Name: _____ Datum: _____ Punkte: _____

Passwort-Leaks und Sicherheit von Zugangsdaten

Credential Stuffing, Datenpannen, Hash-Algorithmen, Multi-Faktor-Authentifizierung und Passwortsicherheit.

LERNÜBERSICHT PASSWORT-LEAKS

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 Passwortlecks und Sicherheit von Zugangsdaten. Sie lernen Credential Stuffing, Datenpannen, Hash-Algorithmen, Multi-Faktor-Authentifizierung und Passwortmanager 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/passwoerter-leak/

Ihr Lernfahrplan: Passwortsicherheit

- Risiken offengelegter Zugangsdaten in Dark-Web-Foren verstehen.
- Multi-Faktor-Authentifizierung (MFA) und Überwachung kompromittierter Zugangsdaten einführen.
- Entwerfen Sie Sicherheitsmaßnahmen für Unternehmen gegen gezielte Social-Engineering-Betrugsversuche.

ANLEITUNG ZUM LEITFADEN PASSWORT-LEAKS

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: Schutz von Zugangsdaten. Zum Schluss folgt die Bonusaufgabe Schnell denken.

PASSWORT-LEAKS UND SICHERHEIT VON ZUGANGSDATEN (EINFÜHRUNG)

Bei Passwort-Leaks werden Zugangsdaten von Nutzern auf öffentlichen Websites und im Darknet offengelegt. Eindeutige Passwörter aus einem Passwortmanager, die Prüfung auf bereits geleakte Passwörter und Multi-Faktor-Authentifizierung (MFA) verringern das Risiko von Credential Stuffing, während gesalzenes, langsames Passwort-Hashing den Schaden begrenzt, falls eine Passwortdatenbank gestohlen wird.

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

Kontrollpunkt 1: Auswahlaufgaben

1 **1. Was ist Credential Stuffing?**

- A. Automatisiertes Ausprobieren geleakter Kombinationen aus Benutzername und Passwort auf mehreren Websites
- B. Verschlüsseln lokaler Datenbankspeicherdateien
- C. Überlasten von Webservern mit Netzwerkanfragen
- D. Heimliches Überwachen von Tastatureingaben

2 **2. Welchen Algorithmus nennt OWASP heute als erste Wahl für die Speicherung von Passwörtern?**

- A. Argon2id
- B. MD5
- C. SHA-1
- D. ROT13

3 **3. Wie verringert die Multi-Faktor-Authentifizierung (MFA) das Risiko durch geleakte Passwörter?**

- A. Sie erfordert einen zusätzlichen Verifizierungsfaktor, sodass ein gestohlenes Passwort allein nicht ausreicht
- B. Sie ändert das Passwort automatisch jede Stunde
- C. Sie verschlüsselt den Benutzernamen während der Übertragung
- D. Sie meldet betrügerische Anfragen an die Kreditauskunftei

4 **4. Was ist ein Datenleck-Dump?**

- A. Eine Sammlung geleakter Zugangsdaten, die online veröffentlicht oder in Hackerforen verkauft wird
- B. Eine extern gespeicherte Sicherungskopie der Datenbankdateien
- C. Ein temporärer Cache von Webserver-Protokollen
- D. Ein Verwaltungswerkzeug zum Zurücksetzen von Benutzerpasswörtern

5 **5. Welche Rolle spielt ein Passwort-Manager?**

- A. Erzeugen und Speichern einzigartiger, starker Passwörter für jedes Konto
- B. Überwachen des Netzwerkverkehrs auf Passwortlecks
- C. Blockieren automatisierter Brute-Force-Angriffe am Gateway
- D. Durchsuchen von Datenbank-Speicherblöcken nach unverschlüsselten Passwörtern

Kontrollpunkt 2: Richtig oder falsch

6 Frage 6

6. Die Wiederverwendung von Passwörtern für mehrere Konten erhöht das Risiko von Credential Stuffing.

○ Richtig ○ Falsch

7 Frage 7

7. SHA-1 ist eine empfohlene Hashfunktion für die moderne Speicherung von Passwörtern.

○ Richtig ○ Falsch

8 Frage 8

8. Allein die Durchsetzung komplexer Passwörter (ohne MFA) stoppt Credential Stuffing vollständig.

○ Richtig ○ Falsch

9 Frage 9

9. Dark-Web-Monitoring-Tools durchsuchen das Internet nach kompromittierten Unternehmenszugangsdaten.

○ Richtig ○ Falsch

10 Frage 10

10. Gesalzene Hashes fügen Passwörtern vor dem Hashen eindeutige Zufallsdaten hinzu, um Rainbow-Table-Angriffe zu vereiteln.

○ 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. Das Durchprobieren geleakter Zugangsdaten bei vielen Webanwendungen heißt Credential _____ .

2. Ein langsamer, adaptiver Hash-Algorithmus für Passwörter, den OWASP weiterhin akzeptiert, ist _____ .

3. Die Offenlegung vertraulicher Datenbankdateien im Internet ist eine _____ .

4. Das Hinzufügen zufälliger Werte zu Passwörtern vor dem Hashing nennt man _____ .

5. Eine sichere lokale Datenbank für Zugangsdaten ist ein _____ für Passwörter.

6. Für einen zweiten Prüfschritt bei der Anmeldung nutzt man _____ .

WORTSCHATZ-WORTBANK

BCRYPT | DATENPANNE | MANAGER | MFA | PHISHING | RAINBOW TABLE | SALTING | STUFFING

Schreiben Sie Ihre Antworten hier:

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

Kontrollpunkt 4: Zuordnung von Sicherheits-Begriffen

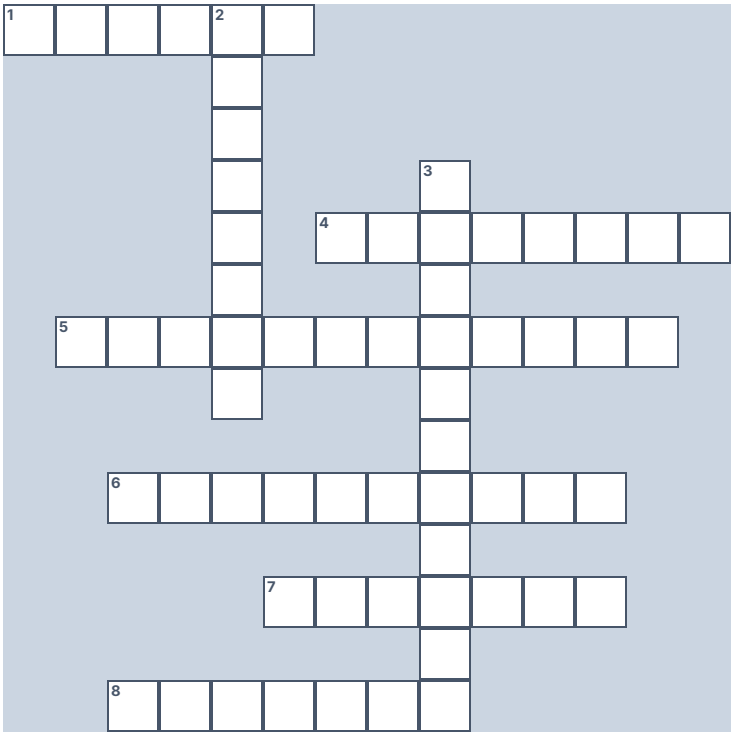
DEFINITIONEN ZUORDNEN

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

☐	1. STUFFING	A	Vorberechnete Tabelle mit Passwort-Hashes.
☐	2. BCRYPT	B	Anmeldeprüfung mit mehreren Faktoren.
☐	3. DATENPANNE	C	Werkzeug zur Speicherung von Zugangsdaten.
☐	4. SALTING	D	Unbefugte Offenlegung von Datenbanken.
☐	5. MANAGER	E	Social Engineering zum Stehlen von Anmeldedaten.
☐	6. MFA	F	Testen geleakter Zugangsdaten.
☐	7. RAINBOW	G	Hinzufügen eines zufälligen Salts zum Passwort-Hash.
☐	8. PHISHING	H	Langsamer Algorithmus zum Hashen von Passwörtern.

Kontrollpunkt 5: Kreuzworträtsel

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



WAAGERECHT

1. Langsamer Hash-Algorithmus für Passwörter. (6)

4. Testen geleakter Zugangsdaten. (8)

5. Vorab berechnete Sammlung von Passwort-Hashes. (12)

6. Unbefugte Offenlegung einer Datenbank. (10)

7. Hinzufügen eines zufälligen Salts zum Passwort-Hash. (7)

8. Werkzeug zur Speicherung von Zugangsdaten. (7)

SENKRECHT

2. Social Engineering zum Stehlen von Anmeldedaten. (8)

3. Anmeldeprüfung mit mehreren Faktoren. (11)

Kontrollpunkt 5, Alternative: Barrierefreie Kreuzworträtsel-Hinweise

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

WAAGERECHT

1 waagerecht: Langsamer Hash-Algorithmus für Passwörter. (6 Buchstaben):

4 waagerecht: Testen geleakter Zugangsdaten. (8 Buchstaben):

5 waagerecht: Vorab berechnete Sammlung von Passwort-Hashes. (12 Buchstaben):

6 waagerecht: Unbefugte Offenlegung einer Datenbank. (10 Buchstaben):

7 waagerecht: Hinzufügen eines zufälligen Salts zum Passwort-Hash. (7 Buchstaben):

8 waagerecht: Werkzeug zur Speicherung von Zugangsdaten. (7 Buchstaben):

SENKRECHT

2 senkrecht: Social Engineering zum Stehlen von Anmeldedaten. (8 Buchstaben):

3 senkrecht: Anmeldeprüfung mit mehreren Faktoren. (11 Buchstaben):

Kontrollpunkt 6: Suchsel

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

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

WORTSCHATZ-WORTLISTE

STUFFING BCRYPT DATENPANNE SALTING MANAGER MULTIFAKTOR RAINBOWTABLE PHISHING

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. STUFFING**
- **B. BCRYPT**
- **C. DATENPANNE**
- **D. SALTING**
- **E. MANAGER**
- **F. MULTIFAKTOR**
- **G. RAINBOWTABLE**
- **H. PHISHING**

DEFINITIONEN UND ZUORDNUNGSFELDER

1. Social Engineering zum Stehlen von Anmeldedaten.
2. Unbefugte Offenlegung einer Datenbank.
3. Langsamer Hash-Algorithmus für Passwörter.
4. Vorab berechnete Sammlung von Passwort-Hashes.
5. Testen geleakter Zugangsdaten.
6. Hinzufügen eines zufälligen Salts zum Passwort-Hash.
7. Werkzeug zur Speicherung von Zugangsdaten.
8. Anmeldeprüfung mit mehreren Faktoren.

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. NFFSITGU
2. NEDANEANPT
3. AMGRNEA
4. LTBIWEOBARAN
5. YRTBPC
6. NLISTGA
7. KIMUARTOLFT
8. SHHGPNII

Bonusaufgabe: Schnell denken

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

1	Sichere Gewohnheiten, mit denen Sie heute beginnen können			
2	Regeln für ein starkes Passwort			
3	Passwort-Manager, die Sie kennen			
4	Sicherheitswerkzeuge, die Sie kennen			
5	Warnzeichen in einer E-Mail			
6	Lustige Wörter für eine lange Passphrase			
7	Möglichkeiten, sich ohne Passwort anzumelden			
8	Informationen, die Sie niemals weitergeben sollten			
9	Gründe, Software zu aktualisieren			
10	Dinge, die zu tun sind, wenn ein Passwort geleakt wird			
11	Konten, die MFA brauchen			
12	Orte, an denen Passwörter niemals gespeichert werden sollten			
13	Anzeichen, dass ein Computer infiziert ist			
14	Schlechte Passwörter, die Menschen verwenden			
15	Dinge, von denen Sie ein Backup machen			

Kontrollpunkt 8: Fallstudien zur Cybersicherheit

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

FALLSTUDIE 1: BEHEBUNG EINES LECKS VON UNTERNEHMENSZUGANGSDATEN

👷

Szenario: Ein Darknet-Überwachungsdienst warnt eine Organisation, dass ein Datenbank-Dump mit Passwörtern von Systemadministratoren des Unternehmens online veröffentlicht wurde.

Diskussionsfrage: Analysieren Sie die Risiken des Lecks von Zugangsdaten und schlagen Sie eine Strategie zum Zurücksetzen der Administratorkonten vor.

FALLSTUDIE 2: EINFÜHRUNG VON STANDARDS FÜR PASSWORT-HASHING

👷

Szenario: Eine Unternehmensdatenbank speichert Nutzerpasswörter derzeit als veraltete MD5-Hashes ohne kryptografischen Salt, wodurch sie schnell geknackt werden können.

Diskussionsfrage: Entwerfen Sie eine Migrationsstrategie, um den Hash-Algorithmus der Datenbank zu modernisieren.

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

19	3	8	21	5	20	26	5	14		19	9	5

16	1	19	19	23	15	5	18	20	5	18		13	9	20

13	21	12	20	9	6	1	11	20	15	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 zur Cybersicherheit (Teil A)

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

Q1: Was ist ein Passwort-Leak?

Ein Passwortleck entsteht, wenn Anmeldedaten von Nutzern durch Datenpannen oder fehlerhafte Serverkonfigurationen offengelegt werden.

Q2: Wie finden Hacker geleakte Passwörter?

Hacker durchsuchen Darknet-Foren, öffentliche Datenbank-Dumps und Paste-Sites, auf denen Daten aus Datenpannen veröffentlicht werden [8].

Q3: Ist die Wiederverwendung von Passwörtern gefährlich?

Ja, denn wenn eine Website kompromittiert wird, können Hacker dieselben Anmeldedaten auf Tausenden anderen Plattformen ausprobieren [3].

Q4: Was ist ein kryptografisches Salt?

Ein Salt sind Zufallsdaten, die einem Passwort vor dem Hashen hinzugefügt werden, wodurch Angriffe mit vorberechneten Tabellen wirkungslos werden [2].

Q5: Warum ist MD5 veraltet?

MD5 ist ein schneller, veralteter Allzweck-Hash, sodass Angreifer Passwort-Vermutungen extrem schnell testen können, besonders wenn die Hashes ungesalzen sind [2].

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

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

Q6: Wie schützt ein Passwort-Manager die Nutzer?

Er erzeugt automatisch komplexe, eindeutige Zugangsdaten für jede Website und verringert so Gedächtnisfehler und Wiederverwendung.

Q7: Was ist ein Brute-Force-Angriff?

Ein Angriff, der systematisch jede mögliche Zeichenkombination ausprobiert, bis das richtige Passwort gefunden ist [4].

Q8: Wie hilft eine Kontosperre nach Fehlversuchen?

Kontosperren oder Ratenbegrenzung verlangsamen wiederholtes Online-Raten und verringern zusammen mit Überwachung und MFA das Risiko von Brute-Force-Angriffen [4].

Q9: Sind Master-Passwörter sicher?

Sie sind sicher, wenn es Passphrasen mit hoher Entropie sind, die nie auf anderen Websystemen wiederverwendet werden.

Q10: Sollten Passwörter regelmäßig geändert werden?

Laut NIST sollen keine regelmäßigen Änderungen erzwungen werden; Passwörter werden bei Hinweisen auf eine Kompromittierung geändert, und Vorrang haben Länge, Sperrlisten und MFA [1].

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

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

Q1: Wie schneidet Argon2 im Vergleich zu bcrypt ab?

OWASP nennt Argon2id als erste Wahl; seine speicherintensiven Einstellungen widerstehen dem Knacken mit GPUs und ASICs besser als bcrypt [2].

Q2: Was ist Key Stretching?

Ein Verfahren, das einen Hash-Algorithmus tausendfach wiederholt, um die Passwortprüfung zu verlangsamen und das Knacken teuer zu machen [2].

Q3: Wie funktionieren Rainbow Tables?

Es sind vorberechnete Nachschlagetabellen, die Klartext-Passwörter mit ihren Hashes verknüpfen und genutzt werden, um ungesalzene Hashes schnell umzukehren [2].

Q4: Was ist Credential Recycling?

Wiederverwendung gestohlener Kombinationen aus Benutzername und Passwort aus einem Datenleck, um Zugang zu anderen Diensten zu erlangen, insbesondere wenn Personen Passwörter mehrfach verwendet haben [3].

Q5: Können Passwort-Manager gehackt werden?

Ja. Viele verwenden Zero-Knowledge-Verschlüsselung, sodass ein Server-Einbruch nur verschlüsselte Tresore offenlegt; schwache Master-Passwörter können jedoch trotzdem offline geknackt werden.

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 Wörterbuchangriff?

Eine Variante des Brute-Force-Angriffs, die statt zufälliger Buchstaben gängige Wörter, Phrasen und früher geleakte Passwörter ausprobiert.

Q7: Warum werden Passphrasen bevorzugt?

Passphrasen bestehen aus mehreren zufälligen Wörtern und erzeugen eine hohe Entropie, die für Menschen leicht zu merken, aber rechnerisch aufwendig zu knacken ist [1].

Q8: Wie wirkt sich Single Sign-On (SSO) auf Passwortlecks aus?

SSO verringert die Zahl der Passwörter, doch der Identitätsanbieter wird zu einem besonders lohnenden Ziel, das eine starke, möglichst phishing-resistente MFA benötigt [6].

Q9: Was ist Session-Hijacking?

Ein Angreifer verschafft sich ein gültiges Sitzungstoken oder missbraucht es, um sich als angemeldeter Nutzer auszugeben, ohne das Passwort erneut zu benötigen [5].

Q10: Wie erkennt man Password Spraying?

Durch Suche nach denselben wenigen Passwörtern, die bei vielen Konten ausprobiert werden, oft langsam, um unter den Sperrschwellen zu bleiben [7].

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

NIST SP 800-63B verlangt, neue Passwörter mit Sperrlisten gängiger und kompromittierter Passwörter abzugleichen [1].

2. SICHERHEITS-EINBLICK

Der Datenleak 'Collection #1' aus dem Jahr 2019 führte Daten aus vielen früheren Datenlecks zu einer riesigen Datei mit Paaren aus E-Mail-Adresse und Passwort zusammen [8].

3. SICHERHEITS-EINBLICK

Das NIST verlangt inzwischen, dass Passwörter, die als einziger Authentifizierungsfaktor dienen, mindestens 15 Zeichen lang sind [1].

4. SICHERHEITS-EINBLICK

ASIC-Hardware kann Milliarden SHA-256-Hashes pro Sekunde berechnen, weshalb einfaches SHA-Hashing für Nutzerpasswörter unsicher ist [2].

5. SICHERHEITS-EINBLICK

Eindeutige Salts bewirken, dass zwei Nutzer mit genau demselben Passwort unterschiedliche Hashes in der Datenbank erhalten [2].

6. SICHERHEITS-EINBLICK

Viele Passwort-Manager verschlüsseln die Tresordaten lokal mit starker Kryptografie, die aus dem Master-Passwort des Nutzers abgeleitet wird.

7. SICHERHEITS-EINBLICK

Credential Stuffing funktioniert, weil viele Menschen dasselbe Passwort für Onlineshopping-, Banking- und E-Mail-Konten verwenden [3].

8. SICHERHEITS-EINBLICK

Laut NIST SP 800-63B dürfen Prüfstellen keine regelmäßigen Passwortänderungen verlangen, sondern nur Änderungen nach Hinweisen auf eine Kompromittierung [1].

9. SICHERHEITS-EINBLICK

Ein zusätzlicher Großbuchstabe und ein Sonderzeichen in einem kurzen Passwort halten moderne automatisierte GPU-Wörterbuchangriffe nicht auf [1].

10. SICHERHEITS-EINBLICK

MFA kann viele Credential-Stuffing-Versuche auch nach einem Passwort-Leak blockieren; Phishing-resistente MFA ist stärker als SMS-Codes [3].

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] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.

https://pages.nist.gov/800-63-4/sp800-63b.html

[2] OWASP. (n.d.). Password Storage Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

[3] OWASP. (n.d.). Credential Stuffing Prevention Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html

[4] OWASP. (n.d.). Authentication Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

[5] OWASP. (n.d.). Session Management Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

[6] CISA. (2022). Implementing Phishing-Resistant MFA (fact sheet).

https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

[7] CISA. (2018). Brute Force Attacks Conducted by Cyber Actors (Alert TA18-086A).

https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors

[8] Hunt, T. (2019). The 773 Million Record "Collection #1" Data Breach. Troy Hunt.

https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

Lösungsschlüssel: Kontrollpunkt 1 – Auswahlaufgaben

1 Frage 1

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Beim Credential Stuffing werden geleakte Kombinationen aus Benutzername und Passwort automatisiert auf anderen Websites ausprobiert [3].

2 Frage 2

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

OWASP empfiehlt in erster Linie Argon2id; bcrypt ist vor allem für Altsysteme gedacht, in denen Argon2id oder scrypt nicht verfügbar sind [2].

3 Frage 3

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

MFA erfordert einen zusätzlichen Faktor, daher kann ein gestohlenes Passwort allein das Konto nicht entsperren [3].

4 Frage 4

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Breach Dumps sind Sammlungen geleakter Zugangsdaten, etwa die Zusammenstellung Collection #1 von 2019 [8].

5 Frage 5

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Ein Passwort-Manager erzeugt und speichert für jedes Konto ein einzigartiges, starkes Passwort und verhindert so die Wiederverwendung [3].

Lösungsschlüssel: Kontrollpunkt 2 – Richtig oder Falsch

6 Frage 6

Richtige Antwort: Richtig

HINWEIS FÜR LEHRKRÄFTE

Richtig: Wiederverwendete Passwörter ermöglichen es Angreifern, auf einer Website geleakte Zugangsdaten auf anderen Websites erneut einzusetzen [3].

7 Frage 7

Richtige Antwort: Falsch

HINWEIS FÜR LEHRKRÄFTE

Falsch: SHA-1 ist ein schneller Hash; OWASP empfiehlt stattdessen Argon2id, scrypt, bcrypt oder PBKDF2 [2].

8 Frage 8

Richtige Antwort: Falsch

HINWEIS FÜR LEHRKRÄFTE

Falsch: Komplexitätsregeln allein können Stuffing mit wiederverwendeten geleakten Passwörtern nicht verhindern; MFA ist erforderlich [3].

9 Frage 9

Richtige Antwort: Richtig

HINWEIS FÜR LEHRKRÄFTE

Richtig: Überwachungsdienste durchsuchen Breach Dumps und Quellen im Darknet nach offengelegten Zugangsdaten [8].

10 Frage 10

Richtige Antwort: Richtig

HINWEIS FÜR LEHRKRÄFTE

Richtig: Ein eindeutiger Salt pro Passwort macht vorberechnete Rainbow Tables wirkungslos [2].

Vokabelschlüssel und Bewertungsraster

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

KONTROLLPUNKT 4: LÖSUNG BEGRIFFSZUORDNUNG

F 1. STUFFING	H 2. BCRYPT	D 3. DATENPANNE	G 4. SALTING
C 5. MANAGER	B 6. MFA	A 7. RAINBOW	E 8. PHISHING

KONTROLLPUNKT 3: LÖSUNG SCHLÜSSELBEGRIFFE

1 STUFFING	2 BCRYPT	3 DATENPANNE	4 SALTING
5 MANAGER	6 MFA		

KONTROLLPUNKT 6, ALTERNATIVE: LÖSUNG WORTZUORDNUNG

1 H – PHISHING	2 C – DATENPANNE	3 B – BCRYPT	4 G – RAINBOWTABLE
5 A – STUFFING	6 D – SALTING	7 E – MANAGER	8 F – MULTIFAKTOR

DISKUSSIONSHINWEISE FÜR LEHRKRÄFTE

Schlüsselbegriffe:
Prüfen Sie, ob die Lernenden STUFFING, BCRYPT und DATENPANNE 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.

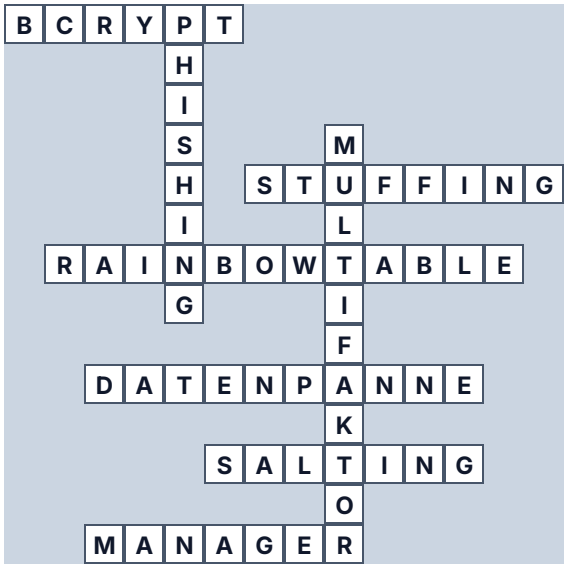
Quellenbewertung:
Lassen Sie die Lernenden mindestens eine Aussage anhand der Quellen des Arbeitsblatts prüfen und besprechen Sie, warum sich Zahlen, Preise und Regeln mit der Zeit ändern können.

Rätsellösungen und Hinweise für Lehrkräfte

LÖSUNG DES SUCHSELS

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

KREUZWORTRÄTSEL-LÖSUNG



LEITFADEN FÜR LEHRKRÄFTE ZU DEN KREUZWORTRÄTSEL-LÖSUNGEN

WAAGERECHT

1 waagerecht: BCRYPT Langsamer Hash-Algorithmus für Passwörter. (6 Buchstaben)

4 waagerecht: STUFFING Testen geleakter Zugangsdaten. (8 Buchstaben)

5 waagerecht: RAINBOWTABLE Vorab berechnete Sammlung von Passwort-Hashes. (12 Buchstaben)

6 waagerecht: DATENPANNE Unbefugte Offenlegung einer Datenbank. (10 Buchstaben)

7 waagerecht: SALTING Hinzufügen eines zufälligen Salts zum Passwort-Hash. (7 Buchstaben)

8 waagerecht: MANAGER Werkzeug zur Speicherung von Zugangsdaten. (7 Buchstaben)

SENKRECHT

2 senkrecht: PHISHING Social Engineering zum Stehlen von Anmeldedaten. (8 Buchstaben)

3 senkrecht: MULTIFAKTOR Anmeldeprüfung mit mehreren Faktoren. (11 Buchstaben)

Lösungsschlüssel für Buchstabensalat und Chiffre

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

LÖSUNGSSCHLÜSSEL BUCHSTABENSALAT

1. NFFSITGU — **STUFFING**
2. NEDANEANPT — **DATENPANNE**
3. AMGRNEA — **MANAGER**
4. LTBIWEOBARAN — **RAINBOWTABLE**
5. YRTBPC — **BCRYPT**
6. NLISTGA — **SALTING**
7. KIMUARTOLFT — **MULTIFAKTOR**
8. SHHGPNII — **PHISHING**

LÖSUNGSSCHLÜSSEL ZUR GEHEIMEN CHIFFRE-AUFGABE

"SCHUETZEN SIE PASSWOERTER MIT MULTIFAKTOR"

Lösungsschlüssel zu den Fallstudien

A Fallstudie 1: Behebung eines Lecks von Unternehmenszugangsdaten

Lösung für Lehrkräfte

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Szenarioanalyse: Ein Dark-Web-Überwachungsdienst warnt eine Organisation, dass ein Datenbank-Dump mit Passwörtern ihrer Systemadministratoren online veröffentlicht wurde.
- Empfohlene Strategie und Lösung: Widerrufen Sie alle aktiven Administratorsitzungen und setzen Sie die Zugangsdaten mit einem Generator für hohe Entropie neu. Setzen Sie für Admin-Portale phishing-resistente MFA durch [6], tauschen Sie betroffene API-Schlüssel aus, prüfen Sie die Anmeldeprotokolle, ermitteln Sie die ursprüngliche Offenlegung und überprüfen Sie andere privilegierte Konten.

B Fallstudie 2: Einführung von Standards für Passwort-Hashing

Lösung für Lehrkräfte

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Szenarioanalyse: Eine Unternehmensdatenbank speichert Benutzerpasswörter derzeit als veraltete MD5-Hashes ohne kryptografisches Salt, wodurch sie sich schnell auslesen lassen.
- Empfohlene Strategie und Lösung: Führen Sie Argon2id (oder bcrypt auf Altsystemen) mit einem eindeutigen Salt pro Benutzer ein [2]. Verpacken Sie vorhandene MD5-Hashes sofort mit dem neuen Algorithmus, hashen Sie bei der nächsten Anmeldung jedes Benutzers direkt neu und erzwingen Sie für lange inaktive Konten ein Zurücksetzen.