UNIWERSYTET IM. ADAMA MICKIEWICZA W POZNANIU
Prorektor ds. cyfryzacji i współpracy z gospodarką

Poznań, dnia 03/03/2022r.

POWIADOMIENIE O ZMIANACH SWZ

Dotyczy: specyfikacji warunków zamówienia w przetargu nieograniczonym na **dostawę klastra urządzeń klasy UTM (urządzenia do transmisji danych cyfrowych) oraz 2 serwerów wraz z oprogramowaniem – 2 części,** nr postępowania ZP/5493/D/21.

Szanowni Państwo,

Zgodnie z art. 135 ust. 1 i 2 oraz art. 137 ust. 1,2 i 6 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. 2021 poz. 1129 ze zm.) uprzejmie informuję, że wpłynęło zapytanie dotyczące specyfikacji warunków zamówienia. Poniżej Zamawiający przedstawia zadane pytania i dotyczące ich odpowiedzi oraz modyfikacje SWZ.

Pytania do części I – dostawa klastra urządzeń klasy UTM (urządzenia do transmisji danych cyfrowych)

PYTANIE 1

Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks - i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. **2.1.7** określa wymaganie

„Moduł zarządzania musi posiadać wbudowane mechanizmy wersjonowania polityki bezpieczeństwa. Nowa wersja polityki bezpieczeństwa powinna być tworzona każdorazowo w momencie opublikowania zmian przez administratora systemu. System wersjonowania musi zapewniać administratorom możliwość wglądu w wybraną wersję polityki bezpieczeństwa a także opcję cofnięcia konfiguracji do wybranej wersji."

Funkcja wersjonowania samej polityki bezpieczeństwa w formie opisanej przez Zamawiającego jest dostępna tylko w urządzeniach Checkpoint, nie jest ona dostępna w urządzeniach produkcji Fortinet oraz produkcji Palo Alto Networks. Zwykle bowiem wersjonowana jest cała zapisywana konfiguracja, a nie wersje polityki.

Zamawiający opisuje zatem w wymaganiach konkretny sposób realizacji zadania – unikalny dla jednego producenta – nie dopuszczając by zaoferowane zostały urządzenia innych producentów.

Opis przedmiotu zamówienia przygotowany jest więc w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

ul. H. Wieniawskiego 1, Collegium Minus, 61-712 Poznań
NIP 777 00 06 350, REGON 000001293
tel. +48 61 829 40 58, fax +48 61 829 44 44
michal.banaszak@amu.edu.pl

W związku z zaistniałą sytuacją wnosimy o zmianę wymagania **2.1.7** w taki sposób, iż przyjmie ono np. treść.
„Moduł zarządzania musi posiadać wbudowane mechanizmy wersjonowania polityki bezpieczeństwa. Nowa wersja polityki bezpieczeństwa lub całościowa konfiguracja urządzenia powinna być tworzona każdorazowo w momencie zapisania zmian przez administratora systemu. System wersjonowania musi zapewniać administratorom możliwość wglądu w wybraną wersję polityki bezpieczeństwa lub w całościową konfigurację urządzenia, a także opcję cofnięcia konfiguracji do wybranej wersji polityki lub całościowej konfiguracji urządzenia."

Jeżeli Zamawiający nie wyrazi zgody na zmianę to wnosimy o wykreślenie wymagania 2.1.7. w całości jako wskazujące - wprost bądź łącznie z pozostałymi - na konkretne rozwiązanie.

Chcemy zaznaczyć, że oba zaproponowane przez nas rozwiązania pozwolą na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji - jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów

bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania wskazane przez Zamawiającego, podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający odrzuci możliwości zmian lub wykreślenie punktu 2.1.7 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają wymaganie 2.1.7 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający zmieni treść wymagania 2.1.7 na następujący:
„Moduł zarządzania musi posiadać wbudowane mechanizmy wersjonowania polityki bezpieczeństwa. Nowa wersja polityki bezpieczeństwa lub całościowa konfiguracja urządzenia powinna być tworzona każdorazowo w momencie zapisania zmian przez administratora systemu. System wersjonowania musi zapewniać administratorom możliwość wglądu w wybraną wersję polityki bezpieczeństwa lub w całościową konfigurację urządzenia, a także opcję cofnięcia konfiguracji do wybranej wersji polityki lub całościowej konfiguracji urządzenia."

PYTANIE 2
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. 2.1.18 określa wymaganie
„Moduł zarządzania musi pozwalać na wyszukiwanie wymaganych informacji (logów, incydentów bezpieczeństwa) zapisanych w wewnętrznej bazie danych bez konieczności definiowania wartości dla poszczególnych atrybutów (tzw.freetext search)"

Funkcja wyszukiwania informacji w formie opisanej przez Zamawiającego jest dostępna tylko w rozwiązaniu Checkpoint, nie jest ona dostępna w urządzeniach produkcji Fortinet oraz produkcji Palo Alto Networks.
Zwykle bowiem w przypadku wyszukiwania konieczne jest wskazanie, którego pola/kolumny ma dotyczyć zapytanie.

Zamawiający opisuje zatem w wymaganiach konkretną funkcję – unikalną dla jednego producenta – nie dopuszczając by zaoferowane zostały urządzenia innych producentów.

Opis przedmiotu zamówienia przygotowany jest więc w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

Biorąc pod uwagę powyższe wnosimy o wykreślenie wymagania 2.1.18. w całości jako wskazujące - wprost bądź łącznie z pozostałymi - na konkretne rozwiązanie.

Chcemy zaznaczyć, że celem tej zmiany jest umożliwienie złożenia oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji - jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania wskazane przez Zamawiającego, podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający podtrzyma wymaganie punktu 2.1.18 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają wymaganie 2.1.18 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający zmieni treść wymagania 2.1.18 na następujący:
„Moduł zarządzania musi pozwalać na wyszukiwanie wymaganych informacji (logów, incydentów bezpieczeństwa) zapisanych w wewnętrznej bazie danych"

PYTANIE 3
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. 2.1.25 określa wymaganie
„Moduł zarządzania musi posiadać możliwość generowania raportów w formacie PDF oraz Microsoft Excel. Musi istnieć możliwość przesyłania wygenerowanych raportów poprzez pocztę elektroniczną do wskazanych odbiorców„

Wg naszej najlepszej wiedzy ani Fortinet ani Palo Alto Networks nie posiadają wprost możliwości generowania raportów w formacie Microsoft Excel. Podani producenci pozwalają za to na wygenerowanie raportów w formacie CSV lub XML, które mogą być otwarte przy użyciu narzędzia Microsoft Excel.

Zamawiający opisuje zatem w wymaganiach konkretną funkcję – unikalną dla jednego producenta – nie dopuszczając by zaoferowane zostały urządzenia innych producentów.

Opis przedmiotu zamówienia przygotowany jest więc w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

W związku z zaistniałą sytuacją wnosimy o zmianę wymagania 2.1.25. w taki sposób, iż przyjmie ono np. treść.

„Moduł zarządzania musi posiadać możliwość generowania raportów w formacie PDF oraz CSV lub XML. Musi istnieć możliwość przesyłania wygenerowanych raportów poprzez pocztę elektroniczną do wskazanych odbiorców"

Jeżeli Zamawiający nie wyrazi zgody na zmianę to wnosimy o wykreślenie wymagania 2.1.25. w całości jako wskazujące - wprost bądź łącznie z pozostałymi - na konkretne rozwiązanie.

Chcemy zaznaczyć, że oba zaproponowane przez nas rozwiązania pozwolą na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji - jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania wskazane przez Zamawiającego, podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający odrzuci możliwości zmian lub wykreślenie punktu 2.1.25 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają wymaganie 2.1.25 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający zmieni treść wymagania 2.1.25 na następującą:
„Moduł zarządzania musi posiadać możliwość generowania raportów w formacie PDF. Moduł zarządzania musi posiadać możliwość generowania raportów w formacie Microsoft Excel lub CSV lub XML. Musi istnieć możliwość przesyłania wygenerowanych raportów poprzez pocztę elektroniczną do wskazanych odbiorców.„

PYTANIE 4
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. 2.1.12 określa wymaganie
„Moduł zarządzania musi dostarczać mechanizmy pozwalające na monitorowanie i prezentowanie za pomocą graficznej konsoli parametrów sprzętowych zarządzanych urządzeń UTM takich jak: średnie

obciążenie procesora, zajętość pamięci operacyjnej, zajętość przestrzeni dyskowej, wersję oprogramowania zapory sieciowej, nazwę i wersję zainstalowanej polityki bezpieczeństwa, listę uruchomionych modułów bezpieczeństwa)„

Funkcje zarządzania realizowane w formie opisanej przez Zamawiającego są dostępne tylko w rozwiązaniu Checkpoint, i nie są jednocześnie dostępne w urządzeniach produkcji Fortinet oraz produkcji Palo Alto Networks.
Wynika to m.in. z cech własnościowych i sposobu realizacji firewalla oraz powiązanego systemu zarządzania przez firmę Checkpoint. W ten sposób Zamawiający odrzuca możliwość pozyskania rozwiązania innego producenta jeżeli jego podejście do uzyskania tego samego celu jest inne niż wskazane przez Zamawiającego – przykładowo nie wersjonuje on polityki bezpieczeństwa, a całą konfigurację urządzenia.

Opis przedmiotu zamówienia przygotowany jest więc w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

W związku z zaistniałą sytuacją wnosimy o wykreślenie wymagania 2.1.12. w całości jako wskazujące - wprost bądź łącznie z pozostałymi - na konkretne rozwiązanie.

Pozwoli to na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji - jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania wskazane przez Zamawiającego, podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający podtrzyma wymaganie punktu 2.1.12 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają wymaganie 2.1.12 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający nie usunie wymagania 2.1.12.

PYTANIE 5
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. 2.1.12 określa wymaganie
„Moduł zarządzania musi dostarczać mechanizmy pozwalające na monitorowanie i prezentowanie za pomocą graficznej konsoli parametrów sprzętowych zarządzanych urządzeń UTM takich jak: średnie obciążenie procesora, zajętość pamięci operacyjnej, zajętość przestrzeni dyskowej, wersję oprogramowania zapory sieciowej, nazwę i wersję zainstalowanej polityki bezpieczeństwa, listę uruchomionych modułów bezpieczeństwa)"

Funkcje zarządzania realizowane w formie opisanej przez Zamawiającego są dostępne tylko w rozwiązaniu Checkpoint, i nie są jednocześnie dostępne w urządzeniach produkcji Fortinet oraz produkcji Palo Alto Networks.
Wynika to m.in. z cech własnościowych i sposobu realizacji firewalla oraz powiązanego systemu zarządzania przez firmę Checkpoint. W ten sposób Zamawiający odrzuca możliwość pozyskania rozwiązania innego producenta jeżeli

jego podejście do uzyskania tego samego celu jest inne niż wskazane przez Zamawiającego – przykładowo nie wersjonuje on polityki bezpieczeństwa, a całą konfigurację urządzenia.

Opis przedmiotu zamówienia przygotowany jest więc w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

W związku z zaistniałą sytuacją wnosimy o wykreślenie wymagania 2.1.12. w całości jako wskazujące - wprost bądź łącznie z pozostałymi - na konkretne rozwiązanie.

Pozwoli to na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji - jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania wskazane przez Zamawiającego, podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający podtrzyma wymaganie punktu 2.1.12 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają wymaganie 2.1.12 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający nie usunie wymagania 2.1.12.

PYTANIE 6
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. 2.1.15 określa wymaganie
„Moduł zarządzania musi realizować funkcję serwera logów w ramach której musi umożliwiać agregację i indeksowanie logów ze wszystkich zarządzanych zapór sieciowych. W ramach funkcji serwera logów muszą istnieć wbudowane mechanizmy ochrony przestrzeni dyskowej przed przepełnieniem Mechanizm powinien umożliwiać wykonywanie różnych akcji systemu w zależności od poziomu zajętości dysku. Możliwe akcje to minimum wysyłanie alertów do administratorów oraz automatyczne usuwanie najstarszych plików logów„

Funkcje zarządzania realizowane w formie opisanej przez Zamawiającego są dostępne tylko w rozwiązaniu Checkpoint, i nie są jednocześnie dostępne w urządzeniach produkcji Fortinet oraz produkcji Palo Alto Networks.

Zamawiający opisuje zatem w wymaganiach konkretną funkcję – unikalną dla jednego producenta – nie dopuszczając by zaoferowane zostały urządzenia innych producentów.

Opis przedmiotu zamówienia przygotowany jest więc w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

W związku z zaistniałą sytuacją wnosimy o zmianę wymagania 2.1.15 w taki sposób, iż przyjmie ono np. treść.
„Moduł zarządzania musi realizować funkcję serwera logów w ramach której musi umożliwiać agregację i indeksowanie logów ze wszystkich zarządzanych zapór sieciowych"

Pozwoli to na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jeżeli Zamawiający nie wyrazi zgody na zmianę to wnosimy o wykreślenie wymagania 2.1.15. w całości jako wskazujące - wprost bądź łącznie z pozostałymi - na konkretne rozwiązanie.

Chcemy zaznaczyć, że oba zaproponowane przez nas rozwiązania pozwolą na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji - jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania wskazane przez Zamawiającego, podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający odrzuci możliwości zmian lub wykreślenie punktu 2.1.15 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają wymaganie 2.1.15 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający nie zmieni we wnioskowany sposób i nie usunie wymagania 2.1.15.

PYTANIE 7
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. 3.1.2 określa wymaganie
„Mechanizm klastrowania musi natywnie umożliwiać połączenie do min. 5 urządzeń w ramach pojedynczego klastra w każdym z trybów pracy (Active-Standby lub Active-Active). Mechanizm

klastrowania musi umożliwiać skalowanie klastra do większej liczby urządzeń (minimum 10) bez potrzeby wykorzystania urządzeń niepochodzących od producenta systemu bezpieczeństwa"

Funkcja klastrowania urządzeń w zakresie wskazanym przez Zamawiającego jest dostępna tylko w urządzeniach Checkpoint, nie jest ona dostępna w urządzeniach produkcji Fortinet oraz produkcji Palo Alto Networks.

Wynika to z tego, że różni producenci używają różnej terminologii przy opisywaniu klastrowania firewalli i realizacji wysokiej dostępności. Klastry niezawodnościowe zazwyczaj działają w modelu 1+1 i mogą działać w trybie Active-Standby lub Active-Active).

Klastry wydajnościowe (lub geoklastry) pozwalają na grupowanie kilku urządzeń, które działają w modelu Active-Active. Wielu producentów umożliwia klastrowanie do 6 urządzeń.

Zabieg w kierunku zwiększenia tej liczby do 10 jest typowy dla rozwiązań firmy Checkpoint, gdzie możliwe uzyskanie większej liczby urządzeń, przy czym eliminuje to konkurentów.

Warto też zaznaczyć, iż sześciokrotne zwiększenie przepustowości jest bardzo dużym zwiększeniem względem obecnych wymagań określonych w specyfikacji.

Zamawiający wskazuje w p. 3.11.3 swoje potrzeby i określa je następująco:

„6 Gbit/s dla kontroli firewall z włączoną funkcją IPS oraz kontrolą aplikacji oraz nie mniej niż 3.5 Gbit/s dla kontroli zawartości (moduły firewall, kontrola aplikacji, katagoryzacja URL, moduł antywirusowy, IPS, ochrona Zero-Day)"

Jeżeli Zamawiający przewiduje, iż w ciągu widocznej przyszłości kilku lat osiągnie przepustowość 60Gbps (klaster 10 urządzeń) wówczas zasadnym wydaje się zwiększenie wymagań wydajnościowych dla nabywanych firewalli, już w chwili obecnej - celem lepszego doboru rozwiązania dla Zamawiającego.

Nie zmienia to faktu, iż opis przedmiotu zamówienia przygotowany jest w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

W związku z zaistniałą sytuacją wnosimy o zmianę wymagania 3.1.2. na treść.
„Mechanizm klastra niezawodnościowego musi natywnie umożliwiać połączenie dwóch urządzeń w ramach pojedynczego klastra w każdym z trybów pracy (Active-Standby lub Active-Active).

Mechanizm klastrowania wydajnościowego musi natywnie umożliwiać połączenie do min. 5 urządzeń w ramach pojedynczego klastra przy czym wszystkie urządzenia w klastrze aktywnie obsługują ruch."

Jeżeli Zamawiający nie wyrazi zgody na zmianę to wnosimy o wykreślenie wymagania 3.1.2. w całości jako wskazujące - wprost bądź łącznie z pozostałymi - na konkretne rozwiązanie.

Chcemy zaznaczyć, że oba zaproponowane przez nas rozwiązania pozwolą na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji - jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania wskazane przez Zamawiającego, podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający odrzuci możliwości zmian lub wykreślenie punktu 3.1.2 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych

producentów, które spełniają wymaganie 3.1.2 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający zmieni treść wymagania 3.1.2 na następującą:
„Mechanizm klastra niezawodnościowego musi natywnie umożliwiać połączenie dwóch urządzeń w ramach pojedynczego klastra w każdym z trybów pracy (Active-Standby lub Active-Active). Mechanizm klastrowania wydajnościowego musi natywnie umożliwiać połączenie do min. 5 urządzeń w ramach pojedynczego klastra przy czym wszystkie urządzenia w klastrze aktywnie obsługują ruch. Mechanizm klastrowania wydajnościowego musi umożliwiać skalowanie do min. 60 Gbit/s."

PYTANIE 8
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks - i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. 3.1.6 określa wymaganie
„System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q z obsługą do 1024 znaczników VLAN w trybie Gateway oraz 4096 znaczników w trybie wirtualnych systemów„

Funkcja obsługi znaczników 802.1q w urządzeniach firewall w zakresie wskazanym przez Zamawiającego może być i najprawdopodobniej jest dostępna tylko w urządzeniach Checkpoint, nie jest ona dostępna w urządzeniach produkcji Fortinet oraz produkcji Palo Alto Networks.

Symptomatycznym jest tu przede wszystkim wskazanie trybów pracy urządzenia – tryb Gateway oraz tryb wirtualnych systemów. Terminologia jak i oznaczenia ilościowe nie pozostawiają wątpliwości, iż opisany został tutaj

produkt firmy Checkpoint. Żaden inny dopuszczony w p.1.12 producent według naszej wiedzy nie opisuje trybów pracy urządzenia w ten sposób i nie różnicuje również liczby obsługiwanych znaczników od trybu pracy urządzeń.

Z innej strony - należy wprost wskazać, iż urządzenia sieciowe obsługują realnie 4094 znaczniki, zatem wymaganie 4096 jest niemożliwe do spełnienia przez jakiegokolwiek producenta (być może za wyjątkiem Checkpoint). Z technicznego punktu widzenia wg. standardu 802.1q znacznik kodowany jest na 12 bitach co dopuszcza wartości od

0 do 4095, ale skrajne wartości 0 i 4095 są wg. standardu zarezerwowane i z tego właśnie względu nie mogą być realnie wykorzystane przez urządzenie sieciowe.

Nie zmienia to faktu, że opis przedmiotu zamówienia przygotowany jest więc w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

W związku z zaistniałą sytuacją wnosimy o zmianę wymagania 3.1.6 w taki sposób, iż przyjmie ono np. treść.

„System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q z obsługą do 4094 znaczników VLAN."
Jeżeli Zamawiający nie wyrazi zgody na zmianę to wnosimy o wykreślenie wymagania 3.1.6. w całości jako wskazujące - wprost bądź łącznie z pozostałymi - na konkretne rozwiązanie.

Chcemy zaznaczyć, że oba zaproponowane przez nas rozwiązania pozwolą na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji - jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania wskazane przez Zamawiającego, podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający odrzuci możliwości zmian lub wykreślenie punktu 3.1.6 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają wymaganie 3.1.6 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający zmieni treść wymagania 3.1.6 na następującą:
„System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q z obsługą do min. 4094 znaczników VLAN

PYTANIE 9
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. 3.2.3 określa wymaganie
„Moduł firewall musi posiadać możliwość zaraportowania ilości „trafień" wybranej reguły polityki bezpieczeństwa do serwera zarządzania. Musi istnieć możliwość prezentowania liczby trafień dla reguł w wybranych okresach czasu, minimum w okresie 1 dnia, 7 dni oraz miesiąca."

Funkcja raportowania ilości trafień wybranej reguły polityki bezpieczeństwa jest powszechnie dostępna w większości wiodących rozwiązań. Jednakże wymaganie dotyczące prezentowania liczby trafień w określonych okresach czasu powoduje wskazanie konkretnego rozwiązania technicznego – firmy Checkpoint – i powoduje ograniczenie konkurencji. Jednocześnie warto zauważyć, że Zamawiający wymaga, aby trafienia były tylko dla tych trzech stałych czasokresów, a nie wymaga zliczania trafień dla zadanego okresu czasu np. 10 dni, 45 dni etc. jako okresów, które mogłyby być bardziej przydatne przy analizach. W rozwiązaniach Checkpoint okres 1 dnia, 7 dni i 1 miesiąca są niejako „standardowe" i nie są konfigurowalne.

Zamawiający opisuje zatem w wymaganiach konkretną funkcję – unikalną dla jednego producenta – nie dopuszczając by zaoferowane zostały urządzenia innych producentów.

Opis przedmiotu zamówienia przygotowany jest więc w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

W związku z zaistniałą sytuacją wnosimy o zmianę wymagania 3.2.3 w taki sposób, iż przyjmie ono np. treść.
„Moduł firewall musi posiadać możliwość zaraportowania ilości „trafień" wybranej reguły polityki bezpieczeństwa do serwera zarządzania."

Jeżeli Zamawiający nie wyrazi zgody na zmianę to wnosimy o wykreślenie wymagania 3.2.3. w całości jako wskazujące - wprost bądź łącznie z pozostałymi - na konkretne rozwiązanie.

Chcemy zaznaczyć, że oba zaproponowane przez nas rozwiązania pozwolą na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji - jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania wskazane przez Zamawiającego, podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający odrzuci możliwości zmian lub wykreślenie punktu 3.2.3 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów,

które spełniają wymaganie 2.1.15 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający nie zmieni we wnioskowany sposób i nie usunie wymagania 3.2.3.

PYTANIE 10
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.
Jednocześnie Zamawiający w p. 3.3.10 określa wymaganie
„Moduł IPS musi posiadać mechanizm automatycznej aktywacji sygnatur minimum w oparciu o następujący zestaw parametrów: poziom zagrożenia, wpływ na wydajność urządzenia, dokładność identyfikacji zagrożenia."

Funkcja automatycznej aktywacji sygnatur jest cechą wskazującą na rozwiązania firmy Checkpoint. Co prawda na rynku podobną cechę mają urządzenia firmy Cisco, jednakże Zamawiający określając całościowe wymagania nie pozwala na złożenie oferty opartej o te właśnie rozwiązania.

Istotnym jest, iż cecha ta jest właściwa dla rozwiązań, których architektura sprzętowo programowa, zakłada że moduł IPS może mieć problem z utrzymaniem deklarowanej wydajności przy założeniu, że wszystkie sygnatury są aktywne.

Jest to zatem przykład, którym Zamawiający nie skupia się na uzyskaniu funkcjonalności jaką jest sprawność i skuteczność systemu IPS, a wymusza konkretną cechę wynikającą z architektury rozwiązania wskazanego w opisie przedmiotu zamówienia.

Precyzując wymaganie 3.3.10 Zamawiający nie dopuszcza urządzeń firewall skonstruowanych w taki sposób, że pracują one na pełnej bazie dostępnych sygnatur IPS bez spadku wydajności, gwarantując jednocześnie najwyższy dostępny poziom bezpieczeństwa. Nie ma wówczas potrzeby balansowania pomiędzy poziomem bezpieczeństwa a wydajnością, a tym samym mechanizm automatycznej aktywacji sygnatur jak został opisany w p. 3.3.10. jest niepotrzebny i bezużyteczny.

Nie ulega więc wątpliwości, że Zamawiający opisuje w wymaganiach konkretną funkcję – unikalną dla jednego producenta – nie dopuszczając by zaoferowane zostały urządzenia innych producentów.

Opis przedmiotu zamówienia przygotowany jest więc w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

W związku z zaistniałą sytuacją wnosimy o wykreślenie wymagania 3.3.10. w całości jako wskazujące - wprost bądź łącznie z pozostałymi - na konkretne rozwiązanie.

Pozwoli to na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji - jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania wskazane przez Zamawiającego, podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający podtrzyma wymaganie punktu 3.3.10 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają wymaganie 3.3.10 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający usunie wymaganie 3.3.10.

PYTANIE 11
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. 3.3.17 określa wymaganie
„Moduł IPS musi posiadać programowy mechanizm pozwalający na wyłączenia ochrony IPS w przypadku wysokiego obciążenia procesora lub pamięci operacyjnej zapory sieciowej. Wartości aktywujące mechanizm muszą być konfigurowalne przez administratora systemu."
Funkcja wyłączenia ochrony IPS w przypadku dużego obciążenia procesora lub pamięci operacyjnej jest cechą wskazującą na rozwiązania firmy Checkpoint.

Jest ona poniekąd powiązana z cechą opisaną przez Zamawiającego w p.3.3.10, gdyż jest to kolejna cecha właściwa dla rozwiązań, których architektura sprzętowo-programowa zakłada, że moduł IPS może mieć problem z utrzymaniem deklarowanej wydajności przy założeniu, że wszystkie sygnatury są aktywne.

Jednocześnie dezaktywacja ochrony IPS – jako jednego z 2-3 najistotniejszych silników bezpieczeństwa opisanych przez Zamawiającego w wymaganiach – każe wręcz zastanowić się czy urządzenie będzie w takiej sytuacji mogło spełnić wymagania przed nim stawiane – w szczególności w zakresie jakości oferowanej ochrony.

Funkcja opisana przez Zamawiającego jest bowiem właściwa dla dedykowanych systemów IPS i jest określana jako fail-open – w przypadku dedykowanych sond IPS ma sens, jednakże w przypadku firewalli następnej generacji przejście w ten tryb pracy należałoby wręcz określić jako słabość rozwiązania, a nie jako cechę, która jest wartością dla Zamawiającego.

Podobnie jak w przypadku wymagania .3.3.10 jest to zatem przykład, którym Zamawiający nie skupia się na uzyskaniu funkcjonalności jaką jest sprawność i skuteczność systemu IPS, a wymusza konkretną cechę wynikającą z architektury rozwiązania wskazanego w opisie – rozwiązanie firmy Checkpoint. Podobnie też jak w przypadku p 3.3.10 Zamawiający nie dopuszcza urządzeń firewall skonstruowanych w taki sposób, że pracują one na pełnej bazie dostępnych sygnatur IPS bez spadku wydajności, gwarantując jednocześnie najwyższy dostępny poziom bezpieczeństwa. W takiej bowiem sytuacji mechanizm pozwalający na automatyczne wyłączenie silnika IPS jak został on opisany w p. 3.3.17. jest niepotrzebny i bezużyteczny.

Nie ulega więc wątpliwości, że Zamawiający opisuje w wymaganiach konkretną cechę – unikalną dla jednego producenta – nie dopuszczając by zaoferowane zostały urządzenia innych producentów.

Opis przedmiotu zamówienia przygotowany jest więc w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

W związku z zaistniałą sytuacją wnosimy o wykreślenie wymagania 3.3.17. w całości jako wskazujące - wprost bądź łącznie z pozostałymi - na konkretne rozwiązanie.

Pozwoli to na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji - jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania wskazane przez Zamawiającego, podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający podtrzyma wymaganie punktu 3.3.17 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają wymaganie 3.3.17 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający usunie wymaganie 3.3.17.

PYTANIE 12
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu

zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. 3.4.1 określa wymaganie
„Baza modułu kontroli aplikacji powinna zawierać nie mniej niż 4000 pozycji. Baza modułu powinna być dostępna do weryfikacji online."

Wg naszej najlepszej wiedzy lista aplikacji obsługiwanych przez Fortinet oraz przez Palo Alto obejmuje ponad 3000 pozycji i nie przekracza 4000.

Oznacza to, że opis przedmiotu zamówienia przygotowany jest w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

W związku z zaistniałą sytuacją wnosimy o zmianę wymagania 3.4.1 w taki sposób, iż przyjmie ono treść.
„Baza modułu kontroli aplikacji powinna zawierać nie mniej niż 3000 pozycji. Baza modułu powinna być dostępna do weryfikacji online."
Jeżeli Zamawiający nie wyrazi zgody na zmianę to wnosimy o wykreślenie wymagania 3.4.1. w całości jako wskazujące - wprost bądź łącznie z pozostałymi - na konkretne rozwiązanie.

Chcemy zaznaczyć, że oba zaproponowane przez nas rozwiązania pozwolą na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji - jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania wskazane przez Zamawiającego, podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający odrzuci możliwości zmian lub wykreślenie punktu 3.4.1 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają wymaganie 3.4.1 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający zmieni treść wymagania 3.4.1 na następującą:
„Baza modułu kontroli aplikacji powinna zawierać nie mniej niż 3000 pozycji. Baza modułu powinna być dostępna do weryfikacji online."

W związku z powyższym Zamawiający modyfikuje kryterium nr 3 dla części 1, vide odpowiedź na pytanie 13.

PYTANIE 13
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w SWZ Zamawiający określa Kryterium 3 – Wielkość bazy modułu kontroli aplikacji
„Ocena kryterium zostanie dokonana w ten sposób, że Komisja przyzna każdej z ocenianych ofert liczbę 0 lub 10 punktów na podstawie poniższego zestawienia:

Wielkość bazy modułu kontroli aplikacji ponad 8000 pozycji 10 pkt.
Wielkość bazy modułu kontroli aplikacji ponad 4000-8000 pozycji 0 pkt."

Jak już wskazano w pytaniu 12 opis przedmiotu zamówienia przygotowany jest w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint. W przypadku kryteriów dodatkowo punktowanych zostały ustanowione tak, że jeszcze bardziej sprzyjają konkretnemu rozwiązaniu – produkcji Checkpoint.

Taka definicja wymagania powoduje iż kryterium to nie jest możliwe do spełnienia prawdopodobnie przez żadnego z liczących się producentów rozwiązań UTM/firewalli następnej generacji.

Należy tu zaznaczyć, iż firma Checkpoint jest jednym w 7-8 kluczowych producentów na rynku – jednocześnie nie jest największym producentem firewalli następnej generacji.

Biorąc pod uwagę, iż żadne rozwiązanie spośród tych firm – Cisco (ok. 7000 aplikacji) , Fortinet (ponad 3500 aplikacji), Forcepoint (około 3000 aplikacji), Huawei (ponad 6000 aplikacji), Juniper (ponad 3500 aplikacji) i Palo Alto Networks (ponad 3500 aplikacji) – nie spełniają tego wymagania, a jednocześnie ich rozwiązania są z powodzeniem stosowane w sieciach rządowych, sieciach przedsiębiorstw czy sieciach akademickich należy podnieść kwestię czy obsługa 8000 aplikacji jest wartością dla Zamawiającego. A jeżeli już to czy są warte prawie 17% wartości ceny oferty

W związku z zaistniałą sytuacją wnosimy o wykreślenie z SWZ Kryterium 3 w całości. Pozwoli to na złożenie oferty w oparciu o urządzenia innych producentów, którzy mogą spełnić uzasadnione potrzeby Zamawiającego, a jednocześnie nie być oceniane gorzej wskutek doboru kryteriów, które nie najprawdopodobniej nie wniosą Zamawiającemu żadnej dodatkowej wartości technicznej czy biznesowej (lub będzie to wartość zaniedbywalna)

Jeżeli Zamawiający odrzuci możliwości wykreślenia czy zmiany Kryterium 3 z SWZ w taki sposób by realnie została zachowana konkurencyjność wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają Kryterium 3 z SWZ w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający zmieni treść Kryterium 3 dla części 1 na następującą:

3. KRYTERIUM – *Wielkość bazy modułu kontroli aplikacji* - Ocena kryterium zostanie dokonana w ten sposób, że Komisja przyzna każdej z ocenianych ofert liczbę 0 lub 10 punktów na podstawie poniższego zestawienia:

- Wielkość bazy modułu kontroli aplikacji **ponad 8000 pozycji** 10 pkt.
- Wielkość bazy modułu kontroli aplikacji **3000-8000 pozycji** 0 pkt.

PYTANIE 14
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń

w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. 3.4.4 określa wymaganie
„Moduł kontroli aplikacji musi posiadać możliwość interakcji z użytkownikami. Interakcja musi być możliwa minimum w zakresie informowania o zablokowaniu dostępu do aplikacji, informowania o monitorowaniu komunikacji oraz pobierania informacji od użytkownika w celu uargumentowania konieczności dostępu do określonej aplikacji."

Funkcja interakcji z użytkownikiem opisana przez Zamawiającego jest cechą właściwą dla konkretnego rozwiązania dostępnego na rynku – firmy Checkpoint. Nie jest ona realizowana przez żadnego innego znanego nam producenta.

Zamawiający opisuje zatem w wymaganiach konkretną cechę urządzenia – unikalną dla jednego producenta – nie dopuszczając by zaoferowane zostały urządzenia innych producentów.

Tym samym opis przedmiotu zamówienia przygotowany jest w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

W związku z zaistniałą sytuacją wnosimy o zmianę wymagania 3.4.4 w taki sposób, iż przyjmie ono treść.
„Moduł kontroli aplikacji musi posiadać możliwość interakcji z użytkownikami. Interakcja musi być możliwa minimum w zakresie informowania o zablokowaniu dostępu do aplikacji."

Jeżeli Zamawiający nie wyrazi zgody na zmianę to wnosimy o wykreślenie wymagania 3.4.4. w całości jako wskazujące - wprost bądź łącznie z pozostałymi - na konkretne rozwiązanie.

Pozwoli to na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji - jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania wskazane przez Zamawiającego, podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający podtrzyma wymaganie punktu 3.4.4 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają wymaganie 3.4.4 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający zmieni treść wymagania 3.4.4 na następującą:
„Moduł kontroli aplikacji musi posiadać możliwość interakcji z użytkownikami. Interakcja musi być możliwa minimum w zakresie informowania o zablokowaniu dostępu do aplikacji."

PYTANIE 15
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu

zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. 3.4.5 określa wymaganie
„Moduł kontroli aplikacji musi umożliwiać modyfikowanie wbudowanych stron z powiadomieniami prezentowanymi użytkownikom oraz musi umożliwiać przekierowanie użytkowników do stron umieszczonych na zewnętrznych serwerach"

Funkcja interakcji z użytkownikiem opisana przez Zamawiającego jest cechą właściwą dla konkretnego rozwiązania dostępnego na rynku – firmy Checkpoint. Nie jest ona realizowana przez żadnego innego znanego nam producenta.

Zamawiający opisuje zatem w wymaganiach konkretną cechę urządzenia – unikalną dla jednego producenta – nie dopuszczając by zaoferowane zostały urządzenia innych producentów.

Tym samym opis przedmiotu zamówienia przygotowany jest w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

W związku z zaistniałą sytuacją wnosimy o zmianę wymagania 3.4.5 w taki sposób, iż przyjmie ono treść.
„Moduł kontroli aplikacji musi umożliwiać modyfikowanie wbudowanych stron z powiadomieniami prezentowanymi użytkownikom."

Jeżeli Zamawiający nie wyrazi zgody na zmianę to wnosimy o wykreślenie wymagania 3.4.5. w całości jako wskazujące - wprost bądź łącznie z pozostałymi - na konkretne rozwiązanie.

Pozwoli to na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji –

jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania wskazane przez Zamawiającego, podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający podtrzyma wymaganie z punktu 3.4.5 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają wymagania 3.4.5 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający nie zmieni we wnioskowany sposób i nie usunie wymagania 3.4.5.

PYTANIE 16
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. 3.4.6 określa wymaganie
„System musi umożliwiać administratorom tworzenie sygnatur nowych aplikacji za pomocą dedykowanego oprogramowania. W przypadku kiedy opisany mechanizm wymaga dodatkowej licencji to powinna ona zostać dostarczona razem z systemem bezpieczeństwa."

Funkcja tworzenia sygnatur nowych aplikacji nie jest funkcjonalnością nową i jest spełniana przez wielu producentów. Większość z nich realizuje jednak tą funkcję bądź natywnie w samym firewallu bądź poprzez komponent zarządczy (system zarządzania czy system logowania).

Tym samym opis przedmiotu zamówienia ponownie wymusza sposób realizacji pożądanej funkcji i dopuszcza lub wręcz wskazuje producentów, którzy posiadają dostępne dedykowane oprogramowanie dla realizacji tego celu.
Biorąc pod uwagę, że zarówno Fortinet jak i Palo Alto realizują podaną funkcję w inny sposób niż wymagany przez Zamawiającego – tym samym nie spełniają literalnie wymagania 3.4.6.

Można więc wprost określić, że opis przedmiotu zamówienia został przygotowany jest w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

W związku z zaistniałą sytuacją wnosimy o zmianę wymagania 3.4.6 w taki sposób, iż przyjmie ono treść.

„System musi umożliwiać administratorom tworzenie sygnatur nowych aplikacji – bezpośrednio na urządzeniu UTM lub za pomocą komponentu zarządzania lub za pomocą dedykowanego oprogramowania. W przypadku kiedy

opisany mechanizm wymaga dodatkowej licencji to powinna ona zostać dostarczona razem z systemem bezpieczeństwa."

Jeżeli Zamawiający nie wyrazi zgody na zmianę to wnosimy o wykreślenie wymagania 3.4.6. w całości jako wskazujące - wprost bądź łącznie z pozostałymi - na konkretne rozwiązanie.

Chcemy zaznaczyć, że oba zaproponowane przez nas rozwiązania pozwolą na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji - jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania wskazane przez Zamawiającego,

podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający odrzuci możliwości zmian lub wykreślenie punktu 3.4.6 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają wymaganie 3.4.6 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający zmieni treść wymagania 3.4.6 na następującą:
„System musi umożliwiać administratorom tworzenie sygnatur nowych aplikacji – bezpośrednio na urządzeniu UTM lub za pomocą komponentu zarządzania lub za pomocą dedykowanego

oprogramowania. W przypadku kiedy opisany mechanizm wymaga dodatkowej licencji to powinna ona zostać dostarczona razem z systemem bezpieczeństwa."

PYTANIE 17

Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń

w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. 3.6.5 określa wymaganie dla inspekcji ruchu szyfrowanego
„System musi umożliwiać utworzenie więcej niż jednego zbioru reguł określających zakres ruchu HTTPS podlegający inspekcji. System musi umożliwiać przypisywanie zbiorów reguł do określonych polityk bezpieczeństwa, a także współdzielenie określonych zbiorów reguł przez więcej niż jedną politykę bezpieczeństwa."

Większość urządzeń oferujących obecnie funkcje inspekcji ruchu szyfrowanego pozwala na współdzielenie określonych zbiorów reguł przez więcej niż jedną politykę bezpieczeństwa oraz ich przypisywanie do określonych

polityk. Jednakże sposób realizacji opisany jak w wymaganiu 3.6.5 jest powiązany z konkretną realizacją sprzętową i programową tego wymagania – realizowany przez firmę Checkpoint.

Część producentów stosuje metodę, w której zasady deszyfracji są opisywane w oddzielnym zestawie reguł przetwarzanym sekwencyjnie na wzór reguł bezpieczeństwa. W porównaniu do mechanizmu opisanego przez Zamawiającego ten sposób realizacji w ocenie Wykonawcy wręcz upraszcza zarządzanie deszyfracją i inspekcją ruchu już zdeszyfrowanego, nie wprowadzając jednocześnie żadnych ograniczeń funkcjonalnych wobec tych wymaganych przez Zamawiającego.

Tym samym opis przedmiotu zamówienia ponownie wymusza sposób realizacji pożądanej funkcji i wskazuje na jednego producenta - przedmiot zamówienia został opisany jest w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

Prosimy o informację czy Zamawiający uzna sposób realizacji wymagania 3.6.5 opisany powyżej za spełniający wymagania. Pozwoli to na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jeżeli Zamawiający nie dopuści realizacji wymagania 3.6.5 w sposób opisany powyżej i nie uzna za spełniający wymagania wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają wymaganie 3.6.5 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:

Zamawiający zmieni treść wymagania 3.6.5 na następującą:
„System musi umożliwiać utworzenie więcej niż jednego zbioru reguł określających zakres ruchu HTTPS podlegający inspekcji. System musi umożliwiać przypisywanie zbiorów reguł do określonych polityk bezpieczeństwa, a także współdzielenie określonych zbiorów reguł przez więcej niż jedną politykę bezpieczeństwa. Dopuszczalne są rozwiązania, w których zasady deszyfracji są opisywane w oddzielnym zestawie reguł przetwarzanym sekwencyjnie na wzór reguł bezpieczeństwa."

PYTANIE 18
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. 3.7.7 określa wymaganie dla IPSec VPN
„Moduł IPSec VPN musi wspierać nawiązywanie połączeń L2TP."

Funkcja ta jest realizowana przez co najmniej kilku producentów. Tym samym funkcja ta sama nie jest cechą właściwą dla któregokolwiek z producentów. Jednakże w tym konkretnym opisie przedmiotu zamówienia trzeba odczytywać wymaganie jej spełnienia łącznie z innymi wymaganiami. Tutaj spowoduje to, iż obsługa połączeń L2TP przez moduł IPSec VPN jest realizowana wyłącznie przez urządzenia firmy Checkpoint. Opis wymagania 3.7.7, którego spełnienie wydaje się proste, okazuje się proste pozornie, gdyż według naszej wiedzy żaden inny producent nie spełnia zestawu wymagań opisanych przez Zamawiającego (w tym p. 3.7.7.)

Ponownie należy podkreślić, iż opis przedmiotu zamówienia przygotowany jest w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

W związku z zaistniałą sytuacją wnosimy o wykreślenie wymagania 3.7.7. w całości jako wskazujące - wprost bądź łącznie z pozostałymi - na konkretne rozwiązanie.

Pozwoli to na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji - jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów

bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania wskazane przez Zamawiającego, podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający podtrzyma wymaganie punktu 3.7.7 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają wymaganie 3.7.7 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający usunie wymaganie 3.7.7.
Jednocześnie Zamawiający doda wymaganie 1.16 o następującej treści:
„System musi wspierać nawiązywanie połączeń L2TP."

PYTANIE 19
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. 3.7.9 określa wymaganie dla SSL VPN
„Urządzenie musi pozwalać na dostęp do wewnętrznych zasobów organizacji tj. aplikacji WEB, zasoby dyskowe SMB, sesje RDP) z Internetu (SSL VPN Portal). Zasoby powinny być udostępniane poprzez portal uruchamiany w przeglądarce internetowej. Ilość jednoczesnych sesji do portalu nie może być ograniczona licencyjnie."

Funkcja ta jest realizowana przez co najmniej kilku producentów. Tym samym funkcja ta sama nie jest cechą właściwą dla któregokolwiek z producentów. Podobnie jednak jak w przypadku wymagania z p.3.7.7 spełnienie tego wymagania jest tylko pozornie proste, gdyż jest ono elementem zamykającym – w powiązaniu z pozostałymi wymaganiami – możliwość zaoferowania rozwiązań innych producentów niż firmy Checkpoint. Według naszej

najlepszej wiedzy żaden inny producent nie spełnia zestawu wymagań opisanych przez Zamawiającego (w tym p. 3.7.9.)

Opis przedmiotu zamówienia przygotowany został zatem w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

W związku z zaistniałą sytuacją wnosimy o zmianę wymagania 3.7.9 w taki sposób, iż przyjmie ono treść.

„Urządzenie musi pozwalać na dostęp do wewnętrznych zasobów organizacji tj. aplikacji WEB, z Internetu (SSL VPN Portal). Zasoby powinny być udostępniane poprzez portal uruchamiany w przeglądarce internetowej. Ilość jednoczesnych sesji do portalu nie może być ograniczona licencyjnie."

Jeżeli Zamawiający nie wyrazi zgody na zmianę to wnosimy o wykreślenie wymagania 3.7.9. w całości jako wskazujące - wprost bądź łącznie z pozostałymi - na konkretne rozwiązanie.

Pozwoli to na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji - jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania wskazane przez Zamawiającego, podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający podtrzyma wymaganie punktu 3.7.9 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają wymaganie 3.7.9 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający nie zmieni we wnioskowany sposób i nie usunie wymagania 3.7.9.

PYTANIE 20

Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. 3.8.6 określa wymaganie

„Moduł filtrowania kategorii URL musi posiadać możliwość interakcji z użytkownikami. Interakcja musi być możliwa minimum w zakresie informowania o zablokowaniu dostępu do określonej witryny, informowania o monitorowaniu komunikacji oraz pobierania informacji od użytkownika w celu uargumentowania konieczności dostępu do określonej witryny."

Funkcja interakcji z użytkownikiem jest cechą urządzeń Web Proxy, Funkcja ta z urządzeniach UTM/NGFW jest zazwyczaj realizowana w taki sposób, iż użytkownik jest informowany o tym, że dostęp do danej witryny jest zablokowany, jednakże firewall daje użytkownikowi możliwość kontynuacji z jednoczesnym wymuszeniem zwrotnego potwierdzenia, że użytkownik jest świadomy, iż jest to wyjątek. Funkcja opisana w taki sposób nie dyskryminowałaby innych producentów niż Checkpoint.

Jednak sposób opisu tego wymagania przez Zamawiającego wskazuje jednoznacznie na rozwiązania firmy Checkpoint, gdyż według naszej najlepszej wiedzy tylko ta firma oferuje rozwiązania posiadające cechę funkcjonalną opisaną w OPZ. Zamawiający opisuje zatem element unikalny dla jednego producenta – nie dopuszczając by zaoferowane zostały urządzenia innych producentów.

Tym samym raz jeszcze wykazujemy, iż opis przedmiotu zamówienia został przygotowany jest w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

W związku z zaistniałą sytuacją wnosimy o zmianę wymagania 3.8.6 w taki sposób, iż przyjmie ono treść. *„Moduł filtrowania kategorii URL musi posiadać możliwość interakcji z użytkownikami. Interakcja musi być możliwa minimum w zakresie informowania o zablokowaniu dostępu do określonej witryny, informowania o monitorowaniu komunikacji oraz pobierania informacji od użytkownika, iż kontynuacja działania musi być związana z uzasadnionymi działaniami służbowymi użytkownika."*

Jeżeli Zamawiający nie wyrazi zgody na zmianę to wnosimy o wykreślenie wymagania 3.8.6. w całości jako wskazujące - wprost bądź łącznie z pozostałymi - na konkretne rozwiązanie.

Chcemy zaznaczyć, że oba zaproponowane przez nas rozwiązania pozwolą na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji - jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania wskazane przez Zamawiającego, podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający odrzuci możliwości zmian lub wykreślenie punktu 3.8.6 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych

producentów, które spełniają wymaganie 3.8.6 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający zmieni treść wymagania 3.8.6 na następującą:
„Moduł filtrowania kategorii URL musi posiadać możliwość interakcji z użytkownikami. Interakcja musi być możliwa minimum w zakresie informowania o zablokowaniu dostępu do określonej witryny, informowania o monitorowaniu komunikacji oraz pobierania informacji od użytkownika."

PYTANIE 21
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. 3.9.4 określa wymaganie:
„Moduł ochrony antywirusowej musi zapewniać ochronę minimum dla następujących protokołów: HTTP/HTTPS, SMTP/TLS, FTP, SMB/CIFS (w tym SMBv3), SFTP/SCP, IMAP, POP3."

Powyższy zestaw protokołów nie jest obsługiwany ani przez Fortinet (lista protokołów obsługiwanych w trybie proxy jak też w trybie Flow nie zawiera wszystkich wymaganych przez Zamawiającego) ani przez Palo Alto.
Tym samym pozostali dopuszczeni producenci nie spełniają wymagań w zakresie opisanym przez Zamawiającego.

Opis przedmiotu zamówienia przygotowany został zatem w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

W związku z zaistniałą sytuacją wnosimy o zmianę wymagania 3.9.4 w taki sposób, iż przyjmie ono treść.
„Moduł ochrony antywirusowej musi zapewniać ochronę minimum dla następujących protokołów: HTTP/HTTPS, SMTP/TLS, FTP, SMB/CIFS (w tym SMBv3), IMAP, POP3."

Jeżeli Zamawiający nie wyrazi zgody na zmianę to wnosimy o wykreślenie wymagania 3.9.4. w całości jako wskazujące - wprost bądź łącznie z pozostałymi - na konkretne rozwiązanie.

Pozwoli to na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji - jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania wskazane przez Zamawiającego, podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający podtrzyma wymaganie punktu 3.9.4 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają wymaganie 3.9.4 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający nie zmieni we wnioskowany sposób i nie usunie wymagania 3.9.4.

PYTANIE 22
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. 3.9.7 określa wymaganie
„Moduł ochrony antywirusowej musi umożliwiać skanowanie plików skompresowanych. Administrator musi mieć możliwość zdefiniowania maksymalnego czasu skanowania pojedynczego archiwum oraz zdefiniowania akcji (przekaż lub zablokuj) która zostanie podjęta w momencie przekroczenia zdefiniowanego limitu."

Funkcje zarządzania realizowane w formie opisanej przez Zamawiającego są dostępne tylko w rozwiązaniu Checkpoint, i nie są jednocześnie dostępne w urządzeniach produkcji Fortinet oraz produkcji Palo Alto Networks.

Warto tutaj nadmienić, że definiowanie maksymalnego czasu skanowania pojedynczego archiwum i definicja akcji są funkcjami wymaganymi przez firewalle realizujące funkcję ochrony antywirusowej w trybie proxy, gdzie plik musi zostać najpierw w całości przechwycony i dopiero wtedy poddany skanowaniu.

Po raz kolejny Zamawiający definiując wymaganie w ten sposób ogranicza konkurencję wymuszając określony sposób realizacji funkcji, a nie skupiając się na wartości funkcji jako takiej.

Należy tutaj wyjaśnić, że zarówno rozwiązania Palo Alto jak i rozwiązanie Fortinet realizują ochronę antywirusową w trybie strumieniowym (Flow-mode) czyli na bieżąco i bez konieczności przechwycenia pliku w

całości. Oznacza to, że technicznie nie umożliwiają one konfiguracji w/w atrybutów dla silnika antywirusowego, bo nie mają one w takim przypadku żadnego zastosowania

Opis przedmiotu zamówienia przygotowany jest więc w taki sposób, że wskazuje konkretny sposób realizacji zadania – unikalny dla jednego producenta, zaś jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

W związku z powyższym prosimy o potwierdzenie że Zamawiający dopuści rozwiązanie, w którym w przypadku zastosowania silnika antywirusowego działającego w trybie strumieniowym nie będzie wymagana możliwość zdefiniowania maksymalnego czasu skanowania pojedynczego archiwum oraz zdefiniowania akcji.

Jeżeli Zamawiający nie wyrazi na to zgody to wnosimy o wykreślenie wymagania 3.9.7. w całości jako wskazujące - wprost bądź łącznie z pozostałymi - na konkretne rozwiązanie.

Pozwoli to na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji - jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania

wskazane przez Zamawiającego, podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający podtrzyma wymaganie punktu 3.9.7 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają wymaganie 3.9.7 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający zmieni treść wymagania 3.9.7 na następującą:
„Moduł ochrony antywirusowej musi umożliwiać skanowanie plików skompresowanych."

PYTANIE 23
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. 3.9.8 określa wymaganie
„Moduł ochrony antywirusowej musi posiadać możliwość blokowania dostępu do określonych witryn internetowych w oparciu o informację o ich reputacji."

Funkcje zarządzania realizowane w formie opisanej przez Zamawiającego są dostępne tylko w rozwiązaniu Checkpoint, i nie są jednocześnie dostępne w urządzeniach produkcji Fortinet oraz produkcji Palo Alto Networks.

Po raz kolejny Zamawiający definiując wymaganie ogranicza konkurencję w taki sposób że wymusza określony sposób realizacji funkcji –realizację zadania przez moduł ochrony antywirusowej, a nie skupiając się na realizacji funkcji jako takiej. Niejednokrotnie jest kwestią dyskusyjną czy sposób realizacji takiej czy innej funkcji przez urządzenie jest najlepszym z dostępnych sposobów. Zamawiający zaś określa w wymaganiach jeden „jedynie słuszny" sposób realizacji.

Należy tutaj wskazać że realizacja funkcji blokowania dostępu do określonych witryn internetowych w oparciu o informację o ich reputacji jest przez dominującą część producentów realizowany przez silnik URL Filtering i

zarówno Fortinet jak i Palo Alto posiadają analogiczną funkcjonalność jednakże realizowaną właśnie przez silnik URL Filtering.

Opis przedmiotu zamówienia wymuszający realizację blokowania dostępu do określonych witryn internetowych w oparciu o informację o ich reputacji przez silnik antywirusowy wskazuje na konkretną implementację i unikalną cechę jednego z producentów. Opis przygotowany jest więc w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

W związku z powyższym prosimy o potwierdzenie że Zamawiający dopuści rozwiązanie, w którym możliwość blokowania dostępu do określonych witryn internetowych będzie realizowana w oparciu o informację o ich reputacji jednakże realizowaną przez inny moduł aniżeli moduł ochrony antywirusowej.

Jeżeli Zamawiający nie wyrazi na to zgody to wnosimy o wykreślenie wymagania 3.9.8. w całości jako wskazujące na konkretny sposób realizacji celu i cechę własnościową jednego producenta.

Chcemy zaznaczyć, że zaproponowane przez nas rozwiązania pozwolą na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji - jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania wskazane przez Zamawiającego, podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający podtrzyma wymaganie punktu 3.9.8 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają wymaganie 3.9.8 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający zmieni treść wymagania 3.9.8 na następującą:
„Moduł ochrony antywirusowej musi posiadać możliwość blokowania dostępu do określonych witryn internetowych w oparciu o informację o ich reputacji. Powyższa funkcjonalność może być realizowana przez inne elementy systemu np. silnik URL filtering."

PYTANIE 24
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na

rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. 3.9.10 określa wymaganie

„System bezpieczeństwa musi umożliwiać rozszerzenie bazy informacji o zagrożeniach poprzez dodawanie zewnętrznych definicji IoC (Indicator of Compromise) z formacie CSV lub STIX XML (STIX 1.0)"

Po raz kolejny Zamawiający definiując wymaganie w ten sposób ogranicza konkurencję wymuszając określony sposób realizacji funkcji. Obecne rozwiązania NGFW pozwalają na zaimportowanie informacji o IoC w szeregu innych standardów i metod aniżeli te wskazane przez Zamawiającego.

W szczególności zarówno Fortinet jak i Palo Alto pozwalają na automatyczne pobieranie IoC przez firewall ze wskazanego URL co de facto jest nieporównywalnie wygodniejszym sposobem w codziennym działaniu aniżeli ręczne wgrywanie plików CSV, a funkcjonalnie odpowiada integracji z feedem STIX.

Wymóg realizacji tej funkcji w bardzo określony sposób powoduje, iż Zamawiający z jednej strony ogranicza konkurencję, z drugiej zaś pozbawia się możliwości pozyskania rozwiązań które realizują tożsamą funkcję w formie znacznie nowocześniejszej i wygodniejszej niż rozwiązanie Checkpoint.

Opis przedmiotu zamówienia przygotowany jest więc w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

W związku z powyższym wnosimy o zmianę wymagania w p 3.9.10 na
„System bezpieczeństwa musi umożliwiać rozszerzenie bazy informacji o zagrożeniach poprzez dodawanie zewnętrznych definicji IoC (Indicator of Compromise)"

Jeżeli Zamawiający nie wyrazi na to zgody to wnosimy o wykreślenie wymagania 3.9.10. w całości jako wskazujące na konkretny sposób realizacji celu.

Chcemy zaznaczyć, że oba zaproponowane przez nas rozwiązania pozwolą na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji - jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania wskazane przez Zamawiającego, podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów

bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający podtrzyma wymaganie punktu 3.9.10 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają wymaganie 3.9.10 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający zmieni treść wymagania 3.9.10 na następującą:
„System bezpieczeństwa musi umożliwiać rozszerzenie bazy informacji o zagrożeniach poprzez dodawanie zewnętrznych definicji IoC (Indicator of Compromise) z formacie CSV, STIX XML (STIX 1.0) lub pobieranie ze wskazanego URL."

PYTANIE 25
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. 3.9.5 określa wymaganie
„Moduł ochrony antywirusowej musi w zależności od konfiguracji posiadać możliwość inspekcji lub blokowania pobierana pozczególnych typów plików - minimum bat, cab, dll, doc, pdf, jpg, jpeg, exe, com, pif, scr, gif, png, tif, asf, mp3, mdb, bmp, ps, rtf, rar, tgz, tar.gz, bz2, tar.bz2, tbz2, tb2, jar, , arc, reg, arj, zoo, ace, wmf, emf, xml, doc, ppt, xls, swf, mov, mpeg, js, wav, tar, ico, zip, hml, htm, hta."

Zamawiający wskazuje tutaj listę plików, która jest spełniana przez jednego producenta, trzeba jednoznacznie wskazać, iż silniki AV firm Fortinet oraz Palo Alto Networks nie zawierają wszystkich typów podanych przez Zamawiającego.

Jednocześnie należy wskazać, iż silniki ochrony antywirusowej konkurencyjne do firmy Checkpoint zawierają typy plików które nie są ujęte w powyższym zestawieniu. Pozwala ta wyciągnięcie co najmniej wniosku, iż na etapie weryfikacji opisu przedmiotu zamówienia względem rozwiązań dostępnych na rynku nie dopełniono sprawdzenia podanej listy z ofertą rynkową inną niż Checkpoint – nie wyodrębniono części wspólnej – zestawu plików, które byłyby obsługiwane przez więcej niż jednego producenta.

Ponadto Zamawiający ponownie wskazuje, że określona cecha funkcjonalna musi być realizowana przez wskazany moduł – tutaj moduł ochrony antywirusowej. Należy podkreślić, iż sama inspekcja odbywa się w module antywirusowym jednakże blokowanie pobierania poszczególnych plików nie jest funkcjonalnie powiązana z tym modułem i może być skutecznie realizowana w innych modułach urządzenia.

Przedmiot zamówienia został w p.3.9.5 opisany w sposób nadzwyczaj precyzyjny – nie pozwalający na realizację zadania w sposób odmienny niż wskazał Zamawiający. Równocześnie precyzja opisu – lista plików – eliminuje jakąkolwiek konkurencję.

Opis przedmiotu zamówienia przygotowany jest więc w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

W związku z powyższym wnosimy o zmianę wymagania w p 3.9.5 na
„Moduł ochrony antywirusowej musi w zależności od konfiguracji posiadać możliwość inspekcji lub blokowania pobierana pozczególnych typów plików - minimum bat, cab, dll, doc, pdf, jpeg, exe, com, gif, png, tif, mp3, bmp, rtf, rar, jar, reg, arj, doc, ppt, xls, mov, mpeg, js, tar, zip, hta.

Funkcja blokowania pobierania poszczególnych typów plików może być zrealizowana w innym module urządzenia UTM aniżeli moduł ochrony antywirusowej"

Powyższa lista jest według naszej najlepszej wiedzy spełniana przez co najmniej trzech producentów.

Jeżeli Zamawiający nie wyrazi zgody na zmianę to wnosimy o wykreślenie wymagania 3.9.5. w całości jako wskazujące na konkretne rozwiązanie.

Chcemy zaznaczyć, że oba zaproponowane przez nas rozwiązania pozwolą na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji - jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania wskazane przez Zamawiającego, podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający podtrzyma wymaganie punktu 3.9.5 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają wymaganie 3.9.5 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający nie zmieni we wnioskowany sposób i nie usunie wymagania 3.9.5.

PYTANIE 26
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce

na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. 3.10.2 określa wymaganie
„Moduł musi zapewniać możliwość analizowania następujących typów plików:

- *.7z - 7z Archive*
- *.bz2 - bzip2 compressed archive*
- *.CAB - Compressed archive*
- *.csv - Comma-separated values file*
- *.doc Microsoft Word 97-2003 Document*
- *.docx Microsoft Word Document*
- *.dot / .dotx - Microsoft Word Template*
- *.dotm / .docm - Microsoft Word macro-enabled template*
- *.gz - Gz Archive*
- *.hwp*
- *.iqy - Excel Web Query file*
- *.iso -*
- *.jar - Java Browser Applet*
- *.msg - Mail message file format used by Microsoft Outlook and Exchange*
- *.pdf - Adobe Acrobat document*
- *.ppt - Microsoft PowerPoint 97-2003 Presentation*
- *.pptx - Microsoft PowerPoint Presentation*
- *.pps - Legacy Microsoft PowerPoint slideshow*
- *.pptm - Microsoft PowerPoint macro-enabled presentation*
- *.potx - Microsoft PowerPoint template*
- *.potm - Microsoft PowerPoint macro-enabled template*
- *.ppam - Microsoft PowerPoint add-in*
- *.ppsx - Microsoft PowerPoint slideshow*
- *.ppsm - Microsoft PowerPoint macro-enabled slideshow*
- *.rar - Rar Archive*
- *.rtf - Rich Text Format file*
- *.sldx - Microsoft PowerPoint slide*
- *.sldm - Microsoft PowerPoint macro-enabled slide*
- *.swf - Flash*
- *.tar - Tar Archive*
- *.tgz - Tgz Archive*
- *.xlt - Legacy Microsoft Excel 97-2003 templates*
- *.xls - Microsoft Excel 97-2003 Worksheet*
- *.xlsx - Microsoft Excel Worksheet*
- *.xlm - Microsoft Excel macro*
- *.xltx - Microsoft Excel template*
- *.xlsm - Microsoft Excel macro-enabled workbook*
- *.xltm - Microsoft Excel macro-enabled template*
- *.xlsb - Microsoft Excel binary worksheet*
- *.xla - Microsoft Excel add-on or macro*
- *.xlam - Microsoft Excel add-on*
- *.xll - Microsoft Excel XLL (DLL based) add-on*
- *.xlw - Microsoft Excel workspace*
- *.zip - Zip Archive"*

Zamawiający wskazuje tutaj konieczność obsługi przez moduł ochrony przed nieznanymi zagrożeniami określonej grupy plików. Pełna lista tych plików – w całości - jest obsługiwana tylko przez jednego producenta.

Trzeba bowiem jednoznacznie wskazać, iż moduły analizy ZeroDay firm Fortinet oraz Palo Alto nie zawierają wszystkich typów podanych przez Zamawiającego.

Jednocześnie należy wskazać, iż silniki ochrony przed nieznanymi zagrożeniami - konkurencyjne do firmy Checkpoint - zawierają typy plików które nie są ujęte w powyższym zestawieniu. W szczególności warto tutaj podkreślić, że obie firmy konkurencyjne do Checkpoint (dopuszczone w niniejszym postępowaniu) obsługują zdecydowanie więcej typów plików uchodzących za potencjalnie najbardziej złośliwe – plików binarnych czy skryptów (Zamawiający wymaga jedynie jar i swf).

Pozwala to wyciągnięcie co najmniej wniosku, iż na etapie weryfikacji opisu przedmiotu zamówienia względem rozwiązań dostępnych na rynku nie dopełniono sprawdzenia podanej listy z ofertą rynkową inną niż Checkpoint

– nie wyodrębniono części wspólnej – zestawu plików, które byłyby obsługiwane przez więcej niż jednego producenta.

Opis przedmiotu zamówienia przygotowany jest więc w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

W związku z powyższym wnosimy o zmianę wymagania w p 3.10.2 na
„Moduł musi zapewniać możliwość analizowania następujących typów plików:

- *.Archiwa – co najmniej*
  - *7z - 7z Archive*
  - *zip - Zip Archive"*
  - *rar - Rar Archive*
- *Pliki Microsoft Office*
- *.jar - Java Browser Applet*
- *.pdf - Adobe Acrobat document*
- *.swf – Flash"*

Powyższa lista jest według naszej najlepszej wiedzy spełniana przez co najmniej trzech producentów.

Jeżeli Zamawiający nie wyrazi zgody na zmianę to wnosimy o wykreślenie wymagania 3.10.2. w całości jako wskazujące na konkretne rozwiązanie.

Chcemy zaznaczyć, że oba zaproponowane przez nas rozwiązania pozwolą na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji - jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania wskazane przez Zamawiającego, podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający podtrzyma wymaganie punktu 3.10.2 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają wymaganie 3.10.2 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający nie zmieni we wnioskowany sposób i nie usunie wymagania 3.10.2.

PYTANIE 27
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. 3.10.8 określa wymaganie
„Moduł musi umożliwiać opisywanie zagrożeń za pomocą sygnatur YARA."

Samo wymaganie nie jest dla Wykonawcy jasne i konkretne – nie wynika z niego co system powinien zapewniać. Domysłem Wykonawcy jest, iż sandbox powinien sam z siebie produkować sygnaturę YARA.

Biorąc pod uwagę, że YARA jest jedną z metod opisu zagrożeń – ponownie jest to określenie konkretnego sposobu realizacji funkcji – wnosimy o rozszerzenie dopuszczalnych metod o XML.

Chcemy nadmienić, iż pozostawienie tylko sygnatur YARA powoduje, że opis przedmiotu zamówienia przygotowany jest w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

W związku z powyższym wnosimy o zmianę wymagania w p 3.10.8 na
„Moduł musi umożliwiać opisywanie zagrożeń za pomocą sygnatur YARA lub XML."

Jeżeli Zamawiający nie wyrazi zgody na zmianę to wnosimy o wykreślenie wymagania 3.10.8. w całości jako wskazujące - wprost bądź łącznie z pozostałymi - na konkretne rozwiązanie.

Chcemy zaznaczyć, że oba zaproponowane przez nas rozwiązania pozwolą na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji –

jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania wskazane przez Zamawiającego, podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający podtrzyma wymaganie punktu 3.10.8 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają wymaganie 3.10.8 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający zmieni treść wymagania 3.10.8 na następującą:
„Moduł musi umożliwiać opisywanie zagrożeń za pomocą sygnatur YARA lub XML."

PYTANIE 28
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce

na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. 3.10.3 określa wymaganie
„Moduł musi umożliwiać otwarcie dostarczonego za pośrednictwem wspieranych protokołów pliku w wirtualnym systemie operacyjnym, analizę skutków otwarcia pliku w tym systemie a następnie podjęcie akcji (zablokuj/przekaż do odbiorcy) w zależności od uzyskanych wyników analizy. Szczegółowy wynik analizy powinien zostać udokumentowany w formie raportu i przesłany na wskazany serwer logów."

Według naszej najlepszej wiedzy, żaden z producentów dopuszczonych przez Zamawiającego literalnie nie spełnia tego wymagania wprost. Wynika to z tego, że w naszym rozumieniu urządzenie UTM musiałoby buforować dowolną liczbę plików przez cały okres przeprowadzania analizy w środowisku Sandbox. Analiza w wirtualnym systemie operacyjnym jest de facto wykonywana asynchronicznie wobec ruchu sieciowego, bo wynik pełnej analizy nie jest natychmiastowo dostępny.

Najnowocześniejsze zdobycze techniki w zakresie wykrywania złośliwego kodu pozwalają na bardzo skuteczne wykrywania i zatrzymywanie zagrożeń zero day z wykorzystaniem analizy statycznej bezpośrednio na urządzeniach next generation firewall bez potrzeby analizy próbki w zew. systemach sandbox. Analiza statyczna działa na podstawie modeli ML przygotowywanych w globalnym sandboxie realizującym dynamiczną analizę w wirtualnych systemach operacyjnych co gwarantuje wysoką skuteczność i dostosowywanie się na bieżąco do technik wykorzystywanych przez cyberprzestępców. Według najlepszej wiedzy Wykonawcy taką funkcjonalność posiadają zarówno rozwiązania Checkpoint, Fortinet jak i Palo Alto.

Rozwiązania producentów, którzy nie implementują analizy statycznej dla zagrożeń zero day bezpośrednio wewnątrz firewalla następnej generacji muszą bazować na werdykcie z zew. sandboxa, którego wygenerowanie zajmuje od kilkudziesięciu do kilkuset sekund i tym samym muszą wstrzymać dostarczenie pliku do odbiorcy.

W świetle powyższych faktów zwracamy się z prośbą o potwierdzenie iż Zamawiający dopuści rozwiązania UTM/firewall realizujące ochronę przez zagrożeniami zero day jako połączenie lokalnej analizy statycznej oraz analizy statycznej i dynamicznej w zewnętrznym systemie sandbox.

Jeżeli Zamawiający nie wyrazi na to zgody to wnosimy o wykreślenie wymagania 3.10.3. w całości jako uniemożliwiające złożenie ważnej oferty na sprzęcie produkowanym przez któregokolwiek z dopuszczonych przez Zamawiającego dostawców.

Jeżeli Zamawiający podtrzyma wymaganie punktu 3.10.3 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają

wymaganie 3.10.3 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający zmieni treść wymagania 3.10.3 na następującą:
„Moduł musi umożliwiać otwarcie dostarczonego za pośrednictwem wspieranych protokołów pliku w wirtualnym systemie operacyjnym, analizę skutków otwarcia pliku w tym systemie a następnie podjęcie akcji (zablokuj/przekaż do odbiorcy) w zależności od uzyskanych wyników analizy. Szczegółowy wynik analizy powinien zostać udokumentowany w formie raportu i przesłany na wskazany serwer logów. Dopuszczalne są rozwiązania UTM/firewall realizujące ochronę przez zagrożeniami zero day jako połączenie lokalnej analizy statycznej oraz analizy statycznej i dynamicznej w zewnętrznym systemie sandbox."

PYTANIE 29

Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w p. 3.10.4 określa wymaganie

„Niedopuszczalne jest przekazanie pliku do odbiorcy przed uzyskaniem wyniku z procesu analizy w środowisku wirtualnym potwierdzającego że analizowany plik jest bezpieczny. Wyjątkiem jest dostarczenie do użytkownika bezpiecznej wersji pliku, tzn. wersji pozbawionej całej treści aktywnej. Jako treść aktywna rozumiane są między innymi makra pakietu MS Office, odnośniki do zewnętrznych zasobów, obrazy, kwerendy do baz danych, skrypty JavaScript, filmy i inne."

Funkcje modułu sandbox realizowane w formie opisanej przez Zamawiającego są dostępne tylko w rozwiązaniu Checkpoint, i nie są jednocześnie dostępne w urządzeniach produkcji Fortinet oraz produkcji Palo Alto Networks.

Abstrahując od wartości jaką ma dla odbiorcy plik, który jest pozbawiony znaczącej części treści chcemy raz jeszcze podkreślić, iż wymagania, które stawia Zamawiający w sekcji wymagań 3.10 wydają się nie adresować najpoważniejszych obecnie zagrożeń, za to skupione są na pewnych elementach funkcjonalnych, które nie będą stanowiły o poziomie jakości ochrony,
Po raz kolejny Zamawiający ogranicza konkurencję wymuszając określony podzbiór funkcji, a nie skupiając się na wartości funkcji jako takiej.

Opis przedmiotu zamówienia przygotowany jest więc w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint – co może stanowić naruszenie prawa zamówień publicznych.

W związku z powyższym wnosimy o zmianę wymagania w p 3.10.4 na

„Niedopuszczalne jest przekazanie pliku do odbiorcy przed uzyskaniem wyniku z procesu analizy w środowisku wirtualnym lub lokalnej analizy z wykorzystaniem algorytmów uczenia maszynowego, potwierdzającego że analizowany plik jest bezpieczny."

Taki zapis jest według naszej najlepszej wiedzy spełniany przez co najmniej trzech producentów.

Jeżeli Zamawiający nie wyrazi zgody na zmianę to wnosimy o wykreślenie wymagania 3.10.4. w całości jako wskazujące - wprost bądź łącznie z pozostałymi - na konkretne rozwiązanie.

Chcemy zaznaczyć, że oba zaproponowane przez nas rozwiązania pozwolą na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji - jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania wskazane przez Zamawiającego, podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający odrzuci możliwości zmian lub wykreślenie punktu 3.10.4 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają wymaganie 3.10.4 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający zmieni treść wymagania 3.10.4 na następującą:
„Niedopuszczalne jest przekazanie pliku do odbiorcy przed uzyskaniem wyniku z procesu analizy w środowisku wirtualnym lub lokalnej analizy z wykorzystaniem algorytmów uczenia maszynowego, potwierdzającego że analizowany plik jest bezpieczny."

PYTANIE 30
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w sekcji wymagań p. 3.11.x określa wymaganie sprzętowe

Wymagania te określone są w taki sposób, iż wprost nie ma możliwości zaoferowania urządzeń produkcji Palo Alto, a jednocześnie zaoferowanie rozwiązań firm Fortinet i Palo Alto nie jest możliwe w powiązaniu z innymi wymaganiami

W związku z powyższym celem zwiększenia konkurencyjności postępowania wnosimy o zmianę wymagania w p 3.11.3 na

„Urządzenie pełniące rolę zapory sieciowej musi posiadać przepływność w ruchu full-duplex nie mniej niż 6 Gbit/s dla kontroli firewall z włączoną funkcją IPS oraz kontrolą aplikacji oraz nie mniej niż 3.5 Gbit/s dla kontroli zawartości (moduły firewall, kontrola aplikacji, kategoryzacja URL, moduł antywirusowy, IPS, ochrona Zero-Day) i obsługiwać nie mniej niż 3 000 000 jednoczesnych połączeń z możliwością obsługi przyrostu 100 000 połączeń na sekundę."

Jeżeli Zamawiający nie wyrazi zgody na zmianę to wnosimy o wykreślenie wymagania 3.11.3. w całości jako wskazujące - wprost bądź łącznie z pozostałymi - na konkretne rozwiązanie.

Chcemy zaznaczyć, że oba zaproponowane przez nas rozwiązania pozwolą na złożenie oferty w oparciu o urządzenia innych producentów niż Checkpoint, którzy mogą spełnić uzasadnione potrzeby Zamawiającego.

Jednocześnie zwracamy uwagę na fakt, iż wskazanie na rozwiązania firmy Checkpoint jest tak rażące, iż nawet wykreślenie wymagania 1.12 w żaden sposób nie zniweluje problemu niedozwolonego ograniczenia konkurencji - jest bowiem bardzo mało prawdopodobne by producenci nie oferujący najbardziej zaawansowanych systemów bezpieczeństwa dostępnych na rynku spełniali łącznie wszystkie wymagania wskazane przez Zamawiającego, podczas gdy nie są one spełnione przez liderów rynkowych. Poszerzenie wachlarza dostawców systemów bezpieczeństwa o producentów, oferujących rozwiązania, które w dalszym ciągu nie spełniają wymagań stawianych przez Zamawiającego nie czyni postępowania w żaden sposób bardziej konkurencyjnym.

Jeżeli Zamawiający odrzuci możliwości zmian lub wykreślenie punktu 3.11.3 wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają wymaganie 3.11.3 w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający zmieni treść wymagania 3.11.3 na następującą:
„Urządzenie pełniące rolę zapory sieciowej musi posiadać przepływność w ruchu full-duplex nie mniej niż 6 Gbit/s dla kontroli firewall z włączoną funkcją IPS oraz kontrolą aplikacji oraz nie mniej niż 3.5 Gbit/s dla kontroli zawartości (moduły firewall, kontrola aplikacji, kategoryzacja URL, moduł antywirusowy, IPS, ochrona Zero-Day) i obsługiwać nie mniej niż 3 000 000 jednoczesnych połączeń z możliwością obsługi przyrostu 100 000 połączeń na sekundę."

PYTANIE 31
Zamawiający w Opisie Przedmiotu Zamówienia część 1 w punkcie 1.12 zawarł wymaganie określające, iż wykonawcy mogą zaoferować urządzenia tylko tych dostawców, którzy oferują produkty „o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) w latach 2018, 2019 i 2020"

Oznacza to w szczególności, iż Zamawiający dopuszcza rozwiązania tylko trzech dostawców – Checkpoint, Fortinet oraz Palo Alto Networks- i w tym świetle należy rozważać wszystkie pozostałe wymagania dla przedmiotu Zamówienia.

Jednocześnie Zamawiający w SWZ Zamawiający określa Kryterium 2 – Wysokość pojedynczego urządzenia

„Ocena kryterium zostanie dokonana w ten sposób, że Komisja przyzna każdej z ocenianych ofert liczbę 0 lub 10 punktów na podstawie poniższego zestawienia:

Wysokość pojedynczego urządzenia 1U 10 pkt.
Wysokość pojedynczego urządzenia 2U 0 pkt."

Jak już wskazano w poprzednich pytaniach opis przedmiotu zamówienia przygotowany jest w taki sposób, iż jego treść wprost bądź łącznie umożliwia złożenie oferty tylko na rozwiązaniu jednego producenta – firmy Checkpoint.

W przypadku kryteriów dodatkowo punktowanych zostały ustanowione tak, że jeszcze bardziej sprzyjają konkretnemu rozwiązaniu – produkcji Checkpoint.

Taka definicja wymagania powoduje iż kryterium to nie jest możliwe do spełnienia prawdopodobnie przez żadnego z liczących się producentów rozwiązań UTM/firewalli następnej generacji.

Zarówno Fortinet jak i Palo Alto Networks nie posiadają bowiem w swojej ofercie urządzeń, które spełniłyby to wymaganie Zamawiającego.

Patrząc zatem na całokształt opisu przedmiotu zamówienia można doszukiwać się tutaj dodatkowego faworyzowania jednego z producentów. W przypadku wymagań obligatoryjnych w wielu punktach Zamawiający wskazał cechy unikalne rozwiązania Checkpoint – uniemożliwiające złożenie oferty innym producentom.

Podobnie w przypadku Kryterium 2 – jest ono spełniane tylko przez rozwiązania Checkpoint. O ile bowiem na rynku jest dostępnych więcej urządzeń posiadających obsadę interfejsów oraz wydajność, które są realizowane w obudowie o wielkości 1U to w przypadku tego konkretnego postępowania parametry fizyczne są dobrane w taki sposób, iż jednym producentem spełniającym to Kryterium jest Checkpoint.

Kryterium 2 jest też samo w sobie kwestionowalne – trudno jest doszukać się wartości technicznej lub biznesowej dla Zamawiającego w zakupie urządzeń o wielkości 1U w porównaniu do urządzeń 2U, gdzie wartość ta stanowiłaby aż 17% wartości projektu.

W powiązaniu z Kryterium 3 firma Checkpoint uzyskuje tutaj przewagę – nie tyle techniczną czy biznesową (chociażby w postaci dłuższego okresu gwarancji czy usług) – co mocno naciąganą, a jednak na tyle dużą iż trudno mówić tutaj o poszanowaniu zasady konkurencyjności.

W związku z tym wnosimy o wykreślenie z SWZ Kryterium 2 w całości. Pozwoli to na złożenie oferty w oparciu o urządzenia innych producentów, którzy mogą spełnić uzasadnione potrzeby Zamawiającego, a jednocześnie nie oferty nie będącej ocenionej gorzej wskutek doboru kryteriów, które nie najprawdopodobniej nie wniosą Zamawiającemu żadnej dodatkowej wartości technicznej czy biznesowej (lub będzie to wartość zaniedbywalna)

Jeżeli Zamawiający odrzuci możliwości wykreślenia czy zmiany Kryterium 2 z SWZ w taki sposób by realnie została zachowana konkurencyjność wówczas prosimy o wskazanie co najmniej dwóch (2) producentów oraz wskazanie konkretnych produktów oferowanych przez tych producentów, które spełniają Kryterium 2 z SWZ w powiązaniu/łącznie ze wszystkimi pozostałymi wymaganiami w opisie przedmiotu zamówienia.

ODPOWIEDŹ:
Zamawiający nie zmieni treści Kryterium 2.

PYTANIE 32 - Pytanie do części II – dostawa serwera wraz o oprogramowaniem.

Czy Zamawiający dopuści jako spełniające wymagania, serwery wyposażone w możliwość zarządzania bezpośredniego poprzez złącze USB 2.0 umieszczone na froncie obudowy?

ODPOWIEDŹ:
Zamawiający dopuści jako spełniające wymagania, serwery wyposażone w możliwość zarządzania bezpośredniego poprzez złącze USB 2.0 umieszczone na froncie obudowy.

Pytanie 33
Formularz cenowy dla części 1 - VAT 0% We wzorze formularza cenowego dla części 1 Zamawiający wskazał stawkę podatku VAT 0% dla całego oferowanego przedmiotu zamówienia. Jednak przedmiot zamówienia obejmuje:
a) klaster urządzeń UTM (czyli dwa urządzenia do transmisji danych
cyfrowych) z fabrycznie zainstalowanym oprogramowaniem
b) licencje rozbudowujące funkcjonalność oprogramowania urządzeń
c) licencja na dodatkowe oprogramowanie zarządzające
d) pakiet serwisowy zapewniający obsługę serwisową producenta na wymaganym przez Zamawiającego poziomie Zgodnie z ustawą o podatku od towarów i usług stawkę podatku VAT 0% można zastosować wyłącznie do klastra urządzeń UTM, wskazanego w punkcie a.
Licencje oprogramowania opisane w punktach b i c oraz pakiet serwisowy z punktu d objęte są 23-procentową stawką podatku VAT.
Proszę o wyjaśnienie i/lub zmianę formularza.

ODPOWIEDŹ:
Zamawiający dokona zmiany formularza cenowego.

Pytanie 34
Definicja sprzętu fabrycznie nowego
SWZ punkt 4.12 zawiera następujący zapis: "Dostarczony sprzęt musi być fabrycznie nowy, tzn. wyprodukowany nie wcześniej niż 90 dni przed dniem dostawy (...)"
Podobnie sprzęt fabrycznie nowy definiuje § 1 ust. 2 umowy: "Wykonawca oświadcza, że zaoferowane przez niego urządzenia są fabrycznie nowe, wyprodukowane nie wcześniej niż 90 dni przed dniem dostawy"

Natomiast opis przedmiotu zamówienia wskazuje: "Zamawiający wymaga aby dostarczone urządzenia były nowe oraz pochodziły z bieżącej produkcji (wyprodukowane nie wcześniej niż 180 dni od dnia dostawy)"
Proszę o ujednolicenie wymagań. Biorąc pod uwagę utrzymujące się na rynku trudności z dostępnością urządzeń wywołane ogólnoświatowymi brakami półprzewodników, ograniczenie terminu do 90 dni może znacząco utrudnić realizację zamówienia, uniemożliwiając skorzystanie z zasobów magazynowych dystrybutorów i producentów (terminy dostaw urządzeń sieciowych z bieżącej produkcji sięgają nawet kilku miesięcy). Z tego względu proszę o wybór wariantu 180 dni.

ODPOWIEDŹ:
Za sprzęt nowy uznamy sprzęt nie starszy niż 180 dni.

W związku z powyższym Zamawiający modyfikuje wszystkie zapisy SWZ jej załączników, we wszystkie miejsca, gdzie był zapis: „Dostarczony sprzęt musi być fabrycznie nowy, tzn. wyprodukowany **nie wcześniej niż 90 dni przed dniem dostawy**...", wprowadza zapis **„nie wcześniej niż 180 dni"**

Pytanie 35
Kary umowne
W § 7 ust. 1 c i e umowy przewidziano kary umowne związane ze zwłoką w świadczeniu gwarancji:
"c) za zwłokę w w dokonaniu wymiany uszkodzonego urządzenia lub jego elementu w okresie gwarancji - w wysokości 0,1% wartości danego urządzenia, którego dotyczy zwłoka, wyliczonej zgodnie z cenami brutto zawartymi w formularzu cenowym Wykonawcy, za każdy dzień zwłoki licząc od terminu wskazanego zgodnie z § 5 w odniesieniu do Części 1, za wyjątkiem winy Zamawiającego.
e) za zwłokę w usunięciu wady w okresie gwarancji - w wysokości 0,1% wartości danego urządzenia, którego dotyczy zwłoka, wyliczonej zgodnie z cenami brutto zawartymi w formularzu cenowym Wykonawcy, za każdy dzień zwłoki licząc od terminu wskazanego zgodnie z § 5 w odniesieniu do Części 2, za wyjątkiem winy Zamawiającego."
Kary te nie mają racji bytu ze względu na wymagany przez Zamawiającego sposób świadczenia gwarancji - bezpośrednio przez serwis producenta, z możliwością pominięcia Wykonawcy zamówienia przy zgłaszaniu awarii. Może więc dojść do sytuacji, kiedy Zamawiający zgłosi awarię bezpośrednio do serwisu producenta, nie informując Wykonawcy, a następnie - w wyniku niedotrzymania przez producenta terminu wymiany urządzenia lub usunięcia wady - naliczy Wykonawcy kary umowne, mimo że Wykonawca nie wiedział o awarii i nie miał żadnej możliwości przeciwdziałania przekroczeniu terminu.
Systemy obsługowe producentów dają możliwość wskazania Wykonawcy zamówienia jako jednego z administratorów konta Zamawiającego, co umożliwia dostęp do informacji o awariach i bieżącą współpracę z serwisem producenta i Zamawiającym w diagnozowaniu problemu i obsłudze zgłoszenia. Nie gwarantuje to jednak rzeczywistego wpływu na terminowość świadczenia usług przez producenta, która w razie zdarzeń losowych może zostać poważnie naruszona.
Proszę więc o ograniczenie możliwości naliczenia tych kar umownych do sytuacji, kiedy za okoliczności powodujące zwłokę odpowiada Wykonawca - proponuję następującą treść:
"c) za zwłokę w w dokonaniu wymiany uszkodzonego urządzenia lub jego elementu w okresie gwarancji - w wysokości 0,1% wartości danego urządzenia, którego dotyczy zwłoka, wyliczonej zgodnie z cenami brutto zawartymi w formularzu cenowym Wykonawcy, za każdy dzień zwłoki licząc od terminu wskazanego zgodnie z § 5 w odniesieniu do Części 1, wyłącznie w razie winy Wykonawcy.
e) za zwłokę w usunięciu wady w okresie gwarancji - w wysokości 0,1% wartości danego urządzenia, którego dotyczy zwłoka, wyliczonej zgodnie z cenami brutto zawartymi w formularzu cenowym Wykonawcy, za każdy dzień zwłoki licząc od terminu wskazanego zgodnie z § 5 w odniesieniu do Części 2, wyłącznie w razie winy Wykonawcy."

ODPOWIEDŹ:
Zgodnie z par. 7 ust. 1 pkt c) i e) wykonawca odpowiada tylko za zwłokę, która jest zdefiniowana w art. 476 kc. Zgodnie z tym przepisem kara nie dotyczy wypadku, gdy opóźnienie jest następstwem okoliczności, za które wykonawca nie ponosi odpowiedzialności. W tej sytuacji nie jest konieczne dokonywanie zmian w/w par. 7.

Jednocześnie Zamawiający informuje, iż w związku z powyższymi odpowiedziami zmianie ulegają :

- Opisu przedmiotu zamówienia dla części 1 - załącznik nr A do SWZ
- Formularza ofertowego – załącznik nr 1 do SWZ
- Formularza cenowego dla części 1 – załącznik nr 2 do SWZ
- Treści SWZ w zakresach wskazanych w powyższych odpowiedziach na pytania.

Nowe załączniki do SWZ stanowią załączniki do niniejszego pisma.

Zamawiający informuje, że w związku z powyższymi zmianami SWZ zmianie uległy terminy składania i otwarcia ofert, zgodnie z pismem z dnia 15/02/-2022, opublikowanym w dniu 18/02/...2022 r.:

Termin składania ofert zostaje przesunięty z dnia 24-02-2022 r., godz. 10:00 na dzień 18/03/**2022 r., godz.: 10:00.**

Termin otwarcia ofert zostaje przesunięty z dnia 24-02-2022 r., godz. 10:15 na dzień 18/03/**2022 r., godz.: 10:15.**

W związku z powyższym zmianie ulegają zapisy rozdziału 15 SWZ. Punkt. 15.1 SWZ otrzymuje następujące brzmienie: „15.1 Wykonawca pozostaje związany ofertą do dnia: 15/06/**2022 r.**"

PROREKTOR
prof. dr hab. Michał Banaszak

SPECJALISTA
ds zamówień publicznych
mgr Ilona Zerbin