OPIS PRZEDMIOTU ZAMÓWIENIA

na **“Przeprowadzenie kampanii cyberawereness oraz szkoleń z zakresu cyberbezpieczeństwa”.**

1. Wstęp

1.1. Cel zamówienia

Celem zamówienia jest kompleksowe podniesienie poziomu świadomości i kompetencji pracowników Urzędu Zamówień Publicznych w zakresie cyberbezpieczeństwa, ze szczególnym uwzględnieniem ograniczenia ryzyka ataków socjotechnicznych (phishing, smishing, ataki przez komunikatory) oraz wdrożenia nowoczesnych praktyk ochrony informacji. Program ma na celu trwałą zmianę postaw i nawyków użytkowników, budowę kultury bezpieczeństwa oraz zwiększenie odporności organizacji na zagrożenia związane z działalnością człowieka.

1.2. Kontekst projektu i źródła finansowania

Projekt realizowany jest w ramach Krajowego Planu Odbudowy i Zwiększania Odporności oraz programu „Cyberbezpieczny Rząd”, finansowanego ze środków NextGenerationEU. Stanowi element strategii bezpieczeństwa organizacji, mający na celu wzmocnienie infrastruktury teleinformatycznej oraz podniesienie kompetencji pracowników w zakresie cyberbezpieczeństwa.

1.3. Zakres czasowy i możliwość przedłużenia

Umowa zostanie zawarta na okres do 15 czerwca 2026. Zamawiający przewiduje prawo opcji, na warunkach określonych w dokumentacji zamówienia.

1.4. Odbiorcy programu

Program podnoszenia świadomości cyberbezpieczeństwa skierowany jest do wszystkich pracowników Urzędu Zamówień Publicznych, z uwzględnieniem ich zróżnicowanych ról, zakresów obowiązków oraz poziomu dostępu do informacji. Program obejmuje zarówno działania edukacyjne wspólne dla całej organizacji, jak i dedykowane ścieżki szkoleniowe dla wybranych grup funkcyjnych.

2. Zakres przedmiotu zamówienia

Program szkoleniowy obejmuje działania edukacyjne prowadzone w kilku komplementarnych formatach, dostosowanych do specyfiki i potrzeb poszczególnych grup pracowników Urzędu Zamówień Publicznych. Cykl szkoleniowy łączy bloki wspólne dla wszystkich oraz dedykowane moduły dla grup funkcyjnych, a także szkolenia indywidualne dla nowych pracowników. W całym cyklu szkoleniowym wykonawca omówi tematy: najpopularniejsze zagrożenia, phishing, socjotechnika, incydenty bezpieczeństwa, złośliwe oprogramowanie, higiena cyfrowa, bezpieczeństwo poczty elektronicznej, bezpieczeństwo urządzeń przenośnych, MFA, ślady cyfrowe, ochrona danych osobowych, praca zdalna, bezpieczeństwo nośników, OSINT, ransomware, polityka haseł, bezpieczeństwo w mediach społecznościowych, praktyczne ćwiczenia i symulacje ataków. Dedykowane bloki tematyczne w ramach szkoleń stacjonarnych i webinarów uwzględniać mają specyfikę pracy, typowe zagrożenia oraz praktyczne aspekty bezpieczeństwa.

2.1. Zakres rzeczowy – podział na komponenty

2.1.1. Szkolenia stacjonarne

- Realizacja szkoleń stacjonarnych w siedzibie zamawiającego (ul. Postępu 17a, Warszawa) obejmujących dwa cykle szkoleniowe dla w sumie 160 osób, w grupach do 40 osób, bez cateringu, w sali zapewnionej przez zamawiającego. Jedno szkolenie trwające maksymalnie 45 minut.
- Pierwszy cykl szkoleń ma obejmować swoim zakresem Wdrożenie kluczy sprzętowych U2F
- Tematykę drugiego cyklu szkoleniowego proponuje wykonawca do akceptacji zamawiającego.

2.1.2. Szkolenia zdalne

- Realizacja szkoleń zdalnych prowadzonych na platformie MS Teams zamawiającego, z możliwością zadawania pytań na żywo, nagrywane i archiwizowane przez zamawiającego.
- Minimum 10 szkoleń w trakcie realizacji umowy, każde trwające 60 minut.
- Co najmniej dwa webinary poświęcone zostaną wykorzystaniu platformy MS Teams i realizacji dobrych praktyk bezpieczeństwa w oparciu o mechanizmy oferowane przez te platformę.
- Materiały na szkolenie przygotuje Wykonawca.

2.1.3. Szkolenia dla nowych pracowników

- Szkolenia dla nowych pracowników trwające min. 30 minut, do 10 szkoleń w okresie umowy, realizowane zdalnie na żądanie, w dni robocze w godzinach pracy urzędu, z możliwością udziału więcej niż 1 osoby w przypadku zatrudnienia w danym miesiącu więcej niż 1 osoby.
- Szkolenia dla nowych pracowników obejmują zakresem treści regulaminów wewnętrznych (regulamin użytkowania sprzętu służbowego, zgłaszanie incydentów) w zakresie zasad cyberhigieny i zgłaszania incydentów oraz przedstawienie przykładowych socjotechnik, którym posługują się adwersarze celem przejęcia loginu i hasła użytkownika, oraz zakres dotyczący kluczy opisany w 2.1.6.
- Każdy nowy pracownik otrzymuje przewodnik po bezpieczeństwie (2 strony, elektronicznie). Przewodnik nie wymaga aktualizacji w trakcie umowy, a jego zakres obejmuje aktualne strategie ataków cyber, sposoby rozpoznania zagrożeń oraz omówienie zasad zgłaszania incydentów obowiązujących w urzędzie.

2.1.4. Spotkania indywidualne dla kierownictwa i dyrektorów

- **Kierownictwo (5 osób)**: Spotkania indywidualne 1:1 (stacjonarne), trwające 45–60 minut, przygotowane na podstawie OSINT rozszerzonego, z czasem na pytania indywidualne. Zakres spotkania obejmuje przekrojowe zagadnienia, analizę indywidualnych zagrożeń, odpowiedzialność prawną i organizacyjną, zarządzanie ryzykiem oraz wdrażanie kultury bezpieczeństwa, klucze U2F.
- **Dyrektorzy (17 osób)**: Spotkania indywidualne 1:1 (stacjonarne), 45–60 minut, przygotowane na podstawie OSINT podstawowego, z naciskiem na praktyczne aspekty zarządzania ryzykiem, ochronę danych i komunikację w zespole, klucze U2F.
- Spotkania nie są dokumentowane, nie przewiduje się przekazywania materiałów podsumowujących.
- W przypadku, kiedy w trakcie trwania umowy nastąpi zmiana na stanowisku kierowniczym lub dyrektorskim jedno ze spotkań dla nowych pracowników opisane w 2.1.3 przeznaczone będzie indywidualnie dla tej osoby zgodnie z powyższym zakresem, wyłączając OSINT.

2.1.5. Kampanie cyber awareness i symulacje ataków

- W ramach programu realizowane będą regularne kampanie cyber awareness, których celem jest praktyczne wzmacnianie odporności pracowników Urzędu Zamówień Publicznych na ataki socjotechniczne oraz utrwalanie nawyków bezpiecznego zachowania. Każda kampania (z wyjątkiem SMS i vishing) obejmuje ok. 200 użytkowników.
- Wykonawca będzie prowadził regularne kampanie phishingowe, smishingowe (SMS) oraz przez komunikatory (MS Teams i inne popularne komunikatory), oraz podrzucenie pendrive w siedzibie Zamawiającego. Każda forma wykorzystana dwukrotnie w okresie umowy.
- Kampanie mogą być mieszane po uzgodnieniu z Zamawiającym.
- Kampania SMS – kierowane do wąskiej grupy osób. Zakres i scenariusz kampanii zostaną uzgodniony w trakcie realizacji umowy.
- Kampania telefoniczna – vishing do trzech ustalonych indywidualnie osób funkcyjnych wskazanych przez Zamawiającego na etapie realizacji umowy. Zakres i scenariusz kampanii zostaną uzgodniony w trakcie realizacji umowy.
- Szablony wiadomości każdorazowo zatwierdzane przez zamawiającego.
- Zamawiający wymaga realizacji usługi w dni robocze w godzinach 8:00 – 15:00 według harmonogramów opracowanych przez Wykonawcę w uzgodnieniu z Zamawiającym.
- Raporty z kampanii zawierają szczegółową analizę skuteczności szablonów, statystyki uczestnictwa, rekomendacje naprawcze dla grup z niskim zaangażowaniem oraz konsultacje z zespołem ds. Bezpieczeństwa.
- Kampanie mają być prowadzone z różnych domen, a telefoniczne/sms z innych numerów.
- Zamawiający zapewnia integrację z Microsoft Entra ID na potrzeby przeprowadzenia kampanii.

2.1.6. Wdrożenie kluczy sprzętowych U2F

- Szkolenia z obsługi kluczy realizowane w siedzibie UZP w grupach do 40 osób, z instrukcjami elektronicznymi (Windows, Android).
- Użytkownicy będą dysponować 2 sztukami kluczy U2F.
- Szkolenie powinno uwzględniać: wyjaśnienie czym jest klucz i do czego dokładnie służy, jak zadbać o jego bezpieczeństwo, logowanie do środowisk

M365 oraz innych środowisk wykorzystywanych w trakcie realizacji zadań służbowych oraz wykorzystanie klucza w zastosowaniach prywatnych na wybranych portalach społecznościowych oraz dostępie do wybranych dostawców usług pocztowych.

- Szkolenie follow-up miesiąc po wydaniu wszystkich kluczy, w formie wideokonferencji z możliwością nagrania.

2.1.7. Wsparcie i konsultacje

- Przewidziane są okresowe konsultacje/przeglądy programu online, których celem jest omówienie postępów, wyników raportowania oraz rekomendacji dotyczących dalszych działań edukacyjnych.
- Wszelka komunikacja prowadzona jest drogą elektroniczną (e-mail), a w przypadku konsultacji – również w formie wideokonferencji.

2.1.8. Minimalne wymagania dotyczące OSINT

- W zakresie OSINT podstawowy Wykonawca powinien przeszukać rejestry publiczne (REGON, CEIDG, KRS), portale społecznościowe (Facebook, Instagram, LinkedIn);
- W zakresie OSINT rozszerzony, wykonawca realizuje zakres OSINT podstawowy oraz przeszukuje zasoby tzw. „darkweb" (wycieki haseł, tematy dyskusyjne na temat osoby) – na podstawie adresu email służbowego i prywatnego.
- Pozyskany materiał stanowi informacje poufne. Wykonawca zapewnia, że informacje te będą znane wyłącznie pracownikowi wykonującego OSINT oraz osobie, z którą planowane jest spotkanie.

2.1.9. Organizacja i komunikacja

- Podział na grupy jest stały przez cały okres trwania programu; nie przewiduje się zmian liczebności grup ani przypisywania pracowników do więcej niż jednej grupy.
- Wykonawca prowadzi komunikację z uczestnikami szkoleń i nowych pracowników wyłącznie drogą e-mail (potwierdzenie terminu).
- Komunikacja dotycząca terminów szkoleń prowadzona jest przez Zamawiającego
- Szkolenia mogą być nagrywane na platformie MS Teams zamawiającego, za zgodą uczestników; wykonawca wyraża zgodę na utrwalenie wizerunku.
- Materiały szkoleniowe przygotowuje wykonawca dla wszystkich szkoleń.

- Wykonawca prowadzi statystyki liczby przeprowadzonych szkoleń kwartalnie i na koniec umowy.

3. Cele i mierzalne efekty programu

3.1. Cele strategiczne i operacyjne

Celem programu jest trwałe podniesienie poziomu świadomości i kompetencji pracowników Urzędu Zamówień Publicznych w zakresie cyberbezpieczeństwa, co ma przełożyć się na:

- **Zmniejszenie podatności organizacji na ataki socjotechniczne** (phishing, smishing, ataki przez komunikatory),
- **Wzrost liczby zgłoszeń podejrzanych wiadomości** i proaktywnego reagowania na zagrożenia,
- **Zwiększenie zaangażowania użytkowników** w działania edukacyjne i utrwalenie nawyków bezpiecznego zachowania,
- **Budowę kultury bezpieczeństwa** oraz trwałą zmianę postaw pracowników w zakresie ochrony informacji,
- **Zwiększenie odporności organizacji** na wycieki danych, naruszenia bezpieczeństwa systemów oraz konsekwencje prawne i wizerunkowe.

Program ma charakter ciągły i adaptacyjny, a jego celem jest nie tylko realizacja szkoleń, ale przede wszystkim trwała zmiana postaw i zachowań użytkowników.

3.2. Wskaźniki efektywności (KPI)

Efektywność programu będzie monitorowana na bieżąco za pomocą narzędzi analitycznych platformy szkoleniowej oraz raportów eksperckich. Główne KPI obejmują:

- **Phishing Failure Rate** – odsetek użytkowników, którzy dali się złapać na symulowany phishing (kliknięcie, podanie danych).
- **Phishing Report Rate** – odsetek użytkowników, którzy prawidłowo zgłosili podejrzaną wiadomość.
- **Liczba użytkowników niebiorących udziału w kampaniach** – monitorowanie i raportowanie wskaźników również dla użytkowników, którzy nie wzięli udziału w kampanii phishingowej.

Wskaźniki będą raportowane ogólnie oraz w segmentacji użytkowników (wg działów, ról) w raportach i kampaniach.

3.3. Sposób pomiaru, raportowania i ewaluacji

- **Pomiar bazowy:** Przed rozpoczęciem programu wykonawca przeprowadzi symulację phishingu. Średnia z efektów symulacji osiągniętych przez Wykonawcę oraz efekty osiągnięte przez Zamawiającego przy realizacji symulacji phishingu skierowanej do wszystkich pracowników, stanowić będą poziom wyjściowy odporności (% kliknięć w link oraz % podania danych logowania). Dodatkowym wskaźnikiem nie mierzonym wcześniej będzie % zgłoszeń podejrzanej treści.
- **Forma raportów:** Brak wymagań co do formy graficznej; raporty mogą być w formie tabelarycznej lub graficznej, zgodnie z możliwościami platformy.
- **Archiwizacja:** Raporty i rekomendacje przekazywane zamawiającemu po każdej kampanii, bez konieczności prowadzenia archiwum przez wykonawcę.

3.3.1. Raportowanie i analityka cyber awareness i symulacje ataków

- Po każdej kampanii wykonawca przygotowuje raport zawierający: szczegółową analizę skuteczności poszczególnych szablonów ataków (np. które szablony były najskuteczniejsze), statystyki liczby użytkowników, którzy nie wzięli udziału w kampanii, statystyki uczestnictwa,
- Wykonawca przestawi rekomendacje eksperckie dotyczące konkretnych działań naprawczych dla grup z niskim zaangażowaniem.

Raporty będą każdorazowo konsultowane z zespołem ds. bezpieczeństwa zamawiającego po każdej kampanii (forma konsultacji elastyczna: spotkanie online, raport pisemny lub inna uzgodniona).

4. Wymagania formalne i zgodność

4.1. Oznaczenia materiałów i dokumentów

Wszystkie materiały, dokumenty i efekty pracy muszą być oznaczone zgodnie z wymogami Księgi Identyfikacji Wizualnej KPO oraz zawierać informację o finansowaniu ze środków KPO i NextGenerationEU. Zamawiający udostępni wzory oznaczeń i logotypów.

4.2. Wymogi informacyjne i promocyjne

Wykonawca zobowiązany jest do stosowania się do wytycznych dotyczących komunikacji i promocji projektu, w tym do przygotowania materiałów komunikacyjnych do kampanii wewnętrznej.

4.3. Zasady przetwarzania i usuwania danych

Wszystkie dane osobowe muszą być przetwarzane zgodnie z RODO/GDPR. Przetwarzanie i retencja danych odbywa się wyłącznie w regionie UE/EOG.

4.3.1. Retencja i archiwizacja danych

Nie przewiduje się szczególnych wymagań dotyczących archiwizacji i retencji danych po zakończeniu projektu poza okresem przejściowym uzgodnionym w umowie.

4.4. Zasady równego traktowania wykonawców

Wszyscy wykonawcy są traktowani równo, a wymagania określone w OPZ mogą być spełnione rozwiązaniami równoważnymi pod względem funkcjonalnym i jakościowym.

4.5. Wymagania dotyczące języka i formatu materiałów

Materiały szkoleniowe, komunikaty i raporty przygotowywane są w języku polskim (na życzenie zamawiającego raporty mogą być dostępne w języku angielskim). Brak wymagań dotyczących formatu plików materiałów (np. PDF, DOCX, PPTX).

Załącznik nr 1

Szczegółowa wycena

Opis	Czas trwania	Wartość
2x szkolenie stacjonarne w siedzibie Zamawiającego: cykl szkoleń dla 160 pracowników każde, podzielonych na 40-sobowe tury	Maks. 45 minut	
10 x szkolenia zdalne	60 minut	
10 x szkolenia dla **nowych** pracowników	Min. 30 minut	
5x spotkania 1:1 (stacjonarne) dla **kierownictwa**	Maks. 60 minut	
17x spotkania 1:1 (stacjonarne) dla **dyrektorów**	Maks. 60 minut	
Kampanie cyber awereness	-	
Konsultacje	Łącznie 10h/mc	
Łączna wartość		