ZP.271.02.2026 Załącznik nr 7

Opis Przedmiotu Zamówienia

Spis treści

[Słownik 2](#_Toc211252482)

[1. Organizacja realizacji zamówienia 3](#_Toc211252483)

[2. Przeprowadzenie audytów KRI 4](#_Toc211252484)

[2.1. Przeprowadzenie audytów zgodności z Krajowymi Ramami Interoperacyjności 4](#_Toc211252485)

[2.2. Zakres audytu oraz sposób prowadzenia audytu KRI 4](#_Toc211252486)

[3. Przygotowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) 7](#_Toc211252487)

[3.1. Inwentaryzacja zasobów informacyjnych 7](#_Toc211252488)

[3.2. Szacowanie ryzyka 8](#_Toc211252489)

[3.3. Przeprowadzenie audytu w celu przygotowania dokumentacji 8](#_Toc211252490)

[4. Przeprowadzenie audytu bezpieczeństwa technicznego 9](#_Toc211252491)

[4.1. Zakres prac objętych audytem bezpieczeństwa technicznego 10](#_Toc211252492)

[4.2. Raport 11](#_Toc211252493)

[4.3. Sposób przygotowania dokumentacji SZBI 11](#_Toc211252494)

[4.4. Przygotowanie rejestru ryzyka zgodnie z SZBI 12](#_Toc211252495)

[5. Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji 14](#_Toc211252496)

[5.1. Zakres i sposób wdrożenia 14](#_Toc211252497)

[5.2. Przeszkolenie użytkowników z zakresu SZBI 16](#_Toc211252498)

[6. Przeprowadzenie testów socjotechnicznych 18](#_Toc211252499)

[6.1. Warunki wstępne i sposób realizacji 19](#_Toc211252500)

[6.2. Szczegółowy opis testów 19](#_Toc211252501)

[6.2.1. Stworzenie fałszywych stron 19](#_Toc211252502)

[6.2.2. Wysłanie wiadomości pocztą elektroniczną 20](#_Toc211252503)

[7. Przeprowadzenie testów odporności haseł użytkowników na złamanie 22](#_Toc211252504)

[8. Przeprowadzenie szkoleń 24](#_Toc211252505)

[8.1. Wymagania ogólne dla szkolenia 24](#_Toc211252506)

[8.2. Przeszkolenie użytkowników z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa 25](#_Toc211252507)

[8.3. Szkolenia dla nauczycieli z zakresu cyberbezpieczeństwa 26](#_Toc211252508)

[8.4. Szkolenie ze stosowania i budowania silnych haseł, wykorzystywania menadżerów haseł oraz szyfrowania danych osobowych 27](#_Toc211252509)

[8.5. Szkolenie specjalistyczne dla informatyka Urzędu Gminy 27](#_Toc211252510)

[8.6. Szkolenie z ochrony przed wyłudzeniem danych osobowych i informacji 28](#_Toc211252511)

[8.7. Szkolenia z zabezpieczenia sprzętu prywatnego wykorzystywanego do celów służbowych 29](#_Toc211252512)

[9. Kryteria jakościowe dla odbioru przedmiotu Zamówienia 30](#_Toc211252513)

[W zakresie krytycznych systemów teleinformatycznych 30](#_Toc211252514)

[Dokumentacji projektowej (w tym SZBI, raportów i innych) 30](#_Toc211252515)

[W zakresie szkoleń 30](#_Toc211252516)

[10. Prawa autorskie i majątkowe 30](#_Toc211252517)

# Słownik

|  |  |  |
| --- | --- | --- |
| **L.P** | Pojęcie | **Opis** |
|  | Zamawiający | Gmina Tarnów Opolski i jednostki gminne |
|  | Test socjotechniczny | Kontrolowany i systematyczny proces symulacji prób manipulacji ludźmi w celu uzyskania poufnych informacji, dostępu do systemów komputerowych lub wywołania określonych działań, które mogą zagrozić bezpieczeństwu organizacji. Testy socjotechniczne są przeprowadzane w celu oceny świadomości pracowników na temat zagrożeń związanych z inżynierią społeczną oraz identyfikacji potencjalnych luk w procesach bezpieczeństwa organizacji. |
|  | Środowisko aplikacyjne | Zintegrowane środowisko, które obejmuje wszystkie zasoby, narzędzia, oprogramowanie, usługi i konfiguracje niezbędne do uruchamiania, testowania, wdrażania oraz utrzymania aplikacji w ramach infrastruktury IT. Jest to ekosystem, w którym aplikacja funkcjonuje, obejmujący zarówno komponenty sprzętowe, jak i programowe, które wspierają działanie i rozwój aplikacji.  Kluczowe Elementy Środowiska Aplikacyjnego:  **Sprzęt (Hardware):**   * Serwery: Maszyny fizyczne lub wirtualne, na których uruchamiane są aplikacje. * Pamięć Masowa: Dyski twarde, SSD, systemy SAN/NAS do przechowywania danych. * Sieć: Urządzenia sieciowe, takie jak routery, przełączniki, firewalle, które umożliwiają komunikację między komponentami systemu.   **Oprogramowanie (Software):**   * System Operacyjny: Podstawowe oprogramowanie, które zarządza zasobami sprzętowymi i dostarcza usług dla aplikacji (np. Windows, Linux). * Serwer Aplikacji: Oprogramowanie, które uruchamia aplikacje i zarządza ich działaniem (np. Apache Tomcat, Microsoft IIS). * Baza Danych: System zarządzania bazą danych (DBMS) używany do przechowywania i zarządzania danymi aplikacji (np. MySQL, PostgreSQL, Oracle). * Narzędzia Programistyczne: IDE, frameworki, biblioteki i inne narzędzia używane do tworzenia i testowania aplikacji (np. Eclipse, Visual Studio, Spring, Django). * Usługi i Infrastruktura (Services and Infrastructure): * Chmura: Usługi chmurowe, które oferują skalowalne zasoby obliczeniowe i pamięciowe (np. AWS, Microsoft Azure, Google Cloud Platform). * Usługi Wspomagające: Usługi takie jak serwery DNS, serwery proxy, usługi cache’owania (np. Redis, Memcached).   **Konfiguracja i Zarządzanie (Configuration and Management):**   * Konfiguracja Systemu: Ustawienia i parametry konfiguracyjne aplikacji i jej środowiska. * Automatyzacja i Zarządzanie Konfiguracją: Narzędzia do zarządzania konfiguracją i automatyzacji wdrożeń (np. Ansible, Puppet, Chef). * Monitorowanie i Logowanie: Systemy monitorowania wydajności i dostępności aplikacji, oraz logowania błędów i zdarzeń (np. Nagios, Prometheus, ELK Stack).   **Bezpieczeństwo (Security):**   * Kontrole Dostępu: Mechanizmy autoryzacji i uwierzytelniania użytkowników. * Ochrona Danych: Szyfrowanie danych, backupy, polityki zarządzania danymi. * Testy Bezpieczeństwa: Regularne audyty i testy penetracyjne w celu identyfikacji i eliminacji podatności.   **Dla aplikacji webowej, środowisko aplikacyjne może obejmować:**   * Serwer WWW: Apache HTTP Server lub Nginx. * System Operacyjny: Ubuntu Linux. * Baza Danych: MySQL lub PostgreSQL. * Język Programowania: Python z frameworkiem Django. * Usługi Chmurowe: AWS EC2 dla serwerów aplikacji, S3 dla przechowywania danych, RDS dla bazy danych. * Narzędzia Monitorujące: Prometheus dla monitorowania wydajności, Grafana dla wizualizacji danych. * Mechanizmy Bezpieczeństwa: Certyfikaty SSL/TLS dla zabezpieczenia komunikacji, usługi WAF (Web Application Firewall) dla ochrony przed atakami. |
|  | 2700X | Zamawiający ilekroć mowa o 27001 ma na myśli normy:  PN-EN ISO/IEC 27001:2023-08 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności -- Systemy zarządzania bezpieczeństwem informacji -- Wymagania,  PN-EN ISO/IEC 27002:2023-01 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Zabezpieczanie informacji. |
|  | **SZBI** | System Zarządzania Bezpieczeństwem Informacji – zestaw polityk, procedur i kontroli zapewniających bezpieczeństwo informacji. |
|  | **KRI** | Krajowe Ramy Interoperacyjności – rozporządzenie określające wymagania dla systemów teleinformatycznych w administracji publicznej. |
|  | **WAF** | Web Application Firewall – mechanizm ochrony aplikacji webowych przed atakami. |
|  | **UTM** | Unified Threat Management – urządzenie integrujące funkcje bezpieczeństwa (firewall, IPS, AV). |
|  | **CVSS** | Common Vulnerability Scoring System – standard oceny podatności (wersja 4.0 w dokumencie). |
|  | **CVE** | Common Vulnerabilities and Exposures – słownik znanych podatności. |
|  | **Phishing** | Atak polegający na podszywaniu się pod zaufane źródło w celu wyłudzenia danych. |
|  | **2FA** | Podwójne uwierzytelnienie – dodatkowa warstwa zabezpieczeń przy logowaniu. |
|  | **Typosquatting** | Rejestracja domen podobnych do oryginalnych w celu oszustwa. |
|  | **VPN** | Virtual Private Network – szyfrowane połączenie chroniące transmisję danych. |
|  | **SSL/TLS** | Protokoły szyfrowania komunikacji w sieci. |
|  | **Hardening** | Proces wzmacniania konfiguracji systemów i aplikacji w celu zwiększenia bezpieczeństwa. |
|  | **Penetration Testing Execution Standard (PTES)** | Standard realizacji testów penetracyjnych. |
|  | **NSC** | Narodowe Standardy Cyberbezpieczeństwa – rekomendacje dla zabezpieczeń sieci i systemów. |
|  | **Rainbow Tables** | Prekomputowane tablice używane do łamania hashy haseł. |
|  | **OSCP** | Offensive Security Certified Professional – certyfikat potwierdzający umiejętności pentestera. |
|  | **CIPP/E** | Certified Information Privacy Professional/Europe – certyfikat z zakresu ochrony danych osobowych. |
|  | **ACO** | Approved Compliance Officer (ACO) to osoba posiadająca formalne kwalifikacje i uprawnienia do nadzorowania zgodności organizacji z obowiązującymi przepisami prawa, regulacjami branżowymi oraz wewnętrznymi politykami. |

# Organizacja realizacji zamówienia

1. Komunikacja w ramach niniejszego zamówienia oraz podczas jego realizacji może odbywać się telefonicznie, poprzez komunikatory, ale wszelkie uzgodnienia w zakresie realizacji przedmiotu muszą być uzgadniane pomiędzy stronami pisemnie, w tym elektronicznie, poprzez wymianę informacji pocztą elektroniczną na wskazane adresy email.
2. Realizacja przedmiotu zamówienia odbywać się będzie zdalnie oraz lokalnie w zakresie właściwym dla zadania. Realizacja zleconych zadań może wymagać w uzasadnionych przypadkach obecności Wykonawcy w siedzibie Zamawiających nawet jeżeli określono realizację zdalną wybranego zakresu, jeżeli zdalna realizacja będzie niemożliwa lub może negatywnie wpływać na jakość wykonania przedmiotu projektu.
3. Wykonawca musi przekazywać w trakcie realizacji czynności przewidzianych niniejszym zamówieniem informacje o wszelkich wykrytych podatnościach, w celu umożliwienia Zamawiającemu podjęcia natychmiastowych działań naprawczych.
4. Wykonawca każdorazowo, winien uzgadniać z Zamawiającym termin prowadzenia bardziej inwazyjnych czynności ze szczególnym uwzględnieniem: DoS, i prowadzić je dopiero po uzyskaniu pisemnej, w tym poprzez środki elektronicznej komunikacji, zgody osoby Zamawiającego. Wykonawca musi prowadzić prace, które umożliwią mu zakończenie w każdym momencie takich testów.
5. Jakiekolwiek czynności prowadzone przez Wykonawcę nie mogą spowodować przestoju w świadczeniu usług przez Zamawiającego. Gdyby jednak przeprowadzenie testów rodziło ryzyko przestoju w pracy, Wykonawca w porozumieniu z Zamawiającym Wykonawcą opracuje, zaakceptowany przez Zamawiającego, scenariusz alternatywny przeprowadzenia testów tak aby zminimalizować ryzyku problemów.
6. Wykonawca może prowadzić prace po uprzednim uzgodnieniu ich zakresu z każdym z Zamawiających. Przez uzgodnienie należy rozumieć precyzyjne wskazanie daty oraz czasu rozpoczęcia a także zakończenia prac.
7. Wykonawca ma obowiązek ścisłej współpracy z Zamawiającym na każdym etapie realizacji zamówienia.
8. Wykonawca winien uwzględniać wszelkie uwagi Zamawiającego, które doprecyzowują lub uzupełniają zapisy w zapytaniu ofertowym i nie są z nimi sprzeczne.
9. Zamawiający we współpracy z Wykonawcą ustalą harmonogram spotkań mających na celu weryfikację stanu projektu. Zakłada się minimalną częstotliwość spotkań raz w tygodniu.
10. Wykonawca musi dostosować się do polityk bezpieczeństwa Zamawiającego.

# Wymagania wobec wykonawcy przed podpisaniem umowy

Wykonawca wybrany w toku postępowania zobowiązany jest, przed podpisaniem umowy,   
do przedstawienia oświadczenia potwierdzającego dysponowanie zespołem osób spełniających wymagania określone poniżej zgodnie z zapisami Rozdziału XXXII pkt 2 lit. c :

* 1. Audytor bezpieczeństwa organizacyjnego (dwie osoby):
     1. co najmniej 3 letnie doświadczenie w zakresie prowadzenia audytów bezpieczeństwa uwzględniających założenia wynikające z normy ISO 27001 i/lub KRI,
     2. doświadczenie w przygotowaniu kompleksowej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z normą PN-EN ISO/IEC 27001 poparte dwiema referencjami albo protokołem odbioru zadania, w którym wskazana osoba brała udział,
     3. certyfikat uprawniający do przeprowadzenia audytu zgodnie z rozporządzeniem Ministra Cyfryzacji 1 z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu,
  2. Audytor zgodności z RODO (jedna osoba):
     1. Co najmniej jedna osoba posiadająca:
     2. Wykształcenie i kwalifikacje:
        1. Wykształcenie wyższe.
        2. Ukończone studia podyplomowe z zakresu ochrony danych osobowych lub audytu wewnętrznego albo certyfikat potwierdzający CIPP/E (Certified Information Privacy Professional/Europe) lub Approved Compliance Officer lub równoważny.
        3. Jeden z certyfikatów wymienionych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzania audytu
     3. Doświadczenie zawodowe
        1. Minimum 5 lat doświadczenia zawodowego w zakresie ochrony danych osobowych, w tym co najmniej 3 lata w roli audytora RODO.
        2. Udokumentowane przeprowadzenie co najmniej trzech audytów zgodności z RODO w jednostkach sektora publicznego w ciągu ostatnich 5 lat.
     4. Wymagania dodatkowe
        1. Brak powiązań osobistych lub zawodowych z podmiotem zamawiającym (wymóg niezależności).
  3. Pentester (co najmmiej dwie osoby)
     1. co najmniej 3 letnie doświadczenie w zakresie pełnienia funkcji audytora bezpieczeństwa technicznego w zakresie stosowania środków ochrony danych przetwarzanych w postaci elektronicznej potwierdzone certyfikatem OSCP (Offensive Security Certified Professional) albo innym certyfikatem inżynierskim potwierdzającym kompetencje techniczne w obszarze cyberbezpieczeństwa,
     2. co najmniej 3 letnie doświadczenie w zakresie prowadzenia audytów bezpieczeństwa technicznego uwzględniających założenia OWASP top 10 poparte dwiema referencjami albo protokołem odbioru zadania, w którym wskazana osoba brała udzi~~ał,~~
     3. wykonywał testy penetracyjne w przynajmniej 3 projektach dedykowanych do korzystania dla sumarycznie co najmniej 100 tysięcy użytkowników,
     4. wykonywał testy socjotechniczne w przynajmniej 2 projektach, dedykowanych dla przynajmniej 100 osób w każdym projekcie, stanowiących próbę testową,
     5. posiada doświadczenie w przygotowaniu kompleksowej dokumentacji testów penetracyjnych z przynajmniej 2 testów,
     6. jeden z pentesterów winien posiadać certyfikat Offensive Security Web Expert) lub równoważny.
  4. Trener bezpieczeństwa przynajmniej dwie osoby (mogą występować w roli Audytora bezpieczeństwa organizacyjnego albo Audytora bezpieczeństwa technicznego)
     1. Każda z dedykowanych osób przeprowadziła co najmniej 5 szkoleń z obszaru cyberbezpieczeństwa (szkolenia dla jednego trenera nie mogą powielać się u drugiego) dedykowane dla jednostek administracji publicznej,
     2. Każda z dedykowanych osób przeprowadziła przynajmniej dwa szkolenia w zakresie użytkowania Systemu Zarządzania Bezpieczeństwem Informacji,
     3. Każda osoba posiada minimalnie 5 letnie doświadczenie w zakresie prowadzenia szkoleń w obszarze cyberbezpieczeństwa.

2.5 Za certyfikaty równoważne do:

\* certyfikatu CIPP/E (Certified Information Privacy Professional/Europe)

\* certyfikatu ACO (Approved Compliance Officer)

\* certyfikatu OSCP (Offensive Security Certified Professional)

\* certyfikatu OSWE (Offensive Security Web Expert)

Za certyfikat równoważny Zamawiający uzna certyfikat, który spełnia **łącznie** następujące warunki:

1. **Został wydany przez niezależną i wiarygodną instytucję certyfikującą**, posiadającą udokumentowane kompetencje i uprawnienia do potwierdzania kwalifikacji zawodowych   
   w obszarze:
   * ochrony danych osobowych i prywatności (dla CIPP/E),
   * compliance i zgodności regulacyjnej (dla ACO),
   * bezpieczeństwa technicznego systemów informatycznych i testów penetracyjnych (dla OSCP i OSWE).
2. **Dotyczy tego samego obszaru kwalifikacji zawodowych**, co certyfikat referencyjny,   
   w szczególności:
   * dla CIPP/E – prawa ochrony danych osobowych w UE, RODO, nadzoru, praw osób, transferów danych,
   * dla ACO – systemów compliance, zarządzania zgodnością, ryzyk regulacyjnych   
     i audytów zgodności,
   * dla OSCP – praktycznych testów penetracyjnych systemów i sieci,
   * dla OSWE – zaawansowanych testów bezpieczeństwa aplikacji webowych.
3. **Potwierdza zakres wiedzy i umiejętności zasadniczo tożsamy z oficjalnym sylabusem egzaminacyjnym** certyfikatu, do którego zgłaszana jest równoważność.
4. **Został uzyskany w wyniku przejścia sformalizowanej procedury certyfikacyjnej**, obejmującej:
   * egzamin teoretyczny i/lub praktyczny,
   * weryfikację wiedzy i umiejętności kandydata,
   * ocenę dokonywaną przez niezależny podmiot certyfikujący,  
     przy czym procedura ta musi być **porównywalna co do poziomu trudności, zakresu oraz metodyki oceny** z procedurą certyfikacji certyfikatu referencyjnego.

**W celu potwierdzenia równoważności certyfikatu Wykonawca zobowiązany jest opisać w oświadczeniu uzasadnienie równoważności, wskazujące na zgodność zakresu wiedzy, umiejętności oraz procedury certyfikacyjnej z certyfikatem referencyjnym.**

# Przeprowadzenie audytów KRI

## Przeprowadzenie audytów zgodności z Krajowymi Ramami Interoperacyjności

Dla każdej jednostki wymienionej w tabeli poniżej wymagane jest przeprowadzenie audytu zgodności z KRI

|  |  |
| --- | --- |
| Nazwa jednostki | Liczba |
| Urząd Gminy w Tarnowie Opolskim | 1 |
| Gminny Ośrodek Pomocy Społecznej | 1 |
| Biuro Obsługi Oświaty Samorządowej | 1 |
| Publiczna Szkoła Podstawowa w Kątach Opolskich | 1 |
| Publiczna Szkoła Podstawowa w Nakle | 1 |
| Publiczna Szkoła Podstawowa im. Mikołaja Kopernika w Tarnowie Opolskim | 1 |
| Przedszkole Publiczne w Kosorowicach | 1 |
| Przedszkole Publiczne w Przyworach | 1 |
| Przedszkole Publiczne z Oddziałami Integracyjnymi im. bł. Edmunda Bojanowskiego w Tarnowie Opolskim | 1 |

## Zakres audytu oraz sposób prowadzenia audytu KRI

Audyt zgodności z Krajowymi Ramami Interoperacyjności nie może zostać wykonany zdalnie. Musi zostać zrealizowany w siedzibie Zamawiającego.

Przygotowanie do Audytu

a. Zebranie Informacji

* Dokumentacja Organizacji: Zebranie wszelkiej dokumentacji organizacji dotyczącej polityki bezpieczeństwa, procedur, procesów, systemów IT, architektury sieciowej, itp.
* Spotkanie Wstępne: Organizacja spotkania wstępnego z kierownictwem i kluczowymi interesariuszami w celu omówienia zakresu audytu, harmonogramu i oczekiwań.

b. Planowanie Audytu

* Definiowanie Zakresu Audytu: Określenie zakresu audytu zgodnie z wymaganiami KRI, w tym systemów, procesów i jednostek organizacyjnych, które będą objęte audytem. Zakres audytu musi być wynikiem odwołania się do §20 rozporządzenia z dnia 21 maja 2024 r w sprawie Krajowych Ram Interoperacyjności. Wykonawca ma obowiązek przygotować listę szczegółową sprawdzeń (tzw. kontrolek), które doprecyzują zakres ogólnie opisany w rozporządzeniu. Lista, o której mowa musi być uzgodniona i zaakceptowana przez Zamawiającego.
* Tworzenie Harmonogramu: Ustalenie szczegółowego harmonogramu audytu, w tym daty przeglądów dokumentacji, wywiadów, inspekcji i analiz technicznych.
* Zespoły Audytowe: Skład zespołów audytowych z przypisaniem ról i odpowiedzialności.

2. Przegląd Dokumentacji

a. Analiza Dokumentów

* Przegląd Polityk i Procedur: Analiza polityk i procedur organizacji w celu sprawdzenia zgodności z wymaganiami KRI.
* Analiza Dokumentacji Technicznej: Przegląd dokumentacji technicznej, w tym konfiguracji systemów, schematów architektury sieciowej, raportów z testów bezpieczeństwa.
* Zgromadzenie Dowodów: Zbieranie dowodów potwierdzających zgodność, takich jak protokoły, logi systemowe, raporty z audytów wewnętrznych, wyniki testów penetracyjnych.

b. Ocena Zgodności

* Ocena Wymagań KRI: Porównanie polityk i procedur organizacji z wymaganiami KRI, identyfikacja obszarów zgodności i niezgodności.
* Dokumentowanie Wyników: Dokumentowanie wyników przeglądu dokumentacji, w tym wykazanie obszarów zgodności oraz wszelkich wykrytych niezgodności.

3. Inspekcje Techniczne i Wywiady

a. Inspekcje Techniczne

* Inspekcje Systemów IT: Przeprowadzanie inspekcji systemów IT w celu weryfikacji ich konfiguracji i zabezpieczeń.
* Testy Bezpieczeństwa: Wykonywanie testów bezpieczeństwa, takich jak skanowanie podatności, testy penetracyjne, analiza logów, weryfikacja ustawień zabezpieczeń.
* Ocena Sieci i Infrastruktur: Analiza topologii sieciowej, konfiguracji firewalli, VPN, systemów wykrywania i zapobiegania włamaniom.

b. Wywiady z Kluczowymi Pracownikami

* Wywiady z Kierownictwem: Rozmowy z kierownictwem IT oraz kierownikami odpowiedzialnymi za bezpieczeństwo informacji w celu oceny ich świadomości i zaangażowania w kwestie zgodności z KRI.
* Wywiady z Pracownikami Technicznymi: Wywiady z pracownikami odpowiedzialnymi za administrację systemów, bezpieczeństwo IT, zarządzanie siecią, w celu zrozumienia ich codziennych praktyk i procedur.

4. Analiza i Ocena Wyników

a. Analiza Zebranych Danych

* Porównanie z Wymaganiami KRI: Analiza zebranych danych i wyników testów w kontekście wymagań KRI.
* Identyfikacja Luk: Identyfikacja wszelkich luk bezpieczeństwa, braków w procedurach, niezgodności z wymaganiami KRI.

b. Opracowanie Raportu z Audytu

* Tworzenie Raportu: Przygotowanie szczegółowego raportu z audytu, zawierającego opis przeprowadzonych działań, wyniki inspekcji, wykryte niezgodności oraz rekomendacje dotyczące poprawy.
* Rekomendacje: Opracowanie konkretnych rekomendacji dotyczących działań korygujących i zapobiegawczych w celu zapewnienia pełnej zgodności z KRI.
* Podsumowanie: Przygotowanie podsumowania wyników audytu dla kierownictwa, zawierającego kluczowe wnioski i zalecenia.

5. Prezentacja i Omówienie Wyników

a. Prezentacja Raportu

* Spotkanie z Kierownictwem: Przedstawienie raportu z audytu kierownictwu organizacji, omówienie kluczowych wyników, niezgodności i rekomendacji.
* Dyskusja i Pytania: Umożliwienie kierownictwu i interesariuszom zadawania pytań, dyskusja nad wynikami audytu i proponowanymi działaniami korygującymi.

b. Plan Działań Korygujących

* Opracowanie Planu Działań: Wspólne opracowanie planu działań korygujących, ustalenie priorytetów, terminów realizacji i odpowiedzialności.
* Monitorowanie Realizacji: Ustalenie mechanizmów monitorowania realizacji działań korygujących i okresowych przeglądów zgodności.

6. Follow-up i Monitorowanie

a. Wdrożenie Działań Korygujących

* Realizacja Rekomendacji: Wdrożenie zaleceń zawartych w raporcie audytu, zmiany w politykach, procedurach, konfiguracjach systemów.
* Weryfikacja Zgodności: Przeprowadzenie dodatkowych testów i inspekcji w celu weryfikacji skuteczności wdrożonych działań korygujących.

b. Ciągłe Monitorowanie

* Regularne Przeglądy: Organizowanie regularnych przeglądów zgodności z KRI, monitorowanie przestrzegania wprowadzonych zmian i procedur.
* Aktualizacja Polityk: Aktualizacja polityk i procedur w odpowiedzi na zmiany w wymaganiach KRI oraz nowe zagrożenia i technologie.

Produkt Audytu

Produktem audytu będzie szczegółowy raport zawierający:

* Opis przeprowadzonych działań audytowych.
* Wyniki przeglądów dokumentacji i inspekcji technicznych.
* Zidentyfikowane niezgodności i luki bezpieczeństwa.
* Rekomendacje dotyczące działań korygujących i zapobiegawczych.
* Podsumowanie kluczowych wniosków i zaleceń dla kierownictwa organizacji.

# Przygotowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

Dokumentacja SZBI nie może być wygenerowana przez sztuczną inteligencję. Wykonawca jest zobowiązany przekazać Zamawiającemu oświadczenie potwierdzające, że wytworzył dokumentację i posiada do niej prawa autorskie i majątkowe.

Wykonawca zobowiązany jest opracować dokumentację Systemu Zarządzania Bezpieczeństwem Informacji (dalej SZBI) dla:

|  |  |
| --- | --- |
| Nazwa jednostki | Liczba |
| Urząd Gminy w Tarnowie Opolskim | 1 |
| Gminny Ośrodek Pomocy Społecznej | 1 |
| Biuro Obsługi Oświaty Samorządowej | 1 |
| Publiczna Szkoła Podstawowa w Kątach Opolskich | 1 |
| Publiczna Szkoła Podstawowa w Nakle | 1 |
| Publiczna Szkoła Podstawowa im. Mikołaja Kopernika w Tarnowie Opolskim | 1 |
| Przedszkole Publiczne w Kosorowicach | 1 |
| Przedszkole Publiczne w Przyworach | 1 |
| Przedszkole Publiczne z Oddziałami Integracyjnymi im. bł. Edmunda Bojanowskiego w Tarnowie Opolskim | 1 |

## Inwentaryzacja zasobów informacyjnych

Należy pozyskać informacje na temat:

* Krytycznych systemów teleinformatycznych służących do przetwarzania informacji – należy przez to rozumieć, że Wykonawca wraz z Zamawiającym winien pośród wszystkich systemów teleinformatycznych zidentyfikować systemy krytyczne, które są kluczowe dla prawidłowego funkcjonowania działalności realizowanej przez Zamawiającego. Systemy krytyczne to takie systemy, które w przypadku niedostępności w istotny sposób uniemożliwiają całkowicie i/lub obniżają zdolność Zamawiającego do prowadzenie przez niego podstawowej działalności i/lub informacje przetwarzane w tych systemach stanowią dla Zamawiającego istotną wartość albo generują wysokie ryzyko w przypadku naruszenia przetwarzanych w nich danych. Zamawiający informuje, że samodzielnie zidentyfikował 5 takich systemów, ale podczas prowadzenia prac z Wykonawcą ww. systemów może zostać zidentyfikowanych więcej.
* Krytycznych procesów przetwarzania informacji – należy przez to rozumieć zidentyfikowanie i opisanie procesów przetwarzania informacji, które są kluczowe dla prawidłowego funkcjonowania działalności realizowanej przez Zamawiającego. Przez proces należy rozumieć zestaw połączonych ze sobą sekwencyjnie czynności, wykonywanych przez osoby przypisane do ról, w określonym czasie oraz przy pomocy określonych systemów teleinformatycznych w tym krytycznych systemów teleinformatycznych. Procesy krytyczne to takie, które w przypadku zakłócenia w istotny sposób ograniczają lub uniemożliwiają prowadzenie działalności podstawowej Zamawiającego i/lub takie, w których informacje przetwarzane w ramach tych procesów stanowią dla Zamawiającego istotną wartość albo generują wysokie ryzyko w przypadku naruszenia przetwarzanych w nich danych. Zamawiający informuje, że w jego ocenie minimalna liczba procesów to 10, ale podczas prowadzenia prac z Wykonawcą ww. systemów może zostać zidentyfikowanych więcej.
* Kluczowych osób dla realizacji procesów przetwarzania informacji – należy przez to rozumieć identyfikację osób, których nieobecność albo niedostępność zakłóci w istotny sposób albo uniemożliwi całkowicie i/lub znacząco obniży zdolność Zamawiającego do prowadzenie przez niego podstawowej działalności.

## Szacowanie ryzyka

Należy przeprowadzić Szacowanie ryzyka, które umożliwi identyfikację ryzyka w obszarze:

* technicznym (systemy, narzędzia i zasoby umożliwiające przetwarzanie informacji),
* organizacyjnym (procesy przetwarzania informacji oraz zapewnienia ciągłości działania),
* zasobów ludzkich (osoby przetwarzające informacje),

Kluczowym dla Zamawiającego jest by precyzyjnie określić sposób minimalizacji ryzyka środkami, który dysponuje przy założeniu, że wynik minimalizacji będzie dla Zamawiającego akceptowalny. W przypadku braku właściwych środków dla celów minimalizacji Wykonawca zaproponuje środki zastępcze, które mogą od Zamawiającego wymagać inwestycji.

Szacowanie ryzyka należy przeprowadzić w oparciu o kryteria ogólne (generyczne) np.: ryzyko pożaru, zalania, przegrzania, dostępności, umowy wsparcia i serwisu (SLA) ale przede wszystkim winno być prowadzone w oparciu o kryteria rzeczowe, charakterystyczne dla wybranego systemu teleinformatycznego, procesu, osoby. Należy przez to rozumieć, że w zależności od przedmiotu analizy należy np.: analizować dostępność wybranych komponentów teleinformatycznych, teletechnicznych na rynku polskim, potencjał dostawcy/wykonawcy do utrzymania systemu, zdolność do dostosowania się do zmieniającego otoczenia, dostępność kompetencji osób kluczowych na rynku pracy, konkurencję pośrednią i bezpośrednią itp.

## Przeprowadzenie audytu w celu przygotowania dokumentacji

Audyt bezpieczeństwa informacji na zgodność z normą ISO 2700X winien odnosić się do weryfikacji pełnego zakresu normy. Jest on wymagany dla potrzeb właściwego przygotowania dokumentacji SZBI. Należy przez to rozumieć, że audytowi winne zostać poddane wszystkie krytyczne systemy teleinformatyczne, krytyczne procesy oraz kluczowe osoby na zgodność z normą.

Z uwagi na fakt, że ww. norma nie zawiera listy kontrolnej (elementów wymagających do sprawdzenia potocznie kontrolek) wymaganych dla weryfikacji. Wykonawca do oferty musi dołączyć zestaw zagadnień, które będzie wykorzystywał podczas prowadzonych czynności audytowych. Przez zestaw zagadnień należy rozumieć stwierdzenie i/lub pytanie, które umożliwia sprawdzenie bezpieczeństwa w wybranym obszarze.

Audyt bezpieczeństwa winien posłużyć Wykonawcy do przygotowanie dokumentacji SZBI, którą Wykonawca będzie wdrażał we współpracy z Zamawiającym w kolejnych etapach projektu.

Audyt bezpieczeństwa winien być prowadzony przez Wykonawcę we współpracy z osobami piastującymi kluczowe stanowiska w strukturach organizacji Zamawiającego. Należy przez to rozumieć, że Wykonawca zobowiązany jest spotkać się z osobą kluczową wskazaną przez Zamawiającego i przeprowadzić wraz z nią analizę ryzyka dotyczącą procesów krytycznych oraz krytycznych systemów teleinformatycznych, w których wybrana osoba przetwarza informacje. Zamawiający informuje, że liczba osób kluczowych wynosi 15, ale może wzrosnąć. Przez osoby kluczowe należy rozumieć takie osoby, które w strukturach Zamawiającego pełnią funkcje kierownicze i/lub piastują stanowiska samodzielne i/lub wykonują czynności kluczowe dla realizacji zadań Zamawiającego.

# Przeprowadzenie audytu bezpieczeństwa technicznego

Testy bezpieczeństwa mają zostać przeprowadzone wyłącznie w Urzędzie Gminy.

Celem Zamawiającego jest sprawdzenie, czy wytworzone oraz dostarczone przez wykonawców, podwykonawców i dostawców elementy infrastruktury oraz aplikacje są bezpieczne do użytkowania.

W ramach zamówienia należy przeprowadzić audyt bezpieczeństwa technicznego, którego celem jest między innymi wykrycie:

* luk i podatności związanych z zastosowaną architekturą aplikacji,
* luk i podatności wynikających z zastosowanych wzorców projektowych,
* luk i podatności związanych z zastosowanymi technologiami na poziomie warstwy prezentacji danych,
* luk i podatności związanych z zastosowanymi technologiami na poziomie warstwy aplikacji,
* luk i podatności związanych z zastosowanymi serwerami WWW lub ich niewłaściwej konfiguracji,
* luk i podatności związanych z zastosowanym środowiskiem aplikacyjnym lub jego niewłaściwą konfiguracją,
* luk i podatności związanych z niewłaściwą walidacją danych wejściowych,
* luk i podatności związanych z zaimplementowanymi mechanizmami uwierzytelniania i autoryzacji.

Zamawiający informuje, że pod pojęciem testów bezpieczeństwa technicznego należy rozumieć przeprowadzenie ręcznych czynności przez audytorów bezpieczeństwa wchodzących w skład zespołu Wykonawcy, co oznacza, że wyklucza się wykorzystanie narzędzi np. typu Nessus, Greenbone (Open VAS), Acunetix i podobnych do prowadzenia audytu. Zamawiający wyklucza możliwość wskazania badania na występowanie znanych podatności jako potwierdzenie wykonania audytu technicznego. Jednocześnie Zamawiający wskazuje, że przedmiot zamówienia obejmuje również skanowanie i identyfikację znanych podatności, do których Wykonawca może użyć wyżej wymienionych narzędzi.

Wykonywane przez Wykonawcę testy mają być uzgodnione z Zamawiającym przez co należy rozumieć uzgodnienie daty i czasu wykonania oraz wpływu testu na infrastrukturę Zamawiającego. O ile wykonanie testu może wpłynąć negatywnie na dostępność testowanego elementu Wykonawca musi o tym poinformować Zamawiającego. Wykonawca zobowiązany jest bezpośrednio kontaktować się z dostawcami systemów teleinformatycznych, które testuje i później w których wykrył podatności albo zidentyfikował ryzyka celem wskazania sposobu postępowania.

Wykonawca zobowiązany jest do wykonania retestów celem weryfikacji poprawnego postąpienia z odnalezionymi podatnościami.

Testy muszą zostać wykonane zgodnie z Penetration Testing Execution Standard.

## Zakres prac objętych audytem bezpieczeństwa technicznego

1. Ocena zagrożeń, wynikających ze zidentyfikowanych podatności oraz opisanie sposobu minimalizacji zidentyfikowanych zagrożeń w celu podjęcia przez Zamawiającego czynności mających na celu zwiększenie odporności na wszelkie, znane na dzień audytu, formy zagrożeń.
2. Oceny wpływu podatności muszą zostać ocenione w skali CVSS wersji 4.0.
3. Analiza i wykazanie potencjalnego nieautoryzowanego dostępu do danych i zasobów w obrębie badanego systemu.
4. Na podstawie wyników przeprowadzonego audytu przygotować zalecenia w zakresie tzw. hardeningu aplikacji, systemów operacyjnych, usług serwerowych oraz infrastruktury sprzętowej (serwerów, przełączników, routerów oraz innych urządzeń aktywnych) w postaci gotowych do implementacji zaleceń, które może wykonać Zamawiający, wykonawca kluczowych komponentów platformy, wyłoniony w ramach postępowań, o których mowa wyżej, lub inna firma trzecia, posiadająca wiedzę i doświadczenie w zakresie wybranych technologii.
5. Przygotować inwentaryzację komponentów, na które składa się środowisko Zamawiającego.
6. Przygotować ocenę ryzyka wykorzystania, utrzymania, rozwoju każdego ze zidentyfikowanych w toku wykonywanych testów komponentów. Przygotować analizę ryzyk dotyczącą wyników i wniosków przeprowadzanych testów penetracyjnych i bezpieczeństwa, oraz dodatkowo:
7. występowania pojedynczych punktów awarii krytycznych, skutkującej całkowitym brakiem możliwości korzystania przez użytkowników;
8. występowania pojedynczych punktów usterek, skutkujących czasowym lub ograniczonym funkcjonowaniem konkretnych komponentów;
9. wpływu na systemy Zamawiającego ataków typu DoS;
10. Wykonawca ma podjąć próbę przełamania lub ominięcia zabezpieczeń WAF (z ang. Web Application Firewall), urządzeń UTM (z ang. Unified Threat Management), VPN.
11. O ile Wykonawca z powodzeniem przełamie zabezpieczenia i uzyska dostęp do sieci wewnętrznej Zamawiającego winien podjąć próbę przełamania zabezpieczeń sieci wewnętrznej w zakresie opisanym poniżej.
12. Wykonawca ma przeprowadzić testy bezpieczeństwa wewnątrz sieci Zamawiającego w tym:
13. Wykonać rekonesans celem identyfikacji słabych punktów,
14. Podjąć próbę podsłuchiwania ruchu sieciowego
15. Wykonawca zobowiązany jest do przeprowadzenia analizy stacji roboczych pod kątem wykazania błędów konfiguracyjnych oraz opisania sposobu ich naprawy.

## Raport

Na potwierdzenie wykonania powyższego zakresu prac Wykonawca sporządzi raport zawierający minimum:

1. Pełny spis i opis przeprowadzonych prac,
2. Szczegółowy wykaz wykrytych podatności, wraz z pełnymi dowodami ich występowania,
3. Każda znana podatność zostanie oznaczona odpowiednim kodem ze słownika CVE (Common Vulnerabilities and Exposures),
4. Opisowe rekomendacje w zakresie sposobu postępowania z wykrytymi podatnościami wraz z podaniem zaleceń i instrukcji do wprowadzenia zmian konfiguracyjnych lub czynności naprawczych w celu właściwego postępowania z ryzykiem,

## Sposób przygotowania dokumentacji SZBI

SZBI ma określać wewnętrzne wymagania dotyczące bezpieczeństwa informacji i zapewni praktyczne rozwiązania w tym zakresie poprzez odpowiednio ustanowione metody, czynności oraz narzędzia. Przez praktyczne rozwiązania Zamawiający rozumie opisanie w ramach dokumentacji SZBI sposobów zapewnienia bezpieczeństwa informacji, które będą minimalizowały ryzyka wystąpienia zdarzeń (incydentów) związanych z bezpieczeństwem informacji, w tym dotyczących naruszenia ochrony danych osobowych. Zamawiający wymaga od Wykonawcy określenia propozycji działań w ramach postępowania ze zidentyfikowanymi ryzykami, w tym dotyczących wdrożenia określonych środków organizacyjnych i technicznych:

* prewencyjnie (poprzez ograniczenie możliwości popełnienia błędu przez człowieka oraz naprawę błędów, które wystąpiły),
* odstraszająco (poprzez zastosowanie środków, które w sposób zrozumiały określą konsekwencje wynikające z niewłaściwego postępowania z informacją),
* reaktywnie (które umożliwią Zamawiającemu prowadzenie analiz po naruszeniach informacji oraz będą stanowiły źródło informacji analitycznych),

Zamawiający wymaga, aby zapisy SZBI były zgodne i kompletne, tj. odnosiły się wprost, do wymagań określonych w normach:

* PN-EN ISO/IEC 27001:2023-08 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności -- Systemy zarządzania bezpieczeństwem informacji -- Wymagania,
* PN-EN ISO/IEC 27002:2023-01 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Zabezpieczanie informacji.
* Dalej obszar opisany w obu normach zwany jest ISO 2700X.

Zamawiający wymaga, żeby zapisy dokumentacji SZBI odnosiły się do wszystkich, i w każdym przypadku do konkretnych, rozdziałów i punktów ww. norm, z literalnym zachowaniem numeracji i nazewnictwa.

Ponadto Zamawiający wymaga, aby dokumentacja SZBI zawierała zapisy dotyczące środków organizacyjnych i technicznych zgodne z rekomendacjami Narodowych Standardów Cyberbezpieczeństwa (NSC), których treść dostępna jest pod adresem https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber. Zgodność w tym zakresie ma być osiągnięta poprzez zawarcie w dokumentacji SZBI wymagań NSC w sposób, który umożliwi Zamawiającemu jednoznaczną identyfikację i odniesienie w zapisach SZBI określonych w NSC wymagań dotyczących zabezpieczeń sieci i systemów informatycznych. Wykonawca wraz z Zamawiający uzgodnią przed realizacją zakres NSC, który należy uwzględnić w zadaniach Wykonawcy.

Dokumentacja SZBI musi zostać przygotowana w sposób umożliwiający Zamawiającemu w przyszłości zgłoszenie gotowości do certyfikacji SZBI przez zewnętrzną, akredytowaną przez Polskie Centrum Akredytacji, jednostkę certyfikującą.

Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji stanowi podstawę dla formalnego rozliczenia się z ochrony informacji. Wykonawca opracuje SZBI bazując na zakresie opisanym w normach ISO 2700X.

Zakres przedmiotowy dokumentacji SZBI musi bezpośrednio pokrywać się z tytułami punktów i podpunktów normy, aby nie było konieczności poszukiwania w dokumentacji zakresu, którego dotyczy wybrana jej część.

## Przygotowanie rejestru ryzyka zgodnie z SZBI

Należy wykonać rejestr ryzyka zgodnie z poniższym wzorem dla każdej jednostki, dla której wykonano SZBI..

Przykład rejestru ryzyka, który docelowo zostanie uzgodniony z Zamawiającym.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Wskaźnik statusu ryzyka** | **ID Ryzyka** | **Data identyfikacji ryzyka** | **Narażony zasób** | **Kategoria ryzyka** | **Opis ryzyka** | **Wpływa na** | | | **Wstępna ocena ryzyka** | | | | | **Ocena ryzyka** | **Status ryzyka** | **Właściciel ryzyka** | **Sposób postępowania z ryzykiem** | **Opis minimalizacji ryzyka** | **Szacowany koszt minimalizacji ryzyka w PLN brutto** | **Koszt minimalizacji ryzyka - dodatkowe informacja** | **Czy sposób minimalizacji wpływa na prywatność pracowników?** | **Czy wpływa na prywatność klientów albo wprowadza ograniczenia?** | **Wpływa na** | | | **Ocena ryzyka szczątkowego** | | | | | **Ocena ryzyka** | **Status ryzyka** | **Ryzyko po minimalizacji** | **Data kolejnego przeglądu** |
| **Finanse** | **Wizerunek** | **Zgodność z prawem** | **Poufność** | **Integralność** | **Dostępność** | **Prawdopodobieństwo** | **Wpływ** | **Finanse** | **Wizerunek** | **Zgodność z prawem** | **Poufność** | **Integralność** | **Dostępność** | **Prawdopodobieństwo** | **Wpływ** |
| **y** | **autonumer** | **19.10.2021** | **Dane biznesowe** | **Organizacyjne** | **Opis ryzyka** | **T** | **N** | **N** | **T** | **T** | **T** | **1 -5** | **1-5** | **1 - 25** | **Wysokie** | **Imię Nazwisko** | **Minimalizować** | **Opis minimalizacji ryzyka** | **Czas naszych pracowników** |  | **T** | **N** | **N** | **N** | **N** | **N** | **N** | **N** | **4** | **4** | **16** | **Średnie** | **Poważne** | **17.04.2022** |

# Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji

Wdrożenie SZBI musi zostać zrealizowane z uwzględnieniem poniżej opisanych czynności, zadań oraz kryteriów. Kluczowe dla wdrożenia SZBI jest dostosowanie go, do wymagań oraz możliwości jednostki, dla której jest opracowywany. Wdrożeniem są objęte wszystkie jednostki, dla których przygotowano SZBI.

## Zakres i sposób wdrożenia

1. Przygotowanie i Planowanie

Zadania:

* Zrozumienie Wymagań: Przeprowadzenie analizy wymagań norm PN-EN ISO/IEC 27001:2023-08 i PN-EN ISO/IEC 27002:2023-01.
* Polityka Bezpieczeństwa: Opracowanie i zatwierdzenie polityki bezpieczeństwa informacji, która będzie stanowić fundament SZBI.
* Zaangażowanie Kierownictwa: Upewnienie się, że najwyższe kierownictwo jest zaangażowane i wspiera wdrożenie SZBI.

Kryteria jakościowe:

* Polityka bezpieczeństwa informacji jest formalnie zatwierdzona przez kierownictwo.
* Dokumentacja zakresu SZBI jest zgodna z celami organizacji i wymaganiami norm.
* Wszyscy pracownicy są przeszkoleni w siedzibie Zamawiającego przez Wykonawcę.
* Wszyscy pracownicy zdali test wiedzy w zakresie właściwym dla Zadań, który potwierdza umiejętność stosowania SZBI.

2. Ocena Ryzyka

Zadania:

* Identyfikacja Zagrożeń i Wartości: Przeprowadzenie analizy zagrożeń i identyfikacja wartości informacyjnych.
* Analiza Ryzyka: Określenie prawdopodobieństwa wystąpienia zagrożeń oraz potencjalnych skutków zgodnie z opisem zamieszczonym poniżej.
* Ocena Ryzyka: Zdefiniowanie poziomu ryzyka dla poszczególnych zagrożeń.
* Plany Postępowania z Ryzykiem: Opracowanie i wdrożenie planów redukcji ryzyka, akceptacji, przeniesienia lub unikania ryzyka.

Kryteria jakościowe:

* Analiza i ocena ryzyka.
* Plany postępowania z ryzykiem są zgodne z polityką bezpieczeństwa i zatwierdzone przez kierownictwo.
* Wszyscy pracownicy są przeszkoleni w siedzibie Zamawiającego przez Wykonawcę.
* Wszyscy pracownicy zdali test wiedzy w zakresie właściwym dla Zadań, który potwierdza umiejętność stosowania SZBI.

3. Kontrole Bezpieczeństwa

Zadania:

* Dobór Kontroli: Na podstawie wyników oceny ryzyka wybór odpowiednich kontroli bezpieczeństwa zgodnie z ISO 27002:2023.
* Wdrożenie Kontroli: Implementacja wszystkich wymaganych kontroli technicznych, organizacyjnych i proceduralnych.
* Dokumentacja Kontroli: Utworzenie i utrzymanie dokumentacji wszystkich wdrożonych kontroli.

Kryteria jakościowe:

* Kontrole bezpieczeństwa są skutecznie wdrożone i działają zgodnie z założeniami.
* Dokumentacja jest kompletna i odzwierciedla aktualny stan wdrożonych kontroli.
* Wszyscy pracownicy są przeszkoleni w siedzibie Zamawiającego przez Wykonawcę.
* Wszyscy pracownicy zdali test wiedzy w zakresie właściwym dla Zadań, który potwierdza umiejętność stosowania SZBI.

4. Monitorowanie i Przegląd

Zadania:

* Monitorowanie Efektywności: Ciągłe monitorowanie efektywności wdrożonych kontroli bezpieczeństwa.
* Przeglądy Wewnętrzne: Regularne przeprowadzanie audytów wewnętrznych SZBI.
* Przeglądy Zarządzania: Okresowe przeglądy SZBI przez najwyższe kierownictwo.

Kryteria jakościowe:

* Raporty z monitorowania i przeglądów są regularnie generowane i analizowane.
* Audyty wewnętrzne są przeprowadzane zgodnie z harmonogramem i normami.
* Wszyscy pracownicy są przeszkoleni w siedzibie Zamawiającego przez Wykonawcę.
* Wszyscy pracownicy zdali test wiedzy w zakresie właściwym dla Zadań, który potwierdza umiejętność stosowania SZBI.

5. Doskonalenie

Zadania:

* Zarządzanie Incydentami: Wdrożenie procedur zarządzania incydentami bezpieczeństwa informacji.
* Działania Korygujące: Identyfikowanie i wdrażanie działań korygujących oraz zapobiegawczych.
* Ciągłe Doskonalenie: Regularne przeglądy i aktualizacje polityki, procedur oraz kontrol SZBI.

Kryteria jakościowe:

* Wszystkie incydenty są rejestrowane, analizowane i odpowiednio zarządzane.
* Działania korygujące i zapobiegawcze są dokumentowane i śledzone pod kątem efektywności.
* Regularne aktualizacje SZBI w odpowiedzi na zmieniające się zagrożenia i wymagania.
* Wszyscy pracownicy są przeszkoleni w siedzibie Zamawiającego przez Wykonawcę.
* Wszyscy pracownicy zdali test wiedzy w zakresie właściwym dla Zadań, który potwierdza umiejętność stosowania SZBI.

## Przeszkolenie użytkowników z zakresu SZBI

Wykonawca musi przeszkolić użytkowników w zakresie gwarantującym nabycie umiejętności umożliwiających utrzymanie SZBI w kolejnych latach co oznacza, że Wykonawca winien przeprowadzić szkolenia we właściwym zakresie. Termin szkolenia musi zostać uzgodniony pomiędzy wykonawcą a jednostką, która będzie szkolona. Przeszkoleni muszą zostać wszyscy pracownicy jednostki. Wdrożeniem są objęte wszystkie jednostki, dla których przygotowano SZBI.

Wykonawca musi przygotować szkolenia dedykowane dla dwóch grup użytkowników:

Liderów – którzy będą odpowiedzialni za skuteczne doskonalenie oraz utrzymanie SZBI

Pozostałych użytkowników SZBI – którzy będą odpowiedzialni za skuteczne stosowania SZBI

**Agenda Szkolenia z Zakresu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)**

Dla Liderów SZBI

1. Wprowadzenie do SZBI

Wprowadzenie do ISO 27001 i ISO 27002

Znaczenie SZBI dla organizacji

1. Rola Liderów w Utrzymaniu SZBI

Obowiązki i odpowiedzialności liderów SZBI

Kształtowanie kultury bezpieczeństwa informacji

1. Zarządzanie Ryzykiem

Identyfikacja i ocena ryzyka

Implementacja planów zarządzania ryzykiem

Przykłady skutecznego zarządzania ryzykiem

1. Polityki i Procedury Bezpieczeństwa Informacji

Tworzenie i aktualizacja polityk bezpieczeństwa

Procedury operacyjne i techniczne

Zarządzanie dokumentacją SZBI

1. Kontrole Bezpieczeństwa

Wybór i implementacja odpowiednich kontroli bezpieczeństwa

Monitorowanie i przegląd efektywności kontroli

Studium przypadku z wdrożenia kontroli bezpieczeństwa

1. Audyt i Przeglądy SZBI

Przygotowanie do audytów wewnętrznych i zewnętrznych

Proces audytu i dokumentacja

Analiza wyników audytu i wdrażanie działań korygujących

1. Zarządzanie Incydentami Bezpieczeństwa

Identyfikacja i klasyfikacja incydentów

Procedury reagowania na incydenty

Dokumentacja i analiza incydentów

1. Ciągłe Doskonalenie SZBI

Procesy ciągłego doskonalenia

Rola liderów w inicjowaniu zmian

Narzędzia i techniki doskonalenia SZBI

1. Szkolenia i Podnoszenie Świadomości

Programy szkoleniowe dla pracowników

Metody podnoszenia świadomości bezpieczeństwa

Testowanie i ocena skuteczności szkoleń

1. Zarządzanie Zgodnością

Przegląd kluczowych regulacji dotyczących bezpieczeństwa informacji

Utrzymywanie zgodności z przepisami i normami

Dokumentowanie zgodności

Agenda Szkolenia z Zakresu SZBI

Dla Pozostałych Pracowników

1. Wprowadzenie do SZBI

Podstawy bezpieczeństwa informacji

Znaczenie SZBI dla organizacji

1. Podstawowe Polityki i Procedury Bezpieczeństwa Informacji

Kluczowe polityki bezpieczeństwa

Zasady i procedury, których należy przestrzegać

1. Rozpoznawanie i Reagowanie na Zagrożenia

Najczęstsze zagrożenia bezpieczeństwa informacji

Jak rozpoznawać i zgłaszać podejrzane działania

1. Bezpieczne Praktyki Pracy z Danymi

Bezpieczne korzystanie z systemów informatycznych

Ochrona danych osobowych i wrażliwych

Praktyki bezpiecznego zarządzania hasłami

1. Zarządzanie Dostępem i Autoryzacją

Zasady zarządzania dostępem do informacji

Procedury uzyskiwania i zmiany uprawnień

1. Reagowanie na Incydenty Bezpieczeństwa

Co robić w przypadku wykrycia incydentu bezpieczeństwa

Procedury zgłaszania incydentów

1. Ochrona Przed Złośliwym Oprogramowaniem

Rozpoznawanie i unikanie złośliwego oprogramowania

Zasady korzystania z programów antywirusowych

1. Bezpieczne Korzystanie z Internetu i Poczty E-mail

Zasady bezpiecznego korzystania z Internetu

Jak unikać phishingu i innych oszustw online

1. Znaczenie Szkolenia i Podnoszenia Świadomości

Rola każdego pracownika w utrzymaniu bezpieczeństwa informacji

Dostępne programy szkoleniowe i zasoby edukacyjne

1. Podsumowanie i Q&A

Kluczowe wnioski ze szkolenia

Sesja pytań i odpowiedzi

# Przeprowadzenie testów socjotechnicznych

Testy socjotechniczne muszą być realizowane na przestrzeni co najmniej 70 dni roboczych aby pomiędzy jednym a kolejnym testem użytkownicy nie orientowali się, że test jest częścią kampanii phishingowej. Częstotliwość prowadzenia testów musi być uzgodniona z Zamawiającym.

Testy socjotechniczne mają zostać przeprowadzone dla następujących jednostek:

|  |  |
| --- | --- |
| Nazwa jednostki | Liczba |
| Urząd Gminy w Tarnowie Opolskim | 1 |
| Gminny Ośrodek Pomocy Społecznej | 1 |
| Biuro Obsługi Oświaty Samorządowej | 1 |
| Publiczna Szkoła Podstawowa w Kątach Opolskich | 1 |
| Publiczna Szkoła Podstawowa w Nakle | 1 |
| Publiczna Szkoła Podstawowa im. Mikołaja Kopernika w Tarnowie Opolskim | 1 |
| Przedszkole Publiczne w Kosorowicach | 1 |
| Przedszkole Publiczne w Przyworach | 1 |
| Przedszkole Publiczne z Oddziałami Integracyjnymi im. bł. Edmunda Bojanowskiego w Tarnowie Opolskim | 1 |

## Warunki wstępne i sposób realizacji

W celu przeprowadzenia testów muszą zostać spełnione następujące warunki:

**Sposób realizacji testów**

Testy będą prowadzone w oparciu o konkretne scenariusze. Każdy scenariusz będzie oznaczony jako osobna część, która będzie podlegała oddzielnej weryfikacji względem wyników. Planowane jest dzielenie poszczególnych testów na części oraz grupy docelowe, możliwa będzie zmiana charakterystyki testów w trakcie ich trwania w celu weryfikacji skuteczności. Zmiana będzie możliwa w przypadku, gdy nie wpłynie w sposób znaczący na modyfikację scenariusza i nie wymusi przebudowy środowiska testowego.

**Środowisko testowe**

W celu przeprowadzenia testów Wykonawca przygotuje dedykowane dla celów testów środowisko testów, w którym składowane będą w sposób bezpieczny wszystkie dane pochodzące z testów. W ww. środowisku musza zostać udostępnione narzędzia umożliwiające przeprowadzenie testów stanowiących przedmiot projektu. Środowisko testowe będzie zbudowane w oparciu o sprzęt i oprogramowanie należące do Wykonawcy.

**Zaangażowanie Wykonawcy**

Wykonawca musi zapewnić wszystkie komponenty wymagane do przeprowadzenia testów bez ponoszenia przez Zamawiającego dodatkowych kosztów. Ze strony Wykonawcy musi zostać dedykowany zespół co najmniej dwóch osób, które będą odpowiedzialne za przeprowadzenie testów. Tylko wybrane osoby będą komunikowały się z Klientem w celu wymiany informacji pochodzących z testów. Środowisko testów zostanie zabezpieczone w celu ochrony przed nieautoryzowanym dostępem.

**Zaangażowanie Zamawiającego**

Ze strony Zamawiającego zostaną dedykowane osoby, które będą kompetentne i władne weryfikować przedmiot i wynik poszczególnych faz testów w trakcie ich trwania. Osoby wchodzące w skład zespołu powinny mieć możliwość swobodnego podejmowania decyzji w zakresie realizacji testów.

## Szczegółowy opis testów

W celu przeprowadzenia testów dobór grup oraz zasięg będzie prowadzony wraz z Zamawiającym.

### Stworzenie fałszywych stron

Zadaniem Wykonawcy jest opracowanie trzech fałszywych stron dostępnych pod trzema różnymi domenami, które będą przypominały strony zarządzane przez Urząd. Sposób działania strony Wykonawca przedstawi do akceptacji Zamawiającemu i po akceptacji podłączy strony pod domeny również uzgodnione z Zamawiającym.

**Przygotowanie Fałszywych Stron**

Wykonawca przygotuje zestaw fałszywych stron internetowych, które będą naśladować wygląd i funkcjonalność autentycznych stron Zamawiającego. Strony te będą analizowane pod kątem ich skuteczności w oszukiwaniu użytkowników oraz zdolności do zbierania poufnych informacji.

**Rejestracja Domen (Typosquatting)**

Wykonawca przeprowadzi analizę możliwości rejestracji domen, które mogą być wykorzystane do typosquattingu. Zostaną zarejestrowane przykładowe domeny, które różnią się od prawdziwych domen Zamawiającego minimalnymi zmianami w pisowni.

**Identyfikacja Zagrożeń**

Wykonawca przeprowadzi szczegółową analizę przygotowanych fałszywych stron oraz zarejestrowanych domen, aby zidentyfikować potencjalne zagrożenia i podatności. Analiza obejmie ocenę skuteczności tych stron w oszukiwaniu użytkowników oraz potencjalne skutki wyłudzenia danych.

**Raport z Testów**

Wyniki testów zostaną przedstawione w szczegółowym raporcie, który obejmie:

* Opis przeprowadzonych działań i zastosowanej metodyki.
* Listę zidentyfikowanych fałszywych stron i domen.
* Liczbę oraz opis użytkowników, którzy wzięli udział w testach wraz z przypisanym im wynikom.

**Rekomendacje**

Na podstawie przeprowadzonych testów, Wykonawca przedstawi Zamawiającemu rekomendacje dotyczące:

* Wzmocnienia mechanizmów wykrywania i blokowania fałszywych stron.
* Poprawy procedur weryfikacji domen.
* Szkolenia pracowników w zakresie rozpoznawania phishingu.
* Implementacji dodatkowych środków bezpieczeństwa.

### Wysłanie wiadomości pocztą elektroniczną

Celem testów jest sprawdzenie efektywności działania funkcji serwera poczty w zakresie wykrywania i ochrony przed phishingiem. Zamawiający oczekuje, że w tym celu Wykonawca wyśle co najmniej trzy spreparowane wiadomości, które winny być zablokowane przez serwer, bo stanowią phishing.

W celu przeprowadzenia testów phishingu Zamawiający dokona, poprzez dodanie adresu IP serwera Wykonawcy, modyfikacji ustawień poczty w sposób zezwalający Wykonawcy na dostarczenie spreparowanych wiadomości.

**Przygotowanie Fałszywych Wiadomości Email**

Wykonawca przygotuje zestaw fałszywych wiadomości email, które będą naśladować wygląd i treść autentycznych wiadomości pochodzących od Zamawiającego. Wiadomości te mogą zawierać:

* Linki do fałszywych stron internetowych.
* Złośliwe załączniki.
* Prośby o ujawnienie poufnych informacji.

**Scenariusze Ataków**

Wykonawca przeprowadzi symulowane ataki phishingowe według różnych scenariuszy, które mogą obejmować:

* **Spear Phishing:** Ukierunkowane ataki na konkretne osoby lub grupy pracowników.
* **Whaling:** Ataki skierowane na wysokiego szczebla menedżerów lub decydentów.
* **Clone Phishing:** Tworzenie kopii autentycznych wiadomości email z drobnymi zmianami prowadzącymi do złośliwych zasobów.

**Wysyłka Fałszywych Wiadomości Email**

Wykonawca przeprowadzi kontrolowaną wysyłkę fałszywych wiadomości email do wybranej grupy pracowników Zamawiającego. Celem jest ocena, jak wielu użytkowników zostanie oszukanych przez te wiadomości i jakie działania podejmą.

**Identyfikacja Zagrożeń**

Wykonawca przeprowadzi szczegółową analizę reakcji pracowników na fałszywe wiadomości email, w tym:

* Procent użytkowników, którzy kliknęli w złośliwe linki.
* Procent użytkowników, którzy pobrali złośliwe załączniki.
* Procent użytkowników, którzy ujawnili poufne informacje.

**Raport z Testów**

Wyniki testów zostaną przedstawione w szczegółowym raporcie, który obejmie:

* Opis przeprowadzonych działań i zastosowanej metodologii.
* Analizę skuteczności fałszywych wiadomości email.
* Identyfikację podatności i zagrożeń.
* Rekomendacje dotyczące działań korygujących i środków zapobiegawczych.

**Rekomendacje**

Na podstawie przeprowadzonych testów, Wykonawca przedstawi Zamawiającemu konkretne rekomendacje dotyczące:

* Wzmocnienia mechanizmów wykrywania i blokowania fałszywych wiadomości email.
* Poprawy procedur weryfikacji autentyczności wiadomości email.
* Implementacji dodatkowych środków bezpieczeństwa.

**Podsumowanie**

Realizacja testów zgodnie z powyższym opisem ma umożliwić Zamawiającemu zidentyfikowanie potencjalnych zagrożeń związanych z phishingiem opartym na fałszywych wiadomościach email, a także na wdrożenie skutecznych środków ochrony, zwiększających bezpieczeństwo informacji i danych osobowych.

# Przeprowadzenie testów odporności haseł użytkowników na złamanie

Wykonawca winien przeprowadzić testy odporności haseł użytkowników na przełamanie. Testom będzie podlegać baza hashy Microsoft Active Directory oraz baza hashy dwóch wskazanych przez Zamawiającego systemów dziedzinowych.

Testy należy przeprowadzić dla:

|  |  |
| --- | --- |
| Nazwa jednostki | Liczba audytów |
| Urząd Gminy w Tarnowie Opolskim | 1 |

**Cel Testów**

Celem testów jest ocena bezpieczeństwa haseł w systemie Active Directory oraz dwóch aplikacji dziedzinowych, poprzez próbę łamania hashy, które są używane do przechowywania haseł użytkowników. Testy te mają na celu zidentyfikowanie słabych haseł oraz ocenę skuteczności polityk haseł organizacji. Testy mogą być prowadzone w środowisku chmurowym dostarczonym przez Amazon, Microsoft albo Google zlokalizowanym w Europejskim Obszarze Gospodarczym. Jeżeli Wykonawca chciałby zastosować inne środowisko chmurowe Zamawiający oczekuje, że Wykonawca opisze parametry tego środowiska i możliwość jego wykorzystania uzgodni z Zamawiającym.

Wykonawca powinien dysponować wiedzą i doświadczeniem umożliwiającym wykonanie testów na sprzęcie i oprogramowaniu umożliwiającym wykonanie testów. Wykonawca może sprzęt i oprogramowania wynająć, ale na czas testu musi sprawować nadzór nad cały procesem i bazami danych hashy, a po testach bazy danych trwale usunąć.

**Sprzęt**

1. Serwer Przeznaczony do łamania hashy:
   * Procesor: Wielordzeniowy procesor o wysokiej wydajności, co najmniej 8 rdzeni.
   * Pamięć RAM: Minimum 64 GB RAM, aby zapewnić płynność przetwarzania dużych ilości danych.
   * Karty Graficzne (GPU): 2 wysokowydajne karty graficzne z możliwością równoległego przetwarzania, każda z co najmniej 8 GB pamięci.
   * Dyski SSD: Szybkie dyski SSD o dużej pojemności (minimum 1 TB) dla szybkiego dostępu do danych.
2. Infrastruktura Sieciowa:
   * Połączenia Sieciowe: Wysokoprzepustowe połączenia sieciowe do przesyłania danych między serwerami oraz do zarządzania zdalnego.
   * Bezpieczeństwo Sieci: Zabezpieczone połączenia sieciowe (VPN) i firewalle do ochrony testowanych danych.

**Oprogramowanie**

1. System Operacyjny:
   * Linux: Zalecany system operacyjny dla serwerów łamiących hashe, ze względu na stabilność i wydajność w obliczeniach intensywnych.
   * Sterowniki GPU: Zainstalowane sterowniki graficzne odpowiednie dla używanych kart graficznych, optymalizowane pod kątem obliczeń równoległych.
2. Oprogramowanie do Łamania Hashy:
   * Narzędzia do Pobierania Hashy: Oprogramowanie zdolne do ekstrakcji hashy z Active Directory (np. narzędzia wykorzystujące techniki dumpowania pamięci).
   * Framework do Łamania Hashy: Wysokowydajne frameworki i narzędzia do łamania hashy, wspierające przetwarzanie równoległe na GPU.
   * Algorytmy i Techniki Łamania: Obsługa różnych algorytmów hashujących używanych w Active Directory, takich jak NTLM, oraz technik takich jak brute-force, słownikowe, ataki hybrydowe, rainbow tables.
3. Bazy Danych Haseł:
   * Słowniki Haseł: Duże słowniki haseł zawierające najczęściej używane hasła, w różnych kombinacjach i językach.
   * Rainbow Tables: Precomputed rainbow tables dla NTLM, MD5,SHA-1, SHA-2, SHA-256 przyspieszające proces łamania hashy.
4. Narzędzia Monitorujące i Raportujące:
   * Monitorowanie GPU i CPU: Oprogramowanie do monitorowania wydajności GPU i CPU, w celu optymalizacji i zarządzania zasobami podczas testów.
   * Generowanie Raportów: Narzędzia do dokumentowania wyników testów, generowania raportów o złamanych hashach, analizie słabych haseł oraz rekomendacji.

Proces Przeprowadzania Testów

1. Przygotowanie Środowiska:
   * Instalacja i konfiguracja serwera przeznaczonego do łamania hashy, w tym systemu operacyjnego, sterowników GPU i niezbędnego oprogramowania.
   * Zapewnienie bezpieczeństwa środowiska testowego poprzez zabezpieczenie połączeń sieciowych i kontrolę dostępu.
2. Ekstrakcja Hashy:
   * Wykorzystanie narzędzi do ekstrakcji hashy z Active Directory, zapewniając zgodność z politykami bezpieczeństwa organizacji.
3. Łamanie Hashy:
   * Uruchomienie oprogramowania do łamania hashy z użyciem technik brute-force, słownikowych, hybrydowych oraz rainbow tables.
   * Monitorowanie wydajności i optymalizacja procesów łamania w trakcie testów.
   * Czas trwania procesu łamania hashy: 48 godzin dla każdej bazy danych.
4. Analiza Wyników:
   * Dokumentacja złamanych hashy i analiza najczęściej używanych słabych haseł.
   * Ocena skuteczności polityk haseł i identyfikacja potencjalnych zagrożeń.
5. Generowanie Raportów:
   * Przygotowanie szczegółowego raportu zawierającego wyniki testów, wnioski oraz rekomendacje dotyczące poprawy polityk haseł i ogólnego bezpieczeństwa systemu.
6. Działania Korygujące:
   * Przekazanie raportu oraz omówienie wyników.
   * Wdrożenie rekomendacji mających na celu wzmocnienie polityk haseł i zabezpieczeń.

# Przeprowadzenie szkoleń

Wszystkie szkolenia winny być przeprowadzone dla jednostek wymienionych poniżej

## Wymagania ogólne dla szkolenia

* + 1. Szkolenie musi odbyć się w siedzibie Zamawiającego, ale Wykonawca powinien również dostarczyć platformę umożliwiającą prowadzenie szkoleń i być gotowym do organizacji szkolenia online.
    2. Wykonawca przygotuje również szkolenie dla użytkowników końcowych (wszystkich pracowników oraz współpracowników Zamawiającego), które będzie dotyczyło dokumentów sklasyfikowanych jako wewnętrzne. W ramach szkolenia Wykonawca omówi zakres opisany w tych dokumentach oraz przygotuje w postaci elektronicznej test wiedzy użytkowników.
    3. Zamawiający udostępni bezpłatnie pomieszczenie wyposażone w rzutnik oraz dostęp do Internetu, na potrzeby szkolenia stacjonarnego.
    4. Każde szkolenie powinno trwać od 2 do 5 godzin szkoleniowych dla 1 grupy szkoleniowej w ciągu dnia.
    5. Liczba osób uczestniczących w szkoleniu nie przekroczy 30 osób na grupę.
    6. Szkolenia będą odbywać się w dni robocze od poniedziałku do piątku w godzinach 8.00 – 15.30 w siedzibie Zamawiającego albo każdej jednostki w zależności od wyboru Zamawiającego.
    7. W przypadku szkolenia prowadzonego dla szkół Wykonawca musi się liczyć z możliwością prowadzenia szkoleń w godzinach pomiędzy 14:00 a 19:00.
    8. W celu maksymalizacji czasu nie przewiduje się przerw podczas szkolenia.
    9. W przypadku błędów albo braku możliwości uruchomienia szkolenia z uwagi na usterki techniczne Wykonawca zobowiązany jest do naprawy ww. szkolenia.
    10. W ramach organizacji szkoleń Wykonawca zapewni:
        1. Materiały szkoleniowe dla każdego uczestnika szkolenia w postaci elektronicznej, które Zamawiający będzie mógł wykorzystać nieodpłatnie i wydrukować dla każdego uczestnika. Materiały muszą zawierać szczegółowe informacje, które będą omawiane podczas szkolenia.
        2. Wydanie Uczestnikom szkolenia zaświadczeń o ukończeniu danego szkolenia.
        3. Prowadzenie dokumentacji wszystkich szkoleń w jednakowy sposób. Na dokumentację szkolenia składają się:
           1. Lista obecności Uczestników szkolenia (dzienne, wypełniane oddzielnie każdego dnia szkolenia).
           2. Lista odbioru zaświadczeń o ukończeniu szkolenia.
           3. Ankieta satysfakcji ze szkolenia.

## Przeszkolenie użytkowników z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa

Szkolenie należy przeprowadzić dla:

|  |  |
| --- | --- |
| Nazwa jednostki | Liczba audytów |
| Urząd Gminy w Tarnowie Opolskim | 1 |

* Gwarantującym nabycie praktycznych umiejętności w zakresie:
  + Wprowadzenie do Bezpieczeństwa Informacji

Przegląd zagrożeń cybernetycznych

Podstawowe zasady bezpieczeństwa informacji

* + Wykorzystywanie Mechanizmów Podwójnego Uwierzytelnienia (2FA)

Co to jest podwójne uwierzytelnienie (2FA) i dlaczego jest ważne

Rodzaje 2FA (SMS, aplikacje uwierzytelniające, tokeny sprzętowe)

Konfiguracja 2FA na popularnych platformach

Ćwiczenia praktyczne: wdrażanie i używanie 2FA

* + Skuteczne Szyfrowanie Danych

Podstawy szyfrowania danych: symetryczne i asymetryczne

Najlepsze praktyki szyfrowania danych w spoczynku i w tranzycie

Przykłady narzędzi do szyfrowania danych (VeraCrypt, BitLocker, PGP)

Ćwiczenia praktyczne: szyfrowanie i deszyfrowanie plików

* + Stosowanie VPN

Co to jest VPN i jak działa

Korzyści z używania VPN

Przegląd popularnych usług VPN

Praktyczne ćwiczenia: konfiguracja i korzystanie z VPN

* + Stosowanie SSL/TLS

Podstawy SSL/TLS: co to jest i jak działa

Rola certyfikatów SSL/TLS

Jak sprawdzić poprawność certyfikatów SSL/TLS na stronach internetowych

Praktyczne ćwiczenia: konfiguracja SSL/TLS na serwerze

* + Rozpoznawanie Fałszywych Stron i Domen (Typosquatting, Punycode i ich Odmiany)

Co to jest typosquatting i punycode

Techniki rozpoznawania fałszywych stron i domen

Narzędzia do weryfikacji domen i URL

Praktyczne ćwiczenia: identyfikacja fałszywych stron

* + Obrona przed Fałszywymi Sieciami WiFi

Zagrożenia związane z fałszywymi sieciami WiFi (evil twin, rogue AP)

Jak rozpoznać i unikać fałszywych sieci WiFi

Narzędzia i techniki zabezpieczania się przed fałszywymi sieciami

Praktyczne ćwiczenia: analiza sieci WiFi i identyfikacja zagrożeń

* + Bezpieczeństwo w Użytkowaniu Sztucznej Inteligencji

Wprowadzenie do sztucznej inteligencji i jej zastosowań

Zagrożenia związane z wykorzystaniem AI (deepfake, automatyzacja ataków)

Najlepsze praktyki w bezpiecznym używaniu AI

Przykłady narzędzi i rozwiązań wspierających bezpieczeństwo AI

## Szkolenia dla nauczycieli z zakresu cyberbezpieczeństwa

|  |  |
| --- | --- |
| Nazwa jednostki | Liczba |
| Przedszkole Publiczne w Kosorowicach | 1 |
| Przedszkole Publiczne w Przyworach | 1 |
| Przedszkole Publiczne z Oddziałami Integracyjnymi im. bł. Edmunda Bojanowskiego w Tarnowie Opolskim | 1 |
| Publiczna Szkoła Podstawowa w Kątach Opolskich | 1 |
| Publiczna Szkoła Podstawowa w Nakle | 1 |
| Publiczna Szkoła Podstawowa im. Mikołaja Kopernika w Tarnowie Opolskim | 1 |

* Wprowadzenie do cyberbezpieczeństwa w edukacji
  + Rola nauczyciela w kształtowaniu bezpiecznych nawyków cyfrowych
  + Charakterystyka zagrożeń online dla dzieci i młodzieży
  + Przegląd najpopularniejszych platform społecznościowych używanych przez uczniów
* Zagrożenia w mediach społecznościowych
  + Cyberprzemoc (cyberbullying), hejt, wykluczenie cyfrowe
  + Grooming, sexting, niebezpieczne kontakty
  + Uzależnienie od mediów społecznościowych i wpływ na zdrowie psychiczne
  + Fake newsy, dezinformacja i manipulacja
* Bezpieczne korzystanie z mediów społecznościowych
  + Zasady prywatności i ustawienia kont
  + Rozpoznawanie podejrzanych treści i profili
  + Odpowiedzialne publikowanie zdjęć i informacji
  + Kultura cyfrowa i etykieta online
* Rola nauczyciela i szkoły w edukacji cyfrowej
  + Jak rozmawiać z uczniami o zagrożeniach online
  + Współpraca z rodzicami w zakresie bezpieczeństwa cyfrowego
  + Wdrażanie zasad bezpiecznego korzystania z Internetu w klasie
  + Przykłady dobrych praktyk i scenariuszy lekcji

## Szkolenie ze stosowania i budowania silnych haseł, wykorzystywania menadżerów haseł oraz szyfrowania danych osobowych

* Szkolenie ma być przeprowadzone dla:

|  |  |
| --- | --- |
| Nazwa jednostki | Liczba |
| Urząd Gminy Tarnów Opolski | 1 |
| Gminny Ośrodek Pomocy Społecznej | 1 |
| Biuro Obsługi Oświaty Samorządowej |  |
| Przedszkole Publiczne w Kosorowicach | 1 |
| Przedszkole Publiczne w Przyworach | 1 |
| Przedszkole Publiczne z Oddziałami Integracyjnymi im. bł. Edmunda Bojanowskiego w Tarnowie Opolskim | 1 |
| Publiczna Szkoła Podstawowa w Kątach Opolskich | 1 |
| Publiczna Szkoła Podstawowa w Nakle | 1 |
| Publiczna Szkoła Podstawowa im. Mikołaja Kopernika w Tarnowie Opolskim | 1 |

* Skuteczne Tworzenie Haseł
  + Zasady tworzenia silnych haseł
  + Częste błędy przy tworzeniu haseł
  + Narzędzia do generowania silnych haseł
  + Praktyczne ćwiczenia: tworzenie i ocena haseł
* Skuteczne Szyfrowanie Danych
  + Podstawy szyfrowania danych: symetryczne i asymetryczne
  + Najlepsze praktyki szyfrowania danych w spoczynku i w tranzycie
  + Przykłady narzędzi do szyfrowania danych (VeraCrypt, BitLocker, PGP)
* Wykorzystywanie Menedżerów Haseł
  + Dlaczego menedżery haseł są ważne
  + Przegląd popularnych menedżerów haseł (1Password, Bitwarden, Keepass)
  + Jak bezpiecznie korzystać z menedżerów haseł

## Szkolenie specjalistyczne dla informatyka Urzędu Gminy

Zaawansowane zarządzanie systemem

* Wprowadzenie do architektury UTM
  + Omówienie roli UTM w infrastrukturze bezpieczeństwa
  + Tryby pracy: NAT vs Transparent
* Konfiguracja początkowa i zarządzanie urządzeniem
  + Interfejsy sieciowe i strefy bezpieczeństwa
  + Konfiguracja przez GUI i CLI
  + Zarządzanie przez
  + Backup i restore konfiguracji
  + Aktualizacje firmware’u i planowanie ich
* Polityki bezpieczeństwa i kontrola ruchu
  + Tworzenie i zarządzanie politykami firewall
  + Profile bezpieczeństwa: AV, Web Filter, App Control, IPS, SSL Inspection
  + Deep Packet Inspection vs Flow-based Inspection
  + Konfiguracja polityk z użyciem tożsamości użytkownika (FSSO, LDAP, RADIUS)
* Zaawansowane funkcje sieciowe
  + Routing statyczny i dynamiczny (OSPF, BGP)
  + SD-WAN – konfiguracja i optymalizacja
  + VLAN, agregacja portów,
  + High Availability (HA) – Active-Passive i Active-Active
* VPN – konfiguracja i zarządzanie
  + IPsec VPN (site-to-site, dial-up)
  + SSL VPN (portal, tunel, polityki dostępu)
  + Diagnostyka i troubleshooting VPN
* Monitorowanie, logowanie i analiza zdarzeń
  + Logi systemowe
  + Alerty, raporty i korelacja zdarzeń
  + Diagnostyka CLI i narzędzia debugowania

## Szkolenie z ochrony przed wyłudzeniem danych osobowych i informacji

Szkolenie ma być przeprowadzone dla:

|  |  |
| --- | --- |
| Nazwa jednostki | Liczba audytów |
| Urząd Gminy Tarnów Opolski | 1 |
| Przedszkole Publiczne w Kosorowicach | 1 |
| Przedszkole Publiczne w Przyworach | 1 |
| Przedszkole Publiczne z Oddziałami Integracyjnymi im. bł. Edmunda Bojanowskiego w Tarnowie Opolskim | 1 |
| Publiczna Szkoła Podstawowa w Kątach Opolskich | 1 |
| Publiczna Szkoła Podstawowa w Nakle | 1 |
| Publiczna Szkoła Podstawowa im. Mikołaja Kopernika w Tarnowie Opolskim | 1 |
| Gminny Ośrodek Pomocy Społecznej | 1 |
| Biuro Obsługi Oświaty Samorządowej | 1 |

* Wprowadzenie do Bezpieczeństwa Informacji
  + Cel i znaczenie szkolenia
  + Przegląd zagrożeń cybernetycznych
  + Podstawowe zasady bezpieczeństwa informacji
* Podstawy RODO
  + Podstawowe Zasady RODO
  + Zasady przetwarzania danych osobowych (legalność, celowość, minimalizacja danych, dokładność, ograniczenie przechowywania, integralność i poufność, rozliczalność)
  + Prawa osób, których dane dotyczą
* Konkretne Przypadki Stosowania RODO
  + Zbieranie i Przetwarzanie Danych Osobowych
  + Udostępnianie Danych Osobowych
  + Przechowywanie i Usuwanie Danych Osobowych
  + Reagowanie na Incydenty Bezpieczeństwa
* Wykrywanie Phishingu oraz Jego Odmian
  + Definicja i rodzaje phishingu (email, SMS, spear phishing, whaling)
  + Metody rozpoznawania phishingu
  + Przykłady ataków phishingowych
  + Praktyczne ćwiczenia w wykrywaniu phishingu
* Wykorzystywanie Mechanizmów Podwójnego Uwierzytelnienia (2FA)
  + Co to jest podwójne uwierzytelnienie (2FA) i dlaczego jest ważne
  + Rodzaje 2FA (SMS, aplikacje uwierzytelniające, tokeny sprzętowe)
  + Konfiguracja 2FA na popularnych platformach
  + Ćwiczenia praktyczne: wdrażanie i używanie 2FA
* Stosowanie VPN
  + Co to jest VPN i jak działa
  + Korzyści z używania VPN
  + Przegląd popularnych usług VPN
  + Praktyczne ćwiczenia: konfiguracja i korzystanie z VPN
* Stosowanie SSL/TLS
  + Podstawy SSL/TLS: co to jest i jak działa
  + Rola certyfikatów SSL/TLS
  + Jak sprawdzić poprawność certyfikatów SSL/TLS na stronach internetowych
  + Praktyczne ćwiczenia: konfiguracja SSL/TLS na serwerze
* Rozpoznawanie Fałszywych Stron i Domen (Typosquatting, Punycode i ich Odmiany)
  + Co to jest typosquatting i punycode
  + Techniki rozpoznawania fałszywych stron i domen
  + Narzędzia do weryfikacji domen i URL
  + Praktyczne ćwiczenia: identyfikacja fałszywych stron
* Obrona przed Fałszywymi Sieciami WiFi
  + Zagrożenia związane z fałszywymi sieciami WiFi (evil twin, rogue AP)
  + Jak rozpoznać i unikać fałszywych sieci WiFi
  + Narzędzia i techniki zabezpieczania się przed fałszywymi sieciami
* Bezpieczeństwo w Użytkowaniu Sztucznej Inteligencji
  + Wprowadzenie do sztucznej inteligencji i jej zastosowań
  + Zagrożenia związane z wykorzystaniem AI (deepfake, automatyzacja ataków)
  + Najlepsze praktyki w bezpiecznym używaniu AI
  + Przykłady narzędzi i rozwiązań wspierających bezpieczeństwo AI

## Szkolenia z zabezpieczenia sprzętu prywatnego wykorzystywanego do celów służbowych

Szkolenie ma być przeprowadzone dla:

|  |  |
| --- | --- |
| Nazwa jednostki | Liczba audytów |
| Urząd Gminy Tarnów Opolski | 1 |
| Gminny Ośrodek Pomocy Społecznej | 1 |
| Przedszkole Publiczne w Kosorowicach | 1 |
| Przedszkole Publiczne w Przyworach | 1 |
| Przedszkole Publiczne z Oddziałami Integracyjnymi im. bł. Edmunda Bojanowskiego w Tarnowie Opolskim | 1 |
| Publiczna Szkoła Podstawowa w Kątach Opolskich | 1 |
| Publiczna Szkoła Podstawowa w Nakle | 1 |
| Publiczna Szkoła Podstawowa im. Mikołaja Kopernika w Tarnowie Opolskim | 1 |
| Biuro Obsługi Oświaty Samorządowej | 1 |

* Wprowadzenie: znaczenie bezpieczeństwa sprzętu prywatnego w pracy zdalnej i hybrydowej
  + Podstawowe zasady ochrony urządzeń prywatnych
  + Aktualizacje systemu i oprogramowania — dlaczego są kluczowe
  + Uwierzytelnianie i zarządzanie hasłami
  + Szyfrowanie danych na urządzeniu
  + Bezpieczne korzystanie z sieci Wi-Fi i VPN
  + Antywirus i ochrona przed malware czy wystarczy?
  + Backup danych i przywracanie systemu
  + Bezpieczne korzystanie z aplikacji służbowych i chmurowych
  + Ochrona prywatności i zapobieganie wyciekom danych
  + Zasady bezpiecznego korzystania z nośników zewnętrznych
  + Świadomość zagrożeń — phishing, ransomware i socjotechnika
  + Procedury postępowania w przypadku podejrzenia incydentu bezpieczeństwa
  + Podsumowanie i najlepsze praktyki ochrony sprzętu prywatnego

# Kryteria jakościowe dla odbioru przedmiotu Zamówienia

## W zakresie krytycznych systemów teleinformatycznych

* Przygotowano propozycje postępowania z oszacowanym ryzykiem, ze wskazaniem możliwych do wdrożenia środków technicznych i organizacyjnych.
* Zweryfikowano kompletność zapisów wymagań SZBI pod kątem zgodności pokrycia z zakresem wymagań określonych w normach 2700X.

## Dokumentacji projektowej (w tym SZBI, raportów i innych)

* Pokrywa pełny zakres norm ISO 2700X.
* Każdy punkt normy zawiera opis środków organizacyjnych oraz technicznych zapewniających ochronę informacji. Należy przez to rozumieć, że obowiązkiem Wykonawcy jest opisanie środków ochrony informacji, którymi dysponuje lub które może / powinien wdrożyć Zamawiający w ramach przygotowanej dokumentacji.
* Dokumentacja jest przygotowana poprzez użycie funkcji automatyzujących formatowanie (punktatory, listy, formatowania i inne) w formacie DOCX.
* Dokumentacja nie jest wygenerowana przez sztuczną inteligencję.
* Istnieje możliwość demonstracji pełnego pokrycia przygotowanej dokumentacji na zgodność z ISO 2700X.

## W zakresie szkoleń

* Użytkownicy zostali przeszkoleniu w zakresie opisanym w niniejszym zamówieniu.
* Użytkownicy zdali testy wiedzy potwierdzające nabycie umiejętności w wybranym zakresie.

# Prawa autorskie i majątkowe

* 1. Prawa autorskie majątkowe w odniesieniu do wszystkich dokumentów będących utworami w rozumieniu ustawy z dnia 04 lutego 1994 r. o prawie autorskich i prawach pokrewnych, zwanych dalej „Utworami”, dostarczonych przez Wykonawcę w trakcie realizacji niniejszej umowy przechodzą na Zamawiającego z chwilą ich dostarczenia Zamawiającemu. Z tą też chwilą na Zamawiającego przechodzi prawo własności do nośników, na których Utwory zostały utrwalone.
  2. Przeniesienie autorskich praw majątkowych, o którym mowa w ust. 1 obejmuje następujące pola eksploatacji:
* prawo do utrwalania i zwielokrotniania,
* prawo wprowadzania dokumentacji do pamięci komputerów i serwerów sieci komputerowych,
* prawo do wielokrotnego korzystania z dokumentacji przez Zamawiającego bez ograniczeń czasowych.
  1. Z chwilą przekazania Zamawiającemu Utworów, Wykonawca zezwala na rozporządzanie i korzystanie przez Zamawiającego z utworów zależnych stanowiących opracowania tych Utworów i przenosi na Zamawiającego wyłączne prawo zezwalania na wykonywanie zależnego prawa autorskiego do Utworów na polach eksploatacji określonych w ust. 2.
  2. Przeniesienie praw oraz udzielenie zezwoleń i upoważnień których mowa w ust. 1- 3 następuje bez jakichkolwiek dalszych czynności stron oraz bez ograniczeń czasowych, terytorialnych i ilościowych.
  3. Przeniesienie autorskich praw majątkowych oraz udzielenie zezwoleń i upoważnień, o których mowa w ust. 1-3 następuje bez dodatkowego wynagrodzenia dla Wykonawcy.
  4. Wykonawca wyraża zgodę na wykorzystanie lub rozporządzanie przez Zamawiającego Utworami oraz ich opracowaniami w części lub całości oraz łączenia z innymi dziełami.
  5. Wykonawca zobowiązuje się do niewykonywania wobec Zamawiającego przysługujących mu autorskich praw osobistych, o których mowa w art. 16 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, do Utworów i zezwala Zamawiającemu na ich wykonywanie w jego imieniu.