

Ostrów Mazowiecka, 07.06.2022r.

Odpowiedzi na zapytania do zaproszenia do składania ofert na:

Przeprowadzenie diagnozy cyberbezpieczeństwa w Urzędzie Miasta Ostrów Mazowiecka, w ramach projektu „Cyfrowa Gmina”.

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

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

2. Ilość pracowników/użytkowników - **80**
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) - **93**
 - b. Ilość serwerów (fizycznych, wirtualnych) – **8, 3**
 - c. Ilość pozostałych urządzeń podłączonych do sieci - **56**
4. Ilość adresów zewnętrznych - **4**
5. Ilość podsieci (jaki zakres maski każdej podsieci?) - **0**
6. Ilość serwerowni i ich lokalizacja? – **1**
7. Czy mają Państwo wdrożoną Active Directory? - **Tak**
8. Jaki budżet (brutto) wpisali Państwo we wniosku grantowym na realizację samej Diagnozy cyberbezpieczeństwa z całej puli przydzielonych środków? - **Budżet na realizację samej Diagnozy pokrywa się z kwotą przeznaczoną na sfinansowanie zamówienia, która zostanie ujawniona w dniu otwarcia ofert.**
9. Z jaką datą podpisali Państwo Umowę grantową? **01.04.2022r.**
10. Czy poza wypełnieniem zał. 8 konkursu dla NASK wymagają Państwo również raportu z audytu dla Urzędu? - **Tak**
11. 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 któregośkolwiek 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 oraz 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?		-	
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			
4.1	Czy wdrożone jest monitorowanie i wykrywanie incydentów? Kto za nie odpowiada? (stanowiska, funkcje itp. - bez danych osobowych)	+		
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.	+		

Zamawiający