sygn. akt:KIO 39/26

WYROK

Warszawa, dnia 3 marca 2026 r.

Krajowa Izba Odwoławcza - w składzie:

Przewodniczący:Maciej Sikorski

Protokolant:Krzysztof Chmielewski

po rozpoznaniu na rozprawie w dniu 25 lutego 2026 roku w Warszawie odwołania wniesionego do Prezesa Krajowej Izby Odwoławczej w dniu 2 stycznia 2026 r. przez wykonawcę Trafford IT Spółka z ograniczoną odpowiedzialnością spółka komandytowa z siedzibą w Warszawie, w postępowaniu prowadzonym przez Skarb Państwa - Państwowe Gospodarstwo Leśne Lasy Państwowe, Zakład Informatyki Lasów Państwowych im. S.K. w Raszynie,

przy udziale uczestnika postępowania odwoławczego po stronie zamawiającego VENTUS Communications spółka z ograniczoną odpowiedzialnością z siedzibą w Poznaniu

orzeka:

1.uwzględnia odwołanie w zakresie zarzutów naruszenia:

- art. 226 ust. 1 pkt 5 ustawy z dnia 11 września 2019 roku – Prawo zamówień publicznych (Dz.U. z 2024 roku, poz. 1320 ze zm.) (dalej: PZP) poprzez bezzasadne odrzucenie oferty wykonawcy Trafford IT Spółka z ograniczoną odpowiedzialnością spółka komandytowa z siedzibą w Warszawie, pomimo że treść jego oferty jest zgodna z warunkami zamówienia,
- art. 226 ust. 1 pkt 5 PZP poprzez zaniechanie odrzucenia oferty VENTUS Communications spółka z ograniczoną odpowiedzialnością z siedzibą w Poznaniu w sytuacji, gdy treść oferty tego wykonawcy jest niezgodna z warunkami zamówienia w zakresie połączenia do linii komend,
- art. 226 ust. 1 pkt 2) lit. b) PZP poprzez zaniechanie odrzucenia oferty VENTUS Communications spółka z ograniczoną odpowiedzialnością z siedzibą w Poznaniu, pomimo że wykonawca ten nie wykazał spełnienia warunku udziału w postępowaniu

i nakazuje zamawiającemu – Skarbowi Państwa - Państwowemu Gospodarstwu Leśnemu Lasy Państwowe, Zakładowi Informatyki Lasów Państwowych im. S.K. w Raszynie – unieważnienie czynności wyboru najkorzystniejszej oferty, unieważnienie czynności odrzucenia oferty wykonawcy Trafford IT Spółka z ograniczoną odpowiedzialnością spółka komandytowa z siedzibą w Warszawie, odrzucenie oferty wykonawcy VENTUS Communications spółka z ograniczoną odpowiedzialnością z siedzibą w Poznaniu i dokonanie ponownej oceny ofert;

2.w pozostałym zakresie oddala odwołanie;

3.kosztami postępowania obciąża odwołującego Trafford IT Spółka z ograniczoną odpowiedzialnością spółka komandytowa z siedzibą w Warszawie w 1/6 kosztów i zamawiającego Skarb Państwa - Państwowe Gospodarstwo Leśne Lasy Państwowe, Zakład Informatyki Lasów Państwowych im. S.K. w Raszyniew 5/6 kosztów i:

3.1.zalicza w poczet kosztów postępowania odwoławczego kwotę 15 000 zł 00 gr (słownie: piętnaście tysięcy złotych zero groszy), poniesioną przez wykonawcę Trafford IT Spółka z ograniczoną odpowiedzialnością spółka komandytowa z siedzibą w Warszawie tytułem wpisu od odwołania,

3.2.zasądza od zamawiającego – Skarbu Państwa - Państwowego Gospodarstwa Leśnego Lasy Państwowe, Zakładu Informatyki Lasów Państwowych im. S.K. w Raszynie– na rzecz wykonawcy Trafford IT Spółka z ograniczoną odpowiedzialnością spółka komandytowa z siedzibą w Warszawie kwotę 12 500 zł 00 gr (słownie: dwanaście tysięcy pięćset złotych zero groszy), tytułem zwrotu różnicy pomiędzy poniesioną a zasądzoną kwotą kosztów postępowania odwoławczego.

Stosownie do art. 579 ust. 1 i art. 580 ust. 1 i 2 PZP, na niniejszy wyrok, w terminie 14°dni od dnia jego doręczenia, przysługuje skarga, za pośrednictwem Prezesa Krajowej Izby Odwoławczej, do Sądu Okręgowego w Warszawie – sądu zamówień publicznych.

Przewodniczący:……..

Uzasadnienie

Zamawiający – Skarb Państwa - Państwowe Gospodarstwo Leśne Lasy Państwowe, Zakład Informatyki Lasów Państwowych im. S.K. w Raszynie – prowadzi postępowanie o udzielenie zamówienia w trybie przetargu nieograniczonego, zgodnie z ustawą z dnia 11.09.2019 r. – Prawo zamówień publicznych (Dz.U. t.j. 2024 r., 1320 ze zm.) (dalej PZP), którego przedmiotem jest: *„Zakup i wdrożenie centralnego systemu ochrony dla urządzeń końcowych funkcjonujących w PGL LP", nr referencyjny: DZ.270.121.2024.*

Szacunkowa wartość zamówienia przekracza kwoty określonej w obwieszczeniu Prezesa Urzędu Zamówień Publicznych wydanym na podstawie art. 3 ust. 3 PZP.

Pismem z dnia 2 stycznia 2026 r. wykonawca Trafford IT Spółka z ograniczoną odpowiedzialnością spółka komandytowa z siedzibą w Warszawie (dalej: Odwołujący lub Trafford) wniósł

1.odwołanie od czynności i zaniechań Zamawiającego t.j.:

przeprowadzenia nieprawidłowej czynności oceny i badania ofert, co doprowadziło do błędnej oceny oferty Odwołującego oraz Ventus Communications sp. z o.o. z siedzibą w Poznaniu, ul. Swoboda 12, 60-391 Poznań (dalej jako: „Ventus") w wyniku której niesłusznie uznano, że treść oferty tego wykonawcy jest zgodna z warunkami zamówienia;

a w konsekwencji,

1.1.bezzasadnego odrzucenia oferty Odwołującego,
1.2.zaniechania odrzucenia oferty Ventus,
1.3.dokonania wyboru oferty Ventus jako najkorzystniejszej,

2.Zamawiającemu zarzucił naruszenie następujących przepisów:

2.1.art. 226 ust. 1 pkt 5) PZP poprzez bezzasadne odrzucenie oferty Odwołującego, pomimo, że treść jego oferty jest zgodna z warunkami zamówienia,

2.2.art. 226 ust. 1 pkt 5) PZP poprzez zaniechanie odrzucenia oferty Ventus w sytuacji, gdy treść oferty tego wykonawcy jest niezgodna z warunkami zamówienia, w zakresie opisanym szerzej w dalszej części Odwołania.

2.3.art. 226 ust. 1 pkt 2 lit. b) PZP poprzez zaniechanie odrzucenia oferty Ventus pomimo, iż wykonawca ten nie wykazał spełnienia warunków udziału w postępowaniu, ewentualnie, naruszenie art. 128 ust. 1 PZP, poprzez zaniechanie wezwania Ventus do uzupełnienia podmiotowych środków dowodowych – wykazu dostaw oraz dokumentów potwierdzających, że zostały one wykonane należycie, w zakresie warunku udziału w postępowaniu zdefiniowanego w pkt VII.4.1. SWZ.

3.Stawiając powyższe zarzuty, Odwołujący wniósł o merytoryczne rozpatrzenie przez Krajową Izbę Odwoławczą (dalej jako: „KIO" lub „Izba") niniejszego Odwołania oraz uwzględnienie go w całości, jak również nakazanie Zamawiającemu:

3.1.unieważnienia czynności wyboru oferty Ventus jako najkorzystniejszej w Postępowaniu,
3.2.unieważnienia czynności odrzucenia oferty Odwołującego,
3.3.odrzucenia oferty Ventus,
3.4.ewentualnie – na wypadek uznania przez Izbę, że nie zachodzą podstawy do odrzucenia oferty Ventus – wezwania Ventus do uzupełnienia wykazu dostaw oraz dokumentów potwierdzających, że zostały one wykonane należycie, w zakresie warunku udziału w postępowaniu zdefiniowanego w pkt VII.4.1. SWZ, w odniesieniu do pozycji 2 wykazu – zamówienia realizowanego na rzecz PKN Orlen S.A., które nie spełnia wymagań postawionych w warunku,
3.5.przeprowadzenia ponownego badania i oceny ofert z uwzględnieniem oferty Odwołującego i z pominięciem oferty Ventus

Pismem z dnia 3 stycznia 2026 r. VENTUS Communications spółka z ograniczoną odpowiedzialnością z siedzibą w Poznaniu (dale: VENTUS lub Przystępujący) zgłosił przystąpienie do postępowania odwoławczego po stronie Zamawiającego.

Zamawiający w piśmie datowanym na dzień 19 lutego 2026 r. wniósł odpowiedź na odwołanie wnosząc o oddalenie odwołania w całości.

VENTUS pismem z dnia 20 lutego 2026 r. przedstawił pismo procesowe stanowiące odpowiedź na wniesione przez Trafford odwołanie.

W piśmie z dnia 20 lutego 2026 r. Odwołujący wniósł o przeprowadzenie dowodów z następujących dokumentów i nagrań, na wskazane poniżej okoliczności, tj.:

1. Oświadczenie producenta Palo Alto z dnia 17 lutego 2026 r., na okoliczność faktów w nim stwierdzonych, tj. tego, że:
   1.1. Cortex XDR v. 4 zapewnia możliwość odzwierciedlenia wielostopniowej struktury organizacyjnej za pomocą automatycznej synchronizacji, za pomocą grup dynamicznych filtrujących stacje robocze i serwery m.in. po ich nazwie lub innych parametrach, w wyniku czego możliwe jest zróżnicowanej widoczności stacji i serwerów dla różnych użytkowników/grup użytkowników.
   1.2. Cortex XDR v. 4 umożliwia definiowanie pojedynczych wskaźników kompromitacji IOC w formie: MD5, SHA256, nazwy domenowej, adresu IPv4 oraz adresu IPv6, wraz z oznaczeniem okresu wygaśnięcia wskaźnika.
   1.3. *Cortex XDR v. 4 posiada mechanizm ochronny przed nieautoryzowanymi próbami wyłączenia agenta, w tym przez użytkowników z uprawnieniami administratora. System może być skonfigurowany w ten sposób, że próba ręcznego wyłączenia modułów bezpieczeństwa lub odinstalowanie agenta na stacji roboczej oraz na serwerach Windows i Linux wymagać będzie dodatkowego potwierdzenia tej czynności poprzez podanie hasła lub autoryzację użytkownika z określonymi uprawnieniami.*
2. Zapytanie ofertowe Orlen S.A. nr 2100107637 wraz z załącznikiem nr 7 – Arkusz wyceny, na okoliczność tego, że:

   Przedmiotem postępowania referencyjnego wskazanego przez Ventus w pkt 2 wykazu dostaw była dostawa licencji i wsparcia technicznego, natomiast nie obejmowało ono wymaganego przez Zamawiającego wdrożenia.

3. Nagranie (hasło: „Oswiadczenia2026!@") z instalacji Cortex XDR v. 4 w systemie Linux, na okoliczność tego, że:

   Cortex XDR spełnia wszystkie wymogi SWZ, w tym, wymogi w zakresie mechanizmów ochronnych przed nieautoryzowanymi próbami wyłączenia agenta.

Zamawiający pismem z dnia 24 lutego 2026 r. w odniesieniu do wniosku dowodowego w postaci „Zapytanie ofertowe Orlen S.A. nr 2100107637 wraz z załącznikiem nr 7 – Arkusz wyceny" zaprezentował następujące stanowisko:

zastrzeżeniu poufności wskazanego dokumentu przez ORLEN S.A. oraz wskazanie dotyczące braku zgody bezpośredniej na dysponowania ww. dokumentem Zamawiający powziął wątpliwości co do autentyczności przedłożonego dokumentu. W konsekwencji wnoszę za pośrednictwem Krajowej Izby Odwoławczej o nieuwzględnianie przesłanego Zapytania ofertowego nr 2100107637, ewentualnie o przedstawienie przez Odwołującego oryginału dokumentu wraz ze wskazaniem źródła jego pozyskania.

VENTUS pismem datowanym na 25 lutego 2026 r. złożonym na rozprawie w dniu 25°lutego 2026 r. przedstawił stanowisko procesowe stanowiące replikę w związku z wnioskami dowodowymi Odwołującego z dnia 20 lutego 2026 r.

Izba ustaliła, co następuje:

Przedmiotem zamówienia, zgodnie z zapisami Specyfikacji Warunków Zamówienia (dalej: SWZ), opisanym w rozdziale IV, jest wdrożenie u Zamawiającego systemu klasy EDR/XDR (Extended/Endpoint Detection and Response – zaawansowane oprogramowanie do ochrony stacji roboczych, serwerów przed zagrożeniami cybernetycznymi) (dalej jako: „System"), z konsolą zarządzającą w formie usługi chmurowej (SaaS), który ma zapewniać:

1) aktywną ochronę stacji końcowych i serwerów przed działaniem złośliwego oprogramowania i innych zaawansowanych cyberzagrożeń;
2) detekcję zagrożeń, identyfikację działań cyberprzestępców oraz zdarzeń z kategorii APT (Advanced Persistent Threats);
3) aktywną reakcję i odpowiedzi na wykryte zdarzenia oraz incydenty;
4) realizację działań proaktywnych, w tym aktywnego wyszukiwania intruzów w infrastrukturze informatycznej,

dostarczone rozwiązanie musi zapewniać obsługę 25.000 szt. urządzeń końcowych.

Zgodnie z zapisami Opisu Przedmiotu Zamówienia (dalej: OPZ) w zakresie struktury organizacyjnej Zamawiającego, w pkt 2.10 i 2.11 OPZ, zapisano:

Pkt 2.10: *System MUSI umożliwić odzwierciedlenie trójstopniowej struktury podziału stacji roboczych i serwerów w PGL LP.*

1) Poziom najwyższy – widoczność wszystkich stacji i serwerów;
2) Poziom pośredni – widoczność stacji i serwerów w obrębie regionu;

3)*Poziom najniższy – widoczność stacji i serwerów w obrębie podstawowej jednostki.*

Pkt 2.11: *Odzwierciedlenie struktury organizacyjnej Zamawiającego zgodnie z punktem 2.10 MUSI być osiągnięte za pomocą automatycznej synchronizacji Microsoft Active Directory Zamawiającego lub za pomocą grup dynamicznych filtrujących stacje robocze i serwery np. po ich nazwie, lub innych automatycznych metod synchronizacji.*"

Pkt 2.37 OPZ – deinstalacja agenta w systemach Linux - przedmiotowe wymaganie OPZ brzmi:

System musi posiadać mechanizm ochronny przed nieautoryzowanymi próbami wyłączenia agenta nawet przez użytkowników z uprawnieniami administratora. Ręczne wyłączenie modułów bezpieczeństwa lub odinstalowanie agenta na stacji roboczej oraz na serwerach Windows i Linux MUSI wymagać dodatkowego potwierdzenia tej czynności

Pkt 2.38 OPZ - Wymagania techniczne dotyczące oferowanego rozwiązania.

System MUSI umożliwiać połączenie do linii komend systemu operacyjnego wybranej stacji roboczej z zainstalowanym agentem z poziomu konsoli zarządzającej Systemu.

W dniu 13 listopada 2025 r. Zamawiający w toku ponownej oceny ofert powziął wątpliwości co do spełnienia trzech wymagań opisanych w Opisie Przedmiotu Zamówienia (dalej: „OPZ"), t.j. w zakresie pkt 2.10., 2.11, 2.15 oraz 2.37.

W wyjaśnieniach z dnia 21 listopada 2025 r. Odwołujący wskazał, że odwzorowanie trójstopniowej struktury Zamawiającego będzie możliwe i wykazał, w jaki sposób zostanie to zapewnione. W pozostałym zakresie Odwołujący przedstawił Zamawiającemu wyjaśnienia.

W piśmie z dnia 21 listopada 2025 r. na wezwanie Zamawiającego z dnia 13 listopada 2025 r. Przystępujący wskazał m.in.:

Poniżej wybrane kategorie zagrożeń, dla których wykonano mapowanie, w wyniku którego podjęto decyzję o zakresie dostępnych komend w funkcji Remote Shell/Remote Access:

a.Luka w aplikacji umożliwia dostęp do danych osobowych klientów (PII).
b.Luka w aplikacji pozwala atakującym kontrolować zasoby obliczeniowe i wykorzystywać je do kopania kryptowalut lub uzyskania trwałego dostępu.
c.Atak typu man-in-the-middle może przechwycić ruch między klientem a usługą.
d.Oszuści phishingowi wykorzystują aplikację webową do ujawnienia danych uwierzytelniających aplikacji.
e.Luka w aplikacji prowadzi do wykonania kodu z uprawnieniami aplikacji.
f.Dane przechowywane przez aplikację w chmurze są niewystarczająco chronione. co umożliwia nieuprzywilejowanym podmiotom i atakującym ujawnienie wrażliwych informacji.
g.Atakujący mogą modyfikować system, zacierać ślady lub omijać systemy monitorujące.

W toku rozprawy w sprawie o sygn. KIO 3776/25 i KIO 3798/25. VENTUS oświadczył przed Izbą, w ramacl prezentacji rozwiązania wskazanego w ofercie, że zaoferowany produkt Trend Micro:

jest w stanie uruchomić każde polecenie, każdą komendę na systemie końcowym (310 poleceń linii komend wskazane przez Odwołującego), mimo iż nie jest to wymagane w SWZ. Następuje to poprzez przesłanie pliku na dowolną stację i za pomocą tego pliku następuje uruchomienie komend tej stacji. Wskazuje na komendę run (skryptu) wskazanego w dokumentacji technicznej jest w stanie uruchomić każdą komendę na dowolnej stacji roboczej.

Sprawa wykonywania poleceń na zdalnej stacji roboczej za pomocą skryptów była przedmiotem pytania nr 11 do OPZ. Zamawiający w odpowiedzi z dnia 16 czerwca 2025 r. wskazał, że nie dopuszcza takiej możliwości:

Pytanie 11:

Rozdział II pkt 2.38 – Czy zamawiający dopuszcza, aby wykonywane polecenia na zdalnej stacji roboczej były możliwe do wykonania za pomocą skryptów wypychanych na stacje robocze? Producent oferowanego rozwiązania planuje dodanie konsoli zdalnego dostępu na początku roku 2026."

Odpowiedź:

Zamawiający nie dopuszcza takiego rozwiązania.

W dniu 13 listopada 2025 r., Zamawiający zwrócił się o wyjaśnienie kwestii związanej z możliwością zapewnienia dostępu do poleceń/komend za pomocą skryptu. W odpowiedzi na wezwanie Zamawiającego VENTUS wskazał:

Przedmiotowe pytanie dotyczy rozwiązania, które nie posiada żadnej możliwości dostępu do linii komend systemu operacyjnego wybranej stacji roboczej z zainstalowanym agentem ani żadnej konsoli zdalnego dostępu. W takiej sytuacji jedyną możliwością dostępu do zdalnej stacji roboczej, jakie może być zastosowane jest „wypychanie skryptów na stacje robocze" i ich uruchamianie w trybie automatycznym bez żadnej kontroli środowiska uruchomieniowego skryptu.

Zgodnie z pkt VII.4.1. SWZ:

4.1 Warunek dotyczący doświadczenia: Zamawiający uzna ten warunek za spełniony, jeżeli Wykonawca wykaże, nie później niż na dzień składania ofert, że w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie – wykonał należycie, co najmniej dwa zamówienia polegające na dostawie i wdrożeniu systemu EDR lub XDR dla stacji roboczych i serwerów na minimum 2000 urządzeń

albo

wykonał należycie, co najmniej dwa zamówienia polegające na dostawie i wdrożeniu systemu EDR lub XDR dla stacji roboczych i serwerów na minimum 2000 urządzeń, w tym jednego na dostawę i wdrożenie systemu EDR lub XDR dla stacji roboczych i serwerów na minimum 2000 urządzeń oraz drugiego zamówienie na dostawę i wdrożenie rozwiązania klasy endpoint security chroniącego użytkowników przed ransomware oraz kradzieżą tożsamości na minimum 2000 urządzeń o ile wdrożenie rozwiązania klasy endpoint security obejmowało konsolę chmurową."

VENTUS wykazał spełnienie powyższego warunku poprzez wskazanie na umowę realizowaną przez IT Solution Factor sp. z o. o. na rzecz PKN Orlen SA. Na potwierdzenie należytego wykonania zamówienia, VENTUS przedstaw dokument w postaci protokołu odbioru potwierdzający wykonanie dostawy.

Zamawiający pismem z dnia 8 grudnia 2025 r. zwrócił się do VENTUS o wyjaśnienia, wskazując:

Z dostarczonego protokołu odbioru wynika, że dostawa i wdrożenie zostały wykonane w jeden dzień – proszę o wyjaśnienie przedmiotowej kwestii w kontekście możliwości technicznych/logistycznych wykonania wdrożenia w tak krótkim czasie.

W odpowiedzi z dnia 11 grudnia 2025 r. VENTUS wskazał, iż:

Szczegółowe kwestie dotyczące wdrożenia objęte są tajemnicą przedsiębiorstwa oraz są informacjami wrażliwymi ze względu na charakter odbiorcy (Orlen SA). Tym samym nie jest możliwe przekazywanie tych informacji w jawnym postępowaniu o udzielenie zamówienia publicznego.

Do wyjaśnień VENTUS załączył korespondencję mailową z pracownikiem PKN Orlen S.A. z dnia 3 grudnia 2025 r o treści:

Wdrożenie było przeprowadzone prawidłowo i zakończyło się sukcesem ale wystawianie referencji w ORLENIE wymaga przeprocesowania, zarejestrowania, uzyskania odpowiednich zgód korporacyjnych i podpisania przez osoby upoważnione.

Zamawiający, pismem z dnia 23 grudnia 2025 r. zawiadomił o wyborze oferty najkorzystniejszej oraz poinformował o odrzuceniu oferty Odwołującego.

W uzasadnieniu odrzucenia Zamawiający przedstawił następujące uzasadnienie faktyczne:

a) Brak mechanizmu „dodatkowego potwierdzenia" przy deinstalacji agenta na Linux (Niezgodność z OPZ 2.37): Zamawiający wymagał, aby odinstalowanie agenta na systemach Windows i Linux wymagało „dodatkowego potwierdzenia tej czynności". Trafford wskazał na funkcję Mandatory Root Access. Jak wynika z analizy technicznej, oznacza to jedynie, że do wykonania operacji potrzebne są uprawnienia root'a (administratora systemu). Po uzyskaniu tych uprawnień, agenta można usunąć standardowymi komendami systemowymi (np. rpm -e) bez żadnego dodatkowego potwierdzenia ze strony Systemu (np. hasła deinstalacyjnego). Jest to standardowy model uprawnień systemu operacyjnego, a nie wymagany przez Zamawiający mechanizm ochronny aplikacji „anti-tamper" z dodatkową autoryzacją.

b) Niezgodność w zakresie wskaźników IOC i IPv6 (Niezgodność z OPZ 2.15): Zamawiający wymagał natywnego definiowania wskaźników kompromitacji (IOC) m.in. w formie adresu IPv6.

– Brak funkcjonalności: Moduł IOC w zaoferowanej wersji Cortex XDR 4.x odrzuca adresy IPv6. Proponowane przez wykonawcę obejście (Lookup Dataset + reguły korelacyjne BIOC) nie jest tożsame z wymaganym repozytorium IOC – wymaga tworzenia skomplikowanych reguł zamiast prostych wskaźników i nie spełnia

wymogu prostego dodawania wskaźników z „oznaczeniem okresu wygaśnięcia" w sposób literalnie wymagany przez OPZ

– *Rozbieżność licencyjna: Funkcjonalność dodawania reguł IOC w wymaganym zakresie może być dostępna dopiero w licencji Cortex XDR Pro, podczas gdy w ofercie wskazano wersję „Cortex XDR Wersja 4". Stanowi to rozbieżność produktową, sugerującą, że zaoferowany wariant licencyjny nie posiada wymaganych funkcjonalności.*

c) *Brak struktury hierarchicznej (Niezgodność z OPZ 2.10/2.11): System opiera się na płaskim modelu danych z filtrowaniem (RBAC/SBAC), co nie tworzy wymaganej trójstopniowej struktury hierarchicznej (drzewa) zagnieżdżonych węzłów (Centrala -> Region -> Jednostka). Filtrowanie widoków nie jest równoważne z odwzorowaniem struktury organizacyjnej w modelu danych.*

Izba zważyła co następuje:

Izba ustaliła, że Odwołujący jest uprawniony do korzystania ze środków ochrony prawnej w rozumieniu art. 505 ust. 1 PZP. Okoliczność ta nie była pomiędzy stronami sporna.

Zgłoszenie VENTUS Communications spółka z ograniczoną odpowiedzialnością z siedzibą w Poznaniu, do postępowania odwoławczego po stronie Zamawiającego, Izba uznała za skuteczne.

Izba uznała za uzasadniony zarzut naruszenia art. 226 ust. 1 pkt 5 ustawy z dnia 11 września 2019 roku – Prawo zamówień publicznych (Dz.U. z 2024 roku, poz. 1320 ze zm.) (dalej: PZP) poprzez bezzasadne odrzucenie oferty wykonawcy Trafford IT Spółka z ograniczoną odpowiedzialnością spółka komandytowa z siedzibą w Warszawie, pomimo że treść jego oferty jest zgodna z warunkami zamówienia.

Zamawiający zarzucił ofercie Odwołującego brak trójstopniowej struktury hierarchicznej zagnieżdżonych węzłów i stwierdził, że nie jest dopuszczalne odwzorowanie struktury organizacyjnej poprzez filtrowanie widoków. W ocenie Zamawiającego oferta Odwołującego nie spełnia wymagania z pkt. 2.10 i 2.11 OPZ.

Z ustaleń dokonanych w sprawie wynika, że w pkt 2.10 i 2.11 OPZ (ani w żadnym innym postanowieniu OPZ czy też wyjaśnień treści SWZ), nie ma ani wymagania, by w systemie miała być tworzona trójstopniowa struktura zagnieżdżonych węzłów, ani nie ma zakazu zrealizowania wymagania poprzez filtrowanie widoków. Wymagania z pkt 2.10 i 2.11 OPZ przewidują jedynie, że odzwierciedlenie trójstopniowej struktury opisanej w pkt 2.10 ma być realizowane jakąkolwiek automatyczną metodą synchronizacji (w tym – jak wprost stwierdzono w wymaganiu – za pomocą grup dynamicznych filtrujących stacje robocze i serwery, np. po ich nazwie). Zamawiający nie wykazał ani nawet nie uprawdopodobnił tezy, że tak sformułowane wymagania nie są przez Odwołującego spełnione.

Zamawiający zarzucił ofercie Odwołującego niezgodność z wymaganiem 2.15 OPZ – w zakresie wskaźników IOC i IPv6.

Zamawiający w informacji o odrzuceniu oferty Odwołującego stwierdził, że wymagał natywnego definiowania wskaźników kompromitacji, m.in. adresu IPv6. Moduł IOC w wersji Cortex 4.x odrzuca adresy IPv6, a Odwołujący proponuje obejście, które nie spełnia wymagania Zamawiającego, ponieważ *wymaga tworzenia skomplikowanych reguł zamiast prostych wskaźników i nie spełnia wymogu prostego dodawania wskaźników z oznaczeniem okresu wygaśnięcia w sposób literalnie wymagany przez OPZ. Funkcjonalność dodawania reguł IOC w wymaganym zakresie będzie dostępna dopiero w licencji Cortex XDR Pro, podczas gdy w ofercie wskazano wersję Cortex XDR Wersja 4.*

W tym miejscu trzeba odnotować, że w OPZ brak jest wymagania „natywnego" definiowania wskaźników kompromitacji i brak jest zakazu ich dodawania poprzez funkcjonalność reguł korelacyjnych.

W następnej kolejności stwierdzić należy, że Zamawiający sam potwierdził, że oferta Odwołującego spełnia postawiony wymóg. Zamawiający w dokumentach postępowania nie wymagał osiągnięcia danej funkcjonalności w określony sposób, jak również nie zakazał sposobu, jakim posłużył się Odwołujący. W szczególności Zamawiający nie wymagał, by dane rozwiązanie osiągnąć w sposób o określonym stopniu skomplikowania.

Referując do tzw. „prostego dodawania wskaźników" należy podkreślić, że dodawanie omawianych wskaźników nie wymaga tworzenia „skomplikowanych" reguł, lecz jest metodą tzw. reguł korelacyjnych BIOC (behavioral indicators of compromise), której zastosowanie jest typowe w ramach obsługi systemu tej klasy, jaki objęty jest zamówieniem.

Należy zgodzić się z Odwołującym, iż dodawanie wskaźników kompromitacji nie jest zadaniem dedykowanym do przeciętnego użytkownika, lecz administratora systemu, czyli osoby z definicji posiadającej wysoki poziom wiedzy i umiejętności. Ponadto ani w zapisach SWZ ani w wyjaśnieniach jej treści nie postawiono wymagania, by dodawanie wskaźników kompromitacji miało być „proste", a już tym bardziej nie zdefiniowano, jak ową „prostotę" należy rozumieć.

Odnosząc się do zarzutu w zakresie „rozbieżności licencyjnej", Izba wskazuje, że Odwołujący szczegółowo wyjaśnił tę kwestię w piśmie z 21 listopada 2025 r., przytaczając stosowne postanowienia dokumentacji producenta. Zamawiający w żaden sposób się do tych wyjaśnień nie odniósł. Uzasadnienie odrzucenia oferty Odwołującego jest lakoniczne i praktycznie jednozdaniowe.

Zamawiający zarzucił, że oferta Odwołującego nie spełnia wymagania z pkt. 2.37 OPZ. Zamawiający zakwestionował spełnienie wymagania poprzez tzw. „mandatory root access", stwierdzając, że jest to s*tandardowy model uprawnień systemu operacyjnego, a nie wymagany przez Zamawiającego mechanizm obrony aplikacji „anti-tamper" z dodatkową autoryzacją".*

Odwołujący wywodzi, iż, Zamawiający w uzasadnieniu odrzucenia oferty istotnie rozszerza i modyfikuje postawione w OPZ wymagania. Otóż, wymaganie z pkt 2.37 OPZ stanowi, że nawet użytkownik z uprawnieniami administratora nie może ręcznie wyłączyć modułu bezpieczeństwa ani odinstalować agenta na stacji roboczej, a wykonanie takiej czynności musi wymagać dodatkowego potwierdzenia.

Odwołujący w wyjaśnieniach z dnia 21 listopada 2025 r., wskazał, że funkcja Mandatory Root Access powoduje, że *próba ręcznego wyłączenia modułu bezpieczeństwa lub odinstalowania agenta przez dowolnego użytkownika (w tym z uprawieniami administratora) zakończy się niepowodzeniem, konieczna będzie akcja ze strony roota*. W ocenie Izby Odwołujący wykazał spełnienie przedmiotowego wymagania. Rozwiązanie zaoferowane przez Odwołującego posiada funkcjonalności wskazane w pkt. 2.37 OPZ i odpowiada opisowi zawartemu w opisie tego punktu. Jednocześnie stwierdzić należy, że Zamawiający ani w°pkt°2.37, ani w żadnym innym postanowieniu SWZ czy jej wyjaśnień nie wymagał „mechanizmu obronnego anti-tamper" ani też nie zakazywał realizacji wymagania poprzez wykorzystanie standardowych modeli uprawnień.

Izba uznała za uzasadniony zarzut naruszenia art. 226 ust. 1 pkt 5 PZP poprzez zaniechanie odrzucenia oferty VENTUS Communications spółka z ograniczoną odpowiedzialnością z siedzibą w Poznaniu w sytuacji, gdy treść oferty tego wykonawcy jest niezgodna z warunkami zamówienia w zakresie połączenia do linii komend.

Izba stwierdza, że pomiędzy stronami nie było sporu w zakresie tego, iż Przystępujący zaoferował niepełny dostęp do linii komend. Istota zarzutu sprowadza się do ustalenia, czy Przystępujący był uprawniony do zaoferowania niepełnego dostępu do linii komend.

Wymagania techniczne dotyczące oferowanego rozwiązania w pkt 2.38 OPZ brzmią:

System MUSI umożliwiać połączenie do linii komend systemu operacyjnego wybranej stacji roboczej z zainstalowanym agentem z poziomu konsoli zarządzającej Systemu.

Redakcja cytowanego wymogu nie zakłada częściowego czy zdefiniowanego dostępu do linii komend. Skoro dostęp ten nie jest w żaden sposób limitowany, nie można zasadnie formułować tezy, zgodnie z którą Zamawiający oczekiwał bądź dopuszczał ograniczony dostęp do linii komend. Gdyby nawet założyć, że intencją Zamawiającego było dopuszczenie limitowanego dostępu do linii komend zamiast pełnego (niczym nie ograniczonego) to winno takie oczekiwanie zostać odzwierciedlone w dokumentacji przetargowej, a tak się jednak nie stało.

Jak wynika z pkt 2.38 OPZ „System MUSI umożliwiać połączenie do linii komend systemu operacyjnego wybranej stacji roboczej z zainstalowanym agentem z poziomu konsoli zarządzającej Systemu." Wymaganie to jasno wskazuje, że Zamawiający żądał umożliwienia połączenia do linii komend systemu operacyjnego, przy czym Zamawiający w żadnym miejscu nie wskazał na potrzebę dostępu limitowanego tj. ograniczonego do jakiegoś mniej lub bardziej zdefiniowanego zbioru komend.

Izba uznała za nieuzasadniony zarzut dotyczący nieprawidłowej oceny wyjaśnień złożonych przez VENTUS, ponieważ z dokumentów złożonych przez VENTUS, w tym wyjaśnień z dnia 21 listopada 2025 r., nie wynika, aby rozwiązanie polegające na wykonywaniu poleceń za pomocą skryptów było oferowane przez VENTUS.

Niezależnie od powyższego, Izba oddaliła wniosek o powołanie dowodu z opinii biegłego, stwierdzając, że fakty, które miały zostać wykazane opinią biegłego, mogą zostać stwierdzone innymi dowodami złożonymi w postępowaniu.

Izba uznała za uzasadniony zarzut niewykazania przez VENTUS spełnienia warunków udziału w postępowaniu.

Należy zauważyć, że z przedstawionych przez VENTUS dokumentów oraz z wyjaśnień z dnia 16 grudnia 2025 r. wynika, że projekt realizowany na rzecz PKN Orlen S.A. nie obejmował wymaganego przez Zamawiającego wdrożenia.

Z treści dokumentów wynika, iż wdrożenie systemu EDR/XDR na min. 2000 urządzeń zostało wykonane w czasie 4 godzin, co budziło uzasadnione wątpliwości w zakresie możliwości realizacji we wskazanym czasie. Jednocześnie brak jest jakiegokolwiek dowodu potwierdzającego, że wdrożenie takie miało miejsce i zostało wykonane należycie.

Z ustaleń dokonanych w sprawie wynika, że Zamawiający zwrócił się do VENTUS o wyjaśnienia w zakresie możliwości wykonania dostawy i wdrożenia w jeden dzień. W odpowiedzi VENTUS stwierdził, że nie może przedmiotowej kwestii wyjaśnić w jawnym postępowaniu o udzielenie zamówienia publicznego, ponieważ jest objęta tajemnicą przedsiębiorstwa PKN Orlen S.A. Dodatkowo, VENTUS dołączył do wyjaśnień korespondencję mailową z kierownikiem działu cyberbezpieczeństwa PKN Orlen S.A., który oświadczył, że wdrożenie było przeprowadzone prawidłowo, ale wystawianie referencji w PKN Orlen S.A. jest skomplikowanym procesem.

Izba podziela stanowisko Odwołującego, że Przystępujący w istocie nie udzielił wyjaśnień w zakresie, o który został zapytany przez Zamawiającego. Wskazać należy, że przepisy PZP przewidują instrumenty mające na celu zachowanie w poufności informacji przekazywanych Zamawiającemu. Przystępujący z instrumentów tych nie skorzystał. Ponadto Izba przeanalizowała złożoną przez Przystępującego korespondencję z kierownikiem działu cyberbezpieczeństwa PKN Orlen S.A. i skonstatowała, że przyznał on, że nie jest osobą uprawnioną do udzielania informacji w zakresie dotyczącym realizacji usługi.

Tym samym stwierdzić należy, że Przystępujący nie potwierdził i nie wyjaśnił faktu wdrożenia systemu dla PKN Orlen S.A. co jest równoznaczne z tym, iż nie wykazał spełniania warunku udziału w postępowaniu.

Z uwagi na powyższe orzeczono jak na wstępie.

O kosztach postępowania odwoławczego orzeczono na podstawie art. 575 PZP, stosownie do wyniku postępowania oraz na podstawie § 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. z 2020 r. poz. 2437).

Przewodniczący:…….