Name: _____ Datum: _____ Punkte: _____

So verbergen Sie Ihre IP-Adresse Arbeitsblatt

IP-Adressen verbergen, Standort verschleiern, Proxy, Tor und das Verhindern von DNS-/WebRTC-Lecks

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, wie IP-Adressen funktionieren und wie sie Standorte preisgeben.
- Stellen Sie Proxys, Tor und VPNs zur Verschleierung von Netzwerkadressen gegenüber.
- Methoden zur Erkennung und Vermeidung von DNS- und WebRTC-Lecks bestimmen.
- Verstehen, wie Websites Nutzer über ihre öffentliche IP verfolgen.
- Bewerten Sie Multi-Hop-Routing und verschlüsselte Tunnel zum Schutz der IP-Adresse.

ANLEITUNG: ARBEITSBLATT IP-SCHUTZ

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: Verbergen Ihrer IP-Adresse und Verhindern von Lecks. Zum Schluss folgt die Bonusaufgabe Schnell denken.

IHRE IP VERBERGEN (EINFÜHRUNG)

Ihre IP-Adresse ist eine digitale Postanschrift, die Ihren physischen Standort und Ihre Netzwerkgewohnheiten offenlegt. Das Verbergen Ihrer IP-Adresse ist die erste Verteidigungslinie gegen Online-Tracking, gezielte Profilbildung und standortbasierte Sperren. Wer versteht, wie man seine Adresse sicher verbirgt, kann seine Privatsphäre im Internet besser schützen.

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

Kontrollpunkt 1: Auswahlaufgaben

1. Was verrät die öffentliche IP-Adresse eines Geräts den Websites, die Sie besuchen?

- A. Die Kreditkartennummer des Nutzers
- B. Ihren ungefähren Standort und den Namen Ihres Internetanbieters
- C. Das vollständige lokale Dateiverzeichnis
- D. Die Spracheinstellungen der Tastatur

2. Welche Methode verbirgt Ihre IP und verschlüsselt den gesamten Datenverkehr systemweit?

- A. Ein gewöhnlicher Web-Proxy
- B. Löschen Ihrer Browser-Cookies
- C. Ein virtuelles privates Netzwerk (VPN)
- D. Deaktivieren Ihrer nativen Firewall

3. Was ist eine wesentliche Datenschutzeinschränkung bei der Nutzung eines kostenlosen Web-Proxys?

- A. Es verschlüsselt den Datenverkehr in öffentlichen Netzwerken nicht
- B. Es erfordert die Installation eines externen Betriebssystems
- C. Es ist in den Vereinigten Staaten vollständig illegal
- D. Es erfordert einen eigenen Telefonanschluss

4. Wie bietet das Tor-Netzwerk seinen Nutzern ein hohes Maß an Anonymität?

- A. Durch Beschleunigung der Verbindungsgeschwindigkeit
- B. Durch Weiterleitung des Datenverkehrs über drei von Freiwilligen betriebene Relays
- C. Durch Eintragung Ihres Namens in eine globale Datenbank
- D. Durch Beschränkung des Zugangs auf Regierungsbehörden

5. Was ist ein DNS-Leak?

- A. Ein Fehler, bei dem eine E-Mail an die falsche Adresse gesendet wird
- B. Wenn DNS-Anfragen den VPN-Tunnel umgehen und an den Internetanbieter gehen
- C. Ein Hardwaredefekt im Netzteil des lokalen Routers
- D. Ein Update des lokalen Netzwerkadaptertreibers

Kontrollpunkt 2: Richtig oder falsch

6 Frage 6

6. Ein Proxyserver verschlüsselt den Hintergrundverkehr des Betriebssystems genau wie ein VPN.

○ Richtig ○ Falsch

7 Frage 7

7. Tor-Routing ist sehr sicher, verringert aber die Surfgeschwindigkeit im Netzwerk.

○ Richtig ○ Falsch

8 Frage 8

8. WebRTC-Leaks können während einer aktiven VPN-Sitzung Ihre echte IP-Adresse offenlegen.

○ Richtig ○ Falsch

9 Frage 9

9. Bei eingeschaltetem VPN und ohne Lecks kann Ihr Internetanbieter nicht sehen, welche Websites Sie besuchen.

○ Richtig ○ Falsch

10 Frage 10

10. Das Verbergen Ihrer IP-Adresse blockiert Tracking per Browser-Fingerprinting.

○ 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 Umgehung des sicheren Tunnels, bei der Ihre Domain-Anfragen offengelegt werden, nennt man _____ .

2. Browserbasierte Kommunikationsschnittstellen wie _____ können versehentlich Ihre echte IP-Adresse preisgeben.

3. Ein _____ leitet Browser-Datenverkehr um, verschlüsselt die Nutzdaten der Pakete aber nicht.

4. Die mehrschichtige Verschlüsselung im _____ bietet ein hohes Maß an Anonymität.

5. Ihre öffentliche _____ wird von Ihrem Telekommunikationsanbieter vergeben und verrät Ihre Region.

6. Regionale Mediensperren lassen sich durch die _____ des Standorts umgehen.

WORTSCHATZ-WORTBANK

DNS-LEAK IP-ADRESSE ISP-TRACKING MASKIERUNG TOR-NETZWERK VPN-TUNNEL WEB-PROXY WEBRTC

Schreiben Sie Ihre Antworten hier:

1. **2.**

3. **4.**

5. **6.**

Kontrollpunkt 4: Zuordnung von Netzwerk-Begriffen

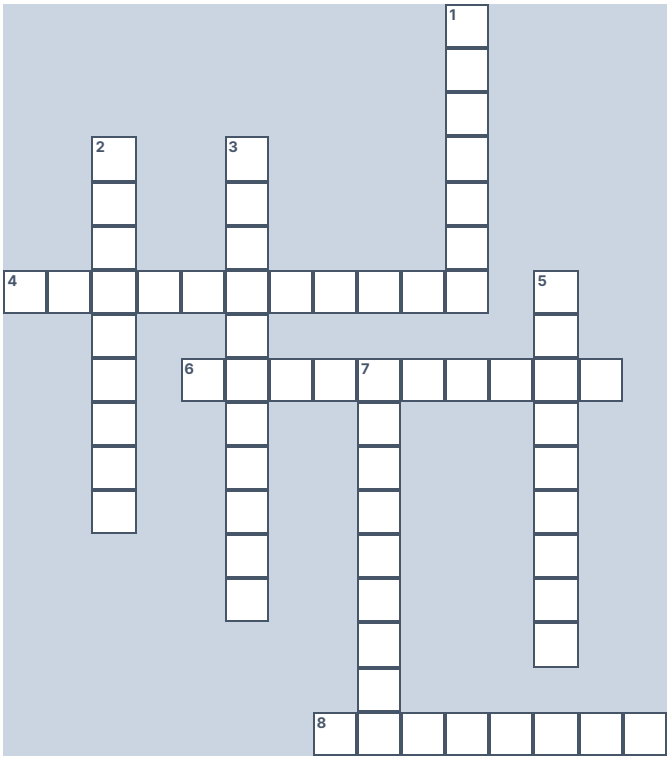
DEFINITIONEN ZUORDNEN

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

1. IP-Adresse	A	Verschlüsselt den gesamten Datenverkehr eines Geräts und leitet ihn über einen VPN-Server.
2. VPN-Tunnel	B	Leitet Daten über drei Server von Freiwilligen und verschlüsselt dabei bei jedem Schritt eine Schicht.
3. Tor-Netzwerk	C	Verbindung über einen Server in einem anderen Land leiten, um Geoblocking zu umgehen.
4. Web-Proxy	D	Eindeutige numerische Bezeichnung, die eine Geräteschnittstelle im Internet identifiziert.
5. DNS-Leck	E	Leitet Browserverkehr auf der Anwendungsebene um, ohne systemweite Verschlüsselung.
6. WebRTC-API	F	Die Protokollierung der Ziele unverschlüsselten Internetverkehrs durch Ihren Telekommunikationsanbieter.
7. Standortverschleierung	G	Anfragen, die außerhalb des VPN-Tunnels aufgelöst werden, sodass die besuchten Domains für den Internetanbieter sichtbar sind.
8. ISP-Tracking	H	Browserfunktion für Sprache/Video, die Tunnel umgehen und echte IP-Adressen offenlegen kann.

Kontrollpunkt 5: Kreuzworträtsel

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



WAAGERECHT

4. Leitet Daten über drei Server von Freiwilligen und verschlüsselt bei jedem Schritt eine Schicht (11)

6. Umleitung der Verbindung über einen Server in einem anderen Land, um Geoblocking zu umgehen (10)

8. Leitet Browser-Datenverkehr auf Anwendungsebene um, ohne systemweite Verschlüsselung (8)

SENKRECHT

1. Anfragen, die außerhalb des VPN-Tunnels aufgelöst werden und dem Internetanbieter die besuchten Domains verraten (7)

2. Browserfunktion für Sprache/Video, die Tunnel umgehen und echte IP-Adressen offenlegen kann (9)

3. Protokollierung der Ziele unverschlüsselten Datenverkehrs durch Ihren Telekommunikationsanbieter (11)

5. Verschlüsselt den gesamten Datenverkehr eines Geräts und leitet ihn über einen VPN-Server (9)

7. Eindeutige numerische Kennung einer Geräteschnittstelle im Internet (9)

Kontrollpunkt 5, Alternative: Barrierefreie Kreuzworträtsel-Hinweise

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

WAAGERECHT

4 waagerecht: Leitet Daten über drei Server von Freiwilligen und verschlüsselt bei jedem Schritt eine Schicht (11 Buchstaben):

6 waagerecht: Umleitung der Verbindung über einen Server in einem anderen Land, um Geoblocking zu umgehen (10 Buchstaben):

8 waagerecht: Leitet Browser-Datenverkehr auf Anwendungsebene um, ohne systemweite Verschlüsselung (8 Buchstaben):

SENKRECHT

1 senkrecht: Anfragen, die außerhalb des VPN-Tunnels aufgelöst werden und dem Internetanbieter die besuchten Domains verraten (7 Buchstaben):

2 senkrecht: Browserfunktion für Sprache/Video, die Tunnel umgehen und echte IP-Adressen offenlegen kann (9 Buchstaben):

3 senkrecht: Protokollierung der Ziele unverschlüsselten Datenverkehrs durch Ihren Telekommunikationsanbieter (11 Buchstaben):

5 senkrecht: Verschlüsselt den gesamten Datenverkehr eines Geräts und leitet ihn über einen VPN-Server (9 Buchstaben):

7 senkrecht: Eindeutige numerische Kennung einer Geräteschnittstelle im Internet (9 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 V A B C P X L K
G Y K X T K D P Q M W J D I N
N K N K Q P G N M M E Q R S T
I A T G C S Q T O H B S B W D
K E S Z V T C U Z W R F K M H
C L Z D N O D N Q X T P C A U
A S B A Z R N N I D C K A S D
R N O D F N H E P W A I D K R
T D Q M E E I L A E P R Z I S
P F Q V F T A A D B I Q O E N
S P T X Q Z K R R P U S D R N
I Y B F S W X W E R J A R U Z
Y Y L G I E M R S O J M L N T
O H Q Q H R Z A S X O V G G U
B Y R Y B K H L E Y Z G J O P

WORTSCHATZ-WORTLISTE

IPADRESSE, VPNTUNNEL, TORNETZWERK, WEBPROXY, DNSLEAK, WEBRTCAPI, MASKIERUNG, ISPTRACKING

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. IPADRESSE**
- **B. VPNTUNNEL**
- **C. TORNETZWERK**
- **D. WEBPROXY**
- **E. DNSLEAK**
- **F. WEBRTCAPI**
- **G. MASKIERUNG**
- **H. ISPTRACKING**

DEFINITIONEN UND ZUORDNUNGSFELDER

1. Leitet Browser-Datenverkehr auf Anwendungsebene um, ohne systemweite Verschlüsselung.
2. Umleitung der Verbindung über einen Server in einem anderen Land, um Geoblocking zu umgehen.
3. Browserfunktion für Sprache/Video, die Tunnel umgehen und echte IP-Adressen offenlegen kann.
4. Eindeutige numerische Kennung einer Geräteschnittstelle im Internet.
5. Leitet Daten über drei Server von Freiwilligen und verschlüsselt bei jedem Schritt eine Schicht.
6. Protokollierung der Ziele unverschlüsselten Datenverkehrs durch Ihren Telekommunikationsanbieter.
7. Anfragen, die außerhalb des VPN-Tunnels aufgelöst werden und dem Internetanbieter die besuchten Domains verraten.
8. Verschlüsselt den gesamten Datenverkehr eines Geräts und leitet ihn über einen VPN-Server.

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. ERDPISSEA
2. EKOTRTREWZN
3. LDEKSAN
4. ENIGKURMAS
5. NUPLNTVEN
6. XYPOWREB
7. CWPIARETB
8. ICGAPIRSNKT

Bonusaufgabe: Schnell denken

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

1	Gründe, auf Reisen ein VPN zu nutzen			
2	Browser, die Sie kennen			
3	Dinge, die ein VPN verbergen kann			
4	Wörter rund um Privatsphäre			
5	Wörter aus diesem Arbeitsblatt, die Sie sich merken möchten			
6	Dinge, die eine Website aus Ihrer IP ableiten kann			
7	Zahlen oder Zeichen in einer IP-Adresse			
8	Mythen über VPNs			
9	VPN-Dienste, die Sie kennen			
10	Dinge, die Ihr Internetanbieter sehen kann			
11	Versprechen, die ein guter VPN-Anbieter gibt			
12	Dinge, die Ihre echte IP preisgeben können			
13	Gründe, Ihren Standort zu verbergen			
14	Möglichkeiten, Ihre IP-Adresse zu verbergen			
15	Geräte, die ein VPN nutzen können			

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 zur IP-Verschleierung abzuschließen, entschlüsseln Sie diese geheime Nachricht über das Verbergen Ihrer digitalen Spuren.

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 2 5 18 7 5 14 19 9 5 9 8 18 5

1 4 18 5 19 19 5 13 9 20

20 1 18 14 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: Verbirgt ein Web-Proxy meine IP-Adresse?

Ja, aber nur für den Datenverkehr, der darüber gesendet wird, meist Ihr Browser. Die meisten Web-Proxys verschlüsseln Ihre Daten nicht, sodass Ihr ISP oder der Netzwerkbetreiber weiterhin sehen kann, was Sie senden und empfangen.

Q5: Ist es legal, meine IP zu verbergen?

In vielen Ländern ja, aber einige beschränken oder verbieten VPNs und andere Werkzeuge zum Verbergen einer IP-Adresse. Das Verbergen Ihrer IP macht eine illegale Handlung niemals legal; prüfen Sie daher vor der Nutzung die örtlichen Gesetze.

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: Verbirgt Tor meine IP?

Ja. Tor leitet Ihren Datenverkehr über drei von Freiwilligen betriebene Relays (Guard, Middle und Exit), sodass Websites die Adresse des Exit-Relays sehen und kein einzelnes Relay sowohl weiß, wer Sie sind, als auch, wohin Sie gehen. [1]

Q7: Was verrät meine IP?

Ihre öffentliche IP-Adresse verrät in der Regel Ihren Internetanbieter und einen ungefähren Standort, etwa Ihr Land oder Ihre Stadt. Websites können sie außerdem nutzen, um Ihre Besuche miteinander zu verknüpfen und Geoblocking anzuwenden.

Q8: Wie prüfe ich, ob sie verborgen ist?

Verbinden Sie sich mit Ihrem VPN, rufen Sie dann eine Website zur IP-Prüfung auf und führen Sie DNS- und WebRTC-Leak-Tests durch. Die angezeigten IP- und DNS-Server sollten zum VPN gehören, nicht zu Ihrem ISP. Wenn Ihre echte IP erscheint, aktivieren Sie den Leak-Schutz.

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: Warum können Websites mich noch verfolgen, nachdem ich meine IP-Adresse verborgen habe?

Das Verbergen Ihrer IP verhindert kein Browser-Fingerprinting. Tracker können Details wie Bildschirmauflösung, installierte Schriftarten und Browsereinstellungen zu einer Kennung kombinieren, und auch Cookies oder angemeldete Konten können Sie identifizieren; nutzen Sie daher zusätzlich einen datenschutzorientierten Browser. [3]

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: Kann IPv6-Traffic meine echte IP-Adresse preisgeben?

Ja, wenn Ihr VPN nur IPv4 tunnelt. Ihr Gerät kann dann IPv6-Verkehr außerhalb des Tunnels senden und eine von Ihrem Internetanbieter zugewiesene Adresse preisgeben. Verwenden Sie ein VPN, das IPv6 tunnelt oder blockiert, und überprüfen Sie dies mit einem IPv6-Leak-Test.

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: Legt Split-Tunneling meine echte IP-Adresse offen?

Ja, für die Apps, die Sie ausnehmen. Datenverkehr außerhalb des Tunnels verwendet Ihre echte IP-Adresse, und RFC 8828 weist darauf hin, dass WebRTC unter einem Split-Tunnel-VPN die Adresse des Internetanbieters preisgeben kann, sofern der Browser dies nicht einschränkt. [2]

Q7: Was ist eine gemeinsam genutzte IP-Adresse und wie hilft sie der Privatsphäre?

Bei einer geteilten IP erscheinen viele VPN-Nutzer gleichzeitig mit derselben Adresse online. Dadurch ist es für eine Website viel schwerer, einen einzelnen Besuch Ihnen zuzuordnen, als bei einer dedizierten IP, die nur Sie nutzen.

Q8: Kann mein Internetanbieter sehen, dass ich ein VPN nutze, um meine IP zu verbergen?

In der Regel ja. Ihr ISP kann sehen, dass Sie sich mit der IP-Adresse eines VPN-Servers verbinden, wann Sie sich verbinden und wie viele Daten Sie senden, nicht aber die Websites, die Sie besuchen, oder die Inhalte im verschlüsselten Tunnel.

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: Ist ein Proxy oder ein VPN besser, um meine IP zu verbergen?

Ein VPN ist in der Regel die bessere Wahl. Es verbirgt Ihre IP-Adresse für alle Apps auf dem Gerät und verschlüsselt den Datenverkehr, während ein Web-Proxy meist nur den Browser abdeckt und oft keine Verschlüsselung hinzufügt.

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.

2. FINGERPRINTING

Das Verbergen Ihrer IP verhindert kein Browser-Fingerprinting, das Sie anhand von Details wie Bildschirmauflösung und installierten Schriftarten identifizieren kann. [3]

3. WIREGUARD-REVOLUTION

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

4. OFFENLEGUNG DER ADRESSE ÜBER WEBRTC

RFC 8828 warnt, dass WebRTC sowohl die öffentliche Adresse eines VPN als auch die Adresse des Internetanbieters, über die das VPN läuft, ermitteln kann, sofern der Browser dies nicht einschränkt. [2]

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. WIEDERVERWENDUNG VON TOR-CIRCUITS

Tor verwendet denselben Circuit etwa zehn Minuten lang und baut dann einen neuen auf, wodurch sich Ihre Browsing-Aktivitäten schwerer miteinander verknüpfen lassen. [1]

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. [1]

10. PROXYS VS. VPN-TUNNEL

Ein Web-Proxy ändert die IP-Adresse, die eine Website für Ihren Browserverkehr sieht, verschlüsselt diesen Verkehr aber im Gegensatz zu einem VPN meist nicht und deckt auch keine anderen Apps auf Ihrem Gerät ab. [5]

Technische Referenzen und Quellen

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

WISSENSCHAFTLICHE UND FACHLICHE QUELLEN

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

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

[2] IETF. (2021). RFC 8828: WebRTC IP Address Handling Requirements.

https://www.rfc-editor.org/rfc/rfc8828

[3] Electronic Frontier Foundation. (n.d.). Cover Your Tracks: Learn.

https://coveryourtracks.eff.org/learn

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

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

[5] 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

Lösungsschlüssel: Verbergen von IP-Adressen, Standortverschleierung, Proxy, Tor und Verhindern von DNS-/WebRTC-Lecks

1 Frage 1

Richtige Antwort: B

HINWEIS FÜR LEHRKRÄFTE

Was verrät die öffentliche IP-Adresse eines Geräts den Websites, die Sie besuchen? → Ihren ungefähren Standort und den Namen Ihres Internetanbieters

2 VPN-Systemverschlüsselung LATENZ

Richtige Antwort: C

HINWEIS FÜR LEHRKRÄFTE

Anders als Proxys, die nur den Browserverkehr umleiten, erstellt ein VPN einen systemweiten verschlüsselten Tunnel und schützt so Hintergrundanwendungen, Spiele und Anfragen des Betriebssystems. Quelle: Tor Project Relays, W3C WebRTC API.

3 Fehlende Proxy-Verschlüsselung WLAN-SICHERHEIT

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Web-Proxys leiten nur den Browser-Datenverkehr weiter, ohne die Paketinhalte zu verschlüsseln. Ihr Netzwerkbetreiber oder ISP kann Ihren Datenverkehr daher weiterhin nachverfolgen. Quelle: IETF Proxy Vulnerabilities.

4 Frage 4

Richtige Antwort: B

HINWEIS FÜR LEHRKRÄFTE

Wie bietet das Tor-Netzwerk seinen Nutzern ein hohes Maß an Anonymität? → Durch Weiterleitung des Datenverkehrs über drei von Freiwilligen betriebene Relays

5 DNS-Leaks im Tunnel PRIVATSPHÄRE

Richtige Antwort: B

HINWEIS FÜR LEHRKRÄFTE

Ein DNS-Leck entsteht, wenn Anfragen zur Namensauflösung den VPN-Tunnel umgehen und direkt an die Resolver Ihres ISP gehen, wodurch die besuchten Domains offengelegt werden. Quelle: DNSSEC Tunnel Testing, EFF Tracking Evasion.

Lösungsschlüssel: Kontrollpunkt 2 – Richtig oder Falsch

6 **Einzelheiten zu den Grenzen von Proxys** IP-VERSCHLEIERUNG — **Richtige Antwort: Falsch**

HINWEIS FÜR LEHRKRÄFTE

Proxys arbeiten auf der Anwendungsebene und haben nicht die systemweite Einbindung auf Netzwerktreiberebene eines VPN-Tunnels. Quelle: IETF Proxy Vulnerabilities.

7 **Frage 7** — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

Die Weiterleitung über drei freiwillige Relays mit mehrschichtiger Verschlüsselung erhöht die Latenz, daher ist Tor meist langsamer als eine direkte Verbindung.

8 **Frage 8** — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

WebRTC kann lokale Adressen und bei manchen VPN-Konfigurationen die vom Internetanbieter zugewiesene öffentliche IP unter dem Tunnel preisgeben (RFC 8828).

9 **Frage 9** — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

Ohne DNS- oder WebRTC-Lecks sieht der Internetanbieter nur verschlüsselten Datenverkehr zum VPN-Server, nicht die Websites, die Sie besuchen.

10 **Grenzen beim Fingerprinting** NO-LOGS — **Richtige Antwort: Falsch**

HINWEIS FÜR LEHRKRÄFTE

Fingerprinting zielt auf Merkmale der Gerätekonfiguration (Bildschirmauflösung, Schriftarten, Plug-ins), die auch dann sichtbar bleiben, wenn die IP verborgen ist. Quelle: EFF Tracking Evasion.

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

D 1. IP-Adresse	A 2. VPN-Tunnel	B 3. Tor-Netzwerk	E 4. Web-Proxy
G 5. DNS-Leck	H 6. WebRTC-API	C 7. Standortverschleierung	F 8. ISP-Tracking

KONTROLLPUNKT 3: LÖSUNG SCHLÜSSELBEGRIFFE

1 DNS-LEAK	2 WEBRTC	3 WEB-PROXY	4 TOR-NETZWERK
5 IP-ADRESSE	6 MASKIERUNG		

KONTROLLPUNKT 6, ALTERNATIVE: LÖSUNG WORTZUORDNUNG

1 D – WEBPROXY	2 G – MASKIERUNG	3 F – WEBRTCAPI	4 A – IPADRESSE
5 C – TORNETZWERK	6 H – ISPTRACKING	7 E – DNSLEAK	8 B – VPNTUNNEL

DISKUSSIONSHINWEISE FÜR LEHRKRÄFTE

Schlüsselbegriffe:
Prüfen Sie, ob die Lernenden IP-Adresse, VPN-Tunnel und Tor-Netzwerk 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.

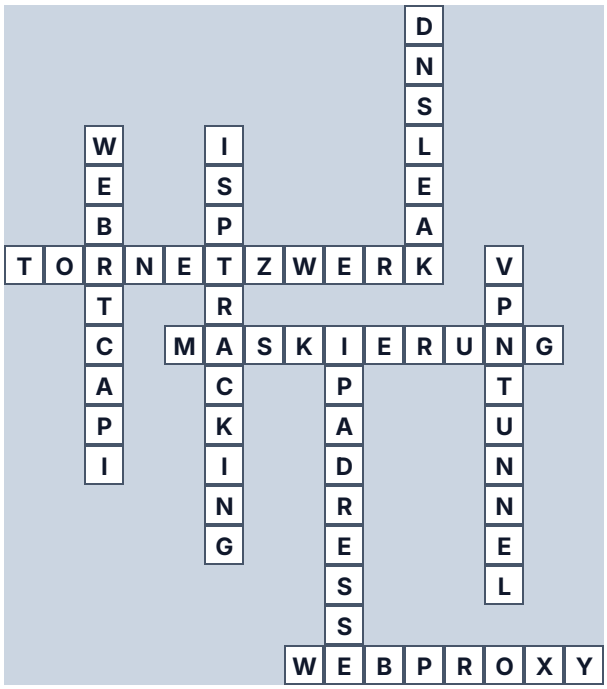
Quellenbewertung:
Lassen Sie die Lernenden mindestens eine Aussage anhand der Quellen des Arbeitsblatts prüfen und besprechen Sie, warum sich Zahlen, Preise und Regeln mit der Zeit ändern können.

Rätsellösungen und Hinweise für Lehrkräfte

LÖSUNG DES SUCHSELS

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

KREUZWORTRÄTSEL-LÖSUNG



LEITFADEN FÜR LEHRKRÄFTE ZU DEN KREUZWORTRÄTSEL-LÖSUNGEN

WAAGERECHT

4 waagerecht: TORNETZWERK Leitet Daten über drei Server von Freiwilligen und verschlüsselt bei jedem Schritt eine Schicht (11 Buchstaben)

6 waagerecht: MASKIERUNG Umleitung der Verbindung über einen Server in einem anderen Land, um Geoblocking zu umgehen (10 Buchstaben)

8 waagerecht: WEBPROXY Leitet Browser-Datenverkehr auf Anwendungsebene um, ohne systemweite Verschlüsselung (8 Buchstaben)

SENKRECHT

1 senkrecht: DNSLEAK Anfragen, die außerhalb des VPN-Tunnels aufgelöst werden und dem Internetanbieter die besuchten Domains verraten (7 Buchstaben)

2 senkrecht: WEBRTCAPI Browserfunktion für Sprache/Video, die Tunnel umgehen und echte IP-Adressen offenlegen kann (9 Buchstaben)

3 senkrecht: ISPTRACKING Protokollierung der Ziele unverschlüsselten Datenverkehrs durch Ihren Telekommunikationsanbieter (11 Buchstaben)

5 senkrecht: VPNTUNNEL Verschlüsselt den gesamten Datenverkehr eines Geräts und leitet ihn über einen VPN-Server (9 Buchstaben)

7 senkrecht: IPADRESSE Eindeutige numerische Kennung einer Geräteschnittstelle im Internet (9 Buchstaben)

Lösungsschlüssel für Buchstabensalat und Chiffre

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

LÖSUNGSSCHLÜSSEL BUCHSTABENSALAT

1. E R D P I S S E A — **IPADRESSE**
2. E K O T R T R E W Z N — **TORNETZWERK**
3. L D E K S A N — **DNSLEAK**
4. E N I G K U R M A S — **MASKIERUNG**
5. N U P L N T V E N — **VPNTUNNEL**
6. X Y P O W R E B — **WEBPROXY**
7. C W P I A R E T B — **WEBRTCAPI**
8. I C G A P I R S N K T — **ISPTRACKING**

LÖSUNGSSCHLÜSSEL ZUR GEHEIMEN CHIFFRE-AUFGABE

"VERBERGEN SIE IHRE ADRESSE MIT TARNSYSTEM"

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.