN (portal/agent) z MFA/2FA.

1.15 Obsługa QUIC/HTTP-3; kontrola i egzekwowanie DoH/DoQ.

1.16 GUI, CLI i API; integracja z syslog/SIEM; raporty PDF/CSV; role RBAC.

1.17 Centralne zarządzanie (fizyczne lub wirtualne), HA dla konsoli; eksport/import polityk.

1.18 Moduły ochrony antywirusowej oraz zapobiegania komunikacji z sieciami botnet.

1.19 System zapobiegania komunikacji z sieciami botnet musi umożliwiać wykrycie oraz zablokowanie podejrzanego zachowania w chronionych segmentach sieci.

1.20 System zapobiegania komunikacji z sieciami botnet w celu identyfikacji podejrzanych zachowań musi wykorzystywać mechanizmy zabezpieczeń oparte o reputację adresów IP, URL oraz DNS w połączeniu z wykrywaniem wzorców ruchu specyficznych dla połączeń kierowanych do serwerów C&C.

1.21 System zapobiegania komunikacji z sieciami botnet musi posiadać możliwość identyfikacji urządzeń wewnętrznych będących źródłem podejrzanych zapytań DNS w przypadku kiedy wykorzystują one wewnętrzny serwer DNS pośredniczący w generowaniu zapytań. Mechanizm musi umożliwiać modyfikację/fałszowanie odpowiedzi DNS i przekierowywanie urządzeń do wcześniej ustalonego adresu IP (tzw. DNS malware trap lub DNS Sinkhole).

1.22 Moduł ochrony antywirusowej musi zapewniać ochronę minimum dla następujących protokołów: HTTP/HTTPS, FTP, SMB/CIFS (w tym SMBv3).

1.23 Moduł ochrony antywirusowej musi umożliwiać skanowanie adresów URL oraz załączników znajdujących się w wiadomościach poczty elektronicznej.

1.24 Moduł ochrony antywirusowej musi umożliwiać skanowanie plików skompresowanych.

1.25 Moduł ochrony antywirusowej musi posiadać możliwość blokowania dostępu do określonych witryn internetowych w oparciu o informację o ich reputacji.

1.26 Moduły ochrony antywirusowej oraz zapobiegania komunikacji z sieciami botnet muszą posiadać możliwość interakcji z użytkownikami w zakresie informowania o zablokowaniu dostępu do niebezpiecznych zasobów.

1.27 Moduł filtrowania kategorii URL musi posiadać możliwość tworzenia reguł polityki zawierających jednocześnie wiele kategorii URL.

1.28 Moduł filtrowania kategorii URL musi dostarczać wbudowane kategorie URL opisujące niebezpieczne witryny kategoryzowane w oparciu o poziom zagrożenia (np. CriticalRisk lub High Risk), a także w oparciu o rodzaj zagrożenia (np. witryny wyłudzające dane lub witryny będące centrami C&C).

1.29 Moduł filtrowania kategorii URL musi umożliwiać tworzenie własnych obiektów opisujących witryny URL oraz ich kategoryzowanie.

1.30 Moduł filtrowania kategorii URL musi umożliwiać modyfikowanie wbudowanych stron z powiadomieniami prezentowanymi użytkownikom oraz musi umożliwiać przekierowania użytkowników do stron umieszczonych na zewnętrznych serwerach.

1.31 Moduł IPS musi posiadać możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system).

1.32 Moduł IPS musi posiadać możliwość pracy zarówno w trybie pasywnym (Detect) jak i aktywnym (z możliwością blokowania ruchu)

1.33 Moduł IPS musi zapewniać co najmniej poniższe sposoby wykrywania zagrożeń:

1.33.1 sygnatury ataków opartych na exploitach

1.33.2 reguły oparte na zagrożeniach

1.33.3 mechanizm wykrywania anomalii w protokołach

1.34 Moduł IPS musi mieć możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakres protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu.

1.35 Moduł IPS musi posiadać wiele możliwości reakcji na zdarzenia takie jak: tylko monitorowanie, blokowanie ruchu zawierającego zagrożenia oraz mieć możliwość zapisywania pakietów generujących zagrożenie.

1.36 Moduł IPS musi posiadać możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji.

1.37 Moduł IPS musi zapewniać mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera aktualizacji w sposób uniemożliwiający ich modyfikację podczas przesyłania pomiędzy serwerem aktualizacji oraz serwerem zarządzania/zaporą sieciową.

1.38 Moduł IPS musi zapewniać możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednoczenie.

1.39 Moduł IPS musi zapewniać możliwość detekcji i blokowania ataków i zagrożeń opartych na protokole IPv6.

1.40 Moduł IPS musi pozwalać posiadać możliwość aktywowania ochrony dla wybranych zasobów definiowanych minimum w postaci adresów hostów, adresów sieci oraz zakresów adresów IP i przypisywanie do tych zasobów dedykowanych zestawów sygnatur.

1.41 Moduł IPS musi posiadać programowy mechanizm pozwalający na wyłączenie ochrony IPS w przypadku wysokiego obciążenia procesora lub pamięci operacyjnej zapory sieciowej. Wartości aktywujące mechanizm muszą być konfigurowalne przez administratora systemu.

1.42 Moduł IPS musi posiadać mechanizmy wykrywania i blokowania operacji tunelowania ruchu w ramach innych protokołów, np. DNS tunneling.

2 Oprogramowanie:

2.1 Urządzenie musi być dostarczone ze wszystkimi licencjami/subskrypcjami umożliwiającymi uzyskanie funkcjonalności opisanej w pkt 1 opisu technicznego przedmiotu zamówienia.

2.2 Długość trwania licencji/subskrypcji nie może być krótsza niż okres wsparcia technicznego, tj. 24 miesiące od dnia podpisania protokołu odbioru.

2.3 Zabrania się stosowania licencji ograniczających programowo liczbę sesji, użytkowników, VLAN-ów lub przepustowość.

2.4 Wykonawca w formularzu podzespołów oświadczy, że liczba sesji i przepustowość nie są ograniczane licencyjnie (soft-limitami) przez producenta, a wartości graniczne wynikają z architektury sprzętowej i wersji modelowej.

2.5 Zamawiający wymaga, aby wdrożony sprzęt i oprogramowanie było zaktualizowane do najnowszej dostępnej i stabilnej wersji (dotyczy w szczególności oprogramowania układowego i sterowników).

3 Gwarancja i wsparcie techniczne:

3.1 Wykonawca udziela gwarancji na dostarczone urządzenie i oprogramowanie na okres 24 miesięcy.

3.2 W okresie gwarancyjnym Wykonawca zapewnia:

3.2.1 bieżące aktualizacje oprogramowania i sygnatur;

3.2.2 wsparcie techniczne w dni robocze w godz. 8.00–16.00;

3.2.3 naprawę lub wymianę urządzenia w przypadku awarii w terminie nie dłuższym niż 7 dni kalendarzowych od zgłoszenia.

4 Inne warunki:

4.1 Urządzenie musi być fabrycznie nowe, nieużywane.

4.2 Nie może pochodzić z odsprzedaży/refurbished.

4.3 Zamawiający wymaga, aby dostarczone urządzenia były sprzętem zakupionym w oficjalnym kanale sprzedaży producenta na terenie Unii Europejskiej. Zamawiający zastrzega możliwość weryfikacji.

4.4 Wykonawca zobowiązuje się dostarczyć rozwiązanie kompletne i gotowe do eksploatacji, zgodne z wymaganiami Zamawiającego.

4.5 Wykonawca zobowiązuje się do dokonania konfiguracji dostarczonego urządzenia w środowisku Zamawiającego oraz przeszkolenia i przekazania administratorom Zamawiającego kompletu niezbędnych danych, informacji i dostępów umożliwiających prawidłową obsługę, konfigurację i utrzymanie dostarczonego przedmiotu umowy.

4.6 Zamawiający wymaga, aby prace wdrożeniowe skutkujące niedostępnością infrastruktury IT Zamawiającego były realizowane po godzinach pracy w dni robocze.

4.7 Zamawiający wymaga opracowania dokumentacji powykonawczej wdrożenia, obejmującej całość wykonanych prac, w tym dokumentację zmian w infrastrukturze zależnej.

4.8 Zamawiający wymaga dostarczenia wraz z zaoferowanym sprzętem kompletnego okablowania niezbędnego do poprawnego zainstalowania i skonfigurowania całości proponowanego rozwiązania.

4.9 Zamawiający wymaga, aby Wykonawca do oferty dołączył kartę katalogową urządzenia.