Name: _____ Datum: _____ Punkte: _____

Dark Web vs. Deep Web: Sicherheit und Unterschiede

Suchmaschinenindexierung, Datenbanken im Deep Web, Onion-Routing mit Tor, Anonymität im Netzwerk und Risiken

LERNÜBERSICHT: DARK WEB VS. DEEP WEB

GESICHERT
DATENVERSCHLÜSSELUNG
256-Bit-AES-Standard

KONFORM
GLOBALE STANDARDS
Rahmenwerke DSGVO (GDPR) und CCPA

ZERO-TRUST
ZUGRIFFSRICHTLINIE
Mehr-Faktor-Authentifizierung

Willkommen! Dieses Aktivitätspaket führt Sie durch die Unterschiede zwischen Deep Web und Darknet. Sie lernen nicht indexierte Datenbanken, das Onion-Routing des Tor Browsers, kryptografische .onion-Domains und Sicherheitsrisiken der Anonymität kennen.

KONTROLLPUNKTE DES ARBEITSBLATTS

- [ ] **Teil 1-4: Cybersicherheit und Bedrohungsabwehr 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.**

Cybersicherheits-Leitfaden von VPN.com öffnen

URL: https://www.vpn.com/de/cybersicherheit/dark-web-vs-deep-web/

Ihr Lernfahrplan: Strategie für Deep Web und Darknet

- Stellen Sie das Deep Web (nicht indexierte Datenbanken) dem Dark Web (Onion-Dienste) gegenüber.
- Verstehen, wie Onion-Routing Netzwerkverkehr verschlüsselt und weiterleitet.
- Bewerten Sie die Sicherheitsrisiken beim Aufrufen nicht verifizierter Websites im Tor-Netzwerk.
- Setzen Sie Richtlinien für sichere Gateways und Sandboxing beim Crawling für Bedrohungsinformationen ein.
- Analysieren Sie das kryptografische Adressformat der Domains von Onion-Diensten.

ANLEITUNG ZUM DEEP UND DARK WEB

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: Privatsphäre im Deep Web und Dark Web. Zum Schluss folgt die Bonusaufgabe Schnell denken.

DATENBANKEN IM DEEP WEB VS. ONION-ROUTING IM DARK WEB (EINFÜHRUNG)

Das Deep Web besteht aus nicht indexierten Seiten hinter Passwörtern und Anmeldungen, etwa private E-Mails oder Bankportale von Unternehmen. Das Dark Web ist ein absichtlich verborgener Teilbereich des Deep Web, für dessen anonymen Zugriff spezielle Browser (wie Tor) und Onion-Netzwerke nötig sind.

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

Kontrollpunkt 1: Auswahlaufgaben

1. Wodurch unterscheidet sich das Deep Web vom Surface Web?

- A. Seiten im Deep Web werden von öffentlichen Suchmaschinen nicht indiziert
- B. Datenverkehr im Deep Web ist illegal und wird von den Strafverfolgungsbehörden überwacht
- C. Für den Zugriff auf Deep-Web-Seiten sind spezielle Browser wie Tor erforderlich
- D. Seiten im Deep Web laden immer schneller als Seiten im Surface Web

2. Wie greift man auf das Darknet zu?

- A. Über spezielle Browser, die Onion-Routing-Netzwerke nutzen
- B. Durch Konfigurieren benutzerdefinierter DNS-Einstellungen auf Standardroutern
- C. Über private, nur auf Einladung zugängliche Suchkonsolen im Surface Web
- D. Durch Installation einer gewöhnlichen Browsererweiterung zum Blockieren von Werbung

3. Welche Struktur bildet den größten Teil des Deep Web?

- A. Passwortgeschützte Nutzerdatenbanken und private Konten
- B. Illegale Schwarzmarktforen, in denen illegale Waren gehandelt werden
- C. Unverschlüsselte Peer-to-Peer-Filesharing-Protokolle
- D. Cache-Datenbanken öffentlicher Suchmaschinen

4. Was bewirkt Onion Routing beim Netzwerkverkehr?

- A. Es verschlüsselt Pakete und leitet sie über mehrere Relays
- B. Es erhöht die Downloadgeschwindigkeit durch Umgehen der Knoten des Internetanbieters
- C. Es ordnet Hardware-Seriennummern von Geräten IP-Einträgen zu
- D. Es löscht Browser-Cookies nach jedem Klick

5. Welche Domain-Endung wird ausschließlich im Tor-Netzwerk verwendet?

- A. Die kryptografische Top-Level-Endung .onion
- B. Die klassische kommerzielle Standardendung .com
- C. Die dezentrale Web3-Blockchain-Endung .eth
- D. Die Länderendung .ai für Technologie

Kontrollpunkt 2: Richtig oder falsch

6 Frage R/F 6

6. Deep Web und Dark Web bezeichnen denselben Netzwerkbereich.

Richtig Falsch

7 Frage R/F 7

7. Intranet-Portale von Unternehmen gehören zum Deep Web.

Richtig Falsch

8 Frage R/F 8

8. Onion-Routing entschlüsselt Datenpakete an jedem Transitknoten vollständig.

Richtig Falsch

9 Frage R/F 9

9. Der Zugriff auf das Darknet setzt Geräte einem hohen Malware-Risiko aus.

Richtig Falsch

10 Frage R/F 10

10. Herkömmliche Websuchmaschinen durchsuchen und indexieren Onion-Websites.

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. Private Bankportale liegen im nicht indexierten Bereich, dem _____ .
2. Spezielle Tor-Knoten hosten versteckte Dienste im _____ .
3. Tor-Websites nutzen die kryptografische Top-Level-Endung _____ .
4. Die verschlüsselte Weiterleitung über mehrere Schichten nennt man _____ .
5. Suchmaschinen des Surface Web durchsuchen Seiten, die öffentlich _____ sind.
6. Onion-Netzwerke verschlüsseln die IP-Adressen der Clients, um die _____ der Nutzer zu wahren.

WORTSCHATZ-WORTBANK

.ONION | ANONYMITÄT | DARK WEB | DATENBANK | DEEP WEB | EINGANGSKNOTEN | INDEXIERT | ONION-ROUTING

Schreiben Sie Ihre Antworten hier:

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

Kontrollpunkt 4: Zuordnung von Sicherheits-Begriffen

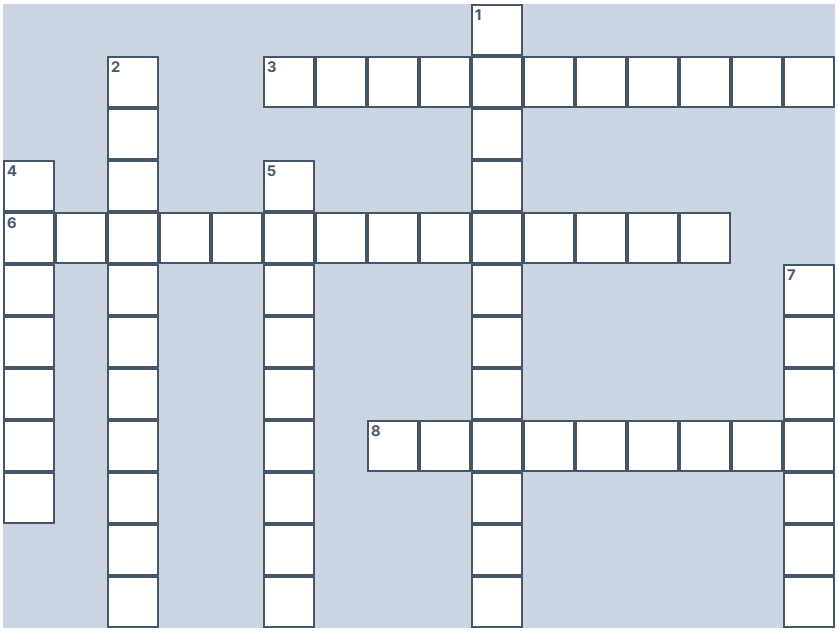
DEFINITIONEN ZUORDNEN

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

1. Segment des Deep Web	A	Verschlüsseltes Netzwerksegment, das nur über spezielle Browser zugänglich ist.
2. Dark-Web-Portal	B	Schichtweise Verschlüsselung von Daten und Weiterleitung über drei Knoten.
3. Onion-Endung	C	Sicherer Backend-Speicher mit nicht indexierten Systemdatensätzen.
4. Tor-Routing	D	Kryptografisches Top-Level-Domain-Suffix, das in Tor-Netzwerken verwendet wird.
5. Indexierte Seiten	E	Der Eingangsknoten, über den man in das Tor-Netzwerk gelangt.
6. Anonymität der Nutzer	F	Inhalte des Surface Web, die von Google erfasst und durchsuchbar sind.
7. Private Datenbank	G	Öffentliche IP-Adressen von Clients vor Servern verborgen halten.
8. Eingangs-Gateway	H	Nicht indexierte Webinhalte wie private Logins, E-Mails und Datenbankeinträge.

Kontrollpunkt 5: Kreuzworträtsel

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



WAAGERECHT

3. Kryptografische Top-Level-Domain-Endung im Tor-Netzwerk (11)

6. Knoten, über den man in das Tor-Netzwerk einsteigt (14)

8. Gesicherter Backend-Speicher für nicht indexierte Systemeinträge (9)

SENKRECHT

1. Verschlüsseln von Daten in mehreren Schichten und Weiterleiten über drei Knoten (12)

2. Verbergen der öffentlichen IP-Adresse des Clients vor Servern (11)

4. Nicht indexierte Webinhalte wie private Logins, E-Mails und Datenbankeinträge (7)

5. Inhalte des Surface Web, die von Google erfasst und durchsuchbar sind (9)

7. Verschlüsselter Netzbereich, der nur über spezielle Browser erreichbar ist (7)

Kontrollpunkt 5, Alternative: Barrierefreie Kreuzworträtsel-Hinweise

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

WAAGERECHT

3 waagerecht: Kryptografische Top-Level-Domain-Endung im Tor-Netzwerk (11 Buchstaben):

6 waagerecht: Knoten, über den man in das Tor-Netzwerk einsteigt (14 Buchstaben):

8 waagerecht: Gesicherter Backend-Speicher für nicht indexierte Systemeinträge (9 Buchstaben):

SENKRECHT

1 senkrecht: Verschlüsseln von Daten in mehreren Schichten und Weiterleiten über drei Knoten (12 Buchstaben):

2 senkrecht: Verbergen der öffentlichen IP-Adresse des Clients vor Servern (11 Buchstaben):

4 senkrecht: Nicht indexierte Webinhalte wie private Logins, E-Mails und Datenbankeinträge (7 Buchstaben):

5 senkrecht: Inhalte des Surface Web, die von Google erfasst und durchsuchbar sind (9 Buchstaben):

7 senkrecht: Verschlüsselter Netzbereich, der nur über spezielle Browser erreichbar ist (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.

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

WORTSCHATZ-WORTLISTE

DEEPWEB DARKWEB ONIONENDUNG ONIONROUTING INDEXIERT
ANONYMITAET DATENBANK EINGANGSKNOTEN

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. DEEPWEB**
- **B. DARKWEB**
- **C. ONIONENDUNG**
- **D. ONIONROUTING**
- **E. INDEXIERT**
- **F. ANONYMITAET**
- **G. DATENBANK**
- **H. EINGANGSKNOTEN**

DEFINITIONEN UND ZUORDNUNGSFELDER

1. Verbergen der öffentlichen IP-Adresse des Clients vor Servern.
2. Gesicherter Backend-Speicher für nicht indexierte Systemeinträge.
3. Verschlüsseln von Daten in mehreren Schichten und Weiterleiten über drei Knoten.
4. Nicht indexierte Webinhalte wie private Logins, E-Mails und Datenbankeinträge.
5. Verschlüsselter Netzbereich, der nur über spezielle Browser erreichbar ist.
6. Kryptografische Top-Level-Domain-Endung im Tor-Netzwerk.
7. Knoten, über den man in das Tor-Netzwerk einsteigt.
8. Inhalte des Surface Web, die von Google erfasst und durchsuchbar sind.

Kontrollpunkt 7: Buchstabensalat

Bringen Sie die Buchstaben unten in die richtige Reihenfolge, um zentrale Begriffe der Cybersicherheit aufzudecken. Schreiben Sie Ihre Antworten in die vorgesehenen Eingabefelder.

1. PEDWBEE
2. NGNONEIUDNO
3. IIXNETERD
4. NKNEABDAT
5. WBKRDEA
6. GNTIRNUONOIO
7. TYANITAEOMN
8. GSTNKNINEGNEOA

Bonusaufgabe: Schnell denken

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

1	Gründe, sich vom Darknet fernzuhalten			
2	Dinge, die eine Suchmaschine nicht finden kann			
3	Geräte, die gehackt werden können			
4	Legale Gründe, Tor zu nutzen			
5	Gründe, Software zu aktualisieren			
6	Warnzeichen in einer E-Mail			
7	Dinge, die im Darknet illegal verkauft werden			
8	Personen, die Sie um IT-Hilfe bitten können			
9	Sichere Gewohnheiten, mit denen Sie heute beginnen können			
10	Dinge, die nach einem Datenleck zu tun sind			
11	Dinge, die zum Deep Web gehören			
12	Websites, die Sie mit einer Anmeldung nutzen			
13	Wörter rund um Anonymität			
14	Informationen, die Sie niemals weitergeben sollten			
15	Dinge, die „unter der Oberfläche“ liegen			

Kontrollpunkt 8: Fallstudien zur Cybersicherheit

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

FALLSTUDIE 1: ERKENNUNG VON DATENLECKS



Szenario: Bei einer Sicherheitsprüfung in einem Unternehmen wird festgestellt, dass sensible Kundendatensätze auf einem Onion-Marktplatz gehandelt werden. Die Daten sind bei Google nicht indexiert.

Diskussionsfrage: Erklären Sie, welche Bereiche des Webs betroffen sind und wie es zu diesem Leck kam.

FALLSTUDIE 2: ANONYMITÄT VS. MALWARE-RISIKEN



Szenario: Ein Analyst möchte Threat-Intelligence-Feeds auf einer Tor-Website einsehen. Er lädt den Tor-Browser herunter und ruft die Seite auf.

Diskussionsfrage: Bewerten Sie die Vorteile für die Anonymität und skizzieren Sie Maßnahmen zur Abwehr von Malware.

Kontrollpunkt 9: Entschlüsselung der Chiffre

Eine Fachkraft für Cybersicherheit schützt Netzwerkressourcen vor Bedrohungsakteuren im Internet. 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

1	14	15	14	25	13		2	12	5	9	2	5	14		4	21	18	3	8

19	9	3	8	5	18	5	19		15	14	9	15	14

18	15	21	20	9	14	7

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 zur Cybersicherheit (Teil A)

Sehen Sie sich häufige Fragen und Antworten zur Abwehr von Online-Bedrohungen an.

Q1: Was ist das Deep Web?

Das Deep Web umfasst alle Webseiten, die Suchmaschinen nicht indexieren können, darunter Online-Banking, E-Mail-Datenbanken und kostenpflichtige Fachzeitschriften.

Q2: Was ist das Darknet?

Das Dark Web ist ein kleiner Teilbereich des Deep Web, der absichtlich verborgen ist und nur über spezielle Browser mit Onion-Netzwerken erreichbar ist.

Q3: Wie indexieren Suchmaschinen Seiten?

Suchmaschinen setzen automatisierte Programme (Spider) ein, die öffentlichen Links folgen und Seiten indizieren, die das Crawling nicht über Robots-Anweisungen blockieren.

Q4: Warum gilt Online-Banking als Teil des Deep Web?

Banking-Portale liegen hinter Anmeldeseiten und Passwörtern, sodass öffentliche Suchmaschinen Kontoauszugsseiten nicht indexieren können.

Q5: Was ist das Onion-Routing des Tor-Browsers?

Onion-Routing ist ein Übertragungsverfahren, das Datenverkehr in Schichten verschlüsselt und über mehrere Relays leitet, um die IP-Adressen der Nutzer zu verbergen.

Kontrollpunkt 10: Grundlegende häufige Fragen zur Cybersicherheit (Teil B)

Sehen Sie sich häufige Fragen und Antworten zur Abwehr von Online-Bedrohungen an.

Q6: Ist der Zugriff auf das Darknet illegal?

Nein. Der Zugang zum Darknet ist in den meisten Ländern legal, die Teilnahme an illegalen Marktplätzen oder Cyberaktivitäten ist jedoch verboten.

Q7: Warum laden Darknet-Websites so langsam?

Der Datenverkehr wird über mindestens drei weltweite Relays (Eingang, Mitte, Ausgang) geleitet und entschlüsselt, was die Übertragungslatenz erhöht.

Q8: Was bedeutet die Domain-Endung .onion?

Es ist eine spezielle Top-Level-Domain-Endung im Tor-Netzwerk, die auf kryptografisch erzeugte Adressen statt auf normale DNS-Server verweist.

Q9: Welche Risiken sind mit Darknet-Links verbunden?

Die Websites haben keine Sicherheitsprüfung, wodurch Nutzer hohen Infektionsraten mit Schadsoftware, Phishing-Skripten und Betrug bei Transaktionen ausgesetzt sind.

Q10: Wer hat das Routing-Protokoll des Tor-Netzwerks entwickelt?

Die Technologie wurde ursprünglich in den 1990er-Jahren vom U.S. Naval Research Laboratory entwickelt, um Regierungskommunikation zu schützen.

Kontrollpunkt 10: Fortgeschrittene häufige Fragen zur Sicherheit (Teil C)

Erkunden Sie fortgeschrittene technische Aspekte von Sicherheits-Frameworks, Malware-Analyse und Daten-Compliance.

Q1: Wie schützen Zwischenknoten die Anonymität bei Tor?

Jeder Knoten entschlüsselt nur eine Schicht der Routing-Daten und erfährt nur den vorherigen und den nächsten Hop, niemals sowohl Quelle als auch Ziel.

Q2: Welche Rolle spielt der Ausgangsknoten?

Der Ausgangsknoten entschlüsselt die letzte Verschlüsselungsschicht und sendet den Datenverkehr an den öffentlichen Zielserver oder Onion-Server.

Q3: Was ist ein Gateway für Tor-Bridges?

Bridges sind nicht öffentlich gelistete Tor-Eingangsrelays, mit denen sich Sperren des Internetanbieters und Zensur in Regionen umgehen lassen, die den Zugang zum Tor-Browser einschränken.

Q4: Wie nutzen Akteure im Darknet Kryptowährungen aus?

Akteure nutzen anonyme Kryptowährungen, um auf Darknet-Marktplätzen Finanzgeschäfte abzuwickeln und dabei die üblichen Kontrollen von Banktransaktionen zu umgehen.

Q5: Warum können herkömmliche Suchmaschinen tiefe Datenbanken nicht durchsuchen?

Crawler können keine Anmeldedaten eingeben, keine Sicherheits-CAPTCHAs lösen und keine Backend-SQL-Abfrageskripte ausführen, die für den Zugriff auf tiefe Datenbanken erforderlich sind.

Kontrollpunkt 10: Fortgeschrittene häufige Fragen zur Sicherheit (Teil D)

Erkunden Sie fortgeschrittene technische Aspekte von Sicherheits-Frameworks, Malware-Analyse und Daten-Compliance.

Q6: Was ist ein Verzeichnisserver in Tor-Netzwerken?

Es ist ein vertrauenswürdiger Server, der die Liste der aktiven Eingangs-, Mittel- und Ausgangsrelais führt, aus denen Clients ihre Routing-Pfade aufbauen.

Q7: Wie spähen böswillige Akteure Daten an Exit-Knoten aus (Sniffing)?

Betreiber bösartiger Exit-Nodes können unverschlüsselten HTTP-Verkehr abfangen, wenn er das Tor-Netzwerk verlässt, und so Benutzernamen und Cookies stehlen.

Q8: Was ist der Unterschied zwischen Tor und I2P?

Tor nutzt ein zentrales Relay-Verzeichnis und Ausgangsknoten für den Zugriff auf das öffentliche Web, während I2P eine dezentrale Peer-to-Peer-Struktur für internes Hosting verwendet.

Q9: Wie verfolgen Strafverfolgungsbehörden Darknet-Marktplätze?

Behörden nutzen Blockchain-Analysen, ermitteln physische Server-Hosting-Standorte und führen Täuschungsoperationen durch, um Betreiber zu identifizieren.

Q10: Wie gefährdet ein DNS-Leak die Anonymität des Clients?

DNS-Leaks entstehen, wenn DNS-Anfragen des Browsers direkt über den lokalen Internetanbieter gesendet werden, statt durch das verschlüsselte Tor-Netzwerk geleitet zu werden.

Teil 11: 10 Fakten und Einblicke zur Cybersicherheit aus der Praxis

Lernen Sie reale Fakten zu Sicherheitsvorfällen, Abwehrmechanismen und Compliance-Standards kennen.

1. SICHERHEITS-EINBLICK

Das Deep Web ist weit größer als das durchsuchbare Surface Web, da die meisten Inhalte hinter Anmeldungen und in Datenbanken liegen.

2. SICHERHEITS-EINBLICK

Das Dark Web ist ein kleiner, absichtlich verborgener Teil des Deep Web, der mit Werkzeugen wie Tor erreicht wird.

3. SICHERHEITS-EINBLICK

Beim Tor-Routing werden Datenpakete dreifach verschlüsselt; an jedem Relay-Knoten wird wie bei einer Zwiebel eine Verschlüsselungsschicht abgeschält.

4. SICHERHEITS-EINBLICK

Tor ging aus dem Onion-Routing-Projekt des U.S. Naval Research Lab hervor, und sein Code wurde als freie Software veröffentlicht. [1]

5. SICHERHEITS-EINBLICK

Onion-Adressen sind 56-stellige alphanumerische Zeichenfolgen, die kryptografisch aus öffentlichen Schlüsselpaaren erzeugt werden.

6. SICHERHEITS-EINBLICK

Exit-Knoten können Klartext-Datenverkehr lesen, daher ist TLS/HTTPS auch bei Tor für sichere Sitzungsdaten weiterhin nötig.

7. SICHERHEITS-EINBLICK

Intranet-Seiten, Cloud-Laufwerke und private Datenbanken bilden die größten Datenspeicherbereiche im Deep Web.

8. SICHERHEITS-EINBLICK

Spezialisierte Suchmaschinen wie DuckDuckGo betreiben Onion-Portale, um anonyme Suchen im Tor-Netzwerk zu ermöglichen.

9. SICHERHEITS-EINBLICK

Über 2 Millionen Nutzer verbinden sich täglich mit dem Tor-Netzwerk, um Zensur zu umgehen und die Vertraulichkeit ihrer Kommunikation zu wahren.

10. SICHERHEITS-EINBLICK

Weltweite Polizeieinsätze (wie Operation Bayonet) haben große Darknet-Marktplätze durch die Beschlagnahme von Hosting-Hardware stillgelegt.

Technische Referenzen und Quellen

Der Lernleitfaden und die interaktiven Rätsel wurden aus globalen Standards von NIST und OWASP sowie aus Datenschutz-Compliance-Standards zusammengestellt.

WISSENSCHAFTLICHE UND FACHLICHE QUELLEN

[1] Tor Project. (n.d.). Why is it called Tor?

https://support.torproject.org/about/why-is-it-called-tor/

[2] Tor Project. (n.d.). How do Onion Services work?

https://community.torproject.org/onion-services/overview/

[3] Tor Project. (n.d.). Users – Tor Metrics.

https://metrics.torproject.org/userstats-relay-country.html

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

Lösungsschlüssel: Kontrollpunkt 1 – Auswahlaufgaben

1 **Indexierung durch Suchmaschinen** DEEP WEB — **Richtige Antwort: A**

HINWEIS FÜR LEHRKRÄFTE

Deep-Web-Seiten liegen hinter Anmeldeschranken und in Datenbanken, sodass Such-Crawler sie nicht erfassen können. Quelle: IETF RFC 3986.

2 **Tor-Zugang** DARK WEB — **Richtige Antwort: A**

HINWEIS FÜR LEHRKRÄFTE

Das Dark Web besteht aus versteckten Onion-Diensten, die nur über Browser wie Tor erreichbar sind. Quelle: IETF RFC 3986.

3 **Deep-Web-Datenbanken** DATENBANKEN — **Richtige Antwort: A**

HINWEIS FÜR LEHRKRÄFTE

Passwortgeschützte Konten und Unternehmensdaten bilden den größten Teil des Deep Web. Quelle: NIST Digital Identity.

4 **Onion-Routing** TOR-NETZWERK — **Richtige Antwort: A**

HINWEIS FÜR LEHRKRÄFTE

Onion-Routing verschlüsselt Datenpakete in Schichten und leitet sie zur Anonymisierung über mehrere Knoten weiter. Quelle: IETF RFC 3986.

5 **Onion-Domain** ENDUNG — **Richtige Antwort: A**

HINWEIS FÜR LEHRKRÄFTE

Die kryptografische Domain-Endung.onion leitet Datenverkehr innerhalb von Tor ohne öffentliches DNS weiter. Quelle: IETF RFC 3986.

Lösungsschlüssel: Kontrollpunkt 2 – Richtig oder Falsch

6 **Web-Segmente** STRUKTUR — **Richtige Antwort: Falsch**

HINWEIS FÜR LEHRKRÄFTE

Das Deep Web umfasst alle nicht indexierten Seiten, während das Dark Web ein kleiner, verschlüsselter Onion-Teilbereich ist. Quelle: IETF RFC 3986.

7 **Unternehmens-Intranets** DEEP WEB — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

Intranet-Seiten liegen hinter Passwortportalen und werden nicht indexiert, gehören also zum Deep Web. Quelle: NIST Digital Identity.

8 **Verschlüsselungsebene** RELAYS — **Richtige Antwort: Falsch**

HINWEIS FÜR LEHRKRÄFTE

Onion-Relays entschlüsseln jeweils nur eine Routing-Schicht, um die Anonymität der Nutzer zu schützen, nie das ganze Paket. Quelle: IETF RFC 3986.

9 **Gefährdung durch Malware** BEDROHUNGEN — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

Marktplätze im Dark Web haben keine Sicherheitsfilterung und bergen ein extrem hohes Risiko einer Malware-Infektion. Quelle: Center for Internet Security (CIS).

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

HINWEIS FÜR LEHRKRÄFTE

Gewöhnliche Suchmaschinen-Crawler nutzen kein Tor und können .onion-Seiten daher weder erreichen noch indexieren.

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. Segment des Deep Web	A 2. Dark-Web-Portal	D 3. Onion-Endung	B 4. Tor-Routing
F 5. Indexierte Seiten	G 6. Anonymität der Nutzer	C 7. Private Datenbank	E 8. Eingangs-Gateway

KONTROLLPUNKT 3: LÖSUNG SCHLÜSSELBEGRIFFE

1 DEEP WEB	2 DARK WEB	3 .ONION	4 ONION-ROUTING
5 INDEXIERT	6 ANONYMITÄT		

KONTROLLPUNKT 6, ALTERNATIVE: LÖSUNG WORTZUORDNUNG

1 F – ANONYMITAET	2 G – DATENBANK	3 D – ONIONROUTING	4 A – DEEPWEB
5 B – DARKWEB	6 C – ONIONENDUNG	7 H – EINGANGSKNOTEN	8 E – INDEXIERT

DISKUSSIONSHINWEISE FÜR LEHRKRÄFTE

Schlüsselbegriffe:
Prüfen Sie, ob die Lernenden Segment des Deep Web, Dark-Web-Portal und Onion-Endung 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

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

KREUZWORTRÄTSEL-LÖSUNG

								O						
		A			O	N	I	O	N	E	N	D	U	N	G
		N							I						
D		O			I				O						
E	I	N	G	A	N	G	S	K	N	O	T	E	N		
E		Y			D				R						D
P		M			E				O						A
W		I			X				U						R
E		T			I		D	A	T	E	N	B	A	N	K
B		A			E				I						W
		E			R				N						E
		T			T				G						B

LEITFADEN FÜR LEHRKRÄFTE ZU DEN KREUZWORTRÄTSEL-LÖSUNGEN

WAAGERECHT

3 waagerecht: ONIONENDUNG Kryptografische Top-Level-Domain-Endung im Tor-Netzwerk (11 Buchstaben)

6 waagerecht: EINGANGSKNOTEN Knoten, über den man in das Tor-Netzwerk einsteigt (14 Buchstaben)

8 waagerecht: DATENBANK Gesicherter Backend-Speicher für nicht indexierte Systemeinträge (9 Buchstaben)

SENKRECHT

1 senkrecht: ONIONROUTING Verschlüsseln von Daten in mehreren Schichten und Weiterleiten über drei Knoten (12 Buchstaben)

2 senkrecht: ANONYMITAET Verbergen der öffentlichen IP-Adresse des Clients vor Servern (11 Buchstaben)

4 senkrecht: DEEPWEB Nicht indexierte Webinhalte wie private Logins, E-Mails und Datenbankeinträge (7 Buchstaben)

5 senkrecht: INDEXIERT Inhalte des Surface Web, die von Google erfasst und durchsuchbar sind (9 Buchstaben)

7 senkrecht: DARKWEB Verschlüsselter Netzbereich, der nur über spezielle Browser erreichbar ist (7 Buchstaben)

Lösungsschlüssel für Buchstabensalat und Chiffre

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

LÖSUNGSSCHLÜSSEL BUCHSTABENSALAT

1. PEDWBEE — **DEEPWEB**
2. NGNONEIUDNO — **ONIONENDUNG**
3. IIXNETERD — **INDEXIERT**
4. NKNEABDAT — **DATENBANK**
5. WBKRDEA — **DARKWEB**
6. GNTIRNUONOIO — **ONIONROUTING**
7. TYANITAEOMN — **ANONYMITAET**
8. GSTNKNINEGNEOA — **EINGANGSKNOTEN**

LÖSUNGSSCHLÜSSEL ZUR GEHEIMEN CHIFFRE-AUFGABE

"ANONYM BLEIBEN DURCH SICHERES ONION ROUTING"

Lösungsschlüssel zu den Fallstudien

A Fallstudie 1: Erkennung von Datenlecks

Lösung für Lehrkräfte

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Szenarioanalyse: Bei einem Sicherheitsaudit im Unternehmen wird entdeckt, dass sensible Datensätze aus der Kundendatenbank auf einem Onion-Marktplatz gehandelt werden. Die Daten sind bei Google nicht indexiert.
- Empfohlene Strategie und Lösung: Beteiligte Bereiche: Die private Datenbank gehört zum Deep Web (nicht indexiert, aber gesichert). Der Marktplatz, auf dem die gestohlenen Daten gehandelt werden, befindet sich im Dark Web (Onion-Netzwerk). Wie es dazu kam: Hacker umgingen die Serverabwehr, stahlen die Datenbank aus dem Deep Web und boten sie anonym im Dark Web an, um sich der Verfolgung durch Strafverfolgungsbehörden zu entziehen.

B Fallstudie 2: Anonymität vs. Malware-Risiken

Lösung für Lehrkräfte

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Szenarioanalyse: Ein Analyst möchte Threat-Intelligence-Feeds auf einer Tor-Website prüfen. Er lädt den Tor-Browser herunter und ruft die Website auf.
- Empfohlene Strategie und Lösung: Vorteile: Tor leitet den Traffic über drei Knoten und verbirgt so die Unternehmens-IP des Analysten. Risiken und Abhilfe: Darknet-Links werden nicht auf ihre Seriosität geprüft. Analysten müssen Tor in isolierten virtuellen Maschinen (VMs) ausführen, Javascript in den Tor-Einstellungen deaktivieren und keine Dateien herunterladen, um das Unternehmensnetzwerk zu schützen.