Kraków, 2 października 2024 r.

IT-03-2.271.24.2024

Wykonawcy w postępowaniu

Dotyczy: postępowania o udzielenie zamówienia publicznego pn.: „Zakup specjalistycznej ochrony antywirusowej EDR dla urządzeń końcowych na 36 miesięcy (1000 licencji) - projekt finansowany ze środków UE w ramach Projektu grantowego «Cyberbezpieczny Samorząd» pn.: «Cyberbezpieczny Kraków”.

Zamawiający: Gmina Miejska Kraków – Urząd Miasta Krakowa, z siedzibą w Krakowie, Pl. Wszystkich Świętych 3-4, 31-004 Kraków - działając na podstawie **art. 284 ustawy** z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2024 r. poz. 1320), zwanej dalej „ustawą”, informuje że w przedmiotowym postępowaniu w dniu 29 września 2024 r. wpłynęły pytania od Wykonawcy. Treść pytań w oryginalnym brzmieniu oraz odpowiedzi Zamawiającego znajduje się poniżej.

Pytanie:

„Wnosimy o zmianę zapisów SWZ i doprowadzenie postępowania do zgodności z przepisami ustawy Prawo Zamówień Publicznych jak i umożliwienie Wykonawcy złożenie konkurencyjnej oferty w przedmiotowym postepowaniu. W obecnym stanie faktycznym postępowanie narusza elementarne zasady udzielania zamówień publicznych poprzez opis przedmiotu zamówienia możliwy do spełnienia tylko i wyłącznie przez jedno rozwiązanie. W konsekwencji prowadzi to do uzależnienia wyniku postępowania od producenta jednego systemu lub jego przedstawiciela w Polsce, co jest prawnie niedopuszczalne i odbywa się ze szkodą dla Zamawiającego oraz potencjalnego Wykonawcy.

Podkreślić należy iż parametry same w sobie nie wykluczają konkurencyjności w przedmiotowym zamówieniu, jednakże stanowią dyskryminujący zbieg wymagań, który konkurencję wyklucza. Jak wskazano w rekomendacji prezesa UZP: z dyskryminującym zbiegiem wymagań mamy do czynienia wtedy, gdy opis przedmiotu zamówienia zawiera wymagania, z których każde z osobna nie prowadzi samoistnie do dyskryminacji jakiegokolwiek producenta, lecz ich koniunkcja (wymaganie łącznego spełnienia) sprawia, że tylko jedno dostępne na rynku urządzenie może je spełnić. Promowana w niniejszych rekomendacjach zasada specyfikowania właściwości użytkowych urządzenia komputerowego, a nie szczegółowych parametrów technicznych jego konstrukcji oraz przedstawiona lista zapisów niedopuszczalnych, ogranicza ryzyko powstania dyskryminującego zbiegu wymagań.

Dokonane przez Zamawiającego zawężenie możliwych do zastosowania rozwiązań stanowi naruszenie zasad uczciwej konkurencji i równego traktowania wykonawców. Zgodnie z wyrokiem KIO z 16 maja 2008 r.; sygn. akt: KIO/UZP 423/08: "Opis przedmiotu zamówienia powinien być dokonany w sposób obiektywny i nieutrudniający uczciwej konkurencji, nie może zawierać sformułowań, które powodują uprzywilejowanie określonych wykonawców lub dyskryminowanie innych, uniemożliwiając im złożenie oferty. Naruszeniem zasady uczciwej konkurencji jest opisanie przedmiotu zamówienia z użyciem oznaczeń wskazujących na konkretnego producenta lub konkretny produkt albo z użyciem parametrów wskazujących na konkretnego producenta, dostawcę albo konkretny wyrób." Orzecznictwo Krajowej Izby Odwoławczej wielokrotnie w swych orzeczeniach podkreślało, że Zamawiający musi potrafić każdorazowo wykazać swoje uzasadnione potrzeby, jeśli nie w ramach postanowień SIWZ to w toku weryfikacji np. podczas rozpatrywania wniesionego odwołania. Należy przywołać za orzecznictwem: "Izba wielokrotnie wskazywała w orzecznictwie, (...) na kwestie: "uzasadnionych potrzeb Zamawiającego" (przykładowo wyrok KIO z dnia 5 lipca 2012 r., sygn. akt: KIO 1307/11, tudzież wyrok KIO z dnia 12 lipca 2012 r., sygn. akt: KIO 1360/12), czy też "obiektywnych okoliczności" (za wyrokiem z dnia 8 lipca 2011 r., sygn. akt: 1344/11). Podobnie, w uchwale KIO z dnia 27 września 2012 r., sygn. akt: KIO/KD 80/12.

Dyskryminujące opisanie przedmiotu zamówienia wpływa bezpośrednio na liczbę złożonych w postępowaniu ofert, oraz może skutkować oferowaniem przez wykonawców produktów wyłącznie jednego producenta. W efekcie prowadzi to do powstania zawężonego rynku kreowanego przez

zamawiających, na którym rzeczywistą konkurencję ceną, walorami użytkowymi i jakością zastępuje quasi-konkurencja między dostawcami tej samej technologii lub produktów tego samego producenta.
Prawo wyraźnie wskazuje również, że przedmiot zamówienia nie można opisywać w sposób który mógłby utrudniać uczciwą konkurencję w związku z tym przedmiot zamówienia opisuje się w sposób jednoznaczny i wyczerpujący, za pomocą dostatecznie dokładnych i zrozumiałych określeń, uwzględniając wszystkie wymagania i okoliczności mogące mieć wpływ na sporządzenie oferty (tj. art. 29 ust. 1 PZP). Przedmiot zamówienia nie można opisywać w sposób, który mógłby utrudniać uczciwą konkurencję (tj. art. 29 ust. 2 PZP) oraz przedmiot zamówienia nie można opisywać przez wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę, jeżeli mogłoby to doprowadzić do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, … (tj. art. 29 ust. 3 PZP). Ponadto z licznego orzecznictwa dotyczącego tego zakresu wynika, że do stwierdzenia faktu nieprawidłowości w opisie przedmiotu zamówienia wystarczające jest jedynie zaistnienie możliwości utrudniania uczciwej konkurencji przez zastosowanie określonych zapisów w specyfikacji. Opisane powyżej zasady znajdują swoje odzwierciedlenie w bogatym orzecznictwie Krajowej Izby Odwoławczej.

W związku z powyższym wnosimy o dopuszczenie poniższych parametrów lub dopuszczenie alternatywnego opisu przedmiotu zamówienia dla rozwiązania:

1. Pytanie do pkt. 3.4

Czy Zamawiający dopuści, aby weryfikacja agenta podłączającego się do konsoli będzie wykonywana na podstawie certyfikatu lub hasła? Jest to rozwiązanie bezpieczniejsze, niż użycie hasła.

2. Pytanie do pkt. 4.2

Średni poziom zużycia CPU jest parametrem zależnym w ogromnej mierze od aktywności danej stacji roboczej/serwera. Większość systemów obciąża procesor średnio w nie więcej niż 5%. Czy Zamawiający zgodzi się na zmianę średniego zużycia CPU poniżej 5%?

3. Pytanie do pkt. 6.1

Wymaganie wskazuje na jednego konkretnego dostawcę i ogranicza konkurencję. Zwracamy się prośbą o wykreślenie tego wymagania.

4. Pytanie do pkt. 6.6 d

Wszystkie wymienione parametry można nadpisać, co w konsekwencji może prowadzić do luki bezpieczeństwa. Ze względu na to, oraz na fakt ograniczenia konkurencji, zwracamy się o wykreślenie tego wymagania.

5. Pytanie do pkt. 6.8

Czy Zamawiający uzna za spełnione to wymaganie w przypadku systemu, który umożliwia detekcję połączeń do złośliwych domen lub adresów IP?

6. Pytanie do pkt. 7.4

Czy Zamawiający uzna za spełnione to wymaganie w przypadku systemu bez wsparcia formatu STIX? Jeżeli nie, to prosimy o podanie jakie obecnie systemy korzystają w Urzędzie z formatu STIX i jakie systemy/źródła miałyby dostarczać dane w formacie STIX do przeprowadzania wyszukiwań?

7. Pytanie do pkt. 7.9b

Czy Zamawiający uzna za spełnione to wymaganie w przypadku systemu, który zbiera informacje o działaniach na plikach, w przypadku operacji CREATE, RENAME oraz DELETE?

8. Pytanie do pkt. 7.9d

Czy Zamawiający uzna za spełnione to wymaganie w przypadku systemu, który zbiera wszystkie wymienione informacje, bez zapytań http?

9. Pytanie do pkt. 7.9f

Czy Zamawiający uzna za spełnione to wymaganie w przypadku systemu, który zdarzenia Registry Events w zakresie operacji CREATE/DELETE/MODIFY?

10. Pytanie do pkt. 7.9f

Czy Zamawiający uzna za spełnione to wymaganie w przypadku systemu, który zdarzenia Registry Events w zakresie operacji CREATE/DELETE/MODIFY?

11. Pytanie do pkt. 10.1

Przedstawione klasy zagrożeń wskazują na konkretnego dostawcę rozwiązania, co ogranicza konkurencję. Zwracamy się z prośbą o ograniczenie wymaganych kategorii do

- Złośliwe
- Podejrzane
- PUP-Potential Unwanted Program

12. Pytanie do pkt. 10.2

Czy Zamawiający uzna za spełnione to wymaganie w przypadku systemu, który posiada następujące reakcje na incydent?

- Zabicie procesu
- Przeniesienie pliku do kwarantanny
- Zablokowanie możliwości uruchomienia pliku wykonywalnego
- Izolacja sieciowa stacji

13. Pytanie do pkt. 10.3

Wysyłanie plików do analizy w chmurze wiąże się z ryzykiem wycieku danych wrażliwych, dodatkowo wymaganie to znacząco ogranicza konkurencję, w związku z tym zwracamy się z prośbą o wykreślenie tego wymagania, lub uznanie go za opcjonalne.

14. Pytanie do pkt. 10.6

Do realizacji tego typu operacji wykorzystywane są systemy klasy SOAR, dlatego zwracamy się z prośbą, aby wykreślić to wymaganie i nie łączyć funkcji systemu innej klasy, co znacząco ograniczy konkurencję.

15. Pytanie do pkt. 10.7c

Czy Zamawiający uzna za spełnione to wymaganie w przypadku systemu, który umożliwia wysyłanie powiadomień za pomocą wiadomości e-mail oraz protokołu syslog, oraz posiada otwarte API do wszelkich innych integracji?

16. Pytanie do pkt. 11.1-11.5

Opisane w punktach 11.1 do 11.5 dotyczą funkcji realizowanych przez skanery podatności, w związku z czym zwracamy się z prośbą o wykreślenie wymagań opisanych w punktach 11.1, 11.2, 11.3, 11.4, 11.5.

17. Pytanie do pkt. 12.3b

Producenci rozwiązań, których dotyczy przedmiotowe zapytanie, bardzo często posiadają umowy o współpracy z komercyjnymi dostawcami baz reputacji, zdejmując jednocześnie z klienta konieczność opłacania własnej licencji. W związku z tym zwracamy się z prośbą o modyfikację punktu 12.3b do postaci: „Możliwość korzystania z komercyjnych baz reputacji plików (np. Virus Total) lub wskazania, z jakich komercyjnych baz reputacji korzysta rozwiązanie (minimum Virus Total).”

18. Pytanie do pkt. 14.2

Termin „Raport GDPR” wskazuje na konkretnego dostawcę, zwracamy się z prośbą o modyfikację punktu 14.2 do poniższego brzmienia:

„Dostarczony system musi umożliwiać eksport szczegółowego audytu funkcjonowania systemu zawierającego przynajmniej informacje o tym, kto, kiedy i jakie wprowadzał zmiany w politykach, podejmował akcje, logował się do systemu.”

19. Pytanie do pkt. 15.3

Dobre praktyki bezpieczeństwa sugerują rozdzielenie funkcji systemów EDR i firewall. Firewall powinien być zarządzany przez odrębny zespół, a wprowadzanie reguł blokowania powinno być poprzedzone weryfikacją przez administratorów sieci. Automatyzacja wprowadzania reguł przez EDR może wprowadzać chaos w polityce bezpieczeństwa sieciowego. Ponadto każdy system EDR generuje pewien procent fałszywych alarmów. Jeśli system będzie automatycznie blokował adresy IP na firewallu na podstawie takich alarmów, może to prowadzić do wielu nieuzasadnionych blokad, utrudniając pracę użytkowników i dostęp do zasobów.

Poza tym złośliwe oprogramowanie często wykorzystuje wiele dynamicznie zmieniających się adresów IP, które są jednorazowe lub krótkotrwałe. Blokowanie takich adresów nie zawsze jest skuteczne, ponieważ atakujący mogą szybko zmienić infrastrukturę komunikacyjną, co sprawia, że taka reakcja jest bardzo mało efektywna.

Dodatkowo biorąc pod uwagę szereg podatności wykrywanych sukcesywnie w urządzeniach Firewall, jak np.

- Palo Alto Networks - https://kapitanhack.pl/2024/04/24/nieskategoryzowane/zero-day-w-palo-alto-wykorzystywany-w-atakach-ponad-6000-niezalatanych-podatnych-instancji/
- Fortinet i Cisco - https://kapitanhack.pl/2023/02/20/nieskategoryzowane/uwaga-na-te-krytyczne-podatnosci-w-cisco-oraz-fortinet-dzieki-nim-haker-moze-wlamac-sie-do-twojej-firmy/
- Check Point Software, https://sekurak.pl/gruba-podatnosc-w-urzadzeniach-vpn-od-checkpointa-mozna-czytac-pliki-z-uprawnieniami-root-cve-2024-24919/

prosimy o wykreślenie wymagań z punktów 10.6 i 15.3 dotyczących integracji systemu EDR z Firewall’ami”.

Odpowiedź:

Zamawiający nie zgadza się z twierdzeniami podniesionymi przez Wykonawcę jakoby zapisy SWZ były niezgodne z przepisami ustawy a opis przedmiotu zamówienia ograniczał konkurencję. Prawem Zamawiającego i zarazem jego obowiązkiem jest ocena własnych potrzeb i dokonanie zamówienia zgodnie z tymi potrzebami. Określenie i opisanie przedmiotu zamówienia zostało dokonane stosownie do uzasadnionych potrzeb Zamawiającego i zgodnie z przepisami ustawy.

1. Zamawiający podtrzymuje dotychczasowe zapisy SWZ w tym zakresie.

2. Na podstawie art. 286 ust. 1 ustawy Zamawiający dokonuje modyfikacji zapisów Załącznika do Umowy – Minimalne wymagania dla oprogramowania – specjalistyczna ochrona EDR dla urządzeń końcowych poprzez zmianę treści pkt 4.2., który otrzymuje brzmienie: *Poziom średni zużycia procesora (CPU) dla procesów agenta musi wynosić mniej niż 5%.*
3. Obecnie jest to powszechnie spotykana funkcjonalność. Zamawiający podtrzymuje dotychczasowe zapisy SWZ w tym zakresie.
4. Jest to popularna opcja ułatwiająca tworzenie white list. Zamawiający podtrzymuje dotychczasowe zapisy SWZ w tym zakresie.
5. Zamawiający nie uzna za spełnione wymaganie opisane w pkt 6.8. Załącznika do Umowy – Minimalne wymagania dla oprogramowania – specjalistyczna ochrona EDR dla urządzeń końcowych, w przypadku gdy system umożliwia jedynie detekcję połączeń do złośliwych domen lub adresów IP. Zamawiający podtrzymuje dotychczasowe zapisy SWZ w tym zakresie.
6. Zamawiający nie uzna za spełnione wymaganie opisane w pkt 7.4. Załącznika do Umowy – Minimalne wymagania dla oprogramowania – specjalistyczna ochrona EDR dla urządzeń końcowych, w przypadku systemu bez wsparcia formatu STIX. Obecnie systemy, które korzystają u Zamawiającego z formatu STIX to: Cortex XDR, Microsoft Defender XDR, Splunk. LUMINAR. Zamawiający podtrzymuje dotychczasowe zapisy SWZ w tym zakresie.
7. Zamawiający nie uzna za spełnione wymaganie opisane w pkt 7.9.b Załącznika do Umowy – Minimalne wymagania dla oprogramowania – specjalistyczna ochrona EDR dla urządzeń końcowych, w przypadku systemu, który zbiera informacje o działaniach na plikach, w przypadku jedynie operacji CREATE, RENAME oraz DELETE. Zamawiający podtrzymuje dotychczasowe zapisy SWZ w tym zakresie.
8. Zamawiający nie uzna za spełnione wymaganie opisane w pkt 7.9.d Załącznika do Umowy – Minimalne wymagania dla oprogramowania – specjalistyczna ochrona EDR dla urządzeń końcowych, w przypadku systemu, który zbiera wszystkie wymienione informacje, bez zapytań http. Zamawiający podtrzymuje dotychczasowe zapisy SWZ w tym zakresie.
9. Zamawiający nie uzna za spełnione wymaganie opisane w pkt 7.9f. Załącznika do Umowy – Minimalne wymagania dla oprogramowania – specjalistyczna ochrona EDR dla urządzeń końcowych, w przypadku systemu, który jedynie uwzględnia „zdarzenia Registry Events w zakresie operacji CREATE/DELETE/MODIFY". Zamawiający podtrzymuje dotychczasowe zapisy SWZ w tym zakresie.
10. Zgodnie z odpowiedzią udzieloną na pytanie w pkt 9 powyżej – pytanie z pkt 10 jest jego powtórzeniem.
11. Jest to popularna klasyfikacja. Zamawiający podtrzymuje dotychczasowe zapisy SWZ w tym zakresie.
12. Zamawiający nie uzna za spełnione wymaganie opisane w pkt 10.2. Załącznika do Umowy – Minimalne wymagania dla oprogramowania – specjalistyczna ochrona EDR dla urządzeń końcowych, w przypadku systemu, który posiada następujące reakcje na incydent:
    - Zabicie procesu
    - Przeniesienie pliku do kwarantanny
    - Zablokowanie możliwości uruchomienia pliku wykonywalnego
    - Izolacja sieciowa stacji

    Zamawiający podtrzymuje dotychczasowe zapisy SWZ w tym zakresie.
13. Współcześnie jest to popularne rozwiązanie i swego rodzaju standard. Zamawiający podtrzymuje dotychczasowe zapisy SWZ w tym zakresie.
14. Jest to popularne rozwiązanie. Zamawiający podtrzymuje dotychczasowe zapisy SWZ w tym zakresie.
15. Zamawiający nie uzna za spełnione wymaganie opisane w pkt 10.7. c. Załącznika do Umowy – Minimalne wymagania dla oprogramowania – specjalistyczna ochrona EDR dla urządzeń końcowych, w przypadku systemu, który umożliwia wysyłanie powiadomień za pomocą wiadomości e-mail oraz protokołu syslog, oraz posiada otwarte API do wszelkich innych integracji. Zamawiający podtrzymuje dotychczasowe zapisy SWZ w tym zakresie.
16. Zamawiający podtrzymuje dotychczasowe zapisy SWZ w tym zakresie.
17. Zamawiający podtrzymuje dotychczasowe zapisy SWZ w tym zakresie. System musi umożliwiać analizę reputacji plików, domen, adresów IP, URL-i, podpisów cyfrowych, wykrywanie phishingu, malware, wskaźników kompromitacji (IoC), analizę zachowania plików, sandboxing oraz powiązania między różnymi wskaźnikami zagrożeń.
18. GDPR to RODO standard unijny. Popularne rozwiązanie mające na celu wspomaganie zgodności z przepisami RODO (GDPR - General Data Protection Regulation). Zamawiający podtrzymuje dotychczasowe zapisy SWZ w tym zakresie.
19. Zamawiający podtrzymuje dotychczasowe zapisy SWZ w tym zakresie.

Zamawiający, działając na podstawie art. **286 ust. 3 i 9 ustawy**, dokonuje zmiany SWZ w zakresie pkt 15, 16.1. i 16.4. otrzymują nowe brzmienie:

15. Termin związania ofertą:
Wykonawca składający ofertę pozostaje nią związany do **06/11/2024r.**
16. Termin składania i otwarcia ofert:
16.1. Oferty należy złożyć w formie określonej w pkt 8. oraz w sposób określony w pkt 10. SWZ nie później niż do dnia **08/10/2024 r. do godz. 09:30**.
16.4. Otwarcie ofert nastąpi w dniu **08/10/2024 r. o godz. 11:00**.

W pozostałym zakresie treść SWZ pozostaje bez zmian.

Jednocześnie Zamawiający informuje, iż zgodnie z treścią **art. 286 ust. 6 ustawy** Zamawiający zamieścił informację o przedłużonym terminie składania ofert w ogłoszeniu, o którym mowa w **art. 267 ust. 2 pkt 6**. Zamawiający udostępnił ww. ogłoszenie na stronie internetowej prowadzonego postępowania oraz na stronie BIP UMK w zakładce dot. przedmiotowego postępowania.

z up. PREZYDENTA MIASTA
(-)
Paweł Schmidt
Dyrektor
Centrum Obsługi Informatycznej

Urząd Miasta Krakowa
CENTRUM OBSŁUGI INFORMATYCZNEJ
tel. +48 12 616 12 45, +48 12 616 15 71, it.umk@um.krakow.pl
31-156 Kraków, ul. Basztowa 20
Adres do korespondencji
31-004 Kraków, pl. Wszystkich Świętych 3-4
www.krakow.pl