Mirów, dnia 18.06.2025 r.

Znak sprawy: **BG.271.7.2025**

- do wszystkich Wykonawców –

Zawiadomienie o zmianie treści zapytania ofertowego i przedłużeniu terminu składania ofert

dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym pn.: **„Sporządzenie audytu wraz z realizacją usług szkoleniowych”** w ramach zadania inwestycyjnego pn.: **„Cyberbezpieczny Mirów”.**

Zamawiający informuje, że w odpowiedzi na zadane pytania dotyczące treści zapytania ofertowego nr BG.271.7.2025 z dnia 11.06.2025 r., dotyczącym „Sporządzenie audytu wraz z realizacją usług szkoleniowych”, wprowadza następujące zmiany:

1. W treści zapytania ofertowego:
   1) w pkt. 3 zapytania - opisie przedmiotu zamówienia **było:**

- przeprowadzenie audytu systemu zarządzania bezpieczeństwem informacji wraz z wypełnieniem końcowej ankiety dojrzałości do projektu Cyberbezpieczny Samorząd
- przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa dla pracowników Urzędu Gminy Mirów
- przeprowadzenie szkolenia z zakresu bezpieczeństwa sieci komputerowych oraz Active Directory dla informatyka Urzędu Gminy Mirów

w pkt. 3 zapytania - opisie przedmiotu zamówienia **jest:**

- przeprowadzenie audytu systemu zarządzania bezpieczeństwem informacji
- przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa dla pracowników Urzędu Gminy Mirów wraz z przeprowadzeniem kampanii phishingowej
- przeprowadzenie szkolenia z zakresu bezpieczeństwa sieci komputerowych oraz Active Directory dla informatyka Urzędu Gminy Mirów

   2) w pkt. 7 zapytania - opis warunków udziału w postępowaniu było:
   O udzielenie zamówienia mogą się ubiegać Wykonawcy, którzy:
   - Dysponują co najmniej jednym audytorem posiadającym uprawnienia - certyfikat Audytora Wiodącego Systemu Zarządzania Bezpieczeństwem Informacji wg normy ISO 27001 lub równoważny (skan dokumentu należy dołączyć do oferty);
   - Posiadają niezbędną wiedzę i doświadczenie oraz dysponują potencjałem technicznym i osobami zdolnymi do wykonania zamówienia
   - znajdują się w sytuacji ekonomicznej i finansowej i ekonomicznej zapewniającej wykonanie zamówienia

w pkt. 7 zapytania - opis warunków udziału w postępowaniu **jest:**

O udzielenie zamówienia mogą się ubiegać Wykonawcy, którzy:

- Dysponują co najmniej jednym audytorem posiadającym uprawnienia - certyfikat Audytora Wiodącego Systemu Zarządzania Bezpieczeństwem Informacji wg normy ISO 27001 lub równoważny (skan dokumentu należy dołączyć do oferty);
- dysponują co najmniej jedną osobą posiadającą certyfikat menadżer bezpieczeństwa informacji lub równoważny (skan dokumentu należy dołączyć do oferty);
- posiadają co najmniej dwuletnie doświadczenie osobowe w zakresie realizacji usług audytowych oraz szkoleniowych, przy czym przez dwuletnie doświadczenie rozumie się konieczność przedłożenia referencji potwierdzającej należyte wykonanie przynajmniej jednej usługi audytu systemu zarządzania bezpieczeństwem informacji oraz przynajmniej jednej usługi szkolenia
  z zakresu cyberbezpieczeństwa w okresie ostatnich dwóch lat (referencje należy dołączyć do oferty);
- znajdują się w sytuacji ekonomicznej i finansowej i ekonomicznej zapewniającej wykonanie zamówienia

3) w pkt. 10 ppkt. b zapytania - opis przygotowania oferty **było:**

Zamawiający informuje, że oferta musi zawierać następuje informacje i dokumenty:

- wypełniony Formularz Ofertowy stanowiący Załącznik nr 1;
- wymagany certyfikat Audytora Wiodącego Systemu Zarządzania Bezpieczeństwem Informacji wg normy ISO 27001 lub dokument równoważny (skan dokumentu dołączyć do oferty).

w pkt. 10 ppkt. b zapytania - opis przygotowania oferty **jest:**

Zamawiający informuje, że oferta musi zawierać następuje informacje i dokumenty:

- wypełniony Formularz Ofertowy stanowiący Załącznik nr 1;
- wymagany certyfikat Audytora Wiodącego Systemu Zarządzania Bezpieczeństwem Informacji wg normy ISO 27001 lub dokument równoważny (skan dokumentu dołączyć do oferty).
- certyfikat menadżer bezpieczeństwa informacji lub równoważny (skan dokumentu należy dołączyć do oferty);
- dokumenty potwierdzające co najmniej dwuletnie doświadczenie osobowe w zakresie realizacji usług audytowych oraz szkoleniowych, przy czym przez dwuletnie doświadczenie rozumie się konieczność przedłożenia referencji potwierdzającej należyte wykonanie przynajmniej jednej usługi audytu systemu zarządzania bezpieczeństwem informacji oraz przynajmniej jednej usługi szkolenia z zakresu cyberbezpieczeństwa w okresie ostatnich dwóch lat (referencje należy dołączyć do oferty);

2. W opisie przedmiotu zamówienia:
   1) W pkt.2/ OPZ - przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa dla pracowników Urzędu Gminy Mirów **było:**

Zamawiający wymaga jednokrotnego przeprowadzenia szkolenia dla pracowników Urzędu Gminy Mirów. Ilość pracowników: 21 osób. Zamawiający wymaga, aby szkolenie przeprowadzone zostało z podziałem na dwie grupy szkoleniowe, po 2 h szkolenia dla każdej z grup. Szkolenie dla obu grup powinno odbyć się w formie online i zostać zorganizowane w trakcie jednego dnia roboczego.

Tematyka szkolenia powinna zawierać minimum omówienie poprawnych zasad związanych z cyberbezpieczeństwem. Ponadto wymaga się, aby zostały omówione zagrożenia w sieci takie jak phishing, ransomware oraz malware, które powodują poważne zagrożenia dla bezpieczeństwa informacji.

Zamawiający określa minimalny zakres szkolenia:

1. Wprowadzenie do cyberbezpieczeństwa - definicja i znaczenie cyberbezpieczeństwa w administracji publicznej. Omówienie roli i odpowiedzialności pracowników w utrzymaniu bezpieczeństwa informacji.
2. Podstawowe zasady cyberbezpieczeństwa - omówienie fundamentalnych reguł i procedur dotyczących ochrony danych, zarządzania hasłami, autoryzacji i bezpiecznego korzystania z zasobów informatycznych.
3. Phishing i inne ataki socjotechniczne - rozpoznawanie i ochrona przed próbami wyłudzenia informacji, atakami phishingowymi oraz innymi technikami socjotechnicznymi.
4. Zagrożenia związane z oprogramowaniem typu ransomware i malware - identyfikacja, mechanizmy działania oraz metody zapobiegania i reagowania na zagrożenia związane z ransomware i malware.
5. Bezpieczna obsługa poczty elektronicznej - zasady korzystania z e-maila, rozpoznawanie podejrzanych wiadomości, załączników oraz linków, a także ochrona przed spamem i phishingiem.
6. Zarządzanie hasłami i autoryzacja - tworzenie silnych haseł, korzystanie z menedżerów haseł, wprowadzenie autoryzacji dwuetapowej oraz znaczenie kluczy sprzętowych.
7. Ochrona urządzeń mobilnych - zabezpieczanie urządzeń przenośnych, takich jak smartfony
   i tablety, przed utratą danych, kradzieżą oraz złośliwym oprogramowaniem.
8. Bezpieczne przetwarzanie i przechowywanie danych - szyfrowanie danych, zasady bezpiecznego przechowywania informacji, zarządzanie dostępem oraz udostępnianie danych w sposób bezpieczny.
9. Zarządzanie ryzykiem w cyberbezpieczeństwie - identyfikacja i ocena ryzyka, zarządzanie ryzykiem oraz wdrażanie odpowiednich środków zabezpieczających.
10. Ochrona przed spoofingiem i atakami telefonicznymi - mechanizmy ochrony przed spoofingiem, fałszowaniem numerów telefonów oraz innymi technikami oszustw telefonicznych.

11. **Bezpieczna komunikacja w środowisku cyfrowym**- szyfrowanie komunikacji, korzystanie z bezpiecznych kanałów komunikacyjnych, zabezpieczenie wideokonferencji oraz przesyłania danych.
12. **Ochrona przed wyłudzeniami danych osobowych (PII)** - zapobieganie wyłudzeniom danych osobowych za pomocą metod socjotechnicznych oraz przeciwdziałanie kradzieży tożsamości.

Zamawiający wymaga, aby Wykonawca wydał uczestnikom imienne certyfikaty oznaczone zgodnie z wymaganiami projektu Cyberbezpieczny Samorząd.

W pkt.2/ OPZ - przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa dla pracowników Urzędu Gminy Mirów **jest:**

Zamawiający wymaga jednokrotnego przeprowadzenia szkolenia dla pracowników Urzędu Gminy Mirów. Ilość pracowników: 21 osób. Zamawiający wymaga, aby szkolenie przeprowadzone zostało z podziałem na dwie grupy szkoleniowe, po 2 h szkolenia dla każdej z grup. Szkolenie dla obu grup powinno odbyć się w formie online i zostać zorganizowane w trakcie jednego dnia roboczego.
Tematyka szkolenia powinna zawierać minimum omówienie poprawnych zasad związanych z cyberbezpieczeństwem. Ponadto wymaga się, aby zostały omówione zagrożenia w sieci takie jak phishing, ransomware oraz malware, które powodują poważne zagrożenia dla bezpieczeństwa informacji.

Zamawiający określa minimalny zakres szkolenia:

1. **Wprowadzenie do cyberbezpieczeństwa** - definicja i znaczenie cyberbezpieczeństwa w administracji publicznej. Omówienie roli i odpowiedzialności pracowników w utrzymaniu bezpieczeństwa informacji.
2. **Podstawowe zasady cyberbezpieczeństwa** - omówienie fundamentalnych reguł i procedur dotyczących ochrony danych, zarządzania hasłami, autoryzacji i bezpiecznego korzystania z zasobów informatycznych.
3. **Phishing i inne ataki socjotechniczne** - rozpoznawanie i ochrona przed próbami wyłudzenia informacji, atakami phishingowymi oraz innymi technikami socjotechnicznymi.
4. **Zagrożenia związane z oprogramowaniem typu ransomware i malware** - identyfikacja, mechanizmy działania oraz metody zapobiegania i reagowania na zagrożenia związane z ransomware i malware.
5. **Bezpieczna obsługa poczty elektronicznej** - zasady korzystania z e-maila, rozpoznawanie podejrzanych wiadomości, załączników oraz linków, a także ochrona przed spamem i phishingiem.

6. Zarządzanie hasłami i autoryzacja - tworzenie silnych haseł, korzystanie z menedżerów haseł, wprowadzenie autoryzacji dwuetapowej oraz znaczenie kluczy sprzętowych.
7. Ochrona urządzeń mobilnych - zabezpieczanie urządzeń przenośnych, takich jak smartfony
   i tablety, przed utratą danych, kradzieżą oraz złośliwym oprogramowaniem.
8. Bezpieczne przetwarzanie i przechowywanie danych - szyfrowanie danych, zasady bezpiecznego przechowywania informacji, zarządzanie dostępem oraz udostępnianie danych w sposób bezpieczny.
9. Zarządzanie ryzykiem w cyberbezpieczeństwie - identyfikacja i ocena ryzyka, zarządzanie ryzykiem oraz wdrażanie odpowiednich środków zabezpieczających.
10. Ochrona przed spoofingiem i atakami telefonicznymi - mechanizmy ochrony przed spoofingiem, fałszowaniem numerów telefonów oraz innymi technikami oszustw telefonicznych.
11. Bezpieczna komunikacja w środowisku cyfrowym - szyfrowanie komunikacji, korzystanie z bezpiecznych kanałów komunikacyjnych, zabezpieczenie wideokonferencji oraz przesyłania danych.
12. Ochrona przed wyłudzeniami danych osobowych (PII) - zapobieganie wyłudzeniom danych osobowych za pomocą metod socjotechnicznych oraz przeciwdziałanie kradzieży tożsamości.
13. Omówienie wyników kampanii phishingowej.

Zamawiający wymaga, aby Wykonawca wydał uczestnikom imienne certyfikaty oznaczone zgodnie z wymaganiami projektu Cyberbezpieczny Samorząd.

Przeprowadzenie szkolenia musi poprzedzać wykonanie kampaii phishgowej zgodnie z poniższym harmonogramem:

Tydzień 1: planowanie i przygotowanie techniczne

Dzień 1 - analiza i planowanie:

- Rozmowa z Wykonawcą - omówienie potrzeb Zamawiającego oraz ustalenie szczegółowych celów kampanii;
- Zbieranie informacji - identyfikacja grup docelowych i preferowanych metod ataku phishingowego.

Dzień 2 - wybór scenariuszy i metod

- wybór scenariuszy - wybór realistycznych scenariuszy z użyciem platformy Proofpoint, takich jak:
  - Drive-by phishing - kampania, która próbuje skłonić użytkownika do kliknięcia na link do symulowanej złośliwej strony. Po kliknięciu użytkownik jest przekierowywany do platformy szkoleniowej (*opcjonalnie – do ustalenia);

- Data Entry phishing - kampania, która próbuje nakłonić użytkownika do wprowadzenia danych uwierzytelniających na fałszywej stronie. Użytkownicy są następnie przekierowywani do platformy szkoleniowej (*opcjonalnie – do ustalenia);
- Classic Attachment phishing - kampania, która próbuje nakłonić użytkownika do otwarcia symulowanego złośliwego załącznika w formacie DOC lub HTML. Po otwarciu użytkownicy otrzymują dostosowaną treść edukacyjną (*opcjonalnie – do ustalenia);
- Attachment phishing - kampania, która próbuje nakłonić użytkownika do otwarcia symulowanego złośliwego załącznika w formacie PDF, DOCX lub XLSX. Użytkownicy są przekierowywani do platformy szkoleniowej lub otrzymują standardową wiadomość z linkiem do platformy szkoleniowej (*opcjonalnie – do ustalenia).

Dzień 3 - przygotowanie techniczne

- Konfiguracja platformy - ustawienia platformy, dodanie użytkowników;
- Przygotowanie szablonów - konfiguracja symulacji phishingowych z użyciem dostępnych szablonów.

Dzień 4 - testy techniczne

- Testy systemu - przeprowadzenie testów kampanii, weryfikacja poprawności działania e-maili phishingowych.

Dzień 5 - finalizacja przygotowań

- Ostateczne dostosowanie - finalizacja konfiguracji i scenariuszy, przygotowanie do wdrożenia kampanii.

Tydzień 2 - pierwsza tura kampanii phishingowych

Dzień 1 – 3: rozpoczęcie Kampanii

- Wysyłka e-maili phishingowych #1: Rozesłanie pierwszej serii e-maili phishingowych, obejmujących różne metody (Drive-by, Data Entry, Classic Attachment, Attachment);
- Monitorowanie reakcji - śledzenie reakcji użytkowników i zbieranie danych;
- Informacja zwrotna - pracownicy, którzy padli ofiarą phishingu, otrzymają natychmiastową zwrotną informację z opisem błędu oraz dostępem do specjalistycznego szkolenia (*opcjonalnie – do ustalenia).

Dzień 4 - 5: kontynuacja kampanii

- Wysyłka e-maili phishingowych #2 - rozesłanie drugiej serii e-maili phishingowych;
- Monitorowanie reakcji - śledzenie reakcji i analizowanie wyników;
- Informacja zwrotna - pracownicy, którzy padli ofiarą phishingu, otrzymają zwrotną informację i zaproszenie na szkolenie (*opcjonalnie – do ustalenia).

Tydzień 3 - druga tura kampanii phishingowych

1 Dzień - analiza i Edukacja

- Analiza wyników - przegląd wyników z pierwszej tury;
- Edukacja użytkowników - szkolenia dla pracowników, którzy padli ofiarą phishingu. Informacje zwrotne będą zawierały szczegóły o ataku oraz instrukcje, jak unikać podobnych sytuacji (*opcjonalnie – do ustalenia).

Dzień 2 – 3: kontynuacja kampanii

- Wysyłka e-maili phishingowych #3 - rozesłanie trzeciej serii e-maili phishingowych;
- Monitorowanie reakcji: Śledzenie i analiza reakcji użytkowników;
- Informacja zwrotna: Pracownicy otrzymają informację o ich reakcji oraz zaproszenie do dalszego szkolenia (*opcjonalnie – do ustalenia).

Dzień 4 – 5: kontynuacja kampanii

- Wysyłka e-maili phishingowych #4 - rozesłanie czwartej serii e-maili phishingowych;
- Monitorowanie reakcji - śledzenie i analiza wyników;
- Informacja zwrotna - pracownicy, którzy padli ofiarą phishingu, otrzymają szczegółową informację o ataku i dostęp do zaawansowanego szkolenia z zakresu bezpieczeństwa (*opcjonalnie – do ustalenia).

Tydzień 4 - trzecia tura kampanii phishingowych i ewaluacja

Dzień 1 - analiza i ewaluacja

- Analiza wyników - przegląd wyników z drugiej tury;
- Edukacja i wsparcie - dodatkowe szkolenia dla pracowników, uwzględniające różnorodne techniki i metody ataków, takie jak złośliwe załączniki i niebezpieczne adresy URL (*opcjonalnie – do ustalenia).

Dzień 2- 3: kontynuacja kampanii

- Wysyłka e-maili phishingowych #5 - rozesłanie piątej serii e-maili phishingowych.

- Monitorowanie reakcji - śledzenie i analiza reakcji użytkowników.
- Informacja zwrotna - pracownicy, którzy padli ofiarą ataków, otrzymają pełne informacje o ataku oraz dostęp do specjalistycznego szkolenia (*opcjonalnie – do ustalenia).

Dzień 4 - kontynuacja kampanii

- Wysyłka e-maili phishingowych #6 - rozesłanie szóstej serii e-maili phishingowych;
- Monitorowanie reakcji - śledzenie i analiza wyników.

Dzień 5 - podsumowanie Kampanii

- Raport końcowy - przygotowanie raportu z wynikami kampanii;
- Rozmowa z Zamawiającym - przedstawienie wyników, wniosków i rekomendacji na przyszłość.

(*opcjonalnie – do ustalenia) – pracownicy Zamawiającego mogą być na bieżąco informowani o popełnieniu błędu i o ofiarą ataku phishingowego, bądź informacja taka może zostać udostępniona dopiero na końcowym etapie kampanii (wszelkie informacje o atakach na dane stanowiska będą zbierane i udostępnione pracownikowi zbiorczo po zakończeniu kampanii) – do decyzji Zamawiającego na każdym etapie prowadzenia kampanii.

W związku z powyższymi zmianami wprowadzonymi w przedmiotowym postępowaniu, Zamawiający **przedłuża termin składania ofert do dnia 26.06.2025 r. do godz. 10.00.** Otwarcie ofert odbędzie się w dniu **26.06.2025 r. do godz. 10.30.**

Artur
Wawrzyniec
Siwiorek

Elektronicznie podpisany przez Artur Wawrzyniec Siwiorek
Data: 2025.06.18 09:23:30 +02'00'