Name: _____ Datum: _____ Punkte: _____

Malware-Analyse und Abwehr von Bedrohungen Leitfaden

Trojaner, Ransomware, Spyware, Rootkits, Virtualisierungs-Sandboxes, Eindämmung

LERNÜBERSICHT: MALWARE-ANALYSE

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 Malware-Analyse und -Prävention. Sie lernen Spyware, Trojaner, Ransomware-Schadcode, Werkzeuge zum Reverse Engineering, das Verhalten von Rootkits und Eindämmungsstrategien 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/malware/

Ihr Lernfahrplan: Abwehr von Schadsoftware

- Unterscheiden Sie zwischen den Malware-Typen Trojaner, Wurm und Rootkit.
- Ausführung in virtualisierten Sandboxes für die Code-Analyse einsetzen.
- Entwerfen Sie Pläne zur Eindämmung und Bereinigung aktiver Ransomware-Payloads.

ANLEITUNG ZUM LEITFADEN MALWARE-ANALYSE

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: Eindämmung von Schadsoftware. Zum Schluss folgt die Bonusaufgabe Schnell denken.

MALWARE-ANALYSE UND EINDÄMMUNG VON BEDROHUNGEN (EINFÜHRUNG)

Schadcode wie Trojaner, Würmer und Ransomware stellt eine schwerwiegende Bedrohung für Endgeräte und Server dar. Sicherheitsteams analysieren Schadsoftware in virtuellen Sandboxes und isolieren Netzwerke schnell, um die Ausbreitung der Schadlast einzudämmen.

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

Kontrollpunkt 1: Auswahlaufgaben

1. Was ist das kennzeichnende Merkmal eines Trojanischen Pferdes?

- A. Es tarnt sich als legitime Software, um Nutzer zur Ausführung zu verleiten
- B. Es repliziert sich automatisch über lokale Netzwerkleitungen
- C. Es infiziert Dateien in isolierten virtuellen Sandboxes
- D. Es fängt den Datenverkehr des Internetdienstanbieters ab

2. Welche Art von Malware verschlüsselt Dateien und verlangt eine Zahlung?

- A. Ransomware
- B. Spyware
- C. Rootkit
- D. Adware

3. Was beschreibt Spyware?

- A. Malware, die heimlich Tastatureingaben und Browseraktivitäten von Nutzern überwacht
- B. Programmcode, der in einem abgeschotteten virtuellen Container (Sandbox) ausgeführt wird
- C. Anti-Malware-Updates, die aus Datenbank-Registrys heruntergeladen werden
- D. Automatische Anpassung der Bildschirmhelligkeit

4. Warum verwenden Malware-Entwickler Rootkits?

- A. Um aktive Prozesse und schädliche Dateien vor dem Betriebssystem zu verbergen
- B. Um die CPU-Verarbeitungsgeschwindigkeit auf Endgeräten zu erhöhen
- C. Um Datenbankdateien in sicheren Cloud-Tresoren zu sichern
- D. Um die Akkulaufzeit von Laptops zu verbessern

5. Was bedeutet Sandboxing in der Malware-Analyse?

- A. Ausführen verdächtiger Dateien in einem isolierten virtuellen Tresor, um ihr Verhalten gefahrlos zu beobachten
- B. Abgleich von Datei-Hashes mit Datenbanken bekannter Bedrohungen
- C. Wiederherstellen von Datenbank-Backups nach einem Einbruch
- D. Trennen lokaler Netzwerkrouter von öffentlichen Leitungen

Kontrollpunkt 2: Richtig oder falsch

6 Frage 6

6. Computerwürmer benötigen eine Interaktion des Benutzers, um sich in lokalen Netzwerken zu verbreiten.

- ◯ Richtig
- ◯ Falsch

7 Frage 7

7. Adware ist immer harmlos und verfolgt weder das Nutzerverhalten noch den Browserverlauf.

- ◯ Richtig
- ◯ Falsch

8 Frage 8

8. Durch Wiederherstellung sauberer Offline-Backups können Betroffene verschlüsselte Dateien zurückgewinnen, ohne das Lösegeld zu zahlen.

- ◯ Richtig
- ◯ Falsch

9 Frage 9

9. Signaturbasierter Virenschutz stoppt Zero-Day-Malware zuverlässig, bevor eine Signatur dafür existiert.

- ◯ Richtig
- ◯ Falsch

10 Frage 10

10. Dateilose Malware führt schädliche Skripte im Arbeitsspeicher aus und vermeidet es, Dateien auf die Festplatte zu schreiben.

- ◯ 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. Schadsoftware, die als sicheres Hilfsprogramm getarnt ist, nennt man _____ .
2. Schädliche Nutzlasten, die Datenbanksysteme gegen Geld sperren, sind _____ .
3. Keylogger, die heimlich Passwörter aufzeichnen, sind eine Form von _____ .
4. Um sich tief im Kernel des Betriebssystems zu verstecken, braucht es ein _____ .
5. Verdächtige Dateien werden in einem isolierten Bereich analysiert, einer virtuellen _____ .
6. Um die Ausbreitung aktiver Schadsoftware zu stoppen, ist eine sofortige _____ im Netzwerk erforderlich.

WORTSCHATZ-WORTBANK

DATEILOS | EINDÄMMUNG | RANSOMWARE | ROOTKIT | SANDBOX | SPYWARE | TROJANER | WURM

Schreiben Sie Ihre Antworten hier:

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

Kontrollpunkt 4: Zuordnung von Sicherheits-Begriffen

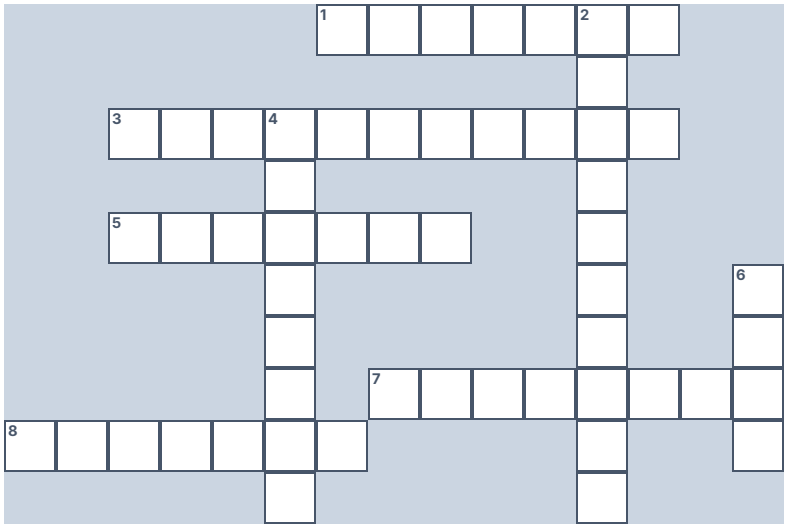
DEFINITIONEN ZUORDNEN

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

☐	1. TROJANER	A	Programm, das heimlich Nutzeraktivitäten und Eingaben überwacht und aufzeichnet.
☐	2. RANSOMWARE	B	Schadsoftware, die direkt im RAM ausgeführt wird, um der Erkennung durch Festplattenscanner zu entgehen.
☐	3. SPYWARE	C	Abschottung infizierter Endgeräte, um die Ausbreitung von Schadcode zu verhindern.
☐	4. ROOTKIT	D	Schadsoftware, getarnt als harmloses oder nützliches Hilfsprogramm.
☐	5. SANDBOX	E	Sich selbst vervielfältigende Schadsoftware, die sich ohne menschliches Zutun in Netzwerken ausbreitet.
☐	6. EINDÄMMUNG	F	Schadsoftware, die den Systemspeicher verschlüsselt und für die Herausgabe des Schlüssels eine Zahlung verlangt.
☐	7. WURM	G	Isolierte virtuelle Umgebung, in der schädliche Dateien sicher analysiert werden.
☐	8. DATEILOS	H	Getarnte Schadsoftware, die sich tief im Systemkern versteckt, um die administrative Kontrolle zu behalten.

Kontrollpunkt 5: Kreuzworträtsel

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



WAAGERECHT

1. Programm, das Nutzeraktivitäten und Eingaben heimlich überwacht und aufzeichnet. (7)

3. Isolierung infizierter Endgeräte, um die Ausbreitung schädlicher Nutzlasten zu verhindern. (11)

5. Getarnte Schadsoftware, die sich tief im Systemkern versteckt, um administrative Kontrolle zu behalten. (7)

7. Schadsoftware, die als harmloses oder nützliches Hilfsprogramm getarnt ist. (8)

8. Isolierte virtuelle Umgebung zur sicheren Analyse schädlicher Dateien. (7)

SENKRECHT

2. Schadsoftware, die den Systemspeicher verschlüsselt und für die Herausgabe des Schlüssels eine Zahlung fordert. (10)

4. Art von Schadsoftware, die direkt im RAM ausgeführt wird, um Festplattenscannern zu entgehen. (8)

6. Sich selbst vervielfältigende Schadsoftware, die sich ohne menschliches Zutun über Netzwerke verbreitet. (4)

Kontrollpunkt 5, Alternative: Barrierefreie Kreuzworträtsel-Hinweise

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

WAAGERECHT

1 waagerecht: Programm, das Nutzeraktivitäten und Eingaben heimlich überwacht und aufzeichnet. (7 Buchstaben):

3 waagerecht: Isolierung infizierter Endgeräte, um die Ausbreitung schädlicher Nutzlasten zu verhindern. (11 Buchstaben):

5 waagerecht: Getarnte Schadsoftware, die sich tief im Systemkern versteckt, um administrative Kontrolle zu behalten. (7 Buchstaben):

7 waagerecht: Schadsoftware, die als harmloses oder nützliches Hilfsprogramm getarnt ist. (8 Buchstaben):

8 waagerecht: Isolierte virtuelle Umgebung zur sicheren Analyse schädlicher Dateien. (7 Buchstaben):

SENKRECHT

2 senkrecht: Schadsoftware, die den Systemspeicher verschlüsselt und für die Herausgabe des Schlüssels eine Zahlung fordert. (10 Buchstaben):

4 senkrecht: Art von Schadsoftware, die direkt im RAM ausgeführt wird, um Festplattenscannern zu entgehen. (8 Buchstaben):

6 senkrecht: Sich selbst vervielfältigende Schadsoftware, die sich ohne menschliches Zutun über Netzwerke verbreitet. (4 Buchstaben):

Kontrollpunkt 6: Suchsel

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

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

WORTSCHATZ-WORTLISTE

TROJANER
RANSOMWARE
SPYWARE
WURM
ROOTKIT
DATEILOS
SANDBOX
EINDAEMMUNG

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. TROJANER**
- **B. RANSOMWARE**
- **C. SPYWARE**
- **D. ROOTKIT**
- **E. SANDBOX**
- **F. EINDAEMMUNG**
- **G. WURM**
- **H. DATEILOS**

DEFINITIONEN UND ZUORDNUNGSFELDER

1. Getarnte Schadsoftware, die sich tief im Systemkern versteckt, um administrative Kontrolle zu behalten.
2. Isolierung infizierter Endgeräte, um die Ausbreitung schädlicher Nutzlasten zu verhindern.
3. Art von Schadsoftware, die direkt im RAM ausgeführt wird, um Festplattenscannern zu entgehen.
4. Sich selbst vervielfältigende Schadsoftware, die sich ohne menschliches Zutun über Netzwerke verbreitet.
5. Schadsoftware, die den Systemspeicher verschlüsselt und für die Herausgabe des Schlüssels eine Zahlung fordert.
6. Programm, das Nutzeraktivitäten und Eingaben heimlich überwacht und aufzeichnet.
7. Schadsoftware, die als harmloses oder nützliches Hilfsprogramm getarnt ist.
8. Isolierte virtuelle Umgebung zur sicheren Analyse schädlicher Dateien.

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. EJATNRRO
2. SYERAWP
3. DSBXNOA
4. MRWU
5. AMEASWORRN
6. IOKRTTO
7. MAEIMGUNNED
8. EAISDOLT

Bonusaufgabe: Schnell denken

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

1	Orte, an denen Sie sichere Apps herunterladen können			
2	Geräte, die gehackt werden können			
3	Dinge, von denen Sie ein Backup machen			
4	Warnzeichen in einer E-Mail			
5	Anzeichen, dass ein Telefon Malware hat			
6	Malware-Arten, die Sie kennen			
7	Dateitypen, bei denen Sie vorsichtig sein sollten			
8	Wege, auf denen Malware auf einen PC gelangt			
9	Sichere Gewohnheiten, mit denen Sie heute beginnen können			
10	Wörter rund um Cybersicherheit			
11	Dinge, die nach einem Datenleck zu tun sind			
12	Gründe, Software zu aktualisieren			
13	Tiere oder Figuren mit Namen, die nach Malware klingen			
14	Dinge, die Malware stehlen kann			
15	Dinge, die zu tun sind, wenn Sie auf den falschen Link geklickt haben			

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. Legen Sie Eindämmungsrichtlinien fest.

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

FALLSTUDIE 2: DATEILOSE MALWARE UND SPEICHERINJEKTION



Szenario: Ein Analyst entdeckt verdächtige Skriptmuster, die mit gewöhnlichen Verwaltungswerkzeugen direkt im flüchtigen Arbeitsspeicher des Systems ausgeführt werden, ohne dass sich schädliche Dateien auf der Festplatte befinden.

Diskussionsfrage: Erklären Sie die Strategie zur Speicheranalyse und nennen Sie Werkzeuge, die dateilose Ausführung blockieren.

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

5	18	11	5	14	14	5	14		19	9	5													
19	3	8	1	4	3	15	4	5		13	9	20												
22	5	18	8	1	12	20	5	14	19	1	14	1	12	25	19	5								

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 Schadsoftware (Malware)?

Schadsoftware, die von Angreifern entwickelt wurde, um Geräte und Netzwerke zu beschädigen, zu kapern oder Daten von ihnen zu stehlen.

Q2: Was ist der Unterschied zwischen einem Virus und einem Wurm?

Ein Virus braucht zur Verbreitung menschliches Zutun (etwa das Öffnen einer Datei), während sich ein Wurm automatisch über Netzwerke verbreitet.

Q3: Wie infiziert ein Trojanisches Pferd einen Computer?

Es täuscht Nutzer, indem es sich als harmloses oder sicheres Programm tarnt und seine schädliche Nutzlast darin versteckt.

Q4: Was ist Ransomware?

Eine Art Malware, die Dateien auf dem Zielsystem verschlüsselt und eine Zahlung im Austausch für den Entschlüsselungsschlüssel verlangt. [1]

Q5: Was ist Spyware?

Schadsoftware, die heimlich Tastatureingaben, Passwörter und Surfgewohnheiten aufzeichnet, um sie an Angreifer zu senden.

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 Sandboxing?

Ausführen verdächtiger Dateien in einer sicheren, isolierten virtuellen Umgebung, um ihr Verhalten ohne Risiko für Produktivsysteme zu beobachten.

Q7: Was ist dateilose Malware?

Schadsoftware, die direkt im Arbeitsspeicher (RAM) mithilfe legitimer Hilfsprogramme läuft und keine Dateien auf die Festplatte schreibt, um einfache Scanner zu umgehen.

Q8: Wie schützt ein Rootkit Schadsoftware?

Es verbirgt schädliche Prozesse und Dateien, oft durch Manipulation des Betriebssystemkerns, sodass Antivirenscanner sie möglicherweise übersehen.

Q9: Was ist dynamische Verhaltensüberwachung?

Antiviren-Scan, der aktive Prozesse in Echtzeit überwacht, um für Schadsoftware typische Aktionen wie die massenhafte Verschlüsselung von Dateien zu blockieren.

Q10: Warum ist die Eindämmung bei der Reaktion auf Sicherheitsvorfälle so dringend?

Die Isolierung kompromittierter Endgeräte verhindert, dass sich aktive Malware auf andere Geräte im Netzwerk ausbreitet.

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

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

Q1: Wie umgehen Malware-Entwickler signaturbasierte Antivirenscanner?

Sie nutzen Polymorphie und ändern bei jeder Infektion den Hash und die Codestruktur der Datei, während das schädliche Verhalten gleich bleibt.

Q2: Welches Risiko bergen Dual-Use-Werkzeuge in Malware-Kampagnen?

Angreifer nutzen legitime Verwaltungswerkzeuge (wie PowerShell oder Sysinternals), um im normalen Netzwerkverkehr unterzutauchen, was die Erkennung erschwert.

Q3: Wie führt Process Hollowing schädliche Payloads aus?

Sie startet einen legitimen Systemprozess im angehaltenen Zustand, ersetzt seinen Speichercode durch Malware und setzt die Ausführung fort.

Q4: Welche Rolle spielt ein Command-and-Control-Server (C2)?

Ein von Hackern betriebener entfernter Server, der Befehle und Schadcode an Malware auf kompromittierten Rechnern sendet.

Q5: Warum ist Keylogging schwer zu erkennen?

Einfache Keylogger verbrauchen nur minimale CPU-Ressourcen und verstecken ihre Prozesse in legitimen Hilfsprogrammen im Benutzerbereich.

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

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

Q6: Wie verzögert Code-Verschleierung die Malware-Analyse?

Sie verschlüsselt oder verändert den Quellcode so, dass er für Analysewerkzeuge und Sicherheitsscanner unlesbar wird.

Q7: Welche Funktion hat ein Bootkit?

Ein Rootkit, das den Bootvorgang infiziert (MBR, Bootsektor oder UEFI-Firmware) und daher vor dem Betriebssystem geladen wird.

Q8: Wie erkennt heuristisches Scannen Zero-Day-Bedrohungen?

Es sucht nach verdächtigen Codemustern und Administratorbefehlen, statt nach einem passenden Hash in einer Datenbank zu suchen.

Q9: Welche Bedrohung geht von DLL-Hijacking aus?

Eine legitime Anwendung wird gezwungen, eine schädliche Dynamic Link Library (DLL) zu laden, indem diese im Verzeichnispfad der Anwendung abgelegt wird.

Q10: Wie nutzen automatisierte Malware-Analyse-Pipelines Virtualisierung?

Sie führen verdächtige Dateien auf mehreren Betriebssystem-VMs aus und erzeugen automatisch Verhaltensprotokolle und Netzwerk-PCAP-Dateien.

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

Trojaner bleiben ein verbreiteter Infektionsweg, weil sie Schadcode in harmlos wirkenden Programmen verstecken.

2. SICHERHEITS-EINBLICK

Das IC3 des FBI erhielt 2025 über 3.600 Beschwerden zu Ransomware, mit gemeldeten Verlusten von über 32 Millionen $. [3]

3. SICHERHEITS-EINBLICK

Würmer können sich schnell über Netzwerke verbreiten, indem sie ungepatchte Protokollschwachstellen ausnutzen, etwa EternalBlue in SMB.

4. SICHERHEITS-EINBLICK

Dateilose Malware ist schwer zu erkennen, weil sie über legitime Werkzeuge im Arbeitsspeicher läuft und kaum Spuren auf der Festplatte hinterlässt.

5. SICHERHEITS-EINBLICK

Analyse-Sandboxes werden in der Regel nach jedem Durchlauf auf einen sauberen Snapshot zurückgesetzt, damit jeder Test in einem bekannten Zustand beginnt.

6. SICHERHEITS-EINBLICK

Rootkits können Systemaufrufe des Kernels verändern und Anti-Malware-Scannern falsche Diagnoseergebnisse melden.

7. SICHERHEITS-EINBLICK

Code-Verschleierung nutzt Packer-Programme, um die tatsächliche Binärstruktur der Malware-Nutzlast zu komprimieren und zu verbergen.

8. SICHERHEITS-EINBLICK

Polymorphe Schadsoftware verändert ihren Code und damit ihren Datei-Hash mit jeder neuen Kopie, um Signaturprüfungen zu entgehen.

9. SICHERHEITS-EINBLICK

DLL-Hijacking nutzt die Suchreihenfolge in gängigen Betriebssystemen wie Windows aus.

10. SICHERHEITS-EINBLICK

Sicherheitsanbieter finden täglich riesige Mengen neuer Malware-Samples, daher müssen Signaturen ständig aktualisiert werden.

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. (n.d.). Malware, Phishing, and Ransomware.

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

[2] CISA. (2023). #StopRansomware Guide.

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

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

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

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

https://www.ic3.gov/CrimeInfo/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 das kennzeichnende Merkmal eines Trojanischen Pferdes? → Es tarnt sich als legitime Software, um Nutzer zur Ausführung zu verleiten

2 Frage 2

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Welche Art von Malware verschlüsselt Dateien und verlangt eine Zahlung? → Ransomware [1]

3 Frage 3

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Was beschreibt Spyware? → Malware, die heimlich Tastatureingaben und Browseraktivitäten von Nutzern überwacht

4 Frage 4

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Warum verwenden Malware-Entwickler Rootkits? → Um aktive Prozesse und schädliche Dateien vor dem Betriebssystem zu verbergen

5 Frage 5

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Was bedeutet Sandboxing in der Malware-Analyse? → Ausführen verdächtiger Dateien in einem isolierten virtuellen Tresor, um ihr Verhalten gefahrlos zu beobachten

Lösungsschlüssel: Kontrollpunkt 2 – Richtig oder Falsch

6 Frage 6

Richtige Antwort: Falsch

HINWEIS FÜR LEHRKRÄFTE

Falsch: Würmer vervielfältigen sich selbst und verbreiten sich ohne Zutun des Nutzers über Netzwerke.

7 Frage 7

Richtige Antwort: Falsch

HINWEIS FÜR LEHRKRÄFTE

Falsch: Adware ist nicht immer harmlos; ein Großteil davon verfolgt das Surfverhalten, um gezielt Werbung anzuzeigen.

8 Frage 8

Richtige Antwort: Richtig

HINWEIS FÜR LEHRKRÄFTE

Richtig: Saubere Offline-Backups stellen verschlüsselte Dateien ohne Zahlung wieder her, gestohlene Daten können jedoch trotzdem veröffentlicht werden.

9 Frage 9

Richtige Antwort: Falsch

HINWEIS FÜR LEHRKRÄFTE

Falsch: Signaturscanner benötigen ein bekanntes Muster, daher kann brandneue Zero-Day-Malware an ihnen vorbeigelangen.

10 Frage 10

Richtige Antwort: Richtig

HINWEIS FÜR LEHRKRÄFTE

Dateilose Malware führt schädliche Skripte im Arbeitsspeicher aus und vermeidet es, Dateien auf die Festplatte zu schreiben.

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. TROJANER	F 2. RANSOMWARE	A 3. SPYWARE	H 4. ROOTKIT
G 5. SANDBOX	C 6. EINDÄMMUNG	E 7. WURM	B 8. DATEILOS

KONTROLLPUNKT 3: LÖSUNG SCHLÜSSELBEGRIFFE

1 TROJANER	2 RANSOMWARE	3 SPYWARE	4 ROOTKIT
5 SANDBOX	6 EINDÄMMUNG		

KONTROLLPUNKT 6, ALTERNATIVE: LÖSUNG WORTZUORDNUNG

1 D – ROOTKIT	2 F – EINDAEMMUNG	3 H – DATEILOS	4 G – WURM
5 B – RANSOMWARE	6 C – SPYWARE	7 A – TROJANER	8 E – SANDBOX

DISKUSSIONSHINWEISE FÜR LEHRKRÄFTE

Schlüsselbegriffe:
Prüfen Sie, ob die Lernenden TROJANER, RANSOMWARE und SPYWARE 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.

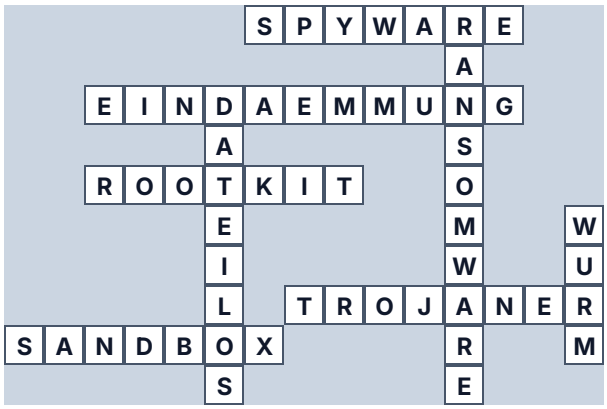
Quellenbewertung:
Lassen Sie die Lernenden mindestens eine Aussage anhand der Quellen des Arbeitsblatts prüfen und besprechen Sie, warum sich Zahlen, Preise und Regeln mit der Zeit ändern können.

Rätsellösungen und Hinweise für Lehrkräfte

LÖSUNG DES SUCHSELS

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

KREUZWORTRÄTSEL-LÖSUNG



LEITFADEN FÜR LEHRKRÄFTE ZU DEN KREUZWORTRÄTSEL-LÖSUNGEN

WAAGERECHT

1 waagerecht: SPYWARE Programm, das Nutzeraktivitäten und Eingaben heimlich überwacht und aufzeichnet. (7 Buchstaben)

3 waagerecht: EINDAEMMUNG Isolierung infizierter Endgeräte, um die Ausbreitung schädlicher Nutzlasten zu verhindern. (11 Buchstaben)

5 waagerecht: ROOTKIT Getarnte Schadsoftware, die sich tief im Systemkern versteckt, um administrative Kontrolle zu behalten. (7 Buchstaben)

7 waagerecht: TROJANER Schadsoftware, die als harmloses oder nützliches Hilfsprogramm getarnt ist. (8 Buchstaben)

8 waagerecht: SANDBOX Isolierte virtuelle Umgebung zur sicheren Analyse schädlicher Dateien. (7 Buchstaben)

SENKRECHT

2 senkrecht: RANSOMWARE Schadsoftware, die den Systemspeicher verschlüsselt und für die Herausgabe des Schlüssels eine Zahlung fordert. (10 Buchstaben)

4 senkrecht: DATEILOS Art von Schadsoftware, die direkt im RAM ausgeführt wird, um Festplattenscannern zu entgehen. (8 Buchstaben)

6 senkrecht: WURM Sich selbst vervielfältigende Schadsoftware, die sich ohne menschliches Zutun über Netzwerke verbreitet. (4 Buchstaben)

Lösungsschlüssel für Buchstabensalat und Chiffre

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

LÖSUNGSSCHLÜSSEL BUCHSTABENSALAT

1. EJATNRRO — **TROJANER**
2. SYERAWP — **SPYWARE**
3. DSBXNOA — **SANDBOX**
4. MRWU — **WURM**
5. AMEASWORRN — **RANSOMWARE**
6. IOKRTTO — **ROOTKIT**
7. MAEIMGUNNED — **EINDAEMMUNG**
8. EAISDOLT — **DATEILOS**

LÖSUNGSSCHLÜSSEL ZUR GEHEIMEN CHIFFRE-AUFGABE

"ERKENNEN SIE SCHADCODE MIT VERHALTENSANALYSE"

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. Legen Sie Maßnahmen zur Eindämmung fest.
- 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: Dateilose Malware und Speicherinjektion

Lösung für Lehrkräfte

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Szenarioanalyse: Ein Analyst entdeckt verdächtige Skriptmuster, die mit Standard-Verwaltungswerkzeugen direkt im flüchtigen Arbeitsspeicher des Systems ausgeführt werden, doch auf der Festplatte befinden sich keine schädlichen Dateien.
- Empfohlene Strategie und Lösung: Isolieren Sie die betroffenen Endgeräte und erstellen Sie zuerst ein Speicherabbild. Prüfen Sie die PowerShell- und WMI-Protokolle, blockieren Sie nicht genehmigte Skripte mit AppLocker und starten Sie dann neu, um die Schadlast zu entfernen.