Sygn. akt: KIO 2475/23 KIO 2478/23

WYROK

z dnia 11 września 2023 r.

Krajowa Izba Odwoławcza - w składzie:

Przewodniczący:Marek Bienias

Członkowie: Anna Chudzik

Elżbieta Dobrenko

Protokolant: **Wiktoria Ceyrowska**

po rozpoznaniu na rozprawie w dniu 6 września 2023 r. w Warszawie odwołań wniesionych do Prezesa Krajowej Izby Odwoławczej w dniu 21 sierpnia 2023 r. przez:

A.wykonawców wspólnie ubiegających się o udzielenie zamówienia: **T4B sp. z o.o. z siedzibą w Warszawie, Atende S.A. z siedzibą w Warszawie (sygn. akt KIO 2475/23)**,

B.wykonawcę **Konwerga Sp. z o.o. z siedzibą w Poznaniu (sygn. akt KIO 2478/23)**,

w postępowaniu prowadzonym przez Zamawiającego: **Centrum Informatyki Resortu Finansów w Radomiu,**

przy udziale:

A.wykonawcy **Innergo Systems Sp. z o.o.z siedzibą w Warszawie,** zgłaszającego przystąpienie do postępowania odwoławczego po stronie Zamawiającego w sprawach o sygn. akt KIO 2475/23 i sygn. akt KIO 2478/23,

B.wykonawców wspólnie ubiegających się o udzielenie zamówienia: **T4B sp. z o.o. z siedzibą w Warszawie, Atende S.A. z siedzibą w Warszawie,** zgłaszających przystąpienie do postępowania odwoławczego po stronie Zamawiającego w sprawie o sygn. akt KIO 2478/23,

C.wykonawcy **S&T Poland Sp. z o.o. z siedzibą w Warszawie,** zgłaszającego przystąpienie do postępowania odwoławczego po stronie Zamawiającego w sprawie o sygn. akt KIO 2478/23,

orzeka:

I.W sprawie KIO 2475/23

1.Oddala odwołanie.

2.Kosztami postępowania obciąża wykonawców wspólnie ubiegających się o udzielenie zamówienia: **T4B sp. z o.o. z siedzibą w Warszawie, Atende S.A. z siedzibą w Warszawie** i

2.1.Zalicza w poczet kosztów postępowania odwoławczego kwotę 15 000 zł 00 gr (słownie: piętnaście tysięcy złotych zero groszy) uiszczoną przez Odwołującego, tytułem wpisu od odwołania.

II.W sprawie KIO 2478/23

1.Oddala odwołanie.

2.Kosztami postępowania obciąża wykonawcę **Konwerga sp. z o.o. z siedzibą w Poznaniu** i

2.1.Zalicza w poczet kosztów postępowania odwoławczego kwotę 15 000 zł 00 gr (słownie: piętnaście tysięcy złotych zero groszy) uiszczoną przez Odwołującego, tytułem wpisu od odwołania.

Stosownie do art. 579 ust. 1 i 580 ust. 1 i 2 ustawy z dnia 11 września 2019r. - Prawo Zamówień Publicznych (Dz. U. z 2023 r. poz. 1605) na niniejszy wyrok - w terminie 14 dni od dnia jego doręczenia - przysługuje skarga za pośrednictwem Prezesa Krajowej Izby Odwoławczej do **Sądu Okręgowego w Warszawie.**

Przewodniczący:……..……..

Członkowie: ……

……

Sygn. akt: KIO 2475/23 KIO 2478/23

U z a s a d n i e n i e

Zamawiający - Centrum Informatyki Resortu Finansów w Radomiu- prowadzi postępowanie o udzielenie zamówienia publicznego, prowadzonego w trybie przetargu nieograniczonego, pn: „Dostawa i wdrożenie Systemu Wi-Fi na przejściach granicznych wraz z Centralnym Systemem Zarządzania", numer referencyjny postępowania: PN/71/22/GDYP. Ogłoszenie o zamówieniu zostało opublikowane w Dzienniku Urzędowym UE w dniu 04 stycznia 2023 r. pod numerem: 2023/S 003-006714.

I.KIO 2475/23:

W dniu 21 sierpnia 2023 r. wykonawcy wspólnie ubiegający się o udzielenie zamówienia: **T4B sp. z o.o. z siedzibą w Warszawie, Atende S.A. z siedzibą w Warszawie** wnieśli odwołanie zarzucając naruszenie przepisów przez Zamawiającego:

(1) **naruszenie art. 226 ust. 1 pkt 5 pzp w zw. z art. 16 pzp** poprzez zaniechania odrzucenia oferty wykonawcy Innergo Systems Sp. z o.o. ul. Odrowąża 15, 03-310 Warszawa; w sytuacji gdy treść przedmiotowej oferty jest niezgodna z warunkami zamówienia, w odniesieniu do:

a) przełącznika dostępowego zewnętrznego:

i. z uwagi na brak funkcjonalności prywatnego VLAN-u na dzień składania ofert, a uwzględnienie zmiany, ktora zaszła w tym zakresie po złożeniu i otwarciu ofert, co prowadzi do naruszenia zasady uczciwej konkurencji i równego traktowania Wykonawców;

ii. z uwagi na brak funkcjonalności zdalnego port mirroring – RSPAN;

b) przełącznika dostępowego wewnętrznego z uwagi na brak funkcjonalności zdalnego port mirroring – RSPAN;

c) zaoferowanego oprogramowania z uwagi na brak zaoferowania oprogramowania zapewniającego realizację wymagań przedmiotu zamowienia (tj. co najmniej: Aruba ClearPass Access, Aruba ClearPass OnGuard, Aruba ClearPass Device Insight);

(2) **naruszenie art. 239 ust. 1 i 2 pzp**, poprzez dokonanie wyboru oferty wykonawcy Innergo Systems Sp. z o.o. ul. Odrowąża 15, 03-310 Warszawa, ktora nie jest najkorzystniejszą ofertą w świetle kryteriów oceny ofert określonych w dokumentach zamówienia, tj. oferty nieprzedstawiającej najkorzystniejszego stosunku jakości do ceny zamówienia, gdyż najkorzystniejszą ofertą jest oferta Odwołującego, a oferta Innergo Systems Sp. z o.o. winna zostać odrzucona.

Odwołujący wniósł o nakazanie Zamawiającemu:

(1) uwzględnienie odwołania,

(2) nakazanie Zamawiającemu:

a) unieważnienia czynności wyboru najkorzystniejszej oferty;

b) powtórzenia czynności wyboru najkorzystniejszej oferty;

c) odrzucenia oferty Innergo Systems Sp. z o.o.;
(3) przeprowadzenie dowodow wskazanych w odwołaniu na poparcie okoliczności faktycznych i prawnych wskazanych w odwołaniu;
(4) zasądzenie na rzecz Odwołującego kosztow postępowania.
Odwołujący wskazał, że:
UZASADNIENIE
1. W dniu 10 sierpnia 2023 r. Zamawiający poinformował uczestników postępowania o wyborze jako najkorzystniejszej oferty Wykonawcy – Innergo Systems Sp. z o.o. W ocenie Odwołującego treść wybranej oferty jest niezgodna z warunkami zamówienia, stosownie do poniższego uzasadnienia.
2. **ZARZUTY DOTYCZĄCE ZAOFEROWANEGO PRZEŁĄCZNIKA DOSTĘPOWEGO ZEWNĘTRZNEGO.**
3. W pkt 1.1.załącznika nr 1 do OPZ (III Tomu OPZ) – Specyfikacja techniczna Urządzeń (strona 1),Zamawiający wymagał:

5. **Funkcjonalność prywatnego VLAN-u**
6. Wymagania szczegołowe dla urządzeń typu przełącznik zewnętrzny sprecyzowane zostały w pkt 1.1.6 przedmiotowego załącznika (strony 8 – 10), gdzie w pkt 5 tych wymagań lit. h) (strona 9 Załącznika nr 1 do OPZ) znalazło się następujące wymaganie (oznaczone czerwoną czcionką):
8. Zgodnie z treścią złożonego przez wykonawcę Innergo Systems Sp. z o.o. Formularza „Formularz_Zestawienie_Glownych_Elementow_Systemu_WiFi_04-04-2023_09.06.06”,
stanowiącego załącznik do formularza ofertowego, wynika, że wskazany wykonawca zaoferował w swojej ofercie jako przełącznik zewnętrzny urządzenie Aruba 4100i, ktore to urządzenie występuje w poz. 3 we wszystkich Oddziałach Celnych objętych przedmiotem zamówienia (oznaczone czerwoną czcionką w przykładowym Oddziale Celnym w Korczowej):
10. Tym samym urządzenie Aruba 4100i jako przełącznik zewnętrzny winno – na dzień złożenia oferty - spełniać wszystkie wymagania wskazane w pkt 1.1.6 Załącznika nr 1 do OPZ, w tym opisany w nb. 7 niniejszego odwołania wymog pkt 5 lit h), a więc „*funkcjonalność prywatnego VLAN-u, czyli możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. porty izolowane) z pozostawieniem możliwości komunikacji z portem nadrzędnym*.”
11. Biorąc pod uwagę treść oficjalnej dokumentacji producenta do urządzeń Aruba 4100i, 6000, 6100 i 6200, aktualnej na dzień składania ofert, tj. 4 kwietnia 2023 r., dostępnej pod adresem internetowym hpps://www.arubanetworks.com/techdocs/AOS CX/10.11/HTML/l2_bridging_4100i-6000-6100-6200/Content/Chp_PVLAN/PVLAN.htm, wymagana przez Zamawiającego funkcjonalność prywatnego VLAN-u (ang. PrivateVLAN) realizowana jest jedynie przez urządzenie serii Aruba 6200, a nie Aruba 4100i:
14. **Dowód:** dokumentacja producenta do urządzeń Aruba 4100i, 6000, 6100 i 6200 (wer. ang.),
dostępna pod adresem internetowym wskazanym w nb. 11 Załącznik nr 5
15. tłumaczenie na język polski dokumentacji producenta do urządzeń Aruba 4100i, 6000, 6100 i 6200, dostępna pod adresem internetowym wskazanym w nb. 11 Załącznik nr 5
16. Zgodnie ze specyfikacją techniczną dla urządzenia Aruba 4100i dostępną na stronie producenta hpps://www.arubanetworks.com/assets/ds/DS_4100iSwitchSeries.pdfurządzenie to nie posiada wsparcia dla funkcjonalności prywatnego VLAN-u. Brak jest bowiem w specyfikacji technicznej informacji, by urządzenie Aruba 4100i obsługiwało funkcjonalność prywatnego VLAN-u. Podobna sytuacja zachodzi w odniesieniu do urządzenia Aruba 6100, które również nie wspiera funkcji prywatnego VLAN-u i w odniesieniu do którego również brak jest stosowych informacji w specyfikacji technicznej tego modelu przełącznika:
hpps://www.arubanetworks.com/assets/ds/DS_6100Series.pdf
17. Jeżeli funkcjonalność prywatnego VLAN-u jest obsługiwana przez dany przełącznik, producent zaznacza ten fakt w specyfikacjach technicznych danego modelu serii przełączników, poprzez przykładową adnotację: “*Private VLAN (PVLAN) provides traffic isolaIon between users on the sameVLAN; typically a switch port can only communicate with other ports in the same community and/or an uplink port, regardless of VLAN ID or desInaIon MAC address. This extends network security by restricIng peer-peer communicaIon to prevent variety of malicious aRacks*.” (tłumaczenie: „*Prywatna sieć VLAN (PVLAN) zapewnia izolację ruchu między użytkownikami w tej samej sieci VLAN; zwykle port przełącznika może komunikować się tylko z innymi portami w tej samej społeczności i/lub portem uplink, niezależnie od identyfikatora sieci VLAN lub docelowego adresu MAC. Rozszerza to bezpieczeństwo sieci, ograniczając komunikację typu peer-to-peer, aby zapobiec rożnym złośliwym atakom*”, tak jak to ma miejsce w przypadku innych przełączników, nieoferowanych Innergo Systems Sp. z o.o. w charakterze przełącznika dostępowego zewnętrznego, jak np. model Aruba 6200 czy 6300, ktore wspierają funkcjonalność prywatnego VLAN-u:
hpps://www.arubanetworks.com/assets/ds/DS_6200Series.pdf – strona 8
hpps://www.arubanetworks.com/assets/ds/DS_6300Series.pdf – strona 9
18. **Dowód:** specyfikacja techniczna dla urządzenia Aruba 4100i (wer. ang.), dostępna na stronie producenta pod adresem internetowym wskazanym w nb. 16 Załącznik nr 6
19. tłumaczenie specyfikacji technicznej dla urządzenia Aruba 4100i (wer. pol.) Załącznik nr 6
20. specyfikacja techniczna dla urządzenia Aruba 6100 (wer. ang.), dostępna na stronie
producenta pod adresem internetowym wskazanym w nb. 16 Załącznik nr 7
21. tłumaczenie specyfikacji technicznej dla urządzenia Aruba 6100 (wer. pol.) Załącznik nr 7
22. specyfikacja techniczna dla urządzenia Aruba 6200 (wer. ang.), dostępna na stronie
producenta pod adresem internetowym wskazanym w nb. 17 Załącznik nr 8
23. tłumaczenie specyfikacji technicznej dla urządzenia Aruba 6200 (wer. pol.) Załącznik nr 8
24. specyfikacja techniczna dla urządzenia Aruba 6300 (wer. ang.), dostępna na stronie
producenta pod adresem internetowym wskazanym w nb. 17 Załącznik nr 9
25. tłumaczenie specyfikacji technicznej dla urządzenia Aruba 6300 (wer. pol.) Załącznik nr 9
26. Powyżej wskazana dokumentacja wskazuje na stan istniejący na dzień składania ofert, potwierdzając, że zaoferowane urządzenie (przełącznik Aruba 4100i) nie spełniało wymagań OPZ. Odwołujący jest świadomy, że Zamawiający (lub firma

Innergo Systems Sp. z o.o.) będzie wskazywać, że aktualnie urządzenie to posiada funkcjonalność prywatnego VLAN-u. Jednak funkcjonalność ta dodana została wraz z wersją oprogramowania 10.12.0006, ktora została wydana dopiero w dniu 31 maja 2023 r. (a zatem już po złożeniu ofert w niniejszym postępowaniu).

27. Odwołujący wskazuje na porównanie funkcjonalności z wykorzystaniem narzędzia producenta (znajdującego się na stronie *hRps://feature-navigator.arubanetworks.com/)*. Dokonane porównanie pomiędzy kolejnymi, bezpośrednio po sobie występującymi wersjami – tj. wersją 10.11.1010 (wydaną w dniu 28 marca 2023 r.) a wersją 10.12.0006 (wydaną w dniu 31 maja 2023 r.) jednoznacznie wskazuje, że urządzenie - przełącznik Aruba 4100i pracując pod kontrolą oprogramowania 10.11.1010 nie posiadało funkcjonalności prywatnego VLAN-u (znak „X" w tabeli przy pozycji „Private VLAN i podpozycjach związanych z Private VLAN") a funkcjonalność ta została dodana w oprogramowaniu w wersji 10.12.0006 (znak "√" w tabeli przy pozycji „Private VLAN i podpozycjach związanych z Private VLAN").

28. **Dowód:** Porównanie funkcjonalności oprogramowania w wersji 10.11.1010 z wersją 10.12.0006 (wer. ang) Załącznik nr 10

29. Tłumaczenie porównania funkcjonalności oprogramowania w wersji 10.11.1010 z wersją 10.12.0006 Załącznik nr 10

30. Rownież sama dokumentacja wersji oprogramowania 10.12.0006 („AOS-CX 10.12.0006 Release Notes 4100i Switch Series") potwierdza następujące okoliczności:

31. - oprogramowanie to zostało wydane w dniu 31 maja 2023 r.:

34. - w sekcji „Enhancements for 4100i Switches in AOS-CX 10.12.0006" (tłumaczenie: "Udoskonalenia przełączników 4100i w AOS-CX 10.12.0006") znalazł się zapis:

37. Dokumentacja oprogramowania we wcześniejszej (bezpośrednio poprzedniej) wersji 10.11.1010, potwierdza, że wydana została ona w dniu 28 marca 2023 r. (a zatem była to wersja oprogramowania aktualna na dzień składania oferty).

38. **Dowód:** Dokument „AOS-CX 10.12.0006 Release Notes 4100i Switch Series" (wer. ang) Załącznik nr 11

39. Tłumaczenie dokumentu „AOS-CX 10.12.0006 Release Notes 4100i Switch Series" (wer. pol) Załącznik nr 11

40. Dokument „AOS-CX 10.11.1010 Release Notes 4100i Switch Series" (wer. ang) Załącznik nr 12

41. Tłumaczenie dokumentu „ AOS-CX 10.11.1010 Release Notes 4100i Switch Series" (wer. pol) Załącznik nr 12

42. Powyższe okoliczności potwierdzają, że firma Innergo Systems Sp. z o.o. złożyła ofertę wskazując urządzenie, które nie spełniało wymagań Zamawiającego, co winno prowadzić do jej odrzucenia zgodnie z art. 226 ust. 1 pkt 5 pzp. Okoliczności tej nie może zmienić fakt, że zaoferowane urządzenie „nabyło" wymaganą funkcjonalność w toku postępowania przetargowego. Dopuszczenie do sytuacji, w której Wykonawca składa ofertę, która nie spełnia wymagań Zamawiającego, a następnie poprzez szczęśliwy dla niego zbieg okoliczności oferta staje się spełniającą wymagania już po terminie składania ofert i ich otwarciu byłaby naruszeniem zasady równego traktowania Wykonawców, zawartej w art. 16 pzp. Inni, racjonalnie działający Wykonawcy nie mieli podstaw do wskazania w ofercie urządzenia – przełącznika Aruba 4000i (jako niespełniającego wymagań OPZ), co prowadzi do zaburzenia zasad uczciwej konkurencji oraz równego traktowania wykonawców. Nie może zostać uznana za uczciwą konkurencja, w której dochodzi do zmiany parametrów zaoferowanego urządzenia po terminie składania ofert i dzięki tej zmianie oferta, która na dzień jej złożenia winna zostać odrzucona staje się ofertą najkorzystniejszą.

43. Odwołujący wskazuje na brzmienie art. 107 pzp, stanowiącego, że „Jeżeli zamawiający żąda złożenia przedmiotowych środków dowodowych, wykonawca składa je wraz z ofertą", co oznacza, że weryfikacja poprawności merytorycznej złożonej oferty oraz potwierdzeniu oferowanych właściwości przedmiotu zamówienia winna odbywać się na moment złożenia oferty.

44. Powyższe stanowisko potwierdza wyrok Krajowej Izby Odwoławczej z 8 marca 2023 r., sygn. akt KIO 482/23: *I, o ile ustawodawca dopuścił możliwość uzupełnienia takich przedmiotowych środków dowodowych,* ***to uzupełnione dokumenty muszą potwierdzać stan na moment złożenia oferty****. Przyjęcie odmiennej interpretacji, jak chciałaby Zamawiający i Przystępujący w analizowanym stanie faktycznym, stałoby w oczywistej sprzeczności z art. 16 ustawy Pzp i wynikającej z niej zasady równego traktowania wykonawców. Dopuszczenie, że wykonawca biorący udział w postępowaniu o udzielenie zamówienia publicznego oferują produkt, którego parametrów nie może potwierdzić na moment złożenia oferty z uwagi na brak stosownej certyfikacji, natomiast może brak taki usunąć przez swego rodzaju „konwalidację" na podstawie art. 107 ust. 2 ustawy Pzp i uzyskanie wymaganych dokumentów po terminie składania ofert byłoby naruszeniem zasady równego traktowania wykonawców.* ***Izba podkreśla, że każdy z wykonawców jest zobowiązany złożyć ofertę zgodną z postanowieniami SWZ oraz potwierdzić zgodność oferowanych produktów w sposób wymagany przez zamawiającego na moment złożenia oferty****. (…)*"

45. Analogiczna sytuacja występuje w zakresie podmiotowych środków dowodowych – nie budzi bowiem wątpliwości, że *„postawione przez zamawiającego warunki udziału w postępowaniu wykonawcy obowiązani są spełniać przez cały czas trwania postępowania,* ***już od wyznaczonego przez zamawiającego dnia składania ofert****."* (tak m.in. wyrok Krajowej Izby Odwoławczej z dnia 11 stycznia 2022 r. **KIO 3753/21**), analogicznie: *„Postawione przez zamawiającego warunki udziału w postępowaniu wykonawca ma spełniać przez cały czas trwania postępowania, tj.* ***od wyznaczonego dnia składania ofert****."* (Wyrok Krajowej Izby Odwoławczej z dnia 23 lutego 2023 r. **KIO 314/23**), także: *„****Warunki udziału w postępowaniu muszą być spełnione na dzień złożenia oferty****, a stan ich spełnienia musi trwać przez całe postępowanie."* (Wyrok Krajowej Izby Odwoławczej z dnia 23 maja 2022 r. **KIO 1200/22**).

46. Sytuacja w niniejszym postępowaniu wykazuje analogię do stanu faktycznego będącego podstawą rozstrzygnięcia we wskazanym wyżej wyroku z dnia 23 maja 2022 r. KIO 1200/22, gdzie Wykonawca na dzień złożenia oferty nie spełniał warunku udziału w postępowaniu (w zakresie ochrony ubezpieczeniowej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia na wymaganą przez zamawiającego sumę gwarancyjną), a do spełnienia tego warunku doszło już po otwarciu ofert, w toku ich badania i oceny. Jak stwierdzono w uzasadnieniu *„Z powyższego wynika zatem, iż Przystępujący był ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia na wymaganą w SWZ sumę gwarancyjną dopiero w dniu 8 kwietnia 2022 r., tj. 1,5 miesiąca po upływie terminu składania ofert (22 lutego 2022 r.). Jednocześnie zauważyć należy, iż wykonawca ALKOM wraz z ofertą złożył oświadczenie JEDZ stanowiące dowód potwierdzający brak podstaw wykluczenia i spełnianie warunków udziału w postępowaniu na dzień składania ofert".*

47. W niniejszym postępowaniu dochodzi do analogicznej sytuacji, gdyż zawarty w ofercie produkt (przełącznik Aruba 4100i) zaczął spełniać wymagania przetargowe dopiero 31 maja 2023 r., **a zatem dopiero po 8 tygodniach od daty składania ofert**. Trudno zatem byłoby uzasadnić sytuację, w której zamówienia nie może uzyskać Wykonawca, co do którego w toku postępowania zmieniły się okoliczności podmiotowe, zaś może uzyskać Wykonawca, co do oferty którego w toku postępowania zmieniły się okoliczności przedmiotowe.

48. Sytuacja powyższa wskazuje również, że gdyby Zamawiający dokonał oceny ofert przed dniem 31 maja 2023 r. to bez żadnych wątpliwości byłby zobowiązany do odrzucenia oferty jako niezgodnej z warunkami zamówienia. Tym samym dochodzi do zaburzenia zasady uczciwej konkurencji i równego traktowania Wykonawców – gdyż przyjęcie, że Zamawiający nie naruszył wskazanych przez Odwołującego przepisów prowadziłoby do wniosku, że możliwą jest sytuacja, w której wynik postępowania zmienia się w zależności od momentu dokonania wyboru oferty najkorzystniejszej.

49. Inną możliwością jest przyjęcie, że wykonawca Innergo Systems Sp. z o.o. dysponował nieznaną innym wykonawcom wiedzą co do tego, że w wyniku przyszłych działań producenta przełącznik Aruba 4100i uzyska wymaganą przez

zamawiającego funkcjonalność i dzięki tej wiedzy zdecydował się go zaoferować, co pozwoliło mu uzyskać przewagę konkurencyjną. Jeśli faktycznie doszło do takiej sytuacji, to (abstrahując od wskazanej powyżej okoliczności niespełniania wymagań zamówienia na dzień złożenia oferty) również jest to nie do pogodzenia z zasadami uczciwej konkurencji. Zgodnie z powszechnie dostępnymi informacjami pochodzącymi od producenta, na dzień składania ofert przełącznik Aruba 4100i nie spełniał wymagań zamówienia w postępowaniu i jego zaoferowanie prowadziło do złożenia oferty niezgodnej z warunkami zamówienia, a tym samym podlegającej odrzuceniu.

50. **Funkcjonalność zdalnego port mirroring – RSPAN**

51. Wymagania szczegółowe dla urządzeń typu przełącznik zewnętrzny sprecyzowane zostały w pkt 1.1.6 przedmiotowego załącznika (strony 8 – 10), gdzie w pkt 7 tych wymagań lit. d) (strona 9 Załącznika nr 1 do OPZ) znalazło się następujące wymaganie (oznaczone czerwoną czcionką):

53. W ramach opisanego wyżej wymagania, Zamawiający oczekuje funkcjonalności przesyłania ruchu przez dedykowany VLAN w warstwie drugiej **do innego urządzenia** [z wymagania Zamawiającego –

„(...) *i przesyłaniu ich* ***do zdalnego urządzenia monitorującego****, przez dedykowaną sieć VLAN (****zdalny port mirroring*** *– RSPAN lub rownoważny)*']. Natomiast zgodnie z dokumentacją producenta urządzenie Aruba 4100i wspiera mechanizm określany przez Arubę jako port-mirroring (inaczej SPAN lub Local SPAN) i jest to replikowanie ruchu z jednego interfejsu na inny interfejs w ramach tego samego przełącznika, a nie do zdalnego urządzenia . Rożnice między wymaganiem Zamawiającego a funkcjonalnością oferowaną przez urządzenie Aruba 4100i prezentuje poniższe zestawienie:

54. **Oferowane rozwiązanie Wymagania Zamawiającego**

55. **Local SPAN (w urządzeniu Aruba 4100i: Mirroring albo Port Mirroring) RSPAN**

56. obserwacja ruchu na określonym porcie przełącznika polegającą na replikowaniu ruchu z jednego portu przełącznika na inny port w **ramach tego samego przełącznika**

zdalna obserwacja ruchu na określonym porcie przełącznika, polegającą na kopiowaniu ruchu z jednego portu przełącznika i **przesyłaniu ich do zdalnego urządzenia monitorującego**, poprzez dedykowaną sieć VLAN (sieć w warstwie drugiej modelu ISO/OSI, ruch może

przechodzić przez wiele przełączników, które przekazują sobie ten VLAN)

57. Fakt braku funkcjonalności RSPAN i oferowanie w urządzeniu Aruba 4100i funkcjonalności Port Mirroring potwierdzają zapisy Monitoring Guide producenta urządzenia (rozdział Mirroring, strona 39), dostępny na stronie hpps://www.arubanetworks.com/techdocs/AOSCX/ 10.11/PDF/monitoring_4100i-6000-6100.pdf zawierające stwierdzenie:

„*The traffic replicated*

using mirroring can be sent to a separate interface on the same switch as the traffic source for

analysis or inspeclon." (tłumaczenie: „*Ruch zreplikowany przy użyciu kopii lustrzanej może zostać wysłany do oddzielnego interfejsu na tym samym przełączniku, co źrodło ruchu w celu analizy lub inspekcji.*"

58. Brak funkcji RSPAN i posiadanie niespełniającej wymagań Zamawiającego funkcjonalności Port Mirroring potwierdza również dostępne na stronie internetowej producenta urządzeń Aruba

(hpps://feature-navigator.arubanetworks.com/) narzędzie feature-navigator służące do sprawdzania, jakie funkcjonalności są wspierane przez poszczegolne urządzenia. Wyświetlając

funkcjonalności dla urządzenia Aruba 4100i na liście dostępnych i obsługiwanych przez to urządzenie funkcjonalności (w sekcji Feature -> Port), brak jest funkcjonalności RSPAN, dostępna jest natomiast funkcjonalność SPAN i Port Mirroring:

60. **Dowód:**

Monitoring Guide dla urządzeń 4100i, 6000, 6100 (wer. ang), dostępna na stronie producenta pod adresem internetowym wskazanym w nb.57 Załącznik nr 13

61. Tłumaczenie Monitoring Guide dla urządzeń 4100i, 6000, 6100 (wer. pol) Załącznik nr 13

62. Efekt zastosowanie narzędzia feature-navigator dla urządzenia Aruba 4100i, dostępnego

na stronie producenta pod adresem internetowym wskazanym w nb.58. (wer. ang) Załącznik nr 14

63. Tłumaczenie efektu zastosowanie narzędzia feature-navigator dla urządzenia Aruba

4100i Załącznik nr 14

64. Powyższe potwierdza, że także w tym zakresie zaoferowane urządzenie Aruba 4100i jest niezgodne z warunkami zamówienia, co winno skutkować odrzuceniem oferty.

65. **ZARZUTY DOTYCZĄCE ZAOFEROWANEGO PRZEŁĄCZNIKA DOSTĘPOWEGO WEWNĘTRZNEGO.**

66. W pkt 1.1.załącznika nr 1 do OPZ (III Tomu OPZ) – Specyfikacja techniczna Urządzeń (strona 1), Zamawiający wymagał:

68. **Funkcjonalność zdalnego port mirroring– RSPAN**

69. Wymagania szczegółowe dla urządzeń typu przełącznik wewnętrzny sprecyzowane zostały w pkt 1.1.5 przedmiotowego załącznika (strony 6 – 8), gdzie w pkt 7 tych wymagań lit. d) (strona 7 Załącznika nr 1 do OPZ) znalazło się następujące wymaganie (oznaczone czerwoną czcionką):

71. Zgodnie z treścią złożonego przez wykonawcę Innergo Systems Sp. z o.o. Formularza „Formularz_Zestawienie_Glownych_Elementow_Systemu_WiFi_04-04-2023_09.06.06", stanowiącego załącznik do formularza ofertowego, wynika, że wskazany wykonawca zaoferował w swojej ofercie jako przełącznik wewnętrzny urządzenie Aruba 6300M, ktore to urządzenie występuje w poz. 3 w zestawieniu głównych elementów CSZ w Centrum Informatyki Resortu Finansów w Radomiu objętych przedmiotem zamówienia (oznaczone czerwoną czcionką):

73. W ramach opisanego wyżej wymagania, Zamawiający oczekuje funkcjonalności przesyłania ruchu przez dedykowany VLAN**w warstwie drugiej** do innego urządzenia [z wymagania Zamawiającego – *„przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, przez dedykowaną sieć VLAN (****zdalny port mirroring*** *– RSPAN lub równoważny)*']. Natomiast zgodnie z dokumentacją producenta urządzenie Aruba 6300M wspiera analogicznie jak urządzenie Aruba 4100i mechanizm określany przez Arubę jako port-mirroring (inaczej SPAN lub Local SPAN) i jest to replikowanie ruchu z jednego interfejsu na inny interfejs w ramach tego samego przełącznika, a nie do zdalnego urządzenia moitorującego, a ponadto wspiera mechanizm określany przez Arubę jako Remote mirroring endpoint, czyli mechanizm, w którym ruch kopiowany do zdalnego odbiorcy przesyłany jest przez dedykowany tunel L3 i w związku wymaga, aby odbiorca tego ruchu

(urządzenie, do którego ruch jest kierowany) miał możliwość skonfigurowania tego tunelu. Jest to inny mechanizm niż mechanizm przesyłania ruchu poprzez dedykowaną sieć VLAN jakim jest RSPAN, gdyż w przypadku mechanizmu RSPAN po stornie urządzenia odbierającego żadna
dodatkowa konfiguracja tunelu nie jest wymagana. Różnice między wymaganiem Zamawiającego a funkcjonalnością oferowaną przez urządzenie Aruba 63100M prezentuje poniższe zestawienie:

74. **Oferowane rozwiązanie Wymagania Zamawiającego**

75. **Local SPAN (w urządzeniu Aruba 6300M: Mirroring albo Port Mirroring) ERSPAN (w urządzeniu Aruba 6300M: ERSPAN albo remote mirroring endpoint) RSPAN**

76. obserwacja ruchu na określonym porcie przełącznika polegającą na replikowaniu ruchu z
jednego portu przełącznika na inny port w **ramach tego samego przełącznika** zdalna obserwacja ruchu na określonym porcie przełącznika, polegającą na kopiowaniu ruchu z jednego portu przełącznika i przesyłaniu ich **do zdalnego urządzenia monitorującego** poprzez przez **dedykowany tunel warstwy trzeciej modelu ISO/OSI (nie dedykowana sieć VLAN, która pracuje w warstwie drugiej modelu ISO/OSI**) zdalna obserwacja ruchu na określonym porcie przełącznika, polegającą na kopiowaniu ruchu z jednego portu przełącznika i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez **dedykowaną sieć VLAN (sieć w warstwie drugiej modelu ISO/OSI**, ruch może przechodzić przez wiele przełączników, które przekazują sobie ten VLAN)

77. Fakt braku funkcjonalności RSPAN i oferowanie w urządzeniu Aruba 6300M funkcjonalności Port Mirroring potwierdzają zapisy Monitoring Guide producenta urządzenia (rozdział Mirroring, strona
72), dostępny na stronie hpps://www.arubanetworks.com/techdocs/AOSCX/ 10.11/PDF/monitoring_6300-6400.pdf zawierające stwierdzenie: „The traffic replicated using
mirroring can be sent to a separate interface on the same switch as the traffic source for analysis or inspec{on. Such a collec{on of interfaces and se|ngs is called a mirror session." (tłumaczenie: „*Ruch zreplikowany przy użyciu kopii lustrzanej może zostać wysłany do oddzielnego interfejsu na tym samym przełączniku, co źrodło ruchu w celu analizy lub inspekcji. Taki zbior interfejsow i ustawień nazywany jest sesją lustrzaną.*"

78. Natomiast fakt braku funkcjonalności RSPAN i oferowanie w urządzeniu Aruba 6300M funkcjonalności Remote mirroring endpoint potwierdzają zapisy wyżej wskazanego MonitoringGuide producenta urządzenia (rozdział Mirroring, strona 80), zawierające stwierdzenie:

81. Brak funkcji RSPAN i posiadanie niespełniającej wymagań Zamawiającego funkcjonalności Port Mirroring oraz Remote mirroring endpoint potwierdza również dostępne na stronie internetowej producenta urządzeń Aruba (hpps://feature-navigator.arubanetworks.com/) narzędzie featurenavigator służące do sprawdzania, jakie funkcjonalności są wspierane przez poszczególne urządzenia. Wyświetlając funkcjonalności dla urządzenia Aruba 4100i oraz Aruba 6300M na liście dostępnych i obsługiwanych przez te urządzenia funkcjonalności (w sekcji Feature -> Port), brak jest funkcjonalności RSPAN, dostępna jest natomiast funkcjonalność Port Mirroring i Remote mirroring endpoint (nieobsługiwana przez urządzenie Aruba 4100i):

83. **Dowód:** Monitoring Guide dla urządzeń 6300, 6400 (wer. ang), dostępna na stronie
producenta pod adresem internetowym wskazanym w nb.77 Załącznik nr 15

84. Tłumaczenie Monitoring Guide dla urządzeń 6300, 6400 (wer. pol) Załącznik nr 15

85. Efekt zastosowanie narzędzia feature-navigator dla urządzenia Aruba 4100i oraz 6300M, dostępnego na stronie producenta pod adresem internetowym wskazanym w nb.81. (wer. ang)
Załącznik nr 16

86. Tłumaczenie efektu zastosowanie narzędzia feature-navigator dla urządzenia Aruba 4100i oraz 6300M Załącznik nr 16

87. Zatem – jak widać z wykazanych powyżej okoliczności faktycznych – zaoferowane przez Innergo Systems Sp. z o.o. urządzenia są niezgodne z warunkami zamówienia.

88. Pismem z dnia 5 czerwca 2023 r. Odwołujący zwrócił Zamawiającemu uwagę m.in. na nieprawidłowości w ofercie Innergo Systems Sp. z o.o. objęte niniejszym odwołaniem. W reakcji na przedmiotowe pismo Zamawiający w dniu 16 czerwca 2023 r. wystosował do firmy Hewlep Packard Enterprise Polska sp. z o.o. pytania obejmujące następujące zagadnienia:

1) Czy Oprogramowanie Aruba ClearPass zapewnia funkcjonalność analizy stanu stacji końcowych w aspekcie podłączających się do sieci (posture), profilowania urządzeń oraz monitoringu behawioralnego. Jeśli ww. funkcjonalność aktywowana jest konkretną licencją lub dodatkiem programowym, prosimy o informacje o nazwie produktowej takiego elementu.

2) Czy przełącznik Aruba 4100i oraz przełącznik Aruba 6300M umożliwiają zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (zdalny port mirroring – RSPAN lub równoważny).

89. W odpowiedzi na powyższe zapytanie, Zamawiający otrzymał odpowiedź pismem z dnia 21 czerwca 2023 r., w którym stwierdzono, że:

1. Oprogramowanie Aruba ClearPass zapewnia funkcjonalność analizy stanu stacji końcowych w aspekcie podłączających się do sieci, profilowania urządzeń za pomocą licencji Aruba ClearPass Access, Aruba ClearPass OnGuard. Analiza behawioralna w ramach rozwiązania Aruba ClearPass jest realizowana za pomocą Aruba ClearPass Device Insight.

2. Rozwiązanie oparte o przełączniki Aruba 4100i oraz Aruba 6300M umożliwia realizację funkcjonalności pozwalającej na zdalną obserwację ruchu z określonego portu, polegającą na
kopiowaniu pojawiających się na nim ramek i ich odbieraniu na zdalnym urządzeniu monitorującym.

90. **Dowód:** Pismo Odwołującego z dnia 5 czerwca 2023 r. Załącznik nr 17

91. Zapytanie Zamawiającego z dnia 16 czerwca 2023 r. Załącznik nr 18

92. Odpowiedź z dnia 21 czerwca 2023 r. Załącznik nr 19

93. Analiza pytania i udzielonej odpowiedzi wskazuje, że zarzuty zawarte w odwołaniu oraz w piśmie Odwołującego z dnia 05 czerwca 2023 r. pozostają aktualne, co pokazuje zestawienie pytań i odpowiedzi (istotne kwestie zaznaczono kolorami):

94. **Pytanie Zamawiającego Odpowiedź**

95. Czy Oprogramowanie Aruba ClearPass zapewnia funkcjonalność analizy stanu stacji końcowych w aspekcie podłączających się do sieci (posture), profilowania urządzeń oraz monitoringu behawioralnego. Jeśli ww. funkcjonalność aktywowana jest konkretną licencją lub dodatkiem programowym, prosimy o informacje o nazwie produktowej takiego elementu. Oprogramowanie Aruba ClearPass zapewnia funkcjonalność analizy stanu stacji końcowych w
aspekcie podłączających się do sieci, profilowania urządzeń za pomocą licencji Aruba ClearPass Access, Aruba ClearPass OnGuard Analiza behawioralna w ramach rozwiązania Aruba ClearPass jest realizowana za pomocą Aruba ClearPass Device Insight.

96. Czy przełącznik Aruba 4100i oraz przełącznik Aruba 6300M umożliwiają zdalną obserwację
ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć Rozwiązanie oparte o przełączniki Aruba 4100i oraz Aruba 6300M

umożliwia realizację funkcjonalności pozwalającej na zdalną obserwację ruchu z określonego portu, polegającą na kopiowaniu pojawiających się na VLAN (zdalny port mirroring – RSPAN lubrównoważny). nim ramek i ich odbieraniu na zdalnym urządzeniu monitorującym.

97. W odniesieniu do pytania pierwszego należy zauważyć, że Zamawiający zdał pytanie wyłącznie o funkcjonalności oprogramowania, a nie o funkcjonalność urządzenia Aruba 4100i. W istocie więc, to że oprogramowanie Aruba zapewnia określone możliwości nie oznacza to, że wymagane możliwości zapewnia oferowane urządzenie. Wystarczy bowiem, że w urządzeniu brak jest wymaganych funkcji technicznych.

98. Istotnym jest jednak, że zadane pytanie (i tym samym odpowiedź) dotyczą wyłącznie oprogramowania Aruba ClearPass, a nie zarzucanego przez Odwołującego braku funkcjonalności prywatnego VLAN-u. Pytanie (i odpowiedź) nie obejmują więc całego zarzutu stawianego oferowanemu urządzeniu Aruba 4100i.

99. W odniesieniu do pytania drugiego należy zwrócić uwagę na różnice między zapytaniem i odpowiedzi, oznaczone kolorem czerwonym. W pierwszej kolejności zwraca uwagę początek udzielonej odpowiedzi, w której autor odnosi się nie do możliwości przełączników, lecz **rozwiązania opartego o przełączniki**, które jest pojęciem zdecydowanie szerszym. Tymczasem wymagania wskazane w Odwołaniu (i piśmie Odwołującego z dnia 05 sierpnia 2023 r.) odnoszą się do przełączników, a nie do rozwiązania opartego o przełączniki.

100. Druga różnica polega na braku w odpowiedzi finalnej części zapytania Zamawiającego, tj. stwierdzenia, że przedmiotowa funkcjonalność jest realizowana „poprzez dedykowaną sieć VLAN (zdalny port mirroring – RSPAN lub równoważny).” Tymczasem brak realizacji wymaganych przez Zamawiającego funkcji właśnie poprzez dedykowaną sieć VLAN (zdalny port mirroring – RSPAN lub równoważny) stanowi istotę stawianych ofercie Innergo Systems Sp. z o.o. zarzutów.

101. Dodatkowo należy wskazać, że jakkolwiek literalnie odpowiedź udzielona została udzielona w imieniu Hawlett Packard Enterprise Polska sp. z o.o., to utor pisma w żaden sposob nie wykazał swojego umocowania do reprezentowania tej firmy. Uznać więc należy, że odpowiedź nie została udzielona w imieniu Hawlett Packard Enterprise Polska sp. z o.o.

102. **ZARZUTY DOTYCZĄCE ZAOFEROWANEGO OPROGRAMOWANIA**

103. **Brak zaoferowania Aruba ClearPass Access, Aruba ClearPass OnGuard, Aruba ClearPass Device Insight**

104. Mając na uwadze treść odpowiedzi na pierwsze pytanie Zamawiającego i wskazane w niej rodzaje oprogramowania (nb. 95), które w ocenie autora odpowiedzi są konieczne do realizowania funkcji oprogramowania Aruba ClearPass (Aruba ClearPass Access, Aruba ClearPass OnGuard, Aruba ClearPass Device Insight), należy zauważyć, że w złożonym przez wykonawcę Innergo Systems Sp. z o.o. Formularzu „Formularz_Zestawienie_Glownych_Elementow_Systemu_WiFi_04-04- 2023_09.06.06”, stanowiącym załącznik do formularza ofertowego, brak jest informacji, by Innergo Systems Sp. z o.o. zaoferował którąkolwiek z wymienionych licencji, mimo że Zamawiający wymagał podania nazwy oprogramowania. Jedynie w pkt I. ppkt 5 Formularza, zawierającego Zestawienie głównych elementów CSZ w Centrum Informatyki Resortu Finansów w Radomiu (oznaczanecczcionką czerwoną) wykonawca wskazał ogólnie na grupę programów Aruba Clearpass, lecz bez konkretyzacji jakie oprogramowanie konkretnie oferuje:

106. Jeśli zatem przyznać rację autorowi odpowiedzi, że wykonawca winien zaoferować oprogramowania Aruba ClearPass Access, Aruba ClearPass OnGuard, Aruba ClearPass Device Insight, wykonawca nie wskazał w ofercie, że takie oprogramowanie oferuje, a zatem treść przedmiotowej oferty jest niezgodna z warunkami zamówienia. Zwrócić także należy uwagę, że w polu „Szacowana liczba licencji” wykonawca wskazał liczbę 2 – co uniemożliwia zaoferowanie wskazanych wyżej co najmniej 3 produktów.

Zamawiający w pisemnej odpowiedzi na odwołanie z dnia 4 września 2023 r. wnosił o oddalenie odwołania w całości.

Zamawiający wskazał, że:

Stan Faktyczny.

1) Zamawiający prowadzi postępowanie o udzielenie zamówienia w trybie przetargu nieograniczonego.

Przedmiotem zamówienia jest dostawa i wdrożenie Systemu Wi-Fi na przejściach granicznych wraz z Centralnym Systemem Zarządzania, (numer referencyjny postępowania: PN/71/22/GDYP).

W zakresie zamówienia podstawowego przedmiotem zamówienia jest wykonanie dostaw i usług na rzecz Zamawiającego w zakresie wdrożenia Systemu Wi-Fi na przejściach granicznych dla 24 lokalizacji wraz z Centralnym Systemem Zarządzania, spełniającego wymagania OPZ, stanowiącego TOM III SWZ. Celem zamówienia jest zbudowaniem

jednolitego Systemu. Mając na uwadze, że powstanie jednolity, spójny, homogeniczny system informatyczny ze strukturą hierarchiczną i możliwością zarządzania wszystkimi lokalizacjami (przejścia graniczne) z poziomu CIRF konieczne jest zapewnienie na każdym etapie spójności i jednolitości rozwiązań.
2) Postępowanie wszczęto w dniu 30.12.2022 r. poprzez przekazanie ogłoszenia o zamówieniu Urzędowi Publikacji Unii Europejskiej, które opublikowane zostało w Dz. Urz. UE: 2023/S 003-006714 w dniu 04.01.2023 r.
3) Termin składania ofert upłynął w dniu 4.04.2023 r. Do upływu tego terminu wpłynęło 5 ofert.
4) W dniu 10.08.2023 r. Zamawiający opublikował oraz przesłał Wykonawcom informację o wyborze najkorzystniejszej oferty za którą została uznana oferty wykonawcy Innegro.
5) W dniu 21.08.2023 r. Odwołujący złożył odwołanie.

Uzasadnienie stanowiska Zamawiającego w zakresie zarzutu dot. przełącznika dostępowego zewnętrznego (funkcjonalność prywatny VLAN).

Zamawiający stoi na stanowisku, że zgłoszony zarzut dotyczący funkcjonalności w zakresie prywatnego VLAN jest chybiony, co oznacza, że podlega on oddaleniu.
Przystępując do jego omówienia, wyjaśnić należy, że pomiędzy Stronami nie ma sporu co do treści wymagania opisanego w Załączniku nr 1do OPZ w pkt 1.1.6 w ppkt 5 lit. h) (str. 9), dotyczącego urządzenia typu przełącznik zewnętrzny, jak również co do tego, że wykonawca Innegro zaoferował przełącznik zewnętrzny producenta Aruba Model 4100i.

Dowód:

- treści wymagania opisanego w Załączniku nr 1 do OPZ w pkt 1.1.6 w ppkt 5 lit. h) (str. 9), dotycząca urządzenia typu przełącznik zewnętrzny, w dokumentacji Postępowania,
- treści oferty wykonawcy Innergo zawarta w Formularzu „Zestawienie głównych elementów Systemu Wi-Fi" (Formularz 2.2.), w dokumentacji Postępowania.

Osią sporu w zakresie postawionego zarzutu jest to, czy zaoferowane urządzenie spełniało wymagania Zamawiającego opisane w Załączniku nr 1 do OPZ w pkt 1.1.6 w ppkt 5 lit. h) dotyczące prywatnego VLAN-u w chwili złożenia oferty przez Przystępującego, tj. w dniu 4.04.2023 r. (dzień, w którym upływał termin składania ofert).
Na gruncie niniejszego Postępowania, należy podkreślić, że nie budzi wątpliwości fakt, że oferowane przez wykonawców rozwiązania już w chwili złożenia oferty musiały spełniać wymagania Zamawiającego postawione w SWZ. Bezsporne jest także stwierdzenie, że nie można było uznać za spełniającą wymagania SWZ oferty, w ramach której Wykonawca zaoferował rozwiązanie, które dopiero na etapie oceny ofert lub po zawarciu umowy uzyskuje cechy lub funkcjonalności zgodne z wymaganiami Zamawiającego.

Nie budzi żadnych wątpliwości Zamawiającego, że zaoferowany przez wykonawcę Innegro przełącznik zewnętrzny producenta Aruba model 4100i już w chwili złożenia oferty, tj. w dniu 4.04.2023 r. spełniał wymagania Zamawiającego opisane w Załączniku nr 1 do OPZ w pkt 1.1.6 w ppkt 5 lit. h) w zakresie możliwość realizacji funkcjonalności prywatnego VLAN. Powyższą okoliczność Zamawiający ustalił na etapie oceny ofert na podstawie informacji zawartych na stronach internetowych producenta Aruba. Zamawiający zwraca uwagę, że kwestionowana przez Odwołującego **funkcjonalność dostępna była już wersji oprogramowania 10.11, która została wydana (release day) w dniu 28.03.2023 r.,** a więc jeszcze przed złożeniem oferty przez Innergo i przed upływem terminu składania ofert.

Dowód: - AOS-CX 10.11.1010 Release Notes 4100i Switch Series, str. 5

W toku badania i oceny ofert Zamawiający ustalił, że informacja o obsłudze prywatnego VLAN (PVLAN) znajduje się w rozdziale „Security" (tłumaczenie: bezpieczeństwo) na stronie 6 specyfikacji przełącznika 4100i dostępnej pod adresem
Tłumaczenie: Prywatna sieć VLAN (PVLAN) zapewnia izolację ruchu między użytkowników w tej samej sieci VLAN; zazwyczaj port przełącznika może tylko komunikować się tylko z innymi portami w tej samej społeczności i/lub portem uplink, niezależnie od VLAN ID lub docelowego adresu MAC. Rozszerza to bezpieczeństwo sieci poprzez ograniczenie komunikacji peer-peer, aby zapobiec różnorodnym złośliwym atakom.

Dowód: ARUBA CX 4100i SWITCH SERIES – data sheet, str. 6, dostępny pod adresem: https://www.arubanetworks.com/assets/ds/DS_4100iSwitchSeries.pdf

Powyższe ustalenie dotyczące wersji 10.11 oprogramowania dla przełącznika 4100i potwierdzają także informacje zawarte na stronie producenta Aruba dostępne pod adresem: 10000/Content/Chp_PVLAN/PVLAN.htm , gdzie wprost wskazano, że ww. wersja oprogramowania 10.11 umożliwia obsługę PVLAN.
Tłumaczenie fragmentu powyżej zaznaczonego na żółto: Funkcja prywatnej sieci VLAN (PVLAN) partycjonuje sieć VLAN, grupując wiele zestawów portów, które wymagają izolacji ruchu warstwy 2, w niezależne poddomeny rozgłoszeniowe. Sieć VLAN, która jest partycjonowana, jest określana jako podstawowa sieć VLAN, a poddomeny wyodrębnione z tej podstawowej sieci VLAN są określane jako podrzędne sieci VLAN. Te podrzędne sieci VLAN są również zwykłymi sieciami VLAN, składającymi się z podgrupy portów oryginalnej sieci VLAN i identyfikowanymi przez unikalny identyfikator VLAN ID. W zależności od zapewnionego poziomu izolacji, podrzędne sieci VLAN mogą być dalej klasyfikowane jako izolowane i społecznościowe sieci VLAN. Ruch w domenie podrzędnej będzie widoczny wewnątrz domeny PVLAN, a gdy ruch opuści domenę PVLAN, przejdzie tylko do podstawowej sieci VLAN.

Seria przełącznika	Maksymalna ilość instancji podstawowego VLAN	Maksymalna ilość instancji podrzędnego VLAN
4100i	32	8

Dowód:- informacje zawarte na stronie internetowej producenta Aruba dostępnej pod adresem: 9300-10000/Content/Chp_PVLAN/PVLAN.htm

Producent Aruba w powyżej przywołanym dokumencie wyjaśnia, że prywatny VLAN (PVLAN) składa się z instancji podstawowych i podrzędnych VLAN. Natomiast zaoferowany przez Innergo przełącznik 4100i obsługuje 32 VLAN podstawowe i 8 VLAN podrzędne **W ocenie Zamawiającego, tak opisana konfiguracja VLAN potwierdza, że przełącznik 4100i posiada funkcjonalność prywatnego VLAN.**
Tym samym chybiony jest argument Odwołującego zawarty w pkt 26 odwołania, w którym wskazano, że „funkcjonalność ta, dodana została wraz z wersją oprogramowania 10.12.0006, która została wydana dopiero w dniu 31 maja 2023 r. (a zatem już po złożeniu ofert w Postępowaniu)".
Powyższemu ustaleniu wprost przeczy powyżej przywołana dokumentacja zamieszczona na stronach internetowych producenta Aruba. Oznacza to, że zaoferowane urządzenie wcale nie nabyło wymaganej funkcjonalności w toku prowadzonego Postępowania, a posiadało ją na moment składania ofert. Biorąc pod uwagę powyższe ustalenia brak jest podstaw do uznania, że oferta Innergo nie spełnia wymagania określonego w Załączniku nr 1 do OPZ w pkt 1.1.6 w ppkt 5 lit. h).
Jedynie dodatkowo należy wskazać, że zgodnie z postanowieniami SWZ TOM I IDW pkt 15.17 wykonawca ubiegający się o udzielenie zamówienia, zobowiązany był złożyć ofertę, którą stanowił:

1) wypełniony Formularz „Oferta" (Formularz 2.1.),
2) wypełniony Formularz „Zestawienie głównych elementów Systemu Wi-Fi" (Formularz 2.2.)
- zwany dalej „Zestawieniem elementów", który został przygotowany przez Zamawiającego i załączony do SWZ. W treści wzoru „Zestawieniem elementów" Zamawiający w zakresie urządzenia wymagał podania danych takich danych jak: „Nazwa urządzenia (Producent, model)".

Dowód: - treść SWZ TOM I IDW w pkt 15.17, w dokumentacji Postępowania,
- wzór Formularza „Zestawienie głównych elementów Systemu Wi-Fi" (Formularz 2.2.),
w dokumentacji Postępowania.

Powołana treść SWZ prowadzi do wniosku, że Zamawiający nie wymagał podania przez wykonawcę danych dotyczących wersji oprogramowania. Rezygnacja z podania powyższych informacji jest uzasadniona tym, że Zamawiający, z uwagi na długi okres realizacji zamówienia przewidywał, że przed odbiorem końcowym i tak konieczne będzie dokonanie aktualizacji oprogramowania na przełącznikach,. Powyższy wymóg Zamawiający ustanowił postanowieniami SWZ w Tom III OPZ w rozdziale VIII w pkt 13)*Wykonawca zobowiązany będzie przed podpisaniem Protokołu Odbioru ostatniej lokalizacji do aktualizacji oprogramowania układowego (firmware) wszystkich dostarczonych i uruchomionych Urządzeń w każdej lokalizacji oraz dostarczonego środowiska programowego do najnowszej wspieranej wersji zalecanej przez producenta Rozwiązania. Brak wykonania aktualizacji, o której mowa w zdaniu poprzednim skutkować będzie brakiem odbioru przez Zamawiającego ostatniej lokalizacji oraz traktowane będzie jako zwłoka Wykonawcy w terminie wdrożenia i uruchomienia tej lokalizacji.*

Dowód: - treść SWZ TOM III OPZ w rozdziale VIII w pkt 13) na str. 9, w dokumentacji Postępowania.

Mając na uwadze powyższe ustalenia przyjąć należy, że brak było jakiegokolwiek uzasadnienia, aby wykonawcy na etapie składania ofert podawali wersję oprogramowania dla zaoferowanych
w postępowaniu przełączników. Zamawiający dokonując badania i oceny oferty wykonawcy Innergo w aspekcie zaoferowanego przełącznika zewnętrznego ustalił, że w złożonej ofercie wykonawca ten podał wszystkie dane wymagane przez Zamawiającego. Wykonawca podał wszystkie wymagane treścią SWZ dane, tj. „Zestawienie głównych elementów Systemu Wi-Fi", tj. nazwę urządzenia (Przełącznik zewnętrzny), producenta (Aruba) oraz model (4100i). Brak jest zatem podstaw aby kwestionować szczegółowość Formularza „Zestawienie głównych elementów Systemu Wi-Fi" (Formularz 2.2.), co nieudolnie próbuje podważać Odwołujący.

Dowód: - treść Formularza „Zestawienie głównych elementów Systemu Wi-Fi" (Formularz 2.2.)
złożonego przez wykonawcę Innerga, w dokumentacji Postępowania.

W konsekwencji stwierdzić należy, że zarzut naruszenia przez Zamawiającego art. 226 ust. 1 pkt 5 ustawy Pzp, zgłoszony przez Odwołującego, jest niezasadny i podlega oddaleniu.

Uzasadnienie stanowiska Zamawiającego w zakresie zarzutu dot. przełącznika dostępowego zewnętrznego z uwagi na brak funkcjonalności zdalnego port mirroring – RSPAN - nie spełnia wymagania „zdalności".

Zamawiający stoi na stanowisku, że zarzut dotyczący funkcjonalności zdalnego port mirroring – RSPAN – nie spełnia wymagania „zdalności" - w przełączniku zewnętrznym jest chybiony, co oznacza, że podlega on oddaleniu.

Przede wszystkim zauważenia wymaga, że Strony są zgodne co do ustaleń stanu faktycznego
w zakresie brzmienia wymagania dotyczącego funkcjonalności związanej z zarządzaniem i monitorowaniem opisanej w Załączniku nr 1 do OPZ w pkt 1.1.6 w ppkt 7 lit. d) dla przełącznika
zewnętrznego, o treści:
„d) implementacja mechanizmu SPAN PORT lub analogiczna funkcjonalność; przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (zdalny port mirroring – RSPAN lub równoważny)".

Dowód: - treść wymagania opisanego w Załączniku nr 1do OPZ w pkt 1.1.6 w ppkt 7 lit. d) (str. 9), dotyczącego urządzenia typu przełącznik zewnętrzny, w dokumentacji Postępowania.

Analizę zacytowanego wymagania należy rozpocząć od tego, że Zamawiający wyraźnie i wprost opisał swoje wymagania w tym zakresie precyzując, że *przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN* Tym samym z zamieszczonego opisu jednoznacznie wynika na osiągnięciu jakiej funkcjonalności, względem opisanych przełączników, Zamawiającemu zależało**. Na kanwie powyższego logicznym i w pełni uzasadnionym jest stwierdzenie, że określenia wskazujące na konkretne rozwiązania, takie jak: zdalny port mirroring, RSPAN - podane w nawiasie - należało traktować jako przykładowe rozwiązania. Za przyjęciem takiej tezy przemawia to, że Zamawiający dopuścił rozwiązania równoważne, bowiem posłużył się określeniem „lub równoważne". Takie ukształtowanie wymagań pozwalało wykonawcom w złożonych ofertach bazować nie tylko na rozwiązaniu zdalny port mirroring, czy też RSPAN, ale wykorzystać rozwiązania wobec nich równoważne.**

W toku badania i oceny ofert Zamawiający w dniu 16.06.2023 r. zwrócił się do producenta Aruba
o wyjaśnienie czy: *Czy przełącznik Aruba 4100i oraz przełącznik Aruba 6300M umożliwiają zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (zdalny port mirroring – RSPAN lub równoważny).*

W odpowiedzi na przedmiotowe zapytanie producent w dniu 21.06.2023 r. potwierdził, że zaoferowany przełącznik 4100i posiada wymaganą w Załączniku nr do OPZ funkcjonalność:*umożliwia realizację funkcjonalności pozwalającej na **zdalną** obserwację ruchu z określonego portu, polegającą na kopiowaniu pojawiających się na nim ramek i ich odbieraniu na zdalnym urządzeniu monitorującym*.

Dowód: - pismo z dnia 16.06.2023 r., znak: CIRF.DZ1.272.88.2022.GDYP.32, w aktach Postępowania,
- pismo HPE Aruba Networking z dnia 21.06.2023 r., w dokumentacji Postępowania.

Wyłącznie na marginesie Zamawiający wskazuje, że nie sposób zgodzić się z twierdzeniami Odwołującego, jakoby treścią SWZ w ramach prowadzonego Postępowania ograniczył zastosowane rozwiązania wyłącznie do RSPAN. Tego rodzaju twierdzenia Odwołującego nie znajdują odzwierciedlenia w wymaganiach OPZ, w szczególności w brzemieniu wymagania dotyczącego funkcjonalności związanej z zarządzaniem i monitorowaniem opisanej w Załączniku nr 1 do OPZ w pkt 1.1.6 w ppkt 7 lit. d) dla przełącznika zewnętrznego. Odwołujący dokonując interpretacji wymagań Zamawiającego wydaje się nie traktować ich jako całości, a skupia się na treści podanej przez Zamawiającego w nawiasie, którą należy traktować jako pomocniczą, służebną względem głównego trzonu wymagania, które stanowiło jego opis.

Podsumowując argumentację przedstawioną wyżej, stwierdzić należy, że zarzut zgłoszony przez Odwołującego jest niezasadny i podlega oddaleniu.

Uzasadnienie stanowiska Zamawiającego w zakresie zarzutu dot. przełącznika dostępowego wewnętrznego z uwagi na brak funkcjonalności zdalnego port mirroring – RSPAN – brak dedykowanej sieci VLAN.

Zamawiający stoi na stanowisku, że zarzut dotyczący funkcjonalności zdalnego port mirroring – RSPAN – brak dedykowanej sieci VLAN - w przełączniku wewnętrznym jest chybiony, co oznacza, że podlega on oddaleniu.

Przede wszystkim zauważenia wymaga, że Strony są zgodne co do ustaleń stanu faktycznego
w zakresie brzmienia wymagania dotyczącego funkcjonalności związanej z zarządzaniem i monitorowaniem opisanej w

Załączniku nr 1 do OPZ w pkt 1.1.5 w ppkt 7 lit. d) dla przełącznika
wewnętrznego, o treści:
„d) implementacja mechanizmu SPAN PORT lub analogiczna funkcjonalność; przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (zdalny port mirroring – RSPAN lub równoważny)".

Dowód: - treści wymagania opisanego w Załączniku nr 1 do OPZ w pkt 1.1.5 w ppkt 7 lit. d) (str. 7), dotyczącego urządzenia typu przełącznik wewnętrzny, w dokumentacji Postępowania.

Analizę zacytowanego wymagania należy rozpocząć od tego, że Zamawiający wyraźnie i wprost opisał swoje wymagania w tym zakresie precyzując, że *przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN* Tym samym z zamieszczonego opisu jednoznacznie wynika na osiągnięciu jakiej funkcjonalności, względem opisanych przełączników, Zamawiającemu zależało. **Na kanwie powyższego logicznym i w pełni uzasadnionym jest stwierdzenie, że określenia wskazujące na konkretne rozwiązania, takie jak: zdalny port mirroring, RSPAN - podane w nawiasie - należało traktować jako przykładowe rozwiązania. Za przyjęciem takiej tezy przemawia to, że Zamawiający dopuścił rozwiązania równoważne, bowiem posłużył się określeniem „lub równoważne". Takie ukształtowanie wymagań pozwalało wykonawcom w złożonych ofertach bazować nie tylko na rozwiązaniu zdalny port mirroring, czy też RSPAN, ale wykorzystać rozwiązania wobec nich równoważne.**

Zwrócenia uwagi wymaga, że Odwołujący w zakresie przełącznika 6300M nie kwestionuje spełnienia samego wymagania w zakresie posiadania funkcjonalności: *zdalnej obserwacji ruchu na określonym porcie, polegającej na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego,* a wyłącznie podważa wymóg przesyłania *poprzez dedykowaną sieć VLAN* Tymczasem w toku badania i oceny ofert Zamawiający ustalił, że w przypadku tego przełącznika istnieje techniczna możliwość realizacji przesyłu poprzez dedykowaną sieć VLAN, zgodnie z wymaganiami SWZ. Zostało to ustalone przez Zamawiającego w oparciu o dostępną na stronach producenta specyfikację techniczną przełącznika. Zauważyć przy tym należy, że pomimo braku wskazania wprost danej funkcjonalności w specyfikacji technicznej, jest ona możliwa do konfiguracji.

Jednocześnie nie sposób zgodzić się ze stwierdzeniami Odwołującego, jakoby treścią SWZ w ramach prowadzonego postępowania ograniczył zastosowane rozwiązania wyłącznie do RSPAN. Tego rodzaju twierdzenia Odwołującego nie znajdują odzwierciedlenia w wymaganiach OPZ, w szczególności w brzmieniu wymagania dotyczącego funkcjonalności związanej z zarządzaniem i monitorowaniem opisanej w Załączniku nr 1 do OPZ w pkt 1.1.5 w ppkt 7 lit. d) dla przełącznika wewnętrznego.

Odwołujący dokonując interpretacji wymagań Zamawiającego wydaje się nie traktować ich jako
całości, a skupia się na treści podanej przez Zamawiającego w nawiasie, którą należy traktować jako pomocniczą, służebną względem głównego trzonu wymagania, które stanowiło jego opis.

Zamawiający wymagał funkcjonalności zdalnej obserwację ruchu na określonym porcie, polegającej na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN, a RSPAN jest tylko jedną z możliwości realizacji tej funkcjonalności wymienionej w przywołanym powyżej punkcie OPZ. Co więcej, treść SWZ pozostawia dowolność wykonawcy, w jakiej warstwie przesył ten ma być realizowany, bowiem Zamawiający w żadnym miejscu nie zdefiniował warstw przesyłu.

Podsumowując, także ten zarzut, jako niepotwierdzony, wymaga oddalenia.

Dodatkowo, w zakresie pkt IV i V niniejszego pisma, Zamawiający zwraca uwagę, że analiza
odpowiedzi producenta Aruba nie może stanowić dowodu na potwierdzenie tez zawartych w odwołaniu, bowiem producent w sformułowaniu odpowiedzi posiada pełną swobodę (nie wiąże go żadna procedura). Słusznie, w ocenie Zamawiającego, producent wskazuje, iż ***rozwiązanie*** *oparte o przełączniki Aruba 4100i oraz Aruba 6300M* zapewnia wymagane przez Zamawiającego funkcjonalności, bowiem zważyć należy, iż urządzenia tego typu nie funkcjonują samodzielnie i w oderwaniu od wbudowanego oprogramowania oraz innych elementów. Co więcej, w odpowiedzi producenta należy interpretować w kontekście pytania Zamawiającego, które wprost odwoływało się do konkretnych urządzeń (zaoferowanych przez Innergo) z uwzględnieniem opisu wymagań podanych w OPZ i posiadało następujące brzmienie: *Czy przełącznik Aruba 4100i oraz przełącznik Aruba 6300M umożliwiają zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (zdalny port mirroring – RSPAN lub równoważny)*W związku z tym za nieprawidłowe należy uznać „wyrywanie" z kontekstu pojedynczych słów i stwierdzeń producenta i nadawanie im przez Odwołującego własnego znaczenia, z pominięciem treści pytania zadanego przez Zamawiającego.

Uzasadnienie stanowiska Zamawiającego w zakresie zarzutu zaoferowania oprogramowania zapewniającego realizację wymagań w zakresie przedmiotu zamówienia.

Zamawiający uznaje zgłoszony zarzut za całkowicie bezzasadny, a tym samym za taki, który
powinien podlegać oddaleniu.

Na wstępie Zamawiający podnosi, że w zakresie rozpoznania zasadności zgłoszonego zarzutu
istotnym jest odwołanie się do wymagań Zamawiającego w zakresie katalogu informacji, które wykonawca zobowiązany był podać w ofercie w Formularzu pt. Zestawienie elementów - w odniesieniu do oprogramowania (Formularz 2.2). Otóż, wykonawca zobowiązany był podać następujące dane takie jak: nazwa oprogramowania, jego producent i ilość oferowanych licencji.

Dowód: - wzór Formularza „Zestawienie głównych elementów Systemu Wi-Fi" (Formularz 2.2.),
w dokumentacji Postępowania.

Wykonawca Innergo w złożonej ofercie w niniejszym formularzu w zakresie Zestawienia głównych elementów CSZ w Centrum Informatyki Resortu Finansów w Radomiu wskazał, że oferuje oprogramowanie o Nazwie Aruba Clearpass, którego producentem jest Aruba w ilości 2 sztuki licencji.

Dowód: - treść Formularza „Zestawienie głównych elementów Systemu Wi-Fi" (Formularz 2.2.),
w dokumentacji Postępowania.

Na kanwie powyższego nie budzi zatem żadnych wątpliwości, że wykonawca Innergo w złożonej ofercie zastosował się do wymagań Zamawiającego i podał wszystkie żądane przez niego informacje. Nie ma racji Odwołujący twierdząc, że Wykonawca w treści swojej oferty powinien wyspecyfikować konkretne licencje, tj. Aruba Clearpass Akcess, Aruba Clearpass OnGuard, Aruba ClearPass Device Insight, bowiem wykonawca zobowiązany był do wskazania: nazwy oprogramowania i jego producenta, co też uczynił.

W tym miejscu wyjaśnić należy, że oprogramowanie Aruba ClearPass składa się z 3 elementów, co znajduje potwierdzenie w dokumentacji producenta dostępnej pod adresami:
https://www.arubanetworks.com/resource/clearpass-solution-overview/
https://www.arubanetworks.com/resource/clearpass-policy-manager-data-sheet/

- gdzie wprost wskazano jakie elementy składają się na zaoferowane oprogramowanie ClearPass.

Dowód:- SOLUTION OVERVIEW Aruba Clearpass Network Access Control dostępny pod adresem: https://www.arubanetworks.com/resource/clearpass-solution-overview/;

- DATA SHEET ARUBA CLEARPASS POLICY MANAGER dostępny pod adresem: https://www.arubanetworks.com/resource/clearpass-solution-overview/.

Sposób wypełnienia formularza oferty, z punktu widzenia SWZ, jest wystarczający do identyfikacji oprogramowania, co było celem Zamawiającego. Oznacza to, że w sytuacji, gdy wykonawca Innergo zastosował się do wymagań Zamawiającego, określonych w SWZ prawidłowo je wypełniając, to nie sposób uznać, że jego oferta podlega podrzuceniu na podstawie art. 226 ust. 1 pkt 5 Pzp z uwagi na niezgodność w warunkami zamówienia.

Na końcu Zamawiający odniesie się do zarzutu, jakoby Przystępujący zaoferował jedynie 2 licencje, co uniemożliwia zaoferowanie wskazanych w ofercie 3 produktów (pkt 106 odwołania). Zamawiający wyjaśnia, że wykonawca Innergo zaoferował następujące urządzenia:

2.	Nazwa urządzenia: Mobility Conductor Hardware Appliance Producent: Aruba Model: ARUBA MOBILITY CONDUCTOR	**2**

Dowód: - treść Formularza „Zestawienie głównych elementów Systemu Wi-Fi" (Formularz 2.2.) wykonawcy Innergo (str. 1), w dokumentacji Postępowania.

Z tego też względu konieczne było zaoferowanie dwóch sztuk licencji Aruba Clearpass (każda ze wskazanych licencji składająca się z 3 elementów obsługuje jedno ww. urządzenie), co wykonawca Innergo uczynił. Tym samym zaoferowane licencje odpowiadały ilości zaoferowanych urządzeń, co było wystarczające dla spełnienia wymagań SWZ.

Biorąc pod uwagę powyższe ustalenia stwierdzić należy, że zarzut zgłoszony przez Odwołującego jest niezasadny i podlega oddaleniu.

Konkludując, Zamawiający stoi na stanowisku, że prawidłowo przeprowadził czynność badania i oceny ofert, która zaowocowała wyborem jako najkorzystniejszej oferty wykonawcy Innergo, która wbrew twierdzeniom Odwołującego spełnia wymagania SWZ, a tym samym nie podlega odrzuceniu.

Oznacza to, że nie znajdują potwierdzenia zarzuty zgłoszone w odwołaniu, polegające na naruszeniu przez Zamawiającego art. 226 ust. 1 pkt 5 ustawy Pzp w zw. z art. 16 ustawy Pzp, oraz art. 239 ust. 1 i 2 ustawy Pzp. Mając powyższe na uwadze, wnoszę jak na wstępie.

Stan faktyczny ustalony przez Izbę:

W dniu 21 sierpnia 2023 r. wykonawcy wspólnie ubiegający się o udzielenie zamówienia: **T4B sp. z o.o. z siedzibą w Warszawie, Atende S.A. z siedzibą w Warszawie** wnieśli odwołanie zarzucając naruszenie przepisów przez Zamawiającego:

(1) **naruszenie art. 226 ust. 1 pkt 5 pzp w zw. z art. 16 pzp** poprzez zaniechania odrzucenia oferty wykonawcy Innergo Systems Sp. z o.o. ul. Odrowąża 15, 03-310 Warszawa; w sytuacji gdy treść przedmiotowej oferty jest niezgodna z warunkami zamówienia, w odniesieniu do:

a) przełącznika dostępowego zewnętrznego:

i. z uwagi na brak funkcjonalności prywatnego VLAN-u na dzień składania ofert, a uwzględnienie zmiany, ktora zaszła w tym zakresie po złożeniu i otwarciu ofert, co prowadzi do naruszenia zasady uczciwej konkurencji i równego traktowania Wykonawców;

ii. z uwagi na brak funkcjonalności zdalnego port mirroring – RSPAN;

b) przełącznika dostępowego wewnętrznego z uwagi na brak funkcjonalności zdalnego port mirroring – RSPAN;

c) zaoferowanego oprogramowania z uwagi na brak zaoferowania oprogramowania zapewniającego realizację wymagań przedmiotu zamowienia (tj. co najmniej: Aruba ClearPass Access, Aruba ClearPass OnGuard, Aruba ClearPass Device Insight);

(2) **naruszenie art. 239 ust. 1 i 2 pzp**, poprzez dokonanie wyboru oferty wykonawcy Innergo Systems Sp. z o.o. ul. Odrowąża 15, 03-310 Warszawa, ktora nie jest najkorzystniejszą ofertą w świetle kryteriów oceny ofert określonych w dokumentach zamówienia, tj. oferty nieprzedstawiającej najkorzystniejszego stosunku jakości do ceny zamówienia, gdyż najkorzystniejszą ofertą jest oferta Odwołującego, a oferta Innergo Systems Sp. z o.o. winna zostać odrzucona.

W wyniku wniesionego odwołania przez wykonawców wspólnie ubiegających się o udzielenie zamówienia: T4B sp. z o.o. z siedzibą w Warszawie, Atende S.A. z siedzibą w Warszawie, Zamawiający pismem wniesionym do Krajowej Izby Odwoławczej w dniu 4 września 2023 r. (pismo z dnia 4 września 2023 r.) wnosił o oddalenie odwołania w całości.

Do postępowania odwoławczego po stronie Zamawiającego skutecznie przystąpił wykonawca Innergo Systems Sp. z o.o. z siedzibą w Warszawie.

Izba stwierdziła, że ww. wykonawca zgłosił przystąpienie do postępowania w ustawowym terminie, wykazując interes w rozstrzygnięciu odwołania na korzyść Zamawiającego.

Stan prawny ustalony przez Izbę:

Zgodnie z art. 226 ust. 1 pkt 5 ustawy PZP, Zamawiający odrzuca ofertę, jeżeli jej treść jest niezgodna z warunkami zamówienia.

Zgodnie z art. 239 ustawy PZP:

1. Zamawiający wybiera najkorzystniejszą ofertę na podstawie kryteriów oceny ofert określonych w dokumentach zamówienia.

2. Najkorzystniejsza oferta to oferta przedstawiająca najkorzystniejszy stosunek jakości do ceny lub kosztu lub oferta z najniższą ceną lub kosztem.

Zgodnie z art. 16 ustawy PZP, zamawiający przygotowuje i przeprowadza postępowanie o udzielenie zamówienia w sposób:

1)zapewniający zachowanie uczciwej konkurencji oraz równe traktowanie wykonawców;

2)przejrzysty;

3)proporcjonalny.

II.KIO 2578/23:

W dniu 21 sierpnia 2023 r. wykonawca Konwerga Sp. z o.o. z siedzibą w Poznaniu wniósł odwołanie od niezgodnych z przepisami Ustawy czynności Zamawiającego podjętych w postępowaniu tj.:

A. czynności odrzucenia oferty Odwołującego jako niezgodnej z SWZ,

B. czynności wyboru oferty złożonej przez wykonawcę Innergo Systems sp. z o.o. jako najkorzystniejszej

C. decyzji Zamawiającego o odtajnieniu części informacji skutecznie zdaniem Odwołującego zastrzeżonych jako tajemnica przedsiębiorstwa przesłanych przez niego w dniu 14.04.2023 i 17.05.2023 jako wyjaśnienia rażąco niskiej ceny oraz w dniu 19.05.2023 jako wyjaśnienia techniczne w zakresie złożonej oferty.

Odwołujący zarzucił naruszenie przepisów przez Zamawiającego:

A. naruszenie art. 226 ust.1 pkt 5 Ustawy poprzez bezpodstawne odrzucenie oferty Odwołującego, pomimo, że jej treść odpowiada SIWZ
B. naruszenie art. 239 ust. 1 Ustawy poprzez dokonanie wyboru oferty nie najkorzystniejszej
C. naruszenie art. 18 ust. 3 ustawy PZP w zw. z art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j, Dz.U. z 2020 r. poz.1983 ze zm.).
Odwołujący wnosił o uwzględnienie odwołania i nakazanie Zamawiającemu:
A. unieważnienie czynności odrzucenia oferty Odwołującego
B. unieważnienie czynności wyboru oferty najkorzystniejszej
C. powtórzenia czynności badania ofert w celu wyboru oferty najkorzystniejszej.
D. unieważnienia czynności odtajnienia dokumentów zastrzeżonych jako tajemnica przedsiębiorstwa.
Odwołujący wskazał, że:
A. Odrzucenie oferty Odwołującego
W piśmie z dnia 10.08.2023 informującym o wyborze oferty najkorzystniejszej Zamawiający poinformował o odrzuceniu oferty Odwołującego na podstawie art. 226 ust 1 pkt 5 Ustawy jako niezgodnej z warunkami zamówienia. Niezgodności te zostały określone przez Zamawiającego jako:
I Niezgodność oferty z wymaganiami CSZ:
1. Telemetria
2. Ochrona przed atakami sieciowymi na sieć bezprzewodową
3. Mechanizmy bezpieczeństwa (posture, profilowanie urządzeń)
4. Analiza widma częstotliwościowego oraz wyświetlanie analizy spektrum dla access-pointów
II. Niezgodność oferty z wymaganiami dla lokalizacji:
1. Funkcjonalność WIPS
2. Ochrona przed atakami sieciowymi na sieć bezprzewodową
3. Analiza widma częstotliwościowego oraz wyświetlanie analizy spektrum dla access-pointów
Ze względu na fakt, iż zarówno argumentacja Zamawiającego jak i argumentacja Odwołującego punktach I.2 i II.2 jak i I.4 i II.3 są identyczne (Zamawiający przekopiował zarówno treść zarzutów jak i uzasadnień), a ich rozdzielnie wynika wyłącznie z układu zapisów w SWZ, to będą one w dalszej części uzasadnienia omawiane łącznie. Należy przez to rozumieć, że uzasadnienie do punktu I.1 dotyczy także punktu II.2, a uzasadnienie do punktu I.4 dotyczy także punktu II.3.
Uzasadnienie Odwołującego odnoszące się wszystkich zarzutów w sekcji A (dalej przywoływane jako „A.0")
Zamawiający w uzasadnieniu nie spełniania zapisów SWZ powołuje się na dokumentację oprogramowania, które nie zostało zaoferowane przez Odwołującego. Dotyczy to oprogramowania Cisco DNA Advantage oraz Cisco ISE Premier. Odwołujący potwierdza, że wskazane przez Zamawiającego oprogramowanie spełnia wymagania SWZ, ale nie może to stanowić dowodu na to, że oprogramowanie zaoferowane przez Odwołującego w wersjach niższych czyli Cisco DNA Essentials oraz Cisco ISE Advantage nie spełniają wymogów SWZ. Oczywistym jest, że oprogramowanie w wyższej wersji posiada wszystkie funkcjonalności oprogramowania w wersji niższej, a ponadto posiada cały szereg dodatkowych funkcjonalności.
Na stronie producenta znajduje się opis systemów:
"Cisco DNA Advantage is our premium tier that gives you the advantage of the latest innovative features. All the features mentioned in the Cisco DNA Essentials section are included in Advantage."
Tłumaczenie:
„Cisco DNA Advantage to nasz poziom premium, który zapewnia przewagę w postaci najnowszych innowacyjnych funkcji. Wszystkie funkcje wymienione w sekcji Cisco DNA Essentials są zawarte w Advantage."
Źródło: https://www.cisco.com/c/en/us/products/collateral/software/dna-software-ebook-cte.html
Dowód 1: Podręcznik oprogramowania Cisco DNA (adres: https://www.cisco.com/c/en/us/products/collateral/software/dna-software-ebook-cte.html)
Nie można zatem uznać za dowód na niespełnienie wymagań SWZ poprzez powoływanie się na spełnianie wymagań przez wyższą wersję oprogramowania. Zamawiający dokonując oceny oferty Odwołującego powinien zatem oceniać spełnianie wymogów zawartych w SWZ przez ofertę Odwołującego. Zatem całość argumentacji Zamawiającego odnosząca się do produktów nie stanowiących oferty Odwołującego należy uznać za nie dotyczącą kwestii spornych.
Jednocześnie zgodnie z art. 99 ust. 1 i 2 zamawiający określa parametry minimalne dotyczące przedmiotu zamówienia. Profesjonalny wykonawca powinien zaoferować produkty i usługi, które spełniają wymagania minimalne. Ze względu na fakt, iż w postępowaniu publicznym głównym kryterium oceny ofert jest cena, Wykonawca powinien zaoferować produkty i usługi, które spełniają wymagania minimalne w 100%, ale nie ma obowiązku spełniania tych wymagań w stopniu wyższym, zwłaszcza jeżeli prowadziłoby do zwiększenia ceny, a co w efekcie przyczyniłoby się do obniżenia oceny oferty.
Krajowa Izba Odwoławcza w wyroku z dnia 26 kwietnia 2022 r. w sprawie KIO 917/22 wskazała, że „aby zamawiający był uprawniony odrzucić ofertę na podstawie przywołanego przepisu jest zobowiązany przeprowadzić analizę porównawczą treści oferty oraz warunków zamówienia (w szczególności, co do zakresu, ilości, jakości, warunków realizacji i innych elementów istotnych dla wykonania zamówienia), które stanowią merytoryczne postanowienia oświadczeń woli odpowiednio: zamawiającego, który w szczególności przez opis przedmiotu zamówienia precyzuje i uszczegóławia, jakiego świadczenia oczekuje po zawarciu umowy w sprawie zamówienia publicznego, oraz wykonawcy, który zobowiązuje się do wykonania tego świadczenia w razie wyboru złożonej przez niego oferty (zdefiniowanej w art. 66 kodeksu cywilnego) jako najkorzystniejszej. Dokonanie takiego porównania przesądza o tym, czy treść złożonej w postępowaniu oferty odpowiada warunkom zamówienia. Niezgodność treści oferty z warunkami zamówienia zachodzi więc, gdy zawartość merytoryczna złożonej w danym postępowaniu oferty nie odpowiada ukształtowanym przez zamawiającego i zawartym w SWZ wymaganiom. Istotnym jest, że niezgodność oferty z warunkami zamówienia musi po pierwsze być oczywista i niewątpliwa, czyli zamawiający musi mieć pewność co do niezgodności oferty z jego oczekiwaniami, przy czym postanowienia SWZ powinny być jasne i klarowne (tak też: wyrok z dnia 22 września 2020 roku, sygn. akt: KIO 1864/20; wyrok z dnia 20 stycznia 2020 roku, sygn. akt: KIO 69/20). Po drugie, odrzucenie oferty nie może nastąpić z błahych, czysto formalnych powodów nie wpływających na treść złożonej oferty, jak również gdy zamawiający ma możliwość poprawienia błędów jakie zawiera oferta."
Ponadto Odwołujący podkreśla, że profesjonalizm wykonawcy (art. 355 K. c.) nie uchyla reguł wykładni z art. 65 § 1 K. c. Co więcej, zamawiający jest również podmiotem profesjonalnym, od którego wymagana jest szczególna staranność wyrażająca się większą zapobiegliwością, rzetelnością, dokładnością w działaniu, dokładnością w prowadzeniu postępowania, w tym wyjaśnień i zadawaniu odpowiednich pytań wykonawcom w toku postępowania. Ustawa nakłada na Zamawiającego konkretne obowiązki i rygory postępowania. W sytuacji gdy, zamawiający otrzymuje oświadczenie wykonawcy w odpowiedzi na własne oświadczenie, które nie odpowiada Zamawiającemu, zawsze ocena takiej odpowiedzi powinna następować w kontekście własnego postępowania — należytej staranności w prowadzeniu wyjaśnień.

Reasumując zgodnie z utrwalonym orzecznictwem Krajowej Izby Odwoławczej niezgodność oferty z warunkami zamówienia musi być oczywista i niewątpliwa, przy czym postanowienia SWZ powinny być jasne i klarowne.

I.1 Niezgodność oferty z zapisami SWZ z zakresie telemetrii

Zgodnie z Tomem III SWZ - OPZ zał. 1 pkt 2.1, Wymagania ogólne dla systemu CSZ, L.p. 33 Zamawiający wymagał:
„System musi posiadać funkcjonalność telemetrii (…)"
oraz zgodnie z Tomem III SWZ - OPZ zał. 1 pkt 2.1, Wymagania ogólne dla systemu CSZ, L.p. 34 Zamawiający wymagał:
„Musi posiadać narzędzie pozwalające na monitoring wydajności sieci wraz z:
a) zbieraniem informacji o aplikacjach w sieci i parametrach ich działania
b) analizą, którzy użytkownicy generują najwięcej ruchu, z jakich korzystają aplikacji oraz jakie jest ich wykorzystanie".

Analiza dowodów Zamawiającego

Zamawiający uzasadnił niezgodność oferty z zapisami SWZ lakonicznie:
„W ramach badania oferty Konwerga Zamawiający ustalił, że licencja Network Essentials dostarczona wraz z urządzeniami (co dodatkowo Konwerga potwierdziła w wyjaśnieniach z dnia 19.05.2023 r.) i funkcjonalność w niej zawarta nie spełnia ww. wymagań w zakresie telemetrii, co zostało ustalone na podstawie danych technicznych zwartych na stronie internetowej producenta Cisco - https://www.cisco.com/c/m/en_us/products/software/dna-subscription-wireless/en-sw-sub-matrix-wireless.html"
Treść wskazanego przez Zamawiającego dokumentu znajduje się w Załączniku nr 1 (Porównanie funkcjonalności Cisco DNA) do niniejszego odwołania.
Dalsze uzasadnienie nie dotyczy zaoferowanej przez Odwołującego wersji oprogramowania Cisco DNA Essentials, a więc nie będzie podlegać analizie (uzasadnienie zawarto w części A.0).
Ze wskazanego przez Zamawiającego dokumentu wcale nie wynika, iż funkcjonalność telemetrii nie została zaoferowana, a Zamawiający nie przytoczył żadnego fragmentu wskazanego tekstu mającego stanowić potwierdzenie jego tezy. Co więcej, ze wskazanego dokumentu wynika wprost, iż funkcjonalność telemetrii jest oferowana w rozwiązaniu Odwołującego, tj. całego CSZ wyposażonego m.in. w oprogramowanie Cisco DNA Essentials.
Dowód 2: Dokument „Porównanie funkcjonalności Cisco DNA" - Załącznik nr 1

Uzasadnienie Odwołującego

Odwołujący potwierdza, iż zaoferowane przez niego oprogramowanie zarządzające Cisco DNA Essentials zawiera funkcjonalność telemetrii i na dowód przywołuje zapisy dokumentu wskazanego przez Zamawiającego stanowiącego Załącznik nr 1 do niniejszego odwołania.

Rysunek 1 - Porównanie funkcjonalności licencji w zakresie telemetrii

Tłumaczenie:
1. „Cisco DNA Software Wireless Feature Matrix" „Oprogramowanie Cisco DNA bezprzewodowe, matryca funkcjonalności"
2. "Perpetual software, compatible with Cisco DNA Essentials subscription license" "Oprogramowanie wieczyste, zgodne z licencją subskrypcyjną Cisco DNA Essentials"
3. „**Telemetry and visibility** Model-driven telemetry lets you monitor your network by streaming data from network devices, continuously providing near-real-time access to operational statistics" **„Telemetria i widoczność** Telemetria oparta na modelach pozwala monitorować sieć poprzez strumieniowe przesyłanie danych z urządzeń sieciowych, dostarczając w sposób ciągły dostęp w czasie zbliżonym do rzeczywistego do statystyk operacyjnych."
4. "**Client health dashboard** Displays operational status of every client connected to Cisco DNA Center, with suggested remediation for any issues, managed by Cisco DNA Center."

„Pulpit nawigacyjny stanu klienta

Wyświetla stan operacyjny każdego klienta podłączonego do Cisco DNA Center, z sugerowanymi środkami zaradczymi dla wszelkich problemów, którymi zarządza przez Cisco DNA Center."
5. "**Application health dashboard**

Displays overall health of all applications on the network, with special section for business-relevant application issues and suggested remediation, managed by Cisco DNA Center." **„Pulpit nawigacyjny stanu aplikacji**

Wyświetla ogólny stan wszystkich aplikacji w sieci, ze specjalną sekcją dotyczącą problemów związanych z aplikacjami biznesowymi i sugerowane środki zaradcze, zarządzane przez Cisco DNA Center."
6. "**Wireless Sensor dashboard**

Shows overall tests, connectivity statistics, and top wireless issues discovered by Cisco Aironet® Active Sensors. Tests include DHCP, DNS, host reachability, RADIUS, email, Microsoft Exchange Server, web, FTP, and a complete IP SLA for data throughput speed, latency, jitter, and packet loss. Provides guided remediation for any test failures."

„Panel sensora bezprzewodowego

Pokazuje ogólne testy, statystyki łączności i najważniejsze problemy z siecią bezprzewodową wykryte przez aktywne czujniki Cisco Aironet®. Testy obejmują DHCP, DNS, osiągalność hosta, RADIUS, poczta e-mail, Microsoft Exchange Server, WWW, FTP i pełna umowa SLA IP dotycząca przepustowości danych prędkość, opóźnienie, jitter i utratę pakietów. Zapewnia wskazówki zaradcze w przypadku niepowodzeń testów."
Na powyższym fragmencie zaznaczono jedynie ogólną funkcjonalność telemetrii.
Z powyższego dokumentu wprost wynika, iż funkcjonalność telemetrii została zaoferowana i jest ona zgodna z zaoferowanym systemem zarządzania Cisco DNA Essentials funkcjonującym w ramach CSZ. Spełnianie wymogu ogólnego („System musi posiadać funkcjonalność telemetrii") potwierdza fragment:
„Telemetria i widoczność
Telemetria oparta na modelach pozwala monitorować sieć poprzez strumieniowe przesyłanie danych z urządzeń sieciowych, dostarczając w sposób ciągły dostęp w czasie zbliżonym do rzeczywistego do statystyk operacyjnych."
Z powyższego zapisu wprost wynika, iż Cisco DNA Essentials posiada funkcjonalność telemetrii, co potwierdza odpowiedni symbol „√" w sekcji „Network Essentials", która zgodnie z zaznaczonym nagłówkiem zawarta jest w licencji Cisco DNA Essentials (zapis „Oprogramowanie wieczyste, zgodne z licencją subskrypcyjną Cisco DNA Essentials").
Z kolei spełnianie wymogu w zakresie szczegółowym:
„Musi posiadać narzędzie pozwalające na monitoring wydajności sieci wraz z:
a) zbieraniem informacji o aplikacjach w sieci i parametrach ich działania
b) analizą, którzy użytkownicy generują najwięcej ruchu, z jakich korzystają aplikacji oraz jakie jest ich wykorzystanie".
potwierdzają funkcjonalności pulpitu:
„Pulpit nawigacyjny stanu aplikacji Wyświetla ogólny stan wszystkich aplikacji w sieci, ze specjalną sekcją dotyczącą problemów związanych z aplikacjami biznesowymi i sugerowane środki zaradcze, zarządzane przez Cisco DNA Center."
Pulpit nawigacyjny umożliwia wyświetlenie stanu wszystkich aplikacji w sieci, parametry ich działania a także sugeruje środki zaradcze. Natomiast dodatkowo pulpity nawigacyjne stanu klienta oraz sensora bezprzewodowego dostarczają cały szereg informacji o ruchu generowanym przez użytkowników.
Dowód 3: Dokument „Porównanie funkcjonalności Cisco DNA" - Załącznik nr 1

Podsumowanie

Z przedstawionych dowodów wprost wynika, iż funkcjonalność telemetrii została zaoferowana i jest ona zgodna z zaoferowanym systemem zarządzania Cisco DNA Essentials funkcjonującym w ramach CSZ. Dotyczy to zarówno wymogu ogólnego (Tom III SWZ - OPZ zał. 1 pkt 2.1, Wymagania ogólne dla systemu CSZ, L.p. 33) jak i wymagań szczegółowych (Tom III SWZ - OPZ zał. 1 pkt 2.1, Wymagania ogólne dla systemu CSZ, L.p. 34). Zamawiający nie przedstawił żadnych dowodów, które świadczyłyby przeciwnie.

I.2 Niezgodność oferty z zapisami SWZ w zakresie ochrony przed atakami sieciowymi na sieć bezprzewodową

Zgodnie z Tom III SWZ - OPZ zał. 1 pkt 1.1.4, Wymagania szczegółowe dla kontrolerów sieci bezprzewodowej – lokalne, Lp. 12, Zamawiający wymagał:

„Kontroler musi posiadać funkcje Bezpieczeństwa:

a) Detekcja i identyfikacja lokalizacji obcych punktów dostępowych (rogue AP). Automatyczna klasyfikacja obcych urządzeń i możliwość ich blokowania poprzez wysyłanie odpowiednio spreparowanych pakietów;

b) Identyfikacja sieci Adhoc;

c) Identyfikacja anomalii sieciowych;

d) Ochrona przed atakami sieciowymi na sieć bezprzewodową, np. DoS, Management Frame Flood, fake AP;

e) Identyfikacja błędów konfiguracji klientów WLAN; Identyfikacja podszywania się pod autoryzowane punkty dostępowe".

Analiza dowodów Zamawiającego cz. 1

Zamawiający uzasadnił niezgodność oferty z zapisami SWZ:

„W ramach badania oferty Konwerga Zamawiający ustalił, że zaoferowana oprogramowanie Cisco DNA na licencji Essentials nie spełnia ww. wymagania ochrony przed atakami sieciowymi na sieć bezprzewodową, np. DoS, co zostało ustalone na podstawie informacji zawartych na stronie internetowej producenta Cisco https://www.cisco.com/c/m/en_us/products/software/dna-subscription-wireless/en-sw-sub-matrix-wireless.html"

Treść wskazanego przez Zamawiającego dokumentu znajduje się w Załączniku nr 1 (Porównanie funkcjonalności Cisco DNA) do niniejszego odwołania. Nie wiadomo jednak, który fragment miałby potwierdzać tezę Zamawiającego, gdyż nie zacytował on nawet najkrótszego fragmentu, ani nie wskazał miejsca, w którym takie potwierdzenie mogłoby się znaleźć. We wskazanym dokumencie nigdzie nie występuje słowo DoS, więc nie wiadomo na jakiej podstawie Zamawiający doszedł do takiego wniosku (na marginesie – sformułowanie to także nie występuje w odniesieniu do wersji Advantage).

Dowód 4: Dokument „Porównanie funkcjonalności Cisco DNA" - Załącznik nr 1

Uzasadnienie Odwołującego cz. 1

W tym miejscu Odwołujący zwraca uwagę na dokładne brzmienie tego wymogu:

„Ochrona przed atakami sieciowymi na sieć bezprzewodową, np. DoS, Management Frame Flood, fake AP"

Ponadto Odwołujący zwraca uwagę, iż wymóg ten dotyczył kontrolerów sieci bezprzewodowej, co zostało wyrażone wprost. Dla Odwołującego nie budziło zatem wątpliwości, że kontroler wśród różnych funkcji bezpieczeństwa powinien posiadać ochronę przed atakami na sieć bezprzewodową, których przykłady podał Zamawiający i wśród których znalazło się sformułowanie „DoS". Odwołujący zwraca uwagę, iż Zamawiający nie użył sformułowań typu „w tym", „minimum", „co najmniej", „zawierające" itp., które w sposób jednoznaczny oznaczałyby bezwzględną konieczność zapewnienia tej funkcjonalności. Oznacza to, iż Zamawiający oczekiwał, iż kontroler będzie zapewniał ochronę przed atakami na sieć bezprzewodową różnego rodzaju.

Na wstępie jednak należy rozstrzygnąć czym jest ochrona przed atakami sieciowymi na sieć bezprzewodową DoS.

Na stronie Ministerstwa Spraw Wewnętrznych i Administracji w zakładce „Cyberbezpieczeństwo" znajdują się następujące definicje pojęcia DoS (https://www.gov.pl/web/mswia/cyberbezpieczenstwo):

„DoS (denial of service; dosłownie: odmowa usługi) - atak, którego skutkiem jest uniemożliwienie dostępu do usługi na serwerze (na przykład skorzystania ze strony www)

DDoS (distributed denial of service) - atak DoS przeprowadzany z wielu źródeł jednocześnie"

Dowód 5: Definicja pojęcia DoS Ministerstwa Spraw Wewnętrznych i Administracji (źródło: (https://www.gov.pl/web/mswia/cyberbezpieczenstwo)

Ponadto na stronie NASK znajduje się następująca definicja (https://www.nask.pl/pl/aktualnosci/oferta/oferta-telekomunikacyjn/bezpieczenstwo/2662,DDoS-Attack-Protection.html):

„Usługa ochrony przed atakami typu DDoS służy do zabezpieczenia łącza Klienta przed skutkami rozległych ataków wolumetrycznych

Definicja

DDoS (Distributed Denial of Service) to rozproszony atak na systemy komputerowe lub usługę sieciową uniemożliwiający poprawne działanie poprzez zajęcie wszystkich wolnych zasobów."

Dowód 6: Definicja pojęcia DoS NASK (źródło: (https://www.nask.pl/pl/aktualnosci/oferta/oferta-telekomunikacyjn/bezpieczenstwo/2662,DDoS-Attack-Protection.html)

Ponadto na stronach Urzędu Komisji Nadzoru Finansowego znajduje się obszerny dokument poświęcony DoS, a zatytułowany „Dobre praktyki w zakresie przeciwdziałania atakom DDoS" (źródło:7.pdf), który załączono do niniejszego odwołania jako Załącznik nr 4 Dobre_praktyki_w_zakresie_przeciwdziaania_atakom_DDoS_77247

Na wstępie czytamy w nim:

„Jednym z popularnych rodzajów działań cyberprzestępców wymierzonych w atrybut dostępności są ataki na tzw. odmowę usługi (ang. Denial of Service, DoS) oraz Distributed Denial of Service (DDoS).

W uproszczeniu, ataki DDoS można scharakteryzować jako ataki powodujące czasową niedostępność systemów teleinformatycznych i usług Organizacji świadczonych drogą elektroniczną. Często ataki DDoS bezpośrednio wpływając na atrybut dostępności powodują również wpływ na atrybuty integralności oraz poufności danych, generując wysokie ryzyko ich utraty przez Organizację."

Dalej dokument omawia szereg różnych metod zapobiegania atakom DoS. Na końcu dokumentu znajduje się następujące podsumowanie:

„Nie istnieją gotowe, kompleksowe rozwiązania ani jedna uniwersalna metoda ochrony przed atakami typu DDoS. Budowanie infrastruktury odpornej na ataki nie może być sprowadzone wyłącznie do kupienia gotowego produktu czy usługi, lecz powinno być systemowym podejściem do zaprojektowania całego łańcucha technologicznego odpowiedzialnego za dostarczenie ostatecznej usługi, tworząc wielowarstwową ochronę Organizacji zgodnie z zasadą defence in depth.

Faktyczna, wypadkowa odporność organizacji na atak jest sumą zastosowanych rozwiązań i technik przeciwdziałania z wykorzystaniem maksymalnej dostępnej dla Organizacji liczby opisanych powyżej rozwiązań i technik oraz uwzględnieniem potencjalnego wpływu najsłabszego ogniwa."

Powyższe wnioski potwierdzają, że nie istnieje coś takiego jak **pełna** ochrona przed atakami sieciowymi na sieć bezprzewodową DoS. Zatem niektóre rozwiązania będą realizowały pewne wybrane funkcje. Należy tutaj zwrócić uwagę, że Zamawiający nie zdefiniował jaką konkretną ochronę przed atakami DoS miał zaoferować Wykonawca, a poprzedzenie jej sformułowaniem „na przykład" nie pozostawiało wątpliwości, iż nie była ona kluczowa dla działania całego systemu będącego przedmiotem dostawy. Na marginesie należy zauważyć, że zgodnie z dokumentem dołączonym do SWZ o

nazwie „Zalacznik_nr_8_-_Opis_aktualnego_srodowiska_WAN_RF_22-03-2023_13.28.54”, Zamawiający dysponuje narzędziami, które będą współpracowały z dostarczaną infrastrukturą podnosząc odporność całości systemu CIRF na ataki typu DoS. Świadczy o tym fragment:

„Na Urządzeniach bezpieczeństwa sieci WAN zostały wydzielone Strefy Bezpieczeństwa (ang. Zones). Każda ze stref stanowi fizyczny lub logiczny (VLAN) obszar sieci złożony z hostów (komputerów, serwerów, drukarek i innych urządzeń sieciowych). Ruch pomiędzy Strefami bezpieczeństwa jest możliwy i nadzorowany wyłącznie za pomocą mechanizmów zaimplementowanych na Urządzeniach bezpieczeństwa.”

Wskazanymi Urządzeniami bezpieczeństwa są m.in. firewall’e, które Zamawiający prezentował w trakcie wizji lokalnych na obiektach.

Dowód 7: Definicja pojęcia DoS Urzędu Komisji Nadzoru Finansowego – Załącznik nr 4

Dowód 8: Zalacznik_nr_8_-_Opis_aktualnego_srodowiska_WAN_RF_22-03-2023_13.28.54

Analiza dowodów Zamawiającego oraz Uzasadnienie Odwołującego

W dalszej części Zamawiający przytoczył treść dokumentu zawartego na stronie https://www.cisco.com/c/en/us/products/collateral/wireless/adaptive-wireless-ips-software/data_sheet_c78-501388.html ,którego treść dołączono do niniejszego odwołania jako Załącznik nr 2 Karta katalogowa Cisco WiFi IPS (oryginalny tytuł: Cisco Wireless Intrusion Prevention System Data Sheet). Odniósł on się jednak do funkcjonalności aWIPS zawartej w licencji Cisco DNA Advantage, a w więc nie będącej przedmiotem oferty Odwołującego i nie dotyczącej wprost kontrolerów sieci bezprzewodowej, a więc nie będzie podlegać analizie (uzasadnienie zawarto w części A.0). Jednakże ten sam dokument zawiera potwierdzenie, że także zaoferowana wersja oprogramowania wspiera ochronę przed atakami sieciowymi na sieć bezprzewodową typu DoS co wprost wynika z zapisu zawartego z poniżej prezentowanej tabeli.

Rysunek 2 Funkcje i korzyści: Wykrywanie, klasyfikacja i łagodzenie nielegalnych działań (funkcjonalność Rogue)

Tłumaczenie

“CleanAir/Spectrum Intelligence

Detects rogue devices and DoS attacks in non-802.11 frequencies, such as Bluetooth, radar, and microwave”

„CleanAir/Inteligencja widma

Wykrywa nieuczciwe urządzenia i ataki DoS na częstotliwościach innych niż 802.11, takich jak Bluetooth, radar i mikrofale”

Zapis dotyczący CleanAir potwierdza funkcjonalność ochrony przed atakami sieciowymi na sieć bezprzewodową typu DoS, realizowaną przez Cisco DNA Essentials.

Dowód 9: Karta katalogowa Cisco WiFi IPS – Załącznik nr 2

W dalszej części uzasadnienia Zamawiający podniósł argument:

Powyższe ustalenie potwierdzają także informacje zawarte na stronie internetowej
producenta Cisco pod adresem:
https://www.cisco.com/c/en/us/td/docs/wireless/technology/wips/deployment/guide/WiPS_deployment_guide.html ,który to dokument jest datowany na dzień 16 marca 2017 roku, a więc dotyczy wersji produktów sprzed ponad 6 lat, a którego treść dołączono do niniejszego odwołania jako Załącznik nr 3 Przewodnik uruchomienia aWIPS.

Rysunek 3 Nagłówek przewodnika uruchomienia Cisco aWIPS

Załączona przez Zamawiającego tabela, która rzekomo miałaby dowodzić braku obsługi DoS w wersji oprogramowania Cisco DNA Essentials została pozbawiona nagłówka, który brzmi:

“**Over-the-Air Attacks**

Cisco Adaptive Wireless IPS embeds complete wireless threat detection and mitigation into the wireless network infrastructure to deliver the industry’s most comprehensive, accurate and operationally cost- effective wireless security solution. Below are the Over-the-Air attacks that are detected by the Cisco Adaptive wIPS solution.”

Tłumaczenie

Ataki z powietrza

„Cisco Adaptive Wireless IPS osadza w infrastrukturze sieci bezprzewodowej pełne wykrywanie i łagodzenie zagrożeń bezprzewodowych, aby zapewnić najbardziej wszechstronne, dokładne i opłacalne pod względem operacyjnym rozwiązanie bezpieczeństwa bezprzewodowego. Poniżej przedstawiono ataki Over-the-Air wykrywane przez rozwiązanie Cisco Adaptive wIPS.”

Ponadto z tabeli usunięto część wierszy. Oryginalny jej wygląd zaprezentowano poniżej.

Rysunek 4 Tabela prezentująca różnice funkcjonalności licencji w odniesieniu do ataków na sieć bezprzewodową

Tabela ta więc dowodzi, iż w wersji oprogramowania w roku 2017 przy atakach na sieć bezprzewodową nie były dostępne uaktualnienia sygnatur do systemu IPS dla sieci bezprzewodowych. Nie dowodzi to jednak, że system IPS w sieciach bezprzewodowych w ogóle wówczas nie był dostępny i że nie zapobiegał on atakom DoS. Co więcej powyższa tabela wręcz dowodzi, iż takie zapobieganie było możliwe już wówczas, o czym świadczą pozostałe funkcjonalności przytoczone przez Zamawiającego. Wprost dowodzi tego usunięty przez Zamawiającego jeden z wierszy o treści:

“Location tracking and containment for DoS attacker and non-authorized device that is trying to associate internal access point”

Tłumaczenie:

„Śledzenie lokalizacji i powstrzymywanie ataków DoS i nieautoryzowanych urządzeń, które próbują powiązać wewnętrzny punkt dostępu”.

Zatem przywołany przez Zamawiającego dokument nie tylko nie potwierdza jego tezy, a wręcz wprost jej zaprzecza i dowodzi, że ochrona przed atakami sieciowymi na sieć bezprzewodową typu DoS jest dostępna w każdej wersji oprogramowania.

Dowód 10: Przewodnik uruchomienia aWIPS – Załącznik nr 3

W dalszej części Zamawiający przywołuje następującą argumentację:

„Zamawiający w ramach dokonanej oceny ofert uwzględnił także informacje zawarte na
stronie internetowej producenta Cisco pod adresem
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-rogue-management-application/2-3-5/quick-start-guide/b_rogue_management_qsg_2_3_5/rogue_management_chapter_01.html#overview_waas w rozdziale „About Advanced Wireless Intrusion Prevention System” (z ang. „O
zaawansowanym bezprzewodowym systemie zapobiegania włamaniom”).”

W tym miejscu Zamawiający przytoczył funkcjonalności określone przez producenta jako Advanced WIPS (aWIPS), które zawiera oprogramowanie w wersji Cisco DNA Advantage (świadczy o tym nagłówek akapiyu, w którym znajduje się tekst), a które nie były przedmiotem oferty Odwołującego, a więc nie będą podlegać analizie (uzasadnienie w części A.0).

Na marginesie można jednak dodać, że zgodnie z przytoczonym dowodem stanowiącym Załącznik nr 14, także przytoczona lista, nie jest pełną listą możliwych ataków DoS. Należy w tym miejscu także podkreślić, że Zamawiający nie

wyspecyfikował żadnych rodzajów ataków DoS w SWZ, a więc na etapie oceny ofert nie może ich teraz definiować. Stanowiłoby to istotną modyfikację SWZ po terminie składania ofert.

Dowód 11: Szybki przewodnik do Cisco DNA Center Rogue Management i aplikacji aWIPS – Załącznik 14

Ze względu na fakt, iż żaden z przytoczonych przez Zamawiającego dowodu nie potwierdza jego tezy, a niektóre wprost potwierdzają tezę przeciwną, to nieprawdziwe jest również sformułowanie w zakresie licencji Cisco DNA Essentials, iż:

„Powyżej przywołane informacje ze stron producenta jednoznacznie potwierdzają, że funkcjonalność wymagana w Tomie III SWZ - OPZ zał. 1 pkt 1.1.4, Wymagania szczegółowe dla kontrolerów sieci bezprzewodowej – lokalne, Lp. 12 lit d), posiada oprogramowanie Cisco DNA na licencji Advantage, która zawiera funkcjonalność aWIPS. Wymagań Zamawiającego nie spełnia natomiast zaoferowane oprogramowanie Cisco DNA na licencji Essentials."

Odnosząc się jednak wprost do zapisów OPZ Odwołujący wskazuje, iż przykładami ataków sieciowych na sieć bezprzewodową typu DoS są:

•• Excessive 802.11 Association Failures (nadmierne nieprawidłowe próby podłączenia się)
•• Excessive 802.1X Authentication Failures (nadmierne nieprawidłowe próby autentykacji)
•• Excessive 802.1X Authentication Timeout (nadmierne błędy czasu autentykacji)
•• Excessive Web Authentication Failures (nadmierne próby autentykacji na portalu web)

W zaoferowanym kontrolerze WLC 9800 zaimplementowano polityki wyłączania klientów (Client Exclusion Policies), który to mechanizm umożliwia zarządzanie takimi atakami w sieci Wi-Fi poprzez tymczasowe wyłączanie klientów z dostępu do sieci. To pozwala na poprawę wydajności i jakości sieci poprzez tymczasowe odseparowanie problematycznych urządzeń.

Funkcjonalność ta jest zawarta w Cisco DNA w licencji Essentials a poniższy zrzut ekranu z konfiguracji zaoferowanego kontrolera potwierdza, iż funkcjonalność ta została na nim zaimplementowana.

Rysunek 5 Zrzut ekranu potwierdzający funkcjonalność kontrolera sieci bezprzewodowej w zakresie ochrony przez atakami typu DoS

Dowód 12: Zrzut z ekranu konfiguracyjnego zaoferowanego kontrolera sieci bezprzewodowej Cisco Catalyst 9800

Podsumowanie

Załączone dowody w postaci zapisów w Załącznikach nr 2 i 3 oraz zrzut ekranu z konfiguracji zaoferowanego kontrolera sieci bezprzewodowej jednoznacznie potwierdzają, że zgodnie z zapisami Tomu III SWZ - OPZ zał. 1 pkt 1.1.4, Wymagania szczegółowe dla kontrolerów sieci bezprzewodowej – lokalne, Lp. 12, kontroler posiada funkcje bezpieczeństwa w zakresie ochrony przed atakami sieciowymi na sieć bezprzewodową typu DoS, a żaden z przytoczonych przez Zamawiającego dowodów nie potwierdza, iż taka funkcjonalność nie została zaoferowana.

I.3 Niezgodność oferty z zapisami SWZ w zakresie mechanizmów bezpieczeństwa (posture, profilowanie urządzeń).

Zgodnie z Tomem III SWZ - OPZ zał. 5 rozdz. II, pkt 4. Ogólne wytyczne dot. bezpieczeństwa

Zamawiający wymagał:

„W ramach wdrożenia zostaną opracowane i dostarczone mechanizmy bezpieczeństwa a w szczególności:

(…)

- Analiza stanu stacji końcowych w aspekcie podłączających się do sieci (posture), profilowanie urządzeń oraz monitoring behawioralny".

Analiza dowodów Zamawiającego

Zamawiający uzasadnił niezgodność oferty z zapisami SWZ lakonicznie:

„W ramach badania oferty Konwerga Zamawiający ustalił, że oprogramowanie i licencje typu Cisco Identity Service Engine Advantage Subscription oraz Cisco ISE Device Admin Node License nie spełnia ww. wymagań w zakresie mechanizmów bezpieczeństwa (posture), co zostało ustalone na podstawie danych technicznych ze strony internetowej producenta Cisco https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/ise-licensing-guide-og.html".

Dokument ten stanowi Załącznik nr 5 Przewodnik licencjonowania Cisco ISE do niniejszego odwołania.

Zamawiający w swojej ocenie skupił się na samym słowie „posture", które jak słusznie sam zauważył trudno precyzyjnie przetłumaczyć. Istotne jest, że różni producenci różnie definiują zakres funkcjonalności noszących zbiorczą nazwę „posture". Dla Odwołującego nie budziło wątpliwości jaką definicję należy przyjąć przy doborze określonej wersji licencji, gdyż Zamawiający jasno i precyzyjnie zdefiniował w SWZ co rozumie przez posture, a mianowicie, analizę stanu stacji końcowych w aspekcie podłączających się do sieci. Tymczasem funkcjonalność Cisco posture znacznie wykracza poza tę, zdefiniowaną w SWZ. W przywołanym przez Zamawiającego dokumencie producent poprzez słowo „posture" rozumie „Compliance". Wprost wskazuje na to fragment tekstu:

"1.3 Compliance (Posture)

1.3.1 Why Compliance Visibility

Saboteurs focus on intentional data corruption (ransomware) and data exfiltration, which compromises endpoints on a network. The most effective and well-publicized compromises take advantage of known issues that could be simply remediated but were overlooked. Compliance Visibility allows organizations to view how user endpoints comply with corporate policy through the use of both Posture and/or integration through Mobile Device Management (MDM) and Enterprise Mobility Management (EMM) systems (supported MDM/EMM systems can be found in Cisco ISE Network Component Compatibility). Using either Cisco ISE's Posture engine or an MDM, an organization can evaluate how many endpoints are compliant, and ensure that noncompliant software is not installed and/or running."

Tłumaczenie

„1.3 Zgodność (posture)

1.3.1 Dlaczego widoczność zgodności

Sabotażyści koncentrują się na celowym uszkodzeniu danych (ransomware) i eksfiltracji danych, co zagraża punktom końcowym w sieci. Najbardziej skuteczne i dobrze rozpowszechnione zagrożenia wykorzystują znane problemy, które można było łatwo naprawić, ale zostały przeoczone. Widoczność zgodności pozwala organizacjom zobaczyć, w jaki sposób punkty końcowe użytkowników są zgodne z polityką korporacyjną dzięki wykorzystaniu zarówno posture, jak i integracji poprzez systemy zarządzania urządzeniami mobilnymi (MDM) i Enterprise Mobility Management (EMM) (obsługiwane systemy MDM/EMM można znaleźć w Cisco ISE Zgodność składników sieciowych). Korzystając z silnika Cisco ISE Posture lub MDM, organizacja może ocenić, ile punktów końcowych jest zgodnych i upewnić się, że niezgodne oprogramowanie nie jest zainstalowane i/lub nie jest uruchomione."

Jak słusznie zauważył Zamawiający tego typu funkcjonalność jest zawarta w licencji ISE Premier i nie jest ona przedmiotem oferty Odwołującego, a zatem nie będzie dalej analizowana (uzasadnienie w części A.0).

Dowód 13: Przewodnik licencjonowania Cisco ISE – Załącznik 5

Uzasadnienie Odwołującego

Tymczasem wymagana przez Zamawiającego funkcjonalność opisana w SWZ realizowana jest przez producenta Cisco Systems przez oprogramowanie w wersji ISE Advantage. Odwołujący zwraca uwagę na dokładnie ten sam fragment tekstu z zakreślonymi funkcjonalnościami i zamieszcza go poniżej.

Rysunek 6 Model licencjonowania ISE - funkcjonalność

Tłumaczenie:
1. „Profiling" „Profilowanie"
2. „Endpoint Analytics Visibility and Enforcement" „Widoczność i egzekwowanie analizy punktów końcowych"
3. „Rapid Threat Containment (Adaptive Network Control)" „Szybkie powstrzymywanie zagrożeń (adaptacyjna kontrola sieci)"
4. "Advantage (Context with Essentials)" "Advantage (zawiera Essentials)"
Z powyższego fragmentu wprost wynik, że licencja ISE Advantage zawiera profilowanie (Profiling), widoczność i egzekwowanie analizy punktów końcowych (Endpoint Analytics Visibility and Enforcement) oraz szybkie powstrzymywanie zagrożeń (Rapid Threat Containment).
Dowód 14: Przewodnik licencjonowania Cisco ISE – Załącznik 5
Na stronach producenta znajduje się dokument „Cisco AI Endpoint Analytics – Deployment guide" (adres: https://community.cisco.com/t5/networking-knowledge-base/cisco-ai-endpoint-analytics-deployment-guide/ta-p/4266702#toc-hld-1269897307; , który stanowi Załącznik nr 6 (Przewodnik wdrożenia - Cisco AI Endpoint Analytics)
W dokumencie tym czytamy między innymi:
Rysunek 7 Fragment dokumentu "Cisco AI Endpoint Analytics - Deployment guide" potwierdzający spełnianie wymogu analizy stanu stacji końcowych w aspekcie podłączających się do sieci, które zawarte jest w licencji Essentials
Tłumaczenie zaznaczonego fragmentu:
"Cisco AI Endpoint Analytics to rozwiązanie, które wykrywa i klasyfikuje punkty końcowe / urządzenia IOT według różnych etykiet, takich jak (typ punktu końcowego, model sprzętu, producent, typ systemu operacyjnego). Można to nazwać klasyfikacją wieloczynnikową (MFC) lub przypisywaniem wielu etykiet do punktów końcowych. Dużą zaletą tego rozwiązania jest kategoryzowanie punktów końcowych na różne sposoby, które można wykorzystać do egzekwowania zasad dostępu z ISE."
Powyższy dokument zawiera dokładny opis sposobu wykorzystania powyższych funkcjonalności wraz z konkretnymi wskazówkami konfiguracyjnymi. Na etapie wdrożenia zostaną opracowane i dostarczone mechanizmy bezpieczeństwa, co przełoży się na odpowiednią konfigurację rozwiązania Cisco ISE, które to z kolei przy wykorzystaniu „Endpoint Analytics Visibility and Enforcement" będzie zapewniać analizę stanu stacji końcowych w aspekcie podłączających się do sieci, a co stanowiło wymóg zawarty w SWZ.
Zamawiający błędnie skupił się na samym słowie „posture", którego jednak definicja producenta Cisco znacznie odbiega w swej treści od definicji użytej przez Zamawiającego w SWZ. Dokładna analiza zapisów SWZ przeprowadzona przez Odwołującego na etapie przygotowania oferty doprowadziła go do wniosku, iż Zamawiający oczekuje funkcjonalności zawartej w komponencie oprogramowania Endpoint Analytics Visibility and Enforcement (Dowód 15), co zostało wykazane powyżej, a które zwarte jest w licencji Cisco DNA Essentials (Dowód 14).
Dowód 15: Przewodnik wdrożenia - Cisco AI Endpoint Analytics – Załącznik 6
Z ostrożności Odwołujący potwierdza także spełnianie pozostałych funkcjonalności, których spełnienia Zamawiający wprost nie podważył.
Pierwszym z nich jest funkcjonalność profilowania urządzeń, która jak wynika z załączonego fragmentu (Rysunek 6), jest zawarta w licencji ISE Advantage, która została zaoferowana przez Odwołującego. Identyfikuje ona urządzenia próbujące uzyskać dostęp do sieci na podstawie zdefiniowanych wcześniej sond zbierających dane o każdym z nich.
Punkty końcowe (urządzenia) są profilowane na podstawie zasad określonych w ISE. Identyfikacja urządzenia końcowego odbywa się na podstawie spełnienia poszczególnych kryteriów, natomiast wynik końcowy powoduje przypisanie odpowiedniego profilu do urządzenia. Zadania te są realizowane przez mechanizm profilowania opisany szczegółowo w dokumencie – https://community.cisco.com/t5/security-knowledge-base/ise-profiling-design-guide/ta-p/3739456
Architekturę i składniki zasad profilowania w ISE przedstawia poniższy fragment.
Rysunek 8 Profilowanie urządzeń - wersja oryginalna
Tłumaczenie:
„Rysunek 2 Architektura i składniki zasad profilowania ISE
Z kolei wymagany przez zamawiającego monitoring behawioralny zapewnia mechanizm Rapid Threat Containment, który został precyzyjniej opisany w dokumencie na stronie producenta https://www.cisco.com/c/en/us/solutions/security/rapid-threat-containment/index.html , a którego treść stanowi Załącznik nr 8 (Cisco Rapid Threat Containment) do niniejszego odwołania. Rapid Threat Containment jest częścią oprogramowania Cisco ISE Advantage, co wprost wynika z Rysunku 6. Jego funkcjonalność potwierdzającą wymagania SWZ potwierdza poniższa grafika:
Rysunek 9 Zasada działania Rapid Threat Containment
Tłumaczenie zaznaczonego na zielono tekstu
1. "**Get answers faster** Organize user, device, and threat details on one platform for decisive action to counter the inevitable attacks" „**Szybciej otrzymuj odpowiedzi** Przetwarzaj szczegółowe informacje o użytkownikach, urządzeniach i zagrożeniach w ramach jednej platformy, aby zdecydowane przeciwdziałać nieuniknionym atakom."
2. "**Stop attacks faster** Block threats immediately by directing Cisco ISE to contain devices. Automatic responses provide protection based on threat level." „**Szybciej zatrzymuj ataki** Natychmiast blokuj zagrożenia, polecając Cisco ISE izolować urządzenia. Ochrona zapewniona jest przez reakcje automatyczne w oparciu o poziom zagrożenia."
3. "**Protect critical data faster** Dynamically change users' access privileges before or after they get on the network if their threat scores rise." „**Szybciej zabezpieczaj dane krytyczne** Dynamicznie zmieniaj uprawnienia dostępu użytkowników przed lub po ich wejściu do sieci, jeśli ich ocena zagrożenia wzrośnie."
Powyższy sposób działania stanowi monitoring behawioralny wymagany przez Zamawiającego w SWZ.
Dowód 16: Podręcznik projektowania ISE Profiling – adreshttps://community.cisco.com/t5/security-knowledge-base/ise-profiling-design-guide/ta-p/3739456
Dowód 17: Dokument „Cisco Rapid Threat Containment" - Załącznik nr 8
Podsumowanie
Przedstawione w tej części dowody potwierdzają, iż oferta złożona przez Odwołującego spełnia wymogi zawarte w Tomie III SWZ - OPZ zał. 5 rozdz. II, pkt 4. Ogólne wytyczne dot. bezpieczeństwa tj.
„W ramach wdrożenia zostaną opracowane i dostarczone mechanizmy bezpieczeństwa a w szczególności:
(…)
- Analiza stanu stacji końcowych w aspekcie podłączających się do sieci (posture), profilowanie urządzeń oraz monitoring behawioralny".
I.4 Niezgodność oferty z zapisami SWZ w zakresie analizy widma częstotliwościowego oraz wyświetlania analizy spektrum dla access-pointów.
Zgodnie z Tom III SWZ - OPZ zał. 1 pkt 1.1.2, Wymagania szczegółowe dla urządzeń Access point (AP) zewnętrzny, L.p. 13 Zamawiający wymagał:
„Funkcji analizy widma częstotliwościowego tj.:
a) zakres identyczny z częstotliwością modułów radiowych AP

b) współpraca z mechanizmami optymalizacji wykorzystania pasma radiowego
c) umożliwia skanowanie off-channel”
oraz zgodnie z Tomem III SWZ - OPZ zał. 1 pkt 2.1, Wymagania ogólne dla systemu CSZ, L.p. 33 Zamawiający wymagał:
„System musi posiadać funkcjonalność telemetrii (…)
•Wyświetlenie analizy spektrum dla access-pointów”.

Analiza dowodów Zamawiającego

Zamawiający uzasadnił niezgodność oferty z zapisami SWZ lakonicznie:
„W ramach badania oferty Konwerga Zamawiający powziął uzasadnione wątpliwości czy wymagane funkcjonalności analizy widma częstotliwościowego oraz wyświetlenia analizy spektrum dla access-pointów są zawarte w oprogramowaniu Cisco DNA na licencji Essentials.
Mając na uwadze powyższe ustalenia Zamawiający pismem z dnia 15.05.2023 r., znak: CIRF.DZ1.272.88.2022.GDYP.27, wezwał Konwergę do złożenia wyjaśnień treści oferty w ww. zakresie.
Wykonawca w piśmie z dnia 19.05.2023 r. wyjaśnił, że w jego opinii oferta spełnia postanowienia OPZ funkcjonalnością ClearAir zawartą w oprogramowaniu Network Essentials.
Zgodnie z wiedzą Zamawiającego oraz dokumentacją Cisco dostępna na stronie producenta https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/cleanair-technology/aag_c22-594304.pdf a także na podstawie dokumentów przekazanych przez Konwerga wraz z wyjaśnieniami z dnia 19.05.2023 r. ustalono, że ClearAir nie spełnia wymagania wyświetlenia analizy spektrum dla access-pointów z poziomu Centralnego Systemu Zarządzania, które zostało wyrażone w Tomie III SWZ - OPZ zał. 1 pkt 2.1, Wymagania ogólne dla systemu CSZ, L.p. 33.”
Zamawiający w tym miejscu nie powołał się na żaden fragmentu tekstu ze wskazanego dokumentu ani ze złożonych wyjaśnień uzasadniających stwierdzony wniosek (wskazany dokument stanowi Załącznik nr 9 do odwołania). Odwołujący analizując treść wskazanego dokumentu także nie znalazł żadnego potwierdzenia postawionej przez Zamawiającego tezy.
Ponadto bardzo istotnym jest fakt, iż wskazany dokument datowany jest na rok 2014, a więc nie dotyczy on obecnego rozwiązania Clean Air, a także współpracy z Cisco DNA Center (zarówno Essentials jak i Advantage), gdyż wówczas oprogramowanie to nie było jeszcze oferowane na rynku. Poniżej zawarto widok pierwszej strony tego dokumentu z rokiem jego publikacji (na ostatniej stronie wskazano także wersję C22-594304-03 i dokładniejszą datę publikacji jako 09/2014).

Rysunek 10 Pierwsza strona dokumentu Cisco Clean Air z zaznaczoną datą publikacji

Poniższy rysunek przedstawia dokładną wersję dokumentu.

Rysunek 11 Ostatnia strona dokumentu Cisco Clean Air z zaznaczoną datą publikacji oraz jego wersją

Oprogramowanie Cisco DNA Center zostało oficjalnie wydane w dniu 2 marca 2016 o czym świadczy fragment dokumentu opublikowany na stronie producenta pod adresem https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2016/m03/cisco-unveils-digital-network-architecture-to-accelerate-customer-digital-transformation.html , który to dokument stanowi Załącznik nr 10 do niniejszego odwołania (Informacja o udostępnieniu DNA Center)

Rysunek 12 Data udostępnienia Cisco DNA Center

Tłumaczenie:
1. „Mar 02, 2016” „2 marca 2016”
2. “Cisco today announces Digital Network Architecture (DNA)” “Cisco dzisiaj ogłasza udostępnienie Digital Network Architecture (DNA)”

Powyższe informacje dowodzą, iż Zamawiający podjął swoją wiedzę na podstawie dokumentu z 2014 roku opisującego technologię CleanAir, która nie mogła być częścią Cisco DNA Essentials, gdyż to oprogramowanie w ogóle nie było jeszcze dostępne na rynku. Oznacza to, że wiele zawartych w tym dokumencie informacji jest nieaktualnych, części nie ma. Z całą pewnością tamta wersja oprogramowania nie została zaoferowana przez Odwołującego.

Dowód 18: Dokument “Cisco Clean Air Technology” - Załącznik nr 9

Dowód 19: Informacja o udostępnieniu DNA Center – Załącznik nr 10

W dalszej części Zamawiający przeanalizował funkcjonalność oprogramowania Spectrum Analyzer, które nie było przedmiotem oferty Odwołującego, a więc nie będzie w tym miejscu podlegać dalszej analizie zgodnie z uzasadnieniem zawartym w części A.0. Na marginesie należy jedynie dodać, że wskazane przez Zamawiającego narzędzie znacznie wykracza funkcjonalnie poza wymagania zawarte w SWZ.
Z powyższych faktów wynika, że Zamawiający nie przedstawił żadnych dowodów na okoliczność nie spełnienia przez ofertę Odwołującego wymogów SWZ zawartych w Tomie III SWZ - OPZ zał. 1 pkt 1.1.2, Wymagania szczegółowe dla urządzeń Access point (AP) zewnętrzny, L.p. 13 oraz Tomie III SWZ - OPZ zał. 1 pkt 2.1, Wymagania ogólne dla systemu CSZ, L.p. 33.

Uzasadnienie Odwołującego

Analiza spektrum jest realizowana przez Cisco CleanAir o czym świadczy wiele dowodów. Pierwszy z nich można znaleźć na stronie https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-2/config-guide/b_wl_17_2_cg/b_wl_17_2_cg_chapter_010011001.html , której treść dotyczącą CleanAir stanowi Załącznik nr 11 do niniejszego odwołania (Analiza spektrum na kontrolerze przy wykorzystaniu Cisco CleanAir). Poniżej przedstawiono fragment tekstu potwierdzającego, iż Cisco CleaAir zawiera analizę spektrum dla access-pointów.

Rysunek 13 Zrzut ekranu z przewodnika konfiguracji kontrolera sieci bezprzewodowej potwierdzający funkcjonalność analizy spektrum dla access-pointów w oprogramowaniu Cisco CleanAir

Tłumaczenie:
1. “Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide” “Przewodnik konfiguracji kontrolera sieci bezprzewodowej serii Cisco Catalyst 9800”
2. “CleanAir Cisco CleanAir Bluetooth Low Energy Persistent Device Avoidance Spektrum Inteligence Spektrum Analysis” “CleanAir Cisco CleanAir Bluetooth Low Energy (technologia Bluetooth) Persistent Device Avoidance (trwałe unikanie urządzeń) Inteligencja spektrum Analiza spektrum”
3. “Cisco DNA Center receives a spectrogram stream from access points and visualizes spectrum analysis as a real-time spectrogram view. Network administrators receive RF violation issues from end users or radio frequency issue from the Cisco DNA Center. To analyze a violation, you should select the corresponding AP and analyze the spectrogram stream.” „Cisco DNA Center odbiera strumień spektrogramu z punktów dostępowych i wizualizuje analizę widma jako widok spektrogramu w czasie rzeczywistym. Administratorzy sieci otrzymują zgłoszenia dotyczące naruszeń RF od użytkowników końcowych lub problemów z częstotliwością radiową z Cisco DNA Center. Aby przeanalizować naruszenie, należy wybrać odpowiedni AP i przeanalizować strumień spektrogramu.”
4. “You can enable spectrum analysis on every AP listed in the web UI and view the graphs based on the corresponding AP. When enabled, the APs send spectrum data to Cisco DNA Centre which then aggregates it into 3 distinct charts.” „Można włączyć analizę widma na każdym punkcie dostępowym wymienionym w internetowym interfejsie użytkownika i przeglądać wykresy dotyczące punktu dostępowego. Po włączeniu punkty dostępowe wysyłają dane widma do Cisco DNA

Center, które następnie agregują je w 3 odrębne wykresy."
5. „Live Spectrum Analysis
You can perform a live spectrum analysis of the AP radios, and monitor the spectrum of frequencies generated by the radios of the corresponding AP using the web UI. The live spectrum capture uses radio 2 if it is available. Otherwise, both radio 0 and radio 1 are used. When you enable live spectrum analysis on radio 2, Cisco DNA Centre displays a consolidated view of the interference in both the 2.4 Ghz and 5 Ghz range. However; if the feature is enabled on radio 0 or radio 1, you can only view the part of the spectrum that the radios are associated with. You can select a radio in the web UI and view a live spectrum associated with this radio, for 10 minutes, and later extend the duration based on your requirement." „Analiza widma na żywo
Można przeprowadzić analizę widma na żywo radia AP i monitorować widmo częstotliwości generowane przez radia odpowiedniego AP za pomocą internetowego interfejsu użytkownika. Przechwytywanie widma na żywo wykorzystuje radio 2, jeśli jest dostępne. W przeciwnym razie używane jest zarówno radio 0, jak i radio 1. Po włączeniu analizy widma na żywo w radiu 2 Cisco DNA Center wyświetla skonsolidowany widok zakłóceń zarówno w zakresie 2,4 Ghz, jak i 5 Ghz. Jednakże jeśli ta funkcja jest włączona w radiu 0 lub radiu 1, można wyświetlić tylko część widma, z którą są powiązane radia. Można wybrać radio w internetowym interfejsie użytkownika i wyświetlić widmo na żywo powiązane z tym radiem przez 10 minut, a później wydłużyć czas trwania w zależności od wymagań."
Z powyższego rysunku wprost wynika, że analiza spektrum jest częścią CleanAir o czym świadczy układ menu. Nie ulega też wątpliwości, że analiza spektrum może być wyświetlana dla access-pointów na wiele sposobów o czym świadczą zapisy:
„Cisco DNA Center odbiera strumień spektrogramu z punktów dostępowych i wizualizuje analizę widma jako widok spektrogramu w czasie rzeczywistym. Administratorzy sieci otrzymują zgłoszenia dotyczące naruszeń RF od użytkowników końcowych lub problemów z częstotliwością radiową z Cisco DNA Center. Aby przeanalizować naruszenie, należy wybrać odpowiedni AP i przeanalizować strumień spektrogramu."
Oraz:
„Można włączyć analizę widma na każdym punkcie dostępowym wymienionym w internetowym interfejsie użytkownika i przeglądać wykresy dotyczące punktu dostępowego. Po włączeniu punkty dostępowe wysyłają dane widma do Cisco DNA Center, które następnie agregują je w 3 odrębne wykresy."
Oprogramowanie analizuje widno częstotliwościowe na żywo co potwierdza następujący zapis:
„Analiza widma na żywo
Można przeprowadzić analizę widma na żywo radia AP i monitorować widmo częstotliwości generowane przez radia odpowiedniego AP za pomocą internetowego interfejsu użytkownika. Przechwytywanie widma na żywo wykorzystuje radio 2, jeśli jest dostępne. W przeciwnym razie używane jest zarówno radio 0, jak i radio 1. Po włączeniu analizy widma na żywo w radiu 2 Cisco DNA Center wyświetla skonsolidowany widok zakłóceń zarówno w zakresie 2,4 Ghz, jak i 5 Ghz. Jednakże jeśli ta funkcja jest włączona w radiu 0 lub radiu 1, można wyświetlić tylko część widma, z którą są powiązane radia. Można wybrać radio w internetowym interfejsie użytkownika i wyświetlić widmo na żywo powiązane z tym radiem przez 10 minut, a później wydłużyć czas trwania w zależności od wymagań".
Dowód 20: Dokument „Analiza spektrum na kontrolerze przy wykorzystaniu Cisco CleanAir" – Załącznik 11
Odwołujący wskazuje ponadto na dokument zawierający pytania i odpowiedzi zamieszczone na stronie producenta pod adresem: https://www.cisco.com/c/en/us/products/collateral/software/one-wireless-subscription/nb-06-dna-acces-wl-sw-faq-ctp-en.html , których pełną treść stanowi Załącznik nr 12 Pytania i odpowiedzi do Cisco DNA.
Poniżej cytujemy jedno z pytań (strona nr 4 Załącznika nr 12):
„Q. If a customer purchases Cisco DNA Essentials or Advantage, do they still need to purchase an access point license?
A. No. Both tiers of the Cisco DNA solution include access point licenses in the packages. An access point license provides centralized configuration, policy, optimization of the wireless network, and innovations such as Identity PSK, Apple Fastlane and Fastlane + support, Cisco CleanAir technology, and flexible radio for access points. It serves as the foundation for other mobility services."
Tłumaczenie:
„Pyt. Jeśli klient kupi Cisco DNA Essentials lub Advantage, czy nadal musi kupować licencję na punkt dostępowy?
Odp. Nie. Oba poziomy rozwiązania Cisco DNA obejmują licencje na punkty dostępowe w pakietach. Licencja na punkt dostępowy zapewnia scentralizowaną konfigurację, politykę, optymalizację sieci bezprzewodowej oraz innowacje, takie jak Identity PSK, wsparcie Apple Fastlane i Fastlane +, technologię Cisco CleanAir oraz elastyczne radio dla punktów dostępowych. Służy jako podstawa dla innych usług mobilności."
Powyższa odpowiedź potwierdza, iż bez względu na wersję oprogramowania Cisco DNA (Essential i Advantage) Access Point (AP) będzie posiadał funkcjonalność wskazaną w SWZ jako optymalizację sieci bezprzewodowej (tożsame z wymaganiami SWZ w podpunkcie b – „współpraca z mechanizmami optymalizacji wykorzystania pasma radiowego") oraz technologię CleanAir spełniającą pozostałe wymagania stawiane AP tj.:
„Funkcje analizy widma częstotliwościowego:
a) zakres identyczny z częstotliwością modułów radiowych AP
c) umożliwia skanowanie off-channel"
Dowód 21: Dokument „Pytania i odpowiedzi do Cisco DNA" – Załącznik nr 12
Mechanizmem zbierającym i analizującym informacje o spektrum sygnału WiFi w kontrolerach 9800 jest Cisco Clean Air, natomiast reprezentacją tej analizy jest Quality Index (AQI). AQI jest wskaźnikiem służącym do indeksowania i raportowania jakość sygnału w ramach analizowanego spektrum radiowego. Szczegóły zostały przedstawione w dokumentacji poniżej zawartej na stronie: https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-2/config-guide/b_wl_17_2_cg/cisco_cleanair.html , która stanowi Załącznik nr 13 Przewodnik konfiguracji kontrolera sieci bezprzewodowej Cisco serii 9800; rozdział CleanAir. Poniżej zaprezentowano fragment tej dokumentacji:
Rysunek 14 Zrzut ekranu przewodnika konfiguracji kontrolera sieci bezprzewodowej; rozdział CleanAir
Tłumaczenie:
1. "Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide" "Przewodnik konfiguracji kontrolera sieci bezprzewodowej serii Cisco Catalyst 9800"
2. "CleanAir Cisco CleanAir Bluetooth Low Energy Persistent Device Avoidance Spektrum Inteligence Spektrum Analysis" "CleanAir Cisco CleanAir Bluetooth Low Energy (technologia Bluetooth) Persistent Device Avoidance (trwałe unikanie urządzeń) Inteligencja spektrum Analiza spektrum"
3. **"Information About Cisco CleanAir**Cisco CleanAir is a solution designed to proactively manage the challenges of a shared wireless spectrum. It allows you to see all the users of a shared spectrum (both native devices and foreign interferers). It also enables the network to act upon this information. For example, you can manually remove the interfering device, or the system can automatically change the channel away from the interference. CleanAir provides spectrum management and Radio Frequency (RF) visibility. A Cisco CleanAir system consists of CleanAir-enabled access points and Cisco Catalyst 9800 Series Wireless Controller . These access points collect information about all the devices that operate in the industrial, scientific, and medical (ISM) bands, identify and evaluate the information as a potential

interference source, and forward it to the controller . The controller controls the access points and displays the interference devices. For every device operating in the unlicensed band, Cisco CleanAir provides information about what it is, how it is impacting your wireless network, and what actions you or your network should take. It simplifies RF so that you do not have to be an RF expert. Wireless LAN systems operate in unlicensed 2.4-GHz and 5-GHz ISM bands. Many devices, such as microwave ovens, cordless phones, and Bluetooth devices also operate in these bands and can negatively affect the Wi-Fi operations. Some of the most advanced WLAN services, such as voice-over-wireless and IEEE 802.11 radio communications, might be significantly impaired by the interference caused by other legal users of the ISM bands. The integration of Cisco CleanAir functionality addresses this problem of RF interference."

„Informacje o Cisco CleanAir

Cisco CleanAir to rozwiązanie zaprojektowane do proaktywnego zarządzania wyzwaniami związanymi ze współdzielonym widmem bezprzewodowym. Pozwala zobaczyć wszystkich użytkowników współdzielonego widma (zarówno rodzimych urządzeń, jak i obcych zakłóceń). Umożliwia również sieci działanie na podstawie tych informacji. Na przykład można ręcznie usunąć urządzenie zakłócające lub system może automatycznie zmienić kanał z dala od źródła zakłóceń. CleanAir zapewnia zarządzanie widmem i widoczność częstotliwości radiowych (RF).

System Cisco CleanAir składa się z punktów dostępowych obsługujących technologię CleanAir oraz kontrolera bezprzewodowego Cisco serii Catalyst 9800. Te punkty dostępowe zbierają informacje o wszystkich urządzeniach pracujących w pasmach przemysłowych, naukowych i medycznych (ISM), identyfikują i oceniają te informacje jako potencjalne źródło zakłóceń i przekazują je do kontrolera. Kontroler steruje punktami dostępowymi i wyświetla urządzenia zakłócające.

Dla każdego urządzenia działającego w nielicencjonowanym paśmie Cisco CleanAir dostarcza informacji o tym, czym ono jest, jaki ma wpływ na Twoją sieć bezprzewodową i jakie działania powinieneś podjąć Ty lub Twoja sieć. Upraszcza RF, dzięki czemu nie musisz być ekspertem RF.

Bezprzewodowe systemy LAN działają w nielicencjonowanych pasmach ISM 2,4 GHz i 5 GHz. Wiele urządzeń, takich jak kuchenki mikrofalowe, telefony bezprzewodowe i urządzenia Bluetooth, również działa w tych pasmach i może negatywnie wpływać na działanie sieci Wi-Fi.

Niektóre z najbardziej zaawansowanych usług WLAN, takie jak komunikacja bezprzewodowa i radiowa IEEE 802.11, mogą być znacznie osłabione przez zakłócenia powodowane przez innych legalnych użytkowników pasm ISM. Integracja funkcji Cisco CleanAir rozwiązuje ten problem zakłóceń radiowych."

4. "AQI - Air Quality Index. The AQI is an indicator of air quality, based on the air pollutants. An AQI of 0 is bad and an AQI > 85 is good." „Indeks jakości pasma. AQI jest wskaźnikiem jakości pasma, opartym na zanieczyszczeniach pasma. AQI równy 0 jest zły, a AQI > 85 jest dobry."

Odwołujący wskazuje na fragment:

„Cisco CleanAir (…) Pozwala zobaczyć wszystkich użytkowników współdzielonego widma (zarówno rodzimych urządzeń, jak i obcych zakłóceń). Umożliwia również sieci działanie na podstawie tych informacji. Na przykład można ręcznie usunąć urządzenie zakłócające lub system może automatycznie zmienić kanał z dala od źródła zakłóceń. CleanAir zapewnia zarządzanie widmem i widoczność częstotliwości radiowych (RF).

System Cisco CleanAir składa się z punktów dostępowych obsługujących technologię CleanAir oraz kontrolera bezprzewodowego Cisco serii Catalyst 9800. Te punkty dostępowe zbierają informacje o wszystkich urządzeniach pracujących w pasmach przemysłowych, naukowych i medycznych (ISM), identyfikują i oceniają te informacje jako potencjalne źródło zakłóceń i przekazują je do kontrolera. Kontroler steruje punktami dostępowymi i wyświetla urządzenia zakłócające.

Dla każdego urządzenia działającego w nielicencjonowanym paśmie Cisco CleanAir dostarcza informacji o tym, czym ono jest, jaki ma wpływ na Twoją sieć bezprzewodową i jakie działania powinieneś podjąć Ty lub Twoja sieć. Upraszcza RF, dzięki czemu nie musisz być ekspertem RF.

Bezprzewodowe systemy LAN działają w nielicencjonowanych pasmach ISM 2,4 GHz i 5 GHz. Wiele urządzeń, takich jak kuchenki mikrofalowe, telefony bezprzewodowe i urządzenia Bluetooth, również działa w tych pasmach i może negatywnie wpływać na działanie sieci Wi-Fi.

Niektóre z najbardziej zaawansowanych usług WLAN, takie jak komunikacja bezprzewodowa i radiowa IEEE 802.11, mogą być znacznie osłabione przez zakłócenia powodowane przez innych legalnych użytkowników pasm ISM. Integracja funkcji Cisco CleanAir rozwiązuje ten problem zakłóceń radiowych."

Powyższy fragment dokumentacji potwierdza, iż Cisco CleanAir jest narzędziem realizującym wymogi zapisane w SWZ „Funkcji analizy widma częstotliwościowego tj.:

a) zakres identyczny z częstotliwością modułów radiowych AP

b) współpraca z mechanizmami optymalizacji wykorzystania pasma radiowego

c) umożliwia skanowanie off-channel"

Przy czym Odwołujący wyjaśnia, iż **skanowanie widma częstotliwościowego**:

a) „**zakresu identycznego z częstotliwością modułów radiowych AP**", to nic innego jak „Pozwala zobaczyć wszystkich użytkowników współdzielonego widma (zarówno rodzimych urządzeń, jak i obcych zakłóceń)"

b) „**współpraca z mechanizmami optymalizacji wykorzystania pasma radiowego**", to nic innego jak „Umożliwia również sieci działanie na podstawie tych informacji. Na przykład można ręcznie usunąć urządzenie zakłócające lub system może automatycznie zmienić kanał z dala od źródła zakłóceń. CleanAir zapewnia zarządzanie widmem i widoczność częstotliwości radiowych (RF)."

c) „**umożliwia skanowanie off-channel**", to nic innego jak „Bezprzewodowe systemy LAN działają w nielicencjonowanych pasmach ISM 2,4 GHz i 5 GHz. Wiele urządzeń, takich jak kuchenki mikrofalowe, telefony bezprzewodowe i urządzenia Bluetooth, również działa w tych pasmach i może negatywnie wpływać na działanie sieci Wi-Fi."

Dowód 22: Dokument „Przewodnik konfiguracji kontrolera sieci bezprzewodowej Cisco serii 9800"; rozdział CleanAir - Załącznik nr 13

Zamawiający w swoim uzasadnieniu nie negował wyjaśnień Odwołującego złożonych w dniu 19.05.23 w zakresie zawierania się funkcjonalności Cisco CleanAir w pakiecie Cisco DNA Essential. Odwołujący podtrzymuje swoje stanowisko w tej sprawie i w tym miejscu cytuje treść tych wyjaśnień (nie stanowiły one tajemnicy przedsiębiorstwa).

Wymagane przez Zamawiającego funkcje analizy widma częstotliwościowego to w przypadku zaoferowanych przez wykonawcę rozwiązań Cisco Systems funkcjonalność o nazwie CleanAir, która jest zawarta w pakiecie licencji Essentials. Informacja ze strony producenta: https://www.cisco.com/c/en/us/td/docs/wireless/access_point/feature-matrix/ap-feature-matrix.html

Ponadto na podanej przez Zamawiającego stronie nie ma informacji, że funkcje analizy widma częstotliwościowego wymagają licencji DNA Advantage. Sama analiza realizowana jest przez AP i mieści się w kategorii „Network Essentials" w zakresie „Optimized radio frequency". Kompatybilność tego oprogramowania z DNA Essentials wskazana jest wprost na tej stronie, gdzie w odniesieniu do typu licencji/Network Essentials wskazano:

„Perpetual software, compatible with Cisco DNA Essentials subscription license"

Tłumaczenie:

“Oprogramowanie wieczyste, kompatybilne z licencją subskrypcyjną Cisco DNA Essentials”
Poniżej znajduje się obraz strony z zaznaczonymi informacjami.
Dokładny opis funkcjonalności potwierdzający spełnianie wymagań SWZ znajduje się w załączniku „Cisco CleanAir_all”.
Pełna treść wspomnianego wyżej dokumentu porównującego funkcjonalności Cisco DNA stanowi Załącznik nr 1 do niniejszego odwołania, a załącznik do składanych wyjaśnień „Cisco CleanAir_all”, stanowi obecnie Załącznik nr 13 do niniejszego odwołania o nazwie „Przewodnik konfiguracji kontrolera sieci bezprzewodowej Cisco serii 9800”; rozdział CleanAir.
Dowód 23: Dokument „Przewodnik konfiguracji kontrolera sieci bezprzewodowej Cisco serii 9800”; rozdział CleanAir - Załącznik nr 13
Podsumowanie
Odwołujący przedstawił dowody na to, że w ramach licencji Cisco DNA Center Essentials zawarta jest funkcjonalność Cisco CleanAir, która z kolei w pełni spełnia wszystkie wymagania SWZ określone w Tomie III SWZ - OPZ zał. 1 pkt 1.1.2, Wymagania szczegółowe dla urządzeń Access point (AP) zewnętrzny, L.p. 13 oraz Tomie III SWZ - OPZ zał. 1 pkt 2.1, Wymagania ogólne dla systemu CSZ, L.p. 33. Zamawiający natomiast nie przedstawił żadnych dowodów na to, iż oferta nie spełnia wymagań SWZ w ww. punktach.
II.1 Niezgodność oferty z zapisami SWZ w zakresie funkcjonalności WIPS
Zgodnie z wymaganiami SWZ zawartymi w Tomie III Opis Przedmiotu Zamówienia (dalej „OPZ”) zał. 1 pkt 1.1.2 Wymagania szczegółowe dla urządzeń Access point (AP) zewnętrzny, L.p. 12 lit. l) Zamawiający wymagał aby licencja obsługiwała WIPS.
Brzmienie dokładne:
„1.1.2 Wymagania szczegółowe dla urządzeń Access point (AP) zewnętrzny.
(…)
Kategoria wymagania:
12. Zarządzanie przez kontroler WLAN z funkcjonalnościami:
(…)
l) obsługa WIPS”.
Analiza dowodów Zamawiającego
Zamawiający uzasadnił niezgodność oferty z zapisami SWZ:
„Zgodnie z wiedzą Zamawiającego, potwierdzoną poprzez treść dokumentacji producenta Cisco zawartą na stronie pod adresem https://www.cisco.com/c/en/us/products/collateral/wireless/adaptive-wireless-ips-software/data_sheet_c78-501388.html [Załącznik nr 2 do niniejszego odwołania] uznać należy, iż funkcjonalność Rogue Detection nie jest funkcjonalnością WIPS, ani też rozwiązaniem równoważnym do WIPS. Na powyższej stronie internetowej producent Cisco opisuje dwie różne funkcjonalności dostępne zarówno w oprogramowaniu oraz licencjach jakie oferuje: aWIPS oraz Rogue Detection. Producent rozróżnia te funkcjonalności nie tylko wprowadzając inne nazwy (aWIPS, Rogue Detection) ale przede wszystkim udostępnia w ich ramach różne rozwiązania techniczne oraz różny poziom ochrony przed atakami sieciowymi. Ponadto producent oferuje wskazane funkcjonalności na innym poziomie licencjonowania (Cisco DNA na licencji Advantage – aWIPS, Cisco DNA na licencji Essentials – Rogue Detection). Potwierdza to wprost poniższy zrzut z ww. strony producenta.
Tłumaczenie fragmentu oznaczonego kolorem żółtym:
Cisco aWIPS jest licencjonowanym zestawem funkcji programowych zawartym w oprogramowaniu Cisco DNA na licencji Advantage i jest dostępny dla wszystkich wydań. Funkcje Cisco Rogue management są dostępne z oprogramowaniem Cisco DNA na licencji Essentials.”
Zamawiający nie podał żadnych argumentów na podstawie których doszedł do przekonania, iż funkcjonalność Rogue Detection nie odpowiada zapisom SWZ w zakresie WIPS. W przytoczonej dokumentacji Odwołujący nie znalazł takich zapisów. Natomiast przytoczone przez Zamawiającego zapisy dotyczą Advanced WIPS (aWIPS), oprogramowania zawartego w wersji Cisco DNA Advantage, które nie było przedmiotem oferty Odwołującego, a więc nie będzie podlegać dalszej analizie (uzasadnienie w części A.0). Na marginesie należy jedynie zauważyć, że funkcjonalność aWIPS znacznie wykracza poza funkcjonalność opisaną przez Zamawiającego w SWZ.
Dowód 24: Karta katalogowa Cisco WiFi IPS – Załącznik nr 2
Uzasadnienie Odwołującego
W ramach postępowania Zamawiający użył nazwy nie mającej wspólnej i jednoznacznej definicji.
Ogólną definicję możemy znaleźć w zakresie IPS (WIPS, to Wereless IPS, czyli system IPS w sieciach bezprzewodowych) w „Słowniku kluczowych pojęć z zakresu cyberbezpieczeństwa NSC 7298 wer. 1.0” opracowanym przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa i dostępnym pod adresem https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjT5p6BjOyAAxW8EBAIHbC7AWg4ChAWegQIExAB&url=https%3A%2F%2Fwww.gov.pl%2Fattachment%2F48226cb6-29d4-49f9-860f-acd703072e60&usg=AOvVaw0dC0TtebGHolk35wk908bg&opi=89978449
„Intrusion Prevention System (IPS) – System prewencji włamań - System, który wykrywa włamania lub próby włamania, ale jest też zdolny do przeciwdziałania tym próbom, najlepiej zanim osiągną one zamierzony cel.”
Posiłkując się definicją Gartnera, uznanej firmy konsultingowej, na raporty której powołuje się wielu Zamawiających określając m.in. wymagania SWZ (https://www.gartner.com/en/information-technology/glossary/wips-wireless-intrusion-prevention-system), można przyjąć, że:
“Wireless Intrusion Prevention System (WIPS) - A wireless intrusion prevention system (WIPS) operates at the Layer 2 (data link layer) level of the Open Systems Interconnection model. WIPS can detect the presence of rogue or misconfigured devices and can prevent them from operating on wireless enterprise networks by scanning the network's RFs for denial of service and other forms of attack.”
Tłumaczenie:
„Bezprzewodowy system zapobiegania włamaniom (WIPS) działa na poziomie warstwy 2 (warstwa łącza danych) modelu Open Systems Interconnection. WIPS może wykryć obecność nielegalnych lub źle skonfigurowanych urządzeń i może uniemożliwić im działanie w bezprzewodowych sieciach korporacyjnych, skanując RF sieci pod kątem odmowy usługi i innych form ataku.”
W dokumentacji producenta pod adresem
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-rogue-management-application/2-3-3/quick-start-guide/b_rogue_management_qsg_2_3_3/rogue_management_chapter_01.html#overview_waas , która stanowi Załącznik nr 14 (Szybki przewodnik do Cisco DNA Center Rogue Management i aplikacji aWIPS) do niniejszego odwołania można znaleźć fragmenty tekstu potwierdzające wymaganą funkcjonalność
Rysunek 15 Fragment przewodnika konfiguracji Cisco DNA Center Rogue Management i aplikacji aWIPS potwierdzający funkcjonalność Rogue Management
Tłumaczenie:

„About Rogue Management
The Rogue Management application in Cisco DNA Center detects and classifies threats and enables network administrators, network operators, and security operators to monitor network threats. Cisco DNA Center helps in quickly identifying the highest-priority threats and allows you to monitor these threats in the Rogue and aWIPS dashboard within Cisco DNA Assurance."
„O Rogue Management
Aplikacja Rogue Management w Cisco DNA Center wykrywa i klasyfikuje zagrożenia oraz umożliwia administratorom sieci, operatorom sieci i operatorom bezpieczeństwa monitorowanie zagrożeń sieciowych. Cisco DNA Center pomaga w szybkiej identyfikacji zagrożeń o najwyższym priorytecie i umożliwia monitorowanie tych zagrożeń na pulpicie nawigacyjnym Rogue i aWIPS w Cisco DNA Assurance."
Ponadto w dokumentacji producenta dotyczącej zabezpieczeń stosowanych w Rogue Management pod adresem https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-rogue-management-application/2-3-3/quick-start-guide/b_rogue_management_qsg_2_3_3/rogue_management_chapter_05.html , która stanowi Załącznik nr 15 (Szybki przewodnik do Cisco DNA Center Rogue Management i aplikacji aWIPS; zabezpieczenia) odnajdujemy fragmenty tekstu potwierdzające spełnianie wymagań SWZ
Rysunek 16 Zrzut ekranu potwierdzający funkcjonalność Rogue Management w zakresie podejmowanych działań w przypadku wykrycia zagrożenia
Tłumaczenie:
"Rogue AP Containment Overview
The Cisco DNA Center Rogue AP Containment feature contains the wired and wireless Rogue AP. In case of Wired Rogue AP Containment, Cisco DNA Center brings the ACCESS mode switchport interface the DOWN state in which the rogue AP is attached. In case of Wireless Rogue AP Containment, Cisco DNA Center instructs the strongest detecting wireless controller to initiate containment on wireless rogue BSSIDs. The wireless controller in turn instructs the strongest detecting AP for those BSSIDs to stream the deauthentication packets to disrupt the communication between the rogue AP and the wireless clients of that rogue AP."
„Omówienie zabezpieczenia Rogue AP
Funkcja Cisco DNA Center Rogue AP Containment zawiera przewodowy i bezprzewodowy Rogue AP. W przypadku Wired Rogue AP Containment, Cisco DNA Center przełącza interfejs przełącznika trybu ACCESS w stan DOWN, w którym podłączony jest nielegalny AP. W przypadku odizolowania bezprzewodowego nielegalnego punktu dostępowego Cisco DNA Center instruuje najsilniejszy wykrywający kontroler bezprzewodowy, aby zainicjował zabezpieczenie bezprzewodowych nielegalnych identyfikatorów BSSID. Kontroler bezprzewodowy z kolei instruuje najsilniejszy wykrywający punkt dostępowy dla tych identyfikatorów BSSID, aby przesyłał strumieniowo pakiety cofnięcia uwierzytelnienia, aby zakłócić komunikację między nielegalnym punktem dostępowym a klientami bezprzewodowymi tego nielegalnego punktu dostępowego."
Przywołując definicję WIPS wg Gartnera można w łatwy sposób porównać wymaganą funkcjonalność z oferowaną.
Definicja:
„Bezprzewodowy system zapobiegania włamaniom (WIPS) działa na poziomie warstwy 2 (warstwa łącza danych) modelu Open Systems Interconnection. WIPS może wykryć obecność nielegalnych lub źle skonfigurowanych urządzeń…"
Zapisy producenta:
„Aplikacja Rogue Management w Cisco DNA Center wykrywa i klasyfikuje zagrożenia oraz umożliwia administratorom sieci, operatorom sieci i operatorom bezpieczeństwa monitorowanie zagrożeń sieciowych"
Definicja:
„… i może uniemożliwić im działanie w bezprzewodowych sieciach korporacyjnych, skanując RF sieci pod kątem odmowy usługi i innych form ataku."
Zapisy producenta:
„Funkcja Cisco DNA Center Rogue AP Containment zawiera przewodowy i bezprzewodowy Rogue AP. W przypadku Wired Rogue AP Containment, Cisco DNA Center przełącza interfejs przełącznika trybu ACCESS w stan DOWN, w którym podłączony jest nielegalny AP. W przypadku odizolowania bezprzewodowego nielegalnego punktu dostępowego Cisco DNA Center instruuje najsilniejszy wykrywający kontroler bezprzewodowy, aby zainicjował zabezpieczenie bezprzewodowych nielegalnych identyfikatorów BSSID. Kontroler bezprzewodowy z kolei instruuje najsilniejszy wykrywający punkt dostępowy dla tych identyfikatorów BSSID, aby przesyłał strumieniowo pakiety cofnięcia uwierzytelnienia, aby zakłócić komunikację między nielegalnym punktem dostępowym a klientami bezprzewodowymi tego nielegalnego punktu dostępowego."
Dowód 25: Definicja pojęcia WIPS wg Pełnomocnika Rządu ds. Cyberbezpieczeństwa (adres: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjT5p6BjOyAAxW8EBAIHbC7AWg4ChAWegQIExAB&url=https%3A%2F%2Fwww.gov.pl%2Fattachment%2F48226cb6-29d4-49f9-860f-acd703072e60&usg=AOvVaw0dC0TtebGHolk35wk908bg&opi=89978449)
Dowód 26: Definicja pojęcia WIPS wg Gartnera (adres:https://www.gartner.com/en/information-technology/glossary/wips-wireless-intrusion-prevention-system)
Dowód 27: Definicja pojęcia WIPS wg Cisco (adres:https://www.gartner.com/en/information-technology/glossary/wips-wireless-intrusion-prevention-system)
Dowód 28: Dokument „Szybki przewodnik do Cisco DNA Center Rogue Management i aplikacji aWIPS" – Załącznik nr 14
Dowód 29: Dokument „Szybki przewodnik do Cisco DNA Center Rogue Management i aplikacji aWIPS; zabezpieczenia" – Załącznik nr 15
Podsumowanie
Odwołujący przedstawił dowody na to, że w ramach licencji Cisco DNA Center Essentials zawarta jest funkcjonalność Cisco Rogue Management, która z kolei w pełni spełnia wszystkie wymagania SWZ określone Tomie III Opis Przedmiotu Zamówienia (dalej „OPZ") zał. 1 pkt 1.1.2 Wymagania szczegółowe dla urządzeń Access point (AP) zewnętrzny, L.p. 12 lit. l) w zakresie obsługi WIPS.
Zamawiający natomiast nie przedstawił żadnych dowodów na to, iż oferta nie spełnia wymagań SWZ w w tym punkcie.
B. Odtajnienie dokumentów zastrzeżonych jako tajemnica przedsiębiorstwa
Zamawiający w dniu 10.08.2023 w piśmie DZ-36 poinformował o podjęciu decyzji o odtajnieniu:
1. Wyjaśnień rażąco niskiej ceny złożonych w dniach 14.04.2023 (wezwanie z dnia 07.04.2023) oraz 17.05.2023 (wezwanie z dnia 09.05.2023)
2. Wyjaśnień w zakresie treści oferty złożonych w dniu 19.05.2023 (wezwanie z dnia 15.05.23).
Jako powód podjętej decyzji wskazał na brak spełnienia przesłanek 2 i 3 uznk. Istotne jest, że Zamawiający w swojej decyzji nie powołał się na przesłankę 1, a więc uznał, że przedstawione informacje mają wartość gospodarczą, a więc zgodził się, że niewątpliwie są to informacje istotne gospodarczo, których ujawnienie może spowodować poniesienie niewymiernych strat przez wykonawcę, którego dotyczą. Zamawiający nie uwzględnił w swojej decyzji jakie informacje

miałyby polegać odtajnieniu, gdyż nie zawarł takiego uzasadnienia w odniesieniu do konkretnych dokumentów czy informacji, a jedynie ogólnikowo odniósł się do wszystkich.
Należy w tym miejscu zwrócić uwagę, że informacje te mają całkowicie odmienny charakter – z jednej strony szczegółowe kalkulacje ceny wraz z obszernymi dowodami, a z drugiej informacje czysto techniczne także z dowodami.
Odwołujący zwraca uwagę, iż przy zastrzeganiu informacji dokładnie zbadał, które z nich powinny zostać objęte tajemnicą, a które nie. W wyniku tego procesu odpowiedzi tylko na część pytań zostały objęte tajemnicą, podczas gdy część z nich taką tajemnicą nie została objęta mimo, iż zostały one zadane jednocześnie.
Odwołujący złożył zatem wyjaśnienia techniczne w postaci dwóch plików wysłanych w tym samym dniu.
Dowód: pliki CIRF_wyjaśnienia_19.05.23 pkt_1_2.pdf (oznaczone jako tajemnica) oraz plik CIRF_wyjaśnienia_19.05.23 pkt 3_6 (oznaczone jako nie objęte tajemnicą).
Rysunek 17 - Zrzut ekranu z portalu przetargowego
W zakresie przesłanki 2 Zamawiający stwierdził iż:
„Wykonawca nie podołał obowiązki wykazania jej spełnienia.
Wskazać należy, że na potwierdzenie spełnienia omawianej przesłanki z uznk, Wykonawca uzasadnieniu zawarł zaledwie trzy akapity tekstu, które ocenić należy jako uzasadnienie ogólne, lakoniczne, możliwe do sporządzenia w zasadzie w każdym postępowaniu o udzielenie zamówienia i przez każdego wykonawcę."
W ocenie Odwołującego nie ma znaczenia objętość składanych oświadczeń, a Zamawiający powinien wskazać, które twierdzenia są niewystarczające biorąc także pod uwagę jakie informacje zamierza ujawnić.
Zgodnie z orzeczeniem KIO 1618/18:
„W orzecznictwie Izby zwraca się uwagę na trudności związane z wykazaniem okoliczności nieujawnienia do wiadomości publicznej zastrzeżonych informacji, jako że dowody w tym przypadku musiałyby potwierdzać okoliczność negatywną i w tym zakresie co do zasady wystarczające może być złożenie przez wykonawcę oświadczenia, podlegającego weryfikacji przez zamawiającego".
Oświadczenie takie o nieujawnieniu tych informacji znajduje się w uzasadnieniu Odwołującego i wyraża się między innymi w słowach:
„Utajnione informacje jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, a uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności. Są one tajemnicą dla podmiotów trzecich i wola ta dla innych osób jest rozpoznawalna."
Należy wziąć także pod uwagę charakter tych informacji. Wyjaśnienia rażąco niskiej zawierają cały szereg informacji które stanowią wartościową wiedzę firmy i czego Zamawiający nie kwestionuje. Podobnie wyjaśnienia techniczne w punktach w zakresie pytań 1 i 2 prezentują rozwiązania techniczne Odwołującego, które mają wpływ na końcową cenę oraz jakość całego systemu.
W zakresie przesłanki 3 Zamawiający zarzucił, iż:
„nie określił oraz jakie konkretnie dane, informacje lub dokumenty związane z przedmiotowym postępowaniem objęte są obowiązkiem zachowania tajemnicy podczas świadczenia pracy"
Zamawiający jednak dostrzegł, iż Odwołujący powołał się na obowiązujący system zarządzania jakością ISO 9001:2015, obowiązującą Politykę Bezpieczeństwa Informacji oraz potwierdzanie podpisem przez każdego pracownika zapoznania się z tymi dokumentami i obowiązku ich przestrzegania. Odwołujący na potwierdzenie dołączył także kopię certyfikatu ISO.
Należy zwrócić uwagę, że fakt posiadania aktualnego certyfikatu ISO oznacza, iż stosuje się zdefiniowane procedury i przestrzega określonych norm, czego potwierdzeniem są audyty certyfikowanej, renomowanej firmy audytorskiej SGS z siedzibą w Wielkiej Brytanii (informacje te znajdują się na załączonej kopii certyfikatu). Polityka Bezpieczeństwa Informacji jest integralną częścią wdrożonej normy ISO, a więc także jest przedmiotem audytu.
Biorąc pod uwagę treść zastrzeżonych informacji zarzut Zamawiającego jest co najmniej niezrozumiały. Oczywistym jest, że właśnie zastrzeżone informacje są objęte obowiązkiem zachowania tajemnicy podczas świadczenia pracy, ale także po jej ustaniu.
Dalej Zamawiający wskazał iż:
„W ocenie Zamawiającego uzasadnienie przedstawione przez Wykonawcę ma charakter ogólny. Z uwagi na brak załączenia jakichkolwiek dowodów nie sposób zweryfikować, czy informacje zawarte w Wyjaśnieniach i dowodach zostały zakwalifikowane jako informacje chronione i tym samym podlegają reżimowi uznk. Wykonawca w żaden sposób nie udowodnił ani nie wykazał, że zastrzeżone dokumenty podlegają ochronie. Ponadto Wykonawca nie określił chociażby kręgu pracowników zobowiązanych do zachowania poufności i w jakim zakresie oraz jakie konkretnie dane, informacje, dokumenty objęte są obowiązkiem zachowania tajemnicy w ramach stosunku pracy.
Rozpatrując natomiast kwestię zasadności zastrzeżenia jako tajemnicy przedsiębiorstwa załączonych do Wyjaśnień dowodów wskazać należy, że nie zostały one opatrzone żadnym zastrzeżeniem, że taką tajemnicą zawierają. W ich treści nie zawarto także żądnych klauzul o konieczności zachowania informacji w nich zawartych w poufności."
Nie można się zgodzić z ogólnikowymi zastrzeżeniami Zamawiającego, które nie mają potwierdzenia w zastrzeżeniu złożonym przez Odwołującego. Zawarł on bowiem dowód w postaci certyfikatu ISO, a ze względów bezpieczeństwa nie może on rozpowszechniać stosowanej Polityki Bezpieczeństwa Informacji, gdyż ujawnienie szczegółów wpłynęłoby na obniżeniu poziomu bezpieczeństwa informacji u Odwołującego, które przecież przetwarza informacje nie tylko związane z tym postępowaniem. Odwołujący chroni istotne informacje, a poprawność stosowanej ochrony podlega corocznemu audytowi wewnętrznemu jak i zewnętrznemu, co wprost wynika z wdrożonych procedur w ramach normy ISO 9001:2015.
Całkowicie niezrozumiałe jest także zastrzeżenie Zamawiającego dotyczące załączników. Odwołujący składając wyjaśnienia zawarł informacje w dokumencie dzieląc go na dokument główny i załączniki w celu lepszego uporządkowania informacji, ale miało to wyłącznie charakter edycyjny. Wszystkie załączniki stanowią integralną część dokumentu głównego i podlegają dokładnie takim samym obostrzeniom. Nie wymagały one zatem żadnych dodatkowych zastrzeżeń, czy klauzul.
Dowody:
1. certyfikat ISO wydany dla Konwerga sp. z o.o. ważny do dnia 20 kwietnia 2024r. – w dokumentacji postepowania
2. Uzasadnienie objęcia informacji tajemnicą przedsiębiorstwa z dnia 14.04.2023
Z uwagi na powyższe, w ocenie Odwołującego, materialna przesłanka uznania zastrzeżonych informacji za tajemnicę przedsiębiorstwa została przez Przystępującego spełniona. Istotnym jest również fakt, że zarówno aspekty techniczne objęte zastrzeżeniem informacji jak i rażąco niska cena nie były podstawą odrzucenia oferty Odwołującego.
Zamawiający w pisemnej odpowiedzi na odwołanie z dnia 4 września 2023 r. wnosił o oddalenie odwołania w całości.
Zamawiający wskazał, że:
Stan Faktyczny.
1) Zamawiający prowadzi postępowanie o udzielenie zamówienia w trybie przetargu nieograniczonego.
Przedmiotem zamówienia jest dostawa i wdrożenie Systemu Wi-Fi na przejściach granicznych wraz z Centralnym Systemem Zarządzania, (numer referencyjny postępowania: PN/71/22/GDYP).

W zakresie zamówienia podstawowego przedmiotem zamówienia jest wykonanie dostaw i usług na rzecz Zamawiającego w zakresie wdrożenia Systemu Wi-Fi na przejściach granicznych dla 24 lokalizacji wraz z Centralnym Systemem Zarządzania, spełniającego wymagania OPZ, stanowiącego TOM III SWZ. Celem zamówienia jest zbudowaniem jednolitego Systemu. Mając na uwadze, że powstanie jednolity, spójny, homogeniczny system informatyczny ze strukturą hierarchiczną i możliwością zarządzania wszystkimi lokalizacjami (przejścia graniczne) z poziomu CIRF konieczne jest zapewnienie na każdym etapie spójności i jednolitości rozwiązań.

2) Postępowanie wszczęto w dniu 30.12.2022 r. poprzez przekazanie ogłoszenia o zamówieniu Urzędowi Publikacji Unii Europejskiej, które opublikowane zostało w Dz. Urz. UE: 2023/S 003-006714 w dniu 04.01.2023 r.
3) Termin składania ofert upłynął w dniu 4.04.2023 r. Do upływu tego terminu wpłynęło 5 ofert.
4) W dniu 10.08.2023 r. Zamawiający opublikował oraz przesłał Wykonawcom informację o wyborze najkorzystniejszej oferty, za którą została uznana oferta wykonawcy Innegro System Sp. z o.o. z siedzibą w Warszawie (dalej: „Innergo").
5) Zamawiający odrzucił ofertę wykonawcy Konwerga na podstawie art. 226 ust. 1 pkt 5 ustawy Pzp, jako niezgodną z OPZ w zakresie:
I. niezgodności oferty wykonawcy Konwerga z wymaganiami dla CSZ:
1. Telemetria,
2. Ochrona przed atakami sieciowymi na sieć bezprzewodową,
3. Mechanizmy bezpieczeństwa (posture, profilowanie urządzeń),
4. Analiza widma częstotliwościowego oraz wyświetlenie analizy spektrum dla access-pointów;
II. niezgodności oferty wykonawcy Konwerga z wymaganiami dla lokalizacji:
1. Funkcjonalność WIPS,
2. Ochrona przed atakami sieciowymi na sieć bezprzewodową,
3. Analiza widma częstotliwościowego oraz wyświetlenie analizy spektrum dla access-pointów.
W piśmie z dnia 8.08.2023 r. (opublikowanym w dnu 10.08.2023 r.), zawierającym decyzję Zamawiającego o odrzuceniu oferty Odwołującego, stwierdzono m. in, że: „*Ustalenia dokonane poprzez skonfrontowanie oferty Odwołującego z informacjami zamieszczonymi na stronach internetowych producenta Cisco oraz wiedzą ekspercką Zamawiającego jednoznacznie dowodzą, że oprogramowanie zaoferowane przez Odwołującego, tj.:*
a) Cisco DNA na poziomie licencjonowania Essentials oraz oprogramowanie Network Essentials nie spełniają wymagań Zamawiającego przywołanych w rozdz. I pkt 1, 2 i 4 oraz rozdz. II pkt 1- 3 powyżej,
b) Cisco Identity Service Engine na poziomie licencjonowania Advantage Subscription oraz Cisco ISE Device Admin Node License nie spełnia wymagań Zamawiającego przywołanych w rozdz. I pkt 3 powyżej.
Nie sposób również przyjąć, że wyjaśnienia złożone przez Odwołującego potwierdzają, że zaoferowane oprogramowanie spełnia wymagania określone w Tomie III SWZ - OPZ. Natomiast w ramach oceny ofert ustalono, że Odwołujący nie zaoferował żadnego innego oprogramowania lub licencji posiadających wymienione w rozdz. I-II niniejszego pisma funkcjonalności, szczegółowo opisane w Tomie III SWZ – OPZ".
Przed merytorycznym odniesieniem się do poszczególnych zarzutów odwołania i argumentacji przedstawionej przez Odwołującego Zamawiający, chciałby poczynić uwagę o charakterze organizacyjnym, która dotyczy sposobu przedstawienia argumentacji odpowiedzi na odwołanie.
Otóż, z powodu zbieżności zarzutów i analogicznej argumentacji Zamawiający, odpowiadając na strukturę przyjętą przez wykonawcę Konwerga, w treści Odwołania, zaprezentuje argumentację wspólną dla zarzutów dotyczących:
1. Ochrony przed atakami sieciowymi na sieć bezprzewodową,
2. Analizy widma częstotliwościowego oraz wyświetlenie analizy spektrum dla access-pointów,
- które stanowiły podstawę do odrzucenia oferty Odwołującego w zakresie jej niezgodności z wymaganiami dla CSZ, jak i niezgodności z wymaganiami dla lokalizacji.
W pierwszej kolejności Zamawiający odniesie się do argumentacji Odwołującego, wspólnej dla wszystkich zarzutów, która została podana na str. 5-7 Odwołania.
Zaprezentowane stanowisko należy rozpocząć od wyjaśnienia kwestii ogólnych, związanych ze sposobem opisywania przez producenta Cisco w wydawanych dokumentach funkcjonalności, które są przypisane do danego oprogramowania oferowanego przez producenta. Opis oprogramowania przez producenta następuje przez wyodrębniania, w ramach oprogramowania, określonych poziomów licencji, od wersji „niższej" (która posiada minimalną liczbę funkcjonalności) do wersji „najwyższej" (która jest wersją najbogatszą w funkcjonalności oferowane przez producenta). Oznacza to, że oprogramowanie w wersji tzw. wyższej posiada wszystkie funkcjonalności oprogramowania w wersji niższej plus dodatkowe funkcjonalności.
Zatem, jeśli dana funkcjonalność pojawia się dopiero na określonym poziomie licencjonowania, a nie posiada jej wersja niższa, to producent to wyraźnie zaznacza. **Z powyższego wynika, że jeśli producent wyraźnie wskazuje że dana funkcjonalność jest dostępna dopiero na danym poziomie licencjonowania, to tym samym nie jest ona dostępna na niższym poziomie. Dana funkcjonalność staje się dostępna na poziomie wskazanym przez producenta oprogramowania.** Schodkowe ujęcie funkcjonalności produktu (w tym przypadku oprogramowania), w jego określonej wersji wydaje się być rozwiązaniem popularnym i praktykowanym, a także często spotykanym nie tylko w branży informatycznej, ale także poza nią (np. w branży motoryzacyjnej).
Zamawiający wskazuje, że treść uzasadnienia odrzucenia oferty Odwołującego wyraźnie wskazuje na braki w funkcjonalnościach zaoferowanego oprogramowania, dzieląc je na braki dotyczące CSZ i lokalizacji. Dodatkowo, mając na uwadze argumentację wskazaną w poprzednim akapicie, która dla Odwołującego jako podmiotu profesjonalnie zajmującego się IT jest oczywista, Zamawiający w uzasadnieniu faktycznym odrzuceniu nawiązał do wyższych wersji oprogramowania. Stąd też taki, a nie inny sposób skonstruowania przez Zamawiającego informacji o odrzuceniu oferty Odwołującego w piśmie z dnia 8.08.2023 r., w którym w sposób maksymalnie obrazowy, dodatkowo z wykorzystaniem opisu „wyższych" wersji oprogramowania Zamawiający wykazał braki danych funkcjonalności. **Oprogramowanie zaoferowane przez Odwołującego nie spełnia wymagań Zamawiającego, które wprost zostały wyartykułowane w OPZ, bowiem nie są one dostępne w zaoferowanym przez Odwołującego oprogramowaniu (poziomie licencjonowania).**
Nie sposób zgodzić się z twierdzeniem Odwołującego, że Zamawiający w informacji o odrzuceniu jego oferty powołuje się jedynie na dokumentację oprogramowania, które nie zostało zaoferowane przez Odwołującego, bowiem Zamawiający w treści uzasadnienia faktycznego odrzucenia wprost referował do oprogramowania zaoferowanych przez wykonawcę Konwerga. Świadczą o tym niezbicie chociażby odesłania zawarte w uzasadnieniu pisma.
Przykładowo, w zakresie Cisco ISE jest to dokument:
https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/ise-licensingguide-og.html Natomiast w odniesieniu do Cisco DNA jest to dokument:
https://www.cisco.com/c/m/en_us/products/software/dna-subscription-wireless/en-sw-sub-matrixwireless.

html. Co istotne, dokument przywołany przez Odwołującego:
https://www.cisco.com/c/en/us/products/collateral/software/dna-software-ebook-cte.html
nie zmienia stanowiska zajętego przez Zamawiającego w treści uzasadnienia odrzucenia oferty
Odwołującego, ponieważ z tego dokumentu nie wynika spełnienie wymagań Zamawiającego opisanych w OPZ. Co więcej, treść rozdziału „Wireless: Picking a tier" (tłum. Bezprzewodowo: Wybór poziomu) punkt „Cisco DNA Advantage" podpunkt „Cisco Adaptive Wireless Intrusion Prevention System" potwierdza prawidłowość decyzji Zamawiającego w zakresie braku spełnienia wymagań Zamawiającego w obszarze funkcjonalności WIPS, co stanowiło również podstawę do odrzucenia oferty wykonawcy Konwerga, opisaną w I pkt 2 pisma z dnia 8.08.2023 r., zawierającego informację o odrzuceniu oferty Odwołującego.
Dodatkowo, Zamawiający zauważa, że twierdzenia zawarte w odwołaniu, że zaoferowane oprogramowanie Cisco ISE Advantage spełnia wymagania SWZ są wyłącznie oświadczeniem
Odwołującego. Mają charakter gołosłownych, ponieważ Odwołujący nie przedstawił jakichkolwiek dowodów w tym zakresie, opierając się jedynie na własnych twierdzeniach, podczas, gdy w tym przypadku ciężar dowodu spoczywa na Odwołującym.
W tym miejscu zaznaczenia wymaga, że w sytuacji, gdy Odwołujący kwestionuje konkretne czynności dokonane przez Zamawiającego, co do zasady **ciężar dowodu spoczywa na Odwołującym, który z danego faktu wywodzi skutki prawne.** Odwołujący praktycznie przy każdym postawionym zarzucie referuje się do „obowiązku dowodowego" Zamawiającego podczas, gdy sam nie przedstawia dowodów na potwierdzenie tez postawionych w odwołaniu.
Zatem w przypadku zarzutów wadliwej czynności odrzucenia oferty Odwołującego ciężar dowodu w zakresie wykazania okoliczności, które uzasadniałby tezę przeciwną, spoczywa właśnie na Odwołującym.
Zamawiający ponownie zwraca uwagę na sposób opisywania funkcjonalności oprogramowania
przez producenta Cisco, które przytaczają obie Strony. Systematyka dokumentów wskazuje, że zwierają one jednoznaczny opis funkcjonalności, która występuje na danym poziomie licencjonowania. Innymi słowy, jeśli dana funkcjonalność wymieniona jest dopiero na wyższym poziomie licencjonowania oznacza to, że nie występuje ona na niższym poziomie licencjonowania. Fakt ten jest również wielokrotnie potwierdzony w przywołanym przez Odwołującego w punkcie Odwołania A.0, w dokumencie Cisco, m. in. w 1 wystąpieniu opisu dotyczącego Cisco DNA Advantage: „Cisco DNA Advantage is our premium tier that gives you the advantage of the latest innovative features. All the features mentioned in the Cisco DNA Essentials section are included in Advantage".
Tłumaczenie : Cisco DNA Advantage to nasz poziom premium, który zapewnia przewagę najnowszych innowacyjnych funkcji. Wszystkie funkcje wymienione w sekcji Cisco DNA Essentials są zawarte w Advantage.
Dokumenty Cisco są tak skonstruowane, że zgodnie z przytoczonym powyżej fragmentem przypisanie w nich danej funkcjonalności do danej licencji wyklucza tą funkcjonalność z niższych poziomów licencjonowania. Hierarchiczność licencjonowania Cisco jest również przejrzyście i jednoznacznie ukazana w przytoczonym przez Odwołującego dokumencie Cisco.
Tłumaczenie fragmentu zaznaczonego na żółto:
Poziomy we wszystkich trzech pakietach mają podobną, zagnieżdżoną strukturę.
Funkcje sieciowe i bezpieczeństwa oraz funkcje zarządzania są rozszerzane w każdym następującym po sobie poziomie.
Biorąc pod uwagę powyższe Zamawiający nie zgadza się z twierdzeniem Odwołującego, że niewłaściwe jest wskazywanie przez Zamawiającego, jakie licencje spełniają wymagania SWZ, bowiem treść uzasadnienia faktycznego odrzucenia wskazuje na braki funkcjonalności w zaoferowanym oprogramowaniu.
Uzasadnienie stanowiska Zamawiającego w zakresie zarzutu dotyczącego telemetrii.
Zamawiający w Tom III SWZ - OPZ w Załączniku 1 w pkt 2.1*Wymagania ogólne dla systemu CSZ*w Lp. 33 i Lp. 34 określił, jaki zakres co najmniej musi wchodzić w skład funkcjonalności telemetrii.
„33. System musi posiadać funkcjonalność telemetrii, w tym minimum:

- *Podgląd statystyk z zarządzanych urządzeń sieciowych*
- *Podgląd zdarzeń związanych z problemem z dostępem do sieci, np. analiza problemu związanego z uwierzytelnieniem 802.1x*
- *Możliwość importu topologii (np. planu budynku, piętra) do systemu centralnego zarządzania*
- *Możliwość zaznaczenia na zaimportowanej topologii lokalizacji zainstalowanych punktów dostępowych*
- *Przegląd tzw. heat map dla access-pointów*
- *Wyświetlenie analizy spektrum dla access-pointów*
- *Wyświetlanie statusów pracy przełączników i access-pointów*
- *Śledzenie procesu uzyskania dostępu klienta do sieci w środowisku z uwierzytelnianiem 802.1x, MAC authentication i Portal authentication*
- *Identyfikacja najpopularniejszych problemów sieciowych związanych z wydajnością interfejsów i sieci, roamingiem, procesem uwierzytelniania. Identyfikacja problemów sieciowych.*

34. Musi posiadać narzędzie pozwalające na monitoring wydajności sieci wraz z:
a) zbieraniem informacji o aplikacjach w sieci i parametrach ich działania
b) analizą, którzy użytkownicy generują najwięcej ruchu, z jakich korzystają aplikacji oraz jakie jest ich wykorzystanie".
Dowód: - treść wymagania opisanego w Załączniku nr 1 do OPZ w pkt 2.1 w Lp. 33 i Lp. 34 (str. 13), w dokumentacji Postępowania.
Zaznaczenia wymaga, że pomiędzy Stronami nie ma sporu co do tego, że dla systemu CSZ wykonawca Konwerga zaoferował oprogramowanie Cisco DNA na licencji Essentials. Zamawiający podtrzymuje stanowisko wyrażone w informacji o odrzuceniu oferty Odwołującego z uwagi na brak spełnienia wymagań w zakresie funkcjonalności telemetria. Żaden z argumentów przytoczonych przez Odwołującego nie potwierdza spełnienia wymagań z SWZ w zakresie telemetrii obejmujących:
- Możliwość importu topologii (np. planu budynku, piętra) do systemu centralnego zarządzania,
- Możliwość zaznaczenia na zaimportowanej topologii lokalizacji zainstalowanych punktów dostępowych,
- Przegląd tzw. heat map dla access-pointów,
- Wyświetlenie analizy spektrum dla access-pointów.

Natomiast z dokumentu Cisco, na który powołują się obie Strony w swojej argumentacji:
https://www.cisco.com/c/dam/m/en_us/products/software/dna-subscription-wireless/en-sw-submatrix-wireless/pdf/C95-742696-10_DNA_software_wireless_feature_matrix_v1a.pdfwynika niezbicie, że ww. wymagania SWZ są dostępne w oprogramowaniu Cisco DNA, ale w licencji
Advantage, a nie w licencji Essentials, a na tym poziomie licencjonowania zostało zaoferowane to oprogramowanie. Potwierdzeniem prawidłowości stanowiska Zamawiającego jest poniższa tabela, z której wprost wynika, że ww. funkcjonalności nie są dostępne na zaoferowanym poziomie licencjonowania Essentials (nie oznaczono tej funkcjonalności przy użyciu oznaczenia „tick").

Tłumaczenie fragmentów oznaczonych żółtym kolorem:
heetmapy i przewidywanie bezprzewodowej wydajności LAN
heetmapy z lokalizacją klientów, Analizator spektrum.

Co więcej, zaoferowane rozwiązanie nie tylko nie spełnia wymagań z punktu 33, ale również wymagania opisanego wyżej w pkt 34 lit. b) związanego z prowadzoną *analizą, którzy użytkownicy generują najwięcej ruchu, z jakich korzystają aplikacji oraz jakie jest ich wykorzystanie*. Odwołujący w argumentacji podniesionej w odwołaniu zupełnie nie odnosi się do tego wymagania pomimo, iż na str. 10-11 opisuje poszczególne cechy zaoferowanego oprogramowania. Tymczasem wymaganie określone w pkt 34 Zamawiający opierał się na monitorowaniu wydajności sieci wraz z zbieraniem informacje o aplikacjach w sieci i parametrach ich działania i analizą, którzy użytkownicy generują najwięcej ruchu, z jakich korzystają aplikacji oraz jakie jest ich wykorzystanie. **Konstrukcja wymagania przytoczona wyżej nakłada na wykonawcę obowiązek zaoferowania oprogramowania, które będzie nie tylko zbierać informacje o aplikacjach w sieci i parametrach ich działania ale także będzie umożliwiało przeprowadzenie analizy, którzy użytkownicy generują najwięcej ruchu, z jakich korzystają aplikacji oraz jakie jest ich wykorzystanie.**

Z jednej strony Odwołujący gołosłownie twierdzi, że zaoferował funkcjonalność telemetrii w kształcie wymaganym przez Zamawiającego w 34 podczas, gdy w przytoczony przez niego opis
funkcjonalności przeczy temu, aby zaoferowane rozwiązanie, opierające się o pulpit nawigacyjny stanu aplikacji potwierdzało spełnienie ww. wymagania Zamawiającego. Zgodnie ze stanowiskiem Odwołującego:

„Pulpit nawigacyjny stanu aplikacji

Wyświetla ogólny stan wszystkich aplikacji w sieci, *ze specjalną sekcją dotyczącą problemów związanych z aplikacjami biznesowymi i sugerowane środki zaradcze, zarządzane przez Cisco DNA Center". Pulpit nawigacyjny* ***umożliwia wyświetlenie*** *stanu wszystkich aplikacji w sieci, parametry ich działania a także sugeruje środki zaradcze. Natomiast dodatkowo pulpity nawigacyjne stanu klienta oraz sensora bezprzewodowego dostarczają cały szereg informacji o ruchu generowanym przez użytkowników.*

Zacytowany opis podany przez wykonawcę Konwerga w treści Odwołania prowadzi do wniosku, że zaoferowane oprogramowanie umożliwia wyświetlanie określonego zakresu
informacji podczas, gdy Zamawiającemu nie zależało na funkcjonalności mającej polegać na wyświetlaniu informacji w tzw. „czasie rzeczywistym", a na ich zbieraniu, a następnie przeprowadzaniu analizy „danych historycznych", celem dalszego wykorzystania.

Oczywistym i niewymagającym szerszej argumentacji jest to, iż czynności wyświetlania danych nie można zrównać z czynnością ich zbierania i analizowania. I już tylko ten wniosek jest wystarczający do tego, aby stwierdzić, że zaoferowane rozwiązanie nie spełnia wymagań Zamawiającego opisanych w pkt 34. Bezsprzecznym jest, że zaoferowane rozwiązanie nie zawiera narzędzia przeprowadzającego analizę określonych danych. Powyższe ustalenia przesądzają jednoznacznie o niezgodności oferty Odwołującego z wymaganiami Zamawiającego określonymi w OPZ, co w konsekwencji prowadzi do konieczności odrzucenia jego oferty na podstawie art. 226 ust. 1 pkt 5 ustawy Pzp. W związku z tym zgłoszony zarzut należy uznać za niezasadny.

Uzasadnienie stanowiska Zamawiającego w zakresie zarzutu dotyczącego ochrony przed atakami sieciowymi na sieć bezprzewodową.

Zgodnie z Tom III SWZ - OPZ w Załączniku 1 pkt 1.1.4 *Wymagania szczegółowe dla kontrolerów sieci bezprzewodowej – lokalne,* Lp. 12 lit. d), Zamawiający wymagał: *„Kontroler musi posiadać funkcje Bezpieczeństwa: (…) d) Ochrona przed atakami sieciowymi na sieć bezprzewodową, np. DoS, Management Frame Flood, fake AP".*

Dowód: - treść wymagania opisanego w Załączniku nr 1 do OPZ w pkt 1.1.4 w Lp. 12 (str. 5), w dokumentacji Postępowania.

Zaznaczenia wymaga, że pomiędzy Stronami nie ma sporu co do tego, że dla systemu CSZ wykonawca Konwerga zaoferował oprogramowanie Cisco DNA na licencji Essentials.

Rozwiązanie zaoferowane przez Odwołującego nie spełnia wymagań Zamawiającego w zakresie ochrony przed atakami sieciowymi na sieć bezprzewodową DoS, co zostało przez Zamawiającego ustalone na podstawie informacji zawartych na stronach internetowych producenta Cisco.

Odwołujący chcąc przekonać o słuszności swoich racji odwołuje się definicji pojęcia DoS, określonych przez inne podmioty publiczne, których Zamawiający nie neguje. Mają one jednak
marginalne znaczenie dla przedmiotowej sprawy. Odwołujący nawiązuje także do przeprowadzonych wizji lokalnych, w trakcie których zapoznał się z infrastrukturą w lokalizacjach. Niemniej jednak w żaden sposób nie można z ww. okoliczności wywodzić rezygnacji z wymagań opisanych w SWZ.

Zamawiający zgadza się z przytoczonymi definicjami i wyłącznie na marginesie wskazuje, że kwestia rozwiązań chroniących WAN RF przed atakami została przedstawiona poglądowo i nie zwalania wykonawcy systemu Wi-Fi z zapewnienia ochrony przed atakami sieciowymi na sieć bezprzewodową, który wykonawca ma zbudować. Opisane w załączniku nr 8 do OPZ rozwiązania nie zabezpieczają przed atakami na dostępność sieci bezprzewodowej (Wi-Fi). Tą ochronę zgodnie z SWZ ma zapewniać infrastruktura zamawiana w przedmiotowym Postępowaniu.

Zamawiający stwierdził, że **w ramach funkcjonalności Clean Air, na którą powołuje się Odwołujący (dostępnej na poziomie licnecjonowania Cisco DNA Essentials) nie ma zabezpieczenia przed atakami DoS w pasmie częstotliwości Wi-Fi, gdyż jak Odwołujący sam przyznał w treści Odwołania: „CleanAir/Inteligentne widma. Wykrywa nieuczciwe urządzenia i ataki DoS na częstotliwościach innych niż 802.11, takich jak Bluetooth, radar i mikrofale" (str. 17). Tymczasem Zamawiający w OPZ w TOMIE III w Załącznik nr 1 pkt 1.1.2 Lp. 2.jasno wskazał, że zamawiana sieć Wi-F ma działać na częstotliwości 802.11.**

Dowód: - treść wymagania opisanego w Załączniku nr 1 do OPZ w pkt 1.1.2 w Lp. 2 (str. 2), w dokumentacji Postępowania.

Wobec tego, skoro Odwołujący sam potwierdza, że w ofercie zapewnił ochronę przed atakami
sieciowymi na sieć bezprzewodową DoS poprzez funkcjonalności Clean Air, która nie pracuje na częstotliwościach 802.11, która była wymagana w OPZ (TOM III SWZ OPZ Załącznik nr 1 pkt 1.1.2 Lp. 2.), to nie ma potrzeby odnoszenia się do pozostałej argumentacji Odwołującego w zakresie funkcjonalności ochrony przed atakami sieciowymi na sieć bezprzewodową.

Podsumowując, stwierdzić należy, że nie budzi żadnych wątpliwości niezgodność oferty Odwołującego z wymaganiami Zamawiającego, a tym samym oferta wykonawcy Konwerga podlega odrzuceniu na podstawie art. 226 ust. 1 pkt 5 ustawy Pzp. W tym kontekście zgłoszony zarzut należy znać za bezzasadny.

Uzasadnienie stanowiska Zamawiającego w zakresie zarzutu dotyczącego mechanizmu bezpieczeństwa (posture, profilowanie urządzeń).

Zgodnie z Tomem III SWZ OPZ w Załączniku 5 rozdział II, pkt 4 *Ogólne wytyczne dot. bezpieczeństwa* Zamawiający wymagał *„W ramach wdrożenia zostaną opracowane i dostarczone mechanizmy bezpieczeństwa a w szczególności: (…)*
- Analiza stanu stacji końcowych w aspekcie podłączających się do sieci (posture), profilowanie urządzeń oraz monitoring behawioralny".

Dowód: - treść wymagania opisanego w Tomie III SWZ OPZ w Załączniku nr 5, pkt 4 (str. 3), w dokumentacji Postępowania.
Nie jest sporne między Stronami, że Odwołujący zaoferował oprogramowanie i licencje Cisco Identity Service Engine Advantage Subscription oraz Cisco ISE Device Admin Node License.
Z wymagań OPZ zacytowanych wyżej wynika, że Zamawiający oczekuje oprogramowania umożliwiającego zarówno profilowanie urządzeń oraz ich monitoring behawioralny oraz analizę stanu stacji końcowych w aspekcie podłączających się do sieci, którą Zamawiający zdefiniował
funkcjonalność „posture". Świadczy o tym zamieszczenie ww. treści przed słowem „posturę", które należy rozumieć, jako analizę stanu tych urządzeń pod kątem poprawności i bezpieczeństwa ich działania. Z tego względu bez znaczenia pozostaje definicja przywołana w odwołaniu, bowiem OPZ wprowadza własne rozumienie pojęcia „posturę".
Wyjaśnić należy, że ww. wymaganie Zamawiającego zostało określone trzema atrybutami:
a) analiza stanu stacji końcowych w aspekcie podłączających się do sieci (posture),
b) profilowanie urządzeń,
c) monitoring behawioralny.

W kontekście powyższego przyjąć należy, że Zamawiający wymagał aby zaoferowane oprogramowanie zapewniało możliwość korzystania ze wszystkich ww. trzech atrybutów. Zamawiający stoi na stanowisku, że oprogramowanie i licencje Cisco Identity Service Engine Advantage Subscription oraz Cisco ISE Device Admin Node License zaoferowane przez Odwołującego nie spełniają tego wymogu. Bezsprzecznym jest, że oprogramowanie i licencje zaoferowane przez Odwołującego zapewniają atrybuty określone w ww. lit. b i c, co wprost wynika zarówno z ustaleń Zamawiającego, jak i treści zawartych w odwołaniu. **Brak jest jednak atrybutu określonego w literze a jako „posturę".**
Zgodnie z dokumentem Cisco przytaczanym przez obie Strony funkcjonalność ta, wymaga licencji ISE Premier, która nie została zaoferowana przez wykonawcę Konwerga. Co istotne, powyższą okoliczność i prawidłowość stanowiska Zamawiającego potwierdza również sam Odwołujący, który w treści Odwołania stwierdził: „*Jak słusznie zauważył Zamawiający tego typu funkcjonalność jest zawarta w licencji ISE Premier i nie jest ona przedmiotem oferty Odwołującego" (str. 24).*
Biorąc pod uwagę powyższe stwierdzić należy, że oferta wykonawcy Konwerga nie spełnia postawionych w SWZ wymagań dotyczące funkcjonalności „posturę", czego konsekwencją jest konieczność odrzucenia jego oferty na podstawie art. 226 ust. 1 pkt 5 ustawy Pzp. Tym samym
zasadnym jest stwierdzenie, że Zamawiający prawidłowo dokonał czynności oceny oferty wykonawcy Konwerga, której wynikiem było wyeliminowanie wadliwej oferty z prowadzonego Postępowania.
Uzasadnienie stanowiska Zamawiającego w zakresie zarzutu dotyczącego analizy widma częstotliwościowego oraz wyświetlenie analizy spektrum dla access-pointów.
Zgodnie z Tom III SWZ - OPZ Załącznik 1 pkt 1.1.2 *Wymagania szczegółowe dla urządzeń Access point (AP) zewnętrzny,* L.p. 13 Zamawiający wymagał: *„Funkcji analizy widma częstotliwościowego tj.:*
a) zakres identyczny z częstotliwością modułów radiowych AP
b) współpraca z mechanizmami optymalizacji wykorzystania pasma radiowego
c) umożliwia skanowanie off-channel"
oraz zgodnie z Tomem III SWZ - OPZ załącznik 1 pkt 2.1 ***Wymagania ogólne dla systemu CSZ***, L.p. 33 Zamawiający wymagał: „*System musi posiadać funkcjonalność telemetrii (…) • Wyświetlenie analizy spektrum dla access-pointów*".

Dowód: - treść wymagania opisanego w Załączniku nr 1 do OPZ w pkt 1.1.6 w Lp. 13 (str. 3), w dokumentacji Postępowania.
- treść wymagania opisanego w Załączniku nr 1 do OPZ w pkt 2.1 w Lp. 33 (str. 13), w dokumentacji Postępowania.
Na kanwie powyższego, Zamawiający chciałby wyjaśnić, że treść omawianego wymagania OPZ dotyczącego „widma częstotliwości" lub „wyświetlenia analizy spektrum dla access-pointów" oznacza, że Zamawiający oczekiwał posiadania przez zaoferowane oprogramowanie całego obrazu widma/spektrum, co wiąże się z koniecznością prezentacji zakresu częstotliwości radiowych zgodnego z częstotliwością modułów radiowych AP na poziomie systemu CSZ.
Zamawiający podczas badania ofert ustalił, że w ramach tego wymagania wykonawca Konwerga posłużył się oprogramowaniem Cisco DNA na licencji Esencials, w ramach którego znajduje się funkcjonalność Cisco Clean Air, co nie jest sporne między Stronami. Odwołujący w treści uzasadnienia podniesionego zarzutu zdaje się jedynie kwestionować aktualność wskazywanych przez Zamawiającego dokumentów, a nie samo rozwiązanie, które Zamawiający ocenił jako niespełniające wymagania SWZ.
Powyższe stanowisko znajduje odzwierciedlenie w stwierdzeniu Odwołującego na str. 43 Odwołania: *„Zamawiający w swoim uzasadnieniu nie negował wyjaśnień Odwołującego złożonych w dniu 19.05.23 r. w zakresie zawierania się funkcjonalności Cisco Clean Air w pakiecie Cisco DNA Essential.Odwołujący podtrzymuje swoje stanowisko w tej sprawie (…)".*
Dowód: - treść uzasadnienia Odwołania w części I.4 na str. 43, w dokumentacji Postępowania.
Analiza niniejszego zarzutu wymaga wyjaśnienia, związanego z tym, że zamawiane rozwiązanie to system na który składa się warstwa centralna określona przez Zamawiającego jako Centralny System Zarządzania (dalej: „CSZ"), której zadaniem jest zarządzanie wszystkimi urządzeniami, znajdującymi się w różnych lokalizacjach na terenie RP, w tym kontrolerami. Z racji roli jaką pełni CSZ w zamawianym systemie Zamawiający był zobowiązany skwantyfikować wymagania dla urządzeń oraz dostarczanego wraz z nimi oprogramowania. Podkreślić przy tym należy, że urządzenia musiały zostać przypisane w taki sposób do oprogramowania na poziomie lokalizacji i CSZ, aby stanowiły spójną całość. Innymi słowy, jeśli Zamawiający ustalił w OPZ konkretne wymaganie dla CSZ, to wymagania dla urządzeń w lokalizacjach musiały je uwzględniać. Z racji różnorodnych rozwiązań dostępnych na rynku, pewne wymagania zostały przypisane do Systemu Wi-Fi
Kolejno odnosząc się do argumentacji Odwołującego, podnieść należy, że skupia się ona jedynie na spełnieniu wymagań postawionych dla oprogramowania w warstwie lokalnej, które zostały opisane w Tom III SWZ - OPZ Załącznik 1 pkt 1.1.2, *Wymagania szczegółowe dla urządzeń* w kształcie przytoczonym wyżej. Przy tym Odwołujący całkowicie pomija wymagania Zamawiającego, opisane dla systemu CSZ (Tom III SWZ - OPZ Załącznik 1 pkt 2.1 *Wymagania ogólne dla systemu CSZ*, Lp. 33) podczas, gdy to właśnie wymogi w zakresie były podstawą odrzucenia jego oferty na podstawie art. 226 ust. 1 pkt 5 ustawy Pzp. Wynika to wprost ze stwierdzenia zawartego w piśmie z dnia 8.08.23 r. w pkt I.4 (str. 10), gdzie Zamawiający podał: *„Zgodnie z wiedzą Zamawiającego oraz dokumentacją Cisco dostępną na stronie producenta (…) a także na podstawie dokumentów przekazanych przez Konwerga wraz z wyjaśnieniami z dnia 19.05.2023 r. ustalono, że* ***ClearAir nie spełnia wymagania wyświetlania analizy spectrum dla access-pointów z poziomu Centralnego Systemu Zarządzania, które zostało wyrażone w Tom III SWZ - OPZ zał. 1 pkt 2.1, Wymagania ogólne dla systemu CSZ, Lp. 33****".*

Dowód: - treść pisma Zamawiającego z dnia 8.08.2023 r. w pkt. I.4 (str. 9-11), w dokumentacji Postępowania.

Biorąc pod uwagę powyższe stwierdzić należy, że Zamawiający w swojej argumentacji w pkt I.4 w uzasadnieniu odrzucenia oferty wykonawcy Konwerga zakwestionował wyłącznie możliwości wyświetlania analizy spektrum z poziomu CSZ. Zamawiający nie podważa natomiast, iż zaoferowane oprogramowanie posiada możliwość wyświetlania analizy widma częstotliwościowego dla acces pointów z poziomu zaoferowanego przez Odwołującego kontrolera Cisco 9800. Wydaje się, że użyta przez Odwołującego argumentacja ma służyć temu, aby przekierować uwagę Izby na spełnienie przez Odwołującego wymagania w zakresie acces pointów dla oprogramowania w warstwie „lokalnej" i odsunięcie na dalszy plan braku w zakresie spełnienia wymagania w warstwie „centralnej", tj. dla systemu CSZ, które było podstawą odrzucenia oferty Odwołującego w pkt I.4.

Zamawiający podtrzymuje pogląd, który zaprezentował już w wcześniej, że aby wyświetlić analizę spektrum z poziomu CSZ potrzebna jest licencja Cisco DNA Advantage, która nie została przez Odwołującego zaoferowana**bowiem wykonawca ten zaoferował oprogramowanie Cisco DNA na niższym poziomie licencjonowania – Essentials**.

Zgodnie z treścią dokumentu, który został już przytoczony w piśmie z dnia 8.08.2023 r., zawierającym uzasadnienie odrzucenia oferty wykonawcy Konwerga (str. 10) uzyskanie funkcjonalności w kształcie opisanym przez Zamawiającego w OPZ wymaga zaoferowania licencji DNA Advantage z funkcjonalnością Spectrum Analyzer (tłumaczenie: analizator widma).

W tym kontekście nie budzi żadnych wątpliwości, że oprogramowanie Cisco DNA na licencji Essentials, które zaoferował Odwołujący nie spełnia wymagań Zamawiającego opisany w OPZ,

przytoczonych wyżej. Wobec tego za prawidłowe należy uznać działanie Zamawiającego, który

odrzucił oferty wykonawcy Konwerga na podstawie art. 226 ust. 1 pkt 5 ustawy Pzp, co powoduje, iż zasadnym jest twierdzenie, iż zgłoszony zarzut podlega oddaleniu.

Uzasadnienie stanowiska Zamawiającego w zakresie zarzutu dot. funkcjonalność WIPS.

Zgodnie z wymaganiami SWZ zawartymi w Tomie III OPZ w Załączniku 1 pkt 1.1.2 Wymagania

szczegółowe dla urządzeń Access point (AP) zewnętrzny, Lp. 12 lit. l) Zamawiający wymagał aby licencja obsługiwała WIPS. Wynika to z następującego zapisu: *„1.1.2 Wymagania szczegółowe dla urządzeń Access point (AP) zewnętrzny. (…) 12. Zarządzanie przez kontroler WLAN z funkcjonalnościami: l) obsługa WIPS".*

Dowód: - treść wymagania opisanego w Załączniku nr 1 do OPZ w pkt 1.1.2 w Lp. 12 (str. 2-3), w dokumentacji Postępowania.

Z ustaleń Zamawiającego wynika, że wykonawca Konwerga w tym zakresie zaoferował oprogramowanie Cisco DNA na licencji Essentials z funkcjonalnością Cisco Rogue, która nie jest wymaganą przez Zamawiającego funkcjonalnością WIPS.

Zamawiającym podtrzymuje swoje stanowisko wyrażone w piśmie z dnia 8.08.23 r., iż **zaoferowana przez Odwołującego funkcjonalność Rogue Detection nie jest funkcjonalnością WIPS, ani też rozwiązaniem równoważnym do WIPS. Funkcjonalność Rogue Detection jedynie jednym z elementów składowych funkcjonalności WIPS. Oznacza to, że Odwołujący zapewnił jedynie częściowe spełnienie funkcjonalności WIPS.** Powyższe rozważania znajduje jednoznaczne odzwierciedlenie w dokumentacji producenta, która została powołana przez Zamawiającego w treści ww. pisma.

Dowód: - treść pisma Zamawiającego o odrzuceniu oferty Odwołującego z dnia 8.08.23 r. w pkt II.1 (str. 11-12) , w dokumentacji Postępowania.

W kontekście powyższego za błędne należy uznać stanowisko Odwołującego, który w treści Odwołania zrównuje funkcjonalność Rogue Detection z funkcjonalnością WIPS. Na różnice między funkcjonalnością Rogue Detection a WIPS wskazuje również przytoczona przez samego Odwołującego definicja Gartnera, zgodnie z którą*„(…)WIPS może wykryć obecność nielegalnych lub źle skonfigurowanych urządzeń i może uniemożliwić im działanie w bezprzewodowych sieciach korporacyjnych, skanując RF **sieci pod kątem odmowy usługi** i innych form ataku".*

Kolejno Zamawiający odniesie się do stwierdzenia Odwołującego,*„że funkcjonalność aWIPS znacznie wykracza poza funkcjonalność opisaną przez Zamawiającego w SWZ".* Zamawiający

wyjaśnia, że wykazał, że wymagania zawarte w OPZ nie są spełnione przez funkcjonalność Rogue Detection, a mogłyby być spełnione przez funkcjonalność aWIPS, która wyczerpuje wymagania Zamawiającego postawione w OPZ.

Prawidłowa jest czynność Zamawiającego, który po dokonaniu oceny oferty Odwołującego oraz

jego wyjasnień uznał, że funkcjonalność Rogue Detection zaoferowana przez wykonawcę Konwerga w ramach oprogramowania Cisco DNA na licencji Essentials nie spełnia wymagania Zamawiającego opisanego w Tomie III OPZ w Załączniku 1 pkt 1.1.2 *Wymagania szczegółowe dla urządzeń Access point (AP) zewnętrzny*, Lp. 12 lit. l) w zakresie obsługi WIPS. Tym samym nie sposób uznać, że Zamawiający naruszył przepis art. 226 ust. 1 pkt 5 ustawy Pzp odrzucając ofertę wykonawcy Konwerga.

Z tych względów zarzut zgłoszony przez Odwołującego powinien podlegać oddaleniu.

Uzasadnienie stanowiska Zamawiającego w zakresie zarzutu dot. tajemnicy przedsiębiorstwa.

W zakresie ustaleń stanu faktycznego, w odniesieniu do omawianego zarzutu, Zamawiający wskazuje, że pismem z dnia 9.08.2023 r. poinformował o odtajnieniu informacji zastrzeżonych przez wykonawcę Konwerga, jako tajemnica przedsiębiorstwa, zawartych w wyjaśnieniach rażąco niskiej ceny wraz z dowodami złożonych w dniu 14.04.2023 r. i 19.05.2023 r. oraz wyjaśnień w zakresie treści oferty wraz z dowodami złożonych w dniu 19.05.2023 r.

Zamawiający w treści przedmiotowego pisma wskazał, że wykonawca Konwerga nie wykazał w sposób dostateczny, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisu art. 11 ust. 2 Uznk.

Dowód: - treść pisma Zamawiającego z dnia 09.08.2023 r., w dokumentacji Postępowania.

Zgodnie z ustaloną linią orzeczniczą Izby, aby skutecznie zastrzec informacje, jako tajemnicę przedsiębiorstwa, należy spełnić łącznie trzy przesłanki wymienione w Uznk. Tym samym wykonawca, składając dokumenty zawierające informacje stanowiące – według niego – tajemnicę przedsiębiorstwa, musi wykazać, że zastrzegane informacje taką tajemnicę stanowią.

Zamawiający w pełni podtrzymuje argumentację zaprezentowaną w piśmie z dnia 9.08.2023 r., a tym samym konsekwentnie stoi na stanowisku, że Odwołujący nie sprostał ustawowemu obowiązkowi wprost wskazanemu w przepisie art. 18 ust. 3 ustawy Pzp, który uzależnia możliwość pozostawienia w poufności zastrzeżonych informacji pod warunkiem wykazania przez wykonawcę zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów Uznk.

Niewykazanie zasadności zastrzeżenia tajemnicy przedsiębiorstwa należy uznać za równoznaczne ze stwierdzeniem, że określone informacje podlegają ujawnieniu. Oznacza to, że dane informacje mogą rzeczywiście stanowić tajemnicę przedsiębiorstwa, ale wykonawca, poza subiektywnym przekonaniem, że informacje te – ze względu na jego interes – nie powinny zostać ujawnione, powinien wykazać, że nie należy ich ujawniać, jako że stanowią tajemnicę przedsiębiorstwa. Z utrwalonego orzecznictwa wynika, że wykonawca powinien starannie i z rozwagą formułować uzasadnienie zastrzeżenia tajemnicy przedsiębiorstwa, a *„samo powoływanie się na klauzule poufności, bez jakiegokolwiek podania ku temu powodów, nie może uzasadniać uznania zastrzeżenia tajemnicy przedsiębiorstwa za skuteczne, a jedynie stwarza*

wrażenie, że klauzule te są wyłącznie pretekstem do uniemożliwienia konkurencji weryfikacji oferty wykonawcy".

Powyższy pogląd został potwierdzony przez Sąd Okręgowy w Warszawie w uzasadnieniu wyroku z dnia 28 kwietnia 2023 r. w sprawie o sygn. akt XXIII Zs 24/23, w którym stwierdzono, że: *„w postępowaniu o udzielenie zamówienia publicznego oprócz spełnienia przesłanek z art. 11 ust. 2 uznk, do skutecznego zastrzeżenia tajemnicy przedsiębiorstwa niezbędne jest także wykazanie tego przez wykonawcę. Wykonawca zobowiązany jest zatem wykazać, iż zostały podjęte przez niego działania mające na celu zachowanie objętych przez niego tajemnicą przedsiębiorstwa informacji w tajemnicy, tj. iż objęte nią informacje nie były dostępne osobom trzecim w normalnym toku zdarzeń, bez żadnych specjalnych starań z ich strony, nie zostały one ujawnione do wiadomości publicznej, a także, że posiadają one określoną wartość. Przy czym podkreślić należy, że tajemnica przedsiębiorstwa jako wyjątek od zasady jawności postępowania powinna być interpretowana w sposób ścisły, a zamawiający powinien z należytą starannością zweryfikować zasadność utajnienia oferty. Ciężar dowodu, że dana zastrzeżona informacja stanowi tajemnicę przedsiębiorstwa spoczywa na wykonawcy, który takiego zastrzeżenia dokonuje. Zamawiający nie może bezkrytycznie akceptować zastrzeżenia tajemnicy przedsiębiorstwa, lecz winien żądać od wykonawcy wykazania i co najmniej uprawdopodobnienia, że zastrzeżenie tajemnicy przedsiębiorstwa nastąpiło w sposób uprawniony, zaś brak wyjaśnień lub udzielenie zbyt ogólnikowych wyjaśnień winno wskazywać na niezasadność dokonanego zastrzeżenia. Nadto warto nadmienić, że obowiązek "wykazania" oznacza coś więcej aniżeli wyjaśnienie (uzasadnienie) przyczyn co do objęcia tajemnicą przedsiębiorstwa. Za wykazanie nie może być uznane ogólne uzasadnienie, sprowadzając się de facto do przytoczenia jedynie elementów definicji legalnej tajemnicy przedsiębiorstwa, wynikającej z przepisu art. 11 ust. 2 ustawy o zwalczaniu nieuczciwej konkurencji bądź gołosłowne zapewnienie, że zastrzegana informacja ma walor tajemnicy przedsiębiorstwa oraz powoływanie się na bogate orzecznictwo Izby i sądów powszechnych dotyczące tej materii. Ocenie zamawiającego podlegać powinna również okoliczność, czy wykonawca zastrzegający dane informacje przedstawił dowody na potwierdzenie tez zawartych w uzasadnieniu zastrzeżenia*".

Kolejno Zamawiający odniesie się do argumentacji zaprezentowanej przez wykonawcę Konwerga w Odwołaniu. Przede wszystkim za irrelewantne należy uznać stwierdzenie Odwołującego, który za istotne uznał to, iż w swojej decyzji Zamawiający nie powołał się przesłankę 1, a więc uznał, że przedstawione informacje mają wartość gospodarczą.

Odwołujący zdaje się nie wiedzieć lub też celowo pomija, **że aby określone informacje mogły zostać uznane za tajemnicę przedsiębiorstwa, muszą w stosunku do nich zostać spełnione łącznie wszystkie przesłanki wskazane przepisie art. 11 ust. 2 Uznk. W tym miejscu podkreślenia wymaga, że w sytuacji, gdy okaże się, że jedna z tych przesłanek nie zostanie spełniona, to określona informacja nie stanowi tajemnicy przedsiębiorstwa i każdy może z niej korzystać bez ograniczeń.** Wobec tego wykonawca, który chce skutecznie utajnić informacje przedstawiane

Zamawiającemu w postępowaniu o udzielenie zamówienia, zobowiązany jest wykazać kumulatywne spełnienie przesłanek wynikających z definicji legalnej tajemnicy przedsiębiorstwa zawartej *de lege lata* w art. 11 ust. 2 Uznk, czyli że zastrzegane informacje: po pierwsze – mają charakter techniczny, technologiczny, organizacyjny przedsiębiorstwa lub inny posiadający wartość gospodarczą, po drugie – jako całość lub w szczególnym zestawieniu i zbiorze nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób. Po trzecie – że uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności. Natomiast rolą Zamawiającego w toku badania ofert jest ustalenie czy wykonawca temu obowiązkowi sprostał udowadniając, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa (KIO 2664/21 i KIO 2665/21)**Zatem najistotniejsze jest to, że skoro Zamawiający uznał, że nie zostały spełnione przesłanki 2 i 3, co opisał w treści informacji przekazanej wykonawcy Konwerga, co wykonawca ten potwierdza w treści Odwołania (str. 52), to stwierdzić należy, że kwestia spełnienia przesłanki 1 nie ma znaczenia.**

Odnosząc się do kwestii argumentacji Odwołującego w zakresie przesłanki 2 Zamawiający wyjaśnia, że Odwołujący ograniczył się jedynie do ogólnego stwierdzenia, które praktycznie stanowi powielenie brzmienia przepisu art. 11 ust. 2 Uznk. Tego rodzaju działanie wykonawcy Konwerga Zamawiający ocenił negatywnie uznając, że wykonawca nie wykazał, nie opisał w sposób prawidłowy spełnienia przesłanki 2.

Podobne stanowisko należy zaprezentować względem wykazania przesłanki 3, dotyczącej działań podejmowanych przez wykonawcę Konwerga w celu zachowania zastrzeżonych informacji w poufności. W tym zakresie Odwołujący ograniczył się do ogólnych wyjaśnień, bez wykazania podjętych działań w stosunku do konkretnych informacji złożonych w Postępowaniu. Wykonawca Konwerga nie przedstawił żadnych dowodów, ograniczając się jedynie do złożenia Certyfikatu ISO, który potwierdza, że wykonawcy legitymuje się tego rodzaju dokumentem w odniesieniu do „Projektowania, wykonawstwa i serwisu urządzeń teleinformatycznych". Jednak z powyższego dokumentu, wbrew twierdzeniom Odwołującego, nie wynikają jakiekolwiek informacje na temat działań podejmowanych w zakresie zachowania określonego katalogu informacji w poufności. Co więcej, wykonawca Konwerga powołuje się na dokument taki, jak Polityka Bezpieczeństwa, którego to dokumentu nie przedstawia.

Podobne wnioski należy wysnuć także względem argumentacji dotyczącej tego, że każdy pracownik potwierdza podpisem obowiązek przestrzegania Polityki Bezpieczeństwa. Na potwierdzenie powołanej okoliczności Odwołujący nie przedstawił jakiekolwiek dowodu, np. w postaci oświadczenia złożonego przez pracownika, mającego dostęp do informacji, dotyczących tego Postępowania lub umowy o zachowaniu poufności. Tym samym Zamawiający na podstawie ogólnikowych wyjaśnień i przy praktycznym braku dowodów ze strony Odwołującego uznał, że wykonawca Konwerga nie wykazał w sposób dostateczny ziszczenia się przesłanki 3, związanej z podejmowaniem przez tego wykonawcę odpowiednich środków celem zachowania w poufności informacji, które zostały przez niego zastrzeżone.

Biorąc pod uwagę powyższy stan faktyczny Zamawiający stwierdził, że wykonawca Konwerga nie wykazał kumulatywnego spełnienia przesłanek wskazanych w art. 11 ust. 2 Uznk. Skutkiem powyższego - po stronie Zamawiającego – było powstanie obowiązku ujawnienia informacji nieskutecznie zastrzeżonych przez wykonawcę Konwerga. Wobec tego, w tym przypadku Zamawiający nie dopuścił się naruszenia art. 18 ust. 3 ustawy Pzp w zw. z art. 11 ust. 2 Uznk, co próbuje bezskutecznie wykazać Odwołujący.

Konkludując stwierdzić należy, że Zamawiający przeprowadził czynność oceny oferty wykonawcy Konwerga w sposób prawidłowy, a jej konsekwencją było jej odrzucenie na podstawie art. 226 ust. 1 pkt 5 ustawy Pzp z powodów opisanych wyżej. Tym samym w działaniu Zamawiającego nie sposób dopatrzyć się naruszenia art. 239 ust. 1 ustawy Pzp, mającego polegać na wadliwym dokonaniu wyboru oferty nie najkorzystniejszej. Analogiczne stanowisko należy względem naruszenia przez Zamawiającego przepisu art. 18 ust. 3 ustawy Pzp w zw. z art. 11 ust. 2 Uznk.

Stan faktyczny ustalony przez Izbę:

W dniu 21 sierpnia 2023 r. wykonawca Konwerga Sp. z o.o. z siedzibą w Poznaniu wniósł odwołanie od niezgodnych z przepisami Ustawy czynności Zamawiającego podjętych w postępowaniu tj.:

A. czynności odrzucenia oferty Odwołującego jako niezgodnej z SWZ,

B. czynności wyboru oferty złożonej przez wykonawcę Innergo Systems sp. z o.o. jako najkorzystniejszej

C. decyzji Zamawiającego o odtajnieniu części informacji skutecznie zdaniem Odwołującego zastrzeżonych jako tajemnica przedsiębiorstwa przesłanych przez niego w dniu 14.04.2023 i 17.05.2023 jako wyjaśnienia rażąco niskiej ceny oraz w dniu 19.05.2023 jako wyjaśnienia techniczne w zakresie złożonej oferty.

Odwołujący zarzucił naruszenie przepisów przez Zamawiającego:

A. naruszenie art. 226 ust.1 pkt 5 Ustawy poprzez bezpodstawne odrzucenie oferty Odwołującego, pomimo, że jej treść odpowiada SIWZ

B. naruszenie art. 239 ust. 1 Ustawy poprzez dokonanie wyboru oferty nie najkorzystniejszej

C. naruszenie art. 18 ust. 3 ustawy PZP w zw. z art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j, Dz.U. z 2020 r. poz.1983 ze zm.).

W wyniku wniesionego odwołania przez wykonawcę Konwerga Sp. z o.o. z siedzibą w Poznaniu, Zamawiający pismem wniesionym do Krajowej Izby Odwoławczej w dniu 4 września 2023 r. (pismo z dnia 4 września 2023 r.) wnosił o oddalenie odwołania całości.

Do postępowania odwoławczego po stronie Zamawiającego skutecznie przystąpili:

- wykonawca Innergo Systems Sp. z o.o. z siedzibą w Warszawie,
- wykonawcy wspólnie ubiegający się o udzielenie zamówienia: T4B sp. z o.o. z siedzibą w Warszawie, Atende S.A. z siedzibą w Warszawie,
- S&T Poland Sp. z o.o. z siedzibą w Warszawie.

Izba stwierdziła, że ww. wykonawcy zgłosili przystąpienie do postępowania w ustawowym terminie, wykazując interes w rozstrzygnięciu odwołania na korzyść Zamawiającego.

Przystępujący - wykonawcy wspólnie ubiegający się o udzielenie zamówienia - T4B sp. z o.o. z siedzibą w Warszawie, Atende S.A. z siedzibą w Warszawie pismem wniesionym do Krajowej Izby Odwoławczej w dniu 1 września 2023 r. (pismo z dnia 1 września 2023 r.) wnosili o oddalenie odwołania w całości.

Stan prawny ustalony przez Izbę:

Zgodnie z art. 226 ust. 1 pkt 5 ustawy PZP, Zamawiający odrzuca ofertę, jeżeli jej treść jest niezgodna z warunkami zamówienia.

Zgodnie z art. 239 ust. 1 ustawy PZP, Zamawiający wybiera najkorzystniejszą ofertę na podstawie kryteriów oceny ofert określonych w dokumentach zamówienia.

Zgodnie z art. 18 ust. 3 ustawy PZP, Nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. z 2022 r.), jeżeli wykonawca, wraz z przekazaniem takich informacji, zastrzegł, że nie mogą być one udostępniane oraz wykazał, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wykonawca nie może zastrzec informacji, o których mowa w .

Zgodnie z art. 11 ust. 2 ustawy o zwalczaniu nieuczciwej konkurencji, Przez tajemnicę przedsiębiorstwa rozumie się informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności.

Krajowa Izba Odwoławcza – po przeprowadzeniu rozprawy w przedmiotowych sprawach, po zapoznaniu się ze stanowiskami przedstawionymi w odwołaniach, odpowiedzi na odwołanie, stanowiskami przystępujących, konfrontując je z zebranym w sprawie materiałem procesowym, w tym z dokumentacją postępowania o udzielenie zamówienia publicznego oraz po wysłuchaniu oświadczeń i stanowisk stron, a także uczestników postępowania odwoławczego złożonych ustnie do protokołu w toku rozprawy – ustaliła i zważyła, co następuje:

Skład orzekający stwierdził, że odwołania dotyczą materii określonej w art. 513 ustawy PZP i podlegają rozpoznaniu zgodnie z art. 517 ustawy PZP. Izba stwierdziła również, że nie została wypełniona żadna z przesłanek określonych w art. 528 ustawy PZP, których stwierdzenie skutkowałoby odrzuceniem odwołań i odstąpieniem od badania meritum sprawy. Ponadto w ocenie składu orzekającego Odwołujący wykazali, że posiadają legitymację materialną do wniesienia środka zaskarżenia zgodnie z przesłankami art. 505 ust. 1 ustawy PZP, tj. mają interes w uzyskaniu zamówienia, a naruszenie przez zamawiającego przepisów ustawy PZP może spowodować poniesienie przez nich szkody polegającej na nieuzyskaniu zamówienia.

Skład orzekający dokonał oceny stanu faktycznego ustalonego w obydwu sprawach mając na uwadze art. 554 ust. 1 pkt 1 ustawy PZP, który stanowi, że Izba uwzględnia odwołanie, jeżeli stwierdzi naruszenie przepisów ustawy, które miało wpływ lub może mieć istotny wpływ na wynik postępowania o udzielenie zamówienia.

Izba – uwzględniając zgromadzony materiał dowodowy przedłożony przez strony i przystępujących, po dokonaniu ustaleń poczynionych na podstawie dokumentacji postępowania, biorąc pod uwagę zakres sprawy zakreślony przez okoliczności podniesione w odwołaniu oraz stanowiska złożone pisemnie i ustnie do protokołu – stwierdziła, że sformułowane przez Odwołujących zarzuty w sprawie o sygn. akt KIO 2475/23 oraz w sprawie KIO 2478/23 nie znajdują oparcia w ustalonym stanie faktycznym i prawnym, a tym samym rozpoznawane odwołania nie zasługują na uwzględnienie.

I.KIO 2475/23:

Zarzut Odwołującego dotyczący przełącznika dostępowego zewnętrznego (funkcjonalność prywatnego VLAN-u) jest zdaniem Izby niezasadny.

Izba zważa, że zgodnie z pkt 1.1.6 w ppkt 5 lit. h Załącznika Nr 1 do OPZ (Wymagania szczegółowe dla urządzeń typu przełącznik zewnętrzny), urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci: *„funkcjonalność prywatnego VLAN-u, czyli możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. porty izolowane) z pozostawieniem możliwości komunikacji z portem nadrzędnym”.*

Izba wskazuje, że Przystępujący w przedmiotowym postępowaniu zaoferował przełącznik zewnętrzny producenta Aruba Model 4100i.

Biorąc powyższe pod uwagę, spór między stronami dotyczył tego, czy na dzień składania ofert, tj. na dzień 4 kwietnia 2023 r. zaoferowane urządzenie przez Przystępującego spełniało ww. wymagania Zamawiającego.

Izba na podstawie dowodów wskazanych przez Zamawiającego w odpowiedzi na odwołanie, jak również dowodów złożonych przez Odwołującego na posiedzeniu (zwłaszcza z dowodu nr 1 i 3) doszła do przekonania, że funkcjonalność prywatnego VLAN-u dla przełącznika Aruba model 4100i była dostępna już w wersji oprogramowania 10.11, która została wydana w dniu 28 marca 2023 r. (Release date – Released fully supported, and posted on the Web), a nie dopiero jak sugeruje Odwołujący z wersją oprogramowania 10.12, co oznacza, że powyższa funkcjonalność była dostępna na dzień składania ofert.

I tak np. z dowodu nr 3 Odwołującego (Aruba Cx 4100i Switch Series) wynika, że: „Prywatna sieć VLAN (PVLAN) zapewnia izolację ruchu pomiędzy użytkownikami w tej samej sieci VLAN; zazwyczaj port przełącznika może komunikować się tylko z innymi portami w tej samej społeczności i/lub portem łącza zwrotnego, niezależnie od identyfikatora sieci VLAN lub docelowego adresu MAC. Zwiększa to bezpieczeństwo sieci, ograniczając komunikację peer-peer, aby zapobiec różnym złośliwym atakom”.

Izba chciałaby w tym miejscu zaznaczyć, że powoływanie się przez Odwołującego, iż w linku na stronie producenta Aruba wskazane jest oprogramowanie 10.12, a przez pomyłkę producent Aruba opisał Private VLAN również w stosunku do przełącznika 4100i, jest tylko i wyłącznie przypuszczeniem Odwołującego, o czym świadczą słowa samego Odwołującego złożone na rozprawie : „ Odwołujący przypuszcza, że zaimplementowane zostały z oprogramowania 10.12, a fragmentaryczne opisy zostały z oprogramowania 10.11."

Nadto Izba zważa, że producent Aruba na swojej stronie internetowej https://www.arubanetworks.com/techdocs/AOS-CX/10.12/HTML/l2_bridging_8100-83xx-9300-10000/Content/Chp_PVLAN/PVLAN.htm wyjaśnia, że prywatny VLAN (PVLAN) składa się z instancji podstawowych i podrzędnych VLAN, z kolei zaoferowany przez Przystępującego przełącznik 4100i obsługuje 32 VLAN podstawowe i 8 VLAN podrzędne. Tym samym, Izba doszła do przekonania, iż przełącznik 4100i posiada funkcjonalność prywatnego VLAN-u.

Na marginesie warto również podkreślić, że Zamawiający nie wymagał w SWZ podania przez wykonawców biorących udział w niniejszym postępowaniu danych dotyczących wersji oprogramowania, ze względu na obowiązek dokonania aktualizacji oprogramowania przed podpisaniem protokołu odbioru, co jednoznacznie wynika z postanowień SWZ w Tomie III OPZ w rozdziale VIII w pkt 13 (Szczegółowy opis przedmiotu zamówienia):Wykonawca zobowiązany będzie przed podpisaniem Protokołu Odbioru ostatniej lokalizacji do aktualizacji oprogramowania układowego (firmware) wszystkich dostarczonych i uruchomionych Urządzeń w każdej lokalizacji oraz dostarczonego środowiska programowego do najnowszej wspieranej wersji zalecanej przez producenta Rozwiązania. Brak wykonania aktualizacji, o której mowa w zdaniu poprzednim skutkować będzie brakiem odbioru przez Zamawiającego ostatniej lokalizacji oraz traktowane będzie jako zwłoka Wykonawcy w terminie wdrożenia i uruchomienia tej lokalizacji".

Tym samym, w ocenie Izby zarzut ten jest niezasadny.

Odnośnie zarzutu dotyczącego przełącznika dostępowego zewnętrznego ze względu na brak funkcjonalności zdalnego port mirroring - RSPAN, jest zdaniem Izby niezasadny.

Izba zważa, że zgodnie w pkt 1.1.6 w ppkt 7 lit. d) Załącznika nr 1 do OPZ (Wymagania szczegółowe dla urządzeń typu przełącznik zewnętrzny), funkcje związane z zarządzaniem i monitorowaniem: *„implementacja mechanizmu SPAN PORT lub analogiczna funkcjonalność; przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (zdalny port mirroring – RSPAN lub równoważny)".*

Biorąc powyższe zapisy SWZ, Izba doszła do przekonania, że określenia wskazujące nazdalny port mirroring – RSPAN lub równoważny (podane w nawiasie) należało traktować jako przykładowe rozwiązania, tym bardziej, że Zamawiający dopuścił rozwiązania równoważne, o czym świadczą słowa „lub równoważny".

Należy zwrócić uwagę, że w toku badania i oceny ofert Zamawiający w dniu 16 czerwca 2023 r. zwrócił się do producenta Aruba o wyjaśnienie czy: *Czy przełącznik Aruba 4100i oraz przełącznik Aruba 6300M umożliwiają zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (zdalny port mirroring – RSPAN lub równoważny).*W odpowiedzi na przedmiotowe zapytanie producent Aruba w dniu 21 czerwca 2023 r. potwierdził, że zaoferowany przełącznik 4100i posiada wymaganą w Załączniku nr 1 do OPZ funkcjonalność, tj. „*umożliwia realizację funkcjonalności pozwalającej na zdalną obserwację ruchu z określonego portu, polegającą na kopiowaniu pojawiających się na nim ramek i ich odbieraniu na zdalnym urządzeniu monitorującym*".

Nadto na podstawie dowodów wniesionych przez Przystępującego w postaci oświadczenia Pana Michała Dudko (Territory Manager HPE Aruba Networking) z dnia 5 września 2023 r., jak również opinii prywatnej dr hab. inż. Andrzeja Zalewskiego z dnia 5 września 2023 r. wynika odpowiednio, iż: „ Odpowiednio skonfigurowane przełączniki Aruba 4100i oraz Aruba 6300M umożliwiają realizację wymagania „przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN" oraz „ Konfigurując odpowiednio protokół ERSPAN można przesyłać (kopiować) ruch generowany na urządzeniu Aruba 4100i przez dowolne podłączone do jego portów urządzenie (na rys. powyżej – przykładowo pokazano stacje roboczą ozn. symbolem komputera z lewej strony rysunku) na wybrane urządzenie w sieci (na rys. ilustracyjnym oznaczone okręgiem z kreską po prawej stronie rysunku, podłączone do urządzenia Aruba 6300M). Funkcjonalność monitorowania urządzeń brzegowych jest w ten sposób zrealizowana. Przesyłanie skopiowanego ruchu może się przy tym odbywać przez dedykowany VLAN".

Tym samym, w ocenie Izby zarzut ten jest niezasadny.

Odnośnie zarzutu Odwołującego dotyczącego przełącznika dostępowego wewnętrznego z uwagi na brak funkcjonalności zdalnego port mirroring – RSPAN, jest zdaniem Izby niezasadny.

Izba zważa, że zgodnie w pkt 1.1.5 w ppkt 7 lit. d) Załącznika nr 1 do OPZ (Wymagania szczegółowe dla urządzeń typu przełącznik wewnętrzny), funkcje związane z zarządzaniem i monitorowaniem: „ *implementacja mechanizmu SPAN PORT lub analogiczna funkcjonalność; przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (zdalny port mirroring – RSPAN lub równoważny)".*

Biorąc powyższe zapisy SWZ, podobnie jak przy przełączniku zewnętrznym), Izba doszła do przekonania, że określenia wskazujące na zdalny port mirroring – RSPAN lub równoważny(podane w nawiasie) należało traktować jako przykładowe rozwiązania, tym bardziej, że Zamawiający dopuścił rozwiązania równoważne, o czym świadczą słowa „lub równoważny".

Izba w pierwszej kolejności chciałaby zwrócić uwagę, że Odwołujący w odwołaniu w zakresie przełącznika 6300M nie kwestionował spełnienia samego wymagania w zakresie posiadania funkcjonalności: „*zdalnej obserwacji ruchu na określonym porcie, polegającej na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego*, a wyłącznie podważa wymóg przesyłania *poprzez dedykowaną sieć VLAN"* (powyższego również Odwołujący nie kwestionował na rozprawie).

Izba zważa, że Zamawiający wymagał funkcjonalności zdalnej obserwacji ruchu na określonym porcie, polegającej na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN, a RSPAN był tylko jedną z możliwości realizacji tej funkcjonalności wymienionej w przywołanym powyżej pkt 1.1.5 w ppkt 7 lit. d) Załącznika nr 1 do OPZ, na co zwrócił uwagę także Zamawiający w odpowiedzi na odwołanie. Potwierdzają to również dowody wniesione przez Przystępującego w postaci powołanego powyżej oświadczenia Pana Michała Dudko z dnia 5 września 2023 r. oraz opinii prywatnej dr hab. inż. Andrzeja Zalewskiego.

Nadto z ww. opinii wynika również, iż „protokół ERSPAN może zostać wykorzystany w miejsceprotokołu RSPAN, w tym sensie są one funkcjonalnie równoważne. Oba protokoły, są własnością firmy CISCO, i realizują funkcję przesyłania danych zebranych (skopiowanych) z portów wielu przełączników sieciowych do innego urządzenia w sieci realizującego funkcję monitorowania ruchu. Różnica funkcjonalna między nimi polega na tym, że protokół RSPAN działa w warstwie 2 stosu protokołów sieciowych a ERSPAN działa w warstwie 3. W rezultacie protokół ERSPAN umożliwia przesyłanie danych z monitorowanych urządzeń nie tylko w obrębie danej sieci lokalnej, ale także między wieloma domenami sieci IP. W pewnym uproszczeniu można powiedzieć, że protokół ERSPAN działa zarówno w skali lokalnej, jak i w skali większych sieci. W rezultacie protokół ERSPAN, jako posiadający szerszy zakres stosowania, może zostać użyty w mniejszej skali, zamiast protokołu RSPAN."

Na marginesie Izba zważa, że to, iż protokół RSPAN działa w warstwie 2, a ERSPAN działa w warstwie 3, na co zwracał uwagę Odwołujący w odwołaniu, nie ma w ocenie Izby znaczenia, ponieważ Zamawiający nie wymagał w jakiej warstwie przesył ma być realizowany.
Tym samym, w ocenie Izby zarzut ten jest niezasadny.
Odnośnie zarzutu zaoferowania oprogramowania z uwagi na brak zaoferowania oprogramowania zapewniającego realizację wymagań przedmiotu zamówienia (tj. co najmniej: Aruba ClearPass Access, Aruba ClearPass OnGuard, Aruba ClearPass Device Insight), jest zdaniem Izby niezasadny.
Izba wskazuje, że zgodnie ze wzorem formularza 2.2 do SWZ (Zestawienie głównych elementów Systemu Wi-Fi), Zamawiający wymagał podania: nazwa oprogramowania, producenta i ilości oferowanych licencji.
Izba zważa, że Przystępujący w złożonej ofercie w zakresie zestawienia głównych elementów CSZ w Centrum Informatyki Resortu Finansów w Radomiu wskazał, że oferuje oprogramowanie o nazwie Aruba Clearpass,producenta Aruba oraz liczbę licencji: 2.
W związku powyższym, Izba nie podziela argumentacji Odwołującego jakoby Przystępujący powinien w treści swojej oferty wyspecyfikować konkretne licencje, tj. Aruba Clearpass Akcess, Aruba Clearpass OnGuard, Aruba ClearPass Device Insight, ponieważ zgodnie z wymogiem opisanym w załączniku 2.2. wykonawca zobowiązany był do wskazania tylko: nazwy oprogramowania, jego producenta oraz szacowaną liczbę licencji, co też Przystępujący uczynił.
Nie zmienia powyższego w ocenie Izby również to, iż oprogramowanie Aruba ClearPass składa się co najmniej z 3 elementów, co znajduje potwierdzenie w dokumentacji producenta wskazanej przez Zamawiającego dostępnej pod adresami: oraz , gdzie wprost wskazano jakie elementy składają się na zaoferowane oprogramowanie ClearPass. Świadczy o powyższym również dowód nr 7 wniesiony przez Odwołującego na posiedzeniu (Aruba ClearPass Policy Manager) powołany także przez Zamawiającego, z którego wynika, że ClearPass obejmuje ClearPass Device Insight, ClearPass Onboard, ClearPass OnGuard, ClearPass Guest. Z kolei z dowodu nr 8 Odwołującego (Aruba ClearPass Network Access Control) wynika, iż ClearPass obejmuje ClearPass Device Insight, ClearPass Onboard, ClearPass OnGuard, ClearPass Guest, ClearPass OnConnect, ClearPass Exchange.
Jednakże, zdaniem Izby, istotne jest to, iż z oświadczenia Pana Michała Dudko z dnia 5 września 2023 r. wynika, iż „… pakiet licencji Aruba ClearPass obejmuje komponent główny i wszystkie licencje oraz dodatki programowe umożliwiające m.in. wdrożenie mechanizmu bezpieczeństwa obejmującego analizę stanu stacji końcowych w aspekcie podłączających się do sieci (posture), profilowanie urządzeń oraz monitoring behawioralny".
W związku z powyższym, biorąc pod uwagę postanowienia SWZ, jak również ww. oświadczenie, w ocenie Izby wystarczającym było wskazanie w formularzu 2.2 nazwy oprogramowania, jego producenta oraz szacowaną liczbę licencji, bez konieczności konkretyzowania, co wchodzi w skład Aruba ClearPass.
Nadto Izba odniesie się jeszcze do zarzutu, jakoby Przystępujący zaoferował jedynie 2 licencje,
co uniemożliwia zaoferowanie wskazanych w ofercie 3 produktów. Izba zważa, że Przystępujący w formularzu 2.2. zaoferował urządzenie Mobility Conductor Hardware Appliance, Producent: Aruba, Model: ARUBA MOBILITY CONDUCTOR w ilości 2 sztuk urządzeń (szacowana liczba urządzeń). To z kolei spowodowało, iż Przystępujący zaoferował 2 sztuki licencji Aruba Clearpass (każda ze wskazanych licencji składająca się z 3 elementów obsługująca jedno ww. urządzenie). Tym samym zaoferowane licencje odpowiadały ilości zaoferowanych urządzeń, co zdaniem Izby było wystarczające i zgodne z postanowieniami SWZ.
Tym samym, w ocenie Izby zarzut ten jest niezasadny.
Izba zważa, że pozostałe dowody wniesione przez Odwołującego nie miały znaczenia dla rozstrzygnięcia sprawy.
Konkludując, w ocenie Izby, Zamawiający nie naruszył art. 226 ust. 1 pkt 5 ustawy PZP w zw. z art. 16 ustawy PZP, jak również art. 239 ust 1 i 2 ustawy PZP.
O kosztach postępowania odwoławczego orzeczono na podstawie art. 574 i 575 ustawy Prawo zamówień publicznych oraz § 2 ust. 1 pkt 2 w zw. z § 8 ust. 2 pkt 1 rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie szczegółowych rodzajów kosztów postępowania odwoławczego, ich rozliczania oraz wysokości i sposobu pobierania wpisu od odwołania (Dz. U. 2020 r. poz. 2437), obciążając kosztami postępowania Odwołującego.

II.KIO 2478/23:

W pierwszej kolejności Izba odniesie się do zarzutu Odwołującego dotyczącego telemetrii, który jest zdaniem Izby niezasadny.
Izba zważa, że zgodnie z pkt 2.1 Załącznika nr 1 do OPZ w Tomie III SWZ *Wymagania ogólne dla systemu CSZ* w Lp. 33 i Lp. 34 Zamawiający określił, jaki zakres minimum musi wchodzić w skład funkcjonalności telemetrii. I tak w pkt (Lp. 33) Zamawiający podał, iż:
„System musi posiadać funkcjonalność telemetrii, w tym minimum:
•Podgląd statystyk z zarządzanych urządzeń sieciowych
•Podgląd zdarzeń związanych z problemem z dostępem do sieci, np. analiza problemu związanego z uwierzytelnieniem 802.1x
•Możliwość importu topologii (np. planu budynku, piętra) do systemu centralnego zarządzania
•Możliwość zaznaczenia na zaimportowanej topologii lokalizacji zainstalowanych punktów dostępowych
•Przegląd tzw. heat map dla access-pointów
•Wyświetlenie analizy spektrum dla access-pointów
•Wyświetlanie statusów pracy przełączników i access-pointów
•Śledzenie procesu uzyskania dostępu klienta do sieci w środowisku z uwierzytelnianiem 802.1x, MAC authentication i Portal authentication
•Identyfikacja najpopularniejszych problemów sieciowych związanych z wydajnością interfejsów i sieci, roamingiem, procesem uwierzytelniania. Identyfikacja problemów sieciowych." Z kolei w pkt (Lp. 34) Zamawiający podał, iż:
„Musi posiadać narzędzie pozwalające na monitoring wydajności sieci wraz z:
a)zbieraniem informacji o aplikacjach w sieci i parametrach ich działania
b)analizą, którzy użytkownicy generują najwięcej ruchu, z jakich korzystają aplikacji oraz jakie jest ich wykorzystanie".
Izba chciałaby w tym miejscu zaznaczyć, iż dla systemu CSZ Odwołujący zaoferował oprogramowanie Cisco DNA na licencji Essentials, które to oprogramowanie w ocenie Izby nie spełnia wymagań SWZ w zakresie telemetrii obejmujących:
- Możliwość importu topologii (np. planu budynku, piętra) do systemu centralnego zarządzania,
- Możliwość zaznaczenia na zaimportowanej topologii lokalizacji zainstalowanych punktów
dostępowych,
- Przegląd tzw. heat map dla access-pointów,
- Wyświetlenie analizy spektrum dla access-pointów.
Izba podziela argumentację Zamawiającego, iż powyższe wymagania są dostępne w oprogramowaniu Cisco DNA na licencji Advantage, a nie na licencji Essentials, co wynika jednoznaczne z dokumentu Cisco (Cisco DNA Software Wireless Feature Matrix), na który powoływał się również Przystępujący (Konsorcjum) w dowodzie 1B:
., w którym to ww. funkcjonalności oznaczono przy użyciu oznaczenia „tick" w Cisco DNA Advantage (tj. Wireless 3D

Analyzer, Proactive issue detection).

Izba zważa, że zaoferowane rozwiązanie przez Odwołującego nie tylko nie spełnia wymagań z pkt 2.1 Załącznika nr 1 do OPZ w Tomie III SWZ (Lp. 33), ale również wymagania opisanego w pkt 2.1 Załącznika nr 1 do OPZ w Tomie III SWZ (Lp. 34 lit. b) związanego z prowadzoną *„analizą, którzy użytkownicy generują najwięcej ruchu, z jakich korzystają aplikacji oraz jakie jest ich wykorzystanie”.*

Izba chciałaby w tym miejscu podkreślić, że aby uzyskać możliwość ww. analizy w oprogramowaniu CISCO, konieczne jest posiadanie licencji obejmującej rozwiązania określone jako „App 360, AP 360, WLC 360 i Client 360”, które dostępne są na poziomie licencjonowania Cisco DNA Advantage.

Biorąc powyższe pod uwagę, zdaniem Izby, Zamawiający wymagał od wykonawców zaoferowania oprogramowania, które będzie nie tylko zbierać informacje o aplikacjach w sieci i parametrach ich działania, ale również będzie umożliwiało przeprowadzenie analizy, którzy użytkownicy generują najwięcej ruchu, z jakich korzystają aplikacji oraz jakie jest ich wykorzystanie. Tym samym, Izba nie zgadza się z Odwołującym, jakoby Cisco DNA Essentials posiadało funkcjonalność telemetrii, o czym świadczy również fragment odwołania na stronie 11, w którym mowa jest tylko o czynności wyświetlania danych, a nie czynności polegającej na zbieraniu i analizowaniu: *„Pulpit nawigacyjny stanu aplikacji. Wyświetla ogólny stan wszystkich aplikacji w sieci, z e specjalną sekcją dotyczącą problemów związanych z aplikacjami biznesowymi i sugerowane środki zaradcze, zarządzane przez Cisco DNA Center”. Pulpit nawigacyjny umożliwia wyświetlenie stanu wszystkich aplikacji w sieci, parametry ich działania a także sugeruje środki zaradcze. Natomiast dodatkowo pulpity nawigacyjne stanu klienta oraz sensora bezprzewodowego dostarczają cały szereg informacji o ruchu generowanym przez użytkowników”.*

Nadto Izba zważa, że zgodnie z pkt 2 Załącznika nr 1 do OPZ, Tom III SWZ *Wymagania dla systemu CSZ*, Zamawiający wymagał: *„Wraz z Urządzeniami Wi-Fi konieczne jest dostarczenie Centralnego Systemu Zarządzania (CSZ). CSZ musi zapewnić obsługę wszystkich Urządzeń Wi-Fi w sieci w zakresie zarządzania, monitorowania, logowania oraz zarządzania incydentami w czasie rzeczywistym. Zamawiający wymaga dostarczenia Szafy RACK 19” wraz z niezbędnym okablowaniem i wyposażeniem oraz instalacji w niej wszystkich komponentów CSZ”.*

W ocenie Izby, biorąc pod uwagę postanowienia SWZ, jak i ww. fragment odwołania, Izba doszła do przekonania, że Zamawiającemu zależało nie tylko na funkcjonalności mającej polegać na wyświetlaniu informacji w tzw. „czasie rzeczywistym”, ale również na ich zbieraniu, a następnie przeprowadzaniu analizy danych historycznych. Zdaniem Izby nie zmienia powyższego, zastosowanie przez Zamawiającego słowa „analiza” zamiast „analiza danych historycznych”, na co zwracał uwagę Odwołujący w piśmie procesowym z dnia 5 września 2023 r.

Tym samym, w ocenie Izby zarzut ten jest niezasadny.

Odnośnie zarzutu dotyczącego ochrony przed atakami sieciowymi na sieć bezprzewodową, jest zdaniem Izby niezasadny.

Izba zważa, że zgodnie z pkt 1.1.4 Załącznika nr 1 do OPZ, Tom III SWZ *Wymagania szczegółowe dla kontrolerów sieci bezprzewodowej – lokalne,* w pkt (Lp. 12), Zamawiający wymagał: *„Kontroler musi posiadać funkcje Bezpieczeństwa:*

a) Detekcja i identyfikacja lokalizacji obcych punktów dostępowych (rogue AP). Automatyczna klasyfikacja obcych urządzeń i możliwość ich blokowania poprzez wysyłanie odpowiednio spreparowanych pakietów.

b) Identyfikacja sieci Adhoc.

c) Identyfikacja anomalii sieciowych,

d) Ochrona przed atakami sieciowymi na sieć bezprzewodową, np. DoS, Management Frame Flood, fake AP”.

Izba chciałaby w tym miejscu podkreślić, iż dla systemu CSZ Odwołujący zaoferował oprogramowanie Cisco DNA na licencji Essentials, które to oprogramowanie w ocenie Izby nie spełnia wymagań SWZ w zakresie ochrony przed atakami sieciowymi na sieć bezprzewodową DoS, co wynika jednoznacznie ze strony producenta Cisco: https://www.cisco.com/c/m/en_us/products/software/dna-subscription-wireless/en-swsub-matrix-wireless.html., czy też ze strony https://www.cisco.com/c/en/us/td/docs/wireless/technology/wips/deployment/guide/WiPS_deployment_guide.html (DoS signature updates; Wireless intrusion signature updates w Base WIPS (zaoferowane przez Odwołującego na poziomie licencjonowania Cisco DNA Essentials) - występuje słowo „No”.

Izba zwraca uwagę, że nie zmienia powyższego poglądu Izby powoływanie się przez Odwołującego na definicję pojęcia DoS przez inne podmioty publiczne (Ministerstwo Spraw Wewnętrznych i Administracji, NASK, Urząd Komisji Nadzoru Finansowego).

Nadto Izba zważa, że w ramach funkcjonalności Clean Air, na którą powołuje się Odwołujący (dostępnej na poziomie licencjonowania Cisco DNA Essentials) nie ma zabezpieczenia przed atakami DoS w pasmie częstotliwości Wi-Fi, co wynika również z samego odwołania na stronie 17: „*CleanAir/Inteligencja widma. Wykrywa nieuczciwe urządzenia i ataki DoS na częstotliwościach innych niż 802.11, takich jak Bluetooth, radar i mikrofale*”, a to w ocenie Izby oznacza, że Odwołujący nie spełnił wymagań określonych w pkt 1.1.2 Załącznika nr 1 do OPZ, TOM III w pkt (Lp. 2), w którym to Zamawiający wymagał: „*Standardy radiowe Wi-Fi: Obsługa standardów 802.11a/b/g/n/ac/ax*”.

Poza tym Izba wskazuje, iż na stronie internetowej producenta Cisco: https://www.cisco.com/c/en/us/products/collateral/wireless/adaptive-wireless-ipssoftware/data_sheet_c78-501388.html, wymagania określone w pkt 1.1.4 Załącznika nr 1 do OPZ,Tom III SWZ,*Wymagania szczegółowe dla kontrolerów sieci bezprzewodowej –lokalne*, w zakresie pkt (Lp. 12 lit. d) spełnia oprogramowanie Cisco DNA na licencji Advantage z funkcjonalnością aWIPS. Licencja ta pozwala na wykrywanie ataków na sieci bezprzewodowe w oparciu o definicje sygnatur ataków, których wykrycie nie jest możliwe w ramach licencji Cisco DNA Essentials.

Tym samym, w ocenie Izby zarzut ten jest niezasadny.

Odnośnie zarzutu dotyczącego mechanizmu bezpieczeństwa (posture, profilowanie urządzeń), jest zdaniem Izby niezasadny.

Izba zważa, że zgodnie z rozdziałem II pkt 4 Załącznika nr 5 do OPZ, Tom III SWZ *Ogólne wytyczne dot. bezpieczeństwa,* Zamawiający wymagał: „*W ramach wdrożenia zostaną opracowane i dostarczone mechanizmy bezpieczeństwa a w szczególności: (…)*

- Analiza stanu stacji końcowych w aspekcie podłączających się do sieci (posture), profilowanie urządzeń oraz monitoring behawioralny”.

W ocenie Izby, biorąc pod uwagę powyższy zapis SWZ, Zamawiający oczekiwał oprogramowania umożliwiającego zarówno profilowanie urządzeń, ich monitoring behawioralny oraz analizę stanu stacji końcowych w aspekcie podłączających się do sieci, którą zdefiniował poprzez użycie słowa „posture”.

Tym samym, zdaniem Izby, Zamawiający wymagał, aby zaoferowane oprogramowanie zapewniało możliwość korzystania ze wszystkich ww. funkcjonalności.

Izba chciałaby w tym miejscu zaznaczyć, że Odwołujący zaoferował oprogramowanie i licencje Cisco Identity Service Engine Advantage Subscription oraz Cisco ISE Device Admin Node License, które w ocenie Izby nie spełniają ww. wymagań w zakresie analizy stanu stacji końcowych w aspekcie podłączających się do sieci (posture), co jednoznacznie wynika ze strony internetowej producenta Cisco: https://www.cisco.com/c/en/us/products/collateral

/security/identityservices-engine/ise-licensing-guide-og.html, przy czym nie było sporu co do tego, iż oprogramowanie i licencje zaoferowane przez Odwołującego zapewniają atrybuty w postaci profilowania urządzeń oraz monitoring behawioralny.

Nadto ze strony producenta wynika, iż funkcjonalność „posture" posiada licencja typu Cisco ISE Premier, o czym świadczy również dowód 3B wniesiony przez Przystępującego (Konsorcjum) na posiedzeniu, jak również złożone oświadczenie na rozprawie: „Odnośnie „posture" jest to analiza stacji końcowej podłączającej do sieci. Aby mieć posture trzeba mieć licencję premiere". Powyższe potwierdza również sam Odwołujący na stronie 24 odwołania: „*Jak słusznie zauważył Zamawiający tego typu funkcjonalność jest zawarta w licencji ISE Premier i nie jest ona przedmiotem oferty Odwołującego".*

Poza tym, Izba zważa, że gdyby producent utożsamiał funkcjonalność określaną jako „posture" z profilowaniem urządzeń oraz monitoringiem behawioralnym, to nie wskazywałby takiej funkcjonalności jako dodatkowej na wyższym poziomie licencjonowania.

Tym samym, w ocenie Izby zarzut ten jest niezasadny.

Odnośnie zarzutu dotyczącego analizy widma częstotliwościowego oraz wyświetlenie analizy spektrum dla access-pointów, jest zdaniem Izby niezasadny.

Izba zważa, że zgodnie z pkt 1.1.2 Załącznika nr 1 do OPZ, Tom III SWZ*Wymagania szczegółowe dla urządzeń Access point (AP) zewnętrzny*, w pkt (Lp. 13) Zamawiający wymagał: *„Funkcje analizy widma częstotliwościowego:*

a) zakres identyczny z częstotliwością modułów radiowych AP

b) współpraca z mechanizmami optymalizacji wykorzystania pasma radiowego

c) umożliwia skanowanie off-channel" oraz w myśl pkt 2.1 Załącznika nr 1 do OPZ, Tom III SWZ*Wymagania ogólne dla systemu CSZ*, w pkt (Lp. 33) Zamawiający wymagał: *„System musi posiadać funkcjonalność telemetrii (…)*

• Wyświetlenie analizy spektrum dla access-pointów".

W związku z powyższym, Izba doszła do przekonania, że Zamawiający wymagając„widma częstotliwości" oraz „wyświetlenie analizy spektrum dla access-pointów" oczekiwał posiadania przez dane oprogramowanie całego obrazu widma/spektrum, co wiązało się z koniecznością prezentacji zakresu częstotliwości radiowych zgodnego z częstotliwością modułów radiowych AP na poziomie systemu CSZ, której zadaniem jest zarządzanie wszystkimi urządzeniami, znajdującymi się w różnych lokalizacjach na terenie Polski, w tym kontrolerami, na co zwrócił uwagę Zamawiający w odpowiedzi na odwołanie.

Izba zważa, iż Odwołujący zaoferował oprogramowanie Cisco DNA na licencji Esencials w ramach, którego znajduje się funkcjonalność Cisco Clean Air, przy czym argumentacja Odwołującego skupia się w odwołaniu jedynie na spełnieniu wymagań postawionych dla oprogramowania w warstwie lokalnej, które zostały opisane w pkt 1.1.2 Załącznika nr 1 do OPZ, Tom III SWZWymagania szczegółowe dla urządzeń Access point (AP) zewnętrzny, w pkt (Lp. 13), a nie na wymaganiach opisanych dla systemu CSZ w pkt 2.1 Załącznika nr 1 do OPZ, Tom III SWZ*Wymagania ogólne dla systemu CSZ* w pkt (Lp. 33), co jak słusznie zauważył Zamawiający było podstawą odrzucenia oferty Odwołującego: „*ClearAir nie spełnia wymagania wyświetlania analizy spectrum dla access-pointów z poziomu Centralnego Systemu Zarządzania, które zostało wyrażone w Tom III SWZ - OPZ zał. 1 pkt 2.1, Wymagania ogólne dla systemu CSZ, Lp. 33".*

Na marginesie Izba wskazuje, że Zamawiający nie kwestionował zaoferowania oprogramowania przez Odwołującego w zakresie możliwości wyświetlania analizy widma częstotliwościowego dla access pointów z poziomu kontrolera Cisco 9800 w warstwie lokalnej.

Biorąc powyższe pod uwagę, Izba podziela argumentację Zamawiającego, iż aby wyświetlić analizę spektrum z poziomu CSZ potrzebna jest licencja Cisco DNA Advantage,a nie licencja Cisco DNA Essentials, co wynika jednoznaczne z dokumentu Cisco (Cisco DNA Software Wireless Feature Matrix), na który powoływał się również Przystępujący (Konsorcjum) w dowodzie 1B:., w którym to ww. funkcjonalność oznaczono przy użyciu oznaczenia „tick" w Cisco DNA Advantage (tj. Proactive issue detection – „Spectrum Analyzer").

Tym samym, w ocenie Izby zarzut ten jest niezasadny.

Odnośnie zarzutu dotyczącego funkcjonalności WIPS, jest zdaniem Izby niezasadny.

Izba zważa, że zgodnie z pkt 1.1.2 Załącznika nr 1 do OPZ, Tom III SWZ*Wymagania szczegółowe dla urządzeń Access point (AP) zewnętrzny,* w pkt (Lp. 12 lit. l), Zamawiający wymagał aby zarządzanie przez kontroler WLAN z funkcjonalnościami obejmowało: „obsługa WIPS".

Izba wskazuje, że Odwołującyzaoferował oprogramowanie Cisco DNA na licencji Essentials z funkcjonalnością Cisco Rogue Detection, która to w ocenie Izby nie jest funkcjonalnością WIPS ani rozwiązaniem równoważnym do WIPS. Izba podziela argumentację Zamawiającego, iż funkcjonalność Rogue Detection jest jedynie jednym z elementów składowych funkcjonalności WIPS, nie stanowi ona całości tej funkcjonalności, co również potwierdził Przystępujący (Konsorcjum) na rozprawie: „Rogue Detection jest tylko wykrywaniem, a z kolei WIPS potrafi zareagować".

Tym samym w ocenie Izby funkcjonalność Rogue Detection nie zapewnia pełnej ochrony przed atakami sieciowymi na sieć bezprzewodową. Powyższe wynika przede wszystkim ze strony producenta pod adresem https://www.cisco.com/c/en/us/products/collateral/wireless/adaptive-wireless-ipssoftware/data_sheet_c78-501388.html, gdzie producent Cisco opisuje dwie różne funkcjonalności dostępne zarówno w oprogramowaniu oraz licencjach jakie oferuje: aWIPS oraz Rogue Detection, przy czym producent oferuje wskazane funkcjonalności na innym poziomie licencjonowania (Cisco DNA na licencji Advantage – aWIPS, z kolei Cisco DNA na licencji Essentials – Rogue Detection).

Izba odniesie się jeszcze w tym miejscu do stwierdzenia Odwołującego, jakoby Zamawiający wymagał funkcjonalności aWIPS, która *„znacznie wykracza poza funkcjonalność opisaną przez Zamawiającego w SWZ".* Izba zwraca uwagę, że jest to wyłącznie kwestia poziomu licencjonowania i funkcjonalności oferowanych na określonych przez producenta oprogramowania poziomach licencjonowania. Istotne bowiem jest to, iż w ramach oprogramowania producenta Cisco nie istnieje taki poziom licencjonowania, który odpowiadałby „jeden do jednego" wymaganiom wynikającym z OPZ, na co zwrócił uwagę Przystępujący (Konsorcjum) w piśmie procesowym z dnia 1 września 2023 r.

Tym samym, w ocenie Izby zarzut ten jest niezasadny.

Niezależnie od powyższego, Izba doszła do przekonania, biorąc pod uwagę dokumenty producenta Cisco, iż w przypadku wyodrębniania oprogramowania poziomów licencji, oprogramowanie w wersji „wyższej" posiada wszystkie funkcjonalności oprogramowania w wersji „niższej", a ponadto posiada dodatkowe funkcjonalności. Tym samym, w ocenie Izby, jeśli producent jednoznacznie wskazuje, że dana funkcjonalność jest dostępna na danym poziomie licencjonowania, to oznacza, że nie jest ona dostępna na niższym poziomie licencjonowania. W takim przypadku mamy do czynienia z zawartością funkcjonalną oprogramowania przedstawioną przez producenta w sposób kaskadowy, na co słusznie zwrócili uwagę Zamawiający, jak również Przystępujący (Konsorcjum).

Izba zważa, że pozostałe dowody wniesione przez Odwołującego i Przystępującego (Konsorcjum) nie miały znaczenia dla rozstrzygnięcia sprawy.

Odnośnie zaś zarzutu dotyczącego tajemnicy przedsiębiorstwa, jest zdaniem Izby niezasadny.

Izba zważa, że ustawa PZP wprowadza generalną zasadę jawności postępowania o udzielenie zamówienia (art. 18 ust. 1 ustawy PZP), czyni jednak zastrzeżenie, iż Zamawiający nie może ujawnić informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeżeli wykonawca składając ofertę

zastrzeże w odniesieniu do tych informacji, że nie mogą być one udostępniane oraz wykazał, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa (art. 18 ust. 3 ustawy PZP).

Tym samym zastrzeżenie jawności informacji ze względu na tajemnicę przedsiębiorstwa stanowi wyjątek od zasady jawności postępowania. W związku z tym, przesłanki umożliwiające jego zastosowanie powinny być interpretowane ściśle. Każde odejście od stosowania zasady jawności wiąże się z powstaniem określonego obowiązku zarówno po stronie Zamawiającego, jak i po stronie podmiotu dokonującego zastrzeżenia. Wykonawca zastrzegający tajność oferty lub innych składanych dokumentów jest zobligowany do przedstawienia w stosunku do każdej informacji objętej tajemnicą przedsiębiorstwa, szczegółowego uzasadnienia oraz wykazania łącznego wystąpienia przestanek definicji legalnej tajemnicy przedsiębiorstwa, o których mowa w art. 11 ust. 2 ustawy o zwalczaniu nieuczciwej konkurencji. Natomiast Zamawiający zobligowany jest do wnikliwego zbadania skuteczności zastrzeżenia tajemnicy przedsiębiorstwa przez wykonawcę i podjęcia stosownych działań w zależności od wyników tej analizy.

Oznacza to, że w dacie składania określonej informacji (jak w niniejszej sprawie w dacie składania wyjaśnień rażąco niskiej ceny wraz z dowodami złożonych w dniu 14 kwietnia 2023 r. i 17 maja 2023 r. oraz wyjaśnień w zakresie treści oferty wraz z dowodami złożonych w dniu 19 maja 2023 r.) wykonawca zastrzegający tajemnicę przedsiębiorstwa musi przedstawić uzasadnione argumenty przekonujące Zamawiającego o tym, iż zastrzegana przez niego informacja zasługuje na ochronę oraz że uzasadnione jest nieujawnianie jej wobec pozostałych uczestników postępowania o udzielenie zamówienia publicznego.

Izba wskazuje, że tajemnicę przedsiębiorstwa definiuje art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji. Zgodnie z tym przepisem, przez tajemnicę przedsiębiorstwa rozumie się informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności. Tym samym, określona informacja stanowi tajemnicę przedsiębiorstwa, jeżeli spełnia kumulatywnie następujące przesłanki:

a. informacje muszą mieć charakter techniczny, technologiczny, organizacyjny przedsiębiorstwa lub inny,
b. informacje muszą posiadać wartość gospodarczą,
c. informacje jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie mogą być powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie mogą być łatwo dostępne dla takich osób,
d. uprawniony do korzystania z informacji lub rozporządzania musi podjąć, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności.

W celu skutecznego zastrzeżenia tajemnicy przedsiębiorstwa, konieczne jest zatem nie tylko wskazanie, iż dane informacje spełniają przesłanki uznania za tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 2 ustawy o zwalczaniu nieuczciwej konkurencji, ale również prawidłowe wykazanie tego faktu. Bezzasadność dokonanego zastrzeżenia, brak złożenia uzasadnienia lub też złożenie niedostatecznie przekonującego uzasadnienia, jego ogólnikowość albo niezłożenie dowodów potwierdzających podjęcie przez wykonawcę środków zmierzających do zachowania informacji w poufności musi skutkować odtajnieniem zastrzeganych informacji.

Izba zwraca uwagę, że zgodnie z wyrokiem Krajowej Izby Odwoławczej z dnia 16 lutego 2018 r, sygn. akt 200/18 *„Dla owego „wykazania" nie wystarczą same deklaracje. Wykonawca winien nie tylko wyjaśnić, ale także udowodnić ziszczenie się poszczególnych przesłanek warunkujących uznanie danej informacji za tajemnicę przedsiębiorstwa. Wbrew twierdzeniom Przystępującego „wykazanie", o którym mowa w art. 8 ust. 3 ZamPublU, oznacza udowodnienie. Pod pojęciem „wykazania" należy rozumieć nie tylko złożenie oświadczenia, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa, ale również przedstawienie stosownych dowodów na jego potwierdzenie".*

Jak wskazał Sąd Okręgowy w Warszawie w wyroku z dnia 1 października 2021 r., sygn. akt XXIII Zs 53/21:,,*Sąd kierując się tym właśnie założeniem uznał, że powinno ono mieć wpływ również na wykładnię pojęcia: „wykazanie", o którym mowa w art. 8 ust. 3 Pzp, w tym sensie, że przewidziany tam przez ustawodawcę obowiązek „wykazania" winien być traktowany jako zbliżony do obowiązku „udowodnienia" w rozumieniu k.p.c.*"

Przenosząc powyższe na kanwę niniejszej sprawy, Izba chciałaby podkreślić, że nie zostały spełnione przez Odwołującego dwie przesłanki z trzech, tj. przesłanka druga i trzecia (informacje jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie mogą być powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie mogą być łatwo dostępne dla takich osób oraz uprawniony do korzystania z informacji lub rozporządzania musi podjąć, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności), co jednoznacznie wynika z pisma Zamawiającego z dnia 9 sierpnia 2023 r. o odtajnieniu informacji zastrzeżonych przez Odwołującego.

Izba doszła do przekonania, iż Odwołujący nie podjął wystarczających działań celem zachowania tych danych w poufności. Mają one charakter na tyle ogólny, że mogłoby w tym samym kształcie zostać przedstawione w każdym innym postępowaniu o udzielenie zamówienia publicznego, o czym świadczą słowa Odwołującego: „Utajnione informacje jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, a uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności. Są one tajemnicą dla podmiotów trzecich i wola ta dla innych osób jest rozpoznawalna."

Nadto Izba zważa, że Odwołujący nie przedstawił dowodu w postaci np. wzoru oświadczenia o zachowaniu w poufności informacji, czy tez wzoru umowy o zachowaniu w poufności, a jedynym dowodem mającym potwierdzać działania celem zachowania danych w poufności, jest dowód w postaci Certyfikatu ISO 9001:2015, który to w ocenie Izby nie stanowi unikatowego charakteru zawartych tam informacji. Z dokumentu tego nie wynikają jakiekolwiek informacje na temat działań podejmowanych w zakresie zachowania określonego katalogu informacji w poufności. Co prawda, Odwołujący powołuje się na dokument w postaci Polityki Bezpieczeństwa Informacji, jednakże nie dołączył go do uzasadnienia objęcia informacji tajemnicą przedsiębiorstwa z dnia 14 kwietnia 2023 r.

Tym samym, w ocenie Izby zarzut ten jest niezasadny.

Konkludując, w ocenie Izby, Zamawiający nie naruszył art. 226 ust. 1 pkt 5 ustawy PZP ani art. 239 ust. 1 ustawy PZP, jak również nie naruszył art. 18 ust. 3 ustawy PZP w zw. z art. 11 ust. 2 ustawy o zwalczaniu nieuczciwej konkurencji.

O kosztach postępowania odwoławczego orzeczono na podstawie art. 574 i 575 ustawy Prawo zamówień publicznych oraz § 2 ust. 1 pkt 2 w zw. z § 8 ust. 2 pkt 1 rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie szczegółowych rodzajów kosztów postępowania odwoławczego, ich rozliczania oraz wysokości i sposobu pobierania wpisu od odwołania (Dz. U. 2020 r. poz. 2437), obciążając kosztami postępowania Odwołującego.

Wobec powyższego orzeczono, jak w sentencji.

Przewodniczący: ……..
Członkowie: ……..
……