Urząd Ochrony Konkurencji i Konsumentów

Warszawa, 2 września 2024 r.

BF-2.262.24.2024

Wszyscy uczestnicy postępowania

Dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego na **dostawę i wdrożenie systemu obejmującego funkcjonalność wielopoziomowej ochrony poczty elektronicznej**

Zamawiający informuje, że w terminie określonym zgodnie z art. 135 ust. 2 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz.U. z 2023 r., poz. 1605 ze zm.), zwanej dalej „ustawą Pzp", Wykonawcy zwrócili się do Zamawiającego z wnioskami (nr 1-15) o wyjaśnienie treści SWZ.
W związku z powyższym, działając na podstawie art. 135 ust. 2 ustawy Pzp, Zamawiający udziela następujących wyjaśnień:

Wniosek nr 1:
Dotyczy: Załącznik nr 1 do SWZ – Opis Przedmiotu Zamówienia, punkt 6. 9)
W ww. punkcie dotyczącym modułu Antyspam Zamawiający zawarł wymaganie, aby oferowane rozwiązanie w ramach ochrony przed atakami Directory Harvest Moduł musiało mieć możliwość zdefiniowania przedziału czasu od 1 sekundy do 1 godziny w ramach ograniczenia maksymalnej ilości połączeń i wiadomości z jednego adresu IP. Zwracamy uwagę, że takie zabezpieczenie nie zwiększa realnego bezpieczeństwa przed atakami typu Directory Harvest polegających na próbach odgadnięcia poprawnych adresów e-mail chronionej domeny. Ponadto taki rodzaj limitów może doprowadzić do czasowego paraliżu komunikacji pomiędzy zaufanymi domenami a naszym serwerem poczty, w okresach intensywniejszej komunikacji email pomiędzy organizacjami.
W związku z powyższym prosimy o dopuszczenie rozwiązania, które umożliwia kontrolowanie ilości połączeń i wiadomości w przedziale 30 minut lub dopuszczanie jako równoważne możliwość zaoferowania rozwiązania, które wykorzystuje inną technikę ochrony przed atakami Directory Harvest poprzez nakładanie limitów połączeń na nadawców, których reputacja przekroczy zdefiniowany próg wyliczany na podstawie podejrzanych zachowań (takich jak próba wysłania maila do nieistniejącego odbiorcy, wysyłka spamu czy wirusów).
W odpowiedzi na powyższy wniosek Zamawiający informuje, że dopuszcza rozwiązanie, które umożliwia kontrolowanie ilości połączeń i wiadomości w przedziale 30 minut oraz uzna za równoważne rozwiązania, które wykorzystują inną technikę ochrony przed atakami Directory Harvest.

Wniosek nr 2:

Dotyczy: Załącznik nr 1 do SWZ – Opis Przedmiotu Zamówienia, punkt 7. 2)

W ww. punkcie dotyczącym modułu Sandbox Zamawiający zawarł wymaganie, aby oferowane rozwiązanie w ramach funkcji modułu Sandbox (Antymalware) pracowało w trybie MTA (ang. Mail Transfer Agent).

Prosimy o dopuszczenie rozwiązania, które posiada natywną integrację między rozwiązaniem/modułem ochrony a Sandbox, gdzie oba moduły pochodzą od tego samego producenta. Natywna integracja umożliwia bezpośrednią kontrolę rozwiązania Sandbox poprzez transfer podejrzanych plików do analizy i oczekiwania na werdykt. Transfer odbywa się za pomocą wewnętrznego protokołu komunikacyjnego w warstwie TCP/IP.

W odpowiedzi na powyższy wniosek Zamawiający informuje, że dopuszcza rozwiązania, które posiadają natywną integrację między rozwiązaniem/modułem ochrony a Sandbox, gdzie oba moduły pochodzą od tego samego producenta.

Wniosek nr 3:

Dotyczy: Załącznik nr 1 do SWZ – Opis Przedmiotu Zamówienia, punkt 7. 5)

W ww. punkcie dotyczącym modułu Sandbox Zamawiający zawarł wymaganie, aby oferowane rozwiązanie w ramach funkcji modułu Sandbox (Antymalware) umożliwiało zwalnianie z kwarantanny zatrzymanych wiadomości.

Prosimy o dopuszczenie rozwiązania które realizuje funkcjonalność zwalniania z kwarantanny zatrzymanych wiadomości w module systemu ochrony poczty. W większości rozwiązań ochrony poczty funkcje kwarantanny wiadomości e-mail są realizowane w module pocztowym, a nie w module Sandbox, który służy do skanowania i detonacji podejrzanych plików/wiadomości. W praktyce moduł ochrony poczty wysyła poprzez natywną komunikację wiadomość do modułu Sandbox, oczekuje na werdykt i ewentualnie przerzuca wiadomość do kwarantanny w przypadku, gdy moduł Sandbox wykrył zagrożenie.

W odpowiedzi na powyższy wniosek Zamawiający informuje, że dopuszcza rozwiązania które realizują funkcjonalność zwalniania z kwarantanny zatrzymanych wiadomości w module systemu ochrony poczty, z zastrzeżeniem, że moduł Sandbox również posiada możliwość zwolnienia wiadomości i przekazania do odbiorcy.

Wniosek nr 4:

Dotyczy: Załącznik nr 1 do SWZ – Opis Przedmiotu Zamówienia, punkt 7. 11)

W ww. punkcie dotyczącym modułu Sandbox Zamawiający zawarł wymaganie, aby oferowane rozwiązanie w ramach funkcji modułu Sandbox (Antymalware) musiało mieć możliwość przepisania adresów URL w przesyłanej wiadomości tak aby pomimo kliknięcia użytkownik nie był przekierowany do potencjalnie złośliwej treści.

Prosimy o dopuszczenie rozwiązania które wyżej wymienione wymaganie zrealizuje w kontekście całościowego systemu ochrony poczty - realizacja funkcji przepisania adresów URL z wiadomości w module ochrony poczty/anty-spam.

W odpowiedzi na powyższy wniosek Zamawiający informuje, że dopuszcza rozwiązania, które w ramach wymaganej funkcji modułu Sandbox (Antymalware) dotyczącego realizacji przypisania adresów URL z wiadomości było realizowane w module ochrony poczty/anty-spam.

Wniosek nr 5:

Dotyczy: Załącznik nr 1 do SWZ – Opis Przedmiotu Zamówienia, punkt 7. 20)

W ww. punkcie dotyczącym modułu Sandbox Zamawiający zawarł wymaganie, aby oferowane rozwiązanie w ramach funkcji modułu Sandbox (Antymalware) musiało mieć możliwość dodawania oznaczenia (X header) do nagłówków wiadomości email zależnie od akcji podjętej przez Moduł analizy.

Prosimy o dopuszczenie rozwiązania które wyżej wymienione wymaganie zrealizuje w kontekście całościowego systemu ochrony poczty - realizacja funkcji dodania nagłówka do wiadomości (X header) odbywa się w module ochrony poczty/anty-spam po otrzymaniu werdyktu od rozwiązania Sandbox, gdzie oba rozwiązania są natywnie zintegrowane ze sobą.

W odpowiedzi na powyższy wniosek Zamawiający informuje, że dopuszcza zaoferowanie rozwiązania, które w ramach wymaganej funkcji modułu Sandbox (Antymalware) dotyczącego realizacji dodania nagłówka do wiadomości (X header) odbywała się w module ochrony poczty/anty-spam po otrzymaniu werdyktu od rozwiązania Sandbox, gdzie oba rozwiązania są natywnie zintegrowane ze sobą.

Wniosek nr 6:

Dotyczy: Załącznik nr 1 do SWZ – Opis Przedmiotu Zamówienia, punkt 6.22)

W ww. punkcie dotyczącym modułu Antyspam Zamawiający opisuje funkcjonalność związaną z mechanizmem DKIM (DomainKeys Identified Mail), która ma mieć możliwość podpisywania własnych nagłówków wiadomości. Zwracamy uwagę, że mechanizm DKIM opisany m.in. w RFC 6376 wprost nie determinuje jakie nagłówki powinny być brane pod uwagę przy generacji podpisu DKIM. Jedna ze strategii mówi o podpisywaniu wszystkich, niepowtarzalnych nagłówków, a inna o podpisywaniu tylko „znanych" nagłówków (tzw. „well-known headers"). Według RFC mocno rekomendowanym jest podpisywanie nagłówków widocznych w wiadomości email takich jak Date, Subject, Reply-To. W związku z tym prosimy o dopuszczenie zaoferowania systemu, który jest literalnie zgodny z RFC 6376 w zakresie DKIM.

W odpowiedzi na powyższy wniosek Zamawiający informuje, że dopuszcza rozwiązanie, które jest zgodne z RFC 6376 w zakresie DKIM.

Wniosek nr 7:

Dotyczy: Załącznik nr 1 do SWZ – Opis Przedmiotu Zamówienia, punkt 6. 22)

W ww. punkcie dotyczącym modułu Antyspam Zamawiający opisuje funkcjonalność związaną z mechanizmem DKIM (DomainKeys Identified Mail), która ma mieć możliwość podpisywania treści wiadomości (ang. Body) bez limitu rozmiaru wiadomości. Zwracamy uwagę, że w praktyce systemy pocztowe narzucają własne limity rozmiaru przyjmowanych i wysyłanych

wiadomości mailowych. Np. w przypadku wielu popularnych serwisów pocztowych limit wysyłanego maila to maksymalnie 25MB, w instytucjach czy korporacjach rozmiar ten jest niejednokrotnie jeszcze mniejszy i wynosi często 5MB. Ponadto sama implementacja danego systemu poczty może narzucać limity na maksymalny rozmiar przetwarzanych wiadomości.
W związku z powyższym wnosimy o dopuszczenie rozwiązania z możliwością ustawienia rozmiaru wiadomości jaka zostanie podpisana, i ustalenie rozsądnego limitu np. 50MB. W ten sposób Zamawiający dopuści systemy implementujące poprawnie mechanizm DKIM, podpisujące wiadomości w obrębie własnych (wewnętrznych) limitów (np. maksimum 50 MB rozmiaru wiadomości).
W odpowiedzi na powyższy wniosek Zamawiający informuje, że dopuszcza rozwiązania z możliwością ustawienia rozmiaru wiadomości ale dla rozmiaru wiadomości minimum 100MB jaka zostanie podpisana.

Wniosek nr 8:
Zamawiający wymaga licencji Microsoft Windows, Microsoft Office. Prosimy o informację ile sumarycznie ma być licencji przy założeniu, że będą 2 szt. Sandbox. Czy w tym wariancie dopuszczalne są subskrypcje licencji Microsoft na okres 36 miesięcy realizowane poprzez tzw. umowy SPLA?
W odpowiedzi na powyższy wniosek Zamawiający informuje, że liczba licencji Microsoft Windows powinna być zgodna ze wskazaną w OPZ liczbą maszyn do detonacji, czyli minimum 4 systemy powinny posiadać licencję na Microsoft Office 2016, 2019, 2021 każdy. Zamawiający wyraża zgodę na zaoferowanie wymaganego oprogramowania w formie minimum 36 miesięcznych subskrypcji.

Wniosek nr 9:
Czy w przypadku, gdy dostarczane są dwa produkty jednego producenta (produkt 1 - ochrona poczty oraz produkt 2 - sandbox) wymagane jest rozwiązanie jednej konsoli do zarządzania całością? (dostarczane jako maszyna VM np. na VMware vSphere).
W odpowiedzi na powyższy wniosek Zamawiający informuje, że zgodnie z zapisami zawartymi w rozdziale 2 pkt. 4 OPZ, każdy moduł musi posiadać jedną osobną konsolę zarządzającą.

Wniosek nr 10:
Zamawiający w punkcie 6.2. wymaga, aby system realizował skanowanie antyspamowe i antywirusowe z wydajnością min. 800 tys. wiadomości/dzień, jednak nie określa metodologii testowania ani przyjętych założeń, co może prowadzić do nieporównywalności różnych rozwiązań. Warto zauważyć, że tylko niektórzy producenci podają takie dane dotyczące przepustowości, jednak często nie wskazują przy tym warunków testowych, co może sugerować preferencję dla konkretnego rozwiązania opartego na specyficznej metryce. Taka sytuacja może prowadzić do wyników, które nie odnoszą się do rzeczywistych warunków działania systemu. Ocenę wydajności takiego systemu można wyrazić zarówno poprzez

określenie jego przepustowości (wiadomości/dzień), jak również alternatywnie liczbę użytkowników (aktywnych i używanych adres email). Takie podejście, przy jednoczesnym pozostawieniu oceny przydatności rozwiązania, pozwoli na uwzględnienie większej liczby producentów, którzy mierzą metryki wydajności i wymiarowanie systemów w inny sposób. Czy Zamawiający wyraża zgodę na rozszerzenie sposobu oceny wiadomości o określenie liczby końcowych użytkowników systemu i w związku z tym określi ich przewidywaną ilość?
W odpowiedzi na powyższy wniosek Zamawiający informuje, że wyraża zgodę na rozszerzenie sposobu oceny wiadomości o określenie liczby końcowych użytkowników systemu. Liczbę adresów mailowych szacuje się na rząd wielkości około 900.

Wniosek nr 11:
Zamawiający w punkcie 3a. określa, że moduł Sandbox musi mieć możliwość pełnej integracji z dostarczanym modułem ochrony poczty e-mail oraz współpracy z systemami zabezpieczeń NGFW (Next Generation Firewall) lub SWG (Security Web Gateway), a także w oparciu o interfejsy programistyczne API.
Bez doprecyzowania, co dokładnie Zamawiający rozumie przez integrację z systemami NGFW lub SWG, trudno jest spełnić ten wymóg w pełni. Dodatkowo, nie jest możliwe domyślenie się intencji Zamawiającego, jeśli ten punkt nie odnosi się do specyficznych integracji OOTB (out-of-the-box) z konkretnymi producentami i ich rozwiązaniami. Dostępność rozbudowanych interfejsów programistycznych API umożliwiłby zintegrowanie systemu z dowolnym innym rozwiązaniem wspierającym takie działania. Czy w związku z powyższym Zamawiający wyraża zgodę, aby dostępność i pełna dokumentacja interfejsów API dostarczonego rozwiązania była uznana za pełne spełnienie warunku w zakresie integracji z systemami NGFW oraz SWG?
W odpowiedzi na powyższy wniosek Zamawiający informuje, że uzna spełnienie warunku w zakresie integracji z systemami NGFW oraz SWG w przypadku zaoferowania rozwiązania z dostępnością rozbudowanych interfejsów programistycznych API umożliwiającym zintegrowanie systemu z dowolnym innym rozwiązaniem wspierającym takie działanie. Interfejs API dostarczonego rozwiązania musi integrować się z systemami NGFW oraz SWG znajdującymi się w grupach produktów Leaders oraz Challenger kwadratu Gartnera w roku 2023/2024.

Wniosek nr 12:
Zamawiający w punkcie 6.9. określa, że ochrona przed atakami Directory Harvest musi polegać na monitorowaniu i ograniczaniu ilości połączeń z jednego adresu IP w określonym przedziale czasu, z możliwością definiowania tego przedziału od 1 minuty do 1 godziny oraz ustalenia maksymalnej ilości połączeń i wiadomości z jednego adresu IP. W ramach skutecznej obrony przed atakami tego rodzaju można zastosować również rozwiązania polegające na weryfikacji odbiorcy wiadomości przed jej akceptacją przez system. W takim podejściu bramka email sprawdza, czy wiadomość może być przekazana dalej do serwera SMTP zgodnie z ustawieniami. Jeśli system stwierdzi, że wiadomość nie może być dostarczona, zostaje ona odrzucona na poziomie SMTP, a nadawca otrzymuje odpowiedni komunikat. Takie

rozwiązanie skutecznie minimalizuje skuteczność ataków Directory Harvest, ponieważ nieprawidłowe zapytania są automatycznie odrzucane, co czyni atak bardzo nieopłacalnym. Wykonawca wnioskuje o rozważenie możliwości wykorzystania różnych zaawansowanych metod ochrony przed atakami Directory Harvest, takich jak wspomniane powyżej, aby zapewnić bardziej elastyczne i skuteczne zabezpieczenie systemu. Czy Zamawiający wyraża zgodne na ochronę przed atakami Directory Harvest za pomocą innych skutecznych technik ochrony?

W odpowiedzi na powyższy wniosek Zamawiający informuje, że dopuszcza jako równoważne rozwiązania, które wykorzystują inną techniki technikę ochrony przed atakami Directory Harvest.

Wniosek nr 13:

Zamawiający w punkcie 7.1. określa, że analiza ataku musi odbywać się za pomocą dynamicznej analizy zachowania kodu, umożliwiającej równoczesną analizę zagrożenia w różnych wersjach systemu operacyjnego i aplikacjach. Dodatkowo, w punkcie 7.6, wymaga się, aby moduł Antymalware umożliwiał uruchomienie minimum 16 instancji wirtualnych systemów MS Windows, zawierających Windows 10 i Windows 11 oraz 1 pakiet biurowy MS Office 2019 oraz MS Office 2021 w celu wykonania analizy Sandbox. Technologia emulacyjna pozwala na szybszą i bardziej efektywną analizę zagrożeń, eliminując jednocześnie wiele problemów związanych z tradycyjną wirtualizacją, takich jak ograniczona skalowalność, wysoki koszt utrzymania oraz długi czas oczekiwania na wyniki analizy. Ponadto, emulacja jest mniej podatna na techniki unikania wykrycia, co czyni ją bardziej niezawodną w identyfikowaniu zagrożeń. W związku z tym, Wykonawca wnioskuje, aby w kontekście punktu 7.1, rozważenie różnych wersji systemów operacyjnych nie było wymagane, ponieważ specyfika technologii emulacyjnej sprawia, że takie wymaganie nie jest istotne i nie może być spełnione w kontekście proponowanej metody. Czy Zamawiający wyraża zgodę na dopuszczenie technologii opartej na emulacji jako bardziej zaawansowanej i efektywnej metody analizy w porównaniu do tradycyjnej wirtualizacji, zwłaszcza w kontekście systemów pocztowych? Analogicznie, odnosząc się do punktu 7.6, który wymaga uruchomienia wirtualnych instancji systemów i programów, należy zauważyć, że technologia emulacyjna, nie opiera się na wirtualizacji. W związku z tym, w takim wypadku nie jest możliwe spełnienie wymogu dotyczącego uruchamiania różnych wersji oprogramowania, ponieważ emulacja zapewnia efektywną analizę zagrożeń bez potrzeby korzystania z wirtualnych instancji systemów operacyjnych. Czy Zamawiający wyraża zgodę na alternatywne zastosowanie zamiast wirtualizacji metody analizy opartej na emulacji, która nie wymaga wirtualizacji, a mimo to oferuje skuteczną ochronę i analizę zagrożeń?

W odpowiedzi na powyższy wniosek Zamawiający informuje, że wyraża zgodę na zastosowanie metody analizy opartej na emulacji, pod warunkiem, że oferowane rozwiązanie jest w stanie emulować środowiska lub wersje systemów o których mowa w rozdziale 7 pkt 6 OPZ.

Wniosek nr 14:

Zamawiający w punkcie 7.3. wymaga, aby każdy Analizator dynamiczny był dostarczony w postaci urządzenia fizycznego Producenta, działającego w oparciu o dedykowane platformy sprzętowe (appliance) dostarczane przez Producenta rozwiązania, z systemem operacyjnym utwardzonym (hardening) przez Producenta. Z uwagi na to, że w punkcie 3 Zamawiający dopuszcza możliwość realizacji poszczególnych elementów systemu w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W szczególności, w sytuacji kiedy rozwiązanie jest realizowane w formie oprogramowania dostarczonego przez Producenta, Wykonawca proponuje możliwość samodzielnej instalacji i konfiguracji na odpowiednio zabezpieczonym sprzęcie, którego hardeningu dokona Wykonawca. Czy Zamawiający wyraża zgodę, aby hardening był przeprowadzony przez Wykonawcę lub Producenta?

W odpowiedzi na powyższy wniosek Zamawiający informuje, że Zamawiający wyraża zgodę, aby hardening był przeprowadzony przez Wykonawcę lub Producenta.

Wniosek nr 15:

Zamawiający w punkcie 3 wymaga, aby System był dostarczony jako moduły, w tym dwa dedykowane urządzenia (appliance) tworzące klaster wysokiej dostępności dla funkcji Antyspam oraz Antymalware. Czy Zamawiający wyraża zgodę na dostarczenie systemu jako dwa dedykowane urządzenia (appliance) tworzące klaster, który zwiększa przepustowość i ciągłość działania środowiska dla funkcji Antyspam oraz Antymalware?

W odpowiedzi na powyższy wniosek Zamawiający informuje, że wymaga aby moduł Sanbox składał się z 2 urządzeń pracujących w klastrze, tak samo moduł Antyspam ma składać się z 2 urządzeń pracujących w klastrze. Każde z urządzeń musi spełniać parametry techniczne zapisane w OPZ.

Zamawiający informuję, że wniosek nr 16 wpłynął po terminie określonym w art. 135 ust. 2 ustawy Pzp, jednak Zamawiający postanowił udzielić następujących wyjaśnień:

Wniosek nr 16:

Dotyczy rozdziału 9 pkt. 4) OPZ- załącznik nr 1: Zamawiający w OPZ wymaga:

Wdrożenie Środowiska realizowane będzie przez autoryzowanych inżynierów posiadających certyfikat maksymalnie o jeden poziom niższy od najwyższego na ścieżce certyfikacyjnej producenta, uprawniający do realizacji prac. Wykonawca załączy certyfikat poświadczający spełnienie warunku na etapie składania ofert.

Prosimy o wyjaśnienie jakiego charakteru dokumentem w postępowaniu jest ww. certyfikat, którego żąda Zamawiający do oferty. Zamawiający nie ustanowił warunku udziału w postępowaniu w zakresie wymagań dot. osób skierowanych do realizacji zamówienia, tym samym nie mieści się on w katalogu dokumentów jakich może żądać Zamawiający zgodnie z

Rozporządzeniem w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy. Prosimy o zmianę ww. zapisu na: „Wdrożenie Środowiska realizowane będzie przez autoryzowanych inżynierów posiadających certyfikat maksymalnie o jeden poziom niższy od najwyższego na ścieżce certyfikacyjnej producenta, uprawniający do realizacji prac. Zamawiający może wezwać Wykonawcę, którego oferta została wybrana do przedłożenia ww. certyfikatu, poświadczającego spełnienie warunku, po wyborze oferty najkorzystniejszej a przed podpisaniem umowy.

W odpowiedzi na powyższy wniosek Zamawiający informuje, że zmienia brzmienie rozdziału 9 pkt. 4 OPZ na następujący „Wdrożenie Środowiska realizowane będzie przez autoryzowanych inżynierów posiadających certyfikat maksymalnie o jeden poziom niższy od najwyższego na ścieżce certyfikacyjnej producenta, uprawniający do realizacji prac. Zamawiający wezwie Wykonawcę, którego oferta została wybrana do przedłożenia ww. certyfikatu, poświadczającego spełnienie wymogu, po wyborze oferty najkorzystniejszej a przed podpisaniem umowy."

Jednocześnie Zamawiający informuje, że na podstawie art. 137 ust. 1 ustawy Pzp, zmienia treść SWZ, poprzez zmianę rozdziału 9 pkt. 4) OPZ, stanowiącego załącznik nr 1 do SWZ.

Zamawiający informuje, że odpowiedzi opublikowane w dniu 23.08.2024 r. dotyczą przedmiotu zamówienia pn. Dostawa i wdrożenie systemu obejmującego funkcjonalność wielopoziomowej ochrony poczty elektronicznej.

Powyższa odpowiedź stanowi modyfikację treści SWZ. Termin składania ofert nie ulega zmianie. Ofertę wraz z wymaganymi dokumentami należy umieścić na Platformie pod adresem **https://platformazakupowa.pl/pn/uokik** - w myśl ustawy Pzp na stronie internetowej prowadzonego postępowania **do dnia 9 września 2024 r. do godziny 11:00.** Otwarcie ofert następuje niezwłocznie po upływie terminu składania ofert, nie później niż następnego dnia po dniu, w którym upłynął termin składania ofert tj. 9 września 2024 r. g. 11:15.

Z poważaniem,

Józef Wacnik
Dyrektor
Biura Informatyki i Ochrony
/podpisano elektronicznie/