

1. Czy Zamawiający dopuszcza przeprowadzenie diagnozy cyberbezpieczeństwa za pomocą środków komunikacji elektronicznej.

Sama diagnoza, jako podsumowanie wykonanych prac, może być uzgodniona i przesłana za pomocą środków komunikacji elektronicznej.

2. Czy diagnoza może zostać przeprowadzona zdalnie

j.w.

3. Czy szkolenia mogą się odbyć na sali u Państwa z naszymi materiałami ale poprzez połączenie zdalne z naszym ekspertem, który poprowadzi szkolenie i będzie dostępny dla uczestników. Różnica cenowa w ofercie ze szkoleniem z przyjazdem to 2500 zł brutto.

Szkolenia, zgodnie z treścią zapytania ofertowego, mają odbywać się stacjonarnie w siedzibie Zamawiającego.

4. Ilość lokalizacji (adresy, info. co znajduje się pod danym adresem)

1 lokalizacja: Urząd Gminy Bukowiec, ul. Dr Fl. Ceynowy 14, 86-122 Bukowiec.

W tej lokalizacji mieszczą się również: Gminny Ośrodek Pomocy Społecznej (GOPS) Zakład Gospodarki komunalnej (ZGK), Zespół Obsługi Oświaty (ZOO)

5. Ilość pracowników/użytkowników

18 pracowników Urzędu, 6 GOPS-u, 2 ZGK, 3 ZOO w ramach jednej sieci /29 użytkowników

6. 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) – **30 sztuk**
 - b. Ilość serwerów (fizycznych, wirtualnych) - **1 serwer**
 - c. Ilość pozostałych urządzeń podłączonych do sieci - **12**
7. Ilość podsieci (jaki zakres maski każdej podsieci?) - **1 podsieć (254 adresy)**
8. Ilość serwerowni - **1**
9. Ilość adresów zewnętrznych – **2 adresy zewnętrzne**
10. Czy mają Państwo wdrożoną Active Directory? - **Nie**
11. Jaki budżet (brutto) wpisali Państwo we wniosku grantowym na realizację samej Diagnozy cyberbezpieczeństwa z całej puli przydzielonych środków?
Kwota będzie udostępniona w dniu otwarcia ofert.
12. Jaki budżet (brutto) wpisali Państwo we wniosku grantowym na realizację szkoleń pracowników z całej puli przydzielonych środków?
Kwota będzie udostępniona w dniu otwarcia ofert.

13. Z jaką datą podpisali Państwo Umowę grantową?

Umowa grantowa podpisana 23 lutego 2022 r.

14. Pytania odnośnie Części I:

- a. Zakresowo ta część ma być pełnym audytem zgodnym z załącznikiem 8 konkursu – a wynikiem ma być podsumowanie co jest do poprawy, jaka dokumentacja do wdrożenia przed właściwą diagnozą? Dobrze to rozumiemy?

Jest to część, która ma zweryfikować potrzeby w zakresie uzupełnienia dokumentacji przed rozpoczęciem diagnozy.

15. Pytania do Części II:

- a. Opracowanie dokumentacji – jaką konkretnie dokumentację mają Państwo na myśli – chodzi ogólnie o dokumentację SZBI typu polityki bezpieczeństwa informacji, ochrony danych, instrukcję zarządzania systemami informatycznymi itp. dokumenty, czy chodzi o opracowanie wszelkiej dokumentacji, która pojawia się do sprawdzenia w załączniku 8 konkursu? Przykładowo arkusz CERT z tego załącznika w punkcie 3, 4, 5 i 6 mówi o sprawdzeniach raportów z różnego rodzaju audytów (www, bezpieczeństwa, poczty e-mail itp.), o ocenie czy istnieją różnego typu procedury, dokumentacje, arkusz KRI mówi również o wspomnianej dokumentacji SZBI – czy oczekują Państwo wykonania podczas części I wszystkich tych audytów, aby powstały z nich raporty i dokumentacja, którą później się weryfikuje podczas Diagnozy właściwej?

Chodzi o wykonanie wszystkich audytów, aby powstały z nich raporty i dokumentacja, którą później się weryfikuje podczas Diagnozy właściwej.

- b. Przeprowadzenie szkolenia i wdrożenia opracowanej dokumentacji w Urzędzie – szkolenie z dokumentacji dla kogo? Ma to być w ramach omówienia tej dokumentacji z wybranymi osobami, które głównie się nią zajmują?

Zgodnie z założeniami projektu Cyfrowa Gmina szkolenia mają służyć podniesieniu poziomu cyberbezpieczeństwa wśród pracowników. Stąd w zapytaniu pojawił się wymóg przeprowadzenia szkoleń dla wszystkich pracowników minimum z zakresu: podstawy bezpieczeństwa informacji, kontrola dostępu do zasobów informacyjnych, szyfrowanie informacji, cyberbezpieczeństwo, bezpieczeństwo pracy zdalnej.

- c. Testy bezpieczeństwa – oczekują Państwo testów penetracyjnych na wszystkich hostach z pytania 3? Jeśli chodzi o strony internetowe wskazane w treści to chodzi o audyt stron www (np. metodyką OWASP) czy o audyt dostępności stron WCAG 2.1?

Testy oraz audyt stron www w celu uzyskania zgodności z wymaganiami diagnozy cyberbezpieczeństwa.

- d. Testy phishingowe mają być 2x na wszystkich pracownikach, czy na wybranych próbach?

Testy phishingowe na uzgodnionej, możliwie jak największej grupie.


mgr Adam Licznarski