1. Przedmiot zamówienia i cel

Przedmiotem zamówienia jest przeprowadzenie szkoleń oraz testów socjotechnicznych dla personelu nietechnicznego Urzędu, w celu podniesienia świadomości zagrożeń oraz umiejętności reagowania na ataki socjotechniczne.

Szkolenia będą oparte na wynikach testów socjotechnicznych i obejmą edukację pracowników w zakresie typowych technik stosowanych przez cyberprzestępców oraz sposobów ich rozpoznawania i przeciwdziałania.

2. Zakres zamówienia

Zakres obejmuje w szczególności:

1. Przygotowanie i realizację testów socjotechnicznych (min. 1 test personalizowany).
2. Opracowanie scenariuszy ataków na podstawie informacji od Zamawiającego.
3. Przeprowadzenie ataków socjotechnicznych (min. 3 ataki na test).
4. Analizę wyników i przygotowanie raportów z rekomendacjami.
5. Organizację i realizację szkoleń stacjonarnych lub zdalnych dla personelu nietechnicznego.
6. Szkolenia oparte na wynikach testów, ukierunkowane na konkretne luki i błędy ludzkie.
7. Praktyczne warsztaty (symulacje ataków, rozpoznawanie prób phishingu, reagowanie).
8. Omówienie wyników oraz wskazanie działań korygujących.
9. (opcjonalnie – jeśli Zamawiający przewiduje) Dostarczenie materiałów edukacyjnych lub dostęp do platformy e-learning.

3. Testy socjotechniczne

3.1. Cel testów

Celem testów socjotechnicznych jest zweryfikowanie podatności personelu Zamawiającego na techniki manipulacji społecznej (np. phishing, vishing, pretexting, baiting i inne), ocena zdolności pracowników do rozpoznawania prób ataku oraz pozyskanie obiektywnych danych niezbędnych do przygotowania działań naprawczych i szkoleniowych.

3.2. Zakres i minimalne wymagania

1. Wykonawca przeprowadzi minimum **1 test personalizowany**.
2. Dla każdego testu Wykonawca przygotuje **co najmniej 3 zdefiniowane scenariusze ataków**. Scenariusze obejmować będą różne techniki socjotechniczne.
3. Każdy test będzie zawierał **minimum 3 ataki** (realizowane zgodnie z opracowanymi scenariuszami). Ataki przeprowadzone będą w warunkach możliwie zbliżonych do rzeczywistych, z uwzględnieniem ochrony danych i bezpieczeństwa systemów.
4. Test personalizowany musi wykorzystywać informacje kontekstowe (np. struktura organizacyjna, nazwy projektów, role pracowników) przekazane przez Zamawiającego i zgromadzone w fazie przygotowawczej, tak aby scenariusze były realistyczne i specyficzne dla organizacji.

3.3. Faza przygotowawcza

1. Zamawiający dostarczy informacje niezbędne do przygotowania scenariuszy (np. lista kontaktów do testu w formie wskazówek/zakresu, zasady wewnętrzne).
2. Wykonawca przeprowadzi analizę ryzyka planowanych scenariuszy i przedstawi propozycję środków minimalizujących wpływ na systemy i działalność Zamawiającego.
3. Wykonawca przedstawi Zamawiającemu opis każdego scenariusza oraz harmonogram wykonania testów; scenariusze zostaną zatwierdzone na piśmie przed wykonaniem testów.

3.4. Zasady wykonywania testów (bezpieczeństwo)

1. Wszystkie techniki ataku muszą być bezpieczne, załączniki i pakiety wykorzystywane w testach nie mogą zawierać szkodliwego oprogramowania powodującego przejęcie

kontroli nad urządzeniami. Dozwolona jest jedynie lekka telemetryka informująca o przebiegu ataku (np. informacja o otwarciu wiadomości, kliknięciu linku, podaniu danych).

2. Testy nie mogą wpływać na dostępność usług Zamawiającego ani powodować utraty danych.
3. Testy prowadzone są zgodnie z obowiązującymi przepisami (w tym RODO w zakresie przetwarzania danych osobowych), procedurami SZBI oraz wymogami Krajowych Ram Interoperacyjności (KRI).
4. Wykonawca zobowiązany jest niezwłocznie poinformować Zamawiającego (wskazaną osobę/kanał) o każdym nieoczekiwanym zdarzeniu powodującym ryzyko dla zasobów lub bezpieczeństwa.

3.5. Metryki i analiza skuteczności

Wykonawca przeprowadzi analizy i przygotuje metryki obrazujące skuteczność testów, w tym w szczególności:

- **wskaźnik otwarć e-maili,**
- **wskaźnik kliknięć w linki,**
- **liczba i procent pracowników, którzy ujawnili dane,**
- **czas reakcji (średni czas od otrzymania wiadomości do wykonania akcji),**
- **inne relewantne wskaźniki uzgodnione z Zamawiającym.**

3.6. Raportowanie i dowody

1. Po zakończeniu prac Wykonawca przygotuje raport końcowy zawierający:
   • szczegółowy opis scenariuszy,
   • wyniki i wskaźniki skuteczności ataków,
   • identyfikację podatnych pracowników i zespołów (możliwość anonimowego przedstawienia w raportach publicznych),
   • analizę ryzyka wynikającą z obserwowanych zachowań,
   • rekomendacje działań naprawczych (proceduralnych, szkoleniowych, technicznych),
   • propozycję harmonogramu działań korygujących i dalszego monitoringu.
2. Raport będzie zawierał materiał dowodowy (logi telemetrii, statystyki, zrzuty ekranów nie zawierające haseł; w przypadku przechwycenia credentiali dowód będzie ograniczony do metadanych i procedury demonstracyjnej, hasła nie będą publikowane), a także opis metod zbierania dowodów.

4. Szkolenia

4. Szkolenia

4.1. Cel szkoleń

Celem szkoleń jest podniesienie świadomości zagrożeń socjotechnicznych wśród personelu nietechnicznego oraz wykształcenie umiejętności rozpoznawania i właściwego reagowania na próby ataków. Szkolenia mają bezpośrednio uwzględniać wyniki przeprowadzonych testów socjotechnicznych, identyfikować najczęstsze błędy ludzkie oraz wskazywać skuteczne sposoby ich eliminacji.

4.2. Powiązanie szkoleń z testami socjotechnicznymi

1. Szkolenia muszą zostać przeprowadzone **po realizacji testów socjotechnicznych**.
2. Treści szkoleń muszą **odnosić się do rzeczywistych wyników testów**, w szczególności:
   - błędów popełnianych przez pracowników,
   - najczęściej występujących technik socjotechnicznych,
   - luk proceduralnych i komunikacyjnych,
   - sytuacji, w których wystąpiła podatność na manipulację.
3. Wykonawca ma obowiązek **uwzględnić rekomendacje wynikające z raportów po testach** oraz przełożyć je na treści edukacyjne i działania naprawcze.
4. Szkolenia powinny obejmować **studium przypadków opartych na rzeczywistych testach**, z zachowaniem anonimowości pracowników.

4.3. Forma realizacji

1. Szkolenia muszą odbywać się **stacjonarnie** w siedzibie Zamawiającego.
2. Wykonawca zapewnia wszystkie niezbędne materiały szkoleniowe.
3. Szkolenia muszą mieć charakter **interaktywny** (dyskusja, pytania, zadania, analiza przypadków), a nie jedynie prezentacyjny.

4.4. Dostosowanie do grup uczestników

Szkolenia muszą być dostosowane do poziomu wiedzy **personelu nietechnicznego** – język prosty, zrozumiały, bez nadmiernego żargonu technicznego.

4.5. Warsztaty praktyczne

1. Szkolenia muszą zawierać **część warsztatową lub symulacyjną**, np.:
   - analiza przykładowych wiadomości phishingowych,
   - ćwiczenia z rozpoznawania elementów manipulacji,
   - symulacje reakcji na incydent (krok po kroku),
   - odgrywanie scenek (np. telefoniczny vishing),
   - wspólne opracowanie checklist.
2. Warsztaty muszą umożliwić **aktywne zaangażowanie uczestników**, a nie bierne słuchanie.

4.6. Organizacja szkoleń

Organizacja szkolenia:

- **III tury po 3 godziny** (grupa max. 10 osób każda).

4.7. Harmonogram

1. Szczegółowy harmonogram szkoleń zostanie uzgodniony z Zamawiającym **z co najmniej 14-dniowym wyprzedzeniem.**
2. Harmonogram powinien uwzględniać:
   - liczbę grup,
   - czas trwania każdej sesji,
   - przerwy.
3. Szkolenia muszą być zrealizowane **po wykonaniu i przeanalizowaniu testów socjotechnicznych**, aby można było włączyć wyniki testów do programu.

4.8. Materiały szkoleniowe

1. Wykonawca zapewnia materiały szkoleniowe w formie papierowej lub elektronicznej.
2. Materiały muszą zawierać:
   - podsumowanie treści szkolenia,
   - checklisty / zasady postępowania,
   - przykłady ataków i sposobów obrony,

- dobre praktyki,
- odniesienie do wyników testów (anonimowo).

3. Materiały muszą być przygotowane w jasnej, zrozumiałej formie (infografiki, przykłady, listy kroków).

4.9. Potwierdzenie udziału

1. Wykonawca przygotuje listy obecności lub elektroniczne potwierdzenia udziału.
2. Na żądanie Zamawiającego Wykonawca może przygotować **test wiedzy końcowej** lub **ankietę oceny szkolenia**.

6. Wymagania wobec Wykonawcy

Wykonawca musi posiadać odpowiednie doświadczenie, kompetencje, zasoby oraz zdolność organizacyjną do kompleksowej realizacji testów socjotechnicznych oraz szkoleń z cyberbezpieczeństwa dla personelu nietechnicznego. Wymagania obejmują w szczególności:

6.1. Doświadczenie w realizacji podobnych usług

1. Wykonawca musi posiadać **udokumentowane doświadczenie w realizacji testów socjotechnicznych (np. phishing, vishing, spear phishing, pretexting)** w organizacjach o strukturze i specyfice podobnej do jednostek sektora publicznego.
2. Wykonawca musi posiadać doświadczenie w **przygotowywaniu scenariuszy ataków, analizie wyników oraz opracowywaniu raportów z rekomendacjami działań korygujących.**
3. Wykonawca musi posiadać minimum dwuletnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość o zagrożeniach cybernetycznych. Przez dwuletnie doświadczenie należy rozumieć okres co najmniej 730 dni (365 dni x 2 lata). Nie ma znaczenia czy jest to doświadczenie ciągłe, czy nie. W celu ustalenia okresu doświadczenia, należy obliczyć okres przygotowania i przeprowadzenia szkolenia, licząc ten okres od daty zawarcia umowy do daty zakończenia realizacji, a jeżeli nie była zawarta umowa od daty otrzymania zlecenia do daty zakończenia realizacji. Nie sumuje się doświadczenia w przypadku realizacji więcej niż jednego szkolenia w tym samym okresie czasie. Zamawiający dopuszcza łączenie funkcji ekspertów przez jedną osobę pod warunkiem łącznego spełniania wymagań określonych dla tych osób.

6.2. Kompetencje techniczne i merytoryczne

Wykonawca musi dysponować kadrą posiadającą wiedzę i praktyczne umiejętności z zakresu:

- socjotechniki i technik manipulacji,
- cyberbezpieczeństwa (aspekty techniczne i organizacyjne),
- testów penetracyjnych i analizy ryzyka,
- norm i standardów (np. ISO/IEC 27001, ISO/IEC 27002),
- edukacji dorosłych i prowadzenia szkoleń.

6.3. Certyfikaty branżowe (mile widziane / preferowane)

Posiadanie przez członków zespołu realizacyjnego certyfikatów potwierdzających kwalifikacje np.:

- ISO/IEC 27001 Lead Auditor / Lead Implementer,
- CEH (Certified Ethical Hacker),
- OSCP (Offensive Security Certified Professional),
- CompTIA Security+ / CySA+,
- CISSP / CISM / CISA,
- inne certyfikaty z obszaru bezpieczeństwa informacji i testów socjotechnicznych.

6.4. Zdolność organizacyjna i zasoby

Wykonawca musi zapewnić:

- możliwość przeprowadzenia testów socjotechnicznych w środowisku Zamawiającego zgodnie z ustalonym harmonogramem,
- narzędzia techniczne do realizacji testów (np. system do kampanii phishingowych, rejestracja telemetryki, statystyk),
- środki komunikacji i platformy do szkoleń zdalnych (jeśli dotyczy),
- materiały edukacyjne (papierowe/elektroniczne),
- odpowiednią liczbę trenerów i konsultantów, aby zrealizować szkolenia w ustalonym czasie.

6.5. Poufność i odpowiedzialność

1. Wykonawca musi zapewnić zachowanie poufności wszystkich danych i informacji uzyskanych w trakcie realizacji umowy.
2. Członkowie zespołu Wykonawcy muszą być zobowiązani do poufności (np. umowy, NDA).
3. W przypadku przetwarzania danych osobowych – Wykonawca musi być gotowy do zawarcia umowy powierzenia danych.
4. Wykonawca musi stosować bezpieczne procedury przechowywania i niszczenia danych pozyskanych podczas testów.
5. Wykonawca ponosi odpowiedzialność za działania swojego personelu i podwykonawców (jeśli występują).