ZFP.042.1.1.2024.IK

GMINA CHOSZCZNO
ul. Wolności 24
73-200 Choszczno
NIP: 594-153-03-07

Cyberbezpieczny Samorząd

Zapytanie ofertowe na zadanie:

„Zakup pakietu szkoleń z zachowania w cyberprzestrzeni, bezpiecznej pracy zdalnej wraz z realizacją kampanii phisingowych dla pracowników"

I. Zamawiający:

Urząd Miejski
ul. Wolności 24
73-200 Choszczno
Tel. +48 95 765 93 00 Fax. +48 95 765 93 06
sekretariat@choszczno.pl
www.choszczno.pl

II. Przedmiot zamówienia:

Opis projektu

W związku z realizacją projektu p.n. „Zwiększenie cyberbezpieczeństwa Urzędu Miejskiego w Choszcznie", realizowanego w ramach programu Cyberbezpieczny Samorząd, zwracamy się z zapytaniem ofertowym.

Celem realizowanego projektu jest zwiększenie poziomu bezpieczeństwa informacji Urzędu Miejskiego w Choszcznie. Projekt realizuje cel szczegółowy Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, Działanie 2.2 - Wzmocnienie Krajowego Systemu Cyberbezpieczeństwa w zakresie zapewnienia cyberbezpieczeństwa Urzędu poprzez budowę, rozwój oraz wdrożenie narzędzi służących do monitorowania bezpieczeństwa, zbierania, analizy i wymiany informacji o zagrożeniach, podatnościach i incydentach, a także poprzez rozwój kompetencji cyfrowych pracowników Urzędu w obszarze cyberbezpieczeństwa.

Przedmiotem zamówienia jest dostarczenie usługi szkolenia pracowników w Urzędu Miejskiego w Choszcznie z zakresu cyberbezpieczeństwa wraz z przeprowadzeniem kampanii phisingowej.

W ramach usługi oczekiwane są następujące działania:

- Przygotowanie cyklu min. 5 szkoleń dla pracowników z zakresu cyberbezpieczeństwa,
- Zaplanowanie i przeprowadzenie 4 kampanii phisingowej dla pracowników Urzędu,
- Przeprowadzenie 2 cykli szkoleń dla pracowników Urzędu z zakresu zachowania się w cyberprzestrzeni.
- Cykle szkoleniowe mają być przeprowadzone w okresie 22 miesięcy,
- Kampanie phisingowe mają być przeprowadzone w okresie 22 miesięcy od podpisania zlecenia.

Liczba osób do przeszkolenia: 100

Klasyfikacja przedmiotu zamówienia zgodnie ze **Wspólnym Słownikiem Zamówień CPV**

80550000-4- Usługi szkolenia w dziedzinie bezpieczeństwa
80533100-0 - Usługi szkolenia komputerowego

II.A Wymagania w zakresie zakresu realizacji szkoleni:

1. Pakiet szkoleniowy w którego skład wchodzą 5 szkoleń oraz moduły treningowe dostępne dla każdego pracownika w formie kursu online do samodzielnego przerobienia przez okres 22 miesięcy.
2. Każde Szkolenie musi kończyć się testem do wypełnienia dla pracowników.

3. Po okresie 12 miesięcy szkolenia mają być uaktualnione o nowe zagadnienia uzgodnione z zamawiającym,
4. Poziom zdawalności testu zostanie ustawiony po konsultacjach z zamawiającym.
5. Zakres raportu końcowego z przeprowadzonych szkoleń:
    a. Podsumowanie Szkolenia
        i. Tytuł i cel szkolenia: Krótki opis szkolenia, jego głównych celów i oczekiwanych korzyści dla uczestników.
        ii. Data i czas trwania: Informacje, kiedy szkolenie zostało zainicjowane i zakończone.
        iii. Format szkolenia: Opis platformy e-learningowej i narzędzi wykorzystanych do przeprowadzenia szkolenia.
    b. Uczestnictwo
        i. Liczba zaproszonych uczestników: Ile osób zostało zaproszonych do udziału w szkoleniu.
        ii. Liczba uczestniczących osób: Ile osób faktycznie wzięło udział w szkoleniu.
        iii. Frekwencja: Procent uczestników, którzy faktycznie wzięli udział w szkoleniu w stosunku do liczby zaproszonych.
    c. Wyniki Szkolenia
        i. Średnie wyniki testów: Średnie wyniki osiągnięte przez uczestników w testach wiedzy przeprowadzonych przed i po szkoleniu.
        ii. Analiza postępów: Porównanie wyników przed i po szkoleniu, aby ocenić przyrost wiedzy.
        iii. Oceny końcowe: Jak uczestnicy poradzili sobie z końcowymi testami lub ocenami.
    d. Zaangażowanie Uczestników
        i. Statystyki z platformy e-learningowej: Dane na temat aktywności uczestników na platformie, np. czas spędzony na kursie, strony odwiedzane najczęściej, interakcje z materiałami.
        ii. Feedback uczestników: Zbieranie i analiza opinii uczestników na temat użyteczności szkolenia, jakości materiałów i ogólnej satysfakcji.
    e. Ocena Efektywności Szkolenia
        i. Analiza osiągniętych celów szkoleniowych: Ocena, czy i w jakim stopniu osiągnięto cele szkoleniowe.
        ii. Rekomendacje dla przyszłych szkoleń: Sugestie dotyczące zmian w treści, formacie lub dostarczaniu materiału szkoleniowego, na podstawie analizy danych i feedbacku.
    f. Działania Poprawkowe i Kontynuacja Edukacji
        i. Zaplanowane działania poprawkowe: Działania zaplanowane w odpowiedzi na wykryte luki w wiedzy lub umiejętnościach.
        ii. Zaplanowane kolejne kroki szkoleniowe: Informacje o przyszłych szkoleniach lub kursach uzupełniających.
    g. Podsumowanie i Wnioski
        i. Ogólne wnioski: Podsumowanie kluczowych wniosków z przeprowadzonego szkolenia.
        ii. Zalecenia strategiczne: Zalecenia na poziomie organizacyjnym dotyczące dalszego rozwoju programów szkoleniowych z cyberbezpieczeństwa.
6. Zakres podstawowy szkoleń:
    a. Podstawowe pojęcia odnośnie bezpieczeństwa informacji, cyberbezpieczeństwa
    b. Zagrożenia związane z cyfrową działalnością gminy
        i. Rodzaje zagrożeń w cyberprzestrzeni
        ii. Rodzaje zabezpieczeń, rodzaje działań zabezpieczających

iii. Podstawy bezpiecznego zachowania w cyberprzestrzeni
c. Rozpoznawanie zagrożeń i im przeciwdziałanie
d. Bezpieczne hasła – jakie, jak je przechowywać
e. Bezpieczne poruszanie się w cyfrowym świecie – media społecznościowe, email, strony www, sklepy internetowe
    i. Zasady bezpiecznej pracy w cyfrowym świecie
f. Nośniki zewnętrzne
g. Komunikatory i media społecznościowe
h. Poczta elektroniczna
    i. Zarządzanie zdarzeniami i incydentami bezpieczeństwa
i. Wdrożenie i utrzymanie systemu zarządzania bezpieczeństwem informacji
    i. Źródła wymagań i zaleceń - norma ISO 27001 oraz ISO 27002.
    ii. Role i odpowiedzialności.
    iii. Klasyfikacja informacji.
    iv. Analiza ryzyka bezpieczeństwa informacji.
    v. Zarządzanie ryzykiem bezpieczeństwa informacji.
    vi. Zabezpieczenia techniczne i organizacyjne.
    vii. Struktura dokumentacji systemu zarządzania.
    viii. Szkolenia pracowników.
    ix. Utrzymanie systemu zarządzania
j. Zagrożenia jakie można spotkać w Internecie,
k. Metodyka skutecznego oceniania wiarygodności otrzymanej wiadomości mailowej,
l. najczęściej spotykane zagrożenia związane z korzystaniem z serwisów społecznościowych,
m. Czym jest ransomware i jak się przed nim bronić.

II.B Wymagania w zakresie realizacji kampanii phisingowej

1. Do przeprowadzenia kampanii phisingowych wykorzystane muszą być komercyjne platformy lub oprogramowanie komercyjne służące do tworzenia tego typu platform,
2. W okresie 22 miesięcy od podpisania zlecenia mają być przeprowadzone 4 kampanie phisingowe,
3. Koszty subskrypcji platformy phisingowej pokrywa wykonawca,
4. Każda z kampanii phisingowych zostanie uzgodniona z zamawiającym w zakresie typów maili i ich formy,
5. Raporty bieżące dotyczące kampanii phisingowej powinny zawierać:
    a. Statystyki kampanii w tym:
        i. Ilość wysłanych maili,
        ii. Ilość dostarczonych maili,
        iii. Ilość skompromitowanych kont pocztowych,
    b. Informacje o użytkownikach, w tym:
        i. Określenie poziomu ryzyka użytkownika dla organizacji,
        ii. Status realizacji kampanii przez użytkownika,
        iii. Status realizacji szkoleń przez użytkownika,
6. Planowanie Kampanii
    a. Realistyczne Symulacje Ataków Phishingowych
        i. Scenariusze dostosowane do administracji publicznej: Symulacje powinny odwzorowywać ataki, na które urząd miasta może być rzeczywiście narażony, np. fałszywe faktury, podrobione pisma urzędowe, próby wyłudzenia informacji o mieszkańcach.
    b. Zaawansowana personalizacja kampanii: Możliwość dostosowywania treści phishingowych do różnych działów urzędu, np. różne kampanie dla działu finansowego, kadr, czy obsługi mieszkańców, z uwzględnieniem

języka specyficznego dla danego obszaru.

7. Śledzenie Postępów i Raportowanie
    a. Zaawansowane narzędzia raportowe: Platforma powinna oferować szczegółowe raporty dotyczące wyników kampanii phishingowych i postępów w szkoleniach, z opcją dostosowania do wymagań urzędu.
    b. Wizualizacja danych: Dashboardy i infografiki prezentujące kluczowe metryki, które pomagają w zrozumieniu skuteczności kampanii i szkoleń.
8. Bezpieczeństwo i Prywatność
    a. Szyfrowanie danych wrażliwych: Pełne szyfrowanie danych osobowych i innych wrażliwych informacji zarówno podczas transmisji, jak i w spoczynku.
    b. Zgodność z RODO i lokalnymi przepisami o ochronie danych: Zapewnienie, że wszystkie operacje na danych są zgodne z obowiązującymi przepisami o ochronie danych osobowych.
9. 6. Zarządzanie Kampaniami
    a. Automatyzacja procesów: Narzędzia do automatyzacji uruchamiania i zarządzania kampaniami phishingowymi, minimalizujące potrzebę interwencji manualnej.
    b. Interaktywny feedback: Możliwość zgłaszania przez użytkowników podejrzanych wiadomości, co może być wykorzystane do poprawy przyszłych kampanii.
10. Wsparcie Techniczne i Szkoleniowe
    a. Dostępność wsparcia technicznego: Łatwy dostęp do wsparcia technicznego w razie wystąpienia problemów z platformą.
    b. Materiały pomocnicze dla administratorów: Kompleksowe przewodniki i materiały szkoleniowe, wspierające zarządzanie platformą.
11. Raport końcowy z zakończenia kampanii phisingowej powinien zawierać:

    a. Podsumowanie Kampanii
        i. Opis kampanii: Krótkie streszczenie celów kampanii, zastosowanych technik phishingowych, i grupy docelowej.
        ii. Okres przeprowadzenia kampanii: Data rozpoczęcia i zakończenia kampanii.
    b. Statystyki Ogólne
        i. Liczba wysłanych wiadomości: Ile e-maili phishingowych zostało wysłanych w ramach kampanii.
        ii. Procent otwartych e-maili: Jaki procent odbiorców otworzył e-mail.
        iii. Procent kliknięć w linki: Jaki procent osób kliknął w linki zawarte w e-mailach phishingowych.
        iv. Liczba wprowadzonych danych: Ile osób podało swoje dane na fałszywej stronie.
    c. Analiza Zachowań Użytkowników
        i. Typowe błędy: Jakie błędy najczęściej popełniali pracownicy, np. ignorowanie oznak ostrzegawczych.
        ii. Wzorce odpowiedzi: Czy istnieją konkretne wzorce w odpowiedziach różnych grup pracowników lub działów.
        iii. Porównanie z innymi kampaniami: Jak kampania wypada na tle danych statystycznych z innych kampanii pod względem efektywności i zachowań pracowników.
        iv. Szczegółowe Wyniki dla Różnych Grup Docelowych
            1. Wyniki według działów: Szczegółowa analiza reakcji różnych działów lub grup zawodowych na kampanię.

2. Wyniki według lokalizacji: Jeśli urząd ma więcej niż jedną lokalizację, analiza, jak reakcje różniły się między lokalizacjami.

d. Rekomendacje i Ścieżki Naprawcze
   i. Obszary wymagające poprawy: Wskazanie, które obszary wiedzy lub świadomości wymagają dodatkowych działań edukacyjnych.
   ii. Zaproponowane działania szkoleniowe: Propozycje konkretnych szkoleń lub warsztatów, które mogłyby zwiększyć świadomość i umiejętności pracowników.
   iii. Plan poprawek: Krótkoterminowe i długoterminowe działania, które urząd powinien podjąć, aby poprawić bezpieczeństwo informacyjne.
e. Feedback od Uczestników
   i. Opinie pracowników: Jak pracownicy odebrali kampanię, co było dla nich szczególnie trudne lub łatwe, oraz jakie mają sugestie.
f. Metodologia
   i. Opis metodologii: Wyjaśnienie, jak dane były zbierane, analizowane i interpretowane.
   ii. Ograniczenia kampanii: Jakie ograniczenia mogły wpłynąć na wyniki i jak mogą być one adresowane w przyszłości.

II.C Wymagania w zakresie wykorzystania platformy szkoleniowej i phisingowej

1. Platforma musi umożliwiać komunikację w języku polskim,
2. Platforma musi być dostępna na platformie www,
3. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW
4. Rozwiązanie musi posiadać możliwość zarządzania
5. Rozwiązanie musi posiadać minimum 80 szablonów kampanii phisingowych, przygotowanych przez producenta do wyboru,
6. Platforma musi umożliwiać tworzenie własnych kampanii phisingowych,
7. Platforma musi umożliwiać wytworzenie materiałów w języku polskim,
8. Platforma musi zapewniać:
   a. Planowanie kampanii (harmonogram uruchamiania treści, wybór adresatów),
   b. Tworzenie grup odbiorców i dedykowanych dla tych grup wariantów maili,
   c. Śledzenie na bieżąco przebiegu kampanii,
9. Raportowanie przebiegu kampanii w postaci:
   a. pliku excela,
   b. pliku cvs,
   c. pliku w formacje pdf,
10. Możliwość tworzenia raportów okresowych:
    a. Dzienne,
    b. Tygodniowe,
    c. Miesięczne,
    d. Roczne.
11. Platforma powinna umożliwiać jednoczesne prowadzenie kampanii phisingowych oraz prowadzenie szkoleń,
12. Możliwość dowiązania szkolenia e-lerningowego do kampanii phisingowej,
13. Platforma e-learningowa powinna umożliwiać:
    a. Tworzenie własnych materiałów,
    b. Modyfikacje materiałów dostępnych na platformie e-lerningowej,
    c. Możliwość wykorzystania różnych form szkoleniowych:
       i. Prezentacja
       ii. Film,
       iii. Testy

14. Indywidualny dostęp dla każdego pracownika do jego konta na platformie,
15. Możliwość zdefiniowania dowolnego okna czasowego w którym platforma szkoleniowa jest dostępna,
16. Możliwość zdefiniowania dowolnego okna czasowego w którym platforma phisingowa jest dostępna,
17. Możliwość wydania zaświadczenia o ukończeniu szkolenia
18. Przygotowanie materiałów do kampanii phisingowych w postaci:
    a. Maile,
    b. Strony pułapki,
    g. Profile wysyłającego maile,

III. Inne Wymagania dla Wykonawcy.

O udzielenie zamówienia mogą się ubiegać Wykonawcy, który posiada doświadczenie w postaci wykonania (a w przypadku świadczeń powtarzających się lub ciągłych również wykonywania) w okresie ostatnich trzech lat, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie co najmniej 3 (trzech) zamówień polegających na świadczeniu usługi szkolenia z zakresu cyberbezpieczeństwa wraz z realizacją kampanii phisingowych dla grupy 100 osób w każdym przypadku,

IV. Harmonogram realizacji zamówienia

Termin realizacji przedmiotu zamówienia - 22 miesiące od dnia podpisania zlecenia.

V. Kryteria i sposób oceny ofert

1. Zamawiający będzie oceniał wyłącznie oferty spełniające poniższe wymagania, w tym podstawowe – iż, złożona oferta dotyczy **Zakup pakietu szkoleń z zachowania w cyberprzestrzeni, bezpiecznej pracy zdalnej wraz z realizacją kampanii phisingowych dla pracowników.**
2. Zamawiający będzie oceniał te oferty, które spełniają wszystkie wymagania zawarte w zapytaniu.

VI. Udzielenie zamówienia

Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiada wszystkim wymaganiom przedstawionym w zaproszeniu do składania ofert.

VII. Termin i miejsce składania ofert

1. Ofertę należy złożyć drogą mailową na adres: ikolanczyk@gmina.choszczno.pl do **dnia 29.07.2024 r. do godz.15.00.** Oferty złożone po tym terminie nie będą brane pod uwagę.
2. Oferta powinna być sporządzona w języku polskim. Cena musi być podana w PLN cyfrowo oraz być wartością brutto. Złożona oferta musi uwzględniać wszystkie zobowiązania, obejmować wszystkie koszty i składniki związane z wykonaniem zamówienia.
3. Do oferty należy dołączyć następujące dokumenty:
   1) formularz ofertowy – wypełniony i podpisany;
   2) aktualny wpis do Centralnej Ewidencji i Informacji o Działalności Gospodarczej Rzeczypospolitej Polskiej lub odpis z KRS;
4. Osoby wyznaczone do kontaktu z Dostawcą: Pan/Pani Izabela Kolańczyk tel. 95/765 93 93 w godz. od 9.00 do 15.00 oraz pod adresem email: ikolanczyk@gmina.choszczno.pl .
5. Zamawiający zastrzega sobie prawo do modyfikowania opisu przedmiotu zamówienia, w tym wzoru umowy oraz do unieważnienia postępowania bez podania przyczyn.

Cyberbezpieczny Samorząd

KLAUZULA INFORMACYJNA Z ART. 13 I 14 RODO

Zgodnie z art. 13 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE Nr 119) zwanym dalej RODO informuję, że:

1. Administratorem Pani/Pana danych osobowych jest Burmistrz Urzędu Miejskiego w Choszcznie,

3. Pani/Pana dane osobowe przetwarzane będą w celu wypełnienia obowiązków prawnych ciążących na gminie w związku z udzieleniem zamówienia publicznego w wybranym trybie postępowania, na podstawie art. 6 ust. 1 lit. c RODO.

4. Odbiorcami Pani/Pana danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa, np. osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o przepisy ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (tekst jednolity: Dz.U. z 2019 r., poz. 869).

5. Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego/organizacji międzynarodowej.

6. Pani/Pana dane osobowe będą przechowywane przez okres niezbędny do realizacji celów określonych w pkt 3, a po tym czasie przez okres oraz w zakresie wymaganym przez przepisy powszechnie obowiązującego prawa, tj. przepisy ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz aktach wykonawczych do tej ustawy.

7. W związku z przetwarzaniem Pani/Pana danych osobowych przysługują Pani/Panu następujące uprawnienia:

a) prawo dostępu do danych osobowych, w tym prawo do uzyskania kopii tych danych;

b) prawo do żądania sprostowania (poprawiania) danych osobowych – w przypadku gdy dane są nieprawidłowe lub niekompletne;

c) prawo do żądania ograniczenia przetwarzania danych osobowych.

8. Nie przysługuje Pani/Panu:

a) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;

b) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;

c) na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

9. Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych, w przypadku gdy przetwarzanie Pani/Pana danych osobowych narusza przepisy dotyczące ochrony danych osobowych.

10. Obowiązek podania Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach prawa, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego. Konsekwencje niepodania określonych danych wynikają bezpośrednio z tej ustawy. Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania.

W załączeniu:

1. „Formularz ofertowy"

BURMISTRZ
mgr Artur Raczyński

19.07.2024 r. .....

(data) (podpis kierownika Zamawiającego lub upoważnionego pracownika)