Powiatowe Centrum Zdrowia w Kamiennej Górze Sp. z o.o.

58 - 400 Kamienna Góra ul. Bohaterów Getta 10

tel. 75 744-9036 http://www.pcz.org.pl

fax. 75 744-3103 e-mail: pcz@pcz.org.pl

KRS 0000169608 Wys. kap. zakł. 5 206 000,00 zł

Kamienna Góra, 20.09.2022 r.

WYJAŚNIENIA TREŚCI SWZ

Nazwa postępowania: **Dostawa urządzeń klasy UTM, serwerów, macierzy i oprogramowania dla Powiatowego Centrum Zdrowia w Kamiennej Górze Sp. z o.o.**

Nr referencyjny nadany sprawie przez Zamawiającego: **TP 5/2022**

I. Działając na podstawie art. 284 ust. 2 i 6 oraz art. 286 ust. 1 i 7 Ustawy z dnia 11 września 2019 roku Prawo Zamówień Publicznych (tj. Dz.U. z 2022 r., poz. 1710 z późn. zm. – dalej ustawa Pzp) Zamawiający informuje, że wpłynęły zapytania o następującej treści:

Pytanie nr 1:
Czy Zamawiający dopuści rozwiązanie posiadające 8x GE interfejsów fizycznych zamiast 12x 1000Base-T RJ45 i 4x 1GbE SFP , z których każdy jest w pełni konfigurowalny i nie ma przypisanej roli LAN czy też WAN co pozwoli Zamawiającemu na pełną dowolność w konfiguracji?

Odpowiedź na pytanie nr 1:
Zamawiający dopuszcza rozwiązanie posiadające 8x GE interfejsów fizycznych zamiast 12x 1000Base-T RJ45 i 4x 1GbE SFP.

Pytanie nr 2:
Czy Zamawiający dopuści rozwiązanie, które zamiast 10tys. sygnatur IPS będzie ich miało 2450 lecz w ramach dostawy Oferent dostarczy ochronę przed sieciami Botnet wraz z Cloud-Sandboxem, które nie wpłyną na finalną ofertę?

Odpowiedź na pytanie nr 2:
Zamawiający dopuszcza rozwiązanie, które zamiast 10 tys. sygnatur IPS będzie ich miało 2450 w połączeniu z dostawą ochrony przed sieciami Botnet wraz z Cloud-Sandboxem.

Pytanie nr 3:
Zamawiający w załączniku nr 1.5. do Formularza oferty nie doprecyzował ilości maszyn wirtualnych, które chce zabezpieczyć. Jeśli zamawiający chciałby zabezpieczyć nielimitowaną ilość maszyn wirtualnych, proszę o podanie ilości fizycznych hostów na których pracują maszyny.

Odpowiedź na pytanie nr 3:
Zamawiający chce zabezpieczyć 6 maszyn wirtualnych.

Pytanie nr 4:
Zamawiający w punkcie 11 załącznika nr 1.5. do Formularza oferty wymaga przywracania pojedynczych elementów domeny Active Directory. Czy zamawiający dopuszcza rozwiązanie umożliwiające przywracanie pełnej konfiguracji domeny?

Odpowiedź na pytanie nr 4:
Zamawiający dopuszcza rozwiązanie umożliwiające przywracanie pełnej konfiguracji domeny.

Pytanie nr 5:
Dla części nr 4 w załączniku 1.4 podają państwo dla pozycji pierwszej: Licencja Windows Server standard 2022 zgodne z licencjonowaniem Microsoft dla ilości CPU w ilości 3 szt. Windows Server 2022 licencjonowany jest w modelu na Rdzeń + CAL, więc aby dobrać odpowiednią ilość potrzebnych licencji

konieczna jest informacja o ilości procesorów i rdzeni posiadanych przez serwer do którego przeznaczone są dane licencje, Niestety w opisie przedmiotu zamówienia ani w innych miejscach nie ma podanej wskazanej informacji. Czy w związku z tym Zamawiający może podać informacje o ilości procesorów i ich rdzeni? ewentualnie czy Zamawiającemu chodzi o dostawę licencji Windows Server 2022 Standard 16 core w ilości 3 szt.?

Odpowiedź na pytanie nr 5:
Zamawiającemu chodzi o dostawę licencji Windows Server 2022 Standard 16 core w ilości 3 szt.

Pytanie nr 6:
Część 1 - Urządzenia klasy UTM
Zamawiający w pkt 5 OPZ określił przepustowość na poziomie 3Gb/s jednak przez oczywistą omyłkę pisarską nie zostało opisane o przepustowość jakiego modułu bezpieczeństwa chodzi Zamawiającemu. W związku z powyższym prosimy Zamawiającego o poprawę oczywistej omyłki pisarskiej na prawidłowe brzmienie:
Przepustowość IPS (pliki HTTP 1 MB) – 3 Gb/s
Znając specyfikę Państwa szpitala informujemy, że zapis w pierwotnym brzmieniu da możliwość zaoferowania rozwiązania które nie będzie w stanie obsłużyć ruchu całego szpitala, a w konsekwencji narazi to Zamawiającego na przestój placówki medycznej.

Odpowiedź na pytanie nr 6:
Zamawiający dokonuje poprawy oczywistej omyłki pisarskiej polegającej na nieuwzględnieniu faktu, że w punkcie tym chodzi o przepustowość modelu IPS.

W związku z powyższym, Zamawiający dokonuje zmiany treści SWZ w zakresie Załącznika nr 1.1. do Formularza oferty. Punkt 5 tego Załącznika przyjmuje następujące brzmienie:

5.	Minimalna przepustowość wymagana IPS (pliki HTTP 1 MB) – 3 Gb/s	3Gb/s

Pytanie nr 7:
Część 1 - Urządzenia klasy UTM
Czy Zamawiający dopuści rozwiązanie równoważne, czołowego, europejskiego producenta, jednego z liderów cyberbezpieczeństwa rozwiązań brzegowych w Europie spełniającego poniższe wymagania?

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe.
Dla elementów systemu bezpieczeństwa wykonawca musi zapewnić wszystkie poniższe funkcjonalności:
• Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.
• System realizujący funkcję Firewall musi dysponować minimum 8 interfejsami miedzianymi Ethernet 10/100/1000.
• System realizujący funkcję Firewall musi dysponować minimum 4 interfejsami optycznymi 1 GbE (SFP).
• Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
• W zakresie Firewall'a obsługa nie mniej niż 1 000 000 jednoczesnych połączeń oraz 50 000 nowych połączeń na sekundę.
• System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 200 GB do celów logowania i raportowania.
• System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. W przypadku kiedy system nie posiada dysku lub nie pozwala na podłączenie zewnętrznych nośników, musi być dostarczony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej.
• W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:
o Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
o Ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, HTTP, FTP, HTTPS). System AV musi umożliwiać skanowanie AV dla plików typu: rar, zip.
o Poufność danych - IPSec VPN oraz SSL VPN
o Ochrona przed atakami - Intrusion Prevention System [IPS/IDS]
o Kontrola stron Internetowych – Web Filter [WF]
o Kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3)
o Kontrola pasma oraz ruchu [QoS i Traffic shaping]
o Kontrola aplikacji oraz rozpoznawanie ruchu P2P
o Analiza ruchu szyfrowanego protokołem SSL
• Wydajność systemu Firewall minimum 15 Gbps

• Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus minimum 2 Gbps
• Wydajność ochrony przed atakami (IPS) minimum 8 Gbps
• Wydajność VPN IPSec, nie mniej niż 2 Gbps
• W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:
o Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site
o Producent oferowanego rozwiązania VPN powinien dostarczać klienta VPN współpracującego z proponowanym rozwiązaniem
o Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
o Praca w topologii Hub and Spoke oraz Mesh
o Obsługa ssl vpn w trybach portal oraz tunel
• Rozwiązanie musi zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP.
• Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
• Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety).
• Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ.
• Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
• Ochrona IPS musi opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków musi zawierać co najmniej 1000 wpisów. Dodatkowo musi być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS.
• Funkcja kontroli aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
• Baza filtra WWW pogrupowana w minimum 50 kategorii tematycznych. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
• Automatyczne ściąganie sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
• System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
o Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
o Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
o Haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych
o Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory
• W zakresie realizowanych funkcjonalności systemu raportowania i przeglądania logów, wymagane jest nie mniej niż:
o Posiadanie predefiniowanych raportów dla ruchu WWW, modułu IPS, skanera antywirusowego i antyspamowego
o Generowanie co najmniej 25 różnych typów raportów
• System raportowania i przeglądania logów wbudowany w system bezpieczeństwa nie może wymagać dodatkowej licencji do swojego działania
• Urządzenie musi:
-posiadać certyfikat Common Criteria EAL
-posiadać certyfikat ICSA Labs dla funkcji: VPN IPSec lub znajdować się na liście produktów kryptograficznych zatwierdzonych przez Radę UE
• Elementy systemu muszą mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
• Wymaga się, aby dostawa obejmowała również:
o Minimum 36-miesięczną gwarancję producentów na dostarczone elementy systemu liczoną od dnia zakończenia wdrożenia całego systemu.
o Licencje dla wszystkich funkcji bezpieczeństwa producentów na okres minimum 36 miesięcy liczoną od dnia zakończenia wdrożenia całego systemu.

Odpowiedź na pytanie nr 7:
Zamawiający dopuszcza rozwiązanie określone w pytaniu.

Pytanie nr 8:
Dotyczy załącznik nr 1.5 do Formularza oferty
Proszę o doprecyzowanie, ile fizycznych procesorów posiadają serwery, które mają zostać objęte oprogramowaniem do backupu. Informacja ta jest niezbędna do rzetelnego oszacowania ceny oprogramowania.

Odpowiedź na pytanie nr 8:
Dwa serwery, które mają zostać objęte oprogramowaniem do backupu będą posiadać po jednym procesorze o minimalnych parametrach 24Core/48Thread.

Pytanie nr 9:
Dotyczy załącznik 1.3 do Formularza oferty punkt 4. Typ dysków.
Zamawiający w załączniku nr 1.2 do Formularza oferty w punkcie 6 dla każdego serwera określił po 8 dysków SSD. W załączniku nr 1.5 do Formularza oferty zamawiający określił parametry oprogramowania do backupu. Czy w związku z tym zamawiający zaplanował macierz z załącznika 1.3 do Formularza oferty jako macierz przeznaczoną do backupu. Jeśli macierz miałaby być przeznaczona do backupu to czy zamawiający zgodzi się na zmianę typu dysków w punkcie 4 z SSD na HDD. Zmiana rodzaju dysków dla macierzy przeznaczonej do backupu pozwoli na zmniejszenie szacunkowej wartości przedmiotu zamówienia.

Odpowiedź na pytanie nr 9:
Tak, Zamawiający zgodzi się na zmianę typu dysków w punkcie 4 z SSD na HDD.

Pytanie nr 10:
Dotyczy załącznik 1.1 do Formularza oferty punkt 43 Rozwiązanie musi umożliwić stanową inspekcję opartą na analizie komunikacji sieciowej, oraz analizie warstwy 7 modelu ISO/OSI w celu kontroli przepływu.
Proszę o doprecyzowanie czy kontrola przepływu ma obejmować również analizę ruchu pod kątem sygnatur znanych zagrożeń oraz wektorów ataku. W skrócie czy zamawiający ma na myśli rozwiązanie o potocznej nazwie ATP Advanced Threat Protection.

Odpowiedź na pytanie nr 10:
Tak, Zamawiający ma na myśli rozwiązanie określone w pytaniu.

Pytanie nr 11:
Dotyczy załącznik 1.1 do Formularza oferty punkt 95 Ilość jednoczesnych połączeń VPN nie może zostać ograniczona licencją.
Czy dotyczy to również wielokrotnych połączeń tego samego użytkownika?

Odpowiedź na pytanie nr 11:
Tak, dotyczy to również wielokrotnych połączeń tego samego użytkownika.

II. Zamawiający informuje, że na podstawie art. 286 ust. 1 i 7 ustawy Pzp dokonuje zmiany treści SWZ dotyczącej poprawy oczywistych omyłek pisarskich w następujący sposób:

1. W pkt 12.1. Tomu I SWZ ppkt 3 przyjmuje następujące brzmienie:

   3) Oświadczenie Wykonawcy o niepodleganiu wykluczenia z postępowania *o udzielenie zamówienia, zgodne z treścią* ***Załącznika nr 2 do Tomu I SWZ (IDW)***

2. W Załączniku nr 2 do Tomu I SWZ zapis (załącznik nr 1a) przyjmuje brzmienie (załącznik nr 2a).

III. Zamawiający informuje, że pytania i odpowiedzi na nie oraz zmiany stają się integralną częścią specyfikacji warunków zamówienia i będą wiążące przy składaniu ofert. Pozostałe warunki nie ulegają zmianie.

PREZES ZARZĄDU
Barbara Kosak