Ogłoszenie o wyniku postępowania
Usługi
Wdrożenie usług z zakresu cyberbezpieczeństwa

SEKCJA I - ZAMAWIAJĄCY

1.1.) Rola zamawiającego
Postępowanie prowadzone jest samodzielnie przez zamawiającego

1.2.) Nazwa zamawiającego: Gmina Rudniki

1.4) Krajowy Numer Identyfikacyjny: REGON 151398586

1.5) Adres zamawiającego

1.5.1.) Ulica: Wojska Polskiego 12A

1.5.2.) Miejscowość: Rudniki

1.5.3.) Kod pocztowy: 46-325

1.5.4.) Województwo: opolskie

1.5.5.) Kraj: Polska

1.5.6.) Lokalizacja NUTS 3: PL524 - Opolski

1.5.7.) Numer telefonu: 34 3595072

1.5.9.) Adres poczty elektronicznej: przetargi@rudniki.pl

1.5.10.) Adres strony internetowej zamawiającego: www.rudniki.pl

1.6.) Adres strony internetowej prowadzonego postępowania:
https://platformazakupowa.pl/pn/rudniki

1.7.) Rodzaj zamawiającego: Zamawiający publiczny - jednostka sektora finansów publicznych - jednostka samorządu terytorialnego

1.8.) Przedmiot działalności zamawiającego: Ogólne usługi publiczne

SEKCJA II – INFORMACJE PODSTAWOWE

2.1.) Ogłoszenie dotyczy:

Zamówienia publicznego

2.2.) Ogłoszenie dotyczy usług społecznych i innych szczególnych usług: Nie

2.3.) Nazwa zamówienia albo umowy ramowej:
Wdrożenie usług z zakresu cyberbezpieczeństwa

2.4.) Identyfikator postępowania: ocds-148610-d1a3e970-e9b9-4c73-b1c9-4c72f0df7482

2.5.) Numer ogłoszenia: 2024/BZP 00524820

2.6.) Wersja ogłoszenia: 01

2.7.) Data ogłoszenia: 2024-10-01

2.8.) Zamówienie albo umowa ramowa zostały ujęte w planie postępowań: Tak

2.9.) Numer planu postępowań w BZP: 2023/BZP 00577880/13/P

2.10.) Identyfikator pozycji planu postępowań:

1.3.2 Wdrożenie usług z zakresu cyberbezpieczeństwa

2.11.) Czy zamówienie albo umowa ramowa dotyczy projektu lub programu współfinansowanego ze środków Unii Europejskiej: Tak

2.12.) Nazwa projektu lub programu:
Cyberbezpieczny samorząd", który jest realizowany w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021 – 2027 (FERC) Działanie 2.2 - Wzmocnienie krajowego systemu cyberbezpieczeństwa.

2.13.) Zamówienie/umowa ramowa było poprzedzone ogłoszeniem o zamówieniu/ogłoszeniem o zamiarze zawarcia umowy: Tak

2.14.) Numer ogłoszenia: 2024/BZP 00488989

SEKCJA III – TRYB UDZIELENIA ZAMÓWIENIA LUB ZAWARCIA UMOWY RAMOWEJ

3.1.) Tryb udzielenia zamówienia wraz z podstawą prawną Zamówienie udzielane jest w trybie podstawowym na podstawie: art. 275 pkt 1 ustawy

SEKCJA IV – PRZEDMIOT ZAMÓWIENIA

4.1.) Numer referencyjny: PRG.271.15.2024

4.2.) Zamawiający udziela zamówienia w częściach, z których każda stanowi przedmiot odrębnego postępowania: Nie

4.3.) Wartość zamówienia: 223577 PLN

4.4.) Rodzaj zamówienia: Usługi

Część 1

4.5.1.) Krótki opis przedmiotu zamówienia
Część I: Świadczenie usług utrzymania środowiska SIEM/SOC wraz z dostawą i wdrożeniem serwera:
1) Świadczenie usług utrzymania systemu Zarządzania Informacjami i Zdarzeniami Bezpieczeństwa (SIEM) oraz Centrum Operacji Bezpieczeństwa (SOC)
a) Skonfigurowanie w ramach platformy witalizacyjnej funkcjonalności kopii zapasowych i odzyskiwania plików i danych oprogramowania dla środowiska SIEM/SOC
b) Opracowanie i wdrożenie planu zarządzania podatnościami. Wykonawca opracuje i przedstawi plan działania na wypadek krytycznych incydentów bezpieczeństwa, który będzie obejmował:
i. Procedury natychmiastowej reakcji na incydenty,
ii. Procedury powiadamiania odpowiednich służb i zespołów reagowania,
iii. Plany przywracania działania systemów po incydentach,
iv. Procedury analizy incydentów po ich wystąpieniu oraz wdrażania działań zapobiegawczych.
c) Monitorowanie, analiza oraz odpowiedź na incydenty bezpieczeństwa w postaci przekazania pełnej informacji do zespołu IT Zleceniodawcy
d) Sporządzanie okresowych raportów:
i. Comiesięczne raporty szczegółowe z działania systemu SOC/SIEM (20 raportów w ciągu 20 miesięcy)
ii. Kwartalne raporty podsumowujące (1-2 strony) z zaleceniami
e) Wdrożenie zaleceń z raportów kwartalnych, wykonane przez 2-osobowy zespół Wykonawcy w ścisłej współpracy z zespołem IT Zamawiającego
2) Dostawa i wdrożenie serwera wraz z oprogramowaniem dla środowiska SIEM/SOC – obejmujące dostawę, instalację oraz konfigurację sprzętu komputerowego, zgodnie z określoną specyfikacją techniczną.
Szczegółowy opis znajduje się się w Opisie przedmiotu zamówienia - załącznik nr 6 do SWZ.

4.5.3.) Główny kod CPV: 72611000-6 - Usługi w zakresie wsparcia technicznego

4.5.4.) Dodatkowy kod CPV:

72250000-2 - Usługi w zakresie konserwacji i wsparcia systemów

30211000-1 - Komputery wysokowydajne

4.5.5.) Wartość części: 85366 PLN

Część 2

4.5.1.) Krótki opis przedmiotu zamówienia
Część II: Audyt bezpieczeństwa infrastruktury IT zgodny z wymogami Krajowymi Ramami Interoperacyjności (KRI) oraz wdrożenie zaleceń poaudytowych:
1) Audyt bezpieczeństwa infrastruktury IT:
a) Przegląd i analiza aktualnej infrastruktury IT
i. Dokumentacja i schematy topologii sieci
ii. Inwentaryzacja urządzeń i systemów
b) Przegląd architektury sieci pod kątem bezpieczeństwa teleinformatycznego
i. Analiza segmentacji sieci
ii. Ocena mechanizmów kontroli dostępu
c) Ocena polityk bezpieczeństwa i procedur, w szczególności przeprowadzenie audytu polityki kopii zapasowych i backup-ów, audyt procedur na wypadek awarii

i. Przegląd polityk zarządzania hasłami
ii. Ocena procedur zarządzania incydentami
d) Testy penetracyjne wewnętrzne i analiza podatności
i. Analiza zabezpieczeń urządzeń sieciowych
ii. Analiza podatności systemów operacyjnych
iii. Testy aplikacji webowych i usług sieciowych
e) Testy penetracyjne zewnętrzne i analiza podatności
i. Testy zabezpieczeń firewalli i routerów
ii. Symulacja ataków z zewnątrz
f) Przegląd konfiguracji urządzeń sieciowych i usług
i. Ocena zabezpieczeń protokołów sieciowych
ii. Sprawdzenie konfiguracji urządzeń pod kątem zgodności z najlepszymi praktykami
g) Ocena zgodności z KRI
2) Przygotowanie raportu z audytu:
a) Szczegółowy raport zawierający wyniki audytu
b) Wizualizacja luk i podatności na schematach sieci
c) Identyfikacja luk i podatności w systemach wraz z wyjaśnieniem ich znaczenia i oceną ryzyka (prawdopodobieństwo/zagrożenie)
d) Określenie priorytetów dla działań naprawczych
e) Wnioski i rekomendacje w celu dokładnego rozpoznania i redukcji zidentyfikowanych ryzyka, zagrożeń i podatności oraz wskazanie adekwatnych działań (zaleceń) mających na celu jak najszybsze ich wyeliminowanie
3) Wdrożenie zaleceń, wykonane przez 3-osobowy zespół Wykonawcy w ścisłej współpracy z zespołem IT Zamawiającego:
a) Analiza możliwości technicznych implementacji zaleceń, pod względem urządzeń, konfiguracji, licencji, ciągłości działania sieci i ciągłości dostępu do usług.
b) Dostosowanie infrastruktury do wdrożenia zaleceń
i. Modyfikacja konfiguracji sieci
ii. Aktualizacja oprogramowania i firmware'u
c) Przygotowanie scenariuszy wdrożenia zaleceń, wraz z procedurami roll-back
d) Wykonanie kopii zapasowych wraz z testami odtworzeniowymi
e) Kontrolowane wdrożenie zaleceń w oknach serwisowych (22:00 – 6:00)
f) Monitorowanie i weryfikacja wdrożonych zaleceń
4) Przygotowanie raportu z wdrożenia zaleceń
Szczegółowy opis znajduje się się w Opisie przedmiotu zamówienia - załącznik nr 6 do SWZ.

4.5.3.) Główny kod CPV: 72800000-8 - Usługi audytu komputerowego i testowania komputerów

4.5.5.) Wartość części: 88618 PLN

Część 3

4.5.1.) Krótki opis przedmiotu zamówienia
Część III: Usługa szkoleniowa z zakresu Cyberbezpieczeństwa:
Przedmiotem zamówienia jest przeprowadzenie 12 szkoleń z tematyki Cyberbezpieczeństwa na przestrzeni 18 miesięcy:
1) ABC Cyberbezpieczeństwa, czas trwania: 2h zegarowe, 4 szkolenia
2) Liderzy Cyberbezpieczeństwa: Szkolenie dla Zarządu, czas trwania: 2h zegarowe, 4 szkolenia
3) Bezpieczeństwo Infrastruktury IT, czas trwania: 2h zegarowe, 4 szkolenia
Szczegółowy opis znajduje się się w Opisie przedmiotu zamówienia - załącznik nr 6 do SWZ.

4.5.3.) Główny kod CPV: 80500000-9 - Usługi szkoleniowe

4.5.5.) Wartość części: 19919 PLN

Część 4

4.5.1.) Krótki opis przedmiotu zamówienia
Część IV: Zabezpieczenie infrastruktury IT – Device Hardening:
Przedmiotem zamówienia jest usługa zabezpieczenia infrastruktury IT poprzez zastosowanie procesu device hardening (uszczelnienia urządzeń) w celu zwiększenia odporności na potencjalne zagrożenia. Usługa obejmuje szereg działań mających na celu zmniejszenie powierzchni ataku oraz wdrożenie mechanizmów ochrony w urządzeniach takich jak: Serwery fizyczne i wirtualne (do 4 sztuk),Routery i firewalle (do 4 sztuk), Przełączniki sieciowe L2 i L3 (do 12 sztuk), Inne urządzenia sieciowe (drukarki, kamery IP, itp.) (do 5 sztuk). Usługa device hardening obejmuje następujące działania:
1) Analiza i inwentaryzacja urządzeń:
a) Identyfikacja wszystkich urządzeń wchodzących w skład infrastruktury IT
b) Określenie typu, modelu, systemu operacyjnego i roli każdego urządzenia
c) Analiza konfiguracji urządzeń pod kątem potencjalnych luk w zabezpieczeniach
2) Opracowanie planu zabezpieczeń:
a) Opracowanie indywidualnego planu device hardening dla każdego typu urządzenia
b) Uwzględnienie specyfiki i wymagań poszczególnych urządzeń oraz całej infrastruktury

c) Konsultacje z Zamawiającym w celu dostosowania planu do jego potrzeb
3) Wdrożenie zabezpieczeń:
a) Wyłączenie zbędnych usług i protokołów
b) Aktualizacja oprogramowania i firmware'u do najnowszych wersji
c) Utworzenie i egzekwowanie polityki silnych haseł
d) Wdrożenie mechanizmów uwierzytelniania dwuskładnikowego (2FA)
e) Konfiguracja logowania i monitorowania zdarzeń
f) Wdrożenie mechanizmów ochrony przed atakami DDoS
g) Inne działania mające na celu zwiększenie bezpieczeństwa urządzeń
4) Testowanie i weryfikacja:
a) Przeprowadzenie testów penetracyjnych w celu weryfikacji skuteczności wdrożonych zabezpieczeń
b) Analiza wyników testów i ewentualne wprowadzenie dodatkowych zabezpieczeń
c) Sporządzenie raportu z testów i rekomendacji
Szczegółowy opis znajduje się się w Opisie przedmiotu zamówienia - załącznik nr 6 do SWZ.

4.5.3.) Główny kod CPV: 72250000-2 - Usługi w zakresie konserwacji i wsparcia systemów

4.5.5.) Wartość części: 29674 PLN

SEKCJA V ZAKOŃCZENIE POSTĘPOWANIA

Część 1

SEKCJA V ZAKOŃCZENIE POSTĘPOWANIA (dla części 1)

5.1.) Postępowanie zakończyło się zawarciem umowy albo unieważnieniem postępowania: Postępowanie/cześć postępowania zakończyła się unieważnieniem

5.2.) Podstawa prawna unieważnienia postępowania: art. 255 pkt 2 ustawy

5.2.1.) Przyczyna unieważnienia postępowania:

Wszystkie oferty zostały odrzucone.

Część 2

SEKCJA V ZAKOŃCZENIE POSTĘPOWANIA (dla części 2)

5.1.) Postępowanie zakończyło się zawarciem umowy albo unieważnieniem postępowania: Postępowanie/cześć postępowania zakończyła się unieważnieniem

5.2.) Podstawa prawna unieważnienia postępowania: art. 255 pkt 2 ustawy

5.2.1.) Przyczyna unieważnienia postępowania:

Wszystkie oferty zostały odrzucone

Część 3

SEKCJA V ZAKOŃCZENIE POSTĘPOWANIA (dla części 3)

5.1.) Postępowanie zakończyło się zawarciem umowy albo unieważnieniem postępowania: Postępowanie/cześć postępowania zakończyła się unieważnieniem

5.2.) Podstawa prawna unieważnienia postępowania: art. 255 pkt 2 ustawy

5.2.1.) Przyczyna unieważnienia postępowania:

Wszystkie oferty zostały odrzucone

Część 4

SEKCJA V ZAKOŃCZENIE POSTĘPOWANIA (dla części 4)

5.1.) Postępowanie zakończyło się zawarciem umowy albo unieważnieniem postępowania: Postępowanie/cześć postępowania zakończyła się unieważnieniem

5.2.) Podstawa prawna unieważnienia postępowania: art. 255 pkt 2 ustawy

5.2.1.) Przyczyna unieważnienia postępowania:

Wszystkie oferty zostały odrzucone.