Załącznik nr 2

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

I. WSTĘP

1) Gmina Miejska Kętrzyn realizuje projekt w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina" (numer umowy o powierzenie grantu: 4389/2/2022).
2) W ramach niniejszego projektu udzielone zostanie zamówienie na realizację usługi pn. „Przeprowadzenie audytu cyberbezpieczeństwa Gminy Miejskiej Kętrzyn", polegającej na wykonaniu audytu bezpieczeństwa IT.
3) Celem niniejszego dokumentu jest przedstawienie wszystkich wymagań dotyczących audytu cyberbezpieczeństwa jakie muszą zostać spełnione w ramach przedmiotowego postępowania.
4) 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 kompleksowego 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 po audytowej - raportu z wytycznymi do doskonalenia i rekomendacjami.
5) Informacje poglądowe dotyczące zamawiającego:
    - Ilość lokalizacji do audytu - 1
    - Ilość pracowników ≈ 85
    - Ilość hostów ≈ 75
    - Ilość komputerów ≈ 85
    - Ilość serwerów – 4

II. Wymagania w zakresie wykonania usługi audytu

1. Diagnoza cyberbezpieczeństwa w Urzędzie Gminy Miejskiej Kętrzyn musi zostać przeprowadzona zgodnie z Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 z późn. zm.) oraz Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tj. Dz.U. 2017 poz. 2247 ze zm.) zwane dalej Rozporządzeniem KRI, w tym opracowanie raportu zawierającego wnioski i rekomendacje oraz przeprowadzenie szkolenia w zakresie cyfrowego bezpieczeństwa pracowników Urzędu.
2. Diagnoza cyberbezpieczeństwa musi zostać przeprowadzona zgodnie z formularzem zamieszczonym w dokumentacji konkursowej projektu Cyfrowa Gmina dostępnym na stronach Centrum Projektów Polska Cyfrowa [https://www.gov.pl/web/cppc/cyfrowa-gmina] - Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa - załącznik nr 8.
3. Audyt musi zostać przeprowadzony przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Wykaz certyfikatów wskazanych w w/w rozporządzeniu:

    - Certified Internal Auditor (CIA)
    - Certified Information System Auditor (CISA)
    - Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PNEN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób
    - Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób
    - Certified Information Security Manager (CISM)
    - Certified in Risk and Information Systems Control (CRISC)
    - Certified in the Governance of Enterprise IT (CGEIT)
    - Certified Information Systems Security Professional (CISSP)
    - Systems Security Certified Practitioner (SSCP)
    - Certified Reliability Professional
    - Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert

4. Diagnozę cyberbezpieczeństwa wykonawca dostarczy w wersji elektronicznej oraz w wersji papierowej
5. Załącznikiem do Szczegółowego Opisu Przedmiotu Zamówienia jest Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa - załącznik nr 8.

III. Minimalne wymagania audytu w zakresie dokumentacji i procesów

1. Ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI)/ Krajowym Systemie Cyberbezpieczeństwa (KSC)

- wyznaczenie osoby do kontaktu – Art. 21 KSC
- przekazanie danych osoby wyznaczonej – Art. 22 pkt 5) KSC
- zapewnienie zarządzania incydentem – Art. 22 pkt 1) KSC
- zgłaszanie incydentu – Art. 22 pkt 2) Art. 23 KSC
- zapewnienie obsługi incydentu – Art. 22 pkt 3) KSC
- zapewnienie dostępu do wiedzy – Art. 22 pkt 4) KSC
- opracowanie, ustanowienie i wdrożenie SZBI – Par. 20 KRI
- monitorowanie i przegląd SZBI – Par. 20 KRI
- doskonalenie SZBI – Par. 20 KRI
- aktualizowanie regulacji wewnętrznych – Par. 20 pkt 1) KRI
- inwentaryzacja sprzętu i oprogramowania – Par. 20 pkt 2) KRI
- przeprowadzanie okresowych analiz ryzyka – Par. 20 pkt 3) KRI
- postępowanie z ryzykiem – Par. 20 pkt 3) KRI
- zarządzanie uprawnieniami – Par. 20 pkt 4), 5) KRI
- szkolenia i uświadamianie – Par. 20 pkt 6) KRI
- monitorowanie dostępu do informacji – Par. 20 pkt 7) a), b) KRI
- monitorowanie nieautoryzowanych zmian – Par. 20 pkt 7) b) KRI
- zabezpieczenie nieautoryzowanego dostępu – Par. 20 pkt 7) c) KRI
- ustanowienie zasad bezpiecznej pracy mobilnej – Par. 20 pkt 8) KRI
- zabezpieczenie informacji przed nieuprawnionym ujawnieniem – Par. 20 pkt 9) KRI
- zabezpieczenie informacji przed nieuprawnioną modyfikacją – Par. 20 pkt 9) KRI
- zabezpieczenie informacji przed nieuprawnionym usunięciem lub zniszczeniem – Par. 20 pkt 9) KRI
- zawieranie w umowach serwisowych zapisów o bezpieczeństwie – Par. 20 pkt 10) KRI
- ustalenie zasad postępowania z informacjami w celu minimalizacji kradzieży informacji i środków przetwarzania – Par. 20 pkt 11) KRI
- aktualizowanie oprogramowania – Par. 20 pkt 12) a) KRI
- minimalizowanie ryzyka utraty informacji w wyniku awarii systemu – Par. 20 pkt 12) b) KRI
- ochrona systemu przed błędami – Par. 20 pkt 12) c) KRI

- stosowanie mechanizmów kryptograficznych w systemach – Par. 20 pkt 12) d) KRI
- zapewnienie bezpieczeństwa plików systemowych – Par. 20 pkt 12) e) KRI
- zarządzanie podatnościami systemów – Par. 20 pkt 12) f), g) KRI
- kontrola zgodności systemów z regulacjami – Par. 20 pkt 12) h) KRI
- zapewnienie audytu bezpieczeństwa informacji nie rzadziej niż raz na rok – Par. 20 pkt 14) KRI

2. Ocena wybranych aspektów bezpieczeństwa systemów Informatycznych

- dokumentacja potwierdzająca wykonane działania wskazanego w ustawie
- opis identyfikacji systemu informacyjnego wspierającego zadanie publiczne
- dokumentacja Systemu Informacyjnego wspierającego zadanie publiczne
- dokumentacja procesu zarządzania incydentami
- aspekty techniczne do weryfikacji

3. Ocena dojrzałości wybranych procesów bezpieczeństwa

- ochrona przed kodem szkodliwym
- ochrona sieci i połączeń
- ochrona urządzeń końcowych
- zarządzanie tożsamością i autoryzacją dostępu
- ochrona fizyczna systemów IT
- bezpieczeństwo urządzeń drukujących
- zarządzanie podatnościami

4. Opracowanie raportu z audytu oraz uzupełnienie arkusza do Oceny

- Weryfikacja dokumentacji sieci, topologii sieci, kluczowych elementów sieci
- Skanowanie sieci – rekonesans sieci: Sprawdzenie jakie hosty są w sieci widoczne, ile ich jest, usługi jakie są uruchomione na hostach, jakie systemy operacyjne działają na wykrytych hostach. W szczególności:
  - skanowanie sieci w poszukiwaniu wszystkich podłączonych hostów
  - wykrycie czy jest dostęp do innych podsieci z danej podsieci
  - wykrycie usług działających na hostach podłączonych do sieci
  - wykrycie podatności na wybranych hostach w sieci

5. Testy penetracyjne infrastruktury sieciowej

- skanowanie najistotniejszych hostów w sieci które zostały wybrane na podstawie wcześniejszej analizy, w tym:

- weryfikacja występowania luk bezpieczeństwa dla konkretnych usług,
- w zależności od wykrytej usługi weryfikacja haseł,
- weryfikacja dostępu użytkowników do odpowiednich usług,
- weryfikacja możliwości dostępu do usługi,
- weryfikacja luk bezpieczeństwa w systemie operacyjnym,
- weryfikacja luk bezpieczeństwa w oprogramowaniu firm trzecich,
- weryfikacja haseł w usługach umożliwiających logowanie,
- sprawdzenie możliwości wylistowania użytkowników oraz zdobycia haseł,
- weryfikacja możliwości uzyskania dostępu do zasobów współdzielonych,
- weryfikacja zabezpieczeń urządzeń sieciowych

6. Zdalne testy adresów publicznych

- Wykonanie zdalnych testów wszystkich adresów publicznych zamawiającego

7. Badanie ankietowe.

- badanie ankietowe pracowników działu IT oraz pracowników Zamawiającego z wiedzy o bezpieczeństwie sieci i procedurach IT stosowanych przez Zamawiającego.
- Grupa ankietowanych pracowników zostanie ustalona podczas Audytu.

8. Testy socjotechniczne

- kontakt telefoniczny – do 10 osób
- kampanie phishingowe dla całej organizacji

9. Wykonanie raportu zawierającego po audytowego

- opis wszystkich elementów, które zostały poddane audytowi
- podział podatności ze względu na ryzyko: wysokie, średnie, niskie
- wskazanie zaleceń, rekomendacji, najlepszych praktyk – dla każdej znalezionej podatności
- wylistowanie wszystkich podatności ze względu na ryzyko: wysokie, średnie, niskie
- określenie bezpieczeństwa informatycznego w organizacji poprzez wskazanie ilości i rodzaju znalezionych podatności

10. Wsparcie po audytowe

- 10 godzin wsparcia po audytowego