Sygn. akt KIO 2478/19

WYROK

z dnia 23 grudnia 2019 r.

Krajowa Izba Odwoławcza – w składzie:

Przewodniczący: Piotr Kozłowski
Monika Kawa-Ogorzałek
Daniel Konicz

Protokolant: Adam Skowroński

po rozpoznaniu na rozprawie **17 grudnia 2019 r**. w Warszawie odwołania wniesionego do Prezesa Krajowej Izby Odwoławczej **6 grudnia 2019 r.**

przez wykonawcę: **S&T Poland sp. z o.o. z siedzibą w Warszawie**

w postępowaniu pn. *Dostawa i montaż urządzeń sieciowych dla POPD w ramach projektu „Rozwój systemu digitalizacji akt postepowań przygotowawczych w sprawach karnych (iSDA 2.0)”* (nr postępowania PK XF 261.52.2019)

prowadzonym przez zamawiającego: **Skarb Państwa – Prokuratura Krajowa z siedzibą w Warszawie**

przy udziale wykonawcy: **Immitis sp. z o.o. z siedzibą w Bydgoszczy** – zgłaszającego przystąpienie do postępowania odwoławczego po stronie odwołującego.

orzeka:

1. **Umarza postępowanie odwoławcze w zakresie wszystkich zarzutów i żądań z wyjątkiem zarzutów nr 5, 12 i 15 oraz związanych z nimi żądań.**

2. **Oddala odwołanie w pozostałym zakresie.**

3. Kosztami postępowania obciąża **Odwołującego** i

   1) zalicza w poczet kosztów postępowania odwoławczego kwotę **15000 zł 00 gr** (słownie: piętnaście tysięcy złotych zero groszy) uiszczoną przez **Odwołującego** tytułem wpisu od odwołania,

2) zasądza od **Odwołującego** na rzecz **Zamawiającego** kwotę **3600 zł 00 gr** (słownie: trzy tysiące sześćset złotych zero groszy) – stanowiącą koszty postępowania odwoławczego poniesione z tytułu uzasadnionych kosztów strony obejmujących wynagrodzenie pełnomocnika.

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) na niniejszy wyrok – w terminie 7 dni od dnia jego doręczenia – przysługuje skarga za pośrednictwem Prezesa Krajowej Izby Odwoławczej do **Sądu Okręgowego w Warszawie**.

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

Zamawiający Skarb Państwa – Prokuratura Krajowa z siedzibą w Warszawie prowadzi na podstawie ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (t.j. Dz. U. z 2019 r. poz. 1843) {dalej również: „ustawa pzp", „ustawa Pzp, „pzp", „Pzp", „p.z.p."} w trybie przetargu nieograniczonego postępowanie o udzielenie zamówienia publicznego na dostawy pn. *„Rozwój systemu digitalizacji akt postepowań przygotowawczych w sprawach karnych (iSDA 2.0)"* (nr postępowania PK XF 261.52.2019). Ogłoszenie o tym zamówieniu 27 listopada 2019 r. zostało opublikowane w Dzienniku Urzędowym Unii Europejskiej nr 2019/S_229 pod poz. 261930. Wartość przedmiotowego zamówienia przekracza kwoty określone w przepisach wydanych na podstawie art. 11 ust. 8 ustawy pzp.

6 grudnia 2019 r. Odwołujący S&T Poland sp. z o.o. z siedzibą w Warszawie wniósł w formie elektronicznej do Prezesa Krajowej Izby Odwoławczej odwołanie (zachowując wymóg przekazania jego kopii Zamawiającemu) od postanowień opisu przedmiotu zamówienia zawartego w załączniku nr 1 do specyfikacji istotnych warunków zamówienia {dalej również: „specyfikacja", „SIWZ" lub „s.i.w.z."} w następującym zakresie:

[Zarzut #1 – Szyfrowanie portów Ethernet z wykorzystaniem technologii MACSec IEEE];

1) *wymaganie POS7-LAN-03 – w zakresie wymagania sprzętowego wsparcia dla szyfrowania portów Ethernet z wykorzystaniem technologii MACSec IEEE 802.1ad i z wykorzystaniem klucza 256 bit dla przełączników LAN (pkt 5.13.1.1.2, str. 60 Załącznika nr 1 do SIWZ – Opis Przedmiotu Zamówienia – dalej „OPZ") [Zarzut #1];*

[Zarzut #2 – Openflow 1.3 dla przełączników LAN]

2) *wymaganie POS7-LAN-07.02 – zakresie wymagania funkcjonalności Openflow 1.3 dla obszaru zarządzania i zabezpieczenia przełącznika dla przełączników LAN (pkt 5.13.1.1.2, str. 61 OPZ) [Zarzut #2];*

[Zarzut #3 – Liczba portów dla przełączników LAN typ I]

3) *wymaganie POS7-LAN-11.01 – w zakresie minimalnej liczby portów 10/25/40/100GE dla przełączników LAN typ I oraz wymaganie POS7-LAN-12.04 – w zakresie przepustowości pakietowej (pkt 5.13.1.1.3, str. 61OPZ) [Zarzut #3];*

[Zarzut #4 – łączna przepływność dla przełączników LAN typ I]

4) *wymaganie POS7-LAN-12.03 – w zakresie obsługiwanej łącznej przepływności (pasmo) min. 6,8Tbps (pkt 5.13.1.1.3, str. 61 OPZ) [Zarzut #4];*

[Zarzut #5 – Liczba portów dla przełączników LAN typ III]

5) *wymaganie POS7-LAN-15.01 – w zakresie minimalnej liczby portów 1/10/25GE*

definiowanych za pomocą wkładek SFP bezpośrednio w obudowie przełącznika lub na karcie liniowej dla przełączników LAN typ III (pkt 5.13.1.1.5, str. 62 OPZ) oraz pozostałych wymagań z nim związanych, tj.: POS7-LAN-15.02, POS7-LAN-16.02, POS7- LAN-16.03; [Zarzut #5];

[Zarzut #6 – Openflow 1.3 dla przełączników LAN typ IV]

6) *wymaganie POS7-LAN-17.46 – w zakresie wymagania funkcjonalności Openflow 1.3 dla obszaru zarządzania i zabezpieczenia przełącznika (pkt 5.13.1.1.6, str. 64 OPZ) [Zarzut #6];*

[Zarzut #7 – Liczba portów dla przełączników LAN typ IV]

7) *wymaganie POS7-LAN-18.03 – w zakresie minimalnej liczby portów przełącznika (pkt 5.13.1.1.6, str. 64 OPZ) [Zarzut #7];*

[Zarzut #8 - Uwierzytelnienie ze wsparciem SAML]

8) *wymaganie POS7-VPN-01.07 – w zakresie wymagania obsługi uwierzytelnienia klientów VPN opartego o RADIUS oraz AD (ze wsparciem SAML) dla modułu zdalnego dostępu VPN – wymagania ogólne dla koncentratora VPN (pkt 5.13.2.1, str. 68 OPZ) [Zarzut#8];*

[Zarzut #9 - Dostępna przestrzeń dla koncentratora VPN typ II]

9) *wymaganie POS7-VPN-12 – w zakresie udostępnienia na potrzeby każdej instancji środowiska bazującego na VMWare vSphere, nie więcej niż 8 GB vHDD – wymagania dla koncentratora VPN typ II (pkt 5.13.2.1.2, str. 70 OPZ) [Zarzut #9];*

[Zarzut #10 – Liczba wykrywanych aplikacji sieciowych – urządzenia NGFW/NGIPS]

10) *wymaganie POS7-NGFW1P5-01.13 lit. a) – w zakresie wymagania klasyfikacji ruchu i wykrywania 3.000 aplikacji sieciowych przez urządzenia NGFW/NGIPS (pkt 5.13.2.2, str. 72 OPZ) [Zarzut #10];*

[Zarzut #11 i 12 – Ochrona antyspamowa]

11) *wymaganie POS7-EMAIL-07.06 – w zakresie możliwości definicji przedziału czasowego przy monitorowaniu i ograniczaniu ilości połączeń z jednego adresu IP w określonym przedziale czasu (pkt 5.13.2.4, str. 85 OPZ) [Zarzut #11];*

12) *wymaganie POS7-EMAIL-07.07 – w zakresie możliwości blokowania na określony czas przyjmowania poczty z adresów IP, dla których odnotowano wiadomości zawierające zdefiniowaną liczbę niewłaściwych adresatów z chronionej domeny (pkt 5.13.2.4, str. 85 OPZ) [Zarzut #12];*

[Zarzut #13 i 14 – Ochrona antywirusowa]

13) *wymaganie POS7-EMAIL-08.01 – w zakresie wymagania co najmniej dwóch niezależnych silników antywirusowych (pkt 5.13.2.4, str. 85 OPZ) [Zarzut #13];*

14) *wymaganie POS7-EMAIL-08.02 – w zakresie wymagania co najmniej dwóch silników antywirusowych (pkt 5.13.2.4, str. 86 OPZ) [Zarzut #14];*

[Zarzut #15 – sygnatury OpenlOC]

15) *wymaganie POS7-ANTVIR-05.11 – w zakresie wymagania wsparcia dla sygnatur OpenlOC (pkt 5.13.2.5, str. 88 OPZ) [Zarzut #15];*

[Zarzut #16-18 – System zarządzania elementami bezpieczeństwa]

16) *wymaganie POS7-MGNTSEC-02 – w zakresie wymagania, aby system zarządzania elementami bezpieczeństwa posiadał możliwość zarządzania funkcjonalnościami urządzeń realizujących funkcjonalności sandbox i ochrony poczty elektronicznej (pkt 5.13.5.2, str. 110 OPZ), oraz w konsekwencji wymagania:*

- POS7-MGNTSEC-05 (w tym: POS7-MGNTSEC-05.01, POS7-MGNTSEC-05.02, POS7-M G NTS EC-05.03)

- POS7-MGNTSEC-06 (w tym: POS7-MGNTSEC-06.01, POS7-MGNTSEC-06.02, POS7-MGNTSEC-06.03, POS7-MGNTSEC-06.04, POS7-MGNTSEC-06.05, POS7-MGNTSEC-06.06, POS7-MGNTSEC-06.07) [Zarzut #16];

17) *wymaganie POS7-MGNTSEC-03.01 – w zakresie wymagania, aby system umożliwiał tworzenie i używanie ról administracyjnych różniących się poziomem dostępu do danego urządzenia lub grupy urządzeń/logicznych systemów (pkt 5.13.5.2, str. 110 OPZ) [Zarzut #17];*

18) *wymaganie POS7-MGNTSEC-06.01 pkt 3 e) – w zakresie wymagania, aby system zapewniał definiowanie polityk poprzez dostarczenie wiadomości z wykonaniem dodatkowych akcji: - zapisanie wiadomości do wskazanej kolejki (pkt 5.13.5.2, str. 112 OPZ) [Zarzut #18];*

[Zarzut #19 – SANDBOX]

19) *wymaganie POS7-SANDBOX-06.02 – w zakresie wymagania konkretnej, minimalnej liczby maszyn wirtualnych możliwych do uruchomienia jednocześnie (pkt 5.13.2.6.1, str. 94 OPZ) [Zarzut #19];*

[Zarzuty #20-22 Przełączniki SAN typ I];

20) *wymaganie POS7-SAN-01.04 – w zakresie możliwości standardowego przydziału minimum 300 kredytów (FC buffer credits) dla przełączników SAN Typ I (pkt 5.13.1.1.1, str. 57 OPZ) [Zarzut #20];*

21) *wymaganie POS7-SAN-01.08 – w zakresie wymagania obsługi agregacji nie mniej niż 8 portów fizycznych FC32G w jedno połączenie logiczne („trunk", „channel") – możliwość włączenia w skład zagregowanego połączenia logicznego dowolnego aktywnego portu dla przełączników SAN Typ I (pkt 5.13.1.1.1, str. 57 OPZ) [Zarzut #21];*

22) *wymaganie POS7-SAN-05.02-w zakresie wymagania inspekcji nagłówków SCSI z pełną wydajnością (wirespeed) dla przełączników SAN Typ 1 (pkt 5.13.1.1.1, str. 57 OPZ) [Zarzut #22];*

23) *wymaganie PCJS7-SAN-05.03 – w zakresie wymagania statystyki ruchu dla iSCSI dla przełączników SAN Typ I (pkt 5.13.1.1.1, str. 57 OPZ) [Zarzut #23];*

[Zarzut #24 Koncentrator VPN typ I];

24) *wymaganie POS7-VPN-09.02 w zakresie wymagania obsługi co najmniej 2.500 jednoczesnych tuneli VPN (site-to-site, remote access lub ich kombinacji – wymagania dla koncentratora VPN typ I (pkt 5.13.2.1.1, str. 69 OPZ) [Zarzut #24].*

Odwołujący zarzucił Zamawiającemu następujące naruszenia przepisów ustawy pzp:

1. Art. 29 ust. 2 – przez postawienie wymagań nieuzasadnionych potrzebami Zamawiającego i ograniczających konkurencję przez niedopuszczenie rozwiązań innych producentów niż preferowany przez Zamawiającego.
2. Art. 7 ust. 1 w zw. z art. 29 ust. 1 – przez prowadzenie postępowania w sposób naruszający zasadę uczciwej konkurencji i równego traktowania wykonawców ze względu na opisanie przedmiotu zamówienia w sposób niedopuszczający rozwiązań innych producentów i tym samym uniemożliwiający złożenie konkurencyjnych ofert innym wykonawcom, którzy nie oferują rozwiązań preferowanego przez Zamawiającego producenta.
3. Art. 30 ust. 4 – przez niedopuszczenie rozwiązań równoważnych.

Odwołujący wniósł o uwzględnienie odwołania i nakazanie Zamawiającemu dokonania następujących zmian kwestionowanych postanowień załącznika nr 1 do SIWZ – OPZ {wnioskowane zmiany podkreślono}:

[Zarzut #1 – Szyfrowanie portów Ethernet z wykorzystaniem technologii MACSec IEEE];

1) wymaganie POS7-LAN-03 – wskazanie, że wymaganie to dotyczy wyłącznie przełącznika LAN typ I [*Sprzętowe wsparcie dla szyfrowania portów Ethernet z wykorzystaniem technologii MACSec IEEE 802.1ad i z wykorzystaniem klucza 256 bit – wymaganie dotyczy tylko przełącznika LAN Typ I*]

[Zarzut #2 – Openflow 1.3 dla przełączników LAN]

2) wymaganie POS7-LAN-07.02 – dopuszczenie równoważnego mechanizmu Directflow [*Openflow lub Directflow*]

[Zarzut #3 – Liczba portów dla przełączników LAN typ I]

3) wymaganie POS7-LAN-11.01 – zmniejszenie liczby portów o 2 (do 32 portów) [*minimum 32 porty 10/25/40/100GE definiowanych za pomocą wkładek QSFP*]
   oraz w konsekwencji modyfikację wymagania POS7-LAN-12.04 [*obsługiwana łączna przepustowość pakietowa przełącznika min. ~~2400~~ 2000 Mpps*]

Zarzut #4 – łączna przepływność dla przełączników LAN typ I]

4) *wymaganie POS7-LAN-12.03* – dopuszczenie łącznej przepływności 6,4Tbps zamiast 6,8Tbps [*obsługiwana łączna przepływność (pasmo) min. 6,4Tbps*]

[Zarzut #5 – Liczba portów dla przełączników LAN typ III]

5) *wymaganie POS7-LAN-15.01* – dopuszczenie spełnienia wymagania przez zaoferowanie dwóch przełączników z 48 portami zamiast jednego przełącznika z 96 portami [*minimum 96 portów 1/10/25GE definiowanych za pomocą wkładek SFP bezpośrednio w obudowie przełącznika lub na karcie liniowej lub dwa przełączniki posiadające minimum 48 portów 1/10/25GE każdy, definiowanych za pomocą wkładek SFP bezpośrednio w obudowie przełącznika lub na karcie liniowej]*

oraz dostosowanie pozostałych wymagań, na które powyższa zmiana ma wpływ:

- POS7-LAN-15.02 [*minimum 12 portów 40/100GE definiowanych za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP musi posiadać możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps lub dwa przełączniki każdy posiadający 12 portów 40/100 GE definiowanych za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP musi posiadać możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps],*
- POS7-LAN-16.02 [*obsługiwana łączna przepływność (pasmo) min. 6,4Tbps lub dwa przełączniki każdy posiadający 4,8Tbps*]
- POS7-LAN-16.03 [*obsługiwana łączna przepustowość pakietowa przełącznika min. 2400 Mpps lub dwa przełączniki każdy posiadający 2000Mpps*]

[Zarzut #6 – Openflow 1.3 dla przełączników LAN typ IV]

6) wymaganie POS7-LAN-17.46 – dopuszczenie równoważnego mechanizmu Directflow [*Openflow lub Directflow*]

[Zarzut #7 – Liczba portów dla przełączników LAN typ IV]

7) *wymaganie POS7-LAN-18.03* – umożliwienie dostarczenia przełącznika posiadającego minimum 4 porty 10GE definiowane za pomocą wkładek SFP+ [*minimum 4 porty 10/~~25/40/100~~GE definiowane za pomocą wkładek ~~QSFP~~ SFP+*]

[Zarzut #8 - Uwierzytelnienie ze wsparciem SAML]

8) wymaganie POS7-VPN-01.07 – usunięcia wymagania „ze wsparciem SAML" [*Obsługa uwierzytelnienia klientów VPN opartego o RADIUS oraz AD ~~(ze wsparciem SAML)~~*]

lub ewentualnie umożliwienie realizacji funkcjonalności SAML poprzez dodatkowe urządzenie

[Zarzut #9 - Dostępna przestrzeń dla koncentratora VPN typ II]

9) *wymaganie POS7-VPN-12* – zwiększenie udostępnionej przestrzeni do 32 GB vHDD [*Koncentrator VPN realizowany jako maszyna wirtualna działający na wirtualizatorze VMWare vSphere. (Zamawiający udostępni na potrzeby każdej instancji środowisko*

bazujące na VMWare vSphere, nie więcej niż 1 vCPU, 2 GB vRAM, 32 GB vHDD – w przypadku większych wymagań wymagane jest zapewnienie właściwej platformy).]

[Zarzut #10 – Liczba wykrywanych aplikacji sieciowych – urządzenia NGFW/NGIPS]

10) wymaganie POS7-NGFW1P5-01.13 lit. a) – zmniejszenie liczby aplikacji sieciowych do 2.000 [*Możliwość wykorzystania w polityce bezpieczeństwa następujących danych:możliwość klasyfikacji ruchu i wykrywania ~~3.000~~ 2.000 aplikacji sieciowych*]

[Zarzut #11 i 12 – Ochrona antyspamowa]

11) wymaganie POS7-EMAIL-07.06 – usunięcie możliwości definicji przedziału czasowego [*i. monitorowania i ograniczania ilości połączeń z jednego adresu IP w określonym przedziale czasu:*

    ~~o możliwość definicji przedziału czasowego~~

    o *opcja ograniczenia maksymalnej ilości połączeń i wiadomości.*

    ii. ograniczanie maksymalnej liczby wiadomości przekazywanych za pomocą pojedynczego połączenia SMTP

    iii. wskazanie timeout'u dla niewykorzystywanego połączenia] *[Zarzut #11]*

12) wymaganie POS7-EMAIL-07.07 – *określenie funkcjonalności jako możliwości ochrony przed podszywaniem pod maile chronionej domeny* [*możliwość ~~blokowania na określony czas przyjmowania poczty z adresów IP, dla których odnotowano wiadomości zawierające zdefiniowaną liczbę niewłaściwych adresatów z~~ ochrony przed podszywaniem pod maile chronionej domeny*] *[Zarzut #12]*

[Zarzut #13 i 14 – Ochrona antywirusowa]

13) wymaganie POS7-EMAIL-08.01 – usunięcie w całości *[Zarzut #13]*

14) wymaganie POS-EMAIL-08.02 – usunięcie wymagania oparcia skanowania antywirusowego o co najmniej dwa silniki antywirusowe *[blokowanie złośliwej treści z wykorzystaniem tradycyjnego skanowania antywirusowego opartego o ~~co najmniej dwa komercyjne~~ silnik antywirusowy oraz bazę sygnatur kodów złośliwych*] *[Zarzut #14]*

[Zarzut #15 – sygnatury OpenIOC]

15) wymaganie POS7-ANTVIR-05.11 – usunięcie w całości

[Zarzut #16-18 – System zarządzania elementami bezpieczeństwa]

16) *wymaganie POS7-MGNTSEC-02 – usunięcie wymagania zarządzania funkcjonalnościami urządzeń realizujących funkcjonalności NGFW, NGIPS, sandobx i ochrony poczty elektronicznej* [*Zarządzanie funkcjonalnościami urządzeń realizujących funkcjonalności NGFW, NGIPS, SSL, WAF, LB~~, sandobx i ochrony poczty elektronicznej~~ – dopuszczalne jest oferowanie w ramach systemu zestawu urządzeń typu appliance i/lub elementów oprogramowania (uruchamianych na serwerach obszaru zarządzania) odpowiedzialnych za zarządzanie poszczególnymi funkcjonalnościami (NGFW, NGIPS,*

SSL, WAF, LB, sandobx, ochrony poczty elektronicznej, ...). W takim przy pad u należy wymienić wszystkie elementy wchodzące w skład zestawu oraz ich producentów.

Zamawiający dopuszcza budowę systemu zarządzania w oparciu o kilka komponentów zarządzania oferowanych przez producenta rozwiązania w danej grupie funkcjonalnej (tj. NGFW, SSL, WAF, LB itp) jednakże pod warunkiem iż komponenty składające się na ten system będą one pochodziły od jednego producenta (producenta rozwiązania w danej grupie funkcjonalnej) i będą przez niego w całości serwisowane.

Zamawiający wymaga jednocześnie aby wymagania dotyczące liczby zarządzanych urządzeń, pojemności przestrzeni dyskowej oraz możliwości rozbudowy były spełnione przez każdy z komponentów tworzących taki system zarządzania]

oraz usunięcia w konsekwencji wymagań:

- POS7-MGNT5EC-05 (w tym: POS7-MGNTSEC-05.01, POS7-MGNTSEC-05.02, POS7-MGNTSEC-05.03)
- POS7-MGNTSEC-06 (w tym: POS7-MGNTSEC-06.01, POS7-MGNTSEC-06.02, POS7-MGNTSEC-06.03, POS7-MGNTSEC-06.04, POS7-MGNTSEC-06.05, P0S7-MGNT5EC-06.06, POS7-MGNTSEC-06.07) *[Zarzut #16];*

17) wymaganie POS7-MGNTSEC-03.01 – usunięcie w całości *[Zarzut #17];*
18) wymaganie POS7-MGNTSEC-06.01 pkt 3 e) – usunięcie w całości *[Zarzut #18];*

[Zarzut #19 – SANDBOX]

19) *wymaganie POS7-SANDBOX-06.02 –*

[*Sandbox musi umożliwiać uruchomienie ~~do najmniej 16~~ odpowiedniej liczby maszyn wirtualnych pracujących jednocześnie, w celu analizy co najmniej 1500 plików dziennie*]

[Zarzuty #20-22 Przełączniki SAN typ I];

20) wymaganie POS7-SAN-01.04 – usunięcie w całości *[Zarzut #20]*
21) wymaganie POS7-SAN-01.08 – usunięcie w całości *[Zarzut #21]*
22) wymaganie POS7-SAN-05.02 – usunięcie wsparcia SCSI [*inspekcja nagłówków FC ~~i SCSI~~ z pełną wydajnością (wirespeed)*] *[Zarzut #22]*
23) wymaganie PCJS7-SAN-05.03 – usunięcie w całości *[Zarzut #23]*

[Zarzut #24 Koncentrator VPN typ I];

24) wymaganie POS7-VPN-09.02 – dodanie alternatywnej możliwości spełnienia wymagania poprzez obsługę co najmniej 2000 jednoczesnych tuneli VPN site-to-site i 10 000 tuneli remote access [*obsługa co najmniej 2.500 jednoczesnych tuneli VPN (site-to-site, remote access lub ich kombinacji) lub co najmniej 2000 jednoczesnych tuneli VPN site-to-site i 10 000 tuneli remote access*]

Ponadto odwołanie zawierało określenie okoliczności faktycznych i prawnych, które według Odwołującego uzasadniają wniesienie odwołania w następującym brzmieniu:

1. WPROWADZENIE

1.1. Zamawiający prowadzi Postępowanie o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego, do którego zastosowanie mają przepisy PZP, które nakładają na Zamawiającego obowiązek opisania przedmiotu zamówienia zgodnie ze swoimi uzasadnionymi potrzebami nie ograniczając przy tym konkurencyjności.

1.2. Z określonych przez Zamawiającego parametrów wynika, jakiej klasy rozwiązania Zamawiający oczekuje i jaki jest cel Zamówienia. Jednocześnie Zamawiający postawił kilka nieuzasadnionych wymagań, które uniemożliwiają złożenie oferty na rozwiązanie producenta jednego z najskuteczniejszych rozwiązań w zakresie ochrony antywirusowej. Zamawiający w części przywołanych w odwołaniu postanowieniach postawił wymagania, które spełniają rozwiązania wyłącznie jednego producenta – CISCO, podczas gdy na rynku istnieją inne rozwiązania, które także spełnią cel Zamówienia.

1.3. Zgodnie z wyrokiem KIO z dnia 30 stycznia 2017 r., KIO 68/17: „Sztuczne – bezpodstawne ograniczanie przez Zamawiającego parametrów, stanowi o ograniczaniu ilości wykonawców, którzy mogą złożyć ofertę. Podkreślić także należy, że istotą konkurencji jest, że każdy z wykonawców chce i powinien zaoferować taki produkt, który ma jak największe szanse i możliwość zdobycia jak największej ilości punktów w postępowaniu. Rolą Zamawiającego jest natomiast opisanie przedmiotu zamówienia stosownie do uzasadnionych potrzeb".

1.4. Należy podkreślić, że Zamawiający nie może w sposób dowolny kreować postanowień SIWZ, lecz wymagania muszą wynikać z jego uzasadnionych potrzeb. Odnosząc się po kolei do zrzutów Odwołujący wykaże, że zaskarżone postanowienia nie mają uzasadnienia i uniemożliwiają zaoferowanie konkurencyjnych rozwiązań, a co za tym idzie, Zamawiający nie ma możliwości otrzymania korzystniejszej ekonomicznie i jakościowo oferty. Zamawiający kosztem parametrów, z których w praktyce nie otrzyma żadnych korzyści, zawęził krąg wykonawców i przez to naraża się na otrzymanie drożej oferty.

1.5. Odwołujący zwraca także uwagę na to, że w postępowaniach odwoławczych toczących się wobec treści SIWZ, ciężar dowodu w zakresie uzasadnienia obiektywnych potrzeb Zamawiającego spoczywa na Zamawiającym. Odwołujący wykazał wystąpienie ograniczenia konkurencji przez Zamawiającego, natomiast w zakresie udowodnienia, że zaskarżone parametry są uzasadnione potrzebami Zamawiającego ciężar dowodu spoczywa na Zamawiającym. Jak wskazuje KIO, zamawiający winien jednak przekonać izbę, że dany parametr znajduje uzasadnienie w jego potrzebach. Tylko bowiem zamawiający wie, jaki konkretnie efekt zamierza osiągnąć w drodze zamówienia publicznego.

2. Zarzut #1 – Szyfrowanie portów Ethernet z wykorzystaniem technologii MACSec IEEE (POS7-LAN- 03)

2.1. Szyfrowanie portów Ethernet z wykorzystaniem technologii MACSec ma zastosowanie zazwyczaj przy podłączeniu pomiędzy zewnętrznymi lokalizacjami i nie jest wykorzystywane w ramach jednego Data Center. Dlatego stosowane jest w urządzeniach szkieletowych (w postępowaniu jest to Przełącznik LAN TYP I). Wymagania te spełniają zazwyczaj tylko przełączniki, które są dedykowanych do szkieletu sieci.

2.2. W ramach Data Center szyfrowanie MACSec było by uzasadnione, gdyby istniała możliwość szyfrowania także do urządzeń końcowych takich jak serwery i firewalle. Niestety takie urządzenia nie posiadają szyfrowania w związku z czym, jeżeli nie da się zaszyfrować całej komunikacji, szyfrowania części nic nie daje.

2.3. Jeden z największych producentów przełączników sieciowych dedykowanych do DataCenter – firma Arista nie posiada takich funkcji dla przełączników spełniających pozostałe wymagania dla typów II, III i IV. W związku z czym nie może zaoferować swoich produktów. Jedynym producentem na rynku, który spełnia to wymaganie, oraz pozostałe wymagania dla przełączników typ II, III i IV jest firma Cisco.

2.4. Z powyższego wynika, że postawienie zaskarżonego wymagania dla przełączników LAN (wymaganie POS7-LAN-03) uniemożliwia zaoferowanie przełączników innych niż produkowanych przez Cisco, pomimo tego, że istnieją na rynku przełączniki spełniające pozostałe wymagania, co stanowi naruszenie art. 29 ust. 2 PZP oraz art. 7 ust. 1 PZP.

3. Zarzut #2 – Openflow 1.3 dla przełączników LAN (POS7-LAN-07.02)

3.1. Zamawiający postawił wymaganie, aby przełączniki LAN posiadały funkcjonalność Openflow 1.3, podczas gdy opisane przez Zamawiającego rozwiązanie nie posiada systemu, który by mógł korzystać z Openflow 1.3, co oznacza, że postawione wymaganie jest funkcjonalnie nieuzasadnione. Jeden z największych producentów przełączników sieciowych dedykowanych do DataCenter firma Arista nie posiada mechanizmu Openflow 1.3., w związku z czym nie może zaoferować swoich produktów pomimo tego, że posiada przełączniki spełniające pozostałe wymagania Zamawiającego oraz posiada mechanizm równoważny do Openflow 1.3. Jedynym producentem na rynku, który spełnia to wymaganie, oraz pozostałe wymagania dla przełączników LAN jest firma Cisco.

3.2. Zamawiający postawił wymaganie (POS7-LAN-07.02), które nie jest mu niezbędne, a jednocześnie uniemożliwia złożenie ofert przez wykonawców oferujących przełączniki jednego z największych producentów przełączników na rynku. Zamawiający dopuszczając równoważny mechanizm - DirectFlow umożliwi złożenie ofert przez wykonawców oferujących inne niż Cisco przełączniki.

4. Zarzut #3 – Liczba portów dla przełączników LAN typ I (POS7-LAN-11.01)

4.1. Wyłącznie produkty CISCO posiadają 34 porty, natomiast na rynku dostępne są rozwiązania posiadające 32 porty. Zgodnie z Rysunkiem nr 3 - Architektura warstwy fizycznej ITS w POPD - Wewnętrzna Strefa Bezpieczeństwa (str. 13 OPZ), Zamawiający zamierza używać zaledwie 8 portów łącznie na dwóch przełącznikach, zatem bezpodstawne jest postawienie takiego wymagania i niedopuszczenie rozwiązań innych producentów, którzy oferują przełączniki zawierające 32 porty.

4.2. Standardem ilości portów w przełącznikach sieciowych jest wielokrotność liczby 8: 24, 32, 40, 48. Zaoferowanie przełączników innych niż Cisco wymaga dostarczenia rozwiązania wyższej klasy, posiadającego 64 porty, które jest droższe i nie może na równych zasadach konkurować z przełącznikami posiadającymi 34 porty.

4.3. Obecnie na rynku tylko przełącznik Nexus 9336C-FX2 posiada 34 porty 10/25/40/100GE.

4.4. W konsekwencji należy także zmodyfikować wymaganie POS7-LAN-12.04, które jest ściśle związane z liczbą portów oraz przepływnością przełącznika. Wartość ta zależy od wielkości pakietu. Im większy pakiet tym wartość ta może być mniejsza. Dla średniej wartości pakietu przy tej ilości portów wartość ta powinna wynosić ok 2000 Mpps. Wartość 2400 Mpps wydaje się być zawyżona i dodatkowo blokuje zaoferowanie produktów wielu producentów w tym jednego z największych producentów przełączników do Data Center firmę Arista.

4.5. Zmiana taka pozwoli na zaoferowanie innych rozwiązań.

5. Zarzut #4 - łączna przepływność dla przełączników LAN typ 1 (POS7-LAN-12.03)

5.1. Zamawiający wymaga dostarczenia przełącznika posiadającego min. 6,8Tbps. Parametr ten jest ściśle powiązany z wymaganiem POS7-LAN-11.01 dotyczącym liczby portów i w przypadku zmiany liczby portów, analogicznie parametr również powinno być mniejsze. Wystarczająca dla Zamawiającego przepustowość wynosi 6,4Tbps.

5.2. Przepustowość jest liczona w następujący sposób: ilość portów x przepustowość portu x 2 (czyli dwa kierunki: wyjście i wejście), co przy 32 portach 100GB daje nam 32x100x2=6400GB czyli 6,4TB.

6. Zarzut #5 – Liczba portów dla przełączników LAN typ III (POS7-LAN-15.01)

6.1. Zamawiający wymaga dostarczenia przełącznika posiadającego 96 portów 1/10/25GE definiowanych za pomocą wkładek SFP. Określone przez Zamawiającego wymagania dla przełączników LAN typ III wraz z wymaganiem 96 portów spełnia wyłącznie przełącznik: Cisco Nexus 93360YC-FX2. Uniemożliwia to zaoferowanie konkurencyjnego rozwiązania. Dopuszczenie przez Zamawiającego możliwości dostarczenia dwóch przełączników posiadających 48 portów 1/10/25GE oraz 12 portów 40/100GE – spełniających punkt 5.13.1.1.4 Przełącznik LAN TYP II zamiast jednego opisanego w punkcie umożliwi

zaoferowanie konkurencyjnych przełączników, innych niż Cisco.

6.2. Zgodnie z Rysunkiem nr 4-Architektura warstwy fizycznej ITS w POPD – Zewnętrzna Strefa (str. 19 OPZ), Zamawiający zamierza używać zaledwie 36 portów 10GB i 8 portów 1GB na dwóch przełącznikach, co daje po 18 portów 10GB i 4 porty 1GB na każdy przełącznik,

6.3. Zamawiający nie ma podstaw aby ograniczać konkurencję stawiając wyjątkowo wysokie, nieuzasadnione wymaganie, w sytuacji gdy dopuszczenie alternatywnego rozwiązania umożliwi zaoferowanie konkurencyjnych rozwiązań. Ponadto, zaoferowanie dwóch przełączników zamiast jednego nie wpłynie na zmniejszenie wydajności systemu oraz zmniejszenie ilości dostępnych portów.

6.4. Zaoferowane, przełączniki spełniałyby by następujące wymagania:

- ilość portów 1/10/25GE 2przełączniki po 48 portów = 96portów

- ilość portów 40/100GE 2przełączniki po 12 portów = 24porty

- obsługiwana łączna przepływność (pasmo) 2 przełączniki 4,8Tbps = 9,6Tbps

- obsługiwana łączna przepustowość pakietowa przełącznika 2 przełączniki 1600 Mpps = 3200Mpps

7. Zarzut #6 – Openflow 1.3 dla przełączników LAN typ IV (POS7-LAN-17.46)

7.1. Argumentacja Odwołującego jest analogiczna jak przy Zarzucie #2 – opisane przez Zamawiającego rozwiązanie nie posiada systemu, który by mógł korzystać z Openfiow 1.3, co oznacza, że postawione wymaganie jest funkcjonalnie nieuzasadnione. Jeden z największych producentów przełączników sieciowych dedykowanych do DataCenter firma Arista nie posiada mechanizmu Openfiow 1.3., w związku z czym nie może zaoferować swoich produktów pomimo tego, że posiada przełączniki spełniające pozostałe wymagania Zamawiającego oraz posiada mechanizm równoważny do Openfiow 1.3. Jedynym producentem na rynku, który spełnia to wymaganie, oraz pozostałe wymagania dla przełączników LAN jest firma Cisco.

7.2. Zamawiający dopuszczając równoważny mechanizm – DirectFlow umożliwi złożenie ofert przez wykonawców oferujących inne niż Cisco przełączniki.

8. Zarzut #7 – Liczba portów dla przełączników LAN typ IV (POS7-LAN-18.03)

8.1. Na rynku nie ma przełącznika spełniającego wszystkie wymagania dla przełączników LAN typ IV. Odwołujący wnosi o zmianą wymagania POS7-LAN-18.03, które pozwoli na dostarczenie przełącznika posiadającego minimum 4 porty 10GE definiowane za pomocą wkładek SFP+ zamiast opisanych 4 portów 10/25/40/100GE definiowanych za pomocą wkładek QSFP. Zmiana pozwoli na zaoferowanie rozwiązania, przy jednoczesnym spełnieniu potrzeb Zamawiającego.

8.2. 4 porty 10GE są portami tzw. „uplink" i służą do komunikacji z innym przełącznikiem.

Zadaniem tych portów jest przesłanie danych z tzw. „portów downlink" czyli 48 portów 100/1000 do innego przełącznika. Czyli potrzeba łącznie przetransportować 48x1GB, co daje nam 48GB. Za pomocą 4 portów 100GE można by przetransportować 400GB co jest zdecydowanie nadmiarowe, dlatego producenci przełączników stosują standard 4 port 10GE uplink przy 48 portach 1GE downlink.

9. Zarzut #8 – Uwierzytelnienie ze wsparciem SAML (POS7-VPN-01.07)

9.1. Protokół SAML zazwyczaj nie jest wykorzystywany do zestawiania tuneli VPN, w związku z czym tylko kilku producentów koncentratorów VPN implementuje ten mechanizm. W związku z czym wnosimy o usunięcie wymagania, co pozwoli na zaoferowanie urządzeń Fortinet, jednego z czołowych producentów tego typu urządzeń.

9.2. Zamawiający może także otrzymać wymaganą funkcjonalność poprzez możliwość dostarczenia dodatkowego urządzenia.

10. Zarzut #9 – Dostępna przestrzeń dla koncentratora VPN typ II (POS7-VPN-12)

10.1. Zamawiający udostępnia jedynie 8GB HDD w celu instalacji wirtualnej maszyny koncentratora VPN. W przypadku większego wymagania Zamawiający wymaga dostarczenia dodatkowego serwera. Różni producenci wirtualnych koncentratorów VPN mają inne wymagania co do przestrzeni dyskowej (HDD). Obecne wymaganie jest charakterystyczne dla firmy Cisco i stawia w gorszej sytuacji innych producentów takich jak Fortinet, PaloAlto i Checkpoint, którzy wymagają większej przestrzeni dyskowej.

10.2. Obecnie przestrzeń dyskowa w infrastrukturze serwerowej to ok40TB, czyli ok 40 000 GB. W przypadku zwiększenia wymagania dysku o 24GB, co jest nieznacznym obciążeniem obecnego serwera, producent Fortinet będzie musiał dostarczyć dodatkowy serwer co jest znacznym zwiększeniem kosztów.

10.3. Wobec powyższego, wnoszę o zmianę wartości dysku twardego, który udostępni Zamawiający, do 32 GB HDD, co pozwoli na zaoferowanie w tym samym przedziale cenowym rozwiązania konkurencyjnego do rozwiązań Cisco.

11. Zarzut #10 – Liczba wykrywanych aplikacji sieciowych - urządzenia NGFW/NGIPS (POS7-NGFWIPS- 01.13 lit. a))

11.1. Zamawiający wymaga dostarczenia urządzenia, które będzie miało możliwość klasyfikacji ruchu i wykrywania 3.000 aplikacji. Urządzenia NGFW/NGIPS innych wiodących producentów wykrywają ok 2.000 aplikacji. Jednym z niewielu producentów NGFW/NGIPS obecnych na rynku, który spełnia to wymaganie jest firma Cisco. Mając na uwadze, fakt, iż większość obecnych na rynku urządzeń NGFW/NGIPS umożliwia tworzenie własnych sygnatur aplikacji wnosimy o zmianę liczby wykrywany aplikacji do 2.000 oraz dopisania wymagania „system pozwala na tworzenie własnych sygnatur aplikacji". Biorąc pod uwagę fakt, że aplikacja iSDA nie będzie standardową aplikacją, istnieje duże prawdopodobieństwo,

że nie będzie znajdowała się w domyślnej bazie aplikacji i będzie potrzeba dopisania jej do systemu.

12. Zarzut #11 Ochrona antyspamowa (POS7-EMAIL-07.06)

12.1. Zamawiający stawiając wymaganie możliwość} definicji przedziału czasowego dla funkcjonalności monitorowania i ograniczania ilości połączeń z jednego adresu IP w określonym przedziale czasu uniemożliwia dostarczenie rozwiązania FortiMail firmy Fortinet, który nie ma możliwości definiowania przedziałów czasowych. FortiMail posiada stały przedział czasowy 30min. Od strony praktycznej, definiowanie przedziału czasowego nie ma większego zastosowania, ponieważ jeżeli chcemy pozwolić na wykonanie z danego adresu IP 100 połączeń w ciągu godziny to możemy również ustawić 50 połączeń na 30min i osiągniemy ten sam efekt. Wprowadzenie takiego ograniczania nie wpływa w żadnym wypadku na zwiększenie bezpieczeństwa a tylko uniemożliwia dostarczenie jednego z wiodących produktów do zabezpieczenia sieci.

13. Zarzut #12 – Ochrona antyspamowa (POS7-EMAIL-07.07)

13.1. Wymaganie POS7-EMAIL-07.07 służy do ochrony przed podszywaniem pod maile chronionej domeny. Jest to jedna z wielu metod ochrony przed takim zagrożeniem. Różni producenci różnie realizują ochronę przed podszywaniem. Powyższa metoda stosowana jest przez firmę Cisco - produkt ESA. Producent rozwiązań do ochrony poczty firma Fortinet realizuję tą funkcjonalność innym metodami m.in.

- sprawdzanie adresatów domeny chronionej, odrzucenie wiadomości, jeżeli domena odbiorcy i „helo" pasują natomiast domena nadawcy jest inna;

- sprawdzenie czy nagłówek "From" i domena autoryzowana są nieprawidłowe;

- możliwość ręcznego zablokowania nagłówków wskazujących na własną domenę do maili zewnętrznych.

13.2. realizują tą funkcjonalność w różny sposób, i nie można stwierdzić, który producent realizuje tą funkcjonalność lepiej, ponieważ cel funkcjonalności jest zachowany. Zamawiający postawił wymaganie opisującego podejście firmy Cisco, blokuje możliwość zaoferowania produktów firmy Fortinet, który również specjalizuje się w ochronie poczty.

13.3. Odwołujący wnosi o zmianę wymagania na „możliwość ochrony przed podszywaniem pod maile chronionej domeny". Taka zmiana nie wpłynie na bezpieczeństwo sieci a zwiększy konkurencyjność.

13.4. Dodatkowo biorąc pod uwagę wymaganie: POS7-EMAIL-09.02 – sprawdzanie plików w oferowanym systemie sandbox, należy zauważyć, że oba produkty muszą pochodzić od tego samego producenta. Integracja różnych producentów technologii sandbox i ochrony poczty jest zazwyczaj niemożliwa. W związku z czym wymaganie to uniemożliwia zaoferowanie produktu sandbox firmy Fortinet.

14. Zarzut #13 i 14 – Ochrona antywirusowa (POS7-EMAIL-08.01 oraz POS7-EMAIL-08.02)

14.1. Wymaganie miałoby zastosowanie, gdyby producenci silników antywirus posiadały inne bazy sygnatur antywirusowych. Obecnie praktycznie wszyscy producenci rozwiązań ochrony przed wirusami działają w tzw. „CYBER THREAT ALLIANCE", czyli dostają takie same próbki wirusów co wpływa na to, że każdy silnik antywirus posiada taką samą listę sygnatur antywirus. Badanie danego pliku w dwóch silnikach antywirus nie powinno wpłynąć na poziom ochrony, ale dodatkowo wprowadza opóźnienia. Należy również zauważyć, że gdyby były jakieś różnice w liczbie sygnatur antywirusowych to zastosowanie dwóch nie daje gwarancji, że akurat posiadają one wszystkie dostępne sygnatury. W związku z powyższym praktycznie wszyscy producenci systemów do ochrony zrezygnowali z zastosowania dwóch silników antywirus. Jedną z niewielu lub jedyną firmą, która posiada dwa silniki jest firma Cisco (produkt ESA).

14.2. Dodatkowo należy zauważyć, że w ramach postępowania dostarczany będzie produkt sandbox. Jest to dodatkowa linia ochrony, która może analizować nieznane pliki, czyli takie które nie mają sygnatur, pod kontem wirusów.

14.3. W związku z powyższym wymaganie to nie wpływa na poprawę bezpieczeństwa sieci i tym samym nie ma praktycznego uzasadnienia, natomiast bardzo ogranicza konkurencję, nie dopuszczając rozwiązań większości producentów takich systemów.

15. Zarzut #15 – sygnatury OpenIOC (POS7-ANTVIR-05.11)

15.1. Open IOC jest metodologią opisującą atrybuty, na postawie których można stwierdzić, że stacja została skompromitowana (skutecznie zaatakowana). Zdefiniowana w ten sposób metodologia jest słuszna dla znanych wyników aktywności złośliwego kodu/ataku.

15.2. Zmiana metodologii ataku – która z założenia powinna być kosztowna dla atakującego - może oznaczać konieczność pisania nowych wskaźników IOC aby wykryć zdarzenie oraz aby uniknąć błędnych alarmów.

15.3. Sygnatury IOC wykorzystują podstawowe metody sprawdzeń, które niczym wyjątkowym nie wyróżniają się a ich pisanie nie jest prostą rzeczą - wymaga gruntownej znajomości systemów, ataków, działania złośliwego kodu i wiąże się z dużym nakładem czasu z punktu widzenia utrzymania i obsługi systemu.

15.4. OpenIOC obsługuje proste i zaawansowane zapytania dotyczące IOC, takich jak:

• poszukiwanie określonego hasha pliku;

• określony wpis w pamięci lub rejestrze systemu Windows;

• zapytania dotyczące rodzin złośliwego oprogramowania / autorów / exploitów itp.;

• możliwość włączenia białych list, które pozwoliłyby śledczym lub kolekcjonerom na porównanie z białą listą w celu wykrycia wartości odstających;

• połączenie powyższych.

15.5. W związku z powyższym, wielu producentów systemów bezpieczeństwa analizując zagrożenia, znając techniki atakowania, posiadając najlepszą wiedzę na temat aktywności złośliwego oprogramowania - przygotowuje własne opisy (atrybuty) świadczące o tym, że system został skompromitowany lub rozpoznając i reagując na aktualną złośliwą aktywność. Dostarczane przez nich opisy zagrożenia są dobrze przygotowane i zoptymalizowane aby cechowały się dużą skutecznością i małym współczynnikiem błędnego trafienia.

15.6. Open IOC jest jednym ze sposobów opisywania zagrożenia - który nie jest standardem przyjętym przez wielu dostawców tego typu systemów zabezpieczeń. Wobec powyższego Odwołujący wnosi o dopuszczenie rozwiązania z wbudowanym skanerem, gdzie feed'y CVE (opisy zagrożenia) są dostarczane przez producenta.

16. Zarzut #16 – System zarządzania elementami bezpieczeństwa (POS7-MGNTSEC-02)

16.1. Zamawiający postawił wymaganie dla Systemu zarządzania elementami bezpieczeństwa, w wymaganiu POS7-MGNTSEC-02 wskazując jedynie wybiórczo (nie wszystkie) elementy systemu, przykładowo, Zamawiający nie postawił wymagania oprogramowania do zarządzania Koncentratorem VPN, Anty-DDOS.

16.2. Oprogramowanie do zarządzania jest przydatne, jeżeli zarządzamy wieloma urządzeniami danego typu. Nie jest natomiast użyteczne w przypadku, jeżeli mamy jedno urządzenie danego typu.

16.3. Centralne oprogramowanie do zarządzania sandbox i ochroną poczty elektronicznej nie jest czymś typowym i większość producentów tego nie posiada. Tym samym nie posiada tego firma Fortinet. Brak tego typu oprogramowania uniemożliwia firmie Fortinet zaoferowanie rozwiązania w częściach: Sandbox oraz ochrona poczty elektronicznej. Jednocześnie patrząc na wymaganie POS7-NGFWIPS-03.03 sprawdzanie plików w oferowanym systemie sandbox, firma Fortinet nie może zaoferować urządzeń typu NGFW, ponieważ urządzenia NGFW działają tylko z systemami sandbox tego samego producenta. Natomiast mając na uwadze wymaganie POS7-EMAIL-09.02sprawdzanie plików w oferowanym systemie sandbox, firma Fortinet nie może zaoferować oprogramowania antywirus.

16.4. Należy zwrócić uwagę na to, że nie ma tutaj mowy o jednym systemie zarządzania do wszystkich produktów. Praktycznie każdy z wymienionych produktów posiada całkowicie niezależny system, który nie komunikuje się z innymi. Rezygnacja z centralnego systemu zarządzania systemem sandbox oraz ochrona poczty elektronicznej, nie utrudni zarządzania danymi systemami, ponieważ zgodnie z przedstawioną architekturą, każdy system będzie pełnił inną rolę i będzie posiadał inną konfigurację. System zarządzania wypadałby na 2 urządzenia sandbox. System zarządzania urządzeniami NGFW ma sens ponieważ zarządza

wieloma urządzeniami. Wobec powyższego, rezygnacja z centralnego systemu zarządzania do systemów sandbox oraz ochrony poczty elektronicznej umożliwi złożenie oferty na konkurencyjne rozwiązania w tym firmy Fortinet.

16.5. Należy zwrócić uwagę, że Zamawiający wymaga integracji urządzeń NGFW, Ochrona poczty, Antywirus z systemem Sandbox. Natomiast taka integracja działa tylko w obrębie jednego producenta tych systemów. Oznacza to, że wykluczenie urządzeń danego producenta z któregokolwiek z wyżej wymienionych, skutkować będzie brakiem możliwości spełnienia wymagań w pozostałych elementach. Tylko kilku producentów na rynku produkuje urządzenia w każdej z tych kategorii (ok 3 producentów). Zmiany powyższych punktów pozwolą na zaoferowanie produktów innego lidera rynku w zakresie tych technologii. Jednocześnie pozwoli na zaproponowanie oferty innej niż firmy Cisco, co natomiast poskutkuje uzyskaniem zdecydowanie lepszych cen oraz zachowa zgodność z przepisami ustawy prawo zamówień publicznych a w szczególności art. 7 ust. 1 i art. 2 "ust. 2 w zakresie niezachowania uczciwej konkurencji oraz art. 29. ust. 3 PZP.

16.6. Mając na uwadze powyższe, wnoszę o usunięcie z wymagania POS7-MGNTSEC-02 zarządzania sandbox oraz pocztą elektroniczną oraz w konsekwencji usunięcie wymagań szczegółowych dotyczących zarządzania funkcjonalnościami sieciowego anty malware (POS7-MGNTSEC-05 oraz zarządzania funkcjonalnościami ochrony poczty elektronicznej (POS7-MGNTSEC-06).

17. Zarzut #17 – System zarządzania elementami bezpieczeństwa (POS7-MGNTSEC-03.01)

17.1. Zgodnie z wymaganiem POS7-MGNTSEC-03.01, System musi umożliwiać tworzenie i używanie ról administracyjnych różniących się poziomem dostępu do danego urządzenia lub grupy urządzeń/logicznych systemów. Powyższe wymaganie jest całkowicie zbędne i nieuzasadnione, ponieważ Zamawiający wymaga dostarczenia urządzenia: 5.13.4.2 SERWER AUTORYZACYJNY. Serwer taki jest centralnym punktem tworzenia i używania ról administracyjnych różniących się poziomem dostępu do danego urządzenia lub grupy urządzeń/logicznych systemów. Przy zastosowaniu centralnego systemu autoryzacji, nie stosuje się dodatkowo pośrednich systemów autoryzacji dla poszczególnych grup produktowych. Taka integracja nie jest możliwa, wobec tego wnoszę o usunięcie wymagania POS7-MGNTSEC-03.01.

18. Zarzut #18 – System zarządzania elementami bezpieczeństwa (POS7-MGNTSEC-06.01 pkt 3 e))

18.1. Zamawiający postawił wymaganie, aby System zapewniał definiowanie polityk poprzez dostarczenie wiadomości z wykonaniem dodatkowych akcji: - zapisanie wiadomości do wskazanej kolejki. Odwołujący wnosi o usunięcie wskazanej funkcjonalności, ponieważ jest ona charakterystyczna dla firmy Cisco. Producent rozwiązań do ochrony poczty, firma

Fortinet nie wykorzystuje dodatkowo kolejkowania, lecz przesyła wiadomość od razu. Pozwala to na szybsze dostarczenie wiadomości. Funkcjonalność ta nie wprowadza dodatkowego bezpieczeństwa a może utrudnić zarządzanie. Powyższe wymaganie jest nie tylko nieuzasadnione, ale także ogranicza konkurencję uniemożliwiając złożenie konkurencyjnych rozwiązań.

19. Zarzut #19 SANDBOX (POS7-SANDBOX-06.02)

19.1. Zamawiający wymaga analizy 1500 plików dziennie i jednocześnie wymaga dostarczenia urządzenia posiadającego 16 maszyn wirtualnych. Oba parametry są ściśle powiązane i od liczby maszyn wirtualnych zależy liczba przeanalizowanych plików. Jedna maszyna wirtualna jest w stanie przeanalizować na urządzeniach Fortinet 20 plików na godzinę co przy 16 maszynach daje 7680 plików dziennie. Obecne wymaganie stawia w niekorzystnej pozycji m.in. firmę Fortinet, ponieważ musi ona zaproponować modele klasę wyżej, z wyższej półki cenowej. Zamawiający stawiając wygórowane wymaganie uniemożliwia złożenie konkurencyjnej oferty, a w przypadku wyboru oferty na rozwiązanie Fortinet, zakupi droższe rozwiązanie, niż jego rzeczywiście potrzebuje.

19.2. Odwołujący wnosi o zmianę wymagania w taki sposób, aby wykonawca dostosował odpowiednią liczbę maszyn do analizy co najmniej 1500 plików dziennie. Taka zmiana pozwoli zachować cel wymagania, jakim jest analiza co najmniej 1500 plików dziennie, przy jednoczesnym nieograniczaniu konkurencji i nie narażaniu się na dodatkowe koszty.

20. Zarzuty #20 Przełączniki SAN typ I (POS7-SAN-01.04)

20.1. Zamawiający wymaga aby przełączniki SAN posiadały możliwość standardowego przydziału minimum 300 kredytów {FC buffer credits). Obecnie na rynku tylko jeden producent (Cisco) spełnia te wymagania. Wymaganie nie ma uzasadnienia technicznego. Przy najnowszej technologii dla prędkości 32Gbit każdy z portów musiałby nadawać na odległość ponad 30KM co jest niemożliwe ze względu na ograniczenia w technologii okablowania która pozwala na transmisję do maksymalnej odległości lOOm przy tej prędkości.

21. Zarzuty #21 Przełączniki SAN typ I (POS7-SAN-01.08)

21.1. Zamawiający wymaga obsługi agregacji nie mniej niż 8 portów fizycznych FC 32G w jedno połączenie logiczne („trunk", „channel") – możliwość włączenia w skład zagregowanego połączenia logicznego dowolnego aktywnego portu przełącznika. Postawione przez Zamawiającego wymaganie jest nieuzasadnione i spełnia je wyłącznie przełącznik Cisco.

22. Zarzuty #22 Przełączniki SAN typ I (POS7-SAN-05.02)

22.1. Obecnie na rynku tylko jeden producent (Cisco) wspiera SCSI w przełącznikach SAN. Protokołem wykorzystywanym w sieciach SAN jest protokół FC. W związku z tym wymaganie

obsługi protokołu SCSI jest nadmiarowe i nieuzasadnione oraz ogranicza konkurencję do jednego producenta – Cisco. Wobec powyższego, Odwołujący wnosi o zmianę wymagania poprzez usunięcia wzmianki o SCSI.

23. Zarzuty #23 Przełączniki SAN typ I (POS7-SAN-05.03)

23.1. Obecnie na rynku tylko jeden producent (Cisco) wspiera iSCSI w przełącznikach SAN. Protokołem wykorzystywanym w sieciach SAN jest protokół FC. W związku z tym wymaganie obsługi protokołu iSCSI jest nadmiarowe, nieuzasadnione i ogranicza konkurencję do jednego producenta _Cisco.

24. Zarzuty #24 Koncentrator VPN TYP I (POS7-VPN-09.02)

24.1. Niektórzy producenci koncentratorów VPN oddzielnie liczą tunele VPN site-to-site oraz remote access. W związku z tym, że tunele typu site-to-site dotyczą połączeń pomiędzy różnymi lokalizacjami, ciężko sobie wyobrazić takie wymaganie u Zamawiającego. Dużo więcej jest zestawianych tuneli typu remote access, czyli tunelu od użytkownika do centrali. Firma Fortinet rozdziela te liczby przy urządzeniu podobnej klasy na 2000 tuneli site-to-site i 50000 tuneli remote-access. Wymóg 2500 tuneli powoduje konieczność zastosowania przez firmę Fortinet urządzenia o kilka klas wyższego (i dużo droższego), który obsługuje 20 000 site-to-site oraz 100 000 remote-access. Co stawia w dużo gorszej sytuacji firmę Fortinet.

24.2. Mając na uwadze powyższe, wnoszę o dopuszczenie możliwości realizacji wymagania poprzez zaoferowanie 2000 jednoczesny tuneli VPN site-to-site oraz 10000 tuneli typu remote access.. Taka zmiana nie wpłynie negatywnie na wydajność i możliwości systemu a jednocześnie pozwoli na zaoferowanie konkurencyjnego rozwiązania

W złożonej na posiedzeniu odpowiedzi na odwołanie z 17 grudnia 2019 r. Zamawiający w pierwszej kolejności poinformował, że 16 grudnia 2019 roku opublikował na stronie internetowej wyjaśnienia i zmianę treści Załącznika nr 1 do SIWZ – Opisu przedmiotu zamówienia (dalej jako „OPZ”), w którym uwzględnił częściowo odwołanie zgodnie z żądaniem Odwołującego w zakresie:

1) zarzutu nr 1 dot. wymagania POS7-LAN-03 – pkt 5.13.1.1.2 na str. 60 OPZ,
2) zarzutu nr 2 dot. wymagania POS7-LAN-07.02 – pkt 5.13.1.1.2 na str. 61 OPZ,
3) zarzutu nr 3 dot. wymagania POS7-LAN-11.01 – pkt 5.13.1.1.3 na str. 61 OPZ,
4) zarzutu nr 4 dot. wymagania POS7-LAN-12.03 –pkt 5.13.1.1.3 na str. 61 OPZ,
5) zarzutu nr 6 dot. wymagania POS7-LAN-17.46 – pkt 5.13.1.1.6 na str. 64 OPZ – przez wykreślenie tego wymagania,
6) zarzutu nr 7 dot. wymagania POS7-LAN-18.03 – pkt 5.13.1.1.6 na str. 64 OPZ,
7) zarzutu nr 8 dot. wymagania POS7-VPN-01.07 – pkt 5.13.2.1 na str. 68 OPZ,

8) zarzutu nr 9 dot. wymagania POS7-VPN-12 – pkt 5.13.2.1.2 na str. 70 OPZ,
9) zarzutu nr 11 dot. wymagania POS7-EMAIL-07.06 – pkt 5.13.2.4 na str. 85 OPZ,
10) zarzutu nr 13 dot. wymagania POS7-EMAIL-08.01 – pkt 5.13.2.4 na str. 85 OPZ,
11) zarzutu nr 14 dot. wymagania POS7-EMAIL-08.02 – pkt 5.13.2.4 na str. 86 OPZ,
12) zarzutu nr 16 dot. wymagań: a) POS7-MGNTSEC-02 – pkt 5.13.5.2 na str. 110 OPZ, b) POS7-MGNTSEC-05 (w tym POS7-MGNTSEC-05.01, POS7MGNTSEC-05.02, POS-MGNTSEC-05.03), c) POS7-MGNTSEC-06 (w tym POS7-MGNTSEC-06.01, POS7MGNTSEC-06.02, POS7-MGNTSEC 06.03, POS7-MGNTSEC-06.04, POS7-MGNTSEC-06.05, POS7-MGNTSEC-06.06, POS7MGNTSEC-06.07),
13) zarzutu nr 18 dot. wymagania POS7-MGNTSEC-06.01 pkt 3 e) – pkt 5.13.5.2 na str. 112 OPZ,
14) zarzutu nr 19 dot. wymagania POS7-SANDBOX-06.02 –pkt 5.13.2.6.1 na str. 94 OPZ,
15) zarzutu nr 20 dot. dot. wymagania POS7-SAN-01.04 – pkt 5.13.1.1.1 na str. 57 OPZ,
16) zarzutu nr 23 dot. wymagania POS7-SAN-05.03 – pkt 5.13.1.1.1 na str. 57 OPZ,
17) zarzutu nr 24 dot. wymagania POS7-VPN-09.02 pkt 5.13.2.1.1 na str. 69 OPZ.

Jednocześnie Zamawiający stwierdził, że pozostałe zarzuty odwołania nie są zasadne, co w szczególności następująco uzasadnił :

(…)

Wbrew twierdzeniom Odwołującego Zamawiający dokonał opisu przedmiotu zamówienia zgodnie ze swoimi uzasadnionymi potrzebami.

Na wstępie wskazać należy, że zgodnie z przepisem art. 29 ust. 2 ustawy Pzp, przedmiotu zamówienia nie można opisywać w sposób, który mógłby utrudniać uczciwą konkurencję. Zgodnie natomiast z przepisem 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. Jak wskazała trafnie Krajowa Izba w wyroku z dnia 14 sierpnia 2015 roku, sygn. akt: KIO 1678/ 15 „postępowanie o udzielenie zamówienia musi być prowadzone tak, by nie prowadziło do wyłączenia bez uzasadnionej przyczyny chociażby jednego wykonawcy lub też znacznego utrudnienia mu wzięcia udziału w postępowaniu, stwarzając korzystniejszą sytuację pozostałym wykonawcom".

Jednocześnie, przedmiot zamówienia powinien być opisany w sposób uwzględniający rzeczywiste potrzeby Zamawiającego: „Obowiązek przestrzegania reguł określonych w art. 29 ust. 1 i 2 p.z.p. nie jest obowiązkiem bezwzględnym. Zamawiający ma prawo określić przedmiot zamówienia i warunki realizacji w sposób uwzględniający jego potrzeby i tak, aby uzyskać oczekiwany (najlepszy) efekt, nawet jeśli wykluczałoby to możliwość realizacji

zamówienia przez wszystkich wykonawców działających w danym segmencie rynku. Jednak wymagania muszą pozostawać w związku z obiektywnymi potrzebami zamawiającego, a nie w sposób nieuzasadniony uprzywilejowywać lub dyskryminować określonych wykonawców" – tak wyrok Krajowej Izby Odwoławczej z dnia 30 czerwca 2017 r., sygn. akt KIO 1080/17.

Nie ulega wątpliwości, że to Zamawiający jest gospodarzem postępowania, który kształtuje przedmiot zamówienia w sposób odpowiadający obiektywnym potrzebom, adekwatny do osiągnięcia zamierzonego celu, w postaci otrzymania zamówienia. Należy bowiem pamiętać, że Zamawiający jest podmiotem publicznym, zobowiązanym do działania na podstawie i w granicach prawa powszechnie obowiązującego, w tym również do przestrzegania zasad racjonalnego wydatkowania środków publicznych oraz kierowania się w trakcie realizacji zleconych zadań o szeroko rozumianym interesem publicznym. Powyższe rozważania prowadzą niewątpliwie do konstatacji, iż ustawa Pzp nie jest jedynym reżimem prawnym, do którego poszanowania zobowiązany jest Zamawiający. Kształtowanie opisu przedmiotu zamówienia i obowiązek rzetelnej, efektywnej realizacji zadań publicznych, stanowią wraz z całokształtem przepisów prawa ramy, w których „porusza się" Zamawiający i do których poszanowania jest zobowiązany.

Powyższe oznacza, że Zamawiający, dokonując opisu przedmiotu zamówienia, ma obowiązek uwzględnić własny interes i realne potrzeby, aby w konsekwencji wyboru oferty najkorzystniejszej i zawarcia umowy, otrzymać taki przedmiot zamówienia, który w możliwie najpełniejszy sposób uwzględnia jego uzasadniony interes.

Istotna w przedmiotowej sprawie jest okoliczność, iż Zamawiający realizuje projekt „Rozwój Systemu Digitalizacji Akt Postępowań Przygotowawczych w Sprawach Karnych (iSDA-2.O)" współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa, Oś priorytetowa nr 2 „E-Administracja i otwarty rząd", Działanie 2.1.

Projekt iSDA-2.O został podzielony na cztery komponenty, które są realizowane w ramach kilku odrębnych postępowań przetargowych POS-2.1: , POS04, POS-05, POS-06, POS-07 oraz-POS-08. Realizacja poszczególnych komponentów Projektu iSDA-2.0 w ramach postępowań przedstawia się następująco:

1. Komponent – System PROK-SYS w ramach postępowania POS-04;

2. Komponent – Centralne Usługi Infrastrukturalne w ramach postępowania POS-05;

3. Komponent – Platforma ITS POPD wykonana w ramach:

a. Projekt techniczny ITS, dostawa sprzętu komputerowego (serwery, macierze itp.) oprogramowania gotowego i instalacja warstwy fizycznej ITS oraz konfiguracja warstwy logicznej ITS wykonywany w ramach postępowania POS-06,

b. Projekt techniczny ITS, dostawa sprzętu sieci LAN i SAN, oprogramowania gotowego

i instalacja na warstwie fizycznej oraz konfiguracja warstwy logicznej ITS w ramach postępowania POS-07,

c. projekt warstwy logicznej ITS w ramach Projektu POS-04.

W ramach postępowania, którego dotyczy niniejsze odwołanie (POS-7), planowane jest m.in. wykonanie projektu technicznego Infrastruktury Techniczno-Systemowej, dostawa sprzętu sieci LAN i SAN oraz oprogramowania gotowego. Istotny jest fakt, iż przedmiot wszystkich postępowań, o których mowa powyżej, jest ze sobą ściśle powiązany, gdyż łącznie prowadzą do realizacji jednego projektu, jakim jest Rozwój Systemu Digitalizacji Akt Postępowań Przygotowawczych. Rozwiązania, sprzęt i oprogramowanie dostarczane w ramach postępowania POS-7 muszą być zatem w pełni kompatybilne z istniejącą infrastrukturą Zamawiającego.

Ocenie w niniejszym postępowaniu powinna podlegać okoliczność czy Odwołujący ma możliwość złożenia oferty ważnej i odpowiadającej wymogom Zamawiającego. przedstawione przez Zamawiającego parametry opisane w SIWZ, do których Odwołujący odnosi się w zarzutach nr 5, 10, 12, 15, 17, 21, 22 nie uniemożliwiają Odwołującemu złożenia ważnej oferty w przedmiotowym postępowaniu.

W tym miejscu należy wskazać, że Odwołujący nie wykazał, a nawet nie uprawdopodobnił, iż nie ma możliwości złożenia w postępowaniu oferty ważnej i zgodnej z wymaganiami Zamawiającego. Wykonawca sugeruje jedynie, iż sposób ukształtowania parametrów sprzętu powoduje, iż Zamawiający naraża się na otrzymanie droższej oferty. Tymczasem Zamawiający dąży do tego, aby otrzymać ofertę najlepszą, co nie jest równoznaczne z ofertą najtańszą. Oferowane przez wykonawców rozwiązania mają z założenia odpowiadać w pełni potrzebom Zamawiającego, a nie oznacza to, iż powinny być rozwiązaniami najtańszymi na rynku. Odwołujący podnosi, iż sposób ukształtowania OPZ przez Zamawiającego stawia w gorszej sytuacji tych producentów, którzy dla zapewnienia spełnienia określonych przez Zamawiającego parametrów, musieliby ponieść dodatkowe koszty. Powyższe potwierdza, że nie jest wykluczona realizacja zamówienia przez wykonawcę przy wykorzystaniu rozwiązań różnych producentów funkcjonujących na rynku, jednakże może się to wiązać z większymi kosztami. Odwołujący nie wykazał zatem, iż złożenie oferty zgodnej z wymaganiami Zamawiającego nie jest możliwe.

Nie można zapominać o tym, iż nie utrudnia uczciwej konkurencji takie opisanie przedmiotu zamówienia, które eliminuje możliwość zrealizowania zamówienia przez niektórych potencjalnych oferentów, jeżeli jest to uzasadnione rzeczywistymi potrzebami zamawiającego. Uzasadnione potrzeby podmiotu zamawiającego mogą usprawiedliwiać ograniczenie kręgu potencjalnych wykonawców oraz wpływać na zakres oferowanych przez nich usług, dostaw i robót budowlanych, o ile wynikają one z celu, dla którego podmiot

zamawiający wszczyna określone postępowanie, a cel ten jest nakierowany na realizację tychże potrzeb i w żaden inny sposób nie może zostać osiągnięty (zasada proporcjonalności), zaś wymagania zamawiającego związane są z istotą przedmiotu zamówienia i jego indywidualnymi właściwościami pozwalającymi na osiągniecie wskazanego wyżej celu (zob. KIO 2184/13). Zamawiający ma prawo określić przedmiot zamówienia w sposób odpowiadający jego indywidualnym potrzebom, a fakt, że nie wszystkie podmioty z danej branży mogą wziąć udział w postępowaniu, nie przesądza o tym, że postępowanie narusza zasady uczciwej konkurencji (zob. KIO/UZP 204/08).

W przytoczonym powyżej wyroku KIO 2184/ 13 uznano, że analiza normy prawnej wyrażonej w art. 29 ust. 2 Pzp „(...) wskazuje, iż aby doszło do złamania określonego w art. 29 ust. 2 ustawy P.z.p. zakazu, sposób i treść merytoryczna opisu przedmiotu zamówienia musi być sformułowana w ten sposób, iż przy określonych realiach rynkowych, prawnych i gospodarczych, tj. w określonej sytuacji na rynku właściwym, dochodzi do faktycznego monopolu jednego wykonawcy, producenta, dystrybutora (monopolu podmiotowego) lub monopolu jednego określonego rodzaju produktu (monopolu przedmiotowego)".

(...)

Odnosząc się szczegółowo do poszczególnych zarzutów Odwołującego, nieuwzględnionych przez Zamawiającego, należy wskazać co następuje:

1. Zarzut nr 5 – wymaganie POS7-LAN-15.01

Zamawiający potrzebuje rozwiązania zapewniającego 77 portów zgodnie z kalkulacją ilości połączeń dla strefy zewnętrznej. Zastosowanie rozwiązania proponowanego nie jest równoważne technicznie – dwa połączenia 48 portowe nie zapewniają tej samej funkcjonalności pod względem przełączania co rozwiązanie 96 portowe.

2. Zarzut nr 10 – POS7-NGFWIPS-01.13 lit. a

Zamawiający stoi na stanowisku, iż wbrew twierdzeniom Odwołującego poziom 3.000 aplikacji jest aktualnie standardem rynkowym, spełnianym przez wiodących dostawców rozwiązań NGFW. Wymaganie spełnia, poza wymienionym rozwiązaniem np. PaLo Alto Networks (https:/_/applipedia.paloaltonetworks.com – ponad 3150 aplikacji), Checkpoint (https://sc1.checkpoint.com/documents/R76/ CP R76 ADDControl WebAdmin/60 902.htm – ponad 4500 aplikacji) czy Fortinet (https://fortiguard.com/appcontrol ponad 4.000 aplikacji).

3. zarzut nr 12 – wymaganie POS7-EMAIL-07.07

Wbrew stanowisku Odwołującego sformułowane w POS7-EMAIL-07.07 wymaganie nie ma na celu ochrony przed podszywaniem się pod maile chronionej domeny, a zabezpieczenie przed skanowaniem domeny w celu zbudowania bazy rzeczywistych adresów dostępnych w danej domenie, która później mogłaby zostać wykorzystana np. w celu przeprowadzenia celowanego ataku phishingowego

4. Zarzut nr 15 – POS7-ANTWIR-05.11

OpenIOC jest standardową metodą opisu wskaźników kompromitacji, umożliwiającą analitykom organizację, archiwizację i współdzielenie informacji o celowych atakach, które często nie są rozpoznawane czy widoczne dla dostawców rozwiązań. Skaner podatności utrzymywany przez dostawcę systemu nie zastępuje mechanizmu OpenIOC, kłów stanowi jego uzupełnienie.

Proponowane przez Odwołującego rozwiązanie nie stanowi rozwiązania równoważnego, bowiem uniemożliwia Zamawiającemu tworzenie własnych charakterystyk zagrożeń, opierając się wyłącznie na opisach dostarczanych przez producenta rozwiązania, co w przypadku niestandardowych aplikacji (w tym iSDA, o charakterze w znacznej mierze zamkniętym, ponadto narażonym na ataki celowane) oparcie się wyłącznie na mechanizmach standardowych, bez możliwości ich uzupełnienia stanowi istotne ograniczenie funkcjonalne.

Metody opisu zgodne z OpenIOC implementuje przy tym wielu producentów rozwiązań klasy EDR, m.in.:

1) FireEye (https://www.fireeye.com/blog/threat-research/2013/ 10/ openioc basics.html)

2) TrendMicro (https://www.tr_endmicro.com/pl DI/ business/ products/ detectionresponse/edr-endpoint-sensor.html)

3) Qualys (https://www.qualys.com/clocs/451 -qualys-en dpoint-saas-edrfunctionality.pdf)

4) Fidelis (https://www.fidelissecuritv.com/solutions/endD0int-detectionresponse)

5. Zarzut nr 17 – wymaganie POS7-MGNTSEC-03.01

Argumentacja Odwołującego nie znajduje potwierdzenia w okolicznościach faktycznych. Na wstępie należy zauważyć, że wymóg obsługi zarządzania opartego o role jest określony także w wymaganiach ogólnych dla wszystkich systemów (POS7-WYMOG-06 d), co do którego Odwołujący nie wnosi zastrzeżeń.

Niezależnie od tego, typową właściwością systemów zarządzania jest hierarchizacja i ograniczanie uprawnień poszczególnych użytkowników. Mając na uwadze, że każdy komponent systemu ma swoje specyficzne właściwości, niemożliwe jest zbudowanie na poziomie centralnego serwera autoryzacyjnego uniwersalnej struktury uprawnień, obejmującej wszystkie komponenty. Zamiast tego powszechnie stosuje się hierarchię polegającą na:

1) określeniu na poziomie serwera autoryzacyjnego przynależności O poszczególnych użytkowników do grup,

2) określenia na poziomie każdego z elementów systemów zarządzania (odpowiedzialnych za poszczególne typy komponentów) mapowania grup użytkowników do ról, określających

zakres uprawnień w ramach danego systemu.

Taki model jest stosowany powszechnie, należy zatem stwierdzić, że zarzut bierze się z braku zrozumienia celu sformułowania wymagania, który powinien zostać wyjaśniony przez skierowanie do Zamawiającego pytań wyjaśniających.

6. Zarzut nr 21 – POS7-SAN-01.08

Możliwość zestawienia jednego łącza grupującego w sobie do 8 łącz 32Gb/s jest dostępne w przełącznikach SAN nie tylko firmy CISCO. Np. przełącznik SAN firmy Brocade G620 zapewnia taką funkcjonalność https://www.dataswitchworks.com/datasheets/switches/brocade-g620-switch-ds.pdf strona 6 („ISL trunking – Frame-based trunking with up to eight 32 Gbps SFP+ ports per ISL trunk or up to two 128 Gbps QSFP ports per ISL trunk. Exchange-based load balancing across ISLs with DPS included in Brocade Fabric OS").

7. Zarzut nr 22 – POS7-SAN-05.02

Zarzut wynika z błędnej interpretacji przez Odwołującego wymagania, które nie odnosi się do wykorzystania SCSI a do inspekcji nagłówków SCSI.

Tak sformułowany zarzut wskazuje na brak zrozumienia działania urządzeń sieci SAN przez Odwołującego. Zamawiający pragnie zauważyć, że każde dostępne na rynku urządzenie sieci SAN obsługuje protokół SCSI, którym komunikują się serwery z urządzeniami pamięci masowych za pomocą protokołu FC który zapewnia transport pakietów SCSI. Używając pewnego rodzaju porównania można napisać, że w tym przypadku protokół PC jest autostradą łącząca dwa miasta (serwer i macierz dyskową) a protokół SCSI to ciężarówki przewożące tą autostradą dane.

Dla przykładu na przełącznikach SAN Brocade występuje funkcjonalność FlowMonitor (w ramach FlowVision https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-00005946en_us), umożliwiająca analizę nagłówków SCSI i budowanie dla nich statystyk.

Zarzut naruszenia przepisu art. 30 ust. 4 ustawy Pzp

W tym miejscu należy wskazać, że Zamawiający w treści Rozdziału IV ust. 8-10 SIWZ zawarł następujący opis równoważności:

„8.Ilekroć w treści SIWZ, w tym w opisie przedmiotu zamówienia, użyte są znaki towarowe, patenty lub pochodzenie, a także normy, Zamawiający dopuszcza rozwiązanie równoważne.

9. Przez produkt równoważny dla wyspecyfikowanego przedmiotu zamówienia rozumie się taki, który posiada lub realizuje te same funkcje/ funkcjonalności jak produkt określony za pomocą wskazania znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty dostarczane przez konkretnego wykonawcę oraz jego zastosowanie nie wymaga żadnych dodatkowych nakładów (finansowych, programistycznych, sprzętowych) związanych z dostosowaniem infrastruktury Zamawiającego określonej w Opisie przedmiotu zamówienia.

10. Przez normę jakościową, równoważną rozumie się taką, która potwierdza, że dostarczane produkty odpowiadają określonym normom lub specyfikacjom technicznym lub poświadcza zgodność działać Wykonawcy z normami jakościowymi lub poświadcza zgodność działań Wykonawcy z równoważnymi normami jakościowymi odwołującymi się do systemów zapewniania jakości opartych na odpowiednich normach europejskich lub potwierdza odpowiednio stosowanie przez Wykonawcę równoważnych środków zapewnienia jakości".

Zamawiający w treści opisu przedmiotu zamówienia nie posługuje się znakami towarowymi, patentami, pochodzeniem lub normami zamawianych produktów. Gdyby natomiast miało to miejsce, wówczas dopuszczalne byłoby przedstawienie przez każdego z Wykonawców rozwiązania równoważnego.

Ponieważ odwołanie nie zawierało braków formalnych, a wpis od niego został uiszczony – podlegało rozpoznaniu przez Izbę.

W toku czynności formalnoprawnych i sprawdzających Izba nie stwierdziła, aby odwołanie podlegało odrzuceniu na podstawie przesłanek określonych w art. 189 ust. 2 pzp i nie zgłaszano w tym zakresie odmiennych wniosków.

Zgodnie z art. 186 ust. 3a pzp w przypadku uwzględnienia przez zamawiającego części zarzutów przedstawionych w odwołaniu i wycofania pozostałych zarzutów przez odwołującego, Izba może umorzyć postępowanie na posiedzeniu niejawnym bez obecności stron oraz uczestników postępowania odwoławczego, którzy przystąpili do postępowania po stronie wykonawcy, pod warunkiem że w postępowaniu odwoławczym po stronie zamawiającego nie przystąpił w terminie żaden wykonawca albo wykonawca, który przystąpił po stronie zamawiającego nie wniósł sprzeciwu wobec uwzględnienia części zarzutów. W takim przypadku zamawiający wykonuje, powtarza lub unieważnia czynności w postępowaniu o udzielenie zamówienia zgodnie z żądaniem zawartym w odwołaniu w zakresie uwzględnionych zarzutów.

Według art. 187 ust. 8 pzp odwołujący może cofnąć odwołanie do czasu zamknięcia rozprawy; w takim przypadku Izba umarza postępowanie odwoławcze. Jeżeli cofnięcie nastąpiło przed otwarciem rozprawy, odwołującemu zwraca się 90% wpisu. Przy czym nie budzi wątpliwości w doktrynie i orzecznictwie, że skoro odwołujący jest uprawniony do wycofania odwołania w całości, ma również prawo zrezygnować z popierania niektórych jego zarzutów. Za taką interpretacją przemawia również art. 186 ust. 3a pzp, który wprost reguluje szczególną sytuację wycofania odwołania w takim zakresie, w jakim nie zostało ono uwzględnione przez zamawiającego.

Jednocześnie z przywołanego art. 186 ust. 3a pzp wynika *a contrario*, że nie dochodzi do umorzenia postępowania odwoławczego, jeżeli odwołujący nie wycofał wszystkich zarzutów nieuwzględnionych przez zamawiającego. W orzecznictwie Izby nie budzi jednak wątpliwości, że zarówno zarzuty uwzględnione przez zamawiającego, jak i zarzuty wycofane przez odwołującego nie podlegają merytorycznemu rozpoznaniu, a w odniesieniu do tych pierwszych zamawiający wykonuje, powtarza lub unieważnia czynności w prowadzonym postępowaniu zgodnie z żądaniami odnoszącymi się do tych uwzględnionych zarzutów. Stąd za prawidłowe należy uznać odzwierciedlenie w orzeczeniu kończącym postępowanie odwoławcze w sprawie danego odwołania, że w zakresie zarzutów uwzględnionych lub wycofanych podlega ono umorzeniu.

W tej sprawie Zamawiający uwzględnił odwołanie w zakresie powyżej wskazanym, a Odwołujący dodatkowo na posiedzeniu oświadczył, że podtrzymuje odwołanie jedynie w zakresie zarzutów nr 5, 10 i 12, więc w zakresie wszystkich pozostałych zarzutów postępowanie odwoławcze podlegało umorzeniu.

Z tych względów – działając na podstawie art. 186 ust. 3a pzp, art. 187 ust. 8 w zw. z art. 192 ust. 1 zd. 2 ustawy Prawo zamówień publicznych – Izba orzekła, jak w pkt 1. sentencji.

Z uwagi na brak podstaw do odrzucenia odwołania lub umorzenia postępowania odwoławczego w całości sprawa – w zakresie zarzutów nieuwzględnionych przez Zamawiającego lub niewycofanych przez Odwołującego, czyli zarzutów nr 5, 10 i 12 – została skierowana do rozpoznania na rozprawie, podczas której Odwołujący, Zamawiający i Przystępujący podtrzymali dotychczasowe stanowiska.

Po przeprowadzeniu rozprawy z udziałem Odwołującego, Zamawiającego i Przystępującego, uwzględniając zgromadzony materiał dowodowy, jak również biorąc pod uwagę oświadczenia i stanowiska zawarte w odwołaniu i piśmie procesowym Odwołującego, odpowiedzi na odwołanie, zgłoszeniu przystąpienia, a także wyrażone ustnie na rozprawie i odnotowane w protokole, Izba ustaliła i zważyła, co następuje:

Z art. 179 ust. 1 pzp wynika, że odwołującemu przysługuje legitymacja do wniesienia odwołania, gdy ma (lub miał) interes w uzyskaniu zamówienia oraz może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy.

Legitymacja Odwołującego jako kwestionującego postanowienia specyfikacji, które negatywnie wpływają na możliwość złożenia przez niego oferty, nie budziła wątpliwości.

{zarzut 5. dot. POS7-LAN-15.01 i wymagań powiązanych}

Odwołujący na rozprawie sprecyzował, że na zarzut składają się dwa aspekty, które łącznie ograniczają konkurencję, tj. wymaganie 96 portów, z których każdy ma być o przepustowości 25 GE. Stąd wystarczające byłoby, aby Zamawiający obniżył wymagania w jednym z tych aspektów.

Niezależnie od powyższego według Odwołującego alternatywą jest również dopuszczenie zaoferowania dwóch przełączników po 48 portów przy utrzymaniu wymaganej przepustowości 25 GE, gdyż z punktu widzenia użytkownika docelowego systemu, który ma być centralnie zarządzany, taka zmiana nie ma żadnego znaczenia.

Natomiast Zamawiający wskazał na rozprawie, że wymagana liczba portów wynika z opartego o projekt wykonawczy systemu (niebędący elementem dokumentacji tego postępowania) wyliczenia potrzeb w tym zakresie poszczególnych urządzeń systemu budowanego w ramach całego projektu, które przedstawił na rozprawie. Wyjaśnił, że uwidoczniono na nim liczbę portów koniecznych dla podłączenia urządzeń znajdujących się w zewnętrznej strefie bezpieczeństwa, na żółto zaznaczono zsumowaną łączną liczbę portów 3 typów – łącznie 170 portów, co po odjęciu 16 portów z obszaru zewnętrznego („DMZ") daje 154 porty, czyli po 77 na przełącznik, a z kolei najbliższy tej liczbie występujący na rynku przełącznik jest 96-portowy.

Jednocześnie Zamawiający zaznaczył, że wymaga wyższej przepustowości niż minimalnie konieczna dla zbudowania systemu, gdyż musi uwzględnić konieczność rozwoju tego systemu, tj. że w przyszłości będzie potrzebna większa przepustowość.

Zamawiający podtrzymał również, że dwa przełączniki 48-portowe nie są ekwiwalentem jednego przełącznika 96-portowego, gdyż z uwagi na konieczność komunikacji pomiędzy dwoma urządzeniami jego wydajność będzie mniejsza niż jednego urządzenia.

Ponadto według Zamawiającego stanowisko Odwołującego nie jest spójne, bo w odniesieniu do wymagania LAN-16.03 postuluje on zmanię polegającą na alternatywnym dopuszczeniu dwóch przełączników o przepustowości 2 000 Mpps każdy, a jednocześnie na str. 12 odwołania w pkt 6.4. wskazuje na chęć zaoferowania dwóch przełączników, każdy o przepustowości 1600 Mpps, co prowadziłoby w konsekwencji do niespełnienia wymagania LAN 16.03 w kształcie postulowanym na str. 5. odwołania.

Zamawiający złożył również wydruk zestawienia produktów producenta ARISTA w zakresie przełączników, wskazując, że jeden z modeli przełączników, tj. 7060CX2-32S spełnia wymagania OPZ(co zaznaczono odręcznie).

W ocenie Izby Zamawiający przekonująco uzasadnił swoje wymaganie zarówno odnośnie liczby portów, jak i ich przepustowości, skoro pierwszy z parametrów zabezpiecza potrzeby wszystkich urządzeń składających się na docelowy system budowany w ramach całego przedsięwzięcia, a drugi gwarantuje skalowalność tego systemu.

Natomiast bezprzedmiotowe okazały się wyliczenia Odwołującego co do liczby portów, gdyż opierały się jedynie na rysunku nr 4 dotyczącym architektury warstwy fizycznej ITS w POPD – Zewnętrznej Strefy Bezpieczeństwa (str. 19 OPZ). Jednocześnie Odwołujący nie wskazał przekonujących argumentów, które wskazywałby na nieracjonalność wymagania przez Zamawiającego przepustowości na poziomie wyższym niż konieczna na początku funkcjonowania budowanego systemu.

Za nieudowodnione (a równocześnie niemające charakteru notoryjnego) należy uznać twierdzenie Odwołującego zrównujące jeden przełącznik 96-portowy z dwoma połączonymi w bliżej niesprecyzowany sposób przełącznikami 48-portowymi. Gdyby takie uproszczenie było adekwatne, na rynku nie występowałyby inne przełączniki niż np. 16-portowe, które można by łączyć po dwa lub więcej.

Niezależnie od powyższego na rozprawie okazało się, że Zamawiający dopuszcza osiągnięcie wymaganej liczby portów przez zastosowanie przewodu rozdzielającego (ang. „breakout cable"), co satysfakcjonuje Odwołującego, który błędnie założył, nie zwracając się w tym zakresie do Zamawiającego o wyjaśnienia, że sformułowanie „porty definiowane przez wkładki SFP" uniemożliwia zaoferowanie takiego rozwiązania. Tym samym zarzut odwołania okazał się bezprzedmiotowy, skoro nie tylko przełączniki Cisco mogą spełnić powyższe wymaganie.

Niczego nie wnosi do sprawy złożone przez Odwołującego jako wniosek dowodowy zestawienie urządzeń jednego z producentów, gdyż może co najwyżej dowodzić, że ten konkretny producent nie ma w ofercie produktów spełniających parametry ujęte w ramach identyfikatora POS7-LAN-15.01.

{zarzut 12. dot. POS7-EMAIL-07.07}

Zarzut zawarty w odwołaniu okazał się bezprzedmiotowy, gdyż jego istotą było zaniechanie dopuszczenia innej metody ochrony przed podszywaniem się pod maile chronionej domeny, podczas gdy w rzeczywistości – jak wyjaśnił Zamawiający w odpowiedzi na odwołanie – wymaganie to służy zabezpieczeniu przed skanowaniem domeny w celu zbudowania bazy rzeczywistych adresów dostępowych w danej domenie, która mogłaby zostać wykorzystana np. w celu przeprowadzenia celowanego ataku phishingowego. Odwołujący nie podważał na rozprawie, że tak jest w istocie, domagając się zamiast

określenia funkcjonalności jako możliwości ochrony przed podszywaniem pod maile chronionej domeny, wprowadzenia, określenia funkcjonalności w sposób odpowiadający powyższemu wyjaśnieniu.

Zgodnie z art. 192 ust. 7 pzp Izba nie może orzekać co do zarzutów, które nie były zawarte w odwołaniu. Oznacza to, że niezależnie od wskazania w odwołaniu przepisu, którego naruszenie jest zarzucane zamawiającemu, Izba jest uprawniona do oceny prawidłowości zachowania zamawiającego (podjętych czynności lub zaniechania czynności), jedynie przez pryzmat sprecyzowanych w odwołaniu okoliczności faktycznych i prawnych uzasadniających jego wniesienie. Mają one decydujące znaczenie dla ustalenia granic kognicji Izby przy rozpoznaniu sprawy, gdyż konstytuują zarzut podlegający rozpoznaniu. Krajowa Izba Odwoławcza wielokrotnie wypowiadała się w tym przedmiocie. W szczególności w wyroku z 1 grudnia 2009 r. (sygn. akt KIO/UZP 1633/09) Izba wskazała, że zarzut odwołania stanowi wskazanie czynności lub zaniechanej czynności zamawiającego (arg. z art. 180 ust. 1 pzp) oraz okoliczności faktycznych i prawnych uzasadniających jego wniesienie. Trafność takiego stanowiska została potwierdzona w orzecznictwie sądów okręgowych, w szczególności w wyroku z 25 maja 2012 r. (sygn. akt XII Ga 92/12) Sąd Okręgowy w Gdańsku wywiódł, że Izba nie może orzekać co do zarzutów, które nie były zawarte w odwołaniu, przy czym stawianego przez wykonawcę zarzutu nie należy rozpoznawać wyłącznie pod kątem wskazanego przepisu prawa, ale również jako wskazane okoliczności faktyczne, które podważają prawidłowość czynności zamawiającego i mają wpływ na sytuację wykonawcy.

W konsekwencji o ile dowody na mocy art. 190 ust. 1 pzp odwołujący może przedstawiać aż do zamknięcia rozprawy, o tyle okoliczności, z których chce wywodzić skutki prawne musi uprzednio zawrzeć w odwołaniu, pod rygorem ich nieuwzględnienia przez Izbę z uwagi na art. 192 ust. 7 pzp. Należy rozgraniczyć bowiem okoliczności faktyczne konstytuujące zarzut, czyli określone twierdzenia o faktach, z których wywodzone są skutki prawne, od dowodów na ich poparcie. Stąd odwołanie, które inicjuje postępowanie odwoławcze, zawsze musi zawierać okoliczności uzasadniające zarzucenie zamawiającemu naruszenia przepisów ustawy pzp. Nawet wtedy, gdy pewne informacje dotyczące działań lub zaniechań zamawiającego są niedostępne z uwagi na uznanie ich przez zamawiającego za stanowiące tajemnicę przedsiębiorstwa (jego lub innego wykonawcy), wykonawca musi zawrzeć w odwołaniu, na czym mogłoby polegać nieprawidłowe postępowanie zamawiającego, licząc że stawiane w ciemno zarzuty znajdą potwierdzenie w toku postępowania odwoławczego.

Ponieważ w tym przypadku Odwołujący sam błędnie zidentyfikował, czemu służy skarżone przez niego wymaganie, i na tym błędnie poczynionym założeniu oparł jego

zakwestionowanie, zarzut zawarty w odwołaniu należało uznać za bezzasadny. Co prawda Odwołujący zmienił na rozprawie żądanie, ale aby było możliwe uczynienie mu zadość, musi ono być skorelowane z zarzutem, a w tym przypadku zgłoszone nowe żądanie jest oderwane od zarzutu, który podlegał rozpoznaniu przez Izbę.

W konsekwencji bez znaczenia dla sprawy jest również zgłoszone przez Odwołującego jako wniosek dowodowy oświadczenie z 12 grudnia 2019 r. dystrybutora sprzętu komputerowego wymienionych w jego treści producentów, gdyż albo dotyczy niewłaściwie postawionego zarzutu w odwołaniu, albo jest związane li tylko tym nowym żądaniem zgłoszonym na rozprawie. Przede wszystkim zauważyć należy, że jest to ogólnikowe stanowisko dotyczące łącznie całego pkt 5.13.2.4 OPZ, czyli wszystkich kilkudziesięciu wymagań ogólnych systemu poczty elektronicznej (rozpisanych w ramach identyfikatorów od POS7-EMAIL-01 do POS7-EMAIL-09) jednocześnie, w tym takich, które zostały już zniesione w ramach zmiany treści s.i.w.z. z 16 grudnia 2019 r. Nie sposób zatem nawet stwierdzić, jakie byłoby stanowisko tego podmiotu w odniesieniu wyłącznie do wymagania POS7-EMAIL-07.07.

{zarzut 15. dot. POS7-ANTVIR-05.11}

Na rozprawie okazało się, że stosowanie OpenIOC jako metodologii opisu tzw. wskaźników kompromitacji nie tylko przez CISCO, ale i przez innych producentów rozwiązań klasy EDR, co podniósł Zamawiający w odpowiedzi na odwołanie, nie jest okolicznością sporną.

Przede wszystkim Izba stwierdziła, że zarzut postawiony w odwołaniu zmierza do dostosowania opisu przedmiotu zamówienia do potrzeb Odwołującego, a nie Zamawiającego, zgodnie z żądaniem, aby w całości usunąć wymaganie POS7-ANTYVIR-05.11. Jeżeli Zamawiający chce mieć możliwość samodzielnego tworzenia własnych charakterystyk zagrożeń według metodologii OpenIOC, a nie tylko polegać na opisach dostarczanych przez producenta danego systemu zabezpieczeń, ma takie prawo, a Odwołujący nie może narzucać rozwiązań bez wsparcia dla sygnatur OpenIOC tylko dlatego, że chciałby je zaoferować w tym postępowaniu. W szczególności bez znaczenia jest dla sprawy, czy tworzenie sygnatur IOC jest skomplikowane, wymaga gruntownej znajomości systemów, ataków, działania złośliwego kodu i wiąże się z dużym nakładem czasu z punktu widzenia utrzymania i obsługi systemu, zwłaszcza że Odwołujący nie ma żadnej wiedzy na temat kompetencji pracowników Zamawiającego w tym zakresie.

Za bez znaczenia dla sprawy należy uznać zgłoszone przez Odwołującego jako wniosek dowodowy oświadczenie z 12 grudnia 2019 r. dystrybutora sprzętu komputerowego

wymienionych w jego treści producentów, gdyż jest to ogólnikowe stanowisko dotyczące łącznie całego pkt 5.13.2.5 OPZ, czyli wszystkich kilkudziesięciu wymagań ogólnych stawianych oprogramowaniu antywirusowemu/EDR dla serwerów (rozpisanych w ramach identyfikatorów od POS7-ANTYVIR-01 do POS7-ANTYVIR-05) jednocześnie, w tym takich, które zostały już zmodyfikowane w ramach zmiany treści s.i.w.z. z 16 grudnia 2019 r. Nie sposób zatem nawet stwierdzić, jakie byłoby stanowisko tego podmiotu w odniesieniu wyłącznie do wymagania POS7-EMAIL-05.11. w aspekcie wsparcia dla sygnatur OpenIOC.

{rozważania wspólne dla 5., 10. i 12. zarzutu}

Podkreślić należy, że Izba nie stwierdziła w tej sprawie ani pośredniego, ani bezpośredniego naruszenia konkurencji przez opis parametrów, których dotyczą rozpoznawane zarzuty, gdyż Odwołujący tego nie wykazał, choć z mocy art. 190 ust. 1 pzp na nim spoczywał ciężar dowodu w tym zakresie. Abstrahując od tego, że nieudowodnione pozostało ogólne twierdzenie Odwołującego, że opis przedmiotu zamówienia w powyższym zakresie wskazuje wyłącznie na produkty CISCO, istotniejszy jest brak wykazania, że zaskarżone parametry nie są uzasadnione zobiektywizowanymi potrzebami Zamawiającego, wynikającymi z potrzeby zbudowania i eksploatowania systemu iSDA 2.0. W takim przypadku nie ma bowiem znaczenia, jak wielu producentów oferuje produkty spełniające parametry techniczne, których nie można uznać za dyskryminujące tylko z tego względu, że w ocenie Odwołującego są zbyt wyśrubowane.

W konsekwencji wszystkie powyższe zarzuty naruszenia przez Zamawiającego art. 29 ust. 2 w zw. z art. 7 ust. 1 pzp należy uznać za bezzasadne, gdyż zakaz dokonywania opisu przedmiotu zamówienia w sposób, który może utrudniać uczciwą konkurencję, należy tak interpretować, jak wskazuje utrwalone w tym zakresie orzecznictwo Izby.

Zasada równego traktowania sprowadza się do konieczności identycznego traktowania takich wykonawców, których sytuacja jest taka sama lub bardzo podobna, nie oznacza to natomiast konieczności identycznego traktowania wszystkich wykonawców znajdujących się na rynku lub aspirujących do wejścia na rynek. Opis przedmiotu zamówienia nie może preferować jedynie niektórych podmiotów. Wszyscy wykonawcy powinni mieć zapewniony równy dostęp do istotnych dla postępowania informacji w jednakowym czasie, dokonywanie oceny warunków oraz ofert powinno następować wedle wcześniej sprecyzowanych i znanych wykonawcom kryteriów, na podstawie przedłożonych dokumentów, a nie wiedzy zamawiającego. Nie oznacza to jednak, że zamawiający tylko wówczas działa w granicach uczciwej konkurencji oraz z zachowaniem wymogu proporcjonalności przy opisie przedmiotu zamówienia, gdy jego działania pozwalają

na uczestnictwo w postępowaniu o udzielenie zamówienia publicznego wszystkim podmiotom występującym na rynku. Jeżeli zatem zamawiający, określając warunki udziału w postępowaniu, w tym warunki kontraktowe, nie czyni tego w sposób, który wskazuje na konkretny produkt lub wykonawcę, nie można uznać, iż narusza zasady uczciwej konkurencji poprzez odniesienie się do przedmiotu zamówienia. Nie jest obowiązkiem Zamawiającego uwzględnianie doświadczenia zawodowego i polityki prowadzenia działalności komercyjnej wszystkich podmiotów działających na rynku, ale uwzględnienie wymagań gwarantującej sprawne wykonanie danego zamówienia, na miarę potrzeb i możliwości Zamawiającego (z uzasadnienia wyroku z 9 września 2019 r. sygn. akt KIO 1636/19).

Opis przedmiotu zamówienia nie może ograniczać uczciwej konkurencji co wynika z przepisu art. 29 ust. 2 p.z.p. jednak nie jest tak, że Zamawiający w każdym przypadku ma otrzymać dokładnie to co wskazuje wykonawca, gdyż Zamawiający jako dysponent postępowania decyduje wobec prowadzonego postępowania co ma być przedmiotem zamówienia – z zastrzeżeniem oczywiście, że opis przedmiotu zamówienia nie może utrudniać uczciwej konkurencji (z uzasadnienia wyroku z 26 sierpnia 2019 r. sygn. akt KIO 1537/19).

Aby wykazać, że opis przedmiotu zamówienia narusza przepisy art. 29 ust. 1 i 2 oraz art. 7 ust. a wiec narusza zasady równego traktowania wykonawców oraz konkurencyjności zamówień, odwołujący winien co najmniej uprawdopodobnić, że w postępowaniu nie można złożyć oferty, spełniającej wymogi zamawiającego. Niemożność ta powinna mieć charakter obiektywny – w tym sensie, że nie tylko odwołujący nie jest w stanie spełnić wymogów zamawiającego co do realizacji przedmiotu zamówienia (z uzasadnienia wyroku z 16 maja 2019 r. sygn. akt KIO 797/19).

Każdy opis przedmiotu zamówienia niesie za sobą ograniczenie konkurencji, pośrednio lub bezpośrednio preferując jednych wykonawców obecnych na rynku i dyskryminując innych. Konieczność zachowania zasady uczciwej konkurencji nie oznacza, że zamawiający nie ma prawa opisać przedmiotu zamówienia w sposób uwzględniający jego osobiste potrzeby, na co wskazywał zamawiający w tym przypadku. Nikt też nie odbiera zamawiającemu prawa, jako gospodarzowi postępowania do wskazania swoich potrzeb poprzez takie ustalenie parametrów sprzętu aby sprzęt ten służył jego specyficznym potrzebom. Zgodzić się o też należy, że zamawiający nie ma także obowiązku zapewnienia możliwości realizacji przedmiotu zamówienia wszystkim podmiotom działającym na rynku w danej branży. Prawie nigdy nie jest możliwe opisanie przedmiotu zamówienia, który w ten czy inny sposób nie uniemożliwia części wykonawcom złożenie oferty, a niektórych stawia w uprzywilejowanej pozycji. Izba wskazuje, iż zamawiający powinien opisać przedmiot

zamówienia w sposób jasny, zrozumiały i kompletny, zachowując zasady uczciwej konkurencji, ich poszanowanie nie oznacza, że zamawiający ma nabyć w ramach postępowania o udzielenie zamówienia przedmiot o niskiej jakości, niezaspokajający jego potrzeb, ma oczywiście prawo wymagać nie tylko odpowiedniej jakości, ale również tak określić przedmiot zamówienia, aby odpowiadał celom dla których ma służyć, wykazując się jednak również szczególną dbałością o racjonalne wydatkowanie środków publicznych (z uzasadnienia wyroku z 18 kwietnia 2019 r. sygn. akt KIO 585/19)

Niewątpliwie opis przedmiotu zamówienia nie może ograniczać uczciwej konkurencji, zgodnie z art. 29 ust. 2 p.z.p., niemniej to zamawiający jako gospodarz postepowania decyduje co ma być przedmiotem zamówienia, z zastrzeżeniem, że opis przedmiotu zamówienia nie może utrudniać uczciwej konkurencji. Nie można zasady uczciwej konkurencji pojmować tak, że zamawiający winien zaakceptować każde świadczenie, nawet niezgodne z jego potrzebami, jedynie dlatego, że może je zrealizować większy krąg podmiotów. Taki tok rozumowania sprowadziłby zamówienia publiczne do roli instrumentu pozyskiwania dóbr o przeciętnej, niczym niewyróżniającej się jakości, a nadto o cechach nieuwzględniających usprawiedliwionych potrzeb zamawiających (z uzasadnienia wyroku z 25 marca 2019 r. sygn. akt KIO 405/19).

Fakt posiadania czy też dostępności przez danego wykonawcę danego produktu nie stanowi o tym, że dany Zamawiający ma nabyć ten produkt tylko dlatego, że wykonawca go posiada i chce mu go sprzedać. Zamawiający ma prawo opisać swoje potrzeby, żądając produktu o cechach odpowiadających jego potrzebom, a w tym o najwyższych dostępnych standardach jakościowych, w oparciu o opinie użytkowników produktów, jednocześnie dokonując tego z uwzględnieniem racjonalnego planowania dokonywanych wydatków zarówno pod względem finansowym jak i użytkowym

Postępowanie o udzielenie zamówienia publicznego nie stanowi postępowania, w którym Zamawiający ma kupić cokolwiek, co wykonawcy zechcą mu sprzedać. W postępowaniu o udzielnie zamówienia publicznego, Zamawiający jak każdy gospodarz dbający o swoje potrzeby uprawniony jest do kupna określonych rzeczy, a w ramach tych określonych rzeczy nieuprawniona jest taka specyfikacja techniczna, która eliminowałaby w sposób niezasadny określone przedmioty, a przez to ich producentów czy dystrybutorów – to stanowi istotę konkurencyjności w ramach danego zamówienia. Podkreślić należy, że konkurencja nie polega na tym, że Zamawiający ma dopuścić możliwość złożenia oferty na cokolwiek, lecz ma prawo określić swoje potrzeby. Opis przedmiotu zamówiona powinien umożliwiać wykonawcom jednakowy dostęp do zamówienia i nie może powodować nieuzasadnionych przeszkód w otwarciu zamówień publicznych na konkurencję, co nie oznacza, że zasada konkurencji ma prowadzić do sytuacji, w której o zamówienie muszą

móc ubiegać się wszyscy wykonawcy, którzy oferują rzeczy zbliżone, podobne do tych wymaganych przez Zamawiającego (z uzasadnienia wyroku z 18 marca 2019 r. sygn. akt KIO 358/19).

Zamawiający uprawniony jest do opisania przedmiotu zamówienia w sposób, który poprzez zawężenie ilości rodzajów spełniających jego potrzeby produktów automatycznie uniemożliwia złożenie oferty pewnemu kręgowi zainteresowanych przedmiotowym zamówieniem wykonawców. Dopóki jednak Zamawiający nie działa w celu ograniczenia dostępu wykonawców do przedmiotu zamówienia, tylko w celu zaspokojenia swoich uzasadnionych potrzeb, jest to działanie dopuszczalne i zgodne z prawem (z uzasadnienia wyroku z 4 grudnia 2017 r. sygn. akt KIO 2428/17).

Nie jest tak, że Zamawiający jest zobowiązany opisać przedmiot zamówienia w taki sposób, aby wszyscy producenci i dostawcy na rynku mogli złożyć ofertę. W pierwszej kolejności Zamawiający winien wskazać swoje potrzeby i wymagania, nawet jeśli przy takim opisie zamówienia nie wszyscy wykonawcy na rynku mogą złożyć ofertę. Jeśli potrzeby Zamawiającego uzasadnione są szczególną sytuacją lub szczególnymi względami, wówczas nie można uznać, aby Zamawiający działał w sposób ograniczający konkurencyjność i naruszył art. 29 ust. 2 i 7 ust. 1 ustawy Prawo zamówień publicznych (z uzasadnienia wyroku z 18 października 2018 r. sygn. akt KIO 2031/18).

W kontekście takiego rozumienia art. 29 ust. 2 pzp oraz poczynionych powyżej w odniesieniu do rozpoznawanych zarzutów ustaleń należy uznać za bez znaczenia dla sprawy argumentację Odwołującego opartą na odwoływaniu się do raportów z badań rynku IT czy zestawień porównawczych produktów różnych producentów z tej branży, co zostało szczególnie zaakcentowane w piśmie procesowym z 17 grudnia 2019 r. Nie sposób dokonywać ustaleń odnośnie naruszenia przez konkretne i szczegółowe wymagania, których dotyczyły rozpoznawane zarzuty, zakazu dokonywania opisu przedmiotu zamówienia z naruszeniem uczciwej konkurencji wyłącznie na podstawie ogólnej oceny sytuacji rynkowej w zakresie różnych segmentów rynku IT, nawet jeżeli została ona wyrażona przez podmiot cieszący się określoną renomą w zakresie badania tendencji na rynku IT.

{zarzut naruszenia art. 30 ust. 4 pzp}

Zgodnie z art. 30 ust. 4 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”.

Izba stwierdziła, że odwołanie nie zawiera żadnych okoliczności dotyczących naruszenia powyższej normy, stąd zarzut sprowadzający się do wskazania jednostki redakcyjnej ustawy pzp, należy uznać za oczywiście bezzasadny.

Z tych względów Izba – działając na podstawie art. 192 ust. 1 i 2 ustawy pzp – orzekła, jak w pkt 2. sentencji.

O kosztach postępowania odwoławczego orzeczono w pkt 3. sentencji stosownie do jego wyniku na podstawie art. 192 ust. 9 i 10 ustawy pzp w zw. z § 3 pkt 2 i § 5 ust. 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) – obciążając Odwołującego kosztami tego postępowania, na które złożył się uiszczony przez niego wpis oraz uzasadnione koszty Zamawiającego w postaci wynagrodzenia pełnomocnika, których poniesienie zostało udokumentowane do zamknięcia rozprawy stosownym rachunkiem.