Centrum Informatyki Statystycznej

Znak: CIS-WAZ.271.2.2026 Warszawa, dnia 09.06.2026 r.

Do zainteresowanych wykonawców

Dotyczy: Postępowania prowadzonego w trybie przetargu nieograniczonego **CIS-WAZ.271.2.2026 pn. Dostawa systemu Web Proxy oraz Sandbox do zapewnienia bezpiecznego dostępu do sieci Internet wraz z wdrożeniem.**

Centrum Informatyki Statystycznej działając na podstawie art. 135 ust. 2 oraz art. 137 ust 1 i 2 ustawy Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320 ze zm.) dalej „ustawa Pzp", informuje , iż wpłynęły pytania do treści Specyfikacji Warunku Zamówienia (dalej SWZ) i udziela następujących wyjaśnień:

Pytanie 17
Dotyczy Załącznika nr.1 do SWZ - Opis Przedmiotu Zamówienia w sekcji „Moduł Sandbox" punkt 7.

Pytanie: W związku z wymogiem zapewnienia zmiany czasu oczekiwania na wykonanie się detonacji, wnosimy o określenie maksymalnego czasu oczekiwania na detonację możliwego do skonfigurowania np.: w przedziale 5 – 10 minut.

Uzasadnienie: Możliwość ustawienia dłuższego czasu zapewnia wychwycenie próbek, które przez dłuższy czas symulują nieszkodliwą działalność, co wiąże się to z ilością detonowanych próbek. Jednakże możliwość ustawienia szerokiego zakresu oczekiwania na zakończenie detonacji pozwala na dobranie warunków odpowiadających bezpieczeństwu organizacji

Odpowiedź
Zamawiający nie określa wymogu maksymalnego czasu dynamicznej analizy / detonacji plików.

Pytanie 18

Dotyczy punktów 1, 5, 7, 8, 13, 15, 17, 20, 21, 22, 25 w korelacji do punku 26 dla „**Moduł Sandbox".**

We wskazanych punktach tj. 1, 5, 7, 8, 13, 15, 17, 20, 21, 22, 25 zawarte pojęcia dotyczą „dynamicznej" analizy lub jawnie określonej „detonacji"

W punkcie 25 Zamawiający zawarł wymóg zaoferowanie rozwiązania zapewniającego 25 jednocześnie uruchomionych maszyn co można przyjmować jako równocześnie wykonywanych detonacji.

Zaś w punkcie 26 Zamawiający zawarł enigmatycznie określoną „analizę" w ilości 32 000 plików na godzinę.

Przyjmując analizę jako detonacja: 25 / (32000(próbek per h) /60(minut) / 60(sekund)) = 2,8215 sec średniego czasu na detonację każdej próbki z 32000 plików per godzina.

Wyliczony średni czas detonacji dla tak określonej liczby próbek nie jest możliwy do wykonania przez 25 równolegle pracujących maszyn. Jeśli przyjąć tak krótki czas na detonację, opisane rozwiązanie będzie się charakteryzowało przepuszczaniem mallware. Zawarty w punkcie 7 wymóg umożliwienia sterowanie czasem wykonania detonacji jest więc iluzorycznym wymogiem przy tak znacznym woluminie plików

Wnosimy o zdefiniowanie pojęcia „analizy plików" zawartej w punkcie 26.

Czy wartość 32000 plików na godzinę dotyczy detonacji plików w systemie Sandbox czy wykonania skanowania AV.

Zatem czy funkcja „analizy" plików w w/w punkcie 26 dla „Moduł Sandbox" dotyczy funkcjonalności Sandboxingu, czyli detonacji plików, czy też jest to zdublowany „Moduł analizy treści" z dodaną funkcją 25 maszyn do detonacji, ale bez określenia ilości detonacji w kwancie czasu?

W przypadku zadeklarowania „Modułu sandbox" jako faktyczna funkcjonalność sandbox wnosimy o określenie faktycznej maksymalnej ilości detonacji per kwant czasu.

Centrum Informatyki Statystycznej

Aleja Niepodległości 208, 00-925 Warszawa
tel. 22 608 31 44
cissek@stat.gov.pl
cis.stat.gov.pl

Odpowiedź
Zamawiający **przywraca punktu 27 w sekcji „Moduł Sandbox" o brzmieniu**:
„Każde z urządzeń musi mieć wydajność umożliwiającą przeprowadzenia analizy minimum 8000 próbek malware w ciągu 24h."

Zamawiający **wykreśla w sekcji „Moduł Sandbox" punkt 26 o treści:**
„Możliwość analizy minimum 32000 plików na godzinę."

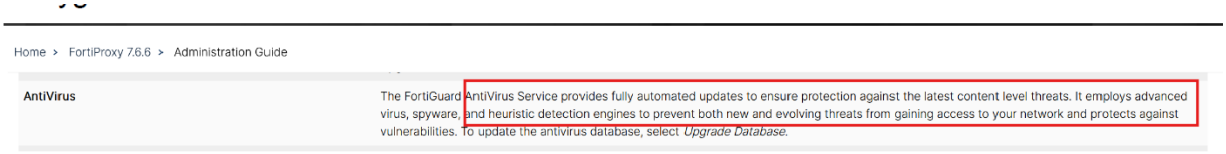
Pytanie 19
W ocenie Wykonawcy kwestionowane wymagania naruszają **art. 16 oraz art. 99 ust. 1 i 4 ustawy Pzp**, ponieważ opisują przedmiot zamówienia w sposób mogący utrudniać uczciwą konkurencję – odpowiadają one wyłącznie rozwiązaniom jednego producenta (**Fortinet: FortiProxy / FortiSandbox**), prowadzi do uprzywilejowania i wyeliminowania pozostałych wykonawców i produktów.
Wniosek nr 1 – sekcja „Moduł analizy treści", pkt 1 lit. b
Kwestionowany zapis: „*minimum 2 silniki AV działające jednocześnie, pochodzące od różnych producentów. Zamawiający dopuszcza rozwiązanie polegające na stosowaniu jednego silnika sygnaturowego oraz silnika do analizy bezsygnaturowej/behawioralnej w ramach jednego zunifikowanego procesu kontroli ruchu***,"**
Uzasadnienie:
Zapis jest wewnętrznie sprzeczny: zdanie pierwsze wymaga zapewnienia dwóch silników antywirusowych (bez określenia wymaganych parametrów i trybów ich pracy), natomiast zdanie drugie wymaga zapewnienia jednego silnika. Taka redakcja uniemożliwia wykonawcom jednoznaczne ustalenie rzeczywistych oczekiwań Zamawiającego (art. 99 ust. 1 Pzp).

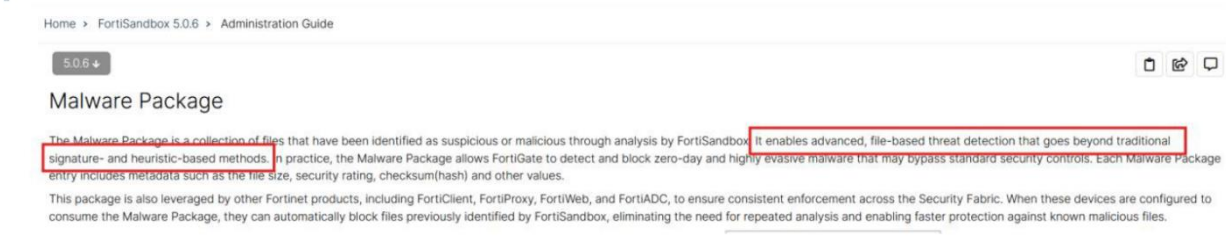
Użyte w zdaniu drugim określenie „bezsygnaturowa i/lub behawioralna" jest błędne merytorycznie. Podczas statycznej analizy zawartości pliku nie zachodzi analiza behawioralna (oparta na obserwacji zachowania), lecz analiza heurystyczna. Funkcje heurystyczne stanowią natomiast standardowy element każdego współczesnego silnika antywirusowego, co potwierdza powszechnie dostępna literatura branżowa

Źródła: Poniżej w kolejności alfabetycznej linki do artykułów opisujących działanie antywirusów z kopia tekstu dotyczącego heurystyki:

https://avlab.pl/jak-dzialaja-antywirusy/ -> „*Następne takie kopie tego wirusa są inne niż oryginał. Utrudnia to jego wykrycie, ponieważ program antywirusowy szuka poprzez sygnatury konkretnego fragmentu kodu, który wirus polimorficzny potrafi zmienić / zamaskować / zaszyfrować. I właśnie dlatego opracowano techniki heurystycznego wykrywania wirusów.*"
https://kapitanhack.pl/co-to-jest-av/ -> „*Skaner, który bada pliki na żądanie lub co jakiś czas. Przeszukuje zawartość dysku i może typować pliki zawierające podejrzany kod na podstawie heurystyki*."
https://niebezpiecznik.pl/post/sekrety-firm-antywirusowych/ -> „*Sygnatury NIE! Heurystyka TAK! Nie należy jednak wpadać w panikę. Mało która firma antywirusowa korzysta dziś jedynie z bazy sygnaturek do wykrywania złośliwego oprogramowania. Drugą linią obrony są algorytmy heurystyczne, próbujące oceniać jak wiele złego może wyrządzić skanowany plik*."
https://sekurak.pl/w-jaki-sposob-dzialaja-programy-antywirusowe/ -> „*Najważniejszą częścią każdego współczesnego programu antywirusowego (oprócz tzw. silnika) jest baza sygnatur wirusów. Sygnatury wirusów to pewne (zazwyczaj bardzo zwięzłe) informacje, które pozwalają na w miarę jednoznaczne zidentyfikowanie danego typu lub nawet całej rodziny wirusów. Najpopularniejsze obecnie trzy typy sygnatur, to:*
sygnatury powstałe z wykorzystaniem funkcji skrótu, sygnatury (wzorce) bajtowe, sygnatury heurystyczne."
Wymaganie jednego silnika wykonującego analizę „poza tradycyjnymi metodami opartymi na sygnaturach" odpowiada opisowi rozwiązania FortiProxy / FortiSandbox zawartemu w dokumentacji producenta, co wskazuje na produkt konkretnego wykonawcy (art. 99 ust. 4 Pzp) Źródło: https://docs.fortinet.com/document/fortiproxy/7.6.6/administration-guide/191172/fortiguard oraz

Poniżej obraz strony dokumentacją ze stron produktu Fotinet Proxy na temat AV opisującej metody skanowania wykraczające poza tradycyjne metody oparte na sygnaturach





d) Niezależnie od powyższego, wymóg jednego silnika obniża poziom bezpieczeństwa w stosunku do równoczesnego wymogu dwóch silników, zwiększając ryzyko przepuszczenia złośliwego oprogramowania.

Żądanie Wykonawcy: wnosimy o usunięcie zdania drugiego w pkt 1 lit. b oraz o doprecyzowanie, że obydwa wymagane silniki antywirusowe powinny realizować zarówno skanowanie sygnaturowe, jak i heurystyczne.

Podstawa prawna: art. 16, art. 99 ust. 1 oraz art. 99 ust. 4 ustawy Pzp**.**

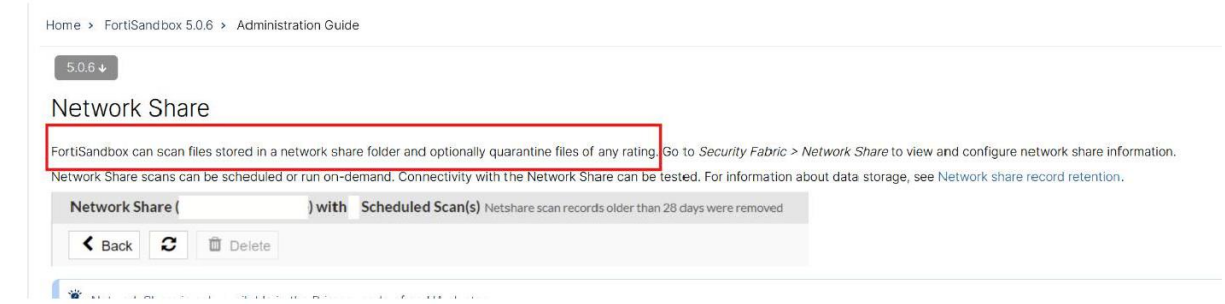
Odpowiedź

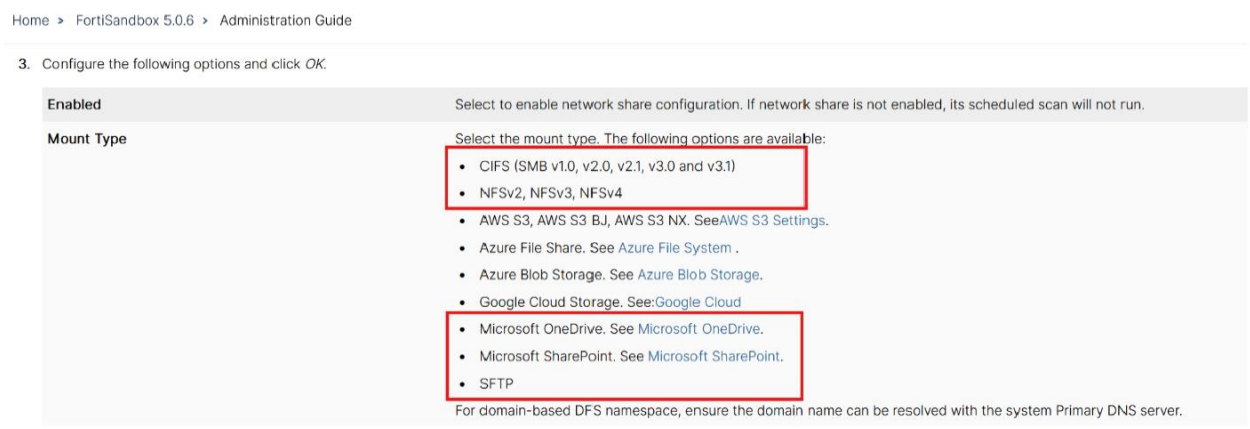
Zamawiający modyfikuje **pkt 1 lit. b** w **sekcja „Moduł analizy treści”**:
Było
„minimum 2 silniki AV działające jednocześnie, pochodzące od różnych producentów. Zamawiający dopuszcza rozwiązanie polegające na stosowaniu jednego silnika sygnaturowego oraz silnika do analizy bezsygnaturowej/behawioralnej w ramach jednego zunifikowanego procesu kontroli ruchu,”

Otrzymuje brzmienie pkt 1 lit. b w **sekcja „Moduł analizy treści”:**:

„Rozwiązanie musi wykorzystywać co najmniej dwa mechanizmy detekcji zagrożeń działające jednocześnie. Zamawiający wymaga zastosowania co najmniej dwóch silników antymalware pochodzących od różnych producentów lub alternatywnie dopuszcza zastosowanie jednego silnika sygnaturowego oraz mechanizmu analizy bezsygnaturowej (np. analiza behawioralna, ML/AI), działających w ramach zunifikowanego procesu kontroli ruchu i plików.”

Pytanie 20
Wniosek nr 2 – sekcja „Moduł Sandbox”, pkt 30
Kwestionowany zapis: „*System musi umożliwiać skanowanie plików na zasobach: SMB, NFS, SFTP, Microsoft OneDrive oraz Sharepoint z możliwością kwarantanny podejrzanych plików.”*
Uzasadnienie:
e) Funkcję odczytu (analizy) udostępnionych zasobów dyskowych realizuje na rynku wyłącznie jedno rozwiązanie sandbox – FortiSandbox. Treść pkt 30 jest tożsama (poza wskazaniem listy protokołów i zasobów) z opisem zawartym w dokumentacji producenta tego rozwiązania.
Źródło:
https://docs.fortinet.com/document/fortisandbox/5.0.6/administration-guide/755608/network-share





Tak sformułowany wymóg ogranicza konkurencję poprzez opisanie cech spełnianych wyłącznie przez produkt jednego wykonawcy (art. 99 ust. 4 Pzp).

Żądanie Wykonawcy: wnosimy o usunięcie pkt 30 w sekcji „Moduł Sandbox".
Podstawa prawna: art. 16 oraz art. 99 ust. 4 ustawy Pzp.

Wniosek końcowy

Mając na uwadze powyższe, wnoszę o dokonanie wskazanych zmian treści SWZ (OPZ) oraz – w razie potrzeby – o odpowiednie przedłużenie terminu składania ofert, tak aby umożliwić przygotowanie ofert przez szersze grono wykonawców. Dokonanie wnioskowanych zmian usunie ryzyko naruszenia zasady uczciwej konkurencji i równego traktowania wykonawców.

Odpowiedź
Zamawiający modyfikuje zapis dla punktu 30 w sekcja „Moduł Sandbox"
Było:
„System musi umożliwiać skanowanie plików na zasobach: SMB, NFS, SFTP, Microsoft OneDrive oraz Sharepoint z możliwością kwarantanny podejrzanych plików"

Otrzymuje brzmienie pkt 30 w sekcja „Moduł Sandbox":

„System musi umożliwiać skanowanie plików pobieranych z zasobów: SFTP oraz dysków chmurowych w tym: Microsoft OneDrive i Sharepoint z możliwością kwarantanny podejrzanych plików."

/-/ Marcin Piekarek
Dyrektor
Centrum Informatyki Statystycznej