

## Zadanie: Testy socjotechniczne

### Założenia ogólne

- 1.** Przedmiotem zamówienia jest wykonanie 6 testów socjotechnicznych (3 ogólnych i 3 personalizowanych) mających na celu wyłudzenie poufnych informacji lub uzyskanie nieautoryzowanego dostępu do systemów Zamawiającego poprzez manipulację i wykorzystanie czynnika ludzkiego.
- 2.** Każdy test socjotechniczny musi obejmować:
  - 2.1.** przygotowania co najmniej 3 zdefiniowanych scenariuszy ataków, na podstawie przekazanych przez Zamawiającego informacji (podejrzane wiadomości e-mail),
  - 2.2.** dostosowania przygotowanych scenariuszy do specyfiki Zamawiającego (wspólne uzgodnienie z Zamawiającym),
  - 2.3.** przeprowadzenia co najmniej 3 ataków socjotechnicznych mających na celu wyłudzenie poufnych informacji lub uzyskanie nieautoryzowanego dostępu do systemów Zamawiającego poprzez manipulację i wykorzystanie ludzkiego czynnika jako wektora ataku,
  - 2.4.** w przypadku skuteczności ataku analizę danych i informacji w skrzynkach pocztowych takich pracowników celem określenia ich przydatności do dalszej eskalacji ataku,
  - 2.5.** przygotowania raportu z przeprowadzonych ataków z odniesieniem do scenariuszy ataków, ich skuteczności oraz z podaniem informacji o „złapanych” pracownikach i wrażliwych/przydatnych informacji do dalszej eskalacji ataku, wraz z rekomendacjami. Raport dotyczący „złapanych” użytkowników musi zawierać poziom skuteczności ataku takie jak min.:
    - wyświetlenie wiadomości
    - „kliknięcie” spreparowanego linku z wiadomości
    - podanie poświadczeń na podstawionej stronie
  - 2.6.** Wykonawca przeprowadzi spersonalizowane szkolenia uświadamiające dla „złapanych użytkowników” z zakresu zagrożeń phishingu i spare-phishingu po każdym z przeprowadzonych testów. Pojedyncze szkolenie musi trwać min. 60 minut i powinno uwzględniać specyfikę środowiska pracy (klient poczty Zimbra, webaccess Outlook) Zamawiającego. Szkolenie po pierwszym personalizowanym teście socjotechnicznym musi zostać zrealizowane stacjonarnie w siedzibie Zamawiającego. Szkolenia po pozostałych testach mogą być przeprowadzone zdalnie.
- 3.** Personalizowane testy socjotechniczne muszą charakteryzować się „podszywaniami” pod istniejące u Zamawiającego usługi / adresy / osoby.



4. Zamawiający zapewni dodanie serwerów wysyłkowych Wykonawcy do list wykluczeni filtrów antyspamowych i antyphishingowych.
5. Wykonawca zapewni, że „złośliwe” załączniki zawierać będą jedynie prosty program odsyłający na serwer Wykonawcy dane telemetryczne na temat zaatakowanej maszyny bez przejęcia nad nią kontroli.
6. Testy będą wykonywane w okresie do 31.05.2026 r. zgodnie z ustalonym po podpisaniu umowy harmonogramem realizacji usług.
7. Po zawarciu umowy uzgodniony zostanie harmonogram realizacji Usług, który musi w szczególności określać terminy planowanych testów oraz skład zespołu testerów.
8. Usługa będzie realizowana na podstawie zawartej umowy.
9. Umowa będzie zawierać kary umowne za ewentualne odstąpienie i za naruszenie zapisów umowy.

## Warunki udziału w postępowaniu

Zamawiający wymaga, aby Wykonawca wykazał przeprowadzenie testów zgodnych z zakresem niniejszego zamówienia w okresie ostatnich 2 lat u minimum 3 zleceniobiorców zatrudniających min 100 pracowników.

## Kary

Wykonawca za odstąpienie od umowy, niewykonanie lub nienależyte wykonanie zapisów umowy przewiduje zastosowanie kar powszechnie stosowanych dla zamówień tego typu.