Name: _____ Datum: _____ Punkte: _____

Leitfaden: Sicherstes VPN

Technische Analyse eines hochsicheren VPN-Designs: reine RAM-Server mit flüchtigem Speicher, Zero-Trust-Zugriffssicherheit, Schutz vor DNS-Lecks durch privates verschlüsseltes DNS und geprüfte WireGuard-Konfigurationen.

LERNÜBERSICHT ZUM LEITFADEN: SICHERSTES VPN

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 technischen Standards hochsicherer VPNs. Sie lernen Server-Hardware, die nur im RAM läuft, Zero-Trust-Zugriffssicherheit, private verschlüsselte DNS-Resolver und geprüfte WireGuard-Konfigurationen kennen.

KONTROLLPUNKTE DES ARBEITSBLATTS

- [ ] **Teil 1-4: VPN- und Netzwerksicherheitskonfigurationen 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.**

Leitfaden „Beste VPNs“ von VPN.com öffnen

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

Ihr Lernfahrplan: Das sicherste VPN

- Analysieren Sie die technische Architektur und die Verschlüsselungsstandards im Leitfaden zum sichersten VPN.
- Konfigurieren Sie die Client-Einstellungen so, dass IP-, DNS- und WebRTC-Leaks verhindert werden.
- Vergleichen Sie proprietäre Tunnelprotokolle mit Standardimplementierungen.

ANLEITUNG ZUM LEITFADEN: SICHERSTES 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: Reine RAM-Serverhardware und Zero-Trust-Systeme. Zum Schluss folgt die Bonusaufgabe Schnell denken.

REINE RAM-INFRASTRUKTUREN UND ZERO-TRUST-NETZWERKE (EINFÜHRUNG)

Ein wirklich sicheres VPN stützt sich auf ein Zero-Trust-Framework, reine RAM-Server (damit bei einer Beschlagnahme von Festplatten keine Protokolle offengelegt werden), private verschlüsselte DNS-Resolver und geprüfte Protokolle wie WireGuard. Diese Maßnahmen schützen zusammen wertvolle digitale Assets vor dem Abfangen von Daten.

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

Kontrollpunkt 1: Auswahlaufgaben

1 **1. Welche Architektur ist grundlegend, um die höchste Sicherheit moderner VPN-Server zu gewährleisten?**

- A) Reine RAM-Serverinfrastruktur
- B) Festplattenbasierter Speicher
- C) Dynamisches DNS-Routing
- D) Aktivierung der Portweiterleitung

2 **2. Welches Protokoll wird allgemein für die sichersten und modernsten VPN-Konfigurationen empfohlen?**

- A) WireGuard
- B) PPTP
- C) L2TP/IPSec
- D) SSTP

3 **3. Welches Sicherheitskonzept verlangt, dass jede Verbindung ausnahmslos und fortlaufend überprüft wird?**

- A) Zero-Trust-Architektur
- B) Perimeter-Firewalls
- C) Dynamisches Routing
- D) Gemeinsame geheime Schlüssel

4 **4. Was ist die Hauptaufgabe des DNS-Leak-Schutzes eines VPN-Clients?**

- A) Alle DNS-Anfragen über private verschlüsselte Resolver leiten
- B) IP-Pakete verschleiern
- C) DNS-Anfragen lokal zwischenspeichern
- D) Nameserver deaktivieren

5 **5. Wie erhöht Multi-Hop-Routing die Gesamtsicherheit eines VPN-Tunnels?**

- A) Leitet Daten nacheinander über zwei getrennte Server
- B) Erhöht die Komprimierungsgeschwindigkeit
- C) Verschlüsselt Daten mit schwachen Chiffren
- D) Umgeht Firewalls

Kontrollpunkt 2: Richtig oder falsch

6 Frage 6

6. Reine RAM-Server speichern Protokolldateien im flüchtigen Speicher, der beim Neustart gelöscht wird.

○ Richtig ○ Falsch

7 Frage 7

7. WireGuard nutzt moderne kryptografische Algorithmen, die weniger anfällig für Geschwindigkeitsengpässe sind.

○ Richtig ○ Falsch

8 Frage 8

8. Ein VPN-Kill-Switch blockiert den gesamten Netzwerkverkehr, wenn der Tunnel abbricht.

○ Richtig ○ Falsch

9 Frage 9

9. Unabhängige Audits durch Dritte sind für die Überprüfung von Sicherheitszusagen unerheblich.

○ Richtig ○ Falsch

10 Frage 10

10. Zero-Trust-Modelle gehen davon aus, dass alle internen Netzwerkverbindungen standardmäßig sicher sind.

○ 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. Administratoren setzen Sicherheit durch, indem sie ein striktes Sicherheitsmodell nach dem Prinzip _____ einführen.

2. Um Pakete über mehrere Einstiegspunkte zu leiten, ist eine sichere Konfiguration mit _____ nötig.

3. Um Datenlecks durch gestohlene Laufwerke zu verhindern, setzen wir auf das Design _____ .

4. Hijacking durch den Internetanbieter wird durch die Konfiguration von integriertem _____ eingedämmt.

5. Um den Datenverkehr bei Verbindungsabbrüchen zu blockieren, aktivieren Sie den _____ .

6. Um gespeicherte Datenbank-Logs zu minimieren, wählen Sie einen Anbieter, dessen System vollständig _____ ist.

WORTSCHATZ-WORTBANK

AUDITIERT DNS-SCHUTZ KILL SWITCH MULTI-HOP PROTOKOLL RAM-SERVER VERSCHLÜSSELUNG ZERO TRUST

Schreiben Sie Ihre Antworten hier:

1. 2.

3. 4.

5. 6.

Kontrollpunkt 4: Zuordnung von VPN- und Netzwerk-Begriffen

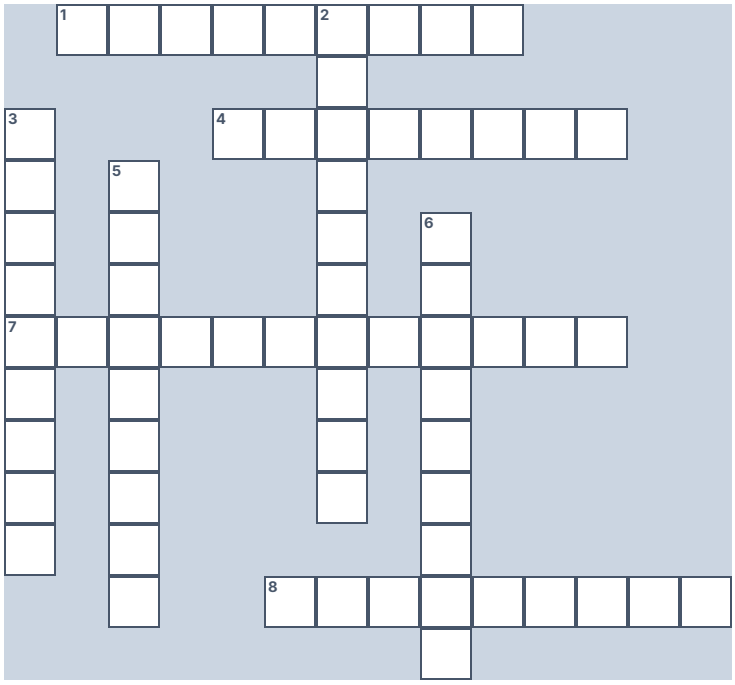
DEFINITIONEN ZUORDNEN

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

☐	1. Zero Trust	A	Unabhängig geprüfte Einrichtung, die bestätigt, dass keine Logs gespeichert werden.
☐	2. Multi-Hop	B	Kryptografisches Verwürfeln von Nutzdaten zur Absicherung der Übertragung.
☐	3. Reiner RAM-Server	C	Sicherheitskonzept, das eine fortlaufende Authentifizierung aller Benutzer verlangt.
☐	4. DNS-Schutz	D	Satz technischer Regeln, der festlegt, wie Daten verpackt und gesendet werden.
☐	5. Kill Switch	E	Kaskadiertes VPN-Routing, das zwei Serverknoten miteinander verkettet.
☐	6. Geprüftes System	F	Serverarchitektur, die Nutzdaten in flüchtigem Speicher ablegt.
☐	7. Verschlüsselung	G	Erzwingen privater DNS-Anfragen, um Nameserver-Abfragen zu schützen.
☐	8. Protokoll	H	Ausfallsicherung, die den Datenverkehr blockiert, wenn das VPN ausfällt.

Kontrollpunkt 5: Kreuzworträtsel

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



WAAGERECHT

1. Satz technischer Regeln, der festlegt, wie Daten verpackt und gesendet werden (9)

4. Kaskadiertes VPN-Routing, das zwei Serverknoten hintereinanderschaltet (8)

7. Kryptografisches Verwürfeln von Nutzdaten zur Sicherung der Übertragung (12)

8. Serverarchitektur, die Daten im flüchtigen Arbeitsspeicher ablegt (9)

SENKRECHT

2. Ausfallsicherung, die den Datenverkehr blockiert, wenn das VPN ausfällt (10)

3. Erzwingen privater DNS-Anfragen zum Schutz von Nameserver-Abfragen (9)

5. Status eines unabhängig geprüften Systems, der bestätigt, dass keine Logs gespeichert werden (9)

6. Sicherheitsmodell, das die fortlaufende Authentifizierung aller Nutzer verlangt (9)

Kontrollpunkt 5, Alternative: Barrierefreie Kreuzworträtsel-Hinweise

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

WAAGERECHT

1 waagerecht: Satz technischer Regeln, der festlegt, wie Daten verpackt und gesendet werden (9 Buchstaben):

4 waagerecht: Kaskadiertes VPN-Routing, das zwei Serverknoten hintereinanderschaltet (8 Buchstaben):

7 waagerecht: Kryptografisches Verwürfeln von Nutzdaten zur Sicherung der Übertragung (12 Buchstaben):

8 waagerecht: Serverarchitektur, die Daten im flüchtigen Arbeitsspeicher ablegt (9 Buchstaben):

SENKRECHT

2 senkrecht: Ausfallsicherung, die den Datenverkehr blockiert, wenn das VPN ausfällt (10 Buchstaben):

3 senkrecht: Erzwingen privater DNS-Anfragen zum Schutz von Nameserver-Abfragen (9 Buchstaben):

5 senkrecht: Status eines unabhängig geprüften Systems, der bestätigt, dass keine Logs gespeichert werden (9 Buchstaben):

6 senkrecht: Sicherheitsmodell, das die fortlaufende Authentifizierung aller Nutzer verlangt (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.

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

WORTSCHATZ-WORTLISTE

ZEROTRUST MULTIHOP RAMSERVER DNSSCHUTZ KILLSWITCH AUDITIERT
CHIFFRIERUNG PROTOKOLL

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. ZEROTRUST**
- **B. MULTIHOP**
- **C. RAMSERVER**
- **D. DNSSCHUTZ**
- **E. KILLSWITCH**
- **F. AUDITIERT**
- **G. CHIFFRIERUNG**
- **H. PROTOKOLL**

DEFINITIONEN UND ZUORDNUNGSFELDER

_____ 1. Ausfallsicherung, die den Datenverkehr blockiert, wenn das VPN ausfällt.

_____ 2. Erzwingen privater DNS-Anfragen zum Schutz von Nameserver-Abfragen.

_____ 3. Kaskadiertes VPN-Routing, das zwei Serverknoten hintereinanderschaltet.

_____ 4. Satz technischer Regeln, der festlegt, wie Daten verpackt und gesendet werden.

_____ 5. Kryptografisches Verwürfeln von Nutzdaten zur Sicherung der Übertragung.

_____ 6. Serverarchitektur, die Daten im flüchtigen Arbeitsspeicher ablegt.

_____ 7. Status eines unabhängig geprüften Systems, der bestätigt, dass keine Logs gespeichert werden.

_____ 8. Sicherheitsmodell, das die fortlaufende Authentifizierung aller Nutzer verlangt.

Kontrollpunkt 7: Buchstabensalat

Bringen Sie die Buchstaben unten in die richtige Reihenfolge, um zentrale Begriffe zu Virtual Private Networks (VPN) aufzudecken. Schreiben Sie Ihre Antworten in die vorgesehenen Eingabefelder.

1. RTOEZUSTR
2. RRESARVEM
3. KWCIISHLTL
4. NEFIIGRURCHF
5. IHUPTMOL
6. TSNUHDCZS
7. IARTEIUTD
8. LOLPTRKOO

Bonusaufgabe: Schnell denken

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

1	Schlösser oder Schlüssel, die Sie jeden Tag benutzen			
2	Dinge, die ein VPN verbergen kann			
3	Dinge, die ein VPN sicher machen			
4	Mythen über VPNs			
5	Gründe, auf Reisen ein VPN zu nutzen			
6	Sichere Orte in der realen Welt			
7	Wörter, die „geschützt“ bedeuten			
8	Versprechen, die ein guter VPN-Anbieter gibt			
9	Wörter rund um Privatsphäre			
10	Arten von Audits oder Prüfungen			
11	Wörter aus diesem Arbeitsblatt, die Sie sich merken möchten			
12	Dinge, die ein Hacker stehlen möchte			
13	Möglichkeiten, ein gefälschtes WLAN zu erkennen			
14	Orte, an denen Sie ein VPN nutzen würden			
15	Dinge, die Ihr Internetanbieter sehen kann			

Kontrollpunkt 8: Fallstudien zu VPN und Netzwerken

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

FALLSTUDIE 1: HÄRTUNG DER UNTERNEHMENSINFRASTRUKTUR

👷

Szenario: Eine Geschäftsbank gestaltet ihre Fernzugriffs-Topologie neu. Sie benötigt eine Zero-Trust-Architektur, die alle Client-Geräte mit sicheren Servern verbindet.

Diskussionsfrage: Was ist der Hauptvorteil der Mikrosegmentierung von Netzwerken in einem Zero-Trust-VPN-Modell?

FALLSTUDIE 2: SCHUTZ DURCH NUR-RAM-SERVER

👷

Szenario: Ein auf Sicherheit ausgerichteter VPN-Anbieter rüstet seine Server auf, damit eine physische Beschlagnahme von Servern keine Nutzerprotokolle offenlegt.

Diskussionsfrage: Erklären Sie, wie reine RAM-Hardwarekonfigurationen bei einer physischen Beschlagnahme von Servern die forensische Datenextraktion verhindern.

Kontrollpunkt 9: Entschlüsselung der Chiffre

Eine Netzwerktechnikerin oder ein Netzwerktechniker sichert Routing-Kanäle und Client-Tunnel. Entschlüsseln Sie mithilfe des Buchstaben-Zahlen-Schlüssels unten die Nachricht, 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

19	9	3	8	5	18	5		22	16	14	19
19	3	8	21	5	20	26	5	14		23	5	18	20	22	15	12	12	5
4	9	7	9	20	1	12	5		7	21	5	20	5	18				

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 zu virtuellen privaten Netzwerken (VPNs) und Tunneling an.

Q1: Was macht ein VPN zum „sichersten“?

Eine Kombination aus Zero Trust, reinen RAM-Servern und geprüften Protokollen.

Q2: Was sind reine RAM-Server?

Server, die im flüchtigen Speicher laufen und so ausgelegt sind, dass sie keine Protokolle auf der Festplatte speichern.

Q3: Was ist ein Zero-Trust-VPN?

Ein Framework, das jede Zugriffsanfrage und jede Verbindung fortlaufend überprüft.

Q4: Warum gilt WireGuard als sicher?

Es hat eine kleine, leicht prüfbare Codebasis und verwendet moderne Chiffren.

Q5: Wie verhindern sichere VPNs DNS-Lecks?

Durch Leiten aller Anfragen über private, verschlüsselte DNS-Resolver.

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

Sehen Sie sich die häufigsten Fragen und Antworten zu virtuellen privaten Netzwerken (VPNs) und Tunneling an.

Q6: Braucht ein sicheres VPN Audits?

Ja, unabhängige Audits überprüfen No-Logs-Versprechen und die Sicherheit des Codes.

Q7: Welche Rolle spielt ein Kill Switch?

Er stoppt den Netzwerkverkehr sofort, wenn die VPN-Verbindung abbricht.

Q8: Welche Verschlüsselung wird in sicheren VPNs verwendet?

AES-256 und ChaCha20 sind die Industriestandards für Verschlüsselung.

Q9: Ist Multi-Hop-Routing sicher?

Ja, es verkettet zwei oder mehr Server, um eine Verkehrsanalyse zu verhindern.

Q10: Wie hilft eine Offshore-Rechtsordnung?

Es kann einschränken, welche Gesetze gelten, bietet aber keine absolute Immunität.

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

Erkunden Sie fortgeschrittene technische Aspekte von VPN-Tunnelprotokollen, der Integration mobiler Clients und des Einsatzes in Unternehmen.

Q1: Wie verhindern reine RAM-Server das Risiko einer Datenbeschlagnahme?

Da sie im RAM laufen, werden beim Ziehen des Steckers die im Speicher gehaltenen Daten gelöscht.

Q2: Wie ersetzt Zero Trust die klassische Perimetersicherheit?

Es behandelt jeden Client als feindlich und verlangt fortlaufende Authentifizierung.

Q3: Warum ist der Quellcode von WireGuard leichter zu prüfen?

Sein Linux-Code umfasst weniger als 4,000 Zeilen und ist damit weit kleiner als typische VPN-Stacks. [4]

Q4: Wie schützt DNSSEC DNS-Anfragen?

Es signiert DNS-Einträge, damit Resolver gefälschte oder manipulierte Antworten erkennen können.

Q5: Wie erschwert Multi-Hop die Korrelation von Traffic?

Durch Trennen eingehender und ausgehender IPs auf verschiedene Hosting-Anbieter.

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

Erkunden Sie fortgeschrittene technische Aspekte von VPN-Tunnelprotokollen, der Integration mobiler Clients und des Einsatzes in Unternehmen.

Q6: Warum sind Rechtsordnungen der Five Eyes für VPNs riskant?

Mitgliedstaaten tauschen Geheimdienstinformationen aus und können Nutzerdaten per gerichtlicher Anordnung anfordern.

Q7: Wie wird ein Kill Switch auf Kernel-Ebene umgesetzt?

Er nutzt Firewall-Regeln des Systems (wie iptables oder WFP), um ausgehenden Verkehr zu blockieren.

Q8: Was ist Forward Secrecy bei VPN-Handshakes?

Sie erzeugt eindeutige Sitzungsschlüssel, sodass vergangene Sitzungen nicht entschlüsselt werden können.

Q9: Wie verringern sichere VPNs WebRTC-Lecks?

Durch Blockieren von WebRTC-Anfragen oder deren Weiterleitung durch den Tunnel.

Q10: Wie stellen unabhängige Audits die Einhaltung des Datenschutzes sicher?

Prüfer führen Penetrationstests durch und untersuchen Serverkonfigurationen.

Teil 11: 10 Fakten und Einblicke zu VPNs aus der Praxis

Lernen Sie reale Fakten zu VPN-Verschlüsselungsgeschwindigkeiten, Protokoll-Audits, mobiler Konnektivität und Remote-Arbeit in Unternehmen kennen.

1. VPN-EINBLICK

Reine RAM-Server laden ihr Betriebssystem beim Start in den Arbeitsspeicher, sodass nach einem Neustart nichts auf der Festplatte verbleibt.

2. VPN-EINBLICK

WireGuard nutzt das Noise-Framework mit Curve25519, ChaCha20, Poly1305, BLAKE2s und HKDF. [3]

3. VPN-EINBLICK

Zero Trust gewährt Zugriff pro Ressource und kein implizites Vertrauen aufgrund des Netzwerkstandorts (NIST SP 800-207). [1]

4. VPN-EINBLICK

Zur Geheimdienstallianz Five Eyes gehören die USA, Großbritannien, Kanada, Australien und Neuseeland.

5. VPN-EINBLICK

WebRTC-Leaks treten auf, wenn Browser die echte öffentliche IP-Adresse des Clients über STUN-Anfragen preisgeben.

6. VPN-EINBLICK

Perfect Forward Secrecy (PFS) stellt sicher, dass die Kompromittierung eines langfristigen Schlüssels keine früheren Sitzungsschlüssel offenlegt. [3]

7. VPN-EINBLICK

Cure53, ein Sicherheitsunternehmen mit Sitz in Berlin, hat Audits mehrerer VPN-Anbieter veröffentlicht.

8. VPN-EINBLICK

DNS-Leaks entstehen, wenn DNS-Anfragen den VPN-Tunnel umgehen und an die Nameserver des lokalen Internetanbieters gehen.

9. VPN-EINBLICK

Flüchtige RAM-Chips benötigen ständig Strom, um Daten zu speichern, und verlieren ihren Inhalt beim Ausschalten.

10. VPN-EINBLICK

Zero-Trust-Systeme in Unternehmen erzwingen Prüfungen des Gerätezustands, bevor eine Verbindung zu geschützten Ressourcen zugelassen wird. [1]

Technische Referenzen und Quellen

Der Lernleitfaden und die interaktiven Rätsel wurden aus globalen technischen Standards, Spezifikationen und Regulierungsrahmen zusammengestellt.

WISSENSCHAFTLICHE UND FACHLICHE QUELLEN

[1] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/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] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

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

Lösungsschlüssel: Kontrollpunkt 1 – Auswahlaufgaben

1 **Reiner RAM-Server** NUR RAM — **Richtige Antwort: A**

HINWEIS FÜR LEHRKRÄFTE

Reine RAM-Server speichern keine Protokolle auf der Festplatte und löschen die Daten beim Neustart. Quelle: Most Secure VPN.

2 **Frage 2** — **Richtige Antwort: A**

HINWEIS FÜR LEHRKRÄFTE

WireGuard verbindet eine kleine, prüfbare Codebasis mit modernen Verschlüsselungsverfahren.

3 **Zero-Trust-Modell** ZERO TRUST — **Richtige Antwort: A**

HINWEIS FÜR LEHRKRÄFTE

Zero-Trust-Modelle überprüfen vor dem Zugriff fortlaufend die Konformität von Geräten. Quelle: Most Secure VPN.

4 **DNS-Schutz** DNS-SCHUTZ — **Richtige Antwort: A**

HINWEIS FÜR LEHRKRÄFTE

Der DNS-Leak-Schutz leitet Suchanfragen über private Resolver. Quelle: Most Secure VPN.

5 **Multi-Hop-Tunnel** MULTI-HOP — **Richtige Antwort: A**

HINWEIS FÜR LEHRKRÄFTE

Multi-Hop-Routing verkettet zwei getrennte Serverknoten hintereinander. Quelle: Most Secure VPN.

Lösungsschlüssel: Kontrollpunkt 2 – Richtig oder Falsch

6 **Reiner RAM-Server** NUR RAM — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

Reine RAM-Server-Hardware schreibt keine Daten auf die Festplatte und wird beim Neustart gelöscht. Quelle: Most Secure VPN.

7 **WireGuard-Geschwindigkeit** WIREGUARD — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

WireGuard nutzt moderne Kryptografie, die Verarbeitungsengpässe vermeidet. Quelle: Most Secure VPN.

8 **Kill Switch** AUSFALLSICHERUNG — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

Ein Kill Switch blockiert den gesamten Datenverkehr, wenn die VPN-Verbindung abbricht. Quelle: Most Secure VPN.

9 **Prüfungen durch Dritte** AUDITS SIND UNERLÄSSLICH — **Richtige Antwort: Falsch**

HINWEIS FÜR LEHRKRÄFTE

Prüfungen durch Dritte sind unerlässlich, um die Datenschutzversprechen von Unternehmen zu überprüfen. Quelle: Most Secure VPN.

10 **Frage 10** — **Richtige Antwort: Falsch**

HINWEIS FÜR LEHRKRÄFTE

Zero Trust gewährt kein implizites Vertrauen aufgrund des Netzwerkstandorts. [1]

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

C 1. Zero Trust	E 2. Multi-Hop	F 3. Reiner RAM-Server	G 4. DNS-Schutz
H 5. Kill Switch	A 6. Geprüftes System	B 7. Verschlüsselung	D 8. Protokoll

KONTROLLPUNKT 3: LÖSUNG SCHLÜSSELBEGRIFFE

1 ZERO TRUST	2 MULTI-HOP	3 RAM-SERVER	4 DNS-SCHUTZ
5 KILL SWITCH	6 AUDITIERT		

KONTROLLPUNKT 6, ALTERNATIVE: LÖSUNG WORTZUORDNUNG

1 E – KILLSWITCH	2 D – DNSSCHUTZ	3 B – MULTIHOP	4 H – PROTOKOLL
5 G – CHIFFRIERUNG	6 C – RAMSERVER	7 F – AUDITIERT	8 A – ZEROTRUST

DISKUSSIONSHINWEISE FÜR LEHRKRÄFTE

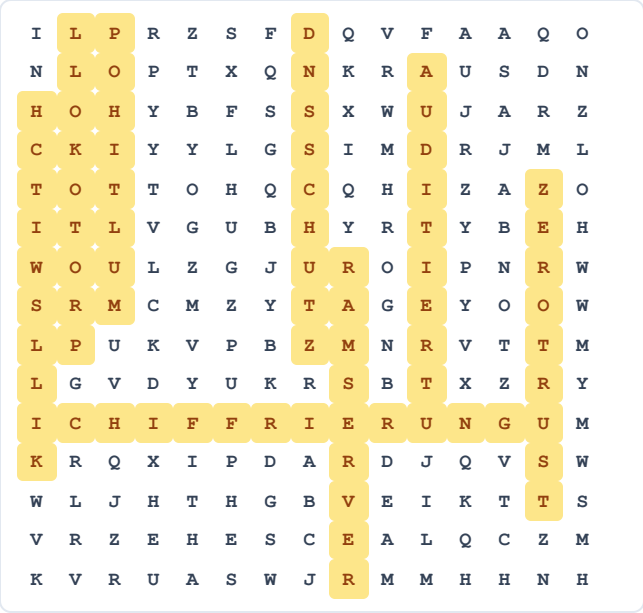
Schlüsselbegriffe:
Prüfen Sie, ob die Lernenden Zero Trust, Multi-Hop und Reiner RAM-Server in eigenen Worten erklären und jeweils ein Beispiel nennen können.

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

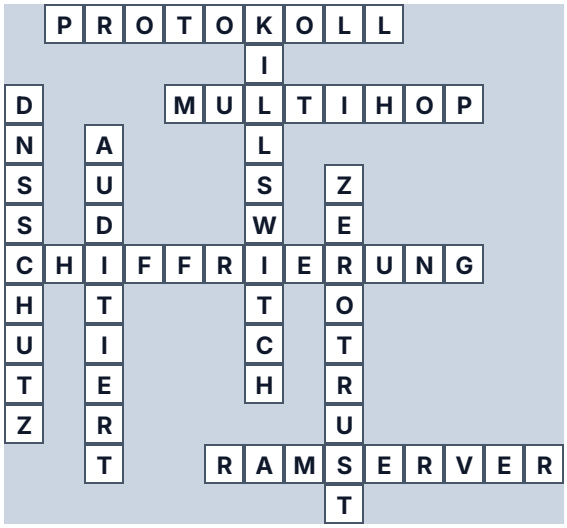
Quellenbewertung:
Lassen Sie die Lernenden mindestens eine Aussage anhand der Quellen des Arbeitsblatts prüfen und besprechen Sie, warum sich Zahlen, Preise und Regeln mit der Zeit ändern können.

Rätsellösungen und Hinweise für Lehrkräfte

LÖSUNG DES SUCHSELS



KREUZWORTRÄTSEL-LÖSUNG



LEITFADEN FÜR LEHRKRÄFTE ZU DEN KREUZWORTRÄTSEL-LÖSUNGEN

WAAGERECHT

1 waagerecht: PROTOKOLL Satz technischer Regeln, der festlegt, wie Daten verpackt und gesendet werden (9 Buchstaben)

4 waagerecht: MULTIHOP Kaskadiertes VPN-Routing, das zwei Serverknoten hintereinanderschaltet (8 Buchstaben)

7 waagerecht: CHIFFRIERUNG Kryptografisches Verwürfeln von Nutzdaten zur Sicherung der Übertragung (12 Buchstaben)

8 waagerecht: RAMSERVER Serverarchitektur, die Daten im flüchtigen Arbeitsspeicher ablegt (9 Buchstaben)

SENKRECHT

2 senkrecht: KILLSWITCH Ausfallsicherung, die den Datenverkehr blockiert, wenn das VPN ausfällt (10 Buchstaben)

3 senkrecht: DNSSCHUTZ Erzwingen privater DNS-Anfragen zum Schutz von Nameserver-Abfragen (9 Buchstaben)

5 senkrecht: AUDITIERT Status eines unabhängig geprüften Systems, der bestätigt, dass keine Logs gespeichert werden (9 Buchstaben)

6 senkrecht: ZEROTRUST Sicherheitsmodell, das die fortlaufende Authentifizierung aller Nutzer verlangt (9 Buchstaben)

Lösungsschlüssel für Buchstabensalat und Chiffre

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

LÖSUNGSSCHLÜSSEL BUCHSTABENSALAT

1. RTOEZUSTR — ZEROTRUST
2. RRESARVEM — RAMSERVER
3. KWCIISHLTL — KILLSWITCH
4. NEFIIGRURCHF — CHIFFRIERUNG
5. IHUPTMOL — MULTIHOP
6. TSNUHDCZS — DNSSCHUTZ
7. IARTEIUTD — AUDITIERT
8. LOLPTRKOO — PROTOKOLL

LÖSUNGSSCHLÜSSEL ZUR GEHEIMEN CHIFFRE-AUFGABE

"SICHERE VPNS SCHUETZEN WERTVOLLE DIGITALE GUETER"

Lösungsschlüssel zu den Fallstudien

A FALLSTUDIE 1: HÄRTUNG DER UNTERNEHMENSINFRASTRUKTUR

Lösung für Lehrkräfte

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Szenarioanalyse: Eine Unternehmensbank gestaltet ihre Topologie für den Fernzugriff neu. Sie benötigt eine Zero-Trust-Architektur, die alle Client-Geräte mit sicheren Servern verbindet.
- Empfohlene Strategie und Lösung: Bewertungshinweise: Es sollte erklärt werden, dass Mikrosegmentierung den Zugriff auf bestimmte Ressourcen beschränkt und so die seitliche Ausbreitung einer Bedrohung verhindert, falls ein Gerät kompromittiert wird.

B FALLSTUDIE 2: SCHUTZ DURCH NUR-RAM-SERVER

Lösung für Lehrkräfte

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Szenarioanalyse: Ein auf Sicherheit ausgerichteter VPN-Anbieter rüstet seine Server auf, damit bei einer physischen Beschlagnahmung keine Protokollverläufe der Nutzer offengelegt werden.
- Empfohlene Strategie und Lösung: Bewertungshinweise: Es sollte dargelegt werden, dass reine RAM-Server keinen physischen Festplattenspeicher haben. Bei einem Stromausfall werden alle flüchtigen Daten im Arbeitsspeicher automatisch gelöscht.