AI Agents

Mit künstlicher Intelligenz Aufgaben autonom lösen

AI-Agents handeln autonom und verfolgen eigenständig Ziele. Sie automatisieren komplexe Abläufe durch die Nutzung verschiedener Tools. Dabei agieren sie auch in bislang unbekannten Kontexten zuverlässig. Gleichzeitig entstehen Risiken bei Kontrolle, Sicherheit und Haftung.

Definition

Ein AI-Agent ist ein autonomes Softwareprogramm. Er wird von einem Dritten initiiert und verfolgt ein klar definiertes Ziel. Der Agent agiert in einer spezifischen Umgebung, mit der er über Sensoren und Aktoren interagieren kann. Dabei ist er in der Lage, mit Unschärfen und Unsicherheiten umzugehen. Entscheidungen trifft er selbstständig, ohne weiteren menschlichen Eingriff.

Im Zentrum steht die **Intelligence** des AI-Agents. Sie beschreibt die Fähigkeit, Handlungen auf Basis von Informationen auszuwählen. Dafür benötigt der Agent drei Bausteine: **Knowledge** umfasst das gespeicherte Wissen und Erfahrungen, auf die der Agent zurückgreift. Das **Goal** stellt das Ziel dar, das erreicht werden soll. Das **Model** stellt das trainiertes Weltverständnis dar. Dieses Modell ermöglicht es, Situationen einzuordnen und passende Handlungen zu wählen. Zusammen bilden sie die Grundlage für autonome Entscheidungen.

Damit ein AI-Agent aktiv handlen kann, ist er auf Schnittstellen zur Umgebung angewiesen. Sensoren liefern kontinuierlich Daten, die den aktuellen Zustand erfassen. Diese Informationen fließen in den Entscheidungsprozess ein und werden mit dem vorhandenen Wissen und Modell abgeglichen. Die daraus abgeleiteten Handlungen setzt der Agent über Aktoren um. Dadurch beeinflusst er wiederum seine Umgebung. Es entsteht ein geschlossener Kreislauf aus Wahrnehmen, Entscheiden und Handeln. Dieser Kreislauf bestimmt die Funktionsweise des AI-Agents. Je nach Ausprägung kann dieser Kreislauf in einem physischen Agenten, etwa einem Roboter, oder in einem rein virtuellen Agenten umgesetzt sein. Virtuelle Agenten agieren ausschließlich in digitalen Systemen.

Technologie & Fortschritt

- Datenverarbeitung
- verfügbare Rechenleistung
- Open Source Modelle & Frameworks

Gesellschaft & Wirtschaft

- Kostensenkung
- Effizienzsteigerung
- Komplexitätsmanagement

AA

Kontrolle & Transparenz

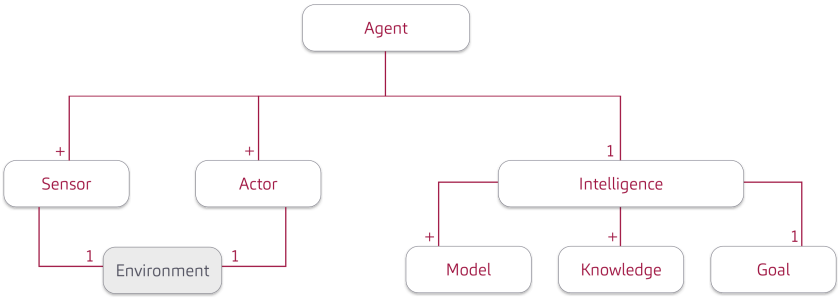
- Unschärfe
- Nachvollziehbarkeit
- Entscheidungshoheit

Politik & Ethik

- Vertrauen
- Verantwortlichkeit
- Recht & Regulatorik

Referenzszenario

AI-Agents entfalten ihr Potenzial überall dort, wo Flexibilität und Autonomie gefragt sind. In komplexen und dynamischen Umgebungen ändern sich die Rahmenbedingungen fortlaufend. Klassische, regelbasierte Systeme stoßen dabei schnell an ihre Grenzen. Sie reagieren nur eingeschränkt auf neue Situationen und benötigen häufig menschliches Eingreifen. AI-Agents übernehmen in solchen Szenarien eigenständig die Wahrnehmung, Entscheidungsfindung und Umsetzung von Handlungen. Dadurch werden Aufgaben auch bei Unsicherheit zuverlässig ausgeführt und Ziele ohne permanente Überwachung erreicht.



Potenzial

Für Unternehmen bieten AI-Agents ein disruptives Potenzial. Sie automatisieren Kundenschnittstellen und gestalten digitale Produkte neu. Dadurch entstehen neue Möglichkeiten in der Wertschöpfung. Auch die Kundenbeziehung verändert sich grundlegend. Unternehmen können AI-Agents in verschiedenen Bereichen einsetzen, von Logistik über interaktive Assistenten bis zur Ablösung klassischer Filialservices. Neue Anbieter haben die Chance, etablierte Marktteilnehmer zu verdrängen. Unternehmen, die auf AI-Agents verzichten, riskieren eine geringere Innovationsgeschwindigkeit und nachhaltige Wettbewerbsnachteile.

Reifegrad

AI-Agents unterscheiden sich von klassischen Software-Agenten durch ihre Fähigkeit, eigenständig zu lernen und komplexe Entscheidungen mithilfe künstlicher Intelligenz zu treffen. Große Sprachmodelle ermöglichen neue Architekturen und Anwendungsfelder für AI-Agents. Erste solche Prototypen entstehen in Forschung und Open-Source-Communities. Auch Unternehmen erproben Pilotprojekte in klar abgegrenzten Szenarien. Gleichzeitig fehlen stabile Standards, belastbare Erfahrungen und breit akzeptierte Good Practices. Viele Ansätze sind experimentell und zeigen Schwächen in Zuverlässigkeit, Steuerbarkeit und Transparenz.

Marktübersicht

Der Markt ist geprägt von schneller Innovation und entwickelt sich mit hoher Dynamik. Eine Konsolidierung oder klare Standards sind bislang nicht absehbar.

Zu den führenden Anbietern zählen Technologiekonzerne wie Google, OpenAI und Anthropic, die eigene Plattformen und Integrationslösungen anbieten. Auch aus der Open-Source-Community werden Libraries und Frameworks wie LangGraph, AutoGen und CrewAI beigetragen. Die Kommunikation und Zusammenarbeit zwischen Agenten wird durch Protokolle gesteuert. Hier ist insbesondere das **Model Context Protocol (MCP)** zu nennen. Neben unterschiedlichen Sprachmodellen kommen auch spezialisierte Ansätze zum Einsatz. Diese decken unterschiedliche Fähigkeiten ab und bilden gemeinsam die Grundlage für agentisches Handeln.

Alternativen

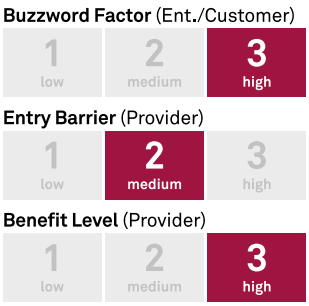
Neben AI-Agents existieren weitere Ansätze, die einzelne Aufgaben automatisieren, aber keine echte Autonomie bieten. In dynamischen und unsicheren Umgebungen können sie die Flexibilität und Zielorientierung von AI-Agents nicht ersetzen.

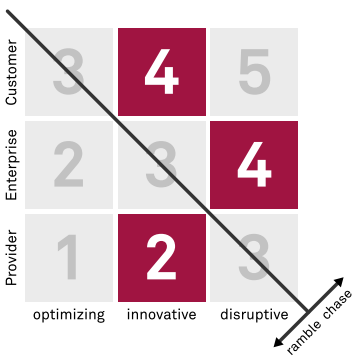
Regelbasierte Systeme arbeiten nach Mustern und eignen sich für klar strukturierte Aufgaben. Jedoch stoßen sie schnell an Grenzen, wenn neue Situationen auftreten. Mit zunehmender Komplexität steigt der Wartungsaufwand der Regeln, und Anpassungen erfordern manuelle Eingriffe.

Expertensysteme beachten zusätzlich eine Wissensbasis, um Entscheidungen in einem abgegrenzten Fachgebiet zu unterstützen. Sie können zwar Empfehlungen ableiten, handeln jedoch nicht eigenständig. Robotic Process Automation hingegen setzt Software-Bots ein, die menschliche Interaktionen mit Anwendungen nachahmen. Sie automatisieren wiederkehrende Tätigkeiten, sind aber auf klar definierte Prozesse beschränkt.

Fazit

- \+ senkt Betriebs- und Arbeitskosten
- \+ vereinfacht komplexe Aufgaben
- \+ trifft eigenständig Entscheidungen
- \- verursacht hohe initiale Kosten
- \- führt zu Kompetenzverlust
- \- erschwert Kontrolle und Steuerung von Entscheidungen





https://msg.direct/techrefresh

Stand: Oktober 2025

msg systems ag

Robert-Bürkle-Straße 1 | 85737 Ismaning/München | Telefon: +49 89 96101-0 | Fax: +49 89 96101-1113 | www.msg.group | info@msg.group