Pytania wraz z odpowiedziami, jakie wpłynęły w odniesieniu do opublikowanego ogłoszenia BTI.271.2.91.2022

Otrzymane pytania i udzielone odpowiedzi:

1. Lokalizacja jednostek audytowanych (adres, adresy)

adresy: https://bip.um.swinoujscie.pl/ (trzy budynki)

https://bip.um.swinoujscie.pl/artykul/177/1156/wydzial-infrastruktury-i-zieleni-miejskiej-wiz (jeden budynek)

2. Ilość pracowników/użytkowników

280

3. Ilość wszystkich hostów podłączonych do sieci (komputery, urządzenia serwerowe, urządzenia sieciowe jak np. drukarki, routery, przełączniki, Access Pointy, urządzenia VoIP etc.). W tym rozgraniczyć:
   a. Ilość komputerów (również przenośnych)
   b. Ilość serwerów (fizycznych, wirtualnych)
   c. Ilość pozostałych urządzeń podłączonych do sieci

Prosimy o zweryfikowanie w czasie diagnozy/testów, również liczby stacji roboczych pracowników oraz instancji serwerowych (odp 2 i 5), podłączonych do sieci. Szczególnie pozostałych urządzeń.

4. Ilość podsieci (jaki zakres maski każdej podsieci?)

j.w.

5. Ilość serwerowni

4

6. Ilość adresów zewnętrznych

1 + zewnętrzny dostawca stron internetowych, + zewnętrzny dostawca poczty i ftp

7. Czy mają Państwo wdrożoną Active Directory?

tak

8. Jaki budżet (brutto) wpisali Państwo we wniosku grantowym na realizację samej Diagnozy cyberbezpieczeństwa z całej puli przydzielonych środków?

9583 pln brutto

9. Jeżeli chodzi o wymaganie „Doświadczenie w administracji publicznej" – czy na dowód doświadczenia wystarczą referencje z audytów bezpieczeństwa informacji KRI w jednostkach publicznych, w tym z Diagnozy cyberbezpieczeństwa (Urzędach Gmin, Miast, Pracy, Starostwach itp.)?

Tak. Pozytywne referencje, wraz z upoważnieniem osób wystawiających podpisane w sposób niebudzący zastrzeżeń (np. profilem zaufanym).

10. Jeżeli chodzi o „Techniczne wymagania" odnoszące się do załącznika 8 konkursu, arkusza CERT pkt 5, czy wystarczą referencje, które zawierają zakres Audytu KRI

oraz Testów penetracyjnych, które swoim zakresem w pełni weryfikują wszystkie informacje z załącznika 8 konkursu?

Tak. Pozytywne referencje po wykonaniu testów technicznych, wraz z upoważnieniem osób wystawiających podpisane w sposób niebudzący zastrzeżeń (np. profilem zaufanym).

11. Jakie uprawnienia musi posiadać wykonawca do realizacji zamówienia?

Do realizacji diagnozy cyberbezpieczeństwa / audytu, niezbędne są uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Wykaz certyfikatów wskazanych w w/w rozporządzeniu znajduje się poniżej:

1. **Certified Internal Auditor (CIA)**
2. **Certified Information System Auditor (CISA)**
3. **Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób**
4. **Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób**
5. **Certified Information Security Manager (CISM)**
6. **Certified in Risk and Information Systems Control (CRISC)**
7. **Certified in the Governance of Enterprise IT (CGEIT)**
8. **Certified Information Systems Security Professional (CISSP)**
9. **Systems Security Certified Practitioner (SSCP)**
10. **Certified Reliability Professional**
11. **Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert**