**Gmina Wojkowice**
**Ul. Jana III Sobieskiego 290a**
**42-580 Wojkowice**

WPM.271.33.2022

Wojkowice, 06 czerwca 2022r.

Do Wykonawców, biorących udział w postępowaniu o udzielenie zamówienia pn. **Przeprowadzenie diagnozy cyberbezpieczeństwa zgodnie z wytycznymi Konkursu Grantowego Cyfrowa Gmina**

**WYJAŚNIENIA TREŚCI OGŁOSZENIA O ZAMÓWIENIU**

W związku z zapytaniami o wyjaśnienie treści ogłoszenia o zamówieniu w postępowaniu o udzielenie zamówienia pn. **Przeprowadzenie diagnozy cyberbezpieczeństwa zgodnie z wytycznymi Konkursu Grantowego Cyfrowa Gmina** przekazuję ich teść wraz z wyjaśnieniami.

1. Ilość lokalizacji (adresy, info. co znajduje się pod danym adresem):
Odpowiedź. 1 lokalizacja; Urząd Miasta Wojkowice, ul. Jana III Sobieskiego 290a, 42-580 Wojkowice
2. Ilość pracowników/użytkowników:
Odpowiedź. 37 osób
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)
Odpowiedź. 40 komputerów
b. Ilość serwerów (fizycznych, wirtualnych)
Odpowiedź. 11 serwerów
c. Ilość pozostałych urządzeń podłączonych do sieci
Odpowiedź. 89 urządzeń
4. Ilość adresów zewnętrznych
Odpowiedź. 5 adresów zewnętrznych
5. Ilość podsieci (jaki zakres maski każdej podsieci?)
Odpowiedź. 4 maska /24
6. Ilość serwerowni i ich lokalizacja?
Odpowiedź. 1 lokalizacja; Urząd Miasta Wojkowice, ul. Jana III Sobieskiego 290a, 42-580 Wojkowice
7. Czy mają Państwo wdrożoną Active Directory?
Odpowiedź. Tak
8. Jaki budżet (brutto) wpisali Państwo we wniosku grantowym na realizację samej Diagnozy cyberbezpieczeństwa z całej puli przydzielonych środków?
Odpowiedź. 20 000,00 zł
9. Z jaką datą podpisali Państwo Umowę grantową?
Odpowiedź. 28.03.2022r.

10. Czy termin realizacji jest negocjowalny przed podpisaniem umowy jeżeli realizacja diagnozy w pełni zmieści się w 6 miesiącach od daty podpisania umowy grantowej?
Odpowiedź. Przed podpisaniem umowy termin nie podlega negocjacjom.
11. Czy poza wypełnieniem zał. 8 konkursu dla NASK wymagają Państwo również raportu z audytu dla Urzędu?
Odpowiedź. Tak
12. Odnosząc się do treści zał. 8 konkursu zawartej w arkuszu CERT (punkty od 3 do 6 włącznie), proszę o informacje czy posiadają Państwo Dokumentację oraz Raporty/Wyniki z audytów tam wskazane, aby było możliwe ich sprawdzenie/ocena podczas Diagnozy?
Czy oczekują Państwo wykonania podczas Diagnozy któregokolwiek z tych audytów lub opracowania dokumentacji – jeśli tak proszę o wskazanie konkretnych punktów z arkusza CERT, które ma opracować Wykonawca i uwzględnić taką informację jako oficjalną zmianę w treści zapytania. Poniżej lista z załącznika nr 8 konkursu (proszę o wpisanie czy Urząd posiada daną dokumentację, raporty oraz czy wymaga jej ewentualnego opracowania):

| 3 | **Dokumentacja Systemu Informacyjnego wspierającego zadanie publiczne** | **Tak** | **Nie** | **Opracowuje Wykonawca** |
|---|---|---|---|---|
| 3.1 | Czy istnieją raporty z audytów systemów informacyjnych wspierających zadanie publiczne? | | x | |
| 3.2 | Czy istnieje dokumentacja architektury zastosowanych zabezpieczeń? | | x | |
| 3.3 | Czy istnieje dokumentacja architektury sieci? | x | | |
| 3.4 | Czy istnieje baza danych konfiguracji urządzeń aktywnych? | x | | |
| 3.5 | Czy istnieje dokumentacja zmian w systemach informacyjnych? | | x | |
| 3.6 | Czy istnieje dokumentacja dotycząca monitorowania w trybie ciągłym? | | x | |
| 3.7 | Czy są dostępne umowy z dostawcami (wsparcie techniczne)? | x | | |
| 3.8 | Czy są zawierane umowy z dostawcami usług z zakresu bezpieczeństwa teleinformatycznego? | | x | |
| 3.9 | Czy są wymagane wyniki audytów u dostawców usług bezpieczeństwa teleinformatycznego? | | x | |
| 3.10 | Czy jest dostępna i aktualna dokumentacja zabezpieczeń fizycznych i środowiskowych? | x | | |
| 3.11 | Czy jest prowadzony rejestr dostępu do dokumentacji systemu informacyjnego? | | x | |
| 4 | **Dokumentacja procesu zarządzania incydentami** | | | |
| 4.1 | Czy wdrożone jest monitorowanie i wykrywanie incydentów? Kto za nie odpowiada? (stanowiska, funkcje itp. - bez danych osobowych) | x | | |
| 4.2 | Czy istnieje procedura informowania o wykrytych incydentach? | x | | |
| 4.3 | Czy istnieją procedury reagowania na incydenty? | x | | |
| 5 | **Aspekty techniczne do weryfikacji** | | | |
| 5.1 | Wyniki audytu serwisów WWW z uwzględnieniem:<br>- wersji serwera HTTP;<br>- wersji systemu CMS (o ile występuje);<br>- bezpieczeństwa komunikacji (aktualność certyfikatów X.509, wersja TLS, stosowane algorytmy kryptograficzne itp.);<br>- dostępności kompetentnego personelu do utrzymania serwisów. | x | | |

| | | | | |
|---|---|---|---|---|
| 5.2 | Wyniki audytu serwisów pocztowych z uwzględnieniem:<br>- poprawności wdrożenia mechanizmów SPF, DKIM i DMARC;<br>- poprawności i bezpieczeństwa wdrożenia mechanizmów TLS;<br>- dostępności kompetentnego personelu do utrzymania serwisów. | x | | |
| 5.3 | Wyniki audytu lokalnych sieci teleinformatycznych z uwzględnieniem:<br>- wdrożenia systemów ochrony przed kodem szkodliwym w sposób zapewniający ich automatyczną aktualizację;<br>- stosowania mechanizmów segmentacji sieci;<br>- izolacji urządzeń końcowych użytkowników;<br>- procesu tworzenia i okresowego odtwarzania kopii zapasowych przetwarzanych informacji;<br>- monitorowania ruchu wewnątrz sieci w zakresie wykrywania symptomów naruszeń bezpieczeństwa;<br>- dostępności kompetentnego personelu do utrzymania infrastruktury sieciowej. | x | | |
| 5.4 | Wyniki audytu połączenia z siecią Internet z uwzględnieniem:<br>- monitorowania ruchu wchodzącego i wychodzącego;<br>- stosowanych zabezpieczeń przed atakami DDoS;<br>- stosowanych zabezpieczeń przed wyciekiem informacji (DLP);<br>- stosowanych zabezpieczeń punktu styku (FW, IDS, IPS, WAF itp.);<br>- dostępności kompetentnego personelu do utrzymania punktu styku z siecią Internet. | x | | |
| 6 | **Aspekty organizacyjne do weryfikacji** | | | |
| 6.1 | Wyniki audytu organizacji zarządzania bezpieczeństwem teleinformatycznym z uwzględnieniem:<br>- regularnego identyfikowania znanych podatności w eksploatowanych systemach IT;<br>- terminowego wprowadzania danych do systemów zarządzania tożsamością i uprawnieniami użytkowników;<br>- prowadzenia okresowego przeglądu uprawnień użytkowników;<br>- prowadzenia okresowych szkoleń użytkowników podnoszących ich świadomość zagrożeń. | x | | |
| 6.2 | Wyniki audytu procesów planowania z uwzględnieniem:<br>- posiadania planów przywracania usług IT na wypadek awarii;<br>- prowadzenia przeglądów oraz doskonalenia planów przywracania usług IT;<br>- cyklu życia systemów IT i eksploatacji produktów nieposiadających wsparcia producenta. | | x | |

**Z upoważnienia Burmistrza**
**Sekretarz**
**/-/ Edyta Cichoń**