Warszawa, 26 listopada 2020 r.

DAZ.262.67.2020

Wszyscy zainteresowani

Dotyczy: postępowania o udzielenie zamówienia publicznego (nr 55/20/PN/P53) *zakup licencji dostępowej do oprogramowania klasy Email Security Gateway w modelu SaaS.*

Działając na podstawie art. 38 ust. 2 ustawy Prawo zamówień publicznych (t.j. Dz. U. 2019 r. poz. 1843. z póź. zm.), uprzejmie informuję, iż do Zamawiającego wpłynęły wnioski o wyjaśnienie treści SIWZ. Poniżej przedstawiam ich treść wraz z wyjaśnieniem udzielonym przez Zamawiającego

Pytanie 1:
Dotyczy „Umowy", paragraf 1, ustęp 1
Czy Zamawiający dopuszcza rozwiązanie dostarczane w formie subskrypcji na określony okres?
Odpowiedź 1:
Zamawiający wymaga, dostępu do oprogramowania w modelu SaaS przez okres 36 miesięcy dla przynajmniej 1001 skrzynek. Zamawiający dopuszcza rozwiązanie dostarczane w formie subskrypcji.

Pytanie 2:
Dotyczy „Umowy", paragraf 3, ustęp 7

Bardzo prosimy o wprowadzenie zapisów symetrycznych, przyznających Wykonawcy te same uprawnienia?

Odpowiedź 2:
Zamawiający nie widzi możliwości wprowadzenia zapisów symetrycznych. Podpisanie przez Zamawiającego protokołu potwierdzającego prawidłową realizację zamówienia stanowi podstawę do wystawienia faktury vat i wypłaty wynagrodzenia w pełnej kwocie.

Pytanie 3:
Dotyczy „Umowy", paragraf 7

W związku z zapisem, że Umowa jest zawarta na okres 36 miesięcy od daty jej podpisania oraz uwzględniając zapisy dotyczące czasu dostarczenia oraz wdrożenia rozwiązania bardzo prosimy o uściślenie na jaki okres ma zostać dostarczona subskrypcja rozwiązania

Odpowiedź 3:
Zgodnie z zapisami SIWZ oraz IPU czas realizacji zamówienia liczony będzie od dnia zawarcia umowy przez okres 36 miesięcy.

Pytanie 4:

Dotyczy „Umowy”, uwagi ogólne

Prosimy o wprowadzenie poniższego zapisu w zakresie sytuacji związanej z epidemią koronawirusa. W chwili podpisywania umowy zagrożenia związane z epidemią są już znane, choć nikt nie jest w stanie przewidzieć ich rozwoju i konsekwencji. Tym niemniej nie są już siłą wyższą.

„4. Strony zgodnie oświadczają i uznają, iż panujące w dacie podpisania Umowy rozprzestrzenianie się Koronawirusa SARS-CoV-2 („Koronowirus”) jest działaniem Siły Wyższej, a zawarcie niniejszej Umowy następuje w warunkach działania Siły Wyższej. Wobec braku możliwości przewidzenia rozwoju rozprzestrzeniania się Koronowirusa (oraz wszelkich możliwych jego mutacji) oraz wpływu tego zdarzania na warunki ekonomiczne, społeczne, polityczne, administracyjne panujące w kraju jak i na świecie, Strony niniejszym akceptują i przyjmują do wiadomości, iż po dacie wejścia w życie Umowy realizacja całości lub części Umowy może być czasowo (przez okres działania Siły Wyższej w postaci rozprzestrzeniania się Koronawirusa) niemożliwa. W takim przypadku Strony zgodnie oświadczają, iż w okresie związanym z rozprzestrzenianiem się Koronawirusa zawieszone będzie mogło być wykonywanie świadczeń Stron Umowy oraz wyłączona będzie jakakolwiek odpowiedzialność Stron za brak możliwości realizacji całości lub części Umowy i/lub brak możliwości realizacji Umowy zgodnie z jej warunkami.”

Odpowiedź 4:
Zamawiający przewiduje płatność za realizację zamówienia jednorazowo po dostarczeniu i konfiguracji zaproponowanego przez Wykonawcę rozwiązania, przez co nie widzi konieczności uwzględniania zaproponowanych zapisów dotyczących zawieszenia realizacji umowy z uwagi na rozprzestrzenianie się Koronowirusa SARS-CoV-2. Ponadto, ustawodawca uregulował przedmiotowe kwestie w ustawie z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych, Dz.U. z 2020 r., poz.1842).

Pytanie 5:
Dotyczy „Specyfikacji Istotnych Warunków zamówienia”, Wymagania funkcjonalne, AS.013

Z doświadczenia Wykonawcy wynika, że mechanizmy definiowania polityk greylistingu są mechanizmami przestarzałymi i mało nieskutecznymi , co więcej powodującą opóźnienia w dostarczaniu poczty elektronicznej, co jest źle odbierane przez Klientów. Oferowane przez nas mechanizmy ochrony radzą sobie doskonale bez korzystania z mechanizmów Greylisting-u. Bardzo prosimy o usunięcie tego zapisu.

Odpowiedź 5:
Zamawiający podtrzymuje zapisy SOPZ.

Pytanie 6:
Dotyczy „Specyfikacji Istotnych Warunków zamówienia”, Wymagania funkcjonalne, AS.018

Prosimy o rozwinięcie przez Zamawiającego tego wymagania o informację jaki docelowy efekt ma zostać osiągnięty dzięki opisanej funkcjonalności. Czy dopuszczalne jest aby był on osiągalny innymi mechanizmami?

Odpowiedź 6:

Zamawiający wymaga „czytania" zawartości plików graficznych i określania czy w obrazie znajduje się treść pasująca do reguł antyspamowych. Zamawiający dopuszcza wszystkie mechanizmy/funkcjonalności, które umożliwią „czytanie" plików graficznych i rozpoznawania czy treść zawarta obrazie jest pożądana czy też nie (czyt. jest spamem).

Pytanie 7:
Dotyczy „Specyfikacji Istotnych Warunków zamówienia", Wymagania funkcjonalne, AS.020

Najlepsze systemu klasy AntiSpam/AntiPhishing posiadają mechanizm uczenia maszynowego. Mechanizm ten jest o wiele skuteczniejszy od filtrów Bayes. Czy w związku z tym, Zamawiający jest skłonny do usunięcia tego wymagania lub uznania filtrów Bayesa jako wymóg opcjonalny?

Odpowiedź 7:
Zamawiający podtrzymuje zapisy SOPZ oraz informuje iż nie wyklucza w SOPZ mechanizmów opartych na uczeniu maszynowym.

Pytanie 8:
Dotyczy „Specyfikacji Istotnych Warunków zamówienia", Wymagania funkcjonalne, AV.002
Z doświadczenia Wykonawcy wynika, że powszechną na rynku bezpieczeństwa IT tendencją jest oferowanie przez producentów silników AV pochodzących głównych vendorów rynku AV na świecie. Takie podejście zwiększa bezpieczeństwo całego środowiska AntiSpam, gdyż jego główną zaletą jest fakt możliwości wyboru silnika AV od innego producenta, który specjalizuje się w skanowaniu AV (silnik taki oczywiście jest oferowany razem z wybranym silnikiem AV przy zakupie produktu). Skanowanie AV odbywa się w ramach silników/mechanizmów ochrony Produktu, bez potrzeby instalacji/konfiguracji osobnego urządzenia itp. Zdaniem Wykonawcy obecny zapis jest preferencją konkretnych producentów rozwiązań AniSpam, a równocześnie nie niesie za sobą żadnych merytorycznych podstaw. Czy w związku z tym faktem Zamawiający jest skłonny do usunięcia tego wymagania lub zmianę zapisu na "Ochrona AV powinna posiadać globalną bazę sygnatur wirusów i innego złośliwego oprogramowania dostarczoną przez wiodących producentów silników AV znajdujących się w kwadracie Gartnera"?
Odpowiedź 8:
Zamawiający podtrzymuje zapisy SOPZ. Zamawiający nie wyklucza wykorzystywania przez oferowane oprogramowanie sygnatur wirusów pochodzących od innych vendorów.

Pytanie 9:
Dotyczy „Specyfikacji Istotnych Warunków zamówienia", Wymagania funkcjonalne, AV.004
Najlepsze systemu klasy AntiSpam/AntiPhishing nie modyfikują zawartości przesyłanych dokumentów. Według ich Producentów byłoby to naruszeniem integralności komunikacji biznesowej. Systemy te posiadają znacznie skuteczniejsze metody blokowania "złośliwych" dokumentów bazujące na mechanizmach SandBox-owych. Czy w świetle tego co napisano, Zamawiający jest skłonny do usunięcia tego wymagania lub zmodyfikowania zapisu na "Opcjonalnie - Mechanizm neutralizacji zawartości w wiadomościach pocztowych, dokumentach MS Office i PDF (usuwanie makr, zawartości aktywne, załączników)"?
Odpowiedź 9:
Zamawiający podtrzymuje zapisy SOPZ.

Pytanie 10:
Dotyczy „Specyfikacji Istotnych Warunków zamówienia”, Wymagania funkcjonalne, AV.005

Najskuteczniejsze systemu klasy AntiSpam/AntiPhishing, umożliwiają przesyłanie wiadomości w bezpieczny i zautomatyzowany sposób. Wykorzystywane są do tego bardzo skuteczne moduły Sandox-owe. Silniki podejmują próbę deszyfracji archiwów zip, oraz dokumentów Ms Office, PDF mechanizmem brute force, z wykorzystaniem słów znalezionych w treści wiadomości. Według producenta ten sposób jest najskuteczniejszy i nie powoduje dodatkowego obciążenia silników skanujących, poprzez wykorzystywanie list haseł Administratora, które to listy mogą być bardzo obszerne. Dodatkowo oferowane jest zablokowanie (np. wrzucenie do kwarantanny) wiadomości/plików, które nie będą mogły być odpakowane/przeskanowane. Dostęp do nich może mieć jedynie administrator systemu, który ma możliwość podjęcia odpowiedniej akcji. Czy w związku z tym, Zamawiający jest skłonny do usunięcia tego wymagania lub zmiany na "Opcjonalnie - Automatyczne deszyfrowanie archiwów, plików PDF i dokumentów biurowych za pomocą wbudowanych i zdefiniowanych przez administratora list haseł oraz funkcji wykrywania słów w treści wiadomości e-mail"?

Odpowiedź 10:
Zamawiający podtrzymuje zapisy SOPZ.

Pytanie 11:
Dotyczy „Specyfikacji Istotnych Warunków zamówienia”, Wymagania funkcjonalne, AV.012

Według najlepszej wiedzy technicznej Wykonawcy wymaganie to nie ma zastosowania w odniesieniu do architektury bramki SMTP. Prosimy o doprecyzowanie celu takiego wymagania lub jego usunięcie.

Odpowiedź 11:
Zamawiający usuwa punkt AV.012 z SOPZ.

Pytanie 12:
Dotyczy „Specyfikacji Istotnych Warunków zamówienia”, Wymagania funkcjonalne, AV.013

Prosimy o doprecyzowanie celu takiego wymagania.

Odpowiedź 12:
Zamawiający usuwa punkt AV.013 z SOPZ.

Pytanie 13:
Dotyczy „Specyfikacji Istotnych Warunków zamówienia”, Wymagania funkcjonalne, SS.004

W przypadku dostępnych na rynku rozwiązaniach pracujących w trybie SaaS za utrzymanie środowiska SaaS odpowiada producent dbając o jego aktualność. Klient nie ma możliwości decydowania o numerze wersji oprogramowania, co według producenta jest optymalne ze względu na aktualność patch-y/wersji, o których Klient mógłby nie pamiętać. Informacja na temat planowanych prac na klastrze Klienta jest dostępna dla jego personelu technicznego, co jest optymalne ze względu na to co napisano wcześniej. Czy w świetle tego co napisano, Zamawiający jest skłonny do usunięcia tego wymagania lub zmodyfikowania na "Producent systemu wraz z informowaniem Klienta jest odpowiedzialny za zarządzanie infrastrukturą, nadzór nad ciągłością działania, aktualizacje systemu, monitorowanie ruchu i poziomu wykorzystanych zasobów, rozwiązywania zgłaszanych problemów/incydentów"?

Odpowiedź 13:
Zamawiający podtrzymuje zapisy SOPZ jednocześnie informując iż zapis ten nie wyklucza informowania przez producenta o zmianach w oprogramowaniu.

Pytanie 14:
Dotyczy „Specyfikacji Istotnych Warunków zamówienia", Wymagania funkcjonalne, SS.006

Według najlepszej wiedzy technicznej Wykonawcy wymaganie to nie jest związany z funkcjonalnością ochrony AntiSpam. Poczta SMTP trafiająca na serwery producenta (SaaS) i podlegająca skanowaniu, może być szyfrowana (TLS) podczas transfer, co powinno być konfigurowane z poziomu konsoli produktu. Dodatkowo dostęp do GUI produktu w SaaS powiniem być realizowany z wykorzystaniem SSL-a (Https). Prosimy więc o doprecyzowanie tego wymagania lub jego usunięcie.

Odpowiedź 14:
Zamawiający usuwa punkt SS.006 z SOPZ.

Pytanie 15:
Dotyczy „Specyfikacji Istotnych Warunków zamówienia", Wymagania funkcjonalne, SS.011

Prosimy o doprecyzowanie tego wymagania.

Odpowiedź 15:
Zamawiający wymaga, aby rozwiązanie umożliwiało separacje danych względem innych podmiotów wykorzystujących oferowane rozwiązanie. Najprostszym przykładem takiej separacji, który niekoniecznie musi być wykorzystywany w oferowanym rozwiązaniu jest chroot – separacja uprawnień/przywilejów w systemie operacyjnym.

Pytanie 16:
Dotyczy „Specyfikacji Istotnych Warunków zamówienia", Wymagania funkcjonalne, SS.014

Producenci systemów klasy AntiSpam/AntiPhishing precyzują, jakie dane są przetwarzane na terenie EOG oraz w centrach danych na terenie USA a w celu zapewnienia wymogów prawnych RODO/GDPR zawierana jest umowa Powierzenia Przetwarzania Danych z Klientem końcowym. Umowa ta zostaje zawarta z oddziałem europejskim producenta zarejestrowanym w Niemczech. Czy w świetle tego co napisano, wg Zamawiającego to wymaganie będzie spełnione?

Odpowiedź 16:
Zamawiający nie przewiduje powierzenia przetwarzania danych osobowych poza EOG. Zgodnie z SOPZ Wykonawca nie może przetwarzać ani przechowywać danych Zamawiającego poza EOG. Wszystkie wymagane środowiska muszą zostać wdrożone, uruchomione i użytkowane w Centrach Danych znajdujących się wyłącznie na terenie państw EOG.

Jeżeli w ramach realizacji umowy nastąpi powierzenie przetwarzania danych osobowych na terenie EOG, to wówczas zostanie zawarta stosowana umowa powierzenia przetwarzania danych osobowych zgodnie ze wzorem przedstawionym przez Zamawiającego i uwzględniająca stan faktyczny.

Działając na podstawie art. 38 ust. 6 ustawy Prawo zamówień publicznych **Zamawiający zmienia termin składania i otwarcia ofert** z dnia 26.11.2020 r. **na dzień 30.11.2020 r.**

Grzegorz Mroczek

Dyrektor

Działu Bezpieczeństwa