Informacja dla Wykonawców nr 1

Podtytuł: „Przeprowadzenie diagnozy cyberbezpieczeństwa w projekcie Cyfrowa Gmina w ramach Działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia" dotyczącego realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

Znak: RI. 271.06.2022.ZO.MP1 Pierzchnica dn. 07.06.2022 r.

Informacja dla Wykonawców nr 1

Dotyczy: Postępowania o udzielenie zamówienia na wykonanie zadania pn.: **„Przeprowadzenie diagnozy cyberbezpieczeństwa w projekcie Cyfrowa Gmina w ramach Działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia" dotyczącego realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00- 0001/21-00**

1. Ilość lokalizacji (adresy, info. co znajduje się pod danym adresem)

   Pozostałe dane poniżej proszę rozgraniczyć na <u>każdą lokalizację z osobna</u>, pozwoli to najdokładniej obliczyć czasochłonność i cenę projektu:

   <u>Jedna jednostka – Urząd Miasta i Gminy Pierzchnica, ul. Urzędnicza 6, 26-015 Pierzchnica</u>

   1. Ilość pracowników/użytkowników – ***<u>około 20</u>***
   2. Ilość <u>wszystkich hostów</u> 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) – ***<u>około 30</u>***
      b. Ilość serwerów (fizycznych, wirtualnych) – ***<u>około 12</u>***
      c. Ilość pozostałych urządzeń podłączonych do sieci – ***<u>około 70</u>***
   3. Ilość adresów zewnętrznych - ***<u>szczegółowe dane dostępne w trakcie realizacji audytu</u>***
   4. Ilość podsieci (jaki zakres maski każdej podsieci?) - ***<u>szczegółowe dane dostępne w trakcie realizacji audytu</u>***
   5. Ilość serwerowni i ich lokalizacja? - ***<u>1</u>***
   6. Czy mają Państwo wdrożoną Active Directory? – ***<u>TAK</u>***
   7. Jaki budżet (brutto) wpisali Państwo we wniosku grantowym na realizację samej Diagnozy cyberbezpieczeństwa z całej puli przydzielonych środków?- ***<u>5000 brutto</u>***
   8. Z jaką datą podpisali Państwo Umowę grantową? – ***<u>31.03.2022r.</u>***
   9. Czy termin realizacji jest negocjowalny przed podpisaniem umowy jeżeli realizacja diagnozy w pełni zmieści się w 6 miesiącach od daty podpisania umowy grantowej? - ***<u>NIE</u>***
   10. Czy poza wypełnieniem zał. 8 konkursu dla NASK wymagają Państwo również raportu z audytu dla Urzędu? - ***<u>TAK</u>***
   11. Odnosząc się do zapisu:

„Zamawiający nie dopuszcza wykonania diagnozy cyberbezpieczeństwa w sposób zdalny. Badanie zabezpieczeń, w tym przeprowadzenie wszelakich testów penetracyjnych sieci LAN, diagnozy cyberbezpieczeństwa, podatności systemów, wykonawca musi wykonać na miejscu w siedzibie Zamawiającego.”

Czy oczekują Państwo wykonania testów penetracyjnych, testów podatności i raportu z tych działań dla Urzędu? Jeśli tak to czy testy mają być wykonane na wszystkich hostach, podsieciach, adresach wskazanych w pytaniach 3-5, czy wybrana przez Państwa próba? Jeśli próba proszę podać ilości. - ***<u>metodologia audytu leży po stronie wykonawcy, zgodnie z wymaganiami z załącznika nr 6</u>***

1. 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 lub czy wymaga jej ewentualnego opracowania):

Załącznik nr 6 ma być kompletnym wynikiem przeprowadzonej diagnozy

3	**Dokumentacja Systemu Informacyjnego wspierającego zadanie publiczne**	**Tak**	**Nie**	**Opracowuje Wykonawca**
3.1	Czy istnieją raporty z audytów systemów informacyjnych wspierających zadanie publiczne?		**X**	**X**
3.2	Czy istnieje dokumentacja architektury zastosowanych zabezpieczeń?		**X**	**X**
3.3	Czy istnieje dokumentacja architektury sieci?		**X**	**X**
3.4	Czy istnieje baza danych konfiguracji urządzeń aktywnych?		**X**	**X**
3.5	Czy istnieje dokumentacja zmian w systemach informacyjnych?		**X**	**X**
3.6	Czy istnieje dokumentacja dotycząca monitorowania w trybie ciągłym?		**X**	**X**
3.7	Czy są dostępne umowy z dostawcami (wsparcie techniczne)?	**X**		**X**
3.8	Czy są zawierane umowy z dostawcami usług z zakresu bezpieczeństwa teleinformatycznego?	**X**		**X**
3.9	Czy są wymagane wyniki audytów u dostawców usług bezpieczeństwa teleinformatycznego?	**X**		**X**
3.10	Czy jest dostępna i aktualna dokumentacja zabezpieczeń fizycznych i środowiskowych?		**X**	**X**
3.11	Czy jest prowadzony rejestr dostępu do dokumentacji systemu informacyjnego?		**X**	**X**
4	**Dokumentacja procesu zarządzania incydentami**			**X**
4.2	Czy istnieje procedura informowania o wykrytych incydentach?	**X**		**X**
4.3	Czy istnieją procedury reagowania na incydenty?	**X**		**X**
5	**Aspekty techniczne do weryfikacji**			**X**
5.1	Wyniki audytu serwisów WWW z uwzględnieniem: - wersji serwera HTTP; - wersji systemu CMS (o ile występuje); - bezpieczeństwa komunikacji (aktualność certyfikatów X.509, wersja TLS, stosowane algorytmy kryptograficzne itp.); - dostępności kompetentnego personelu do utrzymania serwisów.		**X**	**X**
5.2	Wyniki audytu serwisów pocztowych z uwzględnieniem: - poprawności wdrożenia mechanizmów SPF, DKIM i DMARC; - poprawności i bezpieczeństwa wdrożenia mechanizmów TLS; - dostępności kompetentnego personelu do utrzymania serwisów.		**X**	**X**
5.3	Wyniki audytu lokalnych sieci teleinformatycznych z uwzględnieniem: - wdrożenia systemów ochrony przed kodem szkodliwym w sposób zapewniający ich automatyczną aktualizację; - stosowania mechanizmów segmentacji sieci; - izolacji urządzeń końcowych użytkowników; - procesu tworzenia i okresowego odtwarzania kopii zapasowych przetwarzanych informacji; - monitorowania ruchu wewnątrz sieci w zakresie wykrywania symptomów naruszeń bezpieczeństwa; - dostępności kompetentnego personelu do utrzymania infrastruktury sieciowej.		**X**	**X**

5.4	Wyniki audytu połączenia z siecią Internet z uwzględnieniem: - monitorowania ruchu wchodzącego i wychodzącego; - stosowanych zabezpieczeń przed atakami DDoS; - stosowanych zabezpieczeń przed wyciekiem informacji (DLP); - stosowanych zabezpieczeń punktu styku (FW, IDS, IPS, WAF itp.); - dostępności kompetentnego personelu do utrzymania punktu styku z siecią Internet.	**X**	**X**
6	**Aspekty organizacyjne do weryfikacji**		**X**
6.1	Wyniki audytu organizacji zarządzania bezpieczeństwem teleinformatycznym z uwzględnieniem: - regularnego identyfikowania znanych podatności w eksploatowanych systemach IT; - terminowego wprowadzania danych do systemów zarządzania tożsamością i uprawnieniami użytkowników; - prowadzenia okresowego przeglądu uprawnień użytkowników; - prowadzenia okresowych szkoleń użytkowników podnoszących ich świadomość zagrożeń.	**X**	**X**
6.2	Wyniki audytu procesów planowania z uwzględnieniem: - posiadania planów przywracania usług IT na wypadek awarii; - prowadzenia przeglądów oraz doskonalenia planów przywracania usług IT; - cyklu życia systemów IT i eksploatacji produktów nieposiadających wsparcia producenta.	**X**	**X**

(-) Stanisław Strąk

Burmistrz Miasta i Gminy Pierzchnica