Chatbot, Assistent, Workflow, Agent

Die Treppe der KI-Autonomie und was auf jeder Stufe zu sichern ist

Die vier Begriffe werden im Alltag synonym benutzt, dahinter stecken aber völlig verschiedene Konzepte. **Mit jeder Stufe steigt die Autonomie**, und damit der Nutzen, aber auch der nötige Kontrollaufwand. Die Treppe ist kein Ranking, sondern ein Baukasten.

DIE VIER STUFEN

1 CHATBOT

Text im geschlossenen Dialog. Kennt nur den aktuellen Verlauf und hochgeladene Dateien, greift auf keine deiner Systeme zu.

ChatGPT, Claude, Gemini

2 KI-ASSISTENT

Arbeitet mit deinen internen Dokumenten und Wissensdatenbanken. Antworten stehen im Kontext deiner Ablage.

Microsoft Copilot, Gemini Notebook

3 KI-WORKFLOW

Mehrere KI-Schritte in einem festen Prozess. Die Autonomie liegt im Prozessdesign, nicht in der Entscheidungsgewalt der KI.

Automatisierungen, etwa mit Make oder n8n

4 KI-AGENT

Bekommt ein Ziel statt einer Aufgabe, plant die Schritte selbst und nutzt dafür externe Tools.

Höchstes operatives Risiko, auch durch Prompt Injection

WELCHE STUFE BRAUCHST DU?

1. **Nur Text, kein internes Wissen?** Ein Chatbot genügt.
2. **Firmeninterne Daten nötig?** Ein KI-Assistent mit sauberem Rechtemanagement.
3. **Wiederkehrender Standardprozess?** Ein KI-Workflow mit festen Schritten.
4. **Dynamisch lösen, mehrere Tools?** Ein Agent, aber nur mit harten Grenzen.

Beginne auf der untersten Stufe. Ein Agent lohnt sich nur, wenn der Gewinn den Aufwand für Kontrolle übersteigt.

ZWEI ARTEN VON FEHLERN

INHALTLICHE FEHLER

Falsche Aussagen im Text. Ärgerlich, aber korrigierbar, solange ein Mensch liest.

OPERATIVE FEHLER

Falsche Aktionen mit realen Folgen: eine versendete Mail, eine Bestellung, ein geänderter Datensatz. Ab Stufe drei die eigentliche Gefahr.

WAS DU JE STUFE ABSICHERN MUSST

Stufe	Hauptrisiko	Absicherung
Chatbot	erfundene Inhalte	Plausibilität prüfen, nichts Sensibles eingeben
KI-Assistent	Zugriff auf Dokumente, die nicht jeder sehen soll	Rechte sauber vergeben, nur berechtigte Quellen
KI-Workflow	Fehler laufen unbemerkt durch die Kette	Freigaben durch Menschen, saubere Versionierung
KI-Agent	echte Aktionen mit Außenwirkung	Budgets, enge Rechte, engmaschige Überwachung

ZWEI HÄUFIGE VERWECHSLUNGEN

„Der Chatbot kennt unsere Daten.“
Ein reiner Chatbot greift auf nichts zu. Er kennt nur den Verlauf des aktuellen Gesprächs und hochgeladene Dateien.

„Unser Workflow ist ein Agent.“
Beim Workflow steckt die Intelligenz im Prozessdesign. Ein Agent entscheidet selbst, welche Schritte er geht.

WAS DANACH KOMMT

VON REAKTIV ZU PROAKTIV

Alle vier Stufen warten auf einen Auftrag. Die nächste Stufe sind dauerhaft laufende Systeme. Die Frage ist dann strategisch, nicht technisch: Welche Prozesse vertraust du einer laufenden KI an?

MERKSÄTZE

Die vier Stufen sind kein Ranking, sondern ein Baukasten.

Je tiefer der Eingriff, desto stabiler muss die Notbremse sein.