

Sfinansowano w ramach reakcji Unii Europejskiej na pandemię COVID-19

Kuźnica, dn. 13 czerwca 2022 r.

Or.042.1.2022

Odpowiedzi na zapytania

Dotyczy zapytania ofertowego wykonanie diagnozy cyberbezpieczeństwa wg Konkursu Grantowego Cyfrowa Gmina Oś V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia - REACT-EU

Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia w Urzędzie Gminy Kuźnica.

Pytanie nr 2

W nawiązaniu do ogłoszonego postępowania na „wykonanie Diagnozy Cyberbezpieczeństwa wg Konkursu Grantowego Cyfrowa Gmina Oś V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia - REACT-EU. Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia w Urzędzie Gminy Kuźnica”, prosimy o:

- przesłanie edytowalnej wersji formularza ofertowego oraz innych dokumentów, które należy wypełnić składając ofertę
- wskazanie osoby kontaktowej wraz z kontaktem (tel. / e-mail) w celu ustalenia dodatkowych informacji dot. np. Państwa infrastruktury informatycznej, ilości stacji roboczych, serwerów itp.

Odpowiedź:

Edytowalna wersja formularza oraz inne dokumenty, które należy wypełnić składając ofertę zostały wysłane na adres e-mail wskazany w korespondencji.

Osoba kontaktowa: informatyk urzędu: 85 722 92 89; kom. 502-920-330.

Pytanie nr 3

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:

2. Ilość pracowników/użytkowników
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)
 - b. Ilość serwerów (fizycznych, wirtualnych)
 - c. Ilość pozostałych urządzeń podłączonych do sieci

Sfinansowano w ramach reakcji Unii Europejskiej na pandemię COVID-19

4. Ilość adresów zewnętrznych
5. Ilość podsieci (jaki zakres maski każdej podsieci?)
6. Ilość serwerowni i ich lokalizacja?
7. Czy mają Państwo wdrożoną Active Directory?
8. Jaki budżet (brutto) wpisali Państwo we wniosku grantowym na realizację samej Diagnozy cyberbezpieczeństwa z całej puli przydzielonych środków?
9. Z jaką datą podpisali Państwo Umowę grantową?
10. Czy termin realizacji jest negocjowalny przed podpisaniem umowy jeżeli realizacja diagnozy w pełni zmieści się w 6 miesiącach od daty podpisania umowy grantowej?
11. Czy poza wypełnieniem zał. 8 konkursu dla NASK wymagają Państwo również raportu z audytu dla Urzędu?
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 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 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?			
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			

Sfinansowano w ramach reakcji Unii Europejskiej na pandemię COVID-19

5.1	<p>Wyniki audytu serwisów WWW z uwzględnieniem:</p> <ul style="list-style-type: none"> - 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	<p>Wyniki audytu serwisów pocztowych z uwzględnieniem:</p> <ul style="list-style-type: none"> - poprawności wdrożenia mechanizmów SPF, DKIM i DMARC; - poprawności i bezpieczeństwa wdrożenia mechanizmów TLS; - dostępności kompetentnego personelu do utrzymania serwisów. 			
5.3	<p>Wyniki audytu lokalnych sieci teleinformatycznych z uwzględnieniem:</p> <ul style="list-style-type: none"> - 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	<p>Wyniki audytu połączenia z siecią Internet z uwzględnieniem:</p> <ul style="list-style-type: none"> - 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	<p>Wyniki audytu organizacji zarządzania bezpieczeństwem teleinformatycznym z uwzględnieniem:</p> <ul style="list-style-type: none"> - 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	<p>Wyniki audytu procesów planowania z uwzględnieniem:</p> <ul style="list-style-type: none"> - 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:

Etap realizacji przedmiotu zamówienia, który nastąpi po podpisaniu umowy.


mgr inż. Paweł Miklasz