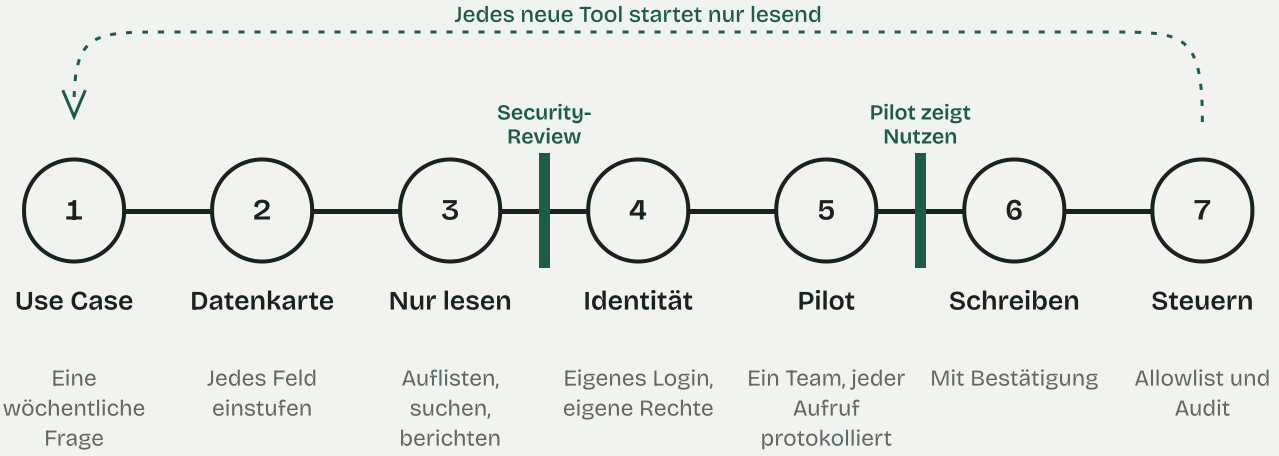


Dominik Heinrich, Multi-Cloud DevOps & AI Solution Architect

Ihr Unternehmen mit MCP an KI anbinden

Wie ich Werkzeuge und Daten über das Model Context Protocol sicher an Claude, ChatGPT und Coding-Agenten anbinde. Sieben Schritte vom ersten Read-only-Server bis zum Einsatz im ganzen Unternehmen.



Sieben Schritte, zwei Gates. Die KI handelt immer nur mit den Rechten der Person, die sie nutzt.

Aus zwei produktiven Plattformen, die ich gebaut habe, anonymisiert

100 %	**0**	**Wöchentlich**	**2**
der App-Oberfläche auch für KI-Agenten per MCP nutzbar	Personendaten in der Read-only-API und dem MCP-Server eines Kunden	automatisiert ein Kunde seine Planung per MCP	produktive Plattformen mit eigenem MCP-Server

Die sieben Schritte

Vom ersten Read-only-Server bis zum Einsatz im ganzen Unternehmen. Abhaken, sobald sie live sind.

01 Mit einer Frage starten, die jede Woche kommt

- [ ] Einen Anwendungsfall mit klarer Verantwortung wählen: Wochenplanung, Sales-Report, Ticket-Triage, Kostenfragen.
- [ ] Aufschreiben, welche Daten die Antwort braucht und wer sie sehen darf.
- [ ] Messen, wie lange es heute dauert, damit der Unterschied später sichtbar wird.

02 Die Daten kennen, bevor man sie öffnet

- [ ] **Jedes Feld einstufen:** öffentlich, intern, personenbezogen, geheim.
- [ ] Personenbezogene und geheime Daten bleiben in der ersten Version draussen. Aggregate reichen meist.
- [ ] Daten, die das eigene Netz nie verlassen dürfen: über denselben MCP-Server an ein lokales Modell geben.

03 Zuerst nur lesen

- [ ] **Der erste Server liest nur:** auflisten, suchen, berichten. Kein Anlegen, Ändern oder Löschen.
- [ ] Ein Tool, eine Aufgabe, mit klarem Namen und einer Beschreibung, die das Modell versteht.
- [ ] Kleine, strukturierte Antworten statt ganzer Tabellen: schneller, günstiger und weniger Datenabfluss.

04 Identität und Schlüssel

- [ ] Jede Person verbindet sich mit der eigenen Identität (OAuth oder OIDC), der Agent handelt also mit deren Rechten, nie mit mehr.
- [ ] API-Keys gehasht gespeichert, pro Tool eingeschränkt, mit Ablaufdatum und Widerruf.
- [ ] Niemals ein gemeinsames Admin-Token.

05 Pilot mit einem Team

- [ ] Fünf bis zehn Personen, zwei Wochen, ein Kanal für Feedback.
- [ ] **Jeden Tool-Aufruf protokollieren:** wer, welches Tool, welche Parameter, wie lange, was zurückkam.
- [ ] Rate-Limits und ein Kostendeckel pro Person ab dem ersten Tag.

06 Schreibzugriffe mit Bestätigung

- [ ] Schreiben nur dort, wo der Pilot den Nutzen gezeigt hat, und jede Aktion bestätigt die Person, bevor sie läuft.
- [ ] Destruktive Aktionen (Löschen, Zahlungen, Berechtigungen) kommen zuletzt, mit ausdrücklicher Bestätigung und denselben Rechten wie in der Oberfläche.
- [ ] Jeder Schreibzugriff ist umkehrbar oder mindestens mit Zustand vorher und nachher protokolliert.

07 Skalieren und steuern

- [ ] Eine freigegebene Liste von MCP-Servern und KI-Clients für das Unternehmen; alles andere per Policy gesperrt.
- [ ] **Neue Tools wie Code prüfen:** Pull Request, Security-Check, eine verantwortliche Person.
- [ ] Ein Monatsbericht zu Nutzung, Fehlern und gesparten Stunden.

Einführung nach Unternehmensgrösse

Startup: ein Server für das eigene Produkt, damit Kunden und Team direkt aus ihrem KI-Assistenten darin arbeiten.

Mittelstand: ein Server pro Kernsystem (ERP, CRM, Ticketing) hinter Single Sign-on.

Konzern: ein zentrales Gateway mit Allowlist, Audit-Logs und Datenklassifizierung, dazu lokale Modelle für vertrauliche Daten.

Die häufigsten Fehler

- Mit Schreibrechten starten, weil die Demo dann besser aussieht.
- Ein gemeinsamer Admin-Key für alle, und im Audit-Trail steht niemand.
- Ganze Datenbanktabellen zurückgeben und sich dann über Kosten und Datenabfluss wundern.
- Personendaten anbinden, bevor jemand den Datenschutz gefragt hat.
- Ungeprüfte Community-MCP-Server auf Laptops mit Firmendaten.

So arbeiten wir zusammen

Dieselbe Qualität für ein Startup mit zehn Leuten und einen globalen Konzern. Das Format passt sich Ihnen an.

Startups **Fractional DevOps- & KI-Lead**	Ein paar Tage im Monat: Architektur, Release-Pipeline und KI-Funktionen, damit sich die Gründer auf Kunden konzentrieren können. Vom Prototyp in die Produktion, ohne Neubau.
KMU und Mittelstand **Ein Projekt mit klarem Ergebnis**	Ein klares Ziel wie tiefere Cloud-Kosten, eine Migration oder die ersten KI-Agenten in Produktion, mit festem Umfang, wöchentlichem Fortschritt und einer Übergabe, die Ihr Team betreiben kann.
Konzerne **Ein Architekt in Ihren Teams**	Eingebettet in Plattform-, Security- und Produktteams: Architekturentscheidungen, Governance für KI und regulierte Umgebungen. Für grössere Vorhaben bringe ich ein erfahrenes Senior-Team mit.

Wie ich arbeite

Entscheidungen schriftlich: Architecture Decision Records mit den Abwägungen, damit Ihr Team weiss, warum, nicht nur was.

Sicher ab Werk: OIDC und Managed Identities, Least Privilege, Secrets im Vault, ein Audit-Trail.

Betrieben, nicht nur geliefert: SLOs, Alerts auf Geschäftsergebnisse und eine Incident-Routine.

Gemessen: Kosten, Durchlaufzeit, Verfügbarkeit und gesparte Stunden, jede Woche berichtet.

Das Wissen bleibt bei Ihnen: Runbooks, Dokumentation und Workshops für Ihr Team.

Ein Ansprechpartner, der mit Engineering und Management spricht, auf Deutsch, Englisch und Spanisch.



Sollen Ihre Systeme sicher mit KI sprechen?

30-Minuten-Call buchen

E-mail mail@dominikheinrich.ch
Web dominikheinrich.ch

Weltweit verfügbar, remote. Vor Ort auf Anfrage, je nach Land.