Name: _____ Datum: _____ Punkte: _____

Ransomware-Angriffe und Unternehmen Wiederherstellung

Ausführung der Schadsoftware, kryptografische Verschlüsselung von Dateien, Offline-Backups, Eindämmungsmaßnahmen und Notfallwiederherstellung.

RANSOMWARE-ANGRIFFE – LERNÜBERSICHT

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 Ransomware-Angriffe und die Wiederherstellung des Geschäftsbetriebs. Sie lernen die Ausführung von Schadcode, Dateiverschlüsselung, Offline-Backups, Eindämmung von Bedrohungen, Zahlungen in Kryptowährung und Notfallwiederherstellungspläne 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/ransomware-angriff/

Ihr Lernfahrplan: Wiederherstellung nach Ransomware

- Unterscheiden Sie zwischen Trojaner-, Ransomware- und Spyware-Payloads.
- Analysieren Sie schädliche Dateien in sicheren Sandbox-Umgebungen.
- Verfahren zur schnellen Netzwerkisolierung und Eindämmung entwickeln.

ANLEITUNG ZU RANSOMWARE-ANGRIFFEN

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: Wiederherstellung nach Ransomware-Angriffen. Zum Schluss folgt die Bonusaufgabe Schnell denken.

RANSOMWARE-ANGRIFFE UND NOTFALLWIEDERHERSTELLUNG (EINFÜHRUNG)

Ransomware-Payloads sperren den Systemspeicher kryptografisch und verlangen Zahlungen in Kryptowährung für die Entschlüsselungsschlüssel. Zur Abwehr dieser Bedrohung gehören Regeln zur Netzwerkisolierung, die Analyse von Malware in einer Sandbox und robuste, physisch getrennte Offline-Backups (Air Gap).

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

Kontrollpunkt 1: Auswahlaufgaben

1. Was ist der Hauptmechanismus eines Ransomware-Angriffs?

- A. Kryptografische Verschlüsselung von Nutzerdateien, um den Systemzugriff zu verweigern
- B. Einschleusen schädlicher SQL-Befehle in Formularfelder
- C. Mitschneiden von Netzwerkpaketen in einem öffentlichen WLAN
- D. Fälschen von E-Mail-Headern, um die SPF-Validierung zu umgehen

2. Was ist ein Offline-Backup (Cold Backup)?

- A. Eine vom Netzwerk getrennte Sicherungskopie, die vor der Ausbreitung von Malware geschützt ist
- B. Eine Sicherung auf der Festplatte des primären Webservers
- C. Ein temporärer Cache von Systemregistrierungsprotokollen
- D. Ein Verwaltungswerkzeug zum Zurücksetzen von Benutzerpasswörtern

3. Wie sollten Sicherheitsteams infizierte Systeme bei einem Ransomware-Angriff isolieren?

- A. Sofort die Netzwerkkabel trennen und die WLAN-Schnittstellen deaktivieren
- B. Aktualisieren der Signaturdatenbank des Virenschutzes
- C. Den primären DNS-Server abschalten
- D. Die Endungen der kompromittierten Dateien umbenennen

4. Warum raten Sicherheitsbehörden davon ab, Lösegeldforderungen von Ransomware zu bezahlen?

- A. Eine Zahlung ermutigt die Angreifer und garantiert nicht, dass der Entschlüsselungsschlüssel geliefert wird
- B. Es macht automatisch alle Versicherungspolicen des Unternehmens ungültig
- C. Es benachrichtigt jeden Kunden automatisch per E-Mail
- D. Es beschädigt die verbleibenden System-Backup-Dateien

5. Was ist ein Notfallwiederherstellungsplan (DRP)?

- A. Ein strukturiertes Verfahren zur Wiederherstellung von Betrieb und Daten nach einer Kompromittierung des Systems
- B. Eine Firewall-Konfiguration, die eingehende Netzwerkports zuordnet
- C. Ein Datenbankschema, das die Administratorrechte der Benutzer auflistet
- D. Ein E-Mail-Authentifizierungsprotokoll, das gefälschte Domains ablehnt

Kontrollpunkt 2: Richtig oder falsch

6 Frage 6

6. Ransomware-Payloads können sich leicht auf Online-Backups ausbreiten, die mit dem Netzwerk verbunden sind.

- ○ Richtig
- ○ Falsch

7 Frage 7

7. Die Zahlung des Lösegelds in Kryptowährung garantiert, dass die Dateien erfolgreich entschlüsselt werden.

- ○ Richtig
- ○ Falsch

8 Frage 8

8. Das Trennen infizierter Systeme vom Netzwerk hilft zu verhindern, dass sich Ransomware auf benachbarte Systeme ausbreitet.

- ○ Richtig
- ○ Falsch

9 Frage 9

9. Symmetrische Kryptografie wird von Ransomware nie zum Verschlüsseln von Systemspeicher verwendet.

- ○ Richtig
- ○ Falsch

10 Frage 10

10. Das regelmäßige Testen der Verfahren zur Datenwiederherstellung ist ein wesentlicher Bestandteil der Notfallwiederherstellung.

- ○ 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. Der Zugriff auf lokale Dateien wird durch kryptografische _____ verwehrt.

2. Der aktive Schadcode, der auf einem System ausgeführt wird, ist die _____ .

3. Getrennt aufbewahrte Speicherkopien an einem externen Ort sind ein sicheres _____ .

4. Um die Ausbreitung von Malware zu stoppen, ist die _____ von Endgeräten im Netzwerk nötig.

5. Die Zahlung in Kryptowährung, die Cyberkriminelle fordern, ist das _____ .

6. Die Wiederherstellung betriebsrelevanter Dateien nach einer Katastrophe ist eine Form der _____ .

WORTSCHATZ-WORTBANK

ISOLIERUNG KATASTROPHE LÖSEGELD NUTZLAST OFFLINE-BACKUP RÜCKSICHERUNG TROJANER VERSCHLÜSSELUNG

Schreiben Sie Ihre Antworten hier:

1. **2.**

3. **4.**

5. **6.**

Kontrollpunkt 4: Zuordnung von Sicherheits-Begriffen

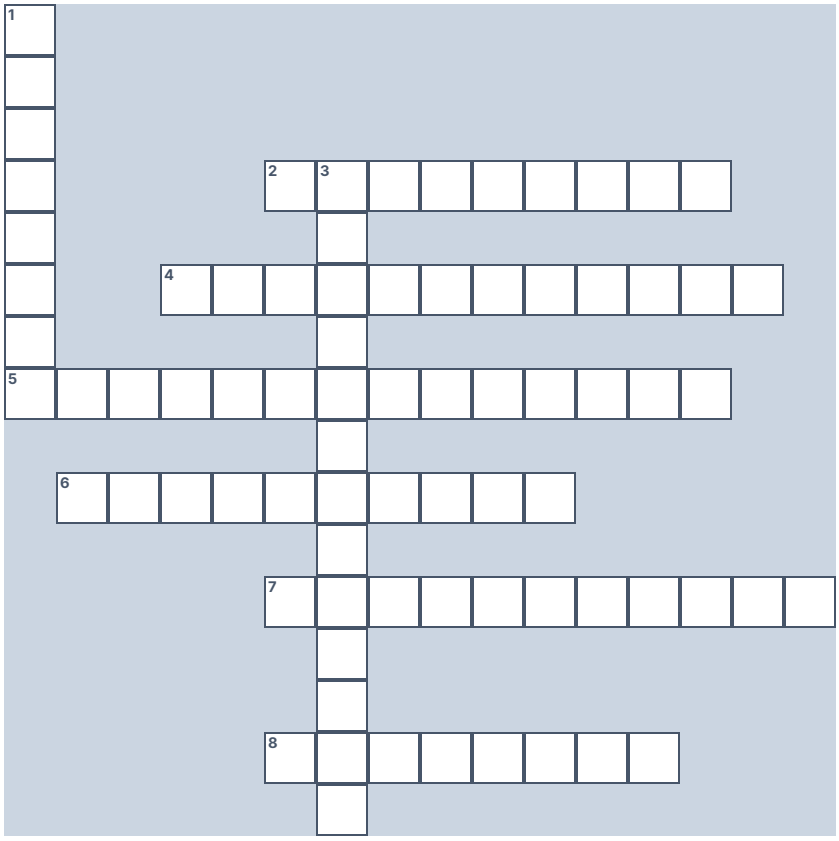
DEFINITIONEN ZUORDNEN

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

☐	1. VERSCHLÜSSELUNG	A	Trennen infizierter Netzwerksysteme.
☐	2. NUTZDATEN	B	Schädliche Datei, getarnt als harmlos.
☐	3. OFFLINE-BACKUP	C	Kryptografisches Sperren von Dateien.
☐	4. ISOLIERUNG	D	Ereignis mit schwerer Systemstörung.
☐	5. LÖSEGELD	E	Ausführen schädlicher Software.
☐	6. WIEDERHERSTELLUNG	F	Getrennte Offline-Kopie.
☐	7. KATASTROPHE	G	Wiederherstellen der Datenbank aus einem Backup.
☐	8. TROJANER	H	Anforderung einer Auszahlung per kryptografischem Schlüssel.

Kontrollpunkt 5: Kreuzworträtsel

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



WAAGERECHT

2. Zahlungsforderung für die Herausgabe des kryptografischen Schlüssels. (9)

4. Kryptografisches Sperren von Dateien. (12)

5. Wiederherstellen der Datenbank aus dem Backup. (14)

6. Trennen infizierter Systeme vom Netzwerk. (10)

7. Ereignis mit schwerer Systemstörung. (11)

8. Ausführung schädlicher Software. (8)

SENKRECHT

1. Schädliche Datei, die als harmlos getarnt ist. (8)

3. Vom Netz getrennte Datenkopie. (13)

Kontrollpunkt 5, Alternative: Barrierefreie Kreuzworträtsel-Hinweise

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

WAAGERECHT

2 waagerecht: Zahlungsforderung für die Herausgabe des kryptografischen Schlüssels. (9 Buchstaben):

4 waagerecht: Kryptografisches Sperren von Dateien. (12 Buchstaben):

5 waagerecht: Wiederherstellen der Datenbank aus dem Backup. (14 Buchstaben):

6 waagerecht: Trennen infizierter Systeme vom Netzwerk. (10 Buchstaben):

7 waagerecht: Ereignis mit schwerer Systemstörung. (11 Buchstaben):

8 waagerecht: Ausführung schädlicher Software. (8 Buchstaben):

SENKRECHT

1 senkrecht: Schädliche Datei, die als harmlos getarnt ist. (8 Buchstaben):

3 senkrecht: Vom Netz getrennte Datenkopie. (13 Buchstaben):

Kontrollpunkt 6: Suchsel

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

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

WORTSCHATZ-WORTLISTE

CHIFFRIERUNG NUTZLAST OFFLINEBACKUP ISOLIERUNG LOESEGELD
RUECKSICHERUNG KATASTROPHE TROJANER

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. CHIFFRIERUNG**
- **B. NUTZLAST**
- **C. OFFLINEBACKUP**
- **D. ISOLIERUNG**
- **E. LOESEGELD**
- **F. RUECKSICHERUNG**
- **G. KATASTROPHE**
- **H. TROJANER**

DEFINITIONEN UND ZUORDNUNGSFELDER

1. Vom Netz getrennte Datenkopie.
2. Schädliche Datei, die als harmlos getarnt ist.
3. Kryptografisches Sperren von Dateien.
4. Zahlungsforderung für die Herausgabe des kryptografischen Schlüssels.
5. Trennen infizierter Systeme vom Netzwerk.
6. Ereignis mit schwerer Systemstörung.
7. Ausführung schädlicher Software.
8. Wiederherstellen der Datenbank aus dem Backup.

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. RREFHIUCNIGF
2. UIFNFOKEPACBL
3. LGEOEDSLE
4. RHETTSPOKAA
5. LAUTZNST
6. NILRUISEGO
7. RNERHUEGSUCCIK
8. JRARTENO

Bonusaufgabe: Schnell denken

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

1	Informationen, die Sie niemals weitergeben sollten			
2	Geräte, die gehackt werden können			
3	Gründe, kein Lösegeld zu zahlen			
4	Sichere Gewohnheiten, mit denen Sie heute beginnen können			
5	Sicherheitswerkzeuge, die Sie kennen			
6	Möglichkeiten, Ihre Konten zu schützen			
7	Anzeichen, dass ein Computer infiziert ist			
8	Orte, an denen Sie ein Backup aufbewahren können			
9	Dateien, die Sie niemals verlieren möchten			
10	Wege, auf denen sich Ransomware verbreitet			
11	Dinge, die in der ersten Stunde eines Angriffs zu tun sind			
12	Personen, die Sie während eines Angriffs kontaktieren sollten			
13	Dinge, die Ransomware sperren kann			
14	Wörter rund um Cybersicherheit			
15	Organisationen, die häufig angegriffen werden			

Kontrollpunkt 8: Fallstudien zur Cybersicherheit

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

FALLSTUDIE 1: EINDÄMMUNG EINER RANSOMWARE-NUTZLAST IM UNTERNEHMEN



Szenario: In das lokale Netzwerk eines Unternehmens ist aktive Ransomware eingedrungen. Auf wichtigen Dateiservern tauchen Dateien mit der Endung .locked auf.

Diskussionsfrage: Beschreiben Sie die Schritte zur Eindämmung und skizzieren Sie das Verfahren zur Datenwiederherstellung.

FALLSTUDIE 2: BEWERTUNG VON OFFLINE-BACKUP-ARCHITEKTUREN



Szenario: Ein Unternehmen möchte eine Backup-Strategie entwerfen, die das Risiko einer Kompromittierung der Backups verringert, selbst wenn das primäre lokale Netzwerk vollständig von Ransomware übernommen wird.

Diskussionsfrage: Entwerfen Sie ein sicheres Offline-Tresorsystem für Backups.

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

4	1	20	5	14		1	21	19		4	5	13		15	6	6	12	9	14	5
									2	1	3	11	21	16						
23	9	5	4	5	18	8	5	18	19	20	5	12	12	5	14					

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 Ransomware?

Ransomware ist Schadsoftware, die den Zugriff auf Computersysteme oder Dateien blockieren soll, bis ein Lösegeld gezahlt wird.

Q2: Wie verbreitet sich Ransomware?

Über Phishing-Anhänge in E-Mails, ungepatchte Software-Schwachstellen und kompromittierte Fernzugriffssysteme. [1]

Q3: Warum wird die Zahlung in Kryptowährung verlangt?

Kryptowährungen wie Bitcoin bieten relative Anonymität, sodass Strafverfolgungsbehörden die Gelder nur schwer nachverfolgen können.

Q4: Blockiert Antivirensoftware Ransomware?

Ja, aber signaturbasierte Antivirenprogramme können bei neu erstellter Zero-Day-Ransomware versagen.

Q5: Was ist ein Air-Gap-Backup (physisch getrennte Sicherung)?

Eine Sicherungskopie ohne physische oder logische Verbindung zum Primärnetzwerk, die so vor einer Ausbreitung geschützt ist.

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

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

Q6: Was ist doppelte Erpressung?

Wenn Angreifer Dateien nicht nur verschlüsseln, sondern auch sensible Daten stehlen, um mit deren Veröffentlichung zu drohen, falls nicht gezahlt wird.

Q7: Was ist ein Decryptor (Entschlüsselungstool)?

Ein Software-Werkzeug mit dem kryptografischen Schlüssel, der nötig ist, um gesperrte Dateien wieder in Klartext herzustellen.

Q8: Wie erkennt man Ransomware frühzeitig?

Durch Überwachen der Dateisysteme auf plötzliche, massenhafte Änderungen und Umbenennungen von Dateien.

Q9: Welche Rolle spielt eine Versicherung?

Eine Cyberversicherung kann helfen, Wiederherstellungskosten zu decken, aber Deckungsbedingungen und Regeln zu Lösegeldzahlungen unterscheiden sich je nach Police.

Q10: Sollte ich ein infiziertes System neu starten?

Nein, ein Neustart kann Beweise im flüchtigen Speicher vernichten; isolieren Sie das Gerät stattdessen vom Netzwerk. [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 nutzt Ransomware asymmetrische Verschlüsselung?

Sie verwendet einen in die Malware eingebetteten öffentlichen Schlüssel, um Dateien zu verschlüsseln; zum Entschlüsseln wird der private Schlüssel des Angreifers benötigt.

Q2: Warum wird auch symmetrische Verschlüsselung verwendet?

Symmetrische Verschlüsselung (wie AES) ist schnell und kann riesige Datenbanken in Minuten sperren, während asymmetrische Schlüssel den AES-Schlüssel sichern.

Q3: Was ist logische Segmentierung?

Aufteilung von Netzwerken in isolierte Zonen, damit sich Malware nicht seitlich von Arbeitsplatzrechnern auf zentrale Server ausbreiten kann.

Q4: Was ist WORM-Speicher?

WORM-Medien (Write Once, Read Many), die verhindern, dass Backup-Daten durch Ransomware bearbeitet, überschrieben oder gelöscht werden.

Q5: Was sind Schattenkopien?

Lokale Sicherungs-Snapshots von Windows; Ransomware löscht diese meist zuerst mit Verwaltungswerkzeugen.

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

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

Q6: Wie ermöglicht der Diebstahl von Zugangsdaten Ransomware?

Angreifer kaufen geleakte Administrator-Zugangsdaten, um sich über Remotedesktops anzumelden und Ransomware manuell im gesamten Netzwerk auszuführen.

Q7: Was ist ein Probelauf zum Testen der Wiederherstellung?

Regelmäßiges Wiederherstellen von Backup-Datenbanken in isolierten Testumgebungen, um zu prüfen, ob Wiederherstellungsgeschwindigkeit und Datenintegrität die Notfallkennzahlen erfüllen.

Q8: Wie stoppt Endpoint Detection (EDR) Ransomware?

Durch Analyse des Prozessverhaltens (z. B. schnelle Verschlüsselung) und schnelles Anhalten der bösartigen Anwendung.

Q9: Was ist ein Ransomware-as-a-Service-Modell (RaaS)?

Ein Franchise-Modell, bei dem Malware-Entwickler Ransomware-Baukästen an Partner vermieten und dafür einen Anteil an den Zahlungen erhalten.

Q10: Wie löst ungepatchtes RDP Ransomware aus?

Offen erreichbare, nicht gepatchte Gateways für das Remote Desktop Protocol ermöglichen es Angreifern, Anmeldungen per Brute Force zu knacken und Malware manuell zu starten.

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

Ransomware-Akteure verwenden häufig Tools wie vssadmin.exe, um Windows-Schattenkopien zu löschen und lokale Wiederherstellungen zu verhindern. [1]

2. SICHERHEITS-EINBLICK

Symmetrische AES-256-Schlüssel werden in der Regel zum Verschlüsseln der Dateiinhalte verwendet, die dann mit öffentlichen RSA-Schlüsseln gesperrt werden.

3. SICHERHEITS-EINBLICK

Die Wiederherstellung nach einem erfolgreichen Ransomware-Angriff kann Wochen dauern, weshalb getestete Offline-Backups wichtig sind.

4. SICHERHEITS-EINBLICK

Das FBI befürwortet keine Lösegeldzahlungen und warnt, dass eine Zahlung nicht garantiert, dass Sie Ihre Daten zurückerhalten. [2]

5. SICHERHEITS-EINBLICK

Notfallwiederherstellungspläne (DRP) sollten ein Recovery Time Objective (RTO) und ein Recovery Point Objective (RPO) festlegen.

6. SICHERHEITS-EINBLICK

Das FBI empfiehlt Backups, die verschlüsselt und unveränderlich sind, also nicht geändert oder gelöscht werden können. [3]

7. SICHERHEITS-EINBLICK

Ransomware-Entwickler nutzen fortgeschrittene Verschleierungstechniken, um herkömmliche signaturbasierte Antivirenscanner zu umgehen.

8. SICHERHEITS-EINBLICK

Netzwerksegmentierung schränkt seitliche Bewegungen ein und hilft so zu verhindern, dass sich Ransomware über den zuerst infizierten Host hinaus ausbreitet. [3]

9. SICHERHEITS-EINBLICK

Offen erreichbare, schlecht gesicherte Ferndienste wie das Remote Desktop Protocol (RDP) sind ein häufiges Einfallstor für Ransomware. [1]

10. SICHERHEITS-EINBLICK

Die CISA empfiehlt, verschlüsselte Backups offline aufzubewahren, da viele Ransomware-Varianten gezielt nach erreichbaren Backups suchen und diese löschen. [1]

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] CISA. (2023). #StopRansomware Guide.

https://www.cisa.gov/stopransomware/ransomware-guide

[2] FBI Internet Crime Complaint Center. (n.d.). Ransomware.

https://www.ic3.gov/CrimeInfo/Ransomware

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[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 Frage 1

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Was ist der Hauptmechanismus eines Ransomware-Angriffs? → Kryptografische Verschlüsselung von Nutzerdateien, um den Systemzugriff zu verweigern

2 Frage 2

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Was ist ein Offline-Backup (Cold Backup)? → Eine vom Netzwerk getrennte Sicherungskopie, die vor der Ausbreitung von Malware geschützt ist

3 Frage 3

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Wie sollten Sicherheitsteams infizierte Systeme bei einem Ransomware-Angriff isolieren? → Sofort die Netzwerkkabel trennen und die WLAN-Schnittstellen deaktivieren

4 Frage 4

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Warum raten Sicherheitsbehörden davon ab, Lösegeldforderungen von Ransomware zu bezahlen? → Eine Zahlung ermutigt die Angreifer und garantiert nicht, dass der Entschlüsselungsschlüssel geliefert wird

5 Frage 5

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Was ist ein Notfallwiederherstellungsplan (DRP)? → Ein strukturiertes Verfahren zur Wiederherstellung von Betrieb und Daten nach einer Kompromittierung des Systems

Lösungsschlüssel: Kontrollpunkt 2 – Richtig oder Falsch

6 Frage 6

Richtige Antwort: Richtig

HINWEIS FÜR LEHRKRÄFTE

Ransomware-Payloads können sich leicht auf Online-Backups ausbreiten, die mit dem Netzwerk verbunden sind.

7 Frage 7

Richtige Antwort: Falsch

HINWEIS FÜR LEHRKRÄFTE

Falsch: Das FBI warnt, dass eine Zahlung keine Garantie dafür ist, dass Sie Ihre Daten zurückbekommen. [2]

8 Frage 8

Richtige Antwort: Richtig

HINWEIS FÜR LEHRKRÄFTE

Richtig: Die CISA rät, infizierte Hosts vom Netz zu trennen oder das Netzwerk offline zu nehmen, um die Ausbreitung einzudämmen.

9 Frage 9

Richtige Antwort: Falsch

HINWEIS FÜR LEHRKRÄFTE

Falsch: Ransomware verschlüsselt Dateien meist mit schnellen symmetrischen Verfahren wie AES.

10 Frage 10

Richtige Antwort: Richtig

HINWEIS FÜR LEHRKRÄFTE

Das regelmäßige Testen der Verfahren zur Datenwiederherstellung ist ein wesentlicher Bestandteil der Notfallwiederherstellung.

Vokabelschlüssel und Bewertungsraster

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

KONTROLLPUNKT 4: LÖSUNG BEGRIFFSZUORDNUNG

C 1. VERSCHLÜSSELUNG	E 2. NUTZDATEN	F 3. OFFLINE-BACKUP	A 4. ISOLIERUNG
H 5. LÖSEGELD	G 6. WIEDERHERSTELLUNG	D 7. KATASTROPHE	B 8. TROJANER

KONTROLLPUNKT 3: LÖSUNG SCHLÜSSELBEGRIFFE

1 VERSCHLÜSSELUNG	2 NUTZLAST	3 OFFLINE-BACKUP	4 ISOLIERUNG
5 LÖSEGELD	6 RÜCKSICHERUNG		

KONTROLLPUNKT 6, ALTERNATIVE: LÖSUNG WORTZUORDNUNG

1 C – OFFLINEBACKUP	2 H – TROJANER	3 A – CHIFFRIERUNG	4 E – LOESEGELD
5 D – ISOLIERUNG	6 G – KATASTROPHE	7 B – NUTZLAST	8 F – RUECKSICHERUNG

DISKUSSIONSHINWEISE FÜR LEHRKRÄFTE

Schlüsselbegriffe:
Prüfen Sie, ob die Lernenden VERSCHLÜSSELUNG, NUTZDATEN und OFFLINE-BACKUP 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.

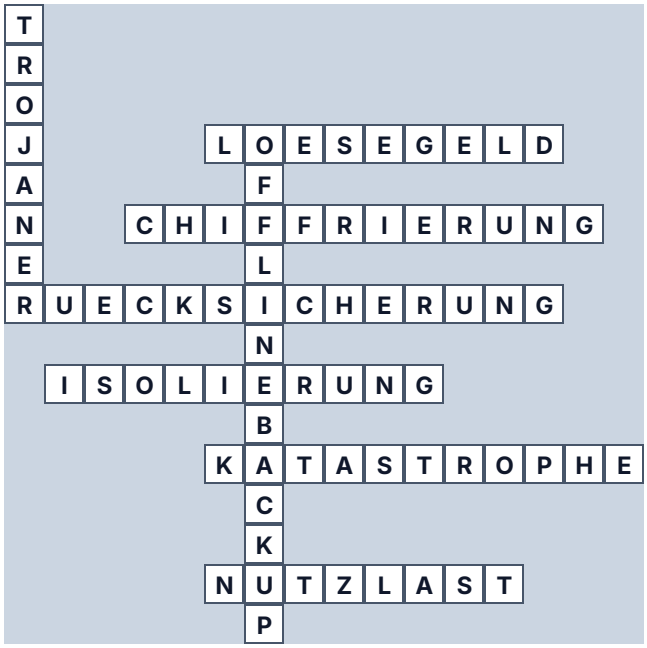
Quellenbewertung:
Lassen Sie die Lernenden mindestens eine Aussage anhand der Quellen des Arbeitsblatts prüfen und besprechen Sie, warum sich Zahlen, Preise und Regeln mit der Zeit ändern können.

Rätsellösungen und Hinweise für Lehrkräfte

LÖSUNG DES SUCHSELS

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

KREUZWORTRÄTSEL-LÖSUNG



LEITFADEN FÜR LEHRKRÄFTE ZU DEN KREUZWORTRÄTSEL-LÖSUNGEN

WAAGERECHT

2 waagerecht: LOESEGELD Zahlungsforderung für die Herausgabe des kryptografischen Schlüssels. (9 Buchstaben)

4 waagerecht: CHIFFRIERUNG Kryptografisches Sperren von Dateien. (12 Buchstaben)

5 waagerecht: RUECKSICHERUNG Wiederherstellen der Datenbank aus dem Backup. (14 Buchstaben)

6 waagerecht: ISOLIERUNG Trennen infizierter Systeme vom Netzwerk. (10 Buchstaben)

7 waagerecht: KATASTROPHE Ereignis mit schwerer Systemstörung. (11 Buchstaben)

8 waagerecht: NUTZLAST Ausführung schädlicher Software. (8 Buchstaben)

SENKRECHT

1 senkrecht: TROJANER Schädliche Datei, die als harmlos getarnt ist. (8 Buchstaben)

3 senkrecht: OFFLINEBACKUP Vom Netz getrennte Datenkopie. (13 Buchstaben)

Lösungsschlüssel für Buchstabensalat und Chiffre

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

LÖSUNGSSCHLÜSSEL BUCHSTABENSALAT

1. RREFHIUCNIGF — **CHIFFRIERUNG**
2. UIFNFOKEPACBL — **OFFLINEBACKUP**
3. LGEOEDSLE — **LOESEGELD**
4. RHETTSPOKAA — **KATASTROPHE**
5. LAUTZNST — **NUTZLAST**
6. NILRUISEGO — **ISOLIERUNG**
7. RNERHUEGSUCCIK — **RUECKSICHERUNG**
8. JRARTENO — **TROJANER**

LÖSUNGSSCHLÜSSEL ZUR GEHEIMEN CHIFFRE-AUFGABE

"DATEN AUS DEM OFFLINE BACKUP WIEDERHERSTELLEN"

Lösungsschlüssel zu den Fallstudien

A Fallstudie 1: Eindämmung einer Ransomware-Nutzlast im Unternehmen

Lösung für Lehrkräfte

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Szenarioanalyse: In ein lokales Unternehmensnetzwerk ist aktive Ransomware eingedrungen. Auf wichtigen Dateiservern erscheinen bereits Dateien mit der Endung .locked.
- Empfohlene Strategie und Lösung: Trennen Sie alle betroffenen Server vom lokalen Netzwerk. Beenden Sie aktive Administratorsitzungen. Stellen Sie nicht kompromittierte Dateien aus einem sicheren, schreibgeschützten Offline-Backup-System wieder her.

B Fallstudie 2: Bewertung von Offline-Backup-Architekturen

Lösung für Lehrkräfte

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Szenarioanalyse: Ein Unternehmen möchte eine Datensicherungsstrategie entwickeln, die das Risiko verringert, dass Backups kompromittiert werden, selbst wenn das primäre lokale Netzwerk vollständig von Ransomware übernommen wird.
- Empfohlene Strategie und Lösung: Setzen Sie WORM-Speicher (Write Once, Read Many) ein. Schaffen Sie einen logischen Air Gap, indem Sie das Backup-System von allen Netzwerken trennen, und setzen Sie eine tägliche Rotation der physischen Datenträger durch.