Bankowy Fundusz Gwarancyjny

DAZ.261.1.2019
numer postępowania DAZ/ZP/1/2019

Warszawa, dnia 14 sierpnia 2019 r.

Do uczestników postępowania

Dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego, pn.: **„Dostawa i wdrożenie systemu zapór sieciowych wewnętrznych (tzw. firewall) wraz z usługą szkolenia".**

Działając na podstawie art. 38 ust. 1, 2 i 4 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2018 r., poz. 1986 z późn. zm.), zwanej dalej „ustawą Pzp", Zamawiający udziela odpowiedzi na pytania Wykonawców dotyczące Specyfikacji istotnych warunków zamówienia, które wpłynęły do ww. postępowania oraz dokonuje modyfikacji treści Specyfikacji istotnych warunków zamówienia (SIWZ):

Pytanie nr 1:
Dotyczy wymagania 1.3
Czy Zamawiający zaakceptuje rozwiązanie które posiada 2 porty 1Gbps/10Gbps SFP/SFP+ ?

Odpowiedź:
Zamawiający podtrzymuje w tym zakresie zapisy SIWZ.
Zamawiający informuje, że ze względu na eksploatowaną architekturę sieciową nie akceptuje rozwiązania, które posiada 2 porty 1Gbps/10Gbps SFP/SFP+.

Pytanie nr 2:
Dotyczy wymagania 1.14
Prosimy o usunięcie wskazanej częsci wymagania gdyż część ta nie jest opisem funkcjonalni, a narzuceniem producentowi sposobu realizacji funkcjonalności na warstwie systemu operacyjnego. Tak postawione wymaganie ogranicza możliwość zaoferowania konkurencyjnych rozwiązań które realizują funkcjonalność rozpoznawania aplikacji tylko wykonują to w sposób określony w wymaganiu.

Odpowiedź:
Zamawiający informuje, że podtrzymuje w tym zakresie zapisy SIWZ.

ul. ks. Ignacego Jana Skorupki 4, 00-546 Warszawa
tel. 22 58 30 700, 58 30 610, fax 22 58 30 589
e-mail: kancelaria@bfg.pl, www.bfg.pl

Pytanie nr 3:

Dotyczy wymagania 1.16

Pragniemy zauważyć, iż funkcjonalność IPS z zasady nie może funkcjonować bez rozpoznawania aplikacji, gdyż moduł IPS chroni przed atakami na konkretne aplikacje. Wiele producentów do rozpoznawania aplikacji oraz do ochrony przez włamaniami (intrusion prevention) wykorzystuje pojedynczy moduł IPS, gdyż jak wspomniano powyżej, z zasady są to powiązane miedzy sobą procesy. Wykonywanie dwóch funkcji przez pojedynczy moduł zwiększa również wydajność systemu. To producent konkretnego rozwiązania dla swoich urządzeń ustala najlepszy sposób na zarządzanie zasobami, zadaniami procesów, metodami realizacji funkcjonaliści na poziomie kodu systemu operacyjnego.

Prosimy o usunięcie wymagania gdyż część ta nie jest opisem funkcjonalni, a narzuceniem producentowi sposobu realizacji funkcjonalności na warstwie systemu operacyjnego. Tak postawione wymaganie ogranicza możliwość zaoferowania konkurencyjnych rozwiązań które realizują funkcjonalność rozpoznawania aplikacji tylko wykonują to w sposób określony w wymaganiu.

Odpowiedź:

Zamawiający informuje, że podtrzymuje w tym zakresie zapisy SIWZ.

Pytanie nr 4:

Dotyczy wymagania 1.21

Tak skonstruowane pytanie ogranicza możliwość zaoferowania Państwu innych rozwiązań niz rozwiązanie Pal Alto Networks, gdyż podany zestaw plików jest wspierany wyłącznie przez urządzenia firmy PaloAlto Networsk. Pozostali producenci nie wpierają co najmniej jednego typu lub kilka typów plików.

Prosimy o modyfikację wymagania na brzmiące :

System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików nie mniej niż: bat, cab, zip, exe, gzip, dfp, text, tif, pliki ms office, pliki zaszyfrowane. rozpoznawanie pliku musi odbywać sie na podstawie nagłówka i typu MIME, a nie na postawie rozszerzenia.

Taka modyfikacja wymagania pozwoli zaoferować Państwo rozwiązana inne niż rozwiązanie Palo Alto networks, a tym samym zwiększy konkurencyjność składanych ofert.

Odpowiedź:

Zamawiający informuje, że **dokonuje w tym zakresie modyfikacji SIWZ**, poprzez nadanie nowego brzmienia ppkt 1.21. znajdującemu się w pkt 1 cz. V Opisu przedmiotu zamówienia stanowiącego Załącznik nr 1 do SIWZ, jak poniżej:

„System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików nie mniej niż: bat, cab, zip, exe, gzip, dfp, text, tif, pliki ms office, pliki zaszyfrowane. rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na postawie rozszerzenia."

Pytanie nr 5:

Dotyczy wymagania 1.23

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.
Czy Zamawiający zaakceptuje rozwiązanie dla które chroni przed atakami typu "drive-by-dowload", a akcja "kontynuuj" jest dostępna już przy próbie wejścia na potencjalnie niebezpieczną stronę.

Odpowiedź:
Zamawiający informuje, że **dokonuje w tym zakresie modyfikacji SIWZ**, poprzez nadanie nowego brzmienia ppkt 1.23. znajdującemu się w pkt 1 cz. V Opisu przedmiotu zamówienia stanowiącego Załącznik nr 1 do SIWZ, jak poniżej:

„System zabezpieczeń firewall musi zapewniać ochronę przed atakami typy "Drive-by-download".

Pytanie nr 6:
Dotyczy wymagania 2.2
Czy zamawiający zaakceptuje rozwiązanie w którym funkcjonalność będzie realizowana przez zewnętrzny system tego samego producenta w postaci maszyny wirtualnej i natywnie współpracującym z systemem zabezpieczeń firewall ? Czy ta maszyna wirtualna może być uruchomiona na zasobach wirtualizacyjnych Zamawiającego ?

Odpowiedź:
Zamawiający informuje, że dopuszcza rozwiązanie, w którym funkcjonalność ta będzie realizowana przez zewnętrzny system tego samego producenta, pod warunkiem dostarczenia przez Wykonawcę kompletnego rozwiązania, bez konieczności wykorzystania środowiska wirtualnego lub fizycznego Zamawiającego na potrzeby realizacji zamawianego systemu.

Pytanie nr 7:
Dotyczy wymagania 3.11
Czy Zamawiający zaakceptuje rozwiązanie, które nie wydziela oddzielnego modułu anti-spyware, lecz ochronę anti-spyware zapewnia jako część funkcjonalności modułu anti-wirus i IPS ?

Odpowiedź:
Zamawiający informuje, że podtrzymuje w tym zakresie zapisy SIWZ.

Pytanie nr 8:
Dotyczy wymagania 3.11
Czy Zamawiający zaakceptuje rozwiązanie, które nie wydziela oddzielnego modułu anti-spyware, lecz ochronę anti-spyware zapewnia jako część funkcjonalności modułu anti-wirus i IPS ?

Odpowiedź:
Zgodnie z odpowiedzią na Pytanie nr 7.

Pytanie nr 9:

Dotyczy wymagania 3.12

Czy Zamawiający zaakceptuje rozwiązanie, które nie wydziela oddzielnego modułu anti-spyware, lecz ochronę anti-spyware zapewnia jako część funkcjonalności modułu anti-wirus i IPS i tym samym nie ma możliwości tworzenia bezpośrednio sygnatur w module antyspyware, lecz umożliwia tworzenie sygnatur antyspyware w module IPS ?

Odpowiedź:

Zamawiający informuje, że podtrzymuje w tym zakresie zapisy SIWZ.

Pytanie nr 10:

Dotyczy wymagania 3.12

Pragniemy strony internetowe wykorzystujace ataki typu "phishing" moga wykorzystywać również innego rodzaju ataki (np. drive-by-download, czy inne). Pozwolenie odwiedzenia takiej strony, a jedynie zablokowanie podania poświadczeń nie wiele podnosi poziom bezpieczeństwa, gdyż niebezpieczne strony mogą wykorzystywać również inne ataki niz ataki typy "phishing".

Czy Zamawiający zaakceptuje rozwiązanie dla które chroni przed atakami typu "phishing" przez całkowite zablokowanie dostępu do takiej strony ?

Odpowiedź:

Zamawiający informuje, że akceptuje rozwiązanie, które chroni przed atakami typu "phishing" przez całkowite zablokowanie dostępu do takiej strony.

Pytanie nr 11:

Dotyczy wymagania 3.20

Czy w ramach postępowania Zamawiajacy oczekuje dostarczenia prywatnego systemu typu Sandbox, czy jedynie licencji do chmurowego systemu Sandbox ?

Odpowiedź:

Zamawiający podkreśla, że w ramach przedmiotowego postepowania wymaga aby wdrożony System posiadał możliwość filtracji URL oraz posiadał funkcje Sandbox, z tym że Zamawiający nie oczekuje w ramach przedmiotowego postępowania wdrożenia i aktywowania funkcjonalności filtrowania URL i Sandbox. Zamawiający chce mieć możliwość aktywowania tych funkcjonalności we wdrożonym Systemie w dowolnym innym terminie po dokupieniu odpowiedniego typu licencji.

Pragniemy zauważyć, że tak postawione wymaganie może być spełnione jedynie przez rozwiązanie producenta Palo Alto Networks, co ogranicza konkucencję i może być niezgodne z ustawą o zamówieniach publicznych.

Czy Zamawiający zaakceptuje rozwiązanie w którym integracja z zewnętrznymi systemami typu "Sand-Box" pozwala administratorowi na przesyłanie wszystkich plików wymagających skanowania do publicznego lub wszystkich plików wymagających skanowania do prywatnego systemu typu "Sand-Box"?

Odpowiedź cd:

Zamawiający informuje, że ze względu na zakres informacyjny przetwarzanych danych nie akceptuje rozwiązania, w którym administrator systemu nie ma możliwości podjęcia każdorazowo decyzji o przekazaniu pliku do zewnętrznego systemu Sand-Box.

Pytanie nr 12:

Dotyczy wymagania 3.21

Pragniemy zauważyć, że tak postawione wymaganie może być spełnione jedynie przez rozwiązanie producenta Palo Alto Networks, co ogranicza konkurencję i może być niezgodne z ustawą o zamówieniach publicznych.

Czy Zamawiający zaakceptuje rozwiązanie które posiada możliwość konfiguracji rodzaju pliku (np.exe, pdf, msofffice, java) które należy wykluczyć z analizy typu „Sand-Box"dla plików przesyłanych w obu kierunkach?

Odpowiedź:

Zamawiający informuje, że ze względu na zakres informacyjny przetwarzanych danych nie akceptuje rozwiązania, w którym administrator systemu nie ma możliwości podjęcia każdorazowo decyzji o przekazaniu pliku do zewnętrznego systemu Sand-Box.

Pytanie nr 13:

Dotyczy wymagania 4.5

Czy Zamawiający zgodzi się na usuniecie wymagania ?

Odpowiedź:

Zamawiający informuje, **że dokonuje w tym zakresie modyfikacji SIWZ,** poprzez nadanie nowego brzmienia ppkt 4.5. znajdującemu się w pkt 4 cz. V Opisu przedmiotu zamówienia stanowiącego Załącznik nr 1 do SIWZ, jak poniżej:

„System zabezpieczeń firewall musi umożliwiać wykrywanie oraz blokowania ataków w ruchu tunelowanym."

Pytanie nr 14:

Dotyczy wymagania 6.3

Czy Zamawiający dopuści rozwiązanie, dla którego funkcjonalność ta jest realizowana z poziomu konsoli zarządzania ?

Odpowiedź:

Zamawiający informuje, że dopuszcza rozwiązanie, w którym funkcjonalność ta może być zrealizowana z poziomu centralnej konsoli zarządzania dedykowanej przez producenta firewall'a.

Pytanie nr 15:

Dotyczy wymagania 6.4

Czy Zamawiający dopuści rozwiązanie, dla którego funckjonalność ta jest realizowana z poziomu konsoli zarządzania ?

Odpowiedź:

Zamawiający informuje, że dopuszcza rozwiązanie, w którym funkcjonalność ta może być zrealizowana z poziomu centralnej konsoli zarządzania dedykowanej przez producenta firewall'a.

Pytanie nr 16:

Dotyczy wymagania 6.5

Proszę o dopuszczenie jako równoważnego rozwiązania które posiada interfejs REST API.

Odpowiedź:

Zamawiający informuje, **że dokonuje w tym zakresie modyfikacji SIWZ,** poprzez nadanie nowego brzmienia ppkt 6.5. znajdującemu się w pkt 6 cz. V Opisu przedmiotu zamówienia stanowiącego Załącznik nr 1 do SIWZ, jak poniżej:

"System zabezpieczeń firewall musi być wyposażony w interfejs XML API lub REST API będący integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI)."

Pytanie nr 17:

Dotyczy wymagania 6.11

W dzisiejszych czasach zagrożenia cybernetyczne rozprzestrzeniają się z niebywałą prędkością, co pokazują chociaż by ostatnie głośne sprawy ataków typu Ramsomware. Jak wiadomo, ataki te wyrządziły najmniejsze szkody i straty finansowe tam, gdzie zasoby były zabezpieczone rozwiązaniami, producenci których w najkrótszym możliwym czasie dostarczali aktualizacji poprawek i sygnatur. W świetle tych wydarzeń, staje się jasne iż przeciąganie z wgrywaniem poprawek bezpieczeństwa niesie za sobą konkretne wymierne finansowo koszty, a co gorsza utratę reputacji instytucji. Dla tego też, w odróżnieniu od rozwiązań starszych generacji, nowoczesne systemy bezpieczeństwa posiadają na bieżąco(nawet kilka razy dziennie) aktualizowane bazy sygnatur i poprawek bezpieczeństwa by nadążyć za ciągle rozwijającymi się zagrożeniami. Pozostawienie możliwości przetestowania aktualizacji w odpowiedzialności administratora niesie ogromne ryzyko, gdyż administrator pojedynczej instytucji najczęściej nie posiada wystarczającej wiedzy na temat chronionych przez system NGFW systemów, a jeszcze mniej wiedzy o aktualnych zagrożeniach i istniejących aktualizacjach sygnatur dotyczących tych systemów. Dodatkowo, administrator nie posiada czasu by testować poprawki bezpieczeństwa i sygnatury aktualizowane kilka razy dziennie. Zważając na powyższe, w świecie dzisiejszych zagrożeń cybernetycznych to do wyspecjalizowanych laboratoriów producentów rozwiązań bezpieczeństwa należy dogłębna weryfikacja poprawności działania sygnatur i opublikowanie zweryfikowanej poprawki możliwie najszybciej.

Prosimy zatem o usunięcie wymagania gdyż jest ono sprzeczne z ideą działania nowoczesnych systemów NGFW jak również jest sprzeczne z najlepszymi praktykami przyjętymi w branży.

Odpowiedź:
Zamawiający informuje, **że dokonuje w tym zakresie modyfikacji SIWZ**, poprzez wykreślenie wymagań stawianych w ppkt 6.11.. znajdującego się w pkt 6 cz. V Opisu przedmiotu zamówienia stanowiącego Załącznik nr 1 do SIWZ.

Pytanie nr 18:
Dotyczy wymagania 6.12
Pragniemy zauważyć, że tak postawione wymaganie może być spełnione jedynie przez rozwiązanie producenta Palo Alto Networks, co ogranicza konkurencję i może być niezgodne z ustawą o zamówieniach publicznych.
Tylko rozwiązanie PaloAlto, posiada możliwość wysyłania logów do różnych serwerów Syslog per polityka bezpieczeństwa bezpośrednio z poziomu systemu firewall. Pozostali producenci najczęściej udostępniają taką funkcjonalność dopiero z dedykowanego systemu zbierania logów(np. Checkpoitn SMS, Fortinet FortiAnayzer, Juniper Junos Space Security Director, itp).

Jednocześnie w punkcie 6.9 Zamawiający pisze:" Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji." I tym samym uniemożliwia zaoferowanie kompletnego rozwiązania innego producenta niż Palo Alto, które by spełniło wszytkie wymagania.

Prosimy zatem o usunięcie wymagania 6.12 lub dopuszczenie jako równoważnego rozwiązania dla którego funkcjonalność jest realizowana z poziomu dedykowanego narzędzia logowania i raportowania tego samego producenta.

Jednocześnie prosimy o informację, czy narzędzie takie może być dostarczona w postaci maszyny wirtualnej u uruchomione w zasobach wirtualizacyjnych Zamawiającego.

Odpowiedź:
Zamawiający informuje, że dopuści rozwiązanie, w którym funkcjonalność, opisana w ppkt 6.12 Opisu przedmiotu zamówienia stanowiącego Załącznik nr 1 do SIWZ, będzie realizowana przez zewnętrzny system, pod warunkiem dostarczenia przez Wykonawcę kompletnego rozwiązania, bez konieczności wykorzystania środowiska wirtualnego lub fizycznego Zamawiającego.

Pytanie nr 19:
Na stronie 2 załącznika nr 1 do SIWZ (opis przedmiotu zamówienia) Zamawiający napisał:

„Zamawiający wymaga aby wdrożony System posiadał możliwość filtracji URL oraz posiadał funkcje Sandbox. Dostawa Systemu nie obejmuje dostawy licencji/subskrypcji na wskazane funkcje tj. filtrowanie URL i Sandbox."

Jednak w dalszej części tego załącznika Zamawiający stawia wymagania obligatoryjne dotyczące funkcjonalności filtrowania URL i Sandbox. Są to punkty 3.1, 3.17 i 3.19.

W związku z powyższym, czy Zamawiający wyrazi zgodę na modyfikację treści tych punktów na poniższą, tak aby treść OPZ była zgodna z intencją Zamawiającego:

3.1

System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL.

Funkcjonalność ta musi być dostępna po zakupie opcjonalnej licencji przez Zamawiającego, która nie jest przedmiotem niniejszego postępowania.

3.17

System zabezpieczeń firewall musi umożliwiać zdefiniowanie stron WWW i serwisów do których użytkownicy mogą wysyłać swoje poświadczenia. W przypadku próby wysłania poświadczeń do niezaufanej strony lub serwisu ruch musi zostać zablokowany.

Funkcjonalność ta musi być dostępna po zakupie opcjonalnej licencji przez Zamawiającego, która nie jest przedmiotem niniejszego postępowania.

3.19

System zabezpieczeń firewall musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box" plików różnych typów (exe, dll, pdf, msofffice, java, jpg, swf, apk) przechodzących przez firewall z wydajnością modułu anty-wirus, czyli nie mniej niż 3 Gbit/s, w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym.

Funkcjonalność ta musi być dostępna po zakupie opcjonalnej licencji przez Zamawiającego, która nie jest przedmiotem niniejszego postępowania.

Odpowiedź:
Zamawiający informuje, że podtrzymuje w tym zakresie zapisy SIWZ.
Zamawiający podkreśla, że w ramach przedmiotowego postepowania wymaga aby wdrożony System posiadał możliwość filtracji URL oraz posiadał funkcje Sandbox, z tym że Zamawiający nie oczekuje w ramach przedmiotowego postępowania wdrożenia i aktywowania funkcjonalności filtrowania URL i Sandbox. Zamawiający chce mieć możliwość aktywowania tych funkcjonalności we wdrożonym Systemie w dowolnym innym terminie po dokupieniu odpowiedniego typu licencji.

Powyższe odpowiedzi oraz zmiany SIWZ stanowią jej integralna część i są wiążące dla Zamawiającego i Wykonawców. Pozostała część SIWZ pozostaje bez zmian.

Dyrektor Departamentu
Administracji i Zamówień
Cesław Fik