**Gmina Miejska**
**Lidzbark Warmiński**
ul. Aleksandra Świętochowskiego 14
11-100 Lidzbark Warmiński

tel. +48 89 767 85 00
fax +48 89 767 23 03
www.lidzbarkw.eu
um@lidzbarkw.pl

Lidzbark Warmiński, 13.04.2021r.

**Do wszystkich Wykonawców**

Dotyczy: Postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego pn. **Dostawa sprzętu informatycznego, wyposażenia i oprogramowania niezbędnego do realizacji e- usług w ramach Projektu: „Opracowanie i wdrożenie e-usług dla społeczeństwa Miasta Lidzbark Warmiński"**, Znak sprawy: GKI.271.3.2021

Działając zgodnie z art. 135 ust. 6 ustawy z dnia 11.09.2019 r. Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 2019 ze zm.), w imieniu Gminy Miejskiej Lidzbark Warmiński, zwanej dalej: „Zamawiającym", zawiadamiam, że jeden z Wykonawców zwrócił się do Zamawiającego z pismem o udzielenie wyjaśnień. Poniżej przedstawiam treść pytań zawartych w piśmie wraz z udzielonymi przez Zamawiającego wyjaśnieniami:

**Pytanie nr 1:**
„Szanowni Państwo Zwracam się z uprzejmą prośbą o udzielenie odpowiedzi na poniższe pytanie dotyczące części II przedmiotowego postępowania: Minimalne wymagania w zakresie rozwiązania UTM pozwalają na zaoferowanie rozwiązanie tylko jednego producenta urządzeń w związku z tym, aby umożliwić zaoferowanie konkurencyjnego rozwiązania innego producenta niż FORTINET, czy Zamawiający dopuści zaoferowanie równoważnego rozwiązania, realizującego te same funkcje co opisane rozwiązanie.
Zamawiajacy zdaje sobie sprawę, że rozwiązanie pochodzące od innego producenta może mieć podobne parametry wydajnościowe ale nie będzie identyczne do opisanego. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe.
Dla elementów systemu bezpieczeństwa wykonawca musi zapewnić wszystkie poniższe funkcjonalności:
Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent. System realizujący funkcję Firewall musi dysponować minimum 8 interfejsami miedzianymi Ethernet 10/100/1000. System realizujący funkcję Firewall musi dysponować minimum 2 interfejsami optycznymi 1GbE (SFP). Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q. W zakresie Firewall'a obsługa nie mniej niż 1 000 000 jednoczesnych połączeń oraz 45 000 nowych połączeń na sekundę. System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 200 GB do celów logowania i raportowania. System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. W przypadku kiedy system nie posiada dysku lub nie pozwala na podłączenie zewnętrznych nośników, musi być dostarczony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych: Kontrola dostępu - zaporaogniowa klasy Stateful Inspection Ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3,HTTP, FTP, HTTPS). System AV musi umożliwiać skanowanie AV dla plików typu:

rar, zip. Poufność danych- IPSec VPN oraz SSL VPN Ochrona przed atakami - Intrusion Prevention System [IPS/IDS] Kontrola stron Internetowych – Web Filter [WF] Kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3)
Kontrola pasma oraz ruchu [QoS i Traffic shaping] Kontrola aplikacji oraz rozpoznawanie ruchu P2P
Analiza ruchu szyfrowanego protokołem SSL Wydajność systemu Firewall minimum 12 Gbps Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus minimum 2 Gbps Wydajność ochrony przed atakami (IPS) minimum 7 Gbps Wydajność VPN IPSec, nie mniej niż 2 Gbps W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż: Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site Producent oferowanego rozwiązania VPN powinien dostarczać klienta VPN współpracującego z proponowanym rozwiązaniem
Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności Praca w topologii Hub and Spoke oraz Mesh Obsługa ssl vpn w trybach portal oraz tunel Rozwiązanie musi zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP. Translacja adresów NAT adresu źródłowego i NAT adresu docelowego. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety). Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). Ochrona IPS musi opierać się co
najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków musi zawierać co najmniej 1000 wpisów. Dodatkowo musi być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS. Funkcja kontroli aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. Baza filtra WWW pogrupowana w minimum 50 kategorii tematycznych. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW. · Automatyczne ściąganie sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL. · System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości
użytkowników za pomocą nie mniej niż: o Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP Haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory W zakresie realizowanych funkcjonalności systemu raportowania i przeglądania logów, wymagane jest nie mniej niż:
Posiadanie predefiniowanych raportów dla ruchu WWW, modułu IPS, skanera antywirusowego i antyspamowego Generowanie co najmniej 25 różnych typów raportów System raportowania i przeglądania logów wbudowany w system bezpieczeństwa nie może wymagać dodatkowej licencji do swojego działania Urządzenie musi: -posiadać certyfikat Common Criteria EAL4+ -posiadać certyfikat ICSA Labs dla funkcji: VPN IPSec lub znajdować się na liście produktów kryptograficznych zatwierdzonych przez Radę UE Elementy systemu muszą mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania. Komunikacja
systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem
szyfrowanych protokołów. Wymaga się, aby dostawa obejmowała również: Minimum 60-miesięczną gwarancję producentów na dostarczone elementy systemu liczoną od dnia zakończenia wdrożenia całego systemu. Licencje dla wszystkich funkcji bezpieczeństwa producentów na okres minimum 60 miesięcy liczoną od dnia zakończenia wdrożenia całego systemu.”

**Wyjaśnienie na pytanie nr 1:**

1) Zamawiający w SWZ określił minimalne wymagania dotyczące urządzenia sieciowego UTM, które musi spełnić produkt. Wykonawca może zaoferować produkt o lepszych parametrach.
2) Zamawiający informuje, że zmienia zapisy Opisu Przedmiotu Zamówienia (OPZ) :
   z: „a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres [60] miesięcy."
   na: „a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres min. [24] miesięcy."

**ZMIANA SPECYFIKACJI WARUNKÓW ZAMÓWIENIA**

W związku z powyższymi wyjaśnieniami, działając zgodnie z art. 137 ust. 1 i 2 ustawy Pzp, Zamawiający zawiadamia o następujących zmianach treści specyfikacji warunków zamówienia, zwanej dalej: „SWZ":

1/ w Opisie Przedmiotu Zamówienia (OPZ) stanowiącym załącznik nr 13 do SWZ w Rozdziale VIII. Część 2 – Dostawa urządzenia sieciowego UTM zmienia się istniejące zapisy pkt. 1.1.18.1 lit. a):
   z: „a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres [60] miesięcy."
   na: „a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres min. [24] miesięcy."
2/ uchyla się istniejący Opis Przedmiotu Zamówienia (OPZ), stanowiący załącznik nr 13 do SWZ,
3) dodaje się obowiązujący Opis Przedmiotu Zamówienia (OPZ), stanowiący załącznik nr 13 do SWZ, uwzględniający dokonane zmiany.

Dokonane zmiany zapisów SWZ są obowiązujące i należy traktować je jako jedyne obowiązujące. Inne zapisy SWZ nie ulegają zmianie.

Załącznik:
1/ Opis Przedmiotu Zamówienia (OPZ), stanowiący załącznik nr 13 do SWZ.

B U R M I S T R Z

*Jacek Wiśniowski*