

Zapytanie ofertowe

Skan pasywny bezpieczeństwa aplikacji i systemów IT

Przedsiębiorstwo Usług Komunalnych „USKOM” Sp. z o.o. w Kozuchowie zaprasza do złożenia oferty na wykonanie jednorazowej usługi skanowania i analizy podatności bezpieczeństwa systemów, aplikacji oraz infrastruktury IT, wraz z kontrolowaną weryfikacją wykrytych podatności i sporządzeniem raportu. Zamówienie jest realizowane w ramach projektu „Cyberbezpieczne Wodociągi”.

1. Zamawiający i kontakt

Przedsiębiorstwo Usług Komunalnych „USKOM” Sp. z o.o. w Kozuchowie, ul. Elektryczna 9, 67-120 Kozuchów; tel. 68 355 22 08; e-mail: sekretariat@uskom.eu. Osoba prowadząca postępowanie i adres do składania ofert: p.malczyk@uskom.eu

2. Przedmiot zamówienia

Przedmiotem zamówienia jest jednorazowe badanie podatności zasobów IT wskazanych przez Zamawiającego, w szczególności serwerów, urządzeń sieciowych, systemów operacyjnych, usług sieciowych oraz wykorzystywanych systemów i aplikacji. Szczegółowe wymagania określa załącznik nr 1 – Opis przedmiotu zamówienia (OPZ): „Skan bezpieczeństwa aplikacji i systemów IT”, który stanowi integralną część zapytania.

Zakres ilościowy zasobów objętych badaniem, na potrzeby przygotowania oferty: 10 serwerów, 15 urządzeń sieciowych, 10 systemów/aplikacji oraz maksymalnie 100 adresów IP. Zamawiający przekaże wybranemu Wykonawcy przed rozpoczęciem badania szczegółową listę zasobów, w tym adresy IP, nazwy hostów, systemów, urządzeń i usług oraz informacje o konfiguracji.

Wykonawca zidentyfikuje dostępne hosty, otwarte porty, uruchomione usługi i ich wersje, o ile ich ustalenie jest możliwe przy użyciu standardowych, niedestrukcyjnych metod. Zidentyfikuje znane podatności, w szczególności opisane w bazach CVE, nieaktualne oprogramowanie i brakujące aktualizacje bezpieczeństwa, ryzykowne usługi, protokoły lub mechanizmy oraz podstawowe błędy i słabości konfiguracji. Przeprowadzi kontrolowaną weryfikację wyników w zakresie niezbędnym do ograniczenia

wyników fałszywie dodatnich, oceni ryzyko i wskaże zalecenia dotyczące usunięcia, ograniczenia lub dalszej weryfikacji podatności. Przypadki, w których nie udało się ustalić wersji, należy wskazać w raporcie.

Zamawiający nie dopuszcza ofert częściowych ani wariantowych; zamówienie obejmuje jedną kompletną usługę zgodną z OPZ.

3. Terminy, raportowanie i odbiór

Termin wykonania usługi, wraz z przekazaniem kompletnego raportu: do 15 listopada 2026 r. Przed rozpoczęciem badania Wykonawca uzgodni z Zamawiającym termin, zakres i sposób prowadzenia czynności, w szczególności tych, które mogą powodować zwiększone obciążenie infrastruktury.

Po zakończeniu badania Wykonawca prześle raport w formie elektronicznej, np. w formacie PDF. Raport musi zawierać co najmniej: opis zakresu testów, zastosowaną metodykę i narzędzia, wykaz przebadanych zasobów, opis podatności, słabości i nieprawidłowości, ocenę ryzyka poszczególnych ustaleń, odniesienia do CVE i wartości CVSS, jeżeli mają zastosowanie, dowody umożliwiające weryfikację ustaleń, zalecenia oraz krótkie podsumowanie najistotniejszych zagrożeń wymagających priorytetowych działań.

Podatności i słabości należy sklasyfikować co najmniej na poziomach: krytyczny, wysoki, średni, niski i informacyjny, z uwzględnieniem wpływu na poufność, integralność i dostępność systemów oraz danych. Jeżeli dostępna jest ocena CVSS, Wykonawca wskaże jej wartość punktową oraz, w miarę możliwości, wektor CVSS. Dla ustaleń, dla których CVSS nie ma zastosowania, poziom ryzyka określi na podstawie oceny eksperckiej, z krótkim uzasadnieniem.

Podstawą odbioru będzie przekazanie kompletnego raportu zgodnego z OPZ. Zamawiający zweryfikuje jego kompletność, zgodność z zakresem zamówienia oraz czytelność ustaleń i zaleceń. Odbiór nastąpi po zaakceptowaniu raportu przez Zamawiającego i może zostać potwierdzony protokołem odbioru lub innym dokumentem potwierdzającym prawidłową realizację zamówienia.

Na żądanie Zamawiającego Wykonawca udzieli wyjaśnień oraz omówi zidentyfikowane podatności, poziomy ryzyka i zalecenia. Braki, nieścisłości lub konieczność doprecyzowania wyników wyjaśni lub uzupełni bez dodatkowego wynagrodzenia, w terminie nie dłuższym niż 3 dni robocze od przekazania uwag przez Zamawiającego, chyba że Zamawiający wyrazi zgodę na inny termin.

4. Warunki udziału w postępowaniu

O udzielenie zamówienia mogą ubiegać się Wykonawcy posiadający doświadczenie niezbędne do prawidłowego i bezpiecznego przeprowadzenia badania. Zamawiający uzna warunek za spełniony, jeżeli Wykonawca wykaże, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, należycie wykonał co najmniej jedną usługę obejmującą testy bezpieczeństwa, skanowanie podatności lub analizę podatności infrastruktury albo

systemów IT. Dopuszcza się doświadczenie zdobyte przy realizacji usług na rzecz podmiotów publicznych i prywatnych.

Na potwierdzenie spełnienia warunku Wykonawca dołączy do oferty Wykaz wykonanych usług według wzoru stanowiącego załącznik nr 4. Wykaz musi zawierać co najmniej nazwę lub przedmiot usługi, podmiot, na rzecz którego została wykonana, oraz datę realizacji. Do wykazu należy dołączyć dokument potwierdzający należyte wykonanie wskazanej usługi, np. referencję, protokół odbioru, poświadczenie odbiorcy usługi lub inny równoważny dokument.

O udzielenie zamówienia nie może ubiegać się Wykonawca, wobec którego zachodzą przesłanki wykluczenia określone w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego. Wykonawca składa wraz z ofertą oświadczenie o braku podstaw wykluczenia. Oświadczenie składa się w Formularzu oferty stanowiącym załącznik nr 2 do niniejszego zapytania ofertowego. Zamawiający zastrzega możliwość weryfikacji oświadczenia w publicznie dostępnych rejestrach oraz wezwania Wykonawcy do złożenia wyjaśnień.

5. Sposób realizacji i wymagania bezpieczeństwa

Usługa może być realizowana zdalnie lub w siedzibie Zamawiającego, zależnie od metodyki Wykonawcy i uzgodnień organizacyjnych oraz technicznych. Wykonawca może stosować specjalistyczne narzędzia automatyczne, uzupełnione w razie potrzeby manualną weryfikacją wyników. W przypadku realizacji zdalnej Zamawiający zapewni uzgodniony sposób dostępu do badanych zasobów, zgodny z obowiązującymi u niego zasadami bezpieczeństwa.

Badanie musi być prowadzone wyłącznie w uzgodnionym zakresie, w sposób bezpieczny i kontrolowany, ograniczający ryzyko wpływu na ciągłość działania, dostępność, wydajność i poprawność funkcjonowania środowiska IT. Zamówienie nie obejmuje pełnego testu penetracyjnego ani działań destrukcyjnych, o ile Zamawiający nie wyrazi na określone czynności odrębnej zgody.

Bez uprzedniej, wyraźnej zgody Zamawiającego niedopuszczalne są: testy DoS/DDoS i celowe przeciążanie systemów lub usług; usuwanie, niszczenie, modyfikowanie lub szyfrowanie danych; celowe wyłączanie usług; trwałe zmiany konfiguracji; instalowanie dodatkowego oprogramowania, agentów lub komponentów; wykorzystywanie podatności w sposób mogący spowodować zatrzymanie, destabilizację lub utratę dostępności usług oraz inne działania wykraczające poza uzgodniony zakres badania.

Jeżeli dalsza weryfikacja podatności mogłaby wiązać się z ryzykiem zakłócenia pracy systemu, Wykonawca przerwie czynności w tym zakresie i poinformuje Zamawiającego.

6. Cena i kryterium wyboru

Wykonawca podaje jedną łączną cenę za kompletną realizację zamówienia, obejmującą wszystkie koszty określone w zapytaniu ofertowym i OPZ, wyrażoną w PLN, z dokładnością do dwóch miejsc po przecinku.

Wykonawca wskazuje cenę netto, stawkę i kwotę VAT oraz cenę brutto, jeżeli podatek ma zastosowanie.

Jedynym kryterium oceny ofert jest koszt porównawczy – 100%.

Do oceny ofert przyjmuje się:

w przypadku wykonawców naliczających VAT – cenę netto;

w przypadku wykonawców nienaliczających VAT – całkowitą kwotę oferty;

w pozostałych przypadkach – rzeczywisty koszt zamówienia po uwzględnieniu rozliczenia VAT.

Liczba punktów zostanie obliczona według wzoru:

$$P = (K_{min} / K_{bad}) \times 100$$

gdzie:

K_{min} – najniższy koszt porównawczy spośród ocenianych ofert,

K_{bad} – koszt porównawczy badanej oferty.

Wynik zostanie zaokrąglony do dwóch miejsc po przecinku. Maksymalnie można uzyskać 100 punktów.

W przypadku ofert z jednakowym najniższym kosztem porównawczym Zamawiający wezwie wykonawców do złożenia ofert dodatkowych z ceną nie wyższą od pierwotnie zaoferowanej.

7. Przygotowanie i złożenie oferty

Ofertę należy sporządzić na formularzu stanowiącym załącznik nr 2 do zapytania. Oferta musi zostać podpisana przez osobę uprawnioną do reprezentowania Wykonawcy. Dopuszcza się:

- 1) podpisanie oferty własnoręcznie i przesłanie skanu podpisanego dokumentu w formacie PDF albo
- 2) sporządzenie oferty w postaci elektronicznej i opatrzenie jej kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym. Jeżeli ofertę podpisuje osoba działająca na podstawie pełnomocnictwa, do oferty należy dołączyć dokument potwierdzający jej umocowanie. Ofertę wraz z wymaganymi załącznikami należy przesłać drogą elektroniczną na adres e-mail: p.malczyk@uskom.eu. W temacie wiadomości należy wpisać: „Oferta – skan bezpieczeństwa aplikacji i systemów IT – USKOM”. Termin składania ofert: 26.10.2026 r. do godz. 9.00. O zachowaniu terminu decyduje wpływ wiadomości do Zamawiającego.

Pytania dotyczące zapytania należy kierować na adres: p.malczyk@uskom.eu, najpóźniej do 22.10.2026 r. Odpowiedzi i ewentualne zmiany zapytania Zamawiający przekaże w sposób zapewniający jednakowy dostęp zainteresowanym wykonawcom. Wykonawca pozostaje związany ofertą przez okres 30 dni od dnia upływu terminu składania ofert.

Wraz z ofertą Wykonawca składa:

- 1) formularz oferty – załącznik nr 2;
- 2) wykaz wykonanych usług – załącznik nr 4;
- 3) dowody potwierdzające należyte wykonanie usług wskazanych w wykazie, o których mowa w pkt 4 niniejszego zapytania;
- 4) oświadczenie o braku podstaw wykluczenia, zawarte w Formularzu oferty;
- 5) dokument potwierdzający umocowanie osoby podpisującej ofertę – jeżeli umocowanie nie wynika z właściwego rejestru lub ofertę podpisuje pełnomocnik.

Zamawiający może wezwać Wykonawcę do złożenia wyjaśnień dotyczących treści oferty lub do uzupełnienia brakujących dokumentów lub oświadczeń, wyznaczając w tym celu odpowiedni termin, o ile nie prowadzi to do zmiany ceny ani istotnej zmiany oferowanego świadczenia. Zamawiający nie będzie oceniał oferty złożonej po terminie, oferty niezgodnej z wymaganiami OPZ ani oferty Wykonawcy podlegającego wykluczeniu lub niespełniającego warunków udziału w postępowaniu, jeżeli pomimo wezwania nie wykazał ich spełnienia lub nie uzupełnił wymaganych dokumentów lub oświadczeń w wyznaczonym terminie. O wyniku postępowania Zamawiający poinformuje Wykonawców, którzy złożyli oferty.

8. Poufność, dane osobowe i dokumentacja projektu

Wykonawca zobowiązany jest zachować w poufności wszelkie informacje uzyskane w związku z realizacją zamówienia, w szczególności dotyczące architektury środowiska IT, adresacji, konfiguracji, wykrytych podatności oraz danych uwierzytelniających. Informacje i materiały mogą być wykorzystywane wyłącznie w celu wykonania zamówienia i nie mogą być udostępniane osobom trzecim bez uprzedniej zgody Zamawiającego. Wykonawca zastosuje odpowiednie środki organizacyjne i techniczne chroniące dane przed nieuprawnionym dostępem, utratą, ujawnieniem lub modyfikacją.

Raport, wyniki skanowania, dane dostępne i pozostałe materiały zawierające informacje o podatnościach lub konfiguracji środowiska muszą być przechowywane i przekazywane w sposób zabezpieczony przed dostępem osób nieuprawnionych. Hasła lub inne sekrety umożliwiające odszyfrowanie materiałów należy przekazywać odrębnym kanałem komunikacji.

Po zakończeniu usługi i przekazaniu wymaganej dokumentacji Wykonawca bezpiecznie usunie kopie danych i materiałów pozyskanych podczas badania, chyba że dalsze przechowywanie wynika z obowiązujących przepisów prawa lub zostanie odrębnie uzgodnione z Zamawiającym.

Jeżeli realizacja usługi będzie wymagała przetwarzania danych osobowych przez Wykonawcę w imieniu Zamawiającego, strony zawrą wymaganą umowę powierzenia zgodnie z art. 28 RODO. Wykonawca zapewni

Zamawiającemu dokumentację potwierdzającą wykonanie usługi w zakresie niezbędnym do rozliczenia projektu, z zachowaniem zasad poufności określonych w OPZ.

Załączniki

1. Załącznik nr 1 – Opis przedmiotu zamówienia: „Skan bezpieczeństwa aplikacji i systemów IT”.
2. Załącznik nr 2 – Formularz oferty na skan bezpieczeństwa aplikacji i systemów IT.
3. Załącznik nr 3 – Umowa na wykonanie skanu bezpieczeństwa aplikacji i systemów IT.
4. Załącznik nr 4 – Wykaz wykonanych usług testów bezpieczeństwa, skanowania lub analizy podatności infrastruktury albo systemów IT.