Załącznik nr 1 do zapytania ofertowego

**Opis Przedmiotu Zamówienia**

**Przeprowadzenie diagnozy cyberbezpieczeństwa dla Gminy Bierawa 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" o numerze POPC.05.01.00-00-0001/21-00.**

Legenda:
**MIN** parametry minimalne
**MAX** parametry maksymalne
**RWN** parametry dokładne, równe (nie większe i nie mniejsze)

## 1. Audyt cyberbezpieczeństwa IT (1 sztuka)

Audyt cyberbezpieczeństwa (dalej zwany audytem lub diagnozą) musi zostać przeprowadzony zgodnie z wymogami projektu Cyfrowa Gmina oraz 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. Załączono go również w dokumentach do niniejszego postepowania. Od Wykonawcy wymaga się doświadczenia w przeprowadzaniu przedmiotowych diagnoz oraz audytów oraz posiadania certyfikatu ISO 27001. Zadanie zrealizuje MIN: certyfikowany audytor (lub zespół audytorów) spełniający wymagania opisane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu. Audyt musi spełnić MIN: wszystkie ustalone wymogi Projektu „Cyfrowa Gmina" oraz wszystkie założenia opisane poniżej i powinien zostać przeprowadzony 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.).

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:

a) Certified Internal Auditor (CIA);
b) Certified Information System Auditor (CISA);
c) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN 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;
d) 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:
e) Certified Information Security Manager (CISM);
f) Certified in Risk and Information Systems Control (CRISC);
g) Certified in the Governance of Enterprise IT (CGEIT);
h) Certified Information Systems Security Professional (CISSP);
i) Systems Security Certified Practitioner (SSCP);
j) CertifiedReliability Professional;
k) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

Diagnozę cyberbezpieczeństwa należy dostarczyć w wersji elektronicznej oraz w wersji papierowej.

**PLAN REALIZACJI USŁUGI AUDYTU BEZPIECZEŃSTWA IT (MINIMUM):**

AUDYT STANU OPROGRAMOWANIA U ZAMAWIAJĄCEGO ZGODNIE Z ZAŁĄCZNIKIEM NR 8 DO REGULAMINU PROJEKTU CYFROWA GMINA:

- Inwentaryzacja kluczowego oprogramowania występującego na wszystkich komputerach Zamawiającego poprzez zdalne i fizyczne skanowanie urządzeń (stacji roboczych, serwerów, maszyn wirtualnych),
- Inwentaryzacja zebranych atrybutów licencji (faktur zakupu, oryginalnych nośników, pudełek, certyfikatów autentyczności, umów licencyjnych, itd.),
- Identyfikacja procedur zarządzania oprogramowaniem – weryfikacja zapisów Polityki Bezpieczeństwa Informacji oraz Systemu Zarządzania Bezpieczeństwem Informacji,
- Analiza i weryfikacja oprogramowania:

- utworzenie raportu wstępnego – przedstawienie wyników i rozbieżności między zainstalowanym oprogramowaniem, a posiadanymi licencjami oraz sporządzenie spisu oprogramowania do usunięcia lub uzupełnienia licencji,
- rekomendacje i wnioski dotyczące wykorzystywanego oprogramowania oraz licencji,
- prace naprawcze po stronie Zamawiającego, skutkujące wyeliminowaniem wskazanych na podstawie zaleceń nieprawidłowości.

AUDYT DOKUMENTACJI I PROCESÓW

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

TESTY PENETRACYJNE INFRASTRUKTURY SIECIOWEJ

1. **Przedstawienie założeń Audytu:**

Audyt wykonywany będzie w sposób manualny oraz automatyczny za pomocą specjalistycznych narzędzi oraz własnych skryptów przygotowanych na podstawie wiedzy i doświadczeń.

2. **Weryfikacja dokumentacji sieci, topologii sieci, kluczowych elementów sieci.**
3. **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 ten etap polega na:

- skanowaniu sieci w poszukiwaniu wszystkich podłączonych hostów;
- wykryciu czy jest dostęp do innych podsieci z danej podsieci;
- wykryciu usług działających na hostach podłączonych do sieci;
- wykryciu podatności na wybranych hostach w sieci.

4. **Skanowanie będzie powtórzone dla każdej wskazanej przez zamawiającego sieci:**

Przeprowadzenie skanowania w prawidłowo działającej sieci nie powinno mieć negatywnego wpływu na działanie sieci. Po przeskanowaniu sieci wraz z Zamawiającym zostanie wybrana pula hostów do dalszego badania.

5. **Skanowanie najistotniejszych hostów w sieci (serwery, kluczowe stacje końcowe, kamery, rejestratory), które zostały wybrane na podstawie wcześniejszej analizy:**
   - 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.
6. **Sprawdzenie domyślnych haseł dla najistotniejszych hostów w sieci (serwery, bramy, switche, access point), które zostały wybrane na podstawie wcześniejszej analizy:**
   - weryfikacja haseł w usługach umożliwiających logowanie.
7. **Sprawdzenie możliwości wylistowania użytkowników oraz zdobycia haseł.**
8. **Weryfikacja możliwości uzyskania dostępu do zasobów współdzielonych.**
9. **Weryfikacja zabezpieczeń urządzeń sieciowych:**
   - badanie odporności switchy na ataki sieciowe.
10. **Testy sieci bezprzewodowej oraz weryfikacja zabezpieczeń sieci bezprzewodowej:**
    - weryfikacja pod kątem dostępu;
    - weryfikacja pod kątem zabezpieczeń;
    - wykrycie możliwości przechwycenia haseł;
    - w przypadku przechwycenia hasła – weryfikacja pod kątem możliwości złamania hasła.
11. **Zdalne testy adresów publicznych.**
12. **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.

13. **Testy socjotechniczne:**
    - kontakt bezpośredni – do 5 osób;
    - kontakt telefoniczny – do 5 osób;
    - kampanie phishingowe – możliwe dla całego Urzędu.
14. **Wykonanie raportu zawierającego:**
    - 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 Urzędzie poprzez wskazanie ilości i rodzaju znalezionych podatności.

**15. Wsparcie poaudytowe, MIN: 60 dni**

Udzielenie informacji (poprzez telefon i e-mail) na temat audytowanych elementów wynikających z raportu. Czas dla Zamawiającego na zapoznanie się z raportem i zadawanie pytań odnośnie raportu to 60 dni.

**16.** Termin przeprowadzenia audytu ustala się na: **01.06.2022-30.06.2022.**

**17.** Szczegółowe parametry zamówienia:

a) Ilość pracowników: 27;
b) Ilość lokalizacji: 1;
c) Ilość serwerów fizycznych: 1;
d) Ilość stacji komputerowych: 27;
e) Ilość komputerów przenośnych: 5;
f) Ilość stacji komputerowych do obsługi ewidencji ludności i dowodów osobistych: 2.