Jméno: _____ Datum: _____ Body: _____

Ochrana dat a podnikové úložiště Průvodce zabezpečením

Maskování dat, tokenizace, šifrování v klidu vs. při přenosu, offline zálohy

PŘEHLED VÝUKY: OCHRANA DAT

ZABEZPEČENO

ŠIFROVÁNÍ DAT

Standard 256bitového AES

VYHOVUJÍCÍ

GLOBÁLNÍ STANDARDY

Rámce GDPR a CCPA

ZERO-TRUST

ZÁSADY PŘÍSTUPU

Vícefaktorové ověřování

Vítejte! Tento balíček aktivit vás provede standardy a kontrolami ochrany dat. Prozkoumáte šifrování celého disku, bezpečné řízení přístupu, hardwarové zálohy, zabezpečení cloudu a techniky maskování dat.

KONTROLNÍ BODY PRACOVNÍHO LISTU

- [ ] **Část 1-4: Zvládněte kyberbezpečnost a prevenci hrozeb.**
- [ ] **Část 5-7: Vyřešte křížovku a osmisměrku.**
- [ ] **Část 8-9: Vyřešte případové studie a šifrovací výzvu.**
- [ ] **Část 10: Projděte si stránky se základními i pokročilými FAQ.**
- [ ] **Část 11: Prozkoumejte 10 zajímavých faktů z praxe.**
- [ ] **Bonus: výzva Mysli rychle.**

Otevřete průvodce kyberbezpečností od VPN.com

URL: https://www.vpn.com/cs/kyberneticka-bezpecnost/ochrana-dat/

Váš studijní plán: strategie ochrany dat

- Rozlište techniky maskování dat a tokenizace.
- Zavést šifrování v klidu pro úložné disky a šifrování při přenosu pomocí TLS.
- Navrhněte offline, síťově izolované zálohovací systémy pro ochranu před ransomwarem.

POKYNY K PRŮVODCI OCHRANOU DAT

Odpovězte na otázky s výběrem odpovědí a otázky pravda/nepravda, doplňte věty s vynechanými slovy pomocí banky slov, přiřaďte definice a vyřešte křížovku a osmisměrku. Uplatněte své znalosti na ochranu dat. Zakončete bonusovou aktivitou Mysli rychle.

OCHRANA DAT A ZABEZPEČENÍ PODNIKOVÝCH ÚLOŽIŠŤ (ÚVOD)

Ochrana dat chrání firemní datová aktiva pomocí maskování, tokenizace, šifrování databází v klidu a zabezpečených přenosových protokolů. Návrh síťově izolovaných záloh pomáhá zajistit, že klíčové databáze půjde obnovit i v případě aktivního průniku.

PŘEČTĚTE SI POZORNĚ KAŽDÝ KONTROLNÍ BOD A VYBERTE NEBO NAPIŠTE SPRÁVNOU ODPOVĚĎ.

Kontrolní bod 1: Výzva s výběrem odpovědí

1. **1. Jaký je primární účel maskování dat?**
   - A. Nahrazování citlivých identifikátorů smyšlenými, ale realistickými znaky na ochranu soukromí
   - B. Komprese velkých databázových souborů kvůli úspoře fyzického úložiště serveru
   - C. Mazání starých kontaktních e-mailů zákazníků z archivních záložních systémů
   - D. Skrytí veřejné IP adresy databázového serveru před internetovými skeny

2. **2. Jaký mechanismus šifruje soubory uložené na pevném disku databázového serveru?**
   - A. Šifrování celého disku v klidovém stavu
   - B. Protokoly TLS handshake relace při přenosu
   - C. Pravidla přesměrování dynamických DNS jmenných serverů
   - D. Vícefaktorová autentizace pomocí hardwarových klíčů

3. **3. Co představují data při přenosu?**
   - A. Datové pakety putující přes síťové routery a přepínače
   - B. Uložené transakční logy databáze na studeném záložním disku
   - C. Archivované uživatelské soubory uložené v izolovaném cloudovém trezoru
   - D. Statické systémové konfigurační soubory na místním desktopovém úložišti

4. **4. Proč je pravidelná offline záloha kritická pro ochranu před ransomwarem?**
   - A. Poskytuje čistou offline kopii k obnovení souborů bez placení výkupného
   - B. Brání hackerům ve skenování otevřených portů
   - C. Zvyšuje šířku pásma přenosu v místní síti
   - D. Automatizuje logy souhlasů s cookies v prohlížečích

5. **5. Co dělá tokenizace dat?**
   - A. Nahrazuje citlivá čísla karet necitlivými náhodnými tokeny
   - B. Směruje webový provoz přes několik zabezpečených onion uzlů
   - C. Skenuje systémové adresáře na malware podle signatur
   - D. Audituje časy přihlašovacích relací správců databáze

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. Maskování dat mění databázové záznamy v produkčním prostředí trvale.

○ Pravda ○ Nepravda

7 Otázka 7

7. Zálohy mimo pracoviště musí být izolovány od hlavní firemní sítě, aby se zabránilo šíření ransomwaru.

○ Pravda ○ Nepravda

8 Otázka 8

8. Certifikáty SSL/TLS zabezpečují databáze šifrováním dat uložených v klidu na fyzických médiích.

○ Pravda ○ Nepravda

9 Otázka 9

9. Zero-trust network access (ZTNA) ověřuje identitu každého uživatele před udělením přístupu k databázi.

○ Pravda ○ Nepravda

10 Otázka 10

10. Tokenizace s trezorem ukládá původní hodnoty karet v zabezpečeném centrálním trezoru tokenů.

○ Pravda ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

Přečtěte si každou větu níže a doplňte do vynechaného místa správný termín ze slovní banky.

1. Nahrazování osobních jmen realistickými zástupnými hodnotami se nazývá _____ dat.

2. Šifrování fyzických úložných bloků chrání databázová aktiva _____ .

3. Protokoly TLS šifrují aktivní datové pakety během _____ .

4. Oprávnění podle rolí omezují, kteří uživatelé získají _____ k databázi.

5. Obnova čistých firemních souborů po incidentu vyžaduje bezpečnou offline _____ .

6. Audit cloudových konfigurací hodnotí bezpečnostní _____ organizace.

ZÁSOBNÍK SLOV

MASKOVÁNÍ | MINIMALIZACE | PŘENOS V KLIDU | PŘIPRAVENOST | PŘÍSTUP | ŠIFROVÁNÍ | ZÁLOHA

Sem napište své odpovědi:

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

Kontrolní bod 4: Přiřazování bezpečnostních pojmů

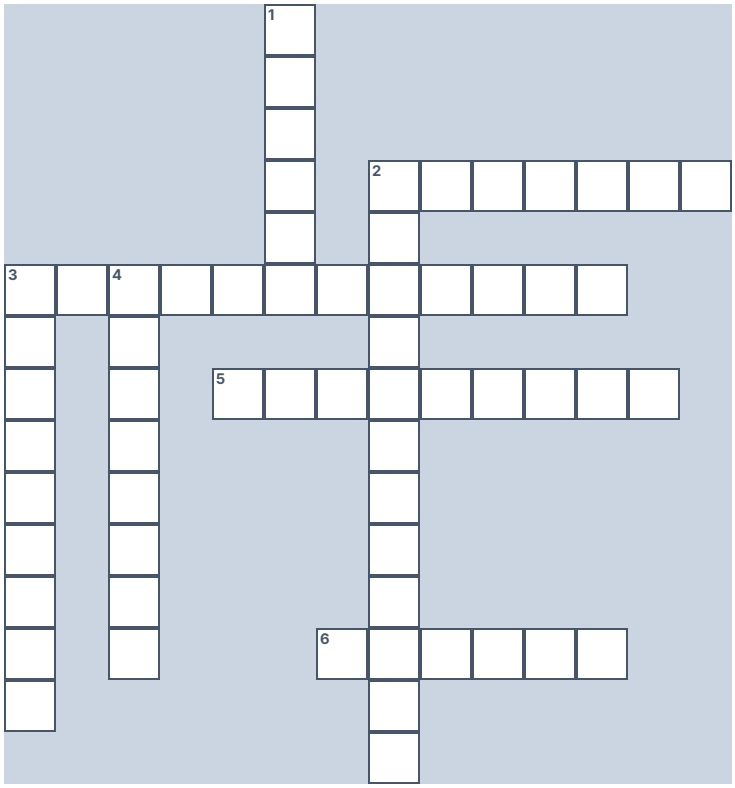
PŘIŘAZOVÁNÍ DEFINIC

Přiřaďte každý slovníčkový pojem vlevo k jeho správné definici vpravo zapsáním odpovídajícího písmene (A–H) do vyplnitelného pole.

☐	1. ŠIFROVÁNÍ	A	Vytváření bezpečných kopií dat mimo pracoviště pro obnovu při selhání systémů.
☐	2. ZÁLOHA	B	Přeměna prostého textu na nečitelný šifrovaný text, aby zachycená data zůstala soukromá.
☐	3. MINIMALIZACE	C	Souhrnný stav zabezpečení a obranná připravenost cloudu organizace.
☐	4. PŘÍSTUP	D	Plnění regulačních standardů, jako je GDPR nebo CCPA, při správě soukromých údajů uživatelů.
☐	5. STAV ZABEZPEČENÍ	E	Bezpečnostní incident, při němž jsou chráněná data zpřístupněna nebo zveřejněna bez oprávnění.
☐	6. NARUŠENÍ	F	Omezení práv čtení a zápisu do databáze na ověřené uživatelské role.
☐	7. SOULAD S PŘEDPISY	G	Nahrazování citlivých znaků v databázových polích k ochraně osobních identit.
☐	8. MASKOVÁNÍ	H	Omezení sběru osobních údajů na naprosté minimum nutné pro provoz.

Kontrolní bod 5: Křížovka

Vyřešte křížovku zapisováním písmen do aktivních bílých políček. Čísla odpovídají nápovědám níže.



VODOROVNÉ NÁPOVĚDY

2. Omezení oprávnění ke čtení a zápisu v databázi na ověřené uživatelské role. (7)

3. Omezení sběru osobních údajů na naprosté minimum nutné pro provoz. (12)

5. Přeměna čitelného textu na nečitelný šifrovaný text, aby zachycená data zůstala soukromá (9)

6. Plnění regulačních standardů jako GDPR nebo CCPA při správě soukromých údajů uživatelů. (6)

SVISLÉ NÁPOVĚDY

1. Vytváření bezpečných kopií dat mimo pracoviště pro obnovu při selhání systémů. (6)

2. Souhrnný stav zabezpečení a obranná připravenost cloudu organizace. (12)

3. Nahrazování citlivých znaků v databázových polích na ochranu osobních identit. (9)

4. Bezpečnostní incident, při němž dojde k neoprávněnému přístupu k chráněným datům nebo jejich vyzrazení (8)

Kontrolní bod 5, alternativa: Přístupná zadání křížovky

Uživatelé čteček obrazovky a klávesnice mohou odpovědi křížovky zapisovat přímo do textových polí níže.

VODOROVNÉ NÁPOVĚDY

2 vodorovně: Omezení oprávnění ke čtení a zápisu v databázi na ověřené uživatelské role. (7 písmen):

3 vodorovně: Omezení sběru osobních údajů na naprosté minimum nutné pro provoz. (12 písmen):

5 vodorovně: Přeměna čitelného textu na nečitelný šifrovaný text, aby zachycená data zůstala soukromá (9 písmen):

6 vodorovně: Plnění regulačních standardů jako GDPR nebo CCPA při správě soukromých údajů uživatelů. (6 písmen):

SVISLÉ NÁPOVĚDY

1 svisle: Vytváření bezpečných kopií dat mimo pracoviště pro obnovu při selhání systémů. (6 písmen):

2 svisle: Souhrnný stav zabezpečení a obranná připravenost cloudu organizace. (12 písmen):

3 svisle: Nahrazování citlivých znaků v databázových polích na ochranu osobních identit. (9 písmen):

4 svisle: Bezpečnostní incident, při němž dojde k neoprávněnému přístupu k chráněným datům nebo jejich vyzrazení (8 písmen):

Kontrolní bod 6: Hledání skrytých slov

Najděte 8 klíčových pojmů skrytých v mřížce níže. Slova mohou být vodorovně, svisle nebo úhlopříčně.

T	I	D	S	Ř	N	E	M	I	Š	Ž	T	É	Ř	Ů
S	E	A	Á	Ř	P	O	A	Q	U	N	Y	R	J	S
O	P	U	Š	Č	Ň	Ý	S	B	Ě	A	Š	X	W	Í
N	U	A	S	S	Ž	Ý	K	Ý	L	R	F	I	N	S
E	T	J	N	O	M	Ť	O	P	G	U	R	Ř	Š	G
V	S	Ž	Á	U	Ó	Ů	V	Ě	Ú	Š	C	Ý	I	Š
A	Í	Ý	B	L	G	M	Á	Ž	F	E	J	Ó	F	Q
R	Ř	O	X	A	C	N	N	Ž	Z	N	Ě	Ý	R	P
P	P	W	Ú	D	L	Ů	Í	Q	B	Í	Ó	V	O	Ť
I	N	F	Ů	Č	Ý	Ú	K	S	Á	X	Ž	Y	V	N
Ř	M	I	N	I	M	A	L	I	Z	A	C	E	Á	Š
P	R	X	H	P	D	Á	Č	J	Ř	V	W	X	N	L
Í	H	Z	Á	L	O	H	A	U	H	Ě	B	E	Í	I
K	Ť	Š	V	Ř	Z	E	H	E	Š	C	A	M	R	C
Ž	N	K	V	Š	Ú	Á	Š	X	J	N	N	G	H	Ň

SEZNAM SLOV

ŠIFROVÁNÍ ZÁLOHA MINIMALIZACE PŘÍSTUP PŘIPRAVENOST NARUŠENÍ SOULAD MASKOVÁNÍ

Kontrolní bod 6, alternativa: Přístupné přiřazování slovíček

Přiřaďte každý z 8 slovníčkových pojmů z osmisměrky k jeho správné definici zapsáním písmene (A–H) do prázdného pole.

POJMY SLOVNÍ ZÁSOBY

- **A. ŠIFROVÁNÍ**
- **B. ZÁLOHA**
- **C. MINIMALIZACE**
- **D. PŘÍSTUP**
- **E. PŘIPRAVENOST**
- **F. NARUŠENÍ**
- **G. SOULAD**
- **H. MASKOVÁNÍ**

DEFINICE A POLE K PŘIŘAZENÍ

1. Bezpečnostní incident, při němž dojde k neoprávněnému přístupu k chráněným datům nebo jejich vyzrazení.
2. Nahrazování citlivých znaků v databázových polích na ochranu osobních identit.
3. Omezení oprávnění ke čtení a zápisu v databázi na ověřené uživatelské role.
4. Souhrnný stav zabezpečení a obranná připravenost cloudu organizace.
5. Plnění regulačních standardů jako GDPR nebo CCPA při správě soukromých údajů uživatelů.
6. Omezení sběru osobních údajů na naprosté minimum nutné pro provoz.
7. Přeměna čitelného textu na nečitelný šifrovaný text, aby zachycená data zůstala soukromá.
8. Vytváření bezpečných kopií dat mimo pracoviště pro obnovu při selhání systémů.

Kontrolní bod 7: Výzva s přeházenými slovy

Přeuspořádejte písmena níže a odhalte klíčové pojmy a termíny kybernetické bezpečnosti. Odpovědi pište do připravených polí.

1. VORIŠÁNÍF
2. EIMAMACNIZLI
3. PŘEVSNIATROP
4. DLUASO
5. OLAZHÁ
6. UÍTPSPŘ
7. NÍŠENAUR
8. ÍONMKAVÁS

Bonusová aktivita: Mysli rychle

3 ODPOVĚDI V KAŽDÉ KATEGORII. VYHRÁVÁ, KDO PRVNÍ VYPLNÍ CELÝ SEZNAM.

1	Věci, které si zálohujete			
2	Slova související s kyberbezpečností			
3	Lidé, kteří smějí vidět citlivá data			
4	Způsoby, jak bezpečně smazat data			
5	Místa, kde jsou data uložena			
6	Věci, které by měly být šifrované			
7	Data, která musí nemocnice chránit			
8	Typy záloh			
9	Informace, které byste nikdy neměli sdílet			
10	Varovné signály v e-mailu			
11	Bezpečné návyky, se kterými můžete začít už dnes			
12	Lidé, které můžete požádat o pomoc s IT			
13	Zařízení, která lze hacknout			
14	Způsoby, jak chránit data			
15	Věci, které mohou zničit data			

Kontrolní bod 8: Případové studie kyberbezpečnosti

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

PŘÍPADOVÁ STUDIE 1: UPGRADE ŠIFROVÁNÍ PODNIKOVÉ DATABÁZE V KLIDOVÉM STAVU



Scénář: Online prodejce ukládá transakční databáze v cloudovém úložišti bez šifrování celého disku. Nedávný compliance audit to označil za vážné riziko zabezpečení dat podle CCPA. Navrhněte architekturu obnovy.

Otázka k diskusi: Analyzujte rizika souladu s CCPA a navrhněte strategii šifrování v klidu.

PŘÍPADOVÁ STUDIE 2: ZADRŽENÍ RANSOMWARU A OBNOVA DAT



Scénář: Aktivní ransomwarový útok šifruje síťové disky ve firemní místní síti. Administrátor infekci odhalil včas. Naplánujte kroky izolace a obnovy.

Otázka k diskusi: Popište okamžité kroky izolace a naplánujte bezpečný proces obnovy.

Kontrolní bod 9: Dešifrování šifry

Profesionál v kyberbezpečnosti chrání síťová aktiva před online útočníky. Pomocí níže uvedeného klíče písmeno–číslo dešifrujte zprávu zapsáním odpovídajících písmen do prázdných polí.

ŠIFROVACÍ KLÍČ PÍSMENO–ČÍSLO

A=1 Á=2 B=3 C=4 Č=5 D=6 Ď=7 E=8 É=9 Ě=10 F=11 G=12 H=13 I=14
Í=15 J=16 K=17 L=18 M=19 N=20 Ň=21 O=22 Ó=23 P=24 Q=25 R=26 Ř=27 S=28
Š=29 T=30 Ť=31 U=32 Ú=33 Ů=34 V=35 W=36 X=37 Y=38 Ý=39 Z=40 Ž=41

4	13	26	1	21	30	8		28	35	2		28	22	32	17	26	22	19	2
6	1	30	1		3	8	40	24	8	5	20	39	19	14		24	26	35	17	38

Dešifrovaná zpráva:

TIP: KAŽDÉ ČÍSLO PŘEDSTAVUJE POZICI DANÉHO PÍSMENE V ABECEDĚ (NAPŘ. 1 = A, 2 = B, 41 = Ž).

Kontrolní bod 10: Základní časté otázky ke kyberbezpečnosti (část A)

Projděte si časté otázky a odpovědi ohledně zmírňování online hrozeb.

Q1: Co je ochrana dat?

Je to proces zabezpečení osobních a firemních dat před neoprávněným přístupem, ztrátou nebo poškozením pomocí technických kontrol.

Q2: Proč je důležité šifrování celého disku?

Zabezpečuje uložené datové bloky na fyzických discích a brání komukoli číst data při fyzické krádeži pevného disku.

Q3: Jaký je rozdíl mezi šifrováním dat v klidu a při přenosu?

Šifrování v klidu zabezpečuje uložené soubory na discích, zatímco šifrování při přenosu zabezpečuje aktivní síťové pakety putující přes směrovače.

Q4: Co je maskování dat?

Nahrazuje citlivé údaje (jako čísla platebních karet) fiktivními, ale realistickými daty pro testování bez odhalení skutečných záznamů.

Q5: Proč je důležitá offline záloha?

Udržuje čistou kopii vašich souborů izolovanou od sítě, což pomáhá chránit vaše zálohy před zašifrováním ransomwarem.

Kontrolní bod 10: Základní časté otázky ke kyberbezpečnosti (část B)

Projděte si časté otázky a odpovědi ohledně zmírňování online hrozeb.

Q6: Co je trezor pro tokenizaci dat?

Zabezpečená, izolovaná databáze, která mapuje náhodné tokeny na jejich původní citlivé hodnoty (jako primární čísla kreditních karet).

Q7: Co znamená zero-trust přístup k databázi?

Znamená to ověřování identity a stavu zařízení každého uživatele při každém přihlášení, místo důvěřování komukoli uvnitř sítě.

Q8: Jak TLS chrání data při přenosu?

TLS šifruje payload relace TCP a brání zlomyslným aktérům na veřejných sítích v odposlechu nebo úpravě přenášených paketů.

Q9: Co je auditování přístupu k databázi?

Průběžné zaznamenávání databázových dotazů a přihlášení k odhalení vzorců neoprávněného přístupu nebo bezpečnostních anomálií.

Q10: Co je audit stavu zabezpečení cloudu?

Proces analyzující cloudové konfigurace k identifikaci otevřených portů, chybně nastavených přístupových pravidel a mezer v souladu se zabezpečením.

Kontrolní bod 10: Pokročilé časté otázky k bezpečnosti (část C)

Prozkoumejte pokročilé technické aspekty bezpečnostních rámců, analýzy malwaru a datové compliance.

Q1: Jak funguje obálkové šifrování?

Šifruje data datovým klíčem a poté tento datový klíč šifruje hlavním klíčem, což zjednodušuje ukládání a rotaci klíčů.

Q2: Co je homomorfní šifrování?

Pokročilá šifrovací metoda umožňující provádět operace přímo nad zašifrovanými daty bez předchozího dešifrování.

Q3: Proč se používá šifrování databáze na úrovni sloupců?

Šifruje jednotlivě konkrétní citlivé sloupce (jako SSN) a chrání je, i když administrátoři získají obecný přístup ke čtení tabulky.

Q4: Co je prevence ztráty dat (DLP)?

Software monitorující výstupní body sítě k detekci a blokování neoprávněných odchozích přenosů citlivých souborů.

Q5: Jak zálohy write-once-read-many (WORM) chrání před ransomwarem?

Zálohy WORM brání smazání nebo úpravě souborů po stanovenou dobu, čímž zabraňují ransomwaru zašifrovat existující zálohy.

Kontrolní bod 10: Pokročilé časté otázky k bezpečnosti (část D)

Prozkoumejte pokročilé technické aspekty bezpečnostních rámců, analýzy malwaru a datové compliance.

Q6: Jaké je riziko opakovaného použití klíčů?

Opakované použití téhož kryptografického klíče v různých databázích znamená, že kompromitace jediného klíče odhalí všechny databáze.

Q7: Jak tokenizace databází zlepšuje soulad s CCPA?

Tokeny pseudonymizují záznamy v neprodukčních systémech a omezují dopad úniku, ale tokenizovaná data mohou stále být osobními údaji.

Q8: Proč je klasifikace dat klíčová?

Kategorizuje soubory podle úrovně citlivosti a pomáhá organizacím uplatnit nejsilnější šifrování a řízení přístupu na vysoce riziková data.

Q9: Jaká je role rotace klíčů?

Pravidelná obměna šifrovacích klíčů omezuje množství historických dat vystavených v případě prolomení jediného klíče.

Q10: Jak zabezpečené enklávy chrání databázové dotazy v paměti?

Zabezpečené enklávy izolují operace dotazů v paměťových blocích chráněných CPU, čímž brání správcům hostitele vidět nešifrovaný text v RAM.

Část 11: 10 faktů a poznatků o kyberbezpečnosti z praxe

Projděte si fakta z praxe o bezpečnostních incidentech, obranných mechanismech a standardech souladu.

1. BEZPEČNOSTNÍ POSTŘEH

Nařízení GDPR vstoupilo v platnost v květnu 2018 a změnilo způsob, jakým globální weby spravují souhlasy s cookies a registry osobních údajů.

2. BEZPEČNOSTNÍ POSTŘEH

Pokuta za porušení GDPR může dosáhnout 20 milionů eur nebo 4% celosvětového obratu, což představuje značné právní riziko. [4]

3. BEZPEČNOSTNÍ POSTŘEH

Zákon CCPA vstoupil v platnost v lednu 2020 a zavedl ve Spojených státech průkopnická spotřebitelská práva na digitální soukromí.

4. BEZPEČNOSTNÍ POSTŘEH

Minimalizace dat zmenšuje objem databázového úložiště, čímž snižuje provozní náklady serverů a zároveň zmenšuje rozsah dopadů úniku.

5. BEZPEČNOSTNÍ POSTŘEH

Kryptografické skartování řeší problém mazání záloh odstraněním klíčů místo úprav historických záložních pásek.

6. BEZPEČNOSTNÍ POSTŘEH

Většina zemí světa už přijala zákony na ochranu osobních údajů, které chrání práva spotřebitelů na soukromí.

7. POSTŘEH K BEZPEČNOSTI

Souhlasové formuláře opt-in s předem zaškrtnutými políčky jsou podle evropských definic regulace ochrany osobních údajů výslovně zakázány.

8. POSTŘEH K BEZPEČNOSTI

GDPR vyžaduje hlášení porušení zabezpečení osobních údajů dozorovému úřadu do 72 hodin od zjištění, je-li to proveditelné. [3]

9. POSTŘEH K BEZPEČNOSTI

Hašování hesel pomalými algoritmy jako bcrypt nebo Argon2 výrazně ztěžuje offline prolamování ukradených hašů. [6]

10. BEZPEČNOSTNÍ POSTŘEH

Data v klidu představují uložené databázové soubory, zatímco data v pohybu zahrnují pakety aktivně se pohybující přes síťové směrovače.

Technické reference a zdroje

Studijní příručka a interaktivní hádanky jsou sestaveny z globálních standardů NIST, OWASP a předpisů o ochraně osobních údajů.

AKADEMICKÉ A OBOROVÉ REFERENCE

[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

Klíč odpovědí: Kontrolní bod 1 - Výběr z možností

1 Otázka 1

Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Jaký je primární účel maskování dat? → Nahrazování citlivých identifikátorů smyšlenými, ale realistickými znaky na ochranu soukromí

2 Otázka 2

Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Jaký mechanismus šifruje soubory uložené na pevném disku databázového serveru? → Šifrování celého disku v klidovém stavu

3 Otázka 3

Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Co představují data při přenosu? → Datové pakety putující přes síťové routery a přepínače

4 Otázka 4

Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Proč je pravidelná offline záloha kritická pro ochranu před ransomwarem? → Poskytuje čistou offline kopii k obnovení souborů bez placení výkupného

5 Otázka 5

Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Co dělá tokenizace dat? → Nahrazuje citlivá čísla karet necitlivými náhodnými tokeny

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

6 **Otázka 6** — **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Maskování mění testovací kopie nebo skrývá hodnoty při dotazu; produkční záznamy zůstávají nezměněné.

7 **Otázka 7** — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Zálohy mimo pracoviště musí být izolovány od hlavní firemní sítě, aby se zabránilo šíření ransomwaru.

8 **Otázka 8** — **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Certifikáty TLS chrání data při přenosu; data v klidu potřebují šifrování disku, souborů nebo databáze.

9 **Otázka 9** — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Zero-trust network access (ZTNA) ověřuje identitu každého uživatele před udělením přístupu k databázi.

10 **Otázka 10** — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Tokenizace s trezorem uchovává původní hodnoty v zabezpečeném trezoru tokenů, který mapuje každý token zpět na jeho data.

Klíče slovní zásoby a hodnoticí rubrika

Hodnoticí rubrika pro vyučující: Udělte 1 bod za každé správné přiřazení (celkem 8 bodů) a kontextový termín (celkem 6 bodů).

KONTROLNÍ BOD 4: KLÍČ K PŘIŘAZOVÁNÍ POJMŮ

B 1. ŠIFROVÁNÍ	A 2. ZÁLOHA	H 3. MINIMALIZACE	F 4. PŘÍSTUP
C 5. STAV ZABEZPEČENÍ	E 6. NARUŠENÍ	D 7. SOULAD S PŘEDPISY	G 8. MASKOVÁNÍ

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 MASKOVÁNÍ	2 V KLIDU	3 PŘENOS	4 PŘÍSTUP
5 ZÁLOHA	6 PŘIPRAVENOST		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 F – NARUŠENÍ	2 H – MASKOVÁNÍ	3 D – PŘÍSTUP	4 E – PŘIPRAVENOST
5 G – SOULAD	6 C – MINIMALIZACE	7 A – ŠIFROVÁNÍ	8 B – ZÁLOHA

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy ŠIFROVÁNÍ, ZÁLOHA a MINIMALIZACE a ke každému uvést příklad.

Případové studie:
Požádejte studenty, aby svá doporučení zdůvodnili fakty z pracovního listu, nikoli domněnkami.

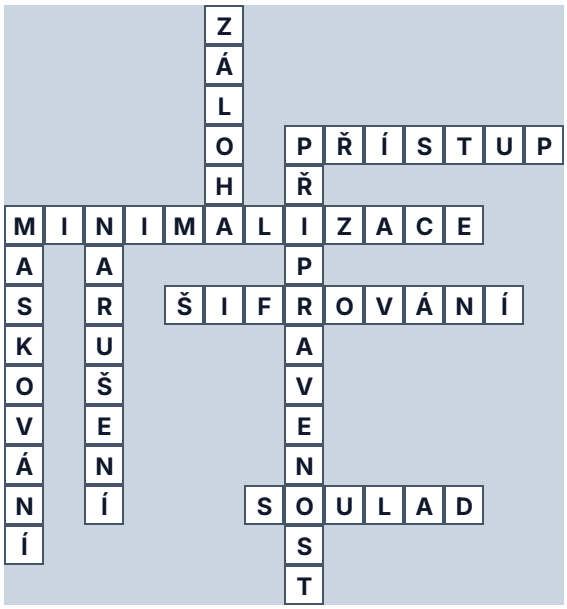
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

T	I	D	S	Ř	N	E	M	I	Š	Ž	T	É	Ř	Ů
S	E	A	Á	Ř	P	O	A	Q	U	N	Y	R	J	S
O	P	U	Š	Č	Ň	Ý	S	B	Ě	A	Š	X	W	Í
N	U	A	S	S	Ž	Ý	K	Ý	L	R	F	I	N	S
E	T	J	N	O	M	Ť	O	P	G	U	R	Ř	Š	G
V	S	Ž	Á	U	Ó	Ů	V	Ě	Ú	Š	C	Ý	I	Š
A	Í	Ý	B	L	G	M	Á	Ž	F	E	J	Ó	F	Q
R	Ř	O	X	A	C	N	N	Ž	Z	N	Ě	Ý	R	P
P	P	W	Ú	D	L	Ů	Í	Q	B	Í	Ó	V	O	Ť
I	N	F	Ů	Č	Ý	Ú	K	S	Á	X	Ž	Y	V	N
Ř	M	I	N	I	M	A	L	I	Z	A	C	E	Á	Š
P	R	X	H	P	D	Á	Č	J	Ř	V	W	X	N	L
Í	H	Z	Á	L	O	H	A	U	H	Ě	B	E	Í	I
K	Ť	Š	V	Ř	Z	E	H	E	Š	C	A	M	R	C
Ž	N	K	V	Š	Ú	Á	Š	X	J	N	N	G	H	Ň

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

2 vodorovně: PŘÍSTUP Omezení oprávnění ke čtení a zápisu v databázi na ověřené uživatelské role. (7 písmen)

3 vodorovně: MINIMALIZACE Omezení sběru osobních údajů na naprosté minimum nutné pro provoz. (12 písmen)

5 vodorovně: ŠIFROVÁNÍ Přeměna čitelného textu na nečitelný šifrovaný text, aby zachycená data zůstala soukromá (9 písmen)

6 vodorovně: SOULAD Plnění regulačních standardů jako GDPR nebo CCPA při správě soukromých údajů uživatelů. (6 písmen)

SVISLÉ NÁPOVĚDY

1 svisle: ZÁLOHA Vytváření bezpečných kopií dat mimo pracoviště pro obnovu při selhání systémů. (6 písmen)

2 svisle: PŘIPRAVENOST Souhrnný stav zabezpečení a obranná připravenost cloudu organizace. (12 písmen)

3 svisle: MASKOVÁNÍ Nahrazování citlivých znaků v databázových polích na ochranu osobních identit. (9 písmen)

4 svisle: NARUŠENÍ Bezpečnostní incident, při němž dojde k neoprávněnému přístupu k chráněným datům nebo jejich vyzrazení (8 písmen)

Klíč řešení přesmyček a šifry

Klíč k hodnocení aktivity s přesmyčkami slovní zásoby a výzvy Tajná šifra.

KLÍČ K PŘESMYČKÁM

1. VORIŠÁNÍF — **ŠIFROVÁNÍ**
2. EIMAMACNIZLI — **MINIMALIZACE**
3. PŘEVSNIATROP — **PŘIPRAVENOST**
4. DLUASO — **SOULAD**
5. OLAZHÁ — **ZÁLOHA**
6. UÍTPSPŘ — **PŘÍSTUP**
7. NÍŠENAUR — **NARUŠENÍ**
8. ÍONMKAVÁS — **MASKOVÁNÍ**

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"CHRAŇTE SVÁ SOUKROMÁ DATA BEZPEČNÝMI PRVKY"

Klíč k případovým studiím

A Případová studie 1: Upgrade šifrování podnikové databáze v klidovém stavu

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Online prodejce ukládá transakční databáze v cloudovém úložišti bez šifrování celého disku. Nedávný audit souladu to označil za závažné riziko zabezpečení dat podle CCPA. Navrhněte architekturu obnovy.
- Doporučená strategie a řešení: Nasaďte šifrování AES-256 celých disků v klidovém stavu na všech souborových systémech. Používejte centralizovanou službu správy klíčů (KMS) s automatickou rotací a vynucujte přísné zásady IAM pro řízení přístupu k dešifrování.

B Případová studie 2: Zadržení ransomwaru a obnova dat

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Aktivní ransomwarový útok šifruje síťové disky ve firemní lokální síti. Administrátor infekci odhalil včas. Naplánujte kroky izolace a obnovy.
- Doporučená strategie a řešení: Okamžitě izolujte kompromitovaný segment. Přeformátujte postižené koncové body a obnovte je z nejnovější offline zálohy typu write-once-read-many (WORM). Před opětovným připojením systémů ověřte integritu zálohy.