A-I.271.23.2022

Pytania do Zaproszenie do składania ofert w postępowaniu

„Diagnoza cyberbezpieczeństwa w projekcie Cyfrowa Gmina w ramach Działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia."

Pytanie 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:
Urząd posiada aktualnie sześć lokalizacji. Szczegółowe dane odnośnie lokalizacji zostaną udostępnione Wykonawcy. Poniżej orientacyjne dane zbiorcze dla wszystkich lokalizacji.

Pytanie 2. Ilość pracowników/użytkowników

Odpowiedź:
Liczba pracowników około 700.

Pytanie 3. 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)

Odpowiedź:
750

b. Ilość serwerów (fizycznych, wirtualnych)

Odpowiedź:
25, 100

c. Ilość pozostałych urządzeń podłączonych do sieci

Odpowiedź:
300

Pytanie 4. Ilość adresów zewnętrznych

Odpowiedź:
20

Pytanie 5. Ilość podsieci (jaki zakres maski każdej podsieci?)

Odpowiedź:
1 podsieć, maska /16

Pytanie 6. Ilość serwerowni i ich lokalizacja?

Odpowiedź:
Dwie

Pytanie 7. Czy mają Państwo wdrożoną Active Directory?

Odpowiedź:
Tak

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

Odpowiedź:
15 000 zł

Pytanie 9. Z jaką datą podpisali Państwo Umowę grantową?

Odpowiedź:
2022-04-27

Pytanie 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:
Termin został jednoznacznie określony w Załączniku nr 2 do Zaproszenia.

Pytanie 11. Czy poza wypełnieniem zał. 8 konkursu dla NASK wymagają Państwo również raportu z audytu dla Urzędu?

Odpowiedź:
Wymagania zamawiającego określa Załącznik nr 2 do Zaproszenia.

Pytanie 12. Czy wymagają Państwo przeprowadzenia testów technicznych/penetracyjnych podczas diagnozy – na ilościach zawartych w pytaniach 3-5?

Odpowiedź:
Wymagania zamawiającego określa Załącznik nr 2 do Zaproszenia.

Pytanie 13. 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 ich ewentualnego opracowania/wykonania podczas prowadzonej diagnozy):

3	Dokumentacja Systemu Informacyjnego wspierającego zadanie publiczne	Tak	Nie	Opracowuje Wykonawca
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.				

Odpowiedź:
Sporządzenie zestawienia zgodnie z tabelą będącą załącznikiem nr 8 konkursu jest przedmiotem zamówienia i leży po stronie Wykonawcy. Niezbędne w tym zakresie informacje zostaną przekazane Wykonawcy w trakcie wykonywania diagnozy. Zakres przedmiotu zamówienia opisuje Załącznik nr 2 do Zaproszenia.

Pytanie 14. Prosimy o przedłużenie terminu składania ofert przynajmniej do 21.06.2022 r.

Odpowiedź:
Ze względu na brak zmian w opisie przedmiotu zamówienia termin składania ofert nie ulega zmianie.

p.o. DYREKTORA
mgr Mirosława Badzińska