Zakład Emerytalno-Rentowy
Ministerstwa Spraw Wewnętrznych i Administracji

Warszawa, dnia 17 SIE. 2022 r.

Nr sprawy: ZER-ZP-8/2022

Wykonawcy

W związku z zapytaniami zgłoszonymi w trybie w trybie art. 284 ust. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2021 r. poz. 1129 z późn. zm.), zwanej dalej „ustawą Pzp", w sprawie postępowania nr ZER-ZP-8/2022, prowadzonego w trybie podstawowym bez negocjacji, zgodnie z art. 275 pkt 1 ustawy Pzp na: ***Zakup firewall-i ze wsparciem technicznym***, Zamawiający, na podstawie art. 284 ust. 2 i 6 ustawy Pzp, udziela wyjaśnienia treści specyfikacji warunków zamówienia, zwanej dalej „SWZ" oraz zmienia treść Opisu przedmiotu zamówienia.

Jednocześnie Zamawiający informuje, że zgodnie z art. 286 ust. 1 i ust. 7 ustawy Pzp dokonał zmiany treści specyfikacji warunków zamówienia, zwanej dalej „SWZ", zgodnie z treścią niniejszego pisma.

I. Wyjaśnienia treści SWZ

Pytanie nr 1:

„Wymaganie nr 9:
Urządzenie musi posiadać kontrolę zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP.
Pytanie:
Czy zamawiający dopuści rozwiązanie, które nie będzie miało kontroli zawartości dla protokołu IMAP, lecz będzie wykorzystywało bazę reputacji IP w celu ochrony przez spamerami i atakami nie tylko spam w protokołach pocztowych SMTP i POP3?"

Odpowiedź na pytanie nr 1:

Zamawiający podtrzymuje zapisy Opisu przedmiotu zamówienia.

Pytanie nr 2:

„Wymaganie nr 11:
Urządzenie musi posiadać możliwość stworzenia/uruchomienia usługi Web-Proxy.
Pytanie:
Uruchomienie/stworzenie usługi Web Proxy, zakładając, że zamawiający pisał wymaganie świadomie, zmniejsza przepustowość urządzanie czasami nawet do 80%, stąd producenci rozwiązań NGFW nie oferują takiego trybu działania, ponieważ wymaga on zaoferowania przeskalowanego urządzenia. Czy zamawiający zaakceptuje rozwiązanie, które będzie kontrolowało ruchu web w trybie transparentnym dla użytkownika a model proxy będzie uruchamiany tylko dla deszyfracji i kontroli ruchu SSL/TLS?"

Odpowiedź na pytanie nr 2:

Zamawiający podtrzymuje zapisy Opisu przedmiotu zamówienia.

Pytanie nr 3:

„Wymaganie nr 16:
Urządzenie musi zapewniać mechanizmy redundancji w tym możliwość konfiguracji urządzenia w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA) active-active, active-passive, clustering.
Pytanie:
Wymaganie tworzenie wysokiej dostępności (HA) clustering nie jest opcją wysokiej dostępności i zapewnienie ciągłości działania, lecz wymaganiem, które zamawiający nigdy nie użyje. Proszę

o usunięcie wymagania wymogu pracy w trybie clustering i dopuszczenie rozwiązania, które będzie miało możliwość pracy w trybie active-active, active-passive oraz możliwości budowania wysokiej dostępności w oparciu o 4 urządzenia rozmieszczone geograficznie?"

Odpowiedź na pytanie nr 3:

Zamawiający podtrzymuje zapisy Opisu przedmiotu zamówienia.

Pytanie nr 4:

„Wymaganie nr 13:
System IPS musi zapewniać możliwość wykrywania modyfikacji znanych ataków (sygnatury), jak i nowo powstałych, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna).
Pytanie:
Założeniem IPS jest ochrona dla zagrożeń już wykrytych poprzez wykrycie za pomocą sygnatur, dlatego nie jest możliwe wykrywanie nowo powstałych zagrożeń. Producenci realizują wykrywanie nowych zagrożeń i zagrożeń typu 0-day poprzez analizę statyczną kodu, analizę dynamiczną w emulowanych środowiskach systemu operacyjnego i korelację zagrożeń. Proszę o dopuszczeni rozwiązania, które będzie realizowało wykrywanie nowo powstałych zagrożeń, które nie zostały jeszcze dogłębnie opisane poprzez funkcjonalność sandbox."

Odpowiedź na pytanie nr 4:

Zamawiający podtrzymuje zapisy Opisu przedmiotu zamówienia.

Pytanie nr 5:

„Wymaganie nr 10:
System IPS musi zapewniać możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, SSH itp.
Pytanie:
Zamawiający wymaga rozwiązania, które będzie miało możliwość pasywnej detekcji predefiniowanych serwisów w tym szyfrowanej komunikacji SSH, lecz nie bierze pod uwagę analizy najbardziej pocztowych - SMTP IMAP, DNS, którymi pobierane są zagrożenia. Protokół SSH nie jest powszechnie stosowany, używany jest głównie do zarządzania i konfiguracji urządzeń sieciowych w wąskim gronie administratorów sieciowych. Chcąc chronić organizacje przez wyrafinowanymi atakami należy wykonywać szerszą inspekcję. Czy Zamawiający dopuści rozwiązanie, które zamiast możliwość pasywnej detekcji predefiniowanych serwisów w tym SSH, będzie miało możliwość inspekcji http, DNS, FTP, POP3, SMTP MSRPC, SUMRPC, Telnet oraz ochrony serwerów Web przez atakami typu SQL injection, XSS, kontroli zewnętrznych linków i hotlinków?"

Odpowiedź na pytanie nr 5:

Zamawiający podtrzymuje zapisy Opisu przedmiotu zamówienia.

Pytanie nr 6:

„Wymaganie 12:
System IPS musi zapewniać możliwość obrony przed atakami skonstruowanymi tak, aby uniknąć wykrycia przez IPS. W tym celu musi zapewnić możliwość blokowania każdego połączenia, które nosi znamiona manipulacji nr sekwencyjnymi segmentów TCP, be względu do jakiego hosta docelowego kierowane jest to połączenie.
Pytanie:
Czy zamawiający dopuści rozwiązanie, które zamiast zapewnić możliwość blokowania każdego połączenia, które nosi znamiona manipulacji nr sekwencyjnymi segmentów TCP będzie wykrywało anomalię w ruchu DNS, FTP, POP3, SMTP MSRPC, SUMRPC, Telnet oraz wykrywało dodatkowo DGA i tunelowanie w protokole DNS?"

Odpowiedź na pytanie nr 6:
Zamawiający podtrzymuje zapisy Opisu przedmiotu zamówienia.

Pytanie nr 7:
„Pytanie o interfejsy:
Czy zamawiający dopuści urządzenie, które będzie miało porty Rj45 jako wkładki w portach SFP 1Gbps?"

Pytanie nr 8:
„Drugie pytanie o interfejsy:
Czy zamawiający dopuści urządzenie, które będzie posiadać porty 8x GE Rj45 i 8xSFP, 2xSFP+?"

Odpowiedź na pytanie nr 7 i nr 8:
Zamawiający informuje, że dokonał odpowiedniej modyfikacji treści SWZ – **Zmiana nr 1 SWZ**.

II. Zmiany treści SWZ
Zmiana nr 1 SWZ

Obecna treść w Tabeli nr 1 Opisu przedmiotu zamówienia:
„Tabela nr 1. *Minimalne wymagania dla każdego firewalla*

Nazwa	Parametry minimalne
Opis urządzenia	1. Urządzenie musi pełnić rolę ściany ogniowej (firewall) typu statefull inspection i ściany ogniowej firewall-a Next-Generation (NGFW). 2. Urządzenie musi być wyposażone w: a) min. 12 portów 1 Gigabit Ethernet (każdy obsługujący prędkość 10/100/1000BaseT Gigabit Ethernet), b) min. 4 porty 1 GE SFP oraz c) min. 2 porty 10 GE SFP+. lub zamiast pozycji lit. b i c Zamawiający dopuszcza 4 porty pracujące z prędkością 1/10 GE SFP/SFP+ 3. Urządzenie musi być wyposażone w dedykowany port konsoli oraz dedykowany port 1 Gigabit Ethernet do zarządzania MGMT. 4. Urządzanie musi posiadać redundantne wbudowane zasilacze zasilane prądem przemiennym 230V. 5. Urządzenie musi posiadać możliwość montażu w szafie RACK 19". Urządzenie będzie dostarczone wraz z elementami montażowymi do szafy RACK 19". 6. Urządzenie musi mieć wysokość nie większą niż 1U. Urządzenie musi posiadać dysk twardy SSD min. 200 GB do zapisu logów.

Zostaje zmieniona na:
„Tabela nr 1. *Minimalne wymagania dla każdego firewalla*

Nazwa	Parametry minimalne
Opis urządzenia	1. Urządzenie musi pełnić rolę ściany ogniowej (firewall) typu statefull inspection i ściany ogniowej firewall-a Next-Generation (NGFW). 2. Urządzenie musi być wyposażone w: a) min. 12 portów 1 Gigabit Ethernet (każdy obsługujący prędkość 10/100/1000BaseT Gigabit Ethernet), b) min. 4 porty 1 GE SFP oraz c) min. 2 porty 10 GE SFP+. d) zamiast pozycji lit. b i c Zamawiający dopuszcza 4 porty pracujące

	z prędkością 1/10 GE SFP/SFP+ e) lub równoważną konfigurację dla punktów lit. a, b, c, d 3. Urządzenie musi być wyposażone w dedykowany port konsoli oraz dedykowany port 1 Gigabit Ethernet do zarządzania MGMT. 4. Urządzanie musi posiadać redundantne wbudowane zasilacze zasilane prądem przemiennym 230V. 5. Urządzenie musi posiadać możliwość montażu w szafie RACK 19". Urządzenie będzie dostarczone wraz z elementami montażowymi do szafy RACK 19". 6. Urządzenie musi mieć wysokość nie większą niż 1U. 7. Urządzenie musi posiadać dysk twardy SSD min. 200 GB do zapisu logów.

„

Proszę o uwzględnienie powyższego przy sporządzaniu oferty.

ZASTĘPCA DYREKTORA
Zakładu Emerytalno-Rentowego
Ministerstwa Spraw Wewnętrznych i Administracji
Jarosław SOKOŁOWSKI

(data i podpis Kierownika Zamawiającego lub osoby przez niego upoważnionej)