2.16 Gesamttrainer – APIs, SaaS und Automatisierung

Dieser Gesamttrainer wiederholt die wichtigsten Inhalte des Kapitels:

- SaaS-, CRM- und Projektmanagement-Systeme
- API-Grundlagen
- REST und HTTP-Methoden
- HTTP-Statuscodes
- JSON
- Authentifizierung und OAuth 2.0
- Webhooks und Polling
- n8n-Workflows
- Fehlerbehandlung
- Sicherheit und Datenschutz
- Onboarding und Offboarding

Die Lösungen befinden sich jeweils unterhalb der Aufgabe und können aufgeklappt werden.

Teil 1 – Grundbegriffe

Aufgabe 1

Wofür steht die Abkürzung SaaS?

- A: System as a Server
- B: Software as a Service
- C: Security as a System
- D: Software and Server

Lösung anzeigen

Richtige Antwort: B

SaaS bedeutet Software as a Service. Eine Software wird als Dienst über ein Netzwerk beziehungsweise das Internet bereitgestellt.

Aufgabe 2

Welche Aussage beschreibt ein CRM-System am besten?

- A: Es verwaltet ausschließlich Netzwerkgeräte.

- B: Es speichert Kunden-, Kontakt- und Vertriebsinformationen.
- C: Es ersetzt jedes Projektmanagement-System.
- D: Es verwaltet nur Benutzerpasswörter.

Lösung anzeigen

Richtige Antwort: B

CRM bedeutet Customer Relationship Management. Ein CRM-System verwaltet Kunden, Interessenten, Kontakte, Angebote und Vertriebsprozesse.

Aufgabe 3

Welche Anwendung ist hauptsächlich ein Kollaborationssystem?

- A: Slack
- B: DHCP
- C: PostgreSQL
- D: RAID

Lösung anzeigen

Richtige Antwort: A

Slack unterstützt Kommunikation, Kanäle, Nachrichten und Zusammenarbeit innerhalb eines Unternehmens.

Aufgabe 4

Was ist eine API?

Lösung anzeigen

Eine API ist eine Programmierschnittstelle. Sie ermöglicht es unterschiedlichen Programmen, Daten auszutauschen oder Funktionen eines anderen Systems aufzurufen.

Aufgabe 5

Ordne die Begriffe richtig zu.

Begriff	Bedeutung
Client	?
Server	?
Request	?
Response	?
Endpoint	?

Lösung anzeigen

Begriff	Bedeutung
Client	sendet eine Anfrage
Server	verarbeitet die Anfrage
Request	Anfrage an ein System
Response	Antwort eines Systems
Endpoint	konkrete Adresse innerhalb einer API

Teil 2 – REST, HTTP und CRUD

Aufgabe 6

Ordne die HTTP-Methoden zu.

Methode	Aufgabe
GET	?
POST	?
PUT	?
PATCH	?
DELETE	?

Lösung anzeigen

Methode	Aufgabe
GET	Daten lesen
POST	neue Daten erstellen

Methode	Aufgabe
PUT	Ressource vollständig ersetzen
PATCH	einzelne Werte ändern
DELETE	Ressource löschen

Aufgabe 7

Was bedeutet CRUD?

Lösung anzeigen

CRUD bedeutet:

- Create
- Read
- Update
- Delete

Es beschreibt die grundlegenden Operationen zum Erstellen, Lesen, Ändern und Löschen von Daten.

Aufgabe 8

Welche Anfrage ruft den Benutzer mit der ID 15 ab?

- A: `POST /users/15`
- B: `GET /users/15`
- C: `PATCH /users`
- D: `DELETE /users/15`

Lösung anzeigen

Richtige Antwort: B

```
GET /users/15
```

GET ruft Daten ab. `/users/15` bezeichnet den Benutzer mit der ID 15.

Aufgabe 9

Welche Anfrage ändert nur die Abteilung eines Benutzers?

- A: `GET /users/15`
- B: `POST /users/15`
- C: `PATCH /users/15`
- D: `DELETE /users/15`

Lösung anzeigen

Richtige Antwort: C

```
PATCH /users/15
```

Request-Body:

```
{
  "department": "IT"
}
```

PATCH verändert einzelne Felder einer Ressource.

Aufgabe 10

Was ist der Unterschied zwischen PUT und PATCH?

Lösung anzeigen

PUT ersetzt normalerweise eine vollständige Ressource.

PATCH verändert nur einzelne Felder.

Merksatz:

> PUT ersetzt vollständig. PATCH ändert teilweise.

Aufgabe 11

Was bedeutet Idempotenz?

Lösung anzeigen

Idempotenz bedeutet, dass eine Anfrage mehrfach ausgeführt werden kann, ohne dass sich das Ergebnis nach der ersten erfolgreichen Ausführung weiter verändert.

GET, PUT und DELETE sind normalerweise idempotent.

POST ist normalerweise nicht idempotent.

Teil 3 – HTTP-Statuscodes

Aufgabe 12

Ordne die Statuscodes zu.

Code	Bedeutung
200	?
201	?
400	?
401	?
403	?
404	?
409	?
429	?
500	?
503	?

Lösung anzeigen

Code	Bedeutung
200	Anfrage erfolgreich
201	Ressource erstellt
400	fehlerhafte Anfrage
401	Authentifizierung fehlt oder ist ungültig

Code	Bedeutung
403	Berechtigung fehlt
404	Ressource nicht gefunden
409	Konflikt mit vorhandenem Zustand
429	zu viele Anfragen
500	interner Serverfehler
503	Dienst vorübergehend nicht verfügbar

Aufgabe 13

Was ist der Unterschied zwischen 401 und 403?

Lösung anzeigen

`401 Unauthorized` bedeutet, dass die Authentifizierung fehlt oder ungültig ist.

`403 Forbidden` bedeutet, dass die Identität bekannt ist, aber die benötigte Berechtigung fehlt.

Merksatz:

> 401: Wer bist du?
> 403: Du bist bekannt, darfst das aber nicht.

Aufgabe 14

Eine API antwortet mit:

```
Status: 409 Conflict

{
  "error": "Email already exists"
}
```

Was ist die wahrscheinlichste Ursache?

Lösung anzeigen

Die E-Mail-Adresse ist bereits einem vorhandenen Benutzerkonto zugeordnet.

Vor einem erneuten POST-Request sollte der bestehende Benutzer gesucht werden.

Aufgabe 15

Eine API antwortet mit:

```
Status: 429 Too Many Requests

Retry-After: 60
```

Was sollte der Workflow tun?

Lösung anzeigen

Der Workflow sollte mindestens 60 Sekunden warten und die Anfrage anschließend begrenzt erneut versuchen.

Zusätzlich sollten Rate Limit, Batch-Verarbeitung und Anzahl der Anfragen geprüft werden.

Teil 4 – JSON

Aufgabe 16

Welche JSON-Struktur ist korrekt?

A

```
{
  name: 'Max Mustermann',
  active: true,
}
```

B

```
{
  "name": "Max Mustermann",
  "active": true
}
```

C

```
[
  "name": "Max Mustermann"
]
```

Lösung anzeigen

Richtige Antwort: B

JSON verwendet:

- doppelte Anführungszeichen
- geschweifte Klammern für Objekte
- kein zusätzliches Komma nach dem letzten Feld

Aufgabe 17

Welche Datentypen besitzen die folgenden Werte?

Wert	Datentyp
`"15"`	?
`15`	?
`true`	?
`"true"`	?
`null`	?
`["IT", "Support"]`	?

Lösung anzeigen

Wert	Datentyp

`"15"`	String
`15`	Zahl
`true`	Boolean
`"true"`	String
`null`	Null-Wert
`["IT", "Support"]`	Array

Aufgabe 18

Welche Ausgabe liefert der Zugriffspfad `department.name`?

```
{
 "name": "Max Mustermann",
 "department": {
  "id": 3,
  "name": "IT"
 }
}
```

Lösung anzeigen

Die Ausgabe lautet:

```
IT
```

`department` ist ein verschachteltes Objekt. Das Feld `name` enthält den Wert `IT`.

Aufgabe 19

Was bedeutet Datenmapping?

Lösung anzeigen

Datenmapping bedeutet, dass Felder eines Quellsystems passenden Feldern eines Zielsystems zugeordnet werden.

Beispiel:

Quellsystem	Zielsystem
`firstName`	`givenName`
`lastName`	`familyName`
`mail`	`primaryEmail`

Teil 5 – Authentifizierung und Berechtigungen

Aufgabe 20

Was ist ein API-Key?

Lösung anzeigen

Ein API-Key ist ein geheimer Schlüssel, der einem Benutzer, Programm oder Projekt zugeordnet wird und den Zugriff auf eine API ermöglicht.

Er sollte geschützt gespeichert und nur mit den notwendigen Rechten ausgestattet werden.

Aufgabe 21

Wie wird ein Bearer-Token normalerweise übertragen?

Lösung anzeigen

Im Authorization-Header:

```
Authorization: Bearer ***
```

Das Token muss wie ein Passwort geschützt werden.

Aufgabe 22

Ordne die OAuth-Begriffe zu.

Begriff	Bedeutung

Access Token	?
Refresh Token	?
Scope	?
Client ID	?
Client Secret	?

Lösung anzeigen

Begriff	Bedeutung
Access Token	wird für API-Anfragen verwendet
Refresh Token	fordert ein neues Access Token an
Scope	begrenzt die erlaubten Aktionen
Client ID	identifiziert eine Anwendung
Client Secret	geheimer Nachweis einer Anwendung

Aufgabe 23

Was bedeutet Least Privilege?

Lösung anzeigen

Benutzer, Anwendungen und Workflows erhalten nur die Rechte, die sie für ihre Aufgabe tatsächlich benötigen.

Ein Workflow zum Senden von Nachrichten benötigt beispielsweise keinen Zugriff zum Löschen von Benutzern.

Aufgabe 24

Warum sollte ein Workflow nicht mit dem persönlichen Administratorkonto eines Mitarbeiters ausgeführt werden?

Lösung anzeigen

Mögliche Probleme:

- zu umfangreiche Rechte
- Abhängigkeit von einer einzelnen Person
- Ausfall beim Mitarbeiterwechsel
- schlechte Nachvollziehbarkeit
- Vermischung persönlicher und technischer Zugriffe

Besser ist ein eigener Service Account mit begrenzten Rechten.

Teil 6 – Webhooks und Polling

Aufgabe 25

Was ist der Unterschied zwischen Webhook und Polling?

Lösung anzeigen

Beim Webhook meldet das Quellsystem ein Ereignis aktiv.

Beim Polling fragt das Zielsystem regelmäßig nach neuen oder geänderten Daten.

Merksatz:

> Beim Webhook wird gesendet. Beim Polling wird nachgefragt.

Aufgabe 26

Welche Vorteile besitzt ein Webhook?

- A: Ereignisse können sofort verarbeitet werden.
- B: Es müssen ständig unnötige API-Abfragen durchgeführt werden.
- C: Die Anzahl der API-Anfragen kann reduziert werden.
- D: Ein Webhook benötigt niemals Sicherheitsmaßnahmen.

Lösung anzeigen

Richtige Antworten: A und C

Webhooks reagieren meist sofort und verursachen nur bei einem tatsächlichen Ereignis eine Übertragung.

Webhook-Endpunkte müssen trotzdem abgesichert werden.

Aufgabe 27

Ein Webhook wird zweimal empfangen und legt zwei identische Aufgaben an.

Welche Schutzmaßnahmen wären sinnvoll?

Lösung anzeigen

- Event-ID prüfen
- bereits verarbeitete Ereignisse speichern
- vorhandene Ressource suchen
- Idempotency-Key verwenden
- doppelte Trigger erkennen

Aufgabe 28

Was ist ein Replay-Angriff?

Lösung anzeigen

Bei einem Replay-Angriff wird eine bereits gültige Nachricht erneut gesendet.

Dadurch könnten Aktionen wie Benutzeranlage, Zahlung oder Aufgabenerstellung mehrfach ausgeführt werden.

Schutz bieten Event-ID, Zeitstempel und Signaturprüfung.

Teil 7 – n8n und Workflow-Logik

Aufgabe 29

Ordne die n8n-Nodes zu.

Node	Aufgabe
Webhook	?
HTTP Request	?
If	?

Node	Aufgabe
Switch	?
Edit Fields	?
Error Trigger	?

Lösung anzeigen

Node	Aufgabe
Webhook	empfängt HTTP-Anfragen
HTTP Request	ruft eine API auf
If	prüft eine Ja-Nein-Bedingung
Switch	unterscheidet mehrere Fälle
Edit Fields	verändert oder erstellt Datenfelder
Error Trigger	startet einen Fehlerworkflow

Aufgabe 30

Welche Expression liest das Feld `email` aus?

- A: `{{$json.email}}`
- B: `{{email.json}}`
- C: `{{$email.json}}`
- D: `{json.email}`

Lösung anzeigen

Richtige Antwort: A

```
{{$json.email}}
```

Aufgabe 31

Welche Expression erstellt einen vollständigen Namen?

Eingangsdaten:

```
{
  "firstName": "Max",
  "lastName": "Mustermann"
}
```

Lösung anzeigen

```
{{$json.firstName + " " + $json.lastName}}
```

Ergebnis:

```
Max Mustermann
```

Aufgabe 32

Wann sollte eine If-Node und wann eine Switch-Node verwendet werden?

Lösung anzeigen

Eine If-Node eignet sich für zwei Wege, beispielsweise wahr oder falsch.

Eine Switch-Node eignet sich für mehrere mögliche Werte, beispielsweise verschiedene Abteilungen.

Aufgabe 33

Ergänze den Workflow.

```
Webhook
  |
  v
Pflichtfelder prüfen
  |
  v
Benutzer vorhanden?
  /      \
```

```
ja          nein
|           |
v           v
 ?        Benutzer anlegen
```

Lösung anzeigen

Im Ja-Pfad sollte der Workflow beispielsweise:

- stoppen
- vorhandenen Benutzer aktualisieren
- oder eine manuelle Prüfung starten

Ein doppeltes Benutzerkonto darf nicht erstellt werden.

Teil 8 – Fehlerbehandlung

Aufgabe 34

Bei welchen Fehlern ist ein Retry meistens sinnvoll?

- A: 400 Bad Request
- B: 403 Forbidden
- C: 429 Too Many Requests
- D: 503 Service Unavailable
- E: 504 Gateway Timeout

Lösung anzeigen

Richtige Antworten: C, D und E

Diese Fehler können vorübergehend sein.

400 und 403 benötigen zunächst eine Korrektur der Anfrage beziehungsweise der Berechtigungen.

Aufgabe 35

Was bedeutet Backoff?

Lösung anzeigen

Backoff bedeutet, dass die Wartezeit zwischen mehreren Wiederholungsversuchen schrittweise erhöht wird.

Beispiel:

- 5 Sekunden
- 15 Sekunden
- 30 Sekunden
- 60 Sekunden

Aufgabe 36

Warum ist ein Retry nach einem Timeout bei einer POST-Anfrage gefährlich?

Lösung anzeigen

Die Ressource könnte im Zielsystem bereits erstellt worden sein, obwohl n8n keine Antwort empfangen hat.

Ein erneuter POST-Request könnte dadurch eine doppelte Ressource erzeugen.

Vor dem Retry sollte geprüft werden, ob der Datensatz bereits existiert.

Aufgabe 37

Welche Daten dürfen nicht vollständig in Logs gespeichert werden?

Lösung anzeigen

- Passwörter
- API-Keys
- Bearer-Tokens
- Refresh Tokens
- Client Secrets
- private Schlüssel
- besonders vertrauliche personenbezogene Daten

Aufgabe 38

Ein Workflow hat folgende Ergebnisse:

Schritt	Ergebnis
Benutzerkonto erstellt	erfolgreich
Gruppe zugewiesen	erfolgreich
Slack-Zugang erstellt	fehlgeschlagen
Hardware-Ticket erstellt	nicht ausgeführt

Darf der Workflow den Vorgang als vollständig erfolgreich markieren?

Lösung anzeigen

Nein.

Es handelt sich um einen Teilerfolg.

Erfolgreiche und fehlgeschlagene Schritte müssen getrennt dokumentiert werden. Zusätzlich sollte eine manuelle Aufgabe oder Fehlermeldung erstellt werden.

Teil 9 – Sicherheit und Datenschutz

Aufgabe 39

Ein Workflow überträgt folgende Daten an ein Kommunikationssystem:

```
{
  "name": "Max Mustermann",
  "email": "max.mustermann@example.com",
  "department": "IT",
  "salary": 50000,
  "privateAddress": "Musterstraße 1"
}
```

Benötigt werden nur Name, E-Mail und Abteilung.

Welches Prinzip wird verletzt?

Lösung anzeigen

Das Prinzip der Datenminimierung wird verletzt.

Es dürfen nur die Daten übertragen werden, die für den festgelegten Zweck benötigt werden.

Aufgabe 40

Welche Maßnahmen schützen einen öffentlichen Webhook?

Lösung anzeigen

- HTTPS
- Signaturprüfung
- API-Key oder Bearer-Token
- Event-ID
- Zeitstempel
- IP-Filter
- Rate Limit
- Eingabevalidierung
- Schutz vor Replay-Angriffen

Aufgabe 41

Warum sollten Test- und Produktivsysteme getrennt werden?

Lösung anzeigen

Damit Tests keine unbeabsichtigten Änderungen an echten Daten, Benutzern, Projekten oder Kommunikationskanälen verursachen.

Testsysteme sollten eigene Daten, Credentials und Endpoints verwenden.

Aufgabe 42

Was ist ein Audit-Log?

Lösung anzeigen

Ein Audit-Log protokolliert sicherheitsrelevante Aktionen.

Beispiele:

- Benutzer angelegt
- Rolle geändert
- Token erzeugt
- MFA deaktiviert
- Administratorrecht vergeben
- Workflow verändert

Teil 10 – Onboarding und Offboarding

Aufgabe 43

Bringe die Onboarding-Schritte in eine sinnvolle Reihenfolge.

- Benutzerkonto anlegen
- Eingangsdaten validieren
- Gruppen zuweisen
- vorhandenes Konto suchen
- Ergebnis dokumentieren
- Hardware-Aufgabe erstellen

Lösung anzeigen

1. Eingangsdaten validieren
2. vorhandenes Konto suchen
3. Benutzerkonto anlegen
4. Gruppen zuweisen
5. Hardware-Aufgabe erstellen
6. Ergebnis dokumentieren

Aufgabe 44

Warum sollte ein Benutzerkonto beim Offboarding häufig zuerst deaktiviert und nicht sofort gelöscht werden?

Lösung anzeigen

- Daten bleiben zunächst erhalten.
- Audit-Logs bleiben nachvollziehbar.
- E-Mails und Dateien können übertragen werden.

- Abhängigkeiten können geprüft werden.
- Das Konto kann bei einem Fehler wieder aktiviert werden.

Aufgabe 45

Welche Maßnahmen gehören zum Offboarding?

- A: aktive Sitzungen beenden
- B: Tokens widerrufen
- C: Administratorrechte erweitern
- D: Gruppen entfernen
- E: Lizenzen freigeben
- F: Geräte zurückfordern

Lösung anzeigen

Richtige Antworten: A, B, D, E und F

Administratorrechte dürfen beim Offboarding nicht erweitert werden.

Aufgabe 46

Warum reicht eine Passwortänderung beim Offboarding möglicherweise nicht aus?

Lösung anzeigen

Bereits aktive Sitzungen, App-Passwörter, OAuth-Verbindungen, API-Tokens oder VPN-Zertifikate könnten weiterhin gültig sein.

Diese Zugänge müssen zusätzlich beendet oder widerrufen werden.

Teil 11 – Systematische Fehlersuche

Aufgabe 47

Ein Workflow startet nicht.

Welche Prüfreihenfolge ist sinnvoll?

Lösung anzeigen

1. Ist der Workflow aktiv?
2. Ist der richtige Trigger eingerichtet?
3. Wurde das Ereignis im Quellsystem ausgelöst?
4. Ist die Webhook-URL korrekt?
5. Wird die richtige HTTP-Methode verwendet?
6. Ist der Endpoint erreichbar?
7. Ist die Authentifizierung gültig?
8. Gibt es einen Eintrag im Trigger-Log?
9. Wurde eine Test- mit einer Produktiv-URL verwechselt?

Aufgabe 48

Eine API antwortet mit `403 Forbidden`.

Welche Punkte sollten geprüft werden?

Lösung anzeigen

- Rolle des Benutzers oder Service Accounts
- Gruppenmitgliedschaften
- API-Scopes
- Administratorfreigabe
- Berechtigung für die konkrete Ressource
- verwendetes Credential

Aufgabe 49

Eine API-Anfrage liefert keinen HTTP-Statuscode.

Welche Fehlerarten kommen infrage?

Lösung anzeigen

- DNS-Fehler
- Netzwerkverbindung unterbrochen
- Port geschlossen
- Firewall blockiert
- TLS-Zertifikatsfehler

- Verbindung zurückgesetzt
- Timeout ohne Serverantwort

Ein HTTP-Statuscode kann nur empfangen werden, wenn der Server eine HTTP-Response zurücksendet.

Aufgabe 50

Bringe die Fehlersuche in eine sinnvolle Reihenfolge.

- Statuscode auswerten
- Trigger prüfen
- Authentifizierung prüfen
- Eingangsdaten prüfen
- Berechtigungen prüfen
- Netzwerk prüfen
- Endpoint und Methode prüfen
- Response-Body lesen
- Ergebnis dokumentieren

Lösung anzeigen

1. Trigger prüfen
2. Eingangsdaten prüfen
3. Netzwerk prüfen
4. Endpoint und Methode prüfen
5. Authentifizierung prüfen
6. Berechtigungen prüfen
7. Statuscode auswerten
8. Response-Body lesen
9. Ergebnis dokumentieren

Abschlussaufgabe – Vollständiger Workflow

Ein neuer Mitarbeiter wird im Personalsystem freigegeben.

Entwirf einen sicheren Ablauf mit folgenden Systemen:

- Personalsystem
- n8n
- Benutzerverwaltung
- Slack

- Ticketsystem

Berücksichtige:

- Trigger
- Validierung
- Prüfung auf Duplikate
- API-Aufrufe
- Rollen und Gruppen
- Fehlerbehandlung
- Logging
- Datenschutz

Musterlösung anzeigen

1. Das Personalsystem sendet einen signierten Webhook.
2. n8n prüft Signatur, Event-ID und Zeitstempel.
3. Pflichtfelder und Datentypen werden validiert.
4. Nur notwendige Mitarbeiterdaten werden übernommen.
5. Der vorhandene Benutzer wird über seine E-Mail-Adresse oder Mitarbeiter-ID gesucht.
6. Ist kein Benutzer vorhanden, wird das Konto über POST angelegt.
7. Gruppen und Rollen werden nach dem Least-Privilege-Prinzip zugewiesen.
8. Das Ticketsystem erhält eine Aufgabe zur Hardwarebereitstellung.
9. Slack erhält eine Nachricht ohne Passwörter oder vertrauliche Daten.
10. Jede API-Response wird auf Statuscode und Inhalt geprüft.
11. Vorübergehende Fehler erhalten einen begrenzten Retry mit Backoff.
12. Dauerhafte Fehler werden protokolliert und an die IT gemeldet.
13. Teilerfolge werden eindeutig dokumentiert.
14. Secrets werden ausschließlich über geschützte Credentials verwendet.
15. Die Event-ID wird als verarbeitet gespeichert.

Vereinfachte Darstellung:

```
      v
Event-ID prüfen
      |
      v
Benutzer suchen
  /       \
 gefunden   nicht gefunden
  |           |
  v           v
prüfen      Konto anlegen
              |
              v
         Gruppen zuweisen
              |
              v
         Hardware-Ticket
              |
              v
         Slack informieren
              |
              v
         Ergebnis protokollieren
```

Bewertung

Richtige Antworten	Einschätzung
45–50	sehr sicher
38–44	guter Stand
30–37	Grundlagen vorhanden
20–29	wichtige Bereiche wiederholen
unter 20	Kapitel systematisch erneut bearbeiten

Abschlussmerksätze

> SaaS beschreibt die Bereitstellung einer Software als Onlinedienst.

>

> Eine API ermöglicht die Kommunikation zwischen Programmen.

> Der Client sendet einen Request und der Server liefert eine Response.

> GET liest, POST erstellt, PUT ersetzt, PATCH ändert und DELETE löscht.

> 401 bedeutet fehlende Authentifizierung, 403 bedeutet fehlende Berechtigung.

> JSON verwendet Schlüssel-Wert-Paare und doppelte Anführungszeichen.

> Beim Webhook wird ein Ereignis aktiv gemeldet, beim Polling wird regelmäßig nachgefragt.

> n8n verbindet Trigger, Daten, Bedingungen und Aktionen.

> Retries müssen begrenzt und gegen Doppelverarbeitung geschützt sein.

> Secrets gehören nicht in Code, Logs oder Dokumentationen.

> Least Privilege bedeutet, nur notwendige Rechte zu vergeben.

> Eine sichere Automatisierung benötigt Validierung, Logging und Fehlerbehandlung.

Quellen

- IETF – HTTP Semantics
- IETF – JSON Data Interchange Format
- IETF – OAuth 2.0
- MDN Web Docs – HTTP
- n8n-Dokumentation
- OWASP – Authorization Cheat Sheet
- OWASP – Secrets Management Cheat Sheet