Pyzdry, 28 sierpnia 2025 r.

OR.FZ.042.8.2024

Zapytanie ofertowe

Zamówienie o wartości szacunkowej nieprzekraczającej równowartości 130 000 złotych, wyłączone z obowiązku stosowania przepisów ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2024 r. poz. 1320 ze zm.)

Burmistrz Pyzdr zwraca się z prośbą o przygotowanie oferty na uruchomienie i świadczenie usługi SOC (Security Operations Center) przy realizacji projektu ,,Cyberbezpieczny Samorząd". Projekt realizowany w ramach Konkursu Grantowego „Cyberbezpieczny Samorząd" (Priorytet II: Zaawansowane usługi cyfrowe. Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa Fundusze Europejskie na Rozwój Cyfrowy 2021-2027).

1. Przedmiot zamówienia:

Uruchomienie i świadczenie kompleksowej usługi Security Operations Center (SOC) dla Urzędu Miejskiego w Pyzdrach. Przedmiot zamówienia obejmuje:

1.1. Monitorowanie i analiza zdarzeń:

a) Operacyjne monitorowanie i zarządzanie zdarzeniami bezpieczeństwa w dni robocze (poniedziałek-piątek) z pominięciem dni wolnych od pracy jeśli wypadają w tygodniu roboczym w godzinach 7:15-16:00 środowiska Zamawiającego obejmującego: 2 serwery fizyczne, 6 serwerów wirtualnych i ok. 40 stacji roboczych i użytkowników domeny.

b) Analiza danych z systemów wykrywania włamań (IDS/IPS), zapór ogniowych, systemów antywirusowych i innych, w szczególności z posiadanych przez Zamawiającego systemów:

- ESET Protect Elite – system klasy XDR – monitoring ma zapewnić bezpieczeństwo ok. 40 końcówek,
- Stormshield UTM – firewall brzegowy + system IPS/IDS – monitoring ma zapewnić bezpieczeństwo sieciowe,
- Domena Active Directory – monitoring ma zapewnić wyłapywanie anomalii

c) Wykonawca w celu zapewnienia odpowiedniego poziomu bezpieczeństwa ma obowiązek monitorować bezpośrednio wskazane systemy jak również korelować zdarzenia z 3 wskazanych wyżej źródeł (zbieranie i analizowanie danych z końcówek oraz sieci)

d) Dopuszcza się zastosowanie dodatkowych źródeł o zagrożeniach i uwzględnienie ich w monitorowaniu systemów,

e) Wykorzystanie zaawansowanych narzędzi SIEM (Security Information and Event Management) do analizowania i korelacji danych w celu wykrycia potencjalnych zagrożeń. Dostawca zapewni odpowiednie licencje na uruchamiane komponenty SIEM a systemy będą pracować na infrastrukturze Zamawiającego. Dopuszcza się stosowanie rozwiązań Open Source.

1.2. Wykrywanie i reagowanie na incydenty:

a) Natychmiastowa identyfikacja i klasyfikacja incydentów bezpieczeństwa.

b) Reagowanie na incydenty poprzez adekwatne działania obronne i łagodzące skutki.

c) Angażowanie zespołu ds. reagowania na incydenty (będącego w strukturach IT) w przypadkach naruszeń bezpieczeństwa o wysokim ryzyku (incydenty krytyczne) poprzez w ustalonej formie – mail lub kontakt telefoniczny ze wskazanymi osobami wskazanymi w umowie.

1.3. Zarządzanie incydentami bezpieczeństwa:

a) Dokumentowanie każdego incydentu bezpieczeństwa oraz ścieżki reakcji.

b) Analiza przyczyn źródłowych incydentów i proponowanie środków zaradczych.

c) Przeprowadzanie przeglądów po incydentach w celu poprawienia strategii obronnej.

d) Prowadzenie Rejestru Incydentów Cyberbezpieczeństwa.
e) Pomoc w zgłaszaniu incydentów do Krajowego Systemu Cyberbezpieczeństwa.

1.4. Proaktywne wykrywanie podatności w infrastrukturze IT:
a) Przeprowadzanie skanów bezpieczeństwa (podatności), testów penetracyjnych (1 raz w miesiącu) w celu wzmocnienia zabezpieczeń infrastruktury IT.
b) Okresowe audyty bezpieczeństwa 1 raz na kwartał.

1.5. Aktualizacje strategii, systemów i narzędzi:
a) Regularne aktualizacje systemów (w tym SIEM) wykrywania i ochrony zagrożeń w celu zabezpieczenia przed najnowszymi zagrożeniami.
b) Konfiguracja narzędzi bezpieczeństwa i ich dostosowywanie do zmieniających się potrzeb Zamawiającego.

1.6. Raportowanie i komunikacja:
a) Generowanie raportów miesięcznych dotyczących zagrożeń, incydentów oraz stanu bezpieczeństwa, dostosowanych do potrzeb Zamawiającego.
b) Organizowanie regularnych (przynajmniej raz w miesiącu) spotkań i sesji informacyjnych w celu omawiania wyników oraz strategii dalszych działań.

1.7. Edukacja i świadomość bezpieczeństwa:
a) Przeprowadzenie szkoleń dla pracowników urzędu dotyczących najlepszych praktyk bezpieczeństwa IT w wymiarze przynajmniej 1 godziny na kwartał.
b) Programy podnoszące świadomość w zakresie ochrony danych i procedur bezpieczeństwa (wewnętrzne informacje kolportowane za pomocą sieci wewnętrznej zawierające np. infografiki, opisy przykładowych incydentów, przykłady dobrych praktyk użytkowników systemów IT)
b) Programy podnoszące świadomość w zakresie ochrony danych i procedur bezpieczeństwa.

UWAGA! Każdy z powyższych elementów powinien być elastycznie dostosowany do specyficznych potrzeb urzędu, uwzględniając istniejące środowisko IT i potencjalne wektory zagrożeń.

2. Wymagania dotyczące wykonawcy:

a) Posiadanie ważnych certyfikatów potwierdzających zgodność z normami bezpieczeństwa, takimi jak ISO/IEC 27001 lub ISO/IEC 22301 nieprzerwanie przynajmniej od 4 lat.
b) Posiadanie wykształcenia w zakresie cyberbezpieczeństwa lub informatycznego lub pokrewnego informatycznemu (studia magisterskie lub podyplomowe).
c) Posiadanie doświadczenia współpracy z jednostkami samorządu terytorialnego w zakresie bezpieczeństwa informacji, ochrony danych osobowych lub informatyki od 2020 roku.

Na potwierdzenie powyższych wymogów oferent przedstawi dokumenty potwierdzające posiadanie certyfikatu, wykształcenia oraz doświadczenia. Niespełnienie któregokolwiek z wymogów skutkować będzie odrzuceniem oferty.

3. Termin realizacji:
Termin świadczenia usługi SOC: **od podpisania umowy do 31.05.2026 r.**

4. Kryteria oceny ofert:
- Cena

Opis kryteriów i sposobu oceny ofert
Zamawiający dokona oceny ofert na podstawie następujących kryteriów:

1) Cena brutto 100%

Jeżeli zostały złożone oferty o takiej samej cenie. Zamawiający wezwie oferentów, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych. Oferenci składający oferty dodatkowe nie mogą zaoferować cen wyższych niż zaoferowane w złożonych ofertach.

5. Opis sposobu przygotowania oferty:
Oferta powinna**:**

- posiadać datę sporządzenia
- zawierać adres lub siedzibę oferenta, numer telefonu, NIP
- być podpisana przez oferenta
- zawierać proponowaną cenę netto i brutto.

6. Miejsce oraz termin składania ofert:
Ofertę należy złożyć **do dnia 8 września 2025 r.** elektronicznie na adres e-mail: admin@pyzdry.pl, lub EPUAP, lub ADE, lub pisemnie na adres: Urząd Miejski w Pyzdrach, ul. Taczanowskiego 1, 62-310 Pyzdry, biuro nr 13. Oferty złożone po terminie oraz oferty, których treść nie odpowiada treści zapytania ofertowego nie będą rozpatrywane.

7. Określenie warunków dokonywania zmian umowy:
Zamawiający dopuszcza możliwość zmian umowy. Zmiany mogą dotyczyć w szczególności:
a) zmiany powszechnie obowiązujących przepisów prawa w zakresie mającym wpływ na realizację przedmiotu zamówienia lub świadczenia stron,
b) zmiany stawki podatku VAT,
c) zmian dotyczących sposobu płatności.
Wszelkie istotne zmiany w umowie wymagają formy pisemnej pod rygorem nieważności.

8. Sposób rozliczenia
Po wykonaniu przedmiotu zamówienia zapłata dokonana będzie przelewem na rachunek bankowy Wykonawcy, wskazany w wystawionej przez Wykonawcę fakturze VAT, w terminie do 21 dni od wystawienia faktury. Z tym, że pierwsza transza wynagrodzenia przekazana zostanie do 31.12.2025 r., druga po wykonaniu przedmiotu zamówienia.

9. Uwagi
Zamawiający nie dopuszcza możliwości powierzenia części lub całości zamówienia podwykonawcom. Zamówienie nie może być udzielane podmiotom powiązanym z Zamawiającym osobowo lub kapitałowo.

10. Dodatkowe informacje:
Dodatkowych informacji w sprawie zamówienia udziela Pani Grażyna Juszczak tel. 63-2768-333, wew. 110.

Burmistrz Pyzdr
/-/ Przemysław Dębski