

Qualitätsjournalismus kostet Geld. Mit Ihrem Abo sorgen Sie dafür, dass unsere Berichterstattung unabhängig bleibt.

Copyright © 2025 Versicherungsmonitor. All rights reserved.

Bots sind nicht geheim, aber brauchen klare Regeln

Posted By [Arndt Gossmann](#) On 13. Mai 2025 In [Abo](#), [Allgemein](#), [Digitaler Dienstag](#), [Kommentare](#), [Top News](#) | [No Comments](#) | [Drucken](#)

Digitaler Dienstag KI-Agenten bieten Versicherern erhebliche Effizienzgewinne – sei es in der Dokumentenanalyse, der Schadenbearbeitung oder der Portfolioauswertung. Sie bewegen sich dabei exakt innerhalb der ihnen zugewiesenen Rollen und Rechte, aber keineswegs frei oder unkontrolliert in IT-Systemen. Es muss sichergestellt werden, dass die Integration von KI-Agenten entlang etablierter Compliance- und Sicherheitsrichtlinien stattfindet.



[1]

Arndt Gossmann ist CEO von DGTAL und geschäftsführender Gesellschafter der Gossmann & Cie. Gruppe

© Arndt Gossmann

wie sie in ersten Unternehmen gerade implementiert werden, basieren auf etablierten Identity-Management-Prinzipien: Jede Agenteninstanz ist als sogenannte „Non-Human Identity“ (NHI) eindeutig identifizierbar, dokumentiert und kontrollierbar.

Governance-Prinzipien für KI-Agenten

Das Konzept der NHI ist nicht neu. Technische Identitäten für Maschinen, Dienste oder Bots existieren seit Langem – und sie sind in den IT-Umgebungen der Versicherungen Standard. Für KI-

Im Versicherungsmonitor vom 7. Mai 2025 wurde unter dem Titel „[Die geheime Identität der Bots](#)“^[2] die These aufgestellt, dass KI-Agenten sich weitgehend unkontrolliert durch die IT-Systeme von Versicherern bewegen – im Gegensatz zu menschlichen Mitarbeitenden, deren Rechte eng begrenzt und überwacht seien. Die damit suggerierte Bedrohung ist plakativ, aber technisch verkürzt – und sie droht, die sachliche Debatte über den sinnvollen Einsatz von KI im Versicherungswesen zu verzerren. Höchste Zeit für eine Einordnung.

Zunächst: KI-Agenten sind keine „Black Boxes“ mit Eigenleben. Sie handeln innerhalb eines klar definierten Rahmens („Agentic Workflows“), erhalten gezielte Aufgabenstellungen („Prompts“) und operieren nur mit solchen Systemrechten und Datenzugängen, die ihnen explizit zugewiesen werden.

Moderne Agentenarchitekturen,

Agenten gilt das Gleiche wie für jede heute im Einsatz befindliche regelbasierte Software. Die Governance-Prinzipien umfassen unter anderem:

- eine zentrale Erfassung und regelmäßige Auditierung aller NHIs,
- ein rollenbasiertes Zugriffsmodell (RBAC), das den Grundsatz „Least Privilege“ konsequent umsetzt,
- Lifecycle-Management für die kontrollierte Erstellung, Nutzung und Deaktivierung von Agenten sowie
- umfassendes Logging und Monitoring aller Aktivitäten, eingebunden in sogenannte SIEM-Systeme, mit denen Unternehmen potenzielle Schwachstellen identifizieren und beheben können.

Ein KI-Agent, der auf Daten zugreift, die nicht seinem definierten Profil entsprechen, würde genauso auffällig wie ein menschlicher Nutzer, der beispielsweise ohne Berechtigung versucht, auf Gehaltsdaten zuzugreifen. Die technischen Möglichkeiten zur Kontrolle sind also vorhanden – und sie werden bei professionellem Einsatz von KI-Agenten auch genutzt.

KI-Agenten schaffen Effizienz

Der Einsatz von KI-Agenten bietet Versicherern erhebliche Effizienzgewinne – sei es in der Analyse großer Dokumentenmengen, in der Schadenbearbeitung oder in der Portfolioauswertung. Wichtig ist: Diese Systeme ersetzen keine menschlichen Entscheidungen, sondern liefern strukturierte Zuarbeit, auf deren Basis Menschen fundierte Entscheidungen treffen können. Agenten sind Assistenzsysteme, die autonom definierte Aufgabenstellungen bearbeiten. Aber es sind keine autonomen Akteure.

Ein KI-Agent ist de facto ein (agentischer) Workflow, der aktiv geschaffen, trainiert und entlang bestehender Unternehmensrichtlinien eingebettet wird – genau wie jede andere Form von Software. Zwar sind KI-Agenten deutlich agiler und flexibler als klassische regelbasierte Systeme, aber auch sie erhalten definierte Ressourcen, spezifische Datenzugriffe und technische Rahmenbedingungen. Sie bewegen sich also keineswegs frei oder unkontrolliert in IT-Systemen, sondern exakt innerhalb der ihnen zugewiesenen Rollen und Rechte.

Deshalb ist es irreführend, wenn KI-Agenten als „heimliche Mitarbeiter“ dargestellt werden, die sich an „Richtlinien vorbei in IT-Systeme einnisten“. Sichergestellt werden muss indes, dass die Integration von KI-Agenten entlang etablierter Compliance- und Sicherheitsrichtlinien stattfindet.

Keine Lösung ist es, diese Technologie zu ignorieren oder gar zu vermeiden. Die einzige Sicherheit, die dadurch erlangt würde, ist, mit Sicherheit mittelfristig die Wettbewerbsfähigkeit einzubüßen.

Arndt Gossmann ist CEO von DGTAL und geschäftsführender Gesellschafter der Gossmann & Cie. Gruppe.

Weitere Kolumnen:

- [Agentic Workforce: Die nächste Evolutionsstufe der KI](#) [3]
- [Die ersten KI-Agenten sind einsatzbereit](#) [4]
- [Warum Versicherer KI-Champions werden müssen](#) [5]

Article printed from Versicherungsmonitor: <https://versicherungsmonitor.de>

URL to article: <https://versicherungsmonitor.de/2025/05/13/bots-sind-nicht-geheim-aber-brauchen-klare-regeln/>

URLs in this post:

[1] Image: https://versicherungsmonitor.de/wp-content/uploads/2025/01/arndt_gossmann_neu-scaled.jpg

[2] Die geheime Identität der Bots: <https://versicherungsmonitor.de/2025/05/02/die-geheime-identitaet-der-bots/>

[3] Agentic Workforce: Die nächste Evolutionsstufe der KI: <https://versicherungsmonitor.de/2025/04/15/agentic-workforce-die-naechste-evolutionsstufe-der-ki/>

[4] Die ersten KI-Agenten sind einsatzbereit: <https://versicherungsmonitor.de/2025/03/18/die-ersten-ki-agenten-sind-einsatzbereit/>

[5] Warum Versicherer KI-Champions werden müssen: <https://versicherungsmonitor.de/2025/02/18/warum-versicherer-ki-champions-werden-muessen/>