
ChatGPT löst kein Verwaltungsproblem
zwischen Wunschbrunnen und Wirklichkeit
MARKUS BEGEROW

DATENBANKEN VERSTEHEN
für Anfänger und Profis

HOCHSCHULE HEILBRONN

Dainalytix
Data | Analytics | AI Research Group

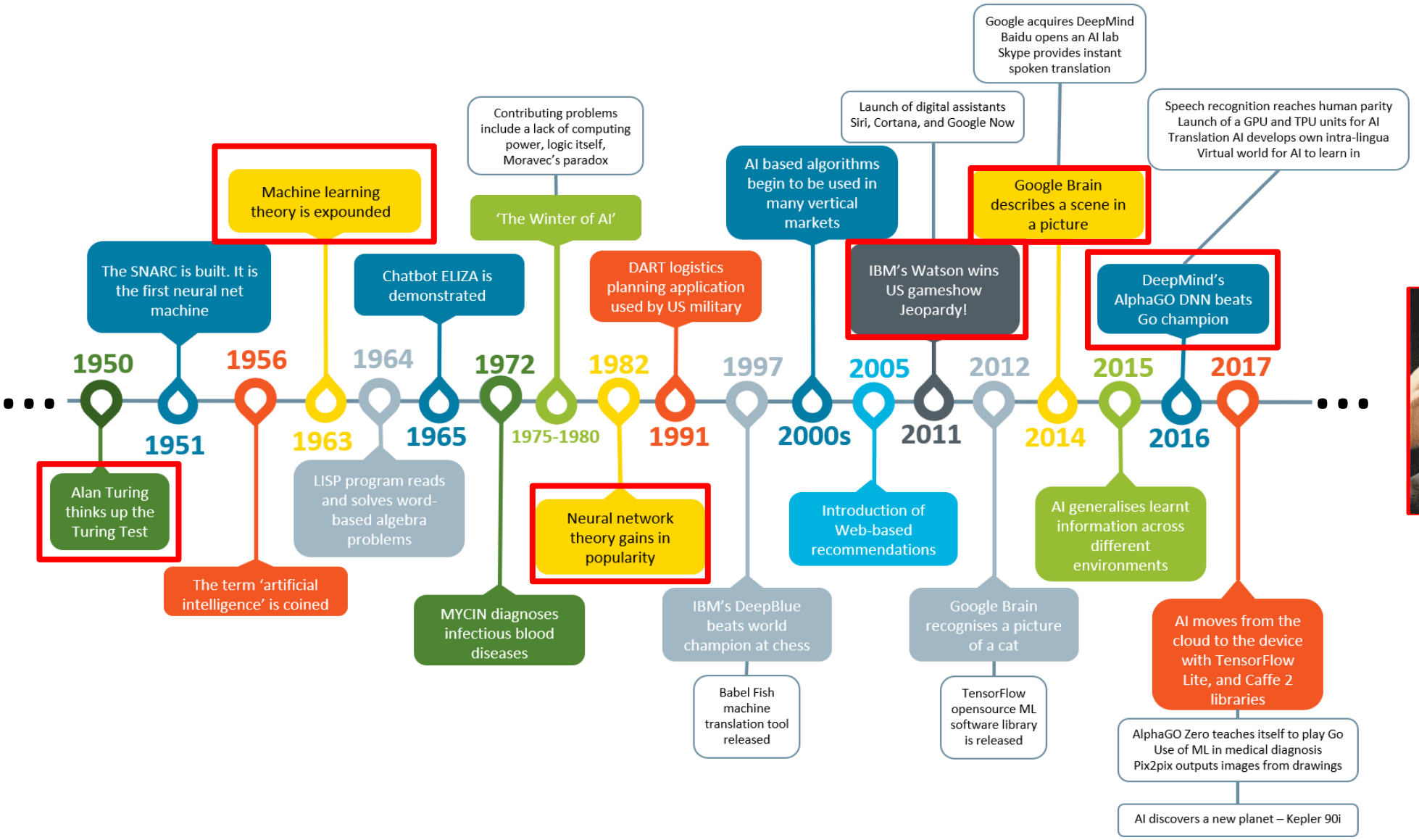
Technische Hochschule Wildau
Technical University of Applied Sciences
WILDAU

Data & AI Campus
Your next level in Data & Analytics

IHK
Industrie- und Handelskammer Heilbronn-Franken

wbh
WILHELM BÜCHNER HOCHSCHULE

Die Entwicklung von KI bis heute



big data
Suchbegriff

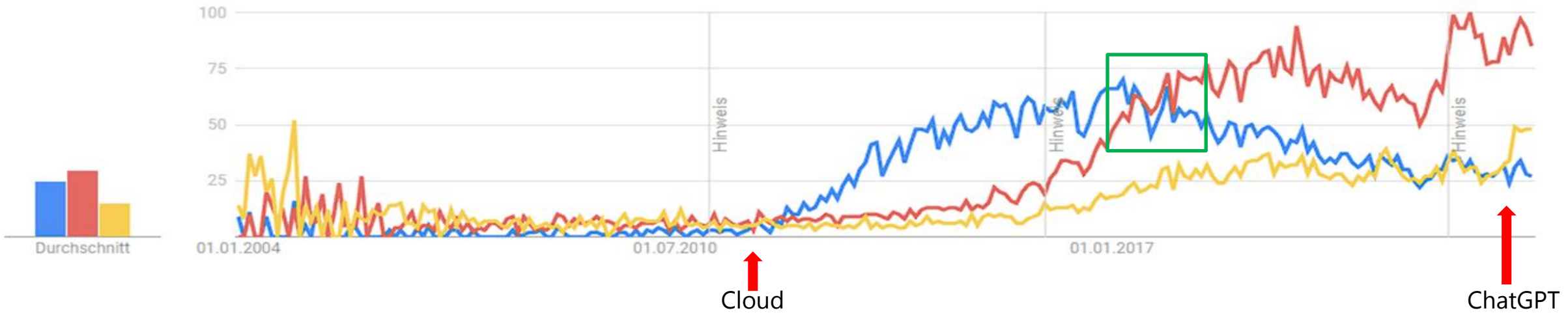
machine learning
Suchbegriff

artificial intelligen...
Suchbegriff

+ Vergleich hinzufügen

Deutschland | 2004 - heute | Alle Kategorien | Websuche

Interesse im zeitlichen Verlauf



Wo stehen wir heute?

Source: Gartner

Source: Heise

Fachkräftemangel: Bis 2030 fehlen über 1 Mio. Beschäftigte

FACHKRÄFTEMANGEL IN BEHÖRDEN

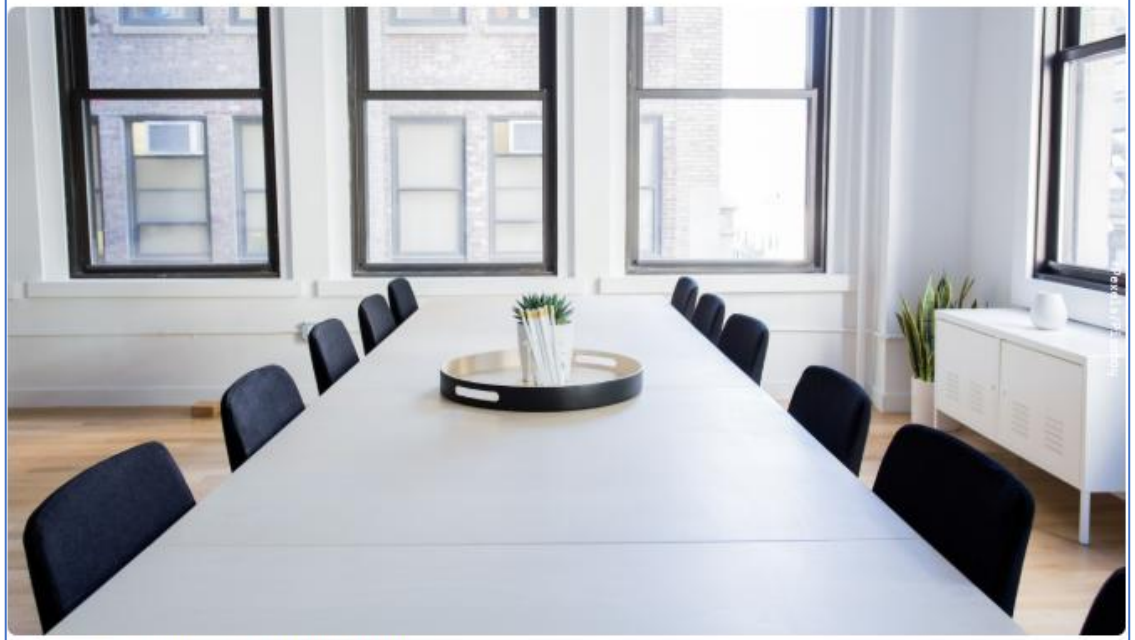
Von der Einsamkeit des Dienststellenleiters

FRUST IM AMT

Ohne Digitalisierung bricht der öffentliche Dienst bald zusammen, weil Fachkräfte fehlen. Ohne die gibt es aber keine Digitalisierung. Wie Mitarbeiter das Dilemma erleben.

19. Mai 2025 um 08:40 Uhr / Eine Analyse von Gerd Mischler

121 News folgen Teilen



Und wer macht jetzt die Digitalisierung?

Source: Golem

Quelle: Shutterstock / jamesteohart

zurück

IT

Fachkräftemangel bremst Smart Cities aus

Mehr als 53 Millionen Euro an Fördermitteln für Smart-Cities-Modellprojekte sind 2024 abgerufen worden. Ein Viertel der da durch geschaffenen Stellen aber konnte nicht besetzt werden.

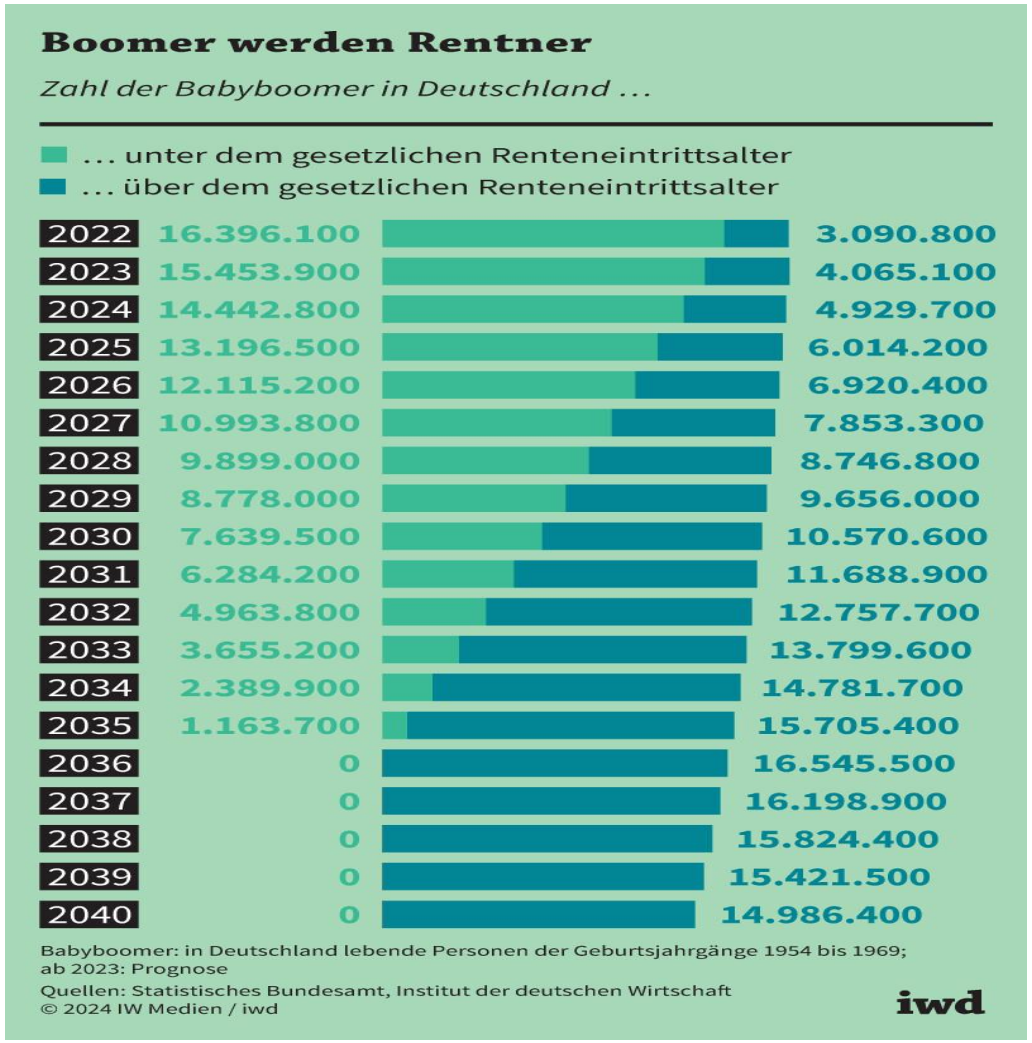
Source: Energie & Management

Demografischer Wandel & Nachwuchsprobleme

ALLGEMEIN 31. JANUAR 2025

Personalmangel gefährdet kommunale Daseinsvorsorge

Source: Klimaschutz Kommune



Source: IWD

Digitalisierung & KI

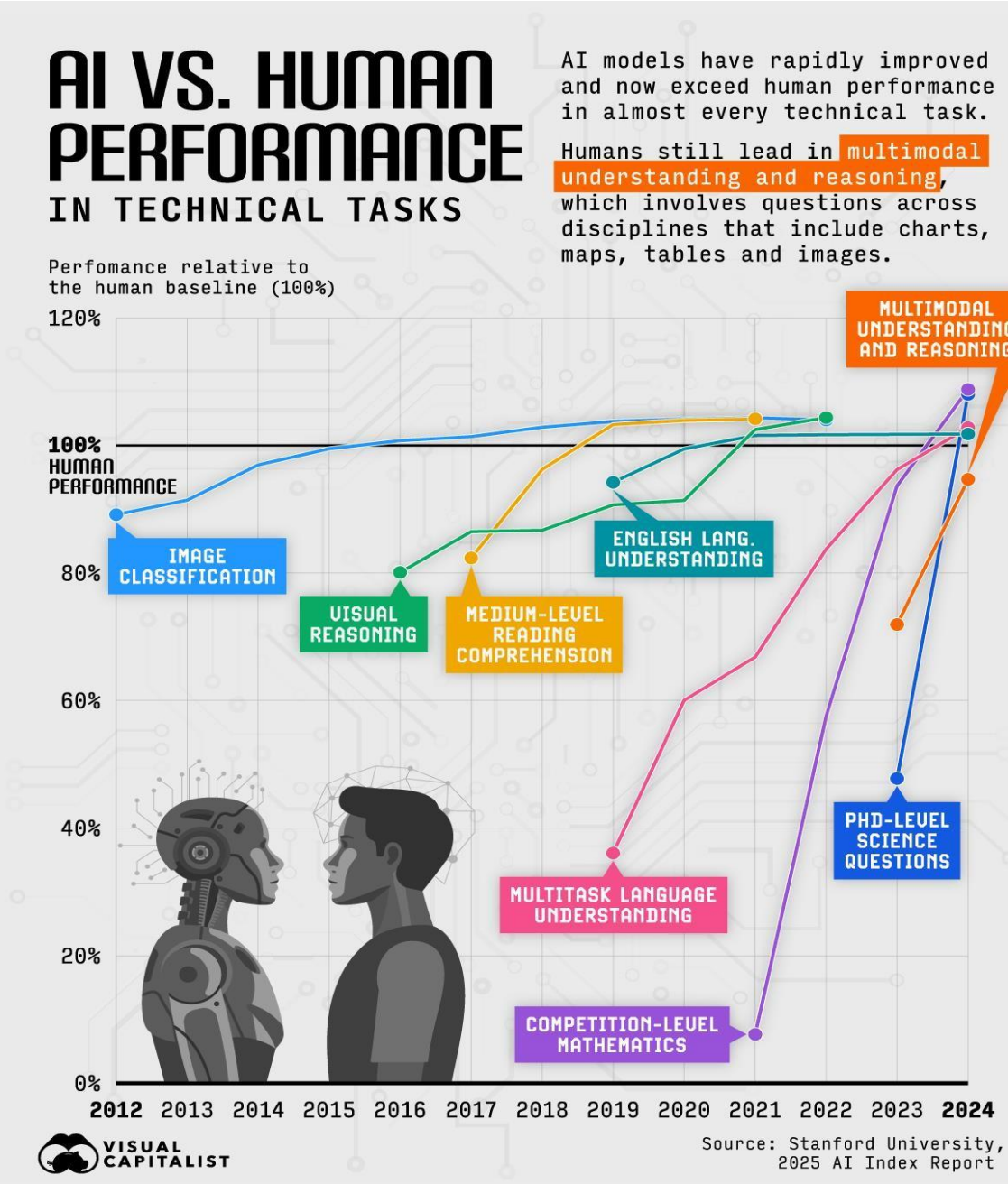
Die langsam voranschreitende Digitalisierung des öffentlichen Dienstes bringt uns auf die Palme!

Der öffentliche Dienst steht aktuell vor zahlreichen Herausforderungen und unter Druck: Mit Verabschiedung des Onlinezugangsgesetzes erwarten Bürger*innen und Unternehmen, dass behördliche Prozesse digital abgewickelt werden. Doch Studienergebnisse zeigen, dass über die Hälfte aller Befragten den Digitalisierungsgrad ihrer Stadt oder Gemeinde als eher oder als sehr rückständig einschätzen (56 % Stand 2023, dbb Monitor 2024). Gegenwärtig sind im Schnitt lediglich 175 Leistungen via Onlineservice digital zugänglich – dies sind 400 weniger als geplant (Behörden Spiegel, Juli 2024).

Source: Golem

Source: Energie & Management

KI wird den Menschen in allen Bereichen, die wir trainieren und testen können, übertreffen - oder hat dies bereits getan.



The AI bubble will burst for firms that can't get beyond demos and LLMs

News Analysis

Feb 16, 2026 • 4 mins

Analysts warn that too many companies are 'chasing the shiny object' wh
the basics of success.

Credit: Bernd von Darl

Source: LMArena.ai; Created by Peter Gostev (https://www.linkedin.com/in/peter-gostev/)

The AI bubble isn't just hype — it's real and could create many corporate casualties if or when it bursts. The companies that will succeed will be the ones solving real-world problems and engaging clients, according to tech industry execs and analysts.

Source: Computerworld

Sam Altman
@sama

Peter Steinberger is joining OpenAI to drive the next
agents. He is a genius with a lot of amazing ideas abo
smart agents interacting with each other to do very u
people. We expect this will quickly become core to ou

OpenClaw will live in a foundation as an open source
will continue to support. The future is going to be ext
and it's important to us to support open source as pa

Post übersetzen

10:39 nachm. · 15. Feb. 2026 · **16,2 Mio.** Mal angezeigt

4.899 8.822 46.299

Relevant

OpenClaw

What People Say

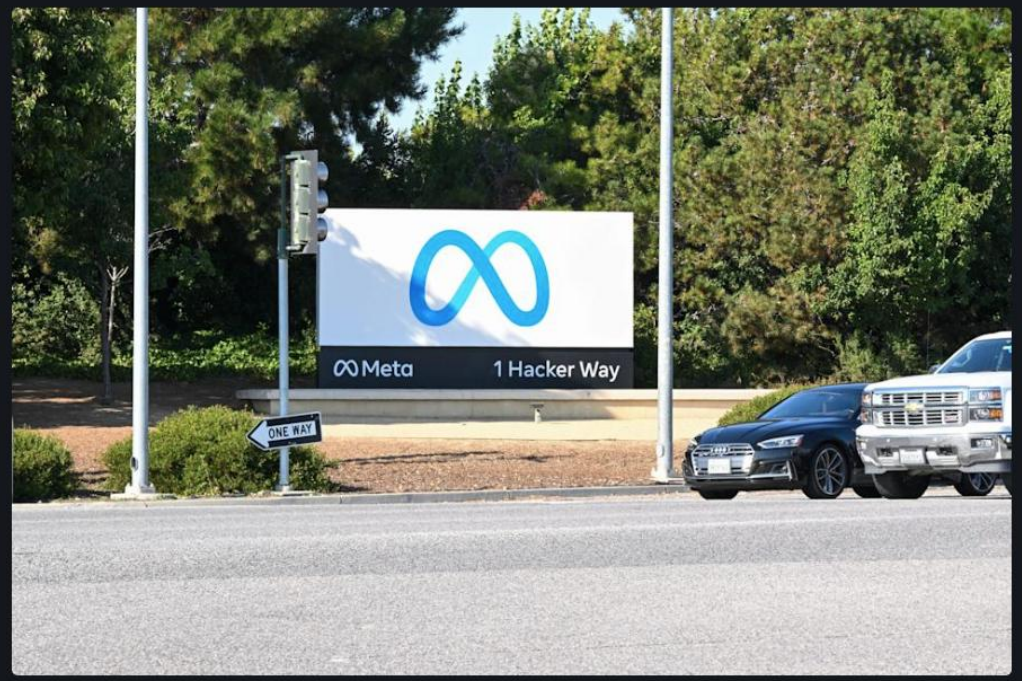
BUSINESS INSIDER

OpenClaw: Meta-Managerin verliert plötzlich die Kontrolle und erlebt einen KI-Albtraum

Henry Chandonnet
Di., 24. Februar 2026 um 12:50 PM MEZ

In diesem Artikel:

BTZI -6,25 %



Meta's Summer Yue bezeichnete ihre OpenClaw-Horrorgeschichte als „Anfängerfehler". - Copyright: Tayfun Coskun/Anadolu Agency via Getty Images

Source: Forbes

AI (artificial intelligence)

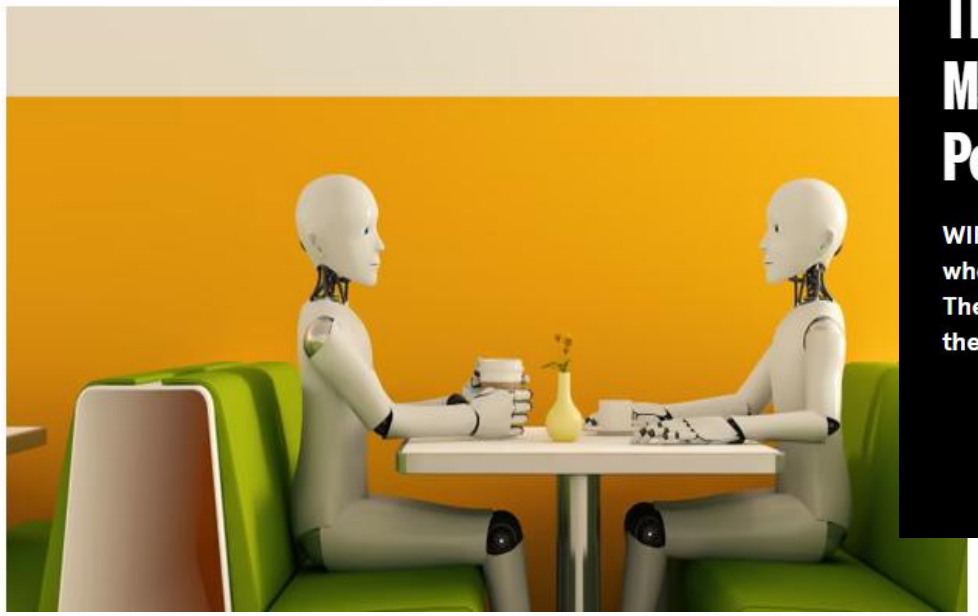
Explainer

What is Moltbook? The strange new social media site for AI bots

A bit like Reddit for artificial intelligence, Moltbook allows AI agents - bots built by humans - to post and interact with each other. People are allowed as observers only

Josh Taylor *Technology reporter*

Mon 2 Feb 2026 06.39 CET



Source: [Forbes](#)

KYLE MACNEILL BUSINESS FEB 18, 2026 6:00 AM

The Rise of RentAHuman, the Marketplace Where Bots Put People to Work

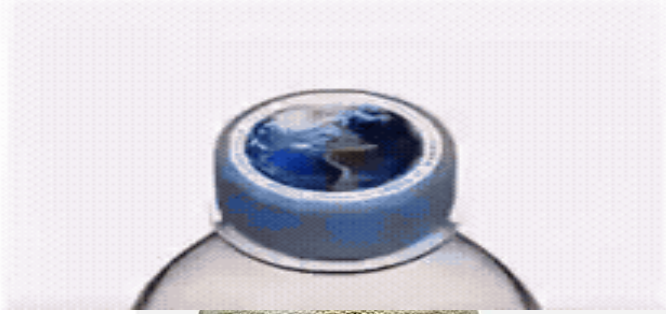
WIRED spoke with the Zoomer founders of a platform where AI agents hire humans to do real-world tasks. Their pitch: "People would love to have a clanker as their boss."

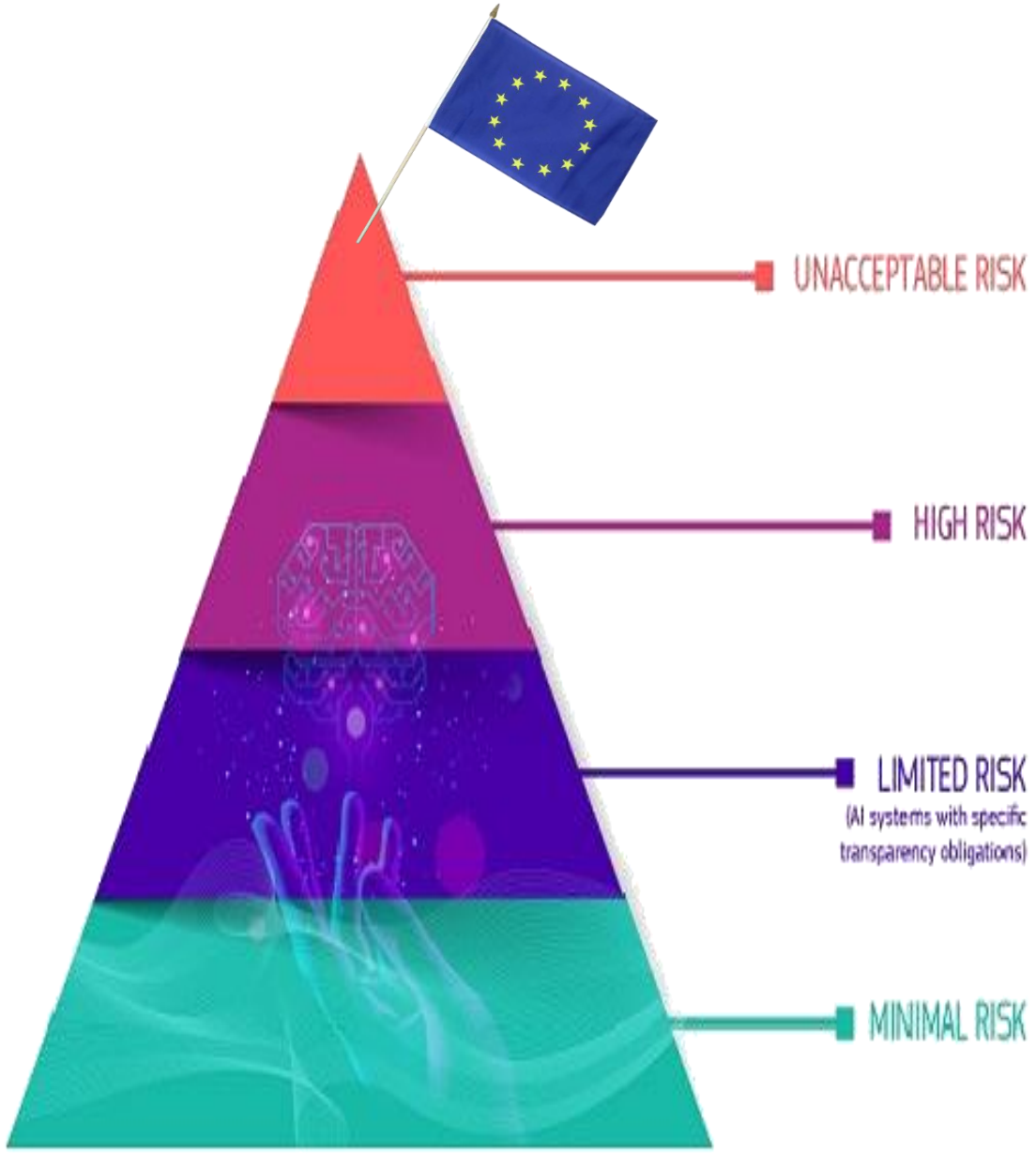
Source: [Wired](#)

CHINA:

USA:

EU:




UNACCEPTABLE RISK
HIGH RISK
LIMITED RISK
(AI systems with specific transparency obligations)
MINIMAL RISK

Zum Glück wird massiv in Sicherheit…

Das Thema „Sicherheit“ bekommt ca. 1% der Ressourcen in der KI-Forschung

FINANCIAL TIMES

My Account

HOME WORLD US COMPANIES TECH MARKETS CLIMATE OPINION LEX WORK & CAREERS LIFE & ARTS HTSI

FT Digital Edition Portfolio myFT

OpenAI Added

OpenAI slashes AI model safety testing time

Testers have raised concerns that its technology is being rushed out without sufficient safeguards

Share

Save

© FT montage/Getty Images

Follow the topics in this article

US companies ✓ Added

Tech start-ups ✓ Added

Artificial intelligence ✓ Added

Technology ✓ Added

OpenAI ✓ Added

Cristina Criddle in San Francisco

Published 2 HOURS AGO

6

OpenAI has slashed the time and resources it spends on testing the safety of its powerful artificial intelligence models, raising concerns that its technology is

START-UP LOCALMIND

Datensichere KI-Plattform aus Tirol

Gruppenfoto der Geschäftsführung: Simon Zanon (CPO), Ivan Dukic (CTO) und Jeremias Fuchs (CEO) bei der Verleihung des Tiroler Innovati (v.l.n.r.).

10.09.2025: https://www.top.tirol/news/datensichere-ki-plattform-aus-tirol

heise online > Heise Serien > Heise Investigativ > Das passiert, wenn der KI-Betreiber die Sicherheit vernachlässigt

Das passiert, wenn der KI-Betreiber die Sicherheit vernachlässigt

Verträge, Rechnungen und weitere sensible Daten erreichten uns via E-Mail. Die Quelle: eine österreichische KI-Firma, die demnach bei der Sicherheit schlampte.

26

Notfall im Rechenzentrum (Bild: vchal/Shutterstock.com)

07.10.2025, 15:43 Uhr Lesezeit: 6 Min. | Security

Von Jürgen Schmidt

07.10.2025: https://www.heise.de/news/Sensible-Unternehmensdaten-ueber-Sicherheitsprobleme-bei-KI-Firma-kompromittiert-10731728.html

KI in der Praxis 10. August 2025

Zenity AgentFlayer: Neue Zero-Click-Hacks gegen populäre KI-Tools

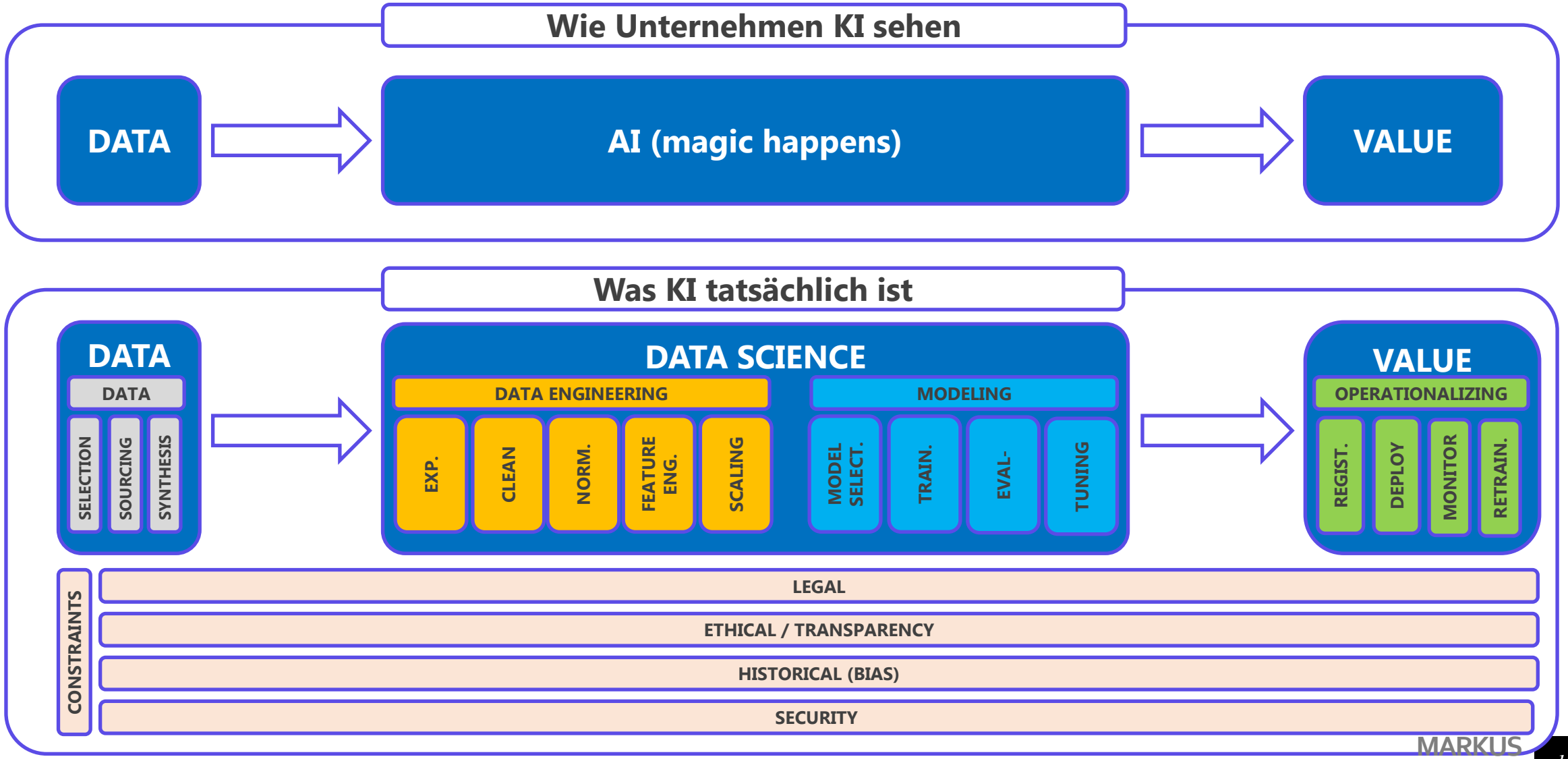
SQL Injection

Prompt Injection

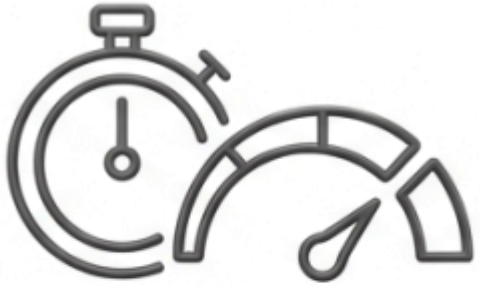
Source: https://the-decoder.de/zenity-agentflayer-neue-zero-click-hacks-gegen-populaere-ki-tools/


Cloud AI
Local AI

Wahrnehmung von Künstlicher Intelligenz



Das Innovations-Dilemma:
Beschleunigung ohne Kontrollverlust.



Der Zwang

Unternehmen müssen innovieren, um wettbewerbsfähig zu bleiben.

Das Risiko

Jeder Mitarbeiter, der unkontrolliert Firmendaten in öffentliche KI-Modelle kopiert, öffnet eine Tür für Datenabfluss.

„Verbote funktionieren nicht -

Steuerung ist die Lösung.“

Die Realität am IT-Radar vorbei:
Die unsichtbare Gefahr der Schatten-KI.

⚠**Status quo**: Die Fachbereiche handeln eigenständig und setzen Tools wie ChatGPT, DeepL & vergleichbare Dienste bereits produktiv ein

⚠**IP-Gefährdung**: Geschäftskritisches Know-how und vertrauliche Informationen verlassen den kontrollierten Unternehmenskontext.

⚠**Steuerungsdefizit im Management**: Die Unternehmensleitung trägt das Haftungs- und Reputationsrisiko.

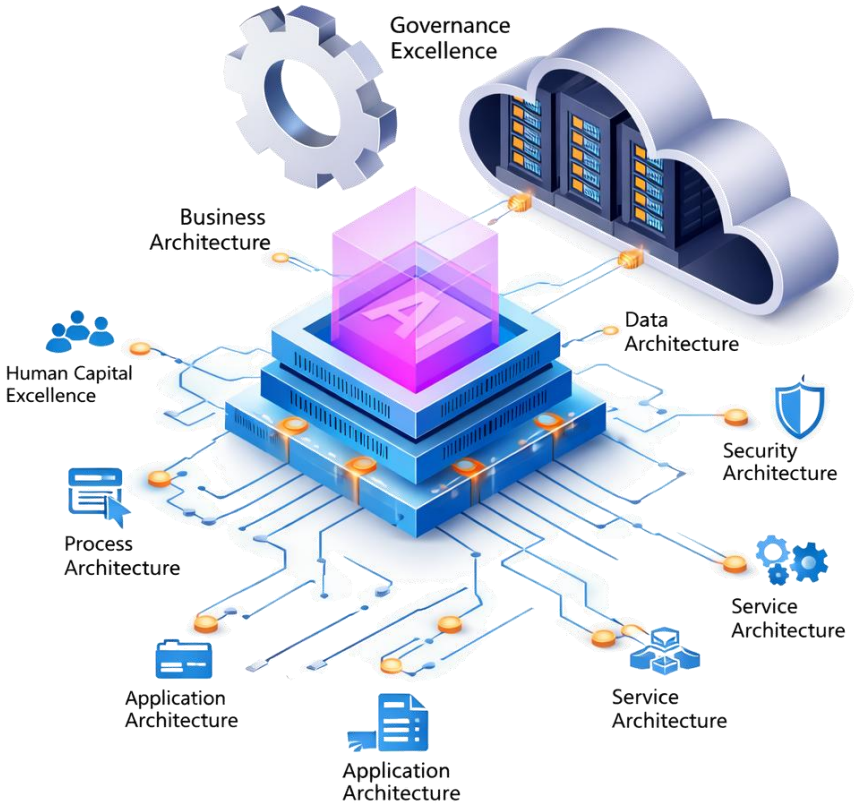
KI ist keine Tech-Frage mehr - **es ist eine Haftungsfrage!**

- **Compliance-Falle**: Unkontrollierter KI-Einsatz ist kein Kavaliersdelikt.
- **EU AI Act**: Die Geschäftsführung haftet für nicht-konforme KI-Anwendungen.
- **DSGVO/GDPR**: Personenbezogene Daten in unsicheren Drittstaat-Clouds können Datenschutzverstöße darstellen.

Compliance darf kein Hindernis sein, sondern muss das automatisierte Fundament bilden.

Strukturen schaffen - Systemarchitekturen aufbauen

Anwendung:
Applikationen werden gezielt über ein differenziertes Rollen- und Berechtigungskonzept bereitgestellt.



Speicherung:
Einsatz unterschiedlicher Datenbanktechnologien mit sicherer, kontrollierter Datenhaltung.

Infrastructure-as-Code: Isolierung einzelner Ökosysteme und Kundenbereiche durch automatisierte, versionierte Infrastruktur.

Governance by Design: Sicherheit ist kein Feature, sondern das Fundament für Vertrauen

Granulares Rollenkonzept:
„Nicht jeder darf alles."
Der Bearbeiter sieht andere Daten als die Sachgebietsleiterin.

Audit-Sicherheit:
Vollständige Nachvollziehbarkeit aller KI-Entscheidungen (Data Lineage) im Einklang mit den Anforderungen des EU AI Act.

Privacy Filters:
Automatische Anonymisierung bzw. Maskierung personenbezogener Daten (PII), bevor sie die Unternehmensgrenzen verlassen.

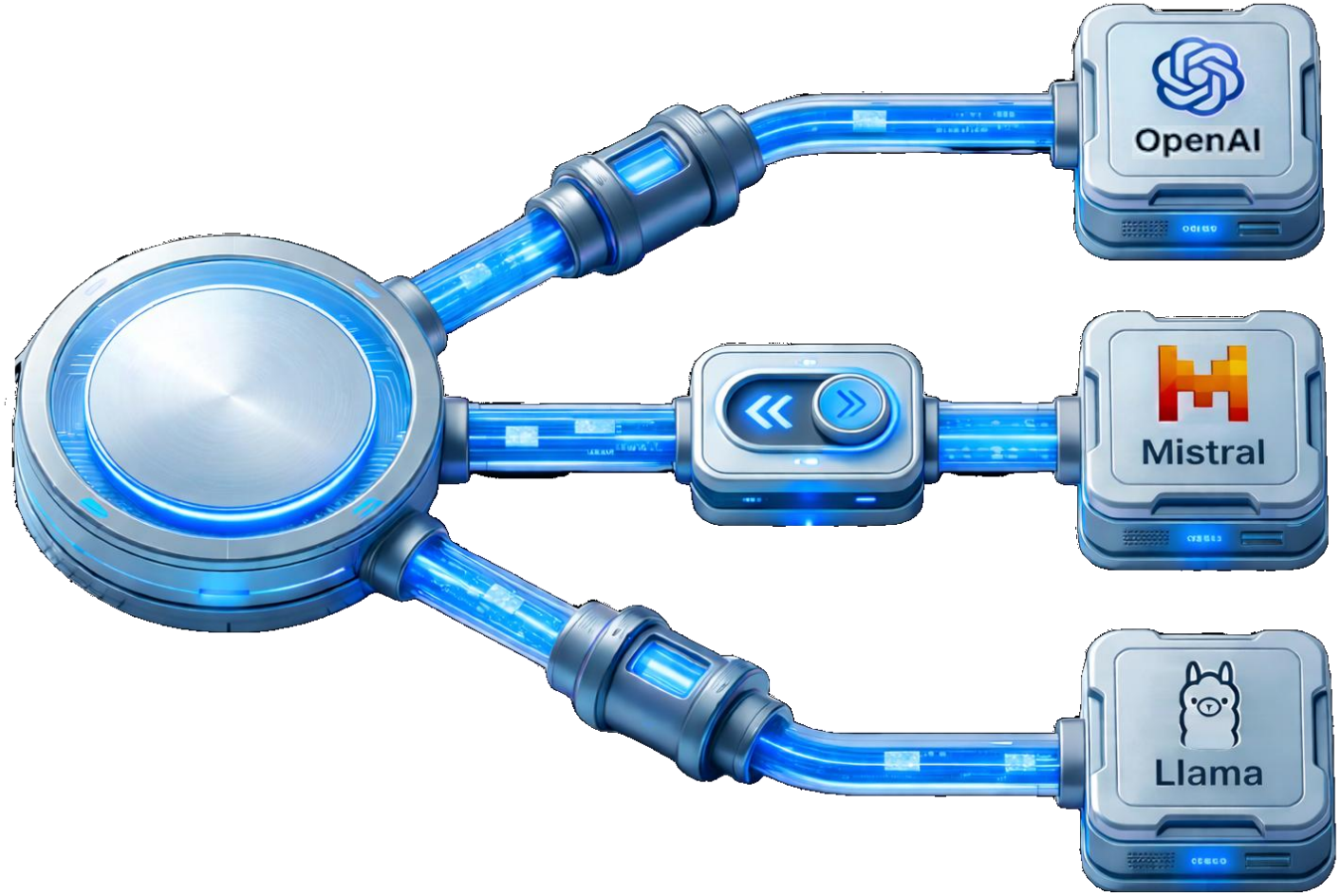
Out-of-the-Box:
DSGVO-konforme Nutzung ohne komplexe Zusatzkonfiguration.

Strategische **Unabhängigkeit durch Modell-Agnostik**

Kein Vendor Lock-in

Heute führt OpenAI, morgen vielleicht Mistral oder Llama.

Eine **gute Architektur** erlaubt Ihnen, die **KI-**Modelle im Hintergrund **zu wechseln**, ohne Ihre Infrastruktur umzubauen.

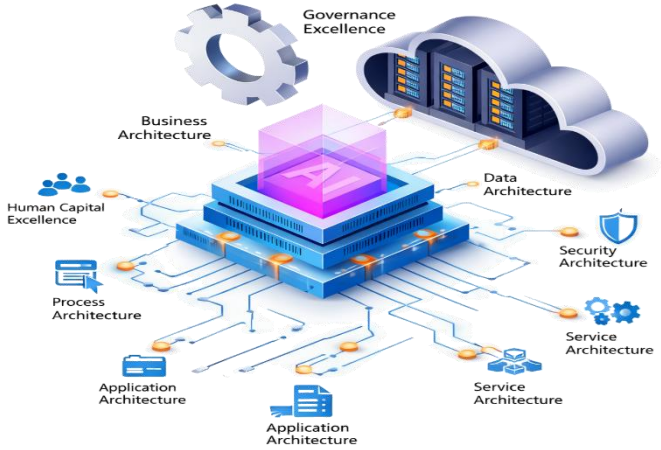


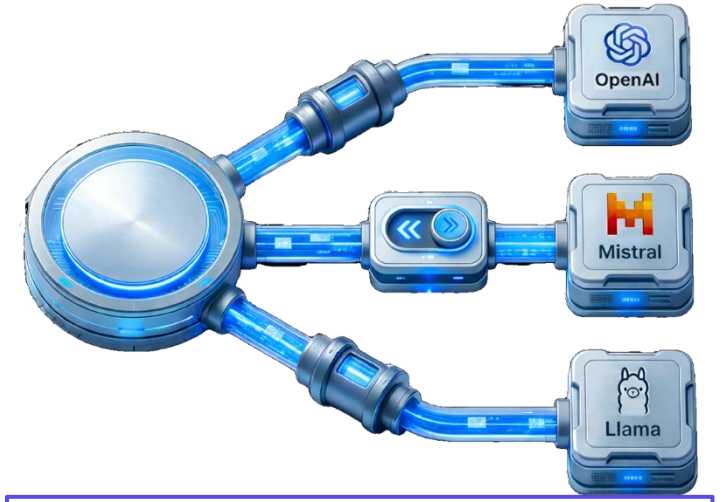
Faktenbasierte Antworten anstatt Halluzinationen

Direkter Vergleich

Kategorie	Cloud AI	Local AI
FOKUS	• Schnelle Skalierung • API-basierte LLM-Nutzung • Generative Use Cases • Globale Verfügbarkeit	• **Interne** Wissensintegration • Kontextualisierte Analyse • **Kontrollierte** Agentenlogik • Unternehmensprozesse unterstützen
ZUGRIFF	• Cloud-Storage • SaaS-Tools • Externe APIs • Vendor-Ökosystem	• Firmen-Datenbanken • ERP/CRM (intern) • Dokumentenmanagement • **Selektive API**-Freigaben
SECURITY	• Abhängig vom Vendor-Setup • Datenübertragung in Cloud • Konfigurationsrisiken • Abhängigkeit von Drittanbieter	• **Voll kontrollierbar** • **Daten** bleiben **intern** • Eigene **Zugriffspolicies** • **Logging** & Audit Trails **vollständig** steuerbar

3 Punkte für den Heimweg…





Kontrolle über Daten

- Daten verlassen nicht das Unternehmen
- Retention & Logs selbst definierbar
- Keine Vendor-Policy-Abhängigkeit

💡 **Souveränität ist Architektur, kein Feature!**

Produktionsreife durch Nachvollziehbarkeit

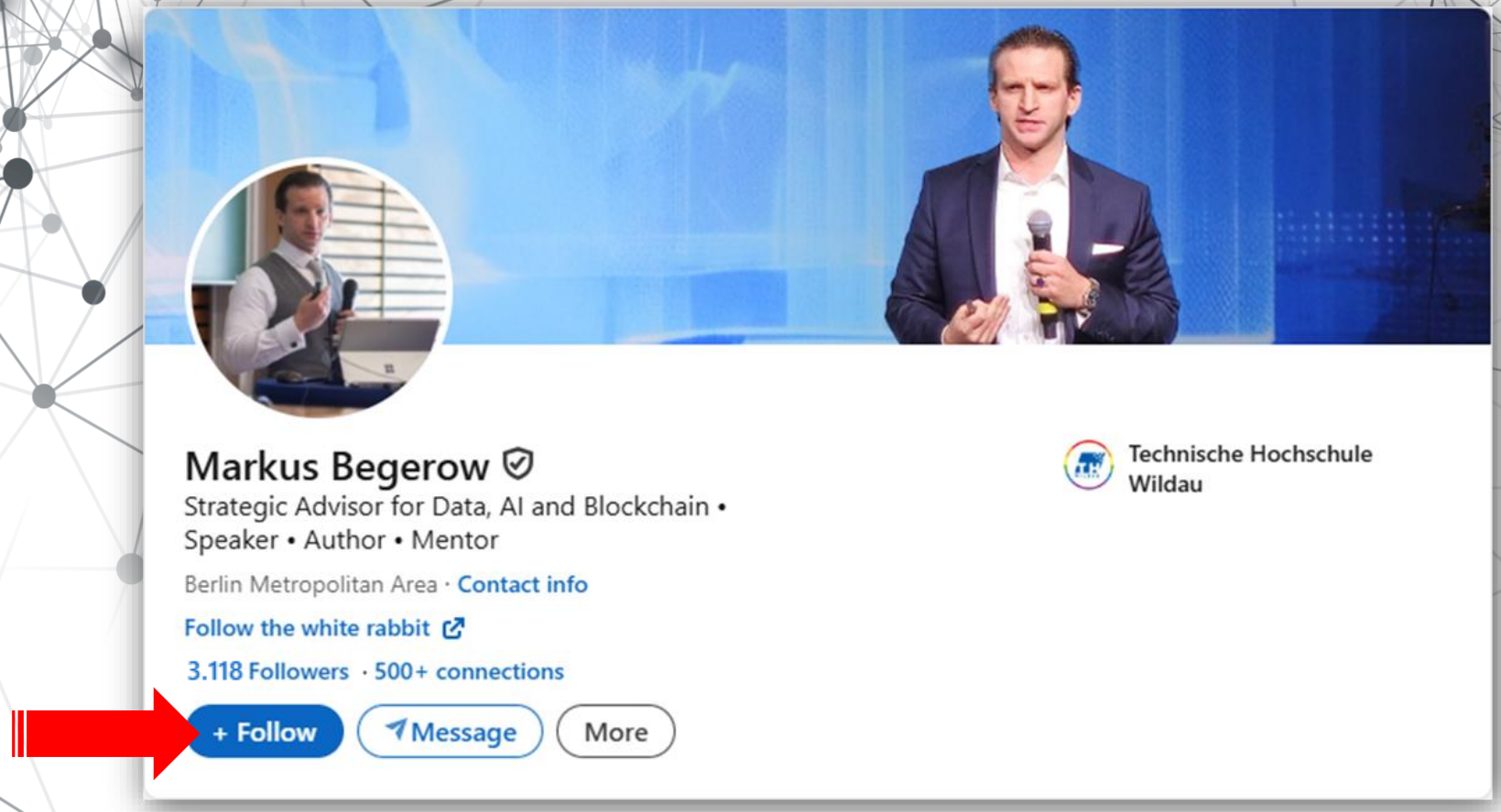
- Vollständige Inference-Logs
- Versionierte Modelle & Prompts
- Nachweis genutzter Datenquellen

💡 **Was nicht prüfbar ist, ist nicht enterprisefähig!!**

Infrastruktur statt Mietlösung

- Keine API-Abhängigkeit
- Kosten langfristig planbar
- Modellwahl frei

💡 **AI ist Infrastruktur - nicht nur ein Service!!!**



THANK YOU!

Slides, Sources, Tools:

markus-begerow.de

@markusbegerow

mail@markus-begerow.de

linkedin.com/in/markusbegerow