# Wildwuchs von KI-Agenten: Warum KI-Governance jetzt ein Thema für den Vorstand ist

**20.8.2026 - Paul Taylor | SAP SE**

**Unternehmen setzen zunehmend agentische KI ein und integrieren autonome KI-Agenten in ihre Geschäftsprozesse. Sie experimentieren mit autonomen KI-Agenten in Frontoffice-Bereichen wie Marketing und Kundenservice sowie in operativen Bereichen wie Sendungsverfolgung, Bedarfsprognose und Lieferkettenoptimierung.**

Agentische KI baut auf dem wirtschaftlichen Potenzial generativer KI auf, das laut McKinsey-Schätzungen jährlich 2,6 bis 4,4 Billionen US-Dollar zur Weltwirtschaft beitragen könnte. Dies stellt die nächste Phase der Einführung von Unternehmens-KI dar: den Übergang von der reinen Inhaltserstellung zur eigenständigen Ausführung und von vereinzelten Pilotprojekten hin zum produktiven Einsatz.

## Unkontrollierte Ausbreitung von KI-Agenten

Dieser Wandel stellt die KI-Governance vor eine neue Herausforderung. Von Agenten-Wildwuchs spricht man, wenn KI-Agenten schneller entwickelt, eingesetzt oder systemübergreifend verknüpft werden, als das Unternehmen in der Lage ist, sie zu erfassen, Verantwortlichkeiten zuzuweisen, Zugriffsrechte zu steuern, ihr Verhalten zu überwachen und sie zu optimieren oder sie stillzulegen, sobald sie ihren Zweck nicht mehr erfüllen.

Eine kürzlich von SAP LeanIX durchgeführte Umfrage zu Agentic AI unterstreicht diesen Wandel, denn sie ergab, dass 98 Prozent der Unternehmen bereits KI-Agenten implementiert haben oder planen dies zu tun. Doch während sich die Einführung immer schneller vollzieht, kommen die Verantwortlichen mit der Umsetzung einer KI-Governance kaum hinterher. Laut demselben Bericht verfügen weniger als die Hälfte der befragten Unternehmen über eine Übersicht, welche KI-Agenten sie eigentlich im Einsatz haben.

Die Mechanismen hinter diesem Agenten-Wildwuchs kennt jedes Technologieunternehmen, das schon einmal eine SaaS-Welle erlebt hat. Einzelne Teams führen Agenten in Eigenregie ein – motiviert durch echte Produktivitätsziele. Jeder KI-Agent ist für eine bestimmte Aufgabe gedacht: ein Marketing-Automation-Agent hier, ein Supply-Chain-Monitoring-Agent dort, ein HR-Onboarding-Bot anderswo. Und alle arbeiten isoliert vor sich hin. Ohne zentrale Plattform oder übergreifendes Governance-Framework entsteht so eine fragmentierte Landschaft von Agenten, in der die einzelnen Tools nicht miteinander kommunizieren, sich nicht einheitlich überprüfen lassen und schneller technische Schulden anhäufen, als sie Mehrwert schaffen.

Laut Gartner wird ein typisches Fortune-500-Unternehmen bis 2028 mehr als 150.000 KI-Agenten im Einsatz haben. Doch nur 13 Prozent der Unternehmen glauben, dass sie über die richtige Governance verfügen, um diese Flut von Agenten zu bewältigen. Max Goss, Senior Director Analyst bei Gartner, warnte sein Publikum auf einer Londoner Konferenz im April: „Während CIOs und IT-Führungskräfte gerade eine wahre Explosion von KI-Agenten in ihren Unternehmen erleben, haben viele mit einem unkontrollierten Wildwuchs zu kämpfen, der ihre Organisationen erheblichen Risiken aussetzt – von Fehlinformationen über übermäßiges Datenteilen bis hin zu Datenverlust.“

Weiter führte er aus: „Viele Unternehmen reagieren darauf, indem sie die Nutzung von KI-Agenten blockieren oder stark einschränken. Aber das ist auf Dauer keine tragfähige Lösung. Wenn Mitarbeitende nicht mit den freigegebenen Tools arbeiten können, werden sie die unternehmenseigenen Kontrollen wahrscheinlich umgehen und auf Schatten-KI ausweichen, was noch deutlich größere Risiken mit sich bringt. Unternehmen müssen die richtige Balance finden: Sie müssen Agenten steuern und den Wildwuchs in den Griff bekommen, gleichzeitig aber ihre Mitarbeitenden in die Lage versetzen, sicher mit diesen Tools an Innovationen zu arbeiten."

Agenten benötigen in der Regel umfassende, systemübergreifende Berechtigungen, um funktionieren zu können, doch diese Berechtigungen werden selten mit der gleichen Sorgfalt verwaltet wie bei menschlichen Nutzern. Das Risiko durch nicht verwaltete oder unkontrollierte KI-Agenten im Unternehmen ist daher real und nimmt stetig zu.

## Sicherheitsbedenken bei KI-Agenten

Aus der Unternehmenspraxis sind mittlerweile Fälle bekannt, in denen KI-Agenten vertrauliche Informationen offenlegten oder ihre vorgesehenen Grenzen überschritten – etwa durch vorsätzliche Anweisungen, die dazu führten, dass Agenten Sicherheitsvorkehrungen umgingen, Produktivdaten löschten oder irreversible Finanztransaktionen auslösten.

Gerade diese Sicherheitsrisiken bereiten führenden Technologieunternehmen großes Kopfzerbrechen. Bei Chatbots und früheren Formen generativer KI beschränkten sich Sicherheitsprobleme meist auf fehlerhafte Ausgaben: eine ungenaue oder unpassende Antwort, die sich in der Regel nachträglich korrigieren ließ. Im Zeitalter der KI-Agenten hingegen können die Folgen von Fehlverhalten oder Sicherheitsvorfällen deutlich schwerwiegender sein – schließlich führen Agenten eigenständig Aktionen aus, nutzen Tools, greifen auf Systeme zu und stoßen Geschäftsprozesse an.

Deshalb ist die Steuerung von Agenten längst keine reine IT-Angelegenheit mehr. Sie berührt zunehmend Themen, die auf Vorstandsebene angesiedelt sind: Risikomanagement, regulatorische Risiken, Datenschutz, Nachvollziehbarkeit, operative Widerstandsfähigkeit und Rechenschaftspflicht für autonome Entscheidungen.

## Die neue KI-Governance-Plattform

Führende Unternehmen denken um: Sie sehen die Steuerung von KI-Agenten nicht mehr als lästige Pflichtaufgabe, sondern als entscheidenden Erfolgsfaktor. Denn davon hängt ab, ob ihre KI-Investitionen sich auszahlen oder zum Problem werden. Infolgedessen ist effektive AI-Agent-Governance schnell zu einem Vorstandsthema geworden und trägt zur Entstehung einer neuen Plattformkategorie bei: KI-Governance-Plattform.

Diese Kategorie befindet sich noch in der Entstehung, aber ihr Zweck wird immer klarer. Unternehmen müssen ihre Agenten im Griff haben: Sie müssen wissen, welche Agenten existieren, was diese tun, welche Zugriffsrechte sie haben, ob sie regelkonform arbeiten und wie sie sich im Produktivbetrieb verhalten.

SAP gehört zu den Pionieren im Bereich Agentic AI – einer neuen Technologiekategorie. Und mit der Übernahme von LeanIX im Jahr 2023 hat die SAP ihre Kompetenzen im Bereich Enterprise Architecture Management deutlich ausgebaut. Dies ist schnell zu einem anerkannten Differenzierungsmerkmal für den SAP AI Agent Hub geworden – indem KI-Artefakte wie Agenten, Modelle und MCP-Server innerhalb der gesamten Architektur und im gesamten Geschäftskontext

des Unternehmens positioniert werden.

Auf dieser Basis funktioniert der SAP AI Agent Hub als zentrale Steuerungszentrale. Von hier aus lassen sich alle KI-Agenten und KI-Tools im Unternehmen verwalten und kontrollieren – unabhängig davon, von welchem Anbieter sie stammen oder auf welchen Systemen sie laufen.

Wie SAP-CTO Philipp Herzig auf der diesjährigen SAP Sapphire auf der Bühne erklärte, soll der SAP AI Agent Hub eine Governance-Rolle für alle KI-Agenten im gesamten Unternehmen übernehmen. „Agenten sind überall“, sagte er. „Manche sind gut, manche nicht, und fast niemand hat ein konsistentes Bild – keine zentrale Governance, keine klare Sicht darauf, was die einzelnen Agenten tun, ob sie Mehrwert bringen oder ob sie den eigenen Richtlinien entsprechen.“

Herzig fuhr fort: „Mit SAP AI Agent Hub ändert sich das. Ein zentraler Einstiegspunkt und eine Kommandozentrale, um alle KI-Agenten, LLMs und MCP-Server in Ihrer Landschaft herstellerunabhängig zu ermitteln, zu verwalten und zu steuern. Der [SAP] AI Agent Hub ermöglicht es Ihnen, alle Ihre Agenten im Kontext zu entdecken: Ihre Landschaft, Ihre Geschäftsprozesse. Sobald Sie die richtigen Agenten identifiziert haben, können Sie ihr Risiko kontrollieren und Entscheidungen im Bereich IT-Architektur oder Compliance-Regeln festlegen.“

## Das Zeitfenster wird kleiner

KI-Agenten werden immer schneller in Unternehmen eingeführt. Dadurch bleibt immer weniger Zeit, um rechtzeitig wirksame Kontrollsysteme einzurichten, bevor etwas schiefgeht. Für CIOs, CEOs und Unternehmensvorstände lautet die Frage nicht mehr, ob KI-Agenten gesteuert werden sollen. Sie lautet, ob Governance von Anfang an in die Architektur eingebaut wird oder erst nach dem ersten ernsthaften Versagen nachgerüstet wird. Es geht darum, ob die Governance von Anfang an in die Architektur integriert wird oder ob man nachrüstet, wenn der erste ernsthafte Fehler aufgetreten ist.

Unternehmen, die die Steuerung von KI-Agenten im Jahr 2026 als strategische Priorität betrachten, werden besser in der Lage sein, sich mit KI einen langfristigen Wettbewerbsvorteil zu verschaffen. Wer die Planung jetzt aufschiebt, wird 2027 wahrscheinlich Chaos beseitigen müssen. In der IT gilt: Schnelles Handeln ohne durchdachte Struktur rächt sich früher oder später. Bei KI-Agenten passiert dies aber deutlich schneller und mit größeren Auswirkungen als bei bisherigen Technologien.

https://news.sap.com/germany/2026/08/ki-governance-vorstandsthema