Państwowe
Gospodarstwo Wodne
Wody Polskie

Warszawa, 15 listopada 2018 r.

KZGW/27/2018

WYJAŚNIENIA TREŚCI SIWZ

Dotyczy: postępowania na realizację zamówienia „Zakup oprogramowania antywirusowego" nr zamówienia KZGW/27/2018.

Państwowe Gospodarstwo Wodne Wody Polskie, Krajowy Zarząd Gospodarki Wodnej, działając na podstawie art. 38 ust. 2 i 4 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz.U. z 2018 r. poz. 1986), dalej „ustawy", zawiadamia, że w przedmiotowym postępowaniu wpłynęły pytania dotyczące treści Specyfikacji Istotnych Warunków Zamówienia oraz zawiadamia, że dokonuje zmiany treści SIWZ. Poniżej treść pytań wraz z odpowiedziami oraz zmiany treści SIWZ.

PYTANIE NR 13

7. System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania.
Czy alternatywnie może być użyty mechanizm inteligentnego skanowania podczas braku aktywności użytkownika w interakcji z systemem operacyjnym?

ODPOWIEDŹ:

Zamawiający dopuszcza takie rozwiązanie.

ZMIANA:

Działając na podstawie art. 38 ust. 4 ustawy, Zamawiający informuje, iż dokonuje zmiany treści SIWZ w poniższym zakresie:
W rozdziale „Ochrona antywirusowa i antyspyware" pkt 7 otrzymuje brzmienie:
7. System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania. Zamawiający akceptuje dla realizacji wymagania użycie mechanizmu inteligentnego skanowania podczas braku aktywności użytkownika w interakcji z systemem operacyjnym.

PYTANIE NR 14

15. Administrator ma możliwość dodania wykluczenia po tzw. HASH'u zagrożenia, wskazującego bezpośrednio na określoną infekcję a nie konkretny plik.
Czy alternatywą może być globalne wykluczenie pliku z detekcji przez producenta rozwiązania AV?

ODPOWIEDŹ

Zamawiający NIE dopuszcza takiego rozwiązania – dodanie pliku do wykluczeń ma spowodować, iż wykrywane przez program AV zagrożenie będzie ignorowane bez względu na nazwę pliku oraz jego lokalizację.

Prezes
Państwowe Gospodarstwo Wodne Wody Polskie
Krajowy Zarząd Gospodarki Wodnej
ul. Grzybowska 80/82, 00-844 Warszawa
tel.: +48 (22) 37 20 210 | faks: +48 (22) 37 20 295 | e-mail: prezes@wody.gov.pl www.wody.gov.pl

PYTANIE NR 15

22. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).
Czy bezpośrednia ochrona serwerów poczty MS Exchange, Sendmail/Postfix lub od ochrona od strony endpointa oferująca nasłuch na portach POP3, IMAP, SMTP usuwająca SPAM lub malware jest akceptowalna jako zamiennik dla konektorów?

ODPOWIEDŹ

Zamawiający dopuszcza rozwiązanie posiadające mechanizm antyspam i antywirus występujący lokalnie na stacji roboczej wykorzystujący skanowanie protokołów.

ZMIANA:

Działając na podstawie art. 38 ust. 4 ustawy, Zamawiający informuje, iż dokonuje zmiany treści SIWZ w poniższym zakresie:
W rozdziale „Ochrona antywirusowa i antyspyware" pkt 22 otrzymuje brzmienie:
22. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego). Dopuszcza się rozwiązanie posiadające mechanizm antyspam i antywirus występujący lokalnie na stacji roboczej wykorzystujący skanowanie protokołów.

PYTANIE NR 16

31. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
Czy bezpośrednia ochrona serwerów poczty MS Exchange, Sendmail/Postfix usuwająca SPAM lub malware jest akceptowalna jako zamiennik dla filtrowania POP3S i IMAPS?

ODPOWIEDŹ

Zamawiający NIE dopuszcza rozwiązania nieposiadającego możliwości skanowania poczty dla klienta pocztowego na stacji roboczej wykorzystującego protokoły POP3S oraz IMAPS.

PYTANIE NR 17

33. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta.
Czy zgłoszenie podejrzanej witryny do producenta rozwiązania AV ze specjalnie przygotowanej witryny www jest akceptowalne?

ODPOWIEDŹ

Zamawiający dopuszcza takie rozwiązanie.

ZMIANA:

Działając na podstawie art. 38 ust. 4 ustawy, Zamawiający informuje, iż dokonuje zmiany treści SIWZ w poniższym zakresie:
W rozdziale „Ochrona antywirusowa i antyspyware" pkt 33 otrzymuje brzmienie:
33. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta. Akceptowana będzie również możliwość zgłoszenia podejrzanej witryny ze specjalnie przygotowanej do tego celu strony producenta programu AV.

PYTANIE NR 18

39. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz

elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
Wskazanie na ESET – prośba o wykreślenie z SIWZ – https://help.eset.com/ees/6/pl-PL/index.html?idh_config_threat_sense.htm

ODPOWIEDŹ

Według wiedzy posiadanej przez zamawiającego powyższe wymaganie nie wskazuje tylko i wyłącznie oprogramowania firmy ESET. Produkty kilku producentów programów AV mają np. dwa silniki antywirusowe.

PYTANIE NR 19

40. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń mają być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
Czy możliwość wysyłania nowych zagrożeń za pośrednictwem Administratora systemu AV jest akceptowalna?

ODPOWIEDŹ

Zamawiający nie akceptuje takiego rozwiązania. Dopuszczalne jest tylko rozwiązanie gdzie nowe zagrożenia będą wysyłane automatycznie – bez ingerencji administratora lub użytkownika.

PYTANIE NR 20

53. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM, urządzeń przenośnych oraz urządzeń dowolnego typu.
Czy blokowanie wskazanych urządzeń może być realizowane przez kontrolę aplikacji (sterowników) je obsługujących?

ODPOWIEDŹ

Zamawiający NIE dopuszcza rozwiązania nie posiadającego mechanizmu blokowania poszczególnych urządzeń konkretnego rodzaju. Blokowanie wszystkich urządzeń danego typu nie jest akceptowane.

PYTANIE NR 21

61. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
a) tryb automatyczny z regułami gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
b) tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
c) tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
d) tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach.
Czy tryb uczenia się jest stanowczo wymagany? Czy możliwe jest zastosowanie wyłącznie trybów a, b, c pod nadzorem Administratora systemu AV/Firewall?

ODPOWIEDŹ

Zamawiający przez moduł HIPS rozumie mechanizm ochrony systemu operacyjnego Windows (nie ochronę w postaci firewall) poprzez kontrolę plików systemowych, wpisów do rejestru, itp. Dopuszczalne jest rozwiązanie bez trybu uczenia się.

ZMIANA:

Działając na podstawie art. 38 ust. 4 ustawy, Zamawiający informuje, iż dokonuje zmiany treści SIWZ w poniższym zakresie:
W rozdziale „Ochrona antywirusowa i antyspyware" pkt 61 otrzymuje brzmienie:
61. Moduł HIPS musi posiadać możliwość pracy w jednym z czterech trybów:
a) tryb automatyczny z regułami gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
b) tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
c) tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
d) tryb inteligentny – w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.

PYTANIE NR 22

62. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
Czy wykluczając elementy rejestru systemowego tworzenie reguł w oparciu o aplikacje, pliki, porty, wyzwalacze może być wystarczające dla modułu HIPS?

ODPOWIEDŹ

Zamawiający informuje, że dokonuje zmiany SIWZ w zakresie powyższego pytania.

ZMIANA:

Działając na podstawie art. 38 ust. 4 ustawy, Zamawiający informuje, iż dokonuje zmiany treści SIWZ w poniższym zakresie:
W rozdziale „Ochrona antywirusowa i antyspyware" pkt 62 otrzymuje brzmienie:
62. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe.

PYTANIE NR 23

66. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
Czy dopuszczalny jest system raportowania, który nie posiada informacji o usługach systemowych, procesach i połączeniach, lecz który oferuje rozległe informacje o sieci, adresacji IP, producencie karty sieciowej, BIOS?

ODPOWIEDŹ

NIE jest akceptowane rozwiązanie nieposiadające wymienionych funkcjonalności.

PYTANIE NR 24

67. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.

Czy system wykrywania słabości/luk w systemie operacyjnym/aplikacjach może być zamiennikiem dla logów informacyjnych?

ODPOWIEDŹ

Zamawiający informuje, że dokonuje zmiany SIWZ w zakresie powyższego pytania.

ZMIANA:

Działając na podstawie art. 38 ust. 4 ustawy, Zamawiający informuje, iż dokonuje zmiany treści SIWZ w poniższym zakresie:
W rozdziale „Ochrona antywirusowa i antyspyware" pkt 67 otrzymuje brzmienie:
67. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa. Akceptowalne jest rozwiązanie, które posiada system wykrywania słabości/luk w systemie operacyjnym/aplikacjach.

PYTANIE NR 25

73. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http.
Czy repozytorium aktualizacji może być oferowane przez bezpieczniejszy protokół niż http?

ODPOWIEDŹ

Zamawiający informuje, że dokonuje zmiany SIWZ w zakresie powyższego pytania. Akceptowane protokoły to http lub HTTPS.

ZMIANA:

Działając na podstawie art. 38 ust. 4 ustawy, Zamawiający informuje, iż dokonuje zmiany treści SIWZ w poniższym zakresie:
W rozdziale „Ochrona antywirusowa i antyspyware" pkt 73 otrzymuje brzmienie:
73. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http, https.

PYTANIE NR 26

76. Program ma być w pełni zgodny z technologią CISCO Network Access Control.
Czy dostęp do sieci może być określany zamiennie przez software'owy moduł Firewall instalowalny wraz z programem AV?

ODPOWIEDŹ

Zamawiający akceptuje możliwości określenia warunków po spełnieniu których dana stacja będzie mogła uzyskać dostęp do sieci.

ZMIANA:

Działając na podstawie art. 38 ust. 4 ustawy, Zamawiający informuje, iż dokonuje zmiany treści SIWZ w poniższym zakresie:
W rozdziale „Ochrona antywirusowa i antyspyware" pkt 76 otrzymuje brzmienie:
76. Program ma być w pełni zgodny z technologią CISCO Network Access Control. Dopuszczalna jest realizacja tej funkcjonalności w oparciu o software'owy moduł Firewall instalowalny wraz z programem AV.

PYTANIE NR 27

77. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym.

78. W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji.
79. Użytkownik ma mieć możliwość skonfigurowania programu tak aby automatycznie program włączał powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie.
Czy możliwość zamykania interakcji software AV-user w wygodnych dla siebie interwałach czasowych może być akceptowalną alternatywą dla niezakłócania trybu pełnoekranowego?

ODPOWIEDŹ

Praca użytkownika nie może być zakłócana również poza wyznaczonymi interwałami czasu. Zamawiający wymaga aby mechanizm ten działał automatycznie. Zapisy pozostają bez zmian.

PYTANIE NR 28

82. Program musi posiadać możliwość utworzenia z poziomu interfejsu aplikacji dziennika diagnostycznego na potrzeby pomocy technicznej.
Czy dziennik diagnostyczny może być akceptowalny w pliku .txt lub .log?

ODPOWIEDŹ

Zamawiający dopuszcza takie rozwiązanie pod warunkiem, że plik będzie zawierał wszystkie wymagane dane potrzebne do rozwiązania problemu.

ZMIANA:

Działając na podstawie art. 38 ust. 4 ustawy, Zamawiający informuje, iż dokonuje zmiany treści SIWZ w poniższym zakresie:
W rozdziale „Ochrona antywirusowa i antyspyware" pkt 82 otrzymuje brzmienie:
82. Program musi posiadać możliwość utworzenia z poziomu interfejsu aplikacji dziennika diagnostycznego na potrzeby pomocy technicznej. Dziennik diagnostyczny może być w postaci .txt lub .log pod warunkiem, że będzie zawierał wszystkie niezbędne informacje niezbędne do rozwiązania problemu.

PYTANIE NR 29

85. W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: ochrona antywirusowa i antyspyware, kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, Obsługa technologii Microsoft NAP.
Czy do dostępu do sieci może służyć software'owy moduł Firewall instalowalny wraz z programem AV nie opierający się/współpracujący z Microsoft NAP?

ODPOWIEDŹ

Funkcjonalność dotyczy możliwości dezaktywacji funkcji produktu na etapie instalacji, nie zastąpienia ich innymi.

PYTANIE NR 30

93. Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.
Czy możliwe jest zastosowanie zmian dla programu wyłącznie takich, które nie naruszają/osłabiają zasad bezpieczeństwa jak aktualizacja baz sygnatur lub aktualizacji plików programu AV?

ODPOWIEDŹ

Zamawiający nie dopuszcza takiego rozwiązania. Produkt powinien posiadać możliwość wyłączenia np. ochrony systemu plików w czasie rzeczywistym za pomocą skryptu aby zautomatyzować np. proces wykonywania backupu przez aplikację zewnętrzną.

PYTANIE NR 31

2. Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
Wskazanie na ESET – prośba o wykreślenie z SIWZ – https://help.eset.com/eav/11/pl-PL/idh_config_emon_clients.html.

ODPOWIEDŹ

Według wiedzy posiadanej przez zamawiającego powyższe wymaganie nie wskazuje tylko i wyłącznie oprogramowania firmy ESET. Program antywirusowy powinien posiadać mechanizm weryfikacji tego co już jest w skrzynce użytkownika w momencie jego instalacji.

PYTANIE NR 32

4. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
Wskazanie na ESET – prośba o wykreślenie z SIWZ – https://www.eset.pl/resources/documents/HE-v9/eset_ess_9_userguide_plk.pdf.

ODPOWIEDŹ

Według wiedzy posiadanej przez zamawiającego powyższe wymaganie nie wskazuje tylko i wyłącznie oprogramowania firmy ESET. Oferowany produkt powinien posiadać możliwość dodawania kontaktów do białej listy przez użytkownika.

PYTANIE NR 33

8. Program ma umożliwiać współpracę w swojej domyślnej konfiguracji z folderem „Wiadomości śmieci" obecnym w programie Microsoft Outlook.
Czy dopuszczalne jest rozwiązanie dające możliwość wskazania dowolnego folderu dla niechcianych wiadomości, lecz nie domyślnie?

ODPOWIEDŹ

Zamawiający dopuszcza takie rozwiązanie pod warunkiem, że dana funkcja może zostać skonfigurowana globalnie z poziomu konsoli centralnego zarządzania.

ZMIANA:

Działając na podstawie art. 38 ust. 4 ustawy, Zamawiający informuje, iż dokonuje zmiany treści SIWZ w poniższym zakresie:
W rozdziale „Ochrona przed spamem" pkt 8 otrzymuje brzmienie:
8. Program ma umożliwiać współpracę w swojej domyślnej konfiguracji z folderem „Wiadomości śmieci" obecnym w programie Microsoft Outlook. Dopuszczalna jest możliwość wskazania dowolnego folderu pod warunkiem, że może to zostać skonfigurowane globalnie z poziomu konsoli centralnego zarządzania.

PYTANIE NR 34

9. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną zmieni jej właściwość jako „nieprzeczytana" oraz w momencie zaklasyfikowania wiadomości jako spam na automatyczne ustawienie jej właściwości jako „przeczytana".

Czy dopuszczalne jest aby system antyspamowy programu AV realizował opisaną funkcję z pominięciem pierwszej wiadomości e-mail zakwalifikowanej lub cofniętej jako SPAM?

ODPOWIEDŹ

Zamawiający nie dopuszcza takiego sposobu realizowania opisanej funkcji.

PYTANIE NR 35

10. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.
Czy możliwe jest zastosowanie funkcji, gdzie czasem wyłączenia modułu antyspamowego zarządza Administrator systemu AV?

ODPOWIEDŹ

Zamawiający dopuszcza ograniczenie wyłączenia modułu dla administratora.

ZMIANA:

Działając na podstawie art. 38 ust. 4 ustawy, Zamawiający informuje, iż dokonuje zmiany treści SIWZ w poniższym zakresie:
W rozdziale „Ochrona przed spamem" pkt 10 otrzymuje brzmienie:
10. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera przez Administratora systemu AV.

PYTANIE NR 36

1. Zapora osobista ma pracować jednym z 4 trybów:
a) tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące, jednocześnie umożliwia utworzenie dodatkowych reguł przez administratora
b) tryb interaktywny – program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo),
c) tryb oparty na regułach – użytkownik/administrator musi ręcznie zdefiniować reguły określające jaki ruch jest blokowany a jaki przepuszczany,
d) tryb uczenia się – umożliwia zdefiniowanie przez administratora określonego okresu czasu w którym oprogramowanie samo tworzy odpowiednie reguły zapory analizując aktywność sieciową danej stacji.
Czy tryb uczenia się jest stanowczo wymagany? Czy możliwe jest zastosowanie wyłącznie trybów a, b, c pod nadzorem Administratora systemu AV/Firewall?

ODPOWIEDŹ

Zamawiający dopuszcza produkt AV bez trybu uczenia się.

ZMIANA:

Działając na podstawie art. 38 ust. 4 ustawy, Zamawiający informuje, iż dokonuje zmiany treści SIWZ w poniższym zakresie:
W rozdziale „Zapora osobista (personal firewall)" pkt 1 otrzymuje brzmienie:
1. Zapora osobista ma pracować jednym z 3 trybów:
a) tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące, jednocześnie umożliwia utworzenie dodatkowych reguł przez administratora
b) tryb interaktywny – program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo),
c) tryb oparty na regułach – użytkownik/administrator musi ręcznie zdefiniować reguły określające jaki ruch jest blokowany a jaki przepuszczany,

PYTANIE NR 37

10. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
Wskazanie na ESET – prośba o wykreślenie z SIWZ – https://support.eset.pl/kb2906/?locale=pl_PL&viewlocale=pl_PL

ODPOWIEDŹ

Według wiedzy posiadanej przez zamawiającego powyższe wymaganie nie wskazuje tylko i wyłącznie oprogramowania firmy ESET. Inne produkty AV posiadają również takie mechanizmy pod nazwą IPS/IDS/Ochrona przed atakami.

PYTANIE NR 38

5. Aplikacja musi posiadać możliwość filtrowania url w oparciu o co najmniej 140 kategorii i pod kategorii.
Czy dopuszczalne jest zastosowanie modułu filtrowania stron o mniejszej liczbie kategorii niż 140, lecz wyposażonego w inteligentne algorytmy mogące blokować witryny upublicznione nawet kilka minut wcześniej w sieci www i niewymagającego aktualizacji url?

ODPOWIEDŹ

Tak sformułowane pytanie nie pozwala Zamawiającemu na udzielenie odpowiedzi ponieważ nie określa dokładnie proponowanej przez Wykonawcę równoważnej funkcjonalności w tym między innymi nie określa konkretnie liczby dostępnych kategorii stron WWW w proponowanym programie AV co jest jednym z wymogów zawartych w OPZ Zamawiającego.

PYTANIE NR 39

15. Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi.
wskazanie na ESET – prośba o wykreślenie z SIWZ – https://www.eset.com/int/business/server-antivirus/shared-local-cache/

ODPOWIEDŹ

Według wiedzy posiadanej przez zamawiającego powyższe wymaganie nie wskazuje tylko i wyłącznie oprogramowania firmy ESET. Produkty AV innych niż ESET producentów posiadają mechanizmy skanowania o takiej funkcjonalności dostępne np. jako skaner sieciowy.

PYTANIE NR 40

1. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2003, 2008, 2012 oraz systemach Linux.
Czy dopuszczalne jest zastosowanie wyłącznie konsoli Administracyjnej lub Web Administracyjnej w systemie Linux?

ODPOWIEDŹ

Zamawiający informuje, iż nie dopuszcza takiego rozwiązania. Zamawiający musi posiadać możliwość wykorzystania własnej infrastruktury bazującej na systemie Windows.

PYTANIE NR 41

2. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance).
Czy dopuszczalne są inne formaty gotowych maszyn wirtualnych i formatów niż OVA?

ODPOWIEDŹ

Zamawiający dopuszcza takie rozwiązanie pod warunkiem, że format jest wspierany przez hypervisorów: Hyper-V, Vmware, VirtualBox, Citrix.

ZMIANA:

Działając na podstawie art. 38 ust. 4 ustawy, Zamawiający informuje, iż dokonuje zmiany treści SIWZ w poniższym zakresie:
W rozdziale „Administracja zdalna" pkt 2 otrzymuje brzmienie:
2. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance). Dopuszczalne są inne formaty gotowych maszyn wirtualnych i formatów niż OVA jeżeli „format" jest wspierany przez hypervisorów: Hyper-V, Vmware, VirtualBox, Citrix.

PYTANIE NR 42

3. Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL.
Czy możliwe jest oparcie w działaniu serwera administracji AV wyłącznie o MS SQL?

ODPOWIEDŹ

Zamawiający nie dopuszcza takiego rozwiązania. Produkt musi wspierać oba typy baz danych.

PYTANIE NR 43

26. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
Czy możliwe jest zastosowanie agenta wbudowanego w aplikację AV?

ODPOWIEDŹ

Zamawiający dopuszcza takie rozwiązanie pod warunkiem, że instalacja oprogramowania może odbyć się zdalnie i nie powoduje konfliktu z obecnie wykorzystywanym oprogramowaniem AV. Musi istnieć możliwości migracji między produktami AV.

ZMIANA:

Działając na podstawie art. 38 ust. 4 ustawy, Zamawiający informuje, iż dokonuje zmiany treści SIWZ w poniższym zakresie:
W rozdziale „Administracja zdalna" pkt 26 otrzymuje brzmienie:
26. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta. Dopuszczalne jest zastosowanie agenta wbudowanego w aplikację AV jeżeli instalacja oprogramowania może odbyć się zdalnie i nie powoduje konfliktu z obecnie wykorzystywanym oprogramowaniem AV. Musi istnieć możliwości migracji między produktami AV.

PYTANIE NR 44

27. Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego.
Czy dopuszczalne jest zastosowanie agenta jednocześnie propagującego się z systemem AV?

ODPOWIEDŹ

Zamawiający dopuszcza takie rozwiązanie pod warunkiem, że instalacja oprogramowania może odbyć się zdalnie i nie powoduje konfliktu z obecnie wykorzystywanym oprogramowaniem AV. Musi istnieć możliwości migracji między produktami AV.

ZMIANA:

Działając na podstawie art. 38 ust. 4 ustawy, Zamawiający informuje, iż dokonuje zmiany treści SIWZ w poniższym zakresie:
W rozdziale „Administracja zdalna" pkt 27 otrzymuje brzmienie:
27. Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego. Dopuszcza się zastosowanie agenta jednocześnie propagującego się z systemem AV jeżeli instalacja oprogramowania może odbyć się zdalnie i nie powoduje konfliktu z obecnie wykorzystywanym oprogramowaniem AV. Musi istnieć możliwości migracji między produktami AV.

PYTANIE NR 45

29. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania.
Czy dopuszczalne są możliwości deinstalacji/instalacji oprogramowania firm trzecich wyłącznie tych, które były propagowane przez Agenta/AV?

ODPOWIEDŹ

Zamawiający nie dopuszcza takiego rozwiązania. Zamawiający wymaga aby Agent umożliwiał deinstalację produktów zainstalowanych również przed instalacją oprogramowania AV pochodzących od innych producentów.

PYTANIE NR 46

34. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play.
Czy dopuszczalne są inne zasoby www niż Google Play?

ODPOWIEDŹ

Zamawiający nie dopuszcza takiego rozwiązania. Taka funkcja wymaga włączenia w systemie Android opcji „Nieznanych" źródeł co jest nieakceptowane.

PYTANIE NR 47

39. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej.
Wskazanie na ESET – prośba o wykreślenie z SIWZ – https://www.eset.pl/biznes/ochrona-dostepu/ESET-Secure-Authentication.

ODPOWIEDŹ

Według wiedzy posiadanej przez zamawiającego powyższe wymaganie nie wskazuje tylko i wyłącznie oprogramowania firmy ESET. Wielu producentów oprogramowania AV posiada mechanizm autoryzacji 2FA do konsoli zarządzającej.

PYTANIE NR 48

54. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu.
Czy dopuszczalne jest stosowanie zewnętrznych skryptów dostarczanych przez producenta rozwiązań AV?

ODPOWIEDŹ

Zamawiający dopuszcza takie rozwiązanie pod warunkiem, że proces odbywa się zdalnie i automatycznie podczas instalacji produktu AV.

ZMIANA:

Działając na podstawie art. 38 ust. 4 ustawy, Zamawiający informuje, iż dokonuje zmiany treści SIWZ w poniższym zakresie:
W rozdziale „Administracja zdalna" pkt 54 otrzymuje brzmienie:
54. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu. Dopuszczalne jest stosowanie zewnętrznych skryptów dostarczanych przez producenta rozwiązań AV pod warunkiem, że proces odbywa się zdalnie i automatycznie podczas instalacji produktu AV.

PYTANIE NR 49

91. Konfiguracja zestawów uprawnień musi umożliwiać przypisanie praw tylko do odczytu, odczytu i użycia, oraz prawo do zapisania zmian w ramach danego zadania lub polityki w konsoli **ERA**.
Wskazanie na ESET – prośba o wykreślenie z SIWZ – Wskazanie nazwy własnej Eset Remote Administrator. ESET.

ODPOWIEDŹ

Zamawiający informuje, iż dokonał zmian SIWZ w zakresie wniosku Wykonawcy w treści wyjaśnień udzielonych w dniu 24 października 2018 r.

PYTANIE NR 50

93. Administrator musi mieć możliwość podłączenia do stacji roboczej z użyciem protokołu RDP bezpośrednio z poziomu konsoli **ERA.**
wskazanie na ESET – prośba o wykreślenie z SIWZ – Wskazanie nazwy własnej Eset Remote Administrator. ESET

ODPOWIEDŹ

Zamawiający informuje, iż dokonał zmian SIWZ w zakresie wniosku Wykonawcy w treści wyjaśnień udzielonych w dniu 24 października 2018 r.

PYTANIE NR 51

94. Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar.
wskazanie na ESET – prośba o wykreślenie z SIWZ – https://www.eset.pl/resources/documents/leaflets/ESET-Remote-Administrator-PL.pdf

ODPOWIEDŹ

Według wiedzy posiadanej przez zamawiającego powyższe wymaganie nie wskazuje tylko i wyłącznie oprogramowania firmy ESET. Oprogramowanie AV innych producentów integruje się z systemami SIEM a takim jest IBM qRadar.

Działając na podstawie art. 38 ust. 4 ustawy, Zamawiający informuje, iż dokonuje zmiany treści SIWZ w poniższym zakresie:

1. Punkt 17.2 SIWZ otrzymuje brzmienie:

   „*Wykonawca zobowiązany jest – niezwłocznie po wyborze oferty, bez odrębnego wezwania – przedłożyć Zamawiającemu szczegółowy opis oferowanych urządzeń z uwzględnieniem wymogów Zamawiającego określonych w załączniku do SIWZ Nr 1 „Opis przedmiotu zamówienia". Opis oferowanych urządzeń musi zawierać co najmniej informacje wskazane w treści Opisu przedmiotu zamówienia stanowiącego załączniki Nr 1 do SIWZ.*".

2. W punkcie 17 Formalności konieczne do zawarcia umowy dodaje się punkt 17.3 w brzmieniu:

„*Brak dopełnienia przez Wykonawcę formalności, o których mowa w pkt. 17.2 SIWZ lub podanie w treści Opisu oferowanych urządzeń informacji niezgodnych z wymogami Opisów przedmiotu zamówienia, równoznaczne będzie z uznaniem przez Zamawiającego, że Wykonawca uchyla się od zawarcia umowy (odmówił podpisania umowy w sprawie zamówienia publicznego na warunkach określonych w ofercie lub że zawarcie umowy w sprawie zamówienia publicznego stało się niemożliwe z przyczyn leżących po stronie Wykonawcy).*".

3. W Załączniku Nr 4 do SIWZ „Wzór umowy":

   W § 7 wprowadza się ust. 6 o następującej treści:

   „Mając na uwadze fakt, że środki finansowe przeznaczone na realizację przedmiotu Umowy zabezpieczone zostały na rok 2018, Zamawiającemu przysługuje prawo do odstąpienia od Umowy w całości lub w części niewykonanej, bez dodatkowego wezwania, ze skutkiem na 31 grudnia 2018 r., jeżeli Wykonawca nie dostarczy przedmiotu Umowy do 31 grudnia 2018 r. (umowne prawo odstąpienia określone w art. 492 Kodeksu cywilnego). Zamawiający złoży Wykonawcy oświadczenie o odstąpieniu od Umowy w terminie nie dłuższym niż 5 dni roboczych od dnia ziszczenia się przesłanki określonej w zdaniu poprzedzającym.".

Powyższe zmiany stanowią integralną część SIWZ. Pozostałe zapisy SIWZ pozostają bez zmian.

Zatwierdził
Dyrektor
Departamentu Organizacyjnego
Państwowego Gospodarstwa Wodnego
Wody Polskie
Marcin Białek