Jméno: _____ Datum: _____ Body: _____

Základy kyberbezpečnosti a online hrozby Prevence

Kyberbezpečnostní hrozby, síťové firewally, vícefaktorová autentizace, bezpečnostní rámce

PŘEHLED VÝUKY: ZÁKLADY KYBERBEZPEČNOSTI

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 základními principy kyberbezpečnosti a prevence online hrozeb. Prozkoumáte malwarové hrozby, vícefaktorové ověřování, síťové firewally a rámce reakce na incidenty.

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/

Váš studijní plán: základy kyberbezpečnosti

- Určete běžné vektory malwaru, phishingu a průniků do firemních sítí.
- Zavést standardní kybernetické kontroly včetně MFA, firewallů a ochrany koncových bodů.
- Vyhodnoťte postupy reakce na incidenty ke zmírnění dopadů úniků dat.
- Analyzujte organizační rizikové faktory a bezpečnostní soulad podle směrnic NIST.
- Nakonfigurujte návyky bezpečnostní hygieny ke zmírnění automatizovaného credential stuffingu.

POKYNY K PRŮVODCI KYBERBEZPEČNOSTÍ

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 prevenci hrozeb. Zakončete bonusovou aktivitou Mysli rychle.

ZÁKLADY KYBERBEZPEČNOSTI A PREVENCE HROZEB (ÚVOD)

Kyberbezpečnost chrání sítě, systémy a data před neoprávněnými digitálními útoky. Budování pevných bezpečnostních návyků, konfigurace firewallů, vyžadování vícefaktorové autentizace a školení zaměstnanců v rozpoznávání hrozeb jsou zásadní součásti obrany firemní sítě.

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

Kontrolní bod 1: Výzva s výběrem odpovědí

1. **1. Jaký je primární cíl phishingového útoku?**
   - A. Krádež přihlašovacích údajů a citlivých uživatelských dat
   - B. Zlepšení viditelnosti webu ve vyhledávačích
   - C. Zvyšování kapacity šířky pásma sítě
   - D. Správa replikace záložního datového centra

2. **2. Jaký mechanismus poskytuje nejsilnější ochranu účtu?**
   - A. Vícefaktorová autentizace pomocí hardwarových klíčů
   - B. Složitá hesla měněná každých třicet dní
   - C. Omezení přihlašování k účtu na pracovní dobu
   - D. Skrytí uživatelského jména účtu z veřejných adresářů

3. **3. Co definuje payload ransomwarové infekce?**
   - A. Šifrování systémových souborů a požadování platby
   - B. Tiché logování stisků kláves na vzdálené servery
   - C. Vkládání neautorizované reklamy do prohlížečů
   - D. Využívání místního CPU k těžbě kryptoměn

4. **4. Jak zero-day exploit ovlivňuje bezpečnostní obranu?**
   - A. Cílí na nezáplatované, neznámé zranitelnosti
   - B. Automaticky vypne firemní firewall
   - C. Vynutí tvrdý restart systému
   - D. Náprava nevyžaduje žádný rozpočet

5. **5. Jaký rámec upravuje firemní bezpečnostní kontroly?**
   - A. Směrnice NIST Cybersecurity Framework
   - B. Specifikace schémat dokumentů W3C HTML5
   - C. Návody k instalaci ovladačů tiskáren
   - D. Definice směrovacích protokolů IETF

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka tf 6

6. Phishingové útoky cílí pouze na osobní e-mailové účty.

○ Pravda ○ Nepravda

7 Otázka tf 7

7. Vícefaktorové ověřování pomáhá blokovat útoky typu credential stuffing.

○ Pravda ○ Nepravda

8 Otázka tf 8

8. Firewally kontrolují síťový provoz a blokují neoprávněný přístup k portům.

○ Pravda ○ Nepravda

9 Otázka tf 9

9. Náprava zero-day exploitů vyžaduje běžné aktualizace antivirových definic.

○ Pravda ○ Nepravda

10 Otázka tf 10

10. Honeypot je návnadový server používaný k nalákání kyberzločinců.

○ Pravda ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

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

1. Síťoví administrátoři instalují _____ k filtrování příchozího provozu.

2. Útočník použije zero-day _____ k obejití systémových oprav.

3. Útočníci rozesílají podvržené e-maily a vedou tak proti zaměstnancům kampaně typu _____ .

4. Ransomware uzamykající uživatelská data je destruktivní forma softwaru označovaného jako _____ .

5. Silná pravidla pro hesla jsou součástí návyků, které se souhrnně označují jako _____ a zmírňují riziko krádeže přihlašovacích údajů.

6. K ochraně citlivé komunikace uživatelé používají protokoly, jejichž základem je _____ .

ZÁSOBNÍK SLOV

EXPLOIT FIREWALL KYBERNETICKÁ HYGIENA MALWARE PHISHING RANSOMWARE ŠIFROVÁNÍ VÍCEFAKTOROVÉ

Sem napište své odpovědi:

1. **2.**

3. **4.**

5. **6.**

Kontrolní bod 4: Přiřazování bezpečnostních pojmů

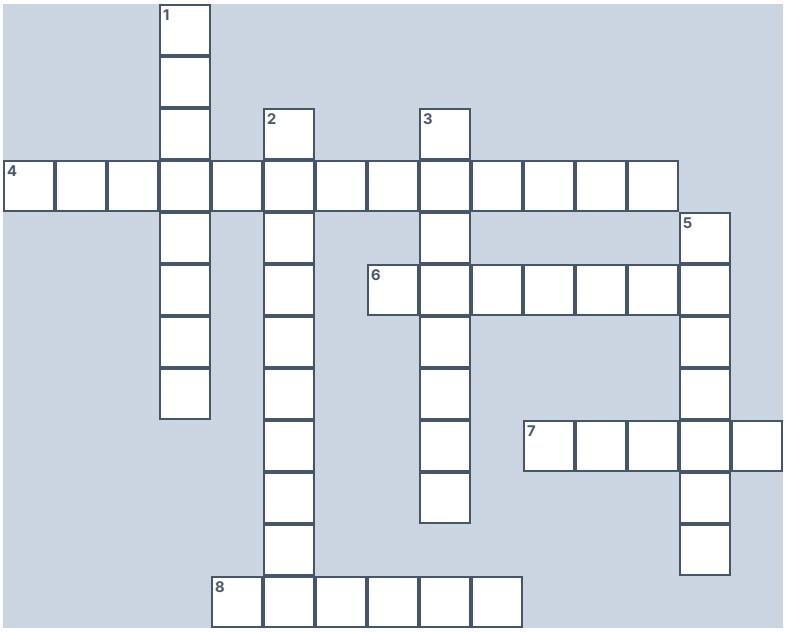
PŘIŘAZOVÁNÍ DEFINIC

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

☐	1. Hrozba ransomwaru	**A**	Strukturované směrnice, jako je NIST, používané k řízení kybernetických rizik.
☐	2. Vícefaktorové ověřování	**B**	Strukturovaný plán pro zvládání a zmírňování bezpečnostních incidentů.
☐	3. Zero-day exploit	**C**	Síťová bariéra filtrující provoz podle bezpečnostních pravidel.
☐	4. Návnadový honeypot	**D**	Malware šifrující data a požadující finanční platbu za dešifrování.
☐	5. Firewall proti průnikům	**E**	Zneužití zranitelnosti cílené dříve, než vydavatel vydá opravu.
☐	6. Reakce na incidenty	**F**	Osvědčené postupy pro správu přihlašovacích údajů a ověřovacích klíčů.
☐	7. Hygiena hesel	**G**	Bezpečnostní ověření vyžadující dva nebo více autentizačních faktorů.
☐	8. Bezpečnostní rámec	**H**	Návnadový systém nastražený k přilákání a analýze útočníků.

Kontrolní bod 5: Křížovka

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



VODOROVNÉ NÁPOVĚDY

4. Bezpečnostní ověření vyžadující dva a více autentizačních faktorů (13)

6. Zneužití zranitelnosti dříve, než výrobce vydá opravu (7)

7. Strukturované směrnice jako NIST používané k řízení kybernetických rizik (5)

8. Strukturovaný plán pro zvládání a zmírňování bezpečnostních incidentů (6)

SVISLÉ NÁPOVĚDY

1. Síťová bariéra filtrující provoz podle bezpečnostních pravidel (8)

2. Malware šifrující data a požadující finanční platbu za dešifrování (10)

3. Návnadový systém nastražený k přilákání a analýze útočníků (8)

5. Osvědčené postupy správy přihlašovacích údajů a autentizačních klíčů (7)

Kontrolní bod 5, alternativa: Přístupná zadání křížovky

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

VODOROVNÉ NÁPOVĚDY

4 vodorovně: Bezpečnostní ověření vyžadující dva a více autentizačních faktorů (13 písmen):

6 vodorovně: Zneužití zranitelnosti dříve, než výrobce vydá opravu (7 písmen):

7 vodorovně: Strukturované směrnice jako NIST používané k řízení kybernetických rizik (5 písmen):

8 vodorovně: Strukturovaný plán pro zvládání a zmírňování bezpečnostních incidentů (6 písmen):

SVISLÉ NÁPOVĚDY

1 svisle: Síťová bariéra filtrující provoz podle bezpečnostních pravidel (8 písmen):

2 svisle: Malware šifrující data a požadující finanční platbu za dešifrování (10 písmen):

3 svisle: Návnadový systém nastražený k přilákání a analýze útočníků (8 písmen):

5 svisle: Osvědčené postupy správy přihlašovacích údajů a autentizačních klíčů (7 písmen):

Kontrolní bod 6: Hledání skrytých slov

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

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

SEZNAM SLOV

RANSOMWARE VÍCEFAKTOROVÉ ZERODAY HONEYPOT FIREWALL REAKCE HYGIENA RÁMEC

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. RANSOMWARE**
- **B. VÍCEFAKTOROVÉ**
- **C. ZERODAY**
- **D. HONEYPOT**
- **E. FIREWALL**
- **F. REAKCE**
- **G. HYGIENA**
- **H. RÁMEC**

DEFINICE A POLE K PŘIŘAZENÍ

1. Síťová bariéra filtrující provoz podle bezpečnostních pravidel.
2. Strukturovaný plán pro zvládání a zmírňování bezpečnostních incidentů.
3. Malware šifrující data a požadující finanční platbu za dešifrování.
4. Bezpečnostní ověření vyžadující dva a více autentizačních faktorů.
5. Osvědčené postupy správy přihlašovacích údajů a autentizačních klíčů.
6. Strukturované směrnice jako NIST používané k řízení kybernetických rizik.
7. Zneužití zranitelnosti dříve, než výrobce vydá opravu.
8. Návnadový systém nastražený k přilákání a analýze útočníků.

Kontrolní bod 7: Výzva s přeházenými slovy

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

1. **RWMOARAESN** _____
2. **ZRYADOE** _____
3. **EIFWALLR** _____
4. **AYEINHG** _____
5. **OOÍCTFÉARK VVE** _____
6. **OTEPHYON** _____
7. **CRKEAE** _____
8. **CRMEÁ** _____

Bonusová aktivita: Mysli rychle

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

1	Profese v kybernetické bezpečnosti			
2	Důvody, proč aktualizovat software			
3	Věci, které může firewall zablokovat			
4	Varovné signály v e-mailu			
5	Věci, které si zálohujete			
6	Známé typy kybernetických útoků			
7	Věci, které může honeypot nalákat			
8	Informace, které byste nikdy neměli sdílet			
9	Známky toho, že je počítač nakažený			
10	Filmy nebo seriály o hackerech			
11	Vrstvy zabezpečení, které můžete vybudovat			
12	Věci, které je dobré nacvičit při bezpečnostním cvičení			
13	Bezpečnostní nástroje, které znáte			
14	Lidé, které můžete požádat o pomoc s IT			
15	Slova, která začínají na „kyber“			

Kontrolní bod 8: Případové studie kyberbezpečnosti

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

PŘÍPADOVÁ STUDIE 1: STRATEGIE OBNOVY PO RANSOMWARU



Scénář: Firemní síť je infikována ransomwarem, který zamyká kritické databáze. Útočníci požadují výkupné 100 000 USD v kryptoměně. Společnost má offline zálohy staré 24 hodin.

Otázka k diskusi: Analyzujte rizika zaplacení a vyhodnoťte strategii obnovy.

PŘÍPADOVÁ STUDIE 2: OBRANA PROTI CREDENTIAL STUFFINGU



Scénář: Online služba čelí útoku typu credential stuffing, při kterém hackeři zkoušejí miliony dvojic uživatelské jméno/heslo ukradených z jiných webů.

Otázka k diskusi: Popište mechanismus tohoto útoku a nastíněte dva obranné systémy.

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

40	1	3	8	40	24	8	5	30	8		28	38	28	30	9	19

35	15	4	8	11	1	17	30	22	26	22	35	39	19

22	35	10	27	8	20	15	19

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: Jaký je hlavní cíl kyberbezpečnosti?

Hlavním cílem je ochrana sítí, zařízení a dat před neoprávněným přístupem, útoky a náhodným poškozením.

Q2: Čím se phishing liší od spear phishingu?

Phishing je široká e-mailová kampaň cílící na náhodné uživatele, zatímco spear phishing cílí na konkrétní osoby pomocí personalizovaných dat.

Q3: Co je síťový firewall?

Firewall je síťový bezpečnostní systém, který monitoruje a filtruje příchozí a odchozí provoz na základě předem definovaných bezpečnostních pravidel.

Q4: Proč je vícefaktorové ověřování (MFA) nutné?

MFA přidává klíčovou vrstvu obrany a zabraňuje přístupu, i když útočníci primární heslo ukradnou nebo prolomí.

Q5: Co definuje počítačový virus?

Virus je samoreplikující se malware, který se připojuje k čistým souborům a po spuštění se šíří napříč systémy.

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

Projděte si časté otázky a odpovědi ohledně zmírňování online hrozeb.

Q6: Jak ransomware zamyká lokální data?

Ransomware používá kryptografické algoritmy k zašifrování uživatelských souborů, které zůstávají nečitelné, dokud není použit dešifrovací klíč.

Q7: Co je zranitelnost zero-day?

Zero-day je bezpečnostní chyba v softwaru, o které výrobce neví, takže před zneužitím není čas na vývoj záplaty.

Q8: Jaká je role frameworku NIST?

Rámec NIST poskytuje dobrovolné pokyny a standardy, které organizacím pomáhají řídit a snižovat kybernetická rizika.

Q9: Co je plán reakce na bezpečnostní incidenty?

Je to zdokumentovaný soubor postupů pro detekci, zadržení a zotavení z bezpečnostních incidentů a kompromitace sítě.

Q10: Jak sociální inženýrství zneužívá uživatele?

Sociální inženýrství využívá psychologickou manipulaci, aby přimělo zaměstnance prozradit hesla nebo stáhnout škodlivé soubory.

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

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

Q1: Jak útok DDoS zahlcuje webové servery?

DDoS útok koordinuje miliony kompromitovaných zařízení botnetu k zahlcení serveru provozem, čímž vyčerpává limity šířky pásma a CPU.

Q2: Jaký je rozdíl mezi symetrickým a asymetrickým šifrováním?

Symetrické šifrování používá jediný klíč pro šifrování i dešifrování, zatímco asymetrické šifrování používá pár veřejného a soukromého klíče.

Q3: Jak hackeři provádějí útoky SQL injection?

Útočníci zadávají škodlivé SQL příkazy do formulářových polí a přimějí tak backendovou databázi vydat neoprávněné uživatelské záznamy.

Q4: Co je laterální pohyb při průnicích do sítě?

Je to technika, kdy útočníci zneužijí počáteční přístup k serveru ke kompromitaci dalších propojených systémů ve vnitřní síti.

Q5: Jak DNS spoofing přesměrovává webový provoz?

DNS spoofing mění záznamy v mezipaměti jmenných serverů a směruje legitimní uživatele na škodlivé napodobující weby místo cílových domén.

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

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

Q6: Co je hardwarový bezpečnostní token?

Je to fyzické zařízení (jako YubiKey) generující kryptografické důkazy ověření, nabízející maximální obranu proti vzdálenému phishingu.

Q7: Jak bezpečnostní týmy využívají návnadové honeypoty?

Týmy nasazují neprodukční návnadové servery (decoy) k včasné detekci průniků a analýze vzorců útoků neautorizovaných aktérů.

Q8: Co je princip nejnižších oprávnění?

Je to bezpečnostní standard omezování přístupových práv uživatelů na absolutní minimum nezbytné k výkonu jejich pracovních rolí.

Q9: Jak útok Man-in-the-Middle zneužívá připojení?

Útočník zachycuje a pozměňuje komunikaci mezi dvěma zařízeními v nešifrovaných sítích a krade tokeny relace a přihlašovací údaje.

Q10: Co jsou indikátory kompromitace (IOC)?

IOC jsou forenzní datové stopy, jako neobvyklé úpravy registru nebo podezřelý IP provoz, ukazující, že systém byl napaden.

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

Útočníci neustále skenují internet a hledají zranitelné servery a posílají phishingové e-maily do schránek zaměstnanců.

2. BEZPEČNOSTNÍ POSTŘEH

Lidská chyba, jako je kliknutí na phishingové odkazy, je častým faktorem úniků dat, a proto je školení důležité.

3. BEZPEČNOSTNÍ POSTŘEH

Náklady na únik dat zahrnují právní pokuty, odliv zákazníků, vyšetřování a nápravu a mohou dosáhnout milionů dolarů.

4. BEZPEČNOSTNÍ POSTŘEH

MFA odolné vůči phishingu, jako jsou hardwarové bezpečnostní klíče, je nejsilnějším typem MFA a standardem, který doporučuje CISA. [2]

5. BEZPEČNOSTNÍ POSTŘEH

Ransomware zůstává velkou hrozbou pro podnikové sítě a CISA doporučuje offline šifrované zálohy jako klíčovou obranu. [4]

6. BEZPEČNOSTNÍ POSTŘEH

NIST Cybersecurity Framework 2.0 (2024) má šest základních funkcí: Govern, Identify, Protect, Detect, Respond, Recover. [1]

7. POSTŘEH K BEZPEČNOSTI

Boti pro credential stuffing testují uniklé páry uživatelských jmen a hesel ve velkém proti přihlašovacím portálům bank a e-shopů.

8. POSTŘEH K BEZPEČNOSTI

Trhy se zero-day exploity existují po celém světě a vysoce závažné zranitelnosti se na nich mohou před opravou prodávat za velké částky.

9. POSTŘEH K BEZPEČNOSTI

Návnadový systém honeypot hlásí upozornění na průnik okamžitě, protože legitimní uživatelé nemají důvod k němu přistupovat.

10. BEZPEČNOSTNÍ POSTŘEH

Transport Layer Security (TLS) šifruje relace prohlížeče a brání odposlechu paketů na veřejných Wi-Fi sítích.

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

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

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

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

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

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

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

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

Klíč odpovědí: Kontrolní bod 1 - Výběr z možností

1 **Phishingové útoky** PHISHING — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Phishingové kampaně se pokoušejí krást přihlašovací údaje a citlivá uživatelská data pomocí podvržených e-mailů.

2 **Ochrana účtu** KLÍČ MFA — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Vícefaktorové ověřování (MFA) s hardwarovými tokeny poskytuje nejsilnější obranu přístupu k účtu.

3 **Hrozba ransomwaru** RANSOMWARE — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Ransomware šifruje kritické systémy a data a za dešifrovací klíče požaduje platbu v kryptoměně.

4 **Zranitelnost zero-day** ZERO-DAY — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Zero-day hrozby zneužívají neopravené, neznámé bezpečnostní chyby dříve, než je k dispozici oprava od výrobce.

5 **Bezpečnostní rámce** RÁMCE — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Rámce jako NIST poskytují strukturované pokyny, které organizacím pomáhají řídit a snižovat kybernetická rizika.

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

6 **Cílený phishing** PHISHING — **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Phishingové útoky cílí na firemní sítě i osobní účty, aby rozšířily vektory útoku.

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

POZNÁMKA PRO VYUČUJÍCÍ

MFA vyžaduje druhý faktor, takže samotné ukradené heslo k přihlášení obvykle nestačí.

8 **Traffic Firewall** FIREWALL — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Firewally kontrolují a blokují provoz na konkrétních síťových portech, aby odfiltrovaly neoprávněná připojení.

9 **Reakce na zero-day** ZERO-DAY — **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Náprava zero-day chyb vyžaduje záplaty kódu a filtrování WAF, protože signatury ještě neexistují.

10 **Návnadové honeypoty** HONEYPOT — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Honeypoty jsou klamné servery používané bezpečnostními týmy k nalákání, upozornění na útočníky a jejich studiu.

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

D 1. Hrozba ransomwaru	G 2. Vícefaktorové ověřování	E 3. Zero-day exploit	H 4. Návnadový honeypot
C 5. Firewall proti průnikům	B 6. Reakce na incidenty	F 7. Hygiena hesel	A 8. Bezpečnostní rámec

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 FIREWALL	2 EXPLOIT	3 PHISHING	4 MALWARE
5 KYBERNETICKÁ HYGIENA	6 ŠIFROVÁNÍ		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 E – FIREWALL	2 F – REAKCE	3 A – RANSOMWARE	4 B – VÍCEFAKTOROVÉ
5 G – HYGIENA	6 H – RÁMEC	7 C – ZERODAY	8 D – HONEYPOT

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy Hrozba ransomwaru, Vícefaktorové ověřování a Zero-day exploit a ke každému uvést příklad.

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

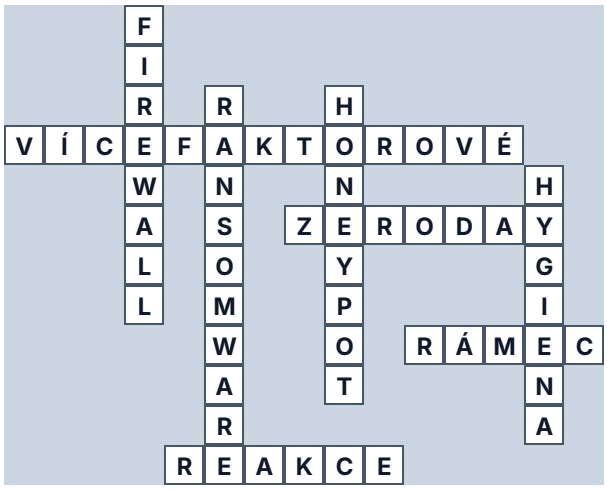
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

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

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

4 vodorovně: VÍCEFAKTOROVÉ Bezpečnostní ověření vyžadující dva a více autentizačních faktorů (13 písmen)

6 vodorovně: ZERODAY Zneužití zranitelnosti dříve, než výrobce vydá opravu (7 písmen)

7 vodorovně: RÁMEC Strukturované směrnice jako NIST používané k řízení kybernetických rizik (5 písmen)

8 vodorovně: REAKCE Strukturovaný plán pro zvládání a zmírňování bezpečnostních incidentů (6 písmen)

SVISLÉ NÁPOVĚDY

1 svisle: FIREWALL Síťová bariéra filtrující provoz podle bezpečnostních pravidel (8 písmen)

2 svisle: RANSOMWARE Malware šifrující data a požadující finanční platbu za dešifrování (10 písmen)

3 svisle: HONEYPOT Návnadový systém nastražený k přilákání a analýze útočníků (8 písmen)

5 svisle: HYGIENA Osvědčené postupy správy přihlašovacích údajů a autentizačních klíčů (7 písmen)

Klíč řešení přesmyček a šifry

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

KLÍČ K PŘESMYČKÁM

1.	RWMOARAESN	RANSOMWARE	5.	OOÍCTFÉARKVVE	VÍCEFAKTOROVÉ
2.	ZRYADOE	ZERODAY	6.	OTEPHYON	HONEYPOT
3.	EIFWALLR	FIREWALL	7.	CRKEAE	REAKCE
4.	AYEINHG	HYGIENA	8.	CRMEÁ	RÁMEC

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"ZABEZPEČTE SYSTÉM VÍCEFAKTOROVÝM OVĚŘENÍM"

Klíč k případovým studiím

A Případová studie 1: Strategie obnovy po ransomwaru

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Firemní síť je infikována ransomwarem, který zamkl kritické databáze. Útočníci požadují výkupné $100,000 v kryptoměně. Firma má offline zálohy staré 24 hodin.
- Doporučená strategie a řešení: Rizika zaplacení: Platba nezaručuje dešifrování souborů, označí firmu jako platící cíl a financuje trestnou činnost. Strategie obnovy: Tým by měl izolovat infikované hostitele, přemazat kompromitované servery a obnovit data z offline záloh. Musí také záplatovat původní vektor průniku (phishing nebo exploit), aby zabránil okamžité reinfekci.

B Případová studie 2: Obrana proti credential stuffingu

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Online služba čelí útoku typu credential stuffing, při kterém hackeři zkoušejí miliony párů uživatelských jmen a hesel ukradených z jiných webů.
- Doporučená strategie a řešení: Mechanismus: Útočníci zneužívají opakované používání hesel napříč weby a pomocí automatizovaných botů se přihlašují k uživatelským účtům. Obrana: 1. Vícefaktorové ověřování (MFA) zablokuje pokusy o přihlášení, i když je heslo správné. 2. Zavedení rate-limitingu a CAPTCHA blokuje automatizovaný provoz botů zahlcující přihlašovací endpointy.