Name: _____ Datum: _____ Punkte: _____

Was ist ein VPN? Arbeitsblatt

Praktische Übungen zu Netzwerkprotokollen, Tunneling und Sicherheitsmaßnahmen.

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

- Erklären Sie das Konzept von Daten-Tunneling und Kapselung.
- Standard-Protokollkonfigurationen und Verschlüsselungsmethoden bestimmen.
- Analysieren Sie die Rolle von Servern und IP-Verschleierung in virtuellen privaten Netzwerken.
- Verstehen, wie ISPs das Surfen verfolgen und wie ein VPN das verhindert.
- Unterscheiden Sie die betrieblichen Grenzen virtueller Netzwerktopologien.

ANLEITUNG: LEITFADEN „WAS IST EIN VPN?“

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: Praxisnahe Szenarien im Fallstudienteil. Zum Schluss folgt die Bonusaufgabe Schnell denken.

WAS IST EIN VPN? (EINFÜHRUNG)

Ein Virtual Private Network ist mehr als nur ein Schalter für die Privatsphäre. Es ist ein verschlüsselter Tunnel, der Ihren Internetverkehr über einen entfernten Server leitet. Dadurch wird Ihre IP-Adresse verborgen, Ihr ISP kann keine Protokolle über Ihre Online-Aktivitäten anlegen, und Ihre Daten sind in öffentlichen Netzwerken geschützt. Die Fachbegriffe zu verstehen ist wichtig, um digital sicher zu bleiben.

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

Kontrollpunkt 1: Auswahlaufgaben

1 **1. Was ist die Hauptfunktion eines Virtual Private Network (VPN)?**

- A. Um die Darstellungsgeschwindigkeit des Webbrowsers zu erhöhen
- B. Um Datenpakete zu verschlüsseln und Ihre öffentliche IP zu verbergen
- C. Um Website-Cookie-Datenbanken lokal zu speichern
- D. Um Ihre physische Computerhardware zu ersetzen

2 **2. Was bedeutet Netzwerk-Tunneling im Zusammenhang mit einem VPN?**

- A. Löschen doppelter Netzwerkprotokolldateien
- B. Installieren lokaler Datenbankspeicherdateien
- C. Teilen von Dateien mit anderen lokalen Computern
- D. Kapseln eines Netzwerkpakets in einem anderen, sicheren Paket

3 **3. Welcher Verschlüsselungsstandard wird häufig zum Schutz von VPN-Datenverkehr verwendet?**

- A. Veraltete DES-Verschlüsselung
- B. Moderner AES-256-Standard
- C. Base64-Kodierung im Klartext
- D. Standard-ROT13-Verschlüsselung

4 **4. Welcher Teil Ihres Netzwerkverkehrs wird von einem VPN verschlüsselt?**

- A. Nur Druckaufträge lokaler Geräte im Netzwerk
- B. Der physische Verlegeweg des Ethernetkabels
- C. Der gesamte Nutzdatenteil des Netzwerkpakets
- D. Nur Ihre Suchverläufe im Webbrowser

5 **5. Was bedeutet der Begriff „Verschlüsselung“ im Netzwerkbereich?**

- A. Umwandeln von Klartextdaten in unlesbaren Chiffretext
- B. Löschen alter Kommunikationsaufzeichnungen
- C. Erhöhung Ihrer lokalen Bandbreitenlimits
- D. Öffentliches Teilen von Datenbank-Zugriffsschlüsseln

Kontrollpunkt 2: Richtig oder falsch

6 Frage 6

6. Ein VPN verschlüsselt Ihren Datenverkehr, um lokales Abhören in öffentlichen WLANs zu verhindern.

○ Richtig ○ Falsch

7 Frage 7

7. Ein VPN verändert physisch die Hardwarekonfiguration Ihres Routers.

○ Richtig ○ Falsch

8 Frage 8

8. Tunnelprotokolle verpacken Datenpakete in eine verschlüsselte Transportschicht.

○ Richtig ○ Falsch

9 Frage 9

9. Symmetrische Verschlüsselung verwendet denselben Schlüssel zum Ver- und Entschlüsseln des Datenverkehrs.

○ Richtig ○ Falsch

10 Frage 10

10. Durch ein VPN wird Ihre Internetverbindung physisch immun gegen jeden Stromausfall.

○ 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. Um Ihren Datenverkehr zu sichern, verpackt das VPN Ihre Datenpakete in ein anderes Protokoll; diesen Vorgang nennt man _____ .

2. Wenn die Download-Geschwindigkeit beim Streaming niedrig ist, kann das an einer begrenzten _____ des Netzwerks liegen.

3. Ein Streamingdienst, der nur in einem bestimmten Land verfügbar ist, nutzt _____ , um Nutzer weltweit einzuschränken.

4. Die Verbindungsregeln, die Verschlüsselung und Verbindungsparameter festlegen, nennt man das _____ des VPN.

5. Ihr Computer nutzt eine lokale _____ , um den Netzwerkverkehr zu überwachen und unsichere Verbindungen zu blockieren.

6. Wenn Sie sich mit einem VPN verbinden, werden Ihre Daten über einen entfernten _____ geleitet, um Ihre öffentliche IP-Adresse zu verbergen.

WORTSCHATZ-WORTBANK

BANDBREITE FIREWALL GEOBLOCKING PRIVATSPHÄRE PROTOKOLL PROVIDER SERVER TUNNELING

Schreiben Sie Ihre Antworten hier:

1. **2.**

3. **4.**

5. **6.**

Kontrollpunkt 4: Zuordnung von Netzwerk-Begriffen

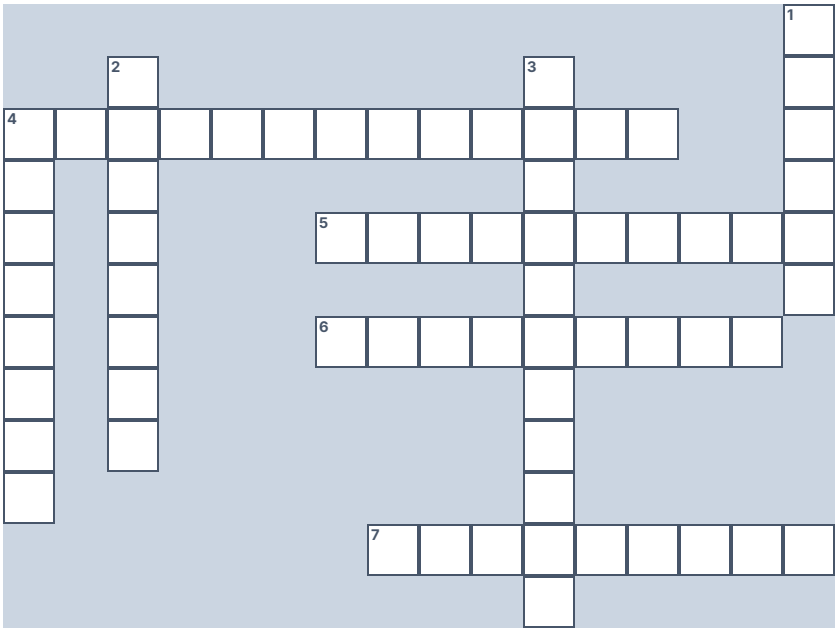
DEFINITIONEN ZUORDNEN

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

☐	**1. Tunneling**	**A**	Ein entfernter Computer, der Ihren Datenverkehr weiterleitet und Ihre IP-Adresse verschleiert.
☐	**2. Protokoll**	**B**	Internetdienstanbieter, der Ihren Datenverkehr transportiert und unverschlüsselte Aktivitäten sehen kann.
☐	**3. Bandbreite**	**C**	Eine Einschränkung, die den Webzugriff abhängig vom physischen Standort verhindert.
☐	**4. Server**	**D**	Ein Sicherheitssystem, das unbefugten Datenverkehr überwacht und blockiert.
☐	**5. Geosperre**	**E**	Ein Regelwerk, das festlegt, wie Daten über das Netzwerk übertragen werden.
☐	**6. Firewall**	**F**	Der Zustand, frei von Tracking oder öffentlicher Überwachung zu sein.
☐	**7. Privatsphäre**	**G**	Die maximale Datenübertragungsrate einer Verbindung.
☐	**8. ISP**	**H**	Verpacken von Datenpaketen in ein anderes Paket für eine sichere Übertragung.

Kontrollpunkt 5: Kreuzworträtsel

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



WAAGERECHT

4. Zustand, frei von Tracking und öffentlicher Überwachung zu sein (13)

5. Maximale Datenübertragungsrate einer Verbindung (10)

6. Regelwerk, das festlegt, wie Daten über das Netzwerk übertragen werden (9)

7. Verpacken von Datenpaketen in ein anderes Paket für die sichere Übertragung (9)

SENKRECHT

1. Entfernter Computer, der Ihren Datenverkehr weiterleitet und Ihre IP-Adresse verbirgt (6)

2. Sicherheitssystem, das unbefugten Datenverkehr überwacht und blockiert (8)

3. Einschränkung, die den Webzugriff abhängig vom physischen Standort verhindert (11)

4. Internetdienstanbieter (ISP), der Ihren Datenverkehr protokolliert, sofern er nicht verschlüsselt ist (8)

Kontrollpunkt 5, Alternative: Barrierefreie Kreuzworträtsel-Hinweise

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

WAAGERECHT

4 waagerecht: Zustand, frei von Tracking und öffentlicher Überwachung zu sein (13 Buchstaben):

5 waagerecht: Maximale Datenübertragungsrate einer Verbindung (10 Buchstaben):

6 waagerecht: Regelwerk, das festlegt, wie Daten über das Netzwerk übertragen werden (9 Buchstaben):

7 waagerecht: Verpacken von Datenpaketen in ein anderes Paket für die sichere Übertragung (9 Buchstaben):

SENKRECHT

1 senkrecht: Entfernter Computer, der Ihren Datenverkehr weiterleitet und Ihre IP-Adresse verbirgt (6 Buchstaben):

2 senkrecht: Sicherheitssystem, das unbefugten Datenverkehr überwacht und blockiert (8 Buchstaben):

3 senkrecht: Einschränkung, die den Webzugriff abhängig vom physischen Standort verhindert (11 Buchstaben):

4 senkrecht: Internetdienstanbieter (ISP), der Ihren Datenverkehr protokolliert, sofern er nicht verschlüsselt ist (8 Buchstaben):

Kontrollpunkt 6: Suchsel

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

D F H I D R Q T M E I R Z S F

G L Q V F A A U Q O P N P T X

N L Q K R U S N S E R V E R D

I A N Y B F S N X W O J A R Z

K W Y Y L G I E M R T J M B L

C E T O H Q Q L H Z O A O A V

O R G U B Y R I Y B K H L N Z

L I G J O P N N W C O M Z D Y

B F G Y O W U G K V L P B B N

O V T M G V D Y U K L R B R X

E P R I V A T S P H A E R E Z

G Y M R Q X I P D A D J Q I V

W W P R O V I D E R L J H T T

H G B E I K T S V R Z E H E E

S C A L Q C Z M K V R U A S W

WORTSCHATZ-WORTLISTE

TUNNELING PROTOKOLL BANDBREITE SERVER GEOBLOCKING FIREWALL PRIVATSPHAERE PROVIDER

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. TUNNELING**
- **B. PROTOKOLL**
- **C. BANDBREITE**
- **D. SERVER**
- **E. GEOBLOCKING**
- **F. FIREWALL**
- **G. PRIVATSPHAERE**
- **H. PROVIDER**

DEFINITIONEN UND ZUORDNUNGSFELDER

_____ 1. Regelwerk, das festlegt, wie Daten über das Netzwerk übertragen werden.

_____ 2. Einschränkung, die den Webzugriff abhängig vom physischen Standort verhindert.

_____ 3. Sicherheitssystem, das unbefugten Datenverkehr überwacht und blockiert.

_____ 4. Zustand, frei von Tracking und öffentlicher Überwachung zu sein.

_____ 5. Internetdienstanbieter (ISP), der Ihren Datenverkehr protokolliert, sofern er nicht verschlüsselt ist.

_____ 6. Verpacken von Datenpaketen in ein anderes Paket für die sichere Übertragung.

_____ 7. Entfernter Computer, der Ihren Datenverkehr weiterleitet und Ihre IP-Adresse verbirgt.

_____ 8. Maximale Datenübertragungsrate einer Verbindung.

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. LENUTINGN
2. TDBABEEIRN
3. GCOKOENGLIB
4. TRHIPAESEAPRV
5. OORLKTPLO
6. EVSRRE
7. FLWALIER
8. VRIRPEDO

Bonusaufgabe: Schnell denken

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

1	Dinge, die eine IP-Adresse verraten kann			
2	Mythen über VPNs			
3	Dinge, die durch das Internet reisen			
4	Versprechen, die ein guter VPN-Anbieter gibt			
5	Geheimnisse, die Sie verschlüsseln würden			
6	Dinge, vor denen ein VPN Sie nicht schützen kann			
7	Möglichkeiten, ein gefälschtes WLAN zu erkennen			
8	Wörter rund um Privatsphäre			
9	Geräte, die ein VPN nutzen können			
10	Dinge, die passieren, wenn Sie auf „Verbinden“ tippen			
11	Orte, an denen Sie ein VPN nutzen würden			
12	Gründe, auf Reisen ein VPN zu nutzen			
13	Dinge im echten Leben, die wie ein Tunnel aussehen			
14	Wörter aus diesem Arbeitsblatt, die Sie sich merken möchten			
15	Wörter, mit denen Sie einem Kind ein VPN erklären			

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

Ein VPN verschlüsselt Ihren Datenverkehr, um ihn zu schützen. Entschlüsseln Sie mithilfe des Buchstaben-Zahlen-Schlüssels unten die Cybersicherheitsnachricht, indem Sie die passenden Buchstaben in die Lücken schreiben.

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

16	18	9	22	1	20	19	16	8	1	5	18	5		19	9	3	8	5	18

16	5	18		20	21	14	14	5	12		19	3	8	21	5	20	26	5	14

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: Ist die Nutzung eines VPN legal?

Die Nutzung von VPNs ist in vielen Ländern legal, doch manche Rechtsordnungen beschränken, regulieren oder sperren VPN-Dienste. Nutzer sollten vor der Verwendung die aktuellen örtlichen Gesetze prüfen. Weitere Informationen finden Sie in den Leitfäden zur Rechtslage auf VPN.com.

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. [4]

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-Verkehr so, dass er wie gewöhnlicher HTTPS-Verkehr (Port 443) aussieht. Das kann helfen, 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: Kann ein VPN die Drosselung durch den Internetanbieter umgehen?

Manchmal. Ein VPN kann helfen, wenn ein Internetanbieter gezielt erkennbare Aktivitäten verlangsamt, aber es hilft nicht gegen Netzüberlastung, Datenvolumengrenzen, kontobezogene Geschwindigkeitsbegrenzungen oder eine schlechte Netzqualität.

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) wurde von einer Herstellergruppe unter Beteiligung von Microsoft entwickelt und im Juli 1999 als RFC 2637 veröffentlicht, um VPNs für den Fernzugriff zu unterstützen. [6]

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. [4]

4. STRENGE PRÜFSTANDARDS

Führende VPN-Anbieter beauftragen externe Prüfer (wie Cure53 oder PwC) mit unabhängigen Code-Reviews, um zu bestätigen, dass sie keine Nutzeraktivitäten protokollieren.

5. URSPRÜNGE DER 5-EYES-ALLIANZ

Die Five-Eyes-Allianz ging aus dem UKUSA-Abkommen von 1946 zur Fernmeldeaufklärung zwischen den USA und Großbritannien hervor; später kamen Kanada, Australien und Neuseeland hinzu.

6. DEEP PACKET INSPECTION

Deep Packet Inspection (DPI) untersucht Paketinhalte und Verkehrsmuster, nicht nur Header, und einige Firewalls nutzen sie, um gängige VPN-Protokolle zu erkennen und zu blockieren.

7. NUTZUNG IN UNTERNEHMEN

Ein großer Teil der Beschäftigten in Unternehmen weltweit nutzt sichere VPNs, um sich bei internen Datenbanken anzumelden, was VPNs zu einem wichtigen Sicherheitsstandard macht.

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 und Exit) schickt, sodass kein einzelnes Relay beide Enden kennt.

10. KOSTEN VON DATENPANNEN

Ein Zero-Trust-Modell für den sicheren Zugriff mit VPN hilft Organisationen, geistiges Eigentum zu schützen und die finanziellen Folgen von Datenpannen abzumildern.

Technische Referenzen und Quellen

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

WISSENSCHAFTLICHE UND FACHLICHE QUELLEN

[1] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[2] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

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

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[5] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637

Lösungsschlüssel: Arbeitsblatt „Was ist ein VPN?“

1 Hauptfunktion

PROTOKOLLE

Richtige Antwort: B

HINWEIS FÜR LEHRKRÄFTE

Die Hauptaufgabe eines VPN besteht darin, einen verschlüsselten Tunnel aufzubauen, der die Paketnutzdaten schützt und die öffentliche IP-Adresse des Nutzers verschleiert. Quelle: IETF Tunnel RFC.

2 Netzwerk-Tunneling

LATENZ

Richtige Antwort: D

HINWEIS FÜR LEHRKRÄFTE

Tunnelprotokolle kapseln die ursprünglichen Datenpakete in äußere Trägerpakete, damit sie öffentliche Netzwerke sicher durchqueren können. Quelle: IETF Tunnel RFC.

3 Frage 3

Richtige Antwort: B

HINWEIS FÜR LEHRKRÄFTE

Welcher Verschlüsselungsstandard wird häufig zum Schutz von VPN-Datenverkehr verwendet? → Moderner AES-256-Standard

4 Verschlüsselte Komponenten

ROUTING-STEUERUNG

Richtige Antwort: C

HINWEIS FÜR LEHRKRÄFTE

Ein VPN verschlüsselt den gesamten Nutzdatenteil von IP-Paketen und hält so die übertragenen Inhalte vertraulich. Quelle: IETF Tunnel RFC.

5 Frage 5

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Verschlüsselung verwendet einen Algorithmus und einen Schlüssel, um Klartext in unlesbaren Geheimtext umzuwandeln.

Lösungsschlüssel: Kontrollpunkt 2 – Richtig oder Falsch

6 **Schutz vor Abhören** IP-VERSCHLEIERUNG — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

Verschlüsselte Tunnel sorgen dafür, dass Paketnutzdaten für Akteure unlesbar bleiben, die Daten in lokalen WLAN-Netzen abfangen. Quelle: Deloitte Advisory.

7 **Hardware-Änderungen** GESCHWINDIGKEITEN — **Richtige Antwort: Falsch**

HINWEIS FÜR LEHRKRÄFTE

VPNs sind softwarebasierte Netzwerktunnel und verändern die Hardware Ihres Gateway-Routers nicht physisch. Quelle: Cure53 Audit.

8 **Tunneln von Paketen** SNIFFING-RISIKO — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

Tunneling funktioniert, indem die ursprünglichen Netzwerkpakete für die Übertragung in Transport-Header verpackt werden. Quelle: IETF Tunnel RFC.

9 **Symmetrische Schlüssel** FIREWALLS — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

Symmetrische Kryptografie verwendet einen gemeinsamen Schlüssel sowohl zum Ver-als auch zum Entschlüsseln von Netzwerkdatenströmen. Quelle: WireGuard Project.

10 **Unempfindlichkeit gegen Stromausfall** NO-LOGS — **Richtige Antwort: Falsch**

HINWEIS FÜR LEHRKRÄFTE

Ein VPN verschlüsselt nur aktive Verbindungssignale; es kann keine Ausfälle durch lokale Stromausfälle verhindern. 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

H 1. Tunneling	E 2. Protokoll	G 3. Bandbreite	A 4. Server
C 5. Geosperre	D 6. Firewall	F 7. Privatsphäre	B 8. ISP

KONTROLLPUNKT 3: LÖSUNG SCHLÜSSELBEGRIFFE

1 TUNNELING	2 BANDBREITE	3 GEOBLOCKING	4 PROTOKOLL
5 FIREWALL	6 SERVER		

KONTROLLPUNKT 6, ALTERNATIVE: LÖSUNG WORTZUORDNUNG

1 B – PROTOKOLL	2 E – GEOBLOCKING	3 F – FIREWALL	4 G – PRIVATSPHAERE
5 H – PROVIDER	6 A – TUNNELING	7 D – SERVER	8 C – BANDBREITE

DISKUSSIONSHINWEISE FÜR LEHRKRÄFTE

Schlüsselbegriffe:
Prüfen Sie, ob die Lernenden Tunneling, Protokoll und Bandbreite 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.

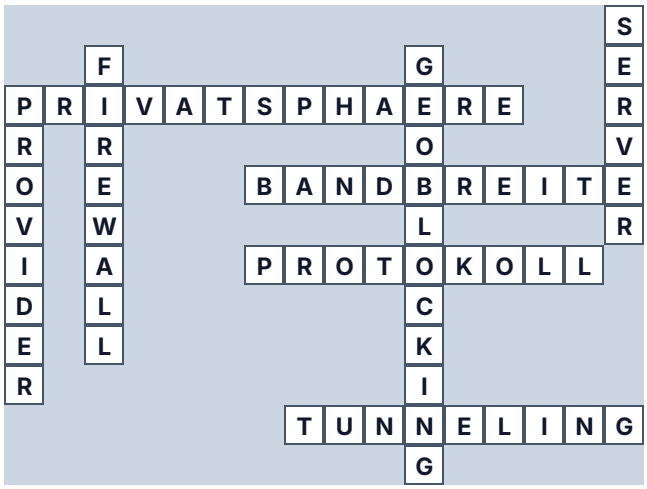
Quellenbewertung:
Lassen Sie die Lernenden mindestens eine Aussage anhand der Quellen des Arbeitsblatts prüfen und besprechen Sie, warum sich Zahlen, Preise und Regeln mit der Zeit ändern können.

Rätsellösungen und Hinweise für Lehrkräfte

LÖSUNG DES SUCHSELS

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

KREUZWORTRÄTSEL-LÖSUNG



LEITFADEN FÜR LEHRKRÄFTE ZU DEN KREUZWORTRÄTSEL-LÖSUNGEN

WAAGERECHT

4 waagerecht: PRIVATSPHAERE Zustand, frei von Tracking und öffentlicher Überwachung zu sein (13 Buchstaben)

5 waagerecht: BANDBREITE Maximale Datenübertragungsrate einer Verbindung (10 Buchstaben)

6 waagerecht: PROTOKOLL Regelwerk, das festlegt, wie Daten über das Netzwerk übertragen werden (9 Buchstaben)

7 waagerecht: TUNNELING Verpacken von Datenpaketen in ein anderes Paket für die sichere Übertragung (9 Buchstaben)

SENKRECHT

1 senkrecht: SERVER Entfernter Computer, der Ihren Datenverkehr weiterleitet und Ihre IP-Adresse verbirgt (6 Buchstaben)

2 senkrecht: FIREWALL Sicherheitssystem, das unbefugten Datenverkehr überwacht und blockiert (8 Buchstaben)

3 senkrecht: GEOBLOCKING Einschränkung, die den Webzugriff abhängig vom physischen Standort verhindert (11 Buchstaben)

4 senkrecht: PROVIDER Internetdienstanbieter (ISP), der Ihren Datenverkehr protokolliert, sofern er nicht verschlüsselt ist (8 Buchstaben)

Lösungsschlüssel für Buchstabensalat und Chiffre

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

LÖSUNGSSCHLÜSSEL BUCHSTABENSALAT

1.	L E N U T I N G N	TUNNELING	5.	O O R L K T P L O	PROTOKOLL
2.	T D B A B E E I R N	BANDBREITE	6.	E V S R R E	SERVER
3.	G C O K O E N G L I B	GEOBLOCKING	7.	F L W A L I E R	FIREWALL
4.	T R H I P A E S E A P R V	PRIVATSPHAERE	8.	V R I R P E D O	PROVIDER

LÖSUNGSSCHLÜSSEL ZUR GEHEIMEN CHIFFRE-AUFGABE

"PRIVATSPHAERE SICHER PER TUNNEL SCHUETZEN"

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.