Sygn. akt: KIO 2493/21

WYROK

z dnia 28 września 2021 r.

Krajowa Izba Odwoławcza - w składzie:

Przewodniczący: Ryszard Tetzlaff

Protokolant: Adam Skowroński

po rozpoznaniu na rozprawie w dniu **23 września 2021 r. w Warszawie** odwołania wniesionego do Prezesa Krajowej Izby Odwoławczej w **23 sierpnia 2021 r.** przez wykonawcę **COMTEGRA S.A., ul. Puławska 474, 02-884 Warszawa** w postępowaniu prowadzonym przez **Skarb Państwa - Państwowe Gospodarstwo Leśne Lasy Państwowe, Zakład Informatyki Lasów Państwowych im. Stanisława Kostki Wisińskiego Sękocin Stary, ul. Leśników 21C, 05-090 Raszyn**

przy udziale wykonawcy **Trafford IT Sp. z o.o. Sp. k., ul. Taneczna 18, 02-829 Warszawa** zgłaszającego swoje przystąpienie do postępowania odwoławczego po stronie zamawiającego

orzeka:

1. **umarza postępowanie w zakresie zarzutów dotyczących:**

a) naruszenia art. 18 ust. 1, 2 i 3 Ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2021 r. poz. 1129) w związku z art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2019 r. poz. 1010 i 1649) poprzez pozbawione podstaw faktycznych i prawnych zaniechanie uznania za bezskuteczne zastrzeżenia jako tajemnicy przedsiębiorstwa treści złożonego przez Trafford Załącznika - „Opis techniczny oferowanego rozwiązania", z uwagi na jego uwzględnienie i brak sprzeciwu,

b) naruszenia art. 226 ust.1 pkt 5 w zw. z art. 16 pkt 1 Ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2021 r. poz. 1129) poprzez zaniechanie odrzucenia oferty Trafford IT Sp. z o.o. Sp. k., pomimo, że zaoferowane w postępowaniu przez tego wykonawcę rozwiązanie nie spełnia wymagań Zamawiającego zawartych w treści Specyfikacji Warunków Zamówienia w zakresie zarzutów szczegółowych - numer: 3. Rozwiązanie nie pozwala na rozkład ruchu opisany w OPZ; 5. Parametrów odrzucenia, 6. 7.2 AV; 7. Braku licencji; 10. Licencji; 11. Skanowania Linuxa oraz 12. Skanowania plików typów, z uwagi na ich wycofanie.

2. **W pozostałym zakresie oddala odwołanie.**

3. kosztami postępowania obciąża **COMTEGRA S.A., ul. Puławska 474, 02-884 Warszawa** i:

   3.1. zalicza w poczet kosztów postępowania odwoławczego kwotę **15 000 zł 00 gr** (słownie: piętnaście tysięcy złotych zero groszy) uiszczoną przez wykonawcę **COMTEGRA S.A., ul. Puławska 474, 02-884 Warszawa** tytułem wpisu od odwołania;

   3.2. zasądza od wykonawcy **COMTEGRA S.A., ul. Puławska 474, 02-884 Warszawa** na rzecz **Trafford IT Sp. z o.o. Sp. k., ul. Taneczna 18, 02-829 Warszawa** kwotę **3 600 zł 00 gr** (słownie: trzy tysiące sześćset złotych zero groszy) stanowiącą koszty postępowania odwoławczego poniesione z tytułu wydatków pełnomocnika.

Stosownie do art. 579 ust. 1 oraz art. 580 ust.1 i 2 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 2019 z późn. zm.) 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:

……

Sygn. akt: KIO 2493/21

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

Postępowanie o udzielenie zamówienia publicznego na: *„Zakup systemu ochrony antyspamowej i antywirusowej poczty LP - postępowanie po unieważnieniu postępowania DZ.270.29.2020”*, Znak sprawy: DZ.270.119.2020 zostało wszczęte ogłoszeniem w ogłoszeniem opublikowanym w Dzienniku Urzędowym Unii Europejskiej w dniu 18.06.2021 r. pod nr 2021/S 117-110582 przez: Skarb Państwa - Państwowe Gospodarstwo Leśne Lasy Państwowe, Zakład Informatyki Lasów Państwowych im. Stanisława Kostki Wisińskiego Sękocin Stary, ul. Leśników 21C, 05-090 Raszyn dalej: *„Zamawiającym”*. Do ww. postępowania o udzielenie zamówienia zastosowanie znajdują przepisy ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (t. j. Dz. U. z 2019 r., poz. 2019 ze. zm., zwana dalej: *„NPzp” albo „ustawy Pzp” albo „Pzp”*.

Dnia 11.08.2021 r. (e-mailem) Zamawiający poinformował o wyborze oferty najkorzystniejszej: Trafford IT Sp. z o.o. Sp. k., ul. Taneczna 18, 02-829 Warszawa zwanej dalej: *„Trafford IT Sp. z o.o. Sp. k.”* albo *„Trafford”* albo *„Przystępującym”.* Drugą pozycje w rankingu złożonych ofert zajęła firma: COMTEGRA S.A., ul. Puławska 474, 02-884 Warszawa zwana dalej: *„COMTEGRA S.A.”* albo *„Odwołującym”*.

W dniu 23.08.2021 r. (wpływ do Prezesa KIO w wersji elektronicznej podpisane podpisem cyfrowym za pośrednictwem elektronicznej skrzynki podawczej - ePUAP) COMTEGRA S.A. wniosła odwołanie na czynności z 11.08.2021 r. Kopie odwołania Zamawiający otrzymał w dniu 23.08.2021 r. (e-mailem).

Zaskarżonym czynnościom zarzucił naruszenie następujących przepisów Pzp:

1) art. 226 ust.1 pkt 5 w zw. z art. 16 pkt 1 Pzp poprzez zaniechanie odrzucenia oferty wykonawcy Trafford, pomimo, że zaoferowane w postępowaniu przez tego wykonawcę rozwiązanie nie spełnia wymagań Zamawiającego zawartych w treści Specyfikacji Warunków Zamówienia zwanej dalej: *„SWZ”*,

2) art. 18 ust. 1, 2, i 3 Pzp w zw. z art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2019 r. poz. 1010 i 1649), poprzez pozbawione podstaw faktycznych i prawnych zaniechanie uznania za bezskuteczne zastrzeżenia jako tajemnicy przedsiębiorstwa treści złożonego przez Trafford Załącznika - „Opis techniczny oferowanego rozwiązania”,

co skutkuje naruszeniem art. 239 ust.1 Pzp w zw. z art. 16 pkt 1 Pzp poprzez wadliwy wybór oferty najkorzystniejszej w postępowaniu. W oparciu o przedstawione wyżej zarzuty na podstawie art. 554 ust. 1 i 3 Pzp wnosił o:

• merytoryczne rozpatrzenie oraz uwzględnienie niniejszego odwołania,

• dopuszczenie i przeprowadzenie dowodu z dokumentacji postępowania - na okoliczności wskazane niniejszym odwołaniem, a także o:

1. unieważnienie czynności wyboru oferty najkorzystniejszej jako obarczonej wadą mającą wpływ na wynik postępowania,

2. powtórzenie czynności oceny ofert w postępowaniu przy odrzuceniu oferty wykonawcy Trafford

3. udostępnienie nieskutecznie zastrzeżonego Załącznika „Opis techniczny oferowanego rozwiązania”,

co powoduje bezpośredni wpływ na wybór oferty najkorzystniejszej w postępowaniu.

Przedmiot zamówienia obejmuje zakup i wdrożenie w Państwowym Gospodarstwie Leśnym Lasy Państwowe centralnego systemu ochrony środowiska pocztowego MS Exchange wraz z niezbędną infrastrukturą sprzętową. Zakres przedmiotu zamówienia obejmuje w szczególności dostawę kompletnego rozwiązania tj. licencji na oprogramowanie, sprzętu wymaganego do sprawnego funkcjonowania systemu, pełnego serwisu producenta dla dostarczonego sprzętu i oprogramowania, dostępu do aktualizacji sygnatur i list reputacji przez okres 36 miesięcy (część obligatoryjna zamówienia).

Część obligatoryjna zamówienia obejmuje:

a) Prace organizacyjne i analityczne,

b) Opracowanie projektu technicznego środowiska wdrożenia Rozwiązania,

c) Dostawa Rozwiązania w części obejmującej sprzęt i licencje,

d) Wdrożenie Rozwiązania,

e) Opracowanie dokumentacji powdrożeniowej,

f) Przeprowadzenie warsztatów i szkoleń z zakresu Systemu,

g) Zapewnienie wsparcia producenta dla wdrożonego Systemu,

h) Zapewnienie wsparcia Wykonawcy dla wdrożonego Systemu,

i) Udzielenie gwarancji na System

Szczegółowy opis przedmiotu zamówienia, opis wymagań zamawiającego w zakresie realizacji i odbioru określają:

1.4.1. opis przedmiotu zamówienia – Załącznik nr 1 do SWZ,

1.4.2. projektowane postanowienia umowy– Załącznik nr 8 do SWZ.

Zgodnie z SWZ - wszystkie wymagania określone w dokumentach wskazanych powyżej stanowią wymagania minimalne, a ich spełnienie jest obligatoryjne. Niespełnienie

ww. wymagań minimalnych będzie skutkować odrzuceniem oferty jako niezgodnej z warunkami zamówienia na podstawie art. 226 ust. 1 pkt 5 ustawy Pzp

Treść oferty w postępowaniu.

Zamawiający wymagał od wykonawców złożenia jako oferty wypełnionego Załącznika nr 2 – Wzór Formularza oferty. Dokument zawiera m.in. wymaganie odnoszące się do konieczności identyfikacji co do tożsamości oferowanego rozwiązania. Zgodnie z SWZ Zamawiający wymagał podania m.in. następujących informacji:

1. Ochrona przed niechcianą pocztą (spam), próbami oszustw i wyłudzeń (phising) oraz złośliwym oprogramowaniem (malware) będzie realizowana poprzez rozwiązanie (należy podać nazwę rozwiązania i krótki opis potwierdzający spełnienie wymagań OPZ):

2. Funkcje ochronne jako druga warstwa bezpieczeństwa. Główną rolą drugiego systemu jest realizowanie dodatkowej ochrony przed złośliwym programowaniem w oparciu o tradycyjne bazy sygnatur jak i również poprzez uruchamianie podejrzanego kodu w izolowanych środowiskach wirtualnych (sandbox) będą realizowana poprzez rozwiązanie (należy podać nazwę rozwiązania i krótki opis potwierdzający spełnienie wymagań OPZ):

Zamawiający nie wymagał złożenia w postępowaniu w powyższym zakresie żadnych dodatkowych oświadczeń ani dokumentów w tym w szczególności przedmiotowych środków dowodowych. Dane zawarte w treści Formularza ofertowego jako jedyne wymagane, identyfikowały przedmiot świadczenia w odniesieniu do zaoferowanego przez wykonawcę rozwiązania. Uwzględniając charakter informacji jako stanowiących ofertę sensu stricte nie istnieje możliwość uzupełnienia ani też zmiany przedmiotu świadczenia wykonawcy w trybie art. 128 Pzp, który nie dotyczy treści oferty. Zatem wykazanie przez Odwołującego, że zaoferowane zidentyfikowane w ofercie w sposób jednoznaczny rozwiązanie nie spełnia wymagań Zamawiającego obliguje do odrzucenia oferty w trybie art. 226 ust.1 pkt 5 Pzp.

Wykonawca Trafford w złożonej ofercie zaoferował następujące rozwiązanie:

„1. Ochrona przed niechcianą pocztą (spam), próbami oszustw i wyłudzeń (phising) oraz złośliwym oprogramowaniem (malware) będzie realizowana poprzez rozwiązanie (należy podać nazwę rozwiązania i krótki opis potwierdzający spełnienie wymagań OPZ):

Producent: Forcepoint

Rozwiązanie: Forcepoint Email Security

Opis: Virus and malware Blocking, Spam Filtering, Content filtering, Email Archiving, DLP,– Virtual dla 27 000 użytkowników wraz z 36 miesięcznym wsparciem Producenta.

Opis oferowanego Rozwiązania, zawarty jest w dokumencie pt. „Opis techniczny oferowanego rozwiązania”.

2. Funkcje ochronne jako druga warstwa bezpieczeństwa. Główną rolą drugiego systemu jest realizowanie dodatkowej ochrony przed złośliwym programowaniem w oparciu o tradycyjne

bazy sygnatur jak i również poprzez uruchamianie podejrzanego kodu w izolowanych środowiskach wirtualnych (sandbox) będą realizowana poprzez rozwiązanie (należy podać nazwę rozwiązania i krótki opis potwierdzający spełnienie wymagań OPZ):
Producent: FireEye
Rozwiązanie: FireEye EX (ochrona maila) i CM (centralne zarządzanie)
Opis: Central Management 2500 Virtual Appliance (2 szt.), Security Equipment 3500EX-HW EMAIL MPS (6 szt.), DTI 3500 EX 2-way sub-3 Year (6 szt.) , Attach/URL engine-49999-3 Year (dla 27 000 użytkowników) wraz z 36 miesięcznym wsparciem Producenta Opis oferowanego Rozwiązania, zawarty jest w dokumencie pt. „Opis techniczny oferowanego rozwiązania”.”

Treść oferty zawiera identyfikację zaoferowanych rozwiązań w sposób umożliwiający ich weryfikację i ocenę pod kątem spełniania wymagań SWZ.

Wykonawca Trafford wraz z ofertą złożył dodatkowo niewymagany załącznik zatytułowany jako „Opis techniczny oferowanego rozwiązania” jednak jego treść nie może pozostawać w niezgodności z danymi identyfikującymi przedmiot oferty zawartymi w wymaganym Formularzu ofertowym. Niezgodność zaoferowanego przez Trafford rozwiązania z wymaganiami Zamawiającego. Wobec faktu, że Formularz ofertowy identyfikuje co do tożsamości zaoferowane przez Trafford w postępowaniu rozwiązanie możliwa była weryfikacja zaoferowanego rozwiązania pod kątem jego zgodności z wymaganiami Zamawiającego zawartymi w OPZ SWZ. Zaoferowane rozwiązanie posiada publicznie dostępną oraz pełną i szczegółową oficjalną dokumentację techniczną produktów bezpośrednio od producenta, co powoduje, że weryfikacja zgodności rozwiązania z SWZ jest możliwa. Odnosząc się do poszczególnych stwierdzonych przez Odwołującego i udokumentowanych niezgodności zaoferowanego przez Trafford rozwiązania z wymaganiami SWZ:

1. Brak skanowania exchange

W OPZ w części wymagania ogólne do systemu Zamawiający specyfikuje funkcjonalność:
„2.6 rozwiązanie musi zapewniać filtrowanie poczty przychodzącej i wychodzącej (w tym poczty wewnętrznej), przy czym musi istnieć możliwość przypisana odrębnych polityk dla każdego z kierunków przesyłania poczty elektronicznej” oraz w punkcie 3 tej samej specyfikacji” Rozwiązanie musi pracować jako gateway dla poczty elektronicznej (jako MTA - Mail Transfer Agent). Dla ochrony poczty wewnętrznej (internal), której ruch nie przechodzi przez gateway a zamyka się wewnątrz farmy serwerów pocztowych, wymagane jest zastosowanie mechanizmu chroniącego pocztę bezpośrednio na serwerach Exchange.”.

Dodatkowo w odpowiedziach na pytania do SWZ z dnia 14 lipca 2021 r. Zamawiający podtrzymuje swoje wymaganie odnośnie skanowania poczty wewnętrznej:
Pytanie nr 1: „Czy Zamawiający pisząc o filtrowaniu poczty wewnętrznej wymaga rozwiązania pozwalającego na filtrowanie pod kątem szkodliwej treści, spamu dla wiadomości nie opuszczających serwerów Exchange?

Wyjaśnienia Zamawiającego: Zamawiający potwierdza, że wymaga rozwiązania pozwalającego na filtrowanie pod kątem szkodliwej treści, spamu dla wiadomości nie opuszczających serwerów Exchange."

Analogicznie pytanie nr 33:
„Rozwiązania bazujące na bezpośredniej ochronie serwerów Exchange są często elementem bardzo obciążającym farmę serwerów. Ponadto, ich funkcjonalność najczęściej ogranicza się do klasy standardowego antywirusa i nie wspiera zaawansowanej analizy bezpieczeństwa jak na przykład sandbox, dodatkowa analiza URL czy antyphising. Czy Zamawiający akceptuje rozwiązanie zewnętrzne, które nie wymaga instalacji na serwerach Exchange, a tylko odpowiedniej konfiguracji i analizuje pocztę wewnętrzną z wykorzystaniem wszystkich narzędzi bezpieczeństwa używanych do analizy poczty przychodzącej?

Wyjaśnienia Zamawiającego:

Zamawiający podtrzymuje zapisy SWZ. W punkcie II.3 OPZ opisał swoje wymagania odnośnie środowiska nie wskazując sposób jego implementacji. Rozwiązanie do ochrony poczty wewnętrznej, nie może zmieniać wewnętrznego routingu przy przepływie poczty wewnętrznej."

Rozwiązanie zaproponowane przez Trafford nie posiada funkcji skanowania bezpośrednio na serwerach Exchange, w wymaganym przez Zamawiającego zakresie, czyli:
„2.1 ochronę przed szkodliwą treścią (m.in. malware, wirusy etc.)
2.2 ochronę przed spamem
2.3 filtrowanie treści przesyłanej w poczcie elektronicznej (w tym załączniki)
2.4 ochronę przez niebezpiecznymi linkami URL w treści wiadomości
2.5 rozwiązanie musi umożliwiać kontrolę protokołu SMTP w tym szyfrowane wersje tego protokołu: SSL i TLS."

Rozwiązanie zaproponowane przez Trafford jest rozwiązaniem sieciowym, pozwalającym na wyeksportowanie z serwerów exchange treści do skanowania, przez co proces skanowania nie odbywa się na serwerach Exchange. Dodatkowo zaproponowane rozwiązanie nie wykonuje skanowania, co najmniej w zakresie wskazanym w punktach: 2.2 oraz 2.3. Powyższe oznacza niezgodność treści oferty z jednoznacznymi wymaganiami Zamawiającego zawartymi w SWZ.

2. Rozwiązanie nie posiada wyszukiwania po zdefiniowanych parametrach

Zamawiający w punkcie 4 OPZ wskazał jakie parametry powinny być logowane oraz po jakich parametrach powinno być możliwe wyszukiwanie wiadomości. Zgodne z SWZ:
„4.1 rozwiązanie powinno pozwalać na przeszukiwanie wiadomości email z wykorzystaniem parametrów minimum:
4.1.1 Nadawca
4.1.2 Odbiorca
4.1.3 Temat
4.1.4 Czas dostarczenia
4.1.5 Nazwa serwera
4.1.6 IP nadawcy
4.1.7 Załącznik
4.1.8 Nagłówek Message-ID
4.1.9 Sumie kontrolnej załącznika (min. MD5 i SHA256)”
przy czym w odpowiedziach na pytania doprecyzował, że wyszukiwanie po sumie kontrolnej załącznika może odbywać się jednocześnie po jednej z wymienionych funkcji skrótu.

Producent oprogramowania zaoferowanego przez Trafford, w dokumentacji: Forcepoint Email Security dla wersji 8.5.x z dnia 1 lipca 2021 r., dostępnej pod adresem: https://www.websense.com/content/support/library/email/v85/email_help/email_help.pdf (dalej jako: „Forcepoint – dokumentacja”) w sekcji „viewing and searching logs” na stronie 32, 33 i 34 (z ang. Przeglądanie i przeszukiwanie logów) podaje listę parametrów wyszukiwania ograniczoną do: Received Date/Time, Subject, Sender Address, Sender IP, Recipient Address, Analysis Result, Message Status, To:Header, From: Header, Spam Score, Message Size (KB), Appliance (z ang. Czas i data otrzymania, Temat, Aders Nadawcy, IP Nadawcy, Adres Odbiorcy, Wynik Analizy, Status Wiadomości, Nagłówek Do, Nagłowek Od, Wynik Spam, Wielkość Wiadomości, Urządzenia. Powyższe potwierdza, że zaoferowane rozwiązanie nie posiada możliwości określonych w OPZ dla następujących parametrów: Załącznik, Nagłówek Message-ID oraz Sumie kontrolnej załącznika.

3. Rozwiązanie nie pozwala na rozkład ruchu opisany w OPZ

Zamawiający opisał w SWZ dopuszczalne mechanizmy wysokiej dostępności i ograniczył je do: *„12.1 Redundancja każdego elementu systemu w obu centrach przetwarzania Lasów Państwowych (activeactive z rozkładem obciążenia. Rozkład obciążenia może być realizowany z wykorzystaniem konfiguracji DNS i rekordów MX).*
12.2 Zastosowanie konfiguracji mieszanej z wykorzystaniem mechanizmów wirtualizatora i mechanizmów układu Active-Pasive oraz mechanizmów w układzie failover
12.3 Zastosowanie konfiguracji Active-Passive, z synchronizacją danych na poziomie klastrów/węzłów.”

Rozwiązanie zaproponowane przez Trafford bazuje na dostarczeniu dwóch rozwiązań, które pracują w konfiguracji MTA, czyli są agentami przyjmującymi wiadomości, wykonującymi zdefiniowane funkcje ochrony i przesyłającymi wiadomości dalej. Rozwiązania te pracują liniowo. Poniżej w odwołaniu przedstawiono rysunek przedstawiający niniejsze rozwiązanie.

W związku z specyfiką oparcia rozwiązania o 2 niezależne mechanizmy skanujące, rozkład obciążenia dla mechanizmu 2 nie może być realizowany w oparciu o DNS i rekordy MX. Rekordy MX (Mail Exchange) są to rekordy DNS (Domain Name System), których zadaniem jest mapowanie nazwy domeny na nazwę serwera poczty oraz jego priorytet. Ponieważ drugi z mechanizmów nie jest wystawiony bezpośrednio do sieci Internet to nie ma możliwości realizacji rozkładu obciążenia w oparciu o wymagany mechanizm.
https://pl.wikipedia.org/wiki/Domain_Name_System

Dodatkowo, Zamawiający wymaga skanowania dla Exchange, które powinno odbywać się na serwerach. Nie ma więc możliwości, aby działający serwer Exchange nie był chroniony przez mechanizm uruchomiony na tym serwerze. Natomiast rozwiązanie proponowane przez Trafford, z wyniesionym mechanizmem skanowania Exchange nie posiada mechanizmów równoważenia obciążenia z racji błędnie zaproponowanej architektury systemu, co skutkuje podstawą odrzucenia oferty wobec niezgodności z SWZ.

4. Kwarantanna centralna.

Zamawiający w pkt. 30.6 OPZ wyspecyfikował swoje wymaganie wskazując że „Kwarantanna oraz oznaczanie spamu. Kwarantanna znajduje się na serwerze zarządzającym (brak potrzeby instalacji dodatkowego serwera kwarantanny).” Zaoferowane przez Trafford IT rozwiązanie składa się z dwóch niezależnych mechanizmów skanowania pracujących jako MTA (Mail Transfer Agent) co w konsekwencji powoduje, że to każde z nich posiada własną kwarantannę. W związku z czym rozwiązanie nie posiada centralnej kwarantanny co jest niezgodne z SWZ. Forcepoint – dokumentacja str. 38.

5. Parametry odrzucenia.
Zamawiający w OPZ w pkt. 37 wskazuje: „37 Rozwiązanie musi umożliwiać:
37.1 monitorowanie i ograniczanie ilości połączeń z jednego adresu IP w określonym przedziale czasu.
37.2 musi zapewniać opcję ograniczenia jednoczesnych aktywnych połączeń
37.3 musi zapewniać opcję ograniczenia maksymalnej ilości połączeń i wiadomości.
37.4 ograniczanie maksymalnej liczby wiadomości przekazywanych za pomocą pojedynczego połączenia SMTP”. Rozwiązanie zaoferowane przez Trafford nie pozwala na zdefiniowanie ograniczenia połączeń i filtrowania połączeń po wskazanych parametrach. Oficjalna i publicznie dostępna oraz aktualna dokumentacja zaoferowanego rozwiązania

wskazuje możliwe parametry i są one ograniczone do: „Liczba wiadomości na połączenie SMTP (s109), Maksymalna liczba wiadomości (109), Liczba jednoczesnych połączeń na IP (112). Jak widać lista jest znacząco mniejsza niż wymagana, co więcej o ile możliwe jest monitorowanie liczby jednoczesnych połączeń z IP to nie ma możliwości ograniczenia połączeń IP z pojedynczego IP w jednostce czasu.

6. 7.2 AV. W OPZ w pkt. 42 Zamawiający wymaga: „Rozwiązanie musi mieć możliwość wyboru z co najmniej dwóch komercyjnych silników antywirusowych (na jednej platformie sprzętowej) lub za pomocą dodatkowego urządzenia". Żadne z rozwiązań oferowanych przez Trafford nie pozwala na wybór z dwóch komercyjnych rozwiązań. Każde z rozwiązań posiada własny silnik antywirusowy, natomiast wymaganie mówi o możliwości wyboru, co za tym idzie takiej możliwości nie ma. Forcepoint – dokumentacja str. 167 i 168.

7. Brak licencji. W OPZ w pkt. 59 Zamawiający wymaga: „Rozwiązanie musi umożliwiać opcjonalnie, oddzielnie licencjonowane, szyfrowanie symetryczne poczty dla wybranych wiadomości, wykonywane bez potrzeby jakiejkolwiek ingerencji w klienta pocztowego oraz bez potrzeby implementacji PKI." Rozwiązanie zaproponowane przez Trafford nie daje możliwości użycia dodatkowej licencji, funkcja nie występuje w żadnym z rozwiązań.

8. Sandboxing załączników jako funkcja bramki pocztowej.

W pkt. 81 OPZ Zamawiający wymaga, aby: „Funkcja sandboxingu dla plików przesyłanych pocztą elektroniczną musi być wbudowana w system ochrony poczty, nie jest dopuszczalne stosowanie zewnętrznych systemów firm trzecich. Dopuszcza się rozwiązanie w postaci dedykowanego urządzenia zintegrowanego z systemem poczty elektronicznej." Rozwiązanie zaproponowane przez Trafford składa się z dwóch osobnych systemów pracujących w trybie MTA, co oznacza że cała komunikacja mailowa jest przekazywana szeregowo z jednego urządzenia do drugiego. Zamawiający natomiast wymaga, aby pliki przesyłane pocztą elektroniczną w postaci załączników były skanowane przez mechanizm wbudowany w system ochrony poczty, czyli załączniki mają być skanowane przez system bez stosowania zewnętrznych systemów firm trzecich. Należy to rozumieć jako zastosowanie wbudowanych w rozwiązanie mechanizmów, które umożliwiają poddanie załączników analizie. Co więcej, w odpowiedziach z dnia 14 lipca 2021 Zamawiający dwukrotnie odpowiedział na pytania wskazując, że nie wymaga aby technologia całego systemu pochodziła od dwóch dostawców, natomiast zastrzegł że podtrzymuje wymagania zawarte w SWZ.

Pytanie 2. Czy Zamawiający wymaga aby całość rozwiązania pochodziła od jednego producenta?

Wyjaśnienia Zamawiającego: Zamawiający nie wymaga aby całość rozwiązania pochodziła od jednego producenta. Dostarczone rozwiązanie musi obejmować swoim zakresem całość zdefiniowanych przez zamawiającego wymagań o których mowa w Załączniku nr 1 do SWZ – OPZ.

Pytanie 48. W przypadku konieczności ochrony poczty, w topologii wskazanej przez Zamawiającego, z reguły stosuje się system złożony z rozwiązań różnych producentów. Taka topologia jednocześnie podnosi poziom ochrony systemu pocztowego. W związku z powyższym, prosimy o wykreślenie wymagania na dostarczenie mechanizmu chroniącego pocztę bezpośrednio na serwerach Exchange lub dopuszczenie rozwiązania, w którym ochrona poczty na bramie MTA realizowana jest przez system jednego producenta, natomiast mechanizm chroniący pocztę bezpośrednio na serwerach Exchange przez system drugiego producenta. Spełnienie całości powyższego wymagania, tak jak jest teraz opisane, przez rozwiązanie jednego producenta, znacząco ogranicza konkurencję. Ewentualnie, czy Zamawiający uzna jako spełniające wymagania rozwiązanie, w którym cała poczta, w tym także wewnętrzna, przechodzi przez Gateway

Wyjaśnienia Zamawiającego: Zamawiający oczekuje dostawy i wdrożenia kompletnego Rozwiązania spełniającego wymagania zawarte w OPZ i SWZ. Nie stawia wymogów odnośnie konieczności dostawy Rozwiązania od dwóch różnych producentów.

9. Użycie chmury.

Zamawiający wielokrotnie w SWZ i OPZ zaznacza, że nie pozwala na transfer informacji dotyczących plików, załączników wiadomości, funkcji skrótu ani innych metadanych do serwerów producenta zlokalizowanych z chmurze obliczeniowej. Natomiast zaoferowane rozwiązanie przez Trafford ma zdefiniowane w dokumentacji, że z zasobów chmurowych korzysta. Pytanie 14. Czy funkcja sandboxingu może być wykonywana na serwerach producenta (w chmurze)? Wyjaśnienia Zamawiającego: Zamawiający nie dopuszcza aby jakiekolwiek dane ze środowiska Zamawiającego opuszczały lokalizacje Zamawiającego.

Pytanie 35. Czy Zamawiający dopuszcza rozwiązania typu sandbox działające w chmurze, czy też wyłącznie rozwiązania działające on-premise (instalowane lokalnie w infrastrukturze Zamawiającego i nie przesyłające żadnych danych do chmury)?

Wyjaśnienia Zamawiającego: Zamawiający dopuszcza jedynie rozwiązanie działające on-premise (instalowane lokalnie w infrastrukturze Zamawiającego i nie przesyłające żadnych danych do chmury). Natomiast głęboka analiza URLi, wymagana przez zamawiającego w OPZ w punktach 98 do 102 jest wykonywana w zaoferowanym przez Trafford rozwiązaniu w chmurze producenta Fireeye. Powyższe znajduje bezpośrednie potwierdzenie

w dokumentacji producenta: https://learn.fireeye.com/tips-and-insights/enabling-fireeyes-advanced-url-defense-feature/

„Hi I'm J. C. . I'm a Channel Engineer here at FireEye. In this video I'd like to share a tip on how to enhance your security operations by enabling FireEye's advanced URL defense feature to increase the ability to find evil with FireEye's email security. (…)

If email security is being managed by configuration management appliance then you should enable it from the configuration manager. From the menu at the top select settings. Then from the left hand column select advanced URL defense. Check the box to enable advanced URL defense. Then select apply.

Now when FireEye's Email Security identifies the suspicious URL it redirects the URL to our dynamic threat intelligence CLOUD for complete analysis." Tłum.

„*Cześć, jestem J. C. . Jestem inżynierem kanału w FireEye. W tym filmie chciałbym podzielić się wskazówką, jak ulepszyć operacje związane z bezpieczeństwem, włączając zaawansowaną funkcję ochrony adresów URL FireEye, aby zwiększyć zdolność do znajdowania zagrożeń dzięki bezpieczeństwu poczty e-mail FireEye. (…).*

Jeśli zabezpieczenia poczty e-mail są zarządzane przez urządzenie do zarządzania konfiguracją, należy je włączyć w menedżerze konfiguracji. Z menu u góry wybierz ustawienia. Następnie z lewej kolumny wybierz zaawansowaną ochronę adresów URL. Zaznacz pole, aby włączyć zaawansowaną ochronę adresów URL. Następnie wybierz Zastosuj.

Teraz, gdy FireEye Email Security zidentyfikuje podejrzany adres URL, przekierowuje go do naszej dynamicznej CHMURY analizy zagrożeń w celu przeprowadzenia pełnej analizy". Licencja dostarczona wraz z oprogramowaniem jest licencją typu two way (dwu stronna/ dwu torowa) co oznacza, że część danych będzie automatycznie wysyłana do producenta oprogramowania.

10. Licencje.

Zgodnie z wymogiem 73 OPZ:

Proponowane rozwiązanie musi być zaoferowane z możliwością instalacji systemu na nieograniczonej liczbie maszyn wirtualnych potwierdzonym przez Zamawiającego odpowiedzią nr 47: Prosimy o usunięcie wymagania, gdyż wymaganie wyklucza rozwiązania producentów licencjonowanych w inny sposób a jednocześnie spełniających pozostałe wymagania funkcjonalne.

Wyjaśnienia Zamawiającego: Zamawiający podtrzymuje zapisy umieszczone w punkcie II.73 OPZ. Zamawiający wymaga, aby całe rozwiązanie a więc i każdy z jego komponentów z osobna w ramach zaoferowanego modelu licencyjnego per skrzynka, pozwalał na instalację systemu na nieograniczonej liczbie maszyn wirtualnych. Zaoferowane rozwiązanie

Fireeye a konkretnie komponent Central Management 2500 Virtual Appliance (2 szt.) jest oferowany w ilości 2ch sztuk czyli licencjonowany jest per ilość maszyn wirtualnych, a nie w dowolnej ilości w obrębie zalicencjonowanych skrzynek, co potwierdza, że rozwiązanie to nie spełnia wymogów Zamawiającego (przykładowa oferta od międzynarodowego dostawcy licencji fireeye dostępna pod adresem: https://www.shi.com/Products/ProductDetail.aspx?SHISystemID=ShiCommodity&ProductIdentity=327554 08

11. Skanowanie Linux

Zgodnie z wymogiem 89 OPZ: Analiza dynamiczna musi być wykonywana z wykorzystaniem różnych wersji systemów operacyjnych Microsoft Windows (przynajmniej Windows 7 oraz Windows 10), i przynajmniej jednej wersji systemu Linux oraz różnych aplikacji i różnych ich wersji (co najmniej FireFox, Chrome, IE, Adobe Reader, Java JDK JRE, MS Office, RunDLL) potwierdzonym w odpowiedzi na pytania nr 50: Informujemy, iż wymagania przedstawione w pkt 81 i 89 samodzielnie spełnia bardzo ograniczona ilość rozwiązań. W przypadku konieczności analizy dynamicznej w zakresie wskazanym przez Zamawiającego często stosuje się rozwiązania złożone z rozwiązań różnych producentów. Czy w związku z powyższym Zamawiający dopuści rozwiązanie składające się systemów dwóch producentów, które łącznie spełni wszystkie wymagania Zamawiającego lub wykreśli wymaganie analizy dynamicznej systemu Linux oraz aplikacji Chrome i Java JDK? Spełnienie całości powyższego wymagania przez rozwiązanie jednego producenta znacząco ogranicza konkurencję.

Wyjaśnienia Zamawiającego: Zamawiający nie stawia wymogu dostawy Rozwiązania od jednego producenta. Zamawiający wymaga aby Rozwiązanie spełniało wszystkie wymagania opisane w OPZ i SWZ.

Zamawiający nie dopuszcza rozwiązań które nie posiadają analizy dynamicznej na systemie Linux oraz aplikacji Chrome i Java JDK. Rozwiązanie Fireeye zaoferowane przez Trafford nie spełnia tego wymagania, gdyż oferuje wyłącznie analizę dynamiczną na systemach Windows oraz MacOS: https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/email/fireeye-ex-series.pdf (Supports analysis against Microsoft Windows and Apple macOS X operating system images; tłum. Obsługuje analizę obrazów systemu operacyjnego Microsoft Windows i Apple macOS X). Jednocześnie rozwiązanie Forcepoint Email Security nie zostało zaoferowane z komponentem Forcepoint Advanced Malware Detection Appliance w wersji on-premise, które oferuje wsparcie dla systemów Linux pod kątem analizy dynamicznej:

https://www.forcepoint.com/sites/default/files/resources/files/brochure_forcepoint_advanced_malware_detect ion_appliance_en.pdf (str. 6: „The sandboxing process begins with Forcepoint Advanced Malware Detection Appliance sending the file to Cuckoo's malware analysis system. Cuckoo can analyze the behavior of a wide array of malicious files (executables, document exploits, Java applets), as well as malicious websites, in Windows, OS X, Linux, and Android virtualized environment." Tłum. Proces sandboxing'u

rozpoczyna się, gdy Forcepoint Advanced Malware Detection Appliance wysyła plik do systemu analizy złośliwego oprogramowania firmy Cuckoo. Oprogramowanie Cuckoo potrafi analizować zachowanie szerokiej gamy złośliwych plików (plików wykonywalnych, exploitów w dokumentach, apletów Java), a także złośliwych stron internetowych w zwirtualizowanym środowisku Windows, OS X, Linux i Android). Zatem pomimo zaoferowania dwóch rozwiązań pokrywających się funkcjonalnie oferta Trafford nadal nie spełnia wymagań Zamawiającego w zakresie skanowania z wykorzystaniem systemu Linux.

12. Skanowanie plików typów

Zgodnie z wymogiem 91 OPZ: Rozwiązanie musi analizować co najmniej następujące rodzaje plików: (Rozszerzenia używane przez pakiet OFFICE-np. DOC/DOCX, XLS/XLSX, PPT/PPTX, oraz EXE, DLL, CHM, RAR, ACE, SCR, PDF, PUB, ZIP, MP3, 7Z, BZ, GZ, JAR, MHT, RTF, CAB. potwierdzonym przez Zamawiającego w odpowiedzi na pytania nr 51 Dotyczy OPZ, p. II.91. Czy Zamawiający uzna jako spełniające wymagania rozwiązanie, w którym analizie nie są poddawane pliki ACE, SCR, PUB i MP3 lecz zamiast nich analizowane są inne często występujące pliki BAT, EML, HTA, ISO, JS, JSE, LNK, MSG, MSI, MHTML, VBE, VBS, WSF, XML, XPS, XZ?

Wyjaśnienia Zamawiającego: Zamawiający w OPZ, p. II.91 umieścił minimalne wymagania dotyczące analizy wskazanych formatów plików.

Zamawiający oczekuje spełnienia wymogów wsparcia dla wszystkich wymienionych w OPZ formatów plików analizowanych dynamicznie w tym ACE, SCR, PUB i MP3, jednocześnie formaty te nie są obsługiwane przez zaoferowane rozwiązanie marki Fireeye, które wykonuje dynamiczną analizę plików:

https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/email/fireeye-ex-series.pdf (strona druga: https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/email/fireeye-ex-series.pdf*„URLs embedded in emails, MS Office documents, PDF and archive files (ZIP, ALZIP, JAR), and other file types (Uuencoded, HTML”)* oraz z dokumentacji integracyjnej technologii Fireeye i Palo Alto

(https://xsoar.pan.dev/docs/reference/playbooks/detonate-file---fire-eye-ax - The detonation supports the following file types - PE32, EXE, DLL, JAR, JS, PDF, DOC, DOCX, RTF, XLS, PPT, PPTX, XML, ZIP, VBN, SEP, XZ, GZ, BZ2, TAR, MHTML, SWF, LNK, URL, MSI, JTD, JTT, JTDC, JTTC, HWP, HWT, HWPX, BAT, HTA, PS1, VBS, WSF, JSE, VBE, CHM.”. (tłum. Uruchomienie próbki obsługuje następujące typy plików - PE32, EXE, DLL, JAR, JS, PDF, DOC, DOCX, RTF, XLS, PPT, PPTX, XML, ZIP, VBN, SEP, XZ, GZ, BZ2, TAR, MHTML, SWF, LNK, URL, MSI, JTD, JTT, JTDC, JTTC, HWP, HWT, HWPX, BAT, HTA, PS1, VBS, WSF, JSE, VBE, CHM). Powyższe potwierdza iż zaoferowane przez Trafford rozwiązanie nie spełnia wymogów Zamawiającego.

13. Algorytmy DKIM

Zgodnie z wymogiem 16 OPZ:

16 Urządzenia muszą wspierać następujące mechanizmy kryptograficzne:

16.1 TLS: TLS w wersji przynajmniej 1.2 z możliwością zablokowania użycia starszych wersji protokołu

16.2 DomainKeys Signing: 512-, 768-, 1024-, 1536- i 2048-bit RSA

Zamawiający wymaga, aby rozwiązanie wspierało mechanizmy kryptograficzne opisane w OPZ o zdefiniowanej złożoności kryptograficznej. Rozwiązanie zaproponowane przez Trafford nie spełnia wymagania dotyczącego długości kluczy, co jest opisane w dokumentacji do produktu na stronach 117-120.

From the section DKIM Signing Keys, click the name of a key.

The Edit Signing Key page displays. The current private key displays in the text field.

2. Generate a new key; click the button Generate Key. Only 1024-bit keys are supported. A new key is generated and displays in the text field. (tłum. - Tylko 1024 bitowe klucze są wspierane. Nowy klucz jest generowany i wyświetlony w polu tekstowym)

3. Click OK. The key is saved and displays in the section DKIM Signing Keys.

Zamawiający wymaga w SWZ kluczy o różnej długości, a co najważniejsze kluczy o większej długości, co z punktu bezpieczeństwa jest słuszne, ponieważ podpisy i szyfrowanie wykonywane kluczami asymetrycznymi o długości 1024 bity są uznawane w 2021r. za niebezpieczne i możliwe do kompromitacji krypto-systemów opartych o takie rozwiązania. Wskazane w treści odwołania niezgodności zaoferowanego rozwiązania z wymaganiami Zamawiającego zawartymi w SWZ dotyczą niezgodności, które mają charakter zasadniczy i nieusuwalny, dotyczą sfery niezgodności zobowiązania zamawianego w SWZ oraz zobowiązania deklarowanego w ofercie. O niezgodności treści oferty z treścią SWZ można mówić, uwzględniając pojęcie "oferta" zdefiniowane w art. 66 k.c., odnoszącym się do oświadczeń woli, a więc w przypadku niezgodności oświadczenia woli wykonawcy z oczekiwaniami zamawiającego, w odniesieniu do merytorycznego zakresu przedmiotu zamówienia. W przedmiotowym postępowaniu z taką właśnie niezgodnością mamy do czynienia.

Nieuprawnione uznanie za skutecznie zastrzeżony jako tajemnica przedsiębiorstwa załącznik do oferty Trafford „Opis techniczny oferowanego rozwiązania”. Wykonawca Trafford poza identyfikacją zaoferowanego rozwiązania złożył dodatkowo wraz z ofertą dokument oznaczony jako „Opis techniczny oferowanego rozwiązania”. Zamawiający nie wymagał złożenia takiego dokumentu poprzestając na wymogu identyfikacji zaoferowanego rozwiązania w treści Formularza oferty. Wraz z Załącznikiem Trafford złożył uzasadnienie tajemnicy przedsiębiorstwa. Dokument zawiera ogólnikowe, gołosłowne i w żaden sposób

nie wykazane dowodowo oświadczenie, którego treść sprowadza się w istocie wyłącznie do istnienia po stronie wykonawcy woli ochrony informacji. Uzasadnienie wskazuje w szczególności, że:

- Zawiera on istotne, z punktu widzenia konkurencyjności biznesu Trafford IT Sp. z o.o. S.K. ,dane o charakterze technicznym i technologicznym przedstawia bowiem koncepcję ochrony poczty E-MAIL oraz optymalnego przepływu ruchu pocztowego opracowanej dzięki doświadczeniu, kompetencjom i specjalistycznej wiedzy inżynierów Trafford IT. Wskazał, że to Zamawiający zidentyfikował w OPZ oraz wyjaśnieniach do SWZ zarówno swoje wymagania odnośnie potrzeb jak również sposobu w jaki potrzeby te mają być przez wykonawców zrealizowane. W istocie rolą wykonawców było wyłącznie zaoferowanie konkretnych istniejących i gotowych rozwiązań, które pokrywały wymagania SWZ. Przedmiot zamówienia nie obejmuje opracowania przez wykonawców koncepcji realizacji zamówienia – przedmiot zamówienia obejmuje wyłącznie przygotowanie opracowanie samego projektu technicznego środowiska wdrożenia Rozwiązania zgodnego z zaoferowanym rozwiązaniem – które jest jawne i zostało zidentyfikowane przez Trafford w ofercie, w części niezastrzeżonej.
- unikalność koncepcji polega na doborze oraz połączeniu kilku technologii i usług programistycznych, które przy właściwej konfiguracji i parametryzacji pozwolą osiągnąć zakładane cele projektu. Swoiste know-how zastosowane przez Trafford IT Sp. z o.o. S.K. zostało wypracowane w wyniku poniesionych nakładów finansowych na budowę środowiska Lab, serię testów i wdrożeń oraz budowę zespołu programistycznego.

Mamy do czynienia w ofercie Trafford z deklaracja wykonania zamówienia przy zastosowaniu powszechnie dostępnych i zidentyfikowanych rozwiązań. Rozwiązania te posiadają pełną i publicznie jawną dokumentację techniczną. Zapewnienie o unikalności koncepcji w tej sytuacji ma służyć wyłącznie próbie ukrycia jednoznacznej niezgodności treści oferty z SWZ. Zastosowanie w celu realizacji zamówienia zidentyfikowanych w Formularzu ofertowym produktów nie może doprowadzić do zgodności z SWZ bez względu na sposób ich zestawienia. Skoro zaoferowane rozwiązanie już pierwotnie jest niezgodne z SWZ jego kompilacja z innym także niezgodnym nie pozwala uzyskać zgodności z wymaganiami Zamawiającego. Ponadto o ile faktycznie mamy do czynienia z konkretną i unikalną koncepcją na potrzeby konkretnego projektu to ten niepowtarzalny charakter (zdeterminowany unikalnymi potrzebami aktualnego Zamawiającego) skutkuje brakiem możliwości wykorzystania tej koncepcji w innych projektach. Gdyby faktycznie sama w sobie powyższa okoliczność była wystarczająca dla uzasadnienia tajemnicy przedsiębiorstwa to w istocie zasadą udzielania zamówień publicznych byłaby nie jawność ale jej brak. Jak wynika z treści udostępnionego przez Zamawiającego uzasadnienia tajemnicy przedsiębiorstwa, ma ono charakter ogólnikowy, lakoniczny, nie dotyczący

przedmiotowego postępowania. W szczególności nie zawierają żadnych konkretnych uzasadnień ani tym bardziej jakichkolwiek dowodów świadczących za zasadnością ochrony informacji. Powyższe wskazuje wprost, że uzasadnienie jest całkowicie sztampowe i nie dotyczy ani aktualnego postępowania ani przedmiotu aktualnego zamówienia. Poza zapewnieniem o przedsięwzięciu środków ochrony brak informacji jakie to konkretnie środki, nie mówiąc już o dowodach (jakichkolwiek) że tak faktycznie jest. W zakresie środków ochrony informacji Trafford ogranicza się do zapewnienia, że: dochował należytej staranności i podjął niezbędne działania w celu zachowania poufności informacji, których jawność zastrzegł. Zatem spełnił przesłanki wykazane w art. 11 ust. 4 UZNK. Trafford IT Sp. z o.o. S.K. stosuje następujące zasady ochrony tajemnicy przedsiębiorstwa:

1) klauzule poufności w umowach z pracownikami i współpracownikami oraz osobami i instytucjami współpracującymi,

2) klauzule poufności w umowach handlowych, które dotyczą kontrahentów, jak i współpracowników oraz osób współpracujących z kontrahentami,

3) wdrożona Polityka Bezpieczeństwa nadzorująca i ograniczająca dostęp pracowników, współpracowników, osób trzecich do umów objętych klauzulami poufności, poprzez nadawanie stosownych uprawnień,

4) Monitoring i/lub ograniczenie dostępu do pomieszczeń, w których są przechowywane dokumenty, umowy, oferty, informacje stanowiące tajemnicę przedsiębiorstwa podmiotów będących odbiorcami Trafford IT Sp. z o.o. S.K.

Jak potwierdza orzecznictwo KIO (sygn. akt: KIO 1632/17, KIO 1662/17, Wyrok KIO z dnia 1 września 2017 r.) treść uzasadnienia zawierająca przywołanie definicji tajemnicy przedsiębiorstwa w ujęciu ustawy o zwalczaniu nieuczciwej konkurencji, przytoczone fragmenty wyroków sądów, wyroków KIO i stanowiska doktryny nie są wystarczające dla skutecznej ochrony informacji. To wykonawca w każdej poszczególnej sprawie powinien wykazać, co i dlaczego stanowi tajemnicę przedsiębiorstwa tego wykonawcy, nie zaś przedstawiać, co wg sądów czy doktryny może zostać uznane za tajemnicę przedsiębiorstwa. Sama wola wykonawcy do ochrony informacji nie jest wystarczająca aby informacje te skutecznie chronić w rozumieniu art. 18 ust. 3 Pzp. Wykonawca w złożonych wyjaśnieniach prezentuje lakoniczne i pozbawione konkretnych przyczyn uzasadnienie ochrony informacji, które nie może korzystać z ochrony, o której mowa w przepisach powołanych w art. 18 ust.3 Pzp. Orzecznictwo KIO wskazuje wprost na obowiązek odtajnienia nieskutecznie zastrzeżonych informacji. Wyrok KIO z dnia 2019-06-27 KIO 1093/19 /Izba stwierdziła, że Przystępujący nie sprostał ciężarowi wykazania żadnej z tych przesłanek. Lektura uzasadnienia zastrzeżenia sporządzonego przez Przystępującego prowadziła do wniosku, że znaczna jego część obejmowała przytoczenie poglądów doktryny i orzecznictwa na temat natury pojęcia tajemnica przedsiębiorstwa w rozumieniu UZNK.

Natomiast nieliczne fragmenty, które miały charakter merytoryczny, pozostały nad wyraz ogólne, lakoniczne, niejasne. Co więcej, w uzasadnieniu, meritum sprawy poświęcono zaledwie kilka akapitów (…)
nie wystarcza stwierdzenie, iż dana informacja ma charakter techniczny, handlowy czy technologiczny, ale musi także ona przedstawiać pewną wartość gospodarczą dla wykonawcy właśnie z tego powodu, że pozostanie poufna. Taka informacja może być dla wykonawcy źródłem jakichś zysków lub pozwalać mu na zaoszczędzenie określonych kosztów.

W ocenie Izby, wykonawca w sposób lakoniczny i niewystarczający opisał wartość gospodarczą zastrzeżonych informacji.

Analogicznie: *„Tym samym informacje przedłożone przez wykonawcę mogą pozostać niejawne tylko w takim zakresie, w jakim wykonawca wywiązał się z ciężaru wykazania ich niejawnego charakteru. Aby wykazać zasadność zastrzeżenia danych informacji jako tajemnicy przedsiębiorstwa, Przystępujący zobowiązany był wykazać łącznie wystąpienie przesłanek tajemnicy przedsiębiorstwa, o których mowa w art. 11 ust. 4 ustawy o zwalczaniu nieuczciwej konkurencji. 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"* (wyrok KIO z dnia 16 lutego 2018 r. KIO 200/18).

Należy stwierdzić, że zasadność odtajnienia uzasadnia nie tylko złożenie wyjaśnień ogólnych, ale również brak przedłożenia dowodów uzasadniających podjęcie działań mających na celu zachowanie informacji w poufności. W wyroku KIO z dnia 9 czerwca 2020 KIO 477/20, Izba wprost stwierdziła, że mimo iż zastrzeżone dokumenty (wyjaśnienia ceny) co do zasady posiadały walor tajemnicy jednak w związku z brakiem dowodów odtajnieniu podlegała cała ich treść. Analogicznie wyrok KIO 2469/19 z dnia 20 stycznia 2020 r. Jawność postępowania jest zasadą postępowania o udzielenie zamówienia publicznego, czyli ma ona pierwszorzędne znaczenie na wszystkich etapach postępowania. Wszelkie odstępstwa od tej zasady muszą być uzasadnione i udowodnione. W szczególności wykonawca powinien wskazać, jakiego rodzaju działania podjął w celu zachowania poufności zastrzeżonych informacji, i jednocześnie złożyć dowody na ich podjęcie. Tym samym, jeżeli wykonawca Trefford nie przedstawił dowodów potwierdzających zasadność utajnienia a na takie złożone uzasadnienie nie wskazuje, odtajnieniu podlega całość złożonych informacji. Nie można uznać za skuteczne zastrzeżenia jawności wyjaśnień jedynie w celu uniemożliwienia innym

wykonawcom weryfikacji prawidłowości oferty, a w konsekwencji weryfikacji działań Zamawiającego polegających na ocenie oferty. Utrzymanie takiego zastrzeżenia, stanowi naruszenie nie tylko art. 18 ust. 3 Pzp, ale również zasady równego traktowania wykonawców i poszanowania zasad uczciwej konkurencji, o której mowa w art. 16 pkt 1 Pzp.

Przedstawione przez Trafford uzasadnienie objęcia informacji jako tajemnica przedsiębiorstwa jest ogólne i w żaden sposób nie potwierdza zasadności poczynionego utajnienia.

a) wyjaśnienia tajemnicy przedstawione przez Trafford nie zawierają żadnych konkretów,

b) przedstawione wyjaśnienia są na tyle ogólne, że nie sposób na ich podstawie ustalić dlaczego konkretne informacje zawarte w dokumencie mają określony charakter, uprawniający do przyjęcia, że ich zastrzeżenie było uzasadnione. Ich poziom ogólności jest na tyle duży, że mogłyby one zostać przedstawione przez dowolnego wykonawcę składającego uzasadnienie na dowolny przedmiot zamówienia,

c) Wykonawca Trafford nie wykazał również, że podjęto w stosunku do zastrzeżonych informacji konkretne środki mające na celu zachowanie informacji w poufności. W uzasadnieniu wskazano, co prawda że wykonawca stosuje środki ochrony informacji, ale twierdzenie to pozostaje gołosłowne, gdyż do uzasadnienia nie zostały dołączone żadne dowody potwierdzające ich podjęcie.

Jak wielokrotnie podkreślano w orzecznictwie KIO jedną z podstawowych zasad udzielania zamówień publicznych, wyrażoną w art. 18 ustawy Pzp, jest jawność postępowania o udzielenie zamówienia. Zasada ta gwarantuje transparentność prowadzonego postępowania i pozwala na urzeczywistnienie zasad uczciwej konkurencji i równego traktowania wykonawców. Odstępstwo od tej zasady, zgodnie z art. 18 ust. 3 ustawy Pzp, może mieć miejsce tylko w przypadkach określonych w ustawie (tak np. Izba w wyroku z dnia 20 stycznia 2020 r. KIO 2469/19, z dnia 13 marca 2017 r. KIO 385/17). W uzasadnieniu do poselskiego projektu ustawy o zmianie ustawy - Prawo zamówień publicznych (Sejm RP VII kadencji, nr druku: 1653) wskazano m.in.: "Wprowadzenie obowiązku ujawniania informacji stanowiących podstawę oceny wykonawców (zmiana art. 8 ust. 3). Przepisy o zamówieniach publicznych zawierają ochronę tajemnic przedsiębiorstwa wykonawcy ubiegającego się o udzielenie zamówienia. Mimo zasady jawności postępowania, informacje dotyczące przedsiębiorstwa nie są podawane do publicznej wiadomości. Jednakże, słuszny w swym założeniu przepis jest w praktyce patologicznie nadużywany przez wykonawców, którzy zastrzegając informacje będące podstawą do ich ocen, czynią to ze skutkiem naruszającym zasady uczciwej konkurencji, tj. wyłącznie w celu uniemożliwienia weryfikacji przez konkurentów wypełniania przez nich wymagań zamawiającego. Realizacja zadań publicznych wymaga faktycznej jawności wyboru

wykonawcy. Stąd te dane, które są podstawą do dopuszczenia wykonawcy do udziału w postępowaniu powinny być w pełni jawne".

Zgodnie z przepisem art. 18 ust. 3 ustawy Pzp to po stronie wykonawcy, zastrzegającego informacje jako tajemnicę gospodarczą, leży ciężar dowodu w zakresie wykazania, że zastrzeżone informacje w istocie spełniają wszystkie elementy konieczne dla jej uznania za tajemnicę przedsiębiorcy w świetle art. 11 ust. 2 uznk (tak np. Izba w wyroku z dnia 30 grudnia 2019 r. KIO 2537/19). W orzecznictwie Krajowej Izby Odwoławczej podkreśla się, że to na wykonawcy ciąży obowiązek przekonywującego i terminowego wykazania, że zastrzegane przez niego informacje stanowią tajemnicę przedsiębiorstwa. Podkreśla się, że „wykazać" oznacza coś więcej niż tylko „wyjaśnić". Zgodnie ze stanowiskiem wyrażonym w wyroku Izby z dnia 17 grudnia 2019 r. KIO 2440/19 „Użyte przez ustawodawcę w art. 8 ust. 3 zdanie pierwsze ustawy Prawo zamówień publicznych sformułowanie zobowiązujące wykonawcę do „wykazania", że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa należy rozumieć jako obowiązek „dowiedzenia", że informacje te mają właśnie taki charakter. Podkreślić należy, że jawność postępowania jest zasadą postępowania o udzielenie zamówienia publicznego, czyli ma ona pierwszorzędne znaczenie na wszystkich etapach postępowania. Wszelkie odstępstwa od tej zasady muszą być uzasadnione i udowodnione.

Złożenie gołosłownych wyjaśnień, bez wskazania konkretnych dowodów, nie może być podstawą do jej ograniczenia. Przyjęcie odmiennej argumentacji pozwoliłoby wykonawcom biorących udział w postępowaniach dokonywanie zastrzeżeń jawności informacji zawartych w ofertach w każdym przypadku, w którym takie zastrzeżenie uznaliby za korzystne dla siebie, bez konieczności poczynienia jakichkolwiek wcześniejszych starań pozwalających na zachowanie poufności tychże informacji. Takie działanie prowadziłoby do nagminnego naruszania zasady jawności postępowania i - jako takie - byłoby zjawiskiem niekorzystnym i niebezpiecznym z punktu widzenia również takich zasad postępowania, jak zachowanie uczciwej konkurencji i równego traktowania wykonawców.

W ocenie Odwołującego, lakoniczność uzasadnienia tajemnicy przedsiębiorstwa dyskwalifikuje je jako skuteczne narzędzie ochrony informacji. Należy pamiętać, że mamy do czynienia z wyjątkiem od zasady jawności postępowania i jak każdy wyjątek podlega on wykładni zawężającej. Brak jakichkolwiek dowodów związanych z ochroną informacji w organizacji Trafford, uzasadnia obowiązek odtajnienia nieskutecznie zastrzeżonych wyjaśnień ceny. Uzasadnienie tajemnicy wyjaśnień sprowadza się de facto do tezy, że skoro są to informacje istotne dla przedsiębiorstwa, to ich ochrona ma niejako automatyczny charakter. Przeczy powyższemu orzecznictwo Izby. Podkreślenia wymaga, że to nie wola ochrony informacji wykonawcy decyduje o skuteczności zastrzeżenia ale to czy wykazał i udowodnił on powyższe składając informacje.

Ustawodawca świadomie wprowadził do art. 18 ust. 3 Pzp obowiązek wykazania, że zastrzegane informacje stanowią tajemnicę przedsiębiorstwa. Owo wykazanie dotyczy przesłanek wynikających z definicji legalnej tajemnicy przedsiębiorstwa i jest warunkiem sine qua non wyłączenia w stosunku do zastrzeżonych informacji zasady jawności postępowania o udzielenie zamówienia publicznego, o której mowa w art. 18 Pzp. Nie może ulegać wątpliwości, że to na podstawie przedstawianego przez wykonawcę uzasadnienia objęcia określonych informacji tajemnicą przedsiębiorstwa, w którym wykonawca wykazuje w odniesieniu do tych informacji spełnienie przesłanek tajemnicy przedsiębiorstwa, zamawiający podejmuje decyzję o wyłączeniu jawności objętych zastrzeżeniem informacji. Stan wiedzy i świadomości zamawiającego, bądź jego poparte doświadczeniami przekonania odnośnie charakteru zastrzeganych informacji są, w przekonaniu Odwołującego, bez znaczenia. Uzasadnienia objęcia spornych informacji tajemnicą przedsiębiorstwa pozbawione jest cech wykazania, o którym mowa powyżej i nie mogły zostać uznane przez Zamawiającego za skuteczne. Stanowią one lakoniczne przytoczenie ogólnikowych argumentów, bez szczegółowego odniesienia zarówno do wszystkich elementów definicji tajemnicy przedsiębiorstwa, jak i do wszystkich rodzajów zastrzeżonych informacji. Dodatkowo, wykonawca odwołał się w uzasadnieniu do rzekomo stosowanych przez niego środków ochrony informacji stanowiących tajemnicę przedsiębiorstwa, tym niemniej – przez zaniechanie załączenia dokumentów, na które się powoływał, bądź chociażby omówienia ich treści – uniemożliwił Zamawiającemu ocenę wykazania przesłanki podjęcia w stosunku do zastrzeganych informacji działań w celu utrzymania ich w poufności. W zakresie odnoszącym się do kwestii wykazania/udowodnienia przyczyn żądanej ochrony informacji Odwołujący wskazuje, za aktualnym orzecznictwem Izby: KIO 59/21, wyrok z dnia 4 lutego 2021 r. /Zgodnie z wykładnią językową art. 18 ust. 3 p.z.p. to po stronie wykonawcy, zastrzegającego informacje jako tajemnicę gospodarczą, leży ciężar dowodu w zakresie wykazania, że zastrzeżone informacje w istocie spełniają wszystkie elementy konieczne dla jej uznania za tajemnicę przedsiębiorcy w świetle art. 11 ust. 2 u.z.n.k. Art. 8 ust. 3 p.z.p. wprost bowiem wskazuje na kim spoczywa ciężar wykazania, iż dana informacja jest tajemnicą przedsiębiorstwa - podmiotem tym jest wyłącznie zastrzegający, co bezpośrednio skorelowane jest z obowiązkiem zamawiającego w postaci ujawnienia informacji wadliwie, lub sprzecznie z prawem zastrzeżonych./; KIO 20/21, wyrok z dnia 3 lutego 2021 r. /Kluczową zasadą systemu zamówień publicznych jest jawność postępowania, która stanowi jedno z narzędzi i gwarancji zachowania w postępowaniu zarówno uczciwej konkurencji, jak i jego przejrzystości. Norma art. 8 ust. 3 p.z.p. wprost wskazuje, iż jedną z przesłanek skutecznego zastrzeżenia określonych informacji jako tajemnicy przedsiębiorstwa jest wykazanie przez wykonawcę, że informacje te w rzeczywistości taką tajemnicę przedsiębiorstwa stanowią. Oznacza to, że informacje złożone przez wykonawcę mogą

pozostać niejawne tylko w takim zakresie, w jakim wykonawca wywiązał się z ciężaru wykazania ich niejawnego charakteru. Ustawodawca posłużył się w tym zakresie sformułowaniem "wykazał", co z całą pewnością nie oznacza wyłącznie "oświadczenia", czy "deklarowania", ale stanowi znacznie silniejszy wymóg "udowodnienia". Tym samym, aby zastrzeżone przez wykonawcę informacje mogły zostać nieujawnione, wykonawca musi najpierw "wykazać", czyli udowodnić, że w stosunku do tych informacji ziściły się wszystkie przesłanki, o których mowa w art. 11 ust. 2 u.z.n.k. (…) Brak wyjaśnień lub złożenie wyjaśnień ogólnikowych powinien być traktowany jako rezygnacja z przewidzianej w art. 8 ust. 3 p.z.p. ochrony, co z kolei aktualizuje po stronie Zamawiającemu obowiązek ujawnienia nieskutecznie utajnionych informacji./; KIO 3483/20, wyrok z dnia 28 stycznia 2021 r. /Nie chodzi o to, by wykonawca uzasadniając zastrzeżenie tajemnicy przedsiębiorstwa powoływał się na jakiekolwiek środki dotyczące jakichkolwiek informacji, ale chodzi o środki chroniące poufność konkretnie tego rodzaju informacji, jakie zostały w danym postępowaniu zastrzeżone. (…) W art. 8 ust. 3 p.z.p. ustawodawca wyraźnie uzależnił zaniechanie ujawnienia określonych informacji od tego, czy wykonawca "wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa". Ustawodawca posłużył się w tym zakresie sformułowaniem "wykazał", co z całą pewnością nie oznacza wyłącznie "oświadczenia", czy "deklarowania", ale stanowi znacznie silniejszy wymóg "udowodnienia". Tym samym, aby zastrzeżone przez wykonawcę informacje mogły zostać nieujawnione, wykonawca musi najpierw "wykazać", czyli udowodnić, że w stosunku do tych informacji ziściły się wszystkie przesłanki, o których mowa w art. 11 ust. 2 u.z.n.k. Zamawiający jest zatem zobowiązany do dokonania - w świetle art. 11 ust. 2 u.z.n.k. - oceny przedstawionego przez wykonawcę uzasadnienia zastrzeżenia informacji i w zależności od wyniku tej oceny, podejmuje decyzję o ujawnieniu bądź nieujawnieniu zastrzeżonych informacji. /; KIO 3370/20, wyrok z dnia 20 stycznia 2021 r. /Regulacja art. 8 ust. 3 ustawy Pzp jednoznacznie stanowi o obowiązku wykazania, czyli udowodnienia istnienia przesłanek uznania konkretnej informacji za informację niejawną w rozumieniu ustawy znk. Wskazać należy ponadto, że faktycznie nie istnieje możliwość realizacji przedmiotu zamówienia skutecznie chroniąc tajemnicę przedsiębiorstwa bowiem dostęp do tej wiedzy będzie miał Zamawiający i jego cały personel a także w przypadku zlecania utrzymania czy też rozwoju zaoferowanego rozwiązania przepisy Pzp obligują Zamawiającego do identyfikacji posiadanego rozwiązania jako warunku zgodnego z art. 99 Pzp OPZ. Zatem w fazie realizacji zamówienia sposób realizacji projektu stanie się jawny, co potwierdza jedynie, że wyłącznym celem ochrony jako tajemnicy przedsiębiorstwa ma być niezezwolenie konkurentowi na weryfikację oferty pod kątem zgodności z SWZ. / Podobnie w orzecznictwie: KIO 2498/18, wyrok z dnia 17 grudnia 2018 r. /Samo podanie parametrów technicznych, które są zawarte w specyfikacjach technicznych produktów nie stanowi jeszcze ujawnienia wiedzy na temat działalności firmy, stosowanych

technologii, materiałów czy rozwiązań technicznych, w szczególności w sytuacji, gdy parametry te potwierdzają spełnianie wymagań określonych w SIWZ. Karty katalogowe produktów, jak i specyfikacje techniczne to dokumenty powszechnie dostępne, przeznaczone do nieograniczonego kręgu odbiorców./; KIO 2314/18, wyrok z dnia 23 listopada 2018 r. /Izba nie dopatrzyła się przyczyn dla uznania za know-how wykonawcy samych nazw oferowanego sprzętu/ (podobne stanowisko Izba zajęła m.in. w wyroku w sprawie KIO 91/15) tak również: KIO 1878/19, wyrok z dnia 10 października 2019 r. /Nie mają zatem waloru tajemnicy przedsiębiorstwa, ponieważ nie można za taką tajemnicę uznać nazw standardowych produktów powszechnie dostępnych na rynku, reklamowanych, znanych powszechnie i ujawnionych w publicznych materiałach./ Podsumowując, w ocenie Odwołującego złożonego uzasadnienia zastrzeżenia tajemnicy przedsiębiorstwa wyjaśnień ceny nie można uznać za skuteczną podstawę ochrony w świetle art. 18 ust. 3 Pzp.

Zamawiający w dniu 24.08.2021 r. (e-mailem) wezwał wraz kopią odwołania, w trybie art. 524 NPzp, uczestników postępowania przetargowego do wzięcia udziału w postępowaniu odwoławczym.

W dniu 25.08.2021 r. (wpływ do Prezesa KIO w wersji elektronicznej podpisane podpisem cyfrowym za pośrednictwem elektronicznej skrzynki podawczej - ePUAP) Trafford IT Sp. z o.o. Sp. k. zgłosiła przystąpienie do postępowania odwoławczego po stronie Zamawiającego wnosząc o oddalenie odwołania w całości.

W dniu 21.09.2021 r. (e-mailem podpisanym podpisem cyfrowym) Zamawiający na podstawie trybie art. 521 NPzp złożył odpowiedź na odwołanie. Stwierdził: *„oświadczam, że uwzględniam zarzuty zawarte w odwołaniu w całości. (…) W związku z powyższym wnoszę o umorzenie postępowania przed Krajową Izbą Odwoławczą w całości, w przypadku nie wniesienia sprzeciwu przez przystępującego tj. Trafford IT Sp. z o.o. Sp.k.”.*

Skład orzekający Krajowej Izby Odwoławczej po zapoznaniu się z przedstawionymi poniżej dowodami, po wysłuchaniu oświadczeń, jak i stanowisk stron (Zamawiający nieobecny na posiedzeniu i rozprawie prawidłowo zawiadomiony) oraz Przystępującego złożonych ustnie do protokołu w toku rozprawy, ustalił i zważył, co następuje.

Skład orzekający Izby ustalił, że nie została wypełniona żadna z przesłanek skutkujących odrzuceniem odwołania na podstawie art. 528 NPzp, a Wykonawca wnoszący odwołanie posiadał interes w rozumieniu art. 505 ust. 1 NPzp, uprawniający do jego złożenia.

Odwołujący w rankingu złożonych ofert zajął drugie miejsce, w wypadku więc potwierdzenia zarzutów, ma szansę na uzyskanie przedmiotowego zamówienia.

Skład orzekający Izby , działając zgodnie z art. 542 ust. 1 NPzp, dopuścił w niniejszej sprawie dowody z: dokumentacji postępowania o zamówienie publiczne nadesłanej przez Zamawiającego w formie elektronicznej, w tym w szczególności postanowień SWZ, załącznika nr 1 do SWZ i Umowy, tj. Opis przedmiotu Zamówienia zwany dalej: *„OPZ”*, odpowiedzi na pytania (pismo z 14.07.2021 r./ oraz oferty Przystępującego wraz z dokumentem „Opis techniczny oferowanego rozwiązania”, jak i informacji o wyborze oferty najkorzystniejszej z 11.08.2021 r.

W poczet materiału dowodowego Izba zaliczyła załączoną do pisma procesowego złożonego na posiedzeniu przez Odwołującego na potwierdzenie okoliczności wskazanych w piśmie:

1) dokumentacje techniczna producenta oferowanego przez Przystępującego rozwiązania – Forcepoint; /pełna wersja oryginalna – tłumaczenie fragmentów w zakresie przedmiotu sporu w ramach złożonego pisma/

2) dokumentacje techniczna producenta oferowanego przez Przystępującego rozwiązania – Fireeye /pełna wersja oryginalna – tłumaczenie fragmentów w zakresie przedmiotu sporu w ramach złożonego pisma/.

Dodatkowo w poczet materiału dowodowego Izba zaliczyła załączone do pisma procesowego złożonego na posiedzeniu przez Przystępującego na potwierdzenie okoliczności wskazanych w piśmie:

1) wyciąg z dokumentacji techniczna producenta oferowanego przez Przystępującego rozwiązania Fireeye /odnośnie - 2. Rozwiązanie nie posiada wyszukiwania po zdefiniowanych parametrach, wersja oryginalna wraz z tłumaczeniem/;

2) wyciąg z dokumentacji techniczna producenta oferowanego przez Przystępującego rozwiązania Fireeye /odnośnie – 4. Kwarantanny centralnej/;

3) wyciąg z dokumentacji techniczna producenta oferowanego przez Przystępującego rozwiązania dokumentacja EMAIL SECURITY – SERVER EDITION – USER GUIDE – RELEASE 9.1.pfe, str. 384 /odnośnie - 9. Użycie chmury/.

Nadto, zaliczono do materiału dowodowego złożone na rozprawie przez Przystępującego:

1) rysunek (schemat) przedstawiający działanie mechanizmu exchange, tj. poczty wewnętrze w zakresie zarzutu dotyczącego - 1. Braku skanowania exchange;

2) dokument oficjalnego supportu, czyli wsparcia producenta w zakresie możliwości zaimplementowania klucza innego niż 1024 bity wraz z tłumaczeniem w zakresie zarzutu dotyczącego - 13. Algorytmy DKIM;

3) schemat przedstawiający przejście informacji z mechanizmu 1, 2, aż do mechanizmu 3 będącego funkcjonalnością mechanizmu 1.

Odnosząc się generalnie do podniesionych w treści odwołania zarzutów, stwierdzić należy, że odwołanie nie zasługuje na uwzględnienie.

Odwołujący sformułował w odwołaniu następujące zarzuty naruszenia:
1) art. 226 ust.1 pkt 5 w zw. z art. 16 pkt 1 Pzp poprzez zaniechanie odrzucenia oferty wykonawcy Trafford, pomimo, że zaoferowane w postępowaniu przez tego wykonawcę rozwiązanie nie spełnia wymagań Zamawiającego zawartych w treści SWZ,
2) art. 18 ust. 1, 2, i 3 Pzp w zw. z art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2019 r. poz. 1010 i 1649), poprzez pozbawione podstaw faktycznych i prawnych zaniechanie uznania za bezskuteczne zastrzeżenia jako tajemnicy przedsiębiorstwa treści złożonego przez Trafford Załącznika - „Opis techniczny oferowanego rozwiązania”,
co skutkuje naruszeniem art. 239 ust.1 Pzp w zw. z art. 16 pkt 1 Pzp poprzez wadliwy wybór oferty najkorzystniejszej w postępowaniu.

Izba dokonała następujących ustaleń odnośnie do przedmiotowego odwołania:

Izba przywołuje stan faktyczny wynikający z treści odwołania, pisma procesowego Przystępującego oraz Odwołującego w szczególności przywołane postanowienia OPZ oraz odpowiedzi na pytania. Jednocześnie, należy zauważyć, że Przystępujący w ramach swojego pisma procesowego złożonego na posiedzeniu oraz na samym posiedzeniu złożył sprzeciw wobec uwzględnienia zarzutów odwołania przez Zamawiającego, za wyjątkiem - zarzutu naruszenia art. 18 ust. 1, 2 i 3 Ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2021 r. poz. 1129) w związku z art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2019 r. poz. 1010 i 1649) poprzez pozbawione podstaw faktycznych i prawnych zaniechanie uznania za bezskuteczne zastrzeżenia jako tajemnicy przedsiębiorstwa treści złożonego przez Trafford Załącznika - „Opis techniczny oferowanego rozwiązania”. W konsekwencji, wobec braku sprzeciwu odnośnie uwzględnienia odwołania w zakresie niniejszego zarzutu przez Zamawiającego – postępowanie odwoławcze w zakresie tego zarzutu zostało umorzone i nie był on kierowany na rozprawę. Dodatkowo, Odwołujący w toku posiedzenia wycofał odwołanie w zakresie następujących zarzutów szczegółowych: zarzutu naruszenia art. 226 ust.1 pkt 5 w zw. z art. 16 pkt 1 Ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2021 r. poz. 1129) poprzez zaniechanie odrzucenia oferty Trafford IT Sp. z o.o. Sp. k., pomimo, że zaoferowane w postępowaniu przez tego wykonawcę rozwiązanie nie spełnia wymagań Zamawiającego zawartych w treści SWZ w zakresie zarzutów szczegółowych - numer: 3.

Rozwiązanie nie pozwala na rozkład ruchu opisany w OPZ; 5. Parametrów odrzucenia, 6. 7.2 AV; 7. Braku licencji; 10. Licencji; 11. Skanowania Linuxa oraz 12. Skanowania plików typów. W konsekwencji, wobec wycofania odwołania w zakresie wskazanych zarzutów – postępowanie odwoławcze w zakresie tych zarzutów zostało umorzone. Ostatecznie przedmiotem rozprawy były następujące podtrzymane zarzutu, w zakresie których uwzględnienia Przystępujący po stronie Zamawiającego wniósł sprzeciw, tj. zarzutu naruszenia art. 226 ust.1 pkt 5 w zw. z art. 16 pkt 1 Ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2021 r. poz. 1129) poprzez zaniechanie odrzucenia oferty Trafford IT Sp. z o.o. Sp. k., pomimo, że zaoferowane w postępowaniu przez tego wykonawcę rozwiązanie nie spełnia wymagań Zamawiającego zawartych w treści SWZ w zakresie zarzutów szczegółowych: 1. Braku skanowania exchange; 2. Rozwiązanie nie posiada wyszukiwania po zdefiniowanych parametrach; 4. Kwarantanny centralnej; 8. Sandboxing załączników jako funkcja bramki pocztowej; 9. Użycie chmury oraz 13. Algorytmy DKIM.

Do pozostałych kwestiach Izba odniesie się w ramach poszczególnych zarzutów.

Biorąc pod uwagę stan rzeczy ustalony w toku postępowania (art. 552 ust.1 NPzp), oceniając wiarygodność i moc dowodową, po wszechstronnym rozważeniu zebranego materiału (art. 542 ust. 1 NPzp), Izba stwierdziła co następuje.

Z uwagi na charakter sformułowanych zarzutów Izba odniesie się do nich łącznie stwierdzając że podlegają one oddaleniu. Jednocześnie zastrzegając, że Izba za wyrokiem SO w Warszawie z 25.08.2015 r., sygn. akt: XXIII Ga 1072/15: *" (…) ma prawo podzielić zarzuty i wartościową argumentację jednego z uczestników, zgodnie z zasadą swobodnej oceny dowodów, co słusznie zauważył uczestnik w odpowiedzi na skargę."*). Nadto, zwracając uwagę, że w orzecznictwie KIO wskazuje się na obowiązek interpretowania wszelkich nieścisłości na korzyść wykonawców, bowiem to Zamawiający, jako gospodarz postępowania, zobowiązany jest do należytego opracowania dokumentacji przetargowej, której brzmienie powinno być jasne, m.in. w wyroku z dnia 21.11.2017 r. o sygn. akt KIO 2336/17, w którym Izba orzekła: "*Zgodnie z orzecznictwem Krajowej Izby Odwoławczej, wszelkie niejasności, nieścisłości treści Specyfikacji Istotnych Warunków Zamówienia należy rozpatrywać na korzyść wykonawcy"*, w wyroku z dnia 16.04.2015 r. o sygn. akt KIO 660/15: *"obowiązuje swoista "święta" zasada, że wszelkie niejasności, dwuznaczności, niezgodności postanowień SIWZ należy rozpatrywać na korzyść wykonawców.",* w wyroku z 24.10.2018 r., sygn. akt: KIO 2100/18*, zgodnie z którym "w przypadku możliwości interpretacji zapisów SIWZ w różny sposób, wszelkie niejasności, które mogą odnosić się do złożonych w postępowaniu ofert, odczytywać należy na korzyść wykonawców"* (Tak również, m.in.

w uchwale z 03.08.2017 r., sygn. akt KIO/KD 38/17 oraz wyroku SO w Szczecinie z 07.03.2018 r., sygn. akt: VIII Ga 102/18). Analogiczne stanowisko zajmują sądy powszechne – np. SO w Nowym Sączu w wyroku z 18.03.2015 r. o sygn. akt: III Ca 70/15 uznał, iż*: "Zapisy w SIWZ (...) muszą mieć charakter precyzyjny i jednoznaczny, a wątpliwości powstałe na tym tle muszą być rozstrzygane na korzyść wykonawcy. Obowiązek takiego formułowania i tłumaczenia ma na celu realizację zasady uczciwej konkurencji i równego traktowania wszystkich wykonawców przystępujących do przetargu (...)."*.

Względem zarzutu - 13. Algorytmy DKIM.

Izba oddaliła zarzut w tym zakresie, gdyż Przystępujący złożył na rozprawie dowód potwierdzający oficjalny suport producenta, czyli wsparcia producenta w zakresie możliwości zaimplementowania klucza innego niż 1024 bity. Jednocześnie wszelkiego rodzaju wątpliwości Odwołującego należy rozwiać zważywszy nadanie przedłożonej informacji przez producenta – Article Number, czyli Numeru KB. Odnośnie kwestii produktu Open SSL, wyjaśnienia przedstawione na rozprawie przez Przystępującego nie zostały zanegowane przez Odwołującego. Nadto, należy potwierdzić, że zgodnie z odpowiedzią na pytanie 11 Zamawiający jednoznacznie stwierdził, że po stronie Wykonawcy jest dostarczenie kompletnej infrastruktury w tym wszelkich niezbędnych licencji. /Załącznika nr 1 do SWZ pkt 68. Czy Zamawiający dostarcza licencje Vmware lub innego systemu wirtualizacyjnego? Jeżeli tak to jaki to będzie system? Wyjaśnienia Zamawiającego: Zamawiający nie dostarcza licencji. Po stronie Wykonawcy jest dostarczenie kompletnej infrastruktury w tym wszelkich niezbędnych licencji./

Biorąc powyższe pod uwagę, Izba uznała jak na wstępie.

Względem zarzutu – 9. Użycie chmury.

Izba oddaliła zarzut w tym zakresie. Zgodnie z wyjaśnieniami Przystępującego z rozprawy, uznał Przystępujący, że Zamawiający zabronił przesyłania całych plików (Rozdz. II pkt 80) jednocześnie wskazując, że kontrola reputacji musi odbywać się na podstawie unikalnych metadanych własnościowych pliku /Kontrola reputacji musi odbywać się na podstawie unikalnych metadanych własnościowych pliku, nie jest dopuszczalne, aby sprawdzenie reputacyjne wymuszało przesłanie pliku na zewnątrz systemu kontroli poczty./ Stwierdził, że badanie reputacji w jego wypadku ma miejsce poprzez metadane pliku (funkcje skrótu, rozmiar, czy też typ pliku) bez przesyłania całego pliku do ogólnoświatowej bazy reputacji. Wskazywał także, że zgodnie z pkt 79 Rozdz. II taka kontrola miała odbywać się w ogólnoświatowej bazie reputacji /Kontrola reputacji dla plików i adresów URL musi odbywać się w ogólnoświatowej bazie reputacji./ W konsekwencji negując tezę

Odwołującego, że nic nie powinno być wysyłane. W ocenie Izby, stanowisko przedstawione przez Przystępującego na rozprawie, jak i w złożonym piśmie jest zasadne. Nie zmieniają tego odpowiedzi na pytanie 14 /Załącznika nr 1 do SWZ pkt 81.Czy funkcja sandboxingu może być wykonywana na serwerach producenta (w chmurze)? Wyjaśnienia Zamawiającego: Zamawiający nie dopuszcza aby jakiekolwiek dane ze środowiska Zamawiającego opuszczały lokalizacje Zamawiającego/ i 35 /Załącznika nr 1 do SWZ II ust. 81. Czy Zamawiający dopuszcza rozwiązania typu sandbox działające w chmurze, czy też wyłącznie rozwiązania działające on-premise (instalowane lokalnie w infrastrukturze Zamawiającego i nie przesyłające żadnych danych do chmury)? Wyjaśnienia Zamawiającego: Zamawiający dopuszcza jedynie rozwiązanie działające on-premise (instalowane lokalnie w infrastrukturze Zamawiającego i nie przesyłające żadnych danych do chmury)./. Rozwiązanie zaproponowane przez Odwołującego na rozprawie niejako w odpowiedzi na stanowisko Przystępującego jest jednym z możliwych obok rozwiązania Przystępującego uwzględniając postanowienia OPZ (pkt 79-83 Rozdz. II: *„79 Kontrola reputacji dla plików i adresów URL musi odbywać się w ogólnoświatowej bazie reputacji. 80 Kontrola reputacji musi odbywać się na podstawie unikalnych metadanych własnościowych pliku, nie jest dopuszczalne, aby sprawdzenie reputacyjne wymuszało przesłanie pliku na zewnątrz systemu kontroli poczty. 81 Funkcja sandboxingu dla plików przesyłanych pocztą elektroniczną musi być wbudowana w system ochrony poczty, nie jest dopuszczalne stosowanie zewnętrznych systemów firm trzecich. Dopuszcza się rozwiązanie w postaci dedykowanego urządzenia zintegrowanego z systemem poczty elektronicznej. 82 Analiza statyczna i dynamiczna muszą się odbywać w na dostarczonych urządzeniach – nie jest dopuszczalne wysyłanie plików do analizy poza siedzibę Zamawiającego. 83 Rozwiązanie powinno umożliwiać uruchomienie nie mniej niż 56 maszyn wirtualnych wykonujących analizę jednocześnie. Zamawiający poprzez liczbę 56 określa ilość dostępnych maszyn wirtualnych, która ma być dostępna do analizy nawet w przypadku awarii jednego z urządzeń analizujących.”*). Ewentualne wątpliwości, które mogłyby zaistnieć wobec jednoznacznej treści pkt 80, że kontrola reputacji musi odbywać się na podstawie unikalnych metadanych własnościowych należy rozpatrzeć na korzyść Przystępującego.

Biorąc powyższe pod uwagę, Izba uznała jak na wstępie.

Względem <u>zarzutu – 1. Braku skanowania Exchange.</u>

Izba oddaliła zarzut w tym zakresie, uznając zasadność stanowiska Przystępującego, iż w świetle odpowiedzi na pytanie 1 i 33 tylko proces filtrowania i ochrony miał odbywać się na serwerach exchange. /Pytanie nr 1: *„Czy Zamawiający pisząc o filtrowaniu poczty wewnętrznej wymaga rozwiązania pozwalającego na filtrowanie pod kątem szkodliwej treści, spamu dla wiadomości nie opuszczających serwerów Exchange? Wyjaśnienia*

Zamawiającego: Zamawiający potwierdza, że wymaga rozwiązania pozwalającego na filtrowanie pod kątem szkodliwej treści, spamu dla wiadomości nie opuszczających serwerów Exchange". Pytanie nr 33: *„Rozwiązania bazujące na bezpośredniej ochronie serwerów Exchange są często elementem bardzo obciążającym farmę serwerów. Ponadto, ich funkcjonalność najczęściej ogranicza się do klasy standardowego antywirusa i nie wspiera zaawansowanej analizy bezpieczeństwa jak na przykład sandbox, dodatkowa analiza URL czy antyphising. Czy Zamawiający akceptuje rozwiązanie zewnętrzne, które nie wymaga instalacji na serwerach Exchange, a tylko odpowiedniej konfiguracji i analizuje pocztę wewnętrzną z wykorzystaniem wszystkich narzędzi bezpieczeństwa używanych do analizy poczty przychodzącej? Wyjaśnienia Zamawiającego: Zamawiający podtrzymuje zapisy SWZ. W punkcie II. 3 OPZ opisał swoje wymagania odnośnie środowiska nie wskazując sposób jego implementacji. Rozwiązanie do ochrony poczty wewnętrznej, nie może zmieniać wewnętrznego routingu przy przepływie poczty wewnętrznej"*./. Jednocześnie przedstawione rozwiązanie przez Przystępującego na rozprawie, jak i w ramach złożonego rysunku (schematu) mieści się w wytycznych Zamawiającego. Nie ulega zmianie wewnętrzny routingu, gdyż wiadomość dociera do odbiorcy. Wykorzystywany jest mechanizm kopii oryginalnej wiadomości. Następuje analiza przez mechanizm 1 i 2 równolegle, a następnie kasowana jest wiadomość na serwerze Exchange u odbiorcy, który je otrzymał. Należy zauważyć, że Zamawiający w odpowiedzi na pytanie 33 nie określał sposobu implementacji wymaga odnośnie środowiska, a funkcja ochronna następuje niezwłocznie po wykryciu zagrożenia, tj. niebezpiecznej wiadomości. Ocenę powyższego nie zmienia pkt 2.6 /2.6 rozwiązanie musi zapewniać filtrowanie poczty przychodzącej i wychodzącej (w tym poczty wewnętrznej), przy czym musi istnieć możliwość przypisana odrębnych polityk dla każdego z kierunków przesyłania poczty elektronicznej.) oraz pkt 3 zdanie drugie /Dla ochrony poczty wewnętrznej (internal), której ruch nie przechodzi przez gateway a zamyka się wewnątrz farmy serwerów pocztowych, wymagane jest zastosowanie mechanizmu chroniącego pocztę bezpośrednio na serwerach Exchange./ Rozdz. II OPZ, ewentualne wątpliwości w świetle odpowiedzi na pytanie 33 i braku wskazania sposobu implementacji i nie zmienieniu wewnętrznego routingu należy rozpatrzeć na korzyść Przystępującego.

Biorąc powyższe pod uwagę, Izba uznała jak na wstępie.

Względem zarzutu – 2. Rozwiązanie nie posiada wyszukiwania po zdefiniowanych parametrach.

Izba oddaliła zarzut w tym zakresie, uznając zasadność stanowiska Przystępującego, iż skoro mechanizm 1 przekazuje wiadomość do mechanizmu 2, to wszystkie wiadomości podlegają analizę według wymaganych przez Zamawianego kryteriów. W konsekwencji okoliczność, że mechanizm 1 nie ma możliwości wyszukiwania po zdefiniowanych przez

Zamawiającego parametrach we wskazanym zakresie jest irrelewantny, gdyż spełnia ta funkcjonalność mechanizm 2, a całe rozwiązanie ma charakter rozwiązania kompleksowego.

Biorąc powyższe pod uwagę, Izba uznała jak na wstępie.

Względem zarzutu – 4. Kwarantanny centralnej.

Izba oddaliła zarzut w tym zakresie. W tym wypadku, Przystępujący wskazywał na rozprawie na możliwość wyłączenia na etapie wdrożenia produktów kwarantanny w jednym z produktów (mechanizmów), przy jednoczesnym pozostawieniu możliwości oznaczenia nagłówka wiadomości odpowiednim znacznikiem, a następnie przesłania takiej wiadomości do kolejnego produktu (mechanizmu), który także dodaje kolejny nagłówek i przesyła do kwarantanny centralnej w mechanizmie 1. W ocenie Izby, biorąc pod uwagę pkt 69 Rozdz. II OPZ /Licencje na bramki przyjmujące pocztę powinny posiadać opcję skalowania w celu uzyskania większej wydajności na kolejne maszyny wirtualne w środowisku wirtualnym będącym w posiadaniu Zamawiającego bez ponoszenia dodatkowych kosztów./, jak i pkt 2 Rozdz. I /Zakres prac obejmuje: 1) Prace organizacyjne i analityczne; 2) Opracowanie projektu technicznego środowiska wdrożenia Rozwiązania; 3) Dostawa Rozwiązania w części obejmującej sprzęt i licencje; 4) Wdrożenie Rozwiązania; 5) Opracowanie dokumentacji powdrożeniowej; 6) Przeprowadzenie warsztatów i szkoleń z zakresu Systemu; 7) Zapewnienie wsparcia producenta dla wdrożonego Systemu; 8) Zapewnienie wsparcia Wykonawcy dla wdrożonego Systemu; 9) Udzielenie gwarancji na System/ oraz pkt 6 ppkt 2 Rozdz. I /W ramach wdrożenia Wykonawca wykona co najmniej: (…) 2) Instalację dostarczonego rozwiązania, konfigurację i parametryzację/ OPZ dotyczący wdrożenia, tj. obowiązek Wykonawcy instalacji dostarczonego rozwiązania, konfiguracji i jego parametryzacji, brak jest podstaw do negowania zaprezentowanego przez Przystępującego na rozprawie rozwiązania.

Biorąc powyższe pod uwagę, Izba uznała jak na wstępie.

Względem zarzutu – 8. Sandboxing załączników jako funkcja bramki pocztowej.

Izba oddaliła zarzut w tym zakresie. Izba podkreśla, że Przystępujący nie negował, że tylko jeden z jego mechanizmów, które zostały zaoferowane, tj. mechanizm 2 ma funkcje sandboxingu. Podnosił przy tym, że zaoferował rozwiązanie kompleksowe, tj. dwa mechanizmy, które jako całość spełniają wszystkie funkcjonalności, w tym także funkcje sandboxingu. Podnosił także, że zaoferowane rozwiązanie nie musiało pochodzić od jednego producenta. Wskazywał na odpowiedź na pytanie 15 /Załącznika nr 1 do SWZ pkt 81. Czy system sandboxingu musi być tego samego producenta co rozwiązanie ochrony poczty? Wyjaśnienia Zamawiającego: System sandboxingu nie musi pochodzić od tego samego producenta co rozwiązanie ochrony poczty. Zamawiający oczekuje dostawy kompletnego

rozwiązania realizującego funkcje opisane w OPZ./. W ocenie Izby, w świetle przytoczonej powyżej odpowiedzi na pytanie 15, gdzie stwierdza się, że - System sandboxingu nie musi pochodzić od tego samego producenta co rozwiązanie ochrony poczty, a Zamawiający oczekuje dostawy kompletnego rozwiązania - brak jest podstaw do zanegowania rozwiązania zaprezentowanego przez Przystępującego na rozprawie.

Biorąc powyższe pod uwagę, Izba uznała jak na wstępie.

W tym stanie rzeczy, Izba oddaliła odwołanie na podstawie art. 553 zdanie pierwsze i art. 554 ust. 1 pkt 1 Pzp oraz orzekła jak w sentencji.

O kosztach postępowania orzeczono stosownie do wyniku na podstawie art. 557 Pzp oraz art. 575 Pzp, z uwzględnieniem postanowień Rozporządzenia Prezesa Rady Ministrów w sprawie szczegółowych rodzajów kosztów postępowania odwoławczego, ich rozliczania oraz wysokości i sposobu pobierania wpisu od odwołania z dnia 30 grudnia 2020 r. (Dz.U. z 2020 r. poz. 2437) w oparciu o § 8 ust. 2 zdanie pierwsze rozporządzenia wskazanego powyżej obciążając kosztami Odwołującego.

Przewodniczący:

……