



Trzebnica, 26.07.2022 r.

nr sprawy: ZP.271.9.2022

**Wszyscy Wykonawcy
biorący udział w postępowaniu**

WYJAŚNIENIA NR 2 TREŚCI SPECYFIKACJI WARUNKÓW ZAMÓWIENIA

Dotyczy postępowania nr ZP.271.9.2022 o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego pn. „Cyfrowa Gmina Trzebnica. Zadanie I - Wdrożenie e-usług w Gminie Trzebnica, Zadanie II - Dostawa urządzenia klasy UTM wraz z szkoleniami i wsparciem”.

Zamawiający, działając na podstawie art. 135 ust. 2 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2021 r., poz. 1129 z późn. zm.), zwanej dalej „ustawą PZP”, udziela wyjaśnień do treści Specyfikacji Warunków Zamówienia, zwanej dalej „SWZ”:

Pytanie 10:

„W nawiązaniu do niniejszego postępowania, prosimy o udzielenie odpowiedzi dotyczących treści SWZ: Pytanie nr 1: Prosimy o wyjaśnienie, jakie możliwości daje oprogramowanie obsługujące ewidencję ludności CLANET w zakresie pobierania aktualnych danych na żądanie użytkownika? Czy wykorzystanie danych w tym zakresie jest możliwe z wykorzystaniem API systemu CLANET? Jaki model integracji w tym zakresie przewiduje Zamawiający? Czy Zamawiający posiada dokumentację umożliwiającą wykonanie tej integracji i udostępni ją Wykonawcy?”

Odpowiedź:

Program daje możliwość podglądu danych, eksportu i zapisu. Wykorzystanie API nie jest możliwe z powodu wydzielonych sieci, eksport danych odbywa się za pomocą plików na żądanie użytkownika, poprzez zewnętrzny nośnik, bez bezpośredniego połączenia aplikacji za pomocą sieci LAN. Zamawiający przewidują integrację na poziomie plików z danymi. Zamawiający nie posiada dokumentacji.

Pytanie 11:

„Ochrona przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony informującej użytkownika o próbie pobrania pliku i możliwości kontynuowania lub zaniechania pobrania.



Rzeczpospolita
Polska



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego





GMINA TRZEBNICA

pl. Marszałka Józefa Piłsudskiego 1, 55-100 Trzebnica
www.trzebnica.pl

Pragniemy zauważyć, że ataki typu "drive-by-download" najczęściej przeprowadzane przy odwiedzaniu/przeglądaniu znanych niebezpiecznych stron internetowych. Pozwolenie odwiedzenia takiej strony, a jedynie zablokowanie pobrania pliku nie wiele podnosi poziom bezpieczeństwa, gdyż niebezpieczne strony mogą wykorzystywać inne ataki niż ataki polegające na pobraniu pliku. Tak zdefiniowane wymagania nie przyczynia się do zwiększenia bezpieczeństwa rozwiązania lecz blokuje możliwość zdobycia dodatkowych punktów dla innych producentów niż Palo Alto Networks. Prosimy o akceptację rozwiązania, które chroni przed atakami typu "drive-by-download", a akcja "kontynuuj" jest dostępną już przy próbie wejścia na potencjalnie niebezpieczną stronę."

Odpowiedź:

Zamawiający podtrzymuje zapisy OPZ. Ochrona z wykorzystaniem strony "kontynuuj" przy próbie pobrania pliku pozwala zmniejszyć powierzchnię ataku a dodatkowo pełni rolę edukacyjną dla użytkowników, którzy stają się bardziej świadomi swojej aktywności w Internecie.

Pytanie 12:

„Firewall musi identyfikować co najmniej 2500 różnych aplikacji, w tym aplikacji tunelowanych w protokołach HTTP i HTTPS m.in.: Skype, Tor, BitTorrent, eMule. Prosimy o dopuszczenie rozwiązania identyfikującego ponad 2100 różnych aplikacji, w tym wszystkie wymienione w ramach wymagania.”

Odpowiedź:

Zamawiający podtrzymuje zapisy OPZ. Identyfikacja aplikacji jest jedną z podstawowych funkcjonalności rozwiązań typu UTM/NGFW i ilość sygnatur aplikacyjnych/identyfikowanych aplikacji ma wpływ na kształt polityk bezpieczeństwa a zatem również na odpowiednie przepuszczanie/blokowanie/monitorowanie ruchu.

Pytanie 13:

„Rozwiązanie musi umożliwiać rozbudowę o możliwość wykrywania domen DGA i ruchu tunelowanego przez DNS. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres minimum 60 miesięcy. Czy dopuszczone zostanie rozwiązanie realizujące funkcję wykrywania domen DGA, w oparciu o kategoryzację w ramach "nowo obserwowanych domen" oraz "domen phishing"?”

Odpowiedź:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie 14:

„Musi mieć możliwość wyboru sposobu blokowania ruchu w politykach bezpieczeństwa. Musi istnieć



Rzeczpospolita
Polska



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego





możliwość ustawienia cichego blokowania ruchu bez wysyłania RST, blokowanie z wysłaniem RST tylko do klienta, blokowanie z wysłaniem RST tylko do serwera, blokowanie z wysłaniem RST do klienta i serwera jednocześnie. Pragniemy zauważyć, że tak postawione wymaganie może być spełnione jedynie przez rozwiązanie producenta Palo Alto Networks, co ogranicza konkurencję. Prosimy o dopuszczenie rozwiązania pozwalającego na globalne włączenie/wyłączenie wysyłania flagi RST do klienta.”

Odpowiedź:

Zamawiający wymaga aby wysyłanie flagi RST było konfigurowalne per polityka. Wyłączenie tej funkcjonalności globalnie sprawi, że rozwiązanie może być bardziej podatne na ataki i skanowanie.

Pytanie 15:

„Firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach. Prosimy o dopuszczenie rozwiązania pozwalającego na realizację wymagania w oparciu o dedykowany kolektor logów.”

Odpowiedź:

Zamawiający podtrzymuje zapisy OPZ. Wprowadzenie kolejnego elementu systemu niepotrzebnie skomplikuje infrastrukturę.

Pytanie 16:

„Urządzenie musi pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni. Prosimy o dopuszczenie rozwiązania pozwalającego na realizację wymagania w oparciu o dedykowany kolektor logów.”

Odpowiedź:

Zamawiający podtrzymuje zapisy OPZ. Wprowadzenie kolejnego elementu systemu niepotrzebnie skomplikuje infrastrukturę.

Pytanie 17:

„Urządzenie musi zapewniać wydajność przynajmniej 3 Gbps dla ruchu IPSec VPN i umożliwiać zestawienie przynajmniej 2500 równoczesnych tuneli site-to-site. Prosimy o dopuszczenie rozwiązania pozwalającego na zestawienie do 2000 jednoczesnych tuneli site-to-site.”

Odpowiedź:

Zamawiający podtrzymuje zapisy OPZ .



Rzeczpospolita
Polska



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego





GMINA TRZEBNICA

pl. Marszałka Józefa Piłsudskiego 1, 55-100 Trzebnica
www.trzebnica.pl

Pytanie 18:

„Urządzenie musi posiadać możliwość rozbudowy o funkcjonalność weryfikacji poziomu bezpieczeństwa komputera użytkownika przed przyznaniem mu uprawnień dostępu do sieci lub wybranych jej zasobów. Pragniemy zauważyć, że tak postawione wymaganie wskazuje na producenta Palo Alto Networks, co ogranicza konkurencję. Prosimy o dopuszczenie rozwiązania pozwalającego realizację wskazanej funkcji dla klientów SSL-VPN”

Odpowiedź:

Zamawiający podtrzymuje zapisy OPZ. Możliwość rozbudowy o funkcjonalność weryfikacji poziomu bezpieczeństwa komputera przed przyznaniem mu uprawnień dostępu do sieci lub wybranych jej zasobów daje możliwość wprowadzenia kolejnej warstwy ochrony, szczególnie przy dostępie do kluczowych zasobów.

Sporządziła:

Monika Białas

Kontakt z Zamawiającym przez Platformę Zakupową



Rzeczpospolita
Polska



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



tel. 071/312 06 11, 071/312 06 12, 071/312 01 45, 071/312 06 42, fax: 071/312 12 48
Bank Spółdzielczy Trzebnica, nr konta: 25 9591 0004 2001 0000 4431 0001
NIP: 915-16-03-770 REGON: 931935135
e-mail: sekretariat@um.trzebnica.pl

