Sfinansowano w ramach reakcji Unii na pandemię COVID-19

MIASTO MŁAWA
REGON 130377830
NIP 5691760034
ul. Stary Rynek 19
06-500 Mława

Pytania Wykonawców do zapytania ofertowego z dnia 20.06.2022r. i odpowiedzi Zamawiającego z dnia 21.06.2022 r.

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

Wykonawca przeprowadzi diagnozę cyberbezpieczeństwa w siedzibie Zamawiającego - Urząd Miasta Mława (cztery lokalizacje, mieszczące się w obrębie 1 km, 96 pracowników).

I lokalizacja (siedziba główna) ul. Stary Rynek 19 – Burmistrz, Zastępca Burmistrza, Sekretarz, Skarbnik Miasta Mława (4 osoby), Wydział Budżetu i Finansów (17 osób), Wydział Gospodarki Komunalnej (8 osób), Audytor wewnętrzny (1 osoba), Inspektorat Zarządzania Kryzysowego (1 osoba), Wydział Komunikacji Społecznej i Medialnej (3 osoby), Wydział Organizacyjny (17 pracowników, bez osób zatrudnionych na stanowiskach robotniczych), Wydział Gospodarki Nieruchomościami i Planowania Przestrzennego (8 osób), Samodzielne Stanowisko ds. Gospodarki Odpadami (1 osoba); razem 60 osób

II lokalizacja ul. Padlewskiego 13 - Straż Miejska (13 osób), Wydział Inwestycji (10 osób) – razem 23 osoby;

III lokalizacja ul. 18 Stycznia 4 lok. 25 – Wydział Oświaty i Polityki Społecznej (5 osób);

IV lokalizacja ul. Sienkiewicza 1 (Park Miejski) Wydział Spraw Obywatelskich (5 osób), Urząd Stanu Cywilnego (4 osoby- 1 osoba odnotowana 2 razy)- razem 8 osób

2. Ilość pracowników/użytkowników
   Odpowiedź

Suma osób zatrudnionych na stanowiskach administracyjno-biurowych 96 osób

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 - **108**
b. Ilość serwerów (fizycznych, wirtualnych)
   Odpowiedź - **25**
c. Ilość pozostałych urządzeń podłączonych do sieci
   Odpowiedź - **91**
4. Ilość adresów zewnętrznych
   Odpowiedź - **4**
5. Ilość podsieci (jaki zakres maski każdej podsieci?)
   Odpowiedź - **10**
6. Ilość serwerowni i ich lokalizacja?
   Odpowiedź - **JEDNA**
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
   10 000,00 zł brutto
9. Z jaką datą podpisali Państwo Umowę grantową?
   Odpowiedź
   14.04.2022 r.
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, termin realizacji nie jest negocjowalny. Został określony w Zapytaniu ofertowym - do dnia **30.07.2022 r.**

11. Czy poza wypełnieniem zał. 8 konkursu dla NASK wymagają Państwo również raportu z audytu dla Urzędu?
    Tak
12. Jednym z wymogów jest wskazanie posiadanych norm związanych z programem cyfrowej gminy. Czy chodzi o normy wskazane w KRI i czy posiadanie norm PN-ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO/IEC 22301 będzie wystarczające aby spełnić ten wymóg?
    Odpowiedź
    Tak, chodzi o standardy **Krajowych Norm Interoperacyjności**. Przedstawione powyżej normy powinny zostać uzupełnione o **Standard COBIT** - Cele Kontrolne dla Technologii Informacyjnej i Technologii Związanych.

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.

Urząd Miasta Mława posiada dokumentację z audytów. Zapoznanie się z dokumentacją zostanie umożliwione Wykonawcy, którego oferta okaże się najkorzystniejsza i z którym zostanie zawarta umowa. Zamawiający oczekuje wykonania oceny cyberbezpieczeństwa całościowo, nie wybiórczo. Obowiązuje **cały arkusz** Cert.