

Wie KI-Agenten wirklich funktionieren: Tool-Aufruf für Entscheider

MANAGEMENT SUMMARY & KERNAUSSAGE

Ein KI-Agent unterscheidet sich von einem Chatbot durch einen iterativen Loop: Er plant (Reason), ruft Werkzeuge auf (Act) und prüft das Ergebnis (Observe) – wiederholt, bis die Aufgabe erledigt ist. Dieser Function-Calling-Mechanismus bestimmt Kosten, Kontrolle und Risiko deiner Agentic-AI-Investition.

KONTEXT & RELEVANZ FÜR ENTSCHEIDER

Wenn ein Vendor dir «agentic AI» verkauft, kaufst du in Wirklichkeit einen Mechanismus: ein Large Language Model, das nicht nur antwortet, sondern in einer Schleife denkt, handelt und das Ergebnis seiner Handlung prüft – so lange, bis eine Aufgabe erledigt ist oder ein Abbruchkriterium erreicht wird. Wer diesen Mechanismus nicht versteht, kann weder Make-vs-Buy-Entscheidungen treffen noch die Governance-Frage beantworten, wer für einen autonomen Fehlentscheid haftet.

Ein Chatbot beantwortet eine Eingabe mit einer Ausgabe. Ein Prompt, eine Antwort, fertig. Ein KI-Agent dagegen erhält ein Ziel und arbeitet selbstständig darauf hin – er entscheidet zwischen mehreren Schritten, ruft externe Systeme auf und passt sein Vorgehen an, wenn ein Zwischenschritt scheitert. Diese Verschiebung von der Einzelantwort zum iterativen Prozess ist der Grund, warum 2026 als Wendepunkt gilt: Details dazu findest du in unserer Einordnung [Warum 2026 das Jahr der autonomen Agenten wird](/ratgeber/von-ai-assistenten-zu-ai-agenten-warum-2026-das-jahr-der-autonomen-agenten-wird).

KERN-HANDLUNGSEMPFEHLUNGEN

- 01 Reason: Das Modell analysiert Ziel, verfügbaren Kontext und mögliche nächste Schritte.
- 02 Act: Es wählt ein Werkzeug aus und ruft es mit strukturierten Parametern auf – eine Datenbankabfrage, eine API, ein Code-Interpreter.
- 03 Observe: Das Ergebnis des Aufrufs wird zurück in den Kontext geschrieben und bewertet.
- 04 Loop oder Stop: Ist das Ziel erreicht, endet der Zyklus – sonst beginnt die nächste Reason-Phase mit erweitertem Wissen.

SCHWEIZER UMSETZUNGSKRITERIEN (REVDSG & IT-ARCHITEKTUR)

- ☑ Vollständige Konformität mit dem neuen Schweizer Datenschutzgesetz (revDSG).
- ☑ Keine Abhängigkeiten: Zero Lock-In auf proprietäre geschlossene Modelle.
- ☑ Schnittstellen zu Schweizer ERPs (Abacus, Bexio, M365) im operativen Betrieb.

Unverbindliche Prozess-Analyse

Lass uns in 20 Minuten prüfen, wo KI-Agenten in deinem Unternehmen sofort messbare Entlastung schaffen.

ki-outsourcing.ch