**Opis przedmiotu zamówienia**

**(zwany dalej „OPZ”)**

Przedmiotem zamówienia jest **dostarczenie w formie usługi, platformy do przeprowadzania testów phishingowych oraz szkoleń elearningowych wspierającej budowanie odporności użytkowników systemów informatycznych na zagrożenia socjotechniczne wraz ze wsparciem przy wdrożeniu   
i podczas użytkowania systemu.** (zwane dalej Rozwiązaniem lub Usługą). Rozwiązanie musi oferować następujące funkcjonalności:

1. Posiadać możliwość konfiguracji i przeprowadzania przez Zamawiającego samodzielnie testów socjotechnicznych pozwalających na weryfikację podatności pracowników na symulowane ataki z wykorzystaniem maili;
2. Posiadać możliwość przekierowania użytkownika, który w ramach prowadzonych testów został skutecznie zaatakowany na zintegrowaną z rozwiązaniem stronę dostarczającą informacje edukacyjne w zakresie błędu popełnionego przez użytkownika.
3. Możliwość przeprowadzania szkoleń z zakresu bezpieczeństwa informacji (w szczególności phishingu) w formule e-learningu, na podstawie bogatej bazy szkoleń zawartych w platformie.

Rozwiązanie należy zwymiarować dla 300 skrzynek pocztowych, na okres eksploatacji 1 roku   
z możliwością przedłużenia na kolejny rok.

A. Zakres podstawowy zamówienia:   
- Dostarczenie rocznej subskrypcji na 300 skrzynek mailowych wraz z najnowszą dostępną wersją oprogramowania oferowanego Rozwiązania w zakresie:

* Platformy do testów socjotechnicznych
* Modułu edukacyjnego z gotowymi materiałami edukacyjnymi do realizacji natychmiast po błędzie użytkownika
* Platformy e-learningowej

- Wsparcie przy wdrożeniu Rozwiązania.  
- Świadczenie wsparcia dla wdrożonego Rozwiązania w zakresie przeprowadzenia co najmniej 12 kampanii phishingowych.

1. **Wymagania funkcjonalne dla Rozwiązania:**
   1. W zakresie platformy wspierającej przeprowadzanie testów socjotechnicznych:
      1. Zaproponowana usługa może być rozwiązaniem chmurowym lub uruchomionym   
         w infrastrukturze Zamawiającego;
      2. Rozwiązanie musi dostarczać szablony przykładowych testów w języku polskim (minimum 600 testów), z możliwością ich modyfikacji przez Zamawiającego – wzorce wiadomości email przesyłanych do potencjalnej ofiary, w której możliwe będzie umieszczenie:
         1. Linku do spreparowanej strony www;
         2. Załącznika o różnym rozszerzeniu: .docx, .doc, .pptx, .pps, .xlsx, .xls, .xlsm, .pdf, .zip, .html
         3. Automatycznego umieszczania dostępnych danych personalnych dostarczonych przez Zamawiającego w treści wiadomości email oraz stron docelowych, co spowoduje, iż ta sama kampania może zostać przesłana do dużej liczby osób jako jeden szablon automatycznie;
         4. Grafik, logotypów, zdjęć oraz stopek pozwalających na jak najwierniejsze   
            i najatrakcyjniejsze przedstawienie wiadomości email, jako autentycznej
      3. Testy muszą dawać możliwość:
         1. Symulacji różnorodnych sposobów ataków w formie przekierowań na fałszywe strony, spreparowanych niebezpiecznych załączników i makr, kodów QR, itp.;
         2. Symulacji, które mogą wyświetlać rzeczywistą politykę haseł wykorzystywaną przez pracowników;
         3. Zbierania informacji o użytkownikach końcowych, takie jak przeglądarki   
            i lokalizacja;
         4. Niestandardowe, dostosowane do potrzeb symulacje naśladujące aplikacje klientów;
         5. Symulacji ataków typu ransomware (bez szyfrowania plików użytkownika);
         6. Funkcjonalność przeprowadzenia testowego ataku poprzez podrzucenie spreparowanego nośnika USB.
         7. Traktowane jako opcja - funkcjonalność dystrybucji ataków z wykorzystaniem kanału telefonicznego (vishing).
      4. Strona WWW musi posiadać:
         1. Możliwość dostępu z wykorzystaniem SSL;
         2. Pozwalać dowolnie w kodzie HTML modyfikować jej funkcjonalności (dotyczy również gotowych szablonów – które powinny być udostępnione do dowolnej modyfikacji i rozbudowy) poprzez wygodny interfejs.
      5. Każdorazowe skuteczne przeprowadzenie ataku musi kończyć się elementem edukacyjnym zgodnie z pkt 1.3.;
      6. Rozwiązanie musi dostarczać scenariusze ataków z wykorzystaniem i naciskiem na aktualnie wykrywane i zidentyfikowane zagrożenia związane z atakami phishingowymi (w tym dostarczać ich wersję polskojęzyczną), posiadać bogaty zbiór predefiniowanych kampanii phishingowych związanych z wieloma różnymi branżami (związanymi   
         i niezwiązanymi bezpośrednio z działalnością Zamawiającego);
      7. Rozwiązanie musi dawać możliwości wysyłania kampanii z różnych domen –umożliwienie używania specyficznych domen jako źródła wysyłanych kampanii, indywidualnej dla każdej kampanii,
      8. Rozwiązanie musi dawać możliwości wysyłania symulacji phishingu w sposób losowy   
         z wykorzystaniem wielu różnych formatek w jednej kampanii, aby wykluczyć możliwość powiadamiania się użytkowników.
      9. Rozwiązanie musi pozwalać na kończenie każdej ścieżki testów / kampanii komunikatem pokazującym użytkownikowi, iż wiadomość jaką otrzymał oraz kroki jakie podjął były symulacją ukierunkowanego ataku na niego oraz kierować go do szkolenia zgodnie z pkt 1.3.;
      10. Rozwiązanie musi dostarczać możliwość administrowania listą odbiorców wiadomości testowych. Traktowane jako opcja - integracja listy odbiorców z systemem Active Directory;
      11. Rozwiązanie musi dostarczać kompleksową informację oraz raportowanie z zakresu przeprowadzanego testu zarówno w sposób szczegółowy jak i zagregowany w celu badania zachowania się użytkowników- ich poziom podatności na przeprowadzony atak, w szczególności: każdy podejmowany przez potencjalną ofiarę kampanii krok pozwalający określić czy potencjalna ofiara wykonała wszystkie kroki, jakie zostały zawarte w kampanii muszą być oddzielnie rejestrowane i raportowane (Przykładowe kroki, jakie podejmuje potencjalna ofiara: Otrzymanie email, Otwarcie email, Otwarcie załącznika/ linku z odsyłaczem, wykorzystanie kodu QR, Wprowadzenie danych/ Pobranie załącznika, wyświetlenie szkolenia, odbycie szkolenia, itp.);
      12. Rozwiązanie powinno wspomagać ocenę ryzyka związanego z phishingiem, zarówno indywidualnego, jak i grupowego. Powinno brać pod uwagę takie czynniki jak: rzetelność realizacji szkoleń z zakresu bezpieczeństwa informacji, wyniki testów socjotechnicznych, pełniona funkcja oraz udział danych użytkowników w znanych incydentach bezpieczeństwa lub obecność adresu email w repozytoriach dostępnych w Internecie. Dodatkowo powinno umożliwiać porównanie wyników z organizacjami o podobnym profilu.
      13. Rozwiązanie musi zapewniać bezpieczeństwo i poufność danych oraz ich pełną kontrolę w całym procesie przeprowadzania testu socjotechnicznego. Konsola zarządzająca musi być udostępniona z wykorzystaniem szyfrowanej komunikacji,   
          a dostęp do niej wymagać wieloskładnikowego uwierzytelnienia.
      14. Rozwiązanie musi zapewniać kompletne rozwiązanie do realizacji testów (tj. serwery poczty, domeny, usługi sieciowe) jak i dostarczenia elementów edukacyjnych (tj. serwery web).
      15. Rozwiązanie musi zapewniać adresowanie testów zgodnie z językiem odbiorcy. Tzn. wysłania kampanii phishingowych w formie zestawu wielojęzycznych emaili symulujących atak do wielojęzycznej grupy użytkowników. Rozwiązanie rozdysponuje emaile w taki sposób, aby dany użytkownik otrzymał wyłącznie symulację w swoim języku.
   2. W zakresie dostarczania informacji edukacyjnych w związku z popełnionymi błędami użytkownika podczas reagowania na testy:
      1. Rozwiązanie musi posiadać możliwość przekierowania ofiary na zintegrowaną   
         z rozwiązaniem stronę informującą o przeprowadzonym teście i prezentującą materiały edukacyjne dot. niebezpieczeństw związanych z phishingiem oraz metod obrony;
      2. Rozwiązanie w treści strony edukacyjnej może prezentować wyszczególnione w treści wiadomości testowej sygnały oznaczone flagami, świadczące o potencjalnie niebezpiecznej korespondencji;
      3. Materiały edukacyjne powinny być prezentowane w formie jak najbardziej atrakcyjnej dla użytkownika, w tym powinny być dostępne w języku polskim;
      4. Materiały edukacyjne muszą posiadać możliwość modyfikacji przez / na zlecenie Zamawiającego.
   3. W zakresie platformy e-learningowej, zapewniającej szkolenia w zakresie bezpieczeństwa informacji:
      1. Platforma musi zapewniać następujące funkcjonalności:
         1. możliwość przeprowadzania szkoleń w formie e-learningowej, do samodzielnej realizacji przez użytkownika;
         2. możliwość śledzenia postępów użytkowników przez administratorów oraz przełożonych;
         3. dostęp dla użytkowników przez dedykowaną aplikację LX (learner experience),   
            o interfejsie dostępnym w języku polskim;
         4. możliwość wysyłki powiadomień o statusie szkoleń (min. o zapisaniu na szkolenie, ponaglenie do realizacji, informacja o przekroczeniu terminu) do użytkownika, przełożonego oraz administratora platformy;
         5. grupowanie użytkowników;
         6. możliwość integracji logowania LX przez SAML/SSO;
         7. możliwość logowania do LX z wykorzystaniem weryfikacji wieloskładnikowej (MFA);
         8. możliwość wprowadzenia elementów rywalizacji;
         9. możliwość automatycznego przypisywania materiałów szkoleniowych do grup na podstawie informacji o użytkowniku (przykładowo: dział, zajmowane stanowisko);
      2. Muszą zostać zapewnione materiały edukacyjne w języku polskim w liczbie minimum 90 o tematyce bezpieczeństwa informacji (w szczególności zagrożeń socjotechnicznych). Materiały powinny być różnorodne w formie i atrakcyjne dla odbiorcy.
      3. Platforma powinna umożliwiać import własnych materiałów edukacyjnych w formatach SCORM oraz MP4.
      4. Platforma e-learningowa powinna być zintegrowana z platformą wspierającą przeprowadzanie testów socjotechnicznych (wymienioną w punkcie 1.1),   
         w szczególności poprzez:
         1. Współdzielenie informacji o użytkownikach, takich jak identyfikator, dane personalne, informacja o ukończonych szkoleniach, informacje o wynikach   
            w testach socjotechnicznych;
         2. Możliwość zarządzania za pomocą wspólnego panelu administratora;
         3. Możliwość wykorzystania danych o porażkach w testach socjotechnicznych do automatycznego skierowania na dodatkowe szkolenie.

1. Dostawa i wdrożenie systemu
   1. W ramach dostawy i wdrożenia rozwiązania Wykonawca zrealizuje:
      1. Wsparcie przy wykonaniu projektu wdrożenia Rozwiązania w infrastrukturze Zamawiającego zapewniającego oraz sprawnej realizacji kampanii phishingowych   
         i szkoleniowych;
      2. Udostępnienie usługi w formie rozwiązania chmurowego w zakresie funkcjonalności testów socjotechnicznych i bazy wiedzy / materiałów edukacyjnych dla dedykowanej grupy operatorów Zamawiającego;
      3. Dostarczenia wszystkich niezbędnych subskrypcji dla 300 użytkowników (adresów email), w okresie 1 roku;
   2. Świadczenie wsparcia w zakresie przeprowadzenia co najmniej 12 kampanii phishingowych.;
   3. Wykonawca musi zapewnić kompletność wszystkich usług wspomagających dla całego procesu wdrożeniowego, co oznacza brak potrzeby korzystania przez Zamawiającego z usług stron trzecich, z wyjątkiem wsparcia technicznego producenta rozwiązania.
2. Zakres wsparcia technicznego oraz utrzymania Systemu
   1. Zapewnienie platformy do komunikacji z Wykonawcą za pomocą środków porozumiewania się na odległość (dalej Hot-Line), dostępnej dla upoważnionych pracowników Zamawiającego, w dni robocze w godzinach od 8:00 do 16:00 z wyjątkiem dni świątecznych i ustawowo wolnych od pracy, obejmującej, co najmniej jeden z następujących kanałów zgłoszeń: serwis WWW, poczta elektroniczna, telefon.
   2. Usuwanie usterek, błędów i błędów krytycznych z zachowaniem poniższych zasad (wymagane czasy napraw):
      1. Usunięcie błędu krytycznego lub wykonanie obejścia błędu krytycznego (umożliwiającego korzystanie z Systemu) nastąpi w czasie 48 godzin zegarowych od przekazania zgłoszenia przez Zamawiającego, przy czym za przyjęcie zgłoszenia rozumie się w przypadku kanału Hot-Line: (i) serwisu WWW oraz poczty elektronicznej – wprowadzenie zgłoszenia do środka komunikacji elektronicznej w taki sposób, aby Wykonawca mógł zapoznać się z treścią zgłoszenia; (ii) telefonu – przekazanie zgłoszenia ustnie w takcie rozmowy z personelem Wykonawcy. Jeżeli jednak bezpośrednią przyczyną powstania błędu krytycznego Systemu jest wada w oprogramowaniu, usunięcie błędu krytycznego nastąpi poprzez współpracę Wykonawcy z producentem Systemu w terminie możliwie najszybszym z punktu widzenia tego producenta, nie dłuższym niż 10 dni roboczych od przekazanie zgłoszenia;
      2. Usunięcie błędu, innego niż błąd krytyczny, nastąpi w ciągu 5 dni roboczych od przekazania zgłoszenia;
      3. Usunięcie usterki nastąpi w ciągu 10 dni roboczych od przekazania zgłoszenia
      4. Rozwiązanie zastępcze może funkcjonować nie dłużej niż 30 dni od daty jego dostarczenia Zamawiającemu