Name: _____ Datum: _____ Punkte: _____

So wählen Sie ein VPN aus Arbeitsblatt

Bewertung von VPN-Anbietern, Sicherheitsstandards, Audits und Protokollierungsrichtlinien

VPN-LERNÜBERSICHT

LERNENDE
STUDIERENDENSTATUS
Lernpfad Netzwerkverteidigung

SICHER
VERBINDUNGSSTATUS
Abschirmung von Datenpaketen

AKTIV
SCHUTZ VOR LECKS
Schutz vor DNS- und IPv6-Leaks

Willkommen! Dieses Aktivitätspaket führt Sie durch die Grundprinzipien virtueller privater Netzwerke (VPNs). Sie erfahren, wie verschlüsselte Tunnel Ihre Daten schützen, wie Netzwerkprotokolle funktionieren und wie man Datenlecks bei der Privatsphäre erkennt und eindämmt.

KONTROLLPUNKTE DES ARBEITSBLATTS

- [ ] **Teil 1-4: VPN-Konzepte und -Protokolle beherrschen.**
- [ ] **Teil 5-7: Kreuzworträtsel und Suchsel lösen.**
- [ ] **Teil 8-9: Fallstudien und Chiffre-Aufgabe lösen.**
- [ ] **Teil 10: Seiten mit grundlegenden und fortgeschrittenen häufigen Fragen durchgehen.**
- [ ] **Teil 11: 10 interessante Fakten aus der Praxis entdecken.**
- [ ] **Bonus: Herausforderung Schnell denken.**

VPN-Leitfaden von VPN.com öffnen

URL: https://www.vpn.com/de/vpn/

Ihr Lernfahrplan: VPN

- Bewerten Sie die Gerichtsbarkeit des Anbieters und No-Logs-Richtlinien im Hinblick auf den Datenschutz.
- Vergleichen Sie Tunnelprotokolle wie WireGuard und OpenVPN hinsichtlich der Geschwindigkeit.
- Analysieren Sie Sicherheitsfunktionen wie Kill Switches und reine RAM-Serverknoten.
- Bei der Auswahl unabhängige Sicherheitsaudits und Preismodelle ermitteln.
- Wählen Sie Serverstandorte entsprechend Ihren Anforderungen an Geschwindigkeit und das Umgehen von Geosperren.

ANLEITUNG ZUM AUSWAHL-ARBEITSBLATT

Beantworten Sie die Auswahlaufgaben und Richtig/Falsch-Fragen, vervollständigen Sie die Lückensätze mithilfe der Wortliste, ordnen Sie die Definitionen zu und lösen Sie das Kreuzworträtsel und das Suchsel. Wenden Sie Ihr Wissen in folgenden Bereichen an: Auswahl einer sicheren VPN-Infrastruktur. Zum Schluss folgt die Bonusaufgabe Schnell denken.

EINEN VPN AUSWÄHLEN (EINFÜHRUNG)

Bei der Wahl des richtigen VPN muss man über Marketingversprechen hinausblicken. Ein zuverlässiger Anbieter sollte eine nachgewiesene Zero-Logs-Richtlinie, sichere Verschlüsselungsprotokolle und Open-Source-Clients bieten. Indem Sie Sicherheitsfunktionen, Gerichtsbarkeiten und Geschwindigkeit bewerten, können Sie ein VPN wählen, das zu Ihren Anforderungen an den digitalen Schutz passt.

LESEN SIE JEDEN KONTROLLPUNKT SORGFÄLTIG UND WÄHLEN ODER SCHREIBEN SIE DIE RICHTIGE ANTWORT.

Kontrollpunkt 1: Auswahlaufgaben

1. Was ist der entscheidende Faktor bei der Wahl eines sicheren VPN-Anbieters?

- A. Die Anzahl der Länder mit Servern
- B. Eine unabhängig geprüfte No-Logs-Richtlinie
- C. Die günstigste monatliche Preisstufe
- D. Auffällige Werbesponsorings

2. Welches VPN-Protokoll bietet das beste Gleichgewicht aus Geschwindigkeit und Überprüfbarkeit?

- A. PPTP (veraltet)
- B. L2TP/IPSec
- C. Nur OpenVPN über TCP
- D. WireGuard

3. Warum sollten Nutzer für sensible Aktivitäten keine kostenlosen VPNs verwenden?

- A. Sie sind in den Vereinigten Staaten verboten
- B. Sie verkaufen oft Ihren Browserverlauf
- C. Sie unterstützen kein einfaches Surfen im Web
- D. Sie benötigen spezielle Hardware für die Verbindung

4. Was bestimmt der Rechtsraum, in dem ein Anbieter seinen Sitz hat?

- A. Die Geschwindigkeit der Serververbindung
- B. Die Arten unterstützter Geräte
- C. Örtliche Gesetze zur Vorratsdatenspeicherung und zu Durchsuchungsbeschlüssen
- D. Das visuelle Design der Client-Anwendung

5. Was ist der Hauptzweck der „Kill Switch"-Funktion eines VPN-Clients?

- A. Um den Internetzugang zu blockieren, wenn die VPN-Verbindung abbricht
- B. Um alle installierten Anwendungen auf dem Gerät zu löschen
- C. Um die Geschwindigkeit der Serververbindung zu verdoppeln
- D. Um das Betriebssystem im Leerlauf neu zu starten

Kontrollpunkt 2: Richtig oder falsch

6 Frage 6

6. Ein VPN schützt Ihr Gerät vor Malware-Downloads und Virendateien.

○ Richtig ○ Falsch

7 Frage 7

7. Unabhängige Audits von Firmen wie Deloitte bestätigen die Zero-Logs-Angaben.

○ Richtig ○ Falsch

8 Frage 8

8. Die Gesetze im Heimatland eines Anbieters haben keinen Einfluss auf den Schutz der Nutzerdaten.

○ Richtig ○ Falsch

9 Frage 9

9. Die kompakte Codebasis von WireGuard lässt sich leichter prüfen als die von OpenVPN.

○ Richtig ○ Falsch

10 Frage 10

10. Kostenlose VPNs verkaufen oft Werbung oder verfolgen Nutzer, um die Serverkosten zu decken.

○ Richtig ○ Falsch

Kontrollpunkt 3: Schlüsselbegriffe einsetzen

Lesen Sie jeden der folgenden Sätze und füllen Sie die Lücke mit dem richtigen Begriff aus der Wortliste.

1. Eine unabhängig verifizierte Richtlinie nach dem Prinzip _____ verpflichtet einen VPN-Anbieter, Ihren Onlineverlauf nicht aufzuzeichnen.

2. Das moderne Protokoll _____ bietet hohe Geschwindigkeit und nutzt eine sehr kleine Codebasis.

3. Eine Sicherheitsfunktion namens _____ stoppt den gesamten Datenverkehr, wenn die VPN-Verbindung plötzlich abbricht.

4. Wer den rechtlichen _____ eines Anbieters prüft, erkennt, ob dieser Überwachungsabkommen unterliegt.

5. Werden Server als _____ betrieben, hilft das zu verhindern, dass Nutzerdaten einen Neustart überdauern.

6. Um eine Zero-Knowledge-Richtlinie zu verifizieren, ist ein _____ durch renommierte externe Firmen nötig.

WORTSCHATZ-WORTBANK

FIVE EYES | GRATIS-VPN | KILL SWITCH | NO-LOGS | RAM-SERVER | RECHTSRAUM | SICHERHEITSAUDIT | WIREGUARD

Schreiben Sie Ihre Antworten hier:

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

Kontrollpunkt 4: Zuordnung von Netzwerk-Begriffen

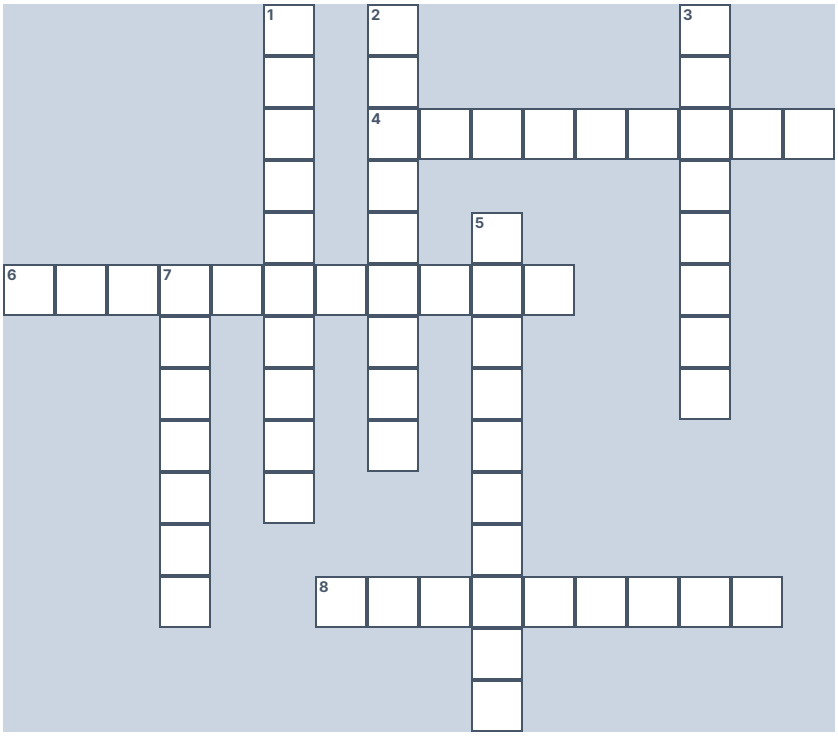
DEFINITIONEN ZUORDNEN

Ordnen Sie jeden Fachbegriff links der richtigen Definition rechts zu, indem Sie den passenden Buchstaben (A–H) in das ausfüllbare Eingabefeld schreiben.

1. WireGuard	A	Verbindungsdienst mit hohem Risiko, der sich oft durch das Protokollieren und Verkaufen von Browserdaten finanziert.
2. Geprüfte Protokolle	B	Sicherheitsmechanismus, der das Routing ins Internet blockiert, wenn der sichere Tunnel getrennt wird.
3. Gerichtsbarkeit	C	Internationale Allianz zum Austausch von Geheimdienstinformationen zwischen USA, UK, CA, AU und NZ.
4. Kill Switch	D	Hardware-Infrastruktur, die mit flüchtigem Arbeitsspeicher läuft, sodass keine Daten auf der Festplatte gespeichert werden.
5. Five Eyes	E	Die geografische Region, deren Recht die rechtlichen Pflichten des VPN-Anbieters bestimmt.
6. Kostenloses VPN	F	Modernes, schnelles Protokoll mit rund 4.000 Zeilen leicht prüfbarem Code.
7. Reine RAM-Server	G	Ausgereiftes, vielfach geprüftes Open-Source-Protokoll mit einer weit größeren Codebasis als WireGuard.
8. OpenVPN	H	Datenschutzversprechen, das von unabhängigen Cybersicherheitsfirmen bestätigt wurde.

Kontrollpunkt 5: Kreuzworträtsel

Lösen Sie das Kreuzworträtsel, indem Sie Buchstaben in die aktiven weißen Felder eingeben. Die Zahlen entsprechen den Hinweisen unten.



WAAGERECHT

4. Hardware-Infrastruktur, die vollständig im flüchtigen Speicher läuft und so keine Daten dauerhaft speichert (9)

6. Datenschutzversprechen, das von unabhängigen Cybersicherheitsfirmen überprüft wurde (11)

8. Riskanter Verbindungsdienst, der oft Geld verdient, indem er Browserdaten protokolliert und verkauft (9)

SENKRECHT

1. Geografische Region, deren Recht die rechtlichen Pflichten des VPN-Anbieters bestimmt (10)

2. Modernes, schnelles Protokoll mit etwa 4.000 Zeilen gut prüfbarem Code (9)

3. Internationale Allianz zum Austausch von Geheimdienstinformationen zwischen US, UK, CA, AU und NZ (8)

5. Sicherheitsmechanismus, der das Internet-Routing blockiert, wenn der sichere Tunnel abbricht (10)

7. Ausgereiftes, vielfach geprüftes Open-Source-Protokoll mit weit größerer Codebasis als WireGuard (7)

Kontrollpunkt 5, Alternative: Barrierefreie Kreuzworträtsel-Hinweise

Nutzer von Screenreadern und Tastatur können die Kreuzworträtsel-Antworten direkt in die Textfelder unten eingeben.

WAAGERECHT

4 waagerecht: Hardware-Infrastruktur, die vollständig im flüchtigen Speicher läuft und so keine Daten dauerhaft speichert (9 Buchstaben):

6 waagerecht: Datenschutzversprechen, das von unabhängigen Cybersicherheitsfirmen überprüft wurde (11 Buchstaben):

8 waagerecht: Riskanter Verbindungsdienst, der oft Geld verdient, indem er Browserdaten protokolliert und verkauft (9 Buchstaben):

SENKRECHT

1 senkrecht: Geografische Region, deren Recht die rechtlichen Pflichten des VPN-Anbieters bestimmt (10 Buchstaben):

2 senkrecht: Modernes, schnelles Protokoll mit etwa 4.000 Zeilen gut prüfbarem Code (9 Buchstaben):

3 senkrecht: Internationale Allianz zum Austausch von Geheimdienstinformationen zwischen US, UK, CA, AU und NZ (8 Buchstaben):

5 senkrecht: Sicherheitsmechanismus, der das Internet-Routing blockiert, wenn der sichere Tunnel abbricht (10 Buchstaben):

7 senkrecht: Ausgereiftes, vielfach geprüftes Open-Source-Protokoll mit weit größerer Codebasis als WireGuard (7 Buchstaben):

Kontrollpunkt 6: Suchsel

Finden Sie die 8 wichtigen Fachbegriffe, die im Gitter unten versteckt sind. Die Wörter können waagerecht, senkrecht oder diagonal verlaufen.

U S T E L J B G A B C P X L K
Y K X T K D Q R M J R D I N N
M N K Q P G M A M Q A R S T T
U P G C S Q O T H S M B W D S
A V Z V C N Z I W F S K H K Z
R N D N D O Q S X P E C U I B
S E A Z N L D V W K R A D L O
T P D F H O I P I F V D R L Q
H O M E I G R N R I E Z S S F
C Q V F A S A Q E V R O N W P
E T X Q K A R U G E S D N I Y
R B F S X U W J U E A R Z T Y
Y L G I M D R J A Y M L T C O
H Q Q H Z I A O R E V G U H B
Y R Y B H T L Z D S G J O P N

WORTSCHATZ-WORTLISTE

WIREGUARD NOLOGSAUDIT RECHTSRAUM KILLSWITCH FIVEEYES
GRATISVPN RAMSERVER OPENVPN

Kontrollpunkt 6, Alternative: Barrierefreie Begriffszuordnung

Ordnen Sie jeden der 8 Fachbegriffe aus dem Suchrätsel der richtigen Definition zu, indem Sie den Buchstaben (A–H) in die Lücke schreiben.

FACHBEGRIFFE

- **A. WIREGUARD**
- **B. NOLOGSAUDIT**
- **C. RECHTSRAUM**
- **D. KILLSWITCH**
- **E. FIVEEYES**
- **F. GRATISVPN**
- **G. RAMSERVER**
- **H. OPENVPN**

DEFINITIONEN UND ZUORDNUNGSFELDER

1. Internationale Allianz zum Austausch von Geheimdienstinformationen zwischen US, UK, CA, AU und NZ.
2. Modernes, schnelles Protokoll mit etwa 4.000 Zeilen gut prüfbarem Code.
3. Ausgereiftes, vielfach geprüftes Open-Source-Protokoll mit weit größerer Codebasis als WireGuard.
4. Riskanter Verbindungsdienst, der oft Geld verdient, indem er Browserdaten protokolliert und verkauft.
5. Sicherheitsmechanismus, der das Internet-Routing blockiert, wenn der sichere Tunnel abbricht.
6. Hardware-Infrastruktur, die vollständig im flüchtigen Speicher läuft und so keine Daten dauerhaft speichert.
7. Geografische Region, deren Recht die rechtlichen Pflichten des VPN-Anbieters bestimmt.
8. Datenschutzversprechen, das von unabhängigen Cybersicherheitsfirmen überprüft wurde.

Kontrollpunkt 7: Buchstabensalat

Bringen Sie die Buchstaben unten in die richtige Reihenfolge, um zentrale VPN-Begriffe aufzudecken. Schreiben Sie Ihre Antworten in die ausfüllbaren Eingabefelder.

1. UGEIWARDR
2. UHRETMRASC
3. EIFEYSEV
4. ERESVRRAM
5. DOUALTGSNIO
6. CSLITKIWHL
7. SGPNVTRIA
8. PNNOPVE

Bonusaufgabe: Schnell denken

3 ANTWORTEN PRO KATEGORIE. WER DIE LISTE ZUERST VOLLSTÄNDIG AUSFÜLLT, GEWINNT.

1	Dinge, die ein VPN verbergen kann			
2	Dinge, die wichtiger sind als der Preis			
3	Orte, an denen Sie VPN-Testberichte lesen können			
4	Dinge, vor denen ein VPN Sie nicht schützen kann			
5	Fragen an das Vertriebsteam eines VPN			
6	Dinge, die Ihr Internetanbieter sehen kann			
7	Punkte auf Ihrer Checkliste bei der Wahl eines VPN			
8	Orte, an denen Sie ein VPN nutzen würden			
9	Warnzeichen bei einem VPN-Anbieter			
10	Wörter rund um Privatsphäre			
11	Dinge, die Sie zuerst testen würden			
12	Versprechen, die ein guter VPN-Anbieter gibt			
13	Gründe, auf Reisen ein VPN zu nutzen			
14	Geräte, die ein VPN nutzen können			
15	Mythen über VPNs			

Kontrollpunkt 8: Fallstudien zu VPNs

Wenden Sie die erlernten Konzepte an, um die folgenden praxisnahen Szenarien zu lösen.

SARAH (STUDENTIN IM CAFÉ)

👩‍💻 „Hallo! Ich sitze bei Coffee & Bytes. Es gibt ein ungesichertes öffentliches Netzwerk namens 'Free_Wi-Fi_No_Password'. Ich möchte mich in meinem Schul-E-Mail-Konto anmelden und meine Hausaufgabe hochladen, mache mir aber Sorgen wegen Hackern. Welche Risiken hat die Nutzung dieses Netzwerks ohne VPN, und wie schützt ein VPN meine Daten?“

ALEX (REISENDER STUDENT)

👩‍💻 „Oh nein! Ich bin für ein Projekt im Ausland unterwegs und versuche, eine Biologie-Dokumentation anzusehen, die auf einem Server in meinem Heimatland gehostet wird. Aber auf der Website steht 'Dieses Video ist an Ihrem aktuellen Standort nicht verfügbar.' Warum werde ich blockiert, und wie kann mir ein VPN helfen, sie anzusehen?“

Kontrollpunkt 9: Entschlüsselung der Chiffre

Um Ihr Training zum Auswahlleitfaden abzuschließen, entschlüsseln Sie diese versteckte Nachricht über die Wahl einer sicheren Infrastruktur.

SCHLÜSSEL FÜR DIE BUCHSTABEN-ZAHLEN-VERSCHLÜSSELUNG

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

22 5 18 7 12 5 9 3 8 5 14 19 9 5

2 5 18 9 3 8 20 5 13 9 20 19 9 3 8 5 18 5 13

19 25 19 20 5 13

Entschlüsselte Nachricht:

TIPP: JEDE ZAHL STEHT FÜR DIE POSITION DIESES BUCHSTABENS IM ALPHABET (Z. B. 1 = A, 2 = B, 26 = Z).

Kontrollpunkt 10: Grundlegende häufige Fragen zu VPN (Teil A)

Sehen Sie sich die häufigsten Fragen und Antworten an, die Interessenten zur Nutzung virtueller privater Netzwerke haben.

Q1: Was ist ein VPN und wie funktioniert es?

Ein Virtual Private Network (VPN) verschlüsselt Ihre Internetverbindung und leitet Ihren Datenverkehr über einen sicheren entfernten Server. Dadurch wird Ihre öffentliche IP-Adresse verschleiert, und es wird eingeschränkt, was Beobachter im lokalen Netzwerk und Ihr ISP über den durch den VPN-Tunnel geleiteten Datenverkehr sehen können.

Q2: Warum sollte ich ein VPN verwenden?

Ein VPN schützt Ihre digitale Privatsphäre, sichert Ihre Verbindung in öffentlichen WLANs (etwa in Cafés oder an Flughäfen), kann eine aktivitätsbasierte Drosselung verringern, wenn der ISP die Art des verschlüsselten Datenverkehrs nicht erkennen kann, umgeht Geoblocking für den Zugriff auf Inhalte weltweit und hilft beim Schutz von Ressourcen für die Remote-Arbeit.

Q3: Macht mich ein VPN online vollständig anonym?

Nein. Ein VPN verbirgt zwar Ihre IP-Adresse und verschlüsselt den Datenverkehr, Sie können aber weiterhin über Browser-Cookies, angemeldete Konten (wie Google oder Facebook) und Browser-Fingerprinting verfolgt werden oder wenn Ihr VPN-Anbieter Ihre Daten protokolliert.

Q4: Verlangsamt ein VPN meine Internetgeschwindigkeit?

Ja, leicht. Der Verschlüsselungsvorgang und die räumliche Entfernung zum VPN-Server erhöhen Latenz und Overhead. Die Auswirkung hängt von Anbieter, Protokoll, Serverentfernung, Gerät und Netzwerkbedingungen ab.

Q5: Wie verdient es Geld?

Prüfen Sie das Geschäftsmodell. Abonnements, Freemium-Stufen und Datenverkäufe beeinflussen alle, wie sehr Sie einem VPN vertrauen können, und ein Dienst, der Ihre Daten nie erhebt, kann sie auch nicht verkaufen. Lesen Sie zuerst die Datenschutzerklärung. [1]

Kontrollpunkt 10: Grundlegende häufige Fragen zu VPN (Teil B)

Sehen Sie sich die häufigsten Fragen und Antworten an, die Interessenten zur Nutzung virtueller privater Netzwerke haben.

Q6: Kann ich ein kostenloses VPN verwenden?

Kostenlose VPNs können auf Werbung, eingeschränkte Funktionen, Nutzungsanalysen, Datenlimits oder andere Erlösmodelle setzen. Nutzer sollten vor der Nutzung die Datenschutzrichtlinie, die Eigentümerstruktur, die Audits und das Geschäftsmodell des Anbieters prüfen.

Q7: Was ist eine „No-Logs“-Richtlinie?

Eine No-Logs-Richtlinie beschreibt, welche Aktivitäts- und Verbindungsdaten ein Anbieter nach eigener Aussage nicht speichert. Der genaue Umfang ist unterschiedlich, daher sollten Leser die Richtlinie und die Ergebnisse unabhängiger Audits prüfen.

Q8: Wie wähle ich das beste VPN aus?

Achten Sie auf geprüfte No-Logs-Richtlinien, starke Protokolle (WireGuard, OpenVPN), sichere Serverstandorte, hohe Geschwindigkeiten, reine RAM-Server, eine Kill-Switch-Funktion und eine Rechtsordnung außerhalb von Geheimdienstallianzen (wie den 5/9/14 Eyes).

Q9: Kann ich ein VPN auf meinem Smartphone und meinem Smart-TV verwenden?

Ja. Moderne VPN-Anbieter bieten eigene Apps für iOS, Android, macOS, Windows, Linux und Smart-TVs sowie Router-Konfigurationen an, um alle Geräte in Ihrem Heimnetzwerk zu schützen.

Q10: Was ist ein Kill Switch?

Ein Kill Switch ist eine Sicherheitsfunktion, die Ihr Gerät automatisch vom Internet trennt, wenn die VPN-Verbindung abbricht. So wird verhindert, dass Ihre unverschlüsselten Daten oder Ihre echte IP-Adresse offengelegt werden.

Kontrollpunkt 10: Fortgeschrittene häufige Fragen zu VPN (Teil C)

Erkunden Sie technische und strukturelle Aspekte virtueller privater Netzwerke und sicherer Tunnelprotokolle.

Q1: Was ist der Unterschied zwischen WireGuard, OpenVPN und IKEv2?

WireGuard ist ein modernes, schlankes Protokoll (nur ca. 4.000 Codezeilen), das hohe Geschwindigkeiten und kurze Verbindungszeiten bietet. OpenVPN ist ein sehr sicheres, praxiserprobtes Open-Source-Protokoll. IKEv2 eignet sich hervorragend für Mobilgeräte, da es sich beim Netzwerkwechsel schnell wieder verbindet.

Q2: Was ist Double VPN bzw. Multi-Hop-Routing?

Multi-Hop leitet Ihren Datenverkehr nacheinander über zwei oder mehr VPN-Server. Das fügt eine zweite Verschlüsselungsebene hinzu und hilft, Ihre echte IP-Adresse vor dem zweiten Hop verborgen zu halten, falls ein Server kompromittiert wird.

Q3: Was sind WebRTC-Lecks und wie verhindert ein VPN sie?

WebRTC ist ein Browserprotokoll, das Ihre echte lokale und öffentliche IP-Adresse preisgeben kann, selbst wenn ein VPN aktiv ist. Premium-VPNs blockieren oder fälschen WebRTC-Anfragen in ihren Desktop- und Mobil-Apps sowie Browsererweiterungen.

Q4: Was sind reine RAM-Server und warum sind sie wichtig?

Herkömmliche Server schreiben Daten auf Festplatten, die beschlagnahmt oder kompromittiert werden können. Reine RAM-Server (ohne Festplatte) laufen vollständig im flüchtigen Arbeitsspeicher (RAM). Wird der Server neu gestartet oder ausgeschaltet, werden die im Speicher gehaltenen Daten gelöscht.

Q5: Wie umgeht Verschleierung (Obfuscation) VPN-Sperren?

Verschleierung (oder „Stealth VPN“) tarnt VPN-Datenpakete so, dass sie wie gewöhnlicher HTTPS-Webverkehr (Port 443) aussehen. Das hilft, die Deep Packet Inspection (DPI) zu umgehen, mit der Regierungen oder Schul- und Firmennetzwerke VPNs blockieren.

Kontrollpunkt 10: Fortgeschrittene häufige Fragen zu VPN (Teil D)

Erkunden Sie technische und strukturelle Aspekte virtueller privater Netzwerke und sicherer Tunnelprotokolle.

Q6: Was ist Split-Tunneling und wann sollte ich es verwenden?

Mit Split Tunneling legen Sie fest, welche Apps durch den verschlüsselten VPN-Tunnel geleitet werden und welche sich direkt mit dem Internet verbinden. Nutzen Sie es, um sensible Banking-Apps durch das VPN zu leiten, während lokale Spiele sich direkt verbinden und so die zusätzliche Latenz durch das VPN vermeiden.

Q7: Wie funktioniert Forward Secrecy (Perfect Forward Secrecy)?

PFS stellt sicher, dass für jede einzelne Sitzung ein eigener, temporärer Schlüssel erzeugt wird. Selbst wenn ein privater Schlüssel künftig kompromittiert wird, kann er nicht zur Entschlüsselung vergangener oder zukünftiger Sitzungen genutzt werden, da diese unabhängige Schlüssel verwendeten.

Q8: Was sind die 5/9/14-Eyes-Allianzen und warum sollten sie mich interessieren?

Die Gerichtsbarkeit kann beeinflussen, welchen rechtlichen Verfahren ein Anbieter ausgesetzt sein kann, das praktische Datenschutzrisiko hängt aber auch davon ab, welche Daten der Anbieter speichert, von seiner technischen Architektur, den Eigentumsverhältnissen, den Transparenzberichten und der Audit-Historie.

Q9: Was ist der Schutz vor DNS-Lecks?

Der DNS-Leak-Schutz sorgt dafür, dass Ihr Gerät Suchanfragen nach Websites (DNS-Anfragen) über die privaten, verschlüsselten DNS-Server des VPN statt über die Server Ihres Internetanbieters sendet. So wird verhindert, dass Ihr Internetanbieter nachverfolgt, welche Websites Sie besuchen.

Q10: Warum sollte man prüfen, wer ein VPN betreibt und empfiehlt?

Der Ruf zählt. Informieren Sie sich über Eigentümer und Führung des Unternehmens, suchen Sie nach öffentlichen Audits durch Dritte und prüfen Sie, was unabhängige Sicherheitsfachleute und die Presse sagen, bevor Sie ihm vertrauen. [1]

Teil 11: 10 interessante VPN-Fakten und Einblicke aus der Praxis

Lernen Sie diese besonders wertvollen, realen Fakten und Erkenntnisse zur Geschichte, zum Markt und zur Technologie von VPNs kennen.

1. ERSTES VPN-PROTOKOLL

PPTP (Point-to-Point Tunneling Protocol), ein frühes VPN-Protokoll einer von Microsoft geführten Gruppe aus den 1990er-Jahren, gilt heute als unsicher, daher nutzen moderne VPNs WireGuard oder OpenVPN. [1]

2. MARKTBEWERTUNG

Der weltweite VPN-Markt ist rasant gewachsen, angetrieben durch steigende Anforderungen an Remote-Arbeit und die Sicherheitsbedürfnisse von Unternehmen.

3. WIREGUARD-REVOLUTION

WireGuard hat eine stark verschlankte, auf Effizienz ausgelegte Codebasis, die sich leichter auf Sicherheitslücken prüfen lässt als herkömmliche Protokolle. [3]

4. STRENGE PRÜFSTANDARDS

Führende VPN-Anbieter beauftragen Firmen wie Deloitte, KPMG oder PwC mit der Überprüfung ihrer No-Logs-Versprechen und Sicherheitsfirmen wie Cure53 mit dem Testen ihrer Apps und Server. [4]

5. URSPRÜNGE DER 5-EYES-ALLIANZ

Die Geheimdienstpartnerschaft Five Eyes aus den USA, Großbritannien, Kanada, Australien und Neuseeland ging aus der Zusammenarbeit der Alliierten bei der Fernmeldeaufklärung im Zweiten Weltkrieg hervor.

6. DEEP PACKET INSPECTION

Fortschrittliche Firewalls setzen Deep Packet Inspection (DPI) ein, um Metadaten von Netzwerkpaketen zu analysieren und typische Merkmale von VPN-Verbindungen zu blockieren.

7. NUTZUNG IN UNTERNEHMEN

Viele Organisationen stellen Mitarbeitenden im Homeoffice ein VPN bereit, um auf interne Systeme wie Datenbanken zuzugreifen, weshalb VPNs ein gängiges Sicherheitswerkzeug am Arbeitsplatz sind.

8. DEZENTRALE VPNS

Dezentrale VPNs (dVPNs) verteilen den Datenverkehr über ein Netzwerk von Knoten, die von Teilnehmern betrieben werden, und verringern so die Abhängigkeit von einem einzigen zentralen Anbieter.

9. ANONYMITÄT: TOR VS. VPN

Ein VPN leitet den Datenverkehr durch einen einzigen Anbieter, während Tor (The Onion Router) ihn über drei freiwillig betriebene Relays (Guard, Middle, Exit) schickt, um die Privatsphäre zu maximieren. [5]

10. KOSTEN VON DATENPANNEN

Die Kombination eines VPN mit einem Zero-Trust-Zugriffsmodell, das jeden Benutzer und jedes Gerät prüft, hilft Organisationen, Daten zu schützen und den Schaden von Datenpannen zu begrenzen.

Technische Referenzen und Quellen

Zitierte Veröffentlichungen, kryptografische Spezifikationen und offizielle Dokumentstandards, die in diesem Arbeitsblatt verwendet werden.

WISSENSCHAFTLICHE UND FACHLICHE QUELLEN

[1] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.

https://ssd.eff.org/module/choosing-vpn-thats-right-you

[2] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.

https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

[3] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.

https://www.wireguard.com/

[4] Yahoo Finance. (2026). NordVPN passes its no-logs assurance assessment for the sixth time.

https://finance.yahoo.com/news/nordvpn-passes-no-logs-assurance-140000101.html

[5] Tor Project. (n.d.). Overview.

https://support.torproject.org/about-tor/how-tor-works/overview/

Lösungsschlüssel: Bewertung von VPN-Anbietern, Sicherheitsstandards, Audits und Protokollierungsrichtlinien

1 **Geprüfte Protokollierungsrichtlinie** PROTOKOLLE — **Richtige Antwort: B**

HINWEIS FÜR LEHRKRÄFTE

Eine unabhängig geprüfte No-Logs-Richtlinie ist der praktikabelste Weg, die Zero-Knowledge-Datenschutzversprechen eines Anbieters zu überprüfen. Auffälliges Marketing oder Eigenangaben reichen nicht aus. Quelle: Deloitte Advisory, Cure53 Audit.

2 **Überlegenheit von WireGuard** LATENZ — **Richtige Antwort: D**

HINWEIS FÜR LEHRKRÄFTE

WireGuard bietet modernes, schnelles Verbindungsrouting im Kernel-Space mit einer kompakten Codebasis (ca. 4.000 Zeilen), was Audits sehr effizient macht. Quelle: IETF Protocol RFC, WireGuard Project.

3 **Frage 3** — **Richtige Antwort: B**

HINWEIS FÜR LEHRKRÄFTE

Auch kostenlose VPNs müssen Server bezahlen, und die FTC warnt, dass einige VPN-Apps Nutzerdaten an Dritte weitergeben, etwa um Werbung auszuspielen.

4 **Rechtsordnungen** ROUTING-STEUERUNG — **Richtige Antwort: C**

HINWEIS FÜR LEHRKRÄFTE

Die Gerichtsbarkeit bestimmt, ob das VPN Überwachungsgesetzen, lokalen Pflichten zur Vorratsdatenspeicherung und geheimen behördlichen Anordnungen unterliegt. Quelle: Privacy Rights Clearinghouse.

5 **Schutz durch Kill Switch** PRIVATSPHÄRE — **Richtige Antwort: A**

HINWEIS FÜR LEHRKRÄFTE

Der Kill Switch trennt sofort das Routing des Systemnetzwerkadapters, wenn der Tunnel abbricht, und verhindert so, dass die echte IP und DNS-Daten offengelegt werden. Quelle: IETF Tunnel RFC.

Lösungsschlüssel: Kontrollpunkt 2 – Richtig oder Falsch

6 **Grenzen beim Malware-Schutz** IP-VERSCHLEIERUNG — **Richtige Antwort: Falsch**

HINWEIS FÜR LEHRKRÄFTE

Ein VPN bietet einen sicheren, verschlüsselten Kanal, scannt aber weder Nutzdaten noch Dateien. Zum Blockieren von Malware ist Antivirensoftware erforderlich. Quelle: Deloitte Advisory.

7 **Unabhängige Audits** GESCHWINDIGKEITEN — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

Auditberichte bestätigen Serversoftwarekonfigurationen, die Einhaltung des reinen RAM-Betriebs und das Fehlen von Protokolldatenbanken. Quelle: Deloitte Advisory, Cure53 Audit.

8 **Frage 8** — **Richtige Antwort: Falsch**

HINWEIS FÜR LEHRKRÄFTE

Anbieter müssen die Gesetze ihres Heimatlandes befolgen, wozu Vorschriften zur Vorratsdatenspeicherung und Anordnungen zur Herausgabe gespeicherter Daten gehören können.

9 **Größe der Protokoll-Codebasis** FIREWALLS — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

Eine kleinere Codebasis verringert die potenzielle Angriffsfläche und erleichtert es Sicherheitsteams, die Integrität des Protokolls zu überprüfen. Quelle: WireGuard Project.

10 **Monetarisierung durch Werbung** NO-LOGS — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

Ohne Abonnementgebühren finanzieren sich kostenlose VPNs über Data Mining, Erstellung von Datenverkehrsprofilen und das Einblenden von Werbung in den Browser. Quelle: EDRi Retention Guidelines.

Vokabelschlüssel und Bewertungsraster

Bewertungsraster für Lehrkräfte: Vergeben Sie 1 Punkt für jede richtige Zuordnung (insgesamt 8 Punkte) und jeden Kontextbegriff (insgesamt 6 Punkte).

KONTROLLPUNKT 4: LÖSUNG BEGRIFFSZUORDNUNG

F 1. WireGuard	H 2. Geprüfte Protokolle	E 3. Gerichtsbarkeit	B 4. Kill Switch
C 5. Five Eyes	A 6. Kostenloses VPN	D 7. Reine RAM-Server	G 8. OpenVPN

KONTROLLPUNKT 3: LÖSUNG SCHLÜSSELBEGRIFFE

1 NO-LOGS	2 WIREGUARD	3 KILL SWITCH	4 RECHTSRAUM
5 RAM-SERVER	6 SICHERHEITSAUDIT		

KONTROLLPUNKT 6, ALTERNATIVE: LÖSUNG WORTZUORDNUNG

1 E – FIVEEYES	2 A – WIREGUARD	3 H – OPENVPN	4 F – GRATISVPN
5 D – KILLSWITCH	6 G – RAMSERVER	7 C – RECHTSRAUM	8 B – NOLOGSAUDIT

DISKUSSIONSHINWEISE FÜR LEHRKRÄFTE

Schlüsselbegriffe:
Prüfen Sie, ob die Lernenden WireGuard, Geprüfte Protokolle und Gerichtsbarkeit in eigenen Worten erklären und jeweils ein Beispiel nennen können.

Fallstudien:
Bitten Sie die Lernenden, ihre Empfehlungen mit Fakten aus dem Arbeitsblatt statt mit Vermutungen zu begründen.

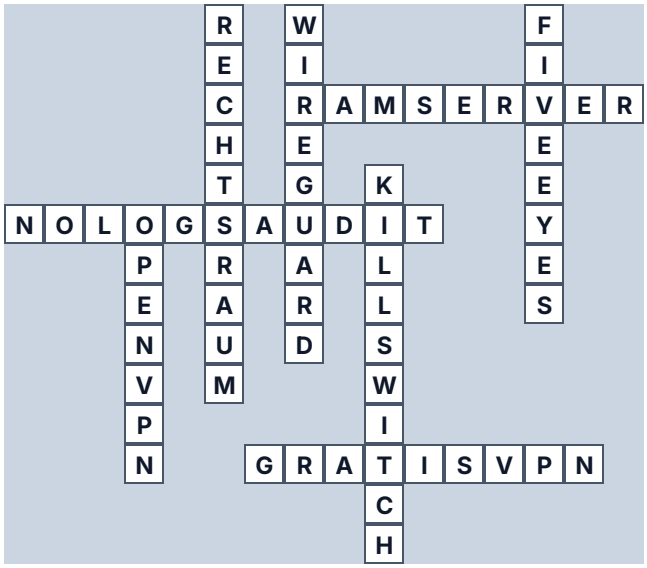
Quellenbewertung:
Lassen Sie die Lernenden mindestens eine Aussage anhand der Quellen des Arbeitsblatts prüfen und besprechen Sie, warum sich Zahlen, Preise und Regeln mit der Zeit ändern können.

Rätsellösungen und Hinweise für Lehrkräfte

LÖSUNG DES SUCHSELS

U	S	T	E	L	J	B	G	A	B	C	P	X	L	K
Y	K	X	T	K	D	Q	R	M	J	R	D	I	N	N
M	N	K	Q	P	G	M	A	M	Q	A	R	S	T	T
U	P	G	C	S	Q	O	T	H	S	M	B	W	D	S
A	V	Z	V	C	N	Z	I	W	F	S	K	H	K	Z
R	N	D	N	D	O	Q	S	X	P	E	C	U	I	B
S	E	A	Z	N	L	D	V	W	K	R	A	D	L	O
T	P	D	F	H	O	I	P	I	F	V	D	R	L	Q
H	O	M	E	I	G	R	N	R	I	E	Z	S	S	F
C	Q	V	F	A	S	A	Q	E	V	R	O	N	W	P
E	T	X	Q	K	A	R	U	G	E	S	D	N	I	Y
R	B	F	S	X	U	W	J	U	E	A	R	Z	T	Y
Y	L	G	I	M	D	R	J	A	Y	M	L	T	C	O
H	Q	Q	H	Z	I	A	O	R	E	V	G	U	H	B
Y	R	Y	B	H	T	L	Z	D	S	G	J	O	P	N

KREUZWORTRÄTSEL-LÖSUNG



LEITFADEN FÜR LEHRKRÄFTE ZU DEN KREUZWORTRÄTSEL-LÖSUNGEN

WAAGERECHT

4 waagerecht: RAMSERVER Hardware-Infrastruktur, die vollständig im flüchtigen Speicher läuft und so keine Daten dauerhaft speichert (9 Buchstaben)

6 waagerecht: NOLOGSAUDIT Datenschutzversprechen, das von unabhängigen Cybersicherheitsfirmen überprüft wurde (11 Buchstaben)

8 waagerecht: GRATISVPN Riskanter Verbindungsdienst, der oft Geld verdient, indem er Browserdaten protokolliert und verkauft (9 Buchstaben)

SENKRECHT

1 senkrecht: RECHTSRAUM Geografische Region, deren Recht die rechtlichen Pflichten des VPN-Anbieters bestimmt (10 Buchstaben)

2 senkrecht: WIREGUARD Modernes, schnelles Protokoll mit etwa 4.000 Zeilen gut prüfbarem Code (9 Buchstaben)

3 senkrecht: FIVEEYES Internationale Allianz zum Austausch von Geheimdienstinformationen zwischen US, UK, CA, AU und NZ (8 Buchstaben)

5 senkrecht: KILLSWITCH Sicherheitsmechanismus, der das Internet-Routing blockiert, wenn der sichere Tunnel abbricht (10 Buchstaben)

7 senkrecht: OPENVPN Ausgereiftes, vielfach geprüftes Open-Source-Protokoll mit weit größerer Codebasis als WireGuard (7 Buchstaben)

Lösungsschlüssel für Buchstabensalat und Chiffre

Lösungsschlüssel für die Wort-Entwirr-Aufgabe und die Geheime Chiffre-Aufgabe.

LÖSUNGSSCHLÜSSEL BUCHSTABENSALAT

1. UGEIWARDR — **WIREGUARD**
2. UHRETMRASC — **RECHTSRAUM**
3. EIFEYSEV — **FIVEEYES**
4. ERESVRRAM — **RAMSERVER**
5. DOUALTGSNIO — **NOLOGSAUDIT**
6. CSLITKIWHL — **KILLSWITCH**
7. SGPNVTRIA — **GRATISVPN**
8. PNNOPVE — **OPENVPN**

LÖSUNGSSCHLÜSSEL ZUR GEHEIMEN CHIFFRE-AUFGABE

"VERGLEICHEN SIE BERICHTE MIT SICHEREM SYSTEM"

Lösungsschlüssel zu den Fallstudien

A Szenario A: Sicherheit in öffentlichen Netzwerken

SNIFFING UND VERSCHLÜSSELUNG | Sarahs Dilemma

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Risiken: Packet Sniffing, Abfangen von Daten und Man-in-the-Middle-Angriffe. Jemand im selben Café-Netzwerk könnte ihre Anmeldedaten oder ihre Hausaufgabendatei abfangen.
- VPN-Schutz: Verschlüsselt die Nutzdaten der Netzwerkpakete, sodass abgefangener Tunnelverkehr für passive Lauscher im lokalen Netzwerk unlesbar ist, wenn das VPN korrekt konfiguriert ist.

B Szenario B: Zugriff auf gesperrte Ressourcen

GEOBLOCKING UND IPS | Alex' Dilemma

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Warum blockiert: Der Streaming-Anbieter nutzt Geoblocking, das die lokale IP-Adresse des Reisenden seinem tatsächlichen Aufenthaltsland zuordnet und sie aufgrund territorialer Lizenzen sperrt.
- So hilft ein VPN: Es verschleiert seinen tatsächlichen Standort, indem es den Datenverkehr über einen Server in seinem Heimatland leitet. Die Website sieht die IP aus dem Heimatland und gewährt den Zugriff.