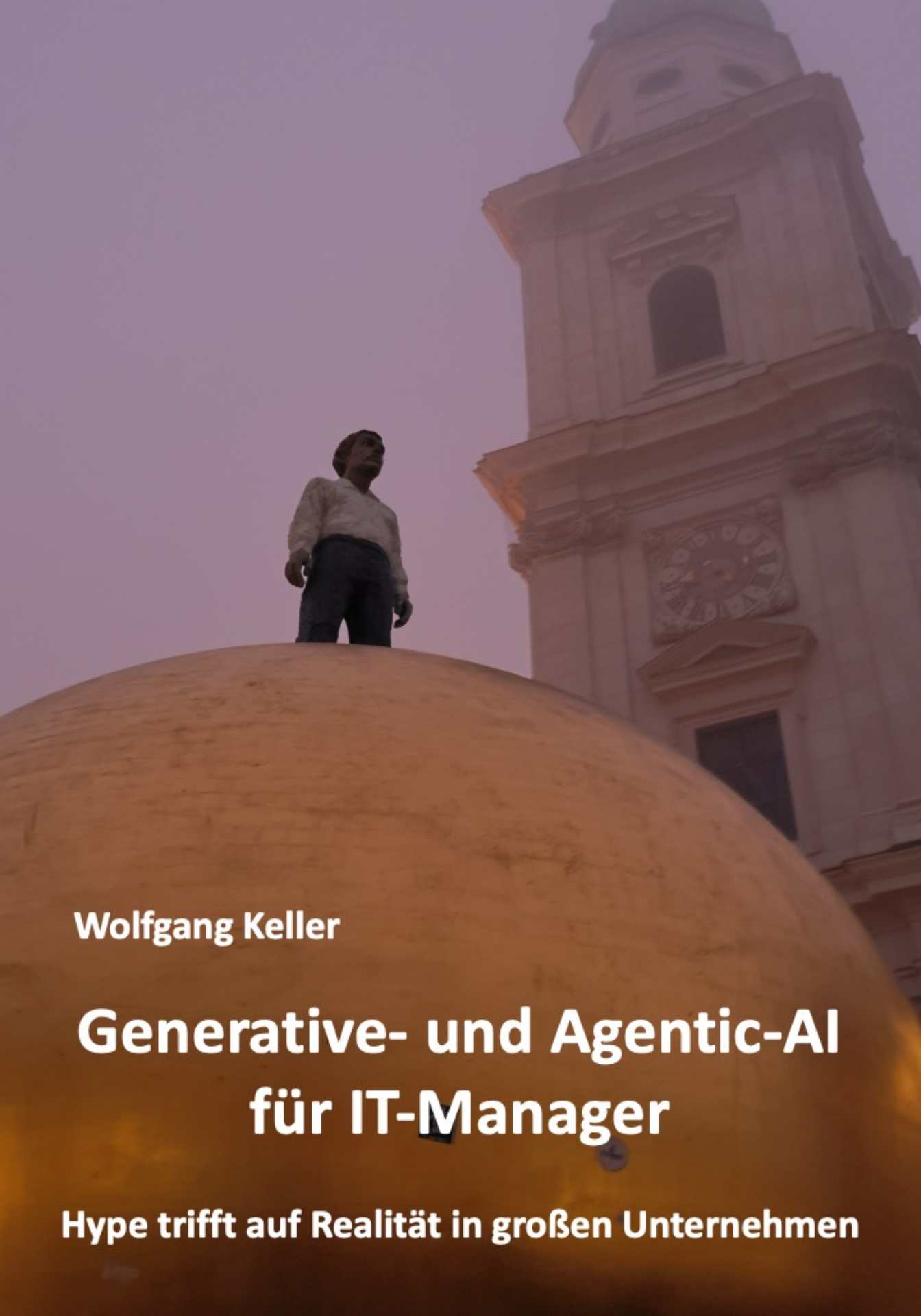

Wolfgang Keller

Generative- und Agentic-AI für IT-Manager

Hype trifft auf Realität in großen Unternehmen

Generative- und Agentic-AI für IT-Manager

Hype trifft auf Realität in großen Unternehmen

Wolfgang Keller

Dieses Buch wird verkauft unter https://leanpub.com/agentai

Diese Version wurde veröffentlicht am 2026-01-20

Inhaltsverzeichnis

Einleitung und Überblick

Generative KI und AI-Agents sind nicht das erste Hype-Thema, das über Unternehmen hereinbricht. Allerdings eines, das offensichtlich eine transformative Kraft entwickeln wird, die die Geschichte bisher noch nicht gesehen hat.

Nach dem ChatGPT-Moment 2022 stellen sich Investoren und angestellte Führungskräfte vom CEO über Enterprise Designer bis zum Fachbereichsmitarbeiter oder Programmierer unter anderem die Frage, wie ihr Unternehmen von KI maximal profitieren kann.

Nebel der Hypes

Generative KI verspricht eine massive Transformation der Unternehmen. Beim „Wie" kann man allerdings schon mal auch im Nebel landen. Dies soll auch das Cover-Bild dieses Buches ausdrücken. Man steht auf einer Kugel aus Gold, aber ein wenig im Nebel. Täglich erscheinen neue Modelle, Agenten-Frameworks und Produktankündigungen. CEOs fragen, wann man „diese KI" endlich einsetzt, Entwicklerteams drängen auf die neuesten Tools, und Berater verkaufen Visionen autonomer Systeme, die Entscheidungen treffen, ohne dafür Menschen zu benötigen.

Zielgruppe für das Buch

Dieses Buch richtet sich an IT-nahe Führungskräfte (Projektmanager, Enterprise Architects, Solution Architects) die die Versprechen umsetzen wollen, die generative KI und AI Agenten machen.

Je nach Brache und Grad der Regulierung stößt man dabei auf unterschiedliche Herausforderungen. Sie werden in diesem Buch vergleichsweise viel über regulierte Branchen wie Banken oder Versicherungen finden. Ähnliche Restriktionen – nur noch härter – gibt es im Gesundheitsbereich. In allen diesen Branchen gibt es vielversprechende Ansätze, aber man kann nicht einfach naiv einen KI-Agenten freilassen und hoffen, dass dadurch der Goldregen über das eigene Unternehmen hereinbricht.

Das Buch wird Ihnen helfen, Herausforderungen zu erkennen, die die Personen, die Ihnen Produkte oder Projekte verkaufen wollen in vielen Fällen entweder nicht kennen oder geflissentlich übersehen.

Dieses Buch ist folglich kein Einführungswerk in den „Maschinenraum“ der KI: Machine Learning oder tiefe Fragen von Agententechnologien. Es geht so tief, wie es nötig ist, um wesentliche Management-Fragen zu erklären. Es ist ein Leitfaden für Menschen, die schon mehr als einen Hype erlebt haben, der regelmäßig über die IT-Welt hereinbricht.

KI in großen und regulierten Unternehmen

Die zentrale These: Generative KI ist ein mächtiges Werkzeug, aber kein Universalwerkzeug. In regulierten Umfeldern kollidieren Autonomie und Nichtdeterminismus mit Anforderungen an Nachvollziehbarkeit, Reproduzierbarkeit und Compliance. Die Frage ist nicht „KI ja oder nein“, sondern „welche KI, wo, unter welchen Kontrollen“. Viele erfolgreiche KI-Anwendungen arbeiten seit Jahren produktiv in der Finanzbranche – ganz ohne autonome Agenten, die selbstständig Entscheidungen treffen.

KI ist mehr als LLMs und Agenten

KI hat eine Geschichte von um die 70 Jahren mit Hochphasen und Eiszeiten. Momentan haben wir eine Warmphase durch LLMs und Agentic AI. Im folgenden Kapitel über Agentic AI findet sich daher zunächst einmal ein Abschnitt darüber, wie Agentic AI und LLMs in Bezug auf die Gesamtgeschichte der KI zu verorten sind.

Struktur: Wer sollte was lesen und warum?

Dieses Buch entsteht aus einzelnen Whitepapers zu Fragen, die rund um den Einsatz von generativer KI und KI-Agenten entstehen müssen, aber oft erst dann auftreten werden, wenn ein Projekt schon eine Weile läuft. In der folgenden Tabelle finden Sie einen Überblick über Inhalte und für welche Zielgruppen welcher Inhalt relevant ist,

Kapitel /Thema	General Management, IT-Management	Enterprise Architects	Solution Architects, BAs, sonstige IT-Professionals
KI die Arbeitet – Keine neuen Direktoren Was sind AI Agenten, wo kann man sie einsetzen und wo nicht	++	++	+
KI und EAM – Die falschen Fragen Wie kann man EAM als Mittel einsetzen, um den Einsatz von KI im Unternehmen voranzubringen. Was passiert, wenn man KI einführt, ohne seine Landschaft aufzuräumen	++	++	o
Agent-Gateways: Die Rache der SOA Argumentiert, dass man zentrale Infrastruktur benötigt, wenn man nicht im Chaos von Punkt zu Punkt-Verbindungen untergehen möchte	+	++	+
Im Land der Lügen: LLMs und Halluzinationen Erklärt was Halluzinationen sind und welche Gefahren sie darstellen	++	++	++
Wie KI auf Unternehmenswissen zugreift Wie kann man ohne teures Training von neuronalen Netzen das Wissen seines Unternehmens in das Wissen von LLMs und Agenten einbeziehen?	+	++	++
Es ist ein Model und es sieht gut aus Erklärt, wie man Vorgehen kann, wenn man KI-Modelle (LLMs) auswählen muss	o	++	++
Antworten zu weiteren Fragen Hier sind Sie gefragt, weitere Fragen zu liefern			

Abbildung 1. Relevanz der Kapitel pro Zielgruppe

Wie geht es weiter?

Das Buch, das Sie vor sich haben ist ein Produkt von „Lean Publishing“. Am Ende kann auch Lean Publishing zu einem seriösen Buch in einem Verlag führen. Aber dieses Medium biete die Möglichkeit, schnell Feedback von seiner Leserschaft zu bekommen.

Die frühen Leser werden dabei mit einem niedrigeren Einstiegspreis belohnt und bekommen, wenn sie das möchten und abonnieren, von leanpub.com automatisch Emails zu Updates. Sie werden also informiert, wenn hier neue Inhalte zur Verfügung gestellt werden.

Sie finden hier auch eine Email-Adresse für Feedback: agentai@objectarchitects.de

Das Buch lebt auch von Ihren Fragen und Verbesserungsvorschlägen.

Warum dieses Buch jetzt schon Geld kostet

Dieses Buch ist kein reiner KI-generierter Schnellschuss, keine Prompt-Sammlung und kein Tool-Katalog. Es ist ein strategisches Fachbuch für Menschen, die Verantwortung tragen. Es adressiert Fragen, die in Projekten oft erst dann auftauchen, wenn es bereits teuer geworden ist:

- Wo sind KI-Agenten sinnvoll – und wo gefährlich?
- Wie kollidieren Autonomie und Regulierung?
- Welche Architekturentscheidungen sind reversibel – und welche nicht?
- Was ist Hype, was ist nachhaltig?

Die Antworten darauf lassen sich nicht aus Marketingfolien ableiten. Der Wert dieses Buches liegt nicht in der Seitenzahl, sondern in der Vermeidung falscher Entscheidungen. Eine einzige falsche Architekturentscheidung, ein falsch eingesetzter Agent oder eine naive Automatisierung in einem regulierten Kontext kann:

- Millionen kosten
- Compliance-Probleme verursachen
- Projekte verzögern
- Vertrauen zerstören Wenn dieses Buch hilft, auch nur eine solche Fehlentscheidung verhindert, hat es sich um ein Vielfaches amortisiert

Wie wurde KI für dieses Buch verwendet?

Ich verwende generative KI – also LLMs – seit mehr als 2 Jahren für diverse Aufgaben aus den Bereichen Beratung, Enterprise Architecture und Solution Architecture. Mein Einsatzgebiet ist dabei vor allem Unterstützung von zunächst Review-Prozessen und in letzter Zeit auch Unterstützung beim Schreiben von Artikeln oder wie hier in diesem Fall Unterstützung beim Schreiben eines Buches. Ich habe für dieses Buch vor allem Claude Opus 4.5 verwendet. Ob das in drei Monaten noch das Top-Modell für solche Aufgaben ist, weiß ich nicht – Heute, im Januar 2026 ist es das für meine Zwecke.

Ein beliebter Spruch im Kontext von Büchern, die mit KI-Hilfe geschrieben werden, ist:

> Wenn sich der Autor keine Mühe gibt, das Buch zu schreiben, dann muss ich mir auch keine Mühe geben, es zu lesen

Das traf auf eine Welle von KI-generierten Büchern in der ersten Begeisterungswelle von KI sicher zu. Inzwischen hat sich das gebessert und auch ein Buch mit KI-Unterstützung kann noch eine kreative Leistung darstellen, wenn Sie sich den Prozess ein wenig ansehen:

- Zunächst braucht ein solches Buch die richtigen Fragen. Die kommen im Fall dieses Buches aus der Erfahrung mit vielen anderen Hypes und aus langjähriger Erfahrung mit großen, komplexen Software-Projekten.
- KI ist nicht gut in Ironie oder dabei, Titel und Thesen zu schreiben, die zum Lesen oder denken anregen.
- Man muss als Autor immer abwägen, wo man die potenziell drögen Aufzählungen typischer KI-generierter Dokumente zulässt, oder wo man sie überschreibt. Dabei helfen heute auch KI-Detektoren – das ist eine eigene Geschichte, die nicht Gegenstand dieses Buches sein soll.
- KI beschleunigt Literaturrecherchen extrem. Die haben zwar zugegeben nicht die Qualität wie „ausgewogene Zitate aus seriösen wissenschaftlichen Werken“ – aber die Welt bewegt sich so schnell, dass das auch nicht für jedes Buch erforderlich ist. Für das Ziel dieses Buches war es wichtig mit der Geschwindigkeit des Hype zumindest einigermaßen mitzuhalten. Und da ist schon der Reviewzyklus für eine Fachzeitschrift zu langsam.
- Und schließlich hat KI geholfen, die ersten LinkedIn-Whitepapers, die ich zu dem Thema geschrieben habe, schnell in das Eingabeformat von Leanpub zu transformieren. Ich habe auch vor 10 Jahren schon ohne KI auf leanpub publiziert. Die Geschwindigkeit von drögen Routineaufgaben und Qualitätschecks hat sich durch den Gebrauch von generativer KI extrem gesteigert.

Alles in allem also Gründe für mich, warum ich auch für die Leser keinen Mehrwert darin sehe, das Buch in „reiner Handarbeit“ zu schreiben. Dafür ist das Thema, das wir hier gemeinsam verfolgen auch viel zu schnell.

KI die arbeitet - Keine neuen Direktoren

Warum Agentic AI in regulierten Umfeldern nicht das Optimum sein muss

Autonome KI-Agenten sollen bald selbstständig entscheiden, planen und handeln. Aber was, wenn genau das in regulierten Umfeldern gefährlich ist?

Agentic AI gilt als nächster Evolutionsschritt der Künstlichen Intelligenz: Systeme, die Ziele formulieren, Pläne entwickeln und eigenständig handeln. Zusammen mit LLM sorgt sie momentan für einen Hype. Für Marketing, Content-Produktion und auch in Teilaspekten der Softwareentwicklung kann das enorme Produktivitätsgewinne bringen. Doch in stark regulierten Branchen wie Versicherungen, Banken oder dem Gesundheitswesen kollidieren genau diese Eigenschaften mit zentralen Anforderungen: Nachvollziehbarkeit, Reproduzierbarkeit, Haftung und Compliance.

Dieser Artikel zeigt, warum Nichtdeterminismus, fehlende Erklärbarkeit und schwer kontrollierbare Autonomie dort nicht nur technische, sondern auch regulatorische und organisatorische Risiken darstellen. Anhand historischer Einordnung, einer verständlichen technischen Analyse moderner KI-Agenten und konkreter Praxisbeispiele wird deutlich: Viele erfolgreiche KI-Anwendungen arbeiten seit Jahren produktiv – ganz ohne autonome Entscheidungslogik.

Statt „mehr Autonomie um jeden Preis“ plädiert der Beitrag für eine differenzierte Sicht: Agentic AI ist ein mächtiges Spezialwerkzeug, aber kein Universalwerkzeug.

Nach der Lektüre wissen Sie, wo Agentic AI das Potential hat echten Mehrwert zu liefern und wann klassische, deterministische KI-Architekturen die bessere, sicherere und langfristig klügere Wahl sind.

AI und der Hype

AI ist viel mehr als LLMs und Agentic AI

Wenn man heute über Künstliche Intelligenz spricht, denken die meisten sofort an ChatGPT, Claude oder andere Large Language Models. Der aktuelle Hype um Agentic AI verstärkt diesen Eindruck noch. Dabei vergisst man leicht, dass KI eine über siebzigjährige Geschichte hat – und dass vieles von dem, was heute in Unternehmen funktioniert, gar nichts mit LLMs zu tun hat.

Die Geschichte beginnt 1950, als Alan Turing in seinem berühmten Paper „Computing Machinery and Intelligence" die Frage stellte: „Can machines think?" [Britannica 2024]. Der Turing-Test, den er in diesem Zusammenhang vorschlug, beschäftigt Philosophen und Informatiker bis heute. Turing selbst arbeitete bereits an frühen Konzepten für neuronale Netze – Ideen, die erst Jahrzehnte später praktische Bedeutung erlangen sollten.

1956 fand am Dartmouth College jene legendäre Konferenz statt, bei der John McCarthy den Begriff „Artificial Intelligence" prägte. Die Teilnehmer – darunter Marvin Minsky, Claude Shannon und Herbert Simon – waren überzeugt, dass binnen einer Generation Maschinen geschaffen würden, die den Menschen in intellektuellen Aufgaben ebenbürtig wären [Britannica 2024]. Diese Zuversicht war nicht unbegründet: In den folgenden Jahren entstanden Programme, die Schach spielten, mathematische Theoreme bewiesen und algebraische Textaufgaben lösten. Die Euphorie dieser frühen Jahre lässt sich kaum überschätzen – man glaubte wirklich, das Geheimnis der Intelligenz sei in greifbarer Nähe.

ELIZA, entwickelt 1966 von Joseph Weizenbaum am MIT, simulierte einen Rogerschen Psychotherapeuten und täuschte viele Nutzer darüber hinweg, dass sie nur mit einem Programm sprachen. Das war beeindruckend – aber auch ein früher Hinweis auf die Probleme, die wir heute bei LLMs wiederfinden: Die Fähigkeit, überzeugend zu klingen, ohne wirklich zu verstehen. Weizenbaum selbst war entsetzt darüber, wie bereitwillig Menschen dem Programm ihre intimsten Geheimnisse anvertrauten, und wurde zu einem der schärfsten Kritiker seiner eigenen Erfindung.

Dann kam der erste „AI Winter" in den 1970er Jahren. Die Versprechen hatten sich nicht erfüllt, die Rechenleistung reichte nicht aus, und die Geldgeber wurden ungeduldig. Wer je erlebt hat, wie ein Hype-Zyklus in sich zusammenfällt, kennt das Muster: Erst grenzenlose Euphorie, dann die Ernüchterung, wenn die Realität hinter den Powerpoint-Folien zum Vorschein kommt. In den 1980er Jahren erlebten Expertensysteme einen kurzen Boom – Programme, die das Wissen menschlicher Experten in Regelwerken kodierten. MYCIN diagnostizierte bakterielle Infektionen, DENDRAL identifizierte chemische Verbindungen. Diese Systeme funktionierten in eng begrenzten Domänen erstaunlich gut, aber sie waren

spröde: Jede neue Situation erforderte neue Regeln, und das Wissen der Experten in formale Logik zu übersetzen, erwies sich als mühsamer als erwartet.

Der nächste Winter folgte Ende der 1980er. Wieder einmal hatte sich gezeigt, dass die Probleme schwieriger waren als gedacht. Die KI-Forschung zog sich in die akademischen Nischen zurück, und wer das Wort „KI“ in einem Förderantrag verwendete, konnte sich auf skeptische Blicke gefasst machen.

Was viele nicht wissen: In dieser scheinbar ruhigen Phase wurden die Grundlagen für den heutigen Erfolg gelegt. Die Backpropagation-Algorithmen für neuronale Netze wurden verfeinert. Statistische Methoden ersetzten symbolische Ansätze. Und in der Finanzbranche begann KI still und leise, echte Arbeit zu verrichten – nur nannte man es nicht so, weil der Begriff verbrannt war.

Kreditscoring-Modelle, die heute jede Bank verwendet, basieren auf maschinellem Lernen – auch wenn die Marketingabteilung das Wort vermeidet. Wenn Ihre Kreditkarte plötzlich gesperrt wird, weil das System eine ungewöhnliche Transaktion erkannt hat, dann war das ein KI-System, das seit den 1990er Jahren weitgehend automatisiert Betrug erkennt. Rückversicherer nutzen komplexe statistische Modelle zur Risikobewertung von Naturkatastrophen, die auf Jahrzehnten von Schadendaten trainiert wurden. PDF-Extraktion und automatische Dokumentenklassifizierung sind in der Schadenbearbeitung großer Versicherer seit Jahren Standard – langweilige, unsichtbare Arbeit, die niemanden begeistert, aber Millionen an Personalkosten spart.

All das ist KI – aber keine, die auf LinkedIn Schlagzeilen macht. Es sind spezialisierte Systeme, die eine Aufgabe gut erledigen, ohne philosophische Fragen aufzuwerfen. Sie planen nicht autonom, sie generieren keine kreativen Texte, und sie führen keine Gespräche. Aber sie funktionieren. Zuverlässig. Seit Jahren. Und darauf kommt es in einem regulierten Umfeld letztlich an.

Der eigentliche Durchbruch kam 2012, als ein neuronales Netz namens AlexNet den ImageNet-Wettbewerb mit einem Vorsprung gewann, der die Fachwelt erschütterte [Britannica 2024]. Deep Learning war plötzlich mehr als ein akademisches Kuriosum. Die Kombination aus riesigen Datenmengen, leistungsfähigen GPUs – ursprünglich für Computerspiele entwickelt, aber perfekt geeignet für Matrixmultiplikationen – und verbesserten Algorithmen ermöglichte Fortschritte, die selbst Optimisten nicht erwartet hatten.

2016 besiegte AlphaGo den Weltmeister im Go – ein Spiel, bei dem die Zahl der möglichen Stellungen die Anzahl der Atome im Universum übersteigt. Das war keine Rechengewalt mehr, das war etwas Neues: ein System, das Intuition zu haben schien. Der entscheidende Zug 37 in Spiel zwei – ein Zug, den kein menschlicher Spieler je machen

würde und der sich als genial erwies – wurde zur Ikone einer neuen Ära.

2022 kam ChatGPT auf den Markt. Plötzlich konnte jeder mit einer KI sprechen, die nicht mehr nach Maschine klang. Die Fragen beantwortete, Texte schrieb, Code generierte – und dabei oft verblüffend kompetent wirkte. Der Hype war geboren, und diesmal erreichte er eine Öffentlichkeit weit jenseits der Tech-Bubble.

Was dabei untergeht: Die meisten Unternehmen, die heute erfolgreich KI einsetzen, tun das weniger mit ChatGPT oder seinen Konkurrenten. Sie nutzen die langweilige, aber bewährte KI der letzten Jahrzehnte – angereichert um moderne Methoden, wo es sinnvoll ist. Der Sachbearbeiter, der täglich Schadenmeldungen bearbeitet, profitiert von der automatischen Dokumentenklassifizierung im Hintergrund. Dass diese auf einem neuronalen Netz basiert, interessiert ihn zu Recht nicht.

Agents Explained

Was unterscheidet LLM-basierte Agenten von anderen Formen der KI

Der Begriff „Agent“ ist in der KI-Forschung nicht neu. Stuart Russell und Peter Norvig definieren in ihrem Standardwerk „Artificial Intelligence: A Modern Approach“ einen Agenten als ein System, das seine Umgebung wahrnimmt und durch Aktionen beeinflusst [Russell/Norvig 2023]. Ein Thermostat ist nach dieser Definition bereits ein Agent – ein sehr einfacher zwar, aber einer, der auf Temperaturänderungen reagiert und entsprechend handelt. Diese breite Definition ist philosophisch sauber, hilft uns aber nicht weiter, wenn wir verstehen wollen, was an der aktuellen Entwicklung neu ist.

Was aber meinen wir, wenn wir heute von „Agentic AI“ oder „KI-Agenten“ sprechen? IBM definiert es so: „Agentic AI refers to artificial intelligence systems designed to autonomously perform tasks, make decisions, and adapt to new information with minimal human intervention“ [IBM 2025]. McKinsey beschreibt es ähnlich: „Agentic AI systems can accomplish complex goals with minimal human input by breaking down a task, creating a plan for achieving it, executing each step in that plan, and adapting based on real-time feedback“ [McKinsey 2025]. Die aktuelle Diskussion meint also etwas Spezifischeres als Russell und Norvig: Systeme, die auf Large Language Models basieren und die Fähigkeit haben, autonom zu planen, Werkzeuge zu nutzen und komplexe Aufgaben ohne ständige menschliche Anleitung zu verfolgen.

Die klassische Unterscheidung zwischen reaktiven und kognitiven Agenten hilft hier. Ein reaktives System reagiert auf Eingaben mit vorprogrammierten Antworten – wie ELIZA oder ein Chatbot mit festgelegten Dialogflüssen, der nach dem Schema „Wenn Kunde sagt X, dann antworte Y“ funktioniert. Ein kognitiver Agent hingegen kann selbsttätig Ziele

setzen, Pläne entwickeln und diese Pläne an veränderte Umstände anpassen. Wenn der erste Weg nicht funktioniert, probiert er einen anderen – ohne dass dieser Alternativweg je programmiert wurde.

Moderne LLM-basierte Agenten kombinieren mehrere Komponenten die in Abbildung 1 gezeigt werden.

Die **Planungskomponente** zerlegt komplexe Aufgaben in Teilschritte. Wenn Sie einem Agenten sagen „Buche mir einen Flug nach Wien und ein Hotel in der Nähe der Staatsoper", muss er verstehen, dass dies mehrere Aktionen erfordert: Flugsuche, Hotelsuche, Verfügbarkeitsprüfung, Buchung. Das sogenannte ReAct-Architekturmuster (Reasoning and Acting) wechselt dabei zwischen Nachdenken und Handeln – der Agent überlegt, was der nächste Schritt sein sollte, führt ihn aus, beobachtet das Ergebnis und plant dann weiter. Wer je eine komplexe Projektplanung gemacht hat, erkennt das Muster: Man zerlegt das große Ziel in handhabbare Pakete und passt den Plan an, wenn die Realität sich als komplizierter erweist als gedacht.

Das **Gedächtnis** ermöglicht es dem Agenten, Kontext über längere Interaktionen hinweg zu bewahren. Kurzfristiges Gedächtnis speichert den aktuellen Gesprächsverlauf – was haben wir gerade diskutiert, welche Informationen wurden bereits ausgetauscht. Langfristiges Gedächtnis, oft über RAG (Retrieval Augmented Generation) implementiert [Keller 2026A], kann Informationen aus früheren Sitzungen oder externen Wissensbasen abrufen. Der Agent „weiß" dann, dass Sie letztes Mal in Wien im Hotel Sacher übernachtet haben und vielleicht eine Alternative suchen.

Die **Werkzeugnutzung** – in der Fachsprache Tool Calling genannt – erlaubt dem Agenten, externe Systeme anzusprechen: Datenbanken abzufragen, APIs aufzurufen, Dokumente zu lesen und zu schreiben, im Internet zu suchen. Ohne diese Fähigkeit wäre ein LLM auf sein Trainingswissen beschränkt, das mit einem bestimmten Stichtag endet und keine unternehmensspezifischen Informationen enthält. Mit Tool Calling kann der Agent aktuelle Flugpreise abrufen, Ihren Kalender prüfen und tatsächlich eine Buchung vornehmen.

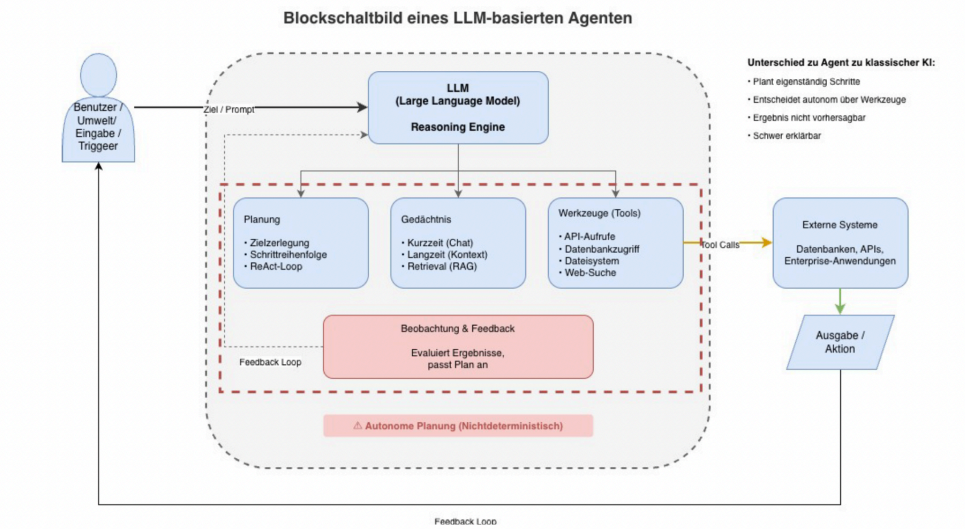

Abbildung 2. Blockschaltbild eines LLM-basierten Agenten

Das entscheidende Unterscheidungsmerkmal zu früherer KI ist die autonome Planung. Ein klassisches Expertensystem folgt vordefinierten Regeln – wenn A und B, dann C. Ein überwachtes Machine-Learning-Modell klassifiziert Eingaben nach gelernten Mustern – dieses Bild zeigt wahrscheinlich eine Katze. Ein LLM-Agent hingegen kann Wege finden, die nie explizit programmiert wurden. Wenn der direkte Weg blockiert ist, probiert er einen Umweg. Er kann improvisieren.

Das klingt großartig – und ist es auch, für viele Anwendungsfälle. Aber es bringt zwei fundamentale Eigenschaften mit sich, die in bestimmten Kontexten zum Problem werden.

Nichtdeterminismus: Derselbe Prompt kann unterschiedliche Antworten erzeugen. Mehr noch: Derselbe Agent mit demselben Ziel kann unterschiedliche Pläne entwickeln und unterschiedliche Aktionen ausführen. Das ist kein Bug, das ist ein Feature – es ermöglicht Flexibilität und Kreativität. Aber es bedeutet auch: Man kann nicht vorhersagen, was der Agent tun wird. Für einen Softwareentwickler, der gewohnt ist, dass derselbe Input immer denselben Output produziert, ist das ein Paradigmenwechsel. Für Compliance Prüfungen kann es ein Show Stopper sein.

Mangelnde Erklärbarkeit: Warum hat der Agent diese Entscheidung getroffen und nicht eine andere? Bei einem neuronalen Netz mit Milliarden Parametern lässt sich das nicht rekonstruieren. Man kann das Ergebnis sehen, aber nicht den Grund. Das macht Debugging schwierig – wenn etwas schiefgeht, weiß man nicht, an welcher Schraube man drehen soll – und Compliance nahezu unmöglich, wie wir gleich sehen werden.

Diese beiden Eigenschaften führen direkt zur Kernfrage dieses Artikels: In welchen Umfeldern ist autonome Planung ein Vorteil – und in welchen wird sie zum Risiko?

Direktoren unerwünscht

Warum Autonomie und Nichtdeterminismus in regulierten Umfeldern ein Problem darstellen können

Stellen Sie sich folgenden Schadenfall bei einer Versicherung vor: Ein Sturm beschädigt das Dach eines Einfamilienhauses. Der Versicherungsnehmer meldet den Schaden über ein Online-Formular mit Fotos. Was passiert danach? In einer hypothetischen „reinen Agentic AI"-Welt sähe das so aus:

- Ein KI-Agent nimmt die Meldung entgegen,
- analysiert die Fotos,
- schätzt die Schadenshöhe,
- prüft die Deckung im Vertrag,
- stellt bei Bedarf Rückfragen und fordert zusätzliche Dokumente an,
- entscheidet am Ende über die Regulierung,
- weist die Zahlung an.

Vollständig autonom, ohne menschliche Eingriffe, und in Minuten statt Tagen erledigt. Das klingt verlockend – schneller, billiger, keine Wartezeiten für den Kunden. Aber lassen Sie uns durchspielen, was dabei schiefgehen kann.

Eskalierende Halluzinationen: LLMs halluzinieren – sie generieren Aussagen, die plausibel klingen, aber faktisch falsch sind. Ich habe das ausführlich in meinem Artikel über Halluzinationen beschrieben [Rippling 2025]. Bei einem Chat mit einem LLM ist das ärgerlich, man merkt den Fehler und korrigiert ihn. Bei einem autonomen Agenten, der auf seine eigenen Ausgaben aufbaut, kann es katastrophal werden. Der Agent schätzt die Schadenshöhe auf 15.000 Euro – basierend auf einer Halluzination über aktuelle Handwerkerpreise in der Region, die das LLM aus seinem Trainingswissen „erinnert", das aber zwei Jahre alt ist. Diese falsche Zahl wird zur Grundlage seiner nächsten Entscheidung. Er genehmigt die Zahlung ohne menschliche Prüfung, weil sie unter dem Schwellenwert liegt. Der Fehler manifestiert sich in der realen Welt als echte Zahlung auf ein echtes Bankkonto.

Die Rippling-Sicherheitsanalyse nennt dieses Phänomen treffend „Cascading Hallucination Attacks" [Rippling 2025]: Eine Halluzination in Schritt eins triggert

eine automatisierte Aktion in Schritt zwei, und so weiter – eine Kettenreaktion fehlerhafter Daten durch das gesamte System. Das ist kein theoretisches Szenario, sondern ein dokumentiertes Risiko bei Multi-Step-Agenten.

Fehlende Nachvollziehbarkeit: Die BaFin, EIOPA und andere Regulatoren verlangen, dass Entscheidungen nachvollziehbar dokumentiert werden. Wenn ein Kunde sich beschwert oder ein Prüfer fragt: Warum wurde dieser Schaden so und nicht anders reguliert? Bei einem regelbasierten System kann ich das beantworten: „Weil Paragraph 12 Absatz 3 unserer Versicherungsbedingungen diese Berechnungsmethode vorschreibt, und die Eingabewerte waren X, Y und Z." Bei einem LLM-Agenten lautet die ehrliche Antwort: „Der Agent hat einen Plan entwickelt und ausgeführt, dessen genaue Logik nicht rekonstruierbar ist." Das ist vor einem Regulator keine akzeptable Antwort.

Die EIOPA hat im August 2025 eine umfassende Opinion zu AI Governance and Risk Management veröffentlicht, die genau diese Punkte adressiert [EIOPA 2025]. Die Kernbotschaft ist unmissverständlich: Versicherungen müssen „human-in-the-loop safeguards" implementieren und sicherstellen, dass Mitarbeiter AI-generierte Outputs verstehen, hinterfragen und überschreiben können. Der EU AI Act, seit 2024 in Kraft, klassifiziert KI-Systeme zur Risikobewertung und Preisgestaltung in Lebens- und Krankenversicherungen als „High Risk" – mit entsprechend strengen Anforderungen an Dokumentation, Transparenz und menschliche Aufsicht [Debevoise 2025].

Mangelnde Eingriffsmöglichkeiten: Wenn ein Agent autonom arbeitet, dann arbeitet er autonom – das ist tautologisch, aber die Konsequenz wird oft übersehen. Wenn der Agent einen falschen Weg einschlägt, wie stoppen Sie ihn? Bei einem Multi-Step-Plan ist der erste Schritt vielleicht schon ausgeführt, bevor jemand bemerkt, dass etwas schiefläuft. E-Mails sind verschickt, Buchungen vorgenommen, Zahlungen angewiesen. Der Rückruf einer bereits versendeten E-Mail ist peinlich, die Stornierung einer Buchung kostet Gebühren, aber eine falsche Schadenzahlung zurückzufordern ist ein rechtlicher Albtraum.

Technische Risiken: Dazu kommen technische Risiken wie zirkuläre Aufrufe und unkontrollierter Ressourcenverbrauch. In Multi-Agenten-Systemen können Agenten andere Agenten aufrufen – das ist gewollt, um komplexe Aufgaben zu bewältigen. Aber was passiert, wenn Agent A eine Aufgabe an Agent B delegiert, der sie an Agent C weitergibt, der wiederum Agent A um Hilfe bittet? Oder wenn ein Agent in eine Schleife gerät, weil er immer wieder dieselbe Aktion versucht, die immer wieder fehlschlägt? Das ist kein theoretisches Problem, sondern passiert in der Praxis, und die Kosten für Cloud-basierte LLM-API-Aufrufe können dabei schnell eskalieren. Ein paar hundert Euro für einen einzelnen Schadenfall, der außer Kontrolle gerät, mögen noch verschmerzbar sein, aber bei tausenden Fällen pro Tag summiert sich das.

Haftung: Wer haftet eigentlich, wenn ein autonomer Agent eine Fehlentscheidung trifft? Das Unternehmen, das ihn einsetzt? Der Anbieter des LLMs? Der Entwickler des Agenten-Frameworks? Die EIOPA-Opinion macht hier eine klare Ansage: Versicherungsunternehmen bleiben verantwortlich für die eingesetzten Systeme, auch wenn diese von Dritten entwickelt wurden [DLA Piper 2025]. Sie können die Haftung nicht auslagern, indem Sie sagen „das hat der Agent entschieden“. Die Entscheidung, den Agenten einzusetzen, war Ihre.

Wie Schadenprozesse heute schon funktionieren

Mit KI, aber ohne Agentic AI

Man braucht keine autonomen Agenten, um KI erfolgreich in der Schadenbearbeitung einzusetzen. Die Versicherungsbranche macht das seit Jahren – mit klassischen, deterministischen KI-Methoden unter einem wohl definierten Geschäftsprozess, der menschliche Kontrolle an den entscheidenden Stellen vorsieht.

Schauen wir uns an, welche KI-Elemente man auch ohne Agentic AI heute schon in einem Schadenprozess vorfinden kann.

- **Bildanalyse**: Der Kunde reicht seine Schadenmeldung mit Fotos und einer Beschreibung ein. Ein Computer-Vision-Modell – trainiert auf zehntausenden historischen Schadenfotos – klassifiziert automatisch die Art des Schadens. Ist das ein Sturmschaden am Dach, ein Wasserschaden im Keller, ein Brandschaden? Das System trifft diese Einordnung mit hoher Zuverlässigkeit, weil es genau diese eine Aufgabe tausendfach trainiert hat.

- **Textanalyse**: Parallel extrahiert ein NLP-Modell strukturierte Informationen aus der Freitextbeschreibung – Datum des Schadens, betroffene Räume, bereits ergriffene Maßnahmen.
- **Deckungsprüfung**: Im nächsten Schritt prüft ein regelbasiertes System anhand der Vertragsdaten, ob der gemeldete Schadenfall grundsätzlich gedeckt ist. Hier gibt es keine Interpretation, nur klare Wenn-Dann-Regeln, die direkt aus den Versicherungsbedingungen abgeleitet sind. Ist der Vertrag aktiv? Ist diese Schadenart eingeschlossen? Wurde die Selbstbeteiligung berücksichtigt? Diese Prüfung ist deterministisch, nachvollziehbar und auditierbar – genau das, was der Regulator sehen möchte. Oft geschieht das ganz klassisch im Rahmen eines sog. Produktservers.
- **Schadenhöhe schätzen**: Ein Machine-Learning-Modell, trainiert auf historischen Schadendaten, liefert dann eine erste Schätzung der Schadenshöhe. Wichtig: Diese Schätzung ist ein Input für den menschlichen Sachbearbeiter, keine finale Entscheidung. Das System sagt: „Basierend auf ähnlichen Fällen liegt der erwartete Regulierungsbetrag bei 8.500 bis 12.000 Euro." Der Sachbearbeiter kann diese Einschätzung übernehmen, anpassen oder verwerfen.
- **Betrugserkennung**: Im Hintergrund prüft ein Anomalie-Detection-System, ob Muster vorliegen, die auf Versicherungsbetrug hindeuten. Hat dieser Kunde auffällig viele Schäden gemeldet? Passen die Fotos zum beschriebenen Schaden? Stimmen die Metadaten der Bilder mit dem angegebenen Zeitpunkt überein? Auch dieses System ist keine autonome Entscheidungsinstanz, sondern ein Hinweisgeber: Es flaggt verdächtige Fälle, die dann von spezialisierten Ermittlern geprüft werden.

Am Ende steht ein Mensch, der alle Eingaben prüft, die finale Entscheidung trifft und die Begründung dokumentiert. Bei Routinefällen unter einem definierten Schwellenwert – sagen wir 2.000 Euro bei klarer Deckung und unauffälligem Fraud-Score – kann auch hier automatisiert werden, aber nach festen Regeln, nicht nach autonomer Planung. Die Zahlung wickelt ein klassisches ERP-System ab: deterministisch, nachvollziehbar, auditierbar, langweilig.

In diesem Prozess arbeiten zahlreiche KI-Komponenten – Bilderkennung, NLP, ML-Modelle, Anomalieerkennung – aber keine davon plant autonom. Jedes System hat eine klar definierte Aufgabe, produziert einen spezifischen Output und übergibt an den nächsten Schritt. Der Mensch bleibt in der Kontrollschleife für alle kritischen Entscheidungen. Das ist nicht so aufregend wie ein vollautonomer Agent, aber es funktioniert, es ist compliant, und es lässt sich vor einem Prüfer verteidigen.

Was die Regulatorik wirklich sagt

Die regulatorischen Rahmenbedingungen favorisieren genau diesen Ansatz. Die EIOPA-Opinion vom August 2025 macht unmissverständlich klar: Versicherungsunternehmen tragen die volle Verantwortung für eingesetzte KI-Systeme, auch wenn diese von Dritten entwickelt wurden [EIOPA 2025]. Es reicht nicht, einen Agenten einzukaufen und zu hoffen, dass er schon das Richtige tun wird. Die Opinion fordert klare Rollen und Verantwortlichkeiten, einen „client-centric approach" mit ethischer Unternehmenskultur, Mitarbeiterschulung und verständlichen Ergebnissen.

Der EU AI Act, seit 2024 in Kraft, klassifiziert KI-Systeme zur Risikobewertung und Preisgestaltung in Lebens- und Krankenversicherungen als „High Risk" – mit entsprechend strengen Anforderungen an Dokumentation, Transparenz und menschliche Aufsicht [Debevoise 2025]. Das bedeutet nicht, dass man keine KI einsetzen darf, aber es bedeutet, dass man dokumentieren muss, was sie tut, warum sie es tut, und dass ein Mensch die finale Kontrolle behält.

Die Botschaft der Regulatoren ist klar: Nutzt KI, aber wisst, was sie tut. Dokumentiert, warum. Und stellt sicher, dass Menschen die letzte Entscheidung treffen. All das spricht nicht gegen KI – es spricht gegen unkontrollierte Autonomie.

Director of Marketing

Wo man AI Agents eher einsetzen kann

Nach all den Warnungen könnte der Eindruck entstehen, Agentic AI sei grundsätzlich problematisch. Das wäre ein Missverständnis. Es gibt zahlreiche Anwendungsfelder, in denen die Vorteile autonomer KI-Agenten die Risiken bei weitem überwiegen – nämlich überall dort, wo Fehler tolerierbar, Konsequenzen reversibel und regulatorische Anforderungen gering sind. Oder anders gesagt: überall dort, wo man sich einen „Direktor" leisten kann, der auch mal daneben liegt.

Marketing

Der Marketing-Bereich ist geradezu prädestiniert für Agentic AI. Hier geht es um Kreativität, Personalisierung in großem Maßstab und schnelle Iteration – alles Stärken von LLM-basierten Agenten. Ein Marketing-Agent kann Zielgruppen analysieren, personalisierte E-Mail-Kampagnen entwickeln, A/B-Tests durchführen und basierend auf den Ergebnissen die nächste Kampagnenwelle optimieren. Wenn dabei mal eine E-Mail nicht perfekt formuliert ist oder eine Kampagne weniger gut performt als erwartet – das ist kein Compliance-Verstoß,

sondern normaler Geschäftsbetrieb. Niemand wird vor Gericht gezerrt, weil ein Newsletter eine unglückliche Betreffzeile hatte.

Unternehmen wie Salesforce mit ihrem Agentforce-Produkt oder spezialisierte Anbieter wie Warmly und Regie.ai setzen bereits erfolgreich KI-Agenten in der Lead-Generierung ein. Die Ergebnisse, die in Fallstudien berichtet werden, sind beeindruckend: Conversion-Raten, die das Siebenfache manueller Outreach-Kampagnen erreichen, und Kosteneinsparungen von bis zu 70 Prozent gegenüber menschlichen SDRs (Sales Development Representatives). Ob diese Zahlen universell replizierbar sind, sei dahingestellt – aber selbst bei deutlich konservativeren Annahmen rechnen sich solche Investitionen schnell.

Software Entwicklung – aber mit großer Vorsicht

Ein weiteres Feld, in dem Agentic AI bereits produktiv eingesetzt wird, ist die Software-Entwicklung. Die Coding-Agenten der aktuellen Generation – Cursor, Windsurf, GitHub Copilot, um nur die bekanntesten zu nennen – sind technisch gesehen bereits Agentic AI. Sie analysieren Anforderungen, generieren Code, führen Tests aus und iterieren basierend auf Fehlermeldungen. Der Agent schreibt nicht nur eine Funktion, sondern versucht sie zu kompilieren, sieht den Fehler, korrigiert ihn und probiert erneut. Ohne darauf jetzt tiefer einzugehen: Der Einsatz ist nicht risikolos. Ohne über Fehler zu diskutieren bietet solches Schnellcoding (oder Vibe Coding) die Chance mit Lichtgeschwindigkeit technische Schulden aufzubauen.

Der Agent beschleunigt den Prozess der Codeproduktion und QS, ersetzt aber eine zweite Meinung bei der Qualitätssicherung genau nicht. McKinsey berichtet von Unternehmen, die mit KI-Agenten Legacy-Code (etwa COBOL) modernisieren – eine Aufgabe, die früher Jahre und Millionen kostete, wird nun in Monaten bewältigt [McKinsey 2025]. Die Agenten analysieren den alten Code, verstehen seine Logik und generieren moderne Äquivalente, die dann von menschlichen Entwicklern geprüft werden. Es gibt jedoch genug Fallstricke, die solche Renovierungsmaschinen ausbremsen können (Stichwort: Terminierungsproblem von Turing Maschinen ist nicht berechenbar).

Support kreativer Arbeit

Content-Erstellung und Kreativarbeit sind ein drittes offensichtliches Anwendungsfeld. Blogs, Social-Media-Posts, Produktbeschreibungen, Präsentationen – all das lässt sich mit KI-Agenten effizienter erstellen. So auch dieser Artikel hier. Der Agent recherchiert, entwirft, iteriert basierend auf Feedback und passt Tonalität an die Zielgruppe an. Das Schlimmste, was passieren kann: Ein Text ist nicht perfekt und muss überarbeitet werden. Das ist kein

katastrophaler Fehler, das ist normaler redaktioneller Prozess. Jede Redaktion der Welt arbeitet so – Entwurf, Feedback, Überarbeitung, Publikation.

Auch für interne Recherche und Wissensmanagement eignen sich Agenten hervorragend. Ein Agent, der interne Dokumentation durchsucht, Informationen aus verschiedenen Quellen zusammenfasst und Fragen beantwortet, kann enorme Produktivitätsgewinne bringen. „Wie haben wir das letzte Mal das Problem mit dem Legacy-Interface gelöst?“ – statt stundenlanger Suche in Confluence und SharePoint liefert der Agent in Sekunden eine Zusammenfassung mit Links zu den relevanten Dokumenten. Wenn er dabei gelegentlich ein Dokument übersieht oder eine Zusammenfassung unvollständig ist – der Mitarbeiter kann nachfragen oder selbst recherchieren. Die Konsequenzen sind überschaubar. Man braucht dafür allerdings noch nicht einmal einen Agenten: Es genügt auch ein LLM mit RAG (Retrieval Augmented Generation).

Automatisierung von Routineaufgaben

Termine koordinieren, Reisen buchen, Berichte aus verschiedenen Datenquellen zusammenstellen, Daten von einem Format in ein anderes konvertieren – klassische Büroarbeit, die Zeit frisst, aber wenig intellektuellen Anspruch hat. Hier können Agenten Menschen entlasten, ohne kritische Risiken zu schaffen. Wenn der Agent einen Termin zehn Minuten zu früh ansetzt, ist das ärgerlich, aber kein Drama.

Das gemeinsame Muster

Was haben all diese „gutartigen“ Anwendungsfälle gemeinsam? Sie operieren in Bereichen, wo Fehler erkennbar und korrigierbar sind, bevor sie zu größerem Schaden führen. Es bestehen keine regulatorischen Anforderungen an die Nachvollziehbarkeit jeder einzelnen Entscheidung. Die Konsequenzen von Fehlentscheidungen sind begrenzt und reversibel – man kann eine E-Mail zurückziehen, einen Blogpost löschen, einen Code-Commit revertieren. Kreativität und Flexibilität sind wichtiger als Determinismus. Und Menschen prüfen die Ergebnisse, bevor sie kritisch werden.

Fazit und Handlungsempfehlung

Die KI-Landschaft ist gigantisch groß. Sie ist viel umfangreicher als der aktuelle Hype um Agentic AI. Von Turings ursprünglicher Frage „Can machines think?“ über die Expertensysteme der 1980er bis zu den LLM-basierten Agenten von heute hat sich viel entwickelt, und viel davon wird eingesetzt und macht als Subsystem einen unauffälligen Job ohne Schlagzeilen.

Unternehmen, die sich nur auf LLM-basierte Agenten konzentrieren, übersehen die bewährten, zuverlässigen KI-Methoden, die seit Jahrzehnten funktionieren und auch weiterhin funktionieren werden.

Agentic AI bringt echte Innovationen: autonome Planung, flexible Problemlösung, kreative Anwendungen, die vor fünf Jahren noch Science Fiction waren. Aber sie bringt auch inhärente Eigenschaften mit, die in regulierten Umfeldern zum Problem werden: Nichtdeterminismus macht Reproduzierbarkeit unmöglich, mangelnde Erklärbarkeit verursacht Compliance-Probleme, Autonomie macht Fehlerkorrektur zum Wettlauf gegen die Zeit.

Die Empfehlung ist daher differenziert. In regulierten Umfeldern (Versicherung, Banking, Gesundheitswesen, öffentliche Verwaltung) sollte Agentic AI mit großer Vorsicht eingesetzt werden, wenn überhaupt. Die klassische Architektur aus deterministischen KI-Komponenten unter einem definierten Geschäftsprozess mit Human-in-the-Loop bleibt ein sicherer Weg [EIOPA 2025]. Nicht weil moderne Technologie grundsätzlich schlecht wäre, sondern weil Regulatoren Nachvollziehbarkeit verlangen und Haftungsrisiken real sind. Ein Sachbearbeiter, der eine vom System vorgeschlagene Entscheidung abnickt, ist etwas fundamental anderes als ein AI Agent, der autonom entscheidet.

In weniger regulierten Bereichen – Marketing, Teile der Software-Entwicklung, Content-Erstellung, interne Produktivität – können Unternehmen die Vorteile von Agentic AI nutzen, ohne unkalkulierbare Risiken einzugehen. Hier überwiegen die Effizienzgewinne die potenziellen Nachteile, und Fehler lassen sich korrigieren, bevor sie existenzbedrohend werden.

Die Kunst liegt darin, für jeden Anwendungsfall die richtige Technologie zu wählen. Nicht jeder Prozess braucht einen autonomen Agenten – manchmal ist die langweilige, deterministische, nachvollziehbare Lösung die bessere. Und manchmal, in Marketing oder Teilen der Softwareentwicklung ist ein Agent genau das Richtige.

Oder um in unserem Bild zu bleiben: In manchen Positionen braucht man keinen Direktor, der eigene Entscheidungen trifft. Manchmal braucht man einfach jemanden, der zuverlässig seine Arbeit macht. Die Kunst liegt darin, zu erkennen, welcher Fall vorliegt.

Literatur

[Britannica 2024]
History of Artificial Intelligence. Encyclopaedia Britannica. Online: https://www.britannica.com/science/history-of-artificial-intelligence

[Debevoise 2025]
Debevoise Data Blog: Europe's Regulatory Approach to AI in the Insurance Industry. Mai 2025. Online: https://www.debevoisedatablog.com/2025/05/21/europes-regulatory-approach-to-ai-in-the-insurance-industry/

[DLA Piper 2025]
DLA Piper: EIOPA publishes opinion on AI governance and risk management. September 2025. Online: https://www.dlapiper.com/en/insights/publications/law-in-tech/2025/eiopa-publishes-opinion-on-ai-governance-and-risk-management

[EIOPA 2025]
European Insurance and Occupational Pensions Authority: Opinion on AI Governance and Risk Management. EIOPA-BoS-25-360, August 2025. Online: https://www.eiopa.europa.eu/document/download/88342342-a17f-4f88-842f-bf62c93012d6_en

[IBM 2025]
IBM Think: What is Agentic AI? Dezember 2025. Online: https://www.ibm.com/think/topics/agentic-ai

[Keller 2026A]
Wolfgang Keller: Wie KI auf Unternehmenswissen zugreift – Retrieval Augmented Generation einfach erklärt. In diesem Buch.

[Keller 2026B]
Wolfgang Keller: EAM als KI-Enabler: Warum Architektur der strategische Navigator für Agentic AI wird. In diesem Buch.

[Keller 2026C]
Wolfgang Keller: Im Land der Lügen: LLMs und Halluzinationen. In diesem Buch.

[McKinsey 2025]
Sukharevsky, A. et al.: Seizing the agentic AI advantage. McKinsey & Company, Juni 2025. Online: https://www.mckinsey.com/capabilities/quantumblack/our-insights/seizing-the-agentic-ai-advantage

[Rippling 2025]
Rippling: Agentic AI Security: A Guide to Threats, Risks & Best Practices 2025. Online: https://www.rippling.com/blog/agentic-ai-security

[Russell/Norvig 2023]
Stuart Russell; Peter Norvig: Künstliche Intelligenz – ein moderner Ansatz, 4. aktualisierte Auflage. Pearson 2023.

[UiPath 2025]
UiPath: What is Agentic AI? Online: https://www.uipath.com/ai/agentic-ai

Die Idee für den Artikel stammt vom menschlichen Autor. Der Artikel ist Teil einer persönlichen Artikelserie über den Einsatz von generativer KI und LLMs in Unternehmen. KI in Gestalt von Claude Opus 4.5 hat bei der Erstellung des Artikels geholfen.

KI und EAM: Die falschen Fragen

Die verlockende Illusion der intelligenten Agenten

Grenzen heutiger KI-Agenten

Context Window: Das Gedächtnisproblem

Halluzinationsrisiko: Das Problem der Plausibilität

Tool Calling: Die Abhängigkeit von sauberen Schnittstellen

Latenz und Kosten: Die ökonomische Realität

Was passiert, wenn etwas schiefgeht?

Reproduzierbarkeit und Nachvollziehbarkeit: Das Compliance-Dilemma

Was muss wirklich aufgeräumt werden?

Dimension 1: KI-Relevanz des Systems

Dimension 2: Datenqualität vs. Datenzugang

Dimension 3: Kritikalität des Use Cases

Die resultierende Priorisierungsmatrix

Die Rolle von EAM: Vom Dokumentar zum Investitionsnavigator

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

KI-Readiness-Assessment als neues EA-Artefakt

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Use-Case-getriebene Investitionsplanung

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Governance für KI-Architekturen

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Kontinuierliche KI-Readiness-Bewertung

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Erfahrung trifft auf Hype: Die aktuelle Diskussion um KI in Unternehmen

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Die dominante Perspektive: KI für EAM

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Legacy-Modernisierung durch KI-Agenten

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Technische Limitationen von LLMs

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Compliance und Erklärbarkeit

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Die resultierende Lücke im Diskurs

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Fazit: Die richtigen Fragen stellen

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Literatur

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Agent-Gateways: Die Rache der SOA im KI-Zeitalter

Der Einstieg: AI-Gateways

Funktionsliste von AI-Gateways

Konsequenz: AI-Gateways sind notwendig, aber nicht hinreichend

Agent-Gateways: Die Urenkel der SOA

Lösung: Agent-Gateways mit MCP, A2A und standardisierten Schnittstellen

Model Context Protocol (MCP): Der Standard für Tool-Anbindung

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Agent2Agent Protocol (A2A): Standard für Agenten-Kollaboration

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Function Calling und REST/gRPC: Die Basis bleibt bestehen

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Compliance und Governance

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Entwicklungsstand von Agent-Gateways – Ein entstehender Markt

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Problem: Unreife Produkte und fragmentierte Lösungen

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Lösung: Evaluation der verfügbaren Produkte

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Industrieller Einsatz: Erste Produktionserfahrungen

Zusammenfassung: Warum man um Agent-Gateways nicht herumkommen wird

Was Agent-Gateways abdecken – und wo Lücken bleiben

Die späte Rache der SOA

Literatur

Im Land der Lügen: LLMs und Halluzinationen

Warum Halluzinationen ein Risiko für Sie und Ihr Unternehmen darstellen

Intro

Halluzinationen und Bullshitting

Bullshit in Boston

Das LLM mit der angeblich geringsten Halluzinationsquote

Geschäftliche Risiken durch Halluzinationen

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Generierte Dokumente

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Agentic AI

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Am Ende des Tages ist es Risikomanagement

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Erkennung und Gegenmaßnahmen

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Persönliche Gegenmaßnahmen

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Skeptisch bleiben bei überzeugend klingenden Aussagen

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Prompt-Techniken

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Websuche aktivieren oder erzwingen

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Konsistenzprüfung durch Mehrfachabfrage

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Chain-of-Thought-Prompts nutzen

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Quellenangaben einfordern und überprüfen

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Nehmen Sie nicht irgendein Modell

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Gegenmaßnahmen der Hersteller

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Retrieval-Augmented Generation (RAG)

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Semantische Entropie und Unsicherheitsschätzung

Token-Level Detection

Guardrails und Output-Filter

Fine-Tuning mit Präferenzoptimierung

Fazit und Ausblick: Implikationen für den Einsatz von LLMs

Vorsicht in regulierten Umfeldern

Autonomie müssen die Modelle sich verdienen

RAG als notwendige, aber nicht hinreichende Bedingung

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Epilog

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Literatur

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Wie KI auf Unternehmenswissen zugreift

Berge von Wissen, aber außer Reichweite für LLMs

Das Problem präzise formuliert

Die Lösung: RAG – von einfach bis komplex

Die einfachste Variante: Manuelle Suche

Etwas fortgeschrittener: Intranet-Suche

Suche mit Vektordatenbanken

Wie füllt man die Vektordatenbank?

Zerlegen von Dokumenten – Chunking

Vektorisierung (Embeddings)

Vektordatenbank

Semantische Suche und Antwortgenerierung

Verbesserungen und Varianten

Die Konsequenzen: Warum RAG die Spielregeln ändert

Kein Training erforderlich

Eigene Dokumente bleiben verwendbar

Vollständige Datenkontrolle

Aktualität ohne Neutraining

Skalierbarkeit und Kosten

Vermeidung von Halluzinationen

Transparenz und Nachvollziehbarkeit

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Fazit: RAG macht KI-gestütztes Wissensmanagement zugänglich

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Literatur

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Es ist ein Model und es sieht gut aus

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Wie IT-Führungskräfte im KI-Projekt zum richtigen Modell kommen

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Warum KI-Modellauswahl keine reine Technikfrage ist

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Warum Benchmarks und Marketing täuschen

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Das Benchmark-Problem

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Es gibt kein „bestes“ Modell

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Ein Modell oder mehrere?

Warum Selbst-Training fast immer falsch ist

Wieder so ein Auswahlprozess

Schritt 1: Strategische Weichenstellungen

Schritt 2: Kosten verstehen

Schritt 3: Anforderungskatalog erstellen

Schritt 4: Shortlist und Proof of Concept

Schritt 5: Entscheidung dokumentieren

Warum Flexibilität wichtiger ist als die perfekte Wahl

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Epilog

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Literatur

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Weiterführende Artikel dieser Serie

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Modellauswahl-Frameworks und Enterprise-Guides

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Benchmark-Kritik und Limitierungen

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

API-Preise und Kostenvergleiche

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Open-Source vs. Proprietäre Modelle

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Hardware-Anforderungen und GPU-Kosten

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

RAG vs. Fine-Tuning

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Allgemeine LLM-Trends und Marktentwicklung 2025

Dieser Inhalt ist in der Leseprobe nicht verfügbar. Das Buch kann bei Leanpub unter https://leanpub.com/agentai gekauft werden.

Hier könnte das Kapitel zu Ihrer Frage stehen

Wie Sie ja schon gewarnt wurden: Dieses Buch ist im Entstehen. Ich lönnte jetzt hier eine Liste möglicher Kapitel anhängen, die ich noch schreiben möchte. Das tue ich bewusst nicht. Ich hoffe, dass ich von Ihnen noch Fragen bekommen werde, aus denen man Artikel machen kann, die dann den Weg in dieses Buch finden und für viele Kollegen hilfreich sein werden.

Dafür habe ich die EMail-Adresse **agentai@objectarchitects.de** eingerichtet.

ToDos und Bugs

ToDos

- eventuell die schönen Bilder aus den LinkedIn Blogs über die Kapitel

Bugs

- sicher viele - Review folgt