Sygn. akt: KIO 1787/19

WYROK

z dnia 30 września 2019 r.

Krajowa Izba Odwoławcza - w składzie:

Przewodniczący: Danuta Dziubińska

Protokolant: Klaudia Ceyrowska

po rozpoznaniu na rozprawie w dniu 27 września 2019 r. odwołania wniesionego do Prezesa Krajowej Izby Odwoławczej w dniu 13 września 2019 r. przez wykonawcę **Intertrading Systems Technology Spółka z ograniczoną odpowiedzialnością** z siedzibą w Warszawie**,** Aleje Jerozolimskie 162A, 02-342 Warszawa w postępowaniu prowadzonym przez zamawiającego: **Kasa Rolniczego Ubezpieczenia Społecznego Centrala** z siedzibą w Warszawie**,** Aleja Niepodległości 190, 00-608 Warszawa

orzeka:

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

Stosownie do art. 198a i 198b ustawy z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (tj. Dz. U. z 2018 r., poz. 1986 z późn.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 1787/19

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

Kasa Rolniczego Ubezpieczenia Społecznego z siedzibą w Warszawie (dalej: „Zamawiający") prowadzi postępowanie o udzielenie zamówienia publicznego na podstawie ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tj. Dz. U. z 2018 r. poz. 1986 z późn.zm.), zwanej dalej: „ustawa Pzp", w trybie przetargu nieograniczonego pn. „Zakup licencji-rozbudowa oprogramowania systemu ochrony stacji końcowych użytkowników i serwerów", nr referencyjny 0000-ZP.261.15.2018 (dalej: „Postępowanie"). Wartość zamówienia przekracza kwoty określone w przepisach wydanych na podstawie art 11 ust. 8 ustawy Pzp. Ogłoszenie o zamówieniu zostało opublikowane w Dzienniku Urzędowym Unii Europejskiej w dniu 22 września 2018 r. pod numerem 2018/S 183-413530. Specyfikacja istotnych warunków zamówienia (dalej: „SIWZ") została zamieszczona na stronie internetowej Zamawiającego

Zamawiający powiadomił wykonawcę Intertrading Systems Technology sp. z o.o. o odrzuceniu jego oferty w dniu 3 września 2019 r. W dniu 13 września 2019 r. wykonawca ten (dalej: „Odwołujący" lub „IST") złożył odwołanie wobec czynności i zaniechań Zamawiającego, polegających na ocenie ofert oraz odrzuceniu jego oferty na podstawie art. 89 ust. 1 pkt 2 ustawy Pzp, jako sprzecznej z treścią SIWZ. Odwołujący zarzucił Zamawiającemu naruszenie:

1) art. 89 ust. 1 pkt 2 ustawy Pzp poprzez błędną ocenę oferty IST i uznanie, że oferta (jej przedmiot) jest sprzeczna z treścią (wymaganiami) SIWZ w zakresie pkt 1.3.2., 1.3.4. i 1.3.6., oraz
2) art. 7 ustawy Pzp poprzez nierówne traktowanie wykonawców.

Wskazując na powyższe, Odwołujący wniósł o uwzględnienie odwołania i nakazanie Zamawiającemu unieważnienia czynności oceny ofert i dokonania ponownej oceny ofert oraz uznania oferty IST za ofertę najkorzystniejszą.

W uzasadnieniu zarzutów Odwołujący wskazał min., iż zaoferował oprogramowanie/ rozwiązanie Symantec Endpoint Protection with Endpoint Detection and Response (dalej jako „Oprogramowanie Symantec"). W jego ocenie rozwiązanie to w całej rozciągłości spełnia wymagania określone w SIWZ i w żaden sposób nie stoi w sprzeczności z tym dokumentem. Zdaniem IST Zamawiający w ogóle nie wziął pod uwagę treści jego wyjaśnień z dnia 14 czerwca oraz 18 lipca 2019 roku. Przede wszystkim w swej decyzji w żaden sposób do tych wyjaśnień (obejmujących przekazane filmy instruktażowe) nie odniósł się, dokonana ocena była pobieżna, na niewystarczającym poziomie.

Odwołujący podał, iż Zamawiający twierdzi, że oferowane Oprogramowanie Symantec jest sprzeczne z treścią pkt 1.3.2 OPZ, zgodnie z którym *proponowane rozwiązanie musi*

zapewniać możliwości monitorowania i zapobiegania atakom poprzez blokowanie szeregu technik ataków bez konieczności połączenia do serwera zarządzania i/lub usługi chmurowej i nie bazując na metodzie sygnaturowej, ponieważ zgodnie z dokumentacją techniczną firmy Symantec funkcjonalność Memory Exploit Migration bazuje na sygnaturach, natomiast Zamawiający zastrzegł w SIWZ, iż ww. funkcjonalność nie może bazować na metodzie sygnaturowej. Tymczasem, jak wskazał IST, rozwiązanie Symantec Endpoint Protection posiada możliwość zapobiegania i monitorowania ataków wykorzystując mechanizmy niebazujące na metodzie sygnaturowej. Zaoferowane przez Odwołującego oprogramowanie wykorzystuje więcej niż jedną metodę ochrony. Funkcjonalność Memory Exploit Mitigation, na którą powołuje się Zamawiający w piśmie z dnia 3.09.2019 r. jest jednym z wielu mechanizmów wykorzystywanych do ochrony przed atakami i nie musi być uruchomiona by produkt „blokował szereg technik ataków". Produkt ten wykorzystuje w tym celu silnik Advanced Machine Learning, który nie bazuje na metodzie sygnaturowej oraz firewall systemowy, a także mechanizm Intrusion Detection, który nie musi korzystać z połączenia do serwera i/lub usługi chmurowej, bowiem istnieje możliwość wyłączenia tej opcji. Oprogramowanie Symantec, które zostało zaoferowane przez Odwołującego, to kompleksowe i modularne rozwiązanie. Wykorzystuje ono wiele metod ochrony, w tym w pewnych zakresach metodę sygnaturową, jednakże tylko jako uzupełnienie innych metod, w żaden sposób niekwestionowanych przez KRUS. Co istotne, bez żadnego uszczerbku dla skuteczności i poprawności działania przedmiotu zamówienia możliwe jest takie jego skonfigurowanie (ustawienie), aby metoda sygnaturowa nie była wykorzystywana.

Odwołujący wyjaśnił, że oferowane Oprogramowanie Symantec stanowi pewnego rodzaju całość i stąd nie można zaoferować go częściowo tj. np. bez określonych funkcjonalności. Możliwe jest natomiast takie jego skonfigurowanie, aby dane funkcjonalności nie były wykorzystywane, co de facto jest równoznaczne z ich brakiem. Taka sytuacja występuje w niniejszej sprawie. Oprogramowanie Symantec może tak zostać skonfigurowane, aby wykorzystywać inne metody niż sygnaturowe. To w praktyce oznacza, że metoda sygnaturowa w przypadku Symantec jest pewną dodatkową funkcjonalnością, a nie podstawową. Zatem gdyby technicznie możliwie było wyłączenie z tego produktu tej funkcjonalności i jego zaoferowanie bez niej, zaoferowany produkt z pewnością byłby zaakceptowany przez Zamawiającego. W ocenie IST możliwość wyłączenia tej funkcji należy traktować należy równoznacznie z taką sytuacją. Nie można bowiem karać wykonawcy za dodatkową funkcjonalność podczas gdy wszystkie podstawowe są spełnione. W ocenie Odwołującego zarzut Zamawiającego byłby zasadny wtedy, gdyby Oprogramowanie Symantec wykorzystywało tylko metodę sygnaturową bez innych metod.

Następnie Odwołujący wskazał, iż w ocenie Zamawiającego zgodnie z dokumentacją techniczną (Installation_and_Administration_Guide_SEP14.2.1(Polish).pdf) dostępną w języku polskim na stronie firmy Symatec oferowane rozwiązanie nie spełnia wymagania określonego w pkt 1.3.4. OPZ, zgodnie z którym *proponowane rozwiązanie musi wykorzystywać „moduły zapobiegania i blokowania technik ataków*". Jego działanie nie może być oparte o metodę sygnaturową, reputacyjną lub analizę heurystyczną pliku, musi istnieć możliwość zastosowania modułów blokowania technik ataków zarówno dla powszechnie znanych i popularnych aplikacji jak również własnych. Jest tak, zdaniem Zamawiającego, ponieważ, w ww. dokumentacji napisano m.in., że: funkcja ograniczenia ataków na pamięć posiada własne sygnatury ściągane wraz z plikami definicji funkcji zapobiegania włamaniom, emulator działający w lekkiej wirtualnej piaskownicy włącza skaner danych statystycznych, który zawiera silnik programu antywirusowego oraz mechanizm heurystyczny oraz współpracuje z innymi technologiami ochronnymi takimi jak analiza reputacji. Funkcja SONAR stosuje analizę heurystyczna oraz dane o reputacji w celu wykrywania nowych i nieznanych zagrożeń oraz używa systemu heurystycznego wykorzystującego sieć wywiadu internetowego firmy Symatec. Zamawiający wskazuje jednocześnie, że wykonawca w odpowiedzi na pytania z dnia 18 lipca br. sam wskazał, że oferowane przez niego rozwiązanie do celów technik analizy exploitów wykorzystuje mechanizmy Memory Exploit Mitigation oraz mechanizm heurystyczny SONAR. Tym samym Zamawiający stwierdził, że ofertowane rozwiązanie wykorzystuje moduły zapobiegania i blokowania technik ataków sprzecznych z pkt 1.3.4 SIWZ. Odwołujący nie zgodził się ze stanowiskiem Zamawiającego i wskazał, że mechanizm ograniczania ataków na pamięć zgodnie z nazewnictwem, znajdującym się w dokumentacji Symantec, nie wykonuje zadań zapobiegania i blokowania technik ataków, a jedynie je ogranicza. Funkcja ta nie musi być uruchomiona by całe rozwiązanie zapobiegało i blokowało techniki ataków. Mechanizmem właściwym dla zapobiegania i blokowania technik ataków jest system zapobiegania włamaniom, który nie bazuje na metodzie sygnaturowej. Emulator (inaczej mechanizm symulacyjny) zgodnie z SIWZ jest mechanizmem statycznej analizy plików spakowanych i w żaden sposób nie jest wykorzystywany w procesie zapobiegania i blokowania technik ataków. Pozwala on zapobiegać infekcjom szkodliwego oprogramowania, co następuje już po procesie diagnozy i blokowania technik ataków. Z punktu widzenia Odwołującego, Zamawiający myli wykorzystanie mechanizmów i celów jakie określił w OPZ. Funkcja SONAR zgodnie z opisem stosuje analizę heurystyczną i współpracuje z osobnym silnikiem Insight, który bazuje na mechanizmie reputacyjnym, ale oba silniki nie są wykorzystywane do zapobiegania i blokowania technik ataków. Funkcją ww. silników jest monitorowanie i analiza zachowania plików i aplikacji na systemach operacyjnych.

Wykonawca IST wskazał, że w odpowiedzi na pytania z Zamawiającego z dnia 18.07.2019 r. podał, że ofertowany przez niego produkt spełnia wymienione punkty dzięki użyciu technologii o nazwie Memory Exploit Mitigation (dalej: ,.MEM'"). MEM posiada szereg technik blokowania znanych i nieznanych ataków bazując jedynie na technikach blokowania eksploatowania aplikacji. Sama biblioteka nie potrzebuje do tego sygnatur, heurystyki, reputacji czy sandboxa (kontenera), ponieważ zawiera cały kod potrzebny do „zaszczepienia" działającego procesu. „Szczepionki" dostarczane są w formie zmiennej i mogą zostać automatyczne zaktualizowane razem z aktualizacją agenta Symantec Endpoint Protection. Kiedy system Symantec Endpoint Protection wykryje próbę ataku zatrzyma aplikację uniemożliwiając wykonanie złośliwego kodu oraz wyświetli nazwę ataku.

Odwołujący zauważył, że dokładnie w ten sam sposób (poprzez DLL Injection) działa konkurencyjne rozwiązania Palo Alto Traps w zakresie ochronny przed eksploitacją procesów, którego to rozwiązania Zamawiający w żaden sposób nie kwestionował. Wskazuje to, zdaniem IST na oczywiste naruszenie zasady równego traktowania wykonawców (art. 7 ustawy Pzp) i niezrozumiałe preferowanie wykonawcy oferującego rozwiązanie Palo Alto Traps, które jest znacznie droższe niż rozwiązanie oferowane przez Odwołującego.

Zdaniem Odwołującego za niezasadne należy uznać również stanowisko Zamawiającego w zakresie spełniania przez Oprogramowanie Symantec wymogów określonych w 1.3.6. OPZ, zgodnie z którym *proponowane rozwiązanie nie może stosować technik analizy exploitów wykorzystujących zasoby sprzętowe, takich jak lokalne środowisko symulacyjne typu „sandbox" lub zwirtualizowany kontener*. Zamawiający bowiem twierdzi, że oferowane Oprogramowanie Symantec jest sprzeczne z tym wymogiem, ponieważ zgodnie z dokumentacją producenta produktu Symantec Endpoint Protection 14.2 używany jest wirtualny sandbox. Tymczasem oferowane rozwiązanie Symantec nie wykorzystuje środowiska symulacyjnego (tzw. „sandbox'a") w celu analizy technik exploitów.

Odwołujący wskazał, że Zamawiający w punkcie 1.3.6 SIWZ określił, że mechanizmy symulacyjne nie mogą być wykorzystywane w celu stosowania technik analizy exploitów nie wykluczając przy tym samego wyposażenia w tę funkcjonalność samego programu czy też zastosowania wyżej wskazanych mechanizmów w inny sposób. Obecność mechanizmów symulacyjnych w oferowanym przez Odwołującego rozwiązaniu w żaden sposób nie stoi w sprzeczności z postanowieniami SIWZ. Obecność tego rozwiązania w oferowanym oprogramowaniu jest wykorzystywana przy technikach niszczenia spakowanych plików lub ewentualnie do niszczenia zawartych w nich szkodliwych plików. Ponadto do technik analizy exploitów oferowane rozwiązanie może wykorzystywać mechanizm SONAR, który to mechanizm służy do celów zapobiegania i blokowania technik ataków (co w żadnej mierze nie stoi w sprzeczności z ww. postanowieniem pkt 1.3.4 SIWZ). Zamawiający, bowiem zabronił

wykorzystania mechanizmów heurystycznych wykorzystywanych przez mechanizm SONAR do analizy exploitów, a nie do celów zapobiegania i blokowania technik ataków. Zamawiający mylnie łączy procesy analizy exploitów z procesami zapobiegania i blokowania technik ataków.

W podsumowaniu Odwołujący stwierdził, że Mechanizm Emulator w oprogramowaniu Symantec Endpoint Protection nie jest wykorzystywany jako technika analizy exploitów, a jako narzędzie wykrywające zawartość spakowanych i zaszyfrowanych plików. Mechanizmem właściwym wykrywającym techniki exploitów jest Memory Exploit Mitigation, który nie wykorzystuje emulacji, sandboxingu i innych form środowisk symulacyjnych. Zamawiający natomiast w ogóle nie wziął pod uwagę treści wyjaśnień Odwołującego z dnia 14 czerwca oraz 18 lipca 2019 roku (w tym także przekazanych filmów instruktażowych) i pomija fakt, że oferowany przez IST system zabezpieczeń składa się z różnych modułów, które Zamawiający z pomocą Odwołującego może wyłączyć i skonfigurować w taki sposób by metody ochrony były w pełni zgodne z SIWZ. Oferowane oprogramowanie stanowi jedną całość, z której Odwołujący nie może całkowicie wykluczyć rozwiązań nieakceptowanych przez Zamawiającego.

Na marginesie Odwołujący zauważył, że postępowanie Zamawiającego w tej sprawie budzi poważne wątpliwości, co do działania w zgodzie z zasadami uczciwiej konkurencji oraz równego traktowania stron. W szczególności. Zamawiający nie poddawał tak szczegółowej ocenie i badaniu rozwiązania konkurencyjnego (Pało Alto). Co więcej, pomimo tego, że rozwiązanie Pało Alto bazuje w niektórych elementach na rozwiązaniach podobnych jak oferowane przez IST (oraz Comtegre) (np. w zakresie wymogu z pkt 1.3.4), Zamawiający kwestionuje to tylko w odniesieniu do oferty Odwołującego, ale już nie oferty obejmującej rozwiązanie Palo Alto.

Pismem z dnia 26 września 2019 r. Zamawiający złożył odpowiedź na odwołanie, w którym wniósł o jego oddalenie w całości.

Odnosząc się do zarzutów odwołania, Zamawiający wskazał m.in., że dokonał odrzucenia oferty na podstawie analizy zgodności funkcji realizowanych przez oferowane przez Odwołującego oprogramowanie, których opis jest zawarty w dokumentacji producenta oprogramowania, z wymaganiami określonymi w SIWZ.

Zamawiający stwierdził, że zgodnie z dokumentacją techniczną (Installation_and_Administration_Guide_SEP14.2.1(Polish).pdf) dostępną w języku polskim na stronie firmy Symatec, oferowane przez Odwołującego oprogramowanie nie spełnia wymagań określonych w Rozdziale II SIWZ - Szczegółowy opis przedmiotu zamówienia (w treści uzasadnienia: „OPZ"). Zgodnie bowiem z dokumentacją techniczną, wskazaną przez Odwołującego w wyjaśnieniach z dnia 18 lipca 2019 r. jako dokumentację techniczną

oferowanego rozwiązania (dalej: „Dokumentacja techniczna”) oferowane przez Odwołującego rozwiązanie nie spełnia wymagań określonych w pkt:

1) 1.3.2. OPZ że względu na fakt, iż w ww. dokumentacji jest zapis, że funkcja ograniczenia ataków na pamięć posiada własne sygnatury ściągane wraz z plikami definicji funkcji zapobiegania włamaniom, a zatem bazuje na metodzie sygnaturowej;

2) 1.3.4 OPZ, ze względu na fakt, iż w ww. dokumentacji są zapisy wskazujące, że:

a) funkcja ograniczenia ataków na pamięć posiada własne sygnatury ściągane wraz z plikami definicji funkcji zapobiegania włamaniom,
b) emulator działający w lekkiej wirtualnej piaskownicy włącza skaner danych statycznych, który zawiera silnik programu antywirusowego oraz mechanizm heurystyczny oraz współpracuje z innymi technologiami ochronnymi takimi jak analiza reputacji,
c) funkcja SONAR stosuje analizę heurystyczna oraz dane o reputacji w celu wykrywania nowych i nieznanych zagrożeń oraz używa systemu heurystycznego wykorzystującego sieć wywiadu internetowego firmy Symantec,

z których wynika, że oferowane przez Odwołującego rozwiązanie wykorzystuje moduły zapobiegania i blokowania technik ataków w oparciu o metodę sygnaturowa, reputacyjną i analizę heurystyczną pliku. Nadto w swoich wyjaśnieniach z dnia 18 lipca 2019 r. Odwołujący wskazał, że oferowane przez niego rozwiązanie do celów technik analizy exploitów wykorzystuje mechanizmy Memory Exploit Mitigation oraz mechanizm heurystyczny SONAR, co jest niezgodne z pkt 1.3.4 SIWZ, gdyż oznacza, że wykorzystuje analizę heurystyczną pliku;

3) 1.3.6 ze względu na fakt, iż w dokumentacji jest zapis, że oferowane rozwiązanie używa emulatora (rodzaju programu komputerowego), który pracuje w lekkiej wirtualnej piaskownicy (sandbox), a zatem stosuje lokalne środowisko symulacyjne typu „sandbox”.

Zamawiający podał, iż nie zgadza się ze stwierdzeniem Odwołującego, zawartym w wyjaśnieniach z dniach 18 lipca 2019 r., że w oferowanym przez niego rozwiązaniu emulator nie ma opcji wyłączenia, jednak nie jest on wykorzystywany do wymaganego przez Zamawiającego celu (czyli do technik analizy exploitów). Z treści Dokumentacji technicznej wynika, bowiem, że emulator, który pracuje w lekkiej wirtualnej piaskownicy (sandbox) jest wykorzystywany w oferowanym rozwiązaniu, gdyż rozpakowuje i niszczy plik spakowany niestandardowym programem kompresującym w lekkiej piaskownicy wirtualnej na komputerze klienckim (...) oraz współpracuje z innymi technologiami ochronnymi, takimi jak funkcja ograniczania ataków na pamięć (str. 498 dokumentacji). Ponadto w kolejnym zdaniu ww. wyjaśnień Odwołujący wskazał, że do celów technik analizy exploitów oferowane przez niego

rozwiązanie wykorzystuje m.in. mechanizm heurystyczny SONAR, co jest niezgodne z pkt 1.3.4. SIWZ. Zamawiający kilkukrotnie zwracał się do Odwołującego o przedstawienie dokumentacji technicznej oferowanego oprogramowania udostępnianej przez jego producenta. W piśmie przekazanym do Zamawiającego w dniu 24 kwietnia 2019 r., Odwołujący przekazał Zamawiającemu dokument opatrzony tytułem „Specyfikacja techniczna oprogramowania oferowanego w odpowiedzi na „ogłoszenie o zamówieniu na zakup licencji - rozbudowa oprogramowania systemu ochrony stacji końcowych użytkowników i serwerów nr 0000-ZP-261.15.2018", który został przez niego sporządzony i podpisany, podczas gdy Odwołujący jest tylko sprzedawcą (dostawcą) oprogramowania i przedstawia dokument nie sygnowany przez producenta oprogramowania. W związku z tym Zamawiający uznał, iż nie może uznać, że jest to dokumentacja techniczna oprogramowania. Wobec powyższego Zamawiający w piśmie z dnia 10 czerwca 2019 r. ponownie wezwał Odwołującego do przedstawienia dokumentacji technicznej producenta oprogramowania dla potwierdzenia faktu, że oferowane oprogramowanie spełnia wymogi SIWZ. W odpowiedzi w dniu 14 czerwca 2019 r. Odwołujący przesłał dokumentację w postaci własnego opisu realizowanych funkcjonalności (opatrzoną klauzulą tajemnicy przedsiębiorstwa) oraz dokumentację filmową prezentującą sposoby wykorzystania (wyłączania) funkcji bliżej nieokreślonego oprogramowania. Tak jak poprzednio przekazane materiały nie posiadały znamion oficjalnej dokumentacji autoryzowanej przez producenta oprogramowania i nie mogły zostać uznane przez Zamawiającego. W przywołanym piśmie Odwołujący dodatkowo wskazywał, że nie istnieje dokumentacja techniczna oferowanego rozwiązania, cyt. "*Warto także w tym miejscu nadmienić, że aktualnie stosunkowo rzadko przygotowywana i udostępniana jest dokumentacja opisująca absolutnie wszystkie funkcjonalności danego oprogramowania, sposoby instalacji, konfiguracji. Niezliczona, bowiem ilość kombinacji tych wszystkich elementów, skutkowałaby tym, że tego rodzaju dokumenty, przy coraz bardziej skomplikowanych oprogramowaniach, gdyby powstawały musiałyby liczyć niekiedy nawet ponad tysiąc lub jeszcze więcej stron."*..... Zamawiający pismem z dnia 15 lipca 2019 r. ponownie zwrócił się z prośbą do Odwołującego o przedstawienie mu dokumentacji technicznej producenta oferowanego oprogramowania.

Zdaniem Zamawiającego Odwołujący nie chciał przedstawić Zamawiającemu przez długi okres czasu dokumentacji technicznej oferowanego rozwiązania pomimo, że producent oferowanego oprogramowania jest jednym z kluczowych światowych dostawców rozwiązań IT w obszarze bezpieczeństwa oprogramowania i w ocenie Zamawiającego przedstawienie ww. informacji nie powinno stanowić dla Odwołującego problemu. Przekazywana przez Odwołującego dokumentacja oprogramowania, w ocenie Zamawiającego nie była dokumentacją techniczną, gdyż nie spełniała wymagań dla takiej dokumentacji, ponieważ nie

zawierała m.in. opisu realizowanych funkcjonalności, sposobu instalacji, opisu konfiguracji. Stanowiła natomiast w znacznym stopniu przeredagowaną kopię wymagań zawartych w OPZ. Nadto oferowane przez Odwołującego oprogramowanie jest oprogramowaniem powszechnie dostępnym tzw. „pudełkowym" i nie zostało wyprodukowane przez firmę Symantec wyłącznie na potrzeby KRUS w zakresie wymagań opisanych przez Zamawiającego w SIWZ. Stąd też niezrozumiałym było postępowanie Odwołującego i nieprzekazywanie przez niego dokumentacji technicznej producenta. Wykonawca IST dopiero w piśmie z dnia 19 lipca 2019 r. przekazał Zamawiającemu link do strony producenta oferowanego Oprogramowania Symantec, gdzie Zamawiający mógł po kilkumiesięcznych próbach uzyskania od Odwołującego przedmiotowych informacji, zapoznać się ze specyfikacją techniczną producenta oferowanego oprogramowania.

Na podstawie przeprowadzonej analizy dokumentacji technicznej producenta oferowanego oprogramowania, Zamawiający podjął decyzję o odrzuceniu oferty, wskazując niezgodności oferowanego oprogramowania z wymaganiami określonymi w SIWZ. Zamawiający zauważył, że w złożonym odwołaniu Odwołujący nie odnosi się stricte do przedstawianych przez Zamawiającego powodów odrzucenia oferty, tylko w poszczególnych punktach ogólnie stwierdza, że jego zdaniem oferowane przez niego oprogramowanie spełnia wymagania SIWZ, nie podając konkretnych argumentów wynikających z dokumentacji producenta.

Zamawiający nie zgodził się również z zarzutem naruszenia zasad równego traktowania Wykonawców, wskazując, iż aktualnie trwa ocena złożonych w postępowaniu ofert i zgodnie z zasadami określonymi w art. 24aa i art. 26 ustawy Pzp, Zamawiający w pierwszej kolejności bada ofertę Wykonawcy, która została najwyżej oceniona. Tym samym, w ocenie Zamawiającego, zarzuty Odwołującego w tym zakresie są bezprzedmiotowe.

Izba dopuściła w poczet materiału dowodowego dokumentację postępowania złożoną przez Zamawiającego oraz dowody złożone na rozprawie przez Odwołującego, do których odniesienie znajduje się w dalszej części uzasadnienia.

Po zapoznaniu się z treścią dokumentacji postępowania, po przeprowadzeniu posiedzenia i rozprawy oraz wysłuchaniu stanowisk Stron Izba ustaliła i zważyła, co następuje:

Nie została wypełniona żadna z przesłanek, skutkujących odrzuceniem odwołania, o których stanowi art. 189 ust. 2 ustawy Pzp.

Wykazując swoje uprawnienie do wniesienia odwołania Odwołujący wskazał m.in., iż posiada w interes w złożeniu tego środka ochrony prawnej. Oferta IST jest ofertą najkorzystniejszą według przyjętych kryteriów oceny ofert. W konsekwencji, gdyby nie

czynność jej odrzucenia, powinna zostać uznana za najkorzystniejszą. Odrzucenie oferty powoduje brak możliwości osiągnięcia przez Odwołującego przychodu na poziomie ustalonej ceny ofertowej oraz utratę zakładanego zysku, a więc powoduje powstanie szkody po jego stronie.

Izba stwierdziła, że zaistniały przesłanki dla wniesienia odwołania, określone w art. 179 ust. 1 ustawy Pzp, tj. posiadanie przez Odwołującego interesu w uzyskaniu zamówienia oraz możliwości poniesienia szkody w wyniku naruszenia przez Zamawiającego przepisów ustawy. W przypadku potwierdzenia się zarzutów odwołania, Odwołujący miałby szansę uzyskania zamówienia i korzyści płynących z realizacji umowy zawartej w jego wyniku.

Pismem z dnia 17 września 2019 r. swoje przystąpienie do postępowania odwoławczego po stronie Zamawiającego zgłosił wykonawca 4PRIME Spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie, wnosząc o oddalenie w całości zarzutów przedstawionych w odwołaniu.

Na posiedzeniu Odwołujący oświadczył, iż nie otrzymał zgłoszenia przystąpienia ww. wykonawcy i nie wiedział, że takie zgłoszenie nastąpiło. Wykonawca 4PRIME Spółka z ograniczoną odpowiedzialnością wyjaśnił, że na prośbę Zamawiającego wysłał do niego swoje zgłoszenie przystąpienia do postępowania odwoławczego drogą elektroniczną oraz za pośrednictwem poczty przesłał je stronom postępowania. Nie jest jednak w stanie tego wykazać, ponieważ nastąpiło to listem zwykłym. Strony oświadczyły, że nie otrzymały zgłoszenia przesłanego pocztą.

Stosownie do art. 185 ust.2 ustawy Pzp *wykonawca może zgłosić przystąpienie do postępowania odwoławczego w terminie 3 dni od dnia otrzymania kopii odwołania, wskazując stronę, do której przystępuje, i interes w uzyskaniu rozstrzygnięcia na korzyść strony, do której przystępuje. Zgłoszenie przystąpienia doręcza się Prezesowi Izby w postaci papierowej albo elektronicznej opatrzone kwalifikowanym podpisem elektronicznym, a jego kopię przesyła się zamawiającemu oraz wykonawcy wnoszącemu odwołanie.*

W ocenie Izby skoro Przystępujący nie wykazał, że przekazał swoje zgłoszenie do postępowania odwoławczego Odwołującemu, należy uznać, iż nie wypełnił wymogów, o których mowa w ww. przepisie. Okoliczność, iż również Zamawiający nie otrzymał zgłoszenia przesłanego, jak twierdzi 4PRIME Sp. z o.o., za pośrednictwem poczty, podważa wiarygodność twierdzeń tego wykonawcy przedstawionych na posiedzeniu, że wysłał pismo do stron pocztą. Z tych względów, należało uznać, iż wykonawca ten nie stał się uczestnikiem postępowania odwoławczego.

Następnie Izba ustaliła, co następuje:

W pkt 1.3. Rozdziału II SIWZ – Szczegółowy opis przedmiotu zamówienia Zakup licencji – rozbudowa oprogramowania Systemu ochrony stacji końcowych użytkowników i serwerów, Opis funkcjonalny, stanowiącego załączniki nr 1do Umowy, przewidziano wymogi w zakresie zapobieganie atakom aplikacyjnym typu exploit. Objęte sporem wymogi dotyczą ppkt 1.3.2., 1.3.4. i 1.3.6., przywołanych w pełnym brzmieniu w przedstawionych powyżej pismach stron, jak i w informacji o odrzuceniu oferty Odwołującego, przedstawianej poniżej.

Pismem z dnia 3 września 2019 r. Zamawiający poinformował Odwołującego o odrzuceniu jego oferty podając, iż nastąpiło to na podstawie art. 89 ust. 1 pkt 2) ustawy Pzp oraz stwierdzając: „W ww. ofercie został zaoferowany przedmiot zamówienia: Symantec Endpoint Protection with Endpoint Detection and Response, który nie spełnia następujących wymagań określonych w Rozdziale II SIWZ- Szczegółowy opis przedmiotu zamówienia:

Pkt 1.3.2 Proponowane rozwiązanie musi zapewniać możliwości monitorowania i zapobiegania atakom poprzez blokowanie szeregu technik ataków bez konieczności połączenia do serwera zarządzania i/lub usługi chmurowej i nie bazując na metodzie sygnaturowej.

Zgodnie z dokumentacją techniczną (Tnstallation_and_Administration_Guide_SEP14.2.1(Polish).pdf) dostępną w języku polskim na stronie firmy Symantec (wskazaną przez Wykonawcę w wyjaśnieniach z dnia 18 lipca br. jako dokumentację techniczną oferowanego rozwiązania), pod adresem internetowym https://support.svmantec.com/us/en/article.aoc 11420.html. oferowane rozwiązanie nie spełnia ww. wymagania, ze względu na fakt, iż w ww. dokumentacji jest zapis, że funkcja ograniczenia ataków na pamięć posiada własne sygnatury ściągane wraz z plikami definicji funkcji zapobiegania włamaniom, a zatem bazuje na metodzie sygnaturowej. Na str. 434 ww. dokumentacji znajduje się następujący zapis: Funkcja Ograniczenie ataków na pamięć jest dostępna wyłącznie wówczas, gdy zainstalowano funkcję zapobiegania włamaniom. Funkcja Ograniczenie ataków na pamięć ma osobne sygnatury, które są pobierane wraz Z plikami definicji funkcji zapobiegania włamaniom.

Pkt 1.3.4 Proponowane rozwiązanie musi wykorzystywać moduły zapobiegania i blokowania technik ataków. Jego działanie nie może być oparte o metodę sygnaturowa, reputacyina lub analizę heurystyczna pliku. Musi istnieć możliwość zastosowania modułów blokowania technik ataków zarówno dla powszechnie znanych i popularnych aplikacji jak również aplikacji własnych.

Zgodnie z dokumentacją techniczną (Installation_and_Administration_Guide_SEP14.2.1(Polish).pdf) dostępną w języku polskim na stronie firmy Symantec (wskazaną przez Wykonawcę w wyjaśnieniach z dnia 18 lipca br.

jako dokumentację techniczną oferowanego oprogramowania), pod adresem internetowym https://suppoiT.symantec.com/us/en/articie.doc 11420.html. oferowane rozwiązanie nie spełnia ww. wymagania, ze względu na fakt, iż w ww. dokumentacji są zapisy, że:

1. Funkcja ograniczenia ataków na pamięć posiada własne sygnatury ściągane wraz z plikami definicji funkcji zapobiegania włamaniom.

2. Emulator działający w lekkiej wirtualnej piaskownicy włącza skaner danych statycznych, który zawiera silnik programu antywirusowego oraz mechanizm heurystyczny oraz współpracuje z innymi technologiami ochronnymi takimi jak analiza reputacji.

3. Funkcja SONAR stosuje analizę heurystyczna oraz dane o reputacji w celu wykrywania nowych i nieznanych zagrożeń oraz używa systemu heurystycznego wykorzystującego sieć wywiadu internetowego firmy Symantec.

Z powyższego wynika zatem, że oferowane rozwiązanie wykorzystuje moduły zapobiegania i blokowania technik ataków w oparciu o metodę sygnaturowa reputacyjna i analizę heurystyczna pliku.

Ad. 1) - na str. 434 ww. dokumentacji jest następujący zapis:

Funkcja Ograniczenie ataków na pamięć jest dostępna wyłącznie wówczas, gdy zainstalowano funkcję zapobiegania włamaniom. Funkcja Ograniczenie ataków na pamięć ma osobne sygnatury, które są pobierane wraz z plikami definicji funkcji zapobiegania włamaniom. Funkcje zapobiegania włamaniom i ograniczenia ataków na pamięć można jednak włączać i wyłączać niezależnie od siebie.

Ad.2 - na str. 498 ww. dokumentacji jest następujący zapis:

Emulator o dużej prędkości w programie Symantec Endpoint Protection powoduje, że złośliwe oprogramowanie myśli, że działa na zwykłym komputerze. Tymczasem emulator rozpakowuje i niszczy plik spakowany niestandardowym programem kompresującym w lekkiej piaskownicy wirtualnej na komputerze klienckim. Złośliwe oprogramowanie uruchamia wtedy całkowicie swoją zawartość, powodując, że zawarte w nim zagrożenia ujawniają się w zamkniętym środowisku. W tym momencie zawartością zajmuje się skaner danych statycznych, który zawiera silnik programu antywirusowego oraz mechanizm heurystyczny. Piaskownica jest ulotna i znika po zlikwidowaniu zagrożenia.

Emulator wymaga zaawansowanych technologii, które naśladują działanie systemów operacyjnych, interfejsów API i instrukcji procesora. Zarządza jednocześnie pamięcią wirtualną i uruchamia różne technologie heurystyczne i wykrywające, które badają zawartość złośliwego oprogramowania.

Emulator współpracuje z innymi technologiami ochronnymi, takimi jak zaawansowane uczenie maszynowe, funkcja ograniczania ataków na pamięć, monitorowanie zachowania i analiza reputacji

Ad.3 - na str. 546 ww. dokumentacji jest następujący zapis:

SONAR to funkcja ochrony w czasie rzeczywistym, która wykrywa potencjalnie destrukcyjne aplikacje podczas ich uruchamiania na komputerach. Funkcja SONAR zapewnia ochronę przed nowymi zagrożeniami, ponieważ wykrywa je, zanim zostaną utworzone tradycyjne definicje wirusów i programów typu spyware umożliwiające eliminację takich zagrożeń.

Funkcja SONAR stosuje również analizę heurystyczną oraz dane o reputacji w celu wykrywania nowych i nieznanych zagrożeń. Funkcja SONAR zapewnia dodatkowy poziom ochrony na komputerach klienckich oraz uzupełnia istniejącą ochronę przed wirusami i programami typu spyware, zapobieganie włamaniom, funkcję Ograniczenie ataków na pamięć oraz zaporę.

Funkcja SONAR używa systemu heurystycznego wykorzystującego sieć wywiadu internetowego firmy Symantec oraz prewencyjne monitorowanie lokalne na komputerach klienckich w celu wykrywania nowych zagrożeń. Funkcja SONAR wykrywa także zmiany lub sposób działania na komputerach klienckich, które należy monitorować.

Ad.3 - na str. 548 jest następujący zapis:

Funkcja SONAR używa analizy heurystycznej oraz danych dotyczących reputacji w celu podejmowania decyzji W przypadku wyłączenia wyszukiwani Insight funkcja SONAR dokonuje wykryć tylko przy użyciu analizy heurystycznej.

Liczba fałszywych alarmów może wzrosnąć, a ochrona zapewniana przez funkcję SONAR jest ograniczona.

Dodatkowo w swoich wyjaśnieniach z dnia 18 lipca br. Wykonawca sam wskazuje, że oferowane przez niego rozwiązanie do celów technik analizy exploitów wykorzystuje mechanizmy Memory Exploit Mitigation oraz mechanizm heurystyczny SONAR, co jest nie zgodne z pkt 1.3.4 SIWZ, gdyż oznacza, że wykorzystuje analizę heurystyczna pliku.

Pkt 1.3.6 Proponowane rozwiązanie nie może stosować technik analizy exploitów wykorzystujących zasoby sprzętowe, takich jak lokalne środowisko symulacyjne typu “sandbox” lub zwirtualizowany kontener.

Zgodnie z dokumentacją techniczną (Installation_and_Administration_Guide_SEP14.2.1(Połish).pdf) dostępną w języku polskim na stronie firmy Symantec (wskazaną przez Wykonawcę w wyjaśnieniach z dnia 18 lipca br. jako dokumentację techniczną oferowanego oprogramowania), pod adresem internetowym

https://support.symantec.com/us/en/article.docll420.html, oferowane rozwiązanie nie spełnia ww. wymagania, ze względu na fakt, iż w dokumentacji jest zapis, że oferowane rozwiązanie używa emulatora (rodzaju programu komputerowego), który pracuje w lekkiej wirtualnej piaskownicy (sandbox), a zatem stosuje lokalne środowisko symulacyjne typu .,sandbox". Na str. 498 ww. dokumentacji jest następujący zapis:

Emulator o dużej prędkości w programie Symantec Endpoint Protection powoduje, że złośliwe oprogramowanie myśli, że działa na zwykłym komputerze. Tymczasem emulator rozpakowuje i niszczy plik spakowany niestandardowym programem kompresującym w lekkiej piaskownicy wirtualnej na komputerze klienckim. Złośliwe oprogramowanie uruchamia wtedy całkowicie swoją zawartość, powodując, że zawarte w nim zagrożenia ujawniają się w zamkniętym środowisku. W tym momencie zawartością zajmuje się skaner danych statycznych, który zawiera silnik programu antywirusowego oraz mechanizm heurystyczny. Piaskownica jest ulotna i znika po zlikwidowaniu zagrożenia.

Jednocześnie Wykonawca w wyjaśnieniach z dniach 18 lipca br. stwierdził, że w oferowanym przez niego rozwiązaniu emulator nie ma opcji wyłączenia jednak nie jest on wykorzystywany do wymaganego przez zamawiającego celu (czyli do technik analizy' exploitów). Zamawiający nie może zgodzić się z tym stwierdzeniem Wykonawcy, gdyż z ww. treści dokumentacji wynika, że emulator, który pracuje w lekkiej wirtualnej piaskownicy (sandbox) jest wykorzystywany w oferowanym rozwiązaniu, gdyż rozpakowuje i niszczy plik spakowany niestandardowym programem kompresującym w lekkiej piaskownicy wirtualnej na komputerze klienckim (...) oraz współpracuje z innymi technologiami ochronnymi, takimi jak funkcja ograniczania ataków na pamięć (str. 498 dokumentacji).

Ponadto w kolejnym zdaniu ww. wyjaśnień Wykonawca wskazuje, że do celów technik analizy exploitów oferowane przez niego rozwiązanie wykorzystuje m.in. mechanizm heurystyczny SONAR. co, jak wskazano wyżej, jest niezgodne z pkt 1.3.4. SIWZ. „

Izba zważyła, co następuje:

Odwołanie nie zasługuje na uwzględnienie.

Zgodnie z art. 89 ust. 1 pkt 2 ustawy Pzp *zamawiający odrzuca ofertę, jeżeli jej treść nie odpowiada treści specyfikacji istotnych warunków zamówienia, z zastrzeżeniem art. 87 ust. 2 pkt 3.*

Przepis ten wskazuje, iż kluczowym dla stwierdzenia wypełnienia się przesłanki odrzucenia oferty na jego podstawie jest wykazanie, iż oferta nie odpowiada wymogom merytorycznym określonym przez zamawiającego w specyfikacji istotnych warunków zamówienia. W orzecznictwie Krajowej Izby Odwoławczej podkreśla się, że niezgodność treści oferty z treścią specyfikacji istotnych warunków zamówienia powinna być oceniania z uwzględnieniem

definicji oferty zawartej w art. 66 k.c., tj. niezgodności oświadczenia woli wykonawcy z oczekiwaniami zamawiającego, odnoszącymi się do merytorycznego zakresu przedmiotu zamówienia, a więc materialnej sprzeczności zakresu zobowiązania zawartego w ofercie z zakresem zobowiązania, którego zamawiający oczekuje, zgodnie z postanowieniami specyfikacji istotnych warunków zamówienia.

W razie wątpliwości co do zgodności treści oferty z treścią specyfikacji istotnych warunków zamówienia w toku badania i oceny ofert zamawiający może żądać od wykonawców wyjaśnień dotyczących treści złożonych ofert. Wynika to z art. 87 ust. 1 ustawy Pzp, który stanowi, iż *w toku badania i oceny ofert zamawiający może żądać od wykonawców wyjaśnień treści złożonych ofert. Niedopuszczalne jest prowadzenie między zamawiającym a wykonawcą negocjacji dotyczących złożonej oferty oraz, z zastrzeżeniem ust. 1a i 2, dokonywanie jakiejkolwiek zmiany w jej treści.*

W okolicznościach przedmiotowej sprawy, jak wynika z odpowiedzi na odwołanie, co znajduje potwierdzenie w przedłożonej dokumentacji postepowania oraz nie jest kwestionowane przez Odwołującego, Zamawiający kilkakrotnie zwracał się do Odwołującego o wyjaśnienia treści oferty. Przepisy ustawy Pzp nie regulują kwestii obowiązku wykonawcy udzielenia wyjaśnień, jednakże, z uwagi na to, że leży to w jego interesie z uwagi na to, że może zapobiec odrzuceniu jego oferty, dochowując staranności w działaniu wymaganej od profesjonalisty, Odwołujący we własnym dobrze pojmowanym interesie, powinien udzielić wyczerpujących, szczegółowych wyjaśnień i wykazać, że jego oferta jest zgodna z oczekiwaniami Zamawiającego. Tymczasem, w ocenie Izby, udzielane wyjaśnienia przez Odwołującego nie spełniają tego wymogu.

Na rozprawie Odwołujący stwierdził, iż decyzja o odrzuceniu jego oferty jest, co najmniej przedwczesna. W jego ocenie bowiem istotą sporu jest to, czy w świetle postanowień SIWZ możliwe było zaoferowanie oprogramowania, które zawiera więcej funkcji, niż oczekuje Zamawiający, z możliwością wyłączenia tych, których nie chce. Natomiast tematy, co do których Zamawiający ma wątpliwości powinien wyjaśnić zwracając się do Odwołującego, tj. pytając, co się stanie w przypadku wyłączenia niechcianych funkcjonalności, tj. czy inne funkcjonalności w takim przypadku będą spełnione. Zdaniem Odwołującego decyzja o odrzuceniu jego oferty nie dotyczy kwestii związanych z jednolitością konfiguracji. Zamawiający nie prosił o jednolitą konfigurację, nie zadał pytania czy wyłączenie niechcianych przez niego funkcji negatywnie wpłynie na inne funkcjonalności. W związku z tym nie dał szansy Odwołującemu ustosunkowania się do takiego stanowiska. Odwołujący zwrócił również uwagę, że OPZ mieści się tylko na 4 stronach, zaś dokumentacja producenta to ok. 1000 stron.

W ocenie Izby zgromadzony w sprawie materiał dowodowy nie potwierdza stanowiska Odwołującego.

Wbrew stanowisku Odwołującego, w ocenie Izby istotą sporu nie jest to, czy w świetle postanowień SIWZ możliwe było zaoferowanie oprogramowania, które zawiera więcej funkcji, niż oczekuje Zamawiający, z możliwością wyłączenia tych, których nie chce. Nie jest bowiem sporne, że w Oprogramowaniu Symantec występuje więcej funkcji, niż wymagane przez Zamawiającego i że istnieje techniczna możliwość ich wyłączania - Zamawiający na rozprawie oświadczył, iż nie neguje możliwości wyłączenia określonych funkcji. Zamawiający nie kwestionował zatem technicznej możliwości wyłączenia określonych funkcjonalności, lecz oczekiwał wykazania spełniania wymogów SIWZ m.in. w zakresie opisu funkcjonalnego – Rozdział II SIWZ, w tym, jego pkt 1.3. dotyczącego zapobieganie atakom aplikacyjnym typu exploit.

Istotą sporu jest natomiast to, czy Odwołujący zaoferował rozwiązanie, które wypełnia wymogi określone w ww. postanowieniach OPZ i wykazał to Zamawiającemu na jego wystąpienia o wyjaśnienia w trybie art. 87 ust. 1 ustawy Pzp.

Jak stwierdził Odwołujący na rozprawie, w sprawie chodzi o konfigurację oprogramowania i kwestie funkcjonalności oraz, że odczytuje, że intencją SIWZ było to, aby Zamawiający otrzymał oprogramowanie, które będzie mógł używać w określony sposób. Nie zostało to zanegowane przez Zamawiającego. Należy, zatem uznać, iż Odwołujący winien wykazać Zamawiającemu, iż zaoferowane przez niego oprogramowanie będzie mogło być używane zgodnie z wymogami określonymi w SIWZ. Tymczasem w ocenie Izby Odwołujący tego nie wykazał Zamawiającemu, pomimo otrzymywanych wystąpień o wyjaśnienia, jak również nie uczynił tego na rozprawie.

W piśmie z dnia 10 czerwca 2019 r. Zamawiający wystąpił o udzielenie szczegółowych wyjaśnień w jaki sposób, w oferowanym produkcie, spełnione są wymagania określone w pkt 1.3.2, 1.3.4. i 1.3.6. Rozdziału II SIWZ. Zamawiający wskazał, iż z analizy zapisów dokumentacji technicznej producenta oferowanego przez Odwołującego oprogramowania, dostępnej na jego stronie internetowej, wynika, że nie spełnia ono wymogów określonych w ww. pkt OPZ. Zamawiający stwierdził również, że w jego ocenie przekazana przez Odwołującego w piśmie z dnia 24 czerwca 2019 r. dokumentacja oferowanego rozwiązania nie jest dokumentacją techniczna, gdyż nie spełnia wymagań dla takiej dokumentacji, ponieważ nie zawiera m.in. opisu realizowanych funkcjonalności, sposobu instalacji, opisu konfiguracji. Przesłana dokumentacja stanowi w znacznym stopniu przeredagowaną kopię wymagań zawartych w Szczegółowym opisie przedmiotu zamówienia (Rozdział II SIWZ). W związku z tym Zamawiający poprosił o przedstawienie szczegółowych informacji odnośnie

opisu funkcjonalności realizowanych przez oferowane rozwiązanie, a także odnośnie sposobu jego instalacji i opisu konfiguracji oraz na potwierdzenie, że oferowane oprogramowanie spełnia wymagania określone w SIWZ – specyfikacji technicznej producenta oferowanego oprogramowania. Ponadto Zamawiający poprosił o informację, czy przedmiotem oferty jest oprogramowanie powszechnie dostępne – „pudełkowe" czy oprogramowanie wyprodukowane przez Symantec wyłącznie na potrzeby KRUS w zakresie wymagań opisanych przez Zamawiającego w SIWZ.

Pismem z dnia 14 czerwca 2019 r., Odwołujący przekazał dokumentację filmową producenta dotyczącą sposobu instalacji oprogramowania oraz jego konfiguracji, potwierdzające jego zdaniem spełnianie ww. pkt SIWZ i wskazał, iż przedmiotem oferty jest pakiet oprogramowania, w skład którego wchodzi standardowe oprogramowanie firmy Symantec, a jego konkretne ustawienia (konfiguracja) umożliwiające spełnienie wszystkich określonych w SIWZ wymogów technicznych dokonywane będzie indywidualnie na potrzeby KRUS. W konsekwencji Zamawiający otrzyma w efekcie produkt przystosowany do jego konkretnych oczekiwań, które zostały zastrzeżone, jako tajemnica przedsiębiorstwa.

Zamawiający ocenił, iż powyższe nie jest wystarczające do potwierdzenia spełniania wymagań SIWZ, określonych w ww. punktach OPZ. Z tych względów pismem z dnia 15 lipca 2019 r. Zamawiający zwrócił się do Odwołującego zaznaczając m.in., iż „zgodnie z treścią SIWZ i wyrokiem KIO z dnia 1 marca 2019 roku sygnatura akt: KIO 265/19 i KIO 266/19, wezwał Wykonawcę do przedłożenia specyfikacji technicznej producenta oferowanego oprogramowania (pismo z dnia 11.04.2019 r.) oraz do wyjaśnień dotyczących oferowanego produktu (pismo z dnia 10.06.2019 r.).Jednakże przedstawiona dotychczas dokumentacja oferowanego oprogramowania firmy SYMANTEC, jak i dodatkowe informacje, nie wyjaśniają wszystkich wątpliwości związanych ze zgodnością oferowanego oprogramowania z wymaganiami zawartymi w SIWZ, a tym samym nie potwierdzają ich spełnienia. Przedstawione dotychczas przez Państwa materiały dotyczące oferowanego oprogramowania są w dużej mierze kopią opisu przedmiotu zamówienia przygotowanego przez Zamawiającego, a nie specyfikacją techniczną, którą zgodnie z wymogami zawartymi w SIWZ Wykonawca zobowiązany był przedłożyć. Dodatkowo przedstawiona dokumentacja nie opisuje w żaden sposób wymaganych funkcjonalności czy sposobu ich instalacji i konfiguracji. W/w dokumentacja nie wyjaśnia Zamawiającemu poniższych wątpliwości. W związku z powyższym na podstawie art. 87 ust. 1 ustawy Pzp, prosimy również o wyjaśnienie następujących kwestii oraz wskazanie w przekazanej dokumentacji technicznej oferowanego produktu opisu tych wyjaśnień:

1. W jaki sposób można wyłączyć usługę „sandbox” oraz jakie funkcjonalności zostaną wyłączone przy wyłączonej usłudze „sandbox” (pkt 1.3.6. Szczegółowego opisu przedmiotu zamówienia);
2. Czy przy wyłączonej usłudze „sandbox” pliki dalej są wysyłane do chmurowego środowiska ATP;
3. Przedmiotem zamówienia jest dostawa licencji a nie instalacja, konfiguracja i modyfikacja zamawianego oprogramowania. Ponieważ w swoich wyjaśnieniach powołują się Państwo na informację, że system zostanie sparametryzowany pod spełnienie wymagań SIWZ, prosimy o wyjaśnienie w jaki sposób firma Symantec będzie kontaktować się Zamawiającym w celu ustalenia parametrów systemów tzn. odpowiednio sparametryzowanych pakietów instalacyjnych oraz czy wersje przygotowane na potrzeby Zamawiającego będą dostępne z poziomu konta firmowego w domenie Symantec.com oraz że firma Symantec będzie utrzymywać, aktualizować i modyfikować wersje oferowanego oprogramowania na potrzeby Zamawiającego.”

Zamawiający oczekiwał odpowiedzi w terminie do 18 lipca 2019 r. Pismem z dnia 18 lipca 2019 r., które do dokumentacji postępowania przekazanej do KIO przez Zamawiającego z prezentatą, wpłynęło do niego w dniu 19 lipca 2019 r., Odwołujący podał:

„1)Zgodnie z wymogami punktu 1.3.6 - „Proponowane rozwiązanie nie może stosować technik analizy exploitów wykorzystujących zasoby sprzętowe, takich jak lokalne środowisko symulacyjne typu „sandbox" lub zwirtualizawany kontener" oświadczamy iż oferowane rozwiązanie Symantec nie wykorzystuje mechanizmu „emulator" do analizy technik exploitów. Zgodnie z opisem technologii w dokumentacji producenta „Symantec™ Endpoint Protection 14.2 Installation and Administration Guide" (link do dokumentacji w załączeniu) strony 449-450 emulator nie ma opcji wyłączenia jednak nie jest on wykorzystywany do wymaganego przez zamawiającego celu. Do celów technik analizy exploitów rozwiązanie Symantec wykorzystuje mechanizmy Memory Exploit Mitigation oraz mechanizm heurystyczny SONAR.

2) Nie należy mylić mechanizmu opisanego w odpowiedzi na pierwsze pytanie- tj. Emulatora z mechanizmem sandbox które oferent zgodnie z wymogiem z punktu 1.5.5 oferuje w rozwiązaniu Symantec. Rozwiązanie Symantec oferuje środowisko sandbox spełniające wszelkie wymogi zapisu 1.5.5 OPZ poprzez chmurowe środowisko analizy i zapobiegania nieznanym złośliwym plikom wykonywalnym a także dostarcza po wykonanej analizie pełny raport z jej wyników. Jednocześnie rozwiązanie oferuje możliwość automatycznego i ręcznego wysyłania plików do analizy w chmurze producenta oraz możliwość wyłączenia tej funkcji przed administratora zamawiającego w pożądanym momencie.

3) Oferent jako parametryzację produktu pod wymagania SIWZ miał na myśli możliwość tworzenia gotowych paczek instalacyjnych dla agentów oraz włączania i wyłączania poszczególnych modułów czy regulowania czułości poszczególnych mechanizmów chroniących przez zamawiającego w dowolnym momencie. Producent oferuje standardowe pakiety instalacyjne które następnie będą przez zamawiającego lub przy asyście wykonawcy/producenta parametryzowane przy procesie instalacji. Taki mechanizm nie powoduje konieczności indywidualizacji pakietu instalacyjnego a co za tym idzie nie wiąże się z koniecznością utrzymywania aktualizacji i modyfikacji indywidualnych wersji dla zamawiającego. Standardowe pakiety instalacyjne z możliwością ich parametryzacji będą dostępne dla zamawiającego na portalach z oprogramowaniem producenta. „

W ustosunkowaniu się do zarzutu nieodpowiedniej dokumentacji z oczekiwaniami Zamawiającego Odwołujący podał, że dokumentacja w pełni odpowiadająca wymaganiom zamawiającego dostępna jest oficjalnie na stronach producenta. Najpełniejszą i wyczerpującą (kwestie instalacji, konfiguracji, wymagań systemowych i opisu technicznego) dokumentacją będzie instrukcja instalacji, administracji i radzenia sobie z problemami dostępna dla klientów firmy Symantec dostępne na podanych przez niego w tym piśmie stronach.

Powyższe wskazuje, że wbrew stanowisku Odwołującego Zamawiający dawał temu wykonawcy szansę wykazania, że pomimo posiadania w standardzie przez zaoferowane przez niego oprogramowanie niechcianych przez niego funkcji, ich wyłączenie nie wpłynie negatywnie na inne funkcjonalności. Skoro, bowiem w piśmie z dnia 10 czerwca 2019 r. Zamawiający (podkreślając ten fragment w tekście) poprosił m.in. o przedstawienie szczegółowych informacji odnośnie opisu funkcjonalności realizowanych przez oferowane rozwiązanie oraz odnośnie sposobu jego instalacji i opisu konfiguracji, to oznacza, że Odwołujący miał szansę wykazania powyższych okoliczności i we własnym dobrze pojętym interesie powinien to uczynić.

Odwołujący, skoro oferuje określone oprogramowanie w postępowaniu o udzielenie zamówienia publicznego, powinien znać dokumentację techniczną tego rozwiązania, niezależnie od tego czy jest jego producentem, partnerem producenta czy jedynie sprzedawcą, bowiem przed złożeniem oferty, znając wymogi określone w SIWZ, winien ocenić czy oferowane przez niego oprogramowanie je spełnia. W razie wątpliwości np. interpretacyjnych co do sposobu rozumienia postanowień SIWZ w tym zakresie, powinien zwrócić się do Zamawiającego w trybie przewidzianym w ustawie Pzp o wyjaśnienia.

Nie jest sporne pomiędzy stronami, że Dokumentacja techniczna zawiera informacje przedstawione przez Zamawiającego w informacji o odrzuceniu oferty wykonawcy IST.

Odwołujący znając dokumentację techniczną producenta oprogramowania musiał wiedzieć, że znajdują się w niej zapisy wskazujące na niezgodność rozwiązania z wymogami SIWZ. Tym bardziej, że wymogi OPZ w tym zakresie, jak zauważył na rozprawie, zawarte są tylko na 4 stronach. Okoliczność, iż jak podał na rozprawie, dokumentacja producenta to ok. 1000 stron, tego nie zmienia. Wiedza o zapisach w treści dokumentacji technicznej producenta, wskazujących na niezgodność rozwiązania z wymogami SIWZ, powinna zatem skłonić Odwołującego do rzetelnego udzielenia wyjaśnień Zamawiającemu w żądanym przez niego zakresie dotyczącym opisu funkcjonalności, w tym do podania skutków ewentualnego wyłączenia poszczególnych niechcianych funkcjonalności dla działania pozostałych funkcjonalności. Nie powinno bowiem budzić wątpliwości, co zauważył Odwołujący, iż Zamawiający ma otrzymać oprogramowanie, które będzie mógł używać w określony sposób. Odwołujący nie wykazał, że SIWZ nie wymaga spójnie pracującego kompleksowego oprogramowania. Przyjąć zatem należy, że celem zamówienia jest pozyskanie przez Zamawiającego kompleksowego rozwiązania, spójnie działającego, zgodnie z wymogami OPZ.

W ocenie Izby z treści wystąpienia Zamawiającego w wyjaśnienia wynika jego oczekiwanie co do uzyskania szczegółowych informacji w zakresie funkcjonalności, w czym, skoro po stronie Odwołującego istniała wiedza m.in. o potrzebie wyłączenia określonych funkcji, zawiera się także przedstawienie z jego strony informacji odnośnie tego co się stanie w przypadku wyłączenia niechcianych przez Zamawiającego funkcji i jakie to będzie miało przełożenie na funkcjonalność Oprogramowania i wypełnienia wymogów SIWZ. Ww. pkt 1.3. OPZ określa wymogi, jakie mają być spełnione przez oferowane oprogramowanie. Odwołujący tego jednak zaniedbał w odpowiedziach na żądanie wyjaśnień z dnia 10 czerwca 2019 r. i 15 lipca 2019 r. Nadto w odpowiedzi na drugie z ww. pism odnośnie pkt 1.3.6. podał, ze emulator nie ma opcji wyłączania. Do technik analizy exploitów rozwiązanie Symantec wykorzystuje mechanizmy Memory Exploit Mitygation oraz mechanizm heurystyczny Sonar, podczas gdy stosownie do pkt 1.3.4. Zamawiający zakazał, aby zastosowanie miało stosowanie technik opartych o metodę reputacyjną i analizę heurystyczną. Nadto, jak słusznie zauważył na rozprawie Zamawiający, w odwołaniu w odniesieniu do argumentacji dotyczącej funkcji Sonar, Odwołujący w odniesieniu do pkt 1.3.6. OPZ wskazuje, że ma być ona włączona (pkt 35 odwołania), natomiast ma być wyłączona dla spełnienia wymogu pkt 1.3.4. OPZ (pkt 27 odwołania). Zamawiający stwierdził, iż jeśli chodzi o pkt 1.3.6. i wskazany tam emulator i odniesienie do Sandbox, to może on być wykorzystywany na 2 sposoby, tj. do niszczenia plików oraz do analizy złośliwych plików w wyselekcjonowanym środowisku, oraz zauważył, że Odwołujący oświadczył, że wykorzystuje ten mechanizm do ograniczenia ataków na pamięć, który musi być włączony, aby spełnić jeden z ww. wymogów, a musi być wyłączony,

żeby spełnić drugi z tych wymogów. Zauważenia wymaga również, iż na rozprawie Odwołujący podał, że jeśli chodzi o metodę sygnaturową, to należy ją rozumieć na 2 sposoby: jako sposób rozpoznawania zagrożenia oraz jako procedurę przygotowania – opis metody ataku oraz, że w Dokumentacji Symantec termin dotyczący metody sygnaturowej używany jest w drugim znaczeniu. Tymczasem, jak stwierdził Zamawiający na rozprawie i co wynika z brzmienia ww. pkt 1.3.2. OPZ, Zamawiający wyłączył możliwość bazowania na metodzie sygnaturowej, nie zawężając tego do jednego z podanych przez Odwołującego sposobu jej rozumienia. Na rozprawie Odwołujący stwierdził, że jest różnica pomiędzy SIWZ, a tym, co oferuje.

Na rozprawie Odwołujący wykazywał, że cele określone we wskazanych przez Zamawiającego w informacji o odrzuceniu jego oferty punktach pkt 1.3.2, 1.2.4 i 1.3.6 OPZ są spełnione za sprawą innych funkcjonalności oferowanego oprogramowania, niż te, których zakazał Zamawiający, a te zakazane przez Zamawiającego w ww. punktach mogą być wyłączone, jednakże ani na rozprawie, ani w toku badania i oceny ofert, pomimo wystąpień o wyjaśnienia, nie wykazał, że wyłączenie określonych funkcjonalności dla celu spełnienia jednego z wymogów, nie wpłynie negatywnie na pozostałe wymogi i działanie oprogramowania, nie wykazał, że wyłączanie określonych funkcjonalności nie spowoduje niespójności z pozostałymi wymogami jego funkcjonalności określonymi w OPZ.

W okolicznościach analizowanej sprawy w wyniku wystąpień o wyjaśnienia Zamawiający nie uzyskał potwierdzenia zgodności oferty Odwołującego z treścią SIWZ, a Dokumentacja techniczna zaoferowanego przez tego Wykonawcę oprogramowania zawiera informacje wskazujące wprost na brak spełnienia wymogów SIWZ.

Analiza dowodów złożonych przez Odwołującego w postaci, według jego oświadczenia, wyciągu z poszczególnych kart Dokumentacji technicznej (dowody nr 1÷11) oraz płyty CD z filmem wskazującym na możliwość wyłączania poszczególnych funkcji oprogramowania (dowód nr 12), co do zasady potwierdzają okoliczności bezsporne. Jak wyżej zostało wskazane, nie jest kwestionowane przez Zamawiającego to, że Oprogramowanie Symantec posiada także inne funkcje, niż te które wyraźnie zaznaczył w OPZ, że nie mają być wykorzystywane. Nadto zauważenia wymaga, iż twierdzenie Odwołującego, że właściwym byłoby wykorzystywanie innych mechanizmów, wskazanych w tabeli zamieszczonej w dowodzie nr 1, który odnosi się do spełnienia wymagań z pkt 1.3.2, nie znajduje potwierdzenia w przedłożonych dowodach. Jak słusznie zauważył Zamawiający z dowodu nr 2 nie wynika, że mechanizm AML oferowany przez Odwołującego będzie zapobiegał atakom poprzez blokowanie szeregu technik ataku, jak tego wymaga pkt 1.3.2.

Z tych względów zarzut naruszenia art. 89 ust. 1 pkt 2 ustawy Pzp należy uznać za nieudowodniony. Ciężar dowodu w tym zakresie stosownie do art. 6 Kodeksu cywilnego w związku z art. 14 ust. 1 ustawy Pzp spoczywał na Odwołującym.

Zgodnie z przepisem art. 192 ust. 2 ustawy Pzp Izba uwzględnia odwołanie w przypadku naruszenia przez zamawiającego przepisów ustawy, które miało wpływ lub może mieć istotny wpływ na wynik postępowania o udzielenie zamówienia. W sprawie nie zostało wykazane, że doszło do naruszenia przepisów, które miało istotny wpływ na wynik postępowania.

Z tych względów na podstawie art. 192 ust. 1 ustawy Pzp, Izba orzekła jak w pkt 2 sentencji wyroku.

O kosztach postępowania orzeczono stosownie do wyniku, na podstawie art. 192 ust. 9 i 10 ustawy Pzp oraz w oparciu o przepisy § 3 pkt 1 i 2 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: ……..……..