Jméno: _____ Datum: _____ Body: _____

Architektura a zabezpečení Zero Trust

Průběžné ověřování, mikrosegmentace sítě, správa identit a přístupu (IAM), nejnižší oprávnění a kontroly stavu zařízení.

PŘEHLED UČIVA: ZABEZPEČENÍ ZERO TRUST

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 architekturou a zabezpečením Zero Trust. Prozkoumáte průběžné ověřování, mikrosegmentaci sítě, správu identit a přístupu (IAM), princip nejnižších oprávnění a auditování relací.

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/zero-trust-kyberneticka-bezpecnost/

Váš studijní plán: strategie Zero Trust

- Pochopte základní princip průběžného ověřování.
- Zavést mikrosegmentaci sítě a přístup s nejnižšími oprávněními.
- Nakonfigurujte kontroly stavu zařízení a auditování aktivních relací.

POKYNY K PŘÍRUČCE ZABEZPEČENÍ ZERO TRUST

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 architekturu Zero Trust. Zakončete bonusovou aktivitou Mysli rychle.

ARCHITEKTURA A ZABEZPEČENÍ ZERO TRUST (ÚVOD)

Zabezpečení Zero Trust nahrazuje staré modely síťového perimetru přísnou zásadou 'nikdy nedůvěřuj, vždy ověřuj'. Zavedení mikrosegmentace, správy identit a přístupů (IAM), nejnižších oprávnění a kontrol stavu zařízení blokuje laterální pohyb hrozeb.

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

Kontrolní bod 1: Výzva s výběrem odpovědí

1 **1. Jaký je základní princip zabezpečení Zero Trust?**

- A. Nikdy nedůvěřuj, vždy ověřuj každý požadavek na přístup bez ohledu na zdroj
- B. Předpoklad, že veškerý provoz uvnitř firemního firewallu je bezpečný
- C. Ukládání databázových souborů bez šifrování kvůli rychlosti
- D. Vynucování ověřování e-mailů pouze pomocí SPF záznamů

2 **2. Co je mikrosegmentace sítě?**

- A. Rozdělení sítí na malé izolované zóny k omezení laterálního pohybu
- B. Šifrování síťových karet během přenosu dat
- C. Připojení všech místních serverů k jedné veřejné IP adrese
- D. Sledování stisků kláves uživatele v relacích prohlížeče

3 **3. Co je princip nejnižších oprávnění?**

- A. Omezení přístupových oprávnění uživatelů jen na to, co je nezbytné pro jejich práci
- B. Udělení všech systémových oprávnění každému uživateli ve výchozím stavu
- C. Povolení anonymních přihlášení k firemním databázovým serverům
- D. Konfigurace veřejných Wi-Fi routerů bez hesel

4 **4. Co je správa identit a přístupu (IAM)?**

- A. Rámce spravující digitální identity a řídící systémová oprávnění
- B. Antivirové nástroje, které skenují místní adresáře souborů
- C. Záložní úložný systém využívající média oddělená od sítě (air-gapped)
- D. Protokol e-mailové brány odmítající podvržené domény

5 **5. Co znamená průběžná autentizace?**

- A. Opakované ověřování identity uživatele a stavu zařízení během aktivní relace
- B. Změna hlavního hesla každých 10 minut
- C. Hashování databázových záznamů více algoritmy
- D. Šifrování síťových paketů pomocí TLS klíčů

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. Zero Trust předpokládá, že veškerý provoz uvnitř firemního firewallu je bezpečný.

○ Pravda ○ Nepravda

7 Otázka 7

7. Mikrosegmentace omezuje schopnost útočníků pohybovat se laterálně mezi interními servery.

○ Pravda ○ Nepravda

8 Otázka 8

8. Nejnižší oprávnění ve výchozím stavu udělují přístup ke všem souborům databáze.

○ Pravda ○ Nepravda

9 Otázka 9

9. Průběžné ověřování validuje stav zařízení a přihlašovací údaje po celou dobu relace.

○ Pravda ○ Nepravda

10 Otázka 10

10. Zavedení Zero Trust snižuje dopad kompromitovaných firemních přihlašovacích údajů.

○ Pravda ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

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

1. Vyžadování přihlašovacích údajů v každém přístupovém bodě se označuje jako průběžné _____ .
2. Rozdělení firemní sítě na drobné zóny se nazývá _____ .
3. Digitální identity a řízení přístupu konfiguruje systém _____ .
4. Omezování uživatelských práv vychází z principu nejmenších _____ .
5. Při hodnocení připojených zařízení se skenuje jejich _____ .
6. Zaznamenávání a kontrola aktivních relací se nazývá bezpečnostní _____ .

ZÁSOBNÍK SLOV

AUDITOVÁNÍ FIREWALL IAM MIKROSEGMENTACE OPRÁVNĚNÍ OVĚŘOVÁNÍ SMĚROVAČ STAV ZABEZPEČENÍ

Sem napište své odpovědi:

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

Kontrolní bod 4: Přiřazování bezpečnostních pojmů

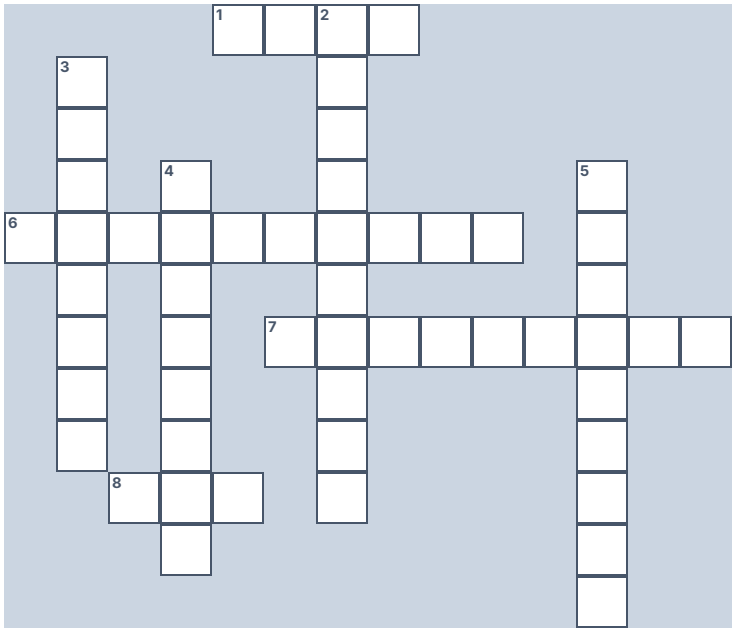
PŘIŘAZOVÁNÍ DEFINIC

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

☐	1. OVĚŘOVÁNÍ	A	Správa přístupu k přihlašovacím údajům uživatelů.
☐	2. MIKROSEGMENTACE	B	Zásada nejnižších přístupových práv.
☐	3. IAM	C	Směrování síťového paketového provozu.
☐	4. OPRÁVNĚNÍ	D	Ochrana vnější síťovou bariérou.
☐	5. STAV ZABEZPEČENÍ	E	Kontrola logovaných přístupových relací.
☐	6. AUDITOVÁNÍ	F	Rozdělování vnitřních síťových zón.
☐	7. FIREWALL	G	Neustálé ověřování přihlašovacích údajů uživatelů.
☐	8. ROUTER	H	Vyhodnocování zdravotního stavu zařízení.

Kontrolní bod 5: Křížovka

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



VODOROVNÉ NÁPOVĚDY

1. Hodnocení zdravotního stavu zařízení. (4)

6. Dělení vnitřních síťových zón. (10)

7. Neustálá kontrola přihlašovacích údajů uživatelů. (9)

8. Správa přístupu k uživatelským údajům. (3)

SVISLÉ NÁPOVĚDY

2. Kontrola zaznamenaných přístupových relací. (10)

3. Vnější bariérová ochrana sítě. (8)

4. Směrování síťového paketového provozu. (8)

5. Princip nejnižších přístupových práv. (9)

Kontrolní bod 5, alternativa: Přístupná zadání křížovky

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

VODOROVNÉ NÁPOVĚDY

1 vodorovně: Hodnocení zdravotního stavu zařízení. (4 písmen):

6 vodorovně: Dělení vnitřních síťových zón. (10 písmen):

7 vodorovně: Neustálá kontrola přihlašovacích údajů uživatelů. (9 písmen):

8 vodorovně: Správa přístupu k uživatelským údajům. (3 písmen):

SVISLÉ NÁPOVĚDY

2 svisle: Kontrola zaznamenaných přístupových relací. (10 písmen):

3 svisle: Vnější bariérová ochrana sítě. (8 písmen):

4 svisle: Směrování síťového paketového provozu. (8 písmen):

5 svisle: Princip nejnižších přístupových práv. (9 písmen):

Kontrolní bod 6: Hledání skrytých slov

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

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

SEZNAM SLOV

OVĚŘOVÁNÍ SEGMENTACE IAM OPRÁVNĚNÍ STAV AUDITOVÁNÍ FIREWALL SMĚROVAČ

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. OVĚŘOVÁNÍ
B. SEGMENTACE
C. IAM
D. OPRÁVNĚNÍ
E. STAV
F. AUDITOVÁNÍ
G. FIREWALL
H. SMĚROVAČ

DEFINICE A POLE K PŘIŘAZENÍ
[ ] 1. Vnější bariérová ochrana sítě.
[ ] 2. Kontrola zaznamenaných přístupových relací.
[ ] 3. Princip nejnižších přístupových práv.
[ ] 4. Dělení vnitřních síťových zón.
[ ] 5. Směrování síťového paketového provozu.
[ ] 6. Hodnocení zdravotního stavu zařízení.
[ ] 7. Správa přístupu k uživatelským údajům.
[ ] 8. Neustálá kontrola přihlašovacích údajů uživatelů.

Kontrolní bod 7: Výzva s přeházenými slovy

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

1. **VOŘVOÁNÍĚ**
2. **MAI**
3. **VSAT**
4. **ELLAWFIR**
5. **ANEEMTESCG**
6. **NÁPĚNOVÍR**
7. **UIAVOÁNÍTD**
8. **RMOČSAVĚ**

Bonusová aktivita: Mysli rychle

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

1	Informace, které byste nikdy neměli sdílet			
2	Bezpečné návyky, se kterými můžete začít už dnes			
3	Věci, které se kontrolují na zařízení			
4	Věci, které se zaznamenávají			
5	Slova související s kyberbezpečností			
6	Věci, které Zero Trust kontroluje			
7	Místa, kde v běžném životě ukazujete doklad			
8	Způsoby, jak prokázat, že jste to opravdu vy			
9	Co udělat po úniku dat			
10	Známky toho, že je počítač nakažený			
11	Důvody, proč aktualizovat software			
12	Úrovně přístupu ve firmě			
13	Bezpečnostní nástroje, které znáte			
14	Zóny, na které lze rozdělit síť			
15	Rčení o důvěře			

Kontrolní bod 8: Případové studie kyberbezpečnosti

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

PŘÍPADOVÁ STUDIE 1: PŘECHOD NA SÍŤOVOU ARCHITEKTURU ZERO TRUST



Scénář: Velký podnik v současnosti používá plochou interní síť, kde jakékoli zařízení v místní síti má přístup ke všem firemním serverům a databázím.

Otázka k diskusi: Navrhněte strategii mikrosegmentace sítě k omezení laterálního pohybu.

PŘÍPADOVÁ STUDIE 2: NASAZENÍ ŘÍZENÍ PŘÍSTUPU S NEJNIŽŠÍMI OPRÁVNĚNÍMI



Scénář: Auditní protokoly odhalí, že dočasní databázoví uživatelé a řadoví zaměstnanci mají globální oprávnění ke čtení i zápisu do kritických účetních databází.

Otázka k diskusi: Proveďte audit a omezte oprávnění IAM databáze k vynucení nejnižších oprávnění.

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

35 41 6 38 22 35 10 27 32 16 30 8 28

1 26 4 13 14 30 8 17 30 32 26 22 32 20 32 18 22 35 9

6 34 35 10 26 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 Zero Trust?

Zero Trust je bezpečnostní rámec předpokládající, že hrozby existují vně i uvnitř hranice sítě, a vyžadující ověření každého požadavku. [1]

Q2: Jaké je základní pravidlo Zero Trust?

Nikdy nedůvěřuj, vždy ověřuj.

Q3: Co je mikrosegmentace?

Rozdělení sítě na malé zabezpečené logické segmenty pro řízení provozu a zadržení průniků.

Q4: Co je princip nejnižších oprávnění?

Udělování pouze minimálních přístupových práv, která uživatelé potřebují k výkonu svých konkrétních pracovních úkolů. [2]

Q5: Co znamená zkratka IAM?

Správa identit a přístupů.

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

Projděte si časté otázky a odpovědi ohledně zmírňování online hrozeb.

Q6: Jak pomáhá kontrola stavu zařízení?

Ověřuje, že zařízení má nainstalované záplaty, běží na něm aktivní antivirus a je zabezpečené, než povolí přístup.

Q7: Co je laterální pohyb?

Proces, kterým se útočníci pohybují sítí od prvotně kompromitovaného uzlu k cennějším systémům.

Q8: Nahrazuje Zero Trust firewally?

Ne, doplňuje je o kontroly zaměřené na identitu a interní segmentační firewally.

Q9: Co je průběžné ověřování?

Průběžné ověřování identity uživatele po celou dobu aktivní relace, nejen při počátečním přihlášení.

Q10: Proč je plochá síť nebezpečná?

V plochých sítích umožňuje jediný kompromitovaný uzel útočníkům snadný přístup k jakékoli databázi v síti.

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

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

Q1: Jak Zero Trust řeší perimetrový model?

Nahrazuje zastaralý model „hradu a příkopu“ a přesouvá obranu z hraničních sítí na konkrétní uživatelské identity a zdroje.

Q2: Co je bod rozhodování o politice (PDP)?

Systémová komponenta, která vyhodnocuje žádosti o autorizaci podle bezpečnostních pravidel a rozhoduje, zda má být přístup udělen.

Q3: Co je bod vynucování zásad (PEP)?

Systémový uzel (například brána nebo proxy), který fyzicky povoluje nebo blokuje požadavky na připojení podle rozhodnutí PDP.

Q4: Jak řízení přístupu na základě rolí (RBAC) podporuje Zero Trust?

RBAC seskupuje oprávnění do konkrétních rolí, a pomáhá tak zabránit tomu, aby uživatelé zdědili nadměrná administrátorská oprávnění.

Q5: Co je kontextové řízení přístupu?

Vyhodnocování přihlašovacích požadavků pomocí druhotných vodítek, jako je geografická poloha, stav zařízení a čas přihlášení, k posouzení rizika.

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

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

Q6: Čím se mikrosegmentace liší od běžných VLAN?

VLAN rozdělují sítě do širokých logických segmentů na vrstvě 2, zatímco mikrosegmentace izoluje jednotlivé workloady softwarovou politikou.

Q7: Co je just-in-time (JIT) přístup?

Dočasné udělení zvýšených administrátorských oprávnění a jejich automatické odebrání po dokončení úkolu.

Q8: Jak se zabezpečují API v rámci Zero Trust?

Vyžadováním kryptograficky podepsaných OAuth tokenů a auditem podpisů požadavků na každé API bráně.

Q9: Co je klient zero-trust network access (ZTNA)?

Softwarový agent, který vytváří zabezpečená, šifrovaná odchozí připojení ke konkrétním aplikacím, nikoli k celým síťovým subnetům.

Q10: Jak audit protokolů pomáhá Zero Trust?

Nepřetržité logování umožňuje automatizovaným nástrojům bezpečnostní analytiky odhalovat anomálie a okamžitě pozastavit podezřelá přihlášení.

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

Architektury Zero Trust nahrazují zastaralý model hradu a příkopu pravidly ověřování zaměřenými na identitu.

2. BEZPEČNOSTNÍ POSTŘEH

Síťová mikrosegmentace zmenšuje prostor, kam malware dosáhne, izolací úloh do malých chráněných zón.

3. BEZPEČNOSTNÍ POSTŘEH

Zero Trust se zaměřuje na ochranu zdrojů, jako jsou aktiva, služby a účty, nikoli na síťové segmenty. [1]

4. BEZPEČNOSTNÍ POSTŘEH

Zásady přístupu s nejnižšími oprávněními snižují riziko odlivu dat z klíčových databází způsobeného vnitřními hrozbami.

5. BEZPEČNOSTNÍ POSTŘEH

Validace stavu zařízení kontroluje úroveň záplat operačního systému a aktivní stav antiviru v reálném čase.

6. BEZPEČNOSTNÍ POSTŘEH

Brokery Zero Trust Network Access (ZTNA) mohou nahradit nebo doplnit firemní VPN a omezit rozsah přístupu uživatelů.

7. POSTŘEH K BEZPEČNOSTI

Delegování administrátorských oprávnění Just-in-Time (JIT) snižuje riziko krádeže přihlašovacích údajů na doménových řadičích.

8. POSTŘEH K BEZPEČNOSTI

Průběžná validace loguje a audituje chování relací a pozastavuje uživatele s anomálními vzorci spouštění skriptů.

9. POSTŘEH K BEZPEČNOSTI

Tradiční perimetrická obrana nedokáže blokovat laterální útoky, jakmile uniknou administrátorské přihlašovací údaje.

10. BEZPEČNOSTNÍ POSTŘEH

NIST Special Publication 800-207 (2020) podává abstraktní definici architektury Zero Trust včetně modelů nasazení. [1]

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. (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

Klíč odpovědí: Kontrolní bod 1 - Výběr z možností

1 Otázka 1 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Jaký je základní princip zabezpečení Zero Trust? → Nikdy nedůvěřuj, vždy ověřuj každý požadavek na přístup bez ohledu na zdroj

2 Otázka 2 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Co je mikrosegmentace sítě? → Rozdělení sítí na malé izolované zóny k omezení laterálního pohybu

3 Otázka 3 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Co je princip nejnižších oprávnění? → Omezení přístupových oprávnění uživatelů jen na to, co je nezbytné pro jejich práci

4 Otázka 4 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Co je správa identit a přístupu (IAM)? → Rámce spravující digitální identity a řídící systémová oprávnění

5 Otázka 5 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Co znamená průběžná autentizace? → Opakované ověřování identity uživatele a stavu zařízení během aktivní relace

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

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

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: Zero Trust nepřiznává žádnou implicitní důvěru podle umístění v síti, uvnitř ani venku.

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

POZNÁMKA PRO VYUČUJÍCÍ

Pravda: malé izolované zóny omezují, jak daleko se vetřelec může mezi servery pohybovat.

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

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: nejmenší oprávnění uděluje jen minimální přístup, který každá role potřebuje.

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

POZNÁMKA PRO VYUČUJÍCÍ

Průběžné ověřování validuje stav zařízení a přihlašovací údaje po celou dobu relace.

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

POZNÁMKA PRO VYUČUJÍCÍ

Zavedení Zero Trust snižuje dopad kompromitovaných firemních přihlašovacích údajů.

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

G 1. OVĚŘOVÁNÍ	F 2. MIKROSEGMENTACE	A 3. IAM	B 4. OPRÁVNĚNÍ
H 5. STAV ZABEZPEČENÍ	E 6. AUDITOVÁNÍ	D 7. FIREWALL	C 8. ROUTER

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 OVĚŘOVÁNÍ	2 MIKROSEGMENTACE	3 IAM	4 OPRÁVNĚNÍ
5 STAV ZABEZPEČENÍ	6 AUDITOVÁNÍ		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 G – FIREWALL	2 F – AUDITOVÁNÍ	3 D – OPRÁVNĚNÍ	4 B – SEGMENTACE
5 H – SMĚROVAČ	6 E – STAV	7 C – IAM	8 A – OVĚŘOVÁNÍ

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy OVĚŘOVÁNÍ, MIKROSEGMENTACE a IAM a ke každému uvést příklad.

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

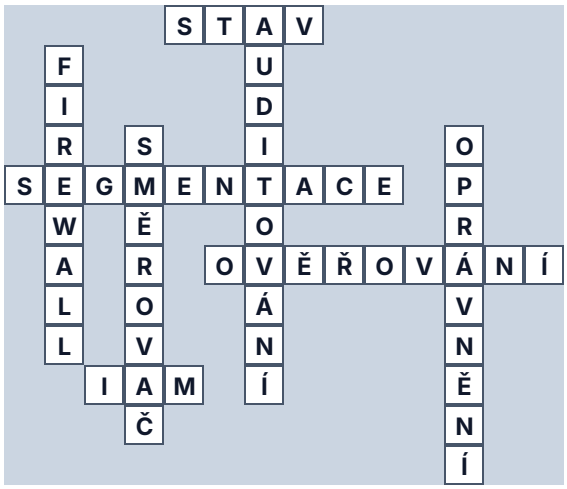
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

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

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

1 vodorovně: STAV Hodnocení zdravotního stavu zařízení. (4 písmen)

6 vodorovně: SEGMENTACE Dělení vnitřních síťových zón. (10 písmen)

7 vodorovně: OVĚŘOVÁNÍ Neustálá kontrola přihlašovacích údajů uživatelů. (9 písmen)

8 vodorovně: IAM Správa přístupu k uživatelským údajům. (3 písmen)

SVISLÉ NÁPOVĚDY

2 svisle: AUDITOVÁNÍ Kontrola zaznamenaných přístupových relací. (10 písmen)

3 svisle: FIREWALL Vnější bariérová ochrana sítě. (8 písmen)

4 svisle: SMĚROVAČ Směrování síťového paketového provozu. (8 písmen)

5 svisle: OPRÁVNĚNÍ Princip nejnižších přístupových práv. (9 písmen)

Klíč řešení přesmyček a šifry

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

KLÍČ K PŘESMYČKÁM

1. VOŘVOÁNÍĚ — OVĚŘOVÁNÍ
2. MAI — IAM
3. VSAT — STAV
4. ELLAWFIR — FIREWALL
5. ANEEMTESCG — SEGMENTACE
6. NÁPĚNOVÍR — OPRÁVNĚNÍ
7. UIAVOÁNÍTD — AUDITOVÁNÍ
8. RMOČSAVĚ — SMĚROVAČ

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"VŽDY OVĚŘUJTE S ARCHITEKTUROU NULOVÉ DŮVĚRY"

Klíč k případovým studiím

A Případová studie 1: Přechod na síťovou architekturu Zero Trust

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Velký podnik aktuálně používá plochou interní síť, kde jakékoli zařízení v lokální síti má přístup ke všem firemním serverům a databázím.
- Doporučená strategie a řešení: Rozdělte plochou síť na izolované zóny podle oddělení. Nasaďte interní firewally pro řízení provozu mezi zónami a vyžadujte ověřování tokenů připojení pro veškerý přístup.

B Případová studie 2: Nasazení řízení přístupu s nejnižšími oprávněními

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Auditní protokoly odhalí, že dočasní databázoví uživatelé a řadoví zaměstnanci mají globální oprávnění ke čtení i zápisu do kritických účetních databází.
- Doporučená strategie a řešení: Odeberte všechna globální administrátorská oprávnění. Zaveďte řízení přístupu podle rolí (RBAC) přesně podle pracovních pozic a zaveďte týdenní automatizované revize oprávnění.