NACZELNY SĄD ADMINISTRACYJNY
ul. Gabriela Piotra Boduena 3/5
00-011 WARSZAWA

Warszawa, dnia 30 października 2020 r.

Nr sprawy: WAG.262.3.2020

Dotyczy prowadzonego w trybie przetargu nieograniczonego postępowania o udzielenie zamówienia publicznego w sprawie dostawy i wdrożenia systemu zbierania informacji i monitorowania zagrożeń SIEM.

Naczelny Sąd Administracyjny informuje, że w postępowaniu wpłynęły pisma zawierające pytania dotyczące specyfikacji istotnych warunków zamówienia. Działając na podstawie art. 38 ust. 2 ustawy Prawo zamówień publicznych (t.j.: Dz.U. z 2019 r., poz. 1843 ze zm.) – zwanej dalej „ustawą", Zamawiający poniżej przekazuje treść zapytań wraz z wyjaśnieniami:

1. Zamawiający w punkcie 2.2.6 załącznika nr 2 OPZ wymienia następujące przeglądarki:
   - Microsoft Internet Explorer;
   - Microsoft Edge;
   - Mozilla Firefox;
   - Google Chrome.

   W związku informacją producenta (Microsoft) o wygaszaniu wsparcia i rozwoju przeglądarki Microsoft Internet Explorer mamy pytanie.
   Czy Zamawiający uzna za spełniony warunek, gdy interfejs webowy obsługiwany będzie przez standardowe przeglądarki?
   - Microsoft Internet Explorer lub Microsoft Edge;
   - Mozilla Firefox;
   - Google Chrome.

Odpowiedź: Tak, Zamawiający dopuszcza takie rozwiązanie.

2. Zamawiający w punkcie 3.3 załącznika nr 2 OPZ opisuje przykładowe podłączenia źródeł danych. Czy zamawiający oczekuje w ramach dostawy i wdrożenia podłączenia po jednym przykładowym źródle danych z każdego wymienionego typu (syslog, baza danych, plik)?

Odpowiedź: Zamawiający oczekuje w ramach dostawy i wdrożenia podłączenia tylu źródeł danych, ile zostanie uwzględnionionych w sporządzonej w porozumieniu z Zamawiającym koncepcji wdrożenia, o której mowa w wymaganiu 3.1.

3. Czy Zamawiający dopuści rozwiązanie, którego obsługa jest oparta na przeglądarce internetowej i na poziomie operatora systemu nie wymaga instalacji na stacji klienckiej żadnych wtyczek lub środowisk uruchomieniowych, natomiast konfiguracja niektórych elementów, wyłącznie z poziomu konta administratora, wymaga jeszcze zainstalowania wtyczki Adobe Flash? Producent rozwiązania jest obecnie w końcowej fazie przepisywania funkcjonalności z wtyczki Flash na HTML 5 i przewidywana następna wersja wyeliminuje konieczność jej instalacji.

Odpowiedź: Z uwagi na wycofywanie wsparcia dla wtyczki Adobe Flash przez producentów przeglądarek, Zamawiający nie dopuszcza rozwiązania wymagającego zainstalowania wtyczki Adobe Flash dla realizacji jakiejkolwiek z funkcjonalności systemu.

4. Czy Zamawiający dopuszcza rozwiązanie, które jest w stanie parsować pary klucz = wartość, gdzie katalog kluczy jest z góry określony?

Odpowiedź: W pytaniu nie ma wskazania, którego zapisu SIWZ ono dotyczy, a żadne z zapisów w SIWZ nie definiuje wymagania w powyższej kwestii.

5. Dotyczy wymagania 2.2.11. System musi umożliwiać na taką zmianę konfiguracji w przyszłości, aby zapewnić odporność na awarię w zakresie komponentu przechowującego dane - możliwość utworzenia klastra złożonego z co najmniej 2 węzłów oraz zapewni skalowalność poziomą poprzez dodawanie kolejnych węzłów ww. klastra w celu spełnienia wymagań dot. wydajności lub dostępności (zwiększenie liczby kopii danych).

   Proszę o uszczegółowienie tego wymagania – co zamawiający rozumie przez komponent przechowujący dane – czy przestrzeń dyskową / macierze czy dedykowany moduł SIEM zbierania danych wraz z częścią sprzętową lub coś innego ?.

Dodatkowo zamawiający określił, że *„System musi umożliwiać na taką zmianę konfiguracji w przyszłości ,aby zapewnić ..... w celu spełnienia wymagań dot. wydajności i dostępności ....",*

Czy to oznacza, że zaoferowany system nie musi w dniu zero spełniać wymagań aby zapewniać przetwarzanie w trybie ciągłym sumarycznie (jednocześnie)

dla minimum 5 000 zdarzeń (EPS) i dla minimum 3 000 przepływów sieciowych (FPS) na sekundę lub dla minimum 35 GB surowych danych na dobę bo zgodnie z wymaganiem 2.2.11 będzie przez zamawiającego rozbudowane w przyszłości aby spełnić te wymagania ?

Jeżeli tak to jakie są wymagania minimalne na system jakie będą podlegać ocenie przez zamawiającego?

Odpowiedź: Zamawiający wyjaśnia, że w wymaganiu 2.2.11, mając na uwadze także wymaganie 2.2.2, chodzi o możliwość zbudowania klastra modułów przechowywania i zarządzania bazą zebranych informacji działających na odrębnych maszynach wirtualnych.

Wymagania minimalne dotyczące wydajności podane zostały w punkcie 2.3.1 i określają wymagania dla wdrożenia w ramach niniejszego zamówienia. Punkt 2.2.11 określa zaś wymagania dotyczące potencjalnych potrzeb przyszłych, w tym skalowalności poziomej w celu spełnienia potencjalnych przyszłych wymagań wydajnościowych.

6. Dotyczy wymagania 2.3.1. System musi zapewniać przetwarzanie w trybie ciągłym sumarycznie (jednocześnie) dla minimum 5 000 zdarzeń (EPS) i dla minimum 3 000 przepływów sieciowych (FPS) na sekundę lub dla minimum 35 GB surowych danych na dobę. Zdarzenia oraz przepływy sieciowe dla jednego źródła powinny być odbierane i przechowywane przez ten sam moduł zbierający dane.

   Proszę o potwierdzenie, że przez wskazanie przetwarzania w trybie ciągłym sumarycznie (jednocześnie) dla minimum 5 000 zdarzeń (EPS) i dla minimum 3 000 przepływów zamawiający rozumie ruch jaki jest generowany permanentnie w systemie w okresie 24 godzin . Podane przez zamawiającego wartości w relacji z ilością surowych 35 GB/ dobę są znacznie zawyżone w stosunku do standardów i przeliczników ilości GB/dzień do ilości EPS czy FPS i ta rozbieżność jest całkowicie poza jakąkolwiek tolerancją .

   Czy wskazany 5 000 zdarzeń (EPS) i dla minimum 3 000 FSP nie jest przypadkiem peakiem występującym w godzinach szczytu a nie uśrednioną wartości w 24 godzinach ?

Odpowiedź: Wymagania określone w punkcie 2.3.1 nie oznaczają, że w każdej sekundzie będzie występować co najmniej podana liczba zdarzeń EPS i przepływów sieciowych FPS, liczby te należy zatem traktować jako możliwe do wystąpienia wartości szczytowe.

7. Dotyczy wymagania 2.3.2. Oferowane rozwiązanie nie może być ograniczone przez ilość obsługiwanych EPS lub FPS, lub ilość danych per okres czasu. System powinien w miarę dostępności zasobów przetwarzać wszystkie zdarzenia, które do niego wpłyną - pojawienie się tzw. pików nie powinno powodować utraty danych. Ponadto nie może być żadnych programowych blokad dotyczących ilości zdarzeń czy blokowanych funkcjonalności

   Rozumiejąc potrzebę braku jakichkolwiek blokad systemowych ograniczających ilość zbieranych zdarzeń czy funkcjonalności prosimy o potwierdzenie że w tym wymaganiu intencją zamawiającego nie jest ograniczenie konkrecyjności poprzez narzucenie specyficznego sposobu licencjonowania produktów SIEM np. na ilości EPS czy FSP a jedynie zapewnienie że system ten nie będzie ograniczał zbieranych informacji w przypadku wystąpienia peaków, które są typowe w tego typu rozwiązaniach.

   Jeżeli intencja zamawiającego było ograniczenie uczciwej konkurencji poprzez narzucenie sposobu licencjonowania sytemu SIEM , zawężając tym samym ilość wykonawców spełniających takie wymaganie – proszę o usunięcie tego wymagania

Odpowiedź: Zamawiający potwierdza, że w wymaganiu 2.3.2 jego intencją nie jest ani ograniczenie konkurencyjności, ani narzucenie specyficznego sposobu licencjonowania.

8. Dotyczy wymagania 2.7 Wyszukiwanie i przechowywanie danych.

   Proszę o określenie czasu retencji danych jakie mają być przechowywane w systemie w rozbiciu o danych on-line i archiwalne

   Jednocześnie zwracam się z prośbą o przesuniecie terminu składania ofert do 9 listopada 2020.

Odpowiedź: Czas retencji będzie wynikał ze sporządzonej w porozumieniu z Zamawiającym koncepcji wdrożenia, o której mowa w wymaganiu 3.1. Jednocześnie Zamawiający podkreśla, że przedmiotem zamówienia nie jest sprzęt fizyczny, którego przestrzeń dyskowa byłaby determinowana między

innymi czasem retencji danych przechowywanych w systemie.
W odniesieniu do prośby o przesunięcie terminu Zamawiający informuje, że termin składania ofert został przesunięty, co zostało ogłoszone odrębnym pismem.

9. Dotyczy wymagania 2.2.11.

Wg SIWZ System musi umożliwiać na taką zmianę konfiguracji w przyszłości, aby zapewnić odporność na awarię w zakresie komponentu przechowującego dane - możliwość utworzenia klastra złożonego z co najmniej 2 węzłów oraz zapewni skalowalność poziomą poprzez dodawanie kolejnych węzłów ww. klastra w celu spełnienia wymagań dot. wydajności lub dostępności (zwiększenie liczby kopii danych).

Pytania:
1. Proszę o uszczegółowienie tego wymagania – co zamawiający rozumie przez komponent przechowujący dane – czy przestrzeń dyskową / macierze czy dedykowany moduł SIEM zbierania danych wraz z częścią sprzętową lub coś innego ?.

Dodatkowo zamawiający określił, że *„System musi umożliwiać na taką zmianę konfiguracji w przyszłości ,aby zapewnić ..... w celu spełnienia wymagań dot. wydajności i dostępności ....",*
2. Czy to oznacza, że zaoferowany system nie musi w dniu zero spełniać wymagań aby zapewniać przetwarzanie w trybie ciągłym sumarycznie (jednocześnie) dla minimum 5 000 zdarzeń (EPS) i dla minimum 3 000 przepływów sieciowych (FPS) na sekundę lub dla minimum 35 GB surowych danych na dobę bo zgodnie z wymaganiem 2.2.11 będzie przez zamawiającego rozbudowane w przyszłości aby spełnić te wymagania? Jeżeli tak, to jakie są wymagania minimalne systemu, które będą podlegać ocenie przez zamawiającego?

Odpowiedź: Patrz odpowiedź na pytanie nr 5.

10. Dotyczy wymagania 2.3.1.

WG SIWZ: System musi zapewniać przetwarzanie w trybie ciągłym sumarycznie (jednocześnie) dla minimum 5 000 zdarzeń (EPS) i dla minimum 3 000 przepływów sieciowych (FPS) na sekundę lub dla minimum 35 GB surowych danych na dobę. Zdarzenia oraz przepływy sieciowe dla jednego źródła powinny być odbierane i przechowywane przez ten sam moduł zbierający dane.

Pytania:
Proszę o potwierdzenie, że przez wskazanie przetwarzania w trybie ciągłym sumarycznie (jednocześnie) dla minimum 5 000 zdarzeń (EPS) i dla minimum 3 000 przepływów zamawiający rozumie ruch jaki jest generowany permanentnie w systemie w okresie 24 godzin . Podane przez zamawiającego wartości w relacji z ilością surowych 35 GB/ dobę są znacznie zawyżone w stosunku do standardów i przeliczników ilości GB/dzień do ilości EPS czy FPS i ta rozbieżność jest całkowicie poza jakąkolwiek tolerancją .

Czy wskazany 5 000 zdarzeń (EPS) i dla minimum 3 000 FSP nie jest przypadkiem peakiem występującym w godzinach szczytu a nie uśrednioną wartości w 24 godzinach ?

Odpowiedź: Patrz odpowiedź na pytanie nr 6.

11. Dotyczy wymagania 2.3.2.

Wg SIWZ oferowane rozwiązanie nie może być ograniczone przez ilość obsługiwanych EPS lub FPS, lub ilość danych per okres czasu. System powinien w miarę dostępności zasobów przetwarzać wszystkie zdarzenia, które do niego wpłyną - pojawienie się tzw. pików nie powinno powodować utraty danych. Ponadto nie może być żadnych programowych blokad dotyczących ilości zdarzeń czy blokowanych funkcjonalności

Pytanie:
Rozumiejąc potrzebę braku jakichkolwiek blokad systemowych ograniczających ilość zbieranych zdarzeń czy funkcjonalności prosimy o potwierdzenie że w tym wymaganiu intencją zamawiającego nie jest ograniczenie konkrecyjności poprzez narzucenie specyficznego sposobu licencjonowania produktów SIEM np. na ilości EPS czy FSP a jedynie zapewnienie że system ten nie będzie ograniczał zbieranych informacji w przypadku wystąpienia peaków, które są typowe w tego typu rozwiązaniach.

Jeżeli intencja zamawiającego było ograniczenie uczciwej konkurencji poprzez narzucenie sposobu licencjonowania sytemu SIEM , zawężając tym samym ilość wykonawców spełniających takie wymaganie – proszę o usunięcie tego wymagania.

Odpowiedź: Patrz odpowiedź na pytanie nr 7.

12. Dotyczy wymagania 2.7 Wyszukiwanie i przechowywanie danych.
Proszę o określenie czasu retencji danych jakie mają być przechowywane w systemie w rozbiciu o danych on-line i archiwalne.

Odpowiedź: Patrz odpowiedź na pytanie nr 8.

13. SIWZ nie zawiera żadnych wymagań zgodności oferowanego oprogramowania /systemu SIEM z normami międzynarodowymi (np. CC/Common Criteria Evaluation, FIPS 140, Leidos AT&E), jak również z polskimi normami, w tym w szczególności PN -ISO/IEC 27001, i in.

SIWZ nie zawiera również żadnych wymagań pod kątem dokumentów potwierdzających, że oferowany przez dostawcę system SIEM, lub jego część, były przedmiotem badań wykonanych przez niezależne instytucje badawcze specjalizujące się w obszarze badań cyberbezpieczeństwa systemów informatycznych, których wyniki są okresowo publikowane np. raporty Garntera.

Pytanie:

Czy w związku z powyższym można przyjąć, że nie jest warunkiem sine qua non SIWZ, aby system zbierania informacji i monitorowania zagrożeń SIEM, będący przedmiotem postępowania, odpowiadał powołanym wyżej normom i przepisom dotyczącym cvyberbezpieczeństwa? Za takim rozwiązaniem przemawia również fakt, że podstawowym kryterium oceny oferty dostawcy będzie cena, a nie właściwości systemu przewidziane w przepisach ustawy o krajowym systemie cyberbezpieczeństwa i przepisach wykonawczych. ,

Prosimy o wyjaśnienie przedmiotowej kwestii i uszczegółowienie, na podstawie jakich dokumentów Zamawiający dokona technicznej oceny oferowanego systemu? Czy w przypadku dostawcy, który jest jednocześnie producentem własnego oprogramowania SIEM, wystarczająca będzie jego własna deklaracja, że system spełnia wszystkie warunki wymagane przez Zamawiającego, czy też Zamawiający wymagał będzie jednak dodatkowych dokumentów potwierdzających właściwości oferowanego systemu w formie wyników badań zewnętrznych, niezależnych instytucji badawczych w zakresie cyberbezpieczeństwa. Jeśli tak, prosimy o udzielenie odpowiedzi w SIWZ na jakim etapie procedowania postępowania.

Odpowiedź: Zamawiający wyjaśnia, że podstawą dla oceny oferowanego rozwiązania będą oświadczenia Wykonawcy złożone w Ofercie (zał. 1 do SIWZ), dotyczące między innymi spełnienia wszystkich wymogów SIWZ. Dla wyjaśnienia ewentualnych wątpliwości dotyczących spełniania przez oferowane rozwiązanie wymagań postawionych w SIWZ, Zamawiający może zwrócić się do Wykonawcy o udzielenie dodatkowych informacji na każdym etapie realizacji zamówienia, także na etapie wdrożenia.

14. Wniosek o przedłużenie terminu złożenia oferty o 7 dni.

W opinii wnioskodawcy termin na złożenie oferty, wyznaczony przez Zamawiającego jest zbyt krótki. Ogłoszenie postępowania miało miejsce w dniu 23.10.2020. Z uwagi na dwa weekendy do dnia 03.11.2020 oraz przypadający w tym okresie Dzień Wszystkich Zmarłych, a także utrudnienia z powodu sytuacji epidemiologicznej, realnie do przygotowania oferty pozostaje 6 dni.
W związku z powyższym wniosek w tym zakresie jest uzasadniony i konieczny.

Odpowiedź: Zamawiający informuje, że termin składania ofert został przesunięty, co zostało ogłoszone odrębnym pismem.

GŁÓWNY SPECJALISTA
w Wydziale Informatyki
Naczelnego Sądu Administracyjnego
Piotr Siedlikiewicz
Przewodniczący Komisji Przetargowej