Name: _____ Datum: _____ Punkte: _____

Schutz vor Identitätsdiebstahl und Sicherung Sicherheitsleitfaden

Datenlecks bei Zugangsdaten, MFA, Dark-Web-Überwachung, Warnungen zur Sperre der Kreditauskunft, Social Engineering

LERNÜBERSICHT: SCHUTZ VOR IDENTITÄTSDIEBSTAHL

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 Vorbeugung gegen Identitätsdiebstahl und die Schadensbegrenzung. Sie lernen Lecks von Zugangsdaten, Multi-Faktor-Authentifizierung, Überwachung des Darknets, Warnungen bei Kreditsperren und die Abwehr von Social Engineering 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/identitaetsdiebstahl/

Ihr Lernfahrplan: Identitätsschutz

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

ANLEITUNG: LEITFADEN ZU IDENTITÄTSDIEBSTAHL

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: Identitätsschutz. Zum Schluss folgt die Bonusaufgabe Schnell denken.

SCHUTZ VOR IDENTITÄTSDIEBSTAHL UND SICHERUNG VON VERMÖGENSWERTEN (EINFÜHRUNG)

Identitätsdiebstahl nutzt geleakte Zugangsdaten und schwache Anmeldungen aus, um private und geschäftliche Konten zu kapern. MFA, Kreditsperren, Darknet-Scanner und die Rahmenwerke SPF/DKIM/DMARC bilden eine wichtige Verteidigung gegen digitalen Identitätsmissbrauch.

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

Kontrollpunkt 1: Auswahlaufgaben

1. Mit welcher Methode stehlen Identitätsdiebe am häufigsten Anmeldedaten?

- A. Versenden gefälschter E-Mail-Warnungen, die Nutzer dazu bringen, Passwörter auf nachgeahmten Portalen einzugeben
- B. Abhören von Radiosendungen in der Nähe des Firmenbüros eines Nutzers
- C. Defragmentieren des lokalen Serverlaufwerks eines Nutzers
- D. Trennen externer Netzwerk-Backup-Konfigurationen

2. Welche Sicherheitsmaßnahme bietet den stärksten Schutz vor dem Durchsickern von Anmeldedaten?

- A. Multi-Faktor-Authentifizierung mit Hardwareschlüsseln
- B. Erstellen langer Passwörter in Standard-Browserformaten
- C. Ändern der E-Mail-Benutzernamen alle sechs Monate
- D. Löschen gespeicherter Browserverläufe mit Tracking-Cookies

3. Was beschreibt das Einfrieren der Kreditauskunft (Credit Freeze)?

- A. Sperren von Kreditauskünften, damit Diebe keine unbefugten Kredite aufnehmen können
- B. Löschen von Transaktionsverläufen von Bankkonten aus Datenbanken
- C. Deaktivieren der Magnetstreifenleser für Kreditkarten an Lesegeräten
- D. Verschlüsseln lokaler Datenbankfestplatten im Ruhezustand

4. Warum ist eine Überwachung des Dark Web nützlich?

- A. Es warnt Nutzer, wenn ihre geleakten Zugangsdaten in illegalen Datenbanken auftauchen
- B. Es verhindert, dass aktive Schadsoftware in virtuellen Sandboxes ausgeführt wird
- C. Es beschleunigt das Browser-Routing in virtuellen Netzwerken
- D. Es blockiert SQL-Injection-Zugriffsversuche auf Backend-Datenbanken

5. Was bedeutet Social Engineering?

- A. Menschen so manipulieren, dass sie vertrauliche Zugangsdaten freiwillig preisgeben
- B. Scannen der Ports von Unternehmensservern auf aktive Sicherheitslücken
- C. Sichern von Systemdatenbankdateien auf Offline-Festplatten
- D. Routing von Netzwerkpaketen über drei verschlüsselte Onion-Knoten

Kontrollpunkt 2: Richtig oder falsch

6 Frage 6

6. Identitätsdiebstahl betrifft nur digitale Online-Konten, nicht die physische Briefpost.

○ Richtig ○ Falsch

7 Frage 7

7. MFA für alle persönlichen Konten zu erzwingen blockiert die meisten Credential-Stuffing-Angriffe durch Bots.

○ Richtig ○ Falsch

8 Frage 8

8. Eine Kreditsperre blockiert Bonitätsprüfungen, verhindert aber auch, dass Sie auf Ihr eigenes Bankkonto zugreifen können.

○ Richtig ○ Falsch

9 Frage 9

9. Passwortmanager schützen Nutzer vor Phishing, indem sie Passwörter auf gefälschten Domains nicht automatisch ausfüllen.

○ Richtig ○ Falsch

10 Frage 10

10. Phishing-E-Mails verwenden oft dringliche Formulierungen, um emotionale, schnelle Reaktionen auszulösen.

○ 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. Identitätsdiebe haben es auf persönliche Passwörter und _____ von Nutzern abgesehen.

2. Warnungen vor Datenbankeinbrüchen machen private _____ bei Konten sichtbar.

3. Wird zur Anmeldung ein temporärer Code verlangt, spricht man von _____ .

4. Das Durchsuchen von Hackerforen nach gestohlenen Daten ist eine Form der _____ im Darknet.

5. Um unbefugte Bonitätsabfragen zu blockieren, ist eine _____ erforderlich.

6. Durch Phishing-Schulungen für Mitarbeitende entsteht eine aktive _____ gegen Sicherheitsrisiken.

WORTSCHATZ-WORTBANK

ABWEHR DATENLECKS KREDITSPERRE MFA PHISHING SPOOFING ÜBERWACHUNG ZUGANGSDATEN

Schreiben Sie Ihre Antworten hier:

1. **2.**

3. **4.**

5. **6.**

Kontrollpunkt 4: Zuordnung von Sicherheits-Begriffen

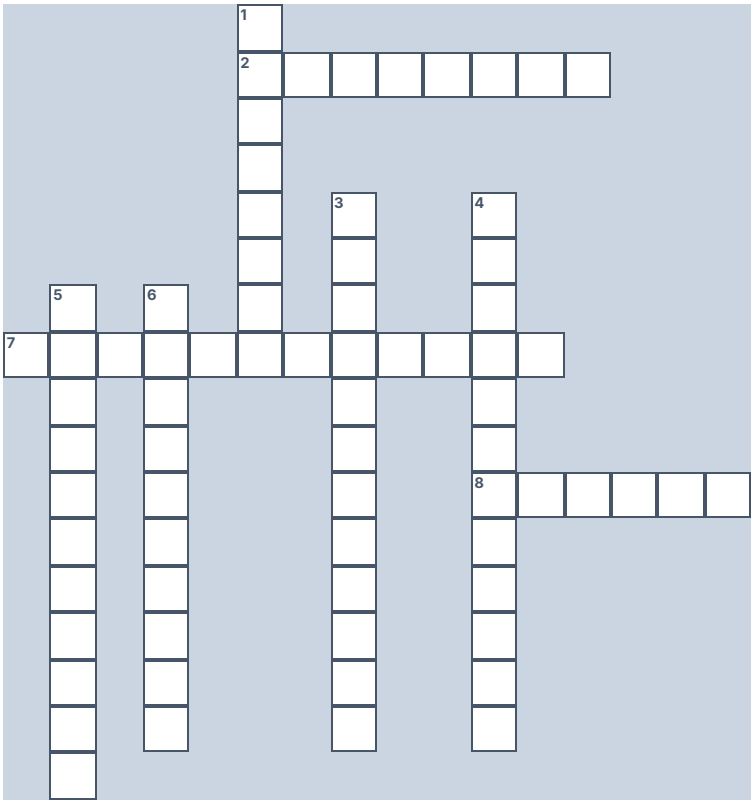
DEFINITIONEN ZUORDNEN

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

☐	1. ZUGANGSDATEN	A	Zusätzlicher Bestätigungsschritt (z. B. Hardware-Schlüssel), der Kontoanmeldungen schützt.
☐	2. LECKS	B	Erstellen einer gefälschten Website oder E-Mail, die eine legitime Organisation nachahmt.
☐	3. MFA	C	Beschränkung des Zugriffs auf Bonitätsakten, um betrügerische Kreditanträge zu verhindern.
☐	4. ÜBERWACHUNG	D	Unbefugte Offenlegung privater Datenbanken mit personenbezogenen Nutzerdatensätzen.
☐	5. EINFRIEREN	E	Schulungen und technische Maßnahmen zum Schutz vor Identitätsdiebstahl.
☐	6. ABWEHR	F	Versenden betrügerischer Nachrichten, um Nutzer zur Preisgabe ihrer Zugangsdaten zu verleiten.
☐	7. SPOOFING	G	Durchsuchen von Online-Foren und Hacker-Kanälen nach gestohlenen Unternehmensdaten.
☐	8. PHISHING	H	Benutzernamen, Passwörter und private Tokens zur Authentifizierung digitaler Identitäten.

Kontrollpunkt 5: Kreuzworträtsel

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



WAAGERECHT

2. Versand betrügerischer Nachrichten, um Nutzer zur Preisgabe ihrer Anmeldedaten zu verleiten. (8)

7. Benutzernamen, Passwörter und private Token zur Authentifizierung digitaler Identitäten. (12)

8. Schulungen und technische Kontrollen zum Schutz vor Identitätsdiebstahl. (6)

SENKRECHT

1. Erstellen einer gefälschten Website oder E-Mail, die eine seriöse Organisation imitiert. (8)

3. Beschränkung des Zugriffs auf Kreditauskünfte, um betrügerische Kreditanträge zu verhindern. (12)

4. Durchsuchen von Onlineforen und Hackerkanälen nach gestohlenen Unternehmensdaten. (12)

5. Zusätzlicher Verifizierungsschritt (z. B. Hardwareschlüssel), der Kontoanmeldungen schützt. (11)

6. Unbefugte Offenlegung privater Datenbanken mit persönlichen Nutzerdatensätzen. (10)

Kontrollpunkt 5, Alternative: Barrierefreie Kreuzworträtsel-Hinweise

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

WAAGERECHT

2 waagerecht: Versand betrügerischer Nachrichten, um Nutzer zur Preisgabe ihrer Anmeldedaten zu verleiten. (8 Buchstaben):

7 waagerecht: Benutzernamen, Passwörter und private Token zur Authentifizierung digitaler Identitäten. (12 Buchstaben):

8 waagerecht: Schulungen und technische Kontrollen zum Schutz vor Identitätsdiebstahl. (6 Buchstaben):

SENKRECHT

1 senkrecht: Erstellen einer gefälschten Website oder E-Mail, die eine seriöse Organisation imitiert. (8 Buchstaben):

3 senkrecht: Beschränkung des Zugriffs auf Kreditauskünfte, um betrügerische Kreditanträge zu verhindern. (12 Buchstaben):

4 senkrecht: Durchsuchen von Onlineforen und Hackerkanälen nach gestohlenen Unternehmensdaten. (12 Buchstaben):

5 senkrecht: Zusätzlicher Verifizierungsschritt (z. B. Hardwareschlüssel), der Kontoanmeldungen schützt. (11 Buchstaben):

6 senkrecht: Unbefugte Offenlegung privater Datenbanken mit persönlichen Nutzerdatensätzen. (10 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 K T S V R Z E H E S C A L Q
N R O T K A F I T L U M C P S
U Z M K A B W E H R V R H P U
H A S W J M M H H N H I O R F
C K T L R W H B U F S O Y O Y
A W S H T X A P U H F N N Z O
W I Q T I P V U I I O U U K A
R E P M K A N N N V G G P Q X
E Y J K V J G G Y W Y P J I Z
B I S K C E L N E T A D J N A
E Z U G A N G S D A T E N E I
U A S A J F W E K Z K E K Q N
J A K R E D I T S P E R R E F
O K N D N C D H I B A P R L P
W T I Y F Y S G X W H F R T N

WORTSCHATZ-WORTLISTE

ZUGANGSDATEN DATENLECKS MULTIFAKTOR UEBERWACHUNG KREDITSPERRE ABWEHR SPOOFING 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. ZUGANGSDATEN**
- **B. DATENLECKS**
- **C. MULTIFAKTOR**
- **D. UEBERWACHUNG**
- **E. KREDITSPERRE**
- **F. ABWEHR**
- **G. SPOOFING**
- **H. PHISHING**

DEFINITIONEN UND ZUORDNUNGSFELDER

_____ 1. Versand betrügerischer Nachrichten, um Nutzer zur Preisgabe ihrer Anmeldedaten zu verleiten.

_____ 2. Benutzernamen, Passwörter und private Token zur Authentifizierung digitaler Identitäten.

_____ 3. Erstellen einer gefälschten Website oder E-Mail, die eine seriöse Organisation imitiert.

_____ 4. Schulungen und technische Kontrollen zum Schutz vor Identitätsdiebstahl.

_____ 5. Durchsuchen von Onlineforen und Hackerkanälen nach gestohlenen Unternehmensdaten.

_____ 6. Beschränkung des Zugriffs auf Kreditauskünfte, um betrügerische Kreditanträge zu verhindern.

_____ 7. Unbefugte Offenlegung privater Datenbanken mit persönlichen Nutzerdatensätzen.

_____ 8. Zusätzlicher Verifizierungsschritt (z. B. Hardwareschlüssel), der Kontoanmeldungen schützt.

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. AGDNUSTZEG NA
2. IRUMOFLTKA T
3. KRPSREETEIR D
4. ONGIFSPO
5. CLSAEENDKT
6. GRHUWNCUE ABE
7. HAERWB
8. SHHGPNII

Bonusaufgabe: Schnell denken

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

1	Dinge, die zu tun sind, wenn Ihre Identität gestohlen wurde			
2	Dinge, die Sie nicht in sozialen Medien teilen sollten			
3	Dinge, von denen Sie ein Backup machen			
4	Karten oder Ausweise in Ihrer Brieftasche			
5	Dokumente, die Sie schützen sollten			
6	Dinge, die nach einem Datenleck zu tun sind			
7	Gründe, Software zu aktualisieren			
8	Informationen, die ein Identitätsdieb haben möchte			
9	Geräte, die gehackt werden können			
10	Orte, an denen Ihre Daten durchsickern können			
11	Sichere Gewohnheiten, mit denen Sie heute beginnen können			
12	Anzeichen, dass ein Computer infiziert ist			
13	Möglichkeiten, nachzuweisen, wer Sie sind			
14	Anzeichen für Identitätsdiebstahl			
15	Warnzeichen in einer E-Mail			

Kontrollpunkt 8: Fallstudien zur Cybersicherheit

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

FALLSTUDIE 1: SCHUTZ VOR IDENTITÄTSMISSBRAUCH VON FÜHRUNGSKRÄFTEN



Szenario: Eine prominente Führungskraft der obersten Ebene wird mit Tippfehler-Domains angegriffen, die ihre persönliche E-Mail-Adresse nachahmen, um Kunden zu betrügen. Entwerfen Sie einen Plan zum Markenschutz.

Diskussionsfrage: Analysieren Sie die Risiken des Marken-Spoofings und beschreiben Sie SPF/DKIM/DMARC sowie Authentifizierungskontrollen.

FALLSTUDIE 2: UNTERNEHMENSZUGANGSDATEN IM DARK WEB



Szenario: Ein Datenbank-Dump im Darknet enthält mehrere hundert Firmenzugangsdaten, die Systemadministratoren eines Unternehmens gehören. Entwerfen Sie eine Strategie zur Schadensbegrenzung.

Diskussionsfrage: Beschreiben Sie den Prozess zur Bereinigung der Zugangsdaten und planen Sie die Einführung eines Passwort-Managers.

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		9	8	18	5
9	4	5	14	20	9	20	1	5	20		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 Identitätsdiebstahl?

Eine Straftat, bei der ein Angreifer persönliche Daten (etwa Passwörter oder Sozialversicherungsnummern) stiehlt, um sich zur persönlichen Bereicherung als jemand anderes auszugeben.

Q2: Was ist die häufigste Ursache von Identitätsdiebstahl?

Phishing ist ein führender Weg, auf dem Diebe an Passwörter gelangen, indem sie Nutzer auf gefälschte Websites locken.

Q3: Wie schützt die Multi-Faktor-Authentifizierung (MFA) Identitäten?

MFA verlangt für die Anmeldung einen zweiten Nachweis (etwa einen Hardwareschlüssel) und blockiert Angreifer selbst dann, wenn sie Ihr Passwort stehlen.

Q4: Was ist eine Kreditsperre (Credit Freeze)?

Ein kostenloser Dienst, der Auskunfteien daran hindert, Ihre Kreditakte weiterzugeben, sodass Diebe keine neuen Kredite in Ihrem Namen aufnehmen können. [2]

Q5: Was ist Darknet-Überwachung?

Software, die Hackerforen nach geleakten E-Mail-Adressen, Passwörtern und persönlichen Daten durchsucht und Sie warnt, wenn Ihre Daten offengelegt wurden.

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

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

Q6: Was bedeutet Credential Stuffing?

Automatisierte Bots, die geleakte Passwortlisten auf Hunderten von Websites ausprobieren, um aktive Konten zu übernehmen.

Q7: Warum ist E-Mail-Spoofing gefährlich?

Damit können Angreifer den Absendernamen in E-Mails fälschen, sodass Phishing-Nachrichten scheinbar von vertrauenswürdigen Kollegen stammen.

Q8: Wie verhindern Passwort-Manager Identitätsdiebstahl?

Sie speichern komplexe, einzigartige Passwörter für jedes Konto und füllen Anmeldedaten auf gefälschten Phishing-Domains nicht automatisch aus.

Q9: Was ist Spear-Phishing?

Ein sehr gezielter Phishing-Angriff, der mit dem Namen und den Daten des Opfers personalisiert wird, um die Erfolgschancen der Täuschung zu erhöhen.

Q10: Worin unterscheidet sich ein Bonitätsalarm von einer Sperre?

Ein Betrugsalarm fordert Kreditgeber auf, vor der Kontoeröffnung Ihre Identität zu prüfen, während eine Sperre den Zugriff auf Ihre Kreditakte vollständig blockiert. [2]

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

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

Q1: Wie führt SIM-Swapping zu Identitätsdiebstahl?

Angreifer überreden Mitarbeitende des Mobilfunkanbieters, die Telefonnummer des Opfers auf eine neue SIM-Karte zu übertragen, und kapern so SMS-basierte 2FA-Codes.

Q2: Welche Rolle spielt DMARC bei der Verhinderung von Identitätsdiebstahl?

Mit DMARC können Domaininhaber verhindern, dass gefälschte E-Mails die Posteingänge erreichen, und so gefälschte E-Mails stoppen, die Unternehmensdomains nachahmen.

Q3: Warum ist synthetischer Identitätsdiebstahl schwer zu erkennen?

Diebe kombinieren echte Sozialversicherungsnummern (SSNs) mit falschen Namen und Geburtsdaten, um völlig neue Kreditprofile aufzubauen, und umgehen so einfache Betrugswarnungen.

Q4: Wie nutzen Datenhändler persönliche Identitäten aus?

Datenhändler sammeln öffentliche Aufzeichnungen, Webverhalten und Kaufhistorien, um Profildossiers zu erstellen, die offengelegt oder verkauft werden können.

Q5: Warum gilt SMS-basierte MFA als anfällig?

SMS-Verkehr ist anfällig für Abfangen, Phishing und SIM-Swapping-Angriffe auf Ebene des Mobilfunkanbieters.

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 eine Sperre der Kreditakte?

Ein kommerzieller Dienst ähnlich einer Kreditsperre, mit dem Nutzer ihre Kreditakte per Mobil-App sofort entsperren oder sperren können.

Q7: Wie fördern Datenpannen in Unternehmen den Identitätsdiebstahl?

Geleakte Datenbanken legen Millionen von Zugangsdaten im Klartext offen und liefern Dieben die Rohdaten für gezielten Identitätsbetrug.

Q8: Welches Risiko birgt es, in sozialen Medien zu viel preiszugeben?

Wer Namen von Haustieren, Geburtsorte und Mädchennamen der Mutter öffentlich teilt, liefert Dieben die Antworten auf gängige Sicherheitsfragen zur Kontowiederherstellung.

Q9: Wie schützen biometrische Anmeldungen Identitätsprofile?

Biometrie verknüpft Anmeldungen mit Merkmalen wie Fingerabdrücken oder Gesichtern; auf dem Gerät gespeichert sind sie schwer zu stehlen, gespeicherte biometrische Daten können aber offengelegt werden.

Q10: Wie bekämpft die Red Flags Rule Identitätsdiebstahl?

Eine US-Bundesvorschrift, die Finanzinstitute verpflichtet, schriftliche Programme zu entwickeln, um Warnzeichen für Identitätsdiebstahl zu erkennen und darauf zu reagieren.

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

Über IdentityTheft.gov, betrieben von der FTC, können Opfer in den USA Identitätsdiebstahl melden und einen persönlichen Wiederherstellungsplan erhalten. [1]

2. SICHERHEITS-EINBLICK

Hardware-Sicherheitsschlüssel sind phishingresistente MFA, die stärkste Form der MFA, zu der CISA dringend rät. [4]

3. SICHERHEITS-EINBLICK

Kompromittierte Passwörter sind ein häufiger Einstiegspunkt bei Datenpannen und begünstigen späteren Identitätsbetrug.

4. SICHERHEITS-EINBLICK

Eine Kreditsperre ist nach US-Bundesrecht kostenlos und verhindert, dass Kreditgeber Ihre Kreditakte einsehen, bis sie aufgehoben wird. [2]

5. SICHERHEITS-EINBLICK

Mit DMARC können Domaininhaber Mailservern mitteilen, gefälschte E-Mails, die Prüfungen nicht bestehen, abzulehnen oder in Quarantäne zu verschieben. [7]

6. SICHERHEITS-EINBLICK

Durch SIM-Swapping können Hacker die SMS-basierte Zwei-Faktor-Authentifizierung auf Banking-Portalen umgehen.

7. SICHERHEITS-EINBLICK

Synthetischer Identitätsbetrug vermischt echte und falsche Angaben, sodass Kreditgeber ihn nur schwer erkennen.

8. SICHERHEITS-EINBLICK

Viele Menschen verwenden dasselbe Passwort für mehrere Online-Konten, sodass ein einziges Datenleck mehrere davon offenlegen kann.

9. SICHERHEITS-EINBLICK

Datenhändler erstellen detaillierte Dossiers über eine große Zahl von Verbrauchern und schaffen so ein konzentriertes Datenschutzrisiko.

10. SICHERHEITS-EINBLICK

Die Bewältigung eines Identitätsdiebstahls kann monatelange Arbeit bedeuten, etwa um Abbuchungen anzufechten und Bonitätsauskünfte zu korrigieren.

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] Federal Trade Commission. (n.d.). IdentityTheft.gov: Report identity theft and get a recovery plan.

https://www.identitytheft.gov/

[2] Federal Trade Commission. (2025). Credit Freezes and Fraud Alerts.

https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts

[3] Federal Trade Commission. (n.d.). What To Know About Identity Theft.

https://consumer.ftc.gov/articles/what-know-about-identity-theft

[4] CISA. (n.d.). More than a Password.

https://www.cisa.gov/MFA

[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

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

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

[7] IETF. (2015). RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC).

https://www.rfc-editor.org/rfc/rfc7489.html

Lösungsschlüssel: Kontrollpunkt 1 – Auswahlaufgaben

1 Frage 1

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Mit welcher Methode stehlen Identitätsdiebe am häufigsten Anmeldedaten? → Versenden gefälschter E-Mail-Warnungen, die Nutzer dazu bringen, Passwörter auf nachgeahmten Portalen einzugeben

2 Frage 2

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Welche Sicherheitsmaßnahme bietet den stärksten Schutz vor dem Durchsickern von Anmeldedaten? → Multi-Faktor-Authentifizierung mit Hardwareschlüsseln

3 Frage 3

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Was beschreibt das Einfrieren der Kreditauskunft (Credit Freeze)? → Sperren von Kreditauskünften, damit Diebe keine unbefugten Kredite aufnehmen können

4 Frage 4

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Warum ist eine Überwachung des Dark Web nützlich? → Es warnt Nutzer, wenn ihre geleakten Zugangsdaten in illegalen Datenbanken auftauchen

5 Frage 5

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Was bedeutet Social Engineering? → Menschen so manipulieren, dass sie vertrauliche Zugangsdaten freiwillig preisgeben

Lösungsschlüssel: Kontrollpunkt 2 – Richtig oder Falsch

6 Frage 6

Richtige Antwort: Falsch

HINWEIS FÜR LEHRKRÄFTE

Identitätsdiebstahl kann auch offline beginnen, etwa durch gestohlene Post oder Dokumente.

7 Frage 7

Richtige Antwort: Richtig

HINWEIS FÜR LEHRKRÄFTE

MFA für alle persönlichen Konten zu erzwingen blockiert die meisten Credential-Stuffing-Angriffe durch Bots.

8 Frage 8

Richtige Antwort: Falsch

HINWEIS FÜR LEHRKRÄFTE

Eine Kreditsperre verhindert neue Bonitätsabfragen, wirkt sich aber nicht auf Ihre bestehenden Konten aus.

9 Frage 9

Richtige Antwort: Richtig

HINWEIS FÜR LEHRKRÄFTE

Passwortmanager schützen Nutzer vor Phishing, indem sie Passwörter auf gefälschten Domains nicht automatisch ausfüllen.

10 Frage 10

Richtige Antwort: Richtig

HINWEIS FÜR LEHRKRÄFTE

Phishing-E-Mails verwenden oft dringliche Formulierungen, um emotionale, schnelle Reaktionen auszulösen.

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. ZUGANGSDATEN	D 2. LECKS	A 3. MFA	G 4. ÜBERWACHUNG
C 5. EINFRIEREN	E 6. ABWEHR	B 7. SPOOFING	F 8. PHISHING

KONTROLLPUNKT 3: LÖSUNG SCHLÜSSELBEGRIFFE

1 ZUGANGSDATEN	2 DATENLECKS	3 MFA	4 ÜBERWACHUNG
5 KREDITSPERRE	6 ABWEHR		

KONTROLLPUNKT 6, ALTERNATIVE: LÖSUNG WORTZUORDNUNG

1 H – PHISHING	2 A – ZUGANGSDATEN	3 G – SPOOFING	4 F – ABWEHR
5 D – UEBERWACHUNG	6 E – KREDITSPERRE	7 B – DATENLECKS	8 C – MULTIFAKTOR

DISKUSSIONSHINWEISE FÜR LEHRKRÄFTE

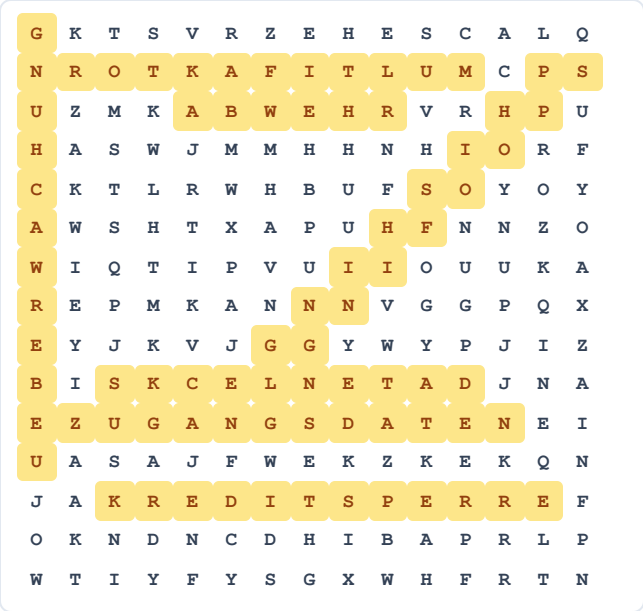
Schlüsselbegriffe:
Prüfen Sie, ob die Lernenden ZUGANGSDATEN, LECKS und MFA in eigenen Worten erklären und jeweils ein Beispiel nennen können.

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

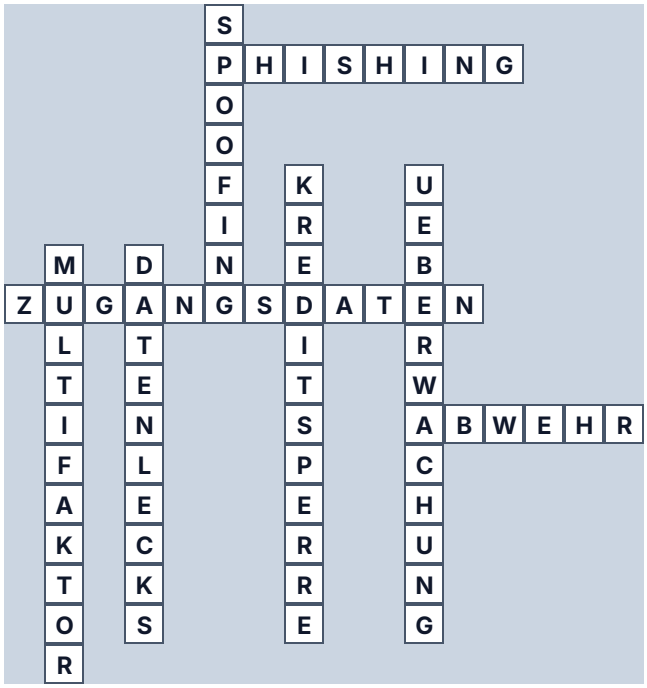
Quellenbewertung:
Lassen Sie die Lernenden mindestens eine Aussage anhand der Quellen des Arbeitsblatts prüfen und besprechen Sie, warum sich Zahlen, Preise und Regeln mit der Zeit ändern können.

Rätsellösungen und Hinweise für Lehrkräfte

LÖSUNG DES SUCHSELS



KREUZWORTRÄTSEL-LÖSUNG



LEITFADEN FÜR LEHRKRÄFTE ZU DEN KREUZWORTRÄTSEL-LÖSUNGEN

WAAGERECHT

2 waagerecht: PHISHING Versand betrügerischer Nachrichten, um Nutzer zur Preisgabe ihrer Anmeldedaten zu verleiten. (8 Buchstaben)

7 waagerecht: ZUGANGSDATEN Benutzernamen, Passwörter und private Token zur Authentifizierung digitaler Identitäten. (12 Buchstaben)

8 waagerecht: ABWEHR Schulungen und technische Kontrollen zum Schutz vor Identitätsdiebstahl. (6 Buchstaben)

SENKRECHT

1 senkrecht: SPOOFING Erstellen einer gefälschten Website oder E-Mail, die eine seriöse Organisation imitiert. (8 Buchstaben)

3 senkrecht: KREDITSPERRE Beschränkung des Zugriffs auf Kreditauskünfte, um betrügerische Kreditanträge zu verhindern. (12 Buchstaben)

4 senkrecht: UEBERWACHUNG Durchsuchen von Onlineforen und Hackerkanälen nach gestohlenen Unternehmensdaten. (12 Buchstaben)

5 senkrecht: MULTIFAKTOR Zusätzlicher Verifizierungsschritt (z. B. Hardwareschlüssel), der Kontoanmeldungen schützt. (11 Buchstaben)

6 senkrecht: DATENLECKS Unbefugte Offenlegung privater Datenbanken mit persönlichen Nutzerdatensätzen. (10 Buchstaben)

Lösungsschlüssel für Buchstabensalat und Chiffre

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

LÖSUNGSSCHLÜSSEL BUCHSTABENSALAT

1. AGDNUSTZEGNA — **ZUGANGSDATEN**
2. IRUMOFLTKAT — **MULTIFAKTOR**
3. KRPSREETEIRD — **KREDITSPERRE**
4. ONGIFSPO — **SPOOFING**
5. CLSAEENDKT — **DATENLECKS**
6. GRHUWNCUEABE — **UEBERWACHUNG**
7. HAERWB — **ABWEHR**
8. SHHGPNII — **PHISHING**

LÖSUNGSSCHLÜSSEL ZUR GEHEIMEN CHIFFRE-AUFGABE

"SCHUETZEN SIE IHRE IDENTITAET MIT MULTIFAKTOR"

Lösungsschlüssel zu den Fallstudien

A Fallstudie 1: Schutz vor Identitätsmissbrauch von Führungskräften

Lösung für Lehrkräfte

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Szenarioanalyse: Eine prominente Führungskraft aus der Geschäftsleitung wurde zum Ziel von Typosquatting-Domains, die ihre persönliche E-Mail-Adresse nachahmen, um Kunden zu betrügen. Entwickeln Sie einen Plan zum Markenschutz.
- Empfohlene Strategie und Lösung: Registrieren Sie alle gängigen Schreibvarianten des Namens der Führungskraft. Setzen Sie E-Mail-Authentifizierungsprotokolle (DMARC, DKIM, SPF) ein, um Domain-Spoofing zu verhindern. Setzen Sie für alle Unternehmensanmeldungen der Geschäftsleitung Hardware-MFA durch.

B Fallstudie 2: Unternehmenszugangsdaten im Dark Web

Lösung für Lehrkräfte

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Szenarioanalyse: Ein Datenbank-Dump im Dark Web enthält mehrere hundert Unternehmenszugangsdaten von Systemadministratoren eines Großunternehmens. Entwickeln Sie eine Strategie zur Schadensbegrenzung.
- Empfohlene Strategie und Lösung: Setzen Sie unternehmensweit alle Passwörter zurück. Schreiben Sie die Nutzung eines Passwort-Managers für Unternehmen vor. Setzen Sie MFA auf allen Systemportalen durch und richten Sie eine kontinuierliche, automatisierte Darknet-Überwachung mit Warnmeldungen ein.