Name: _____ Datum: _____ Punkte: _____

Grundlagen der Cybersicherheit und Online-Bedrohungen Prävention

Bedrohungen der Cybersicherheit, Netzwerk-Firewalls, Multi-Faktor-Authentifizierung, Sicherheitsrahmenwerke

LERNÜBERSICHT ZU DEN GRUNDLAGEN DER CYBERSICHERHEIT

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 Grundprinzipien der Cybersicherheit und der Abwehr von Online-Bedrohungen. Sie lernen Bedrohungen durch Schadsoftware, Multi-Faktor-Authentifizierung, Netzwerk-Firewalls und Rahmenwerke zur Reaktion auf Sicherheitsvorfälle 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/

Ihr Lernfahrplan: Grundlagen der Cybersicherheit

- Gängige Angriffswege für Malware, Phishing und das Eindringen in Unternehmensnetzwerke erkennen.
- Standardmäßige Cybersicherheitskontrollen einführen, darunter MFA, Firewalls und Endpunktschutz.
- Bewerten Sie Verfahren zur Reaktion auf Vorfälle, um die Folgen von Datenpannen abzumildern.
- Analysieren Sie organisatorische Risikofaktoren und die Sicherheitsausrichtung nach den NIST-Leitlinien.
- Richten Sie Sicherheitsgewohnheiten ein, um automatisiertes Credential Stuffing abzuwehren.

ANLEITUNG ZUM LEITFADEN FÜR CYBERSICHERHEIT

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: Gefahrenabwehr. Zum Schluss folgt die Bonusaufgabe Schnell denken.

GRUNDLAGEN DER CYBERSICHERHEIT UND BEDROHUNGSABWEHR (EINFÜHRUNG)

Cybersicherheit schützt Netzwerke, Systeme und Daten vor unbefugten digitalen Angriffen. Robuste Sicherheitsgewohnheiten, die Konfiguration von Firewalls, die verpflichtende Multi-Faktor-Authentifizierung und die Schulung der Mitarbeitenden im Erkennen von Bedrohungen sind wesentliche Bestandteile der Netzwerkabwehr in Unternehmen.

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

Kontrollpunkt 1: Auswahlaufgaben

1. Was ist das Hauptziel eines Phishing-Angriffs?

- A. Stehlen von Zugangsdaten und sensiblen Nutzerdaten
- B. Verbessern der Sichtbarkeit einer Website in Suchmaschinen
- C. Erhöhung der Netzwerkbandbreite
- D. Verwaltung der Replikation von Backup-Rechenzentren

2. Welcher Mechanismus bietet den stärksten Kontoschutz?

- A. Multi-Faktor-Authentifizierung mit Hardwareschlüsseln
- B. Komplexe Passwörter, die alle dreißig Tage geändert werden
- C. Beschränkung der Kontoanmeldung auf Geschäftszeiten
- D. Verbergen des Kontobenutzernamens in öffentlichen Verzeichnissen

3. Was kennzeichnet die Schadfunktion einer Ransomware-Infektion?

- A. Verschlüsseln von Systemdateien und Fordern einer Zahlung
- B. Heimliches Aufzeichnen von Tastatureingaben und Senden an entfernte Server
- C. Einschleusen nicht autorisierter Werbung in Browser
- D. Nutzen lokaler CPU-Ressourcen zum Schürfen von Kryptowährung

4. Wie wirkt sich ein Zero-Day-Exploit auf die Sicherheitsabwehr aus?

- A. Es zielt auf ungepatchte, unbekannte Schwachstellen
- B. Es deaktiviert automatisch die Unternehmensfirewall
- C. Es zwingt das System zu einem Kaltstart
- D. Die Behebung erfordert keinerlei Budget

5. Welches Rahmenwerk regelt Sicherheitskontrollen in Unternehmen?

- A. Leitlinien des NIST Cybersecurity Framework
- B. Spezifikationen des W3C-HTML5-Dokumentschemas
- C. Installationsanleitungen für Druckertreiber
- D. IETF-Definitionen von Routing-Protokollen

Kontrollpunkt 2: Richtig oder falsch

6 Frage R/F 6

6. Phishing-Angriffe richten sich nur gegen private E-Mail-Konten.

Richtig Falsch

7 Frage R/F 7

7. Multi-Faktor-Authentifizierung hilft, Credential-Stuffing-Angriffe abzuwehren.

Richtig Falsch

8 Frage R/F 8

8. Firewalls prüfen den Netzwerkverkehr, um nicht autorisierten Portzugriff zu blockieren.

Richtig Falsch

9 Frage R/F 9

9. Die Behebung von Zero-Day-Exploits erfordert normale Signatur-Updates des Antivirenprogramms.

Richtig Falsch

10 Frage R/F 10

10. Ein Honeypot ist ein Köderserver, mit dem Cyberkriminelle angelockt werden.

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. Netzwerkadministratoren installieren eine _____ , um eingehenden Datenverkehr zu filtern.

2. Ein Angreifer nutzt einen Zero-Day- _____ , um Systempatches zu umgehen.

3. Angreifer versenden gefälschte E-Mails, um _____ -Kampagnen gegen Mitarbeitende durchzuführen.

4. Ransomware ist eine zerstörerische Form von _____ , die Nutzerdaten sperrt.

5. Eine gute Passwort- _____ verringert das Risiko von Zugangsdatendiebstahl.

6. Zum Schutz sensibler Kommunikation setzen Nutzer Protokolle zur _____ ein.

WORTSCHATZ-WORTBANK

EXPLOIT FIREWALL HYGIENE MULTIFAKTOR PHISHING RANSOMWARE SCHADSOFTWARE VERSCHLÜSSELUNG

Schreiben Sie Ihre Antworten hier:

1. **2.**

3. **4.**

5. **6.**

Kontrollpunkt 4: Zuordnung von Sicherheits-Begriffen

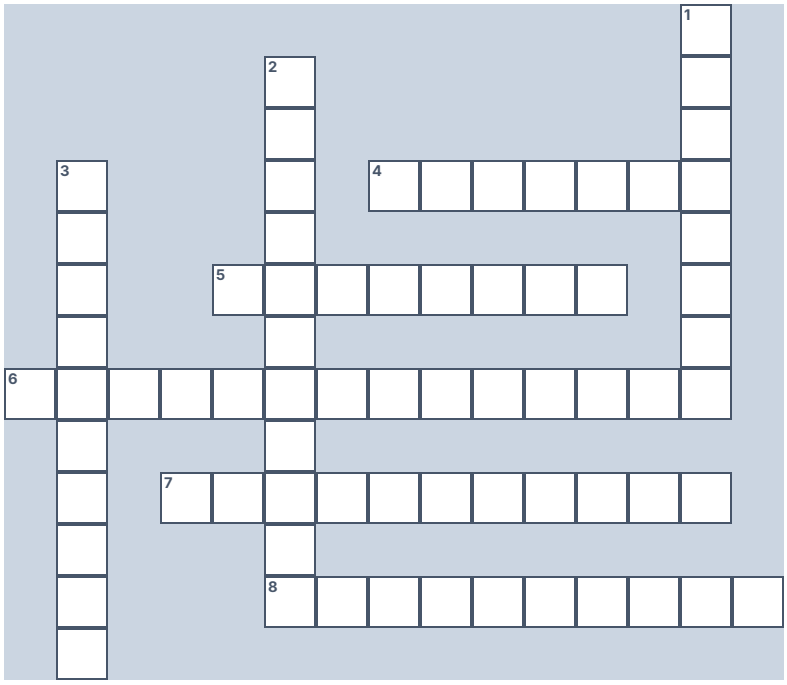
DEFINITIONEN ZUORDNEN

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

1. Bedrohung durch Ransomware	A	Strukturierte Leitlinien wie NIST, die zur Steuerung von Cyberrisiken verwendet werden.
2. Mehr-Faktor-Authentifizierung	B	Strukturierter Plan für den Umgang mit Sicherheitsverletzungen und deren Eindämmung.
3. Zero-Day-Exploit	C	Netzwerkbarriere, die Datenverkehr anhand von Sicherheitsregeln filtert.
4. Köder-Honeypot	D	Schadsoftware, die Daten verschlüsselt und für die Entschlüsselung eine Zahlung verlangt.
5. Firewall gegen Eindringlinge	E	Ausnutzung einer Schwachstelle, bevor der Hersteller einen Patch veröffentlicht.
6. Reaktion auf Vorfälle	F	Bewährte Verfahren für die Verwaltung von Zugangsdaten und Authentifizierungsschlüsseln.
7. Passworthygiene	G	Sicherheitsprüfung, die zwei oder mehr Authentifizierungsfaktoren verlangt.
8. Sicherheits-Framework	H	Ködersystem, das eingerichtet wird, um Angreifer anzulocken und zu analysieren.

Kontrollpunkt 5: Kreuzworträtsel

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



WAAGERECHT

4. Bewährte Verfahren für den Umgang mit Zugangsdaten und Authentifizierungsschlüsseln (7)

5. Netzwerkbarriere, die Datenverkehr anhand von Sicherheitsregeln filtert (8)

6. Ausnutzung einer Schwachstelle, bevor der Hersteller einen Patch veröffentlicht (14)

7. Strukturierter Plan zur Bewältigung und Eindämmung von Sicherheitsvorfällen (11)

8. Schadsoftware, die Daten verschlüsselt und für die Entschlüsselung eine Zahlung fordert (10)

SENKRECHT

1. Köder-System, das Angreifer anlocken und ihr Vorgehen analysieren soll (8)

2. Sicherheitsprüfung, die zwei oder mehr Authentifizierungsfaktoren verlangt (11)

3. Strukturierte Leitlinien wie NIST zur Steuerung von Cyberrisiken (10)

Kontrollpunkt 5, Alternative: Barrierefreie Kreuzworträtsel-Hinweise

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

WAAGERECHT

4 waagerecht: Bewährte Verfahren für den Umgang mit Zugangsdaten und Authentifizierungsschlüsseln (7 Buchstaben):

5 waagerecht: Netzwerkbarriere, die Datenverkehr anhand von Sicherheitsregeln filtert (8 Buchstaben):

6 waagerecht: Ausnutzung einer Schwachstelle, bevor der Hersteller einen Patch veröffentlicht (14 Buchstaben):

7 waagerecht: Strukturierter Plan zur Bewältigung und Eindämmung von Sicherheitsvorfällen (11 Buchstaben):

8 waagerecht: Schadsoftware, die Daten verschlüsselt und für die Entschlüsselung eine Zahlung fordert (10 Buchstaben):

SENKRECHT

1 senkrecht: Köder-System, das Angreifer anlocken und ihr Vorgehen analysieren soll (8 Buchstaben):

2 senkrecht: Sicherheitsprüfung, die zwei oder mehr Authentifizierungsfaktoren verlangt (11 Buchstaben):

3 senkrecht: Strukturierte Leitlinien wie NIST zur Steuerung von Cyberrisiken (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.

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

WORTSCHATZ-WORTLISTE

RANSOMWARE MULTIFAKTOR ZERODAYEXPLOIT HONEYPOT FIREWALL
NOTFALLPLAN HYGIENE RAHMENWERK

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. RANSOMWARE**
- **B. MULTIFAKTOR**
- **C. ZERODAYEXPLOIT**
- **D. HONEYPOT**
- **E. FIREWALL**
- **F. NOTFALLPLAN**
- **G. HYGIENE**
- **H. RAHMENWERK**

DEFINITIONEN UND ZUORDNUNGSFELDER

_____ 1. Netzwerkbarriere, die Datenverkehr anhand von Sicherheitsregeln filtert.

_____ 2. Strukturierter Plan zur Bewältigung und Eindämmung von Sicherheitsvorfällen.

_____ 3. Schadsoftware, die Daten verschlüsselt und für die Entschlüsselung eine Zahlung fordert.

_____ 4. Sicherheitsprüfung, die zwei oder mehr Authentifizierungsfaktoren verlangt.

_____ 5. Bewährte Verfahren für den Umgang mit Zugangsdaten und Authentifizierungsschlüsseln.

_____ 6. Strukturierte Leitlinien wie NIST zur Steuerung von Cyberrisiken.

_____ 7. Ausnutzung einer Schwachstelle, bevor der Hersteller einen Patch veröffentlicht.

_____ 8. Köder-System, das Angreifer anlocken und ihr Vorgehen analysieren soll.

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. RWMOARAESN
2. DEARYIZOETPLXO
3. EIFWALLR
4. EYEINHG
5. TUKALRIFMOT
6. OTEPHYON
7. PANOLNLATLF
8. RMNKREAWEH

Bonusaufgabe: Schnell denken

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

1	Berufe in der Cybersicherheit			
2	Gründe, Software zu aktualisieren			
3	Dinge, die eine Firewall blockieren kann			
4	Warnzeichen in einer E-Mail			
5	Dinge, von denen Sie ein Backup machen			
6	Bekannte Arten von Cyberangriffen			
7	Dinge, die ein Honeypot anlocken kann			
8	Informationen, die Sie niemals weitergeben sollten			
9	Anzeichen, dass ein Computer infiziert ist			
10	Filme oder Serien über Hacker			
11	Sicherheitsebenen, die Sie aufbauen können			
12	Dinge, die Sie bei einer Sicherheitsübung trainieren			
13	Sicherheitswerkzeuge, die Sie kennen			
14	Personen, die Sie um IT-Hilfe bitten können			
15	Wörter, die mit „Cyber“ beginnen			

Kontrollpunkt 8: Fallstudien zur Cybersicherheit

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

FALLSTUDIE 1: STRATEGIE ZUR WIEDERHERSTELLUNG NACH RANSOMWARE



Szenario: Ein Firmennetzwerk ist mit Ransomware infiziert, die kritische Datenbanken sperrt. Die Angreifer fordern eine Zahlung von $100,000 in Kryptowährung. Das Unternehmen hat Offline-Backups, die 24 Stunden alt sind.

Diskussionsfrage: Analysieren Sie die Risiken einer Zahlung und bewerten Sie die Wiederherstellungsstrategie.

FALLSTUDIE 2: ABWEHR VON CREDENTIAL STUFFING



Szenario: Ein Onlinedienst wird Ziel eines Credential-Stuffing-Angriffs, bei dem Hacker Millionen von Benutzername-Passwort-Paaren ausprobieren, die auf anderen Websites gestohlen wurden.

Diskussionsfrage: Beschreiben Sie den Mechanismus dieses Angriffs und skizzieren Sie zwei Abwehrsysteme.

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	9	3	8	5	18	14		19	9	5		9	8	18
							19	25	19	20	5	13		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 das Hauptziel der Cybersicherheit?

Das Hauptziel ist der Schutz von Netzwerken, Geräten und Daten vor unbefugtem Zugriff, Angriffen und versehentlicher Beschädigung.

Q2: Wie unterscheidet sich Phishing von Spear-Phishing?

Phishing ist eine breit gestreute E-Mail-Kampagne gegen beliebige Nutzer, während Spear-Phishing mithilfe personalisierter Daten auf bestimmte Personen zielt.

Q3: Was ist eine Netzwerk-Firewall?

Eine Firewall ist ein Netzwerksicherheitssystem, das ein- und ausgehenden Datenverkehr anhand vordefinierter Sicherheitsregeln überwacht und filtert.

Q4: Warum ist die Multi-Faktor-Authentifizierung (MFA) notwendig?

MFA fügt eine entscheidende Verteidigungsebene hinzu und verhindert den Zugriff selbst dann, wenn Angreifer das primäre Passwort stehlen oder knacken.

Q5: Was kennzeichnet einen Computervirus?

Ein Virus ist sich selbst replizierende Malware, die sich an saubere Dateien anhängt und sich nach der Ausführung über Systeme hinweg verbreitet.

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

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

Q6: Wie sperrt Ransomware lokale Daten?

Ransomware verwendet kryptografische Algorithmen, um Benutzerdateien zu verschlüsseln, sodass sie unlesbar sind, bis ein Entschlüsselungsschlüssel angewendet wird.

Q7: Was ist eine Zero-Day-Schwachstelle?

Eine Zero-Day-Lücke ist eine Sicherheitslücke in Software, die dem Hersteller unbekannt ist, sodass vor einem Angriff keine Zeit für die Entwicklung eines Patches bleibt.

Q8: Welche Rolle spielt das NIST-Framework?

Das NIST-Framework bietet freiwillige Leitlinien und Standards, die Organisationen helfen, Cybersicherheitsrisiken zu steuern und zu verringern.

Q9: Was ist ein Plan zur Reaktion auf Sicherheitsvorfälle?

Es ist ein dokumentierter Satz von Verfahren zur Erkennung und Eindämmung von Sicherheitsverletzungen und Netzwerkkompromittierungen sowie zur Wiederherstellung danach.

Q10: Wie nutzt Social Engineering Nutzer aus?

Social Engineering nutzt psychologische Manipulation, um Mitarbeiter dazu zu bringen, Passwörter preiszugeben oder schädliche Dateien herunterzuladen.

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

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

Q1: Wie überlastet ein DDoS-Angriff Webserver?

Ein DDoS-Angriff koordiniert Millionen kompromittierter Botnetz-Geräte, um einen Server mit Datenverkehr zu überfluten und Bandbreite und CPU-Kapazität zu erschöpfen.

Q2: Was ist der Unterschied zwischen symmetrischer und asymmetrischer Verschlüsselung?

Symmetrische Verschlüsselung verwendet einen einzigen Schlüssel zum Ver- und Entschlüsseln, während asymmetrische Verschlüsselung ein Schlüsselpaar aus öffentlichem und privatem Schlüssel verwendet.

Q3: Wie führen Hacker SQL-Injection-Angriffe aus?

Angreifer geben schädliche SQL-Befehle in Formularfelder ein und bringen die Backend-Datenbank dazu, unbefugt Benutzerdatensätze herauszugeben.

Q4: Was ist laterale Bewegung bei Netzwerkeinbrüchen?

Es ist die Technik, bei der Angreifer einen ersten Serverzugriff ausnutzen, um weitere verbundene Systeme im internen Netzwerk zu kompromittieren.

Q5: Wie leitet DNS-Spoofing den Web-Traffic um?

DNS-Spoofing verändert Cache-Einträge von Nameservern und leitet legitime Nutzer statt zur Zieldomain auf bösartige, täuschend ähnliche Websites.

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 Hardware-Sicherheitstoken?

Es ist ein physisches Gerät (etwa ein YubiKey), das kryptografische Authentifizierungsnachweise erzeugt und maximalen Schutz vor Phishing aus der Ferne bietet.

Q7: Wie nutzen Sicherheitsteams Honeypots als Köder?

Teams setzen Köderserver außerhalb der Produktion ein, um Eindringlinge frühzeitig zu erkennen und die Angriffsmuster unbefugter Akteure zu analysieren.

Q8: Was ist das Prinzip der minimalen Rechtevergabe?

Es ist der Sicherheitsgrundsatz, die Zugriffsrechte von Nutzern auf das absolut notwendige Minimum für ihre Aufgaben zu beschränken.

Q9: Wie nutzt ein Man-in-the-Middle-Angriff Verbindungen aus?

Ein Angreifer fängt die Kommunikation zwischen zwei Geräten in unverschlüsselten Netzwerken ab, verändert sie und stiehlt Sitzungstoken und Zugangsdaten.

Q10: Was sind Indicators of Compromise (IOCs)?

IOCs sind forensische Spuren, etwa ungewöhnliche Änderungen in der Registry oder verdächtiger IP-Verkehr, die zeigen, dass ein System kompromittiert wurde.

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

Angreifer durchsuchen das Internet ständig nach verwundbaren Servern und senden Phishing-E-Mails an die Postfächer von Mitarbeitenden.

2. SICHERHEITS-EINBLICK

Menschliches Versagen, etwa das Klicken auf Phishing-Links, ist ein häufiger Faktor bei Datenpannen; deshalb sind Schulungen wichtig.

3. SICHERHEITS-EINBLICK

Die Kosten einer Datenpanne umfassen Bußgelder, Kundenabwanderung, Untersuchung und Behebung und können Millionen von Dollar erreichen.

4. SICHERHEITS-EINBLICK

Phishing-resistente MFA, etwa mit Hardware-Sicherheitsschlüsseln, ist die stärkste MFA-Art und der Standard, den die CISA dringend empfiehlt. [2]

5. SICHERHEITS-EINBLICK

Ransomware bleibt eine große Bedrohung für Unternehmensnetzwerke, und die CISA empfiehlt nachdrücklich verschlüsselte Offline-Backups als zentrale Schutzmaßnahme. [4]

6. SICHERHEITS-EINBLICK

Das NIST Cybersecurity Framework 2.0 (2024) hat sechs Kernfunktionen: Govern, Identify, Protect, Detect, Respond, Recover (Steuern, Identifizieren, Schützen, Erkennen, Reagieren, Wiederherstellen). [1]

7. SICHERHEITS-EINBLICK

Credential-Stuffing-Bots testen geleakte Kombinationen aus Benutzername und Passwort massenhaft an Anmeldeportalen von Banken und Onlineshops.

8. SICHERHEITS-EINBLICK

Weltweit gibt es Märkte für Zero-Day-Exploits, auf denen schwerwiegende Sicherheitslücken für hohe Summen verkauft werden können, bevor sie gepatcht werden.

9. SICHERHEITS-EINBLICK

Ein Honeypot-Ködersystem meldet Einbruchsalarme sofort, da legitime Nutzer keinen Grund haben, darauf zuzugreifen.

10. SICHERHEITS-EINBLICK

Transport Layer Security (TLS) verschlüsselt Browsersitzungen und verhindert so das Mitschneiden von Paketen in öffentlichen WLAN-Netzen.

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. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[2] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[3] 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

[4] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[6] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.
https://csrc.nist.gov/pubs/sp/800/61/r3/final

[7] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[8] OWASP. (n.d.). SQL Injection.
https://owasp.org/www-community/attacks/SQL_Injection

Lösungsschlüssel: Kontrollpunkt 1 – Auswahlaufgaben

1 **Phishing-Angriffe** PHISHING — **Richtige Antwort: A**

HINWEIS FÜR LEHRKRÄFTE

Phishing-Kampagnen versuchen, mit gefälschten E-Mails Zugangsdaten und sensible Nutzerdaten zu stehlen. Quelle: OWASP Secure Configuration.

2 **Kontoschutz** MFA-SCHLÜSSEL — **Richtige Antwort: A**

HINWEIS FÜR LEHRKRÄFTE

Mehr-Faktor-Authentifizierung (MFA) mit Hardware-Token bietet den stärksten Schutz für den Kontozugang. Quelle: NIST Digital Identity.

3 **Ransomware-Bedrohung** RANSOMWARE — **Richtige Antwort: A**

HINWEIS FÜR LEHRKRÄFTE

Ransomware verschlüsselt kritische Systeme und Daten und verlangt eine Zahlung in Kryptowährung für die Entschlüsselungsschlüssel. Quelle: Center for Internet Security (CIS).

4 **Zero-Day-Sicherheitslücke** ZERO-DAY — **Richtige Antwort: A**

HINWEIS FÜR LEHRKRÄFTE

Zero-Day-Bedrohungen nutzen ungepatchte, unbekannte Sicherheitslücken aus, bevor ein Patch des Herstellers verfügbar ist. Quelle: OWASP Secure Configuration.

5 **Sicherheits-Frameworks** FRAMEWORKS — **Richtige Antwort: A**

HINWEIS FÜR LEHRKRÄFTE

Rahmenwerke wie NIST bieten strukturierte Leitlinien, die Organisationen helfen, Cyberrisiken zu steuern und zu verringern. Quelle: NIST Digital Identity.

Lösungsschlüssel: Kontrollpunkt 2 – Richtig oder Falsch

6 **Gezieltes Phishing** PHISHING — **Richtige Antwort: Falsch**

HINWEIS FÜR LEHRKRÄFTE

Phishing-Angriffe richten sich sowohl gegen Unternehmensnetzwerke als auch gegen private Konten, um mehr Angriffswege zu nutzen. Quelle: OWASP Secure Configuration.

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

HINWEIS FÜR LEHRKRÄFTE

MFA erfordert einen zweiten Faktor, daher reicht ein gestohlenes Passwort allein meist nicht für die Anmeldung aus.

8 **Verkehrs-Firewall** FIREWALL — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

Firewalls prüfen und blockieren Datenverkehr auf bestimmten Netzwerkports, um nicht autorisierte Verbindungen herauszufiltern. Quelle: Center for Internet Security (CIS).

9 **Reaktion auf Zero-Day-Angriffe** ZERO-DAY — **Richtige Antwort: Falsch**

HINWEIS FÜR LEHRKRÄFTE

Die Behebung von Zero-Day-Schwachstellen erfordert Code-Patches und WAF-Filterung, da noch keine Signaturen existieren. Quelle: OWASP Secure Configuration.

10 **Honeypots als Köder** HONEYPOT — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

Honeypots sind Täuschungsserver, mit denen Sicherheitsteams böswillige Akteure anlocken, Alarm auslösen und sie untersuchen. Quelle: Center for Internet Security (CIS).

Vokabelschlüssel und Bewertungsraster

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

KONTROLLPUNKT 4: LÖSUNG BEGRIFFSZUORDNUNG

D 1. Bedrohung durch Ransomware	G 2. Mehr-Faktor-Authentifizierung	E 3. Zero-Day-Exploit	H 4. Köder-Honeypot
C 5. Firewall gegen Eindringlinge	B 6. Reaktion auf Vorfälle	F 7. Passworthygiene	A 8. Sicherheits-Framework

KONTROLLPUNKT 3: LÖSUNG SCHLÜSSELBEGRIFFE

1 FIREWALL	2 EXPLOIT	3 PHISHING	4 SCHADSOFTWARE
5 HYGIENE	6 VERSCHLÜSSELUNG		

KONTROLLPUNKT 6, ALTERNATIVE: LÖSUNG WORTZUORDNUNG

1 E – FIREWALL	2 F – NOTFALLPLAN	3 A – RANSOMWARE	4 B – MULTIFAKTOR
5 G – HYGIENE	6 H – RAHMENWERK	7 C – ZERODAYEXPLOIT	8 D – HONEYPOT

DISKUSSIONSHINWEISE FÜR LEHRKRÄFTE

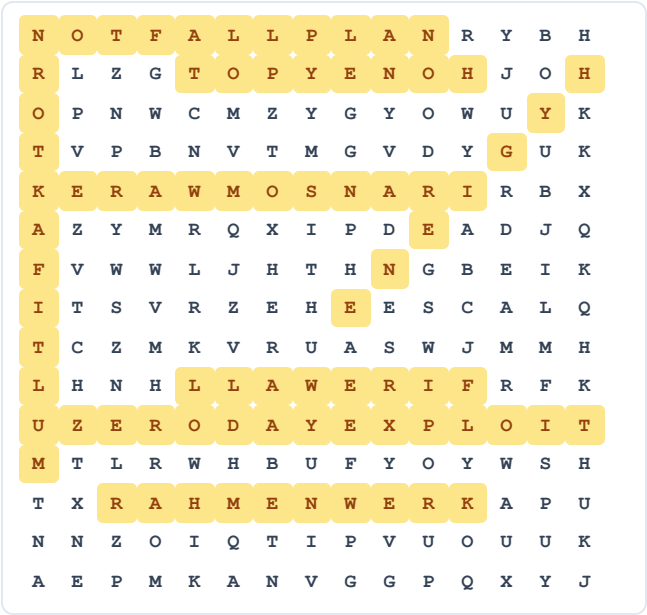
Schlüsselbegriffe:
Prüfen Sie, ob die Lernenden Bedrohung durch Ransomware, Mehr-Faktor-Authentifizierung und Zero-Day-Exploit in eigenen Worten erklären und jeweils ein Beispiel nennen können.

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

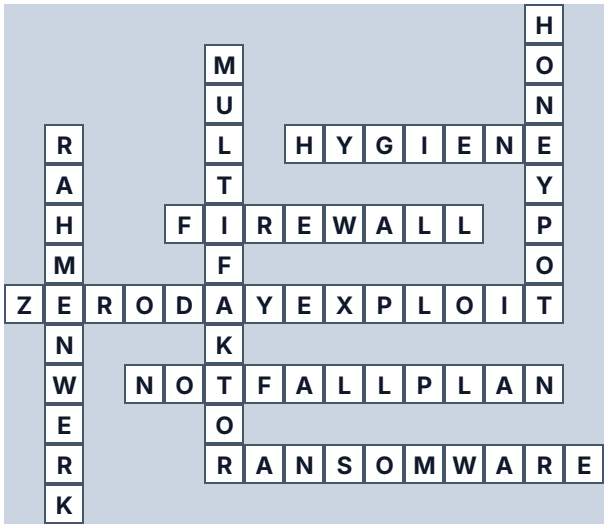
Quellenbewertung:
Lassen Sie die Lernenden mindestens eine Aussage anhand der Quellen des Arbeitsblatts prüfen und besprechen Sie, warum sich Zahlen, Preise und Regeln mit der Zeit ändern können.

Rätsellösungen und Hinweise für Lehrkräfte

LÖSUNG DES SUCHSELS



KREUZWORTRÄTSEL-LÖSUNG



LEITFADEN FÜR LEHRKRÄFTE ZU DEN KREUZWORTRÄTSEL-LÖSUNGEN

WAAGERECHT

4 waagerecht: HYGIENE Bewährte Verfahren für den Umgang mit Zugangsdaten und Authentifizierungsschlüsseln (7 Buchstaben)

5 waagerecht: FIREWALL Netzwerkbarriere, die Datenverkehr anhand von Sicherheitsregeln filtert (8 Buchstaben)

6 waagerecht: ZERODAYEXPLOIT Ausnutzung einer Schwachstelle, bevor der Hersteller einen Patch veröffentlicht (14 Buchstaben)

7 waagerecht: NOTFALLPLAN Strukturierter Plan zur Bewältigung und Eindämmung von Sicherheitsvorfällen (11 Buchstaben)

8 waagerecht: RANSOMWARE Schadsoftware, die Daten verschlüsselt und für die Entschlüsselung eine Zahlung fordert (10 Buchstaben)

SENKRECHT

1 senkrecht: HONEYPOT Köder-System, das Angreifer anlocken und ihr Vorgehen analysieren soll (8 Buchstaben)

2 senkrecht: MULTIFAKTOR Sicherheitsprüfung, die zwei oder mehr Authentifizierungsfaktoren verlangt (11 Buchstaben)

3 senkrecht: RAHMENWERK Strukturierte Leitlinien wie NIST zur Steuerung von Cyberrisiken (10 Buchstaben)

Lösungsschlüssel für Buchstabensalat und Chiffre

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

LÖSUNGSSCHLÜSSEL BUCHSTABENSALAT

1. RWMOARAESN — **RANSOMWARE**
2. DEARYIZOETPLXO — **ZERODAYEXPLOIT**
3. EIFWALLR — **FIREWALL**
4. EYEINHG — **HYGIENE**
5. TUKALRIFMOT — **MULTIFAKTOR**
6. OTEPHYON — **HONEYPOT**
7. PANOLNLATLF — **NOTFALLPLAN**
8. RMNKREAWEH — **RAHMENWERK**

LÖSUNGSSCHLÜSSEL ZUR GEHEIMEN CHIFFRE-AUFGABE

"SICHERN SIE IHR SYSTEM MIT MULTIFAKTOR"

Lösungsschlüssel zu den Fallstudien

A Fallstudie 1: Strategie zur Wiederherstellung nach Ransomware

Lösung für Lehrkräfte

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Szenarioanalyse: Ein Unternehmensnetzwerk ist mit Ransomware infiziert, die wichtige Datenbanken sperrt. Die Angreifer fordern eine Zahlung von $100,000 in Kryptowährung. Das Unternehmen hat Offline-Backups, die 24 Stunden alt sind.
- Empfohlene Strategie und Lösung: Risiken einer Zahlung: Eine Zahlung garantiert nicht die Entschlüsselung der Dateien, kennzeichnet das Unternehmen als zahlungsbereites Ziel und finanziert kriminelle Aktivitäten. Wiederherstellungsstrategie: Das Team sollte infizierte Hosts isolieren, kompromittierte Server bereinigen und die Daten aus Offline-Backups wiederherstellen. Es muss den ursprünglichen Zugangsweg (Phishing oder Exploit) schließen, um eine sofortige erneute Infektion zu verhindern.

B Fallstudie 2: Abwehr von Credential Stuffing

Lösung für Lehrkräfte

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Szenarioanalyse: Ein Onlinedienst wird Ziel eines Credential-Stuffing-Angriffs, bei dem Hacker Millionen von Benutzername-Passwort-Paaren testen, die auf anderen Websites gestohlen wurden.
- Empfohlene Strategie und Lösung: Mechanismus: Angreifende nutzen die Wiederverwendung von Passwörtern über mehrere Websites aus und melden sich mit automatisierten Bots bei Nutzerkonten an. Abwehrmaßnahmen: 1. Multi-Faktor-Authentifizierung (MFA) blockiert Anmeldeversuche, selbst wenn das Passwort korrekt ist. 2. Rate-Limiting und CAPTCHAs blockieren automatisierten Bot-Verkehr, der Anmelde-Endpunkte mit Anfragen überflutet.