



Przedsiębiorstwo Wodociągów i Kanalizacji Sp. z o.o. w Gorzowie Wielkopolskim

OPIS PRZEDMIOTU ZAMÓWIENIA

I. Przedmiot zamówienia.

Przedmiotem zamówienia są:

Usługi doradcze, wsparcie w pozyskaniu grantu w ramach programu „Cyberbezpieczne wodociągi” w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

II. Przedmiot zamówienia obejmuje w szczególności:

1. Przygotowanie koncepcji projektu w oparciu o przeprowadzoną analizę ryzyka dla systemów IT i OT. Określenie potrzeb Zamawiającego w zakresie wzmocnienia cyberodporności systemów informacyjnych IT i OT, w tym do zwiększenia bezpieczeństwa, ciągłości działania oraz zwiększenia wydajności. Wyznaczenie celów i efektach projektu, w tym w odniesieniu do celów Funduszy Europejskich, przy zapewnieniu zgodności projektu z zasadami konkursu i wniosku o grant.
 - a) Analiza ryzyka przeprowadzona w oparciu o aktualne standardy i metodyki np. normę ISO 27005, ISO 31000, COBIT, NIST - identyfikacja i inwentaryzacja aktywów, zidentyfikowanie potencjalnych zagrożeń, określenie podatności, luk w zabezpieczeniach systemów IT i OT, a także ocena skuteczności obecnych procedur i polityk bezpieczeństwa w zakresie dostępności, poufności i integralności. Określenie ryzyka – wpływu podatności. (Analiza systemów informatycznych, w tym infrastruktura sprzętowa, serwerowa, sieciowa, aplikacje, bazy danych, systemy zarządzania, procedury backupowe, analiza systemów sterowania i monitorowania w infrastrukturze wodociągowej i kanalizacyjnej, w tym systemów SCADA, PLC, czujników oraz urządzeń końcowych).
 - b) Zidentyfikowanie zagrożeń i podatności - ryzyk: Opracowanie listy ryzyk związanych z bezpieczeństwem IT i OT, takich jak ataki cybernetyczne, awarie systemów, zagrożenia ludzkie, zagrożenia fizyczne czy zagrożenia administracyjne.
 - c) Zalecenia: Sformułowanie raportu z rekomendacjami i potrzebami dotyczącymi wzmocnienia cyberodporności systemów informacyjnych IT i OT, w tym do zwiększenia bezpieczeństwa, ciągłości działania oraz zwiększenia wydajności, które powinny być dostosowane do specyfiki przedsiębiorstwa i jego infrastruktury.
2. Na podstawie zidentyfikowanych ryzyk i potrzeb opracowanie we współpracy z Zamawiającym zakresu projektu możliwego do sfinansowania w ramach grantu, realizowanego w ramach programu „Cyberbezpieczne wodociągi” w podziale na cele:

- 1) wdrożenie środków organizacyjnych służących zapewnieniu cyberbezpieczeństwa;
- 2) zakup lub modernizację środków technicznych służących zapewnieniu cyberbezpieczeństwa;
- 3) rozwój kompetencji personelu w zakresie cyberbezpieczeństwa.

Działania jakie m.in. mogą być finansowane w ramach obszaru 1) to:

- przegląd, aktualizacja lub opracowanie i wdrożenie systemu zarządzania bezpieczeństwem informacji,
- wprowadzenie środków obejmujących m.in.: politykę analizy ryzyka i bezpieczeństwa systemów informatycznych, obsługę incydentu, ciągłość działania i zarządzanie kryzysowe, polityki i procedury stosowania kryptografii i szyfrowania, politykę kontroli dostępu, stosowanie uwierzytelniania wieloskładnikowego,
- audyt systemu zarządzania bezpieczeństwem informacji przeprowadzonego przez wykwalifikowanego audytora, stanowiącego dowód wdrożenia i stosowania ww. systemu w organizacji lub instytucji.

Działania jakie m.in. mogą być finansowane w ramach obszaru 2) to:

- zakup i wdrożenie systemów teleinformatycznych, w tym urządzeń, oprogramowania i usług zapewniających prewencję, reakcję i detekcję zagrożeń cyberbezpieczeństwa,
- usługi wdrożenia i konfiguracji urządzeń i oprogramowania oraz wsparcia eksperckiego w zakresie cyberbezpieczeństwa,
- zakup i wdrożenie systemów lub usług na potrzeby operacyjnych centrów bezpieczeństwa (SOC),
- zakup lub rozwój systemów lub usług zarządzania podatnościami i skanerów podatności.

Działania jakie m.in. mogą być finansowane w ramach obszaru 3) to:

- szkolenia z zakresu cyberbezpieczeństwa dla kadry danego podmiotu istotnej z punktu widzenia wdrożonej polityki cyberbezpieczeństwa lub systemu zarządzania bezpieczeństwem informacji, w tym w szczególności w zakresie środków wdrażanych w ramach przedsięwzięcia,
- szkolenia z zakresu cyberbezpieczeństwa dla: informatyków odpowiedzialnych za cyberbezpieczeństwo, kadry kierowniczej oraz pozostałych pracowników podmiotu, obejmujących m.in. symulowane cyberataki na użytkowników sieci i systemów informacyjnych w organizacji (np. phishing).

3. Przygotowanie kompletnego wniosku o grant zgodnego z ROZPORZĄDZENIEM MINISTRA CYFRYZACJI w sprawie udzielania pomocy de minimis na wsparcie przedsiębiorstw wodociągowo-kanalizacyjnych objętych krajowym systemem cyberbezpieczeństwa w ramach Krajowego Planu Odbudowy i Zwiększania Odporności (aktualny projekt rozporządzenia, uzasadnienie, ocena skutków regulacji w załączeniu) oraz warunkami i zakresem określonym w regulaminie konkursu.
4. Reagowanie na każde wezwanie Grantodawcy, na etapie oceny złożonego wniosku, udzielanie szczegółowych wyjaśnień, uzupełnień, korekt w terminach wskazanych przez Grantodawcę.

III. Informacje o Zamawiającym dostępne są na:

1. <https://pwik.gorzow.pl>
2. <http://www.pwikgorzow.4bip.pl>

Załączniki:

1. Projekt ROZPORZĄDZENIA MINISTRA CYFRYZACJI w sprawie udzielania pomocy de minimis na wsparcie przedsiębiorstw wodociągowo-kanalizacyjnych objętych krajowym systemem cyberbezpieczeństwa w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.
<https://legislacja.gov.pl/projekt/12395454/katalog/13115605#13115605>
2. Uzasadnienie do rozporządzenia
3. Ocena skutków regulacji