Załącznik nr 1 do zapytania ofertowego

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest przeprowadzenie szkoleń powiązanych z testami socjotechnicznymi, weryfikujących świadomość zagrożeń i reakcje personelu, w szczególności sposób postępowania specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami, szkoleń z zakresu cyberbezpieczeństwa istotnych z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji dla kadry, szkoleń podstawowych dla pracowników Starostwa Powiatowego w Aleksandrowie Kujawskim oraz szkoleń specjalistycznych dla informatyka w ramach projektu grantowego „Cyberbezpieczny Samorząd".

I. Ogólny opis przedmiotu zamówienia.

Szkolenia muszą być przeprowadzone w terminach uzgodnionych z Zamawiającym i odbywać się wyłącznie w dni od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy, a w danym terminie może odbywać się tylko jedno ze wskazanych dalej szkoleń. Wykonawca w ramach realizacji przedmiotu zamówienia przygotuje harmonogram oraz program szkoleń i dostarczy go do akceptacji przez Zamawiającego, w terminie nie późniejszym niż 5 dni roboczych przed początkiem terminu szkoleń.

Wykonawca zapewni:

- materiały dydaktyczne dla uczestników szkolenia, odzwierciedlające całość omawianych zagadnień, w tym dostęp do certyfikowanych materiałów szkoleniowych;
- trenera / trenerów posiadającego/posiadających odpowiednie kwalifikacje zawodowe.

Wykonawca zrealizuje usługę szkoleniową zgodnie z dalej podanym opisem i dla dalej wskazanej liczby uczestników.

II. Szczegółowy podział przedmiotu zamówienia.

1) Szkolenie z zakresu cyberbezpieczeństwa, w obszarze istotnym z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji dla kadry kierowniczej Starostwa Powiatowego,
2) Szkolenie podstawowe z zakresu cyberbezpieczeństwa dla pracowników Starostwa Powiatowego,
3) Szkolenia specjalistyczne dla informatyka,
4) Szkolenie powiązane z testami socjotechnicznymi, weryfikujące świadomość zagrożeń i reakcje personelu, w szczególności sposób postępowania specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

III. Szczegółowy opis podzielonych części przedmiotu zamówienia.

Część I

Szkolenie z zakresu cyberbezpieczeństwa, w obszarze istotnym z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji dla kadry Starostwa

1) **Forma szkolenia:** Szkolenie realizowane w formie stacjonarnej, w siedzibie Zamawiającego

2) **Liczba uczestników szkolenia:** 15 osób.

3) **Czas trwania szkolenia:**
Liczba dni: 3 dni;
Liczba godzin: minimum 18 godzin lekcyjnych;

4) **Zakres merytoryczny szkolenia:**
Dzień 1 – szkolenie dla Sekretarza
1. Rola Sekretarza w systemie bezpieczeństwa informacji
2. Nadzór organizacyjny nad bezpieczeństwem informacji
3. Odpowiedzialność Sekretarza wynikająca z przepisów prawa
4. ISO/IEC 27001:2023 – wymagania wobec kadry zarządczej
5. Krajowy System Cyberbezpieczeństwa – obowiązki JST
6. Krajowe Ramy Interoperacyjności – wymagania organizacyjne
7. Zarządzanie ryzykiem w jednostce samorządu terytorialnego
8. Rejestr ryzyk i nadzór nad jego aktualnością
9. Zarządzanie ciągłością działania w JST
10. Analiza wpływu na działalność (BIA)
11. Plany ciągłości działania i plany odtworzeniowe
12. Zarządzanie incydentami bezpieczeństwa informacji
13. Postępowanie w przypadku naruszeń bezpieczeństwa
14. Współpraca z Inspektorem Ochrony Danych
15. Ocena skutków dla ochrony danych (DPIA)
16. Nadzór nad bezpieczeństwem danych osobowych
17. Zarządzanie zmianą organizacyjną i techniczną
18. Bezpieczeństwo informacji w relacjach z podmiotami zewnętrznymi
19. Dokumentowanie i rozliczalność decyzji zarządczych
20. Audyty wewnętrzne i przeglądy zarządzania
21. Odpowiedzialność dyscyplinarna i organizacyjna
22. Doskonalenie systemu bezpieczeństwa informacji

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Dzień 2 – szkolenie dla Zarządu Powiatu Aleksandrowskiego

1. Bezpieczeństwo informacji jako element zarządzania strategicznego
2. Odpowiedzialność Zarządu JST za bezpieczeństwo informacji
3. System Zarządzania Bezpieczeństwem Informacji – perspektywa decyzyjna
4. Podstawy prawne bezpieczeństwa informacji w JST
5. ISO/IEC 27001:2023 – rola najwyższego kierownictwa
6. Krajowy System Cyberbezpieczeństwa – odpowiedzialność organów JST
7. Zarządzanie ryzykiem strategicznym
8. Akceptacja i nadzór nad ryzykiem
9. Zarządzanie ciągłością działania na poziomie decyzyjnym
10. Krytyczne procesy i usługi publiczne
11. Skutki incydentów bezpieczeństwa dla JST
12. Zarządzanie kryzysowe w obszarze IT i informacji
13. Bezpieczeństwo informacji w inwestycjach i projektach IT
14. Nadzór nad dostawcami i usługami zewnętrznymi
15. Bezpieczeństwo informacji a odpowiedzialność finansowa JST
16. Ochrona danych osobowych – odpowiedzialność organu
17. Współpraca Zarządu z Sekretarzem, IOD
18. Audyty, kontrole i odpowiedzialność przed organami nadzorczymi
19. Kultura bezpieczeństwa informacji w JST
20. Reputacja JST i zaufanie publiczne
21. Decyzje strategiczne w sytuacjach incydentów i naruszeń

Dzień 3 – szkolenie dla naczelników wydziałów

1. Rola naczelników wydziałów w systemie bezpieczeństwa informacji
2. Odpowiedzialność naczelników komórek organizacyjnych
3. Bezpieczeństwo informacji w procesach wydziałowych
4. Klasyfikacja informacji i danych
5. Zarządzanie ryzykiem na poziomie wydziału
6. Identyfikacja zagrożeń i podatności
7. Rejestr ryzyk – obowiązki kierownika
8. Bezpieczeństwo danych osobowych w wydziałach
9. Współpraca z Inspektorem Ochrony Danych
10. Ocena skutków przetwarzania danych (DPIA)
11. Zarządzanie dostępami i uprawnieniami pracowników
12. Zasada minimalnych uprawnień
13. Bezpieczeństwo pracy zdalnej i hybrydowej
14. Bezpieczeństwo dokumentacji papierowej i elektronicznej
15. Postępowanie w przypadku incydentów bezpieczeństwa
16. Zgłaszanie i dokumentowanie naruszeń
17. Ciągłość działania procesów wydziałowych
18. Współpraca z zespołem IT
19. Bezpieczeństwo informacji w kontaktach z podmiotami zewnętrznymi
20. Bezpieczeństwo informacji w zamówieniach i umowach
21. Szkolenia i podnoszenie świadomości pracowników
22. Odpowiedzialność służbowa i dyscyplinarna
23. Budowanie kultury bezpieczeństwa w wydziale

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

5) **Wymagania dotyczące trenerów realizujących szkolenie:**

1. Praktyczna znajomość:
   - Systemów Zarządzania Bezpieczeństwem Informacji (SZBI),
   - normy ISO/IEC 27001 (aktualne wydanie),
   - ustawy o krajowym systemie cyberbezpieczeństwa,
   - Krajowych Ram Interoperacyjności,
   - przepisów RODO i ustawy o ochronie danych osobowych.
2. Osoba prowadząca szkolenie powinna posiadać aktualny certyfikat ISO/IEC27001 lub więcej z poniższych:
   - ISO/IEC 27001 Internal Auditor
   - Certified Information Security Manager (CISM)
   - Certified Information Systems Auditor (CISA)
   - Certified Information Systems Security Professional (CISSP)
   - Certified Data Protection Officer (CDPO) lub równoważny
   - Audytor wiodący lub Audytor wewnętrzny ISO 27001
   - Certyfikat potwierdzający kompetencje trenerskie w obszarze cyberbezpieczeństwa lub ochrony danych

6) **Certyfikat ukończenia szkolenia:**
Po ukończeniu szkolenia, uczestnicy szkolenia muszą otrzymać certyfikat ukończenia szkolenia**.**

Część II
Szkolenie podstawowe z zakresu cyberbezpieczeństwa
dla pracowników Starostwa Powiatowego

1) **Forma szkolenia:** Szkolenie realizowane w formie stacjonarnej, w siedzibie Zamawiającego

2) **Liczba uczestników szkolenia:** 60 osób.

3) **Czas trwania szkolenia:**
Liczba dni: 3 dni
Grupy: pracownicy podzieleni zostaną na 3 grupy.
Każdy pracownik przypisany będzie do jednego dnia szkoleniowego

4) **Zakres merytoryczny szkolenia:**

1. Podstawowe pojęcia z zakresu cyberbezpieczeństwa
2. Znaczenie cyberbezpieczeństwa w administracji publicznej
3. Odpowiedzialność pracowników za bezpieczeństwo informacji
4. Zasady bezpiecznego korzystania z systemów informatycznych
5. Polityka Bezpieczeństwa Informacji obowiązująca w Starostwie
6. Klasyfikacja informacji i danych
7. Ochrona danych osobowych w środowisku teleinformatycznym
8. Bezpieczne hasła i uwierzytelnianie użytkowników

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

9. Zasady korzystania z poczty elektronicznej
10. Phishing, spoofing i inne formy socjotechniki
11. Złośliwe oprogramowanie – podstawowe zagrożenia
12. Bezpieczne korzystanie z Internetu
13. Bezpieczeństwo pracy zdalnej i mobilnej
14. Zasady korzystania z urządzeń służbowych
15. Nośniki danych i urządzenia przenośne
16. Bezpieczne przechowywanie i przesyłanie informacji
17. Ochrona dokumentów papierowych i elektronicznych
18. Zasady czystego biurka i czystego ekranu
19. Incydenty cyberbezpieczeństwa – przykłady
20. Rozpoznawanie incydentów bezpieczeństwa
21. Zgłaszanie incydentów bezpieczeństwa
22. Postępowanie w przypadku podejrzenia naruszenia
23. Konsekwencje naruszeń zasad cyberbezpieczeństwa
24. Odpowiedzialność służbowa i dyscyplinarna pracowników
25. Rola pracownika w budowaniu kultury cyberbezpieczeństwa

5) Wymagania dotyczące trenerów realizujących szkolenie:

3. Praktyczna znajomość:
   - Systemów Zarządzania Bezpieczeństwem Informacji (SZBI),
   - normy ISO/IEC 27001 (aktualne wydanie),
   - ustawy o krajowym systemie cyberbezpieczeństwa,
   - Krajowych Ram Interoperacyjności,
   - przepisów RODO i ustawy o ochronie danych osobowych.
4. Osoba prowadząca szkolenie powinna posiadać aktualny certyfikat zawodowy, w szczególności jeden lub więcej z poniższych:
   - ISO/IEC 27001 Lead Auditor lub Lead Implementer
   - ISO/IEC 27001 Internal Auditor
   - Certified Information Security Manager (CISM)
   - Certified Information Systems Auditor (CISA)
   - Certified Information Systems Security Professional (CISSP)
   - Certified Data Protection Officer (CDPO) lub równoważny
   - Audytor wiodący lub Audytor wewnętrzny ISO 27001
   - Certyfikat potwierdzający kompetencje trenerskie w obszarze cyberbezpieczeństwa lub ochrony danych

   Dopuszcza się certyfikaty równoważne potwierdzające porównywalny poziom wiedzy i kompetencji.

6) Certyfikat ukończenia szkolenia:

Po ukończeniu szkolenia, uczestnicy szkolenia muszą otrzymać certyfikat ukończenia szkolenia.

Część III
Szkolenia specjalistyczne dla informatyka

1) Forma szkolenia: Szkolenie realizowane w formie stacjonarnej, w siedzibie Zamawiającego

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

2) **Liczba uczestników szkolenia:** 1 osoba.

3) **Czas trwania szkolenia:**
Liczba dni: 3 dni

4) **Zakres merytoryczny szkolenia:**

A. Systemy Microsoft – Active Directory i Windows Server
   1. Architektura Active Directory w środowisku JST
   2. Projektowanie i utrzymanie struktury domenowej
   3. Zarządzanie kontrolerami domeny
   4. Role FSMO i ich administracja
   5. Replikacja Active Directory
   6. Zarządzanie kontami użytkowników i grup
   7. Zasada najmniejszych uprawnień w AD
   8. Group Policy Objects (GPO) – projektowanie i utrzymanie
   9. Bezpieczeństwo GPO
   10. Audyt i monitorowanie zdarzeń w AD
   11. Integracja AD z usługami zewnętrznymi
   12. Hardening Windows Server
   13. Aktualizacje i zarządzanie poprawkami
   14. Zarządzanie usługami sieciowymi (DNS, DHCP, NTP)
   15. Kopie zapasowe i odtwarzanie AD
   16. Odzyskiwanie po awarii kontrolera domeny
   17. Zabezpieczenia kont uprzywilejowanych

B. Wirtualizacja i infrastruktura – Proxmox VE
   1. Architektura Proxmox VE
   2. Zarządzanie klastrami Proxmox
   3. Wysoka dostępność (HA)
   4. Zarządzanie maszynami wirtualnymi i kontenerami
   5. Zarządzanie storage (LVM, ZFS, Ceph – w kontekście Proxmox)
   6. Backup i replikacja maszyn wirtualnych
   7. Odtwarzanie środowisk po awarii
   8. Aktualizacje i bezpieczeństwo Proxmox
   9. Zarządzanie dostępami i rolami użytkowników
   10. Monitorowanie zasobów i wydajności
   11. Integracja Proxmox z systemami backupu

C. Bezpieczeństwo i monitoring – Wazuh / SIEM / SOC
   1. Architektura Wazuh
   2. Integracja Wazuh z systemami serwerowymi
   3. Integracja z Windows Server i Active Directory
   4. Monitorowanie logów systemowych i aplikacyjnych
   5. Wykrywanie incydentów bezpieczeństwa
   6. Konfiguracja reguł detekcji i alertów
   7. Analiza zdarzeń bezpieczeństwa
   8. Reakcja na incydenty
   9. Integracja z innymi narzędziami bezpieczeństwa

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

10. Raportowanie zdarzeń i incydentów
11. Retencja logów i zgodność z polityką bezpieczeństwa

D. Kopie zapasowe i archiwizacja – biblioteka taśmowa
   1. Zasady backupu i archiwizacji danych
   2. Obsługa biblioteki taśmowej
   3. Konfiguracja i zarządzanie biblioteką taśmową
   4. Rotacja taśm i harmonogramy backupu
   5. Bezpieczne przechowywanie nośników
   6. Testy odtwarzania danych z taśm
   7. Procedury awaryjnego odtwarzania danych
   8. Dokumentowanie procesów backupowych
   9. Integracja biblioteki taśmowej z systemami backupu
   10. Ochrona przed ransomware (air-gap, offline backup)

E. Monitoring infrastruktury – Axcence nVision i narzędzia pokrewne
   1. Architektura systemów monitoringu infrastruktury
   2. Monitorowanie serwerów, usług i zasobów
   3. Monitorowanie sieci i urządzeń peryferyjnych
   4. Konfiguracja alertów i progów
   5. Analiza wydajności i dostępności
   6. Raportowanie stanu infrastruktury
   7. Integracja monitoringu z systemami bezpieczeństwa

F. Sieci i bezpieczeństwo infrastruktury
   1. Segmentacja sieci i VLAN
   2. Zabezpieczenia sieciowe
   3. Firewalle i kontrola ruchu
   4. VPN i bezpieczny dostęp zdalny
   5. Monitoring ruchu sieciowego
   6. Zarządzanie konfiguracją urządzeń sieciowych

G. Zarządzanie podatnościami i aktualizacjami
   1. Identyfikacja podatności technicznych
   2. Skanowanie podatności
   3. Zarządzanie poprawkami bezpieczeństwa
   4. Reagowanie na podatności krytyczne
   5. Dokumentowanie działań naprawczych

H. Zarządzanie incydentami i ciągłość działania
   1. Procedury reagowania na incydenty
   2. Współpraca z IOD i kadrą zarządzającą
   3. Dokumentowanie incydentów
   4. Analiza przyczyn źródłowych (RCA)
   5. Testy planów awaryjnych
   6. Odtwarzanie systemów po awarii

I. Dokumentacja, audyt i zgodność
   1. Prowadzenie dokumentacji technicznej
   2. Rejestry zmian i konfiguracji
   3. Przygotowanie do audytów ISO 27001
   4. Współpraca z audytorami i organami kontrolnymi
   5. Dowody zgodności i raportowanie

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

6. Doskonalenie środowiska IT

5) Wymagania dotyczące trenerów realizujących szkolenie:

1. Praktyczna znajomość:
   - Systemów Zarządzania Bezpieczeństwem Informacji (SZBI),
   - normy ISO/IEC 27001 (aktualne wydanie),
   - ustawy o krajowym systemie cyberbezpieczeństwa,
   - Krajowych Ram Interoperacyjności,
   - przepisów RODO i ustawy o ochronie danych osobowych.
   - Administracja środowiskami **Microsoft Active Directory** w środowiskach produkcyjnych.
   - Administracja systemami **Windows Server** (co najmniej wersje wspierane producenta).
   - Zarządzanie środowiskami wirtualizacji opartymi o **Proxmox VE**.
   - Konfiguracja i utrzymanie systemów monitoringu i bezpieczeństwa typu **SIEM / XDR / Wazuh** lub równoważnych.
   - Realizacja i nadzór nad systemami **kopii zapasowych i archiwizacji**, w tym:
   - obsługa bibliotek taśmowych,
   - procedury odtwarzania danych.
   - Monitorowanie infrastruktury IT przy użyciu narzędzi klasy **Axcence nVision** lub równoważnych.
   - Utrzymanie środowisk IT w jednostkach sektora publicznego lub organizacjach o podwyższonych wymaganiach bezpieczeństwa.
2. Osoba prowadząca szkolenie powinna posiadać aktualny certyfikat ISO/IEC 27001 lub więcej z poniższych:
   - ISO/IEC 27001 Internal Auditor
   - Certified Information Security Manager (CISM)
   - Certified Information Systems Auditor (CISA)
   - Certified Information Systems Security Professional (CISSP)
   - Certified Data Protection Officer (CDPO) lub równoważny
   - Audytor wiodący lub Audytor wewnętrzny ISO 27001
   - Certyfikat potwierdzający kompetencje trenerskie w obszarze cyberbezpieczeństwa lub ochrony danych

6) Certyfikat ukończenia szkolenia:

Po ukończeniu szkolenia, uczestnicy szkolenia muszą otrzymać certyfikat ukończenia szkolenia**.**

Część IV

Szkolenie powiązane z testami socjotechnicznymi, weryfikujące świadomość zagrożeń i reakcje personelu, w szczególności sposób postępowania specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami

1) Forma szkolenia: Szkolenie realizowane w formie stacjonarnej, w siedzibie Zamawiającego

2) Liczba uczestników szkolenia: 70 osób.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

3) Czas trwania szkolenia:
Liczba dni: 3 dni

4) Zakres merytoryczny szkolenia:

ETAP I – Przeprowadzenie testów socjotechnicznych

1. Opracowanie planu testów socjotechnicznych (harmonogram, kanały, grupy uczestników, scenariusze).
2. Dobór scenariuszy testowych adekwatnych do specyfiki JST oraz ról w SZBI.
3. Realizacja testów socjotechnicznych w uzgodnionym zakresie, obejmująca co najmniej:
   - testy e-mail (phishing / spear phishing),
   - testy telefoniczne (vishing),
   - testy wiadomości tekstowych (smishing) lub równoważne,
   - testy bezpośrednie w zakresie bezpieczeństwa fizycznego (bez naruszania porządku pracy).
4. Monitorowanie przebiegu testów i rejestracja wyników w sposób umożliwiający analizę.
5. Weryfikacja reakcji personelu na testy, w szczególności:
   - rozpoznanie zagrożenia,
   - zastosowanie zasad bezpieczeństwa,
   - zgłoszenie/eskalacja zdarzenia zgodnie z procedurami,
   - zachowanie specjalistów realizujących obowiązki w SZBI.
6. Dokumentacja przebiegu testów (z zachowaniem zasad poufności i minimalizacji danych).

ETAP II – Opracowanie i omówienie wyników testów

1. Analiza wyników testów socjotechnicznych, w tym:
   - wskaźniki skuteczności (np. reakcji prawidłowych/nieprawidłowych),
   - analiza kanałów (e-mail/telefon/SMS),
   - analiza wg grup (pracownicy/kierownicy/specjaliści SZBI),
   - analiza zgodności reakcji z procedurami.
2. Identyfikacja obszarów wymagających doskonalenia: kompetencyjnych, proceduralnych i organizacyjnych.
3. Opracowanie raportu z testów zawierającego co najmniej:
   - zestawienie zastosowanych scenariuszy (bez ujawniania treści operacyjnych),
   - zbiorcze wyniki i wnioski,
   - rekomendacje działań korygujących i zapobiegawczych.
4. Przeprowadzenie spotkania/omówienia wyników z Zamawiającym wg wskazania Zamawiającego.
5. Uzgodnienie zakresu szkolenia korygującego na podstawie wyników.

ETAP III – Szkolenie po testach (szkolenie korygujące i utrwalające)

1. Realizacja szkolenia dla personelu w oparciu o wyniki testów, obejmującego co najmniej:
   - rozpoznawanie technik socjotechnicznych,
   - prawidłowe reakcje i zachowania,
   - zasady zgłaszania i eskalacji incydentów,

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

- obowiązki i odpowiedzialności ról w SZBI.

2. Szkolenie dedykowane dla specjalistów realizujących obowiązki w SZBI w zakresie:
   - obsługi zgłoszeń, klasyfikacji zdarzeń, eskalacji, dokumentowania,
   - komunikacji wewnętrznej i koordynacji działań.
3. Przeprowadzenie testu wiedzy po szkoleniu (forma pisemna lub elektroniczna).
4. Przekazanie materiałów szkoleniowych (forma elektroniczna).
5. Przekazanie raportu poszkoleniowego (lista obecności, wyniki testu, rekomendacje dalszych działań).

5) Katalog przykładowych scenariuszy testów socjotechnicznych

1) Phishing „pilna wiadomość służbowa”
- Kanał: e-mail
- Cel weryfikacji: rozpoznanie presji czasu, weryfikacja nadawcy, reakcja wg procedury
- Obszary: poczta, zgłaszanie incydentu, eskalacja

2) Spear phishing do komórek merytorycznych
- Kanał: e-mail
- Cel weryfikacji: identyfikacja dopasowanych treści, ostrożność przy załącznikach
- Obszary: obieg dokumentów, załączniki, komunikacja wewnętrzna

3) „Zmiana danych kontrahenta / rachunku bankowego”
- Kanał: e-mail
- Cel weryfikacji: procedury potwierdzania zmian, zasada dwóch par oczu
- Obszary: finanse, księgowość, zamówienia/public procurement

4) „Prośba o szybkie udostępnienie danych / zestawienia”
- Kanał: e-mail
- Cel weryfikacji: klasyfikacja informacji, minimalizacja danych, autoryzacja odbiorcy
- Obszary: dane osobowe, informacje wewnętrzne, udostępnienia

5) „Komunikat IT o konieczności potwierdzenia tożsamości”
- Kanał: e-mail / komunikator
- Cel weryfikacji: odporność na podszywanie się pod IT, stosowanie oficjalnych kanałów
- Obszary: helpdesk, weryfikacja zgłoszeń, MFA/hasła

6) Vishing do sekretariatu
- Kanał: telefon
- Cel weryfikacji: weryfikacja rozmówcy, przekazywanie informacji, eskalacja do właściwych ról
- Obszary: obsługa połączeń, procedury kontaktowe, notatki służbowe

7) Vishing „reset hasła / pilna pomoc z dostępem”
- Kanał: telefon
- Cel weryfikacji: ochrona poświadczeń, procedura resetu, tożsamość dzwoniącego
- Obszary: konta uprzywilejowane, helpdesk, AD/Windows

8) Smishing „powiadomienie systemowe”
- Kanał: SMS
- Cel weryfikacji: kliknięcia w linki, zgłoszenie incydentu, użycie urządzeń służbowych
- Obszary: urządzenia mobilne, praca w terenie

9) Smishing „dopłata/kurier/faktura”
- Kanał: SMS
- Cel weryfikacji: odporność na bodźce finansowe, raportowanie podejrzanych treści
- Obszary: finanse, zakupy, prywatne/służbowe urządzenia

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

10) „Załącznik z rzekomą skargą/wnioskiem”
- Kanał: e-mail
- Cel weryfikacji: higiena pracy z dokumentami, zgłaszanie podejrzeń, izolacja zdarzenia
- Obszary: kancelaria, ePUAP/korespondencja, bezpieczeństwo stacji roboczych

11) „Link do pliku w chmurze”
- Kanał: e-mail
- Cel weryfikacji: weryfikacja źródła, zasady wymiany informacji, ocena ryzyka
- Obszary: współpraca zewnętrzna, udostępnienia

12) „Zaproszenie na spotkanie / agenda”
- Kanał: e-mail / kalendarz
- Cel weryfikacji: sprawdzanie zaproszeń, bezpieczne otwieranie treści
- Obszary: kalendarze, wideokonferencje

13) „Nowy regulamin/zarządzenie do podpisu”
- Kanał: e-mail
- Cel weryfikacji: obieg dokumentów, autoryzacja, zasady akceptacji
- Obszary: kadry kierownicze, workflow, podpis elektroniczny

14) Podszycie pod obywatela/petenta – „prośba o przyspieszenie sprawy”
- Kanał: telefon / e-mail
- Cel weryfikacji: ujawnianie informacji o sprawach, wrażliwość danych
- Obszary: obsługa interesantów, tajemnica postępowania

15) Podszycie pod instytucję kontrolną
- Kanał: e-mail / telefon
- Cel weryfikacji: procedury kontaktu z organami, ścieżka formalna, eskalacja
- Obszary: sekretariat, zarząd, korespondencja formalna

16) „Prośba o listę pracowników / strukturę organizacyjną”
- Kanał: e-mail
- Cel weryfikacji: ochrona informacji organizacyjnych, minimalizacja danych
- Obszary: HR, organizacja, informacje wewnętrzne

17) „Weryfikacja uprawnień / dostępów”
- Kanał: e-mail / telefon
- Cel weryfikacji: zasady IAM, brak ujawniania informacji o kontach i rolach
- Obszary: AD, dostęp uprzywilejowany, procedury nadawania uprawnień

18) „Prośba o instalację / aktualizację pilnego narzędzia”
- Kanał: e-mail / telefon
- Cel weryfikacji: proces zmian, autoryzacja instalacji, zatwierdzenia
- Obszary: zarządzanie zmianą, bezpieczeństwo oprogramowania

19) „Odzyskanie danych / backup na żądanie”
- Kanał: e-mail / telefon
- Cel weryfikacji: procedury odtwarzania, autoryzacja wniosku, rola specjalistów SZBI
- Obszary: backup, biblioteka taśmowa, dokumentowanie

20) „Prośba o logi / raport bezpieczeństwa”
- Kanał: e-mail
- Cel weryfikacji: retencja, poufność logów, kanały przekazywania, zatwierdzenia
- Obszary: Wazuh/SIEM, rejestry, incydenty

21) „Wejście do budynku – osoba z serwisu”
- Kanał: kontakt bezpośredni
- Cel weryfikacji: procedury weryfikacji, rejestr wejść, asysta pracownika

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

- Obszary: bezpieczeństwo fizyczne, serwerownia/punkty dystrybucyjne

22) „Dostarczenie nośnika / pendrive / płyta”
- Kanał: fizyczny
- Cel weryfikacji: zasady pracy z nośnikami, izolacja, zgłoszenie zdarzenia
- Obszary: DLP, stacje robocze, procedury

23) „Prośba o szybkie wydrukowanie / skanowanie”
- Kanał: bezpośredni / e-mail
- Cel weryfikacji: czyste biurko/ekran, ochrona dokumentów, odbiór wydruków
- Obszary: drukarki/skanery, obieg papierowy

24) Test reakcji specjalistów SZBI – „eskalacja incydentu”
- Kanał: zgłoszenie wewnętrzne
- Cel weryfikacji: przyjęcie zgłoszenia, klasyfikacja, ścieżka eskalacji i dokumentowanie
- Obszary: rejestr incydentów, komunikacja kryzysowa, role SZBI

25) Test „komunikacja wewnętrzna o incydencie”
- Kanał: e-mail / komunikator / telefon
- Cel weryfikacji: spójność komunikacji, kanały, rola kierownictwa i IT
- Obszary: ciągłość działania, zarządzanie kryzysowe, procedury

6) Wymagania dotyczące trenerów realizujących szkolenie:

1. Praktyczna znajomość:
   - Systemów Zarządzania Bezpieczeństwem Informacji (SZBI),
   - normy ISO/IEC 27001 (aktualne wydanie),
   - ustawy o krajowym systemie cyberbezpieczeństwa,
   - Krajowych Ram Interoperacyjności,
   - przepisów RODO i ustawy o ochronie danych osobowych.
   - Trener musi posiadać doświadczenie praktyczne w realizacji testów socjotechnicznych lub kampanii podnoszenia świadomości bezpieczeństwa.
2. Osoba prowadząca szkolenie powinna posiadać aktualny certyfikat ISO/IEC 27001 lub więcej z poniższych:
   - ISO/IEC 27001 Internal Auditor
   - Certified Information Security Manager (CISM)
   - Certified Information Systems Auditor (CISA)
   - Certified Information Systems Security Professional (CISSP)
   - Certified Data Protection Officer (CDPO) lub równoważny
   - Audytor wiodący lub Audytor wewnętrzny ISO 27001
   - Certyfikat potwierdzający kompetencje trenerskie w obszarze cyberbezpieczeństwa lub ochrony danych
3. Osoba prowadząca szkolenie powinna wykazać min. 3-letnie doświadczenie obejmujące:
   - Projektowanie i realizacja testów socjotechnicznych (phishing, vishing, smishing lub równoważne).
   - Analiza zachowań użytkowników w kontekście bezpieczeństwa informacji.
   - Ocena reakcji organizacji na incydenty bezpieczeństwa.
   - Praca z procedurami SZBI, w tym: procedurami reagowania na incydenty, procedurami eskalacji, rejestrowaniem i dokumentowaniem zdarzeń.
   - Doświadczenie w pracy z jednostkami sektora publicznego lub organizacjami o podwyższonych wymaganiach bezpieczeństwa.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

7) **Certyfikat ukończenia szkolenia:**
Po ukończeniu szkolenia, uczestnicy szkolenia muszą otrzymać certyfikat ukończenia szkolenia**.**

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA