MATERIAŁ DLA UCZNIA / SPRAWDZIAN NR 1

POWTÓRZENIE WIADOMOŚCI

Podstawy cyberbezpieczeństwa systemów IT

KLASA 1 • TECHNIK CYBERBEZPIECZEŃSTWA

Co obejmuje sprawdzian?

Pięć bloków materiału zrealizowanych przed pierwszym sprawdzianem. Dokument porządkuje definicje, rodzaje zagrożeń, przykłady incydentów oraz zasady bezpiecznego reagowania.

01	**BHP i bezpieczna praca w pracowni**	INF.11.1: 4.3
02	**Pojęcia, triada CIA i legalność działań**	INF.11.2: 1.1–1.5
03	**Zagrożenia, podatności, malware**	INF.11.2: 2.1, 2.2, 2.3b
04	**Włamania, cele ataków, DoS/DDoS**	INF.11.2: 2.3a, 2.3c, 2.4
05	**Ataki fizyczne i scenariusze ataków**	INF.11.2: 2.3d, 2.5

Jak korzystać z tego pliku?

Najpierw naucz się znaczenia pojęć. Następnie przećwicz rozpoznawanie sytuacji: **co jest zagrożone → jaka jest słabość → jaki to rodzaj ataku → jaki skutek → co zrobić bezpiecznie**. Na końcu znajdziesz listę wymagań do samosprawdzenia.

ZSP Niemce • Materiał powtórzeniowy • Listopad 2026

INF.11.1 • KRYTERIUM 4.3

01 BHP w pracowni bezpieczeństwa

Najważniejsze: bezpieczna obsługa komputerów i urządzeń, przestrzeganie zasad BHP oraz ochrona zdrowia i sprzętu.

Bezpieczne stanowisko

Obszar	Prawidłowe postępowanie
Ergonomia	Ustaw monitor na wprost, dbaj o wygodne podparcie pleców, ustaw wysokość krzesła i rób przerwy od długiej pracy przy ekranie.
Energia elektryczna	Nie dotykaj uszkodzonych przewodów, nie otwieraj zasilacza i nie manipuluj przy urządzeniach pod napięciem. Awarię zgłoś nauczycielowi.
Porządek i płyny	Nie stawiaj napojów przy sprzęcie; nie blokuj wentylacji urządzeń; nie pozostawiaj kabli w przejściach.
Sprzęt komputerowy	Nie rozkręcaj komputerów, nie przepinaj kabli i nie podłączaj nośników lub urządzeń bez zgody prowadzącego.
Dane i konta	Nie udostępniaj haseł, blokuj ekran po odejściu, nie instaluj oprogramowania bez pozwolenia.

Wypadek, dym, przegrzanie – co robić?

- **Przerwij pracę**, ostrzeż innych i nie podejmuj ryzykownych prób naprawy.
- **Powiadom nauczyciela**; stosuj się do instrukcji i procedury ewakuacji.
- W przypadku zagrożenia zdrowia lub życia wezwanie pomocy odbywa się zgodnie z procedurą szkoły; numer alarmowy to **112**.
- W razie pożaru sprzętu elektrycznego nie używaj wody na urządzenia znajdujące się pod napięciem. Dobór i użycie gaśnicy należy do przeszkolonych osób.

Zapamiętaj

W pracowni bezpieczeństwo człowieka jest ważniejsze niż komputer i dane. Gdy zauważysz zagrożenie, **nie improwizuj** i **zgłoś je nauczycielowi**.

INF.11.2 • KRYTERIA 1.1–1.4

02 Pojęcia i triada CIA

Triada CIA to podstawowy model opisujący, co powinniśmy chronić w systemie informatycznym.

C

POUFNOŚĆ

Poufne dane i konta

I

INTEGRALNOŚĆ

Poprawność informacji

A

DOSTĘPNOŚĆ

Usługa gotowa do pracy

Co oznaczają trzy litery?

Cel	Znaczenie	Przykładowe naruszenie
C – Confidentiality	**Poufność**: dane widzą wyłącznie uprawnione osoby.	Ktoś odczytuje dane uczniów bez pozwolenia.
I – Integrity	**Integralność**: dane są poprawne i nie zostały zmienione bez uprawnienia.	Napastnik podmienia ocenę w dzienniku.
A – Availability	**Dostępność**: usługa i dane działają, gdy są potrzebne.	Serwer jest przeciążony i uczniowie nie mogą się zalogować.

Słowniczek podstawowy

- **Cyberbezpieczeństwo** – ochrona systemów, sieci, urządzeń i informacji przed zagrożeniami oraz ograniczanie skutków incydentów.
- **Cyberatak** – celowe działanie wymierzone w bezpieczeństwo systemu, sieci lub danych; próba może się nie powieść.
- **Zasób** – to, co chronimy, np. konto ucznia, plik, kopia zapasowa, serwer, dane osobowe.
- **Incydent** – zdarzenie naruszające lub mogące naruszać bezpieczeństwo, które należy wyjaśnić; nie każdy incydent to atak.
- **Włamanie** – uzyskanie lub próba uzyskania nieuprawnionego dostępu; nie każde zakłócenie usługi jest włamaniem.

Jedno zdarzenie może naruszać kilka elementów CIA

Ransomware może uniemożliwiać odczyt plików (**A**) i jednocześnie kraść dane (**C**). Nieuprawniona zmiana pliku narusza przede wszystkim **I**. Sama awaria serwera zagraża **A**, ale nie musi być cyberatakiem.

INF.11.2 • KRYTERIUM 1.5

03 Legalność działań i etyka

Bezpieczeństwo IT nie polega na wykonywaniu dowolnych testów. Kluczowe są zgoda, uprawnienia i zakres działania.

Kiedy test jest uprawniony?



Etyczny specjalista sprawdza wyłącznie systemy i funkcje, do których ma upoważnienie, działa zgodnie z ustalonym zakresem oraz odpowiedzialnie zgłasza wykryte problemy. Samo posiadanie narzędzia nie stanowi upoważnienia.

Sytuacja	Ocena i uzasadnienie
Uczeń bada swoją maszynę wirtualną w dozwolonym ćwiczeniu.	Dopuszczalne w zakresie zgody i zasad pracowni.
Uczeń próbuje odgadnąć hasło kolegi „dla żartu”.	Niedopuszczalne: brak upoważnienia.
Administrator testuje usługę zgodnie z pisemnym zleceniem.	Uprawnione, jeśli działa w granicach ustalonego zakresu.
Ktoś skanuje obcy serwer, twierdząc, że chce pomóc.	Nie należy zakładać legalności; brak zgody lub przekroczenie uprawnień może naruszać prawo.

Trzy pojęcia, których nie wolno mylić

Pojęcie	Ważne rozróżnienie
Błąd / awaria	Serwer przestał odpowiadać po aktualizacji. Nie ma dowodu celowego działania napastnika.
Próba cyberataku	W logach widać próby nieuprawnionego dostępu, ale żadna nie zakończyła się zalogowaniem.
Udane włamanie	Potwierdzono nieuprawnione zalogowanie do konta lub systemu.

Zasada obowiązująca w pracowni

Analizujemy fikcyjne scenariusze i ćwiczymy wyłącznie w wyznaczonym środowisku. Nie skanujemy cudzych urządzeń, nie podejmujemy prób logowania na obce konta i nie uruchamiamy szkodliwego kodu.

INF.11.2 • KRYTERIA 2.1–2.2

04 Zagrożenia, podatności i ryzyko

Na sprawdzianie szczególnie ważne będzie odróżnienie **zagrożenia** od **podatności**.

Pojęcie	Wyjaśnienie	Przykład
Zagrożenie	Potencjalna przyczyna szkody dla zasobu.	Kradzież danych, awaria dysku, nieuprawniony dostęp.
Podatność	Słabość systemu, konfiguracji, człowieka lub procedury.	Domyślne hasło, nieaktualny system, otwarte drzwi do serwerowni.
Ryzyko	Ocena możliwości wystąpienia szkody i wielkości jej skutków.	Wysokie, gdy ważna usługa ma łatwą do wykorzystania lukę.
Incydent	Zdarzenie wymagające reakcji lub sprawdzenia.	Potwierdzone zalogowanie na obce konto.

Jak łączą się te pojęcia?



Przykład: szkolny panel administracyjny (**zasób**) ma hasło „admin123” (**podatność**). Osoba nieuprawniona może spróbować się zalogować (**zagrożenie / próba ataku**) i zmienić dane (**skutek: naruszenie integralności**).

Wewnętrzne czy zewnętrzne?

Źródło	Przykłady
Wewnętrzne	Błąd pracownika, zbyt szerokie uprawnienia, zgubienie służbowego pendrive’a, celowe działanie osoby z dostępem.
Zewnętrzne	Oszust wysyłający e-mail, napastnik atakujący publiczny serwer, złośliwy kod pobrany z Internetu.

Nie każde niebezpieczeństwo to działalność napastnika

Zagrożeniem może być również **usterka sprzętu, pożar, zalanie, przerwa w dostawie prądu albo błąd użytkownika**. Nie należy diagnozować infekcji wyłącznie na podstawie wolnej pracy komputera czy braku dostępu do strony.

Pytanie diagnostyczne

Co jest słabością? – otwarta serwerownia. **Co może się zdarzyć?** – ktoś wyniesie dysk. **Co stracimy?** – poufność danych lub dostępność plików.

INF.11.2 • KRYTERIUM 2.3B

05 Złośliwe oprogramowanie (malware)

Malware to ogólne określenie programów służących szkodliwym działaniom. Jego kategorie mogą się nakładać.

Rodzaj	Charakterystyczne działanie	Skojarzenie
Wirus	Dołącza kod do plików lub programów i rozprzestrzenia się wraz z nimi.	Infekuje pliki.
Robak (worm)	Samodzielnie replikuje się i może przenosić się przez sieć.	Rozprzestrzenia się bez dołączania do gospodarza.
Trojan	Udaje zaufany lub przydatny program, aby skłonić ofiarę do uruchomienia.	Fałszywa aplikacja.
Ransomware	Blokuje dostęp do danych, często je szyfruje, i stosuje wymuszenie okupu.	Żądanie zapłaty.
Spyware	Potajemnie zbiera informacje o użytkowniku.	Szpiegowanie.
Keylogger	Rejestruje wciskane klawisze; złośliwa wersja może kraść hasła.	Przechwytywanie wpisywanych danych.
Backdoor	Pozwala ominąć normalną kontrolę dostępu lub utrzymać ukryty dostęp.	Ukryte wejście.
Bot / botnet	Złośliwy bot wykonuje polecenia operatora; botnet to grupa przejętych urządzeń.	Może służyć do DDoS.

Drogi infekcji i ochrona

Typowe drogi: niebezpieczny załącznik, fałszywa instalacja, nieznany nośnik USB, wykorzystanie niezałatanej podatności. **Ochrona:** aktualizacje, ostrożność przy plikach, ograniczone uprawnienia, ochrona punktów końcowych i sprawdzane kopie zapasowe.

Trzy bardzo częste pomyłki

Phishing jest metodą oszustwa, a nie rodzajem malware. **Trojan** nie musi samodzielnie się rozprzestrzeniać. **Ransomware** nie zawsze oznacza wyłącznie szyfrowanie – może wystąpić także kradzież danych.

INF.11.2 • KRYTERIA 2.3A I 2.4

06 Włamania sieciowe i cele ataków

Cel atakującego nie zawsze jest tym samym, co obserwowany skutek. Analiza powinna opierać się na dowodach.

Włamanie a atak na dostępność

Zdarzenie	Najważniejszy cel lub mechanizm
Włamanie sieciowe	Uzyskanie nieuprawnionego dostępu, np. do konta, urządzenia, usługi albo danych.
DoS / DDoS	Zakłócenie działania systemu bez konieczności włamywania się lub kradzieży informacji.
Atak malware	Użycie szkodliwego oprogramowania: kradzież, sabotaż, wymuszenie lub przejęcie urządzenia.

Pięć celów i skutków wymienionych w podstawie

Cel / skutek	Przykładowa sytuacja	CIA
Pozyskanie informacji	Ktoś kopiuje poufne dane uczniów.	C
Modyfikacja danych	Napastnik zmienia kwotę przelewu lub ocenę.	I
Kradzież tożsamości	Osoba podszywa się pod właściciela konta, wykorzystując jego dane.	C / I
Zakłócenie działania	Platforma edukacyjna staje się niedostępna wskutek przeciążenia.	A
Wymuszenie okupu	Sprawca grozi nieodblokowaniem danych albo ich ujawnieniem.	A / C

Co może wskazywać na próbę włamania?

- Wiele nieudanych logowań, logowanie z nietypowego miejsca lub nowo nadane nieznane uprawnienia.
- Nieautoryzowane modyfikacje plików albo zmiany konfiguracji usług.
- Nietypowe zdarzenia odnotowane w **logach**, czyli dziennikach zdarzeń systemu.

Ostrożność we wnioskowaniu

Pojedynczy adres IP, jedna awaria albo nieudane logowanie nie wystarczają do ustalenia sprawcy lub potwierdzenia włamania. Najpierw zbiera się fakty, dopiero później formułuje hipotezy.

INF.11.2 • KRYTERIUM 2.3C

07 Ataki DoS i DDoS

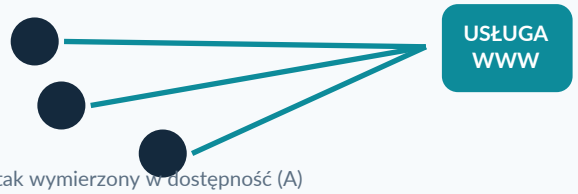
DoS i DDoS uderzają przede wszystkim w dostępność usługi, czyli element A triady CIA.

DoS • jedno źródło



Atak wymierzony w dostępność (A)

DDoS • wiele źródeł



Atak wymierzony w dostępność (A)

DoS (Denial of Service) – próba uniemożliwienia korzystania z usługi. **DDoS (Distributed Denial of Service)** – podobny cel, ale ruch lub działania pochodzą z wielu źródeł, często z urządzeń botnetu.

Przykładowe mechanizmy – zrozumienie, nie wykonywanie

Mechanizm	Co zostaje obciążone?
HTTP flood	Aplikacja WWW musi przetwarzać nadmierną liczbę żądań.
SYN flood	Zasoby związane z obsługą prób nawiązywania połączeń TCP.
UDP flood	Przepustowość łącza lub zasoby urządzeń i sieci.
Amplification	Wykorzystanie pewnych usług do uzyskania odpowiedzi o większej objętości niż wysyłane zapytanie.

Objawy i wskaźniki

Można zauważyć wysokie opóźnienia, błędy 503/504, niedostępność WWW, wzrost liczby żądań na sekundę (**RPS**), pakietów na sekundę (**pps**) lub wykorzystania łącza (**bps**). **Uwaga:** podobny wzrost ruchu może być całkowicie legalny, np. w dniu ogłoszenia wyników.

Obrona i ograniczanie skutków

Mechanizm ochrony	Rola
Rate limiting	Ogranicza częstotliwość żądań lub prób z danego źródła według reguł.
WAF	Filtruje ruch do aplikacji WWW na podstawie reguł.
CDN / cache	Rozkłada ruch i pozwala obsługiwać część treści z pamięci podręcznej.
Monitoring / operator ISP	Pozwala rozpoznać anomalię i wspólnie ograniczać duży ruch sieciowy.

INF.11.2 • KRYTERIUM 2.3D

08 Ataki fizyczne i sprzętowe

Do incydentu nie trzeba zaawansowanego programu. Czasem wystarczy dostęp do urządzenia, pomieszczenia lub nośnika.

Sytuacja	Ryzyko	Jak się chronić?
Kradzież laptopa lub dysku	Ujawnienie informacji; utrata dostępu do danych.	Kontrola dostępu, szyfrowanie urządzeń, kopie zapasowe.
Znaleziony pendrive USB	Możliwy szkodliwy plik lub niebezpieczne urządzenie.	Nie podłączaj, nie otwieraj plików, przekaż nauczycielowi.
Odblokowany komputer	Ktoś może zobaczyć, skopiować lub zmienić dane.	Blokuj ekran po odejściu; nie pozwalaj korzystać ze swojego konta.
Osoba obca w serwerowni	Może odłączyć urządzenia lub uzyskać dostęp do sprzętu.	Kontrola wejść, zamki, nadzór, zasada ograniczonego dostępu.
Podejrzane urządzenie przy kablach	Możliwy podsłuch lub zakłócenie komunikacji.	Nie manipuluj sam; zgłoś nieznany element administratorowi.
Uszkodzenie, zalanie lub przegrzanie	Przerwa w pracy, utrata lub uszkodzenie danych.	Porządek, wentylacja, nadzór nad zasilaniem, kopie.

Dwie formy ochrony działają razem

Fizyczna	Cyfrowa
Zamknięte pomieszczenia, nadzór, bezpieczne szafy, ewidencja sprzętu.	Szyfrowanie nośników, hasła, blokada ekranu, kopie zapasowe, monitoring zdarzeń.

Przykład ważny na sprawdzian

Gdy ktoś wynosi niezabezpieczony pendrive z bazą danych szkoły, zagrożona jest przede wszystkim **poufność (C)**. Gdy odłącza zasilanie serwera, zagrożona jest **dostępność (A)**.

INF.11.2 • KRYTERIUM 2.5

09 Cztery scenariusze ataków

Podstawa programowa wymienia cztery proste scenariusze. Umiej je rozpoznać, opisać zagrożenie i bezpieczną reakcję.

1. Fałszywy e-mail (phishing)

Sytuacja: Uczeń dostaje wiadomość: „Twoje konto zostanie zamknięte. Otwórz link i wpisz hasło”.

Na czym polega zagrożenie? Próba wyłudzenia informacji i uzyskania dostępu do konta.

Bezpieczna reakcja: Nie używaj linku; sprawdź sprawę niezależnym kanałem i zgłoś wiadomość. • **CIA: C, potencjalnie I**

2. Podrzucony nośnik USB

Sytuacja: Na korytarzu ktoś znajduje pendrive oznaczony „Wyniki egzaminów”.

Na czym polega zagrożenie? Ciekawość może skłonić do uruchomienia złośliwego pliku lub podłączenia niebezpiecznego urządzenia.

Bezpieczna reakcja: Nie podłączaj nośnika. Przekaż go nauczycielowi/administratorowi. • **CIA: C / I / A**

3. Automatyczne próby łamania haseł

Sytuacja: W logach konta widać setki nieudanych prób logowania w krótkim czasie.

Na czym polega zagrożenie? Możliwy atak na uwierzytelnianie, szczególnie groźny przy prostych lub powtarzanych hasłach.

Bezpieczna reakcja: Zgłoś zdarzenie; administrator analizuje logi i stosuje zabezpieczenia, np. limity prób oraz MFA. • **CIA: C / I**

4. Podsłuch komunikacji

Sytuacja: Nieuprawniona osoba może przechwytywać informacje podczas transmisji.

Na czym polega zagrożenie? Ujawnienie przesyłanych danych, szczególnie gdy komunikacja jest słabo zabezpieczona.

Bezpieczna reakcja: Korzystaj z bezpiecznych połączeń, nie udostępniaj danych w podejrzanej sieci; zgłoś problem. • **CIA: C**

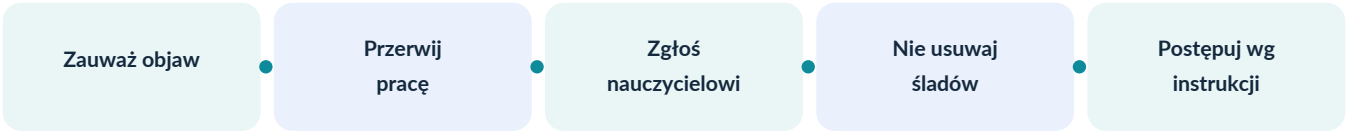
Szczegółowa analiza technik socjotechnicznych będzie osobnym działem. W tym powtórzeniu liczy się rozpoznanie powyższych scenariuszy.

POŁĄCZENIE WSZYSTKICH POZNANYCH TREŚCI

10 Reagowanie na incydent

Twoim zadaniem nie jest samodzielne „odwetowe” działanie, lecz ochrona bezpieczeństwa i poprawne zgłoszenie.

Co powinien zrobić uczeń w pracowni?



Prawidłowe zgłoszenie zawiera: **stanowisko, czas, zaobserwowane objawy i podjęte działania**. Nie należy dopisywać przypuszczeń jako pewnych faktów. Dalsze czynności, takie jak izolacja komputera od sieci, analiza logów i odtwarzanie systemu, koordynuje nauczyciel lub administrator.

Przykład z wcześniejszej lekcji: stanowisko P-07

Informacja	Fakt czy hipoteza?
Na ekranie komputera pojawił się komunikat z żądaniem okupu.	**Fakt** – jeśli został rzeczywiście zaobserwowany.
Na komputer przyszedł załącznik „plan_lekcji.pdf.exe”.	**Fakt** – jeśli potwierdza to zapis poczty; sam załącznik nie dowodzi wykonania.
Wszyscy uczniowie mają już zaszyfrowane pliki.	**Hipoteza**, dopóki nie sprawdzono zasięgu problemu.
Sprawca na pewno dostał się przez e-mail.	**Hipoteza** – droga infekcji wymaga ustalenia.

Czego nie robić?

- Nie kasuj podejrzanych plików i logów „na wszelki wypadek”; nie uruchamiaj ponownie komputera bez polecenia osoby odpowiedzialnej.
- Nie podłączaj dysku z kopią zapasową do podejrzanego urządzenia.
- Nie pobieraj próbek szkodliwego oprogramowania ani nie uruchamiaj testów na prawdziwej sieci szkoły.

Warstwy ochrony

Aktualizacje zmniejszają liczbę znanych podatności. **Ochrona kont i ograniczone uprawnienia** utrudniają nadużycia. **Monitoring** pomaga wykrywać incydenty. **Kopie zapasowe** wspomagają odtworzenie danych – muszą być bezpieczne i sprawdzane.

PRZYKŁADY Z OBJAŚNIENIAMI

11 Rozpoznaj sytuację

Na sprawdzianie możesz otrzymać opis zdarzenia zamiast samej definicji. Ćwicz poprawne rozpoznawanie.

Nr	Opis	Wniosek
A	Hasło konta administratora nadal ma fabryczną wartość.	Podatność; jeszcze nie dowód włamania.
B	Nieznajomy odczytuje prywatne dane uczniów.	Naruszenie poufności (C).
C	Ktoś nielegalnie zmienia oceny w e-dzienniku.	Naruszenie integralności (I).
D	Wiele przejętych urządzeń przeciąża stronę szkoły.	DDoS; naruszona dostępność (A).
E	Program udaje instalator i zbiera zapisane hasła.	Trojan / spyware – kategorie mogą się łączyć.
F	System jest wolny w dniu zapisów na konkurs.	Może to być legalny ruch, nie ma dowodu DoS.
G	Ktoś zostawia USB pod drzwiami pracowni.	Możliwy atak fizyczny z użyciem nośnika; nie podłączaj.
H	Nieznany człowiek wchodzi do pomieszczenia z serwerami.	Naruszenie kontroli fizycznej / potencjalne zagrożenie.
I	W logach pojawia się 400 nieudanych logowań.	Podejrzenie automatycznej próby łamania hasła; sprawdź logi.
J	Uczeń sprawdza hasła kolegi bez pytania.	Brak autoryzacji; zachowanie niedopuszczalne.
K	Program szyfruje dane i żąda zapłaty.	Ransomware; przede wszystkim A, możliwe także C.
L	Napastnik przechwytuje informacje przesyłane siecią.	Podsłuch; naruszenie poufności (C).

Metoda analizy

Przy nowym opisie odpowiedz po kolei: **(1) Co się stało? (2) Jaki zasób? (3) Jaki rodzaj zagrożenia/ataku? (4) C, I czy A? (5) Jaka bezpieczna reakcja?** Dzięki temu nie opierasz odpowiedzi na jednym słowie-kluczu.

SAMODZIELNE POWTÓRZENIE

12 Lista kontrolna przed sprawdzianem

Zaznacz każde zagadnienie, które potrafisz wyjaśnić własnymi słowami i zastosować w krótkim przykładzie.

BHP • INF.11.1 (4.3)

□ Wskazuję bezpieczne zachowania przy komputerze i przewodach.

□ Wiem, co zrobić po zauważeniu zagrożenia dla zdrowia lub sprzętu.

Terminologia i etyka • INF.11.2 (1.1–1.5)

□ Wyjaśniam cyberbezpieczeństwo, cyberatak, zasób i incydent.

□ Rozwijam skrót CIA i rozpoznaję naruszenie C, I oraz A.

□ Wiem, dlaczego zgoda i zakres upoważnienia są konieczne.

Zagrożenia i malware • INF.11.2 (2.1, 2.2, 2.3b)

□ Odróżniam zagrożenie od podatności i potrafię podać przykład.

□ Rozróżniam zagrożenia wewnętrzne i zewnętrzne.

□ Rozpoznaję wirusa, robaka, trojana, ransomware, spyware i backdoor.

□ Wiem, czym jest botnet i dlaczego phishing nie jest nazwą malware.

Włamania i DoS/DDoS • INF.11.2 (2.3a, 2.3c, 2.4)

□ Rozpoznaję włamanie, DoS, DDoS i ich różne cele.

□ Wymieniam pięć celów/skutków ataków wskazanych w podstawie.

□ Wyjaśniam znaczenie rate limiting, WAF, CDN i monitoringu.

□ Rozumiem, że wzrost ruchu sam w sobie nie dowodzi ataku.

Fizyczne zagrożenia i scenariusze • INF.11.2 (2.3d, 2.5)

□ Rozpoznaję zagrożenia związane z laptopem, serwerownią i nośnikami.

□ Wiem, jak postąpić ze znalezionym nośnikiem USB.

□ Opisuję cztery scenariusze: phishing, USB, próby haseł i podsłuch.

□ Potrafię odróżnić fakty od hipotez i prawidłowo zgłosić incydent.

Ostatnia powtórka

Najważniejsze rozróżnienia: **zagrożenie ≠ podatność**; **atak ≠ włamanie**; **DoS ≠ DDoS**; **phishing ≠ malware**; **fakt ≠ hipoteza**; **autoryzacja ≠ posiadanie narzędzia**.

DLA UCZNIA I NAUCZYCIELA

13 Mapa zakresu i źródła

Powtórzenie opiera się na zrealizowanych tematach i wybranych kryteriach z podstawy zawodowej INF.11.

Powiązanie z tematami w dzienniku

Temat z dziennika	Zakres powtórzenia
BHP w pracowni	Strona 2 • obsługa sprzętu i bezpieczne postępowanie.
Terminologia, CIA, legalność	Strony 3–4 • definicje, poufność, integralność, dostępność, uprawnienia.
Zagrożenia i malware	Strony 5–6 • zagrożenie/podatność, źródła, rodzaje malware.
Ataki sieciowe i DoS	Strony 7–8 • włamania, cele, DoS/DDoS, obrona.
Ataki fizyczne i sprzętowe	Strony 9–10 • fizyczny dostęp, USB, scenariusze 2.5.
Utrwalenie wiadomości	Strony 11–13 • reakcja, przykłady, lista kontrolna.

Podstawowe materiały

- Rozkład materiału i wymagania edukacyjne z przedmiotu **Podstawy cyberbezpieczeństwa systemów IT**, ZSP Niemce, rok szkolny 2026/2027.
- Wcześniejsze materiały do lekcji: „Zagrożenia IT, podatności i złośliwe oprogramowanie” oraz „Analiza celów i skutków ataków sieciowych, włamania, ataki DoS”.
- Podstawa programowa kształcenia w zawodzie **technik cyberbezpieczeństwa**, kwalifikacja INF.11, jednostki INF.11.1 i INF.11.2, według aktualnych przepisów szkolnictwa branżowego.

Oficjalny akt prawny

Rozporządzenie Ministra Edukacji z 22 czerwca 2026 r. zmieniające rozporządzenie w sprawie podstaw programowych kształcenia w zawodach szkolnictwa branżowego (Dz.U. z 2026 r. poz. 1009). https://dziennikustaw.gov.pl/DU/2026/1009

Zakres sprawdzianu jest zamknięty

Materiał kończy się na zagadnieniach wymienionych przed **Sprawdzianem 1** w dzienniku. Rozwinięta socjotechnika, MFA, kryptografia i administracja sieciami będą odrębnymi częściami kursu.

Opracowanie: materiał edukacyjny do powtarzania wiadomości • ZSP Niemce • 2026