Sygn. akt: KIO 3352/20

WYROK
z dnia 8 stycznia 2021 roku

Krajowa Izba Odwoławcza - w składzie:

Przewodniczący: Irmina Pawlik

Protokolant: Piotr Kur

po rozpoznaniu na rozprawie w dniu 4 stycznia 2021 r. w Warszawie odwołania wniesionego do Prezesa Krajowej Izby Odwoławczej w dniu 16 grudnia 2020 r. przez wykonawcę allclouds.pl Spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie w postępowaniu prowadzonym przez zamawiającego Urząd Komisji Nadzoru Finansowego z siedzibą w Warszawie

orzeka:

1. oddala odwołanie;
2. kosztami postępowania obciąża odwołującego allclouds.pl Spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie i zalicza w poczet kosztów postępowania odwoławczego kwotę **15 000 zł 00 gr** (słownie: piętnaście tysięcy złotych zero groszy) uiszczoną przez odwołującego tytułem wpisu od odwołania.

Stosownie do art. 198a i 198b ustawy z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (t.j. Dz. U. z 2019 r., poz. 1843 ze zm.) w zw. z art. 92 ust. 1 ustawy z dnia 11 września 2019 r. Przepisy wprowadzające ustawę – Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 2020 ze zm.) na niniejszy wyrok - w terminie 7 dni od dnia jego doręczenia - przysługuje skarga za pośrednictwem Prezesa Krajowej Izby Odwoławczej do Sądu Okręgowego w Warszawie.

Przewodniczący: ……

Sygn. akt: KIO 3352/20

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

Zamawiający Urząd Komisji Nadzoru Finansowego z siedzibą w Warszawie (dalej jako „Zamawiający") prowadzi postępowanie o udzielenie zamówienia publicznego pn. „Zakup usług budowy nowego systemu Sandbox'owego" (nr ref. DZA-DZAZZP.2610.48.2020). Ogłoszenie o zamówieniu zostało opublikowane w Dzienniku Urzędowym Unii Europejskiej z dnia 7 grudnia 2020 r. pod numerem 2020/S 238-587649. Postępowanie prowadzone jest w trybie przetargu nieograniczonego na podstawie ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tj. Dz. U. z 2019 r., poz. 1843 ze zm., dalej „ustawa Pzp"). Wartość szacunkowa zamówienia przekracza kwoty określone w przepisach wydanych na podstawie art. 11 ust. 8 ustawy Pzp.

W dniu 16 grudnia 2020 r. wykonawca allclouds.pl Spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie (dalej jako „Odwołujący") wniósł odwołanie do Prezesa Krajowej Izby Odwoławczej wobec treści specyfikacji istotnych warunków zamówienia („SIWZ"). Odwołujący zarzucił Zamawiającemu naruszenie:

1. art. 29 ust. 1 ustawy Pzp przez niejednoznaczny i niewyczerpujący opis przedmiotu zamówienia, bez uwzględnienia wszystkich wymagań i okoliczności mogących mieć wpływ na sporządzenie oferty;
2. art. 29 ust. 2 ustawy Pzp przez opisanie przedmiotu zamówienia w sposób utrudniający uczciwą konkurencję;
3. art. 29 ust. 3 ustawy Pzp przez opisanie przedmiotu zamówienia przez wskazanie pochodzenia, źródła, szczególnego procesu, który charakteryzuje wyłącznie producenta FireEye, przez co Zamawiający eliminuje wykonawców chcących zaoferować konkurencyjny produkt i nie jest to uzasadnione specyfiką przedmiotu zamówienia i Zamawiający może opisać przedmiot zamówienia za pomocą dostatecznie dokładnych określeń i może użyć wyrazów „lub równoważny";
4. art. 30 ust. 4 ustawy Pzp przez zaniechanie dopuszczenia rozwiązań równoważnych opisywanych i zaniechaniu użyciu wyrazów „lub równoważne", zaniechanie opisania warunków równoważności;
5. art. 7 ust. 1 ustawy Pzp przez opisanie przedmiotu zamówienia, który eliminuje konkurencję, bo bezpodstawnie łączy przedmiot zamówienia, który można rozdzielić do innych postępowań, i który został jedynie po to połączony, żeby uniknąć konkurencji, przez co nierówno traktuje wykonawców, jest nieproporcjonalny i nieprzejrzysty;

6. art. 5b i 5f ustawy Pzp, bo bezpodstawnie łączy przedmiot zamówienia, który można rozdzielić, i który został jedynie po to połączony, żeby uniknąć konkurencji i umożliwić złożenie oferty wyłącznie na FireEye, co wyklucza innych producentów;
7. art. 66 ust. 1, art. 67 ust. 2 ustawy Pzp przez zaniechanie przeprowadzenia postępowania z wolnej ręki w stosunku do Apple i oddzielnego postępowania konkurencyjnego przetargu nieograniczonego w pozostałym zakresie.

Odwołujący wniósł o uwzględnienie odwołania i nakazanie Zamawiającemu powtórzenia czynności określenia treści SIWZ z uwzględnieniem żądań zawartych w uzasadnieniu, a także o obciążenie Zamawiającego kosztami postępowania odwoławczego.

Uzasadniając zarzuty Odwołujący wskazał, iż Zamawiający powinien dokonać podziału zamówienia i wyłączyć zakres dotyczący Mac OS, ewentualnie zmienić SIWZ poprzez dopuszczenie możliwości emulowania Mac OS o chmurę zamiast na urządzeniu. Odwołujący wskazał, że Zamawiający ma działalność opartą głownie o rozwiązania na platformie Microsoft, a komputery działające na systemie Mac OS stanowią zdecydowaną mniejszość. Objęcie jednym postępowaniem zakresu dotyczącego niszowego rozwiązania Mac OS i dominującego Microsoft uniemożliwia złożenie oferty innym producentom niż FireEye. Działanie Zamawiającego jest w ocenie Odwołującego niedozwolonym łączeniem przedmiotu zamówienia w celu uniknięcia stosowania przepisów prawa. Zamawiający nie ma obiektywnej potrzeby do prowadzenia jednego postępowania na Sandbox do systemów Microsoft i Mac OS. Odwołujący podkreślił, że obecny kształt SIWZ umożliwia złożenie oferty wyłącznie na produkt FireEye (urządzenia 2xEX 3500 plus 2xNX 4500), wygra zatem ten wykonawca, który zarezerwuje sprzedaż w FireEye i producent zagwarantuje mu najlepszą cenę. Tymczasem na rynku są inne produkty, które mogą spełnić potrzeby Zamawiającego przy wprowadzeniu zmian w SIWZ, np. Cisco, Lastline, Check Point, Fortinet, ewentualnie SonicWall, Forcepoint, McAfee, ProofPoint, Symantec. Liderami na rynku są rozwiązania Fortinet, Trend Micro, Lastline, Checkpoint, a produkt FireEye wg badań firmy NSSlabs znajduje się poniżej przeciętnej. Odwołujący wskazał także na okoliczność ataków hakerskich na FireEye, wskazując, że produkt tego producenta posiada luki i nie jest bezpieczny, a jako taki nie odpowiada rzeczywistym potrzebom Zamawiającego.

W zakresie pkt 2f opisu przedmiotu umowy (dalej jako „OPU”), Odwołujący wskazał, iż FireEye jako jeden z niewielu producentów standardowo oferuje licencje systemów operacyjnych. Większość innych producentów oferuje licencje systemów operacyjnych za dodatkową opłatą. Dodatkowo świadczenia (licencje, usługi) FireEye są w języki angielskim. Wersje angielskie i polskie licencji i warunki usług do licencji Apple i Microsoft są utrzymywane osobno i nie są spójne. Poprawki oprogramowania objętego licencjami

określonymi językiem polskim są w innym czasie niż poprawki na język angielski. Zamawiający wymaga dostarczenia licencji na systemy operacyjne, ale nie wymaga ich w wersji polskiej, co stanowi wsparcie dla FireEye, a także wskazuje, że Zamawiający kupi bezużyteczną dla siebie rzecz. Zdaniem Odwołującego Zamawiający powinien wymagać zaoferowania licencji wyłącznie w języku polskim. W konsekwencji Odwołujący wskazał na konieczność zmiany pkt 2 lit f OPU i nadanie mu brzmienia: „Wykonawca musi dostarczyć licencje dla systemów operacyjnych maszyn wirtualnych na których odbywa się analiza plików oraz programów tam zainstalowanych w języku polskim".

W odniesieniu do pkt 3l.a) OPU, w zakresie dotyczącym Mac OS, Odwołujący wskazał, iż uruchomienie systemu Mac OS na urządzeniach innych niż komputery dostarczane przez Apple będzie równoznaczne ze złamaniem warunków licencji oprogramowania Apple. Firma Apple nie zezwala na uruchomienie systemu Mac OS na urządzeniach innych niż oferowane przez nią. Odwołujący wskazał, iż na rynku istnieje tylko jedno rozwiązanie klasy sandbox umożliwiające uruchomienie obrazu systemu Mac OS na urządzeniu (a nie w chmurze) – jest to rozwiązanie FireEye. W systemach sandbox np. Trend Micro i innych producentów można uruchomić (emulować) Mac OS wyłącznie w chmurze, a nie na urządzeniu. Dla Zamawiającego nie ma żaden różnic czy uruchomienie (emulacja) następuje na urządzeniu czy w chmurze bo efekt końcowy jest ten sam. Mac OS jest rzadko stosowany w Polsce, jest drogi, niszowy. Zauważył, że Zamawiający nie wskazał w SIWZ, że posiada systemy firmy Apple, nie udowodnił, że potrzebuje, aby sandbox objął również ochroną Mac OS. W ocenie Odwołującego prawdopodobne jest, że Zamawiający nie używa w ogóle systemów Apple w bieżącej działalności, a zgodnie z art. 29 ust. 1 ustawy Pzp Zamawiający powinien podać wszystkie okoliczności mogące mieć wpływ na sporządzenie oferty. Odwołujący wniósł o nakazanie Zamawiającemu opisania swojego środowiska informatycznego w stosunku, do którego ma być dostarczony sandbox, w tym określenia w SIWZ, czy i jakich systemów Mac OS i Microsoft używa Zamawiający, w tym wskazania liczby komputerów Apple, liczby użytkowników, rodzaju systemów: wersja, rok. Wskazał, iż Zamawiający może używać Microsoft nawet w ponad 95%, a dopiero pokazanie liczb, danych przez Zamawiającego pokaże tę proporcję i udowodni jak nieuzasadnione jest mieszanie w jednym postępowaniu Apple (Mac OS) z Microsoftem. Ponadto Odwołujący wniósł o zmianę pkt 3l.a) OPU i nadanie mu brzmienia: „Urządzanie musi posiadać zainstalowane maszyny wirtualne na których obywa się sandboxing zawierające: a) Obrazy systemów operacyjnych - minimum: Microsoft Windows 7 (w wersjach 32 i 64 bit), Microsoft Windows 10 64-bit, Mac OS (przy czym Mac OS może być uruchamiany (emulowany) w chmurze zamiast na urządzeniu lub w inny równoważny sposób)." Ewentualnie, w przypadku braku uwzględnienia tego żądania Odwołujący wniósł o usunięcie Mac OS z tego postanowienia i nadanie temu postanowieniu

brzmienia: „Urządzanie musi posiadać zainstalowane maszyny wirtualne na których obywa się sandboxing zawierające: a) Obrazy systemów operacyjnych - minimum: Microsoft Windows 7 (w wersjach 32 i 64 bit), Microsoft Windows 10 64-bit”.

Ponadto w zakresie pkt 3l OPU, odnośnie obrazów systemów operacyjnych Microsoft Windows, licencji Windows, MS Office, Odwołujący podniósł, iż według jego wiedzy Zamawiający ma zawartą umowę Enterprise Agreement z Microsoft w wyniku udzielania poprzednich zamówień publicznych, więc ma dostęp do licencji Windows i MS Office we własnym zakresie, za które już zapłacił w ramach innej umowy, a wymaga dostawy licencji Windows oraz MS Office w tym postępowaniu. Zdaniem Odwołującego wyeliminowanie tych kosztów z postępowania jest w interesie Zamawiającego - aby nie płacił dwa razy za to, za co już zapłacił w umowie z Microsoft (w ramach umowy Enterprise Agreement), zawartej w wyniku innych postępowań. Zamawiający opisał wymóg jak gdyby nie miał licencji enterprise, a powinien użyć licencji, które ma. Oczekiwanie dostarczenia dodatkowych licencji Microsoft można ocenić jako niegospodarne w tym zakresie i niewygodne dla Odwołującego, ponieważ żeby złożyć ofertę, trzeba również ustalić warunki z Microsoft (który poprzez swoich dystrybutorów może dać różne ceny różnym wykonawcom), co może zaburzyć konkurencję i uniemożliwić nam równe konkurowanie w przetargu. Tym samym wymóg dostawy licencji Windows oraz MS Office przez Wykonawcę w ramach postępowania dotyczącego sandbox jest nadmiarowy. W ocenie Odwołującego rezygnacja z dostarczania obrazów systemów Microsoft jest dodatkowo uzasadniona tym, że obrazy MS Windows dostarczane są przez wszystkich producentów sandbox w wersji angielskiej, a Zamawiający przecież używa Windows w wersji polskiej (co sprawia, że dostarczone obrazy będą bezużyteczne, bo i tak Zamawiający będzie używał swoich licencji w języku polskim). Ponadto w przypadku licencji OEM-owych (których Zamawiający wymaga) zachodzi ryzyko wykrycia przez malware licencji generycznej-sandboxowej i zastosowania technik unikania (evasion techniques), więc nie jest to preferowane rozwiązanie, bo nie zapewnia odpowiedniego bezpieczeństwa. Odwołujący wniósł o nakazanie Zamawiającemu określenia w SIWZ, czy i do jakich maszyn wirtualnych Microsoft ma dostęp w ramach umowy Enterprise Agreement (specyfikacja maszyn wirtualnych, dat obowiązywania umowy, wersji językowych do których ma dostęp), gdyż informacja taka ma wpływ na sporządzenie oferty. Ponadto Odwołujący zażądał usunięcia pkt a) z pkt 3.l, usunięcia wyrazów „Microsoft Office" z pkt b) w pkt 3.l; usunięcia wyrazów „systemów operacyjnych V z pkt c) w pkt 3.1. Po zmianach pkt 3.l OPU powinien mieć treść: „Urządzenie musi posiadać zainstalowane maszyny wirtualne na których obywa się sandboxing zawierające: a) usunięty b) Zainstalowane oprogramowanie narzędziowe minimum typu: Adobe Reader, Flash Player c) Wszystkie niezbędne licencje do zaproponowanego przez oprogramowania narzędziowego."

W zakresie pkt 4o OPU Odwołujący wskazał, iż urządzenia analizujące ruch sieciowy podłączane do sieci za pomocą TAPów lub analizujące ruch sieciowy ze SPAN portów same w sobie nie posiadają możliwości blokowania ruchu sieciowego. Odwołujący zażądał, aby Zamawiający dopuścił rozwiązanie, które będzie blokowało niebezpieczną komunikację poprzez integrację z innymi urządzeniami sieciowymi takimi jak Check Point, Pało Alto, IBM Security NetWork Protection czy TippingPoint. Odwołujący zakłada, że taki był cel Zamawiającego, skoro dopuścił zastosowanie TAPów i SPAN portów. Odwołujący wniósł o zmianę pkt 4o OPU i nadanie mu brzmienia: „Urządzenie musi blokować dany ruch w przypadku wykrycia zagrożenia pochodzącego z analizy sandboxowej. Blokowanie niebezpiecznej komunikacji może nastąpić przez integrację z innymi urządzeniami sieciowymi które posiada Zamawiający."

Odnośnie pkt 2e OPU Odwołujący wniósł o dopuszczenie przez Zamawiającego dostarczenia elementów zarządzania i raportowania w formie maszyn wirtualnych (virtual appliance), z zastrzeżeniem, że wszystkie elementy systemu będą tego samego producenta. Zażądał zmiany treści pkt 2e OPU na następującą: „System musi mieć element (pojedynczy serwer/interfejs zarządzający) zarządzający z poziomu którego można zarządzać elementami systemu, konfigurować je, przeglądać zdarzenia związane z sandboxingiem oraz generować raporty: elementy zarządzania i raportowania mogą być dostarczone w formie maszyn wirtualnych (virtual appliance).

W zakresie pkt 3a OPU Odwołujący wskazał, iż oczekuje, aby Zamawiający dopuścił dostarczenie rozwiązania, gdzie urządzenia mogą być dostarczone jako zestaw urządzeń z podziałem na poszczególne funkcjonalności (np. urządzenia do analizy ruchu pocztowego, urządzenia do analizy sandbox, urządzenia do logowania i raportowania), bo jest to korzystne dla Zamawiającego. Odwołujący wniósł o zmianę pkt 3a w następujący sposób: „Zamawiający wymaga dostarczenia, zainstalowania i skonfigurowania minimum dwóch fizycznych urządzeń do ochrony kanału pocztowego w sieci UKNF, przy czym urządzenia mogą być dostarczone jako zestaw urządzeń z podziałem na poszczególne funkcjonalności (np. urządzenia do analizy ruchu pocztowego, urządzenia do analizy sandbox, urządzenia do logowania i raportowania)".

W odniesieniu do pkt 3b OPU Odwołujący zażądał, aby Zamawiający zaakceptował rozwiązanie, w którym urządzenia realizujące sandboxing będą dostarczone w postaci zamkniętej platformy sprzętowej a inne elementy systemu mogą być dostarczone w formie maszyny wirtualnej - z zastrzeżeniem, że wszystkie elementy systemu będą tego samego producenta. Odwołujący wniósł o zmianę pkt 3b w następujący sposób: „Elementy Systemu odpowiedzialne za analizę wiadomości email pod kontem zaawansowanej analizy potencjalnie niebezpiecznego kodu (sandboxing) muszą być dostarczone w postaci

zamkniętej platformy sprzętowej. Zamawiający dopuszcza, by urządzenia realizujące sandboxing były dostarczone w postaci zamkniętej platformy sprzętowej, a inne elementy systemu mogą być dostarczone w formie maszyny wirtualnej - przy czym wszystkie elementy systemu będą tego samego producenta."

W zakresie pkt 3c OPU Odwołujący wskazał na brak danych odnośnie liczby jednoczesnych sesji http/https oraz liczby użytkowników systemu pocztowego oraz skrzynek pocztowych, którzy mają podlegać ochronie, co utrudnia określenie przedmiotu oferty i zaoferowanie odpowiedniej ceny, a OPU w tym zakresie jest nieokreślony. Odwołujący wniósł o określenie przez Zamawiającego w pkt 3 liczby jednoczesnych sesji http/https oraz liczby użytkowników systemu pocztowego oraz skrzynek pocztowych, którzy mają podlegać ochronie.

Niezależnie od powyższego Odwołujący wskazał, iż SIWZ jest sprzeczny z aktualnymi rekomendacjami dotyczącymi sporządzania SIWZ na systemy informatyczne, z których wynika, że zakazane jest pośrednie albo bezpośrednie ograniczanie konkurencji. Odwołujący wskazał także na sprzeczność SIWZ z orzecznictwem KIO. Zamawiający tak opisał wymagania, że faktycznie, między innymi, co do Mac OS powinien przeprowadzić wolną rękę (gdy wymaga uruchomienia, emulacji na urządzeniu zamiast w chmurze, co jest bezpodstawnym wymogiem), a co do reszty: przetarg nieograniczony. Wymóg uruchamiania (emulacji) na urządzeniu zamiast na chmurze eliminuje z przetargu innych producentów. Taki zbiór wymogów jaki zamawiający opisał stanowi niedozwolone łączenie w celu promowania FireEye. Zdaniem Odwołującego Zamawiający nie ma obiektywnej potrzeby by emulować Mac Os wyłącznie w urządzeniu a nie w chmurze, nie wymagać języka polskiego, łączyć w jednym postępowaniu Mac OS (Apple) i Microsoft, bo to jest korzystne wyłącznie dla FireEye. Wykonawca ma jedynie uprawdopodobnić, a nie udowodnić roszczenie. Przedmiot zamówienia powinien zostać opisany w taki sposób, żeby dopuszczać inne rozwiązania dostępne na rynku niż Fireeye. Zamawiający nie ma uzasadnionej potrzeby w żądaniu dostarczenia licencji, które ma (Microsoft). Zamawiający nie uzasadnił wyczerpująco, dlaczego, zdecydował się na wykluczenie innych rynkowych rozwiązań, ciężar dowodu jest po stronie Zamawiającego. W ocenie Odwołującego Zamawiający ma prawo nabyć produkt zaspokajający jego potrzeby, jednak żądane cechy tego produktu muszą być uzasadnione jego racjonalnymi potrzebami, a nie nieuzasadnione. Przedmiotem zamówienia nie jest rozbudowa, nie ma więc żadnego powodu, aby SIWZ rzeczywiście dopuszczało tylko jedno z rozwiązań dostępnych na rynku (rozpracowane przez hakerów, nie zapewniające bezpieczeństwa) bez dopuszczenia innych, bez racjonalnej argumentacji, bez prawdziwych potrzeb.

Zamawiający w dniu 4 stycznia 2021 r. złożył pisemną odpowiedź na odwołanie, w której wniósł o oddalenie odwołania w całości jako niezasadnego.

Zdaniem Zamawiającego Odwołujący w sposób bezpodstawny zarzuca Zamawiającemu brak kompetencji, nieznajomość przepisów prawa, a także w niedopuszczalny sposób próbuje narzucić Zamawiającemu rozwiązania nie spełniające uzasadnionych potrzeb Zamawiającego, samemu prezentując brak rozeznania w obszarze cyberbezpieczeństwa lub wręcz celowo próbując manipulować faktami, stwierdzeniami oraz przytoczonymi przykładami w celu wprowadzenia w błąd KIO, powołując się na nierzetelne opracowania oraz źródła internetowe, próbując zdyskredytować przygotowane przez specjalistów Zamawiającego postępowanie. Odwołujący realizując swoje partykularne interesy, tj. w celu sprzedaży produktu/rozwiązania, które posiada w swojej ofercie, ale które najwidoczniej nie spełnia w pełnym zakresie wymagań określonych przez Zamawiającego w treści SIWZ, próbuje wymusić na Zamawiającym odstąpienie od wymagań podyktowanych interesem publicznym oraz uzasadnionymi i obiektywnymi potrzebami Zamawiającego, w tym w szczególności związanymi z realizacją zadań związanych z kwestiami bezpieczeństwa systemu finansowego Państwa. Powyższe naraża Zamawiającego na ryzyka naruszenia bezpieczeństwa danych i informacji, w tym tajemnic chronionych przepisami prawa, przetwarzanych w systemach teleinformatycznych Zamawiającego, jak również w systemach profesjonalnych i nieprofesjonalnych uczestników rynku finansowego. Zamawiający powołał się na orzecznictwo KIO odnoszące się do opisywania przedmiotu zamówienia. Podkreślił, że zgodnie z art. 29 ust. 1 ustawy Pzp, dokonał opisania przedmiotu zamówienia w SIWZ w sposób jednoznaczny i wyczerpujący, za pomocą dostatecznie dokładnych i zrozumiałych określeń, uwzględniając wszystkie wymagania i okoliczności mogące mieć wpływ na sporządzenie oferty. Opisany przez Zamawiającego przedmiot zamówienia, czyni zadość wymogom art. 29 ust 1 ustawy Pzp i w żaden sposób nie utrudnia uczciwej konkurencji.

Zamawiający podkreślił, że nie istnieją na rynku rozwiązania umożliwiające realizację przedmiotu zamówienia tylko i wyłącznie dla systemów Mac OS (Apple), a co za tym idzie Zamawiający musiałby wydatkować kolejne środki finansowe na rozwiązanie tożsame z przedmiotem niniejszego zamówienia, tj. realizujące określone w przedmiocie zamówienia zadania, zarówno dla systemów MS Windows jak i Mac OS (Apple). Żądane przez Odwołującego dokonanie podziału zamówienia spowodowałoby zdublowanie zakupionego rozwiązania informatycznego (o analogicznych funkcjonalnościach w odniesieniu do systemów MS Windows), a co za tym idzie doprowadziłoby do ewidentnej niegospodarności i nieracjonalnego gospodarowania środkami publicznymi, ponieważ wymagałoby zakupu kolejnych nowych urządzeń lub rozwiązań informatycznych do obsługi kanału pocztowego i kanału www wraz z nowym systemem zarzadzania, monitoringu i raportowania. Żądane

przez Odwołującego rozdzielenie zamówienia doprowadziłoby do sytuacji, w której Zamawiający niegospodarnie, wykorzystując publiczne środki finansowe zakupiłby dwa rozwiązania realizujące te same zadania. Wdrożenie dwóch rozwiązań narusza zasadę celowego i racjonalnego gospodarowania publicznymi środkami finansowymi także w związku z koniecznością zapewnienia (rozumianego jako zatrudnienie lub podnoszenie kwalifikacji) dodatkowych zasobów osobowych związanych z utrzymaniem obu rozwiązań Ponadto Zamawiający, realizując postulaty Odwołującego, musiałby używać dwóch niezgodnych i niekompatybilnych ze sobą systemów pochodzących od różnych producentów, służących do wykonywania sandboxingu, gdyż, jak wskazano już wcześniej, na rynku nie ma rozwiązania dedykowanego tylko i wyłącznie pod analizę systemu Mac OS. W tym kontekście co najmniej nietrafiona jest także sugestia Odwołującego, iż rozwiązanie takie Zamawiający miałby kupić w trybie zamówienia z wolnej ręki - nie da się kupić, nawet w trybie niekonkurencyjnym, czegoś co obiektywnie nie istnieje. Zamawiający musiałby stosować wiele rozwiązań mimo, iż na rynku istnieją rozwiązania (co najmniej 2), które zapewniającą kompleksową, jednoczesną ochronę maszyn pracujących na systemach MS Windows i Mac OS. Zamawiający musiałby wykonać szkolenia z administrowania i utrzymania tych produktów dla swoich pracowników, zapewniać wsparcie dla tych systemów, odnawianie licencji oraz zaangażować dodatkowe zasoby ludzkie do ich efektywnej obsługi. Także przez pryzmat bezpieczeństwa nie byłoby między nimi takiej wymiany i korelacji informacji, jaka ma miejsce w systemie jednolitym, pochodzącym od jednego producenta.

Zamawiający wyjaśnił, że nie ma znaczenia liczba posiadanych urządzeń w kontekście wykorzystywanych na nich systemów, ale sam fakt wykorzystywania wskazanych w opisie przedmiotu zamówienia różnych systemów w infrastrukturze teleinformatycznej Zamawiającego. Zamawiający posiada także urządzania pracujące pod kontrolą Mac OS (a nie jedynie Microsoft Windows), które służą do realizacji zadań służbowych (dotyczących także przetwarzania informacji prawnie chronionych) przez pracowników Zamawiającego i dla nich również wymagane jest zachowanie ochrony na tak samo wysokim poziomie. Wskazał, iż szeroko pojęte standardy cyberbezpieczeństwa, nie dopuszczają traktowania bezpieczeństwa w aspekcie ilościowym, nawet jedno urządzenie Zamawiającego nie objęte ochroną może wpłynąć negatywnie na bezpieczeństwo wszystkich systemów teleinformatycznych Zamawiającego, a także co bardzo istotne podmiotów działających na polskim rynku finansowym. Zamawiający wskazał ponadto, iż rozpatrywanie kwestii przedmiotowego zamówienia publicznego musi być prowadzone w odniesieniu do ustrojowej pozycji i roli Zamawiającego w systemie finansowym Państwa, jego roli w krajowym systemie cyberbezpieczeństwa, a także jego zadań ustawowych oraz specyfiki pracy. Zamawiający opisał zadania Komisji Nadzoru Finansowego, podnosząc, że realizuje szereg zadań

wspierających i zapewniających możliwość wykonywanie zadań i kompetencji przez KNF, m.in. prowadząc stałą wymianę informacji, zarówno ze wszystkimi podmiotami polskiego rynku finansowego, których w ogólnym rozrachunku jest około 1200, jak również z klientami tych instytucji, tj. klientami banków, instytucji sektora ubezpieczeniowego, kapitałowego, SKOK, KIP oraz MIP. Z informacji nadzorczych posiadanych przez Urząd KNF wynika, że zarówno profesjonalni (rozumiani jako podmioty polskiego rynku finansowego), jak i nieprofesjonalni uczestnicy (tj. klienci) rynku finansowego korzystają z rozwiązań finny Apple. Jednocześnie Zamawiający wskazał, iż zgodnie z zapisami ustawy o krajowym systemie cyberbezpieczeństwa KNF jako organ właściwy realizuje szereg zadań nadzorczych i wspierających wobec szczególnie istotnych z punktu widzenia państwa polskiego podmiotów rynku finansowego, wskazanych ustawą jako Operatorzy Usług Kluczowych.

Zamawiający mając świadomość swojej roli organu nadzoru oraz organu właściwego jak również ryzyka związanego z obszarem cyberbezpieczeństwa, tak zaplanował i prowadzi przedmiotowe postępowanie przetargowe, aby oprócz ochrony własnych zasobów informacyjnych, wykazując dojrzałość i świadomość w obszarze cyberbezpieczeństwa, ograniczyć ryzyko oraz zapewnić bezpieczeństwo i chronić również uczestników rynku finansowego, tj. podmioty rynku finansowego oraz ich klientów. W sytuacji, w której Zamawiający zrezygnowałby z ochrony systemów operacyjnych Mac OS (Apple), które są wykorzystywane przez niego do działalności operacyjnej i z których to rozwiązań korzystają także nadzorowane podmioty rynku finansowego, istnieje prawdopodobieństwo materializacji ryzyka, polegającego na otrzymaniu oraz - w wyniku nie posiadania odpowiednie infrastruktury chroniącej systemy operacyjne Mac OS (Apple) - dalszej nieświadomej dystrybucji złośliwego oprogramowania do polskich instytucji finansowych, w wyniku czego Zamawiający mógłby ponieść niepoliczalne straty wizerunkowe i w konsekwencji narazić w/w podmioty rynku finansowego na nieokreślone straty zarówno wizerunkowe, jak i finansowe. Zamawiający przedstawił także argumentację wskazującą na istnienie realnego zagrożenia dla systemów Mac OS (Apple) Zamawiający podkreślił, że wymaga dostarczenia systemu do ochrony wszystkich systemów, na jakich pracują jego pracownicy. W związku z tym bezpodstawne jest twierdzenie, że Zamawiający połączył niszowe rozwiązanie z dominującym, ponieważ ochronie podlegać ma każdy system używany przez Zamawiającego Zamawiający zauważył także, że przedmiot zamówienia jest jednolity i nie przewiduje różnorodnych świadczeń, które uzasadniałyby podział zamówienia na części.

Odnosząc się do żądania dotyczącego przetwarzania danych w chmurze obliczeniowej, Zamawiający wskazał, iż jest ono niedopuszczalne nie tylko z punktu widzenia obowiązujących przepisów oraz ochrony interesów Zamawiającego, ale także interesów podmiotów rynku finansowego, na rzecz których Zamawiający realizuje zadania publicznie.

Zamawiający wymienił rodzaje informacji podlegających ustawowej ochronie, które są przetwarzane w jego infrastrukturze, wskazując, iż gdyby zrealizować żądanie Odwołującego, to informacje te musiałby być przetwarzane poza tą infrastrukturą, gdyż system analizujący m.in. pocztę mailową przetwarzałby te dane i informacje (w tym tajemnice prawnie chronione) w celu ich analizy w chmurze obliczeniowej. Obowiązujące przepisy prawa nie dają Zamawiającemu podstawy prawnej do powierzenia ich dalszego przetwarzania przez podmioty trzecie. Ponadto kwestie przetwarzania danych (w tym tajemnic prawnie chronionych) w chmurze obliczeniowej dotykają również kwestii umożliwienia dostępu do tych danych (w tym tajemnic prawnie chronionych) nie tylko dostawcy oprogramowania sandbox, ale również jego ewentualnym poddostawcom, co z punktu widzenia prawa jest niedopuszczalne. Zamawiający zwrócił także uwagę na Narodowe Standardy Cyberbezpieczeństwa - Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO), gdzie wskazano, iż ze względu na wrażliwość niektórych informacji mogą być one przechowywane i przetwarzane tylko w środowisku Rządowej Chmury Obliczeniowej (Poziom SCCO3, do którego należy zaliczyć informacje prawnie chronione, wskazane przez Zamawiającego). Zamawiający wyjaśnił, że jednostki administracji publicznej nie mogą przetwarzać tego rodzaju informacji z wykorzystaniem usług publicznych chmur obliczeniowych, nawet pod warunkiem spełnienia przez dostawcę danych usług organizacyjnych i technicznych wymagań SCCO, brak jest podstawy prawnej do powierzenia przetwarzania krytycznych z punktu widzenia rynku finansowego danych i informacji (w tym informacji prawnie chronionych) podmiotom, które będą przetwarzały te dane w chmurze obliczeniowej, udostępniając je podmiotom realizującym na ich rzecz zadania związane np. z utrzymaniem rozwiązań chmurowych. Stąd celowo, mając na względzie powyższe, Zamawiający wskazał na konieczność przetwarzania ww. danych i informacji (w tym informacji prawnie chronionych) w infrastrukturze Zamawiającego, a nie w rozwiązaniu chmurowym. Nie stanowi to pozornej potrzeby Zamawiającego ani nie służy ograniczeniu konkurencji - tego typu rozwiązania (systemy) istnieją na rynku, a to, że akurat Odwołujący nimi nie dysponuje nie powinno wpływać na treść SIWZ i wymagania Zamawiającego.

Zamawiający podniósł, iż zgodnie ze stanem jego wiedzy na rynku istnieją co najmniej dwa rozwiązania spełniające wymogi, co do systemów operacyjnych zawartych w opisie przedmiotu zamówienia. Zamawiający nie precyzował wymogów pod kątem konkretnego producenta systemów, tylko w sposób rzetelny i kompleksowy, a także obiektywny, opisał swoje potrzeby, uwzględniające jego ustawowe zadania, zakres działania, pozycję ustrojową oraz istotną rolę w systemie finansowym państwa, uwzględniając także zakres i charakter danych i informacji (w tym informacji prawnie chronionych) przetwarzanych w systemach teleinformatycznych Zamawiającego. Ponadto zaznaczył, iż wskazane przez Odwołującego

urządzenia - 2 sztuki EX 3500 oraz 2 sztuki NX 4500 w ocenie Zamawiającego również nie spełniają wszystkich wymogów postawionych w opisie przedmiotu zamówienia, ponieważ zgodnie z jego zapisami Zamawiający wymagał również obsługi interfejsu API, zarządzania, obsługi zdarzeń i generowania raportów. Zdaniem Zamawiającego celem Odwołującego nie jest przeciwdziałanie ograniczeniu konkurencji, które w przedmiotowej sprawie w ogóle nie wystąpiło, tylko dostosowanie wymagań określonych w SIWZ do systemów oferowanych przez Odwołującego. Zamawiający zauważył także, że żaden z innych wykonawców nie przystąpił do odwołania po stronie Odwołującego, jak również nie wniósł odwołania, co budzi wątpliwości co do prawdziwości twierdzeń Odwołującego, w szczególności tych sugerujących, że taki opis przedmiotu zamówienia wskazuje na produkt firmy FireEye i uniemożliwia zaoferowanie rozwiązań przez inne firmy.

Zamawiający wskazał także, że nie precyzował w SIWZ kryteriów jakościowych rozwiązania, odnoszących się czy pozycjonujących oferowany produkt wobec innych produktów z danej kategorii. Używanie w tym przypadku przez Odwołującego argumentów wskazujących na wyższość jednego produktu nad drugim jest bezzasadne i bez znaczenia dla przedmiotu sprawy. Twierdzenia Odwołującego, bez podania kontekstu całego zdarzenia, stanowią manipulację faktami. Artykuły wskazane przez Odwołującego pochodzą z pierwszych dni po wykryciu incydentu bezpieczeństwa przez firmę FireEye, której bezpieczeństwo zostało naruszone w wyniku działań cyberprzestępców wykorzystujących lukę bezpieczeństwa w oprogramowaniu firmy trzeciej, a nie firmy FireEye. Firma FireEye stała się ofiarą cyberprzestępstwa tak, jak pozostała nieustalona na dzień dzisiejszy liczba firm, organizacji i instytucji rządowych korzystających z zainfekowanego oprogramowania firmy trzeciej (nie firmy FireEye). Oprócz firmy FireEye ofiarami tego incydentu mogło paść około 18 tys. firm, organizacji oraz instytucji publicznych korzystających z oprogramowania firmy trzeciej tj. SolarWinds. Zamawiający zauważył, że o właśnie firma FireEye jako pierwsza wykryła przytoczony tu incydent, co świadczy o jej doświadczeniu i zaawansowaniu technologicznym Przytaczany przez Odwołującego incydent jest obecnie uznawany za największy i najpoważniejszy incydent bezpieczeństwa związany z działalnością cyberprzestępczą, które obecnie uznawane jest za akt cyberszpiegostwa, tj. atak przeprowadzony przez grupę/grupy cyberprzestępcze związane z rządem jednego z państw

Odnosząc się do wymagania z pkt 2f OPU Zamawiający wskazał, iż żądanie Odwołującego dostarczenia licencji na systemy operacyjne w języku polskim ogranicza konkurencję. Wyjaśnił, iż celowo nie wskazywał języka, w jakim mają być dostarczone obrazy systemów operacyjnych na potrzeby emulacji dla maszyn wirtualnych, aby nie ograniczać konkurencyjności Od wielu lat Zamawiający korzysta z rozwiązania realizującego zadania sanboxingu, w którym używane są obrazy angielskich systemów operacyjnych, na

których wykonywana jest analiza danych na potrzeby wykrywania zagrożeń cyberbezpieczeństwa, w związku z tym twierdzenie, że kupi „bezużyteczne elementy" jest nieprawdziwe. Zdaniem Zamawiającego nieprawdziwe są także argumenty, że oprogramowanie w języku polskim zapewni bezpieczeństwo większe, niż w innym języku. Tym bardziej, że, jak wskazał sam Odwołujący, poprawki bezpieczeństwa dla języka polskiego i innych języków są dostarczane w różnym czasie. Zamawiający podkreślił, że to właśnie poprawki dla systemów polskojęzycznych dostarczane są później, gdyż natywnym językiem systemu Microsoft Windows jest język angielski.

W zakresie pkt 3l OPU Zamawiający podtrzymał wcześniejszą argumentację odnoszącą się do systemu Mac OS i przetwarzania danych i informacji w chmurze obliczeniowej. Dodał, że argumenty o tym, że rozwiązania firmy Apple są rzadko stosowane w Polsce, są drogie i niszowe, są nie tylko jedynie własnym poglądem Odwołującego, nie popartym żadnymi dowodami. Zamawiający wskazał, iż dokonał analizy wykorzystania przez uczestników rynku finansowego, korzystających z rozwiązań Apple, zasobów i systemów informatycznych Zamawiającego dostępnych w Internecie, tj. strony www Zamawiającego i dostępnych dla uczestników rynku finansowego dedykowanych systemów. Statystyki wskazują na generowanie przez systemy Apple zapytań do systemów teleinformatycznych Zamawiającego na poziomie ok. 12 tys. zapytań dziennie przy całościowej liczbie zapytań ok. 300 tys. dziennie. Zamawiający dodał także, że kryteria ilościowe w odniesieniu do kwestii systemów bezpieczeństwa nie mają zastosowania w przypadku celu realizowanego przez przedmiot niniejszego zamówienia, w związku z tym postulat o wykazanie liczby systemów Microsoft i Mac OS (Apple) jest bezzasadnym wnioskiem Odwołującego - taka informacja nie niesie żadnej wartości dodanej, ani nie jest potrzebna do przygotowania oferty, o czym podmiot profesjonalnie działający na danym rynku winien wiedzieć. Zamawiający wskazał, iż opis środowiska informatycznego Zamawiającego zawarty został w opisie przedmiotu zamówienia i jest on wystarczający do przygotowania oferty. Urządzenia wykonujące sandboxing powołują na bieżąco maszyny wirtualne i wykonują na nich analizy. Rodzaj analizy związany jest wyłącznie z przesyłanymi (otrzymywanymi z zewnątrz) danymi (plikami, linkami, stronami www) nie zaś, jak sugeruje Odwołujący, liczbą komputerów, liczbą użytkowników, rodzajem systemu MAC OS/MS Windows, czy tym bardziej ich wersji i dat wydania. Kryteria ilościowe w odniesieniu do kwestii systemów bezpieczeństwa nie mają zastosowania, ponieważ ważne jest wykonanie analizy plików dla wszystkich urządzeń posiadanych przez Zamawiającego. Infekcja dowolnego (nawet pojedynczego) komputera stanowi nieakceptowalne z punktu widzenia ochrony danych i informacji (w tym informacji prawnie chronionych) przetwarzanych przez Zamawiającego ryzyko, dlatego wychwycenie zainfekowanych plików, w jak największym spektrum, jest z punktu widzenia Zamawiającego

krytyczne i dotyczy równorzędnie systemów Mac OS (Apple) jak i Microsoft Windows. Podanie informacji, których żąda Odwołujący nie jest potrzebne do przygotowania i wyceny, Odwołujący wymaga od Zamawiającego ujawnienia danych nie związanych z przedmiotowym postępowaniem.

Odnośnie pkt 3l OPU, w zakresie dotyczącym obrazów systemów operacyjnych Microsoft Windows, licencji Windows, MS Office, Zamawiający wskazał, iż w umowie Enterprise Agreement nie ma zapisów umożliwiających wykorzystanie licencji dla urządzeń dostarczonych przez inne podmioty w ramach innych umów, a tylko na urządzania używane przez Zamawiającego. Na urządzeniach sandboxa maszyny wirtualne powoływane są za każdym razem automatycznie na dany czas analizy, umowa Enterprise Agreement nie obejmuje swoim zakresem tego typu używania licencji. Ponadto przywołana przez Odwołującego umowa Enterprise Agreement dotyczy obrazów w języku polskim, a jak wykazano i uzasadniono powyżej Zamawiający dopuszcza też analizy sandboxowe na obrazach angielskojęzycznych. Według umowy zużycie licencji musi być rejestrowane i monitorowane, a w przypadku rodzaju systemu, którego dotyczy przedmiotowe postępowanie przetargowe, niemożliwe jest określenie ilości maszyn które będą powoływane do życia, gdyż jest to liczba zmienna i zgodnie z szacunkami Zamawiającego oscyluje ona od 0 do 13000 maszyn wirtualnych dziennie. Użycie maszyn na potrzeby sandboxingu nie zostało ujęte w umowie Enterprise Agreement, która to umowa ekspiruje wcześniej niż planowany zakup sytemu sandboxingu. Zamawiający wskazał także, iż licencje musza być dostarczone z uwagi na to, żeby Zamawiający używał produktów zakupionych legalnie i nie łamiąc prawa autorskiego w stosunku do produktów, do jakich mają one zastosowanie. Żądania formułowane przez Odwołującego nie stoją w zgodzie z interesem i uzasadnionymi obiektywnymi potrzebami Zamawiającego.

Zdaniem Zamawiającego nie jest uzasadnione także żądanie Odwołującego w zakresie wykluczenia pakietu MS Office, ponieważ uniemożliwi w analizie sandboxowej sprawdzenie działania plików bazujących na tym właśnie pakiecie narzędzi biurowych, w związku z tym spowoduje drastyczny spadek wykrywalności złośliwego oprogramowania, narażając Zamawiającego na nieakceptowalne ryzyko. Takie działanie w ocenie Zamawiającego stanowi próbę wymuszenia ograniczenia przedmiotu zamówienia poprzez eliminacje zapisów dot. pakietu MS Office, którego zgodnie z publicznie dostępnymi statystykami firmy Kaspersky, w III kwartale 2019 r. dotyczyło 73 % wszystkich cyberataków, gdzie odsetek ten w I kwartale 2020 r. wynosił już niemal 75 %, a także świadczy o braku znajomości tematu skali zagrożeń cyberbezpieczeństwa przez Odwołującego. Skala ataków na oprogramowanie MS Office jednoznacznie wskazuje, że eliminacja tego zapisu podważa sens wykonywania

analizy sandboxowej, w której pliki nie są uruchamiane w środowisku najbardziej zbliżonym do rzeczywistego.

Odnośnie pkt 4o Zamawiający wskazał na nieprawdziwość twierdzeń Odwołującego, ponieważ Zamawiający zgodnie z zapisami SIWZ dopuszcza rozwiązanie polegające na blokowaniu ruchu przez zastosowanie innych elementów sieciowych (posiadanych przez Zamawiającego bądź też dostarczonych przez wykonawcę) z zastrzeżeniem, że wykonawca wykona ich pełną konfigurację w zakresie tej funkcjonalności oraz dostarczy wszelkie wymagane licencje do realizacji tego zadania.

Odnośnie pkt 2e Zamawiający wskazał, iż zgodnie z SIWZ elementy związane z zarzadzaniem i raportowaniem mogą być dostarczone w formie maszyn wirtualnych, natomiast pozostałe elementy oferowanego rozwiązania muszą być urządzeniami fizycznymi.

W zakresie pkt 3a Zamawiający podniósł, iż wymaga dostarczenia dwóch fizycznych urządzeń do ochrony kanału pocztowego pod względem sandboxingu, natomiast cały System musi być zarządzany oraz posiadać raportowanie i logowanie zdarzeń, wskazane w szczególności w pkt 2e. opisu przedmiotu zamówienia. W odniesieniu do pkt 3b Zamawiający podtrzymał prezentowaną już argumentację. Odnośnie pkt 3c Zamawiający wskazał, iż w opisie przedmiotu zamówienia nie ma zapisu o SPAN portach do ochrony poczty, a w pkt 3. ppkt h. i ppkt d. jest określona ilość skrzynek pocztowych wymaganych do ochrony poczty oraz tryb pracy MTA wymagany przez Zamawiającego. Wymagania stawiane przez Odwołującego dotyczące przedstawienia ilości sesji http/https w stosunku do analizy pocztowej świadczy o braku wiedzy technicznej oraz budzi wątpliwości Zamawiającego co do rozwiązania, które potencjalnie pragnie zaoferować Odwołujący do ochrony skrzynek pocztowych bazującego na ilości sesji http/https - jako spełniającego nie tylko wymagania postawione w SIWZ, ale w ogóle jako narzędzia realizującego skutecznie cele, jakie winien realizować system sandboxingu.

Zamawiający wskazał ponadto, iż Odwołujący przytacza orzecznictwo KIO, które nie jest adekwatne do przedmiotu zamówienia. Nie można mówić o połączeniu w niniejszym postępowaniu zakupu, którego można dokonać w trybie konkurencyjnym z innym zakupem, którego można dokonać w trybie zamówienia z wolnej ręki, gdyż nie istnieje system sandboxingu, który realizowałby stawiane mu cele wyłącznie w odniesieniu do systemów Mac OS, nie da się kupić, nawet w trybie niekonkurencyjnym, czegoś co obiektywnie nie istnieje. Zamawiający podkreślił, że Odwołujący próbuje narzucać Zamawiającemu podejście do kwestii bezpieczeństwa oraz rozwiązania stosowane w tym zakresie, podczas gdy to Zamawiający odpowiada za zapewnienie bezpieczeństwa swoich systemów teleinformatycznych i zna wymaganie oraz ryzyka ich dotyczące. Zamawiający przy

przeprowadzaniu analizy ryzyka dot. bezpieczeństwa danych i informacji (w tym informacji prawnie chronionych) przetwarzanych w systemach teleinformatycznych Zamawiającego bierze pod uwagę m.in. zdarzające się w przeszłości incydenty bezpieczeństwa. Biorąc pod uwagę, że w jeden z takich incydentów bezpieczeństwa (najpoważniejszy w ostatnim roku, związany z danymi i informacjami o charakterze sensytywnym) były zaangażowane osoby wykonujące prace na rzecz Odwołującego, realizującego umowę dla Zamawiającego, nie sposób ograniczać i modyfikować wymagań Zamawiającego w przedmiotowym zakresie pod wytyczne wykonawców. Zamawiający wyjaśnił, że przytoczony incydent bezpieczeństwa stał się przedmiotem zawiadomienia o podejrzeniu popełnienia przestępstwa oraz w jego następstwie postępowania wyjaśniającego prowadzonego przez prokuraturę.

W ocenie Zamawiającego Odwołujący, nie mogąc najwyraźniej spełnić wymogów Zamawiającego, w sposób nierzetelny i niejasny próbuje wymusić zakup rozwiązania nie spełniającego uzasadnionych potrzeb Zamawiającego, podejmując nawet próbę nieuprawnionego redefiniowania tych potrzeb. Zamawiający podkreślił, że uwzględnienie postulatów Odwołującego powodowałoby niegospodarność poprzez zakup dwóch różnych rozwiązań pokrywających się funkcjonalnościami, co skutkowałoby koniecznością wydatkowania dodatkowych środków finansowych na zakup i utrzymanie dwóch rozwiązań, zatrudnienie dodatkowych osób do obsługi dwóch systemów oraz ich przeszkolenia. Doprowadziłoby także do ekspozycji na ryzyko cyberataku na urządzenia Mac OS (Apple), nie tylko w infrastrukturze Zamawiającego (co wygenerowałoby niepoliczalne straty wizerunkowe oraz finansowe), ale również profesjonalnych i nieprofesjonalnych uczestników rynku finansowego (tj. podmioty rynku finansowego oraz ich klientów), którzy narażeni byliby na atak w sytuacji, w której Zamawiający nie posiadający narzędzi do wykrywania takich ataków, w toku realizacji zadań ustawowych doprowadziłby do zainfekowania komputerów Mac OS (Apple) zewnętrznych uczestników rynku finansowego (np. banków lub ich klientów). Ponadto doprowadziłoby do naruszenia przepisów prawa w wyniku udostępnienia szeregu tajemnic oraz danych i informacji wrażliwych, przetwarzanych obecnie w infrastrukturze teleinformatycznej Zamawiającego, podmiotom zewnętrznym, które przetwarzałyby ww. tajemnice i informacje wrażliwe w chmurze obliczeniowej, udostępniając te zasoby chmurowe również innym klientom tych podmiotów oraz nieznanym poddostawcom realizującym na rzecz tych dostawców różnego rodzaju prace wspierające. Doprowadziłoby również w efekcie do faktycznego ograniczenia konkurencji w sytuacji, w której Zamawiający wymagałby dostarczenia licencji na systemy operacyjne tylko w języku polskim. A do tego doprowadziłoby do wyeliminowania krytycznej z punktu widzenia Zamawiającego funkcjonalności analizy plików pakietu MS Office, które, jak wykazano powyżej opierając się na analizach firm zajmujących się zwalczaniem cyberzagrożeń, są

głównym celem ataków cyberprzestępców, co z kolei naraziłoby Zamawiającego na ryzyko ataku i utraty bezpieczeństwa danych i informacji (w tym informacji prawnie chronionych) przetwarzanych w systemach teleinformatycznych Zamawiającego.

Po przeprowadzeniu rozprawy z udziałem Stron postępowania, na podstawie zgromadzonego w sprawie materiału dowodowego oraz oświadczeń i stanowisk Stron postępowania, Krajowa Izba Odwoławcza ustaliła i zważyła, co następuje:

Mając na uwadze treść art. 92 ust. 1 ustawy z dnia 11 września 2019 r. Przepisy wprowadzające ustawę - Prawo zamówień publicznych (Dz.U. z 2019 poz. 2020), zgodnie z którym do postępowań odwoławczych, o których mowa w uchylanej ustawie, wszczętych i niezakończonych przed dniem 1 stycznia 2021 r. stosuje się przepisy dotychczasowe, Izba w przedmiotowej sprawie zastosowała przepisy ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t.j. Dz. U. z 2019 r. poz. 1843 ze zm.).

Izba ustaliła, iż w terminie wynikającym z art. 185 ust. 2 ustawy Pzp do postępowania odwoławczego nie zgłosił przystąpienia żaden wykonawca.

Izba stwierdziła, iż nie została wypełniona żadna z przesłanek skutkujących odrzuceniem odwołania na podstawie art. 189 ust. 2 ustawy Pzp i skierowała odwołanie do rozpoznania na rozprawie.

Izba uznała, iż Odwołujący wykazał interes w uzyskaniu zamówienia oraz możliwość poniesienia szkody w związku z ewentualnym naruszeniem przez Zamawiającego przepisów ustawy Pzp, czym wypełnił materialnoprawne przesłanki dopuszczalności odwołania, o których mowa w art. 179 ust. 1 ustawy Pzp. Mając na względzie, iż Odwołujący deklaruje zainteresowanie przedmiotowym postępowaniem jako podmiot trudniący się usługami objętymi przedmiotem zamówienia, Izba uznała, iż sposób ukształtowania postanowień SIWZ, w tym opisu przedmiotu zamówienia, może przekładać się na jego sytuację w postępowaniu i możliwość złożenia konkurencyjnej oferty, a tym samym Odwołującemu nie sposób odmówić uprawnienia do wniesienia środka ochrony prawnej w postaci odwołania.

Izba dopuściła i przeprowadziła dowody z dokumentacji postępowania o udzielenie zamówienia przekazanej przez Zamawiającego, w szczególności specyfikacji istotnych warunków zamówienia i jej załączników. Skład orzekający Izby wziął pod uwagę również stanowiska i oświadczenia Stron złożone w pismach procesowych (odwołanie, odpowiedź na odwołanie) oraz ustnie do protokołu posiedzenia i rozprawy w dniu 4 stycznia 2021 r. Ponadto Izba dopuściła i przeprowadziła dowody z dokumentów przedstawionych przez Strony na rozprawie, tj.:

I. dowody złożone przez Odwołującego:

1. odpis oświadczenia firmy Trend Micro z dnia 28 grudnia 2020 r.

2. wydruk karty katalogowej produktu Deep Discovery Analyzer firmy Trend Micro (wraz z tłumaczeniem);
3. wydruk korespondencji e-mail pomiędzy Odwołującym a Trend Micro;
4. wydruk ogłoszenia o zamówieniu z dnia 6 grudnia 2018 r. (2018/S 235-536945) oraz SIWZ dla postępowania prowadzonego przez Zamawiającego na rozbudowę systemów ochrony serwerów posiadanych przez UKNF;
5. odpis oświadczenia firmy Fortinet Inc. z dnia 28 grudnia 2020 r.;
6. wydruk ogłoszenia o zamówieniu z dnia 15 grudnia 2020 r. (2020/S 244-604807) oraz SIWZ dla postępowania prowadzonego przez Zamawiającego na zakup licencji dla systemu NGFW wraz ze wsparciem;
7. wydruk SIWZ dla postępowania prowadzonego przez Zamawiającego na wdrożenie Systemu DLP (DAL.WZP.2610.4.2019);
8. wydruk ze strony https://ezamowienia.ms.gov.pl dotyczący postępowania prowadzonego przez Ministerstwo Sprawiedliwości na dostawę rozwiązania informatycznego obejmującego funkcjonalność wykrywania i reakcji na zagrożenia, zapewniającą ochronę stacji roboczych i serwerów przed atakami oraz świadczenie innych usług (WZP-421-10/2020), wydruk opisu przedmiotu zamówienia dla tego postępowania oraz zbiorczego zestawienie ofert;
9. wydruk fragmentów informacji o wynikach kontroli NIK „Wykorzystanie jednolitego pliku kontrolnego w postępowaniach i kontrolach podatkowych”;
10. wydruk odpowiedzi Ministra Finansów na interpelację nr 28436;
11. wydruk Komunikatu KNF dotyczącego przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej (ze zmianą z 26 marca 2020 r.);
12. wydruk licencji ze strony https://apple.com;
13. wydruk analizy porównawczej produktów Trend Micro Deep Discovery oraz FireEye (wraz z tłumaczeniem);
14. wydruki prezentacji i testów produktów dokonanych przez NSS Labs (wraz z tłumaczeniem);
15. wydruk recenzji ze strony www.gartner.com dotyczący oprogramowania typu sandboxing (wraz z tłumaczeniem);
16. wydruk artykułu z portalu DarkReading dotyczący ataku hakerskiego na FireEye (wraz z tłumaczeniem);
17. wydruk artykułu ze strony www.biznes.wprost.pl „Gigant od cyberbezpieczeństwa padł ofiarą hakerów”;
18. wydruk artykułu ze strony www.nytimes.com dotyczący ataku hakerskiego na firmę FireEye (wraz z tłumaczeniem);

19. oświadczenie Fortinet Inc. z dnia 28 grudnia 2020 r.

II. dowody złożone przez Zamawiającego:

1. wydruk artykułu ze strony www.crn.pl „Zaawansowana ochrona przed zagrożeniami z Juniper Networks";
2. wydruk informacji ze strony www.joesecurity.org dotyczących produktu JoeSandbox Complete (wraz z tłumaczeniem);
3. wydruk informacji ze strony www.joesecurity.org dotyczących produktu JoeSandbox Ultimate (wraz z tłumaczeniem);
4. wydruk dokumentu dotyczącego urządzenia ATP (Advanced Threat Prevention) Juniper Networks (wraz z tłumaczeniem oznaczonych fragmentów);
5. wydruk artykułu ze strony www.joesecurity.org „Głęboka analiza złośliwego oprogramowania";
6. wydruk raportu ze strony https://securelist.com - raport firmy Kaspersky „Ewolucja zagrożeń IT w III kwartale 2019 r. Statystyki (wraz z tłumaczeniem);
7. wydruk raportu ze strony https://securelist.com - raport firmy Kaspersky „Ewolucja zagrożeń IT I kwartał 2020 r. Statystyki (wraz z tłumaczeniem);
8. wydruk artykułu ze strony www.reuteurs.com „Microsoft twierdzi, że znalazł złośliwe oprogramowanie w swoich systemach" (wraz z tłumaczeniem);
9. wydruk raportu ze strony www.fireeye.com dotyczącego ataków hakerskich (wraz z tłumaczeniem);
10. wydruk raportu ze strony www.prod-blog.avira.com o zagrożeniach ze strony złośliwego oprogramowania: statystyki i trendy w III kwartale 2020 r. (wraz z tłumaczeniem);
11. wydruk artykułu ze strony www.businessinsider.in dotyczący ataków hakerskich za pośrednictwem oprogramowania SolarWinds (wraz z tłumaczeniem);
12. wydruk artykułu ze strony www.safetydetectives.com „Statystyki, trendy i fakty dotyczące złośliwego oprogramowania i wirusów 2020" (wraz z tłumaczeniem);
13. wydruk artykułu ze strony www.wiadomosci.onet.pl dotyczący ataków hakerskich;
14. wydruk dokumentu Narodowe Standardy Cyberbezpieczeństwa. Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO) v.1.00 – luty 2020.
15. wydruk raportu „Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny 2019 z działalności CERT Polska."

Jako oświadczenie własne Zamawiającego uzupełniające jego stanowisko Izba potraktowała dokument opracowany przez Zamawiającego pn. „Analiza ruchu do sieci UKNF z urządzeń pracujących na systemie Mac Os z dnia 10.11.2020 r."

Izba ustaliła, co następuje:

Na podstawie dokumentacji postępowania przekazanej przez Zamawiającego Izba ustaliła, iż ogłoszenie o zamówieniu zostało opublikowane w Dzienniku Urzędowym Unii Europejskiej z dnia 7 grudnia 2020 r. pod numerem 2020/S 238-587649. W tym samym dniu Zamawiający zamieścił na stronie internetowej SIWZ wraz z załącznikami.

Zgodnie z pkt 3 SIWZ przedmiotem zamówienia jest dostawa wraz z wdrożeniem systemu zapewniającego ochronę przed zaawansowanymi atakami oraz atakami (APT) dla sieci Zamawiającego („System"). W zakresie Przedmiotu zamówienia Wykonawca: dostarczy licencje, o których mowa w pkt 2 lit. f Opisu Przedmiotu Umowy („OPU"); dostarczy sprzęt fizyczny, w tym: minimum dwa fizyczne urządzenia do ochrony kanału pocztowego w sieci UKNF, o których mowa w pkt 3 OPU; minimum dwa fizyczne urządzenia do ochrony ruchu sieci Internet, o których mowa w pkt 4 OPU; wdroży System, o którym mowa w pkt. 2 OPU; zapewni serwis gwarancyjny oraz wsparcie producenta na zainstalowany sprzęt przez okres 36 miesięcy od daty podpisania protokołu odbioru, o którym mowa w § 2 ust 2 Umowy, w zakresie, o którym mowa w pkt 7 OPU; zapewni wsparcie techniczne na wdrożony System w trybie 24/7 (o którym mowa w pkt. 6 OPU), od daty podpisania protokołu odbioru, o którym mowa w § 2 ust. 3 Umowy, do ostatniego dnia wsparcia; przeprowadzi szkolenie dla 7 pracowników Zamawiającego, na zasadach określonych w pkt 8 OPU. Szczegółowe warunki realizacji zamówienia określone zostały w Załączniku nr 2 do SIWZ. Załącznikiem nr 2 do SIWZ jest Projekt Umowy, a załącznik nr 1 do Projektu Umowy stanowi Opis Przedmiotu Umowy.

W OPU zawarto m.in. następujące wymogi:

Pkt 2 – Wymagania ogólne:
e) System musi mieć element (pojedynczy serwer/interfejs zarządzający) zarządzający z poziomu którego można zarządzać elementami systemu, konfigurować je, przeglądać zdarzenia związane z sandboxingiem oraz generować raporty.
f) Wykonawca musi dostarczyć wszystkie niezbędne licencje do działania zaproponowanego Systemu, w tym również licencje dla systemów operacyjnych maszyn wirtualnych na których odbywa się analiza plików oraz programów tam zainstalowanych.

Pkt 3 – Zapewnienie ochrony kanału pocztowego:

a) Zamawiający wymaga dostarczenia, zainstalowania i skonfigurowania minimum dwóch fizycznych urządzeń do ochrony kanału pocztowego w sieci UKNF.
b) Elementy Systemu odpowiedzialne za analizę wiadomości email pod kontem zaawansowanej analizy potencjalnie niebezpiecznego kodu (sandboxing) muszą być dostarczone w postaci zamkniętej platformy sprzętowej. Zamawiający nie dopuszcza

dostarczenia urządzenia w formie maszyny wirtualnej.
c) Zamawiający wyklucza analizę próbki z wiadomości email w chmurze.
d) Zamawiający wymaga pracy w Trybie MTA (Message Transfer Agent).
h) Urządzenie musi zapewniać ochronę co najmniej 1500 skrzynek pocztowych.
l) Urządzanie musi posiadać zainstalowane maszyny wirtualne na których obywa się sandboxing zawierające:

a) Obrazy systemów operacyjnych - minimum: Microsoft Windows 7 (w wersjach 32 i 64 bit), Microsoft Windows 10 64-bit, Mac OS;
b) Zainstalowane oprogramowanie narzędziowe minimum typu: Microsoft Office, Adobe Reader, Flash Player;
c) Wszystkie niezbędne licencje do zaproponowanych przez Wykonawcę systemów operacyjnych i oprogramowania narzędziowego.

Pkt 4 – Zapewnienie ochrony kanału www:

c) Urządzenie musi posiadać możliwość wpięcia w infrastrukturę Zamawiającego w trybie in-line, poprzez zastosowanie danych pochodzących ze SPAN portu urządzeń sieciowych Zamawiającego lub inny umożliwiający pełną ochronę kanału WWW.
o) Urządzenie musi blokować dany ruch w przypadku wykrycia zagrożenia pochodzącego z analizy sandboxowej.

Izba zważyła, co następuje:

Biorąc pod uwagę zgromadzony w sprawie materiał dowodowy, poczynione ustalenia faktyczne oraz orzekając w granicach zarzutów zawartych w odwołaniu, Izba stwierdziła, że odwołanie nie zasługuje na uwzględnienie.

Odwołujący postawił zarzuty naruszenia art. 29 ust. 1-3, art. 30 ust. 4, art. 7 ust. 1, art. 5b i 5f oraz art. 66 ust. 1 i 67 ust. 2 ustawy Pzp. Przywołując ich treść należy wskazać, że zgodnie z art. 7 ust. 1 ustawy Pzp Zamawiający przygotowuje i przeprowadza postępowanie o udzielenie zamówienia w sposób zapewniający zachowanie uczciwej konkurencji i równe traktowanie wykonawców oraz zgodnie z zasadami proporcjonalności i przejrzystości. Art. 29 ust. 1 ustawy Pzp stanowi, iż przedmiot zamówienia opisuje się w sposób jednoznaczny i wyczerpujący, za pomocą dostatecznie dokładnych i zrozumiałych określeń, uwzględniając wszystkie wymagania i okoliczności mogące mieć wpływ na sporządzenie oferty. Wedle ust. 2 tego przepisu przedmiotu zamówienia nie można opisywać w sposób, który mógłby utrudniać uczciwą konkurencję. Z kolei zgodnie z ust. 3 przedmiotu zamówienia nie można opisywać 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, chyba że jest to uzasadnione specyfiką przedmiotu zamówienia i zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń, a wskazaniu takiemu towarzyszą wyrazy „lub równoważny.” Z kolei art. 30 ust. 4 ustawy Pzp opisując przedmiot zamówienia przez odniesienie do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w ust. 1 pkt 2 i ust. 3, zamawiający jest obowiązany wskazać, że dopuszcza rozwiązania równoważne opisywanym, a odniesieniu takiemu towarzyszą wyrazy "lub równoważne".

Zgodnie z art. 5b pkt 1 ustawy Pzp zamawiający nie może w celu uniknięcia stosowania przepisów ustawy łączyć zamówień, które odrębnie udzielane wymagają zastosowania różnych przepisów ustawy. Zgodnie z art. 5f ustawy Pzp jeżeli przedmiot zamówienia nie może zostać podzielony, w szczególności ze względów technicznych, organizacyjnych, ekonomicznych lub celowościowych, do udzielenia zamówienia stosuje się przepisy dotyczące tego rodzaju zamówienia, który odpowiada jego głównemu przedmiotowi. Art. 66 ust. 1 ustawy Pzp odnosi się do udzielenia zamówienia z wolnej ręki, wskazując, iż zamówienie z wolnej ręki to tryb udzielenia zamówienia, w którym zamawiający udziela zamówienia po negocjacjach tylko z jednym wykonawcą. Art. 67 ust. 2 ustawy Pzp odnosi się do obowiązku zawiadamia Prezesa Urzędu o wszczęciu, podając uzasadnienie faktyczne i prawne zastosowania trybu udzielenia zamówienia, wobec czego Izba stwierdziła, że zamiarem Odwołującego było powołanie się na art. 67 ust. 1 regulujący przypadki, w których możliwe jest udzielenie zamówienia z wolnej ręki.

Izba zważyła, że zasadniczą podstawą faktyczną ww. zarzutów była okoliczność połączenia w ramach jednego postepowania usługi budowy systemu sandboxingu obejmującego swym zakresem ochronę systemu operacyjnego Microsoft Windows i systemu Mac Os, przy równoczesnym niedopuszczeniu możliwości emulowania Mac OS w chmurze, co w ocenie Odwołującego wskazywało na preferowanie przez Zamawiającego rozwiązania jednego producenta (FireEye) i ograniczenie konkurencji. Powyższych okoliczności dotyczył także punkt 2.1 uzasadnienia odwołania, w ramach którego kwestionowano wymóg z pkt 3la) OPU (tj. wymóg, aby urządzenie posiadało zainstalowane maszyny wirtualne, na których odbywa się sandboxing, zawierające obrazy systemu operacyjnego Mac Os), wobec czego Izba uznała za zasadne odniesienie się do powyższych kwestii w sposób łączny.

W ocenie Izby Odwołujący nie wykazał, aby sposób ukształtowania postanowień OPU przez Zamawiającego naruszać miał wskazane powyżej przepisy prawa.

Na wstępie należy wskazać, iż sporządzenie opisu przedmiotu zamówienia jest jedną z najważniejszych czynności związanych z przygotowaniem postępowania o udzielenie

zamówienia publicznego. Czynność ta stanowi obowiązek Zamawiającego, ale jednocześnie jego uprawnienie, bowiem odzwierciedla rzeczywiste potrzeby Zamawiającego w danym postępowaniu. To Zamawiający ma prawo, wyznaczając cel, jaki zamierza zrealizować, tak określić przedmiot zamówienia, aby opisać go adekwatnie do wyznaczonego celu, zachowując jednocześnie obiektywizm i precyzję w formułowaniu swoich potrzeb. Zamawiający zobowiązany jest ponadto respektować art. 29 ust. 2 ustawy Pzp, który zakazuje dokonywania opisu przedmiotu zamówienia w sposób dyskryminujący, przy czym podkreślenia wymaga, że powyższa norma nie może być równoważona z obowiązkiem wyeliminowania z opisu przedmiotu zamówienia uzasadnionych wymagań, które dla wykonawcy mogą stanowić źródło ewentualnych niedogodności czy potrzeby stworzenia nowych rozwiązań dostosowanych do realizacji konkretnego zamówienia (podobnie m.in. wyrok KIO z 28 stycznia 2019 r., KIO 26/19, wyrok KIO z dnia 22 lipca 2019 r., sygn. akt KIO 1271/19).

Odwołujący nie podnosił, aby treść OPU w przywołanym powyżej aspekcie była niejednoznaczna, niewyczerpująca, czy też, że nie została sformułowana za pomocą dostatecznie dokładnych i zrozumiałych określeń lub nie uwzględniała wszystkich wymagań i okoliczności mogących mieć wpływ na sporządzenie oferty, wobec czego nie sposób stwierdzić, aby sporządzenie opisu przedmiotu zamówienia naruszało art. 29 ust. 1 ustawy Pzp. Postanowienia OPU nie budziły po stronie Odwołującego wątpliwości interpretacyjnych, było przez niego zrozumiałe. Odwołujący nie wykazał także, aby sposób ukształtowania OPU mógłby wpływać w sposób nieuzasadniony obiektywnymi potrzebami Zamawiającego na ograniczenie konkurencji. Sam fakt, że wprowadzenie postulowanych przez Odwołującego zmian w SIWZ, umożliwiałyby Odwołującemu złożenie oferty w przedmiotowym postępowaniu, nie jest wystarczający do stwierdzenia, że Zamawiający naruszył przepisy ustawy Pzp. Podkreślenia wymaga, iż okoliczność, że nie wszystkie produkty dostępne na rynku odpowiadają wymaganiom OPU, nie stanowi dostatecznej podstawy do uznania, że przedmiot zamówienia został opisany w sposób, który mógłby utrudniać uczciwą konkurencję, a tym bardziej podstawy takiej nie stanowi fakt, że Odwołujący współpracuje z producentami, którzy nie mają rozwiązań, jakie zakupić chce Zamawiający. Ponadto stwierdzić należy, iż okoliczność że art. 29 ust. 2 ustawy Pzp wskazuje na możliwość utrudniania konkurencji, a nie utrudnienie konkurencji (a zatem na prawdopodobieństwo wystąpienia naruszenia konkurencji, a nie konieczność wystąpienia tego naruszenia), nie zmienia faktu, że zgodnie z art. 190 ust. 1 ustawy Pzp obowiązkiem Odwołującego jest udowodnienie okoliczności wskazanych w przepisie, którego naruszenie zarzucane jest Zamawiającemu. To na Odwołującym spoczywał zatem ciężar wykazania tej potencjalnej możliwości wystąpienia utrudniania konkurencji, Odwołujący zaś - zamiast skupić się na

wykazaniu, że sposób ukształtowania wymagań OPU naruszać może konkurencję - przedstawił argumentację wskazującą, że potrzeby Zamawiającego można zaspokoić inaczej, tj. dopuszczając rozwiązanie możliwe do dostarczenia przez Odwołującego bądź rozdzielając przedmiot zamówienia tak, aby Odwołujący w jednej z części mógł złożyć ofertę.

Za bezzasadną Izba uznała argumentację Odwołującego odnoszącą się do konieczności podziału przedmiotowego zamówienia na części w taki sposób, aby wyłączyć z jego zakresu ochronę urządzeń pracujących na systemie operacyjnym Mac OS. Nie znalazło potwierdzenia zawarte w odwołaniu stwierdzenie, iż Zamawiający nie posiada systemów Mac OS i prawdopodobnie w ogóle ich nie używa – Zamawiający okoliczność przeciwną wykazał w toku postępowania odwoławczego. Zamawiający wyjaśnił, że posiada w swojej infrastrukturze urządzenia pracujące pod kontrolą Mac OS, które służą do realizacji zadań służbowych (także przetwarzania informacji prawnie chronionych), a ponadto – co również ma istotne znaczenie – z rozwiązań firmy Apple korzystają uczestnicy rynku finansowego nadzorowani przez Zamawiającego. Analiza przeprowadzona przez Zamawiającego wykazała, iż systemy Apple generują ok 12 000 zapytań dziennie do systemów informatycznych Zamawiającego. Co istotne, sam Odwołujący własnej tezie zaprzeczył przedstawiając jako dowód specyfikację istotnych warunków zamówienia dla postępowania pn. „Wdrożenie Systemu DLP”, która pośrednio potwierdza, że Zamawiający dysponuje systemami operacyjnymi Mac OS.

W ocenie Izby fakt, że urządzeń w infrastrukturze informatycznej Zamawiającego pracujących pod kontrolą Microsoft Windows jest więcej nie powoduje, że równorzędna ochrona dla urządzeń z systemem Mac OS przed złośliwym oprogramowaniem nie stanowi uzasadnionych potrzeb Zamawiającego. Zamawiający istnienie takich potrzeb uzasadnił wyjaśniając m.in., że bezpieczeństwa systemu informatycznego nie należy traktować w aspekcie ilościowym, gdyż nawet jedno urządzenie nie objęte należytą ochroną przed złośliwym oprogramowaniem może negatywnie wpłynąć na bezpieczeństwo całego systemu informatycznego Zamawiającego, a pośrednio także nadzorowanych przez KNF podmiotów. Odwołujący nie odparł twierdzeń Zamawiającego, iż rezygnacja z ochrony systemów Mac OS, które są wykorzystywane przez Zamawiającego w działalności operacyjnej i z których korzystają nadzorowane przez KNF podmioty rynku finansowego, prowadzić może do powstania ryzyka, polegającego na otrzymaniu złośliwego oprogramowania i jego dalszej nieświadomej dystrybucji przez Zamawiającego do instytucji finansowych. Zamawiający przedstawił także argumentację i dowody potwierdzające fakt działania złośliwego oprogramowania atakującego systemy Mac OS i istnienie realnego zagrożenia tego rodzaju atakami (raport Avira, raport CERT). Mając powyższe na względzie, oczekiwanie

Zamawiającego dostarczenia równorzędnej ochrony systemom operacyjnym Microsoft Windows i Mac OS w ocenie Izby uznać należy za uzasadnione.

Odwołujący nie zaprzeczył także twierdzeniom Zamawiającego, że przedmiot zamówienia ma charakter jednorodny – dostarczone rozwiązanie ma w jak najszerszym zakresie zapewniać ochronę systemów informatycznych Zamawiającego, w ramach których przetwarzane są zasoby informacyjne dotyczące istotnego z punktu widzenia ochrony interesów państwa obszaru stabilności rynku finansowego. Odwołujący nie kwestionował także stanowiska Zamawiającego, że na rynku nie istnieje produkt, który umożliwiałby sandboxing tylko i wyłącznie dla systemów Mac OS. Powyższa okoliczność powoduje zaś, że konieczność podzielenia przedmiotu zamówienia oznaczałaby dla Zamawiającego, dla którego niezbędne jest także zapewnienie ochrony systemów Mac OS, konieczność zakupu dwóch rozwiązań realizujących te same zadania – tj. wdrożenia systemu zapewniającego ochronę przed zaawansowanymi zagrożeniami dla systemu Microsoft Windows oraz systemu zapewniającego ochronę przed zaawansowanymi zagrożeniami dla systemu Microsoft Windows i Mac Os. Izba za wiarygodne uznała stanowisko Zamawiającego, że takie działanie pociągałoby za sobą nie tylko zwiększenie wydatkowania środków publicznych, koszty zapewnienia wsparcia dla tych systemów, odnawiania licencji, zapewnienia zasobów ludzkich do ich obsługi, przeszkolenia pracowników z administrowania obu systemów, ale także ryzyko niekompatybilności obu systemów mogących pochodzić od różnych producentów, trudności technicznych w konfiguracji i obsłudze. Odwołujący nie odniósł się do technicznych aspektów rozdzielenia systemu ochrony przed zaawansowanymi zagrożeniami na poszczególne elementy i wpływu takiego podziału na zachowanie wymaganych funkcjonalności i prawidłowość działania systemu jako całości.

W ocenie Izby analiza zarzutów odwołania prowadzi do wniosku, że celem Odwołującego było dostosowanie wymagań do oferowanych przez niego produktów, a nie konwalidacja niezgodnych z prawem działań lub zaniechań Zamawiającego. Żądania Odwołującego zmierzające do podzielenia przedmiotu zamówienia na części czy też – jak podniesiono na rozprawie – uczynienia wymagania w zakresie ochrony systemów Mac OS wymaganiem opcjonalnym, dodatkowo punktowanym w kryteriach oceny ofert, były oderwane od rzeczywistych, uzasadnionych potrzeb Zamawiającego. Za całkowicie nieuzasadnione w świetle powyższych okoliczności uznać należy twierdzenia, że Zamawiający w zakresie Mac OS mógłby udzielić zamówienia z wolnej ręki czy też udzielić zamówienia w ogóle bez stosowania ustawy Pzp. To właśnie skorzystanie przez Zamawiającego z ww. instytucji mogłoby z dużym prawdopodobieństwem zostać uznane za naruszenie przepisów ustawy Pzp, w szczególności art. 5b pkt 2 ustawy Pzp poprzez

dokonanie podziału zamówienia na odrębne zamówienia w celu uniknięcia łącznego szacowania ich wartości.

Podobnie Izba nie uznała za zasadne żądania, aby Zamawiający dopuścił możliwość emulowania obrazów systemu Mac OS w chmurze. Argumentacja przedstawiona w odwołaniu w powyższym zakresie sprowadzała się do wskazania, że uruchomienie systemu Mac OS na urządzeniach innych niż Apple będzie równoznaczne ze złamaniem warunków licencji oprogramowania Apple, podczas gdy dla Zamawiającego nie ma żadnego znaczenia czy uruchomienie nastąpi w chmurze czy na urządzeniu, gdyż efekt końcowy jest ten sam. W ocenie Izby Odwołujący nie wykazał prawdziwości tych twierdzeń, w szczególności okoliczności, że przetwarzanie części informacji pochodzących z systemu informatycznego Zamawiającego w chmurze obliczeniowej pozostawać miałoby bez wpływu na kwestię bezpieczeństwa informacji administrowanych przez Zamawiającego. Po pierwsze argumentacja odwołania w ogóle nie odnosi się do kwestii bezpieczeństwa informacji przetwarzanych w chmurach obliczeniowych, czy to publicznych, hybrydowych czy prywatnych i różnic w stosunku do przetwarzania tych danych w infrastrukturze informatycznej danego podmiotu. Po drugie całkowicie abstrahuje ona od roli Zamawiającego w realizowaniu zadań związanych z bezpieczeństwem finansowym państwa oraz od istotnego ryzyka, jakie wiąże się z niezapewnieniem wymaganej ochrony informacjom przetwarzanym przez Zamawiającego, w tym informacjom prawnie chronionym, które Zamawiający wylistował szczegółowo na stronie 8-9 odpowiedzi na odwołanie. Realizacja postulatu Odwołującego sprowadzałaby się do konieczności przetwarzania części tych informacji poza infrastrukturą Zamawiającego, w chmurze, co kłóci się z wymaganiami i obowiązkami, jakie na Zamawiającego nakładają przepisy prawa i ustalone w zakresie cyberbezpieczeństwa standardy. Na powyższe szczegółowo zwracał uwagę Zamawiający w odpowiedzi na odwołanie i na rozprawie.

Jak wynika z treści Standardów Cyberbezpieczeństwa Chmur Obliczeniowych (który to dokument został złożony przez Zamawiającego jako dowód) odbiorcami tego dokumentu są m.in. jednostki administracji publicznej planujące wykorzystanie lub korzystające z rządowych lub publicznych usług przetwarzania w modelach chmur obliczeniowych, a zatem także Zamawiający (w sytuacji podjęcia decyzji o korzystaniu z usług przetwarzania danych w chmurach obliczeniowych, bowiem jak podnosił Zamawiający, na chwilę obecną z tego rodzaju rozwiązań nie korzysta). SCCO określa m.in. poziomy wymagań bezpieczeństwa determinujące stosowanie poszczególnych modeli chmur obliczeniowych ustalane przez korelację wrażliwości lub poziomu poufności informacji oraz poziomu potencjalnego wpływu zdarzenia powodującego utratę poufności, integralności lub dostępności tych informacji; Wyróżnione zostały cztery Poziomy Wymagań Bezpieczeństwa: SCCO1 – niekontrolowane

informacje nieklasyfikowane, SCCO2 – kontrolowane informacje urzędowe, SCCO3 – kontrolowane wrażliwe informacje urzędowe, SCOO4 – informacje niejawne. Odwołujący nie kwestionował okoliczności, że zgodnie z wytycznymi SCCO określone informacje mogą być przetwarzane tylko w środowisku Rządowej Chmury Obliczeniowej. Odwołujący sam przyznał na rozprawie, że wymóg ten dotyczy informacji, o których mowa w punkcie 3 i 4 tabeli na str. 9 SCCO (kontrolowane wrażliwe informacje urzędowe oraz informacje niejawne), polemizował jedynie z zakresem informacji, które mogą być przetwarzane w chmurze obliczeniowej, podnosząc, że mogą w ten sposób być przetwarzane niekontrolowane informacje nieklasyfikowane i kontrolowane informacje urzędowe. Powyższa okoliczność wskazuje, że nawet jeśli nie całość, to część informacji przetwarzanych przez Zamawiającego ze względu na ich wrażliwość nie może być w ogóle przetwarzana w chmurach obliczeniowych, za wyjątkiem Rządowej Chmury Obliczeniowej. Nie ma przy tym, w ocenie Izby, znaczenia podnoszony przez Odwołującego fakt, że do chmury wysyłane byłyby tylko te pliki, które zostały rozpoznane jako niebezpieczne i plik byłby tam dostępny tylko kilkadziesiąt godzin, po czym byłby usuwany. Sam Odwołujący potwierdził na rozprawie, że aby zweryfikować pliki musiałyby one być nie tylko przetransferowane na chmurę, ale tam odszyfrowane.

Odwołujący pominął także aspekt, że już dla poziomu SCCO2 – kontrolowane informacje urzędowe, stawiane są dodatkowe restrykcyjne wymagania, w tym m.in. dopuszczalność przetwarzania wyłącznie w centrach danych polskich jurysdykcji, konieczność posiadania przez personel poświadczenia bezpieczeństwa na poziomie „poufne” i powyższych wymogów nie odniósł do realiów przedmiotowego postępowania. Jedynie w zakresie poziomu SCCO1 wymagania są obniżone, niemniej ten poziom informacji nie obejmuje informacji prawnie chronionych, a takimi w znacznej mierze dysponuje Zamawiający (tajemnice zawodowe - informacje, o których mowa w ustawie o obrocie instrumentami finansowymi, o giełdach towarowych, o funduszach inwestycyjnych, w Prawie bankowym, w ustawie o usługach płatniczych, o spółdzielczych kasach oszczędnościowo – kredytowych; informacje poufne, o których mowa w ustawie o obrocie instrumentami finansowymi; tajemnica bankowa, o której mowa w Prawie bankowym, tajemnica ubezpieczeniowa, o której mowa w ustawie o działalności ubezpieczeniowej i reasekuracyjnej; dane osobowe; tajemnica skarbowa, o której mowa w Ordynacji podatkowej; tajemnica przedsiębiorstwa, o której mowa w ustawie o zwalczaniu nieuczciwej konkurencji; tajemnica ubezpieczeń społecznych z ustawy o systemie ubezpieczeń społecznych; tajemnica statystyki sektora bankowego, o której mowa w ustawie o Narodowym Banku Polskim; tajemnica statystyczna, o której mowa w ustawie o statystyce publicznej, tajemnica Komitetu Stabilności Finansowej, o której mowa w ustawie o nadzorze

makroostrożnościowym nad systemem finansowym i zarządzaniu kryzysowym w systemie finansowym; inne tajemnice chronione na podstawie powszechnie obowiązujących przepisów prawa.). Izba za wiarygodną uznała argumentację Zamawiającego, iż kwestia przetwarzania danych wrażliwych i tajemnic prawnie chronionych jest niezwykle istotna z perspektywy zadań realizowanych przez KNF. Zamawiający powoływał się na brak podstawy prawnej do powierzenia przetwarzania istotnych z punktu widzenia rynku finansowego danych i informacji (w tym informacji prawnie chronionych) podmiotom, które będą je przetwarzały w chmurze obliczeniowej, udostępniając je podmiotom realizującym na ich rzecz zadania związane np. z utrzymaniem rozwiązań chmurowych, a Odwołujący argumentacji tej nie odparł.

Mając na uwadze powyższe Izba podzieliła stanowisko Zamawiającego, iż przedmiotowy wymóg przetwarzania danych i informacji w infrastrukturze Zamawiającego nie stanowi jego pozornej potrzeby, lecz ma zagwarantować bezpieczeństwo przetwarzania tych danych i informacji, ze szczególnym uwzględnieniem informacji prawnie chronionych. Odwołujący okoliczności przeciwnych nie wykazał. Zdaniem składu orzekającego Odwołujący swoją narracją próbuje narzucić Zamawiającemu rozwiązania nieadekwatne do jego rzeczywistych potrzeb, jednocześnie nie wykazując za pomocą twierdzeń i dowodów, aby z perspektywy bezpieczeństwa informacji, jakimi Zamawiający zarządza, w tym interesów podmiotów rynku finansowego, na rzecz których Zamawiający realizuje zadania publiczne, nie było różnicy czy emulacja obrazów systemów Mac OS następuje na urządzeniu czy w chmurze.

Bez zasadniczego wpływu na ocenę przedmiotowego przypadku pozostaje podnoszona przez Odwołującego okoliczność, iż inni zamawiający stosują rozwiązania chmurowe, ponieważ Izba dokonuje oceny działań i zaniechań Zamawiającego w oparciu o dokumenty konkretnego zamówienia i potrzeby istniejące po stronie konkretnego podmiotu - Zamawiającego, a nie podmiotów trzecich. Sam fakt, że część instytucji decyduje się na wdrożenie rozwiązań informatycznych z wykorzystaniem chmur obliczeniowych nie powoduje, że do takiego działania zobowiązany miałby być także Zamawiający - inne są bowiem potrzeby różnych zamawiających, innego rodzaju dane są przez nich przetwarzane, stosowane są innego rodzaju polityki bezpieczeństwa, różna jest posiadana przez nich infrastruktura informatyczna, wreszcie inne mogą być decyzje strategiczne w zakresie cyberbezpieczeństwa. W konsekwencji nie miały znaczenia dla rozstrzygnięcia złożone przez Odwołującego w tym zakresie dowody z dokumentacji postępowania prowadzonego przez Ministerstwo Sprawiedliwości.

Za niepotwierdzające tez odwołania Izba uznała dowody w postaci wyciągu z informacji o wynikach kontroli NIK oraz odpowiedzi Ministra Finansów na interpelację nr 28436 –

dowody te potwierdzają jedynie okoliczność, że przyjęto określone rozwiązanie gwarantujące bezpieczeństwo przy przesyłaniu danych w postaci plików JPK w warunkach korzystania z usług chmury publicznej Microsoft Azure. Ponadto, jak słusznie zauważył Zamawiający, z dowodu stanowiącego wyciąg z informacji o wynikach kontroli NIK wprost wynika, że rozkodowanie i analiza treści plików JPK jest możliwa tylko w ramach infrastruktury informatycznej Centrum Informatyki Resortu Finansów (CIRF). Tym samym chmura obliczeniowa wykorzystywana jest wyłącznie do transferu zaszyfrowanych danych. Potwierdza to treść ww. odpowiedzi na interpelację, gdzie wskazano, iż „JPK transferowane przez przedsiębiorców poprzez chmurę publiczną są w postaci zaszyfrowanej kluczem publicznym (…). Odszyfrowanie możliwe jest wyłącznie w środowisku CIRF z wykorzystaniem chronionego klucza prywatnego MF. Zaszyfrowane pliki JPK po zakończeniu transferu danych do CIRF, w żaden sposób nie są przechowywane w chmurze publicznej". Sytuacji tej nie sposób zatem porównywać z realiami przedmiotowego zamówienia, kiedy to w celu dokonana analizy w środowisku sandbox dane musiałyby zostać w chmurze odszyfrowane i przetwarzane oraz przez jakiś czas w tej chmurze przechowywane. O braku istnienia uzasadnionych potrzeb po stronie Zamawiającego nie świadczy także fakt, że KNF opublikował komunikat dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej. Komunikat ten stanowi wytyczne dla podmiotów nadzorowanych przez KNF (sektora prywatnego), a nie dla instytucji publicznych, w tym samego Zamawiającego.

Za niewykazane Izba uznała ponadto twierdzenia Odwołującego, jakoby opis przedmiotu umowy pośrednio wskazywać miał na rozwiązanie konkretnego producenta – firmy FireEye. Odwołujący na tę okoliczność nie złożył w zasadzie żadnych dowodów, poza oświadczeniami dwóch producentów – Trend Micro i Fortinet, z których wynikało, że te podmioty nie posiadają produktu spełniającego wymaganie Zamawiającego w zakresie systemów Mac OS, a taki wymóg wskazuje na konkurencyjny produkt - FireEye. Przedstawione przez Odwołującego oświadczenia nie są w ocenie Izby wystarczające do potwierdzenia tezy, że tylko jeden produkt spełnia wymagania Zamawiającego, mając na uwadze okoliczność, że oświadczenia obu producentów mają dokładanie to samo brzmienie i ten sam format, są to podmioty z którymi współpracuje Odwołujący i które pośrednio także pozostają zainteresowane zmianą SIWZ w sposób, który umożliwi złożenie ofert na ich produkty (powyższe wynika wprost z treści tych oświadczeń oraz korespondencji mailowej prowadzonej przez Odwołującego z Trend Micro).

Izba miała ponadto na względzie, iż Odwołujący wskazał w odwołaniu na szereg producentów rozwiązań typu sandbox, jednocześnie poprzestając na gołosłownej tezie, że produkty tych producentów mogłyby spełniać potrzeby Zamawiającego, gdyby

zmodyfikowano SIWZ. Odwołujący nie przedstawił żadnej argumentacji ani dowodów wskazujących, że inne rozwiązania dostępne na rynku nie spełniają wymagań Zamawiającego. Odwołujący poprzestał na lakonicznym stwierdzeniu, że na rynku istnieje tylko jedno rozwiązanie klasy sandbox, które umożliwia uruchomienie obrazu systemu Mac OS, a nie w chmurze, przy czym tezy tej nawet nie uprawdopodobnił. Z kolei Zamawiający złożył na rozprawie dowody wskazujące na okoliczności przeciwne - mające potwierdzać, że sporne wymagania w zakresie Mac OS spełniają chociażby produkty Juniper Networks (Juniper Advanced Threat Prevention) oraz JOESecurity (Joe Sandbox Complete i Joe Sandbox Ultimate). Prawdziwości tych twierdzeń Odwołujący nie podważył. Poza ogólnym stwierdzeniem, że ww. produkty nie spełniają wymagań OPU, Odwołujący nie przedstawił żadnych dalszych argumentów i nie wyjaśnił, których konkretnie wymagań wskazanych przez Zamawiającego produkty miałyby nie spełniać. W szczególności zaś Odwołujący nie kwestionował okoliczności, na którą powołał się Zamawiający, a mianowicie, że rozwiązania ww. producentów spełniają wymóg w zakresie uruchomienia obrazów systemu Mac OS na urządzeniu. Powyższe poddaje w wątpliwość także zasadność twierdzeń Odwołującego, iż firma Apple nie zezwala na uruchomienie systemu Mac OS na urządzeniach innych niż te oferowane przez Apple, skoro część producentów, w tym ww. producenci wskazani przez Zamawiającego oraz wskazywany przez Odwołującego FireEye, oferują wymaganą przez Zamawiającego funkcjonalność uruchomienia obrazów systemu Mac OS na urządzeniu, a zatem założyć należy, że posiadają niezbędne do tego licencje. Odwołujący nie referował do kwestii możliwości nabycia stosownej licencji od Apple ani ewentualnych trudności czy kosztów z tym związanych.

Mając powyższe na względzie, bez znaczenia dla przedmiotowej sprawy pozostaje argumentacja Odwołującego odnosząca się do jakości rozwiązania producenta FireEye i ataków hakerskich, jakie miały miejsce na tę firmę, a także prymatu rozwiązań innych producentów nad rozwiązaniem FireEye. W konsekwencji za nieprzydatne dla rozstrzygnięcia Izba uznała składane przez Odwołującego na ww. okoliczności dowody w postaci wydruków analiz porównawczych produktów, prezentacji i testów produktów dokonanych przez NSS Labs, recenzji ze strony www.gartner.com oraz artykułów dotyczących ataków hakerskich. Nadto argumentacja Odwołującego kwestionująca bezpieczeństwo produktu FireEye jawi się jako niewiarygodna w świetle informacji i dowodów przedstawionych przez Zamawiającego, wskazujących na okoliczność, iż cyberprzestępcy wykorzystali lukę w oprogramowaniu firmy trzeciej (SolarWings), a nie FireEye, na skalę tych ataków (ok. 18 000 firm i instytucji publicznych), jak i na udział firmy FireEye w wykryciu incydentu i dalszych działaniach związanych z jego badaniem. Nie ma także znaczenia dla rozstrzygnięcia okoliczność dowodzona przez Odwołującego na

rozprawie za pomocą dowodów z dokumentacji postępowań prowadzonych przez UKNF, tj. że Zamawiający korzystał już w jakimś zakresie z produktów Trend Micro i Fortinet, że posiada on wiedzę na temat tych rozwiązań czy też że posiada wiedzę w zakresie szyfrowania informacji. Powyższe nie wpływa na sposób ukształtowania postanowień OPU w przedmiotowym postępowaniu, które determinowane są uzasadnionymi potrzebami Zamawiającego, tym bardziej, że postępowania te dotyczyły innych obszarów niż obecnie prowadzone.

Przechodząc do omówienia dalszych zarzutów Izba wskazuje, co następuje.

Za niepotwierdzony Izba uznała zarzut odnoszący się do pkt 2f OPU (pkt 1 uzasadnienia odwołania dotyczącego postulowanych zmian w OPU).

Po pierwsze nie sposób uznać za zasadną argumentacji Odwołującego odnoszącej się do wymogu dostarczenia przez wykonawcę wszystkich niezbędnych licencji do działania systemu, w tym licencji dla systemów operacyjnych maszyn wirtualnych. Oczywistym wydaje się, że Zamawiający oczekując wdrożenia systemu ochrony przed zaawansowanymi zagrożeniami wymagał będzie także dostawy licencji niezbędnych do działania tego systemu, co gwarantuje jego użytkowanie bez naruszania praw własności intelektualnej osób trzecich. Odwołujący nie przedstawił szczegółowej argumentacji mającej wskazywać na okoliczność, że tego rodzaju wymóg narusza przepisy ustawy Pzp, w szczególności, że mógłby on potencjalnie ograniczać konkurencję. Nie złożył także żadnych dowodów na poparcie postawionej w odwołaniu tezy, że niewielu producentów standardowo oferuje licencje systemów operacyjnych, a większość czyni to za dodatkową opłatą. Nie wyjaśnił także jak ta okoliczność miałaby wpływać na możliwość złożenia w postępowaniu konkurencyjnej oferty, uwzględniającej koszty wymaganych licencji. Argumentacja Odwołującego nie koresponduje ponadto z postawionym żądaniem, Odwołujący z jednej strony zwraca bowiem uwagę na okoliczność, że większość producentów oferuje licencje systemów operacyjnych za dodatkową opłatą, a z drugiej strony nie domaga się zmiany pkt 2f OPU w zakresie dotyczącym wymagania dostarczenia licencji dla systemów operacyjnych maszyn wirtualnych.

Żądanie Odwołującego sprowadza się wyłącznie do wprowadzenia wymogu, że ww. licencje dla systemów operacyjnych maszyn wirtualnych powinny być w języku polskim, uzasadnionego tym, że wymaganie to wspiera produkt FireEye, który nie posiada wersji polskojęzycznej. Powyższe twierdzenie nie zostało przez Odwołującego wykazane, nie przedstawiono na tę okoliczność żadnych dowodów. Odwołujący nie wskazał także, aby w tym zakresie miało dojść do naruszenia jakichkolwiek przepisów – wręcz przeciwnie, jak słusznie zauważył Zamawiający, to zmiana postanowień OPU zgodnie z żądaniem odwołania przez wprowadzenie wymogu dostarczenia licencji w języku polskim, zamiast

wpłynąć pozytywnie na konkurencję, mogłaby ją ograniczyć. Również twierdzenie Odwołującego o tym, że produkt z licencją anglojęzyczną miałby być dla Zamawiającego bezużyteczny, nie zostało niczym poparte ani szerzej wyjaśnione. Sam Odwołujący tezie tej pośrednio zaprzeczył wskazując, że wersje angielskie i polskie licencji są utrzymywane osobno, nie są spójne, a poprawki w języku polskim są w innym czasie niż poprawki w języku angielskim. (przy czym Odwołujący nie kwestionował twierdzeń Zamawiającego, że poprawki w języku polskim wprowadzane są później niż w wersjach anglojęzycznych). Argumentacja Odwołującego o bezużyteczności oprogramowania objętego licencją anglojęzyczną jawi się jako bezzasadna także w zestawieniu z faktem, iż Zamawiający od wielu lat korzysta z rozwiązania używającego obrazy angielskich systemów operacyjnych, na których wykonywana jest analiza danych na potrzeby wykrywania zagrożeń cyberbezpieczeństwa, na co wskazano w odpowiedzi na odwołanie i co nie było sporne.

Za niewykazany Izba uznała także zarzut dotyczący pkt 3l OPU (pkt 2 uzasadnienia odwołania). Do pkt 3la), tj. wymogu, aby urządzenie posiadało zainstalowane maszyny wirtualne, na których odbywa się sandboxing, zawierające obrazy systemu operacyjnego Mac Os, Izba odniosła się już we wcześniejszej części uzasadnienia. Natomiast za bezzasadne Izba uznała także stanowisko Odwołującego odnoszące się do wymogu z pkt. 3l OPU w zakresie dotyczącym dostarczenia licencji Windows i MS Office. W ocenie Izby domaganie się usunięcia przedmiotowego wymogu stanowiło przejaw próby ukształtowania przedmiotu zamówienia w sposób bardziej dogodny dla Odwołującego. Na powyższe wskazał sam Odwołujący twierdząc, że „oczekiwanie dostarczenia licencji jest niewygodne dla wykonawcy, ponieważ żeby złożyć ofertę musi ustalić warunki z Microsoft.” Nie taki jest jednak cel postępowania odwoławczego - postępowanie to służy wyeliminowaniu potencjalnych naruszeń prawa, a nie kształtowaniu postanowień SIWZ w sposób korzystny dla wykonawców. Odwołanie nie powinno prowadzić do negocjacji treści postanowień SIWZ pod pretekstem rzekomych naruszeń przepisów. Dodatkowe trudności istniejące po stronie wykonawcy nie stanowią okoliczności wskazującej na naruszenie przepisów ustawy Pzp. Odwołujący w tym zakresie nie przedstawił jakiejkolwiek konstruktywnej argumentacji, za taką nie może być bowiem uznane lakoniczne wskazanie na fakt, że Microsoft przez swoich dystrybutorów może dać różne ceny różnym wykonawcom.

Bezzasadne jest także twierdzenie jakoby działanie Zamawiającego miało być niegospodarne z uwagi na zawarcie przez Zamawiającego umowy Enterprise Agreement z Microsoft. Odwołujący nie wyjaśnił jak fakt posiadania przez Zamawiającego określonych licencji miałby wpływać na realizację przedmiotowego zamówienia, a nadto jego teza postawiona została w oderwaniu od rzeczywistego stanu faktycznego. Jak wskazywał Zamawiający umowa Enterprise Agreement nie zawiera postanowień umożliwiających jej

wykorzystanie dla urządzeń dostarczanych przez inne podmioty, nie obejmuje użycia maszyn na potrzeby sandboxingu, wygasa wcześniej niż planowany zakup systemu sandboxingu. Odwołujący do stanowiska tego nie odniósł się. W ocenie Izby twierdzenie Odwołującego, jakoby działanie Zamawiającego miało być niegospodarne, stanowi kolejną próbę narzucenia Zamawiającemu takiego rozwiązania, jakie z perspektywy Odwołującego byłyby optymalne przy konstruowaniu oferty, przy jednoczesnym pominięciu uzasadnionych potrzeb istniejących po stronie Zamawiającego w tym względzie.

Izba wskazuje także na bezzasadność żądania wykreślenia z OPU wymogu posiadania przez urządzenia maszyn wirtualnych, na których odbywa się sandboxing, zainstalowanego oprogramowania narzędziowego minimum typu Microsoft Office, które dodatkowo nie koresponduje z treścią zarzutu. Jak wskazał Zamawiający realizacja postulatu Odwołującego uniemożliwiłoby w analizie sandboxowej sprawdzenie plików bazujących na tym właśnie pakiecie narzędzi biurowych i spowodowałoby znaczny spadek wykrywalności złośliwego oprogramowania narażając Zamawiającego na ryzyko i podważając sens dokonywania analizy sandboxowej. Zamawiający przedstawił informacje poparte dowodami, obrazujące skalę zagrożeń dla produktów Microsoft, w szczególności Microsoft Office, którego w ostatnim czasie dotyczyło 73-75% wszystkich cyberataków, ja i fakt, że większość złośliwego oprogramowania jest przesyłana za pośrednictwem poczty elektronicznej. Odwołujący nie przedstawił jakichkolwiek argumentów, które pozwalałaby poddać w wątpliwość uzasadnione potrzeby Zamawiającego w powyższym aspekcie. Z kolei podniesione w odwołaniu lakoniczne twierdzenia o ryzyku wykrycia przez malware licencji generycznej sandboxowej i zastosowania technik unikania, mające wskazywać na rzekomy brak zapewnienia odpowiedniego bezpieczeństwa przez zamawiane rozwiązanie, nie zostały przez Odwołującego ani szerzej rozwinięte, ani poparte dowodami, a jako takie nie wykazywały tez odwołania.

Odnosząc się do postanowień OPU, których dotyczyły punkty 3-7 uzasadnienia odwołania, przede wszystkim należy podkreślić wagę, jaką dla wyniku postępowania ma sposób skonstruowania podstaw faktycznych stawianych zarzutów. Nie jest wystarczające zwrócenie uwagi na istnienie określonego problemu, czy proste zasygnalizowanie, że pewien wymóg może nie być do końca uzasadniony albo że możliwe są także inne rozwiązania, lecz niezbędne jest przedstawienie argumentacji, jak te okoliczności przekładają się na naruszenie przepisów prawa, w tym dlaczego świadczyć mają one o spełnieniu wszystkich przesłanek wskazanych w treści przepisu, którego naruszenie zamawiającemu się zarzuca. Sam fakt, że być może zasadne byłoby dopuszczenie przez Zamawiającego pewnych rozwiązań nie przesądza o tym, że doszło do naruszenia prawa. Tymczasem argumentacja przedstawiona przez Odwołującego w omawianym zakresie była nad wyraz lakoniczna i w

żaden sposób nie wyjaśniała, dlaczego wymagania wskazane w postanowieniach OPU, których dotyczyły punkty 3-7 uzasadnienia odwołania, naruszać miałyby przepisy ustawy Pzp, w szczególności art. 29 ust. 1-3 OPZ. W odwołaniu przedstawiono jedynie ogólne, nie poparte szerszym uzasadnieniem, postulaty wprowadzenia modyfikacji w SIWZ, przy czym Odwołujący nie wyjaśnił nawet dlaczego wprowadzone miałyby zostać zmiany określonej treści i dlaczego takie właśnie zmiany prowadziłyby do konwalidacji sprzecznych z prawem działań lub zaniechań Zamawiającego. Ponadto Odwołujący nie podjął na rozprawie żadnej polemiki ze stanowiskiem Zamawiającego przedstawionym w odpowiedzi na odwołanie w zakresie tych zarzutów.

Zarzut dotyczący pkt 4o OPU (pkt 3 uzasadnienia odwołania) sprowadzał się wyłącznie do niczym nieuzasadnionego postulatu dopuszczenia rozwiązania, które będzie blokowało niebezpieczną komunikację poprzez integrację z innymi urządzeniami sieciowymi, które posiada Zamawiający. Odwołujący nie przedstawił szczegółowej argumentacji w tym przedmiocie, zwłaszcza w kontekście tego, jak zaniechanie zarzucane Zamawiającemu miałoby naruszać prawo, co przesądza o bezzasadności zarzutu. Na jego bezzasadność wskazuje także fakt, iż – jak wyjaśniono w odpowiedzi na odwołanie - SIWZ dopuszcza tego rodzaju rozwiązanie, czemu Odwołujący na rozprawie nie zaprzeczał. Z analogicznych względów za nieuzasadniony Izba uznała zarzut dotyczący pkt 2e OPU (pkt 4 uzasadnienia odwołania), który ograniczał się do wniosku o dopuszczenia przez Zamawiającego dostarczania elementów zarządzania i raportowania w formie maszyn wirtualnych, z zastrzeżeniem, że wszystkie elementy systemu będą tego samego producenta. Zarzut ten nie zawiera podstawy faktycznej, a jedynie wniosek, który nie został poparty żadną argumentacją. Ponadto, jak wskazał Zamawiający w odpowiedzi na odwołanie, zgodnie z SIWZ elementy związane z zarządzaniem i raportowaniem mogą być dostarczone w formie maszyn wirtualnych, do czego Odwołujący w ogóle się nie odniósł i czego nie kwestionował.

Podobnie rzecz się ma jeśli chodzi o zarzut dotyczący pkt 3a OPU (pkt 5 uzasadnienia odwołania) – w tym przypadku Odwołujący wyraził wyłącznie własne oczekiwanie, aby Zamawiający dopuścił dostarczenie zestawu urządzeń z podziałem na poszczególne funkcjonalności, gdyż „jest to korzystne dla Zamawiającego”. Odwołujący nawet nie podjął próby wytłumaczenia dlaczego proponowana zmiana miałaby być dla Zamawiającego korzystna, nie mówiąc już o konieczności wyjaśnienia dlaczego przewidziane w SIWZ wymaganie miałoby w ogóle naruszać przepisy ustawy Pzp. Również za przedstawienie jedynie własnego postulatu uznać należy żądanie określenia w pkt 3b OPU (pkt 6 uzasadnienia odwołania), że Zamawiający zaakceptuje rozwiązanie, w którym urządzenia realizujące sandboxing będą dostarczane w postaci zamkniętej platformy sprzętowej, a inne elementy systemu mogą być dostarczone w formie maszyny wirtualnej. W odwołaniu brak

jest jakiejkolwiek argumentacji na poparcie tak sformułowanego żądania, na rozprawie zaś Odwołujący do tej kwestii nie odnosił się, nie polemizował także ze stanowiskiem Zamawiającego przedstawionym w odwołaniu.

Z kolei zarzut wskazany w pkt 7 uzasadnienia odwołania odnosi się do postanowienia pkt 3c OPU o innej treści niż jego rzeczywiste brzmienie. Przywołana przez Odwołującego treść ww. postanowienia nie znajduje się w OPU. Pkt 3c brzmi: „Zamawiający wyklucza analizę próbki z wiadomości email w chmurze" i nie odnosi się do kwestii możliwości wpięcia w infrastrukturę Zamawiającego w trybie in-line poprzez zastosowanie danych pochodzących ze SPAN portu urządzeń sieciowych. Tego rodzaju wymóg wprowadzono w pkt 4c OPU odnoszącym się jednak do zapewnienia ochrony kanału www, a nie ochrony kanału pocztowego, do którego referuje pkt 3 OPU i do którego odnosił się Odwołujący. Ponadto Odwołujący w żaden sposób nie wyjaśnił do czego niezbędna jest mu wiedza co do liczby jednoczesnych sesji http/https oraz liczby użytkowników systemu pocztowego oraz skrzynek pocztowych podlegających ochronie, nie wytłumaczył jak żądane informacje wpływają na kwestię jednoznaczności opisu przedmiotu zamówienia czy możliwość kalkulacji ceny oferty. Oczekiwanie Odwołującego w zakresie podania liczny skrzynek pocztowych podlegających ochronie jest tym bardziej niezrozumiałe, jeśli weźmie się pod uwagę fakt, że Zamawiający w punkcie 3h określił minimalną ilość skrzynek pocztowych, dla których urządzenie ma zapewniać ochronę. Odwołujący nie odniósł się ani do powyższej okoliczności, ani do stanowiska Zamawiającego, który w odpowiedzi na odwołanie wskazywał na wynikający z OPU wymóg trybu pracy Message Transfer Agent.

Biorąc pod uwagę wszystko powyższe Izba stwierdziła, iż nie zostały wykazane zarzuty wskazujące na opisanie przedmiotu zamówienia w sposób niejednoznaczny i niewyczerpujący, bez uwzględnienia wszystkich wymagań i okoliczności mogących mieć wpływ na sporządzenie oferty, czy też w sposób utrudniający uczciwą konkurencję i poprzez wskazanie pochodzenia, źródła, szczególnego procesu, który charakteryzuje wyłącznie producenta FireEye (art. 29 ust. 1-3 ustawy Pzp). Z kolei wskazany w petitum odwołania zarzut naruszenia art. 30 ust 4 ustawy Pzp przez zaniechanie dopuszczenia rozwiązań równoważnych i opisania warunków równoważności nie został nawet w uzasadnieniu odwołania omówiony. W świetle szczegółowo omówionych powyżej okoliczności bezzasadne okazały się także zarzuty odnoszące się do zaniechania podziału zamówienia na części i wyłączenia do odrębnego postępowania zakresu dotyczącego Mac OS.

W tym stanie rzeczy Izba uznała, że odwołanie podlega oddaleniu w całości i na podstawie art. 192 ust. 1 ustawy Pzp orzekła jak w sentencji.

O kosztach postępowania odwoławczego orzeczono stosownie do jego wyniku na podstawie art. 192 ust. 9 i 10 ustawy Pzp oraz § 3 pkt 1 Rozporządzenia Prezesa Rady Ministrów z dnia 15 marca 2010 r. w sprawie wysokości i sposobu pobierania wpisu od odwołania oraz rodzajów kosztów w postępowaniu odwoławczym i sposobu ich rozliczania (t.j. Dz. U. z 2018 r. poz. 972).

Przewodniczący: ……