Imię i nazwisko: _____ Data: _____ Wynik: _____

Ochrona danych i bezpieczeństwo korporacyjnych magazynów danych Przewodnik po bezpieczeństwie

Maskowanie danych, tokenizacja, szyfrowanie danych w spoczynku i w tranzycie, kopie zapasowe offline

PRZEGLĄD NAUKI: OCHRONA DANYCH

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 standardy i kontrole ochrony danych. Poznasz szyfrowanie całego dysku, bezpieczne kontrole dostępu, sprzętowe kopie zapasowe, stan bezpieczeństwa chmury i techniki maskowania danych.

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/ochrona-danych/

Twoja ścieżka nauki: strategia ochrony danych

- Rozróżnij techniki maskowania danych i tokenizacji.
- Wdróż szyfrowanie danych w spoczynku na dyskach oraz szyfrowanie w tranzycie za pomocą TLS.
- Zaprojektuj systemy kopii zapasowych offline, odizolowane od sieci, do ochrony przed ransomware.

INSTRUKCJE DO PRZEWODNIKA PO OCHRONIE DANYCH

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 ochrony danych. Zakończ zadaniem dodatkowym Myśl szybko.

OCHRONA DANYCH I BEZPIECZEŃSTWO PAMIĘCI MASOWEJ W FIRMIE (WPROWADZENIE)

Ochrona danych zabezpiecza firmowe zasoby danych za pomocą maskowania, tokenizacji, szyfrowania baz danych w spoczynku oraz bezpiecznych protokołów transmisji. Projektowanie kopii zapasowych odizolowanych od sieci pomaga zapewnić możliwość przywrócenia kluczowych baz danych w razie trwającego włamania.

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

Punkt kontrolny 1: Wyzwanie – test wielokrotnego wyboru

1. Jaki jest główny cel maskowania danych?

- A. Zastępowanie wrażliwych identyfikatorów fikcyjnymi, ale realistycznymi znakami w celu ochrony prywatności
- B. Kompresowanie dużych plików baz danych, aby oszczędzić fizyczne miejsce na serwerze
- C. Usuwanie starych e-maili kontaktowych klientów z archiwalnych systemów kopii zapasowych
- D. Ukrywanie publicznego adresu IP serwera bazy danych przed skanami internetowymi

2. Który mechanizm szyfruje pliki przechowywane na dysku twardym serwera bazy danych?

- A. Szyfrowanie całego dysku w spoczynku
- B. Protokoły uzgadniania sesji TLS podczas przesyłania
- C. Reguły przekazywania serwerów nazw dynamicznego DNS
- D. Uwierzytelnianie wieloskładnikowe z użyciem kluczy sprzętowych

3. Co reprezentuje dane w tranzycie?

- A. Pakiety danych przemieszczające się przez routery i przełączniki sieciowe
- B. Przechowywane dzienniki transakcji bazy danych na zimnym dysku kopii zapasowych
- C. Zarchiwizowane pliki użytkowników zapisane w izolowanym skarbcu w chmurze
- D. Statyczne pliki konfiguracyjne systemu na lokalnym dysku komputera

4. Dlaczego regularna kopia zapasowa offline jest kluczowa dla ochrony przed ransomware?

- A. Zapewnia czystą kopię offline do przywrócenia plików bez płacenia okupu
- B. Uniemożliwia hakerom skanowanie konfiguracji otwartych portów
- C. Zwiększa przepustowość transmisji w sieci lokalnej
- D. Automatyzuje dzienniki zgody na pliki cookie w przeglądarkach

5. Co robi tokenizacja danych?

- A. Zastępuje wrażliwe numery kart niewrażliwymi losowymi tokenami
- B. Kieruje ruch internetowy przez wiele bezpiecznych węzłów onion
- C. Skanuje katalogi systemowe w poszukiwaniu złośliwego oprogramowania na podstawie sygnatur
- D. Audytuje czasy sesji logowania administratorów bazy danych

Punkt kontrolny 2: Wyzwanie – prawda czy fałsz

6 Pytanie 6

6. Maskowanie danych trwale zmienia rekordy bazy danych w środowiskach produkcyjnych.

- ○ Prawda
- ○ Fałsz

7 Pytanie 7

7. Kopie zapasowe poza siedzibą muszą być odizolowane od głównej sieci firmowej, aby zapobiec rozprzestrzenianiu się ransomware.

- ○ Prawda
- ○ Fałsz

8 Pytanie 8

8. Certyfikaty SSL/TLS zabezpieczają bazy danych, szyfrując dane przechowywane w spoczynku na nośnikach fizycznych.

- ○ Prawda
- ○ Fałsz

9 Pytanie 9

9. Zero-trust network access (ZTNA) weryfikuje tożsamość każdego użytkownika przed przyznaniem dostępu do bazy danych.

- ○ Prawda
- ○ Fałsz

10 Pytanie 10

10. Tokenizacja oparta na skarbcu (vault) przechowuje oryginalne wartości kart w bezpiecznym, centralnym skarbcu tokenów.

- ○ Prawda
- ○ Fałsz

Punkt kontrolny 3: Wstawianie kluczowych terminów

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

1. Zastępowanie nazw osobowych realistycznymi symbolami zastępczymi to _____ danych.

2. Szyfrowanie fizycznych bloków pamięci chroni zasoby bazy danych, czyli dane _____ .

3. Protokoły TLS szyfrują aktywne pakiety danych, czyli dane _____ .

4. Uprawnienia oparte na rolach ograniczają, którzy użytkownicy mogą uzyskać _____ do bazy danych.

5. Aby po naruszeniu przywrócić czyste pliki firmowe, potrzebna jest bezpieczna _____ offline.

6. Audyt konfiguracji chmury ocenia stan bezpieczeństwa organizacji, określany jako _____ .

BANK SŁÓW

DOSTĘP | KOPIA ZAPASOWA | MASKOWANIE | MINIMALIZACJA | NARUSZENIE | POSTURA | W SPOCZYNKU | W TRANZYCIE

Wpisz tutaj swoje odpowiedzi:

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

Punkt kontrolny 4: Dopasowywanie pojęć z zakresu bezpieczeństwa

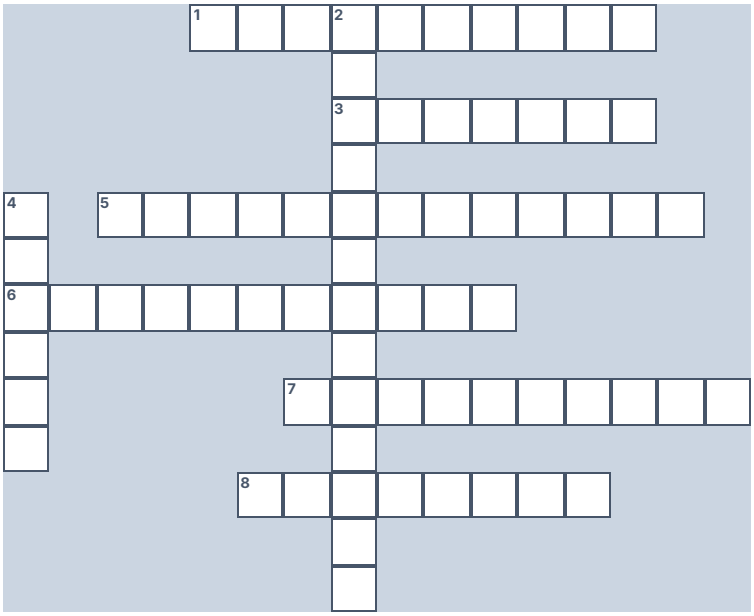
DOPASOWYWANIE DEFINICJI

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

☐	1. SZYFROWANIE	A	Tworzenie bezpiecznych zewnętrznych kopii danych, aby przywrócić je w razie awarii systemu.
☐	2. KOPIA ZAPASOWA	B	Przekształcanie tekstu jawnego w nieczytelny szyfrogram, aby przechwycone dane pozostały prywatne.
☐	3. MINIMALIZACJA	C	Zbiorczy stan bezpieczeństwa i gotowość obronna chmury organizacji.
☐	4. DOSTĘP	D	Spełnianie standardów regulacyjnych, takich jak RODO (GDPR) lub CCPA, w zakresie zarządzania prywatnymi informacjami użytkowników.
☐	5. STAN ZABEZPIECZEŃ	E	Incydent bezpieczeństwa, w którym chronione dane są udostępnione lub ujawnione bez upoważnienia.
☐	6. NARUSZENIE	F	Ograniczanie uprawnień do odczytu i zapisu w bazie danych do uwierzytelnionych ról użytkowników.
☐	7. ZGODNOŚĆ	G	Zastępowanie wrażliwych znaków w polach bazy danych w celu ochrony tożsamości osób.
☐	8. MASKOWANIE	H	Ograniczanie zbierania danych osobowych do absolutnego minimum wymaganego do działania.

Punkt kontrolny 5: Krzyżówka

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



POZIOMO

1. Zastępowanie wrażliwych znaków w polach bazy danych w celu ochrony tożsamości osób (10)

3. Ogólny stan bezpieczeństwa i gotowość obronna chmury organizacji (7)

5. Ograniczanie zbierania danych osobowych do absolutnego minimum potrzebnego do działania (13)

6. Przekształcanie tekstu jawnego w nieczytelny szyfrogram, aby przechwycone dane pozostały prywatne (11)

7. Incydent bezpieczeństwa, w którym chronione dane są udostępniane lub ujawniane bez zezwolenia (10)

8. Spełnianie standardów regulacyjnych, takich jak RODO lub CCPA, przy zarządzaniu prywatnymi danymi użytkowników (8)

PIONOWO

2. Tworzenie bezpiecznych zewnętrznych kopii danych do odtworzenia po awarii systemu (13)

4. Ograniczanie uprawnień do odczytu i zapisu w bazie danych do uwierzytelnionych ról użytkowników (6)

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

1 poziomo: Zastępowanie wrażliwych znaków w polach bazy danych w celu ochrony tożsamości osób (10 liter):

3 poziomo: Ogólny stan bezpieczeństwa i gotowość obronna chmury organizacji (7 liter):

5 poziomo: Ograniczanie zbierania danych osobowych do absolutnego minimum potrzebnego do działania (13 liter):

6 poziomo: Przekształcanie tekstu jawnego w nieczytelny szyfrogram, aby przechwycone dane pozostały prywatne (11 liter):

7 poziomo: Incydent bezpieczeństwa, w którym chronione dane są udostępniane lub ujawniane bez zezwolenia (10 liter):

8 poziomo: Spełnianie standardów regulacyjnych, takich jak RODO lub CCPA, przy zarządzaniu prywatnymi danymi użytkowników (8 liter):

PIONOWO

2 pionowo: Tworzenie bezpiecznych zewnętrznych kopii danych do odtworzenia po awarii systemu (13 liter):

4 pionowo: Ograniczanie uprawnień do odczytu i zapisu w bazie danych do uwierzytelnionych ról użytkowników (6 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 K D L Q N K A Ę O E K Ń Ć N

J C Ć G I Ą Ą Ó R I I Ł P W T

C I Ź Ę Ź S G Y N X N H Ę R T

A Ń U K R Ć T A S Ł A P Ł N Ś

Z H L P H Ź W Ó Ł X W V Ń Z Q

I Q Ą A Ł O Ó N Ą Ł O I Ę J D

L Ń Z B K Ż Ż Ź B N R V Y M O

A C Ę S Ó X P Q Y G F D Ź B S

M X A Ł E G G Ż X C Y O Q K T

I M Y Y R L Ż A N R Z Ż R M Ę

N K O P I A Z A P A S O W A P

I F Ś Z G O D N O Ś Ć W F Ł X

M J N A R U S Z E N I E B Ź C

B Ź O V Ż O Ż U T Ą H W P Y C

N M A R U T S O P H Ó Y Ź Ż Y

LISTA SŁÓW

SZYFROWANIE KOPIAZAPASOWA MINIMALIZACJA DOSTĘP POSTURA NARUSZENIE ZGODNOŚĆ MASKOWANIE

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. SZYFROWANIE**
- **B. KOPIAZAPASOWA**
- **C. MINIMALIZACJA**
- **D. DOSTĘP**
- **E. POSTURA**
- **F. NARUSZENIE**
- **G. ZGODNOŚĆ**
- **H. MASKOWANIE**

DEFINICJE I POLA DOPASOWANIA

1. Incydent bezpieczeństwa, w którym chronione dane są udostępniane lub ujawniane bez zezwolenia.
2. Zastępowanie wrażliwych znaków w polach bazy danych w celu ochrony tożsamości osób.
3. Ograniczanie uprawnień do odczytu i zapisu w bazie danych do uwierzytelnionych ról użytkowników.
4. Ogólny stan bezpieczeństwa i gotowość obronna chmury organizacji.
5. Spełnianie standardów regulacyjnych, takich jak RODO lub CCPA, przy zarządzaniu prywatnymi danymi użytkowników.
6. Ograniczanie zbierania danych osobowych do absolutnego minimum potrzebnego do działania.
7. Przekształcanie tekstu jawnego w nieczytelny szyfrogram, aby przechwycone dane pozostały prywatne.
8. Tworzenie bezpiecznych zewnętrznych kopii danych do odtworzenia po awarii systemu.

Punkt kontrolny 7: Wyzwanie – pomieszane słowa

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

1. RWIZOASNYE F
2. JMIANMCLAZ AII
3. TPUASRO
4. DŚĆONZGO
5. AOOPPAAZSA KWI
6. ĘTDSPO
7. AUNEZNIESR
8. IKWEMOAANS

Zadanie dodatkowe: Myśl szybko

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

1	Rzeczy, z których robisz kopie zapasowe			
2	Słowa związane z cyberbezpieczeństwem			
3	Osoby uprawnione do wglądu w dane wrażliwe			
4	Sposoby na bezpieczne usuwanie danych			
5	Miejsca, w których przechowywane są dane			
6	Rzeczy, które powinny być szyfrowane			
7	Dane, które szpital musi chronić			
8	Rodzaje kopii zapasowej			
9	Informacje, których nigdy nie powinieneś udostępniać			
10	Sygnały ostrzegawcze w e-mailu			
11	Bezpieczne nawyki, które możesz zacząć już dziś			
12	Osoby, które możesz poprosić o pomoc IT			
13	Urządzenia, które można zhakować			
14	Sposoby na ochronę danych			
15	Rzeczy, które mogą zniszczyć dane			

Punkt kontrolny 8: Studia przypadków z cyberbezpieczeństwa

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

STUDIUM PRZYPADKU 1: MODERNIZACJA SZYFROWANIA BAZY DANYCH W SPOCZYNKU W FIRMIE



Scenariusz: Sprzedawca internetowy przechowuje bazy danych transakcji w pamięci chmurowej bez pełnego szyfrowania dysku. Niedawny audyt zgodności oznaczył to jako poważne ryzyko dla bezpieczeństwa danych według CCPA. Zaprojektuj architekturę odzyskiwania.

Pytanie do dyskusji: Przeanalizuj ryzyka związane ze zgodnością z CCPA i zaproponuj strategię szyfrowania danych w spoczynku.

STUDIUM PRZYPADKU 2: OGRANICZENIE RANSOMWARE I ODZYSKIWANIE DANYCH



Scenariusz: Aktywny atak ransomware szyfruje dyski sieciowe w firmowej sieci lokalnej. Administrator wykrył infekcję wcześnie. Zaplanuj kroki powstrzymania i odzyskiwania.

Pytanie do dyskusji: Opisz szczegółowo natychmiastowe działania powstrzymujące i zaplanuj bezpieczny proces przywracania.

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	30	20	13	7		6	1	18	7		33	1	
22	20	17	20	4	2		3	7	33	22	12	7	4	33	18	32	4	11	
14	20	18	27	24	20	15	12												

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 ochrona danych?

To proces zabezpieczania danych osobistych i biznesowych przed nieautoryzowanym dostępem, utratą lub uszkodzeniem za pomocą środków technicznych.

Q2: Dlaczego szyfrowanie całego dysku jest ważne?

Zabezpiecza przechowywane bloki danych na dyskach fizycznych, uniemożliwiając odczyt danych komukolwiek, kto fizycznie ukradnie dysk twardy.

Q3: Jaka jest różnica między szyfrowaniem danych w spoczynku a w tranzycie?

Szyfrowanie danych w spoczynku zabezpiecza pliki zapisane na dyskach, a szyfrowanie danych w tranzycie zabezpiecza aktywne pakiety sieciowe przemieszczające się przez routery.

Q4: Czym jest maskowanie danych?

Zastępuje wrażliwe dane (takie jak numery kart kredytowych) fikcyjnymi, ale realistycznymi danymi do testowania bez ujawniania prawdziwych rekordów.

Q5: Dlaczego kopia zapasowa offline jest ważna?

Przechowuje czystą kopię Twoich plików odizolowaną od sieci, co pomaga chronić kopie zapasowe przed zaszyfrowaniem przez ransomware.

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

Przejrzyj typowe pytania i odpowiedzi dotyczące ograniczania zagrożeń w sieci.

Q6: Czym jest skarbiec tokenizacji danych?

Bezpieczna, izolowana baza danych, która mapuje losowe tokeny na ich oryginalne wrażliwe wartości (takie jak główne numery kart kredytowych).

Q7: Co oznacza dostęp do bazy danych w modelu zero trust?

Oznacza weryfikację tożsamości i stanu urządzenia każdego użytkownika przy każdym logowaniu, zamiast ufania komukolwiek wewnątrz sieci.

Q8: Jak TLS chroni dane w tranzycie?

TLS szyfruje ładunek sesji TCP, uniemożliwiając złośliwym osobom w sieciach publicznych podsłuchiwanie lub modyfikowanie przesyłanych pakietów.

Q9: Czym jest audytowanie dostępu do bazy danych?

Ciągłe rejestrowanie zapytań do bazy danych i logowań w celu wykrywania wzorców nieautoryzowanego dostępu lub anomalii bezpieczeństwa.

Q10: Czym jest audyt stanu bezpieczeństwa chmury?

Proces analizujący konfiguracje chmury w celu identyfikacji otwartych portów, błędnie skonfigurowanych reguł dostępu i luk w zgodności z wymogami bezpieczeństwa.

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 działa szyfrowanie kopertowe?

Szyfruje dane kluczem danych, a następnie szyfruje ten klucz danych kluczem głównym, upraszczając przechowywanie i rotację kluczy.

Q2: Czym jest szyfrowanie homomorficzne?

Zaawansowana metoda szyfrowania pozwalająca wykonywać operacje bezpośrednio na zaszyfrowanych danych bez ich wcześniejszego odszyfrowywania.

Q3: Dlaczego stosuje się szyfrowanie na poziomie kolumn w bazie danych?

Szyfruje osobno wybrane wrażliwe kolumny (np. numery SSN), chroniąc je nawet wtedy, gdy administratorzy uzyskają ogólny dostęp do odczytu tabeli.

Q4: Czym jest zapobieganie utracie danych (DLP)?

Oprogramowanie monitorujące punkty wyjścia z sieci w celu wykrywania i blokowania nieautoryzowanych wychodzących transferów wrażliwych plików.

Q5: Jak kopie zapasowe typu write-once-read-many (WORM) chronią przed ransomware?

Kopie zapasowe WORM uniemożliwiają usuwanie lub modyfikowanie plików przez określony czas, co chroni istniejące kopie zapasowe przed zaszyfrowaniem przez ransomware.

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: Jakie ryzyko wiąże się z ponownym użyciem kluczy?

Używanie tego samego klucza kryptograficznego w różnych bazach danych oznacza, że naruszenie jednego klucza ujawnia wszystkie bazy danych.

Q7: Jak tokenizacja bazy danych poprawia zgodność z CCPA?

Tokeny pseudonimizują rekordy w systemach nieprodukcyjnych i ograniczają skutki naruszenia, ale zatokenizowane dane nadal mogą być danymi osobowymi.

Q8: Dlaczego klasyfikacja danych jest kluczowa?

Kategoryzuje pliki według poziomu wrażliwości, pomagając organizacjom stosować najsilniejsze szyfrowanie i kontrolę dostępu do danych wysokiego ryzyka.

Q9: Jaką rolę odgrywa rotacja kluczy?

Regularna aktualizacja kluczy szyfrowania ogranicza ilość ujawnionych danych historycznych, jeśli pojedynczy klucz zostanie w końcu złamany.

Q10: Jak bezpieczne enklawy chronią zapytania do bazy danych w pamięci?

Bezpieczne enklawy izolują operacje zapytań w blokach pamięci chronionych przez procesor, co uniemożliwia administratorom hosta przeglądanie jawnego tekstu w pamięci RAM.

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

Przepisy RODO (GDPR) weszły w życie w maju 2018 roku, zmieniając sposób, w jaki serwisy na całym świecie zarządzają zgodami na pliki cookie i rejestrami danych osobowych.

2. WGLĄD W BEZPIECZEŃSTWO

Kara za naruszenie RODO (GDPR) może sięgnąć 20 milionów euro lub 4% globalnego obrotu, co oznacza znaczną odpowiedzialność prawną. [4]

3. WGLĄD W BEZPIECZEŃSTWO

CCPA weszła w życie w styczniu 2020 r., ustanawiając pionierskie prawa konsumentów w zakresie prywatności cyfrowej w Stanach Zjednoczonych.

4. WGLĄD W BEZPIECZEŃSTWO

Minimalizacja danych zmniejsza zajmowane miejsce w bazie danych, obniżając koszty działania serwerów, a jednocześnie zmniejsza skalę skutków naruszenia.

5. WGLĄD W BEZPIECZEŃSTWO

Kryptograficzne niszczenie rozwiązuje problem usuwania kopii zapasowych, usuwając klucze zamiast edytować historyczne pliki taśm z kopiami zapasowymi.

6. WGLĄD W BEZPIECZEŃSTWO

Większość krajów na świecie uchwaliła obecnie przepisy o ochronie danych osobowych, aby chronić prawa konsumentów do prywatności.

7. WGLĄD W BEZPIECZEŃSTWO

Formularze zgody typu opt-in z zaznaczonymi z góry polami wyboru są wyraźnie zakazane przez europejskie regulacje dotyczące prywatności danych.

8. WGLĄD W BEZPIECZEŃSTWO

RODO (GDPR) wymaga zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu w ciągu 72 godzin od stwierdzenia naruszenia, o ile jest to możliwe. [3]

9. WGLĄD W BEZPIECZEŃSTWO

Haszowanie haseł powolnymi algorytmami, takimi jak bcrypt lub Argon2, znacznie utrudnia offline'owe łamanie skradzionych skrótów. [6]

10. WGLĄD W BEZPIECZEŃSTWO

Dane w spoczynku to zapisane pliki baz danych, a dane w tranzycie to pakiety aktywnie przemieszczające się przez routery sieciowe.

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. (2025). SP 800-88 Rev. 2, Guidelines for Media Sanitization.

https://csrc.nist.gov/pubs/sp/800/88/r2/final

[2] CISA. (2023). #StopRansomware Guide.

https://www.cisa.gov/stopransomware/ransomware-guide

[3] Intersoft Consulting. (n.d.). Art. 33 GDPR – Notification of a personal data breach to the supervisory authority.

https://gdpr-info.eu/art-33-gdpr/

[4] Intersoft Consulting. (n.d.). Art. 83 GDPR – General conditions for imposing administrative fines.

https://gdpr-info.eu/art-83-gdpr/

[5] California Privacy Protection Agency. (n.d.). Frequently Asked Questions (FAQs).

https://cppa.ca.gov/faq.html

[6] OWASP. (n.d.). Password Storage Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

Klucz odpowiedzi: Punkt kontrolny 1 – test wielokrotnego wyboru

1 Pytanie 1

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Jaki jest główny cel maskowania danych? → Zastępowanie wrażliwych identyfikatorów fikcyjnymi, ale realistycznymi znakami w celu ochrony prywatności

2 Pytanie 2

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Który mechanizm szyfruje pliki przechowywane na dysku twardym serwera bazy danych? → Szyfrowanie całego dysku w spoczynku

3 Pytanie 3

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Co reprezentuje dane w tranzycie? → Pakiety danych przemieszczające się przez routery i przełączniki sieciowe

4 Pytanie 4

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Dlaczego regularna kopia zapasowa offline jest kluczowa dla ochrony przed ransomware? → Zapewnia czystą kopię offline do przywrócenia plików bez płacenia okupu

5 Pytanie 5

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Co robi tokenizacja danych? → Zastępuje wrażliwe numery kart niewrażliwymi losowymi tokenami

Klucz odpowiedzi: Punkt kontrolny 2 – prawda czy fałsz

6 Pytanie 6

Poprawna odpowiedź: Fałsz

UWAGA DLA NAUCZYCIELA

Maskowanie zmienia kopie testowe lub ukrywa wartości w momencie zapytania; rekordy produkcyjne pozostają bez zmian.

7 Pytanie 7

Poprawna odpowiedź: Prawda

UWAGA DLA NAUCZYCIELA

Kopie zapasowe poza siedzibą muszą być odizolowane od głównej sieci firmowej, aby zapobiec rozprzestrzenianiu się ransomware.

8 Pytanie 8

Poprawna odpowiedź: Fałsz

UWAGA DLA NAUCZYCIELA

Certyfikaty TLS chronią dane w tranzycie; dane w spoczynku wymagają szyfrowania dysku, plików lub bazy danych.

9 Pytanie 9

Poprawna odpowiedź: Prawda

UWAGA DLA NAUCZYCIELA

Zero-trust network access (ZTNA) weryfikuje tożsamość każdego użytkownika przed przyznaniem dostępu do bazy danych.

10 Pytanie 10

Poprawna odpowiedź: Prawda

UWAGA DLA NAUCZYCIELA

Tokenizacja oparta na skarbcu (vault) przechowuje oryginalne wartości w bezpiecznym skarbcu tokenów, który przyporządkowuje każdy token do jego danych.

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

B 1. SZYFROWANIE	A 2. KOPIA ZAPASOWA	H 3. MINIMALIZACJA	F 4. DOSTĘP
C 5. STAN ZABEZPIECZEŃ	E 6. NARUSZENIE	D 7. ZGODNOŚĆ	G 8. MASKOWANIE

PUNKT KONTROLNY 3: KLUCZ – KLUCZOWE POJĘCIA

1 MASKOWANIE	2 W SPOCZYNKU	3 W TRANZYCIE	4 DOSTĘP
5 KOPIA ZAPASOWA	6 POSTURA		

PUNKT KONTROLNY 6, WARIANT ALTERNATYWNY: KLUCZ – DOPASOWYWANIE SŁÓW

1 F – NARUSZENIE	2 H – MASKOWANIE	3 D – DOSTĘP	4 E – POSTURA
5 G – ZGODNOŚĆ	6 C – MINIMALIZACJA	7 A – SZYFROWANIE	8 B – KOPIAZAPASOWA

UWAGI DO DYSKUSJI DLA NAUCZYCIELI

Kluczowe pojęcia:
Sprawdź, czy uczniowie potrafią własnymi słowami wyjaśnić pojęcia SZYFROWANIE, KOPIA ZAPASOWA i MINIMALIZACJA 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	K	D	L	Q	N	K	A	Ę	O	E	K	Ń	Ć	N
J	C	Ć	G	I	Ą	Ą	Ó	R	I	I	Ł	P	W	T
C	I	Ź	Ę	Ź	S	G	Y	N	X	N	H	Ę	R	T
A	Ń	U	K	R	Ć	T	A	S	Ł	A	P	Ł	N	Ś
Z	H	L	P	H	Ź	W	Ó	Ł	X	W	V	Ń	Z	Q
I	Q	Ą	A	Ł	O	Ó	N	Ą	Ł	O	I	Ę	J	D
L	Ń	Z	B	K	Ż	Ż	Ź	B	N	R	V	Y	M	O
A	C	Ę	S	Ó	X	P	Q	Y	G	F	D	Ź	B	S
M	X	A	Ł	E	G	G	Ż	X	C	Y	O	Q	K	T
I	M	Y	Y	R	L	Ż	A	N	R	Z	Ż	R	M	Ę
N	K	O	P	I	A	Z	A	P	A	S	O	W	A	P
I	F	Ś	Z	G	O	D	N	O	Ś	Ć	W	F	Ł	X
M	J	N	A	R	U	S	Z	E	N	I	E	B	Ź	C
B	Ź	O	V	Ż	O	Ż	U	T	Ą	H	W	P	Y	C
N	M	A	R	U	T	S	O	P	H	Ó	Y	Ź	Ż	Y

ROZWIĄZANIE KRZYŻÓWKI



PRZEWODNIK DLA NAUCZYCIELA: ROZWIĄZANIA KRZYŻÓWKI

POZIOMO

1 poziomo: MASKOWANIE Zastępowanie wrażliwych znaków w polach bazy danych w celu ochrony tożsamości osób (10 liter)

3 poziomo: POSTURA Ogólny stan bezpieczeństwa i gotowość obronna chmury organizacji (7 liter)

5 poziomo: MINIMALIZACJA Ograniczanie zbierania danych osobowych do absolutnego minimum potrzebnego do działania (13 liter)

6 poziomo: SZYFROWANIE Przekształcanie tekstu jawnego w nieczytelny szyfrogram, aby przechwycone dane pozostały prywatne (11 liter)

7 poziomo: NARUSZENIE Incydent bezpieczeństwa, w którym chronione dane są udostępniane lub ujawniane bez zezwolenia (10 liter)

8 poziomo: ZGODNOŚĆ Spełnianie standardów regulacyjnych, takich jak RODO lub CCPA, przy zarządzaniu prywatnymi danymi użytkowników (8 liter)

PIONOWO

2 pionowo: KOPIAZAPASOWA Tworzenie bezpiecznych zewnętrznych kopii danych do odtworzenia po awarii systemu (13 liter)

4 pionowo: DOSTĘP Ograniczanie uprawnień do odczytu i zapisu w bazie danych do uwierzytelnionych ról użytkowników (6 liter)

Klucz do słów rozsypanych i rozwiązania szyfru

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

KLUCZ DO ROZWIĄZANIA ANAGRAMÓW

1. RWIZOASNYEF — **SZYFROWANIE**
2. JMIANMCLAZAII — **MINIMALIZACJA**
3. TPUASRO — **POSTURA**
4. DŚĆONZGO — **ZGODNOŚĆ**
5. AOOPPAAZSAKWI — **KOPIAZAPASOWA**
6. ĘTDSPO — **DOSTĘP**
7. AUNEZNIESR — **NARUSZENIE**
8. IKWEMOAANS — **MASKOWANIE**

KLUCZ DO WYZWANIA Z TAJNYM SZYFREM

"CHROŃ SWOJE DANE ZA POMOCĄ BEZPIECZNYCH KONTROLI"

Klucz odpowiedzi do studiów przypadków

A Studium przypadku 1: Modernizacja szyfrowania bazy danych w spoczynku w firmie

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Sklep internetowy przechowuje bazy danych transakcji w chmurze bez szyfrowania całego dysku. Niedawny audyt zgodności uznał to za poważne ryzyko dla bezpieczeństwa danych w świetle CCPA. Zaprojektuj architekturę odzyskiwania danych.
- Zalecana strategia i rozwiązanie: Wdróż szyfrowanie całych dysków AES-256 dla danych spoczynkowych we wszystkich systemach plików. Użyj scentralizowanej usługi zarządzania kluczami (KMS) z automatyczną rotacją i egzekwuj ścisłe polityki IAM kontrolujące dostęp do odszyfrowywania.

B Studium przypadku 2: Ograniczenie ransomware i odzyskiwanie danych

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Aktywny atak ransomware szyfruje dyski sieciowe w firmowej sieci lokalnej. Administrator wcześnie wykrył infekcję. Zaplanuj kroki powstrzymania ataku i odzyskiwania danych.
- Zalecana strategia i rozwiązanie: Natychmiast odizoluj naruszony segment. Sformatuj zaatakowane punkty końcowe i przywróć dane z najnowszej kopii zapasowej offline typu WORM (write-once-read-many). Zweryfikuj integralność kopii zapasowej przed ponownym podłączeniem systemów.