Cyberbezpieczne Wodociągi

16/MW/2026

ZAPYTANIE OFERTOWE

ZAMAWIAJĄCY:

ZAKŁAD GOSPODARKI KOMUNALNEJ W JEZIERZYCACH SP. Z O.O.

JEZIERZYCE, UL. KOLEJOWA 5, 76-200 SŁUPSK

Zaprasza do złożenia oferty w postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie zapytania ofertowego na podstawie sektorowego regulaminu wewnętrznego Zamawiającego pn: „**Modernizacja i zabezpieczenie środowiska OT (Operational Technology)”**

Zamówienie realizowane jest w ramach projektu grantowego pod nazwą „Cyberbezpieczne Wodociągi” – Krajowy Plan Odbudowy i Zwiększania Odporności finansowany ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności, Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo Cyberbezpieczeństwo – Cyberbezpieczne Wodociągi. Konkurs grantowy pn.” Cyberbezpieczne Wodociągi” o numerze KPOD.05.10-CW.01-001/25/0370/KPOD.0510-CW.01-001/25/2026

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, wdrożenie i konfiguracja rozwiązań podnoszących poziom cyberbezpieczeństwa infrastruktury technologicznej (OT) Zamawiającego, zgodnie z wymaganiami programu Cyberbezpieczne Wodociągi, KSC, NIS2 oraz dobrymi praktykami bezpieczeństwa przemysłowego ISA/IEC 62443.

2. Zakres zamówienia

2.1 Dostawa przełączników zarządzalnych OT

- dostawa 3 szt. przełączników zarządzalnych,
- parametry techniczne zgodnie z OPZ,
- montaż, konfiguracja i uruchomienie,
- wykonanie dokumentacji powdrożeniowej.

2.2 Usługa segmentacji sieci OT

Zakres obejmuje:

- audyt i inwentaryzację istniejącej infrastruktury OT,
- opracowanie projektu segmentacji sieci,
- wydzielenie stref bezpieczeństwa i VLAN,

- konfigurację urządzeń sieciowych,
- konfigurację firewalli i ACL,
- przygotowanie matrycy przepływów,
- wykonanie testów separacji środowisk,
- opracowanie dokumentacji powykonawczej.

2.3 Dostawa i uruchomienie serwera kopii zapasowych OT

Zakres obejmuje:

- dostawę serwera zgodnego z wymaganiami OPZ,
- instalację w szafie RACK,
- konfigurację RAID,
- konfigurację systemu operacyjnego,
- konfigurację repozytorium kopii bezpieczeństwa,
- przygotowanie procedur odtwarzania danych,
- przeprowadzenie testów odtworzeniowych.

2.4 Wdrożenie i optymalizacja systemu SIEM/XDR Wazuh

Zakres obejmuje:

- audyt istniejącej instalacji Wazuh,
- rekonfigurację i optymalizację rozwiązania,
- hardening środowiska SIEM,
- integrację źródeł logów OT,
- konfigurację reguł korelacyjnych,
- konfigurację dashboardów,
- konfigurację alertowania,
- przygotowanie dokumentacji,
- szkolenie administratora.

2.5 Wdrożenie stacji przesiadkowej (Bastion Host) dla środowiska OT

Zakres obejmuje:

- utworzenie maszyny wirtualnej,
- wdrożenie rozwiązania typu Bastion Host/PAM dla OT,
- konfigurację bezpiecznego dostępu SSH i RDP,
- konfigurację nagrywania sesji,
- centralne logowanie zdarzeń,
- integrację z SIEM,
- testy funkcjonalne i bezpieczeństwa,
- dokumentację powykonawczą.

3. Produkty końcowe

Wykonawca wraz z realizacją przekaże:

- dokumentację projektową,
- dokumentację powdrożeniową,
- instrukcje administracyjne,
- wyniki testów,
- protokoły odbioru,
- szkolenie administratorów.

3. Warunki udziału

O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy:

a) posiadają uprawnienia do wykonywania działalności objętej zamówieniem,
b) dysponują odpowiednim potencjałem technicznym i kadrowym,
c) znajdują się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia,
d) minimum 3 zrealizowane projekty o wartości min. 250 000 zł brutto związane z wdrożeniami SIEM,
e) certyfikat ISO/IEC 27001 lub równoważny,
f) kierownik projektu z certyfikacją PRINCE2/AgilePM/PMP/IPMA,
g) kwalifikacje w zakresie usług dotyczących systemów informatycznych potwierdzone certyfikatem ITIL 3 Expert Certificate in IT Service Management lub równoważny. Za certyfikat równoważny Zamawiajacy uzna np. ITIL 4 Managing Professional lub ITIL 4 Strategic Leader
a) specjaliści wdrożeniowi z doświadczeniem SIEM,
inżynier systemów bezpieczeństwa z doświadczeniem w projektach SIEM

4. Kryteria oceny ofert

Cena oferty brutto 100 pkt,

Za najkorzystniejszą zostanie uznana oferta, która uzyska najwyższą liczbę punktów.

5.Sposób przygotowania oferty

Oferta powinna zawierać:

1. Załącznik nr 1 - formularz ofertowy.
2. Dokumenty potwierdzające doświadczenie, cetryfikaty.
3. Załącznik nr 3 - oświadczenie Wykonawcy.

6. Termin składania ofert

Ofertę podpisaną w formie elektronicznej należy złożyć do dnia 16.11.2026r. Do godz. 09:00 na platformie Baza Usług Konkurencyjności

7. Termin realizacji

Do 21.12.2026r.

Zamawiający zastrzega, iż przedmiotowe zapytanie może zostać unieważnione przez Zamawiającego na każdym etapie zbierania i weryfikacji złożonych ofert, z uwagi na fakt, iż przedmiot zapytania finansowany ze środków zewnętrznych obarczony jest możliwością uzyskania negatywnej oceny finansowania.

II. Opis przedmiotu zamówienia

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, wdrożenie, konfiguracja oraz uruchomienie rozwiązań technicznych i organizacyjnych mających na celu podniesienie poziomu cyberbezpieczeństwa

infrastruktury technologicznej (OT) eksploatowanej przez Zamawiającego. Realizacja zamówienia ma przyczynić się do zwiększenia odporności systemów odpowiedzialnych za realizację procesów technologicznych, ograniczenia ryzyka wystąpienia incydentów bezpieczeństwa oraz zapewnienia zgodności z wymaganiami ustawy o krajowym systemie cyberbezpieczeństwa, Dyrektywy NIS2 oraz dobrymi praktykami bezpieczeństwa systemów automatyki przemysłowej.
Zakres zamówienia obejmuje modernizację warstwy sieciowej środowiska OT, wykonanie segmentacji sieci przemysłowej, wdrożenie bezpiecznego dostępu administracyjnego, rozbudowę systemu monitorowania zdarzeń bezpieczeństwa oraz wdrożenie infrastruktury przeznaczonej do wykonywania i przechowywania kopii bezpieczeństwa.

2. Dostawa i wdrożenie przełączników zarządzalnych
W ramach realizacji zamówienia Wykonawca dostarczy, skonfiguruje oraz uruchomi trzy zarządzalne przełączniki sieciowe przeznaczone do pracy w środowisku przemysłowym lub środowisku o podwyższonych wymaganiach w zakresie niezawodności i bezpieczeństwa.
Oferowane urządzenia będą stanowiły podstawę projektowanej architektury segmentacji sieci OT oraz umożliwią wdrożenie mechanizmów kontroli ruchu sieciowego pomiędzy poszczególnymi strefami bezpieczeństwa.
Dostarczone przełączniki muszą posiadać nie mniej niż 48 portów 10/100/1000Base-T, co najmniej 4 porty SFP+ 10 Gb/s oraz przepustowość przełączania nie mniejszą niż 300 Gbps. Urządzenia muszą wspierać mechanizmy VLAN 802.1Q, ACL, QoS, SNMPv3, 802.1X, RSTP/MSTP oraz funkcje centralnego zarządzania i monitorowania. Każdy przełącznik powinien zapewniać budżet zasilania PoE nie mniejszy niż 360 W.
W ramach wdrożenia Wykonawca zobowiązany będzie do wykonania aktualizacji oprogramowania układowego urządzeń, konfiguracji zgodnie z projektem segmentacji, wdrożenia rekomendowanych ustawień bezpieczeństwa oraz przygotowania dokumentacji powdrożeniowej zawierającej konfigurację urządzeń i sposób ich administracji.

3. Usługa segmentacji sieci OT
Celem zadania jest ograniczenie ryzyka nieautoryzowanego przemieszczania się zagrożeń pomiędzy poszczególnymi obszarami infrastruktury oraz wdrożenie architektury bezpieczeństwa zgodnej z zasadą podziału na strefy bezpieczeństwa.
W ramach realizacji usługi Wykonawca przeprowadzi analizę istniejącej infrastruktury teleinformatycznej i automatyki przemysłowej obejmującą identyfikację urządzeń, systemów, usług oraz przepływów komunikacyjnych funkcjonujących w środowisku OT. Na podstawie przeprowadzonej analizy opracowany zostanie projekt segmentacji logicznej sieci, obejmujący wydzielenie stref bezpieczeństwa, określenie relacji komunikacyjnych pomiędzy strefami oraz przygotowanie matrycy dozwolonej komunikacji.
Po akceptacji projektu Wykonawca przeprowadzi wdrożenie zaprojektowanych mechanizmów segmentacji poprzez konfigurację przełączników sieciowych, utworzenie odpowiednich sieci VLAN, wdrożenie list kontroli dostępu oraz innych mechanizmów ograniczających komunikację do połączeń uzasadnionych technologicznie oraz przeprowadzi inwentaryzację zasobów teleinformatycznych na obiektach SUW.
Efektem prac będzie udokumentowana i zweryfikowana architektura sieci OT spełniająca wymagania bezpieczeństwa oraz umożliwiająca dalszą rozbudowę środowiska.

4. Dostawa i wdrożenie serwera kopii zapasowych

Przedmiotem zadania jest dostarczenie i uruchomienie dedykowanego serwera przeznaczonego do przechowywania kopii bezpieczeństwa systemów oraz danych funkcjonujących w środowisku OT.

Serwer musi zostać dostarczony jako kompletne rozwiązanie sprzętowe i posiadać parametry nie gorsze niż określone w dokumentacji projektowej, w szczególności procesor klasy serwerowej wyposażony w minimum 24 rdzenie obliczeniowe, co najmniej 64 GB pamięci RAM DDR5, sprzętowy kontroler RAID oraz konfigurację dyskową umożliwiającą realizację macierzy RAID1 dla systemu operacyjnego i RAID6 dla danych backupowych. Łączna liczba dysków przeznaczonych do przechowywania danych nie może być mniejsza niż dziesięć sztuk o pojemności 4 TB każda.

W ramach realizacji zamówienia Wykonawca dokona montażu urządzenia, konfiguracji macierzy dyskowych, uruchomienia systemu operacyjnego, przygotowania przestrzeni backupowej, konfiguracji harmonogramów wykonywania kopii bezpieczeństwa oraz przeprowadzenia testów odtworzeniowych potwierdzających poprawność działania rozwiązania.

5. Audyt, rekonfiguracja i optymalizacja środowiska SIEM Wazuh

Zamawiający posiada wdrożone środowisko systemu klasy SIEM oparte o platformę Wazuh. Celem zamówienia nie jest zakup nowego rozwiązania, lecz doprowadzenie istniejącej instalacji do pełnej gotowości produkcyjnej oraz zwiększenie jej skuteczności w zakresie monitorowania zdarzeń bezpieczeństwa.

W ramach realizacji zadania Wykonawca przeprowadzi analizę istniejącej konfiguracji, zweryfikuje architekturę systemu, dokona przeglądu aktualnych źródeł logów oraz oceni skuteczność działania wdrożonych mechanizmów monitorowania.

Na podstawie wyników audytu przeprowadzona zostanie rekonfiguracja i optymalizacja środowiska obejmująca wdrożenie dobrych praktyk bezpieczeństwa, konfigurację mechanizmów Active Response, opracowanie reguł korelacyjnych, przygotowanie dashboardów operacyjnych oraz integrację co najmniej pięciu niestandardowych źródeł logów wykorzystywanych przez Zamawiającego.

W rezultacie Zamawiający otrzyma kompletną dokumentację administracyjną, procedury eksploatacyjne oraz przeszkolenie administratorów odpowiedzialnych za utrzymanie systemu.

6. Wdrożenie stacji przesiadkowej (Bastion Host)

W celu zapewnienia bezpiecznego dostępu administracyjnego do systemów technologicznych Wykonawca wdroży rozwiązanie typu Bastion Host stanowiące centralny punkt dostępu do zasobów środowiska OT.

Rozwiązanie musi umożliwiać realizację połączeń administracyjnych wykorzystujących protokoły SSH oraz RDP, a także zapewniać pełną rejestrację i archiwizację aktywności użytkowników posiadających dostęp uprzywilejowany. Wdrożone rozwiązanie powinno wspierać mechanizmy wieloskładnikowego uwierzytelniania, integrację z usługą katalogową, czasowe przyznawanie uprawnień oraz generowanie raportów dotyczących wykorzystania kont administracyjnych.

System musi umożliwiać rejestrowanie i odtwarzanie sesji administracyjnych oraz przekazywanie informacji o zdarzeniach bezpieczeństwa do środowiska SIEM eksploatowanego przez Zamawiającego.