Załącznik nr 2

Opis przedmiotu zamówienia:

*„P*rzeprowadzenie diagnozy cyberbezpieczeństwa oraz szkoleń w zakresie cyberbezpieczeństwa 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 konkursu grantowego „Cyfrowy Powiat"

1. Wymagania wobec wykonawcy

O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy:

- posiadają wiedzę i doświadczenie oraz dysponują potencjałem technicznym i osobami zdolnymi do wykonania zamówienia (Wykonawca złoży w tym zakresie oświadczenie, które stanowi załącznik nr 4 do oferty),
- posiadają doświadczenie w wykonaniu audytów – wykonawca wykaże, że wykonał co najmniej 1 audyt/diagnozę w zakresie określonym w Załączniku nr 8 do Regulaminu Konkursu Grantowego Cyfrowy Powiat lub zrealizował co najmniej 2 audyty w jednostkach administracji publicznej o podobnym zakresie w ostatnich trzech latach przed złożeniem oferty (w tym zakresie wykonawca złoży oświadczenie będący załącznikiem nr 5 do oferty wraz z dokumentami potwierdzającymi ich wykonanie),
- posiadają uprawnienia o określonej działalności lub czynności, jeśli ustawy nakładają obowiązek z tym związany,
- znajdują się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia.

Wymagania wobec osób realizujących przedmiot zamówienia

- Wykonawca oświadcza, że posiada wiedzę i doświadczenie w zakresie bezpieczeństwa informacji zgodnie z zakresem opisanym poniżej:
    - przynajmniej jedna osoba musi posiadać:
        - co najmniej 3 letnie doświadczenie w zakresie pełnienia funkcji testera bezpieczeństwa (pentestera)*,
        - certyfikat OCSP (Offensive Security Certified Professional),
        - certyfikat uprawniający do przeprowadzenia audytu zgodnie z rozporządzeniem Ministra Cyfryzacji 1 z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu,
        - co najmniej 3 letnie doświadczenie w zakresie prowadzenia audytów bezpieczeństwa uwzględniających założenia wynikające z normy ISO 27001,

- przynajmniej jedna osoba musi posiadać:
  - co najmniej 3 letnie doświadczenie w zakresie prowadzenia audytów bezpieczeństwa uwzględniających założenia wynikające z normy ISO 27001 i/lub KRI,
  - certyfikat uprawniający do przeprowadzenia audytu zgodnie z rozporządzeniem Ministra Cyfryzacji 1 z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu,
  - doświadczenie w prowadzeniu szkoleń w zakresie cyberbezpieczeństwa, którego tematyką była co najmniej ochrona przed złośliwym oprogramowaniem, socjotechniką w tym phishingiem, bezpiecznym korzystaniem z poczty elektronicznej oraz Internetu, wykorzystaniem menadżera haseł,
- przynajmniej jedna osoba musi posiadać:
  - co najmniej 3 letnie doświadczenie w zakresie pełnienia funkcji testera bezpieczeństwa (pentestera) *,
  - certyfikat OCSP (Offensive Security Certified Professional),
  - posiadać wiedzę i doświadczenie w zakresie przygotowywania oraz wykonywania testów socjotechnicznych.

* - przez testy penetracyjne należy rozumieć przeprowadzenie testów mających na celu wykrycie nieznanych podatności. Skanowanie pod kątem znanych podatności narzędziami typu Nessus, OpenVAS (Greenbone), BurpSuite, Acunetix i inne podobne nie spełnia wymagania testów penetracyjnych.

Niepotwierdzenie powyższych wymagań skutkować będzie odrzuceniem oferty.

Wynikiem prac Wykonawcy ma być audyt na podstawie załącznika nr 3 do niniejszego zaproszenia oraz dokumenty audytowe dedykowane pozostałym obszarom objętym zamówieniem. Dokumenty audytowe, o których mowa muszą odzwierciedlać pełny obszar prac objętych zamówieniem. W ramach dokumentacji Wykonawca opisze każde zidentyfikowane ryzyko wraz z precyzyjnym opisem proponowanej metody usunięcia tego ryzyka oraz oceni ryzyka techniczne zgodnie z klasyfikacją CVSS. Ryzyka, o których mowa muszą zostać wprowadzone do rejestru ryzyk.

2. Zestawienie ilościowe.

Przedmiot zamówienia obejmuje przeprowadzenie diagnozy cyberbezpieczeństwa oraz szkoleń z zakresu cyberbezpieczeństwa.

Lp.	Nazwa	Ilość
1.	Przeprowadzenie szkolenia dla pracowników w zakresie cyberbezpieczeństwa	149 osób
2.	Przeprowadzenie diagnozy cyberbezpieczeństwa	1
3.	Przeprowadzenie testów penetracyjnych aplikacji/stron www	1

4.	Przeprowadzenie skanów na występowanie znanych podatności	1
5.	Liczba fizycznych lokalizacji podlegających testom	1
6.	Liczba serwerów	2
7.	Liczba urządzeń sieciowych	5
8.	Liczba łącz do Internetu	3
9.	Liczba stacji roboczych użytkowników	149
10.	Liczba urządzeń mobilnych	0
11.	Liczba użytkowników	149
12.	Liczba użytkowników bezpiecznej poczty elektronicznej	149
13.	Przeprowadzenie szkoleń dla administratorów	1

3. Opis przedmiotu zamówienia

1.1. Przeprowadzenie szkolenia w zakresie cyberbezpieczeństwa.

1.1.1. Wymagania ogólne dla szkoleń:

1. Szkolenie może odbyć się zdalnie. Wykonawca powinien również dostarczyć platformę umożliwiającą prowadzenie szkoleń.
2. Szkolenie powinno trwać do 4 godzin szkoleniowych dla 1 grupy szkoleniowej w ciągu dnia.
3. Szkolenia będą odbywać się w dni robocze od poniedziałku do piątku w godzinach 8.00 – 16.00.
4. W celu maksymalizacji czasu nie przewiduje się przerw podczas szkolenia.
5. W ramach organizacji szkoleń Wykonawca zapewni:
   1) Materiały szkoleniowe dla każdego uczestnika szkolenia w postaci elektronicznej, które Zamawiający będzie mógł wykorzystać nieodpłatnie i wydrukować dla każdego uczestnika. Materiały muszą zawierać szczegółowe informacje, które będą omawiane podczas szkolenia.
   2) Wydanie Uczestnikom szkolenia zaświadczeń o ukończeniu danego szkolenia.
   3) Prowadzenie dokumentacji wszystkich szkoleń w jednakowy sposób. Na dokumentację szkolenia składają się:
      a) Lista obecności Uczestników szkolenia (dzienne, wypełniane oddzielnie każdego dnia szkolenia).
      b) Lista odbioru zaświadczeń o ukończeniu szkolenia.
      c) Ankieta satysfakcji ze szkolenia.
   4) Test wiedzy dotyczący przedmiotu szkolenia realizowany w trybie on-line.

1.1.2. Minimalny zakres szkolenia:

Temat szkolenia

Głównym tematem szkolenia będzie omówienie poprawnych zasad związanych z cyberbezpieczeństwem. Ponadto zostaną omówione zagrożenia w sieci takie jak phishing, ransomware oraz malware, które powodują w dobie Internetu poważne zagrożenia dla urzędu oraz pracowników. Na szkoleniu winny być poruszone sposoby przeciwdziałania oraz zabezpieczania się przed powyższymi zagrożeniami.

Proponowana tematyka szkolenia:

1. Czym jest cyberbezpieczeństwo i dlaczego jest tak ważne w dzisiejszych czasach?
2. Omówienie najczęściej występujących metod nieautoryzowanego pozyskania danych oraz występujących zagrożeń.
3. Omówienie metod obrony oraz przeciwdziałania przed:
   - Wyłudzeniem danych osobowych za pomocą technik socjotechnicznych (phishing).
   - Oprogramowaniem mogącym zablokować dostęp do urządzeń firmowych wraz z plikami znajdującymi się na tych urządzeniach (ransomware).
   - Szkodliwymi programami mogącymi pozyskać dane firmowe oraz osobiste pracowników (malware).
   - Ciekawością pracowników podczas wykonywania ich obowiązków służbowych (czynnik ludzki).
4. Omówienie informacji, które należy chronić.
5. Omówienie 10 zasad bezpieczeństwa informacji.
6. Omówienie 10 zasad zarządzania hasłami.
7. Omówienie stosowania managerów haseł.
8. Omówienie ścieżki postępowania w przypadku naruszenia bezpieczeństwa.

1.2. Przeprowadzenie diagnozy cyberbezpieczeństwa.

1. Diagnoza musi być przeprowadzona lokalnie w siedzibie Zamawiającego.
2. Diagnoza musi być przeprowadzona w zakresie określonym w „Formularzu informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa” stanowiącym załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowy Powiat (załączony do Zapytania ofertowego jako Załącznik nr 3).
3. Diagnoza musi być przeprowadzona przez osobę posiadającą certyfikat uprawniający do przeprowadzenia audytu, o którym mowa w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.
4. Wykonawca przekaże wynik przeprowadzonej diagnozy w wersji papierowej oraz elektronicznej w postaci pliku wypełnionego arkusza kalkulacyjnego formularza, o którym mowa w pkt. 2, podpisanego podpisem cyfrowym (weryfikowanym certyfikatem kwalifikowanym lub przy wykorzystaniu profilu zaufanego) przez osobę posiadającą uprawnienia, o których mowa w pkt. 3.

5. Wykonawca w przypadku stwierdzonych nieprawidłowości przekaże zamawiającemu szczegółowe wytyczne w jaki sposób należy je zniwelować oraz przeprowadzi bezpośrednie konsultacje na ten temat z przedstawicielem zamawiającego.

1.3. Przeprowadzenie testów penetracyjnych aplikacji

Wykonawca powinien przeprowadzić testy penetracyjne zgodnie z zestawieniem kategorii określonych na stronie https://owasp.org/www-project-top-ten/ „Top 10 Web Application Security Risks". Należy przez to rozumieć, że Wykonawca w ramach testów wykona czynności sprawdzające każdy obszar podatności wskazanych w Top 10. Testom podlega witryna portalu internetowego Urzędu.
Przez testy penetracyjne należy rozumieć ręczne poszukiwanie podatności:

- w konfiguracji serwerów baz danych oraz www, które pozostają w dyspozycji Zamawiającego,
- w kodzie źródłowym aplikacji podlegających testom,
- przeprowadzenie testu odporności na atak typu DDoS,
- w sposobie wykonywania się aplikacji.

1.4. Testy socjotechniczne

1.4.1. Szczegółowy opis testów

Wykonawca będzie zobowiązany do przeprowadzenia testów socjotechnicznym w zakresie opisanym poniżej. Wszelkie elementy infrastruktury w tym oprogramowania leżą po stronie Wykonawcy.

1.4.2. Stworzenie fałszywych stron

Wykonawca w ramach wykonywanych działań utworzy 2 fałszywe strony i zamieści je w Internecie w kontrolowanym przez siebie środowisku (lokalizację środowiska Wykonawca uzgodni z Zamawiającym). Na tym środowisku Wykonawca zainstaluje oraz skonfiguruje wymagane komponenty do prawidłowego przeprowadzenia testów socjotechnicznych z wykorzystaniem fałszywych stron.

Opisywany sposób testu winien być powiązany z innymi formami ataków, które mają na celu skłonienie do odwiedzenia spreparowanej strony. W tym celu Wykonawca użyje metod: spoofing wiadomości e-mail.

Wykonawca otrzyma listę adresów e-mail, które będą poddane testom.

Wykonawca w uzgodnieniu z Zamawiającym zarejestruje domeny, które poprzez zastosowanie techniki typosquatting posłużą do uruchomienia stron wyłudzających informacje.

1.4.3. Wysłanie wyłudzających informację wiadomości e-mail (spoofing)

Wykonawca przygotuje scenariusze testu, które przedstawi Zamawiającemu do akceptacji a następnie na ich podstawie przygotuje i uzgodni z Zamawiającym treść 3 wiadomości e-mail, które posłużą do nakłonienia odbiorcy do wykonania czynności określonych w wiadomości.

Przynajmniej jedna z wiadomości musi zawierać specjalnie przygotowany plik, którego wykonanie przez odbiorcę wiadomości będzie powodowało automatyczne przekazanie danych świadczących o podjęciu takiej czynności.

1.4.4. Zakres zbieranych informacji

W ramach testów Wykonawca będzie zbierał wyłącznie minimalny zakres informacji stanowiący potwierdzenie dla wykonania przez odbiorcę czynności przekazanych w wiadomości. Zakres minimalny to:

- Nazwa użytkownika
- Data i godzina wykonania czynności

Wykonawcy nie wolno zbierać jakichkolwiek haseł albo informacji poufnych.
W celu uzyskania najlepszych wyników prowadzonych testów Wykonawca uzgodni z Zamawiającym wykonanie w odpowiednich przerwach oraz o określonych godzinach. Pod uwagę zostaną wzięte również lokalizacje fizyczne w celu rozproszenia informacji przekazywanych pomiędzy osobami znającymi się na określonym środowisku.