2.13 Praxisprojekt – Automatisiertes Onboarding und Offboarding

Beim Onboarding erhält ein neuer Mitarbeiter die benötigten Benutzerkonten, Geräte, Rollen und Zugriffsrechte.

Beim Offboarding werden diese Zugänge kontrolliert entzogen, Daten gesichert und Lizenzen freigegeben.

Beide Prozesse eignen sich gut für eine teilweise Automatisierung.

> Onboarding richtet Zugänge ein. Offboarding entfernt oder überträgt sie kontrolliert.

Lernziele

Nach dieser Seite solltest du erklären können:

- wie ein automatisiertes Onboarding aufgebaut ist
- welche Schritte beim Offboarding notwendig sind
- welche Systeme beteiligt sein können
- welche Daten benötigt werden
- welche Schritte automatisiert werden dürfen
- wo Freigaben notwendig sind
- wie Fehler und Teilerfolge behandelt werden
- welche Sicherheitsregeln gelten

Beteiligte Systeme

Ein Onboarding- oder Offboarding-Prozess kann mehrere Systeme verbinden.

Beispiele:

System	Aufgabe
Personalsystem	liefert Mitarbeiterdaten
n8n	steuert den Workflow
Google Workspace	E-Mail, Kalender und Benutzerkonto
Slack	interne Kommunikation
Projektmanagement-System	Aufgaben und Projekte

System	Aufgabe
Ticketsystem	Hardware- und Supportaufgaben
Geräteverwaltung	Laptop und Smartphone
CRM-System	Zugriff für Vertrieb oder Kundenbetreuung
Dokumentation	Protokoll und Anleitungen

Benötigte Eingangsdaten

Typische Onboarding-Daten:

```
{
  "employeeId": "EMP-105",
  "firstName": "Max",
  "lastName": "Mustermann",
  "email": "max.mustermann@example.com",
  "department": "IT",
  "role": "IT Support",
  "startDate": "2026-08-03",
  "manager": "Teamleitung IT"
}
```

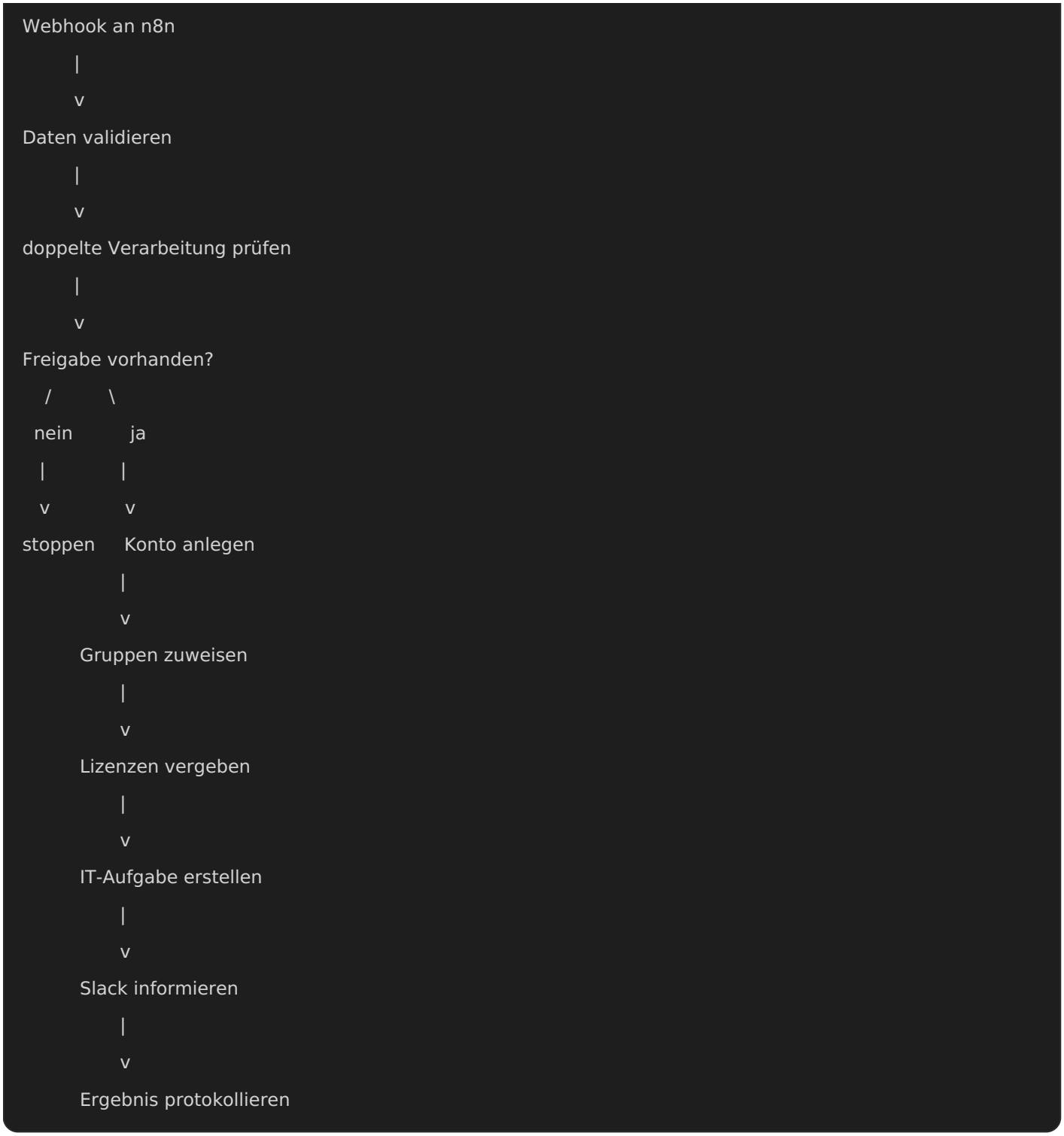
Wichtige Pflichtfelder:

- eindeutige Mitarbeiter-ID
- Vorname
- Nachname
- dienstliche E-Mail-Adresse
- Abteilung
- Rolle
- Startdatum
- zuständige Führungskraft

Onboarding-Ablauf

Ein möglicher automatisierter Ablauf:

```
Mitarbeiter freigegeben
        |
        v
```



Schritt 1: Trigger

Der Workflow startet beispielsweise durch:

- Webhook aus dem Personalsystem
- neue Zeile in einer Datenquelle
- freigegebenes Formular
- manuelle Ausführung
- festgelegten Zeitplan

Beispielereignis:

```
{
 "eventId": "evt-20015",
 "event": "employee.approved"
}
```

Die Event-ID verhindert eine doppelte Verarbeitung.

Schritt 2: Daten validieren

Vor der Verarbeitung werden geprüft:

- Pflichtfelder vorhanden
- E-Mail-Adresse gültig
- Startdatum plausibel
- Abteilung bekannt
- Rolle erlaubt
- Mitarbeiter-ID eindeutig
- keine unerlaubten Sonderzeichen
- keine unnötigen Daten enthalten

Fehlerhafte Daten dürfen nicht automatisch weiterverarbeitet werden.

Schritt 3: Vorhandene Konten prüfen

Vor dem Anlegen sollte geprüft werden, ob bereits ein Konto existiert.

Beispiel:

```
GET /users?email=max.mustermann@example.com
```

Mögliche Ergebnisse:

Ergebnis	Reaktion
kein Konto vorhanden	Benutzer anlegen
Konto vorhanden	Workflow stoppen oder prüfen
mehrere Treffer	manuelle Bearbeitung
API-Fehler	Fehlerpfad starten

Dadurch werden doppelte Benutzerkonten vermieden.

Schritt 4: Benutzerkonto anlegen

Beispiel:

```
POST /users

{
  "name": "Max Mustermann",
  "email": "max.mustermann@example.com",
  "department": "IT",
  "active": true
}
```

Mögliche Response:

```
Status: 201 Created

{
  "id": 105,
  "email": "max.mustermann@example.com"
}
```

Die neue Benutzer-ID sollte gespeichert werden.

Schritt 5: Gruppen und Rollen zuweisen

Die Abteilung kann bestimmen, welche Gruppen benötigt werden.

Beispiel:

Abteilung	Gruppen
IT	Mitarbeitende, IT-Support
Vertrieb	Mitarbeitende, CRM
Buchhaltung	Mitarbeitende, Finance
Projektmanagement	Mitarbeitende, Projekte

Beispielablauf:

```
Abteilung prüfen
  /     |      \
 IT   Vertrieb  Buchhaltung
 |      |         |
 v      v         v
IT-Gruppe CRM     Finance
```

Berechtigungen müssen nach dem Least-Privilege-Prinzip vergeben werden.

Schritt 6: Lizenzen vergeben

Mögliche Lizenzen:

- Google Workspace
- Slack
- Projektmanagement-System
- CRM-System
- Office-Anwendungen
- VPN
- weitere Fachsoftware

Vor der Vergabe sollte geprüft werden:

- Wird die Lizenz wirklich benötigt?
- Welche Lizenzstufe ist erforderlich?
- Sind noch freie Lizenzen vorhanden?
- Ist die Lizenz kostenpflichtig?
- Muss eine Freigabe erfolgen?

Schritt 7: Hardware-Aufgabe erstellen

Eine Aufgabe kann automatisch im Ticketsystem angelegt werden.

Beispiel:

```
{
  "title": "Laptop für Max Mustermann vorbereiten",
  "department": "IT",
  "startDate": "2026-08-03",
  "priority": "normal"
}
```

Mögliche Teilaufgaben:

- Laptop auswählen
- Betriebssystem aktualisieren
- Software installieren
- Festplattenverschlüsselung prüfen
- Geräteeigentümer eintragen
- MFA vorbereiten
- Übergabe dokumentieren

Schritt 8: Benachrichtigung senden

Nach erfolgreicher Vorbereitung kann eine Nachricht gesendet werden.

Beispiel:

```
Onboarding für Max Mustermann wurde vorbereitet.

Konto: erstellt
Gruppen: zugewiesen
Hardware-Aufgabe: erstellt
Startdatum: 03.08.2026
```

Die Nachricht darf keine Passwörter, Tokens oder vertraulichen Personaldaten enthalten.

Schritt 9: Ergebnis protokollieren

Protokolliert werden sollten:

- Mitarbeiter-ID
- Zeitpunkt
- ausgeführte Schritte
- erstellte Konten
- zugewiesene Gruppen
- vergebene Lizenzen
- fehlgeschlagene Schritte
- zuständige Person
- Workflow-Ausführung

Beispiel:

Schritt	Ergebnis
Benutzerkonto	erfolgreich

Schritt	Ergebnis
IT-Gruppe	erfolgreich
Slack-Zugang	erfolgreich
Hardware-Ticket	erfolgreich
MFA	noch offen

Manuelle Freigaben

Nicht jeder Schritt sollte vollständig automatisch erfolgen.

Freigaben können sinnvoll sein bei:

- Administratorrechten
- Zugriff auf Finanzsysteme
- Zugriff auf sensible Kundendaten
- teuren Softwarelizenzen
- besonderen Sicherheitsrollen
- externen Benutzerkonten
- privilegierten VPN-Zugängen

Beispiel:

Offboarding

Ein Offboarding beginnt, wenn ein Mitarbeiter das Unternehmen verlässt oder keinen Zugriff mehr benötigt.

Typische Eingangsdaten:

```
{
  "employeeId": "EMP-105",
  "email": "max.mustermann@example.com",
  "endDate": "2027-01-22",
  "manager": "Teamleitung IT"
}
```

Offboarding-Ablauf

```
Austritt freigegeben
        |
        v
Identität prüfen
        |
        v
Zeitpunkt festlegen
        |
        v
aktive Sitzungen beenden
        |
        v
Benutzerkonto sperren
        |
        v
Tokens widerrufen
        |
        v
Gruppen entfernen
        |
        v
Daten übertragen
        |
        v
Lizenzen freigeben
        |
        v
Geräte zurückfordern
        |
```

```
      v
Vorgang dokumentieren
```

Konto deaktivieren statt sofort löschen

Benutzerkonten sollten häufig zuerst deaktiviert werden.

Vorteile:

- Daten bleiben erhalten
- E-Mails können übertragen werden
- Audit-Logs bleiben nachvollziehbar
- Konto kann bei Fehlern wieder aktiviert werden
- Abhängigkeiten können geprüft werden

Beispiel:

```
PATCH /users/105

{
  "active": false
}
```

Eine endgültige Löschung kann später nach internen Regeln erfolgen.

Aktive Sitzungen beenden

Beim Offboarding sollten aktive Sitzungen beendet werden.

Dazu gehören:

- Browser-Sitzungen
- mobile Apps
- Desktop-Anwendungen
- VPN-Verbindungen
- gespeicherte Anmeldungen
- OAuth-Verbindungen

Nur das Passwort zu ändern reicht möglicherweise nicht aus.

Tokens und API-Zugänge widerrufen

Zu prüfen sind:

- API-Keys
- Bearer-Tokens
- Refresh Tokens
- persönliche Zugriffstokens
- SSH-Schlüssel
- VPN-Zertifikate
- App-Passwörter

Persönliche Tokens dürfen nach dem Austritt nicht aktiv bleiben.

Datenübertragung

Vor der Sperrung oder Löschung können Daten übertragen werden.

Beispiele:

- E-Mails an Führungskraft übertragen
- Dateien einem Team zuweisen
- Kalendertermine übergeben
- Projekte neu zuordnen
- offene Aufgaben übertragen
- persönliche Freigaben entfernen

Der Verantwortliche für die Datenübernahme muss festgelegt sein.

Lizenzen freigeben

Nach dem Offboarding können Lizenzen entfernt und erneut vergeben werden.

Beispiele:

- Google Workspace
- CRM
- Projektmanagement
- Office
- VPN
- Fachsoftware

Dadurch werden unnötige Kosten vermieden.

Geräte und Hardware

Zu prüfen sind:

- Laptop zurückgegeben
- Smartphone zurückgegeben
- Sicherheitsschlüssel zurückgegeben
- Zugangskarte deaktiviert
- lokale Daten gesichert
- Gerät zurückgesetzt
- Inventarsystem aktualisiert

Der Workflow kann dafür automatisch Aufgaben erstellen, die eigentliche Übergabe erfolgt jedoch manuell.

Zeitgesteuertes Offboarding

Ein Offboarding kann für einen bestimmten Zeitpunkt vorbereitet werden.

Beispiel:

> “ Konto am letzten Arbeitstag um 18:00 Uhr deaktivieren.

Dabei müssen Zeitzone und Austrittszeitpunkt eindeutig sein.

Kritische Zugänge können auch sofort gesperrt werden, wenn:

- ein Sicherheitsvorfall besteht
- der Austritt kurzfristig erfolgt
- Missbrauch vermutet wird
- eine ausdrückliche Anweisung vorliegt

Teilerfolge behandeln

Beispiel:

Schritt	Ergebnis
Konto deaktiviert	erfolgreich
Sitzungen beendet	erfolgreich
Slack-Zugang entfernt	fehlgeschlagen
Datenübertragung	noch offen
Lizenz entfernt	nicht ausgeführt

Der Vorgang ist nicht vollständig abgeschlossen.

Der Workflow sollte:

- fehlgeschlagene Schritte markieren
- abhängige Aktionen prüfen
- IT benachrichtigen
- manuelle Aufgabe erstellen
- Teilerfolg dokumentieren

Fehlerbehandlung

Mögliche Fehler:

- Benutzer nicht gefunden
- mehrere Benutzer mit gleicher E-Mail
- fehlende Berechtigung
- API nicht erreichbar
- Konto bereits deaktiviert
- Datenübertragung nicht möglich
- zuständige Führungskraft fehlt
- Lizenzsystem antwortet nicht

Behandlung:

```
Fehler erkannt
      |
      v
sicherheitskritisch?
   /        \
 ja          nein
 |            |
 v            v
sofort       Retry oder
eskalieren   Aufgabe erstellen
```

Rollback

Beim Onboarding kann ein Rollback sinnvoll sein.

Beispiel:

1. Konto wurde angelegt.
2. erforderliche Sicherheitsgruppe konnte nicht zugewiesen werden.
3. Konto wird vorsorglich deaktiviert.

4. IT erhält eine Fehlermeldung.

Beim Offboarding ist ein vollständiger Rollback häufig schwieriger.

Deshalb sollten kritische Schritte gut dokumentiert und möglichst reversibel sein.

Sicherheitsregeln

- Service Account verwenden
- nur notwendige Scopes vergeben
- keine Passwörter in Logs speichern
- Webhook authentifizieren
- Event-ID prüfen
- Eingabedaten validieren
- Administratorrechte nur nach Freigabe
- Test- und Produktivsysteme trennen
- sensible Daten minimieren
- alle wichtigen Änderungen protokollieren

Praxisablauf Onboarding

1. Personalsystem sendet Webhook.
2. Signatur und Event-ID werden geprüft.
3. Pflichtfelder werden validiert.
4. Vorhandenes Konto wird gesucht.
5. Benutzerkonto wird angelegt.
6. Gruppen werden anhand der Abteilung zugewiesen.
7. notwendige Lizenzen werden vergeben.
8. Hardware-Ticket wird erstellt.
9. IT wird benachrichtigt.
10. Ergebnis wird protokolliert.
11. offene Schritte werden markiert.

Praxisablauf Offboarding

1. Austritt wird freigegeben.
2. Benutzerkonto wird eindeutig identifiziert.
3. Zeitpunkt der Sperrung wird geprüft.
4. Sitzungen und Tokens werden widerrufen.
5. Konto wird deaktiviert.
6. Gruppen und Rollen werden entfernt.
7. Daten und Aufgaben werden übertragen.
8. Lizenzen werden freigegeben.
9. Geräteaufgabe wird erstellt.

10. Abschluss wird dokumentiert.
11. offene Punkte werden eskaliert.

Systematische Fehlersuche

Wenn ein Onboarding oder Offboarding fehlschlägt:

1. Wurde der richtige Trigger ausgelöst?
2. Ist die Event-ID eindeutig?
3. Sind alle Pflichtfelder vorhanden?
4. Ist der Benutzer eindeutig identifizierbar?
5. Existiert bereits ein Konto?
6. Sind die Credentials gültig?
7. Besitzt der Service Account ausreichende Rechte?
8. Welche Node ist fehlgeschlagen?
9. Welcher Statuscode wurde zurückgegeben?
10. Welche Schritte waren bereits erfolgreich?
11. Besteht ein Sicherheitsrisiko?
12. Ist ein Retry gefahrlos möglich?
13. Muss das Konto vorsorglich deaktiviert werden?
14. Welche manuelle Aufgabe muss erstellt werden?

Wichtige Begriffe

Begriff	Bedeutung
Onboarding	technische Einrichtung eines Mitarbeiters
Offboarding	kontrollierter Entzug von Zugängen
Event-ID	eindeutige Kennung eines Ereignisses
Service Account	technischer Benutzer für Automatisierungen
Freigabe	bestätigte Erlaubnis für eine Aktion
Deaktivierung	Zugang sperren, Daten zunächst erhalten
Datenübertragung	Übergabe von Dateien, E-Mails oder Aufgaben
Teilerfolg	nur ein Teil des Prozesses war erfolgreich
Rollback	bereits ausgeführte Änderungen zurücknehmen
Inventarsystem	verwaltet Geräte und Eigentümer

Gesamtmerksatz

> Ein automatisiertes Onboarding legt Benutzerkonten, Gruppen, Lizenzen und Aufgaben nach festgelegten Regeln an. Beim Offboarding werden Sitzungen, Tokens, Rollen und Zugänge kontrolliert entfernt, Daten übertragen und Lizenzen freigegeben. Kritische Rechte benötigen Freigaben und jeder Schritt muss nachvollziehbar protokolliert werden.

Kontrollfragen

Was ist Onboarding?

Die technische Einrichtung eines neuen Mitarbeiters.

Was ist Offboarding?

Der kontrollierte Entzug von Konten, Rechten und Zugängen beim Austritt.

Warum sollte vor dem Anlegen eines Kontos gesucht werden?

Damit kein doppeltes Benutzerkonto entsteht.

Warum wird ein Konto häufig zunächst deaktiviert statt gelöscht?

Damit Daten, Protokolle und Abhängigkeiten erhalten bleiben.

Welche Schritte benötigen häufig eine manuelle Freigabe?

Administratorrechte, sensible Datenzugriffe und kostenintensive Lizenzen.

Warum müssen aktive Sitzungen beendet werden?

Weil ein Benutzer trotz Passwortänderung noch angemeldet sein könnte.

Was muss mit persönlichen API-Tokens geschehen?

Sie müssen widerrufen werden.

Was ist ein Teilerfolg?

Einige Schritte wurden erfolgreich ausgeführt, andere sind fehlgeschlagen.

Warum ist die Event-ID wichtig?

Sie verhindert eine doppelte Verarbeitung desselben Vorgangs.

Warum dürfen Passwörter nicht im Workflow-Log stehen?

Weil Logs sonst selbst zu einem Sicherheitsrisiko werden.

Quellen

- NIST – Least Privilege
- OWASP – Authorization Cheat Sheet
- OWASP – Secrets Management Cheat Sheet
- n8n-Dokumentation – Workflows
- n8n-Dokumentation – Error Handling