Projekt **FERS.01.05-IP.08-008/23**:
„Uczelnia Rozwoju Kompetencji Osób Dorosłych” finansowany w ramach **Funduszy Europejskich dla Rozwoju Społecznego,** *Wsparcie na rzecz szkolnictwa wyższego* (z wyłączeniem infrastruktury)
na lata 2021-2027.

# Program szkolenia: Cyberbezpieczeństwo i ochrona wrażliwych danych

Nr zadania: 6

*Stanisław Czapnik*

## Spis treści

# Cyberbezpieczeństwo – nr zadania: 6

# Program szkolenia

**Program Szkolenia: Cyberbezpieczeństwo i Ochrona Wrażliwych Danych**

**Czas trwania: 25 godzin**

**Osoba prowadząca: mgr Stanisław Czapnik**

Kierownik zespołu Cybersecurity w firmie NT Group Systemy Informatyczne Sp. z o.o. Doświadczony pracownik dydaktyczny, autor wielu programów szkoleń i audytów. Prelegent w zakresie cyberbezpieczeństwa, przepisów NIS 2 oraz DORA na forach i konferencjach. Ekspert – konsultant w zakresie cyberbezpieczeństwa wydawnictw branżowych. Kierownik projektu rozwoju audytów w zakresie cyberbezpieczeństwa i ochrony danych. Audytor dostępności, pasjonat dostępności, rozwiązań chmurowych oraz sztucznej inteligencji.

## Cele:

- Zapewnienie kompleksowego zrozumienia zasad cyberbezpieczeństwa i dobrych praktyk
- Wyposażenie uczestników w wiedzę i umiejętności ochrony danych wrażliwych w kontekście zawodowym i prywatnym
- Podniesienie świadomości na temat technik inżynierii społecznej oraz powszechnych metod ataków hakerskich
- Umożliwienie uczestnikom identyfikacji, łagodzenia i reagowania na zagrożenia cyberbezpieczeństwa

# Program szkolenia:

## 1. Wprowadzenie do Cyberbezpieczeństwa

Moduł rozpocznie szkolenie, dostarczając uczestnikom kompleksowego zrozumienia cyberbezpieczeństwa i jego kluczowej roli we współczesnym świecie. Omówione zostaną podstawowe definicje i pojęcia, takie jak cyberprzestrzeń, ataki cybernetyczne, zagrożenia i podatności. Szczególną uwagę poświęcimy na zrozumienie różnych typów zagrożeń, w tym złośliwego oprogramowania, ataków hakerskich, wycieku danych i kradzieży tożsamości.

Omówienie ogólnych zasad cyberbezpieczeństwa, takie jak wdrażanie wielowarstwowej ochrony, stosowanie zasady minimalizacji uprawnień, monitorowanie i reagowanie na incydenty. Uczestnicy poznają obowiązujące regulacje prawne i standardy dotyczące ochrony danych osobowych, w tym RODO i inne właściwe dla danego sektora.

Kluczowym elementem będzie zrozumienie znaczenia cyberbezpieczeństwa zarówno na poziomie organizacyjnym, jak i indywidualnym. Uczestnicy dowiedzą się, w jaki sposób zagrożenia cybernetyczne mogą wpływać na działalność firmy, reputację, finanse i bezpieczeństwo pracowników. Omówimy również konsekwencje lekceważenia lub niedoceniania kwestii cyberbezpieczeństwa.

## 2. Podstawy Ochrony Danych

W tym module uczestnicy zdobędą kompleksową wiedzę na temat bezpiecznego przetwarzania, przechowywania i ochrony danych. Począwszy od klasyfikacji danych, różnych kategorii informacji, takie jak dane osobowe, dane finansowe, dane medyczne i inne dane wrażliwe. Uczestnicy dowiedzą się, jak prawidłowo identyfikować, oznaczać i segregować dane w zależności od poziomu ich poufności.

Omówienie kluczowych technologii i technik ochrony danych, w tym szyfrowania, zarządzania kluczami, kontroli dostępu i uwierzytelniania. Uczestnicy poznają najlepsze

praktyki w zakresie bezpiecznego przechowywania danych, takie jak stosowanie zaszyfrowanych dysków, kopii zapasowych i mechanizmów monitorowania integralności danych.

Istotnym elementem będzie również zrozumienie zasad zarządzania tożsamością i uprawnień dostępu. Omówimy metody identyfikacji i uwierzytelniania użytkowników, w tym zastosowanie haseł, tokenów, biometrii i mechanizmów autoryzacji. Uczestnicy dowiedzą się, jak wdrażać polityki ograniczania uprawnień oraz monitorować i analizować działania użytkowników.

Analiza wymagań prawnych i regulacyjnych dotyczących ochrony danych, takich jak RODO, oraz konsekwencje nieprzestrzegania tych przepisów. Uczestnicy poznają praktyczne narzędzia i techniki, które mogą wdrożyć, aby zapewnić zgodność z obowiązującymi normami.

## 3. Inżynieria Społeczna i Podatności Ludzkie

Zrozumienie i łagodzenie ryzyka związanego z inżynierią społeczną - jednym z najskuteczniejszych narzędzi wykorzystywanych przez cyberprzestępców. Uczestnicy poznają różne techniki inżynierii społecznej, w tym phishing, pretexting, podrzucanie przynęty, social media mining i wiele innych.

Zrozumienie, w jaki sposób cyberprzestępcy wykorzystują ludzkie podatności, takie jak nadmierna ufność, ciekawość, chęć pomocy czy lęk. Omówienie sposobu jak cyberprzestępcy manipulują emocjami i psychologią ofiar, aby uzyskać dostęp do poufnych informacji lub zainfekowania systemów złośliwym oprogramowaniem.

Uczestnicy dowiedzą się, jak rozpoznawać typowe sygnały ostrzegawcze i techniki inżynierii społecznej, zarówno w kontekście zawodowym, jak i prywatnym. Omówienie case studies rzeczywistych ataków, aby lepiej zrozumieć modus operandi cyberprzestępców i wypracować skuteczne mechanizmy obrony.

Wypracowanie strategii łagodzenia ryzyka inżynierii społecznej. Uczestnicy poznają najlepsze praktyki w zakresie podnoszenia świadomości pracowników, wdrażania procedur bezpieczeństwa oraz testowania odporności organizacji na ataki socjotechniczne.

## 4. Higiena Cyfrowa i Zarządzanie Ryzykiem

Budowanie nawyków i praktyk bezpieczeństwa, które powinny stać się standardem w codziennej pracy i życiu prywatnym uczestników. Podstawowa higiena cyfrowa, zarządzanie hasłami, korzystanie z uwierzytelniania wieloskładnikowego oraz bezpieczne praktyki przeglądania internetu i korzystania z poczty elektronicznej.

Uczestnicy dowiedzą się, w jaki sposób chronić swoje urządzenia mobilne, w tym smartfony i tablety, przed zagrożeniami, takimi jak kradzież, złośliwe oprogramowanie i wycieki danych. Omówimy metody bezpiecznego przechowywania i synchronizacji danych, w tym stosowanie szyfrowania i bezpiecznych usług chmurowych.

Zrozumienie zasad zarządzania ryzykiem cyberbezpieczeństwa na poziomie indywidualnym i organizacyjnym. Uczestnicy nauczą się identyfikować, oceniać i minimalizować różne rodzaje ryzyka, takie jak ryzyko utraty danych, ryzyko naruszenia reputacji czy ryzyko finansowe. Wypracujemy strategie tworzenia kopii zapasowych, odzyskiwania po awariach i reagowania na incydenty.

Świadomośćbezpieczeństwa i budowania kultury cyberbezpieczeństwa w organizacji. Uczestnicy dowiedzą się, jak promować dobre praktyki wśród pracowników, wdrażać polityki bezpieczeństwa i zapewniać ciągłe szkolenia z zakresu cyberbezpieczeństwa.

## 5. Bezpieczeństwo Sieci i Reagowanie na Incydenty

abezpieczanie sieci i infrastruktury IT przed zagrożeniami. Podstawowe koncepcje, takie jak segmentacja sieci, kontrola dostępu, monitorowanie aktywności i wykrywanie anomalii.

Szczególną uwagę poświęcimy zabezpieczaniu sieci bezprzewodowych oraz urządzeń Internetu Rzeczy (IoT). Uczestnicy poznają techniki szyfrowania, uwierzytelniania, zarządzania uprawnieniami i monitorowania tych podatnych na ataki elementów infrastruktury.

Zrozumienie procesu reagowania na incydenty bezpieczeństwa. Uczestnicy dowiedzą się, jak rozpoznawać, klasyfikować i zgłaszać incydenty, a także jak wdrażać procedury powstrzymywania, eliminowania i odzyskiwania po atakach. Omówimy również role i obowiązki poszczególnych zespołów, takich jak zespół ds. cyberbezpieczeństwa, zespół ds. zarządzania kryzysowego i zespół ds. komunikacji.

Analiza case studies rzeczywistych incydentów bezpieczeństwa, identyfikując kluczowe błędy i wypracowując najlepsze praktyki w zakresie planowania ciągłości działania, tworzenia kopii zapasowych i odzyskiwania po awariach.

## 6. Złośliwe Oprogramowanie i Techniki Hakerskie

Złośliwe oprogramowanie oraz podstawowe techniki i narzędzia wykorzystywane przez hakerów. Uczestnicy poznają różne rodzaje złośliwego oprogramowania, takie jak wirusy, robaki, konie trojańskie, ransomware i keyloggery, oraz zrozumieją, w jaki sposób mogą one infekować systemy i powodować szkody.

Omówienie typowych wektorów infekcji, takich jak załączniki e-mail, nielegalne oprogramowanie, podatności w oprogramowaniu i techniki phishingowe. Uczestnicy dowiedzą się, jak rozpoznawać oznaki infekcji, a także jak zapobiegać rozprzestrzenianiu się złośliwego oprogramowania i minimalizować jego skutki.

Zrozumienie podstaw etycznego hakowania i testów penetracyjnych. Uczestnicy zapoznają się z narzędziami i technikami wykorzystywanymi przez hakerów, takimi jak skanowanie portów, exploity, techniki social engineeringu i narzędzia do analizy złośliwego oprogramowania.

W ramach praktycznych warsztatów uczestnicy będą mieli okazję przeanalizować rzeczywiste próbki złośliwego oprogramowania, zidentyfikować luki w zabezpieczeniach i przetestować podatności infrastruktury IT. Pozwoli im to zdobyć cenne doświadczenie w zakresie detekcji, analizy i reagowania na zagrożenia.

## 7. Świadomość Bezpieczeństwa i Kultura Organizacyjna

Budowanie świadomości bezpieczeństwa i kształtowanie kultury cyberbezpieczeństwa w organizacji. Uczestnicy zrozumieją, że zapewnienie bezpieczeństwa danych i systemów IT to nie tylko kwestia wdrożenia odpowiednich zabezpieczeń technicznych, ale również ukształtowanie odpowiednich postaw i zachowań wśród pracowników.

Strategiczne cele cyberbezpieczeństwa i przełożenie ich na konkretne polityki, procedury i standardy, które będą obowiązywać w organizacji. Uczestnicy dowiedzą się, jak opracowywać i wdrażać spójne ramowe dokumenty bezpieczeństwa, zapewniając ich skuteczne egzekwowanie.

Zrozumienie roli szkoleń i programów podnoszenia świadomości. Uczestnicy poznają różne metody i narzędzia, które mogą wykorzystać, aby skutecznie edukować pracowników i promować dobre praktyki cyberbezpieczeństwa w codziennej pracy.

Kluczowe czynniki budowania kultury organizacyjnej zorientowanej na bezpieczeństwo. Uczestnicy dowiedzą się, jak angażować kadrę zarządzającą, promować otwartą komunikację na temat zagrożeń, a także nagradzać i wspierać pracowników za właściwe postawy i zachowania.

## 8. Ćwiczenia Praktyczne i Symulacje Warsztatowe

Praktyczne aspekty cyberbezpieczeństwa. Uczestnicy będą mieli możliwość zastosowania zdobytej wiedzy w symulowanych scenariuszach.

Uczestnicy wezmą udział w warsztatach obejmujących różne ataki i incydenty bezpieczeństwa, takie jak phishing, wyłudzanie informacji, infekcje złośliwym

oprogramowaniem czy naruszenia danych. Będą mieli okazję wcielić się w role ofiar, napastników i zespołów reagujących, aby lepiej zrozumieć mechanizmy działania, konsekwencje i sposoby radzenia sobie z tego typu zagrożeniami.

Ćwiczenia z zakresu inżynierii społecznej. Uczestnicy będą brani na cele różnych technik socjotechnicznych, aby nauczyć się je rozpoznawać, a następnie wypracować strategie obrony i przeciwdziałania.

Uczestnicy wezmą udział w symulacjach incydentów bezpieczeństwa, takich jak naruszenie systemu, wyciek danych lub atak typu ransomware. Będą musieli uruchomić procedury reagowania, zapewnić ciągłość działania, przeprowadzić dochodzenie i podjąć działania naprawcze.

Wszystkie ćwiczenia i symulacje będą poprzedzone wprowadzeniem merytorycznym, a następnie podsumowane omówieniem wniosków, zidentyfikowanych słabości i najlepszych praktyk. Pozwoli to uczestnikom zdobyć cenne doświadczenie praktyczne i lepiej przygotować się do rzeczywistych wyzwań związanych z cyberbezpieczeństwem.

# Opis modułów szkolenia

## Moduł 1: Wprowadzenie do cyberbezpieczeństwa (2h)

**Definicja cyberbezpieczeństwa**

- Kompleksowe omówienie pojęcia cyberbezpieczeństwa w kontekście współczesnych zagrożeń
- Ewolucja cyberbezpieczeństwa na przestrzeni lat - od pierwszych wirusów po współczesne zagrożenia
- Znaczenie cyberbezpieczeństwa w życiu prywatnym i zawodowym
- Wpływ cyberbezpieczeństwa na funkcjonowanie organizacji i społeczeństwa
- Podstawowe filary cyberbezpieczeństwa: poufność, integralność, dostępność
- Rola człowieka w systemie cyberbezpieczeństwa
- Odpowiedzialność indywidualna i organizacyjna w kontekście cyberbezpieczeństwa

**Aktualne zagrożenia w cyberprzestrzeni**

- Mapowanie współczesnego krajobrazu zagrożeń
- Trendy w cyberprzestępczości i prognozowane kierunki rozwoju zagrożeń
- Motywacje cyberprzestępców: finansowe, polityczne, ideologiczne
- Zagrożenia dla różnych sektorów: finanse, służba zdrowia, administracja publiczna
- Wpływ nowych technologii (AI, IoT, 5G) na bezpieczeństwo
- Zagrożenia dla użytkowników indywidualnych vs. organizacji
- Geograficzna dystrybucja zagrożeń i główne źródła ataków

**Statystyki i przykłady głośnych cyberataków**

- Szczegółowa analiza najgłośniejszych ataków ostatnich lat
- Omówienie przypadku Wannacry - przebieg, skutki, wnioski
- Analiza ataku na SolarWinds - mechanizm działania, zasięg, konsekwencje

- Przypadek wycieku danych z Yahoo - przyczyny, skala, następstwa
- Statystyki dotyczące różnych typów ataków i ich skuteczności
- Koszty finansowe i wizerunkowe cyberataków
- Czas wykrycia i reakcji na incydenty - statystyki i trendy

**Podstawowe pojęcia i terminologia**

- Słownik kluczowych terminów cyberbezpieczeństwa
- Techniczne aspekty zabezpieczeń: firewall, IPS/IDS, SIEM
- Rodzaje podatności i ich klasyfikacja
- Metody zabezpieczeń: techniczne, organizacyjne, fizyczne
- Standardy i frameworki bezpieczeństwa
- Certyfikacje w obszarze cyberbezpieczeństwa
- Regulacje prawne dotyczące cyberbezpieczeństwa

**Ćwiczenie: Analiza przypadków rzeczywistych ataków**

- Szczegółowa analiza wybranego ataku krok po kroku
- Identyfikacja słabych punktów w zabezpieczeniach
- Analiza możliwych środków zapobiegawczych
- Dyskusja nad alternatywnymi scenariuszami obrony
- Tworzenie timeline'u ataku i reakcji
- Ocena skuteczności podjętych działań obronnych
- Formułowanie wniosków i rekomendacji

## Moduł 2: Bezpieczeństwo haseł i uwierzytelnianie (3h)

**Zasady tworzenia silnych haseł**

- Matematyczne podstawy siły hasła
- Długość vs. złożoność - analiza skuteczności różnych podejść
- Metody tworzenia zapamiętywalnych, silnych haseł
- Najczęstsze błędy przy tworzeniu haseł
- Techniki łamania haseł stosowane przez przestępców

- Okresowa zmiana haseł - zalety i wady
- Unikalne hasła dla różnych serwisów - uzasadnienie i praktyka

**Menedżery haseł**

- Przegląd dostępnych rozwiązań: LastPass, 1Password, Bitwarden, KeePass
- Architektura bezpieczeństwa menedżerów haseł
- Metody synchronizacji i kopii zapasowych
- Bezpieczeństwo chmurowe vs. lokalne
- Funkcje dodatkowe: generatory haseł, audyt bezpieczeństwa
- Współdzielenie haseł w organizacji
- Procedury awaryjne i odzyskiwanie dostępu

**Uwierzytelnianie dwuskładnikowe (2FA)**

- Rodzaje drugiego składnika uwierzytelniania
- SMS vs. aplikacje autentykacyjne - zalety i wady
- Klucze sprzętowe (YubiKey, itp.) - zastosowanie i bezpieczeństwo
- Implementacja 2FA w organizacji
- Procedury awaryjne i kody zapasowe
- Integracja z różnymi systemami i serwisami
- Zarządzanie 2FA w zespole

**Biometria i inne metody uwierzytelniania**

- Rodzaje biometrii: odciski palców, twarz, tęczówka
- Bezpieczeństwo danych biometrycznych
- Skuteczność różnych metod biometrycznych
- Single Sign-On (SSO) - zasada działania i implementacja
- Uwierzytelnianie kontekstowe
- Przyszłość uwierzytelniania - trendy i innowacje
- Zagrożenia związane z biometrią

### Ćwiczenia praktyczne

- Instalacja i konfiguracja wybranego menedżera haseł
- Generowanie i testowanie siły różnych haseł
- Konfiguracja 2FA dla popularnych serwisów
- Tworzenie polityki haseł dla organizacji
- Symulacja utraty dostępu i procedury odzyskiwania
- Testowanie różnych metod uwierzytelniania
- Analiza bezpieczeństwa istniejących haseł

## Moduł 3: Socjotechnika i manipulacja (3h)

### Podstawy socjotechniki

- Psychologiczne podstawy manipulacji
- Teoria wpływu społecznego Cialdiniego w kontekście cyberbezpieczeństwa
- Mechanizmy poznawcze wykorzystywane w atakach
- Rola emocji w podatności na ataki
- Presja czasu jako narzędzie manipulacji
- Budowanie zaufania przez atakujących
- Wykorzystanie autorytetów w atakach

### Typy ataków socjotechnicznych

- Pretekstotwórstwo (pretext calling)
- Quid pro quo
- Podszywanie się (impersonation)
- Tailgating/piggybacking
- Dumpster diving
- Shoulder surfing
- Reverse social engineering

**Phishing i jego odmiany**

- Klasyczny phishing emailowy
- Spear phishing
- Whaling
- Vishing (voice phishing)
- Smishing (SMS phishing)
- Pharming
- Business Email Compromise (BEC)

**Manipulacja psychologiczna**

- Techniki wywierania wpływu
- Wykorzystanie lęku i poczucia pilności
- Manipulacja emocjami
- Socjotechnika w mediach społecznościowych
- Techniki budowania fałszywego zaufania
- Manipulacja w komunikacji pisemnej i ustnej
- Rozpoznawanie oznak manipulacji

**Ćwiczenia praktyczne**

- Analiza prawdziwych wiadomości phishingowych
- Symulacja rozmowy socjotechnicznej
- Tworzenie profilu atakującego
- Identyfikacja technik manipulacji
- Budowanie świadomości zagrożeń
- Tworzenie procedur weryfikacji
- Scenariusze reakcji na próby manipulacji

# Moduł 4: Złośliwe oprogramowanie (2h)

### Rodzaje malware

- Klasyfikacja złośliwego oprogramowania
- Ewolucja malware na przestrzeni lat
- Metody rozprzestrzeniania się złośliwego oprogramowania
- Źródła infekcji: email, strony internetowe, nośniki USB
- Mechanizmy ukrywania się przed systemami bezpieczeństwa
- Polimorficzne i metamorficzne malware
- Trendy w rozwoju złośliwego oprogramowania

### Wirusy, robaki, trojany

- Charakterystyka wirusów komputerowych
- Mechanizmy replikacji i infekcji
- Specyfika działania robaków sieciowych
- Różnice między wirusami a robakami
- Trojany - metody działania i ukrywania się
- Backdoory i ich zastosowanie przez atakujących
- Rootkity i ich wpływ na bezpieczeństwo systemu

### Ransomware

- Ewolucja ataków ransomware
- Mechanizmy szyfrowania danych
- Metody dystrybucji ransomware
- Żądania okupu i komunikacja z atakującymi
- Procedury zapobiegania atakom
- Strategie odzyskiwania danych
- Współpraca z organami ścigania

**Cryptojacking**

- Mechanizmy działania cryptojackingu
- Wpływ na wydajność systemów
- Metody wykrywania nielegalnego kopania kryptowalut
- Zabezpieczenia przed cryptojackingiem
- Straty energetyczne i finansowe
- Prawne aspekty cryptojackingu
- Trendy w atakach cryptojackingowych

**Ćwiczenie: Analiza przypadków zainfekowania malware**

- Studium przypadku infekcji ransomware
- Analiza wektorów ataku
- Identyfikacja objawów infekcji
- Procedury izolacji zainfekowanych systemów
- Metody usuwania złośliwego oprogramowania
- Przywracanie systemu po infekcji
- Tworzenie raportów z incydentów

## Moduł 5: Bezpieczeństwo danych w firmie (3h)

**Polityka bezpieczeństwa informacji**

- Struktura polityki bezpieczeństwa
- Procedury i instrukcje wykonawcze
- Role i odpowiedzialności w organizacji
- Zarządzanie dostępem do informacji
- Klasyfikacja informacji i aktywów
- Procedury kontroli i audytu
- Aktualizacja i rewizja polityk

**RODO i ochrona danych osobowych**

- Podstawowe pojęcia i definicje RODO
- Prawa podmiotów danych
- Obowiązki administratora danych
- Rejestr czynności przetwarzania
- Ocena skutków dla ochrony danych (DPIA)
- Zgłaszanie naruszeń ochrony danych
- Międzynarodowy transfer danych

**Klasyfikacja danych**

- Kryteria klasyfikacji informacji
- Poziomy poufności danych
- Oznaczanie i etykietowanie informacji
- Procedury przetwarzania danych
- Przechowywanie i archiwizacja
- Bezpieczne usuwanie danych
- Inwentaryzacja zasobów informacyjnych

**Procedury bezpieczeństwa**

- Standardowe procedury operacyjne (SOP)
- Procedury dostępu do systemów
- Zarządzanie incydentami
- Procedury tworzenia kopii zapasowych
- Plany ciągłości działania
- Procedury reagowania kryzysowego
- Dokumentacja procedur bezpieczeństwa

**Ćwiczenia praktyczne**

- Tworzenie polityki bezpieczeństwa
- Implementacja procedur RODO
- Klasyfikacja przykładowych dokumentów

- Projektowanie procedur bezpieczeństwa
- Symulacja audytu bezpieczeństwa
- Tworzenie rejestru czynności przetwarzania
- Opracowanie planu reagowania na incydenty

## Moduł 6: Bezpieczeństwo sieci firmowej (2h)

**Podstawy działania sieci**

- Architektura sieci komputerowych
- Protokoły sieciowe i ich bezpieczeństwo
- Segmentacja sieci
    - Routing i switching
    - Monitoring ruchu sieciowego
- Wykrywanie anomalii
- Zarządzanie przepustowością

**Zabezpieczenia sieciowe**

- Firewalle nowej generacji
- Systemy IDS/IPS
    - Systemy antywirusowe
    - Web Application Firewalls
    - Network Access Control
- Security Information and Event Management
- Zarządzanie podatnościami

**VPN i praca zdalna**

- Rodzaje połączeń VPN
- Protokoły tunelowania
- Szyfrowanie w VPN
- Uwierzytelnianie użytkowników
- Bezpieczeństwo endpoint
- Polityki dostępu zdalnego
- Monitoring połączeń VPN

**Bezpieczne WiFi**

- Standardy zabezpieczeń WiFi
- Konfiguracja punktów dostępowych
- Segmentacja sieci bezprzewodowej
- Uwierzytelnianie użytkowników
- Monitoring sieci WiFi
- Wykrywanie nieautoryzowanych AP
- Zarządzanie gośćmi w sieci

## Moduł 7: Ochrona prywatności online (2.5h)

**Media społecznościowe**

- Zagrożenia prywatności w social media
- Ustawienia prywatności na różnych platformach
- Cyfrowy ślad i jego znaczenie
- Ochrona przed śledzeniem
- Bezpieczne udostępnianie treści
- Weryfikacja dwuetapowa
- Zarządzanie tożsamością online

### Śledzenie online

- Mechanizmy śledzenia użytkowników
- Pliki cookies i ich rodzaje
- Fingerprinting przeglądarki
- Reklamy behawioralne
- Techniki anti-tracking
- Prywatne przeglądarki
- Narzędzia do ochrony prywatności

### Prywatne przeglądarki i wyszukiwarki

- Porównanie przeglądarek pod kątem prywatności
- Konfiguracja ustawień prywatności
- Rozszerzenia zwiększające prywatność
- Alternatywne wyszukiwarki
- Tryb incognito i jego ograniczenia
- Tor Browser i jego zastosowanie
- Zarządzanie historią przeglądania

### Szyfrowanie komunikacji

- Podstawy kryptografii
- Protokoły szyfrowania
- End-to-end encryption
- Bezpieczne komunikatory
- Szyfrowanie poczty email
- PGP i jego implementacja
- Zarządzanie kluczami

## Moduł 8: Bezpieczeństwo urządzeń mobilnych (2.5h)

### Zabezpieczenia smartfonów

- Mechanizmy blokady urządzenia
- Szyfrowanie danych
- Aktualizacje systemu
- Zarządzanie uprawnieniami aplikacji
- Bezpieczne przechowywanie danych
- Lokalizacja i zdalne wymazywanie
- Mobile Device Management

### Bezpieczne aplikacje

- Weryfikacja bezpieczeństwa aplikacji
- Oficjalne i alternatywne sklepy z aplikacjami
- Uprawnienia aplikacji
- Aplikacje do zabezpieczania urządzenia
- Bezpieczne płatności mobilne
- Aplikacje do szyfrowania danych
- Zarządzanie hasłami na urządzeniach mobilnych

## Moduł 9: Reagowanie na incydenty (2h)

### Rozpoznawanie incydentów

- Definicja incydentu bezpieczeństwa
- Klasyfikacja incydentów
- Wskaźniki kompromitacji (IoC)
- Systemy wykrywania incydentów
- Analiza logów
- Monitoring bezpieczeństwa
- Zarządzanie alertami

**Procedury reagowania**

- Fazy reagowania na incydenty
- Izolacja systemów
- Zbieranie dowodów
- Analiza szkód
- Usuwanie zagrożenia
- Przywracanie systemów
- Dokumentacja działań

## Moduł 10: Warsztaty praktyczne (3h)

**Symulacje różnych typów ataków**

- - Phishing i social engineering
- - Złośliwe oprogramowanie
- - Ataki na hasła
- - Próby włamania do sieci
- - Ataki na aplikacje webowe
- - Zagrożenia mobilne
- - Scenariusze złożone

**Test wiedzy i umiejętności**

- Weryfikacja wiedzy teoretycznej
- Ocena umiejętności praktycznych
- Analiza przypadków
- Rozwiązywanie problemów
- Dokumentacja incydentów
- Tworzenie rekomendacji
- Plan rozwoju kompetencji

# Efekty uczenia się:

Efekty kształcenia dla szkolenia "Cyberbezpieczeństwo i ochrona wrażliwych danych" w zakresie wiedzy, umiejętności oraz kompetencji społecznych.

## WIEDZA

Po ukończeniu szkolenia uczestnik:

**1. W zakresie podstaw cyberbezpieczeństwa**

- Zna i rozumie podstawowe pojęcia z zakresu cyberbezpieczeństwa
- Identyfikuje aktualne zagrożenia w cyberprzestrzeni
- Rozumie mechanizmy działania różnych typów ataków cybernetycznych
- Zna statystyki i przykłady głośnych cyberataków

**2. W zakresie ochrony danych**

- Zna zasady tworzenia i zarządzania silnymi hasłami
- Rozumie zasady działania różnych metod uwierzytelniania
- Zna podstawy kryptografii i szyfrowania danych
- Rozumie wymagania RODO i przepisy dotyczące ochrony danych osobowych

**3. W zakresie bezpieczeństwa systemów i sieci**

- Zna architekturę zabezpieczeń sieciowych
- Rozumie zasady działania różnych typów malware
- Zna metody zabezpieczania systemów i sieci
- Rozumie zasady bezpiecznej konfiguracji urządzeń

## UMIEJĘTNOŚCI

Po ukończeniu szkolenia uczestnik potrafi:

**1. W zakresie praktycznego bezpieczeństwa**

- Tworzyć i zarządzać silnymi hasłami
- Konfigurować dwuskładnikowe uwierzytelnianie
- Prawidłowo używać menedżerów haseł
- Implementować podstawowe zabezpieczenia na urządzeniach

**2. W zakresie reagowania na zagrożenia**

- Rozpoznawać oznaki potencjalnego ataku
- Przeprowadzać podstawową analizę incydentów
- Podejmować odpowiednie działania w przypadku naruszenia bezpieczeństwa
- Dokumentować i raportować incydenty bezpieczeństwa

**3. W zakresie ochrony organizacji**

- Wdrażać polityki bezpieczeństwa informacji
- Przeprowadzać klasyfikację danych
- Zarządzać uprawnieniami użytkowników
- Implementować procedury bezpieczeństwa

# KOMPETENCJE SPOŁECZNE

Po ukończeniu szkolenia uczestnik:

**1. W zakresie świadomości bezpieczeństwa**

- Jest świadomy znaczenia cyberbezpieczeństwa w organizacji
- Rozumie odpowiedzialność związaną z ochroną danych
- Wykazuje proaktywną postawę wobec zagrożeń
- Promuje kulturę bezpieczeństwa w swoim środowisku

**2. W zakresie komunikacji**

- Potrafi efektywnie komunikować zagadnienia bezpieczeństwa
- Umie współpracować w zespole podczas incydentów
- Skutecznie przekazuje wiedzę innym pracownikom
- Potrafi jasno raportować problemy bezpieczeństwa

**3. W zakresie rozwoju zawodowego**

- Jest gotów do ciągłego aktualizowania swojej wiedzy
- Wykazuje inicjatywę w zakresie podnoszenia kwalifikacji
- Potrafi adaptować się do nowych zagrożeń i technologii
- Dzieli się wiedzą i doświadczeniem z innymi

**4. W zakresie etyki i odpowiedzialności**

- Rozumie etyczne aspekty cyberbezpieczeństwa
- Jest świadomy konsekwencji naruszeń bezpieczeństwa
- Zachowuje poufność informacji wrażliwych
- Działa zgodnie z przyjętymi procedurami i regulacjami