



Opis przedmiotu zamówienia

Szkolenia powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcji personelu, w szczególności reagowanie specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami.

Cel szkolenia: Celem szkolenia jest podniesienie świadomości zagrożeń związanych z cyberatakami oraz doskonalenie umiejętności reagowania na incydenty bezpieczeństwa wśród pracowników jednostek samorządu terytorialnego (JST), w szczególności specjalistów odpowiedzialnych za zarządzanie bezpieczeństwem informacji (SZBI).

Szkolenie obejmuje praktyczne testy socjotechniczne, które pozwolą na weryfikację skuteczności przyjętych procedur oraz ocenę gotowości personelu do wykrywania i neutralizowania zagrożeń.

Grupa docelowa: Pracownicy Urzędu Gminy Zbuczyn oraz 8 jednostek organizacyjnych

Tryb szkolenia: Wykonawca do przeprowadzania szkoleń w formie zdalnej udostępni platformę do realizacji usługi. Dostęp do platformy powinien być możliwy dla Zamawiającego przez co najmniej 30 dni.

Liczba uczestników: 50

Salę szkoleniową: nie dotyczy

Catering podczas szkoleń: nie dotyczy

Materiały szkoleniowe: po stronie Wykonawcy w formie elektronicznej

Dokumentacja szkolenia:

Ponadto Wykonawca zobowiązany jest do:

- zapewnienia każdemu uczestnikowi imiennego certyfikatu/zaświadczenia potwierdzającego ukończenie szkolenia,
- prowadzenia udziału w szkoleniu poprzez zgromadzenie podpisów/logów itp.,
- oznaczenia wszelkich materiałów, prezentacji i innych dokumentów opracowanych na potrzeby szkolenia zgodnie z wymaganiami regulaminu konkursu „Cyberbezpieczny Samorząd”, umowy o powierzenie grantu oraz wniosku o dofinansowanie.

Program szkolenia powinien obejmować przykładowe zagadnienia:

1. Czytelne zasady obsługi - przedstawione w ramach zorganizowanego szkolenia.
2. Bezpieczny sposób sprawdzenia oraz poznania typowych zagrożeń występujących w obszarze przestrzeni internetowej na dedykowanej platformie dostępnej na stronie www. dostosowanej do standardu WCAG 2.1, bez możliwości zapisu oraz archiwizacji wprowadzonych danych.
3. Realizację minimum ośmiu scenariuszy zagrożeń popularnych przestępstw internetowych typu: Phishing Clone, PhishingSpear, PhishingSpear Chat, PhishingWhaling, Pharming, Malware Post, Malware Email.
4. Możliwość tworzenia nowych scenariuszy zagrożeń w obszarze cyberbezpieczeństwa.
5. Nieograniczony dostęp do modułów spełniających poniższe możliwości:



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



- a) Moduł podstron (fałszywych witryn) do tworzenia witryn nakłaniających do pobierania zainfekowanych załączników, podawania wrażliwych danych lub dokonywania płatności internetowych.
- b) Moduł czatu z botami, symulujący wyłudzenia danych osobowych i numerów kart kredytowych.
- c) Moduł e-mail do przeglądania wiadomości z linkami lub załącznikami, symulującymi działanie malware.
- d) Moduł edukacyjny z informacjami o cyberprzestępstwach, identyfikacji zagrożeń, sposobach zapobiegania i działania po oszustwie.
- e) Moduł postów społecznościowych, prezentujący potencjalne ataki phishingowe lub pharmingowe.

W ramach zagadnień wymienionych w pkt a-e) Wykonawca powinien wybrać co najmniej 3 moduły które uwzględni podczas realizacji szkolenia.