Jméno: _____ **Datum:** _____ **Body:** _____

Zabezpečení CyberGhost

Hodnocení bezpečnostní infrastruktury CyberGhost, vlastních polí serverů NoSpy v Rumunsku, bezdiskových serverových uzlů pouze s RAM, šifrování AES-256 a automatické ochrany kill switch.

PŘEHLED VÝUKY: ZABEZPEČENÍ CYBERGHOST

STUDENT
STUDENTSKÝ STATUS
Dráha obránce sítě

ZABEZPEČENÝ
STAV PŘIPOJENÍ
Stínění datových paketů

AKTIVNÍ
OCHRANA PROTI ÚNIKŮM
Ochrana proti únikům DNS a IPv6

Vítejte! Tento balíček aktivit vás provede bezpečnostními funkcemi CyberGhost. Prozkoumáte vlastní pole serverů NoSpy, bezdiskový hardware pouze s RAM, šifry a kill switche.

KONTROLNÍ BODY PRACOVNÍHO LISTU

- [ ] **Část 1-4: Zvládněte konfigurace VPN a zabezpečení sítě.**
- [ ] **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 nejlepšími VPN od VPN.com

URL: https://www.vpn.com/cs/vpn/cyberghost/bezpecnost/

Váš studijní plán: zabezpečení CyberGhost

- Analyzujte technickou architekturu a konfigurační pravidla zabezpečení CyberGhost.
- Nakonfigurujte nastavení klienta tak, aby bránilo únikům IP, DNS a WebRTC provozu.
- Porovnejte vlastní ceny, zkušební verze a výkonnostní funkce se standardními modely.

POKYNY K BEZPEČNOSTNÍMU PRŮVODCI CYBERGHOST

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 šifrování a servery NoSpy. Zakončete bonusovou aktivitou Mysli rychle.

VLASTNÍ SERVEROVÁ INFRASTRUKTURA NOSPY A BEZDISKOVÉ UZLY (ÚVOD)

CyberGhost provozuje soukromě spravované servery NoSpy ve své centrále v Bukurešti v Rumunsku, čímž obchází rizika komerčního hostingu. Bezpečnost zajišťují šifry AES-256, bezdiskový hardware pouze s RAM a automatické kill switche.

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

Kontrolní bod 1: Výzva s výběrem odpovědí

1. Který protokol nabízí CyberGhost na všech hlavních platformách?
   - A) WireGuard
   - B) OpenVPN
   - C) IKEv2
   - D) L2TP

2. Jakou šifru používají připojení CyberGhost přes OpenVPN a IKEv2?
   - A) AES-256
   - B) Blowfish-128
   - C) DES-56
   - D) RC4

3. Kde se nacházejí vlastní NoSpy servery CyberGhost?
   - A) Rumunsko
   - B) Německo
   - C) Spojené státy
   - D) Švýcarsko

4. Jaký typ infrastruktury nezanechá při vypnutí žádné logy na disku?
   - A) Servery pouze v RAM
   - B) Servery s HDD
   - C) Virtuální servery
   - D) Hybridní servery

5. Jaká funkce blokuje připojení během výpadků VPN?
   - A) Kill switch
   - B) Rozdělené tunelování
   - C) Smart DNS
   - D) Přesměrovat port

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. CyberGhost má sídlo v Rumunsku, mimo skupinu 14 Eyes.

○ Pravda ○ Nepravda

7 Otázka 7

7. Servery NoSpy jsou pronajaté od komerčních datacenter třetích stran.

○ Pravda ○ Nepravda

8 Otázka 8

8. RAM-only servery zapisují data uživatelských relací na trvalé SSD disky.

○ Pravda ○ Nepravda

9 Otázka 9

9. Klientská aplikace obsahuje vestavěnou ochranu proti únikům DNS.

○ Pravda ○ Nepravda

10 Otázka 10

10. Politika nulových logů CyberGhost byla ověřena nezávislými audity.

○ Pravda ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

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

1. Vysoce výkonným protokolem doporučovaným pro mobilní připojení je _____ .
2. Datový provoz je šifrován vysoce bezpečnou symetrickou šifrou _____ .
3. Země, ve které má společnost sídlo a jejíž jurisdikce se na ni vztahuje, je _____ .
4. Samostatně spravované vysoce zabezpečené servery vlastněné přímo firmou se označují jako _____ .
5. Aby data nepřetrvala po vypnutí, používají se bezdisková pole typu _____ .
6. Odhalení nešifrovaného provozu při výpadku spojení brání pojistná funkce _____ .

ZÁSOBNÍK SLOV

AES-256 AUDIT KILL SWITCH NOSPY RAM-ONLY RUMUNSKO ÚNIK DAT WIREGUARD

Sem napište své odpovědi:

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

Kontrolní bod 4: Přiřazování pojmů VPN a sítí

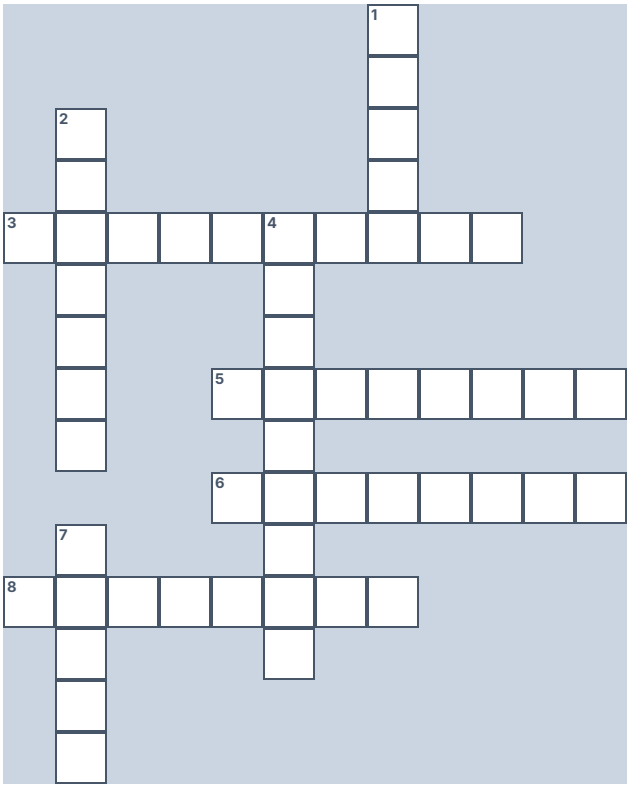
PŘIŘAZOVÁNÍ DEFINIC

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

☐	1. WIREGUARD	A	Národní jurisdikce ochrany soukromí ležící mimo aliance 14 očí.
☐	2. AES-256	B	Bezdisková serverová infrastruktura nezapisující žádné trvalé logy.
☐	3. RUMUNSKO	C	Nechtěný únik dotazů resolveru mimo VPN.
☐	4. NOSPY	D	Vysokorychlostní open-source protokol dostupný v aplikacích CyberGhost.
☐	5. RAM-ONLY	E	Ověření třetí stranou přezkoumávající tvrzení o dodržování nulových logů.
☐	6. KILL SWITCH	F	Standard symetrické šifry zabezpečující přenos payloadů tunely.
☐	7. ÚNIK	G	Plně vlastněné pole vysoce zabezpečených serverů provozované v Rumunsku.
☐	8. AUDIT	H	Pojistná klientská utilita přerušující internetový provoz při výpadcích.

Kontrolní bod 5: Křížovka

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



VODOROVNÉ NÁPOVĚDY

3. Pojistka klienta přerušující internetový provoz při výpadku spojení (10)

5. Standard symetrické šifry (AES-256) zabezpečující přenosy dat tunely (8)

6. Národní jurisdikce ochrany soukromí ležící mimo aliance 14 očí (8)

8. Bezdisková serverová infrastruktura nezapisující žádné trvalé logy (8)

SVISLÉ NÁPOVĚDY

1. Ověření třetí stranou přezkoumávající tvrzení o dodržování nulových logů (5)

2. Nechtěné odhalení požadavků na překlad DNS mimo VPN (7)

4. Rychlý open-source protokol dostupný napříč aplikacemi CyberGhost (9)

7. Plně vlastněné vysoce zabezpečené serverové pole provozované v Rumunsku (5)

Kontrolní bod 5, alternativa: Přístupná zadání křížovky

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

VODOROVNÉ NÁPOVĚDY

3 vodorovně: Pojistka klienta přerušující internetový provoz při výpadku spojení (10 písmen):

5 vodorovně: Standard symetrické šifry (AES-256) zabezpečující přenosy dat tunely (8 písmen):

6 vodorovně: Národní jurisdikce ochrany soukromí ležící mimo aliance 14 očí (8 písmen):

8 vodorovně: Bezdisková serverová infrastruktura nezapisující žádné trvalé logy (8 písmen):

SVISLÉ NÁPOVĚDY

1 svisle: Ověření třetí stranou přezkoumávající tvrzení o dodržování nulových logů (5 písmen):

2 svisle: Nechtěné odhalení požadavků na překlad DNS mimo VPN (7 písmen):

4 svisle: Rychlý open-source protokol dostupný napříč aplikacemi CyberGhost (9 písmen):

7 svisle: Plně vlastněné vysoce zabezpečené serverové pole provozované v Rumunsku (5 písmen):

Kontrolní bod 6: Hledání skrytých slov

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

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

SEZNAM SLOV

WIREGUARD AESŠIFRA RUMUNSKO NOSPY POUZERAM KILLSWITCH ÚNIKDAT AUDIT

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. WIREGUARD
B. AESŠIFRA
C. RUMUNSKO
D. NOSPY
E. POUZERAM
F. KILLSWITCH
G. ÚNIKDAT
H. AUDIT

	DEFINICE A POLE K PŘIŘAZENÍ
	1. Nechtěné odhalení požadavků na překlad DNS mimo VPN.
	2. Rychlý open-source protokol dostupný napříč aplikacemi CyberGhost.
	3. Plně vlastněné vysoce zabezpečené serverové pole provozované v Rumunsku.
	4. Pojistka klienta přerušující internetový provoz při výpadku spojení.
	5. Standard symetrické šifry (AES-256) zabezpečující přenosy dat tunely.
	6. Národní jurisdikce ochrany soukromí ležící mimo aliance 14 očí.
	7. Ověření třetí stranou přezkoumávající tvrzení o dodržování nulových logů.
	8. Bezdisková serverová infrastruktura nezapisující žádné trvalé logy.

Kontrolní bod 7: Výzva s přeházenými slovy

Přeuspořádejte písmena níže a odhalte klíčové pojmy a termíny virtuální privátní sítě (VPN). Odpovědi pište do připravených polí.

1. **UGEIWARDR**
2. **UROUKSNM**
3. **ZOPERMAU**
4. **TNDKAÚI**
5. **IFEAŠARS**
6. **PNSYO**
7. **ILKIWTCHSL**
8. **TADIU**

Bonusová aktivita: Mysli rychle

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

1	Streamovací služby, které sledujete			
2	Tlačítka nebo nabídky ve VPN aplikaci			
3	Nastavení, která zapnete pro extra bezpečnost			
4	VPN služby jiné než CyberGhost			
5	Věci, které šifrování chrání			
6	Věci, které CyberGhost dokáže skrýt před vaší sítí			
7	Hrozby na veřejné Wi-Fi			
8	Typy úniků u VPN			
9	Bezpečnostní funkce v CyberGhost			
10	Věci, které může audit prověřit			
11	Situace, kdy pomůže kill switch			
12	Země známé přísnými zákony na ochranu soukromí			
13	Slova, která popisují dobrou VPN aplikaci			
14	Země, kde byste chtěli servery CyberGhost			
15	Způsoby, jak vytvořit silné heslo			

Kontrolní bod 8: Případové studie VPN a sítí

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

PŘÍPADOVÁ STUDIE 1: AUDIT SOUKROMÍ Z HLEDISKA JURISDIKCE



Scénář: Mediální společnost chce zajistit, aby záznamy firemního zpravodajství nemohly být na základě soudního příkazu vyžádány zahraničními orgány činnými v trestním řízení.

Otázka k diskusi: Jak rumunské sídlo CyberGhost chrání společnost před sledovacími příkazy?

PŘÍPADOVÁ STUDIE 2: BEZPEČNOST PŘI ZABAVENÍ HARDWARU



Scénář: V serverovém zařízení dojde k neoprávněnému fyzickému vniknutí a serverový rack VPN je zabaven.

Otázka k diskusi: Jaký hardwarový design brání vetřelcům v extrakci klíčů relací nebo historie uživatelů?

Kontrolní bod 9: Dešifrování šifry

Síťový inženýr zabezpečuje směrovací kanály a klientské tunely. 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

20 22 28 24 38 28 8 26 35 8 26 38

40 1 16 14 29 31 32 16 15 19 1 37 14 19 2 18 20 15

28 22 32 17 26 22 19 15

Dešifrovaná zpráva:

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

Kontrolní bod 10: Základní časté otázky k VPN (část A)

Projděte si nejčastější otázky a odpovědi o virtuálních privátních sítích (VPN) a tunelování.

Q1: Je CyberGhost bezpečný?

Ano, používá šifrování AES-256, bezpečné protokoly a působí podle rumunských zákonů na ochranu soukromí.

Q2: Co jsou servery NoSpy?

Servery NoSpy vlastní, staví a spravuje výhradně CyberGhost ve svém rumunském sídle pro maximální bezpečnost.

Q3: Uchovává CyberGhost logy?

Ne, uplatňuje přísné zásady nulových logů, což znamená, že se neukládá historie prohlížení ani logy připojení.

Q4: Kde sídlí CyberGhost?

CyberGhost sídlí v Bukurešti v Rumunsku, jehož Ústavní soud v letech 2009 a 2014 zrušil plošné zákony o uchovávání dat, ačkoli zákon z roku 2015 opět vyžaduje, aby poskytovatelé elektronických komunikací uchovávali některá provozní data.

Q5: Jaké protokoly používá?

Podporuje protokoly WireGuard, OpenVPN (TCP/UDP) a IKEv2 v závislosti na typu zařízení.

Kontrolní bod 10: Základní časté otázky k VPN (část B)

Projděte si nejčastější otázky a odpovědi o virtuálních privátních sítích (VPN) a tunelování.

Q6: Blokuje reklamy?

Ano, klientská aplikace obsahuje vestavěný blokátor obsahu pro reklamy, sledovací skripty a malwarové domény.

Q7: Existuje kill switch?

Ano, nabízí automatický kill switch, který zablokuje přístup k internetu, pokud se připojení VPN přeruší.

Q8: Chrání CyberGhost před úniky?

Ano, aplikace obsahují vestavěnou ochranu proti únikům DNS a IP, která skrývá vaši skutečnou IP adresu.

Q9: Jsou servery auditovány?

Ano, zero-logs politika a infrastruktura CyberGhost jsou nezávisle auditovány společností Deloitte. [2]

Q10: Používá RAM servery?

Ano, serverová síť CyberGhost je dle CyberGhost provozována na bezdiskovém hardwaru pouze s RAM.

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

Prozkoumejte pokročilé technické aspekty VPN tunelovacích protokolů, integrací mobilních klientů a podnikového nasazení.

Q1: Který protokol se používá ve výchozím nastavení?

Aplikace vybírá nejlepší protokol automaticky, ale kdykoli jej můžete přepnout.

Q2: Jak funguje rozdělené tunelování?

Umožňuje vám zvolit, které aplikace a weby používají VPN a které tunel obcházejí.

Q3: Kam směřují DNS dotazy?

Jsou odesílány VPN tunelem na vlastní DNS servery CyberGhost, nikoli na servery vašeho ISP.

Q4: Kdo vlastní CyberGhost?

CyberGhost vlastní Kape Technologies, která vlastní také ExpressVPN a Private Internet Access. [7]

Q5: Jaká šifra se používá s WireGuardem?

WireGuard používá moderní symetrický šifrovací standard ChaCha20-Poly1305. [9]

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

Prozkoumejte pokročilé technické aspekty VPN tunelovacích protokolů, integrací mobilních klientů a podnikového nasazení.

Q6: V čem se liší servery NoSpy?

Mají výkonnější hardware s vyšší šířkou pásma, vyhrazené uplinky a jsou umístěny v privátním datacentru.

Q7: Jsou dedikované IP anonymní?

Ano, IP adresa je spárována s náhodným tokenem místo vašeho účtu a token je poté smazán.

Q8: Kdo audituje politiku nulových logů?

Deloitte Audit Romania, která v roce 2025 dokončila svůj třetí audit CyberGhost bez logů.

Q9: Dešifruje blokátor reklam HTTPS?

Ne, blokátor reklam pracuje na úrovni DNS a překládá reklamní domény do černých děr.

Q10: Mohu použít CyberGhost na routeru?

Ano, nastavte CyberGhost na routeru kompatibilním s VPN a pokryjte tak každé zařízení v domácnosti.

Část 11: 10 faktů a poznatků o VPN z praxe

Projděte si fakta z praxe o rychlostech VPN šifrování, auditech protokolů, mobilní konektivitě a podnikové práci na dálku.

1. VPN POSTŘEH

CyberGhost má sídlo v Rumunsku, mimo zpravodajskou alianci Five Eyes. [1]

2. VPN POSTŘEH

OpenVPN a IKEv2 používají AES-256, zatímco WireGuard používá ChaCha20-Poly1305. [5]

3. VPN POSTŘEH

Servery NoSpy vlastní a interně spravuje personál CyberGhost. [3]

4. VPN POSTŘEH

Deloitte pravidelně audituje a ověřuje jejich provozní zásady nulových logů. [2]

5. VPN POSTŘEH

Bezdisková serverová pole pouze s RAM brání přetrvání dat po vypnutí. [1]

6. VPN POSTŘEH

Klientská aplikace obsahuje automatický kill switch pro případ výpadku VPN připojení.

7. POSTŘEH K VPN

Vestavěná ochrana proti únikům DNS a IP pomáhá udržet vaši skutečnou IP skrytou.

8. POSTŘEH K VPN

Protokoly WireGuard, OpenVPN a IKEv2 jsou nativně podporovány v klientovi. [4]

9. POSTŘEH K VPN

Dedikované IP adresy se přidělují pomocí zabezpečeného systému tokenů s nulovou znalostí. [8]

10. VPN POSTŘEH

Vestavěné malwarové filtry skenují dotazy na domény a blokují škodlivé cíle. [6]

Technické reference a zdroje

Studijní příručka a interaktivní hádanky jsou sestaveny z globálních technických standardů, specifikací a regulačních rámců.

AKADEMICKÉ A OBOROVÉ REFERENCE

[1] CyberGhost VPN. (n.d.). No-Logs VPN: Secure & Private VPN with Zero Tracking.
https://www.cyberghostvpn.com/features/no-logs-vpn

[2] CyberGhost VPN. (2025). Third Deloitte Romania Audit Verifies Our Commitment to Privacy.
https://www.cyberghostvpn.com/privacyhub/privacy-audit-2025/

[3] CyberGhost VPN. (n.d.). CyberGhost's NoSpyServers: Complete Privacy & Anonymity.
https://www.cyberghostvpn.com/features/nospy

[4] CyberGhost VPN Support Center. (n.d.). Which VPN Protocols Do You Support?
https://support.cyberghostvpn.com/hc/en-us/articles/213983829-Which-VPN-Protocols-Do-You-Support

[5] CyberGhost VPN. (n.d.). VPN Encryption: How VPNs Help Secure Your Browsing.
https://www.cyberghostvpn.com/features/vpn-encryption

[6] CyberGhost VPN. (n.d.). VPN Features and Use Cases.
https://www.cyberghostvpn.com/features

[7] Kape Technologies. (n.d.). Our Brands.
https://www.kape.com/our-brands/

[8] CyberGhost VPN. (n.d.). Dedicated IP VPN | Get a Secure Static IP Address.
https://www.cyberghostvpn.com/dedicated-ip-vpn

[9] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[10] Nir, Y., & Langley, A. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols.
https://www.rfc-editor.org/rfc/rfc8439

[11] National Institute of Standards and Technology. (n.d.). FIPS 197: Advanced Encryption Standard (AES).
https://csrc.nist.gov/pubs/fips/197/final

[12] European Digital Rights (EDRi). (2014). Romania: The aftermath of the second CCR data retention ruling.
https://edri.org/our-work/romania-aftermath-of-second-ccr-data-retention-ruling/

Klíč odpovědí: Kontrolní bod 1 - Výběr z možností

1 Otázka 1 — Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Který protokol nabízí CyberGhost na všech hlavních platformách? → A) WireGuard

2 Otázka 2 — Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Jakou šifru používají připojení CyberGhost přes OpenVPN a IKEv2? → A) AES-256

3 Otázka 3 — Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Kde se nacházejí vlastní NoSpy servery CyberGhost? → Rumunsko

4 Otázka 4 — Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Jaký typ infrastruktury nezanechá při vypnutí žádné logy na disku? → Servery pouze v RAM

5 Otázka 5 — Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Jaká funkce blokuje připojení během výpadků VPN? → Kill switch

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

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

POZNÁMKA PRO VYUČUJÍCÍ

CyberGhost má sídlo v Rumunsku, mimo skupinu 14 Eyes. [1]

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

POZNÁMKA PRO VYUČUJÍCÍ

Servery NoSpy jsou pronajaté od komerčních datacenter třetích stran.

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

POZNÁMKA PRO VYUČUJÍCÍ

RAM-only servery zapisují data uživatelských relací na trvalé SSD disky.

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

POZNÁMKA PRO VYUČUJÍCÍ

Klientská aplikace obsahuje vestavěnou ochranu proti únikům DNS.

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

POZNÁMKA PRO VYUČUJÍCÍ

Politika nulových logů CyberGhost byla ověřena nezávislými audity.

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. WIREGUARD	F 2. AES-256	A 3. RUMUNSKO	G 4. NOSPY
B 5. RAM-ONLY	H 6. KILL SWITCH	C 7. ÚNIK	E 8. AUDIT

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 WIREGUARD	2 AES-256	3 RUMUNSKO	4 NOSPY
5 RAM-ONLY	6 KILL SWITCH		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 G – ÚNIKDAT	2 A – WIREGUARD	3 D – NOSPY	4 F – KILLSWITCH
5 B – AESŠIFRA	6 C – RUMUNSKO	7 H – AUDIT	8 E – POUZERAM

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy WIREGUARD, AES-256 a RUMUNSKO a ke každému uvést příklad.

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

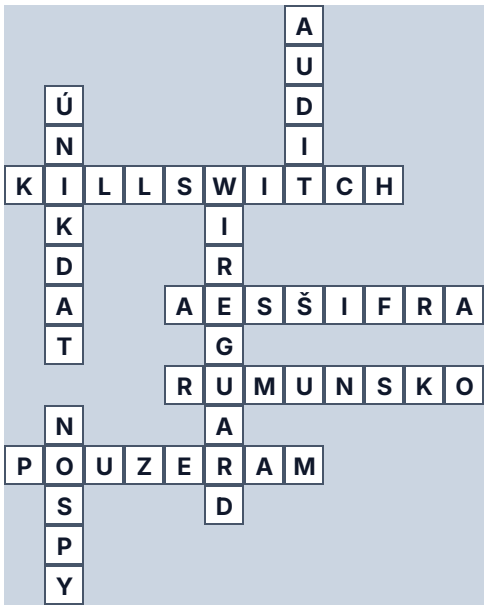
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

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

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

3 vodorovně: KILLSWITCH Pojistka klienta přerušující internetový provoz při výpadku spojení (10 písmen)

5 vodorovně: AESŠIFRA Standard symetrické šifry (AES-256) zabezpečující přenosy dat tunely (8 písmen)

6 vodorovně: RUMUNSKO Národní jurisdikce ochrany soukromí ležící mimo aliance 14 očí (8 písmen)

8 vodorovně: POUZERAM Bezdisková serverová infrastruktura nezapisující žádné trvalé logy (8 písmen)

SVISLÉ NÁPOVĚDY

1 svisle: AUDIT Ověření třetí stranou přezkoumávající tvrzení o dodržování nulových logů (5 písmen)

2 svisle: ÚNIKDAT Nechtěné odhalení požadavků na překlad DNS mimo VPN (7 písmen)

4 svisle: WIREGUARD Rychlý open-source protokol dostupný napříč aplikacemi CyberGhost (9 písmen)

7 svisle: NOSPY Plně vlastněné vysoce zabezpečené serverové pole provozované v Rumunsku (5 písmen)

Klíč řešení přesmyček a šifry

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

KLÍČ K PŘESMYČKÁM

1. UGEIWARDR — WIREGUARD
2. UROUKSNM — RUMUNSKO
3. ZOPERMAU — POUZERAM
4. TNDKAÚI — ÚNIKDAT
5. IFEAŠARS — AESŠIFRA
6. PNSYO — NOSPY
7. ILKIWTCHSL — KILLSWITCH
8. TADIU — AUDIT

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"NOSPY SERVERY ZAJIŠŤUJÍ MAXIMÁLNÍ SOUKROMÍ"

Klíč k případovým studiím

A PŘÍPADOVÁ STUDIE 1: AUDIT SOUKROMÍ Z HLEDISKA JURISDIKCE

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Mediální společnost chce zajistit, aby záznamy firemního zpravodajství nemohly být předvolány zahraničními orgány činnými v trestním řízení.
- Doporučená strategie a řešení: Rumunsko má silné zákony na ochranu soukromí a není členem zpravodajských aliancí Five-Eyes ani Fourteen-Eyes.

B PŘÍPADOVÁ STUDIE 2: BEZPEČNOST PŘI ZABAVENÍ HARDWARU

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: V serverovém zařízení dojde k neoprávněnému fyzickému vniknutí a je zabaven rack s VPN servery.
- Doporučená strategie a řešení: Server běží na RAM-only architektuře, takže při přerušení napájení jsou všechna data okamžitě ztracena.