**Imię i nazwisko:** _____ **Data:** _____ **Wynik:** _____

# Podstawy cyberbezpieczeństwa i zagrożenia online Zapobieganie

Zagrożenia cyberbezpieczeństwa, zapory sieciowe, uwierzytelnianie wieloskładnikowe, ramy bezpieczeństwa

## PRZEGLĄD NAUKI: PODSTAWY CYBERBEZPIECZEŃSTWA

**CHRONIONY**
**SZYFROWANIE DANYCH**
Standard AES 256-bitowy

**ZGODNY**
**STANDARDY GLOBALNE**
Ramy prawne RODO (GDPR) i CCPA

**ZERO TRUST**
**POLITYKA DOSTĘPU**
Uwierzytelnianie wieloskładnikowe

**Witaj!** Ten pakiet ćwiczeń przeprowadzi cię przez podstawowe zasady cyberbezpieczeństwa i zapobiegania zagrożeniom online. Poznasz zagrożenia ze strony złośliwego oprogramowania, uwierzytelnianie wieloskładnikowe, zapory sieciowe i ramy reagowania na incydenty.

### PUNKTY KONTROLNE KARTY PRACY

- [ ] **Część 1–4: Opanuj cyberbezpieczeństwo i zapobieganie zagrożeniom.**
- [ ] **Część 5–7: Rozwiąż krzyżówkę i wykreślankę.**
- [ ] **Część 8–9: Rozwiąż studia przypadków i wyzwanie z szyfrem.**
- [ ] **Część 10: Przejrzyj strony z podstawowymi i zaawansowanymi najczęściej zadawanymi pytaniami.**
- [ ] **Część 11: Poznaj 10 ciekawych faktów z praktyki.**
- [ ] **Bonus: wyzwanie Myśl szybko.**

**Otwórz przewodnik VPN.com po cyberbezpieczeństwie**

URL: https://www.vpn.com/pl/cyberbezpieczenstwo/

# Twoja ścieżka nauki: podstawy cyberbezpieczeństwa

- Rozpoznaj typowe wektory ataków złośliwego oprogramowania, phishingu i włamań do sieci firmowych.
- Wdróż standardowe zabezpieczenia cyberbezpieczeństwa, w tym MFA, zapory sieciowe i ochronę punktów końcowych.
- Oceń procedury reagowania na incydenty służące łagodzeniu skutków naruszeń danych.
- Przeanalizuj czynniki ryzyka organizacyjnego i zgodność z bezpieczeństwem według wytycznych NIST.
- Skonfiguruj praktyki higieny bezpieczeństwa, aby ograniczać zautomatyzowany credential stuffing.

## INSTRUKCJE DO PRZEWODNIKA PO CYBERBEZPIECZEŃSTWIE

Odpowiedz na pytania testu wielokrotnego wyboru oraz pytania prawda/fałsz, uzupełnij zdania z lukami za pomocą banku wyrazów, dopasuj definicje i rozwiąż krzyżówkę oraz wykreślankę. Zastosuj swoją wiedzę z zakresu zapobiegania zagrożeniom. Zakończ zadaniem dodatkowym Myśl szybko.

## PODSTAWY CYBERBEZPIECZEŃSTWA I ZAPOBIEGANIE ZAGROŻENIOM (WPROWADZENIE)

Cyberbezpieczeństwo chroni sieci, systemy i dane przed nieautoryzowanymi atakami cyfrowymi. Wypracowanie solidnych nawyków bezpieczeństwa, konfigurowanie zapór sieciowych, wymaganie uwierzytelniania wieloskładnikowego i szkolenie pracowników w rozpoznawaniu zagrożeń to podstawowe elementy obrony sieci firmowej.

**PRZECZYTAJ UWAŻNIE KAŻDY PUNKT KONTROLNY I WYBIERZ LUB NAPISZ POPRAWNĄ ODPOWIEDŹ.**

## Punkt kontrolny 1: Wyzwanie – test wielokrotnego wyboru

**1. Jaki jest główny cel ataku phishingowego?**

- A. Kradzież danych uwierzytelniających i wrażliwych danych użytkowników
- B. Poprawa widoczności witryny w wyszukiwarkach
- C. Zwiększanie przepustowości sieci
- D. Zarządzanie replikacją zapasowego centrum danych

**2. Który mechanizm zapewnia najsilniejszą ochronę konta?**

- A. Uwierzytelnianie wieloskładnikowe z użyciem kluczy sprzętowych
- B. Złożone hasła aktualizowane co trzydzieści dni
- C. Ograniczanie logowania do konta do godzin pracy
- D. Ukrywanie nazwy użytkownika konta w publicznych katalogach

**3. Co definiuje ładunek infekcji ransomware?**

- A. Szyfrowanie plików systemowych i żądanie zapłaty
- B. Po cichu rejestrowanie naciśnięć klawiszy na zdalnych serwerach
- C. Wstrzykiwanie nieautoryzowanych reklam do przeglądarek
- D. Wykorzystywanie lokalnych zasobów procesora do wydobywania kryptowalut

**4. W jaki sposób exploit typu zero-day wpływa na zabezpieczenia?**

- A. Atakuje niezałatane, nieznane luki
- B. Automatycznie wyłącza firmową zaporę sieciową
- C. Wymusza twarde ponowne uruchomienie systemu
- D. Nie wymaga żadnego budżetu na usunięcie skutków

**5. Jakie ramy regulują korporacyjne zabezpieczenia?**

- A. Wytyczne NIST Cybersecurity Framework
- B. Specyfikacje schematu dokumentów W3C HTML5
- C. Podręczniki instalacji sterowników drukarek
- D. Definicje protokołów routingu IETF

## Punkt kontrolny 2: Wyzwanie – prawda czy fałsz

**6 Pytanie (prawda/fałsz) 6**

6. Ataki phishingowe są skierowane wyłącznie przeciw osobistym kontom e-mail.

○ Prawda ○ Fałsz

**7 Pytanie (prawda/fałsz) 7**

7. Uwierzytelnianie wieloskładnikowe pomaga blokować ataki credential stuffing.

○ Prawda ○ Fałsz

**8 Pytanie (prawda/fałsz) 8**

8. Zapory sieciowe sprawdzają ruch sieciowy, aby blokować nieautoryzowany dostęp do portów.

○ Prawda ○ Fałsz

**9 Pytanie (prawda/fałsz) 9**

9. Usuwanie exploitów zero-day wymaga standardowych aktualizacji definicji antywirusowych.

○ Prawda ○ Fałsz

**10 Pytanie (prawda/fałsz) 10**

10. Honeypot to serwer-wabik używany do zwabiania cyberprzestępców.

○ Prawda ○ Fałsz

# Punkt kontrolny 3: Wstawianie kluczowych terminów

Przeczytaj każde poniższe zdanie i uzupełnij lukę poprawnym terminem z banku słów.

1. Aby filtrować ruch przychodzący, administratorzy sieci korzystają z narzędzia, jakim jest _____ .

2. Kod wykorzystujący lukę typu zero-day, który pozwala atakującemu ominąć poprawki systemu, to _____ .

3. Atakujący wysyłają sfałszowane e-maile, aby prowadzić przeciwko pracownikom kampanie oparte na technice, jaką jest _____ .

4. Ransomware, które blokuje dane użytkownika, jest destrukcyjną formą oprogramowania określanego mianem: _____ .

5. Silna _____ haseł ogranicza ryzyko kradzieży poświadczeń.

6. Aby chronić wrażliwą komunikację, użytkownicy stosują protokoły oparte na mechanizmie, jakim jest _____ .

**BANK SŁÓW**

EXPLOIT HIGIENA HONEYPOT PHISHING SZYFROWANIE WIELOCZYNNIKOWE ZAPORA SIECIOWA ZŁOŚLIWE OPROGRAMOWANIE

**Wpisz tutaj swoje odpowiedzi:**

1. 
2. 
3. 
4. 
5. 
6. 

# Punkt kontrolny 4: Dopasowywanie pojęć z zakresu bezpieczeństwa

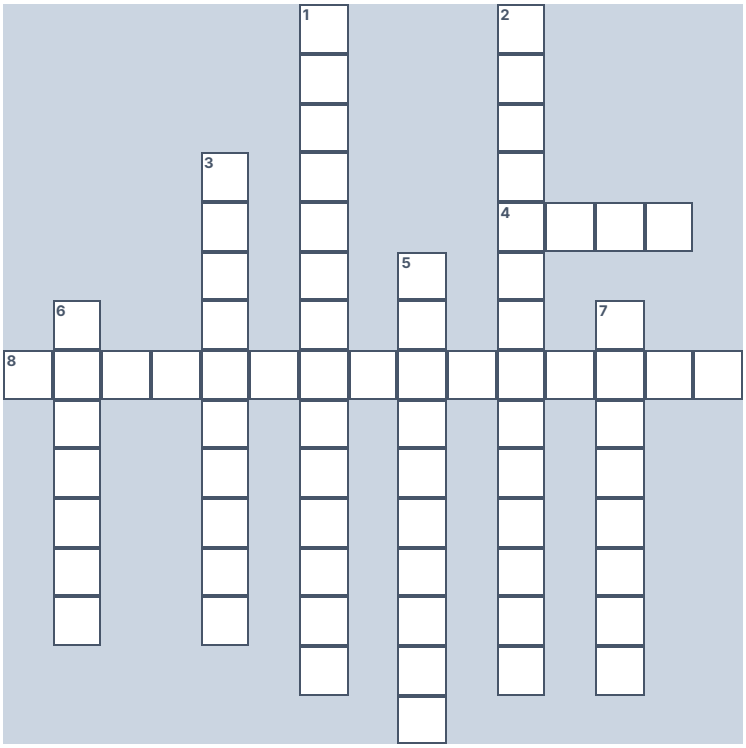
## DOPASOWYWANIE DEFINICJI

Dopasuj każde pojęcie po lewej stronie do jego poprawnej definicji po prawej, wpisując odpowiednią literę (A-H) w edytowalne pole.

| | | | |
|---|---|---|---|
| ☐ | 1. Zagrożenie ransomware | A | Ustrukturyzowane wytyczne, takie jak NIST, używane do zarządzania ryzykiem cybernetycznym. |
| ☐ | 2. Uwierzytelnianie wieloskładnikowe | B | Ustrukturyzowany plan postępowania w przypadku naruszeń bezpieczeństwa i ograniczania ich skutków. |
| ☐ | 3. Exploit typu zero-day | C | Bariera sieciowa filtrująca ruch na podstawie reguł bezpieczeństwa. |
| ☐ | 4. Przynęta typu honeypot | D | Złośliwe oprogramowanie szyfrujące dane i żądające zapłaty za ich odszyfrowanie. |
| ☐ | 5. Zapora przed włamaniami | E | Wykorzystanie luki w zabezpieczeniach przed wydaniem poprawki przez producenta. |
| ☐ | 6. Reagowanie na incydenty | F | Najlepsze praktyki zarządzania danymi uwierzytelniającymi i kluczami uwierzytelniania. |
| ☐ | 7. Higiena haseł | G | Weryfikacja bezpieczeństwa wymagająca dwóch lub więcej czynników uwierzytelniania. |
| ☐ | 8. Ramy bezpieczeństwa | H | System-przynęta, który ma zwabić i pozwolić analizować złośliwych aktorów. |

# Punkt kontrolny 5: Krzyżówka

Rozwiąż krzyżówkę, wpisując litery w aktywne białe pola. Numery odpowiadają wskazówkom poniżej.




## POZIOMO

**4. Ustrukturyzowane wytyczne, takie jak NIST, służące do zarządzania ryzykiem cybernetycznym (4)**

**8. Weryfikacja bezpieczeństwa wymagająca dwóch lub więcej czynników uwierzytelniania (15)**

## PIONOWO

**1. Exploit wykorzystujący lukę przed wydaniem poprawki przez dostawcę (14)**

**2. Bariera sieciowa filtrująca ruch według reguł bezpieczeństwa (14)**

**3. Ustrukturyzowany plan postępowania z naruszeniami bezpieczeństwa i ograniczania ich skutków (10)**

**5. Złośliwe oprogramowanie szyfrujące dane i żądające zapłaty za odszyfrowanie (10)**

**6. Najlepsze praktyki zarządzania poświadczeniami i kluczami uwierzytelniania (7)**

**7. Fałszywy system zastawiony w celu zwabienia i analizy złośliwych aktorów (8)**

# Punkt kontrolny 5, wariant alternatywny: Dostępne wskazówki do krzyżówki

Użytkownicy czytników ekranu i klawiatury mogą wpisywać odpowiedzi do krzyżówki bezpośrednio w polach tekstowych poniżej.

## POZIOMO

**4 poziomo: Ustrukturyzowane wytyczne, takie jak NIST, służące do zarządzania ryzykiem cybernetycznym (4 liter):**

**8 poziomo: Weryfikacja bezpieczeństwa wymagająca dwóch lub więcej czynników uwierzytelniania (15 liter):**

## PIONOWO

**1 pionowo: Exploit wykorzystujący lukę przed wydaniem poprawki przez dostawcę (14 liter):**

**2 pionowo: Bariera sieciowa filtrująca ruch według reguł bezpieczeństwa (14 liter):**

**3 pionowo: Ustrukturyzowany plan postępowania z naruszeniami bezpieczeństwa i ograniczania ich skutków (10 liter):**

**5 pionowo: Złośliwe oprogramowanie szyfrujące dane i żądające zapłaty za odszyfrowanie (10 liter):**

**6 pionowo: Najlepsze praktyki zarządzania poświadczeniami i kluczami uwierzytelniania (7 liter):**

**7 pionowo: Fałszywy system zastawiony w celu zwabienia i analizy złośliwych aktorów (8 liter):**

## Punkt kontrolny 6: Ukryte słowa w wykreślance

Znajdź w poniższej siatce 8 kluczowych terminów słownictwa. Wyrazy mogą biec poziomo, pionowo lub po przekątnej.

A Ę O K Ń Ć N W C Ć G I Ą Ą Ó
R Ł P W T I Ź I Ę Ź E S A G Y
X H Ę R T Ń U E K R X Ć W T S
Ł P Ł N R Ś H L L P P H O Ź Ó
Ł X H V A Y Ń O Z Q L Q I Ą A
E Ł O Ó N M N C Ą Ł O I C Ę H
I J N Ń S A Z Z B Ż I Ż E Ź I
N B E N O R V Y Y M T C I Ę G
A Ó Y X M P Q N Y G Z D S Ź I
W B P X W Ł E N G G E Ż A X E
O C O O A Q K I Y Y R R R L N
G Ż T A R N R K Ż R O M O F A
A Ś W F E Ł X O J B D Ź P C B
E Ź O V Ż O Ż W U T A Ą A H W
R P Y C N M H E Ó Y Y Ź Z Ż Y

**LISTA SŁÓW**

RANSOMWARE WIELOCZYNNIKOWE EXPLOITZERODAY HONEYPOT
ZAPORASIECIOWA REAGOWANIE HIGIENA RAMY

# Punkt kontrolny 6, wariant alternatywny: Dostępne dopasowywanie słownictwa

Dopasuj każde z 8 pojęć z wykreślanki do jego poprawnej definicji, wpisując literę (A-H) w puste pole.

**TERMINY ZE SŁOWNICZKA**

- **A. RANSOMWARE**
- **B. WIELOCZYNNIKOWE**
- **C. EXPLOITZERODAY**
- **D. HONEYPOT**
- **E. ZAPORASIECIOWA**
- **F. REAGOWANIE**
- **G. HIGIENA**
- **H. RAMY**

**DEFINICJE I POLA DOPASOWANIA**

_____ 1. Bariera sieciowa filtrująca ruch według reguł bezpieczeństwa.

_____ 2. Ustrukturyzowany plan postępowania z naruszeniami bezpieczeństwa i ograniczania ich skutków.

_____ 3. Złośliwe oprogramowanie szyfrujące dane i żądające zapłaty za odszyfrowanie.

_____ 4. Weryfikacja bezpieczeństwa wymagająca dwóch lub więcej czynników uwierzytelniania.

_____ 5. Najlepsze praktyki zarządzania poświadczeniami i kluczami uwierzytelniania.

_____ 6. Ustrukturyzowane wytyczne, takie jak NIST, służące do zarządzania ryzykiem cybernetycznym.

_____ 7. Exploit wykorzystujący lukę przed wydaniem poprawki przez dostawcę.

_____ 8. Fałszywy system zastawiony w celu zwabienia i analizy złośliwych aktorów.

## Punkt kontrolny 7: Wyzwanie – pomieszane słowa

Rozszyfruj poniższe litery, aby odkryć kluczowe pojęcia i terminy związane z cyberbezpieczeństwem. Wpisz odpowiedzi w przygotowanych polach.

1. RWMOARAESN
2. OXIPTAEDZY ROEL
3. ZEAWIACIPSR AOO
4. AIEINHG
5. EILWONNCEZ KYIWO
6. OTEPHYON
7. EGRAWNIEOA
8. RYMA

# Zadanie dodatkowe: Myśl szybko

3 ODPOWIEDZI W KAŻDEJ KATEGORII. WYGRYWA OSOBA, KTÓRA PIERWSZA WYPEŁNI LISTĘ.

| | | | | |
|---|---|---|---|---|
| 1 | Zawody w cyberbezpieczeństwie | | | |
| 2 | Powody, dla których warto aktualizować oprogramowanie | | | |
| 3 | Rzeczy, które może blokować zapora sieciowa | | | |
| 4 | Sygnały ostrzegawcze w e-mailu | | | |
| 5 | Rzeczy, z których robisz kopie zapasowe | | | |
| 6 | Dobrze znane rodzaje cyberataków | | | |
| 7 | Rzeczy, które może zwabić honeypot | | | |
| 8 | Informacje, których nigdy nie powinieneś udostępniać | | | |
| 9 | Oznaki, że komputer jest zainfekowany | | | |
| 10 | Filmy lub seriale o hakerach | | | |
| 11 | Warstwy zabezpieczeń, które możesz zbudować | | | |
| 12 | Rzeczy do przećwiczenia podczas ćwiczeń z zakresu bezpieczeństwa | | | |
| 13 | Narzędzia bezpieczeństwa, które znasz | | | |
| 14 | Osoby, które możesz poprosić o pomoc IT | | | |
| 15 | Słowa zaczynające się od „cyber” | | | |

# Punkt kontrolny 8: Studia przypadków z cyberbezpieczeństwa

Zastosuj poznane pojęcia, aby rozwiązać poniższe scenariusze z życia wzięte.

## STUDIUM PRZYPADKU 1: STRATEGIA ODZYSKIWANIA PO RANSOMWARE

👷

**Scenariusz:** Sieć firmowa została zainfekowana ransomware, które zablokowało krytyczne bazy danych. Atakujący żądają okupu w kryptowalucie w wysokości 100 000 USD. Firma ma kopie zapasowe offline sprzed 24 godzin.

**Pytanie do dyskusji: Przeanalizuj ryzyka związane z zapłatą i oceń strategię odzyskiwania.**

## STUDIUM PRZYPADKU 2: OBRONA PRZED CREDENTIAL STUFFING

👷

**Scenariusz:** Usługa online doświadcza ataku credential stuffing, w którym hakerzy testują miliony par nazwa użytkownika/hasło skradzionych z innych witryn.

**Pytanie do dyskusji:** Opisz szczegółowo mechanizm tego ataku i wskaż dwa systemy obrony.

# Punkt kontrolny 9: Odszyfruj szyfr

Specjalista ds. cyberbezpieczeństwa chroni zasoby sieciowe przed cyberprzestępcami. Użyj poniższego klucza liter i liczb, aby odszyfrować wiadomość, wpisując pasujące litery w puste miejsca.

**KLUCZ SZYFROWANIA LITERA-LICZBA**

A=1 Ą=2 B=3 C=4 Ć=5 D=6 E=7 Ę=8 F=9 G=10 H=11 I=12
J=13 K=14 L=15 Ł=16 M=17 N=18 Ń=19 O=20 Ó=21 P=22 Q=23 R=24
S=25 Ś=26 T=27 U=28 V=29 W=30 X=31 Y=32 Z=33 Ź=34 Ż=35

| 4 | 11 | 24 | 20 | 19 | | 25 | 32 | 25 | 27 | 7 | 17 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | |

| 28 | 30 | 12 | 7 | 24 | 33 | 32 | 27 | 7 | 15 | 18 | 12 | 1 | 18 | 12 | 7 | 17 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | |

| 30 | 12 | 7 | 15 | 20 | 4 | 33 | 32 | 18 | 18 | 12 | 14 | 20 | 30 | 32 | 17 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | |

**Odszyfrowana wiadomość:**

WSKAZÓWKA: KAŻDA LICZBA OZNACZA POZYCJĘ TEJ LITERY W ALFABECIE (NP. 1 = A, 2 = B, 35 = Ż).

# Punkt kontrolny 10: Podstawowe najczęściej zadawane pytania o cyberbezpieczeństwo (Część A)

Przejrzyj typowe pytania i odpowiedzi dotyczące ograniczania zagrożeń w sieci.

### Q1: Jaki jest główny cel cyberbezpieczeństwa?

Głównym celem jest ochrona sieci, urządzeń i danych przed nieautoryzowanym dostępem, atakami i przypadkowymi uszkodzeniami.

### Q2: Czym phishing różni się od spear phishingu?

Phishing to szeroka kampania e-mailowa kierowana do przypadkowych użytkowników, natomiast spear phishing jest skierowany do konkretnych osób z użyciem spersonalizowanych danych.

### Q3: Czym jest sieciowa zapora (firewall)?

Zapora sieciowa to system bezpieczeństwa sieci, który monitoruje i filtruje ruch przychodzący i wychodzący na podstawie wstępnie zdefiniowanych reguł bezpieczeństwa.

### Q4: Dlaczego uwierzytelnianie wieloskładnikowe (MFA) jest konieczne?

MFA dodaje kluczową warstwę ochrony, uniemożliwiając dostęp nawet wtedy, gdy atakujący ukradną lub złamią główne dane uwierzytelniające hasła.

### Q5: Co definiuje wirusa komputerowego?

Wirus to samoreplikujące się złośliwe oprogramowanie, które dołącza się do czystych plików i rozprzestrzenia się w systemach po ich uruchomieniu.

# Punkt kontrolny 10: Podstawowe najczęściej zadawane pytania o cyberbezpieczeństwo (Część B)

Przejrzyj typowe pytania i odpowiedzi dotyczące ograniczania zagrożeń w sieci.

### Q6: Jak ransomware blokuje dane lokalne?

Ransomware używa algorytmów kryptograficznych do szyfrowania plików użytkownika, czyniąc je nieczytelnymi do czasu zastosowania klucza deszyfrującego.

### Q7: Czym jest luka typu zero-day?

Zero-day to luka bezpieczeństwa w oprogramowaniu nieznana dostawcy, przez co nie ma czasu na opracowanie poprawki przed wykorzystaniem exploita.

### Q8: Jaką rolę odgrywa ramy NIST?

Ramy NIST zawierają dobrowolne wytyczne i standardy, które pomagają organizacjom zarządzać ryzykiem cyberbezpieczeństwa i je zmniejszać.

### Q9: Czym jest plan reagowania na incydenty bezpieczeństwa?

To udokumentowany zestaw procedur wykrywania naruszeń bezpieczeństwa i przejęcia sieci, ich powstrzymywania i odzyskiwania po nich.

### Q10: Jak inżynieria społeczna wykorzystuje użytkowników?

Socjotechnika wykorzystuje manipulację psychologiczną, aby nakłonić pracowników do ujawnienia haseł lub pobrania złośliwych plików.

# Punkt kontrolny 10: Zaawansowane najczęściej zadawane pytania o bezpieczeństwo (Część C)

Poznaj zaawansowane aspekty techniczne ram bezpieczeństwa, analizy złośliwego oprogramowania i zgodności danych z przepisami.

### Q1: Jak atak DDoS przeciąża serwery WWW?

Atak DDoS koordynuje miliony zainfekowanych urządzeń botnetu, aby zalać serwer ruchem i wyczerpać limity przepustowości i procesora.

### Q2: Jaka jest różnica między szyfrowaniem symetrycznym a asymetrycznym?

Szyfrowanie symetryczne używa jednego klucza do szyfrowania i deszyfrowania, natomiast szyfrowanie asymetryczne używa pary kluczy: publicznego i prywatnego.

### Q3: Jak hakerzy przeprowadzają ataki typu SQL injection?

Atakujący wpisują złośliwe polecenia SQL w pola formularzy, nakłaniając bazę danych zaplecza do ujawnienia nieautoryzowanych rekordów użytkowników.

### Q4: Czym jest ruch boczny (lateral movement) we włamaniach do sieci?

To technika, w której atakujący wykorzystują początkowy dostęp do serwera do przejęcia innych połączonych systemów w sieci wewnętrznej.

### Q5: Jak DNS spoofing przekierowuje ruch internetowy?

Spoofing DNS zmienia rekordy w pamięci podręcznej serwera nazw, kierując legalnych użytkowników na złośliwe witryny łudząco podobne do docelowych domen.

# Punkt kontrolny 10: Zaawansowane najczęściej zadawane pytania o bezpieczeństwo (Część D)

Poznaj zaawansowane aspekty techniczne ram bezpieczeństwa, analizy złośliwego oprogramowania i zgodności danych z przepisami.

### Q6: Czym jest sprzętowy token bezpieczeństwa?

To fizyczne urządzenie (np. YubiKey) generujące kryptograficzne dowody uwierzytelnienia, oferujące maksymalną obronę przed zdalnym phishingiem.

### Q7: Jak zespoły bezpieczeństwa wykorzystują pułapki typu honeypot?

Zespoły wdrażają nieprodukcyjne serwery-wabiki, aby wcześnie wykrywać włamania i analizować wzorce ataków nieuprawnionych osób.

### Q8: Czym jest zasada najmniejszych uprawnień?

To standard bezpieczeństwa polegający na ograniczeniu praw dostępu użytkownika do absolutnego minimum niezbędnego do wykonywania jego ról zawodowych.

### Q9: Jak atak typu Man-in-the-Middle wykorzystuje połączenia?

Atakujący przechwytuje i zmienia komunikację między dwoma urządzeniami w nieszyfrowanych sieciach, kradnąc tokeny sesji i dane logowania.

### Q10: Czym są wskaźniki naruszenia bezpieczeństwa (IOC)?

IOC to dane kryminalistyczne, takie jak nietypowe modyfikacje rejestru lub nieautoryzowany ruch IP, wskazujące, że system został naruszony.

# Część 11: 10 faktów o cyberbezpieczeństwie z praktyki i spostrzeżeń

Przejrzyj prawdziwe fakty dotyczące naruszeń bezpieczeństwa, mechanizmów obronnych i standardów zgodności.

**1. WGLĄD W BEZPIECZEŃSTWO**

Atakujący bez przerwy skanują internet w poszukiwaniu podatnych serwerów i wysyłają wiadomości phishingowe do skrzynek odbiorczych pracowników.

**2. WGLĄD W BEZPIECZEŃSTWO**

Błąd ludzki, taki jak klikanie linków phishingowych, jest częstym czynnikiem w naruszeniach danych, dlatego szkolenia mają znaczenie.

**3. WGLĄD W BEZPIECZEŃSTWO**

Koszty naruszenia danych obejmują kary prawne, utratę klientów, dochodzenie i naprawę szkód, a mogą sięgać milionów dolarów.

**4. WGLĄD W BEZPIECZEŃSTWO**

MFA odporne na phishing, takie jak sprzętowe klucze bezpieczeństwa, to najsilniejszy rodzaj MFA i standard, do którego zachęca CISA. [2]

**5. WGLĄD W BEZPIECZEŃSTWO**

Ransomware pozostaje poważnym zagrożeniem dla sieci przedsiębiorstw, a CISA zachęca do tworzenia szyfrowanych kopii zapasowych offline jako kluczowej obrony. [4]

**6. WGLĄD W BEZPIECZEŃSTWO**

NIST Cybersecurity Framework 2.0 (2024) ma sześć podstawowych funkcji: Zarządzanie (Govern), Identyfikacja (Identify), Ochrona (Protect), Wykrywanie (Detect), Reagowanie (Respond), Odzyskiwanie (Recover). [1]

**7. WGLĄD W BEZPIECZEŃSTWO**

Boty credential stuffing testują na dużą skalę wyciekłe pary nazwy użytkownika i hasła na portalach logowania banków i sklepów internetowych.

**8. WGLĄD W BEZPIECZEŃSTWO**

Na całym świecie istnieją rynki exploitów zero-day, na których groźne luki o wysokim stopniu zagrożenia mogą być sprzedawane za duże sumy, zanim zostaną załatane.

**9. WGLĄD W BEZPIECZEŃSTWO**

System-wabik typu honeypot natychmiast zgłasza alerty o włamaniu, ponieważ prawowici użytkownicy nie mają powodu, aby z niego korzystać.

**10. WGLĄD W BEZPIECZEŃSTWO**

Transport Layer Security (TLS) szyfruje sesje przeglądarki, zapobiegając podsłuchiwaniu pakietów w publicznych sieciach Wi-Fi.

# Źródła i odnośniki techniczne

Przewodnik do nauki i interaktywne łamigłówki powstały na podstawie globalnych standardów NIST, OWASP i zgodności z przepisami o ochronie prywatności danych.

## PUBLIKACJE NAUKOWE I BRANŻOWE

[1] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[2] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[3] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[4] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[6] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.
https://csrc.nist.gov/pubs/sp/800/61/r3/final

[7] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[8] OWASP. (n.d.). SQL Injection.
https://owasp.org/www-community/attacks/SQL_Injection

## Klucz odpowiedzi: Punkt kontrolny 1 – test wielokrotnego wyboru

**1** **Ataki phishingowe** PHISHING — **Poprawna odpowiedź: A**

### UWAGA DLA NAUCZYCIELA

Kampanie phishingowe próbują wykraść dane logowania i wrażliwe dane użytkowników za pomocą sfałszowanych e-maili. Źródło: OWASP Secure Configuration.

**2** **Ochrona konta** KLUCZ MFA — **Poprawna odpowiedź: A**

### UWAGA DLA NAUCZYCIELA

Uwierzytelnianie wieloskładnikowe (MFA) z użyciem tokenów sprzętowych zapewnia najsilniejszą ochronę dostępu do konta. Źródło: NIST Digital Identity.

**3** **Zagrożenie ransomware** RANSOMWARE — **Poprawna odpowiedź: A**

### UWAGA DLA NAUCZYCIELA

Ransomware szyfruje krytyczne systemy i dane, żądając zapłaty w kryptowalucie za klucze deszyfrujące. Źródło: Center for Internet Security (CIS).

**4** **Luka zero-day** ZERO-DAY — **Poprawna odpowiedź: A**

### UWAGA DLA NAUCZYCIELA

Zagrożenia zero-day wykorzystują niezałatane, nieznane luki w zabezpieczeniach, zanim dostawca udostępni poprawkę. Źródło: OWASP Secure Configuration.

**5** **Frameworki bezpieczeństwa** FRAMEWORKI — **Poprawna odpowiedź: A**

### UWAGA DLA NAUCZYCIELA

Ramy takie jak NIST zawierają uporządkowane wytyczne, które pomagają organizacjom zarządzać ryzykiem cybernetycznym i je zmniejszać. Źródło: NIST Digital Identity.

## Klucz odpowiedzi: Punkt kontrolny 2 – prawda czy fałsz

**6** **Ukierunkowany phishing** PHISHING — **Poprawna odpowiedź: Fałsz**

### UWAGA DLA NAUCZYCIELA

Ataki phishingowe są skierowane zarówno przeciw sieciom firmowym, jak i kontom osobistym, aby poszerzyć wektory ataku. Źródło: OWASP Secure Configuration.

**7** **Pytanie 7** — **Poprawna odpowiedź: Prawda**

### UWAGA DLA NAUCZYCIELA

MFA wymaga drugiego składnika, więc samo skradzione hasło zwykle nie wystarcza do zalogowania.

**8** **Zapora ruchu** ZAPORA SIECIOWA — **Poprawna odpowiedź: Prawda**

### UWAGA DLA NAUCZYCIELA

Zapory sieciowe sprawdzają ruch na określonych portach sieciowych i go blokują, aby odfiltrować nieautoryzowane połączenia. Źródło: Center for Internet Security (CIS).

**9** **Reagowanie na zero-day** ZERO-DAY — **Poprawna odpowiedź: Fałsz**

### UWAGA DLA NAUCZYCIELA

Usuwanie luk zero-day wymaga poprawek kodu i filtrowania WAF, ponieważ sygnatury jeszcze nie istnieją. Źródło: OWASP Secure Configuration.

**10** **Pułapki typu honeypot** HONEYPOT — **Poprawna odpowiedź: Prawda**

### UWAGA DLA NAUCZYCIELA

Honeypoty to zwodnicze serwery wykorzystywane przez zespoły bezpieczeństwa do wabienia, alarmowania i badania złośliwych aktorów. Źródło: Center for Internet Security (CIS).

# Klucze słownictwa i kryteria oceny

**Schemat oceniania dla nauczyciela: Przyznaj 1 punkt za każde poprawne dopasowanie (łącznie 8 pkt) i pojęcie w kontekście (łącznie 6 pkt).**

## PUNKT KONTROLNY 4: KLUCZ – DOPASOWYWANIE POJĘĆ

| | | | |
|---|---|---|---|
| D 1. Zagrożenie ransomware | G 2. Uwierzytelnianie wieloskładnikowe | E 3. Exploit typu zero-day | H 4. Przynęta typu honeypot |
| C 5. Zapora przed włamaniami | B 6. Reagowanie na incydenty | F 7. Higiena haseł | A 8. Ramy bezpieczeństwa |

## PUNKT KONTROLNY 3: KLUCZ – KLUCZOWE POJĘCIA

| | | | |
|---|---|---|---|
| 1 ZAPORA SIECIOWA | 2 EXPLOIT | 3 PHISHING | 4 ZŁOŚLIWE OPROGRAMOWANIE |
| 5 HIGIENA | 6 SZYFROWANIE | | |

## PUNKT KONTROLNY 6, WARIANT ALTERNATYWNY: KLUCZ – DOPASOWYWANIE SŁÓW

| | | | |
|---|---|---|---|
| 1 E – ZAPORASIECIOWA | 2 F – REAGOWANIE | 3 A – RANSOMWARE | 4 B – WIELOCZYNNIKOWE |
| 5 G – HIGIENA | 6 H – RAMY | 7 C – EXPLOITZERODAY | 8 D – HONEYPOT |

## UWAGI DO DYSKUSJI DLA NAUCZYCIELI

**Kluczowe pojęcia:**
Sprawdź, czy uczniowie potrafią własnymi słowami wyjaśnić pojęcia Zagrożenie ransomware, Uwierzytelnianie wieloskładnikowe i Exploit typu zero-day oraz podać przykład każdego z nich.

**Studia przypadków:**
Poproś uczniów, aby uzasadniali swoje zalecenia faktami z karty pracy, a nie przypuszczeniami.

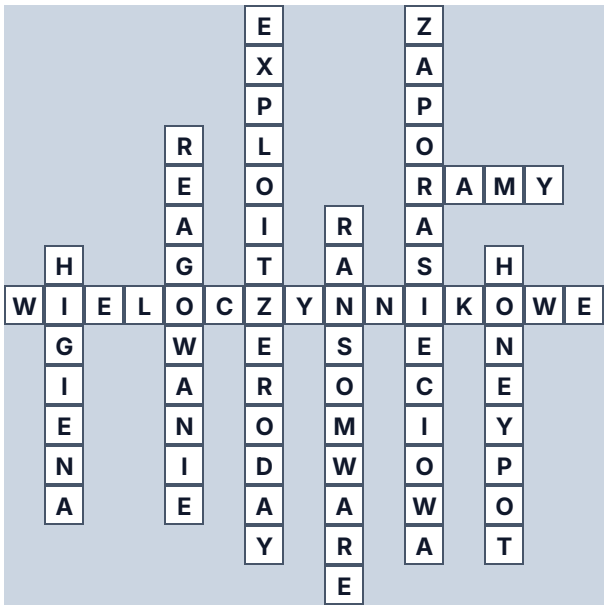
**Ocena źródeł:**
Niech uczniowie sprawdzą co najmniej jedno twierdzenie w źródłach z karty pracy; omówcie, dlaczego liczby, ceny i przepisy mogą się z czasem zmieniać.

# Klucze do łamigłówek i uwagi dla nauczyciela

## ROZWIĄZANIE WYSZUKIWANKI SŁOWNEJ

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | Ę | O | K | Ń | Ć | N | W | C | Ć | G | I | Ą | Ą | Ó |
| R | Ł | P | W | T | I | Ź | I | Ę | Ź | E | S | A | G | Y |
| X | H | Ę | R | T | Ń | U | E | K | R | X | Ć | W | T | S |
| Ł | P | Ł | N | R | Ś | H | L | L | P | P | H | O | Ź | Ó |
| Ł | X | H | V | A | Y | Ń | O | Z | Q | L | Q | I | Ą | A |
| E | Ł | O | Ó | N | M | N | C | Ą | Ł | O | I | C | Ę | H |
| I | J | N | Ń | S | A | Z | Z | B | Ż | I | Ż | E | Ź | I |
| N | B | E | N | O | R | V | Y | Y | M | T | C | I | Ę | G |
| A | Ó | Y | X | M | P | Q | N | Y | G | Z | D | S | Ź | I |
| W | B | P | X | W | Ł | E | N | G | G | E | Ż | A | X | E |
| O | C | O | O | A | Q | K | I | Y | Y | R | R | R | L | N |
| G | Ż | T | A | R | N | R | K | Ż | R | O | M | O | F | A |
| A | Ś | W | F | E | Ł | X | O | J | B | D | Ź | P | C | B |
| E | Ź | O | V | Ż | O | Ż | W | U | T | A | Ą | A | H | W |
| R | P | Y | C | N | M | H | E | Ó | Y | Y | Ź | Z | Ż | Y |

## ROZWIĄZANIE KRZYŻÓWKI




## PRZEWODNIK DLA NAUCZYCIELA: ROZWIĄZANIA KRZYŻÓWKI

### POZIOMO

**4 poziomo: RAMY** Ustrukturyzowane wytyczne, takie jak NIST, służące do zarządzania ryzykiem cybernetycznym (4 liter)

**8 poziomo: WIELOCZYNNIKOWE** Weryfikacja bezpieczeństwa wymagająca dwóch lub więcej czynników uwierzytelniania (15 liter)

### PIONOWO

**1 pionowo: EXPLOITZERODAY** Exploit wykorzystujący lukę przed wydaniem poprawki przez dostawcę (14 liter)

**2 pionowo: ZAPORASIECIOWA** Bariera sieciowa filtrująca ruch według reguł bezpieczeństwa (14 liter)

**3 pionowo: REAGOWANIE** Ustrukturyzowany plan postępowania z naruszeniami bezpieczeństwa i ograniczania ich skutków (10 liter)

**5 pionowo: RANSOMWARE** Złośliwe oprogramowanie szyfrujące dane i żądające zapłaty za odszyfrowanie (10 liter)

**6 pionowo: HIGIENA** Najlepsze praktyki zarządzania poświadczeniami i kluczami uwierzytelniania (7 liter)

**7 pionowo: HONEYPOT** Fałszywy system zastawiony w celu zwabienia i analizy złośliwych aktorów (8 liter)

# Klucz do słów rozsypanych i rozwiązania szyfru

Klucz odpowiedzi do ćwiczenia z rozszyfrowywania słownictwa i Tajemniczego wyzwania szyfrowego.

## KLUCZ DO ROZWIĄZANIA ANAGRAMÓW

1. RWMOARAESN — **RANSOMWARE**
2. OXIPTAEDZYROEL — **EXPLOITZERODAY**
3. ZEAWIACIPSRAOO — **ZAPORASIECIOWA**
4. AIEINHG — **HIGIENA**
5. EILWONNCEZKYIWO — **WIELOCZYNNIKOWE**
6. OTEPHYON — **HONEYPOT**
7. EGRAWNIEOA — **REAGOWANIE**
8. RYMA — **RAMY**

## KLUCZ DO WYZWANIA Z TAJNYM SZYFREM

**"CHROŃ SYSTEM UWIERZYTELNIANIEM WIELOCZYNNIKOWYM"**

# Klucz odpowiedzi do studiów przypadków

## A Studium przypadku 1: Strategia odzyskiwania po ransomware

Rozwiązanie dla nauczyciela

### WYTYCZNE OCENIANIA

**Odpowiedzi uczniów powinny obejmować następujące punkty:**

- Analiza scenariusza: Sieć firmowa została zainfekowana ransomware, który zablokował krytyczne bazy danych. Atakujący żądają okupu w kryptowalucie w wysokości 100,000 USD. Firma ma kopie zapasowe offline sprzed 24 godzin.
- Zalecana strategia i rozwiązanie: Ryzyka zapłaty: Zapłata nie gwarantuje odszyfrowania plików, oznacza firmę jako cel skłonny płacić i finansuje działalność przestępczą. Strategia odzyskiwania: Zespół powinien odizolować zainfekowane hosty, wyczyścić przejęte serwery i przywrócić dane z kopii zapasowych offline. Musi załatać pierwotny wektor dostępu (phishing lub exploit), aby zapobiec natychmiastowej ponownej infekcji.

## B Studium przypadku 2: Obrona przed credential stuffing

Rozwiązanie dla nauczyciela

### WYTYCZNE OCENIANIA

**Odpowiedzi uczniów powinny obejmować następujące punkty:**

- Analiza scenariusza: Usługa online pada ofiarą ataku credential stuffing, w którym hakerzy testują miliony par nazwa użytkownika/hasło skradzionych z innych witryn.
- Zalecana strategia i rozwiązanie: Mechanizm: Atakujący wykorzystują ponowne używanie haseł w różnych witrynach i za pomocą automatycznych botów logują się na konta użytkowników. Zabezpieczenia: 1. Uwierzytelnianie wieloskładnikowe (MFA) blokuje próby logowania, nawet jeśli hasło jest poprawne. 2. Wprowadzenie ograniczeń liczby żądań i CAPTCHA blokuje ruch automatycznych botów zasypujących punkty logowania.