Warszawa, 6 listopada 2023 r.

**ZAPYTANIE OFERTOWE**

**dotyczące usługi przeprowadzenia szkoleniowej kampanii cyberbezpieczeństwa**

1. **NAZWA I ADRES ZAMAWIAJĄCEGO**

Ministerstwo Funduszy i Polityki Regionalnej

Departament Informatyki

ul. Wspólna 2/4

00-926 Warszawa

tel. 22 273 72 00

**Stacjonarne miejsce świadczenia usługi:**

ul. Wspólna 2/4

00-926 Warszawa

1. **PRZEDMIOT ZAMÓWIENIA**
2. Przedmiotem zamówienia jest przeprowadzenie na rzecz Zamawiającego usługi weryfikującej reakcję użytkowników poczty elektronicznej Zamawiającego na symulowane zagrożenia bezpieczeństwa teleinformatycznego, zwanej dalej „Cyberkampanią".
3. Celem Cyberkampanii jest podniesienie poziomu świadomości cyberbezpieczeństwa użytkowników poprzez symulowane ataki phishingowe rozsyłane drogą e-mailową oraz włączenie działań edukacyjnych w trakcie Cyberkampanii.
4. Zakres Cyberkampanii obejmuje:
   1. personalizację i konfigurację Cyberkampanii, zgodnie z wymaganiami określonymi w pkt. 5;
   2. prowadzenie i raportowanie przebiegu Cyberkampanii, zgodnie z wymaganiami określonymi w pkt. 6.
5. Wymagania funkcjonalne modułów Cyberkampanii:
   1. **Moduł „Phishing”** – umożliwia generowanie phishingowych e-maili z różną zawartością i częstotliwością, zależną od zachowania i reakcji użytkownika. Moduł powinien umożliwić wysyłanie „fałszywych" wiadomości e-mailowych, według wcześniej uzgodnionych z Zamawiającym szablonów lub scenariuszy. Po kliknięciu w link zawarty w wiadomości lub element graficzny lub plik w załączniku, użytkownik powinien zostać przekierowany na spersonalizowaną stronę szkoleniową, na której zostanie wyemitowany materiał edukacyjny w formie tekstu lub filmu o długości do 120 sekund. Strona musi zawierać logo Zamawiającego oraz informację o Cyberkampanii;
   2. **Moduł „Raportowanie”** – umożliwia generowanie raportów i zestawień pozwalających na ocenę zachowania i reakcji użytkownika na phishing, zaangażowania użytkownika w przyswajanie oraz wykorzystanie treści edukacyjnych. Moduł musi mieć możliwość wskazania grup użytkowników, którzy:

* poprzez notoryczne niewłaściwe postępowanie z podejrzanymi e-mailami tworzą największe ryzyko bezpieczeństwa teleinformatycznego,
* podatni na nośny i atrakcyjny temat lub treść fałszywych e-maili sporadycznie klikają w podejrzane e-maile z niebezpiecznymi linkami lub załącznikami lub wprowadzają poufne dane,
* przypadkowo klikają złośliwe e-maile, a ich zachowanie jest trudno przewidzieć, gdyż może być wynikiem zbiegu różnych okoliczności,
* prawidłowo reagują na podejrzane e-maile, zgłaszając je do zespołów obsługi incydentu.

Kryteria selekcji grup Wykonawca uzgodni z Zamawiającym na etapie personalizacji i konfiguracji Cyberkampanii.

1. Wymagania dotyczące personalizacji i konfiguracji Cyberkampanii:
   1. Cyberkampania będzie przeprowadzona dla maksymalnie 1300 użytkowników, w okresie 12 pełnych miesięcy, liczonych od faktycznego uruchomienia Cyberkampanii, czyli po dokonaniu jej personalizacji i konfiguracji;
   2. Wykonawca przygotuje 40 ustalonych z Zamawiającym, różnych – w zakresie formy, treści i trudności – szablonów „fałszywych" e-maili, które mogą być uszczegółowiane z Zamawiającym raz na kwartał przed ich wysłaniem do użytkownika. W procesie uzgadniania Zamawiający musi mieć możliwość testowania szablonów;
   3. Zamawiający będzie mieć możliwość przygotowania wspólnie z Wykonawcą indywidualnych treści phishingowych;
   4. w ramach Cyberkampanii każdy użytkownik powinien otrzymać minimum 1 „fałszywą" wiadomość miesięcznie, jednak nie więcej niż 15 w ciągu trwania całej Cyberkampanii. Wiadomości powinny symulować ataki phishingowe o różnym stopniu trudności;
   5. Cyberkampania musi być prowadzona w modelu as-a-service i nie może wymagać od Zamawiającego jakichkolwiek instalacji i konfiguracji, z wyjątkiem konfiguracji związanej z autoryzacją serwerów, z których będą wysyłane „fałszywe" wiadomości e-mailowe (konfiguracja White List itp.).
2. Wymagania dotyczące prowadzenia i raportowania przebiegu Cyberkampanii:
3. w terminie do 22 grudnia 2023 r. Wykonawca zgłosi Zamawiającemu e-mailowo gotowość do uruchomienia Cyberkampanii przedstawiając pierwszy kwartalny harmonogram prowadzenia Cyberkampanii i zestaw 10 szablonów e-maili przewidzianych do uruchomienia w pierwszym kwartale;
4. Wykonawca uruchomi Cyberkampanię w dniu 1 stycznia 2024 r., po wcześniejszym zaakceptowaniu przez Zamawiającego:

* szablonów „fałszywych" wiadomości e-mailowych, przewidzianych do wysłania w pierwszym kwartale świadczenia usługi. Warunkiem koniecznym akceptacji jest przesłanie szablonów na wskazany przez Zamawiającego adres e-mailowy,
* pierwszego kwartalnego harmonogramu prowadzenia Cyberkampanii, o którym mowa w pkt. 6a;

1. przed każdym kolejnym kwartalnym okresem prowadzenia kampanii Wykonawca ustali z Zamawiającym drogą e-mailową kwartalny harmonogram prowadzenia Cyberkampanii uwzględniający m.in.: liczbę i temat uruchamianych „fałszywych" wiadomości e-mailowych, liczbę i liczebność grup docelowych odbiorców „fałszywych" wiadomości e-mailowych, z podziałem na poszczególne tygodnie prowadzenia Cyberkampanii. Harmonogram może ulegać modyfikacji w zależności od stanu prowadzenia Cyberkampanii, wynikającego z raportów miesięcznych;
2. harmonogramy i szablony, o których mowa w pkt 6c, Wykonawca udostępni Zamawiającemu do akceptacji nie później niż na 10 dni przed rozpoczęciem każdego kolejnego kwartału prowadzenia Cyberkampanii;
3. Wykonawca udostępni Zamawiającemu dedykowany portal lub panel z dostępem do raportów zawierających, co najmniej, informacje na temat:

* ilości wysłanych e-maili oraz liczby kliknięć w fałszywe linki lub załączniki (w odniesieniu do wszystkich użytkowników wewnętrznych komórek organizacyjnych Zamawiającego, pełnionych funkcji, itp.),
* komórek organizacyjnych i osób najbardziej podatnych na phishing – o najwyższym poziomie ryzyka,
* wyników analizy wiadomości e-mail używanych do ataków, których treści spowodowały najwięcej kliknięć,
* liczby kliknięć ze względu na stopień trudności symulowanych ataków phishingowych;

1. Zamawiający dopuszcza dodatkowe inne raporty, które pozwolą na precyzyjną ocenę poziomu świadomości cyberbezpieczeństwa uczestników Cyberkampanii;
2. raporty muszą być interaktywne z możliwością drążenia;
3. raporty muszą być generowane w okresie miesięcznym. Raport za dany miesiąc trwania Cyberkampanii musi być dostępny w terminie 10 dni od zakończenia każdego miesiąca trwania Cyberkampanii. Raporty muszą być dostępne ze wszystkich miesięcy trwania Cyberkampanii;
4. Wykonawca przygotuje i zaprezentuje (zdalnie lub stacjonarnie) podsumowanie przeprowadzonej Cyberkampanii po każdym zakończonym kwartale świadczenia usług. W prezentacji Wykonawca przedstawi wnioski z raportów miesięcznych, trendy w zachowaniu użytkowników i propozycje zmian lub modyfikacji szablonów i scenariuszy phishingowych, dopasowujących do tych zachowań i aktualnych wyników Cyberkampanii.

7. Na czas realizacji usługi Wykonawca zapewni Zamawiającemu profesjonalne wsparcie techniczne i merytoryczne w zakresie zastosowanego rozwiązania. Zakłada się minimalny wysiłek po stronie Zamawiającego dzięki funkcjom wbudowanym w poszczególne moduły Cyberkampanii.

1. **WYMAGANIA DODATKOWE DOTYCZĄCE** **WYKONAWCY UBIEGAJĄCEGO SIĘ O REALIZACJĘ PRZEDMIOTU ZAMÓWIENIA**
2. Wykonawca musi posiadać odpowiednie kwalifikacje, wiedzę i doświadczenie niezbędne do należytego wykonania Przedmiotu Zamówienia, a także dysponować odpowiednim personelem i potencjałem ekonomicznym gwarantującym profesjonalną realizację Zamówienia.
3. Wykonawca zobowiązany jest do złożenia oświadczenia potwierdzającego, że nie zatrudnia i nie angażuje w jakiejkolwiek formie prawnej pracowników Zamawiającego oraz będzie zobowiązany w trakcie obowiązywania Umowy do niezatrudniania i nieangażowania w jakiejkolwiek formie prawnej tych pracowników.
4. Zamawiający wymaga posiadania przez Wykonawcę doświadczenia niezbędnego do należytego wykonania Przedmiotu Zamówienia. Zamawiający uzna ww. warunek za spełniony jeżeli Wykonawca – posługując się Wykazem usług, którego wzór stanowi Załącznik nr 3 do Zapytania ofertowego – wykaże, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wykonał należycie co najmniej 2 odrębne usługi weryfikujące reakcję użytkowników poczty elektronicznej na symulowane zagrożenia bezpieczeństwa teleinformatycznego, z których każda była świadczona dla co najmniej 400 użytkowników i w okresie co najmniej 30 dni z wykorzystaniem narzędzia zaoferowanego przez Wykonawcę.
5. **TERMIN REALIZACJI ZAMÓWIENIA**

Wykonawca zobowiązany jest.

1. wykonać usługi personalizacji i konfiguracji Cyberkampanii w terminie 7 dni roboczych[[1]](#footnote-1) od dnia zawarcia Umowy;
2. przeprowadzić Cyberkampanię i raportować Zamawiającemu jej przebieg przez okres 12 miesięcy, licząc od dnia 1.01.2024 r.
3. **SPOSÓB I TERMIN SKŁADANIA OFERT**
4. Ofertę należy przesłać za pośrednictwem poczty elektronicznej na adres**:** [**baza.ofert@mfipr.gov.pl**](mailto:baza.ofert@mfipr.gov.pl) **w** **terminie do 13 listopada 2023 r.**
5. Oferty dostarczone po terminie nie będą rozpatrywane.
6. Zamawiający informuje o możliwości zadania przez Wykonawcę pytania do treści niniejszego zapytania drogą e-mailową na adres [**baza.ofert@mfipr.gov.pl**](mailto:baza.ofert@mfipr.gov.pl).
7. **SPOSÓB PRZYGOTOWANIA OFERT**
8. Cena oferty powinna uwzględniać wszystkie zobowiązania, musi być podana w walucie polskiej, tj. PLN cyfrowo, wraz z należytym podatkiem VAT – jeżeli występuje.
9. Cena podana w ofercie powinna obejmować wszystkie koszty i składniki związane z wykonaniem zamówienia.
10. Ofertę należy złożyć w formie wypełnionego i podpisanego formularza ofertowego wraz z wykazem usług i dowodami potwierdzającymi, że wskazane usługi zostały należycie wykonane lub są należycie wykonywane – załączniki nr 1 i 3.
11. **WYBÓR NAJKORZYSTNIEJSZEJ OFERTY**
12. Zamawiający dokona oceny ofert, na podstawie następującego kryterium oceny ofert:

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Nazwa kryterium | Waga kryterium (w %) | Liczba punktów możliwych do uzyskania |
| 1 | Cena | 100% | 100 punktów |

1. Zamawiający dokona oceny ofert przyznając punkty w ramach poszczególnych kryteriów oceny ofert, przyjmując zasadę, że 1% = 1 punkt.
2. Punkty za kryterium „Cena” zostaną obliczone według wzoru:

Cena oferty najtańszej

------------------------------- x 100 = liczba punktów

Cena oferty badanej

Końcowy wynik powyższego działania zostanie zaokrąglony do dwóch miejsc po przecinku.

1. Za najkorzystniejszą zostanie uznana oferta z największą liczbą punktów.
2. Oferta, która nie spełni warunku, o którym mowa w pkt III.3 zostanie odrzucona.
3. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści zgłoszonych ofert.
4. Weryfikując ofertę pod względem poprawności, zamawiający zastrzega sobie prawo do poprawienia zaistniałych w niej:
5. oczywistych omyłek pisarskich,
6. oczywistych omyłek rachunkowych (uwzględniając konsekwencje rachunkowe dokonanych poprawek), niepowodujących istotnych zmian w treści oferty.
7. Zamawiający zastrzega sobie prawo do odpowiedzi tylko na wybraną ofertę.
8. Zamawiający zastrzega sobie prawo do rezygnacji z zamówienia bez podania przyczyny oraz bez wyboru którejkolwiek ze złożonych ofert.
9. **INFORMACJE DODATKOWE**
10. Zamawiający zawiera umowy na podstawie własnych wzorów umów stosowanych w  Ministerstwie Funduszy i Polityki Regionalnej. Wzór umowy stanowi załącznik nr 2 do Zapytania ofertowego.
11. Ilekroć w dokumentacji zapytania zostały użyte nazwy własne, patenty, pochodzenie itp. Zamawiający dopuszcza rozwiązania równoważne. Na Wykonawcy spoczywa ciężar wykazania równoważności. W przypadku zaoferowania przez Wykonawcę rozwiązania równoważnego, Wykonawca jest zobowiązany do pokrycia wszelkich możliwych kosztów, wymaganych w czasie wdrożenia oferowanego rozwiązania.
12. Niniejsze ogłoszenie rozeznania rynku nie stanowi oferty w myśl art. 66 Kodeksu Cywilnego, jak również nie jest postępowaniem o udzielenie zamówienia publicznego w rozumieniu przepisów Prawa Zamówień Publicznych.
13. **KLAUZULA INFORMACYJNA ZAMAWIAJĄCEGO**
14. Na podstawie art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO”, informuje się, że:
15. Administratorem Państwa danych osobowych jest Minister Funduszy i Polityki Regionalnej, z siedzibą przy ul. Wspólnej 2/4, 00-926 Warszawa.
16. Administrator wyznaczył Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych za pośrednictwem adresu e-mail: [IOD@mfipr.gov.pl](mailto:IOD@mfipr.gov.pl) lub pisemnie na adres Administratora.
17. Państwa dane osobowe będą przetwarzane w celu przeprowadzenia postępowania, a następnie w celu zawarcia i realizacji umowy o zamówienie oraz dochodzenia ewentualnych roszczeń z tytułu realizacji umowy, w przypadku wyboru Państwa oferty, jak również w celu realizacji praw oraz obowiązków wynikających z art. 6 ust. 1 lit. b) lub art. 6 ust. 1 lit. c) i f) RODO w związku z art. 44 ust. 3 pkt 1 ustawy z dnia 27.08.2009 r. o finansach publicznych (Dz. U. z 2023 r. poz. 1270, ze zm.).
18. Państwa dane osobowe mogą zostać przekazane podmiotom lub organom upoważnionym na podstawie przepisów prawa lub podmiotom zewnętrznym, na podstawie umowy powierzenia przetwarzania danych osobowych.
19. Państwa dane osobowe będą przechowywane przez okres niezbędny do realizacji ww. celu z uwzględnieniem okresów archiwizacji dokumentów wynikający z przepisów powszechnie obowiązujących oraz przepisów wewnętrznych Administratora.
20. Państwa dane osobowe nie będą przetwarzane w sposób zautomatyzowany, w tym nie będą podlegać profilowaniu.
21. Państwa dane osobowe nie będą przekazywane poza Europejski Obszar Gospodarczy obejmujący Unię Europejską, Norwegię, Liechtenstein i Islandię.
22. Podanie przez Państwo danych osobowych jest dobrowolne, ale niezbędne do przeprowadzenia postępowania w celu zawarcia i wykonania umowy o zamówienie, w przypadku wyboru Państwa oferty. Odmowa podania tych danych skutkować będzie brakiem realizacji celu, o którym mowa w pkt. 3.
23. W przypadku danych osobowych należących do osób nie będących Wykonawcą, Zamawiający otrzymał dane osobowe tych osób od Wykonawcy składającego ofertę.
24. Zamawiający będzie przetwarzał następujące kategorie danych osobowych osób nie będących Wykonawcą: imię i nazwisko, PESEL, służbowy adres e-mailowy i numer telefonu.
25. W związku z przetwarzaniem Państwa danych osobowych, przysługują Państwu następujące prawa:
26. prawo dostępu do swoich danych;
27. prawo do sprostowania (poprawiania) swoich danych osobowych;
28. prawo ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO;
29. prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
30. prawo sprzeciwu wobec przetwarzania dotyczących Pani/Pana danych osobowych, na zasadach określonych w art. 21 RODO;
31. prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy o ochronie danych osobowych.
32. Nie przysługuje Państwu prawo do usunięcia danych osobowych, w związku z art. 17 ust. 3 lit. b), d) lub e) RODO.
33. W przypadku przekazywania Zamawiającemu danych osobowych należących do osób innych niż Wykonawca, Wykonawca zobowiązany jest do przekazania tym osobom Klauzuli informacyjnej Zamawiającego zamieszczonej w niniejszym Zapytaniu ofertowym.
34. **ZAŁĄCZNIKI**

Załącznik nr 1 – Formularz ofertowy,

Załącznik nr 2 – Wzór umowy,

Załącznik nr 3 – Wykaz usług (załącznik do Formularza ofertowego).

1. Przez „dzień roboczy” Strony zgodnie rozumieją każdy dzień: od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy [↑](#footnote-ref-1)