W związku pytaniami, które zostały przekazane przez Państwa dot. Zapytania ofertowego pn.: „Audyt cyberbezpieczeństwa w Urzędzie Gminy Krotoszyce w ramach projektu „Cyfrowa Gmina", poniżej przekazuję odpowiedzi:

Pytanie nr 1: Ilość lokalizacji (adresy, info co znajduje się pod danym adresem)

Pozostałe dane poniżej proszę rozgraniczyć na każdą lokalizację z osobna, pozwoli to najdokładniej obliczyć czasochłonność i cenę projektu

Odpowiedź:

1

Pytanie nr 2: Ilość pracowników/użytkowników

Odpowiedź:

20

Pytanie nr 3: Ilość wszystkich hostów podłączonych do sieci (komputery, urządzenia serwerowe, urządzenia sieciowe jak np. drukarki, routery, przełączniki, Access Pointy, urządzenia VolP etc.). W tym rozgraniczyć:

a. Ilość komputerów (również przenośnych)
b. Ilość serwerów (fizycznych, wirtualnych)
c. Ilość pozostałych urządzeń podłączonych do sieci

Odpowiedź:

a. 27

b. 8

c. 8

Pytanie nr 4: Ilość adresów zewnętrznych

Odpowiedź:

1

Pytanie nr 5: Ilość podsieci (jaki zakres maski każdej podsieci?)

Odpowiedź:

1 (10.0.0.1)

Pytanie nr 6: Ilość serwerowni

Odpowiedź:

1

Pytanie nr 7: Czy mają Państwo wdrożoną Active Directory?

Odpowiedź:

TAK

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

Odpowiedź:

15000

Pytanie nr 9: Z jaką datą podpisali Państwo Umowę grantową?

Odpowiedź:

05.04.2022

Pytanie nr 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:

TAK

Pytanie nr 11: Czy Odnosząc się do zapisu:

„W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany będzie do dokonania oceny zgodności funkcjonujących zasad i procedur dotyczących zarządzania bezpieczeństwem informacji, w tym przetwarzania danych osobowych, z obowiązującymi aktami prawnymi do przeprowadzenia kompleksowej diagnozy/ audytu bezpieczeństwa informacji w zakresie ustawowych obszarów działalności podmiotu (w tym w szczególności weryfikacji struktury organizacji oraz przepływu dokumentów elektronicznych, analizy zewnętrznej i wewnętrznej sieci komputerowej, analizy serwerów, testów dostępu do sieci wewnętrznej i zewnętrznej, analizy stacji roboczych, analizy kopii zapasowych, analizy poczty email, analizy ogólnego bezpieczeństwa danych i mechanizmów kontroli w podmiocie) oraz opracowania dokumentacji poaudytowej – raportu z wytycznymi do doskonalenia i rekomendacjami.”

Czy w związku z powyższym oczekują Państwo:

- przeprowadzenia pełnego audytu ochrony danych osobowych?
- przeprowadzenia testów penetracyjnych infrastruktury IT? A jeśli tak to czy testy mają być wykonane na wszystkich hostach, podsieciach, adresach wskazanych w pytaniach 3-5, czy na wybranej przez Państwa próbie? Jeśli próba proszę podać ilości.
- poza załącznikiem 8 konkursu również osobno raportu dla Urzędu z całości przeprowadzonych działań?
- czy poza ewentualnym powyższym jest jeszcze coś czego Państwo oczekują i mogliśmy to przegapić??

Odpowiedź:

z audytem danych osobowych, poza załącznikiem 8 konkursu również osobno ma być raport dla Urzędu z całości przeprowadzonych działań

Pytanie nr 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 lub 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	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	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		
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	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	X
4	**Dokumentacja procesu zarządzania incydentami**			
4.2	Czy istnieje procedura informowania o wykrytych incydentach?	X		
4.3	Czy istnieją procedury reagowania na incydenty?		X	X
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.		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**			
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

Signature Not Verified

Dokument podpisany przez Wojciech Woźniak, Gmina Krotoszyce
Data: 2022.06.13 11:47:24 CEST