Sygn. akt: KIO 4137/26

WYROK

Warszawa, 12 października 2026 r.

Krajowa Izba Odwoławcza – w składzie:

Przewodnicząca:Anna Chudzik

Protokolant: W.Z.

po rozpoznaniu na rozprawie odwołania wniesionego do Prezesa Krajowej Izby Odwoławczej 21 sierpnia 2026 r. przez wykonawcę ITT-Pro Sp. z o.o. z siedzibą w Warszawie,

w postępowaniu prowadzonym przez Pocztę Polską S.A. z siedzibą w Warszawie,

orzeka:

1.Umarza postępowanie odwoławcze w zakresie zarzutów opisanych w odwołaniu w poz. tabeli: od 4 do 13, od 15 do 19 oraz 21;

2.W pozostałym zakresie oddala odwołanie;

3.Kosztami postępowania obciąża wykonawcę ITT-Pro Sp. z o.o. z siedzibą w Warszawie i:

3.1.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 oraz kwotę 3 600 zł 00 gr (słownie: trzy tysiące sześćset złotych zero groszy) poniesioną przez Zamawiającego tytułem wynagrodzenia pełnomocnika;

3.2.zasądza od Odwołującego na rzecz Zamawiającego kwotę 3 600 zł 00 gr (słownie: trzy tysiące sześćset złotych zero groszy) stanowiącą koszty postępowania odwoławczego poniesione przez Zamawiającego.

Na orzeczenie – w terminie 14 dni od dnia jego doręczenia – przysługuje skarga za pośrednictwem Prezesa Krajowej Izby Odwoławczej do Sądu Okręgowego w Warszawie – Sądu Zamówień Publicznych.

Przewodnicząca:……

Sygn. akt: KIO 4137/26

Uzasadnienie

Zamawiający – Poczta Polska S.A.– prowadzi w trybie przetargu nieograniczonego postępowanie o udzielenie zamówienia pn. *Dostawa licencji bezpieczeństwa do Systemu DNS* Wartość zamówienia jest większa niż progi unijne. Ogłoszenie o zamówieniu zostało opublikowane w Dzienniku Urzędowym Unii Europejskiej 11 sierpnia 2026 r. nr 553969-2026.

Wykonawca ITT-Pro Sp. z o.o.wniósł 21 sierpnia 2026 r. odwołanie wobec treści dokumentów zamówienia, zarzucając Zamawiającemu naruszenie przepisów:

1)art. 99 ust. 1, 2, 4 i 5 w zw. z art. 101 ust. 1 pkt 1 w zw. z art. 16 pkt 1-3 ustawy Pzp, poprzez wprowadzenie w dokumentach zamówienia, w szczególności w rozdz. IV ust. 1 SWZ oraz w rozdz. I OPZ nazwy konkretnego produktu, który zamierza nabyć Zamawiający, tj. dodatkowych tokenów security dla oprogramowania Infoblox, posiadanego aktualnie przez Zamawiającego, podczas gdy Zamawiający mógł opisać przedmiot zamówienia w wystarczająco precyzyjny i zrozumiały sposób, bez podawania nazwy konkretnego produktu i producenta, w szczególności poprzez określenie obiektywnych wymagań dotyczących wydajności lub funkcjonalności oczekiwanego rozwiązania, co prowadzi do nieuzasadnionego ograniczenia zasady uczciwej konkurencji i równego traktowania wykonawców poprzez uprzywilejowanie produktów jednego producenta – Infoblox oraz do naruszenia zasady proporcjonalności i efektywności,

2)art. 99 ust. 5 i 6 w zw. z art. 16 pkt 1-3 ustawy Pzp, poprzez dopuszczenie w rozdziale II f OPZ rozwiązań równoważnych do licencji Infoblox, podczas gdy sformułowane kryteria równoważności spełnia tylko jedno rozwiązanie dostępne na rynku, tj. Infoblox, co prowadzi do wniosku, że równoważność ta ma charakter wyłącznie

pozorny, a tym samym prowadzi do nieuzasadnionego ograniczenia zasady uczciwej konkurencji i równego traktowania wykonawców poprzez uprzywilejowanie jednego wykonawcy – Infoblox oraz do naruszenia zasady proporcjonalności i efektywności (zarzut ewentualny do zarzutu 1);

3)art. 99 ust. 1, 2, 4 i 5 w zw. z art. 101 ust. 1 pkt 1 ustawy Pzp, poprzez sformułowanie kryteriów równoważności w sposób ograniczający uczciwą konkurencję i pozbawiający Odwołującego szans na złożenie oferty, mimo że Odwołujący jest w stanie zapewnić rozwiązanie zaspokajające potrzeby Zamawiającego (zarzut ewentualny do zarzutu 2).

Odwołujący wniósł o nakazanie Zamawiającemu:

–wykreślenia z dokumentów zamówienia wszystkich odniesień do produktów firmy Infoblox oraz opisanie przedmiotu zamówienia za pomocą obiektywnych parametrów odnoszących się do wymagań dotyczących wydajności lub funkcjonalności – tak, aby umożliwić ubieganie się o zamówienie wszystkim wykonawcom oferującym rozwiązania spełniające te parametry (Zarzut nr 1);

–ewentualnie – gdyby Zamawiający wykazał istnienie obiektywnych przesłanek z art. 99 ust. 5 ustawy Pzp – zmodyfikowanie lub uzupełnienie sformułowanie kryteriów równoważności przy zastosowaniu obiektywnych parametrów odnoszących się do wymagań dotyczących wydajności lub funkcjonalności, bez wskazywania na funkcjonalności Infoblox, np. w sposób opisany w tabeli na stronach 9 – 23 odwołania (Zarzuty nr 2 i 3 – ewentualne).

Na podstawie dokumentacji przedmiotowego postępowania oraz biorąc pod uwagę stanowiska stron, Izba ustaliła i zważyła, co następuje:

Izba umorzyła postępowanie odwoławcze w zakresie zarzutów opisanych w odwołaniu w poz. tabeli: od 4 do 13, od 15 do 16, od 18 do 19 i 21 – z uwagi na ich uwzględnienie przez Zamawiającego, a także w poz. 17 – z uwagi na złożenie przez Odwołującego oświadczenia o wycofaniu tego zarzutu.

W zakresie podlegającym merytorycznemu rozpoznaniu odwołanie nie zasługuje na uwzględnienie.

Izba ustaliła następujący stan faktyczny:

Zgodnie z rozdz. IV SWZ (Opis przedmiotu zamówienia):

1. Przedmiotem zamówienia jest dostarczenie i wdrożenie przez Wykonawcę na rzecz Zamawiającego rozwiązania informatycznego obejmującego funkcjonalność ochrony użytkowników przed zagrożeniami na bazie protokołu DNS (System) zgodnie z Ofertą: poprzez rozszerzenie posiadanych przez Zamawiającego subskrypcji, o których mowa w OPZ, o dodatkowe tokeny security dla 44 000 urządzeń albo poprzez dostarczenie rozwiązania równoważnego spełniającego wymagania określone w OPZ, jak i konfigurację Systemu, w sposób niezbędny do poprawnego działania tego Systemu.

2. W ramach przedmiotu zamówienia Wykonawca zobowiązuje się w szczególności:

1)dostarczyć, wdrożyć, uruchomić i skonfigurować System,

2)wykonać Dokumentację,

3)wykonać transfer wiedzy w postaci warsztatów dla osób wskazanych przez Zamawiającego,

4)udzielić lub zapewnić udzielenie wszelkich licencji wymaganych do prawidłowego działania Systemu, jako całości jak i poszczególnych jego elementów, na zasadach określonych w Umowie oraz OPZ,

5)przenieść na Zamawiającego autorskie prawa majątkowe do Dokumentacji opracowanej przez Wykonawcę w ramach Umowy,

6)udzielić Zamawiającemu Gwarancji na dostarczony w ramach umowy System na okres 36 miesięcy od dnia podpisania bez zastrzeżeń Protokołu Odbioru Wdrożenia Systemu oraz świadczyć w tym okresie usługi gwarancyjne, w ramach wynagrodzenia wynikającego z Umowy.

W załączniku nr 6 do SWZ Zamawiający zamieścił Szczegółowy opis przedmiotu zamówienia oraz zasady realizacji przedmiotu zamówienia (dalej: OPZ).

Zamawiający podał w OPZ, że obecnie posiada 2 subskrypcje Infoblox BloxOne Threat Defense Essentials dla serwerów klasy Infoblox TE-2326 oraz subskrypcję Infoblox Security Ecosystem Business dla systemu typu grid składającego się z maks. 20 serwerów. Subskrypcje te są ważne do dnia 10 października 2027.

W punkcie II lit. f OPZ Zamawiający opisał wymagania w zakresie Systemu ochrony użytkowników przed zagrożeniami na bazie protokołu DNS dla rozwiązania równoważnego, wskazując m.in. na następujące wymagania:

1.2.4.Kierowane pośrednio poprzez wirtualny serwer *forwarding DNS*, przekazujący zapytania do wskazanych serwerów, możliwy do zaimplementowania w sieci wew. Zamawiającego jako maszyna wirtualna możliwa do zainstalowania na platformach Vmware, Microsoft Hyper-V oraz KVM.

(1)Proxy musi dodawać do zapytań DNS informację o wew. prywatnym adresie IP komputera.

(2)Proxy musi przesyłać zapytania DNS do Usługi w sposób zaszyfrowany poprzez protokół DNS-over-TLS lub DNS-over-HTTPS.

(3)Usługa musi obejmować prawo do instalacji dowolnej liczby serwerów typu *forwarding*

1.2.5.poprzez oprogramowanie agenta DNS dostarczone wraz z usługą i uruchomione na komputerach pracowników Zamawiającego

1)Agent musi wspierać systemy operacyjne MS Windows 11 oraz Mac OS w wersjach Tahoe, Sequoia, Sonoma, Linux, Android 11+, iPhone IOS 14+, iPad IOS 14+

2)Agent musi dodawać do zapytań DNS informację o nazwie komputera, adresie MAC komputera, nazwę użytkownika i wersję systemu operacyjnego.

3)Agent musi przesyłać zapytania DNS do usługi Bezpieczny DNS w sposób zaszyfrowany poprzez protokół DNS-over-TLS lub DNS-over-HTTPS.

4)Agent musi wspierać możliwość instalacji w środowisku Active Directory przy wykorzystaniu mechanizmu GPO oraz w środowisku Apple z wykorzystaniem Apple Remote Desktop, a w przypadku urządzeń Android/iPhone/iPad przy pomocy systemu klasy mobile device management, jak i bez takiego systemu.

9.2.Raporty bezpieczeństwa muszą zapewniać możliwość identyfikacji urządzenia i użytkownika z zapytaniem i odpowiedzią na nie, oraz akcją podjętą w ramach polityki bezpieczeństwa rozwiązania niezależnie od tego czy Użytkownik jest objęty monitoringiem innych systemów bezpieczeństwa Zamawiającego i czy jego tożsamość jest powiązana z systemami Zamawiającego.

9.3.grupowania zdarzeń per użytkownik, źródło zapytań (serwery DNS, agent, sieć IP), oryginalne źródło zapytania (prywatny adres IP z sieci LAN, adres publiczny, lub nazwa komputera z oprogramowaniem agenta).

15.Usługa musi być świadczona na bazie licencji ważnej co najmniej 3 lata od daty podpisania protokołu odbioru wdrożenia Systemu przez Zamawiającego i obejmującej wsparcie Usługodawcy.

Licencje muszą gwarantować dostęp do Usługi w celu ochrony min. 44 000 urządzeń generujących zapytania o domeny internetowe oraz muszą umożliwiać przesyłanie co najmniej 330 000 000 zdarzeń bezpieczeństwa miesięcznie do systemu SIEM Zamawiającego. Jeśli oferowane rozwiązanie licencjonowane jest od liczby pracowników, to należy przyjąć, że Usługę należy dostarczyć z licencją dla 50 000 pracowników z równoczesnym zapewnieniem licencji dla 2 000 serwerów.

Izba zważyła, co następuje:

Zgodnie z art. 99 ustawy Pzp:

- ust. 1: Przedmiot zamówienia opisuje się w sposób jednoznaczny i wyczerpujący, za pomocą dostatecznie dokładnych i zrozumiałych określeń, uwzględniając wymagania i okoliczności mogące mieć wpływ na sporządzenie oferty.
- ust. 2: Zamawiający określa w opisie przedmiotu zamówienia wymagane cechy dostaw, usług lub robót budowlanych. Cechy te mogą odnosić się w szczególności do określonego procesu, metody produkcji, realizacji wymaganych dostaw, usług lub robót budowlanych, lub do konkretnego procesu innego etapu ich cyklu życia, nawet jeżeli te czynniki nie są ich istotnym elementem, pod warunkiem że są one związane z przedmiotem zamówienia oraz proporcjonalne do jego wartości i celów.
- ust. 4: Przedmiotu zamówienia nie można opisywać w sposób, który mógłby utrudniać uczciwą konkurencję, w szczególności przez wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę, jeżeli mogłoby to doprowadzić do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów.
- ust. 5. Przedmiot zamówienia można opisać przez wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę,

jeżeli zamawiający nie może opisać przedmiotu zamówienia w wystarczająco precyzyjny i zrozumiały sposób, a wskazaniu takiemu towarzyszą wyrazy "lub równoważny".

–ust. 6: Jeżeli przedmiot zamówienia został opisany w sposób, o którym mowa w ust. 5, zamawiający wskazuje w opisie przedmiotu zamówienia kryteria stosowane w celu oceny równoważności.

Stosownie do art. 101 ust. 1 pkt 1 ustawy Pzp przedmiot zamówienia opisuje się, z uwzględnieniem odrębnych przepisów, w jeden z następujących sposobów przez: 1) określenie wymagań dotyczących wydajności lub funkcjonalności, w tym wymagań środowiskowych, pod warunkiem że podane parametry są dostatecznie precyzyjne, aby umożliwić wykonawcom ustalenie przedmiotu zamówienia, a zamawiającemu udzielenie zamówienia.

Art. 16 ustawy Pzp stanowi, że zamawiający przygotowuje i przeprowadza postępowanie o udzielenie zamówienia w sposób: 1) zapewniający zachowanie uczciwej konkurencji oraz równe traktowanie wykonawców; 2) przejrzysty; 3) proporcjonalny.

W ocenie Izby Odwołujący nie wykazał, że Zamawiający naruszył przytoczone wyżej przepisy ustawy.

Na wstępie podkreślenia wymaga, że odwołania dotyczące postanowień dokumentów zamówienia, w tym opisu przedmiotu zamówienia, tak jak dotyczące każdej innej czynności lub zaniechania zamawiającego, służą ochronie wykonawców przed działaniami niezgodnymi z przepisami prawa (art. 513 ustawy Pzp), nie są natomiast narzędziem służącym „negocjowaniu" przez wykonawców bardziej korzystnych dla nich warunków zamówienia. Izba może uwzględnić odwołanie wyłącznie w sytuacji, gdy stwierdzi naruszenie przez Zamawiającego przepisów ustawy mające wpływ lub mogące mieć istotny wpływ na wynik postępowania lub niezgodność projektowanego postanowienia umowy z wymaganiami wynikającymi z przepisów ustawy (art. 554 ust. 1 ustawy Pzp). Nie korzystają zatem z ochrony prawnej dążenia wykonawców ukierunkowane jedynie na ukształtowanie korzystniejszej dla siebie treści dokumentów zamówienia.

Następnie zauważyć należy, że wymagania dotyczące przedmiotu zamówienia zawsze stanowią pewne ograniczenie dla poszczególnych wykonawców, czy to powodujące konieczność podjęcia określonego wysiłku w celu przygotowania i skalkulowania oferty oraz zapewnienia prawidłowej realizacji zamówienia, czy nawet nieopłacalność lub niemożliwość złożenia oferty. Okoliczność, że określone warunki realizacji zamówienia nie są dla danego wykonawcy dogodne, nie świadczy o naruszeniu przepisów ustawy i nie może być utożsamiana z obiektywną niemożliwością złożenia oferty, wynikającą z wymagań bezpodstawnie blokujących dostęp do udziału w postępowaniu. Celem postępowania o udzielenie zamówienia nie jest bowiem zapewnienie możliwości realizacji zamówienia wszystkim podmiotom działającym na danym rynku, ale umożliwienie zamawiającemu nabycia świadczeń odpowiadających jego zapotrzebowaniu, bez jednoczesnego dyskryminowania podmiotów chcących te świadczenia zaoferować. O niedopuszczalnym ograniczeniu konkurencji można więc mówić dopiero w sytuacji, gdy wymagania zamawiającego nie mają uzasadnienia w jego obiektywnych potrzebach i nie służą zapewnieniu ich realizacji, a są ukierunkowane jedynie na uprzywilejowanie jednych wykonawców kosztem innych.

W zakresie zarzutu nr 1 Odwołujący ograniczył się w odwołaniu do twierdzenia, że Zamawiający w OPZ wskazał znak towarowy oraz nazwy handlowe (Infoblox BloxOne Threat Defense Essentials oraz Infoblox Security Ecosystem Business), mimo że mógł opisać przedmiot zamówienia w wystarczająco precyzyjny i zrozumiały sposób z pominięciem znaków towarowych, gdyż oprogramowanie zapewniające bezpieczeństwo przed zagrożeniami na bazie protokołu DNS jest typowym produktem branży IT, dla którego istnieją opisowe parametry funkcjonalne, pozwalające na sporządzenie jednoznacznego opisu bez używania nazw producentów. Odwołanie nie zawiera żadnego wywodu dotyczącego możliwości opisania przedmiotu zamówienia z pominięciem znaków towarowych w kontekście rozwiązania wykorzystywanego obecnie przez Zamawiającego i kwestii celowości całkowitej zmiany tego rozwiązania. Jak wskazał Zamawiający w odpowiedzi na odwołanie, nie tworzy on nowego systemu ochrony DNS, ale posiada już wdrożoną, zintegrowaną z infrastrukturą sieciową i produkcyjnie eksploatowaną platformę, dla której nabył subskrypcje ważne do października 2027 r. Okoliczność ta została uwzględniona w dokumentach zamówienia. Odwołujący natomiast w uzasadnieniu zarzutu nie odniósł się szerzej do tej okoliczności (ograniczając się do zaprzeczenia, że fakt posiadania aktualnie licencji Infoblox uzasadnia takie opisanie przedmiotu zamówienia), mimo że ma ona zasadnicze znaczenie dla oceny prawidłowości opisu przedmiotu zamówienia.

Zdaniem Izby ocena potrzeb Zamawiającego nie może abstrahować od okoliczności, w których działa, w tym wykorzystywanych systemów i narzędzi, ich dalszej przydatności i kwestii możliwości korzystania z nich bez potrzeby całkowitej wymiany i ponoszenia związanych z tym kosztów. Biorąc pod uwagę posiadany już przez Zamawiającego system, potrzeba rozszerzenia posiadanych uprawnień licencyjnych (subskrypcji) o dodatkowe jednostki licencyjne (tokeny) pozwalające objąć ochroną 44 000 urządzeń końcowych, jest obiektywnie uzasadniona i tak został określony

przedmiot zamówienia w wariancie podstawowym. Nie można bowiem wymagać od Zamawiającego, aby w oderwaniu od swoich potrzeb ponosił koszty i ryzyka wdrożenia drugiego, równoległego systemu innego producenta. Konieczność rozszerzenia konkurencji w postępowaniu nie może być rozumiana jako nakaz umożliwienia złożenia oferty jak najszerszej grupie wykonawców, bez uwzględnienia uzasadnionego interesu Zamawiającego.

Jak wskazał Zamawiający: *każdy taki system musi zostać objęty procesami korporacyjnymi stosowanymi w Poczcie Polskiej wobec nowych aplikacji i systemów: analizą dopuszczającą do użytkowania, okresowym szacowaniem ryzyka dla rozwiązania i ryzyka łańcucha dostaw, opracowaniem planu wyjścia z korzystania z aplikacji po zakończeniu jej cyklu życia oraz planu działań na wypadek zerwania współpracy z dostawcą, uwzględnieniem w scenariuszach Planu Ciągłości Działania, objęciem procesami zarządzania podatnościami i utrzymania w stanie wsparcia producenckiego. Do tego dochodzą koszty operacyjne (przeszkolenie personelu, integracja z pozostałymi systemami cyberbezpieczeństwa, modyfikacje procesów i procedur operacyjnych) oraz koszty infrastruktury sieciowo-serwerowej, na której niezależne rozwiązanie byłoby utrzymywane, a także konieczność utrzymywania dwóch platform do czasu wygaśnięcia posiadanych subskrypcji w październiku 2027 r.* W ocenie Izby uzasadnienie przedstawione przez Zamawiającego jest przekonujące i stanowi potwierdzenie jego usprawiedliwionych potrzeb.

Jednocześnie należy zgodzić się z Zamawiającym, że rozszerzenia uprawnień licencyjnych do konkretnego, posiadanego oprogramowania nie da się opisać w sposób wystarczająco precyzyjny i zrozumiały bez wskazania tego oprogramowania, biorąc pod uwagę, że jednostki licencyjne do platformy Infoblox rozszerzają zakres eksploatacji konkretnego, już wdrożonego oprogramowania. Jest to zatem okoliczność uzasadniająca – w świetle art. 99 ust. 5 ustawy Pzp – opisanie przedmiotu zamówienia przez wskazanie nazwy konkretnego systemu.

Odnosząc się do tezy Odwołującego, że ochrona przed zagrożeniami na bazie protokołu DNS może być zrealizowany przy zastosowaniu rozwiązań wielu producentów, wskazać należy, że okoliczność ta nie jest przedmiotem sporu. Istotą sporu jest to, czy Zamawiający był uprawniony do decyzji, aby w wariancie podstawowym nabyć przedmiot zamówienia uwzględniający wykorzystywane już rozwiązania, a alternatywnie dopuścić rozwiązania inne, wiążące się z koniecznością wdrożenia całkowicie nowego systemu. W ocenie Izby na tak postanowione pytanie należy udzielić odpowiedzi twierdzącej.

Za niezasadne należy również uznać zarzuty nr 2 i 3, dotyczące opisu rozwiązań równoważnych.

Zarzuty te zostały oparte na tezie, że jedynymi rozwiązaniami, które spełniają parametry równoważności sformułowane w rozdz. II f OPZ, są produkty firmy Infoblox, co sprawia, że parametry równoważności mają charakter pozorny. Wskazać należy, że formułując taki zarzut Odwołujący zobowiązany był udowodnić powyższą tezę. Twierdzenie Odwołującego pozostało jednak całkowicie gołosłowne. Jedynym dowodem przedstawionym przez niego w terminie określonym w art. 535 ust. 1 ustawy Pzp jest dokumentacja techniczna Infoblox z tłumaczeniami na język polski. Dowód ten dowodzi jednak tylko tego, że Infoblox posiada rozwiązania spełniające wymagania opisane w rozdz. II f OPZ, w żadnej mierze nie dowodzi jednak, że jest jedynym podmiotem, który te wymagania może spełnić. Odwołujący nie przedstawił analizy dostępnych na rynku rozwiązań ani dotyczącej ich dokumentacji, które przynajmniej uprawdopodobniłyby jego twierdzenia. Dowody na taką okoliczność Odwołujący przedstawił dopiero po pierwszym terminie posiedzenia z udziałem stron, zatem należało je uznać za objęte prekluzją dowodową. Poza nieudowodnioną tezą o spełnieniu wymagań równoważności wyłącznie przez rozwiązania Infoblox, Odwołujący sformułował w odwołaniu szereg wniosków o zmianę poszczególnych wymagań, wskazujących na próbę dostosowania wymaganych parametrów do rozwiązań, które może lub chce zaoferować.

Odwołanie ogranicza się więc do gołosłownej tezy, że parametry dla drugiego wariantu przedmiotu zamówienia spełnia tylko rozwiązanie referencyjne oraz do sformułowania wniosków dostosowujących opis przedmiotu zamówienia do możliwości Odwołującego. Już tylko ta okoliczność powoduje, że zarzuty odwołania należy uznać za niezasadne, bez szczegółowej analizy technicznej poszczególnych rozwiązań. Prowadzona w kolejnych pismach procesowych polemika między Odwołującym a Zamawiającym co do szczegółowych aspektów technicznych jest bowiem bezprzedmiotowa wobec niewykazania zasadniczej przesłanki warunkującej uznanie opisu przedmiotu zamówienia za niezgodny z ustawą.

W tej sytuacji dodatkowo jedynie wskazać należy, że Zamawiający jest uprawniony do takiego opisania parametrów równoważności, które zapewnią zaspokojenie jego uzasadnionych potrzeb. Nawet jeśli opis ten zawęża krąg wykonawców mogących złożyć ofertę, to o ile służy on realizacji tych potrzeb, nie może być uznany za niezgodny z przepisami ustawy. Zamawiający wyjaśnił w postępowaniu odwoławczym, czym podyktowane są poszczególne wymagania, wskazując m.in.:

–rozdz. II f pkt 1.2.4 OPZ; poz. 1 i 2 tabeli

Zamawiający stosuje architekturę DNS typu split-horizon, w której hosty korzystające z wewnętrznej infrastruktury

DNS otrzymują na zapytania o strefy Zamawiającego odpowiedzi odmienne od udostępnianych publicznie. Aby użytkownicy chronieni przez System zachowali dostęp do wewnętrznych stref DNS (por. rozdz. II f pkt 2.5 OPZ), a jednocześnie zapytania o domeny zewnętrzne podlegały ochronie, w sieci wewnętrznej musi działać komponent przekazujący zapytania: o domeny wewnętrzne do wskazanych serwerów DNS Zamawiającego, a o pozostałe do Usługi, z zachowaniem informacji o wewnętrznym adresie IP źródła (niezbędnej do przypisania zdarzenia do urządzenia) oraz z szyfrowaniem transmisji.

Komponent taki jest, jak wynika z samego załącznika nr 1 do Odwołania, rekurencyjnym serwerem DNS skonfigurowanym do przekazywania zapytań, a więc elementem opisanym przez funkcję, którą realizuje, a nie przez cechy właściwe jednemu producentowi; wraz z korzystającymi z niego agentami zapewnia on użytkownikom Systemu dostęp do wewnętrznych stref DNS Zamawiającego oraz zachowanie informacji o wewnętrznym adresie źródłowym zapytania. Wymóg został sformułowany funkcjonalnie: możliwość uruchomienia jako maszyna wirtualna na trzech powszechnie stosowanych platformach wirtualizacji, dodawanie informacji o adresie źródłowym, szyfrowanie DoT lub DoH oraz prawo instalacji dowolnej liczby instancji. (…)

–rozdz. II f pkt 1.2.5 OPZ; poz. 3 tabeli

Po pierwsze, ochrona DNS musi być wymuszona w scenariuszach pracy zdalnej oraz dostępu do zasobów Zamawiającego z urządzeń prywatnych pracowników (BYOD), nad których konfiguracją systemową Zamawiający nie ma kontroli. Bez agenta użytkownik może zmienić resolver w konfiguracji systemu, przez co ochrona staje się opcjonalna, co jest sprzeczne z Polityką Bezpieczeństwa Informacji Zamawiającego. Po drugie, agent dostarcza atrybuty (nazwa komputera, adres MAC, nazwa użytkownika, wersja systemu operacyjnego) pozwalające przypisać zdarzenie bezpieczeństwa do użytkownika i urządzenia niezależnie od tego, czy urządzenie jest w danej chwili uwierzytelnione w sieci korporacyjnej i czy jego tożsamość pochodzi z usług katalogowych Zamawiającego. Po trzecie, agent umożliwia realizację architektury splithorizon na urządzeniach mobilnych i pracujących poza siecią wewnętrzną (kierowanie zapytań o domeny wewnętrzne do wewnętrznego DNS, a pozostałych do Usługi). Po czwarte, rezygnacja z agenta oznaczałaby konieczność zmiany konfiguracji DNS na około 30 000 zróżnicowanych urządzeń i systemów, co jest nieproporcjonalnie kosztowne i nietrwałe. (…)

–rozdz. II f pkt 9.2 i 9.3 OPZ; poz. 14 tabeli

Przyjęcie tej propozycji oznaczałoby brak możliwości przypisania zdarzeń do użytkowników, którzy w chwili zdarzenia nie są podłączeni i uwierzytelnieni w sieci korporacyjnej, oraz do użytkowników, których tożsamość nie pochodzi z usług katalogowych Zamawiającego (BYOD), a także zwiększenie nakładu pracy analityków w związku z koniecznością ręcznej korelacji danych z wielu źródeł. Celem wymagania jest uniezależnienie ustalania tożsamości od innych systemów i narzędzi. Jest to wymaganie dotyczące efektu, a nie sposobu jego realizacji ii pozostaje w bezpośrednim związku z wymogiem agenta (pkt D.2).

–rozdz. II f pkt 15 OPZ; poz. 20 tabeli

OPZ określa parametry wymiarowania przez wskaźniki chronionego środowiska: minimalną liczbę chronionych urządzeń (44 000), minimalny wolumen zdarzeń przesyłanych do SIEM (330 000 000 miesięcznie), a dla rozwiązań licencjonowanych według liczby użytkowników liczbę pracowników (50 000) i serwerów (2 000). Sam Odwołujący przyznaje w tabeli, że „podana skala jest uzasadniona". Zarzut sprowadza się zatem do żądania, aby Zamawiający przedstawił dodatkowo „jeden spójny harmonogram wymiarowania" obejmujący liczbę jednoczesnych połączeń, szczytową liczbę zapytań na sekundę, lokalizacje, nadmiarowość i prognozowany wzrost. Zamawiający, jako organizacja podlegająca dynamicznej transformacji technologicznej, nie dysponuje wiarygodną prognozą szczytowego ruchu DNS na okres trzech lat i nie ma obowiązku jej tworzenia; (…)

Polemika Odwołującego z powyższym uzasadnieniem, bez uprawdopodobnienia, że którekolwiek z tych wymagań jest niemożliwe do spełnienia przez rozwiązania innych producentów, w tym rozwiązania oferowane przez niego, nie może stanowić podstawy uwzględnienia zarzutów i nakazania Zamawiającemu zmiany OPZ, z narażeniem go na konieczność nabycia rozwiązań nieodpowiadających jego potrzebom.

Wobec powyższego orzeczono, jak w sentencji.

O kosztach postępowania orzeczono na podstawie art. 557, art. 574 i art. 575 ustawy Pzp oraz § 5 pkt 1 oraz § 8 ust. 2 , stosownie do wyniku postępowania obciążając kosztami Odwołującego.

Przewodnicząca:……