



# KI - aber sinnvoll

---

Was im Mittelstand funktioniert und wie Sie die Kontrolle behalten



# Agenda

- Kurze Vorstellung
- Versprechen vs. Realität
- KI in der Praxis
- Datenhoheit & Kontrolle
- Lessons Learned
- Q&A

Wir sind  
 **Startpunkt Digital.**

---



**Matthias**  
Hofmann



**Philipp**  
Herpich



**Leon**  
Strößner



**Tobias**  
Wirth



2022 in  
Hof/Bayern



Prozesse, Software,  
Maschinendaten



Agiles Team mit einem  
Herz für Digitalisierung



# Unsere Fokuspunkte

Digitale Prozesse und Software im Bereich  
Produktion

Evaluation und Beratung zu IT-Security und  
Zertifizierung nach ISO 27001

Edge-KI Lösungen unabhängig von  
großen Anbietern





# Warum wir?

Kenntnis der Prozesse und Herausforderungen  
bei der digitalen Produktion

Keine Herstellerbindung und keine  
Festlegung auf bestimmte Systeme

Erfahrung beim Einsatz und der Integration von  
Open Source Systemen

Interesse an langfristigen Kundenbeziehungen  
und tiefgehenden Projekten





# Kurze Bestandsaufnahme per Reaktion im Chat

„Ich möchte KI in der Zukunft gern einsetzen,  
ich bin aber noch sehr am Anfang.“

„Ich habe einen konkreten Plan für den Einsatz  
von KI oder nutze es schon regelmäßig.“

„Ich finde KI interessant, aber ich bin skeptisch,  
was den produktiven Einsatz betrifft oder  
habe noch Hindernisse im Unternehmen“



# Versprechen vs. Realität

---



# Die Frage, die alle beschäftigt

Experiment mit einem Avatar

## Wie eine KI mich einmal (beinahe) ersetzt hätte

von Florian Neuhann

29.04.2026 | 06:00

Für eine Doku haben wir ein besonderes Experiment gewagt: Kann Künstliche Intelligenz einen menschlichen Wirtschaftskorrespondenten ersetzen? Das Ergebnis ist erschreckend.

<https://www.zdfheute.de/wissen/ki-im-journalismus-kuenstliche-intelligenz-avatar-fuer-doku-100.html>

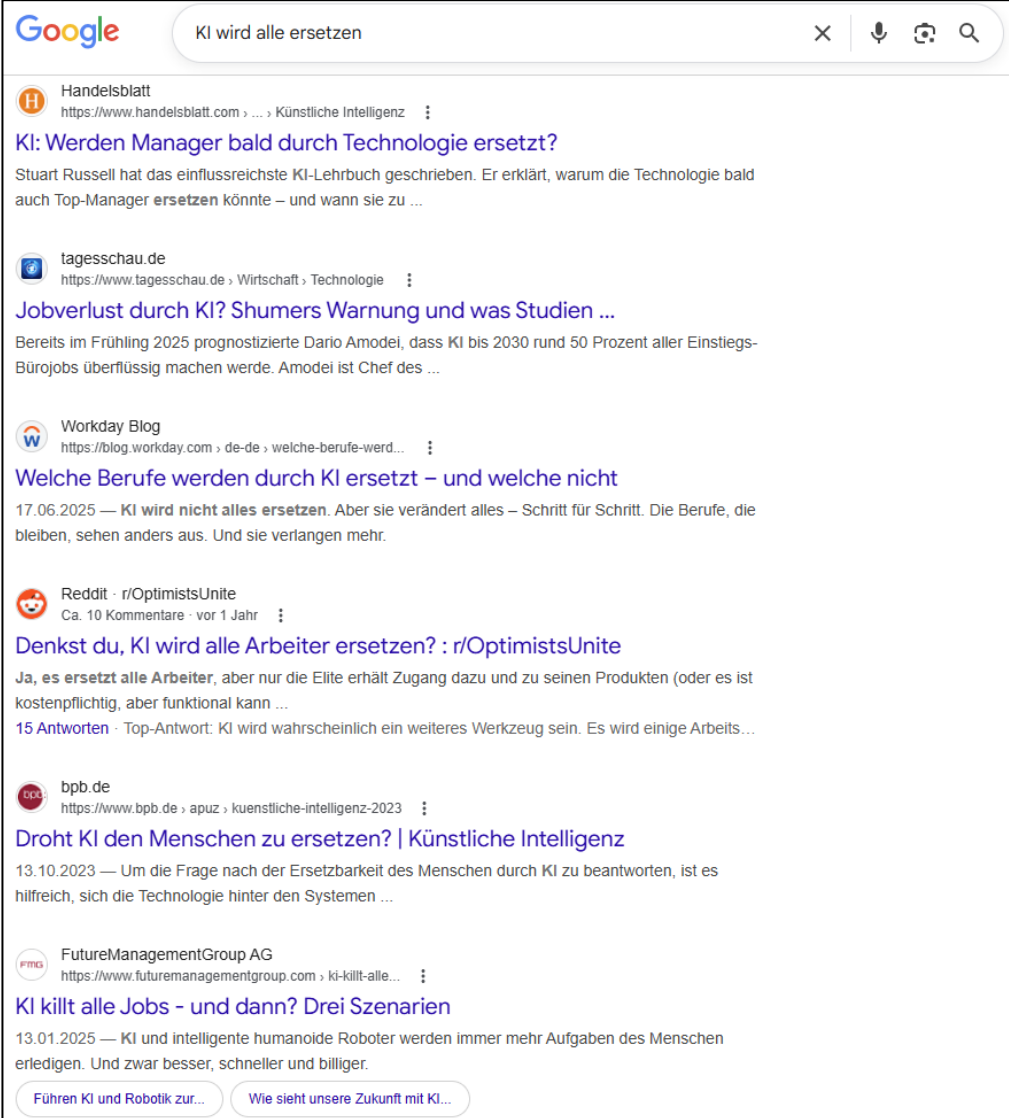
## Wirklich alle...



## Werden Manager bald durch Technologie ersetzt?

Aus dem Handelsblatt-Archiv: Stuart Russell hat das einflussreichste KI-Lehrbuch geschrieben. Im Interview erklärt er, warum die Technologie bald auch Top-Manager ersetzen könnte.

<https://www.handelsblatt.com/technik/ki/ki-werden-manager-bald-durch-technologie-ersetzt/100189694.html>



Google KI wird alle ersetzen

- Handelsblatt**  
<https://www.handelsblatt.com> › ... › Künstliche Intelligenz  
**KI: Werden Manager bald durch Technologie ersetzt?**  
Stuart Russell hat das einflussreichste KI-Lehrbuch geschrieben. Er erklärt, warum die Technologie bald auch Top-Manager ersetzen könnte – und wann sie zu ...
- tagesschau.de**  
<https://www.tagesschau.de> › Wirtschaft › Technologie  
**Jobverlust durch KI? Shumers Warnung und was Studien ...**  
Bereits im Frühling 2025 prognostizierte Dario Amodei, dass KI bis 2030 rund 50 Prozent aller Einstiegs-Bürojobs überflüssig machen werde. Amodei ist Chef des ...
- Workday Blog**  
<https://blog.workday.com> › de-de › welche-berufe-werd...  
**Welche Berufe werden durch KI ersetzt – und welche nicht**  
17.06.2025 — KI wird nicht alles ersetzen. Aber sie verändert alles – Schritt für Schritt. Die Berufe, die bleiben, sehen anders aus. Und sie verlangen mehr.
- Reddit · r/OptimistsUnite**  
Ca. 10 Kommentare · vor 1 Jahr  
**Denkst du, KI wird alle Arbeiter ersetzen? : r/OptimistsUnite**  
Ja, es ersetzt alle Arbeiter, aber nur die Elite erhält Zugang dazu und zu seinen Produkten (oder es ist kostenpflichtig, aber funktional kann ...  
15 Antworten · Top-Antwort: KI wird wahrscheinlich ein weiteres Werkzeug sein. Es wird einige Arbeits...
- bpb.de**  
<https://www.bpb.de> › apuz › kuenstliche-intelligenz-2023  
**Droht KI den Menschen zu ersetzen? | Künstliche Intelligenz**  
13.10.2023 — Um die Frage nach der Ersetzbarkeit des Menschen durch KI zu beantworten, ist es hilfreich, sich die Technologie hinter den Systemen ...
- FutureManagementGroup AG**  
<https://www.futuremanagementgroup.com> › ki-killt-alle...  
**KI killt alle Jobs - und dann? Drei Szenarien**  
13.01.2025 — KI und intelligente humanoide Roboter werden immer mehr Aufgaben des Menschen erledigen. Und zwar besser, schneller und billiger.

Führen KI und Robotik zur... Wie sieht unsere Zukunft mit KI...

<https://www.google.com/search?q=KI+wird+alle+ersetzen>



# KI-Versprechen

positiv und negativ

**Alles** wird automatisiert

**Riesige** Projekte nötig

**Datenverlust** droht

**Zukunftsmusik...**

# Die Realität

Fokus Mittelstand

**Einzelne Aufgaben** werden einfacher

**Kleine Piloten** funktionieren besser

Mit richtiger **Infrastruktur** und **Konzept** sicher

**Heute schon** einsetzbar



# KI in der Praxis

---

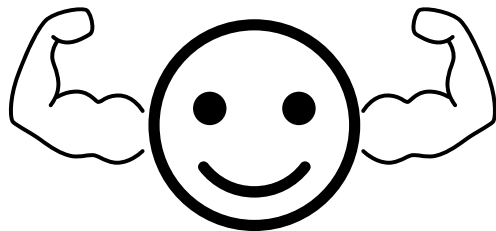


# Assistent vs. Agent vs. Multi-Agenten-System



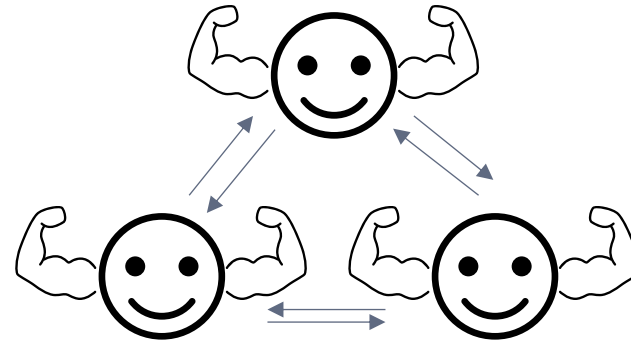
## Assistent

Nimmt Informationen und Anweisungen entgegen, verarbeitet diese und gibt Antworten zurück.  
„Er bleibt in seinem Fenster.“



## Agent

Auch er verarbeitet Informationen, ist aber nicht auf bloßes Antworten beschränkt. Er kann innerhalb der ihm gesetzten Grenzen operieren und Aktionen ausführen.



## Multi-Agenten

Mehrere einzelne, spezialisierte Agenten arbeiten zusammen. Jeder hat dabei seinen Arbeits- und Fachbereich.



# Eine Information vorab

Dieser Vortrag ist kein Musterbeispiel  
und die Lösungen kein Allheilmittel

Die Integration von KI ist genauso ein Individualprojekt wie jede  
andere System Einführung auch.

Es ist sogar eher noch damit vergleichbar, neue MitarbeiterInnen  
einzustellen, denen man Aufgaben und Verantwortlichkeiten überträgt.



# Eine Information vorab

Dieser Vortrag ist kein Musterbeispiel  
und die Lösungen kein Allheilmittel

Die Integration von KI ist genauso ein Individualprojekt wie jede  
andere System Einführung auch.

Es ist sogar eher noch damit vergleichbar, neue MitarbeiterInnen  
einzustellen, denen man Aufgaben und Verantwortlichkeiten überträgt.

Beispiel 1:

# Angebotserstellung

Delegierung an KI zur  
Entlastung und Vorhaltung  
von Kapazitäten



## Problem

Repetitive Standardaufgaben  
nehmen viel Zeit in Anspruch,  
sind aber zu komplex für einfache  
Workflows



## Lösung

KI-gestützte Angebotserstellung;  
Ein Agent wertet Standard-  
anfragen aus und erstellt  
individuelle Angebote, die direkt  
versendet werden (können)



## Ergebnis

Entlastung des Vertriebs zum  
Fokus auf komplexe Anfragen  
und Konzepte + schnellere  
Antwortzeiten

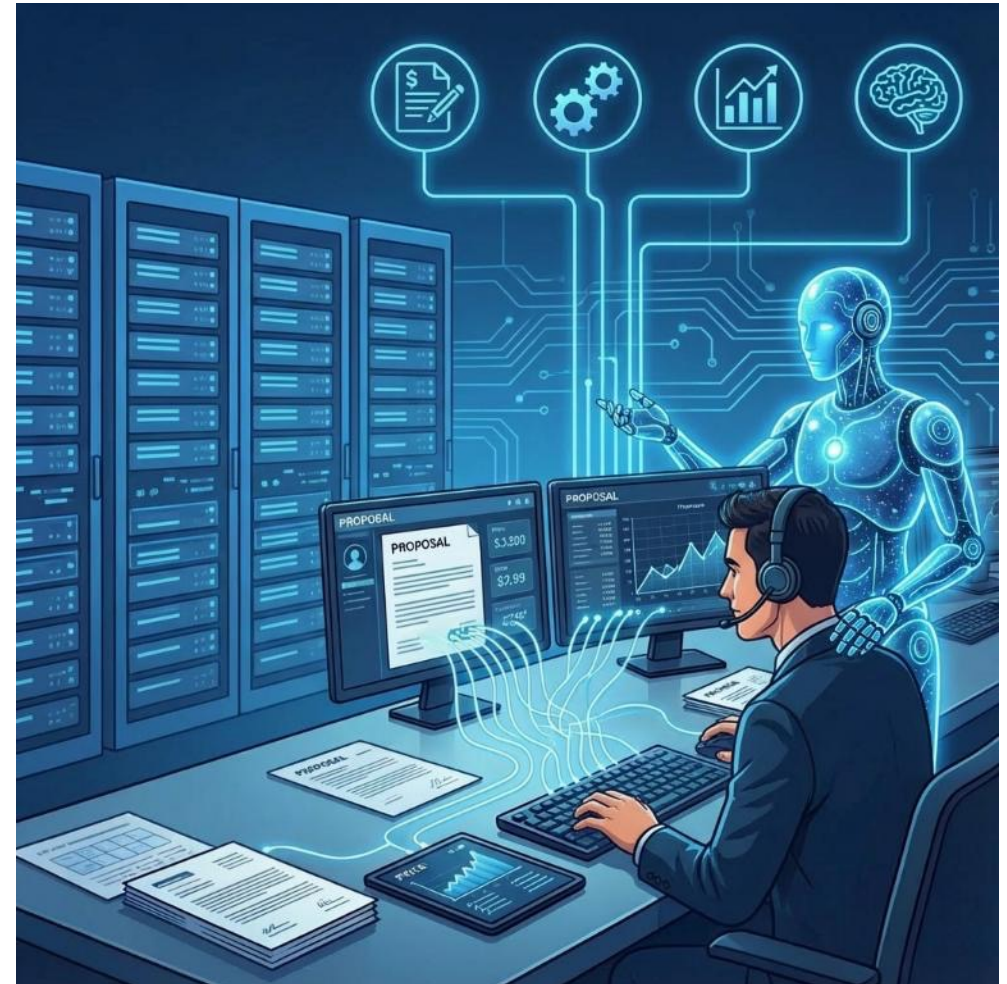
*"Hier teilen Praktiker  
Erfahrungen und Lösungen"*



**Mehr Wachstum, weniger Aufwand: Mit Prozess-Exzellenz  
& Digitalisierung das Auftragsmanagement revolutionieren**

**Fallbeispiel „Angebotsassistent“**

Düsseldorf/ Hof, 30. April 2026





## Bottleneck Angebotserstellung - ein Bremsklotz für Ihr Wachstum?

### Ausgangssituation (Beispiel Stahlhändler)

- **Hoher Aufwand** bereits bei der Erfassung von **Angebotsanfragen**
    - „Schwierige“ Produkte und Werkstoffe
    - Unübersichtliche Regularien, Normen und Gesetze
    - Komplexe Endanwendungen
    - Angebotsanfragen oft unstrukturiert, wichtige Details fehlen
  - **Hohe fachliche Anforderungen** bei der **Angebotserstellung**
    - Spezialistenwissen erforderlich, oft erfahrungsbasiert
    - Hohe Gesamtauslastung/ Fachkräftemangel

➔ Angebotsprozess manuell, fehleranfällig und langsam
- ➔ Angebotserstellung erfolgt verzögert. Gefahr: Aufträge gehen verloren, Kunden wandern ab

### Konsequenzen

- **Operative Last:**  
Hohe Prozesskosten durch manuelle Doppelarbeit, Systembrüche und ständige Rückfragen.
- **Strategische Gefahr:**  
Gebremste Skalierbarkeit. Wachstum ist durch Anzahl der Köpfe limitiert, nicht durch die Nachfrage am Markt.
- **Mitarbeiterfrust:**  
Routineaufgaben & ständiger Druck führen zu Demotivation & Fluktuation, eine Katastrophe im aktuellen Fachkräftemangel.

● Während Sie noch Daten suchen, hat der Wettbewerber das Angebot schon abgeschickt!

## Die **BUHLMANN** Gruppe

### BUHLMANN Rohr-Fittings-Stahlhandel GmbH + Co. KG



#### **International tätiger Stahlhändler (23 Länder)**

- Branchen: Energieversorger, Nuklear, Prozessindustrie, Chemie, Öl & Gas, Offshore, weitere
- Europäische / Amerikanische Normen (DIN EN, ASTM, ASME ...)
- Mitarbeiter insgesamt: 750 weltweit
- Vertriebsmitarbeiter: 250 in Europa

## Die Lösung: **Intelligenter Angebots-Assistent**

- Anfragen werden automatisiert entgegen genommen (Telefon, Mail, PDF, ...)
- Benötigtes Material wird durch einen/mehrere KI-Assistenten vorgeschlagen
  - passend – zur Einhaltung von Normen & Gesetzen
  - passend – für den Anwendungsfall
  - passend – für den individuellen Kunden
- Besondere Kundenanforderungen/-konditionen werden berücksichtigt
- Angebote werden automatisch generiert
- Vertriebsmitarbeiter können
  - Angebote prüfen und die Versendung manuell freigeben („human in the loop“) oder
  - kriterienbasiert automatisch versenden lassen (z.B. nach Angebotsvolumen, kundenspezifisch)

- Die Angebotserstellung erfolgt hoch automatisiert und ist unter Berücksichtigung aller Randbedingungen innerhalb von Minuten abgeschlossen.

# Fallbeispiel: Hochautomatisierter und sicherer Ablauf

- Angebotsanfrage (E-Mail) kommt rein
- Angebotsanfrage wird anonymisiert
- Angebotsanfrage wird bearbeitet
- Angebot wird erstellt
- Angebot wird nachgebessert
- Angebot wird individualisiert
- Angebot wird ins ERP übernommen
- Mitarbeiter gibt Angebot frei
- Angebot wird versendet (E-Mail)

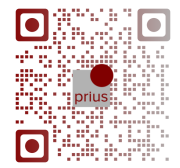
**Produktvorschläge**

Artikelnummer	Beschreibung	Material Code	Artikel Kategorie Code	Produkt Typ	Außen-durchmesser	Wandstärke	Herkunft	Zeugnis
1200005606	Pipe-s-16Mo3	2320	P	S	114.3	3.6	EU	32T

**BUHLMANN ANGEBOT**

Pos.	Beschreibung	Menge ME	Gewicht KG	Preis EUR	PE	Gesamtpreis EUR
	Nahlose Röhre EN 10216-2, Material 16Mo3 EN 10204-2004 AP2 32 TÜV 114,3 x 3,60 Zylinder 73045882	12,00 M	117,95	39,95 M		475,92
	Freight Charges / Frachtkosten	1,00 RT		250,00 RT		250,00
	Logische festlogischeaufschlag					61,90
	<b>Gesamtgewicht</b>	<b>117,95 KG</b>		<b>Total EUR ohne MwSt.</b>		<b>787,82</b>
				<b>10% MwSt.</b>		<b>145,59</b>
				<b>Total EUR inkl. MwSt.</b>		<b>933,41</b>

Keine Lust auf Screenshots? Fragen zu individuellen Herausforderungen? Vereinbaren Sie einen persönlichen Termin für eine **Live Demo** und Möglichkeiten zum **Austausch mit unseren Experten**.



# Fallbeispiel: Hochautomatisierter und sicherer Ablauf (1)

Angebotsanfrage (E-Mail) kommt rein

Angebotsanfrage wird anonymisiert

Angebotsanfrage wird bearbeitet

Angebot wird erstellt

Angebot wird nachgebessert

Angebot wird individualisiert

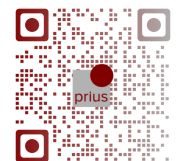
Angebot wird ins ERP übernommen

Mitarbeiter gibt Angebot frei

Angebot wird versendet (E-Mail)

ME	Gewicht KG	Preis EUR	PE	Gesamtpreis EUR
01 M	117,36	39,96 M		473,32
01 RT		268,00 RT		268,00
Total EUR ohne MwSt.				741,32
10% MwSt.				145,59
Total EUR inkl. MwSt.				886,91

Keine Lust auf Screenshots? Fragen zu individuellen Herausforderungen? Vereinbaren Sie einen persönlichen Termin für eine **Live Demo** und Möglichkeiten zum **Austausch mit unseren Experten**.



## Fallbeispiel: Hochautomatisierter und sicherer Ablauf (2)

Angebotsanfrage (E-Mail) kommt rein

Angebotsanfrage wird anonymisiert

Angebotsanfrage wird bearbeitet

Angebot wird erstellt

Angebot wird nachgebessert

Angebot wird individualisiert

Angebot wird ins ERP übernommen

Mitarbeiter gibt Angebot frei

Angebot wird versendet (E-Mail)

Anfrage bearbeiten - "[EXT] - Anfrage"

Verkäufer: hendrik.wuelbers

Kunde: [Redacted]

Extrahierte Daten

Artikel 1

Artikelcode: P

Art: [Redacted]

Form: [Redacted]

Materialcodes: 2300, 2310, 2320

Wandstärke 1: 3.6

Außendurchmesser 1: 114.3

Wandstärke 2: [Redacted]

Außendurchmesser 2: [Redacted]

Material: 16 Mo 3

Menge (Stück/Meter): 12

Hinweise: [Redacted]

Mail

Hallo Herr Wülbers,

erbitten Preis und Lieferzeit:

12 m  
Rohr, Kesselrohr 16 Mo3 114,3x3,6

Mit freundlichen Grüßen

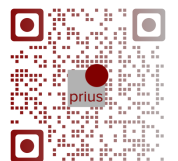
i.A. [Redacted]

Produktvorschläge

Artikel 1

Artikelnummer	Beschreibung	Material Code	Artikel Kategorie Code	Produkt Typ	Außen-durchmesser	Wandstärke	Herkunft	Zeugnis	Lagerbestand
1200005606	Pipe-s-16Mo3	2320	P	S	114.3	3.6	EU	32T	298.88

Keine Lust auf Screenshots? Fragen zu individuellen Herausforderungen? Vereinbaren Sie einen persönlichen Termin für eine **Live Demo** und Möglichkeiten zum **Austausch mit unseren Experten**.

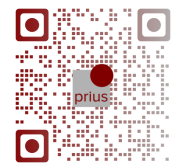


# Fallbeispiel: Hochautomatisierter und sicherer Ablauf (3)

- Angebotsanfrage (E-Mail) kommt rein
- Angebotsanfrage wird anonymisiert
- Angebotsanfrage wird bearbeitet
- Angebot wird erstellt
- Angebot wird nachgebessert
- Angebot wird individualisiert
- Angebot wird ins ERP übernommen
- Mitarbeiter gibt Angebot frei
- Angebot wird versendet (E-Mail)

The screenshot shows a web browser window with the URL 's-entw-rpa2.merentisenw.local:3001/#/inquiries/157/edit'. The main interface is titled 'Anfrage bearbeiten' (Edit Inquiry) and shows a 'Warenkorb' (Shopping Cart) modal. The cart contains one item: 'Artikel 1400004508' with variant code 'DRL' and quantity '48'. Below the cart, there is a table for 'Sachkonten' (Account Types) with columns 'Typ', 'Menge', and 'Preis'. A dropdown menu is open, showing various account types such as 'Erhaltene Anzahlungen', 'Management Fees BOP (Haben)', 'IC Erlöse 19%', 'Freight Charges / Frachtkosten', etc. A red arrow points to the 'Anfrage weiterverarbeiten' button at the bottom of the modal.

Keine Lust auf Screenshots? Fragen zu individuellen Herausforderungen? Vereinbaren Sie einen persönlichen Termin für eine **Live Demo** und Möglichkeiten zum **Austausch mit unseren Experten**.

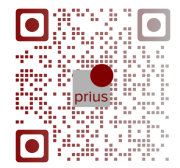


# Fallbeispiel: Hochautomatisierter und sicherer Ablauf (4)

- Angebotsanfrage (E-Mail) kommt rein
- Angebotsanfrage wird anonymisiert
- Angebotsanfrage wird bearbeitet
- Angebot wird erstellt
- Angebot wird nachgebessert
- Angebot wird individualisiert
- Angebot wird ins ERP übernommen
- Mitarbeiter gibt Angebot frei
- Angebot wird versendet (E-Mail)

Pos.	Beschreibung	Menge ME	Gewicht KG	Preis EUR	PE	Gesamtpreis EUR
	Nahtlose Rohre EN 10216-2, Material 16Mo3 EN 10204:2004 APZ 3.2 TÜV 114,3 x 3,60 Zollpos.: 73045982	HL 10-12 m 12,00 M		117,96	39,66 M	475,92
	Freight Charges / Frachtkosten	1,00 ST			250,00 ST	250,00
	Logistics fee/Logistikpauschale					61,90
	<b>Gesamtgewicht</b>	117,96 KG				
<b>Total EUR ohne MwSt.</b>						<b>787,82</b>
<b>19% MwSt.</b>						<b>149,69</b>
<b>Total EUR inkl. MwSt.</b>						<b>937,51</b>

Keine Lust auf Screenshots? Fragen zu individuellen Herausforderungen? Vereinbaren Sie einen persönlichen Termin für eine **Live Demo** und Möglichkeiten zum **Austausch mit unseren Experten.**





## Fallbeispiel: Signifikanter Mehrwert – Quantensprünge für Vertrieb und Kunden

Angebotsanfrage (E-Mail) kommt rein

Angebotsanfrage wird anonymisiert

Angebotsanfrage wird bearbeitet

Angebot wird erstellt

Angebot wird nachgebessert

Angebot wird individualisiert

Angebot wird ins ERP übernommen

Mitarbeiter gibt Angebot frei

Angebot wird versendet (E-Mail)

### Automatisierungsgrad

- Deutliche Steigerung des Volumens und der Effektivität
- Signifikant geringerer Aufwand bei der Angebotserstellung

### Geschwindigkeit

- Schnellere Bearbeitung von Anfragen
- 24/7 Verfügbarkeit

### Fachkräftemangel

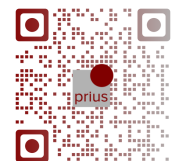
- Entlastung vorhandener Fachkräfte
- Verkürzte Einarbeitung neuer Fachkräfte

### Qualität & Nutzerfreundlichkeit

- Erhöhte Qualität bei der Bearbeitung
- Einfaches und strukturiertes Abarbeiten der Anfragen



Keine Lust auf Screenshots? Fragen zu individuellen Herausforderungen? Vereinbaren Sie einen persönlichen Termin für eine **Live Demo** und Möglichkeiten zum **Austausch mit unseren Experten**.





### Zum 13. Mal in Folge in guter Gesellschaft

Zusammen mit Statista hat brand eins zum 13. Mal in Folge den Markt untersucht und die Besten Berater des Jahres 2026 zusammengestellt:

Insbesondere in den wichtigen prius Beratungsfeldern Einkauf und Supply Chain Management, Innovation und Wachstum sowie Nachhaltigkeit ist prius von Kollegen und Klienten auf die Bestenliste gewählt worden.

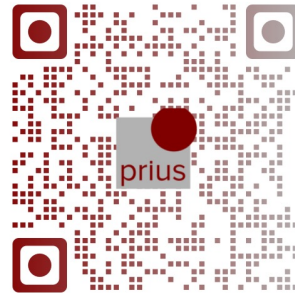
#### Beratungsfelder (Klienten-Beurteilung)

- Einkauf, Supply Chain Management
- Innovation, Wachstum
- Nachhaltigkeit, Sustainability

#### Branchen (Klienten-Beurteilung)

- Agrar, Nahrungsmittel und Getränke
- Auto & Zulieferer

● Diese Auszeichnung auf Basis von Empfehlungen von Klienten und Branchenexperten basiert auf erprobten Methoden, belastbaren Ergebnissen und Lösungen, die im Alltag funktionieren.



### Nachhaltigkeit, Sustainability



Unternehmen	Kollegen-Empfehlungen	Klienten-Beurteilungen
Ritzenhoefer & Company	●●●	●
PricewaterhouseCoopers (PwC)	●●	●●●
sustainable	●●	●●●
BCG – The Boston Consulting Group	●●	●●
<b>prius consult</b>	●●	●●
acondas <sup>1)</sup>	●●	●
LBD-Beratungsgesellschaft	●●	●
Accenture	●	●●●
Deloitte Consulting	●	●●●
EY Consulting	●	●●●
KPMG Advisory	●	●●●
Roland Berger	●	●●●
AFRY Management Consulting	●	●●
Consileon Business Consultancy <sup>2)</sup>	●	●●
accilium	●	●
EFESO Management Consultants	●	●
System	●	●

<sup>1)</sup>Teil von Rambell Management Consulting <sup>2)</sup>inkl. ehemals ajco solutions

Tabelle aus brand eins Heft 33 2025 entnommen

Beispiel 2:

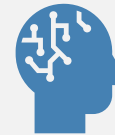
# PZE & Multiagenten

Stundenprüfung und  
Kommunikation über KI-  
Agenten



## Problem

Manuelle Stundenkontrolle kostet den Mitarbeitenden in der Verwaltung viel Zeit



## Lösung

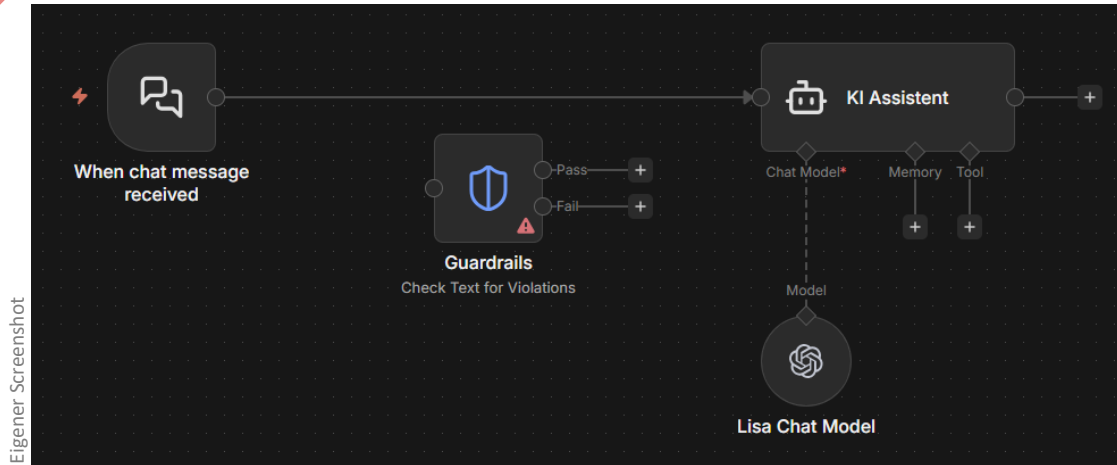
Multiagenten-System mit Lesezugriff auf PZE-Datenbank; Kommunikation direkt über Teams



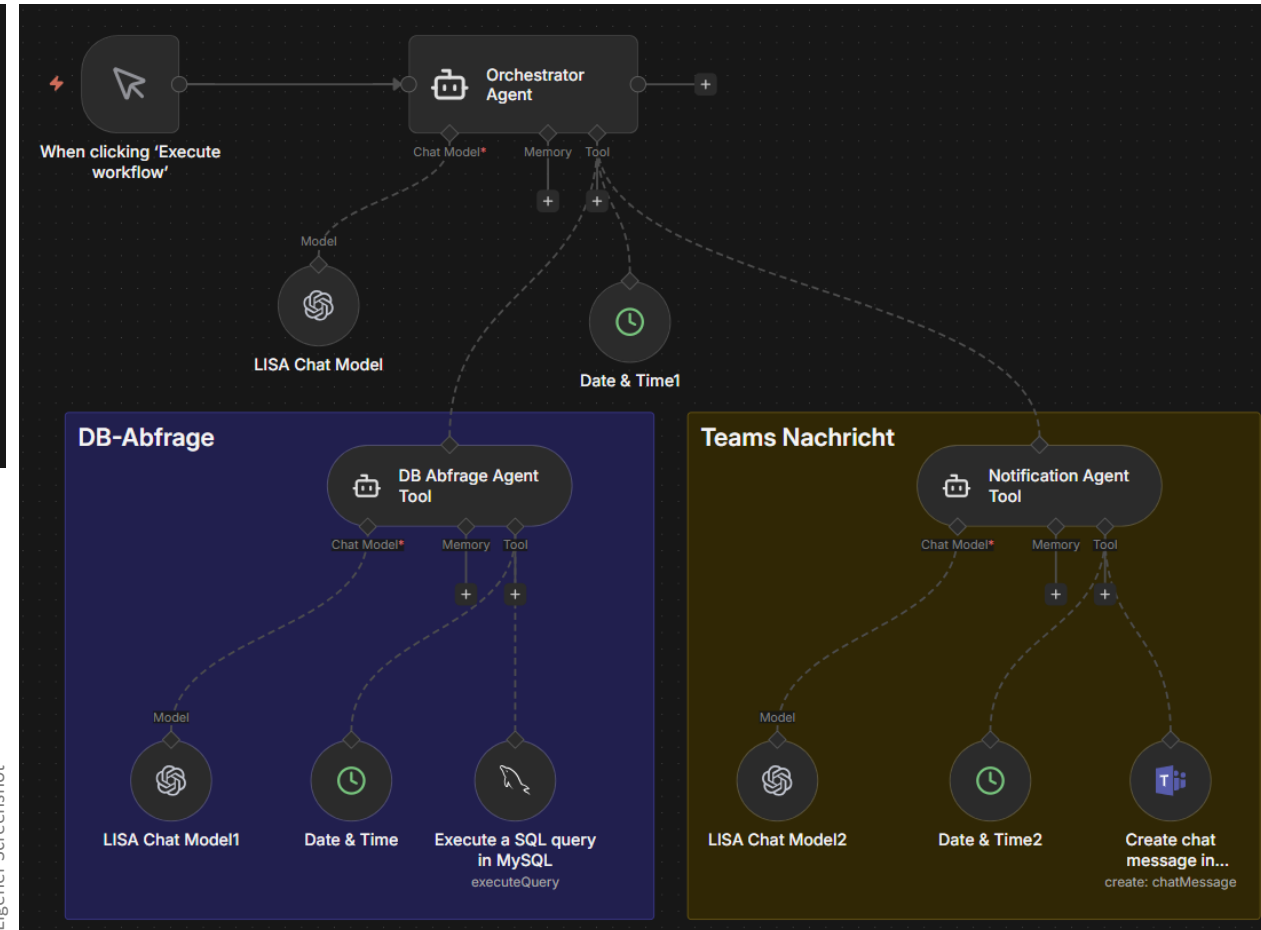
## Ergebnis

Die KI überwacht, gibt Auskunft, kontaktiert und klärt offene Fragen

# Beispiel 2: PZE & Multiagenten

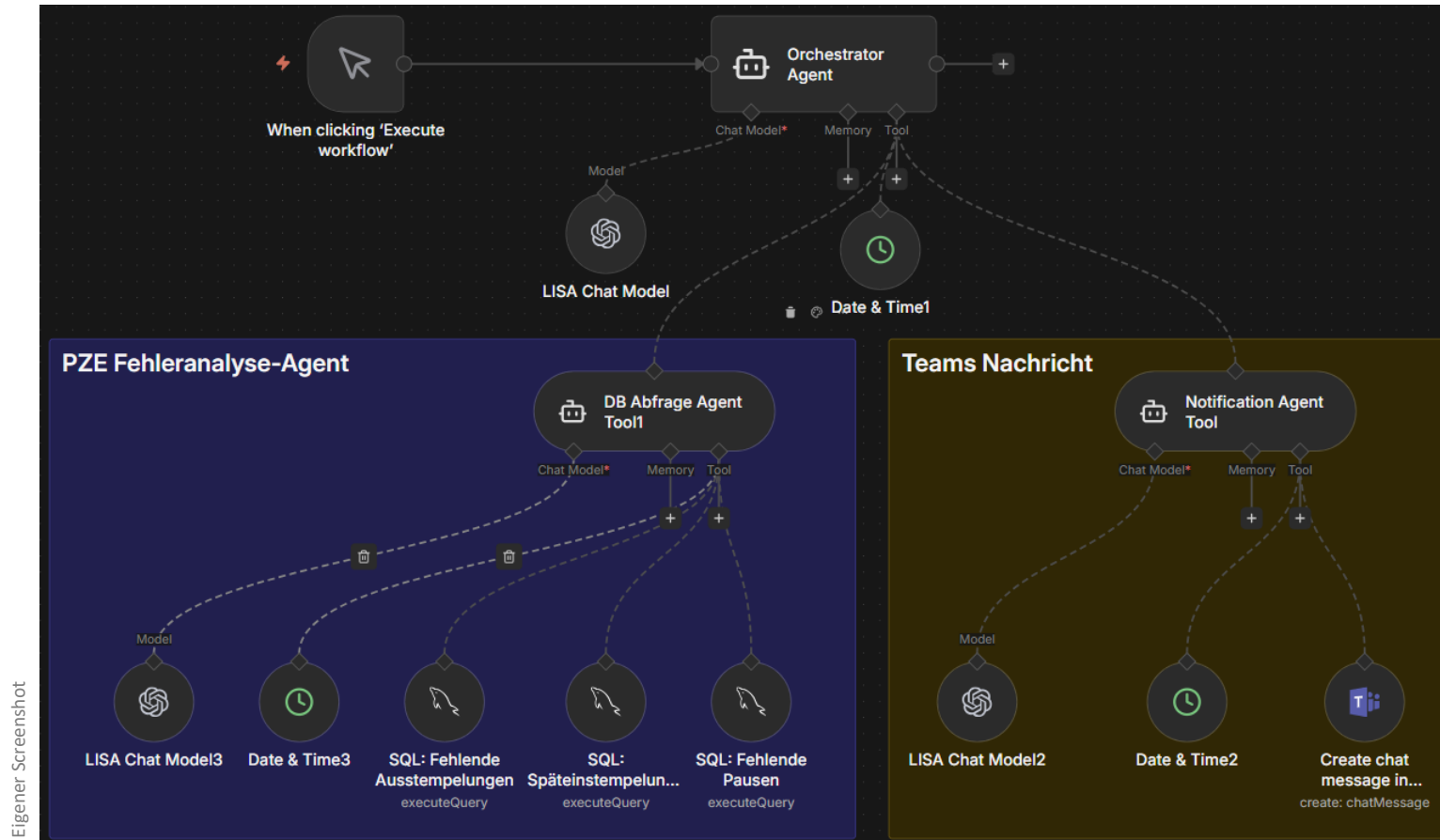


Einfacher Funktionstest, ob das lokale Chat-Model überhaupt angesprochen werden kann



Multiagenten-Workflow: Orchestrator kümmert sich um die Anfrage und delegiert Aufgaben an DB-Abfrage- und Teams-Agent

# Beispiel 2: PZE & Multiagenten



Schritt für Schritt Erweiterung um weitere Tools

Beispiel 3.1:

# Vibe Coding

Fachabteilung baut eigene Software, ohne Entwickler



## Problem

Spezifische Anforderungen, Standardsoftware passt nicht, klassische Entwicklung zu teuer



## Lösung

KI-gestütztes Vibe Coding: Anforderungen in natürlicher Sprache beschreiben



## Ergebnis

Funktionsfähige Anwendung im echten Einsatz, wird jetzt professionell ausgebaut

# Beispiel 3.1:

# Vibe Coding

Als User

Eigener Screenshot

```
6871 // =====
6872 // INIT
6873 // =====
6874 load();
6875 go("dash");
6876 updBadge();
6877 </script>
6878
6879
6880 </body></html>
```

Schon mit einfachen Prompts generieren KIs viel Quellcode, der am Ende eine bedienbare Lösung ergibt. Die Wartung und Weiterentwicklung kann sich mit zunehmender Größe schwierig gestalten.

KI-generierter Code ist nicht frei von Fehlern und kann Sicherheitslücken enthalten. Fachfremden Nutzern fehlt hier oft die Erfahrung und Awareness.

Eigener Screenshot

```
4073 const COLOR_SWATCHES = ['#F5C518', '#E87722', '#4CAF50', '#E91E96', '#42A5F5', '#9C27B0', '#8BC34A'];
4074 > const DEFAULT_STANDORTE = [...];
4082 ⚡ const DEFAULT_USERS = [{ id: 'u1', username: 'admin', password: 'admin123', displayName: 'Administrator' }];
4083 const ROLE_LABELS = { admin: 'Administrator', editor: 'Bearbeiter', viewer: 'Betrachter' };
4084 const DAYS = ['Montag', 'Dienstag', 'Mittwoch', 'Donnerstag', 'Freitag'];
4085 const QS_LABELS = { offen: 'QS OFFEN', ok: 'QS ✓', freigabe: 'FREIGABE AUSSTEHEND' };
4086 const MAX_CARDS = 3;
```

# Beispiel 3.1: Vibe Coding

Als User

KI schafft Zugang zu Individuell programmierten Lösungen

Schnelle Prototypenentwicklung oder Lösung kleiner, spezifischer Aufgaben

„Lastenheft zum Anfassen“

## Sicherheitslücken durch Vibe-Coding: Sensible Website-Daten sind oft leicht auffindbar

Vibe-Coding ist praktisch: Dank moderner Tools kann heute jeder ohne Vorkenntnisse ganze Websites bauen. Eine aktuelle Recherche zeigt allerdings: Viele davon sind von massiven Sicherheitslücken betroffen.

Von Noëlle Bölling

29.04.2026, 13:35 Uhr • © 2 Min.

<https://t3n.de/news/sicherheit/sluecken-durch-vibe-coding-sensible-website-daten-sind-oft-leicht-auffindbar-1740385/>

### FAST JEDE ZWEITE ZEILE FEHLERHAFT

## KI-Code voller Sicherheitslücken

Eine neue Studie deckt gravierende Schwachstellen in KI-generiertem Code auf. 45 Prozent aller von KI erstellten Programme enthalten Sicherheitslücken.

31. Juli 2025 um 07:21 Uhr / [Andreas Donath](#)

<https://www.golem.de/news/fast-jede-zweite-zeile-fehlerhaft-ki-code-voller-sicherheitsluecken-2507-198664.html>

Mehr Probleme, je komplexer die Anwendung

Fehlendes Fachwissen der Benutzer bedeutet auch fehlenden Input für die KI

Mangelnde Sicherheit oder Skalierbarkeit

Beispiel 3.2:

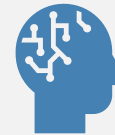
# Vibe Coding

Softwareentwickler  
werden von KI unterstützt



## Problem

Großer Workload mit viel Standardaufgaben oder Einarbeiten und Änderungen in fremden Projekten



## Lösung

KI-gestütztes Vibe Coding: KIs als Werkzeug zur Analyse oder zur gezielten Erzeugung einzelner Teile Quellcode



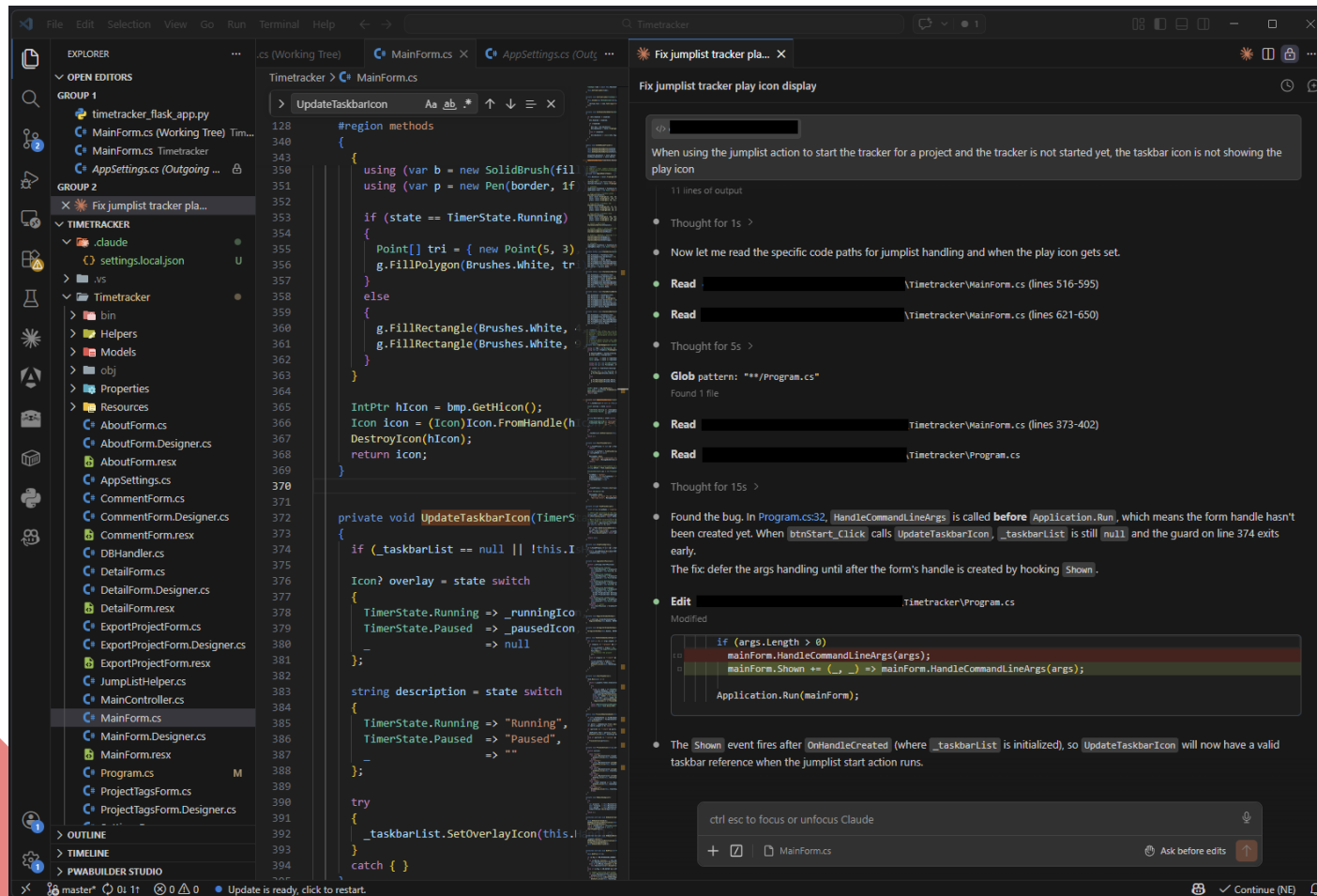
## Ergebnis

Effizienteres Arbeiten durch spezifische Einzelaufgaben mit kontrollierten Ergebnissen

# Beispiel 3.2:

# Vibe Coding

Als Entwickler



## Mensch und KI arbeiten Hand in Hand

Bei guter Führung und spezifischen Anforderungen ergeben die Diskussionen schnell verwendbaren Code. Das hilft vor allem bei Code, der ursprünglich von anderen Entwicklern stammt.

# Beispiel 3.2: Vibe Coding

Als Entwickler

Steigerung der Effizienz

Co-Working Ansatz mit Kontrolle schafft gute Ergebnisse

Schnelles Einarbeiten in fremde Projekte

\*natürlich ein Extrembeispiel, aber nicht das Erste...

CURSOR

## KI-Agent löscht Produktivdatenbank

Weil ein Cursor-Agent mit Claude -Modell im Hintergrund einen Authentifizierungsfehler lösen wollte, löschte er die gesamte Datenbank eines SaaS-Anbieters.

28. April 2026 um 08:54 Uhr / Andreas Donath

<https://www.golem.de/news/cursor-ki-agent-loescht-aus-versehen-produktiv-datenbank-2604-208074.html>

Hoher Tokenverbrauch bei großen oder komplexen Projekten

Ohne genaues Inspizieren am Schluss weniger Kenntnis über den Programmcode

Zu hohe Eigenständigkeit der KI kann Fehler verursachen

# Beispiel 4: Anomalieerkennung in Log-Dateien

Aus Datenchaos wird  
Überblick



## Problem

Netzwerkprobleme → Masse an Logdaten → manuelle Analyse sehr aufwändig



## Lösung

KI-generierte Oberfläche mit Zeitreihen-Charts und automatischer Hervorhebung von Auffälligkeiten



## Ergebnis

Ursache in Minuten statt Stunden gefunden



# Beispiel 4: Anomalieerkennung in Log-Dateien

Schnelle und übersichtliche  
Aufbereitung von Daten

Gewisse Interpretationsmöglichkeiten  
der KI („Was fällt dir auf?“)

Kann nach erster Erstellung immer  
wieder mit neuen Versionen des Logs  
gefüttert werden

Hoher Tokenverbrauch bei großen Logs

Muss auf den speziellen Fall  
zugeschnitten sein

Interpretationen der KI müssen trotzdem  
geprüft und kritisch hinterfragt werden  
(→ Scheinkorrelation)

Eine **Scheinkorrelation** (englisch *spurious correlation*) ist ein statistischer Zusammenhang zwischen zwei Variablen, der **nicht** auf einem kausalen Ursache-Wirkungs-Prinzip beruht. Die Werte korrelieren zwar mathematisch, oft zufällig oder durch eine nicht berücksichtigte dritte Variable (Konfundierung). Wikipedia +4

<https://www.google.com/search?q=scheinkorrelation; KI-Zusammenfassung;>



# Datenhoheit und Kontrolle

---



# Technische Optionen

## KI-Dienst

z.B. ChatGPT, Claude, Copilot, ...



Einfach und schnell



Datenschutz, Transparenz, Kontrolle

## Gehostetes Model

Fertiges OpenSource Model bei Hostinganbieter, zahlbar nach Auslastung



Mehr Kontrolle



Weniger Planbar, trotzdem nicht komplette Kontrolle

## Gehosteter Server

KI-Ready Server bei Hostinganbieter



Fast volle Kontrolle



Höhere (mtl.) Kosten, höherer Aufwand

## Selfhost

Eigenes Model auf eigener Hardware



Volle Kontrolle



Hoher Invest, hoher Aufwand, evtl. weniger Performance

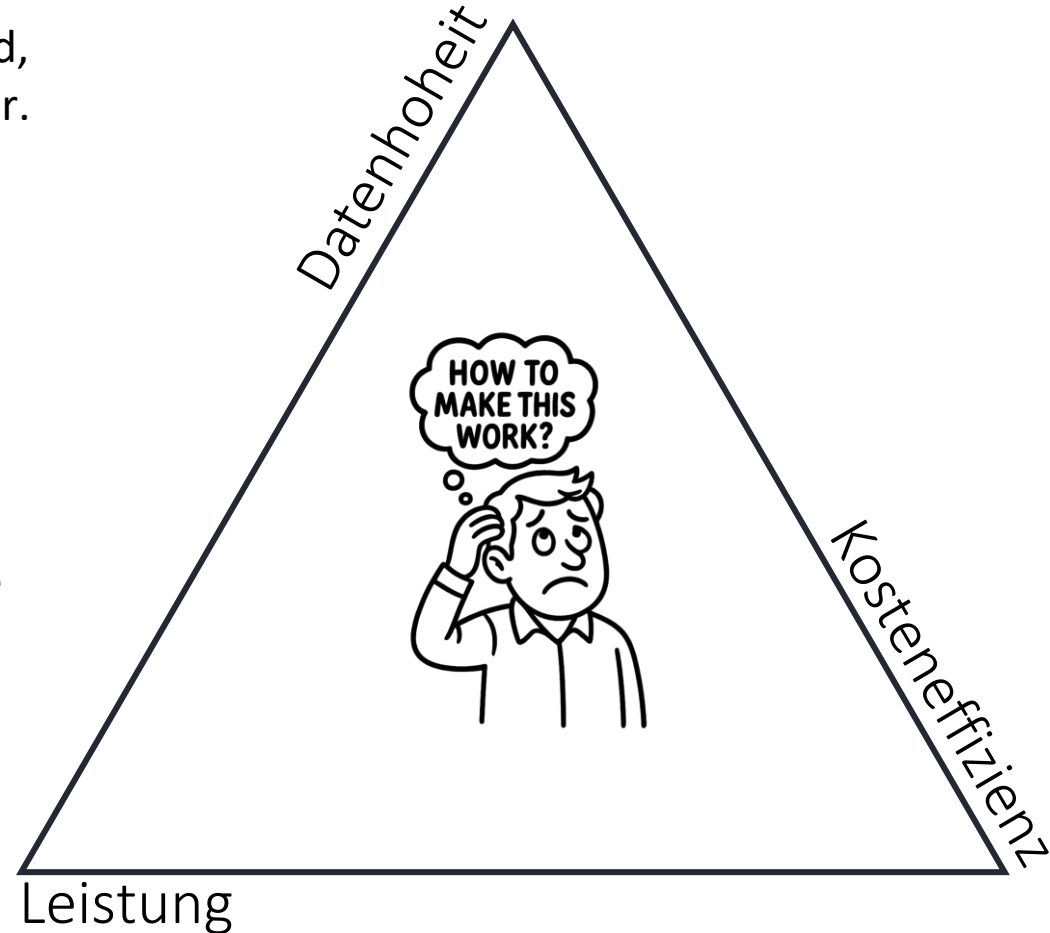


# Der Trade-Off

Die Nutzung von KI-Diensten erfordert kaum Aufwand, liefert schnell gute Ergebnisse und ist (i.d.R) bezahlbar. Die Datenhoheit ist aber nicht gegeben.



Der eigene KI-Server im Unternehmen gibt die vollste Kontrolle über die Daten. Gleichzeitig muss aber je nach Leistungsanspruch in adäquate Hardware investiert und diese auch gewartet werden.





# Zusammenfassung

	<b>KI-Dienst</b>	<b>Private Cloud</b>	<b>Selfhost</b>
Geeignet für	Allgemeine Texte, interne Drafts	DSGVO-konform, volle Kontrolle	Hochsensible Daten, regulierte Branchen
Ungeeignet für	Kundendaten, Verträge, Vertrauliches (Anonymisierung ggfs. möglich, muss aber zweifelsfrei sichergestellt werden)	Eventuelle kundenspezifische Auflagen („Daten nur im direkten Verwaltungsbereich des Unternehmens“)	(Evtl.) Verarbeitungen und Aufgaben mit hohen Leistungsanforderungen



Informationssicherheit bedeutet nicht  
„keine KI“, sondern geregelte KI.



Wie immer bei Daten gilt:

„Würden Sie diese Information auch einem externen Berater zeigen, ohne ihn persönlich getroffen zu haben?“



# Lessons Learned

---



# Die Beispiele im Überblick



(Multi)-  
Agentensysteme



Vibe Coding



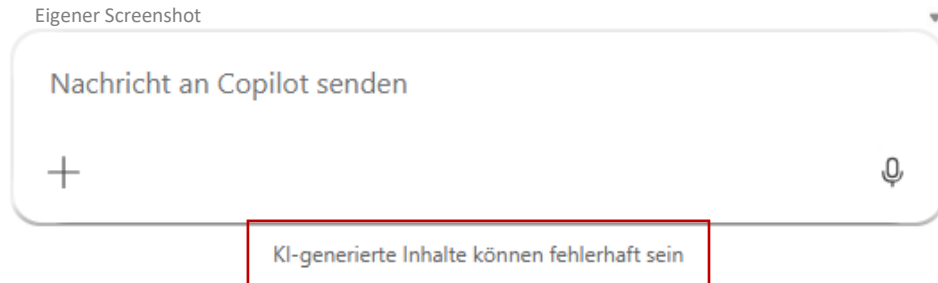
Log-Analyse

**Agentisches Arbeiten,  
Generierung von Quellcode,  
Datenaufbereitung,**  
das funktioniert alles direkt auf Anhieb.  
Und die 99 Mal danach.

Aber was passiert beim 100. Mal,  
wie gehe ich damit um  
und wie verhindere ich es?



# KI macht Fehler, das weiß sie auch selbst



**Fehler müssen erwartet und frühzeitig entdeckt werden**

Wann immer möglich  
→ Human-in-the-Loop und kritische Aktionen vorher bestätigen lassen

Außerdem:

- Guardrails definieren
- Nur die nötigsten Zugriffe gewähren
- Backupstrategie

**CURSOR**  
**KI-Agent löscht Produktivdatenbank**  
Weil ein Cursor-Agent mit Claude -Modell im Hintergrund einen Authentifizierungsfehler lösen wollte, löschte er die gesamte Datenbank eines SaaS-Anbieters.  
28. April 2026 um 08:54 Uhr / [Andreas Donath](#)  
<https://www.golem.de/news/cursor-ki-agent-loescht-aus-versehen-produktiv-datenbank-2604-208074.html>



# Wo KI oder Projekte scheitern können

## Halluzinationen

KI erfindet Dinge mit Zuversicht

**Lösung:** Prüfschleife einbauen,  
Informationsquelle fest definieren

## Integrationsaufwand

Prototyp  $\neq$  Produktion

**Lösung:** Klein anfangen, dann  
skalieren

## Fehlende Domänenkenntnis

Ohne Kontext = generische  
Antworten

**Lösung:** Systemprompts, RAG, eigene  
Wissensbasis

## Change-Management

Bestes Tool nützt nichts ohne  
Akzeptanz

**Lösung:** Mitarbeiter früh einbinden



# Exemplarischer 5 Schritte Plan

Den richtigen Pilotbereich wählen

- repetitiv, messbar, motiviertes Team

Einen Use Case definieren

- eng und konkret, nicht „wir machen KI“

Mitarbeiter von Anfang an einbinden

- sie lösen ihre eigenen Probleme

Erfolg vorher definieren

Zeit, Fehler, Zufriedenheit messen

Erst beweisen, dann skalieren

Pilot → Nachweis → Ausbau



# Fragen und Antworten

---



Wir sind auch nach dem Webinar  
gern für Ihre Fragen und Ideen erreichbar.  
**Kontaktieren Sie uns gern für ein kostenloses KI Scouting.**



**Matthias**

Hofmann

[matthias@startpunkt.digital](mailto:matthias@startpunkt.digital)



**Tobias**

Wirth

[tobias@startpunkt.digital](mailto:tobias@startpunkt.digital)

Digitalisierung hat kein Ende. Aber einen Anfang.



**STARTPUNKT**  
**DIGITAL**

Startpunkt Digital GmbH // Albert-Einstein-Straße 1, 95028 Hof // [info@startpunkt.digital](mailto:info@startpunkt.digital)

<https://www.startpunkt.digital>