Urząd Ochrony Konkurencji i Konsumentów

Maciej Jabłoński
Dyrektor Generalny Urzędu
Ochrony Konkurencji
i Konsumentów

Warszawa, 18 września 2019 r.

BBA.2.262.29.2019

Wszyscy uczestnicy postępowania

W nawiązaniu do prowadzonego postępowania przetargowego na **Zakup, dostawę i wdrożenie systemu wspomagającego ochronę danych w postaci elektronicznej - DLP,** informuję, że wpłynęły zapytania dotyczące zapisów Specyfikacji Istotnych Warunków Zamówienia o następującej treści:

Pytanie 1
W SOPZ (Załącznik nr 1 do SIWZ) w pkt. 15 zamawiający wymaga aby administrator miał możliwość ustalenia limitu ilości przesyłanych plików w danej jednostce czasu. System, który chcemy zaoferować posiada inne podejście (bardziej precyzyjne) do kontroli przesyłanych plików i w związku z tym chcemy zadać pytanie.
Czy zamawiający dopuszcza możliwość zmiany treści pkt 15 na następujący? Administrator musi mieć możliwość ustalenia limitu ilości przesyłanych plików w danej jednostce czasu lub w oparciu o ich rozmiar, datę modyfikacji, właściwości pliku.

W odpowiedzi na powyższe pytanie informuję, iż Zamawiający pozostaje przy dotychczasowych zapisach SIWZ.

Pytanie 2
Proszę o informację, ile komputerów ma zainstalowane systemy:
- Windows
- MAC

W odpowiedzi na powyższe pytanie informuję, iż ilość komputerów z zainstalowanym systemem Windows wynosi ok. 500 szt., natomiast ilość komputerów z zainstalowanym systemem MAC wynosi 3 szt.

Pytanie 3
Czy zamawiający dopuszcza rozwiązanie, w którym serwer będzie mógł być zainstalowany na systemie Windows Server?

W odpowiedzi na powyższe pytanie informuję, iż Zamawiający pozostaje przy dotychczasowych zapisach SIWZ.

Pytanie 4
Czy zamawiający dopuszcza rozwiązanie wspierające następujące platformy - Windows (7, 8, 10)?

W odpowiedzi na powyższe pytanie informuję, iż Zamawiający pozostaje przy dotychczasowych zapisach SIWZ.

Pytanie 5
Czy zamawiający dopuszcza rozwiązanie, które posiada możliwość generowania raportów z informacjami nt. monitorowanych plików w oparciu o datę i godzinę oraz rozszerzenie i rozmiar?

W odpowiedzi na powyższe pytanie informuję, iż Zamawiający pozostaje przy dotychczasowych zapisach SIWZ.

Pytanie 6
Czy zamawiający dopuszcza rozwiązanie, które będzie informowało administratora poprzez wiadomość e-mail, że została przekroczona wskazana ilość przesyłanych danych?

W odpowiedzi na powyższe pytanie informuję, iż Zamawiający pozostaje przy dotychczasowych zapisach SIWZ.

Pytanie 7
Czy zamawiający dopuszcza rozwiązanie, którego filtry będą działać na poniższym rodzaju oprogramowania:
Microsoft Office (w pełnej wersji),
Libre Office,
Adobe Acrobat.

W odpowiedzi na powyższe pytanie informuję, iż Zamawiający pozostaje przy dotychczasowych zapisach SIWZ.

Pytanie 8
Czy zamawiający dopuszcza możliwość konfiguracji predefiniowanych filtrów za pomocą wyrażeń regularnych, co może wpływać na znacznie mniejszy poziom występowania fałszywych alarmów (FALSE POSITIVE).

W odpowiedzi na powyższe pytanie informuję, iż Zamawiający pozostaje przy dotychczasowych zapisach SIWZ.

Pytanie 9
Czy zamawiający dopuszcza możliwość zablokowania kopiowania pliku z wrażliwymi danymi, a tym samym zapobiegnięciu potencjalnemu wyciekowi danych, zamiast stosowania funkcji file shadow, która może doprowadzić do przepełnienia bazy danych, a w najgorszym przypadku do jej zatrzymania.

W odpowiedzi na powyższe pytanie informuję, iż Zamawiający pozostaje przy dotychczasowych zapisach SIWZ.

Pytanie 10
Czy zamawiający dopuszcza skanowanie stacji w poszukiwaniu plików z konkretnym rozszerzeniem w systemie Windows i wykonie raportu z takiego skanowania?
W odpowiedzi na powyższe pytanie informuję, iż Zamawiający pozostaje przy dotychczasowych zapisach SIWZ.

Pytanie 11
Administrator systemu DLP musi mieć możliwość zdefiniowania minimum następujących akcji dla przenośnych pamięci masowych używanych wewnątrz organizacji:
a. blokuj,
b. zezwól,
c. tylko do odczytu.
Pytanie: Czy zamawiający dopuszcza akcje jak Blokuj/Zezwól/Szyfruj przy kopiowaniu plików na pamięci masowe?

W odpowiedzi na powyższe pytanie informuję, iż Zamawiający pozostaje przy dotychczasowych zapisach SIWZ.

Pytanie 12
Administrator musi mieć możliwość ustalenia limitu ilości przesyłanych plików w danej jednostce czasu.
Pytanie: Czy zamawiający dopuszcza zastosowanie metody Drip DLP – ochrony, monitorowania i agregacji incydentów w jednostce czasu jako mechanizmu zastępczego.

W odpowiedzi na powyższe pytanie informuję, iż Zamawiający pozostaje przy dotychczasowych zapisach SIWZ.

Pytanie 13
Predefiniowane filtry zawartości muszą umożliwiać administratorom zautomatyzowane zarządzanie transferem plików zawierających dane wrażliwe, rozumiane jako co najmniej:
a. numery kart kredytowych,
b. numery IBAN,
c. numery SWIFT,
d. numery PESEL,
e. adresy e-mail,
f. numery telefonów,
g. numery dowodów osobistych,
h. numery paszportów,
i. numery NIP,
j. adresy protokołów internetowych w wersji 4 i 6.
Pytanie: Czy zamawiający dopuszcza przygotowanie tego typu filtrów przez integratora a nie producenta?

W odpowiedzi na powyższe pytanie informuję, iż Zamawiający dopuszcza przygotowanie tego typu filtrów przez integratora a nie producenta.

Pytanie 14
Oferowane rozwiązanie powinno umożliwiać przeprowadzanie klasyfikacji informacji. Mechanizm klasyfikacji oparty na etykietach powinien funkcjonować na zasadzie: - automatycznego nadawania etykiet w zależności od folderu sieciowego w którym dany plik się znajduje lub - ręcznego nadawania etykiet przez użytkowników.
Pytanie: Czy zamawiający oczekuje dostarczenia niniejszej funkcjonalności w ramach tego postępowania czy jedynie oczekuje zapewnienia możliwości technicznych do uruchomienia takiej funkcjonalności w przyszłości po dostarczeniu osobnych licencji w ramach odrębnego postępowania?

W odpowiedzi na powyższe pytanie informuję, iż zgodnie z zapisami SIWZ Zamawiający wymaga dostarczenia niniejszej funkcjonalności w ramach postępowania.

Pytanie 15
Rozwiązanie musi posiadać funkcjonalność aktualizacji, umożliwiającą instalowanie najnowszych dostępnych wersji.
Pytanie: Czy zamawiający dopuszcza dystrybucję oprogramowania klienta za pomocą natywnych rozwiązań Windows?

W odpowiedzi na powyższe pytanie informuję, iż Zamawiający dopuszcza dystrybucję oprogramowania klienta za pomocą natywnych rozwiązań Windows.

Pytanie 16
System DLP musi pozwalać administratorowi na opcjonalne tworzenie polityki aktywnego sprawdzania/skanowania danych znajdujących się na chronionych komputerach Mac i Windows, umożliwiając egzekwowanie wewnętrznej polityki bezpieczeństwa danych firmy oraz zarządzanie ryzykiem stwarzanym przez przypadkowe lub zamierzone wycieki danych. Administrator musi mieć możliwość zarządzania wynikami skanowania, w tym listą wszystkich komputerów, które były skanowane. Rozwiązanie (w zakresie funkcjonalności aktywnego skanowania) musi pozwalać na podjęcie minimum następujących akcji:
a. usuwanie,
b. szyfrowanie lub odszyfrowywanie plików.
Administrator musi mieć możliwość zastosowania żądanej akcji do każdego elementu indywidualnie lub do grupy wybranych elementów jednocześnie.
Pytanie: Czy zamawiający dopuszcza możliwość skanowania zasobów i jednocześnie wymuszenia polityki bezpieczeństwa z różnymi akcjami (blokowanie, monitorowanie, potwierdzenie itp. na różnych kanałach ochrony – poczta, web, kopiowanie na pendrive itd.) zamiast sztywnych po akcji jak usuwanie i/lub szyfrowanie/odszyfrowanie plików.

W odpowiedzi na powyższe pytanie informuję, iż Zamawiający pozostaje przy dotychczasowych zapisach SIWZ.

Pytanie 17
System musi wykrywać zagrożenia związane z utratą, wyciekiem lub kradzieżą danych generowanych przez kontrolowane urządzenia, przenośne pamięci masowe podłączane

przez porty USB. Rozwiązanie musi zapewniać ochronę danych będących w ruchu, filtrować poufne dane organizacji, które mogą być przesyłane poza sieć wewnętrzną poprzez różne punkty wyjścia, takie jak: przeglądarki, emaile, usługi chmurowe, media społecznościowe.
Pytanie: Zgodnie z wiedzą i doświadczeniem Wykonawcy spełnienie wymogu ochrony danych „które mogą być przesyłane poza sieć wewnętrzną" wymaga wdrożenia kompleksowej ochrony. Do tego celu należy zastosować komplementarny moduł sieciowy DLP będący w stanie wychwycić wyciek danych, który zostanie niezauważony przez klienta DLP instalowanego na komputerach PC/Mac. Sieciowy moduł DLP jest w stanie przeprowadzić analizę OCR skanowanych dokumentów, kontrolować treść wysyłanych wiadomości e-mail na poziomie serwera pocztowego i chronić przed utratą danych z niemonitorowanych hostów takich jak komputery gości, urządzenia mobilne, serwery aplikacji, serwery bazodanowe. W związku z powyższym Wykonawca prosi o potwierdzenie, że oferowane rozwiązanie musi chronić przed tego typu zagrożeniami.

W odpowiedzi na powyższe pytanie informuję, iż Zamawiający pozostaje przy dotychczasowych zapisach SIWZ. Zamawiający wymaga rozwiązania umożliwiającego kontrolowanie informacji opuszczających lokalną sieć wymienionymi kanałami. Opis Przedmiotu Zamówienia stanowiący integralną część SIWZ w dalszej treści precyzuje wymagania Zamawiającego.

Powyższe odpowiedzi nie stanowią zmiany treści Specyfikacji Istotnych Warunków Zamówienia.
Dotychczasowy termin składania oraz otwarcia ofert ulega zmianie. Oferty należy składać do dnia **24 września 2019 r. do godz. 11:00. Termin otwarcia ofert 24 września 2019 r. o godz. 11:30**

Dyrektor Generalny Urzędu

Maciej Jabłoński