Ciechanowiec, 24.06.2022 r.

Znak sprawy: OR.041.1.2022

WSZYSCY OFERENCI

Pytania o odpowiedzi dotyczące postępowania:

Przeprowadzenie diagnozy cyberbezpieczeństwa w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina" o numerze POPC.05.01.00-00-0001/21-00.

Pytanie z dnia 21-06-2022

Szanowni Państwo, Czy Zamawiający dopuszcza podpisanie umowy o dzieło z osobami fizycznymi?

Odpowiedź: **TAK**

Pytanie nr 1 z dnia 23-06-2022

Czy usługa może być wykonana on-line?

Odpowiedź: **NIE**

Pytania nr 2 z dnia 23-06-2022

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:

   Odpowiedź: **Jedna lokalizacja – Urząd Miejski w Ciechanowcu, ul. Mickiewicza 1, 18-230 Ciechanowiec**

2. Ilość pracowników/użytkowników
   Odpowiedź: **29**

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: **34**

b. Ilość serwerów (fizycznych, wirtualnych)
Odpowiedź: **0**

c. Ilość pozostałych urządzeń podłączonych do sieci
Odpowiedź: **21**

4. Ilość adresów zewnętrznych
Odpowiedź: **1**
5. Ilość podsieci (jaki zakres maski każdej podsieci?)
Odpowiedź: **1 (zakres 0-255)**
6. Ilość serwerowni i ich lokalizacja?
Odpowiedź: **Jedna serwerownia w budynku siedziby zamawiającego**
7. Czy mają Państwo wdrożoną Active Directory?
Odpowiedź: **NIE**
8. Jaki budżet (brutto) wpisali Państwo we wniosku grantowym na realizację samej Diagnozy cyberbezpieczeństwa z całej puli przydzielonych środków?
Odpowiedź: **Zamawiający odmawia udzielenia odpowiedzi na tym etapie postępowania, ponieważ byłoby to sprzeczne z zasadą konkurencyjności.**
9. Z jaką datą mają Państwo podpisaną Umowę grantową (chodzi o datę podpisu złożonego przez Grantodawcę)?
Odpowiedź: **02-02-2022**
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: **NIE**
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 KRI i CERT, proszę o informacje czy posiadają Państwo Dokumentację oraz Raporty/Wyniki z audytów tam wskazane, aby było możliwe ich sprawdzenie/ocena podczas Diagnozy?

3	**Dokumentacja Systemu Informacyjnego wspierającego zadanie publiczne**	**Tak**	**Nie**
3.1	Czy istnieją raporty z audytów systemów informacyjnych wspierających zadanie publiczne?		
3.2	Czy istnieje dokumentacja architektury zastosowanych zabezpieczeń?		
3.3	Czy istnieje dokumentacja architektury sieci?		
3.4	Czy istnieje baza danych konfiguracji urządzeń aktywnych?		
3.5	Czy istnieje dokumentacja zmian w systemach informacyjnych?		
3.6	Czy istnieje dokumentacja dotycząca monitorowania w trybie ciągłym?		
3.7	Czy są dostępne umowy z dostawcami (wsparcie techniczne)?		
3.8	Czy są zawierane umowy z dostawcami usług z zakresu bezpieczeństwa teleinformatycznego?		
3.9	Czy są wymagane wyniki audytów u dostawców usług bezpieczeństwa teleinformatycznego?		

3.10	Czy jest dostępna i aktualna dokumentacja zabezpieczeń fizycznych i środowiskowych?		
3.11	Czy jest prowadzony rejestr dostępu do dokumentacji systemu informacyjnego?		
4	**Dokumentacja procesu zarządzania incydentami**		
4.2	Czy istnieje procedura informowania o wykrytych incydentach?		
4.3	Czy istnieją procedury reagowania na incydenty?		
5	**Aspekty techniczne do weryfikacji**		
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.		
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.		
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.		
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.		
6	**Aspekty organizacyjne do weryfikacji**		
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.		
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.		

7	Opracowanie, ustanowienie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)		

Odpowiedź: **Zamawiający odmawia udzielenia odpowiedzi na to pytanie, ponieważ jego treść stanowi część zakresu zamówienia przeznaczoną do realizacji po podpisaniu umowy.**

Pytanie nr 3 z dnia 23-06-2022

Proszę o odpowiedź czy akceptują Państwo przeprowadzenie Diagnozy Cyberbezpieczeństwa w formie zdalnej czy konieczna jest fizyczna obecność audytora w Państwa siedzibie?

Odpowiedź: **Nie akceptujemy zdalnej formy przeprowadzenia Diagnozy Cyberbezpieczeństwa.**

Burmistrz

Eugeniusz Święcki

Eugeniusz Święcki

Elektronicznie podpisany przez Eugeniusz Święcki
Data: 2022.06.24 13:37:58 +02'00'