Jméno: _____ Datum: _____ Body: _____

Ransomwarové útoky a firemní Obnova

Spuštění payloadu, kryptografické šifrování souborů, offline zálohy, postupy izolace a obnova po havárii.

ÚTOKY RANSOMWARU – PŘEHLED UČIVA

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 ransomwarovými útoky a obnovou podnikání. Prozkoumáte spuštění payloadu, šifrování souborů, offline zálohy, izolaci hrozeb, kryptoměnové platby a plány obnovy po havárii.

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/utok-ransomwarem/

Váš studijní plán: obnova po ransomwaru

- Rozlište payloady trojského koně, ransomwaru a spywaru.
- Analyzujte škodlivé soubory v zabezpečených sandboxových prostředích.
- Formulovat postupy rychlé izolace sítě a zamezení šíření.

PRŮVODCE ÚTOKY RANSOMWARU – POKYNY

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 obnovu po ransomwaru. Zakončete bonusovou aktivitou Mysli rychle.

ÚTOKY RANSOMWARU A OBNOVA PO HAVÁRII (ÚVOD)

Payloady ransomwaru kryptograficky uzamykají systémová úložiště a za dešifrovací klíče požadují výplaty v kryptoměnách. Zmírnění této hrozby zahrnuje pravidla síťové izolace, sandboxovou analýzu malwaru a robustní air-gapped studené zálohy.

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

Kontrolní bod 1: Výzva s výběrem odpovědí

1. **1. Jaký je primární mechanismus ransomwarového útoku?**
   - A. Kryptografické zašifrování uživatelských souborů k zamezení přístupu do systému
   - B. Vkládání škodlivých SQL příkazů do formulářových polí
   - C. Odposlech síťových paketů na veřejné Wi-Fi
   - D. Falšování hlaviček e-mailů k obejití validace SPF

2. **2. Co je offline (studená) záloha?**
   - A. Kopie úložiště odpojená od sítě, aby byla chráněna před šířením malwaru
   - B. Záloha uložená na pevném disku primárního webového serveru
   - C. Dočasná mezipaměť logů systémového registru
   - D. Administrátorský nástroj pro resetování uživatelských hesel

3. **3. Jak by bezpečnostní týmy měly izolovat infikované systémy během ransomwarového útoku?**
   - A. Okamžitě odpojit síťové kabely a vypnout bezdrátová rozhraní
   - B. Aktualizovat databázi antivirových signatur
   - C. Vypnout primární DNS server
   - D. Přejmenovat přípony napadených souborů

4. **4. Proč bezpečnostní agentury nedoporučují platit ransomwarové výkupné?**
   - A. Zaplacení povzbuzuje útočníky a nezaručuje dodání dešifrovacího klíče
   - B. Automaticky ruší platnost všech firemních pojistek
   - C. Automaticky upozorní každého zákazníka e-mailem
   - D. Poškodí zbývající záložní soubory systému

5. **5. Co je plán obnovy po havárii (DRP)?**
   - A. Strukturovaný proces obnovy provozu a dat po kompromitaci systému
   - B. Konfigurace firewallu mapující příchozí síťové porty
   - C. Databázové schéma s výpisem administrátorských oprávnění uživatelů
   - D. Protokol ověřování e-mailů odmítající podvržené domény

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. Payloady ransomwaru se mohou snadno rozšířit i na online zálohy připojené k síti.

- ○ Pravda
- ○ Nepravda

7 Otázka 7

7. Zaplacení výkupného v kryptoměně zaručuje, že soubory budou úspěšně dešifrovány.

- ○ Pravda
- ○ Nepravda

8 Otázka 8

8. Odpojení infikovaných systémů od sítě pomáhá zastavit šíření ransomwaru do sousedních systémů.

- ○ Pravda
- ○ Nepravda

9 Otázka 9

9. Symetrická kryptografie není ransomwarem k šifrování systémového úložiště nikdy používána.

- ○ Pravda
- ○ Nepravda

10 Otázka 10

10. Pravidelné testování postupů obnovy dat je klíčovou součástí disaster recovery.

- ○ Pravda
- ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

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

1. Kryptografickou technikou, kterou útočník odepře přístup k místním souborům, je _____ .
2. Aktivní škodlivý kód spuštěný v napadeném systému se označuje jako _____ .
3. Odpojené kopie dat uložené mimo pracoviště tvoří bezpečná _____ .
4. Zastavení šíření malwaru vyžaduje opatření zvané síťová _____ .
5. Platba v kryptoměně, kterou kyberzločinci požadují, se nazývá _____ .
6. Závěrečnou fází zotavení po útoku je _____ provozních datových souborů.

ZÁSOBNÍK SLOV

HAVÁRIE IZOLACE OBNOVA OFFLINE ZÁLOHA PAYLOAD ŠIFROVÁNÍ TROJSKÝ KŮŇ VÝKUPNÉ

Sem napište své odpovědi:

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

Kontrolní bod 4: Přiřazování bezpečnostních pojmů

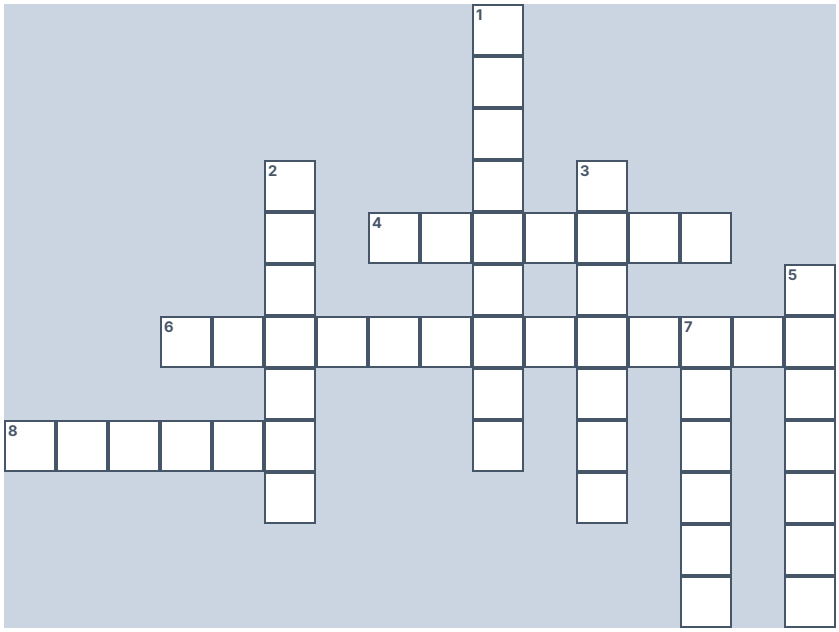
PŘIŘAZOVÁNÍ DEFINIC

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

☐	1. ŠIFROVÁNÍ	A	Odpojování infikovaných síťových systémů.
☐	2. PAYLOAD	B	Škodlivý soubor maskovaný jako neškodný.
☐	3. OFFLINE ZÁLOHA	C	Kryptografické uzamčení souborů.
☐	4. IZOLACE	D	Událost velkého narušení systému.
☐	5. VÝKUPNÉ	E	Spouštění škodlivého softwaru.
☐	6. OBNOVA	F	Odpojená offline kopie.
☐	7. KATASTROFA	G	Obnova databáze ze zálohy.
☐	8. TROJSKÝ KŮŇ	H	Žádost o výplatu za kryptografický klíč.

Kontrolní bod 5: Křížovka

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



VODOROVNÉ NÁPOVĚDY

4. Odpojení nakažených systémů od sítě. (7)

6. Odpojená offline kopie. (13)

8. Škodlivý soubor maskovaný jako neškodný. (6)

SVISLÉ NÁPOVĚDY

1. Kryptografické uzamčení souborů. (9)

2. Požadavek platby za kryptografický klíč. (7)

3. Událost velkého narušení systému. (7)

5. Spuštění škodlivého softwaru. (7)

7. Obnovení databáze ze zálohy. (6)

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: Odpojení nakažených systémů od sítě. (7 písmen):

6 vodorovně: Odpojená offline kopie. (13 písmen):

8 vodorovně: Škodlivý soubor maskovaný jako neškodný. (6 písmen):

SVISLÉ NÁPOVĚDY

1 svisle: Kryptografické uzamčení souborů. (9 písmen):

2 svisle: Požadavek platby za kryptografický klíč. (7 písmen):

3 svisle: Událost velkého narušení systému. (7 písmen):

5 svisle: Spuštění škodlivého softwaru. (7 písmen):

7 svisle: Obnovení databáze ze zálohy. (6 písmen):

Kontrolní bod 6: Hledání skrytých slov

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

H A V Á R I E I I D S Ř N E I

Š Ž T É Ř Ů E Z P A Á Ř P O Q

U É Y R J S U O Š A Č Ň Ý B Ě

Í N Š X T W Í L A S Y Ž Ý Ý L

N P F I R N S A J N M L Ť P G

Á U R Ř O G Ž C Á Ó Ů Ě O Ú C

V K Ý Š J Ý B E G M Ž F J A Ó

O Ý Q O A X C N Ž Z Ě Ý P W D

R V Ú L N Ů Q B Ó V Ť N F Ů Č

F Ý Ú K S Á X Ž Y N Š R X H P

I S T U D E N Á Z Á L O H A D

Š Á Č J Ř V W X L Í H U H Ě B

E I O B N O V A 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 H S Ě L Ť M S

SEZNAM SLOV

ŠIFROVÁNÍ PAYLOAD STUDENÁZÁLOHA IZOLACE VÝKUPNÉ OBNOVA HAVÁRIE TROJAN

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. PAYLOAD**
- **C. STUDENÁZÁLOHA**
- **D. IZOLACE**
- **E. VÝKUPNÉ**
- **F. OBNOVA**
- **G. HAVÁRIE**
- **H. TROJAN**

DEFINICE A POLE K PŘIŘAZENÍ

1. Odpojená offline kopie.
2. Škodlivý soubor maskovaný jako neškodný.
3. Kryptografické uzamčení souborů.
4. Požadavek platby za kryptografický klíč.
5. Odpojení nakažených systémů od sítě.
6. Událost velkého narušení systému.
7. Spuštění škodlivého softwaru.
8. Obnovení databáze ze zálohy.

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. **HETNUSOÁAÁ LZD**
3. **UVPÉKNÝ**
4. **EARÁIHV**
5. **ODLYPAA**
6. **COAILEZ**
7. **VOOANB**
8. **ONTAJR**

Bonusová aktivita: Mysli rychle

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

1	Informace, které byste nikdy neměli sdílet			
2	Zařízení, která lze hacknout			
3	Důvody, proč neplatit výkupné			
4	Bezpečné návyky, se kterými můžete začít už dnes			
5	Bezpečnostní nástroje, které znáte			
6	Způsoby, jak chránit své účty			
7	Známky toho, že je počítač nakažený			
8	Místa pro uložení zálohy			
9	Soubory, které nikdy nechcete ztratit			
10	Způsoby, jak se ransomware šíří			
11	Věci, které je třeba udělat v první hodině útoku			
12	Lidé, které je třeba kontaktovat během útoku			
13	Věci, které může ransomware zamknout			
14	Slova související s kyberbezpečností			
15	Organizace, které bývají častým cílem			

Kontrolní bod 8: Případové studie kyberbezpečnosti

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

PŘÍPADOVÁ STUDIE 1: ZADRŽENÍ RANSOMWAROVÉHO PAYLOADU V PODNIKU



Scénář: Firemní lokální síť byla napadena aktivním ransomwarem. Klíčové souborové servery začaly zobrazovat přípony souborů s .locked.

Otázka k diskusi: Popište kroky izolace a nastíněte protokol obnovy dat.

PŘÍPADOVÁ STUDIE 2: HODNOCENÍ ARCHITEKTUR OFFLINE ZÁLOH



Scénář: Podnik chce navrhnout strategii zálohování dat, která snižuje riziko kompromitace záloh i v případě, že je primární místní síť zcela ovládnuta ransomwarem.

Otázka k diskusi: Navrhněte zabezpečený systém offline zálohovacího trezoru.

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

22	3	20	22	35	30	8		29	14	11	26	22	35	1	20	2

6	1	30	1		40	8		28	30	32	6	8	20	9

40	2	18	22	13	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 ransomware?

Ransomware je škodlivý software navržený k zablokování přístupu k počítačovým systémům nebo souborům, dokud není zaplaceno výkupné.

Q2: Jak se ransomware šíří?

Prostřednictvím phishingových e-mailových příloh, nezáplatovaných softwarových zranitelností a kompromitovaných systémů vzdáleného přístupu. [1]

Q3: Proč je platba požadována v kryptoměně?

Kryptoměny jako Bitcoin nabízejí relativní anonymitu, takže je pro orgány činné v trestním řízení obtížné prostředky vysledovat.

Q4: Blokuje antivirus ransomware?

Ano, ale antivirus založený na signaturách může selhat proti nově vytvořeným zero-day ransomwarovým payloadům.

Q5: Co je air-gapped záloha?

Záložní kopie, která nemá žádné fyzické ani logické spojení s primární sítí, což ji chrání před šířením nákazy.

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

Projděte si časté otázky a odpovědi ohledně zmírňování online hrozeb.

Q6: Co je dvojité vydírání?

Když útočníci soubory nejen zašifrují, ale také ukradnou citlivá data a hrozí jejich zveřejněním, pokud nezaplatíte.

Q7: Co je dešifrovací nástroj (decryptor)?

Softwarový nástroj obsahující kryptografický klíč potřebný k obnovení zamčených souborů do prostého textu.

Q8: Jak se ransomware odhaluje včas?

Sledováním souborových systémů kvůli náhlé, masivní aktivitě úprav a přejmenovávání souborů.

Q9: Jaká je role pojištění?

Kybernetické pojištění může pomoci pokrýt náklady na obnovu, ale podmínky krytí a pravidla plateb výkupného se liší podle pojistky.

Q10: Mám infikovaný systém restartovat?

Ne, restart může zničit důkazy v operační paměti; místo toho jej izolujte od sítě. [1]

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

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

Q1: Jak ransomware používá asymetrické šifrování?

Používá veřejný klíč vložený do malwaru k šifrování souborů, k jejichž dešifrování je potřeba soukromý klíč útočníka.

Q2: Proč se používá také symetrické šifrování?

Symetrické šifrování (jako AES) je rychlé a dokáže uzamknout obrovské databáze během minut, zatímco asymetrické klíče zabezpečují klíč AES.

Q3: Co je logická segmentace?

Rozdělování sítí do izolovaných zón, které brání malwaru v laterálním šíření z pracovních stanic na klíčové servery.

Q4: Co je úložiště WORM?

Média Write-Once, Read-Many, která brání úpravě, přepsání nebo smazání zálohovaných dat ransomwarovými payloady.

Q5: Co jsou stínové kopie?

Místní záložní snímky vytvářené Windows; ransomware je obvykle maže jako první pomocí administrátorských nástrojů.

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

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

Q6: Jak krádež přihlašovacích údajů umožňuje ransomware?

Útočníci kupují uniklé přihlašovací údaje správců, přihlašují se přes vzdálené plochy a ručně spouštějí ransomware napříč sítí.

Q7: Co je zkušební (dry-run) test obnovy?

Pravidelné obnovování zálohovaných databází do izolovaných testovacích prostředí k ověření, že rychlost obnovy a integrita dat splňují metriky disaster recovery.

Q8: Jak detekce na koncových bodech (EDR) zastavuje ransomware?

Analýzou chování procesů (např. rychlé šifrování) a rychlým pozastavením podezřelé aplikace.

Q9: Co je model ransomware-as-a-service (RaaS)?

Franšízový model, kdy vývojáři malwaru pronajímají nástroje pro tvorbu ransomwaru přidruženým subjektům výměnou za procento z výnosů.

Q10: Jak neopravené RDP spouští ransomware?

Vystavené, nezáplatované brány Remote Desktop Protocolu umožňují útočníkům hrubou silou prolomit přihlášení a ručně spustit malware.

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

Aktéři ransomwaru často používají nástroje jako vssadmin.exe k odstranění stínových kopií Windows a zablokování lokálních obnov. [1]

2. BEZPEČNOSTNÍ POSTŘEH

Symetrické klíče AES-256 se obvykle používají k šifrování payloadů souborů, které se pak uzamykají veřejnými klíči RSA.

3. BEZPEČNOSTNÍ POSTŘEH

Zotavení z úspěšného ransomwarového útoku může trvat týdny, a proto jsou důležité otestované offline zálohy.

4. BEZPEČNOSTNÍ POSTŘEH

FBI placení výkupného nepodporuje a varuje, že zaplacení nezaručuje, že nějaká data dostanete zpět. [2]

5. BEZPEČNOSTNÍ POSTŘEH

Plány obnovy po havárii (DRP) by měly definovat cílovou dobu obnovy (RTO) a cílový bod obnovy (RPO).

6. BEZPEČNOSTNÍ POSTŘEH

FBI doporučuje zálohy, které jsou šifrované a neměnné, tedy je nelze upravit ani smazat. [3]

7. POSTŘEH K BEZPEČNOSTI

Vývojáři ransomwaru využívají pokročilé obfuskační techniky k obejití tradičních signaturních antivirových skenerů.

8. POSTŘEH K BEZPEČNOSTI

Segmentace sítě omezuje laterální pohyb a pomáhá zastavit šíření ransomwaru za prvního nakaženého hostitele. [3]

9. POSTŘEH K BEZPEČNOSTI

Vystavené, špatně zabezpečené vzdálené služby, jako je Remote Desktop Protocol (RDP), jsou běžným vstupním bodem ransomwaru. [1]

10. BEZPEČNOSTNÍ POSTŘEH

CISA doporučuje uchovávat šifrované zálohy offline, protože mnoho variant ransomwaru dostupné zálohy vyhledává a maže. [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] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[2] FBI Internet Crime Complaint Center. (n.d.). Ransomware.
https://www.ic3.gov/CrimeInfo/Ransomware

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

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

[5] 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

Klíč odpovědí: Kontrolní bod 1 - Výběr z možností

1 Otázka 1

Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Jaký je primární mechanismus ransomwarového útoku? → Kryptografické zašifrování uživatelských souborů k zamezení přístupu do systému

2 Otázka 2

Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Co je offline (studená) záloha? → Kopie úložiště odpojená od sítě, aby byla chráněna před šířením malwaru

3 Otázka 3

Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Jak by bezpečnostní týmy měly izolovat infikované systémy během ransomwarového útoku? → Okamžitě odpojit síťové kabely a vypnout bezdrátová rozhraní

4 Otázka 4

Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Proč bezpečnostní agentury nedoporučují platit ransomwarové výkupné? → Zaplacení povzbuzuje útočníky a nezaručuje dodání dešifrovacího klíče

5 Otázka 5

Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Co je plán obnovy po havárii (DRP)? → Strukturovaný proces obnovy provozu a dat po kompromitaci systému

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

6 **Otázka 6** — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Payloady ransomwaru se mohou snadno rozšířit i na online zálohy připojené k síti.

7 **Otázka 7** — **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: FBI varuje, že zaplacení nezaručuje, že dostanete jakákoli data zpět. [2]

8 **Otázka 8** — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Pravda: CISA radí odpojit infikované hostitele nebo vzít síť offline, aby se šíření omezilo.

9 **Otázka 9** — **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: ransomware obvykle šifruje soubory rychlými symetrickými šiframi, jako je AES.

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

POZNÁMKA PRO VYUČUJÍCÍ

Pravidelné testování postupů obnovy dat je klíčovou součástí disaster recovery.

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

C 1. ŠIFROVÁNÍ	E 2. PAYLOAD	F 3. OFFLINE ZÁLOHA	A 4. IZOLACE
H 5. VÝKUPNÉ	G 6. OBNOVA	D 7. KATASTROFA	B 8. TROJSKÝ KŮŇ

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 ŠIFROVÁNÍ	2 PAYLOAD	3 OFFLINE ZÁLOHA	4 IZOLACE
5 VÝKUPNÉ	6 OBNOVA		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 C – STUDENÁZÁLOHA	2 H – TROJAN	3 A – ŠIFROVÁNÍ	4 E – VÝKUPNÉ
5 D – IZOLACE	6 G – HAVÁRIE	7 B – PAYLOAD	8 F – OBNOVA

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

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

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

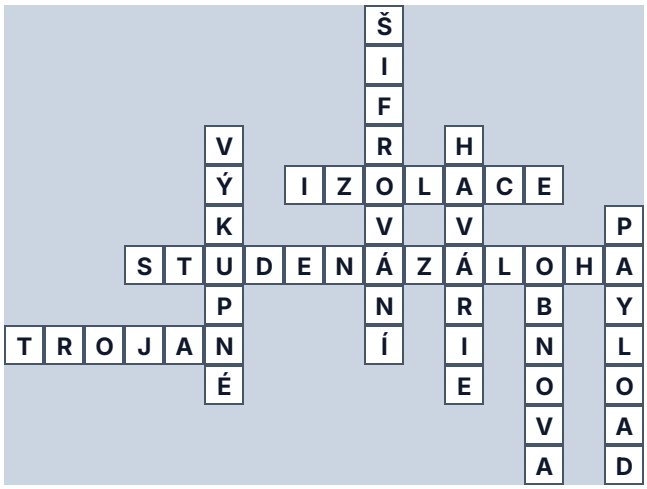
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

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

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

4 vodorovně: IZOLACE Odpojení nakažených systémů od sítě. (7 písmen)

6 vodorovně: STUDENÁZÁLOHA Odpojená offline kopie. (13 písmen)

8 vodorovně: TROJAN Škodlivý soubor maskovaný jako neškodný. (6 písmen)

SVISLÉ NÁPOVĚDY

1 svisle: ŠIFROVÁNÍ Kryptografické uzamčení souborů. (9 písmen)

2 svisle: VÝKUPNÉ Požadavek platby za kryptografický klíč. (7 písmen)

3 svisle: HAVÁRIE Událost velkého narušení systému. (7 písmen)

5 svisle: PAYLOAD Spuštění škodlivého softwaru. (7 písmen)

7 svisle: OBNOVA Obnovení databáze ze zálohy. (6 písmen)

Klíč řešení přesmyček a šifry

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

KLÍČ K PŘESMYČKÁM

1.	VORIŠÁNÍF	ŠIFROVÁNÍ	5.	ODLYPAA	PAYLOAD
2.	HETNUSOÁAÁLZD	STUDENÁZÁLOHA	6.	COAILEZ	IZOLACE
3.	UVPÉKNÝ	VÝKUPNÉ	7.	VOOANB	OBNOVA
4.	EARÁIHV	HAVÁRIE	8.	ONTAJR	TROJAN

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"OBNOVTE ŠIFROVANÁ DATA ZE STUDENÉ ZÁLOHY"

Klíč k případovým studiím

A Případová studie 1: Zadržení ransomwarového payloadu v podniku

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Firemní lokální síť byla napadena aktivním ransomwarem. Na klíčových souborových serverech se začaly objevovat soubory s příponou .locked.
- Doporučená strategie a řešení: Odpojte všechny zasažené servery od lokální sítě. Ukončete aktivní administrátorské relace. Obnovte nekompromitované soubory ze zabezpečeného offline zálohovacího systému chráněného proti zápisu.

B Případová studie 2: Hodnocení architektur offline záloh

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Podnik chce navrhnout strategii zálohování dat, která snižuje riziko kompromitace záloh i v případě, že primární lokální síť bude zcela ovládnuta ransomwarem.
- Doporučená strategie a řešení: Zaveďte úložiště typu write-once-read-many (WORM). Vytvořte logickou vzduchovou mezeru odpojením zálohovacího systému od všech sítí a vynucujte denní rotaci fyzických médií.