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

Architektura i bezpieczeństwo Zero Trust

Ciągła weryfikacja, mikrosegmentacja sieci, zarządzanie tożsamością i dostępem (IAM), zasada najmniejszych uprawnień i kontrole postawy.

PRZEGLĄD NAUKI O BEZPIECZEŃSTWIE ZERO TRUST

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 architekturę i bezpieczeństwo Zero Trust. Poznasz ciągłą weryfikację, mikrosegmentację sieci, zarządzanie tożsamością i dostępem (IAM), zasadę najmniejszych uprawnień i audytowanie sesji.

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/zero-trust-cyberbezpieczenstwo/

Twoja ścieżka nauki: strategia Zero Trust

- Zrozum podstawową zasadę ciągłej weryfikacji.
- Wdróż mikrosegmentację sieci i dostęp zgodny z zasadą najmniejszych uprawnień.
- Skonfiguruj kontrole postawy urządzeń i aktywny audyt sesji.

INSTRUKCJE DO PRZEWODNIKA O BEZPIECZEŃSTWIE ZERO TRUST

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 architektury Zero Trust. Zakończ zadaniem dodatkowym Myśl szybko.

ARCHITEKTURA I BEZPIECZEŃSTWO ZERO TRUST (WPROWADZENIE)

Zabezpieczenia Zero Trust zastępują stare modele obwodu sieci ścisłą polityką „nigdy nie ufaj, zawsze weryfikuj”. Wdrożenie mikrosegmentacji, zarządzania tożsamością i dostępem (IAM), zasady najmniejszych uprawnień oraz kontroli stanu urządzeń blokuje ruch boczny zagrożeń.

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

Punkt kontrolny 1: Wyzwanie – test wielokrotnego wyboru

1. Jaka jest podstawowa zasada bezpieczeństwa Zero Trust?

- A. Nigdy nie ufaj, zawsze weryfikuj każde żądanie dostępu niezależnie od źródła
- B. Zakładanie, że cały ruch wewnątrz firmowej zapory sieciowej jest bezpieczny
- C. Przechowywanie plików bazy danych bez szyfrowania w celu zwiększenia szybkości
- D. Egzekwowanie uwierzytelniania poczty e-mail wyłącznie za pomocą rekordów SPF

2. Czym jest mikrosegmentacja sieci?

- A. Dzielenie sieci na małe, izolowane strefy w celu ograniczenia ruchu bocznego
- B. Szyfrowanie kart sieciowych podczas przesyłania danych
- C. Podłączanie wszystkich lokalnych serwerów do jednego publicznego adresu IP
- D. Monitorowanie naciśnięć klawiszy użytkownika w sesjach przeglądarki

3. Czym jest zasada najmniejszych uprawnień?

- A. Ograniczanie uprawnień dostępu użytkownika tylko do tego, co jest niezbędne do jego pracy
- B. Domyślne nadawanie wszystkich uprawnień systemowych każdemu użytkownikowi
- C. Zezwalanie na anonimowe logowania do firmowych serwerów baz danych
- D. Konfigurowanie publicznych routerów Wi-Fi bez haseł

4. Czym jest zarządzanie tożsamością i dostępem (IAM)?

- A. Frameworki zarządzające tożsamościami cyfrowymi i kontrolujące uprawnienia systemowe
- B. Narzędzia antywirusowe skanujące lokalne katalogi plików
- C. System przechowywania kopii zapasowych z użyciem nośników odizolowanych od sieci (air-gapped)
- D. Protokół bramy poczty e-mail odrzucający sfałszowane domeny

5. Co oznacza ciągłe uwierzytelnianie?

- A. Wielokrotne weryfikowanie tożsamości użytkownika i stanu urządzenia podczas aktywnej sesji
- B. Zmienianie hasła głównego co 10 minut
- C. Haszowanie rekordów bazy danych przy użyciu wielu algorytmów
- D. Szyfrowanie pakietów tranzytowych sieci za pomocą kluczy TLS

Punkt kontrolny 2: Wyzwanie – prawda czy fałsz

6 Pytanie 6

6. Zero Trust zakłada, że cały ruch wewnątrz firmowej zapory sieciowej jest bezpieczny.

- ○ Prawda
- ○ Fałsz

7 Pytanie 7

7. Mikrosegmentacja ogranicza zdolność atakujących do przemieszczania się bocznego między wewnętrznymi serwerami.

- ○ Prawda
- ○ Fałsz

8 Pytanie 8

8. Zasada najmniejszych uprawnień domyślnie przyznaje dostęp do wszystkich plików bazy danych.

- ○ Prawda
- ○ Fałsz

9 Pytanie 9

9. Ciągła weryfikacja sprawdza kondycję urządzenia i poświadczenia przez cały czas trwania sesji logowania.

- ○ Prawda
- ○ Fałsz

10 Pytanie 10

10. Wdrożenie Zero Trust zmniejsza skutki przejęcia firmowych danych logowania.

- ○ Prawda
- ○ Fałsz

Punkt kontrolny 3: Wstawianie kluczowych terminów

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

1. Wymaganie poświadczeń w każdym punkcie dostępu to ciągła _____ .

2. Dzielenie sieci korporacyjnej na maleńkie strefy to mikro- _____ .

3. Konfigurowanie tożsamości cyfrowych i kontroli dostępu wykorzystuje system _____ .

4. Ograniczanie uprawnień użytkowników opiera się na zasadzie: najmniejszy _____ .

5. Ocena stanu połączonych urządzeń sprawdza ich cechę o nazwie: _____ urządzenia.

6. Rejestrowanie i przegląd aktywnych sesji to _____ bezpieczeństwa.

BANK SŁÓW

AUDYT IAM KONDYCJA PRZYWILEJ ROUTER SEGMENTACJA WERYFIKACJA ZAPORA SIECIOWA

Wpisz tutaj swoje odpowiedzi:

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

Punkt kontrolny 4: Dopasowywanie pojęć z zakresu bezpieczeństwa

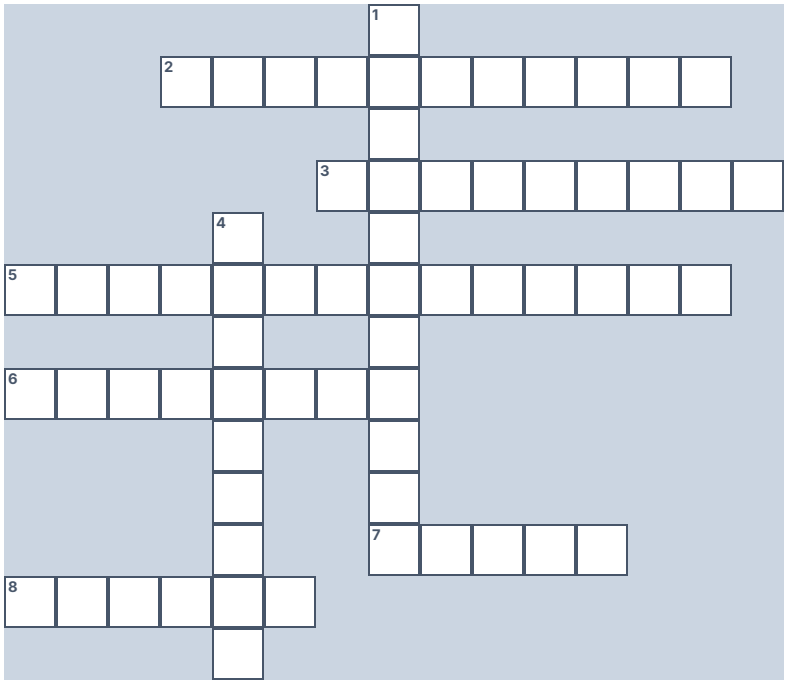
DOPASOWYWANIE DEFINICJI

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

☐	1. WERYFIKACJA	A	Zarządzanie dostępem do danych uwierzytelniających użytkowników.
☐	2. SEGMENTACJA	B	Zasada najmniejszych praw dostępu.
☐	3. IAM	C	Routing ruchu pakietów sieciowych.
☐	4. UPRAWNIENIA	D	Ochrona zewnętrzną barierą sieciową.
☐	5. STAN ZABEZPIECZEŃ	E	Przeglądanie zarejestrowanych sesji dostępu.
☐	6. AUDYTOWANIE	F	Podział wewnętrznych stref sieci.
☐	7. ZAPORA SIECIOWA	G	Stałe sprawdzanie danych uwierzytelniających użytkownika.
☐	8. ROUTER	H	Ocena stanu zdrowia urządzenia.

Punkt kontrolny 5: Krzyżówka

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



POZIOMO

2. Dzielenie wewnętrznych stref sieci. (11)

3. Zarządzanie dostępem do poświadczeń użytkowników. (9)

5. Ochrona zewnętrzną barierą sieci. (14)

6. Ocena stanu zdrowia urządzenia. (8)

7. Przegląd zarejestrowanych sesji dostępu. (5)

8. Kierowanie ruchem pakietów sieciowych. (6)

PIONOWO

1. Ciągłe sprawdzanie poświadczeń użytkowników. (11)

4. Zasada najmniejszych praw dostępu. (9)

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

2 poziomo: Dzielenie wewnętrznych stref sieci. (11 liter):

3 poziomo: Zarządzanie dostępem do poświadczeń użytkowników. (9 liter):

5 poziomo: Ochrona zewnętrzną barierą sieci. (14 liter):

6 poziomo: Ocena stanu zdrowia urządzenia. (8 liter):

7 poziomo: Przegląd zarejestrowanych sesji dostępu. (5 liter):

8 poziomo: Kierowanie ruchem pakietów sieciowych. (6 liter):

PIONOWO

1 pionowo: Ciągłe sprawdzanie poświadczeń użytkowników. (11 liter):

4 pionowo: Zasada najmniejszych praw dostępu. (9 liter):

Punkt kontrolny 6: Ukryte słowa w wykreślance

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

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

LISTA SŁÓW

WERYFIKACJA SEGMENTACJA SYSTEMIAM PRZYWILEJ KONDYCJA AUDYT ZAPORASIECIOWA ROUTER

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. WERYFIKACJA**
- **B. SEGMENTACJA**
- **C. SYSTEMIAM**
- **D. PRZYWILEJ**
- **E. KONDYCJA**
- **F. AUDYT**
- **G. ZAPORASIECIOWA**
- **H. ROUTER**

DEFINICJE I POLA DOPASOWANIA

1. Ochrona zewnętrzną barierą sieci.
2. Przegląd zarejestrowanych sesji dostępu.
3. Zasada najmniejszych praw dostępu.
4. Dzielenie wewnętrznych stref sieci.
5. Kierowanie ruchem pakietów sieciowych.
6. Ocena stanu zdrowia urządzenia.
7. Zarządzanie dostępem do poświadczeń użytkowników.
8. Ciągłe sprawdzanie poświadczeń użytkowników.

Punkt kontrolny 7: Wyzwanie – pomieszane słowa

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

1. FKJEIAWCRAY
2. MSATYMIES
3. DOKYCAJN
4. ASWCOEAAIOIZPR
5. CEATGAENSJM
6. EYRLIPWJZ
7. YTADU
8. URRETO

Zadanie dodatkowe: Myśl szybko

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

1	Informacje, których nigdy nie powinieneś udostępniać			
2	Bezpieczne nawyki, które możesz zacząć już dziś			
3	Rzeczy sprawdzane na urządzeniu			
4	Rzeczy, które są rejestrowane w logach			
5	Słowa związane z cyberbezpieczeństwem			
6	Rzeczy, które sprawdza Zero Trust			
7	Miejsca, w których na co dzień okazujesz dokument tożsamości			
8	Sposoby na udowodnienie, że to naprawdę ty			
9	Rzeczy do zrobienia po wycieku danych			
10	Oznaki, że komputer jest zainfekowany			
11	Powody, dla których warto aktualizować oprogramowanie			
12	Poziomy dostępu w firmie			
13	Narzędzia bezpieczeństwa, które znasz			
14	Strefy, na które można podzielić sieć			
15	Powiedzenia o zaufaniu			

Punkt kontrolny 8: Studia przypadków z cyberbezpieczeństwa

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

STUDIUM PRZYPADKU 1: PRZEJŚCIE NA ARCHITEKTURĘ SIECI ZERO TRUST

👷

Scenariusz: Duże przedsiębiorstwo korzysta obecnie z płaskiej sieci wewnętrznej, w której każde urządzenie w sieci lokalnej może uzyskać dostęp do wszystkich firmowych serwerów i baz danych.

Pytanie do dyskusji: Zaprojektuj strategię mikrosegmentacji sieci, aby ograniczyć ruch boczny (lateral movement).

STUDIUM PRZYPADKU 2: WDRAŻANIE KONTROLI DOSTĘPU OPARTEJ NA ZASADZIE NAJMNIEJSZYCH UPRAWNIEŃ

👷

Scenariusz: Logi audytu pokazują, że tymczasowi użytkownicy bazy danych i pracownicy niskiego szczebla mają globalne uprawnienia do odczytu i zapisu w krytycznych bazach danych księgowych.

Pytanie do dyskusji: Przeprowadź audyt i ogranicz uprawnienia IAM bazy danych, aby wymusić zasadę najmniejszych uprawnień.

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

30	7	24	32	9	12	14	28	13		33	1	30	25	33	7		30

1	24	4	11	12	27	7	14	27	28	24	33	7		33	7	24	20

27	24	28	25	27

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: Czym jest Zero Trust?

Zero Trust to struktura bezpieczeństwa zakładająca, że zagrożenia istnieją zarówno poza granicą sieci, jak i wewnątrz niej, co wymaga weryfikacji każdego żądania. [1]

Q2: Jaka jest podstawowa zasada Zero Trust?

Nigdy nie ufaj, zawsze weryfikuj.

Q3: Czym jest mikrosegmentacja?

Podział sieci na małe, bezpieczne segmenty logiczne w celu kontrolowania ruchu i ograniczania skutków naruszeń.

Q4: Czym jest zasada najmniejszych uprawnień?

Przyznawanie użytkownikom wyłącznie minimalnych praw dostępu wymaganych do wykonywania ich konkretnych zadań. [2]

Q5: Co oznacza skrót IAM?

Zarządzanie tożsamością i dostępem.

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

Przejrzyj typowe pytania i odpowiedzi dotyczące ograniczania zagrożeń w sieci.

Q6: Jak pomaga kontrola stanu urządzenia?

Sprawdza, czy urządzenie jest zaktualizowane, ma działający program antywirusowy i jest bezpieczne, zanim zezwoli na dostęp.

Q7: Czym jest ruch boczny (lateral movement)?

Proces, w którym atakujący przemieszczają się po sieci od początkowo przejętego węzła do systemów o wyższej wartości.

Q8: Czy Zero Trust zastępuje zapory sieciowe?

Nie, wzmacnia je, dodając kontrole zorientowane na tożsamość i wewnętrzne zapory segmentacyjne.

Q9: Czym jest uwierzytelnianie ciągłe?

Ciągła weryfikacja tożsamości użytkownika przez cały czas aktywnej sesji logowania, a nie tylko przy pierwszym logowaniu.

Q10: Dlaczego płaska sieć jest niebezpieczna?

W sieciach płaskich pojedynczy przejęty węzeł pozwala atakującym łatwo uzyskać dostęp do dowolnej bazy danych w sieci.

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 Zero Trust odpowiada na model perymetryczny?

Zastępuje przestarzały model „zamku i fosy", przesuwając obronę z sieci granicznych na konkretne tożsamości użytkowników i zasoby.

Q2: Czym jest punkt decyzyjny polityki (PDP)?

Element systemu, który ocenia żądania autoryzacji względem reguł bezpieczeństwa, aby zdecydować, czy przyznać dostęp.

Q3: Czym jest punkt egzekwowania zasad (PEP)?

Węzeł systemu (np. brama lub serwer proxy), który fizycznie zezwala na żądania połączeń lub je blokuje na podstawie decyzji PDP.

Q4: Jak kontrola dostępu oparta na rolach (RBAC) wspiera model Zero Trust?

RBAC grupuje uprawnienia w określone role, co pomaga zapobiegać dziedziczeniu przez użytkowników nadmiernych uprawnień administracyjnych.

Q5: Czym jest kontekstowa kontrola dostępu?

Ocena żądań logowania na podstawie dodatkowych wskazówek, takich jak lokalizacja geograficzna, stan urządzenia i godzina logowania, w celu oszacowania ryzyka.

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 mikrosegmentacja różni się od standardowych sieci VLAN?

VLAN dzielą sieci na szerokie segmenty logiczne w warstwie 2, a mikrosegmentacja używa polityki programowej do izolowania pojedynczych obciążeń.

Q7: Czym jest dostęp just-in-time (JIT)?

Tymczasowe przyznawanie podwyższonych uprawnień administracyjnych i automatyczne ich cofanie po zakończeniu zadania.

Q8: Jak zabezpiecza się API w modelu Zero Trust?

Przez wymaganie kryptograficznie podpisanych tokenów OAuth i audytowanie sygnatur żądań w każdej bramie API.

Q9: Czym jest klient dostępu do sieci w modelu zero trust (ZTNA)?

Agent programowy, który ustanawia bezpieczne, zaszyfrowane połączenia wychodzące z konkretnymi aplikacjami, a nie z surowymi podsieciami sieciowymi.

Q10: Jak audyt logów wspiera Zero Trust?

Ciągłe logowanie pozwala zautomatyzowanym narzędziom analityki bezpieczeństwa wykrywać anomalie i natychmiast zawieszać nieuprawnione logowania.

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

Architektury Zero Trust zastępują przestarzały model zamku i fosy regułami weryfikacji opartymi na tożsamości.

2. WGLĄD W BEZPIECZEŃSTWO

Mikrosegmentacja sieci zmniejsza obszar, do którego może dotrzeć złośliwe oprogramowanie, izolując obciążenia w małych chronionych strefach.

3. WGLĄD W BEZPIECZEŃSTWO

Zero Trust koncentruje się na ochronie zasobów, takich jak aktywa, usługi i konta, a nie segmentów sieci. [1]

4. WGLĄD W BEZPIECZEŃSTWO

Zasady dostępu z najmniejszymi uprawnieniami zmniejszają ryzyko wycieku danych z głównych baz danych przez osoby z wewnątrz.

5. WGLĄD W BEZPIECZEŃSTWO

Walidacja stanu urządzenia sprawdza w czasie rzeczywistym poziom poprawek systemu operacyjnego i aktywny stan oprogramowania antywirusowego.

6. WGLĄD W BEZPIECZEŃSTWO

Brokerzy Zero Trust Network Access (ZTNA) mogą zastąpić lub uzupełnić firmowe sieci VPN, aby ograniczyć zakres dostępu użytkowników.

7. WGLĄD W BEZPIECZEŃSTWO

Delegowanie uprawnień administracyjnych Just-In-Time (JIT) zmniejsza ryzyko kradzieży danych uwierzytelniających na kontrolerach domeny.

8. WGLĄD W BEZPIECZEŃSTWO

Ciągła walidacja rejestruje i audytuje zachowanie sesji, zawieszając użytkowników wykazujących anomalne wzorce wykonywania skryptów.

9. WGLĄD W BEZPIECZEŃSTWO

Tradycyjne zabezpieczenia obwodowe nie blokują ataków bocznych po wycieku poświadczeń administracyjnych.

10. WGLĄD W BEZPIECZEŃSTWO

Publikacja specjalna NIST 800-207 (2020) podaje abstrakcyjną definicję architektury Zero Trust wraz z modelami wdrożenia. [1]

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. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[2] CISA. (2023). Zero Trust Maturity Model.
https://www.cisa.gov/zero-trust-maturity-model

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

[4] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

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

Klucz odpowiedzi: Punkt kontrolny 1 – test wielokrotnego wyboru

1 Pytanie 1

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Jaka jest podstawowa zasada bezpieczeństwa Zero Trust? → Nigdy nie ufaj, zawsze weryfikuj każde żądanie dostępu niezależnie od źródła

2 Pytanie 2

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Czym jest mikrosegmentacja sieci? → Dzielenie sieci na małe, izolowane strefy w celu ograniczenia ruchu bocznego

3 Pytanie 3

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Czym jest zasada najmniejszych uprawnień? → Ograniczanie uprawnień dostępu użytkownika tylko do tego, co jest niezbędne do jego pracy

4 Pytanie 4

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Czym jest zarządzanie tożsamością i dostępem (IAM)? → Frameworki zarządzające tożsamościami cyfrowymi i kontrolujące uprawnienia systemowe

5 Pytanie 5

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Co oznacza ciągłe uwierzytelnianie? → Wielokrotne weryfikowanie tożsamości użytkownika i stanu urządzenia podczas aktywnej sesji

Klucz odpowiedzi: Punkt kontrolny 2 – prawda czy fałsz

6 **Pytanie 6** — **Poprawna odpowiedź: Fałsz**

UWAGA DLA NAUCZYCIELA

Fałsz: Zero Trust nie przyznaje domyślnego zaufania na podstawie lokalizacji w sieci, wewnątrz ani na zewnątrz.

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

UWAGA DLA NAUCZYCIELA

Prawda: małe izolowane strefy ograniczają, jak daleko intruz może się przemieszczać między serwerami.

8 **Pytanie 8** — **Poprawna odpowiedź: Fałsz**

UWAGA DLA NAUCZYCIELA

Fałsz: zasada najmniejszych uprawnień przyznaje tylko minimalny dostęp potrzebny każdej roli.

9 **Pytanie 9** — **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Ciągła weryfikacja sprawdza kondycję urządzenia i poświadczenia przez cały czas trwania sesji logowania.

10 **Pytanie 10** — **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Wdrożenie Zero Trust zmniejsza skutki przejęcia firmowych danych logowania.

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

G 1. WERYFIKACJA	F 2. SEGMENTACJA	A 3. IAM	B 4. UPRAWNIENIA
H 5. STAN ZABEZPIECZEŃ	E 6. AUDYTOWANIE	D 7. ZAPORA SIECIOWA	C 8. ROUTER

PUNKT KONTROLNY 3: KLUCZ – KLUCZOWE POJĘCIA

1 WERYFIKACJA	2 SEGMENTACJA	3 IAM	4 PRZYWILEJ
5 KONDYCJA	6 AUDYT		

PUNKT KONTROLNY 6, WARIANT ALTERNATYWNY: KLUCZ – DOPASOWYWANIE SŁÓW

1 G – ZAPORASIECIOWA	2 F – AUDYT	3 D – PRZYWILEJ	4 B – SEGMENTACJA
5 H – ROUTER	6 E – KONDYCJA	7 C – SYSTEMIAM	8 A – WERYFIKACJA

UWAGI DO DYSKUSJI DLA NAUCZYCIELI

Kluczowe pojęcia:
Sprawdź, czy uczniowie potrafią własnymi słowami wyjaśnić pojęcia WERYFIKACJA, SEGMENTACJA i IAM oraz podać przykład każdego z nich.

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

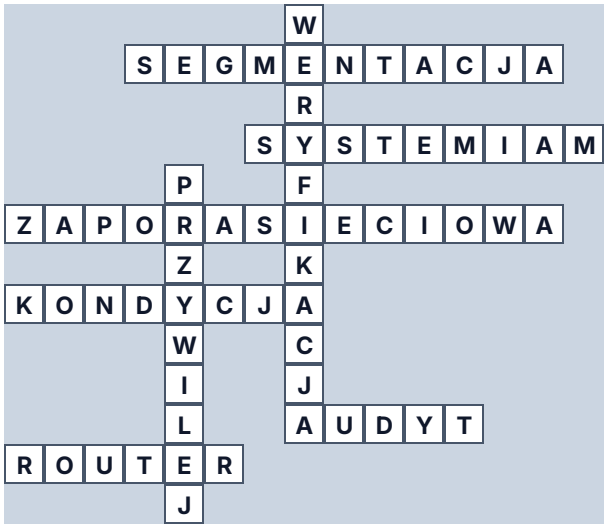
Ocena źródeł:
Niech uczniowie sprawdzą co najmniej jedno twierdzenie w źródłach z karty pracy; omówcie, dlaczego liczby, ceny i przepisy mogą się z czasem zmieniać.

Klucze do łamigłówek i uwagi dla nauczyciela

ROZWIĄZANIE WYSZUKIWANKI SŁOWNEJ

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

ROZWIĄZANIE KRZYŻÓWKI



PRZEWODNIK DLA NAUCZYCIELA: ROZWIĄZANIA KRZYŻÓWKI

POZIOMO

2 poziomo: SEGMENTACJA Dzielenie wewnętrznych stref sieci. (11 liter)

3 poziomo: SYSTEMIAM Zarządzanie dostępem do poświadczeń użytkowników. (9 liter)

5 poziomo: ZAPORASIECIOWA Ochrona zewnętrzną barierą sieci. (14 liter)

6 poziomo: KONDYCJA Ocena stanu zdrowia urządzenia. (8 liter)

7 poziomo: AUDYT Przegląd zarejestrowanych sesji dostępu. (5 liter)

8 poziomo: ROUTER Kierowanie ruchem pakietów sieciowych. (6 liter)

PIONOWO

1 pionowo: WERYFIKACJA Ciągłe sprawdzanie poświadczeń użytkowników. (11 liter)

4 pionowo: PRZYWILEJ Zasada najmniejszych praw dostępu. (9 liter)

Klucz do słów rozsypanych i rozwiązania szyfru

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

KLUCZ DO ROZWIĄZANIA ANAGRAMÓW

1. FKJEIAWCRAY — **WERYFIKACJA**
2. MSATYMIES — **SYSTEMIAM**
3. DOKYCAJN — **KONDYCJA**
4. ASWCOEAAIOIZPR — **ZAPORASIECIOWA**
5. CEATGAENSJM — **SEGMENTACJA**
6. EYRLIPWJZ — **PRZYWILEJ**
7. YTADU — **AUDYT**
8. URRETO — **ROUTER**

KLUCZ DO WYZWANIA Z TAJNYM SZYFREM

"WERYFIKUJ ZAWSZE W ARCHITEKTURZE ZERO TRUST"

Klucz odpowiedzi do studiów przypadków

A Studium przypadku 1: Przejście na architekturę sieci Zero Trust

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Duże przedsiębiorstwo używa obecnie płaskiej sieci wewnętrznej, w której każde urządzenie w sieci lokalnej ma dostęp do wszystkich firmowych serwerów i baz danych.
- Zalecana strategia i rozwiązanie: Podziel płaską sieć na odizolowane strefy działowe. Zainstaluj wewnętrzne zapory sieciowe kontrolujące ruch między strefami i wymagaj walidacji tokenów połączenia przy każdym dostępie.

B Studium przypadku 2: Wdrażanie kontroli dostępu opartej na zasadzie najmniejszych uprawnień

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Dzienniki audytu wskazują, że tymczasowi użytkownicy bazy danych i pracownicy niskiego szczebla mają globalne uprawnienia do odczytu i zapisu w kluczowych bazach danych księgowych.
- Zalecana strategia i rozwiązanie: Cofnij wszystkie globalne uprawnienia administracyjne. Wdróż kontrolę dostępu opartą na rolach (RBAC) dopasowaną do dokładnych ról zawodowych i ustanów cotygodniowe automatyczne przeglądy uprawnień.