

Załącznik nr 7 – 7.20 do SWZ

Opis przedmiotu zamówienia – usługa przeprowadzenia testów phishingowych

1. Przedmiot zamówienia

Przedmiotem zamówienia jest przygotowanie i przeprowadzenie jednej kontrolowanej kampanii phishingowej skierowanej do 12 pracowników Zamawiającego, a następnie udostępnienie użytkownikom platformy e-learningowej zawierającej materiały edukacyjne oraz test wiedzy z zakresu cyberbezpieczeństwa.

Usługa ma stanowić jeden spójny proces obejmujący ocenę podatności użytkowników, działania edukacyjne, weryfikację przyswojenia wiedzy oraz przygotowanie raportu końcowego dla Zamawiającego.

2. Cele zamówienia

- ocena poziomu podatności pracowników na wiadomości phishingowe;
- identyfikacja grup i obszarów wymagających dodatkowej edukacji;
- podniesienie świadomości użytkowników w zakresie cyberzagrożeń;
- przeprowadzenie ukierunkowanych szkoleń po zakończeniu kampanii;
- sprawdzenie wiedzy użytkowników po szkoleniu;
- udokumentowanie udziału użytkowników w kampanii i szkoleniu;
- przekazanie Zamawiającemu wyników, wniosków i rekomendacji dalszych działań.

3. Model realizacji usługi

Realizacja zamówienia powinna przebiegać w następujących etapach:

1. Spotkanie organizacyjne i ustalenie zakresu kampanii.
2. Przygotowanie i akceptacja scenariusza phishingowego.
3. Konfiguracja techniczna kampanii i wykonanie testu kontrolnego.
4. Przeprowadzenie kampanii phishingowej dla uzgodnionej grupy użytkowników.
5. Analiza zachowań użytkowników i przypisanie działań edukacyjnych.
6. Udostępnienie platformy szkoleniowej, materiałów oraz testu wiedzy.
7. Monitorowanie postępów szkoleniowych i wyników testów.
8. Przygotowanie raportu końcowego łączącego wyniki kampanii i szkolenia.
9. Spotkanie podsumowujące z Zamawiającym.

4. Zakres kampanii phishingowej

4.1. Przygotowanie kampanii

- przeprowadzenie spotkania przygotowawczego;
- ustalenie grupy uczestników, harmonogramu oraz zakresu rejestrowanych zdarzeń;

- przygotowanie jednego scenariusza phishingowego dopasowanego do profilu organizacji;
- uzgodnienie domeny, adresu nadawcy, treści wiadomości i strony testowej;
- konfiguracja bezpiecznej infrastruktury kampanii;
- wykonanie testu kontrolnego przed uruchomieniem właściwej kampanii.

4.2. Scenariusz wiadomości

Scenariusz może dotyczyć w szczególności:

- logowania do usługi chmurowej lub poczty elektronicznej;
- wygaśnięcia hasła;
- udostępnienia dokumentu;
- wiadomości od działu HR, administracji lub przełożonego;
- faktury, przesyłki albo dokumentu firmowego.

Treść kampanii musi zostać zaakceptowana przez Zamawiającego. Wiadomość nie może zawierać informacji mogących wywołać nadmierny stres, w szczególności informacji o zwolnieniu, chorobie, śmierci lub zagrożeniu życia.

4.3. Rejestrowane zdarzenia

- dostarczenie wiadomości;
- otwarcie wiadomości, jeżeli pomiar jest technicznie możliwy;
- kliknięcie odnośnika;
- wejście na stronę testową;
- podjęcie próby wpisania danych;
- zgłoszenie wiadomości jako phishing, jeżeli stosowany mechanizm to umożliwia;
- przejście do materiału edukacyjnego;
- ukończenie przypisanego szkolenia i testu wiedzy.

System nie może przechowywać prawdziwych haseł użytkowników. W przypadku użycia formularza logowania dopuszczalne jest zapisanie wyłącznie informacji, że użytkownik podjął próbę wprowadzenia danych.

5. Platforma szkoleniowa

Po przeprowadzeniu kampanii Wykonawca udostępni Zamawiającemu gotową platformę e-learningową działającą przez przeglądarkę internetową. Platforma nie może wymagać instalowania dodatkowego oprogramowania po stronie użytkownika.

- utworzenie przestrzeni dla jednej jednostki organizacyjnej Zamawiającego;
- utworzenie konta administratora Zamawiającego;
- import lub utworzenie kont użytkowników;
- przypisanie materiałów szkoleniowych i testów;
- monitorowanie realizacji szkoleń;

- raportowanie wyników;
- eksport raportów do XLSX, CSV lub formatu równoważnego.

6. Materiały edukacyjne

Materiały szkoleniowe powinny być dostosowane do zagrożeń badanych w kampanii i obejmować co najmniej:

- rozpoznawanie phishingu i smishingu;
- weryfikację nadawcy, domeny i adresu strony;
- bezpieczne korzystanie z linków i załączników;
- rozpoznawanie presji czasu, poufności i nietypowych próśb;
- ochronę danych logowania;
- stosowanie uwierzytelniania wieloskładnikowego;
- zgłaszanie podejrzanych wiadomości;
- postępowanie po kliknięciu podejrzanego linku;
- podstawowe zasady cyberhigieny.

Osoba, która wykonała ryzykowną akcję podczas kampanii, powinna otrzymać materiał wyjaśniający, które elementy wiadomości wskazywały na phishing, czego nie należało robić oraz jak prawidłowo zareagować.

7. Test wiedzy

- pytania jednokrotnego lub wielokrotnego wyboru;
- automatyczne obliczanie wyniku;
- możliwość określenia progu zaliczenia;
- możliwość określenia liczby prób;
- rejestrowanie historii podejść;
- prezentowanie wyniku użytkownikowi;
- zapisywanie wyniku w raporcie administratora.

Test powinien obejmować w szczególności:

- rozpoznanie podejrzanego wiadomości;
- prawidłowe sprawdzenie odnośnika;
- reakcję na prośbę o login lub hasło;
- reakcję na podejrzanego załącznik;
- zgłoszenie incydentu do właściwego kanału.

8. Powiązanie kampanii ze szkoleniem

System lub proces realizowany przez Wykonawcę powinien umożliwiać powiązanie wyników kampanii phishingowej z dalszym działaniem edukacyjnym. Co najmniej użytkownicy, którzy

kliknęli odnośnik, weszli na stronę testową lub podjęli próbę wprowadzenia danych, powinni zostać objęci szkoleniem uzupełniającym.

Zamawiający może zdecydować o objęciu szkoleniem wszystkich uczestników kampanii. W takim przypadku raport powinien umożliwiać porównanie zachowania użytkownika w kampanii z wynikiem szkolenia i testu wiedzy.

9. Monitorowanie postępów

- przypisanie szkolenia do użytkownika;
- rozpoczęcie i ukończenie szkolenia;
- procent realizacji materiału;
- data ostatniej aktywności;
- wynik testu;
- liczba podejść;
- status zaliczony lub niezaliczony.

Jeżeli platforma obsługuje pomiar oglądania materiałów wideo, może dodatkowo rejestrować realny czas oglądania, liczbę uruchomień oraz datę ostatniego odtworzenia.

10. Raportowanie

10.1. Raport z kampanii

- opis zastosowanego scenariusza;
- liczba uczestników i dostarczonych wiadomości;
- liczba otwarć, jeżeli pomiar był możliwy;
- liczba kliknięć;
- liczba wejść na stronę testową;
- liczba prób wprowadzenia danych;
- liczba zgłoszeń phishingu;
- wyniki według działów, lokalizacji lub grup.

10.2. Raport ze szkolenia

- lista użytkowników objętych szkoleniem;
- status realizacji szkolenia;
- data rozpoczęcia lub ostatniej aktywności;
- wynik testu wiedzy;
- liczba podejść;
- status zaliczony lub niezaliczony.

10.3. Raport końcowy

Po zakończeniu usługi Wykonawca przekaże raport końcowy łączący wyniki kampanii phishingowej, realizacji szkolenia oraz testu wiedzy. Raport powinien zawierać co najmniej:

- zestawienie wyników kampanii i szkolenia;
- wskazanie użytkowników lub grup wymagających dalszych działań;
- porównanie wyników według działów lub grup;
- najważniejsze wnioski;
- rekomendacje dotyczące kolejnych kampanii, szkoleń i działań organizacyjnych;
- eksport danych do XLSX, CSV lub formatu równoważnego.

11. Wymagania techniczne i bezpieczeństwa

- dostęp do platformy przez HTTPS;
- obsługa aktualnych wersji popularnych przeglądarek;
- uwierzytelnianie użytkowników i administratorów;
- bezpieczne przechowywanie haseł;
- kontrola uprawnień i separacja danych Zamawiającego;
- brak dostępu użytkowników do danych innych osób lub podmiotów;
- szyfrowanie transmisji;
- ograniczony dostęp do wyników kampanii;
- możliwość dezaktywacji kont;
- możliwość natychmiastowego zatrzymania kampanii;
- usunięcie lub anonimizacja danych po upływie uzgodnionego okresu retencji.

Wykonawca nie może instalować złośliwego oprogramowania, wykonywać kodu na urządzeniach użytkowników, uzyskiwać dostępu do skrzynek pocztowych ani przechwytywać rzeczywistych danych uwierzytelniających.

12. Dane osobowe i poufność

- przetwarzanie danych wyłącznie w celu realizacji zamówienia;
- ograniczenie zakresu danych do minimum niezbędnego;
- ograniczenie liczby osób mających dostęp do wyników;
- zachowanie poufności informacji o Zamawiającym i uczestnikach;
- określenie okresu przechowywania danych;
- usunięcie lub anonimizacja danych po zakończeniu projektu;
- zawarcie umowy powierzenia przetwarzania danych, jeżeli będzie wymagana.

Raport imienny może być dostępny wyłącznie dla osób wyznaczonych przez Zamawiającego.

13. Role użytkowników

- administrator platformy po stronie Wykonawcy;
- administrator Zamawiającego;
- kierownik lub osoba nadzorująca wyniki, jeżeli Zamawiający wymaga takiej roli;
- użytkownik końcowy.

Użytkownik końcowy powinien widzieć wyłącznie przypisane mu szkolenia, testy i własne wyniki. Administrator Zamawiającego powinien mieć dostęp do użytkowników i raportów dotyczących swojej jednostki.

14. Obowiązki Zamawiającego

- przekazanie listy uczestników w uzgodnionym formacie, np. XLSX lub CSV;
- wskazanie osób odpowiedzialnych za akceptację scenariusza i odbiór raportów;
- przekazanie informacji niezbędnych do przygotowania scenariusza;
- zapewnienie współpracy administratorów poczty i bezpieczeństwa, jeżeli będzie wymagana;
- wskazanie kanału zgłaszania podejrzanych wiadomości;
- akceptacja harmonogramu i materiałów kampanii.

15. Dokumentacja i szkolenie administratora

- instrukcja logowania do platformy;
- instrukcja zarządzania użytkownikami;
- instrukcja przypisywania szkoleń i testów;
- instrukcja sprawdzania postępów i wyników;
- instrukcja pobierania raportów;
- opis ról i uprawnień;
- informacja o zasadach wsparcia technicznego.

Wykonawca przeprowadzi krótkie szkolenie lub instruktaż dla administratora Zamawiającego dotyczący obsługi platformy i raportów.

16. Harmonogram realizacji

- Przekazanie danych organizacyjnych i listy uczestników.
- Spotkanie przygotowawcze.
- Przygotowanie i akceptacja scenariusza.
- Konfiguracja techniczna i test kontrolny.
- Przeprowadzenie kampanii.
- Udostępnienie materiałów edukacyjnych i testów.
- Monitoring realizacji szkoleń.
- Przekazanie raportu końcowego.
- Spotkanie podsumowujące.

17. Kryteria odbioru

- przygotowanie i akceptacja scenariusza kampanii;
- przeprowadzenie jednej kampanii dla uzgodnionej grupy użytkowników;
- prawidłowe rejestrowanie uzgodnionych zdarzeń;

- udostępnienie platformy szkoleniowej;
- utworzenie konta administratora Zamawiającego;
- możliwość logowania użytkowników;
- udostępnienie materiałów szkoleniowych i testu wiedzy;
- prawidłowe zapisywanie postępów i wyników;
- działanie eksportu raportów;
- przekazanie raportu końcowego wraz z rekomendacjami;
- przekazanie dokumentacji i przeprowadzenie instruktażu.

18. Wymagania dla Wykonawcy

- doświadczenie w realizacji kampanii phishingowych lub security awareness;
- doświadczenie w dostarczaniu platform e-learningowych lub szkoleniowych;
- doświadczenie w przygotowywaniu raportów z kampanii i szkoleń;
- znajomość zasad bezpieczeństwa aplikacji internetowych i ochrony danych;
- możliwość zapewnienia wsparcia technicznego podczas realizacji zamówienia.