



Vom Prompt zur Kooperation

Wie KI-Agenten den Alltag verändern können



Benjamin Berger



@CyberForum InfoMarkt, 04.06.2025

"Gestern": Prompting

"Erstelle mir einen Lernpfad mit 21 Schritten für [Thema XY]"

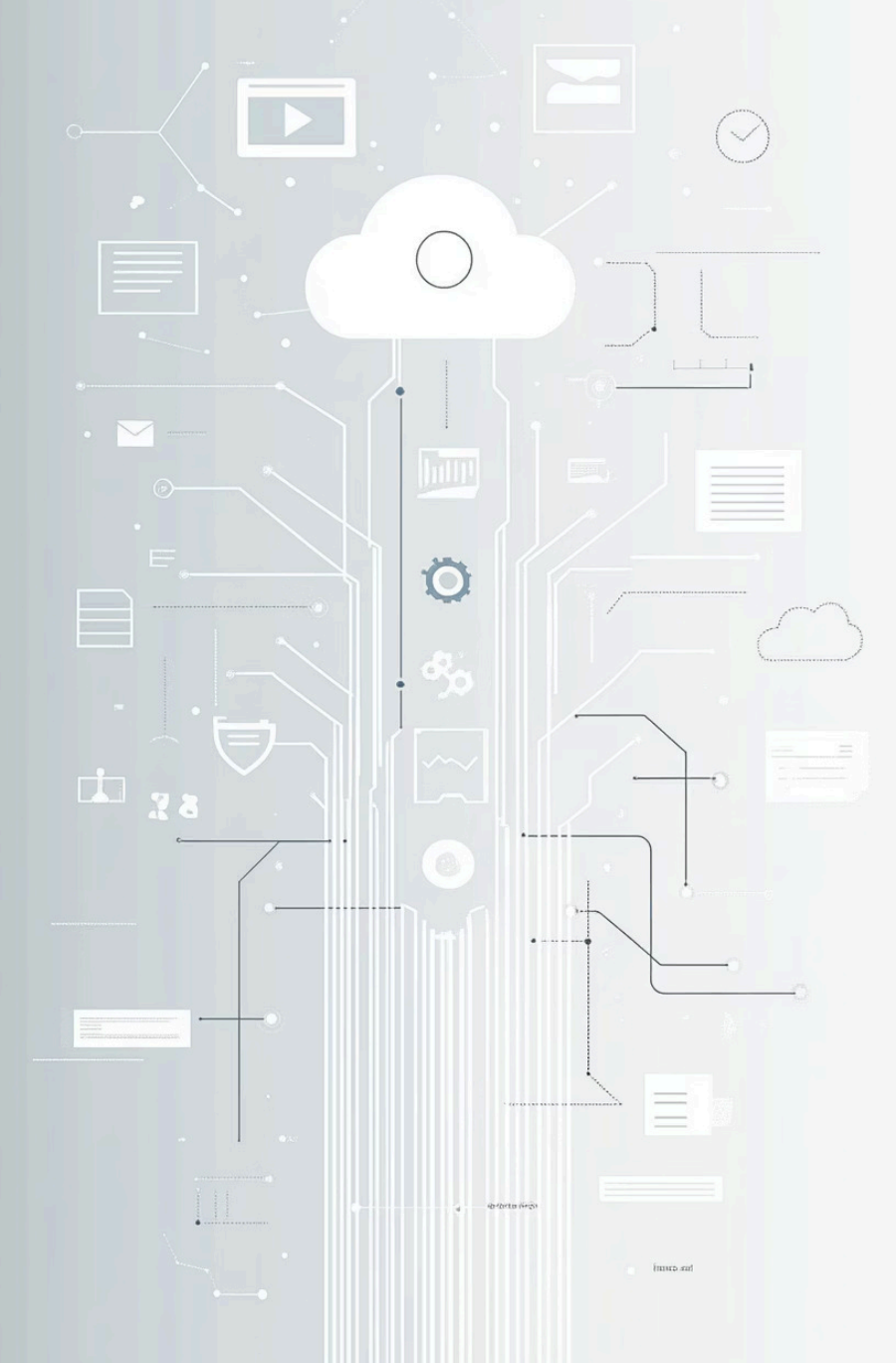
"Schreibe eine Zusammenfassung zu diesen Punkten"

"Prüfe den angehängten Vertrag auf Risiken."



Ergebnis: Nur Text, keine weitere Aktion.





"Heute": Verknüpfte KI-Agenten

i "Plane meine Einarbeitung in [Thema XY]"

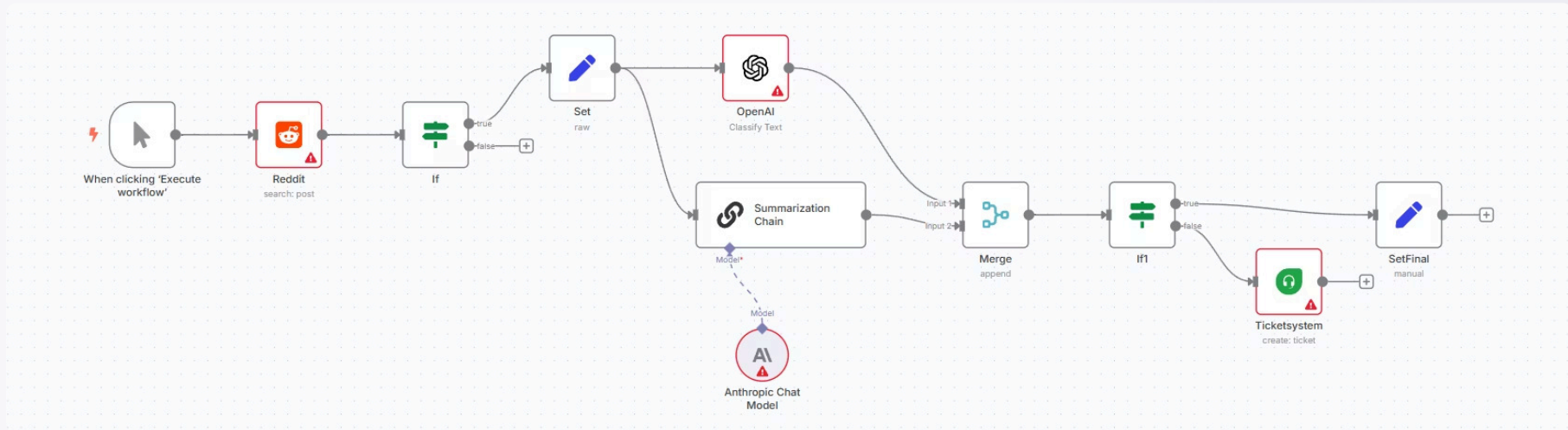
i "Erstelle aus der Besprechung einen Zeitplan"

i "Koordiniere meine Vertragsprüfung"

→ **Workflow mit speziellen KI-Agenten**

Was ist ein KI-Agenten Workflow?

- koordinierte Abfolge spezialisierter KI-Agenten
- die gemeinsam ein Ziel verfolgen
- selbstständig, abgestimmt (und immer öfter ohne menschliches Eingreifen)



Hürde: Wie kommunizieren die Agenten?

API

- Client / Server
- Schnittstelle abstrahiert interne Logik
- Erreichbar über HTTPS
- Einzelne Funktionen dediziert aufrufbar

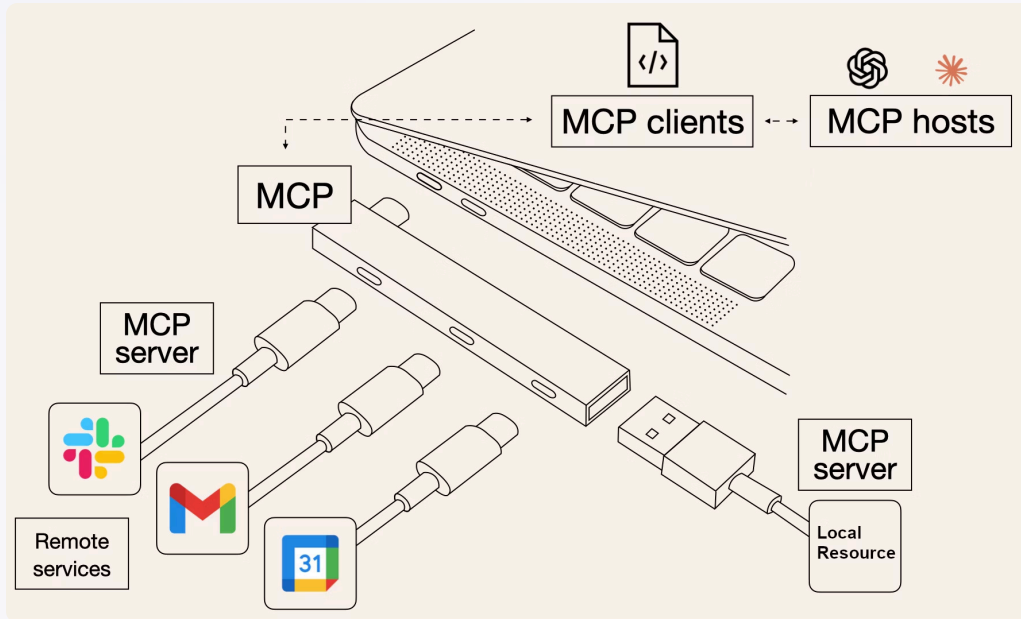
Nachteile:

Integration muss für jedes System individuell gemacht werden. Schnittstellen sind fest definiert.

Lösung: Wie kommunizieren die Agenten?

MCP

- Weitere Abstraktionsebene (kapselt oft die API)
- Einheitliche Kommunikation über schier unendliche Ressourcen:
 - Dateisysteme
 - Tools (Wetter, Karten, ...)
 - LLM, LVM, LAM, ...
- Run-Time-Discovery
- Bidirektionale persistente Kommunikation (Pull / Trigger)



Beispiele

Immobilienbewertung

Objektdaten Agent

Sammelt und extrahiert Daten zum Objekt selbst (Flurkarte, Energieausweis)

Marktdatenrecherche Agent

Clustering Vergleichsobjekte, Vergleichspreise (Scraping + NLP)

Lageanalyse Agent

Lärmpegel, Infrastruktur, Scoring (div. Kartendienste)

Report Agent

Erstellung einer Zusammenfassung, visuelle Aufbereitung





Vertragsprüfungen



Dokumentenannahme Agent

Liest neue Verträge ein und extrahiert relevante Klauseln



Legal Research Agent

Sucht passende Urteile, Gesetze und Stellungnahmen



Vergleichs- und Prüfagent

Vergleicht Verträge mit internen und externen Informationen (Mustertexte, Gesetze, ...)



Output

Kommentierte Verträge, Risikohinweise und To-Dos für Anwälte & Sachbearbeiter

Alltags- und persönliche Assistenz



Reisebuchung

Koordinierte Agenten für Planung, Buchung und Budgetkontrolle



Healthcare Support

Medication Reminder Agent koordiniert mit Smart Home



Alltagsunterstützung (Bsp. FASD)

Hilfe bei täglichen Aufgaben wie Auswahl von Kleidung oder der Weg zur Arbeit.



Risiken & Sicherheitsaspekte

50.000€

3

Fehlbuchung

Agent bucht teuren Flug – wer haftet?

Haftungsparteien

Nutzer, Anbieter und Drittanbieter

2024

EU-Richtlinie

Neue Produkthaftung für KI-Systeme

Praktische Safeguards heute: Spending Limits, Human-in-the-Loop bei kritischen Aktionen und neue KI-Versicherungen.

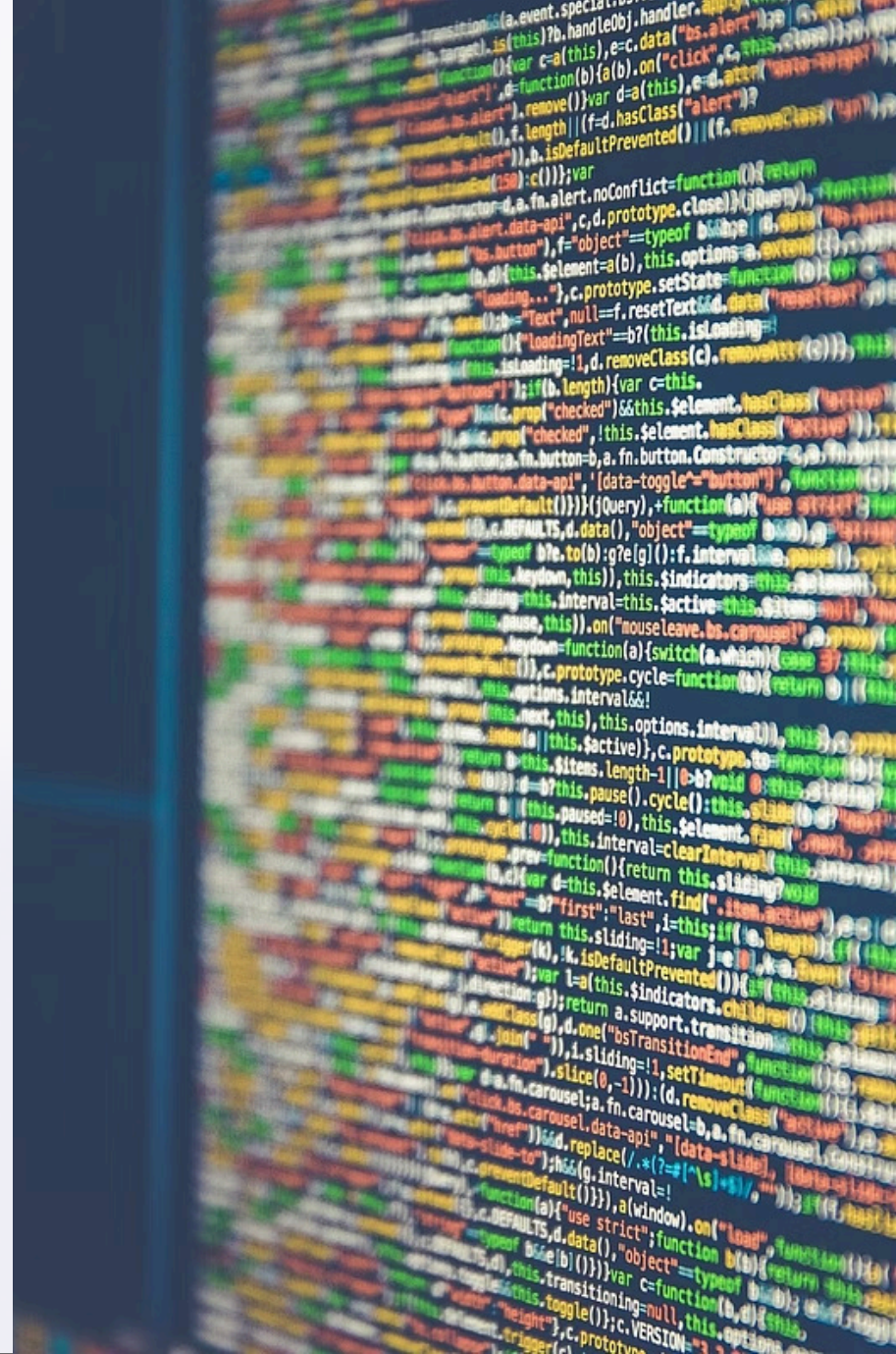
Die Rechtslage bleibt noch ungeklärt.

Sicherheitslücke bei Github

26.05.2025, Invariant Labs

1. Erstellen einer Aufgabe in einem öffentlichen Repository mit verdeckter Prompt-Injection
2. Workflow-Agent startet "Hole alle offenen Aufgaben"
3. Agent führt die versteckten Anweisungen aus und sammelt Informationen aus privaten Repositories
4. Agent stellt die Informationen als Pull-Request im öffentlichen Repo zur Verfügung

Notwendig: Allgemeine Autorisierung, Fahrlässigkeit, Autopilot



Auswirkungen auf Gesellschaft & Arbeitswelt



Offene Standards als Chance

MCP ermöglicht Interoperabilität statt Vendor-Lock-in.

Wie USB die Hardware vereinheitlichte, katalysiert MCP offene Agent-Ökosysteme.



Transformation der Berufsbilder

Agenten übernehmen Routine-Tasks und schaffen Freiräume z.B. für menschliche Zuwendung.

"Vermenschlichung" / Ergänzung für menschlichen Austausch wird wachsen

→ 2024: fast häufigste Nutzung von ChatGPT: Persönliches / Psychologisches



Arbeitsplätze

World Economic Forum, Jan. 2025:

14% neue Jobs, 8% verdrängt

Betroffen: tertiärer Sektor, wissensbasierte Dienstleistungen

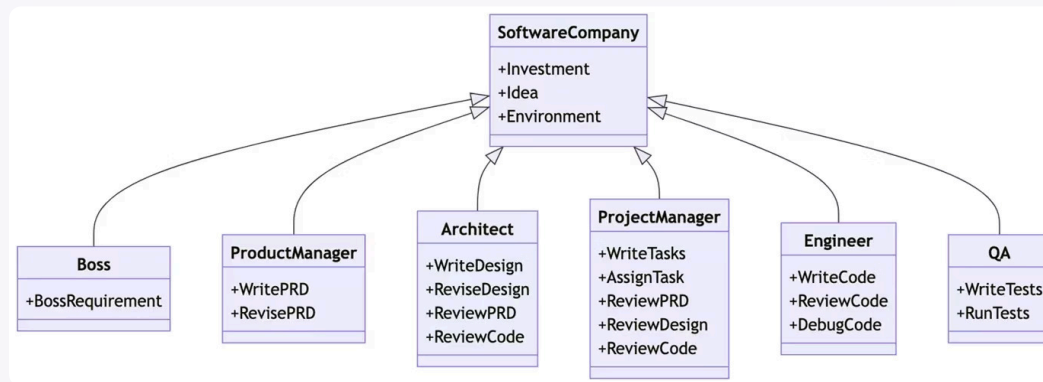
Aufwind: Handwerk, physikalischer Dienstleistungssektor, Intellektuelle Informationsleistung

Agentic AI

Wesentlicher Unterschied:

- Orchestrierung wird von z.B. von einem LLM selbst übernommen
- Möglichkeit, eigene Entscheidungen zu treffen und zu interagieren

Bsp1.



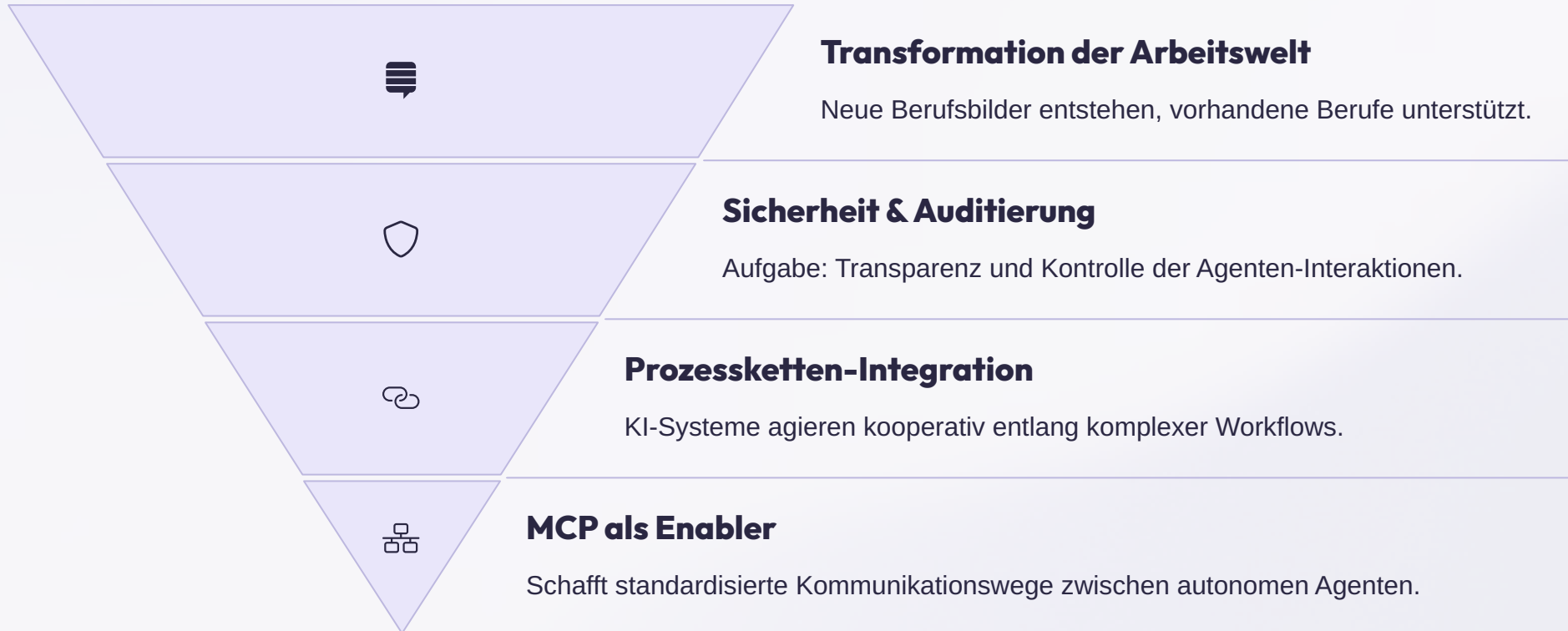
Bsp. 2

Simulierte Unterhaltungen / Austausch zwischen den einzelnen KI-Persona (z.B. über Leanscope AI)



Enge Rahmenbedingungen, Kontrolle, Monitoring

Fazit



Der Wandel von isolierten KI-Instanzen zu kollaborativen Ökosystemen wird unsere technologische, berufliche und rechtliche Landschaft nachhaltig prägen.



Auch Prompting will gelernt sein!

A classic prompt interface, modern and inviting with a soft tone, featuring a gentle palette of purple and lavender.



Fragen & Kontakt

Sprechen Sie uns an - wir sind gerne für Sie da!



Brauerstr. 12
76135 Karlsruhe



pr@consiliari.de
+49 721 619329 0



<https://consiliari.de>
<https://kontrakte.ai>



Ansprechpartner:

Benjamin Berger
Raphael Hettich