Urząd Ochrony Konkurencji i Konsumentów

Warszawa, 5 czerwca 2024 r.

BF-2.262.11.2024

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", Wykonawca zwrócił się do Zamawiającego z wnioskami o wyjaśnienie treści SWZ.

W związku z powyższym, działając na podstawie art. 135 ust. 2 ustawy Pzp, Zamawiający udziela następujących wyjaśnień:

Wniosek nr 1.
W Punkcie 3.a) Zamawiający zawarł wymaganie, aby oferowane rozwiązanie pracowało w trybie transparentnym. Zwracamy uwagę, że wymiana poczty elektronicznej w Internecie realizowana jest poprzez protokół SMTP opisany w RFC nr 5321 który jest oficjalnym dokumentem opisującym jak ma wyglądać implementacja systemu poczty elektronicznej, aby zapewnić kompatybilność komunikacji. We wspomnianym RFC5321 w sekcji 2.3.2 znajdują się definicje stron tj. nadawca oraz odbiorca zaś w sekcji 2.3.4 jest zdefiniowane pojęcia serwera jako Host musi mieć adres IP i być jawnie znany dla drugiej strony, aby poprawnie obsługiwać protokół SMTP. Dodatkowo w punkcie 6.33 OPZ Zamawiający oczekuje możliwości przekierowania wiadomości pocztowej, gdzie tryb transparentny z definicji nie może być stroną nadawczą zgodnie z sekcją 2.3.4 wskazywanego RFC5321.
W związku z powyższym wnosimy o usunięcie wymogu pracy w trybie transparentnym z uwagi na to, że jest to funkcjonalność spoza definicji protokołu SMTP, a więc taki niezdefiniowany tryb będzie powodować błędy w przekazywaniu wiadomości pocztowych z innym systemów obsługi poczty komunikujące się poprzez Internet a które zgodnie z RFC5321 (protokół SMTP) nie będą rozumieć strony pracującej w niezdefiniowanym dla protokołu trybie transparent.

W odpowiedzi na powyższy wniosek Zamawiający informuje, że wyraża zgodę na zaoferowanie rozwiązania bez możliwości pracy w trybie transparentnym, pod warunkiem spełnienia pozostałych wymagań minimalnych określonych w Specyfikacji Warunków Zamówienia.

Wniosek nr 2.

W punkcie 6.15 Zamawiający oczekuje funkcji ponownego sprawdzania wiadomości pocztowej w trakcie próby zwolnienia wiadomości z kwarantanny. Wnosimy o usunięcie tego zapisu z uwagi, że taka funkcja nie zwiększa bezpieczeństwa a co więcej włączenie takiej funkcji spowoduje, że wiadomości nigdy nie da się zwolnic z kwarantanny z uwagi na to że jeśli użytkownik lub administrator zechce świadomie zwolnić przesyłkę to taka akcja nie zostanie wykonana ponieważ wiadomość ponownie zostanie załadowana do kwarantanny. Co więcej w przypadku błędnego zakwalifikowania wiadomości przy włączonej funkcji ponawianej analizy nie zezwoli na zwolnienie wiadomości.

W związku z powyższym prosimy o usunięcie punktu 6.15, świadomy użytkownik musi mieć możliwość zwolnienia wiadomości z kwarantanny, a jeśli nie ma być dostępna taka opcja to normalnym jest wyłączenie zwalania z kwarantanny a nie wykonywanie ponownego skanowania, aby zablokować zwolnienie

W odpowiedzi na powyższy wniosek Zamawiający informuje, że w punkcie 6.15 Zamawiający ma na myśli aby zaoferowane rozwiązanie miało możliwość przepuszczenia wiadomości email z kwarantanny geteway do sandboxa w celu głębszej analizy przed dostarczaniem email do odbiorcy. W związku z powyższym Zamawiający nie wyraża zgody na zmianę zapisów we wnioskowanym zakresie.

Wniosek nr 3.

W punkcie 6.32.f Zamawiający oczekuje filtrowania wiadomości bazujące na statystyce filtrów Bayesa. Zwracamy uwagę, że na filtry Bayesa które bazują na listach pojedynczych słów, znane są ataki o nazwie „Bayesian poisoning". W szczególności w czasach, kiedy w wiadomościach mail wykorzystywane jest formatowanie HTML pozwalające na takie formatowanie tekstu takie jak zmianę koloru i wysokości czcionki a w szczególności wyłączanie widoczności, tak że tylko cześć treści będzie widoczna w czytniku mail dla użytkowania, zaś skaner poczty na bramce będzie analizował cały tekst, a więc wraz z wstawkami które został użyte aby zmniejszyć statystykę występowania słów uznawanych za spam.

W związku z powyższym wnosimy o rozszerzenie tego zapisu o możliwość zaoferowania rozwiązań, które wykorzystują inne techniki wykrywania spamu w treści wiadomości takie jak uczenie AI na bazie wzorców lub logiki rozmytej.

W odpowiedzi na powyższy wniosek Zamawiający informuje, że wyraża zgodę na zmianę zapisów w powyższym zakresie.

W związku z powyższym, na podstawie art. 137 ustawy Pzp, Zamawiający dokonuje zmiany treści pkt 6 ppkt 32 lit f OPZ, stanowiącego załącznik nr 1 do SWZ, który otrzymuje następujące brzmienie:

f. Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen, oraz techniki wykrywania spamu w treści wiadomości takie jak uczenie AI na bazie wzorców lub logiki rozmytej.

Wniosek nr 4.

W punkcie 6.32.h Zamawiający oczekuje wykorzystania techniki opóźnienia dostarczenia przesyłki miał określanej jako greylisting. Z definicji greylisting przy pierwszej próbie przekazania wiadomości miał, kiedy odbiorca nie zna nadawcy (czyli faktycznie jest to pierwsze połączenie lub odbiorca usunąć informacje o ostatnim połączeniu po określonym czasie nieaktywności) to przy odbieraniu takiej wiadomości odbiorca wysyła komunikat typu „mam awarię wróć później" i wewnętrznie włącza odliczanie zdefiniowanego czasu. Jeśli nadawca wróci po skończeniu odliczania to już przy następnej próbie niezależne od tego kto nadaje i co znajduje się w wiadomości mail greylisting przepuści taką przesyłkę licząc, że inne podsystemy zablokują taką wiadomość, jeśli jest spamem. Co więcej, jeśli druga próba przekazania powiedzie się to do kiedy pamiętane jest to połączenie greylisting nie zablokuje nadawcy nawet jeśli w poprzednich połączeniach przekazywany był spam. Dodatkowo, jeśli nadawca jest zaufany ale informacji i tym nadawcy nie ma w bazie greylistingu (nie komunikował się wystarczająco długo aby wpis z bazy greylistingu został usuniety) to wtedy ze względu na blokowania pierwszego połączenia przesyłka zawsze będzie opóźniona.

W związku z powyższym wnosimy o usunięcie wymogu wykorzystywania greylistingu który wprowadza tylko opóźnienia a w zamian wprowadzenie w tym punkcie wymagań na SPF, DKIM oraz DMARC które są standardami do obrony przez spamem i phisingiem opisanymi w RFC i nie wprowadzającymi opóźnień tak jak greylisting

W odpowiedzi na powyższy wniosek Zamawiający informuje, że wyraża zgodę na zmianę zapisów przedstawionych w powyższym wniosku i nie dopuszcza kontroli w oparciu o greylisting.

W związku z powyższym, na podstawie art. 137 ustawy Pzp, Zamawiający dokonuje zmiany treści pkt 6 ppkt 32 lit h OPZ, stanowiącego załącznik nr 1 do SWZ, który otrzymuje następujące brzmienie:

h. Kontrola w oparciu o SPF, DKIM oraz DMARC.

Powyższe odpowiedzi stanowią 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 **do dnia 18.06.2024 r. do godziny 11:00.** Otwarcie ofert następuje w dniu, w którym upłynął termin składania ofert tj. **18.06.2024 r. godz. 11:15**.

Z poważaniem,

Józef Wacnik
Dyrektor
Biura Informatyki i Ochrony
/podpisano elektronicznie/