Warszawa, 17 lipca 2018 r.

ODPOWIEDZI NA PYTANIA DO TREŚCI SIWZ

Dotyczy: postępowania o udzielenie zamówienia publicznego (Nr 31/18/PN) na dostawę i wdrożenie Systemu do zarządzania i rejestracji sesji kont uprzywilejowanych dla Narodowego Centrum Badań i Rozwoju.

Zamawiający, Narodowe Centrum Badań i Rozwoju, uprzejmie informuje, iż w dniu 13.07.2018r. do Zamawiającego wpłynęły drogą elektroniczną wnioski o wyjaśnienie treści specyfikacji istotnych warunków zamówienia (dalej SIWZ) zamieszczonej na stronie internetowej NCBR. Poniżej przedstawiam ich treść wraz z wyjaśnieniami udzielonymi przez Zamawiającego.

Pytanie 1

W szczegółowym opisie przedmiotu zamówienia, zwanym dalej SOPZ, zawartym w załączniku nr 1 do SIWZ, Zamawiający żąda w punkcie 3.12. aby rozwiązanie oferowało "funkcjonalność monitorowania i rejestrowania użycia kont uprzywilejowanych oraz dogłębną analizę wykorzystania uprawnień". W związku z tym, że zwrot "dogłębną analizę wykorzystania uprawnień" można rozumieć na wiele sposobów, proszę o dokładny opis minimalnej funkcjonalności Systemu, przez którą Zamawiający rozumie taką dogłębną analizę.

Odpowiedź

Zamawiający informuje, że jako "dogłębną analizę wykorzystania uprawnień" należy rozumieć: logowanie wykorzystania uprawnień do połączenia do systemu docelowego (w tym również szczegółowe informacje o wykorzystaniu kont współdzielonych przez poszczególnych administratorów), wykrywanie anomalii wykorzystania uprawnień (np. dostęp w nietypowych godzinach, dostęp z nietypowych adresów IP, nadmierna (większa niż standardowo) aktywność wykorzystania kont przez danego administratora), wykrywanie bezpośredniego dostępu (z pominięciem systemu ochrony) do systemu docelowego.

Pytanie 2

W punkcie 3.14 SOPZ Zamawiający żąda, aby rozwiązanie w ramach rejestracji sesji w których pośredniczy, musiało zapewniać m.in. "możliwość wyszukiwania kontekstowego wśród nagranych sesji". Prosimy o wyjaśnienie czy Zamawiający oczekuje wyszukiwania

pełnotekstowego we wszystkich pojawiających się w zarejestrowanej sesji w obszarze wyświetlania tekstach zaakceptuje rozwiązanie, które umożliwia wyszukiwanie tylko w danych tekstowych przesyłanych w ramach protokołu sesji?

Odpowiedź

Zamawiający wymaga dostarczania rozwiązania umożliwiającego konfiguracyjne określenie sposobu wyszukiwania danych w poszczególnych sesjach w zależności od typu protokołu. Kontekstowość należy rozumieć tu jako możliwość wyszukiwania np. Okien systemu Windows uruchomionych w obrębie sesji RDP.

Pytanie 3

W punkcie 4.1.3 SOPZ Zamawiający żąda, aby opisywany System wspierał "obsługę minimum 500 systemów docelowych i wszystkich przypisanych im kont uprzywilejowanych". Prosimy o odpowiedź na pytanie czy przez system Zamawiający rozumie serwer z unikatowym adresem IP czy serwer z unikatowym adresem IP i obsługiwanym protokołem? Pytanie dotyczy serwerów, do których można połączyć się kilkoma protokołami – czy Zamawiający traktuje to jako jeden system czy jako tyle systemów, iloma protokołami (rodzajami sesji) można się do serwera podłączyć?

Odpowiedź

Zamawiający jako jeden system rozumie jeden system operacyjny (identyfikowany poprzez adres IP lub FQDN), niezależnie od ilości obsługiwanych protokołów, które mogą być wykorzystane do połączenia.

Pytanie 4

W celu sporządzenia prawidłowej oferty, prosimy o podanie dla ilu spośród wskazanych powyżej 500 serwerów, zamawiający oczekuje obsługi więcej niż jednego typu protokołu (rodzaju sesji)?

Odpowiedź

Zamawiający wymaga obsługi więcej niż jednego typu protokołu dla każdego z 500 wskazanych systemów docelowych.

Pytanie 5

W punkcie 4.1.4 SOPZ Zamawiający wskazuje, że "System musi zapewniać wsparcie (możliwość zarządzania kontami uprzywilejowanymi wykorzystywanymi w obrębie systemu docelowego) w formie "out of box" dla systemów docelowych takich jak: Cisco, Microsoft Windows, Microsoft SQL, Linux/Unix, Oracle, MySQL, VMWare". Prosimy o wskazanie

a) jakich typów urządzeń i/lub protokołów dotyczy wyżej cytowany zapis w zakresie wsparcia dla systemów Cisco?

odp: Zamawiający wymaga wsparcia dla urządzeń typu przełącznik, router, firewall oraz protokołów ssh, telnet, tacacs, http/https

b) czy wyżej opisane wsparcie dla systemów Microsoft Windows, Microsoft SQL i VMware dotyczy kont zdefiniowanych w domenie AD czy także kont lokalnych na serwerach Windows Server, MS SQL Server i vSphere?

odp: wymagane jest również wsparcie dla kont lokalnych.

c) jaka jest minimalna wersja systemów Oracle, dla którego wsparcia oczekuje Zamawiający?

Odpowiedź

Zamawiający informuje, że wymagane jest wsparcie dla minimalnej wersji systemu Oracle 8i.

Pytanie 6

W punkcie 4.1.5. Zamawiający wskazuje, że System musi umożliwiać weryfikację "spójności haseł poprzez symulację działań użytkownika w sesji aplikacji Web". W celu złożenia prawidłowej oferty, prosimy o szczegółowy opis w jaki sposób System ma raportować spójność haseł w ww. przypadku i czy ta funkcja ma być integralnym elementem funkcjonalności Systemu czy może być realizowana przez zewnętrzne skrypty, przygotowane w ramach wdrożenia?

Odpowiedź

Zamawiający informuje, że wymagane jest aby System był w stanie symulować działania użytkownika (np. zalogowanie do aplikacji Web) i na podstawie poprawności odpowiedzi aplikacji określał czy hasło jest spójne (w Systemie i wspomnianej aplikacji Web). Funkcjonalność ta powinna być integralną częścią Systemu.

Pytanie 7

W punkcie 4.1.6 SOPZ Zamawiający oczekuje, że System umożliwi "zarządzanie i ochronę oraz eliminację poświadczeń uprzywilejowanych zaszytych w aplikacjach - dla minimum 3ch aplikacji". Prosimy o dokładny opis funkcjonalności, której oczekuje Zamawiający, gdyż powyższy opis można rozumieć na wiele sposobów.

Odpowiedź

Zamawiający informuje, że wymagane jest aby System był w stanie dostarczać poświadczenia na żądanie aplikacji (po uprzednim uwierzytelnieniu aplikacji i pozyskaniu z centralnego repozytorium aktualnego hasła) umożliwiające uwierzytelnienie aplikacji np. w systemie bazodanowym, zgodnie m.in. z punktami 11.6 - 11.8 SOPZ

Pytanie 8

W punkcie 4.1.8 SOPZ Zamawiający określa, że "System musi obsługiwać monitorowanie i ochronę nawet kilkudziesięciu jednoczesnych połączeń od jednego użytkownika końcowego, do różnych systemów poprzez różne lub jedno konto uprzywilejowane (...)". Ponieważ stwierdzenie "nawet kilkudziesięciu" jest stwierdzeniem "miękkim" (można rozumieć zarówno jako 20 jak i 90) i nie określa w sposób jasny konkretnej liczby jednoczesnych połączeń, jakiej obsługi oczekuje Zamawiający, prosimy o określenie minimalnej liczby jednoczesnych połączeń wywoływanych w sposób opisany w tym punkcie.

Odpowiedź

Jeden użytkownik końcowy będzie mógł realizować zarówno 20 jak i 90 sesji równolegle w zależności od specyfiki pracy poszczególnego użytkownika końcowego, dlatego zgodnie z punktem 5.5 SOPZ Zamawiający wymaga aby „Rozwiązanie nie może licencyjnie ograniczać ilości modułów odpowiedzialnych za izolację monitoring oraz rejestrację sesji a także interfejsów Web, którymi użytkownik może podłączyć się do systemu ochrony kont uprzywilejowanych (dodanie kolejnych modułów nie może wymagać zakupu dodatkowych licencji producenta systemu ochrony kont uprzywilejowanych).”

Pytanie 9

W punkcie 4.1.9 Zamawiający wskazuje, że "System musi umożliwiać transparentne połączenie do systemu docelowego, bez konieczności podawania przez użytkownika hasła konta uprzywilejowanego na żadnym z etapów połączenia dla systemów Windows, Unix, Linux". Ponieważ opis ten nie jest precyzyjny, prosimy o rozwinięcie go i opisanie jakiej konkretnie funkcjonalności Systemu Zamawiający oczekuje w stosunku do systemów Windows, Unix i Linux. W szczególności, w naszej ocenie proces łączenia wymaga przynajmniej autoryzacji i autentykacji, zatem prosimy o opis jak, wg Zamawiającego, ma być realizowany wymóg połączenia do systemu docelowego bez konieczności podawania użytkownika konta na żadnym z etapów połączenia.

Odpowiedź

Uwierzytelnianie użytkownika musi być realizowane na poziomie Systemu. Po uwierzytelnieniu użytkownika w Systemie, System musi umożliwiać transparentne połączenie do systemu docelowego, bez konieczności podawania przez użytkownika hasła konta uprzywilejowanego do systemu docelowego na żadnym z etapów połączenia dla dowolnych systemów docelowych

Pytanie 10

W SOPZ, w punkcie 5.4. Zamawiający wymaga, aby proponowane rozwiązanie musiało "uwzględniać nie mniej niż: (...) 2x system Disaster Recovery". Prosimy o odpowiedź na pytanie czy zatem Zamawiający oczekuje dostarczenia licencji dla systemów DR umożliwiających ich uruchomienie niezależnie od systemu HA?

Odpowiedź

Zamawiający wymaga dostarczenia systemu złożonego z HA oraz dwóch instancji DR.

Pytanie 11

W punkcie 5.16 SOPZ Zamawiający określa, że "System nie może wymuszać zmiany topologii sieciowej w celu zapewnienia możliwości nagrywania wszystkich sesji uprzywilejowanych." Prosimy o szczegółowe określenie w jaki sposób Zamawiający zamierza usadowić System bez zmiany topologii sieciowej? Jest to potrzebne do sporządzenia projektu i kosztorysu wdrożenia na podstawie wymagań i informacji od Zamawiającego, a zatem stanowi to istotny element umożliwiający złożenie prawidłowej oferty.

Odpowiedź

System musi umożliwiać przekierowanie sesji na poziomie warstwy 3 modelu OSI/ISO. System musi umożliwiać wdrożenie wielu instancji modułów izolująco-nagrywających w celu zapewnienia mikrosegmentacji środowiska sieciowego.

Pytanie 12

W SOPZ, w punkcie 7.1 Zamawiający wymaga by System musiał umożliwić "integrację z systemami SIEM". Prosimy o informację z jakim konkretnie systemem lub systemami SIEM Zamawiający oczekuje integracji – prosimy o wymienienie konkretnej listy takich systemów stanowiących minimalne wymaganie Zamawiającego – i wyjaśnienie co Zamawiający rozumie konkretnie przez integrację z takim rodzajem systemu informatycznego?

Odpowiedź

System musi umożliwiać integrację z systemami SIEM, nie mniej niż: McAfee, IBM, HP, Splunk, RSA. System musi umożliwiać integrację z systemami SIEM w celu wysyłania informacji o zarejestrowanych zdarzeniach w ramach monitorowanych sesji. Musi istnieć możliwość zdefiniowania typu zdarzeń które powinny być wysłane do systemu SIEM. System musi umożliwiać pobieranie danych o aktywności użytkowników z zewnętrznych systemów SIEM. Musi istnieć możliwość zwrotnego przekazywania informacji do systemów typu SIEM o anomaliach wykorzystania kont uprzywilejowanych, wykrytych za pomocą adaptacyjnych algorytmów zachowań użytkowników.

Pytanie 13

W SOPZ, w punkcie 7.2 Zamawiający wymaga by System musiał umożliwić "integrację z systemami ticketowymi". Prosimy o informację z jakim konkretnie systemem lub systemami ticketowymi Zamawiający oczekuje integracji – prosimy o wymienienie konkretnej listy takich systemów stanowiących minimalne wymaganie Zamawiającego – i wyjaśnienie co Zamawiający rozumie konkretnie przez integrację z takim rodzajem systemu informatycznego?

Odpowiedź

System musi umożliwiać integrację z biletowymi systemami zgłoszeń takimi jak: ManageEngine ServiceDesk Plus, BMC Remedy, HP ServiceCenter, ServiceNow oraz innym poprzez otwarte API. System musi umożliwiać weryfikację czy poprawne zgłoszenie istnieje w systemie biletowym i czy posiada odpowiedni status uprawniający do otrzymania poświadczeń uprzywilejowanych. System musi zapewniać w ramach integracji z systemem biletowym zarówno akceptację dostępu do kont uprzywilejowanych jak i wykonywanie zmian.

Pytanie 14

W punkcie 7.5 Zamawiający wskazuje, że "Produkt musi umożliwiać integrację z rozwiązaniami typu vulnerability management Tenable Nessus posiadanego przez Zamawiającego (w celu ochrony kont wykorzystywanych do skanowania podatności)". Prosimy o konkretny opis oczekiwanej przez Zamawiającego minimalnej funkcjonalności takiej integracji – od strony Systemu i od strony Tenable Nessus.

Odpowiedź

System musi umożliwiać przekazywanie odpowiednich poświadczeń niezbędnych dla rozwiązania typu vulnerability management na potrzeby realizacji skanowania podatności, tym samym wyeliminowana zostanie konieczność składowania tych poświadczeń bezpośrednio w konfiguracji skanera. System musi pozwalać na automatyczne zarządzanie hasłami do kont wykorzystywanych przez skaner podatności

Pytanie 15

W punkcie 9.2 SOPZ Zamawiający oczekuje, że "System musi zmieniać wartość hasła na systemie docelowym zgodnie z ustawioną polityką (np. co x dni, x miesięcy, x lat)". Czy funkcja ta dotyczy wszystkich rodzajów obsługiwanych systemów informatycznych, w szczególności tych wymienionych w punkcie 4.1.2 SOPZ, czy tylko ich części? Jeżeli tylko części, prosimy o uściślenie dla jakich typów systemów informatycznych Zamawiający oczekuje spełniania wymogu opisanego w punkcie 9.2 SOPZ.

Odpowiedź

System musi zmieniać wartość hasła na systemie docelowym zgodnie z ustawioną polityką we wszystkich systemach docelowych, również tych wymienionych w punkcie 4.1.2. SOPZ System musi również umożliwiać budowanie szczegółowej polityki rotacji haseł, np. indywidualna polityka dla pojedynczego systemu docelowego.

Pytanie 16

W punkcie 9.6 SOPZ Zamawiający opisie wymóg dla Systemu, który "musi automatycznie porównywać hasło przechowywane w produkcie oraz hasło przechowywane na systemie docelowym." Czy ten wymóg dotyczy wszystkich kont znajdujących się w systemie czy tylko ich części? Jeżeli tylko części – prosimy o określenie konkretnie jakich typów kont ten wymóg dotyczy.

Odpowiedź

Zamawiający informuje, że wymóg ten dotyczy wszystkich kont i systemów docelowych. Minimalne wymagania wskazano w punkcie 4.1.1 SOPZ.

Pytanie 17

W SOPZ, w punkcie 10.1 Zamawiający wskazuje, że "System musi umożliwiać nagrywanie sesji uprzywilejowanych w systemach: (...) dostępu aplikacji web przez przeglądarki internetowe,". Czy wymóg ten zakłada zapisywanie wszystkich elementów sesji dostępu do aplikacji przez przeglądarki internetowej, w tym elementów graficznych i wyrenderowanych stron ukazujących się w przeglądarce?

Odpowiedź

System musi umożliwiać nagrywanie dostępu aplikacji web przez przeglądarki internetowe.

Pytanie 18

W punkcie 10.5 SOPZ, Zamawiający informuje, że "System musi wykorzystywać mechanizmy indeksowania nagrań umożliwiające szybkie przeszukiwanie nagranych i monitorowanych sesji pod kątem występowania wskazanych słów kluczowych". Czy wymóg ten dotyczy wszystkich typów sesji, tj. graficznych, bazodanowych i tekstowych, i pełnej ich zawartości, np. treści pojawiających się w otwieranych oknach?

Odpowiedź

Zamawiający informuje, że wymóg ten dotyczy wszystkich typów sesji.

Pytanie 19

Zamawiający w OPZ użył parametrów wskazujących na rozwiązanie tylko jednego producenta. Działaniem takim naruszył przepisy ustawy Prawo zamówień publicznych:

1) art. 7 ust. 1 ustawy Pzp poprzez prowadzenie postępowania w sposób naruszający zasady uczciwej konkurencji i równego traktowania wykonawców ubiegających się o udzielenie zamówienia;

2) art. 29 ust. 2 poprzez opisanie przedmiotu zamówienia w sposób, który utrudniający uczciwą konkurencję;

3) art. 29 ust 3. Poprzez opis, który charakteryzuje produkty przez konkretnego wykonawcę, a wskazaniu takiemu nie towarzyszą rozwiązanie równoważne;

4) art. 7 ust. 1 w związku z art. 91 ust. 2 Pzp poprzez określenie niektórych kryteriów oceny ofert w sposób, który utrudnia uczciwą konkurencję oraz nie zapewnia równego traktowania wykonawców, faworyzuje sprzęt tylko jednego producenta.

Zasada równego traktowania Wykonawców zabrania zamawiającemu preferowania lub dyskryminacji któregokolwiek z Wykonawców, gwarantuje wykonawcom równe szanse w dostępie uzyskania zamówienia. Zasada równego traktowania wykonawców i uczciwej konkurencji to fundament prawa zamówień publicznych. Zobowiązuje to Zamawiającego do traktowania wszystkich Wykonawców ubiegających się o zamówienie w sposób jednakowy.

Uchwała KIO z 19.05.2016 r. (KIO/KD 34/16, LEX nr 2110662), w której Izba stwierdziła, co następuje: Naruszenie zasady uczciwej konkurencji może nastąpić nie tylko bezpośrednio poprzez wskazanie konkretnego produktu lub wykonawcy, ale także przez takie dokonanie opisu, które umożliwia dostęp do zamówienia jednemu lub kilku wykonawcom, jednocześnie uniemożliwiając go w sposób nieuzasadniony innym, którzy również byliby w stanie wykonać dane zamówienie. Przy czym może zdarzyć się tak, że przy braku możliwości składania ofert częściowych opis nawet jednego z wielu zamawianych produktów może spowodować niemożliwość złożenia niepodlegającej odrzuceniu oferty - zgodnej ze wszystkimi wymaganiami specyfikacji istotnych warunków zamówienia".

Zamawiający w OPZ żąda, aby całość rozwiązania powinna od jednego producenta (Załącznik nr 1 -szczegółowy opis przedmiotu zamówienia, ust. 3 pkt. 3.1, zwany dalej SOPZ), jednocześnie zaznaczając w ogłoszeniu, że nie jest możliwe składanie ofert częściowych.

Przedmiotem zamówienia jest, zgodnie z opisem Zamawiającego, system łączący funkcje systemu PIM (Privileged Identity Manager), systemu PAM (Privileged Access Manager), AIM (Application Identity Manager - SOPZ ust. 11 pkt. 11.7) i modułu ochrony kontrolera domeny (wymaganie dodatkowo punktowane opisane w SOPZ ust. 12 pkt. 12.2). Należy zaznaczyć, funkcjonalności systemu PIM i PAM są rozłączne, tj. istnieją na rynku dedykowane rozwiązania pełniące funkcje wyłącznie funkcję PIM jak i takie, które zapewniają funkcjonalność PAM. Zmawiający pośrednio potwierdza to określając we wzorze umowy (Załącznik nr 7) jej przedmiot jako „systemu do zarządzania i rejestracji kont uprzywilejowanych klasy

PIM/PAM", a więc wskazując dwie różne zakresy funkcjonalności - PIM i PAM, które w nomenklaturze informatycznej są rozłączne, dlatego określane są różnymi określeniami.

Dodatkowo, Zamawiający ukrył w SOPZ dostawę elementu chroniącego systemów informatycznych wprowadzając do SOPZ wysoko punktowaną funkcję ochrony kontrolerów domeny przed atakami i działaniami nieuprawnionymi, która to funkcjonalność nie leży w zakresie systemów PIM ani PAM, a jest częścią jednego konkretnego rozwiązania informatycznego, którego funkcjonalność obejmuje takie funkcje z zakresu bezpieczeństwa informatycznego. Oczywiście, istnieje też wiele dedykowanych rozwiązań z działki bezpieczeństwa IT, zapewniające kompleksową ochronę systemów klasy kontroler domenowy przed atakami opisanymi przez Zamawiającego w SOPZ ust. 12 pkt. 12.2.1 jak i innymi, niewymienionymi w SOPZ.

Zamawiający wymusza też wprowadzenie rozwiązania jednego producenta podając, że całość rozwiązania powinna pochodzić od jednego producenta (SOPZ ust. 3 pkt. 3.1) i jednocześnie wskazując wymóg dostawy jednolitego oprogramowania łączącego funkcjonalność PIM i funkcjonalność PAM (SOPZ ust. 3 pkt. 3.9) i dodatkowo posiadającego jednolity panel zarządzania (SOPZ ust. 3 pkt. 3.10).

Mimo, że istnieje wiele systemów na rynku, które pełnią funkcję PIM, PAM, AIM i wysoko punktowanego (aż 25 punktów), w tym rozwiązania bezpieczeństwa informatycznego, produkowane w Polsce i na terenie Unii Europejskiej, ale tylko jedno rozwiązanie na rynku spełnia wszystkie wymogi Zamawiającego i jest jednolite, zarządzane przez jeden wspólny panel administracyjny - chodzi o amerykański system Cyber Ark.

Co więcej, bezpośrednie wskazanie systemu CyberArk wskazują użyte przez Zamawiającego zwroty i opisane funkcje, które są charakterystyczne dla systemu CyberArk i realizowane tylko przez niego, co nie jest niczym uzasadnione:

- opisany funkcjonalnie moduł składowania kont uprzywilejowanych w formie rozproszonej (SOPZ ust. 5 pkt. 5.8),

- integracja z systemem Tennable Nessus (SOPZ ust. 7 pkt. 7.5),

- generowanie raportów w formacie Microsoft Excel (SOPZ, ust. 8 pkt. 8.5.1) - oprócz uniwersalnego i powszechnie stosowanego formatu CSV,

- integracja z systemami HSM,

- posiadanie SDK dla wszystkich wskazanych w SOPZ ust. 11 pkt. 11.3 platform deweloperskich.

Czytając opis przedmiotu zamówienia, trudno odnieść inne wrażenie niż to, że opisana funkcjonalność jest okrojoną wersją opisu funkcjonalności wszystkich modułów systemu CyberArk znajdującą się na stronach:

hllps://www.cyberark.com/producls/privileged-accounl-security-sohilion/

https://www.cyberark.com/products/privileged-accounl-security-solution/app/ication-idenrity-manager/ https://Ip.C)'berark.com/rs/3J6-CZP-275/images/ds-CyberArk-Privileged-Access-Security-04-30-2018.pdf

W praktyce, jedynie system CyberArk spełnia wszystkie zapisy SOPZ wymagane przez Zamawiającego. Zgodnie z art. 29 ust. 2 Pzp Przedmiotu zamówienia nie można opisywać w sposób, który mógłby utrudniać uczciwą konkurencję. A zatem opis musi umożliwiać Wykonawcom jednakowy dostęp do zamówienia i nie może powodować nieuzasadnionych przeszkód w ubieganiu się o udzielenie zamówienia. W przedmiotowym postępowaniu mamy naruszenie zasady uczciwej konkurencji określonej w art. 29 ust. 2 ponieważ Zamawiający opisał przedmiot zamówienia przez zbytnie dookreślenie parametrów co spowodowało wskazanie konkretnego produktu a jest to bez uzasadnienia i bez możliwości zintegrowanych rozwiązań równoważnych.

Po stronie wykonawcy wystarczy jedynie uprawdopodobnienie, że opis przedmiotu zamówienia mógłby utrudniać uczciwą konkurencję (zob. wyroki KIO: z 24.04.2009 r., KIO/UZP 466/09, KIO/UZP 486/09,

LEX nr 497522; z 26.08.2011 r., KIO 1734/11, LEX nr 960445). Zaistnienie co najmniej możliwości utrudniania uczciwej konkurencji przez zastosowanie określonych zapisów w opisie przedmiotu zamówienia jest wystarczające do uznania, że przepisy art. 29 ust. 2 oraz w art. 7 ust. 1 zostały naruszone (zob. wyrok KIO z 26.04.2011 r., KIO 752/11, LEX nr 795170). Działaniem wbrew zasadzie uczciwej konkurencji jest na tyle rygorystyczne określenie wymagań, jakie powinien spełnić przedmiot zamówienia, że nie jest to uzasadnione obiektywnymi potrzebami zamawiającego, a jednocześnie ogranicza krąg potencjalnych wykonawców zdolnych do wykonania zamówienia (por. wyrok KIO z 14.12.2010 r., KIO/UZP 2608/10, LEX nr 707606). W wyroku z 23.01.2015 r., KIO 43/15, LEX nr 1651710, Krajowa Izba Odwoławcza zwróciła uwagę, że „choć przyjmuje się w orzecznictwie, że w odniesieniu do naruszenia art. 29 ust. 2 Pzp. wystarczające jest wykazanie możliwości ograniczenia konkurencji, nie zwalnia to z obowiązku udowodnienia, że taka sytuacja zachodzi w konkretnej sprawie.

W związku z powyższym zwracamy się z prośba o zmianę opisu przedmiotu zamówienie w sposób zgodny z Pzp oraz gwarantujący dostęp do zamówienia Wykonawcom.

Dodatkowo, wnosimy o podzielenie zamówienia na części co umożliwi dostawę systemu PIM, systemu PAM i systemu AIM.

Zgodnie z treścią znowelizowanego art. 96 ust. 1 pkt 11 p.z.p., który to przepis stanowi transpozycję do polskiego porządku prawnego normy zawartej w art. 46 ust. 1 dyrektywy klasycznej, w przypadku braku podziału zamówienia na części, zamawiający w sporządzonym protokole wskazuje powody niedokonania podziału zamówienia na części. Zamawiający, uzasadniając przyczyny braku podziału zamówienia na części, nie może powoływać się

wyłącznie na korzyści organizacyjne, wynikające z prowadzenia jednego, a nie większej liczby postępowań o udzielenie zamówienia publicznego czy też trudności w nadzorowaniu lub koordynacji kilku wykonawców. Odwołując się do motywów zawartych w preambule do dyrektywy klasycznej, jako przykładowe przyczyny rezygnacji z podziału zamówienia na części można wskazać: ograniczenie konkurencji albo nadmierne trudności techniczne lub nadmierne koszty wykonania zamówienia, lub też znaczące ryzyko zagrożenia wykonania zamówienia wynikające z potrzeby skoordynowania działań różnych wykonawców realizujących poszczególne części zamówienia. Należy zauważyć, że ustawodawca europejski za okoliczność uzasadniającą rezygnację z podziału na części uznał jedynie realne i uzasadnione obawy, a nie ewentualne niewielkie trudności czy koszty wynikające z koordynowania działań wykonawców. Decyzja, co do podziału zamówienia, w tym na określoną ilość części i kryterium przedmiotowe, należy do zamawiającego, który podejmuje ją w zależności od swoich potrzeb, a głównym ograniczeniem dyskrecjonalności zmawiającego jest zasada zachowania uczciwej konkurencji. Prawidłowość postępowania zamawiającego, który nie dokonał podziału lub dokonał podziału zamówienia nie na tyle części, na ile jest to potencjalnie możliwe, oceniana musi być każdorazowo przy uwzględnieniu całokształtu okoliczności sprawy, z uwzględnieniem szczególnych, uzasadnionych złożonością projektu okoliczności danego przypadku.

W naszej ocenie, wynikającej z doświadczenia w instalacji i integracji systemów PIM, PAM i AIM, nie zachodzą tu żaden wskazane przyczyny rezygnacji z podziału zamówienia na części, gdyż większość systemów obecnie współpracuje ze sobą w taki sposób, aby zapewnić bezproblemowe realizowanie funkcjonalności PIM, funkcjonalności PAM i funkcjonalności. Integracja taka może opierać się na wielu płaszczyznach, od integracji z systemem Active Directory po integrację z tzw. password vault systemu PIM. Co więcej, już sama forma opisu przedmiotu zamówienia wskazuje na to. że Zamawiający zdaje sobie sprawę z tego, że zamierza wdrożyć system PIM. system PAM i system AIM. każdy o konretnei. unikatowej funkcjonalności, umieszczając wymagania dot. zarządzania kontami uprzywilejowanymi (a więc funkcjonalność PIM) w ust. 9 SOPZ oraz zarządzanie poświadczeniami aplikacji (funkcjonalność AIM) w ust. 11 SOPZ w osobnych punktach. Co więcej, nagrywanie sesji uprzywilejowanych (a więc funkcjonalność PAM) w ust. 10 SOPZ została także wydzielona do osobnego ustępu SOPZ.

W związku z powyższym zwracamy się o podzielenie zamówienia na 4 części tj.

1. *Część dotyczącą funkcjonalności Privileged Identity Management (PIM),*
2. *Część dotyczącą funkcjonalności Privileged Access Management (PAM) z modułem nagrywaia sesji,*
3. *Część dotyczącą funkcjonalności Application Identity Management (AIM),*
4. *Część dotyczącą ochrony kontrolerów domenowych. Dzięki powyższemu zostanie zwiększona konkurencyjność.*

W obecnym stanie prawnym w Pzp Zamawiający, który podejmuje decyzję o udzieleniu zamówienia w całości, musi wskazać w uzasadnieniu, że ani podział ilościowy, ani jakościowy

nie przyczyni się do zwiększenia udziału małych i średnich przedsiębiorstw (MŚP) w rynku przedmiotu danego zamówienia. Jednym z głównych celów tychże regulacji unijnych implementowanych do naszego prawa było zapewnienie lepszego dostępu do rynku małym i średnim przedsiębiorcom, dzięki ułatwieniu udzielania zamówień w częściach.

Zgodnie z Wyrokiem KIO 920/17 z dnia 23 maja 2017 r.

Kwestię dotyczącą możliwości podziału zamówienia na części, ustawodawca pozostawił do wyłącznej dyspozycji zamawiającego (art. 36aa ust. 1 Pzp). Jednakże decyzja ta, mająca istotne znaczenie dla biegu postępowania o udzielenie zamówienia publicznego, w tym w szczególności na umożliwienie udziału w postępowaniu szerszemu gronu podmiotów, specjalizujących się w danym przedmiocie zamówienia, nie może pozostawać o tyle subiektywna, o ile zamawiający bez głębszej refleksji nie uwzględni faktycznych okoliczności uniemożliwiających mu podzielenie zamówienia na części. Zamawiający podejmując decyzję o przeprowadzeniu postępowania o udzielenie zamówienia publicznego, ma bowiem obowiązek zbadać, czy przedmiot zamówienia jest podzielny, czy podział zamówienia na części znajduje swoje racjonalne uzasadnienie i czy podział zamówienia przyniesie lub może przynieść wymierne korzyści finansowe. Nie należy również zapominać, iż decyzja zamawiającego musi również uwzględniać sytuację podmiotową wykonawców, tj. zamawiający zobowiązany jest zbadać, czyjego decyzja nie naruszy zasady wyrażonej w przepisie art. 7 ust. 1 Pzp, tj. zasady równego traktowania wykonawców oraz uczciwej konkurencji.

Zgodnie z ugruntowanym orzecznictwem KIO prezentowanym w Wyroku KIO 789/17 z dnia 12 maja 2017 r. Dla zastosowania art. 29 ust. 3 Pzp. nie jest wystarczające wskazanie urządzenia danego producenta z określeniem „lub równoważne", lecz należy dokładnie określić, co zamawiający uznaje za rozwiązanie równoważne. Niezbędne jest zatem wskazanie takich kryteriów równoważności, dzięki którym wykonawca i zamawiający w oparciu o metodę zerojedynkową będą w stanie ocenić, czy dane rozwiązanie spełnia istotne parametry wymagane przez zamawiającego i w konsekwencji stwierdzić, czy nosi przymiot urządzenia równoważnego. Ponadto, uznaje się, że jeżeli zamawiający wprawdzie dopuszcza urządzenia równoważne, niemniej takie, które jest całkowicie zgodne pod względem wszystkich parametrów i funkcjonalności z urządzeniem określonego producenta lub określonego modelu, to mamy do czynienia jedynie z równoważnością iluzoryczną, pozorną - takie zaś rozwiązanie jest na gruncie przepisów Pzp. niedopuszczalne.

Oraz w Uchwale KIO KIO/KD 21/16 z dnia 4 kwietnia 2016 r. W przypadku dopuszczenia wyrobów równoważnych, zamawiający winien sprecyzować, jakie cechy zamawianego produktu mają dla niego walor równoważny, które będą brane pod uwagę przy ocenie. Określenie, iż "oferowany asortyment dostawy będzie o takich samych lub nie gorszych bądź lepszych parametrach technicznych, jakościowych, funkcjonalno-użytkowych i gabarytowych" nie spełnia przesłanek ustawowych pojęcia "równoważności" i daje zamawiającemu nieograniczone i arbitralne pole do oceny tej równoważności.

2. Zamawiający określił kryteria oceny ofert: „dodatkowe funkcjonalności".

Zamawiający za funkcjonalność: System posiada funkcję (i zostać dostarczony z odpowiednimi licencjami) identyfikacji ataków na kontroler domeny dla minimum 4ch kontrolerów - przyznaje 25 pkt (co stanowi 25% możliwych do zdobycia punktów).

Wskazaną ochronę, wraz z wymaganą w SOPZ funkcjonalnością PIM, PAM i AIM i dodatkowo spełniający wymagania Zamawiającego, tj. rozwiązanie pochodzące od jednego producenta (SOPZ ust. 3 pkt. 3.1) ze wskazaniem, że musi być to oprogramowanie jednolite, dodatkowo posiadające jednolity panel zarządzania (SOPZ ust, 3 pkt. 3.10). Wskazuje na to m.in. opis zamieszczony na stronie amerykańskiego producenta systemu CyberArk (pobranie dokumentu wymaga rejestracji):

hUps://www.cyberarkxom/resource/maimain-contwl-biisiness

Podkreślenia wymaga, że cechy, właściwości czy funkcjonalności oferowanego przedmiotu, sposób wykonania zamówienia, które wyrażają się w kryteriach jakościowych, podlegających punktacji, powinny obejmować nic jakiekolwiek cechy, ale walory w pewien sposób, właściwy dla zamawianego przedmiotu, reprezentatywne dla oceny jakościowej, możliwości uznania na ich podstawie, że dany produkt albo sposób realizacji zamówienia jest „lepszy" od innego, bardziej pożądany, czy w wyższym stopniu realizujący cele Zamawiającego.

Kryteria oceny ofert muszą być opisane w SIWZ w taki sposób, by Wykonawca na ich podstawie miał wiedzę, jakie parametry oferowanego sprzętu pozwolą na uzyskanie dodatkowych 25 punktów. I owszem, Wykonawca ma wiedzę, że tylko jeden producent zaoferuje dostawę rozwiązania zawierającego tak wysoko punktowaną funkcjonalność dodatkową.

Pzp zabrania dokonywania opisu przedmiotu zamówienia takiego, który utrudnia uczciwą konkurencję, wskazując na konkretny produkt, oraz takiego, który potencjalnie mógłby wpłynąć na konkurencję na rynku. Odnosi się to również do kryteriów oceny ofert, które musza być z zachowaniem uczciwej konkurencji. Zamawiający nie może tak układać kryteriów, że już na etapie składanie ofert wiadomo, że tylko jeden producent ma możliwość otrzymania 25 pkt co spowoduje wyprzedzenie go przed innym Wykonawcami już na starcie o 25%.

Zgodnie z motywem 90 dyrektywy klasycznej i motywem 95 dyrektywy sektorowej: zamówienia powinny być udzielane na podstawie obiektywnych kryteriów zapewniających przestrzeganie zasad przejrzystości, niedyskryminacji i równego traktowania, z myślą o zagwarantowaniu obiektywnego porównania relatywnej wartości ofert, tak aby ustalić - w warunkach efektywnej konkurencji - która z ofert jest najkorzystniejsza ekonomicznie. Zamawiający opisując w taki, a nie inny sposób przedmiot zamówienia, uniemożliwił zaistnienie efektywnej konkurencji i dyskryminuje podmioty, sztucznie łącząc funkcjonalność PIM, PAM, AIM i bezpieczeństwa informatycznego w jednym opisie.

W związku z powyższym wnosimy o usuniecie wskazanego kryterium ewentualnie zastąpienie go innym niedvskrvminuiaevm i nie wskazującym na konkretny sprzęt konkretnego, jednego producenta.

Kryteria oceny ofert służą zapewnieniu Zamawiającemu do uzyskania najkorzystniejszej oferty a nie do preferowania w sposób nieuczciwy, niezgodny z przepisami konkretnego producenta.

Na marginesie zaznaczamy, że przetargi współfinansowane ze środków Unii Europejskiej podlegają korekcie finansowej za naruszenia Pzp. W związku z powyższym zwracamy się z prośbą o zmiany w opisie przedmiotu zamówienia i zmiany kryteriów oceny ofert tak aby zasady Pzp zostały zachowane i aby konkurencyjność nie była naruszona.

Odpowiedź

Zamawiający informuje, że podtrzymuje zapisy SOPZ. Po przeprowadzeniu analizy rynku Zamawiający stwierdza, że dostępne są co najmniej trzy rozwiązania spełniające podstawowe wymagania zawarte w SOPZ oferowane przez różne podmioty.

Opis został przygotowany pod kątem potrzeb Zamawiającego. Wszystkie wymagania, w tym dodatkowe, są bardzo istotne dla Zamawiającego i wszystkie wpisują się w bezpieczeństwo systemów informatycznych.

Zamawiający nie zgadza się na rozbicie zamówienia na kilka mniejszych: PIM, PAM, AIM i bezpieczeństwa informatycznego. Istotne jest (jeżeli tylko jest to możliwe), posiadać jedno rozwiązanie posiadające wszystkie moduły z wielu względów. Główne to ograniczenie kosztów: zakup, wdrożenie, wsparcie jednego systemu jest tańsze w utrzymaniu (koszty licencji, sprzętu, systemów operacyjnych, itd.). Zarządzanie, jednego systemu jest mniej skomplikowane. Jako instytucja sektora finansów publicznych Zamawiający zobowiązany jest do przestrzegania przepisów ustawy z dnia 27 sierpnia 2007 r. o finansach publicznych, w tym przepisu art. 44 ust. 3 przywołanej ustawy, który stanowi, iż „wydatki publiczne powinny być dokonywane w sposób celowy i oszczędny, z zachowaniem zasad: uzyskiwania najlepszych efektów z danych nakładów, optymalnego doboru metod i środków służących osiągnięciu założonych celów w sposób umożliwiający terminową realizację zadań; w wysokości i terminach wynikających z wcześniej zaciągniętych zobowiązań”. Zamawiający informuje, iż ze względu na posiadane już oprogramowania najważniejsze jest, aby system wyłoniony w trakcie przetargu, ze względów bezpieczeństwa, integrował się z posiadanymi już systemami.

Zatwierdzam

Piotr Zerhau – Dyrektor Działu Systemów Informatycznych