Name: _____ Datum: _____ Punkte: _____

Zero-Trust-Architektur und Sicherheit

Kontinuierliche Überprüfung, Mikrosegmentierung des Netzwerks, Identitäts- und Zugriffsverwaltung, geringste Rechte und Prüfungen des Sicherheitsstatus.

LERNÜBERSICHT: ZERO-TRUST-SICHERHEIT

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 Zero-Trust-Architektur und -Sicherheit. Sie befassen sich mit fortlaufender Überprüfung, Mikrosegmentierung von Netzwerken, Identitäts- und Zugriffsmanagement (IAM), dem Prinzip der minimalen Rechte und der Prüfung von Sitzungen.

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/zero-trust-cybersicherheit/

Ihr Lernfahrplan: Zero-Trust-Strategie

- Das Kernprinzip der fortlaufenden Überprüfung verstehen.
- Netzwerk-Mikrosegmentierung und Zugriff nach dem Prinzip der minimalen Rechte umsetzen.
- Konfigurieren Sie Prüfungen des Gerätesicherheitsstatus und die Überwachung aktiver Sitzungen.

ANLEITUNG ZUM ZERO-TRUST-SICHERHEITSLEITFADEN

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: Zero-Trust-Architektur. Zum Schluss folgt die Bonusaufgabe Schnell denken.

ZERO-TRUST-ARCHITEKTUR UND SICHERHEIT (EINFÜHRUNG)

Zero-Trust-Sicherheit ersetzt alte Modelle des Netzwerkperimeters durch die strikte Richtlinie „Niemals vertrauen, immer überprüfen“. Mikrosegmentierung, Identitäts- und Zugriffsverwaltung (IAM), minimale Berechtigungen und Statusprüfungen verhindern die laterale Ausbreitung von Bedrohungen.

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

Kontrollpunkt 1: Auswahlaufgaben

1. Was ist das Grundprinzip der Zero-Trust-Sicherheit?

- A. Niemals vertrauen, jede Zugriffsanfrage unabhängig von ihrer Quelle immer überprüfen
- B. Die Annahme, dass sämtlicher Verkehr innerhalb der Unternehmensfirewall sicher ist
- C. Speichern von Datenbankdateien ohne Verschlüsselung zur Geschwindigkeitssteigerung
- D. Durchsetzen der E-Mail-Authentifizierung nur mit SPF-Einträgen

2. Was ist Netzwerk-Mikrosegmentierung?

- A. Aufteilen von Netzwerken in kleine, isolierte Zonen, um seitliche Bewegungen einzudämmen
- B. Verschlüsseln von Netzwerkkarten während der Datenübertragung
- C. Verbinden aller lokalen Server mit einer einzigen öffentlichen IP-Adresse
- D. Überwachen von Tastenanschlägen in Browsersitzungen

3. Was ist das Prinzip der minimalen Rechtevergabe (Least Privilege)?

- A. Beschränkung der Zugriffsrechte von Nutzern auf das, was für ihre Arbeit notwendig ist
- B. Standardmäßige Vergabe aller Systemrechte an jeden Benutzer
- C. Zulassen anonymer Anmeldungen an Datenbankservern des Unternehmens
- D. Konfigurieren öffentlicher WLAN-Router ohne Passwörter

4. Was ist Identity and Access Management (IAM)?

- A. Frameworks zur Verwaltung digitaler Identitäten und zur Steuerung von Systemberechtigungen
- B. Antivirenprogramme, die lokale Dateiverzeichnisse scannen
- C. Ein Backup-Speichersystem mit physisch getrennten (Air-Gap-)Medien
- D. Ein E-Mail-Gateway-Protokoll, das gefälschte Domains ablehnt

5. Was bedeutet kontinuierliche Authentifizierung?

- A. Wiederholte Überprüfung der Nutzeridentität und des Gerätestatus während einer aktiven Sitzung
- B. Ändern des Master-Passworts alle 10 Minuten
- C. Hashen von Datenbankeinträgen mit mehreren Algorithmen
- D. Verschlüsseln von Netzwerkpaketen bei der Übertragung mit TLS-Schlüsseln

Kontrollpunkt 2: Richtig oder falsch

6 Frage 6

6. Zero Trust geht davon aus, dass der gesamte Datenverkehr innerhalb der Unternehmens-Firewall sicher ist.

○ Richtig ○ Falsch

7 Frage 7

7. Mikrosegmentierung schränkt die Möglichkeiten von Angreifern ein, sich lateral zwischen internen Servern zu bewegen.

○ Richtig ○ Falsch

8 Frage 8

8. Das Prinzip der minimalen Rechte gewährt standardmäßig Zugriff auf alle Datenbankdateien.

○ Richtig ○ Falsch

9 Frage 9

9. Kontinuierliche Überprüfung validiert den Gerätezustand und die Zugangsdaten während der gesamten Anmeldesitzung.

○ Richtig ○ Falsch

10 Frage 10

10. Die Einführung von Zero Trust verringert die Auswirkungen kompromittierter Unternehmensanmeldungen.

○ 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. Wenn an jedem Zugangspunkt Zugangsdaten verlangt werden, spricht man von kontinuierlicher _____ .

2. Die Aufteilung des Unternehmensnetzes in winzige Zonen nennt man _____ im Mikromaßstab.

3. Für die Konfiguration digitaler Identitäten und Zugriffskontrollen nutzt man ein _____ .

4. Bei der Beschränkung von Nutzerberechtigungen gilt das Prinzip der _____ .

5. Bei der Bewertung angeschlossener Geräte wird der _____ geprüft.

6. Das Protokollieren und Überprüfen aktiver Sitzungen gehört zur _____ im Sicherheitsbereich.

WORTSCHATZ-WORTBANK

AUDITIERUNG | FIREWALL | GERÄTESTATUS | IAM-SYSTEM | MINIMALRECHTE
ROUTER | SEGMENTIERUNG | VERIFIZIERUNG

Schreiben Sie Ihre Antworten hier:

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

Kontrollpunkt 4: Zuordnung von Sicherheits-Begriffen

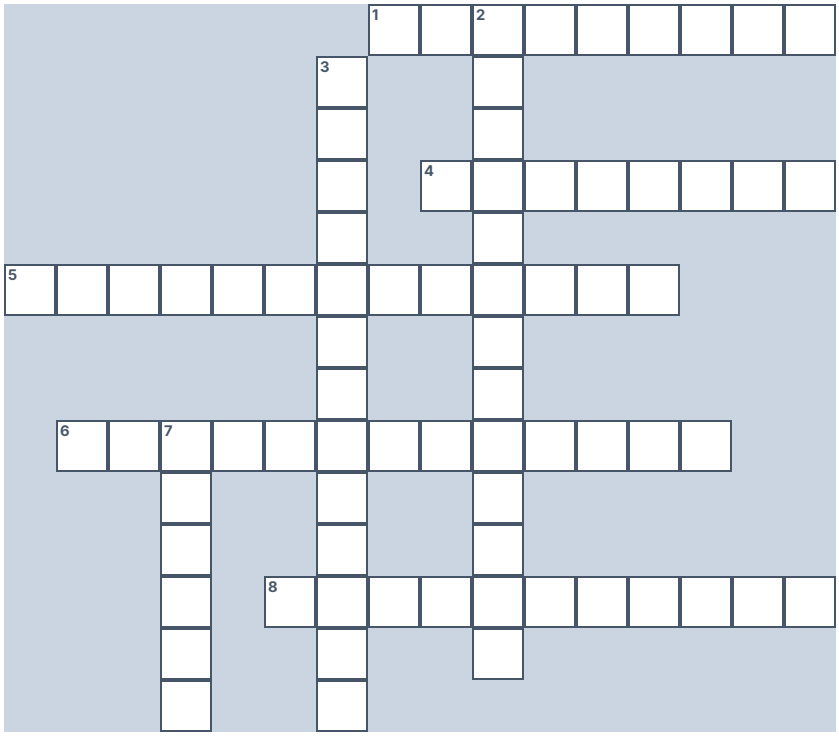
DEFINITIONEN ZUORDNEN

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

☐	1. ÜBERPRÜFUNG	A	Verwaltung des Zugriffs auf Benutzer-Zugangsdaten.
☐	2. SEGMENTIERUNG	B	Prinzip der minimalen Zugriffsrechte.
☐	3. IAM	C	Weiterleitung von Netzwerkpaketen.
☐	4. BERECHTIGUNG	D	Schutzbarriere zum externen Netzwerk.
☐	5. SICHERHEITSSTATUS	E	Überprüfung protokollierter Zugriffssitzungen.
☐	6. PRÜFUNG	F	Aufteilung interner Netzwerkzonen.
☐	7. FIREWALL	G	Ständige Überprüfung der Zugangsdaten von Nutzern.
☐	8. ROUTER	H	Bewertung des Gerätezustands.

Kontrollpunkt 5: Kreuzworträtsel

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



WAAGERECHT

1. Verwaltung des Zugriffs über Benutzeridentitäten. (9)

4. Schutzbarriere zum externen Netzwerk. (8)

5. Bewertung des Gesundheitszustands eines Geräts. (13)

6. Ständige Überprüfung der Zugangsdaten von Nutzern. (13)

8. Überprüfung protokollierter Zugriffssitzungen. (11)

SENKRECHT

2. Grundsatz der geringstmöglichen Zugriffsrechte. (13)

3. Aufteilung interner Netzwerkzonen. (13)

7. Weiterleitung von Netzwerkpaketen. (6)

Kontrollpunkt 5, Alternative: Barrierefreie Kreuzworträtsel-Hinweise

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

WAAGERECHT

1 waagerecht: Verwaltung des Zugriffs über Benutzeridentitäten. (9 Buchstaben):

4 waagerecht: Schutzbarriere zum externen Netzwerk. (8 Buchstaben):

5 waagerecht: Bewertung des Gesundheitszustands eines Geräts. (13 Buchstaben):

6 waagerecht: Ständige Überprüfung der Zugangsdaten von Nutzern. (13 Buchstaben):

8 waagerecht: Überprüfung protokollierter Zugriffssitzungen. (11 Buchstaben):

SENKRECHT

2 senkrecht: Grundsatz der geringstmöglichen Zugriffsrechte. (13 Buchstaben):

3 senkrecht: Aufteilung interner Netzwerkzonen. (13 Buchstaben):

7 senkrecht: Weiterleitung von Netzwerkpaketen. (6 Buchstaben):

Kontrollpunkt 6: Suchsel

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

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

WORTSCHATZ-WORTLISTE

VERIFIZIERUNG
SEGMENTIERUNG
IAMSYSTEM
MINIMALRECHTE
GERAETESTATUS
AUDITIERUNG
FIREWALL
ROUTER

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. VERIFIZIERUNG**
- **B. SEGMENTIERUNG**
- **C. IAMSYSTEM**
- **D. MINIMALRECHTE**
- **E. GERAETESTATUS**
- **F. AUDITIERUNG**
- **G. FIREWALL**
- **H. ROUTER**

DEFINITIONEN UND ZUORDNUNGSFELDER

_____ 1. Schutzbarriere zum externen Netzwerk.

_____ 2. Überprüfung protokollierter Zugriffssitzungen.

_____ 3. Grundsatz der geringstmöglichen Zugriffsrechte.

_____ 4. Aufteilung interner Netzwerkzonen.

_____ 5. Weiterleitung von Netzwerkpaketen.

_____ 6. Bewertung des Gesundheitszustands eines Geräts.

_____ 7. Verwaltung des Zugriffs über Benutzeridentitäten.

_____ 8. Ständige Überprüfung der Zugangsdaten von Nutzern.

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. ZRENIEIRVUG FI
2. MIESASTYM
3. EGSATUSREE TTA
4. ELLAWFIR
5. EUEGIEGNRTS NM
6. MCLAHNTEMI REI
7. RTAUEGUNDII
8. URRETO

Bonusaufgabe: Schnell denken

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

1	Informationen, die Sie niemals weitergeben sollten			
2	Sichere Gewohnheiten, mit denen Sie heute beginnen können			
3	Dinge, die an einem Gerät überprüft werden			
4	Dinge, die protokolliert werden			
5	Wörter rund um Cybersicherheit			
6	Dinge, die Zero Trust überprüft			
7	Orte, an denen Sie im Alltag einen Ausweis zeigen			
8	Möglichkeiten, nachzuweisen, dass Sie es wirklich sind			
9	Dinge, die nach einem Datenleck zu tun sind			
10	Anzeichen, dass ein Computer infiziert ist			
11	Gründe, Software zu aktualisieren			
12	Zugriffsebenen in einem Unternehmen			
13	Sicherheitswerkzeuge, die Sie kennen			
14	Zonen, in die ein Netzwerk aufgeteilt werden kann			
15	Sprichwörter über Vertrauen			

Kontrollpunkt 8: Fallstudien zur Cybersicherheit

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

FALLSTUDIE 1: UMSTIEG AUF EINE ZERO-TRUST-NETZWERKARCHITEKTUR

👷

Szenario: Ein großes Unternehmen nutzt derzeit ein flaches internes Netzwerk, in dem jedes Gerät im lokalen Netz auf alle Firmenserver und Datenbanken zugreifen kann.

Diskussionsfrage: Entwerfen Sie eine Strategie zur Mikrosegmentierung des Netzwerks, um laterale Bewegungen einzuschränken.

FALLSTUDIE 2: EINFÜHRUNG VON ZUGRIFFSKONTROLLEN NACH DEM PRINZIP DER GERINGSTEN RECHTE

👷

Szenario: Auditprotokolle zeigen, dass temporäre Datenbanknutzer und Mitarbeitende auf niedriger Ebene globale Lese- und Schreibrechte für kritische Buchhaltungsdatenbanken besitzen.

Diskussionsfrage: Prüfen und beschränken Sie die IAM-Berechtigungen für die Datenbank, um das Prinzip der geringsten Rechte durchzusetzen.

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

9	13	13	5	18		16	18	21	5	6	5	14		13	9	20
					26	5	18	15		20	18	21	19	20		
				1	18	3	8	9	20	5	11	20	21	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 Zero Trust?

Zero Trust ist ein Sicherheitskonzept, das davon ausgeht, dass Bedrohungen sowohl außerhalb als auch innerhalb der Netzwerkgrenze bestehen, und daher für jede Anfrage eine Überprüfung verlangt. [1]

Q2: Was ist die Grundregel von Zero Trust?

Niemals vertrauen, immer überprüfen.

Q3: Was ist Mikrosegmentierung?

Aufteilung eines Netzwerks in kleine, sichere logische Segmente, um den Datenverkehr zu kontrollieren und Sicherheitsvorfälle einzudämmen.

Q4: Was ist das Prinzip der minimalen Rechtevergabe (Least Privilege)?

Nutzern nur die minimalen Zugriffsrechte gewähren, die sie für ihre konkreten Arbeitsaufgaben benötigen. [2]

Q5: Wofür steht IAM?

Identitäts- und Zugriffsverwaltung.

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

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

Q6: Wie hilft ein Device Posture Check?

Es prüft, ob ein Gerät gepatcht ist, einen aktiven Virenschutz hat und sicher ist, bevor es Zugriff gewährt.

Q7: Was ist laterale Bewegung?

Das Vorgehen, mit dem sich Angreifer von einem zunächst kompromittierten Knoten aus durch ein Netzwerk zu wertvolleren Systemen bewegen.

Q8: Ersetzt Zero Trust Firewalls?

Nein, es ergänzt sie um identitätsbasierte Prüfungen und interne Segmentierungs-Firewalls.

Q9: Was ist kontinuierliche Authentifizierung?

Laufende Überprüfung der Nutzeridentität während einer aktiven Sitzung, nicht nur bei der ersten Anmeldung.

Q10: Warum ist ein flaches Netzwerk gefährlich?

In flachen Netzwerken ermöglicht ein einziger kompromittierter Knoten Angreifern, problemlos auf jede Datenbank im Netzwerk zuzugreifen.

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

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

Q1: Wie geht Zero Trust mit dem Perimetermodell um?

Es ersetzt das veraltete Modell „Burg und Graben“ und verlagert die Verteidigung von der Netzwerkgrenze auf konkrete Nutzeridentitäten und Ressourcen.

Q2: Was ist ein Policy Decision Point (PDP)?

Die Systemkomponente, die Autorisierungsanfragen anhand von Sicherheitsregeln bewertet, um zu entscheiden, ob Zugriff gewährt wird.

Q3: Was ist ein Policy Enforcement Point (PEP)?

Der Systemknoten (etwa ein Gateway oder Proxy), der Verbindungsanfragen aufgrund der PDP-Entscheidung tatsächlich zulässt oder blockiert.

Q4: Wie unterstützt die rollenbasierte Zugriffskontrolle (RBAC) Zero Trust?

RBAC fasst Berechtigungen in bestimmten Rollen zusammen und hilft so zu verhindern, dass Benutzer übermäßige Administratorrechte erben.

Q5: Was ist kontextbezogene Zugriffskontrolle?

Bewertung von Anmeldeanfragen anhand zusätzlicher Hinweise wie geografischer Standort, Gerätezustand und Anmeldezeit, um das Risiko einzuschätzen.

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

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

Q6: Worin unterscheidet sich Mikrosegmentierung von herkömmlichen VLANs?

VLANs teilen Netzwerke auf Schicht 2 in grobe logische Segmente auf, während die Mikrosegmentierung per Software-Richtlinie einzelne Workloads isoliert.

Q7: Was ist Just-in-Time-Zugriff (JIT)?

Erweiterte Administratorrechte vorübergehend gewähren und automatisch entziehen, sobald die Aufgabe erledigt ist.

Q8: Wie sichert man APIs in einem Zero-Trust-Framework?

Indem kryptografisch signierte OAuth-Token verlangt und Anfragesignaturen an jedem API-Gateway geprüft werden.

Q9: Was ist ein Zero-Trust-Network-Access-Client (ZTNA)?

Ein Software-Agent, der sichere, verschlüsselte ausgehende Verbindungen zu bestimmten Anwendungen statt zu ganzen Netzwerk-Subnetzen aufbaut.

Q10: Wie unterstützt die Auswertung von Logs Zero Trust?

Durch kontinuierliche Protokollierung können automatisierte Sicherheitsanalysewerkzeuge Anomalien erkennen und unbefugte Anmeldungen sofort sperren.

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

Zero-Trust-Architekturen ersetzen das veraltete Burg-und-Graben-Modell durch identitätsbasierte Prüfregeln.

2. SICHERHEITS-EINBLICK

Mikrosegmentierung im Netzwerk verkleinert den Bereich, den Schadsoftware erreichen kann, indem Workloads in kleine geschützte Zonen getrennt werden.

3. SICHERHEITS-EINBLICK

Zero Trust konzentriert sich auf den Schutz von Ressourcen wie Assets, Diensten und Konten statt auf Netzwerksegmente. [1]

4. SICHERHEITS-EINBLICK

Richtlinien nach dem Prinzip der minimalen Rechte verringern das Risiko, dass Insider Daten aus zentralen Datenbanken abfließen lassen.

5. SICHERHEITS-EINBLICK

Die Validierung des Gerätezustands prüft in Echtzeit den Patch-Stand des Betriebssystems und den Status des Virenschutzes.

6. SICHERHEITS-EINBLICK

Broker für Zero Trust Network Access (ZTNA) können Unternehmens-VPNs ersetzen oder ergänzen, um den Zugriffsumfang der Nutzer einzuschränken.

7. SICHERHEITS-EINBLICK

Die Just-in-Time-Vergabe (JIT) von Administratorrechten verringert das Risiko des Diebstahls von Zugangsdaten auf Domänencontrollern.

8. SICHERHEITS-EINBLICK

Kontinuierliche Validierung protokolliert und prüft das Sitzungsverhalten und sperrt Nutzer, die auffällige Muster bei der Skriptausführung zeigen.

9. SICHERHEITS-EINBLICK

Herkömmliche Perimeterabwehr kann laterale Angriffe nicht mehr stoppen, sobald ein Administrator-Zugangsdatum durchgesickert ist.

10. SICHERHEITS-EINBLICK

Die NIST Special Publication 800-207 (2020) enthält eine abstrakte Definition der Zero-Trust-Architektur mit Bereitstellungsmodellen. [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] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[2] CISA. (2023). Zero Trust Maturity Model.
https://www.cisa.gov/zero-trust-maturity-model

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

[4] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

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

Lösungsschlüssel: Kontrollpunkt 1 – Auswahlaufgaben

1 Frage 1

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Was ist das Grundprinzip der Zero-Trust-Sicherheit? → Niemals vertrauen, jede Zugriffsanfrage unabhängig von ihrer Quelle immer überprüfen

2 Frage 2

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Was ist Netzwerk-Mikrosegmentierung? → Aufteilen von Netzwerken in kleine, isolierte Zonen, um seitliche Bewegungen einzudämmen

3 Frage 3

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Was ist das Prinzip der minimalen Rechtevergabe (Least Privilege)? → Beschränkung der Zugriffsrechte von Nutzern auf das, was für ihre Arbeit notwendig ist

4 Frage 4

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Was ist Identity and Access Management (IAM)? → Frameworks zur Verwaltung digitaler Identitäten und zur Steuerung von Systemberechtigungen

5 Frage 5

Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Was bedeutet kontinuierliche Authentifizierung? → Wiederholte Überprüfung der Nutzeridentität und des Gerätestatus während einer aktiven Sitzung

Lösungsschlüssel: Kontrollpunkt 2 – Richtig oder Falsch

6 Frage 6

Richtige Antwort: Falsch

HINWEIS FÜR LEHRKRÄFTE

Falsch: Zero Trust gewährt kein implizites Vertrauen aufgrund des Netzwerkstandorts, weder innerhalb noch außerhalb.

7 Frage 7

Richtige Antwort: Richtig

HINWEIS FÜR LEHRKRÄFTE

Richtig: Kleine isolierte Zonen begrenzen, wie weit sich ein Eindringling zwischen Servern bewegen kann.

8 Frage 8

Richtige Antwort: Falsch

HINWEIS FÜR LEHRKRÄFTE

Falsch: Das Prinzip der geringsten Rechte gewährt jeder Rolle nur den minimal erforderlichen Zugriff.

9 Frage 9

Richtige Antwort: Richtig

HINWEIS FÜR LEHRKRÄFTE

Kontinuierliche Überprüfung validiert den Gerätezustand und die Zugangsdaten während der gesamten Anmeldesitzung.

10 Frage 10

Richtige Antwort: Richtig

HINWEIS FÜR LEHRKRÄFTE

Die Einführung von Zero Trust verringert die Auswirkungen kompromittierter Unternehmensanmeldungen.

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

G 1. ÜBERPRÜFUNG	F 2. SEGMENTIERUNG	A 3. IAM	B 4. BERECHTIGUNG
H 5. SICHERHEITSSTATUS	E 6. PRÜFUNG	D 7. FIREWALL	C 8. ROUTER

KONTROLLPUNKT 3: LÖSUNG SCHLÜSSELBEGRIFFE

1 VERIFIZIERUNG	2 SEGMENTIERUNG	3 IAM-SYSTEM	4 MINIMALRECHTE
5 GERÄTESTATUS	6 AUDITIERUNG		

KONTROLLPUNKT 6, ALTERNATIVE: LÖSUNG WORTZUORDNUNG

1 G – FIREWALL	2 F – AUDITIERUNG	3 D – MINIMALRECHTE	4 B – SEGMENTIERUNG
5 H – ROUTER	6 E – GERAETESTATUS	7 C – IAMSYSTEM	8 A – VERIFIZIERUNG

DISKUSSIONSHINWEISE FÜR LEHRKRÄFTE

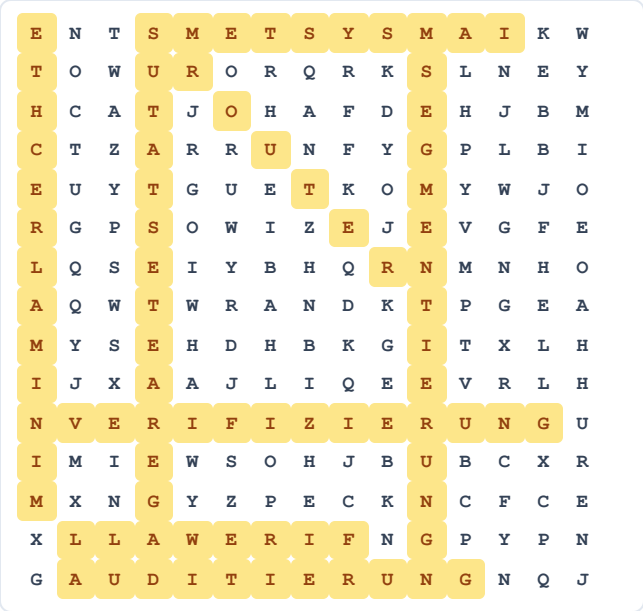
Schlüsselbegriffe:
Prüfen Sie, ob die Lernenden ÜBERPRÜFUNG, SEGMENTIERUNG und IAM in eigenen Worten erklären und jeweils ein Beispiel nennen können.

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

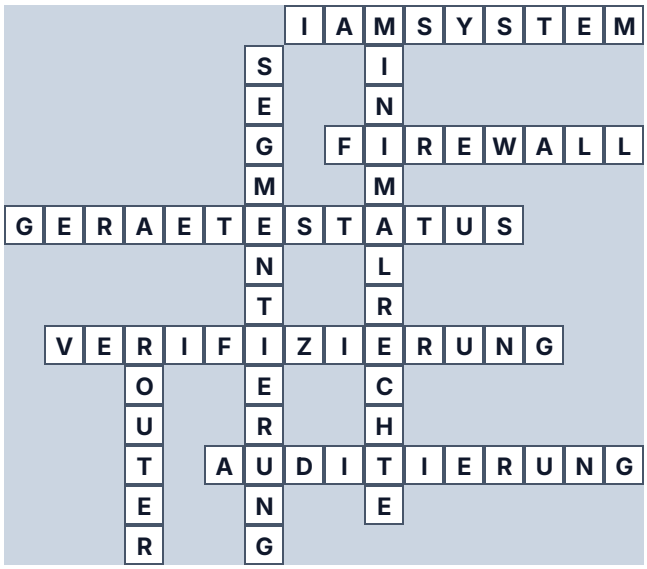
Quellenbewertung:
Lassen Sie die Lernenden mindestens eine Aussage anhand der Quellen des Arbeitsblatts prüfen und besprechen Sie, warum sich Zahlen, Preise und Regeln mit der Zeit ändern können.

Rätsellösungen und Hinweise für Lehrkräfte

LÖSUNG DES SUCHSELS



KREUZWORTRÄTSEL-LÖSUNG



LEITFADEN FÜR LEHRKRÄFTE ZU DEN KREUZWORTRÄTSEL-LÖSUNGEN

WAAGERECHT

1 waagerecht: IAMSYSTEM Verwaltung des Zugriffs über Benutzeridentitäten. (9 Buchstaben)

4 waagerecht: FIREWALL Schutzbarriere zum externen Netzwerk. (8 Buchstaben)

5 waagerecht: GERAETESTATUS Bewertung des Gesundheitszustands eines Geräts. (13 Buchstaben)

6 waagerecht: VERIFIZIERUNG Ständige Überprüfung der Zugangsdaten von Nutzern. (13 Buchstaben)

8 waagerecht: AUDITIERUNG Überprüfung protokollierter Zugriffssitzungen. (11 Buchstaben)

SENKRECHT

2 senkrecht: MINIMALRECHTE Grundsatz der geringstmöglichen Zugriffsrechte. (13 Buchstaben)

3 senkrecht: SEGMENTIERUNG Aufteilung interner Netzwerkzonen. (13 Buchstaben)

7 senkrecht: ROUTER Weiterleitung von Netzwerkpaketen. (6 Buchstaben)

Lösungsschlüssel für Buchstabensalat und Chiffre

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

LÖSUNGSSCHLÜSSEL BUCHSTABENSALAT

1. ZRENIEIRVUGFI — **VERIFIZIERUNG**
2. MIESASTYM — **IAMSYSTEM**
3. EGSATUSREETTA — **GERAETESTATUS**
4. ELLAWFIR — **FIREWALL**
5. EUEGIEGNRTSNM — **SEGMENTIERUNG**
6. MCLAHNTEMIREI — **MINIMALRECHTE**
7. RTAUEGUNDII — **AUDITIERUNG**
8. URRETO — **ROUTER**

LÖSUNGSSCHLÜSSEL ZUR GEHEIMEN CHIFFRE-AUFGABE

"IMMER PRUEFEN MIT ZERO TRUST ARCHITEKTUR"

Lösungsschlüssel zu den Fallstudien

A Fallstudie 1: Umstieg auf eine Zero-Trust-Netzwerkarchitektur

Lösung für Lehrkräfte

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Szenarioanalyse: Ein Großunternehmen nutzt derzeit ein flaches internes Netzwerk, in dem jedes Gerät im lokalen Netzwerk auf alle Unternehmensserver und Datenbanken zugreifen kann.
- Empfohlene Strategie und Lösung: Unterteilen Sie das flache Netzwerk in isolierte Abteilungszonen. Installieren Sie interne Firewalls, um den Verkehr zwischen den Zonen zu kontrollieren, und schreiben Sie für jeden Zugriff eine Validierung von Verbindungstoken vor.

B Fallstudie 2: Einführung von Zugriffskontrollen nach dem Prinzip der geringsten Rechte

Lösung für Lehrkräfte

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Szenarioanalyse: Audit-Protokolle zeigen, dass temporäre Datenbankbenutzer und Mitarbeiter mit niedriger Berechtigungsstufe globale Lese- und Schreibrechte für kritische Buchhaltungsdatenbanken besitzen.
- Empfohlene Strategie und Lösung: Entziehen Sie alle globalen Administratorrechte. Führen Sie eine rollenbasierte Zugriffskontrolle (RBAC) ein, die genau den Aufgabenbereichen entspricht, und richten Sie wöchentliche automatisierte Berechtigungsprüfungen ein.