



KI-LEITFADEN · MITTELSTAND 2026

# AUTONOME SOFTWAREENTWICKLUNG IM MITTELSTAND — **12 SCHRITTE** VOM PILOT ZUM PRODUKTIVEN KI-CODE

*Von der Use-Case-Auswahl bis zur Governance-Routine — alles, was zwischen Idee und erstem produktiven Agenten liegt.*

# ÜBERBLICK

<b>01</b>	Warum dieses Thema jetzt	2
<b>02</b>	Die 12 Schritte im Überblick	3
<b>03–14</b>	Schritt 1 bis 12 — Ausführlich	4
<b>15</b>	Drei Praxisbeispiele	7
<b>16</b>	Selbst-Demo: amazing agents	8
<b>17</b>	Ihr nächster Schritt	8



## WARUM DIESES THEMA JETZT RELEVANT IST

Im Mai 2026 hat Anthropic bekanntgegeben, dass mehr als **80 Prozent seines neuen Produktionscodes von Claude geschrieben werden**. Vercel automatisiert 96 Prozent seiner Marketing-Entwürfe und 93 Prozent seines Supports. Cognition garantiert mit bis zu zehn Millionen US-Dollar (≈ neun Millionen Euro), dass Devin die versprochene Produktivität liefert.

Wir bauen für andere, was wir für uns selbst nutzen — dieser Leitfaden übersetzt diese Zahlen in den Mittelstand-Alltag.



*Mensch als Architekt und Prüfer — KI übernimmt die Umsetzung*

Diese Zahlen stammen nicht aus Laborberichten. Sie stammen aus dem Tagesgeschäft von Unternehmen, die KI-Agenten nicht pilotieren, sondern produktiv einsetzen.

Für den deutschen Mittelstand heißt das: **Die Technologie ist da. Die Frage ist nicht mehr „ob“, sondern „wo anfangen“**. Dieser Leitfaden gibt die Antwort in 12 konkreten Schritten.

---

Quellen: Borncity / Günter Born, 2026-06-07 · VentureBeat, 2026-06-04 · Cognition Blog, 2026-06-06 · SaaStr, 2026-06-06 · keine Anlage- oder Rechtsberatung.

# DIE 12 SCHRITTE AUF EINEN BLICK

SCHRITT	TITEL	KERNFRAGE
01	Use Case auswählen	<i>Wo fällt repetitive Arbeit an, die klar regelbasiert ist?</i>
02	Prozess-Audit	<i>Welche Teilschritte sind automatisierbar?</i>
03	Pilot-Rahmen definieren	<i>Ein Agent, ein Ergebnis, 30 Tage.</i>
04	Daten- und Compliance-Check	<i>DSGVO, EU AI Act — was muss geklärt sein?</i>
05	Tool-Stack wählen	<i>Welches LLM, welche Orchestrierung, welches Hosting?</i>
06	Agent-Prototyp bauen	<i>MVP in einer Woche.</i>
07	Human-in-the-Loop festlegen	<i>Wer prüft was — und wann?</i>
08	Testlauf mit echten Daten	<i>Nicht Sandkasten, sondern Alltag.</i>
09	Metriken definieren	<i>Kosten pro Vorgang, Fehlerquote, Zeitersparnis.</i>
10	Rollout planen	<i>Vom Pilot zur Abteilung.</i>
11	Team-Onboarding	<i>Menschen arbeiten mit Agenten, nicht gegen sie.</i>
12	Governance-Routine	<i>Regelmäßige Überprüfung, Anpassung, Eskalation.</i>

**SCHRITT 01**

**USE CASE AUSWÄHLEN**

*Wo fällt repetitive Arbeit an?*

Nicht jeder Prozess eignet sich für einen KI-Agenten. Der richtige Einstieg ist ein Vorgang mit drei Kriterien: **wiederholbar** (täglich oder wöchentlich), **regelbasiert** (Wenn-Dann-Logik), **dokumentiert** (Vorlagen oder Beispiel-Abläufe vorhanden).

Typische Einstiegspunkte im Mittelstand: Telefonannahme und Anfrage-Qualifizierung, Bewerber-Vorauswahl, Zahlungserinnerungen, Angebotsentwürfe, Support-Erstantworten.

**Tipp:** Starten Sie nicht mit dem komplexesten Prozess. Starten Sie mit dem nervigsten.

**SCHRITT 02**

**PROZESS-AUDIT DURCHFÜHREN**

*Welche Teilschritte sind automatisierbar?*

Zerlegen Sie den gewählten Prozess in Einzelschritte. Markieren Sie jeden als **A (automatisierbar)**, **H (human required)** oder **S (semi-automatisierbar)**. Ein guter Pilot hat mindestens 60 % A- oder S-Schritte.

**SCHRITT 03**

**PILOT-RAHMEN DEFINIEREN**

*Ein Agent, ein Ergebnis, 30 Tage.*

Definieren Sie vor dem Start: **Scope** (genau ein Agent für genau einen Prozess), **Erfolgskriterium** (eine messbare Kennzahl), **Zeitraumen** (30 Tage) und **Budget**. Bei amazing agents: 990 Euro Setup, 149 Euro/Monat.

**SCHRITT 04**

**DATEN- UND COMPLIANCE-CHECK**

*Was verlangt die DSGVO? Was der EU AI Act?*

Klären Sie vor Produktiveinsatz: Rechtsgrundlage (Art. 6 DSGVO), schriftlicher AV-Vertrag (Art. 28 DSGVO), vertraglicher Ausschluss von Kundendaten aus Modelltraining, Risikoeinstufung nach EU AI Act Annex III (HR/Recruiting: Hochrisiko), Transparenzhinweis für Endkunden.

## SCHRITT 05

### TOOL-STACK WÄHLEN

*Welches LLM, welche Orchestrierung?*

Ein KI-Agent besteht aus: Sprachmodell (LLM), Orchestrierungslogik und Hosting/Infrastruktur (EU-basiert bei DSGVO-Pflicht). Für die meisten Mittelstandspilots ist ein Managed Service der schnellste Weg — Sie brauchen keinen ML-Engineer.

## SCHRITT 06

### AGENT-PROTOTYP BAUEN

*MVP in einer Woche.*

Ablauf bei amazing agents: Tag 1–2 Briefing, Tag 3–5 Konfiguration und Integration, Tag 6–7 interner Testlauf. Nach einer Woche steht ein lauffähiger Agent — nicht final, aber prüfbar.

## SCHRITT 07

### HUMAN-IN-THE-LOOP FESTLEGEN

*Wer prüft was — und wann?*

Definieren Sie Freigabestufen, Eskalationspfad und Audit-Trail. Art. 22 DSGVO und Art. 14 EU AI Act verlangen menschliche Aufsicht bei Entscheidungen mit Rechtsfolge. Das ist keine Bürokratie — das ist Vertrauensgrundlage.

## SCHRITT 08

### TESTLAUF MIT ECHTEN DATEN

*Kein Sandkasten, sondern Alltag.*

5–10 Arbeitstage parallel zum bestehenden Prozess. Dokumentieren: korrekte Bearbeitungen, Eskalationsquote, Fehlermuster. Die Fehleranalyse ist die Grundlage für Feinabstimmung in Schritt 9.

## SCHRITT 09

### METRIKEN DEFINIEREN UND MESSEN

*Drei Kennzahlen reichen für den Anfang.*

**1. Kosten pro Vorgang:** Agent vs. manuell. **2. Fehlerquote:** Wie oft muss ein Mensch korrigieren? **3. Zeitersparnis:** Stunden pro Woche. Messen Sie wöchentlich, vergleichen Sie mit der Baseline.

## SCHRITT 10

### ROLLOUT PLANEN

*Vom Pilot zur Abteilung.*

Drei Optionen nach erfolgreichem 30-Tage-Pilot: **Vertiefen** (mehr Volumen), **Erweitern** (zweiter Agent), **Pausieren** (Erkenntnisse sichern, später neu starten). Kein Big Bang. Schrittweise.

## SCHRITT 11

### TEAM-ONBOARDING

*Menschen arbeiten mit Agenten, nicht gegen sie.*

Drei Maßnahmen: Demo mit echten Ergebnissen (Zahlen, nicht Versprechen), Rollen klären (Agent = Zuarbeit, Mensch = Prüfung und Verantwortung), Feedback-Kanal einrichten.

## SCHRITT 12

### GOVERNANCE-ROUTINE EINFÜHREN

*Regelmäßige Überprüfung statt Einmal-Setup.*

Monatliche Routine (ca. 1 Stunde): Metriken-Review, Compliance-Check (EU AI Act Updates), Modell-Update-Prüfung, Eskalations-Review, Team-Feedback. Schützt vor schleichender Qualitätserosion.

## DREI UNTERNEHMEN, DIE ES VORMACHEN



Agentensysteme in Produktionsumgebungen — Mensch prüft, KI führt aus

### BEISPIEL 01 · SOFTWARE-ENTWICKLUNG

#### Cognition: 10 Millionen US-Dollar Garantie auf KI-Produktivität

Cognition hat am 6. Juni 2026 eine AI Productivity Guarantee eingeführt: Wenn Devin weniger Engineering-Wert liefert als bezahlt, deckt Cognition die Kosten — bis zu zehn Millionen US-Dollar ( $\approx$  neun Millionen Euro), ausgezahlt als Credits am Ende der Jahresvertragsperiode. Credits, nicht Cash. Diese Garantie ist eine Enterprise-Konstruktion mit Jahresvertrag — nicht für KMU-Endkunden gedacht. **Aber die Botschaft zählt: KI-Produktivität ist messbar genug, um sie zu versichern.**

### BEISPIEL 02 · ENTERPRISE-SOFTWARE

#### Tencent: WorkBuddy als Agent-Schwarm

Tencent orchestriert mit WorkBuddy Enterprise mehrere KI-Agenten als Team — verbunden über MCP mit Jira, GitHub, Google Drive und Slack. VP Liu Yi formuliert: „*N super individuals don't automatically become a super team.*“ Die Lektion: Ein einzelner Agent löst ein einzelnes Problem. Für unternehmensweite Wirkung braucht es Orchestrierung — ob bei Tencent oder im Handwerksbetrieb.

### BEISPIEL 03 · ENTWICKLER-PLATTFORM

#### **Vercel: 96 % Marketing, 93 % Support**

Vercel hat auf dem SaaStr AI Deploy berichtet: Ein Content-Agent erstellt 96 Prozent der ersten Marketing-Entwürfe, ein Support-Agent löst 93 Prozent der Anfragen autonom. CPO Tom Occhino: „*We build for ourselves first.*“ Das Prinzip gilt branchenübergreifend: Wer autonome Agenten für andere baut, sollte sie zuerst für sich selbst nutzen — als Beweis, nicht als Versprechen.

# WIE AMAZING AGENTS DIE EIGENE PIPELINE NUTZT

**Dieser Leitfaden ist kein theoretisches Dokument.** Er ist selbst ein Produkt der Pipeline, die amazing agents für Kunden baut. Vier KI-Agenten haben daran gearbeitet:

1. **Nadja** (Research Agent) hat die Borncity-Meldung in acht Primärquellen aufgelöst, alle Zahlen verifiziert und Widersprüche zwischen Quellen markiert.
2. **Lena** (Content Agent) hat aus dem Fakten-Report diesen Text geschrieben — Blog, LinkedIn-Posts und diesen Leitfaden.
3. **Sophia** (Image Agent) hat die Begleit-Visuals erstellt.
4. **Uwe** (Webdeploy Agent) hat das fertige PDF in eine E-Mail-Gate-Landingpage eingebaut.

Menschliche Freigabe vor jeder Veröffentlichung. Kein Agent geht live ohne Prüfung. Das ist der Beweis: Autonome Softwareentwicklung funktioniert — auch bei einem Unternehmen, das das, was es für andere baut, zuerst für sich selbst nutzt.

## IHR NÄCHSTER SCHRITT: PILOT IN 30 TAGEN

Sie haben die 12 Schritte gelesen. Die Frage ist nicht, ob autonome KI für den Mittelstand funktioniert — sondern wann Sie starten.

### Drei Optionen:

1. **Strategiegelgespräch buchen:** 30 Minuten, kostenlos. Wir schauen gemeinsam, welcher Prozess bei Ihnen den größten Hebel hat.
2. **Pilot starten:** 990 Euro Einrichtung, 149 Euro/Monat. In 30 Tagen steht Ihr erster Agent.
3. **Weitere Leitfäden lesen:** [amazing-agents.com/wissens-hub](https://amazing-agents.com/wissens-hub)

## STRATEGIEGESPRÄCH BUCHEN

30 Minuten. Kostenlos. Wir zeigen Ihnen, welcher Prozess bei Ihnen als erstes einen Agenten verdient.

[AMAZING-AGENTS.COM/BOOKING](https://amazing-agents.com/booking)

**amazing agents** — Wir bauen für andere, was wir für uns selbst nutzen. · [amazing-agents.com](https://amazing-agents.com)

Quellen: Borncity 07.06.2026 · VentureBeat 04.06.2026 · Cognition Blog 06.06.2026 · SaaStr 06.06.2026

Dieser Leitfaden enthält keine Anlageberatung und keine Rechtsberatung. DSGVO- und EU-AI-Act-Hinweise dienen der Orientierung und ersetzen keine rechtliche Prüfung im Einzelfall.