Sichere Identitäten und KI-Agenten in der Industrie

In der Industrie übernehmen KI-Agenten immer häufiger Steuerungsaufgaben. Damit wächst der Bedarf an klaren Verantwortlichkeiten und sicheren Identitäten. Die EU schafft eine Grundlage für vertrauenswürdige Zusammenarbeit zwischen Systemen.

In der Industrieproduktion greifen viele Prozesse eng ineinander. Eine einzelne Maschine arbeitet selten isoliert. Sie ist Teil einer Kette aus Planung, Materialfluss, Fertigung und Qualitätsprüfung. Schon kleine Abweichungen können Auswirkungen auf nachgelagerte Schritte haben. Das erfordert eine präzise Abstimmung aller Beteiligten und eine hohe Transparenz über den aktuellen Zustand der Produktion.

KI-Agenten als handelnder Akteur

Bisher gilt: Sensoren melden Abweichungen, Softwaresysteme reagieren und passen die realen Abläufe an. Neu ist, dass in einigen Industrieunternehmen KI-Agenten diese Vorgänge steuern. Sie analysieren Daten, treffen Entscheidungen und koordinieren Maßnahmen. In vielen Fällen geschieht das ohne direkte Eingriffe durch Mitarbeitende. Damit verändert sich die Aufgabe der Software. Sie wird vom Werkzeug zum handelnden Akteur.

Koordination in Multi-Agenten-Systemen

Der Ablauf der Arbeit von KI-Agenten sieht ungefähr so aus: Ein Fertigungsleitsystem erkennt ungewöhnliche Vibrationen und einen Temperaturanstieg in einer Maschine. Ein spezialisierter KI-Agent übernimmt die Analyse, identifiziert ein defektes Bauteil und erstellt einen Reparaturplan.

Dafür nimmt er Kontakt mit anderen Agenten auf und vergibt Aufgaben an sie. So prüft ein Lieferantenagent die Verfügbarkeit eines Ersatzteils und ein spezialisierter Serviceagent organisiert einen Techniker.

Der gesamte Ablauf erfolgt automatisiert und teilweise ohne Eingriff von Menschen. Sie kommen erst dann zum Zug, wenn die Agenten auf ein unlösbares Problem stoßen oder bei wichtigen Entscheidungen, beispielsweise über Kosten, die bestimmte Vorgaben überschreiten. Kurz: Die hier vorgestellten Multi-Agenten-Systeme verteilen ihre Aufgaben in eigener Regie auf mehrere spezialisierte Agenten, die entsprechend planen, steuern und koordinieren.

Verantwortung und Identität in Netzen

Solche Szenarien sind heute noch nicht vollständig umgesetzt, doch einzelne Bausteine sind bereits im Einsatz. Sie bringen hohe Effizienzgewinne, aber gleichzeitig auch neue Herausforderungen. Entscheidungen werden automatisiert getroffen und über Unternehmensgrenzen hinweg von den Agenten untereinander abgestimmt. Damit stellt sich die grundlegende Frage, wer handelt und wer Verantwortung trägt. Mit zunehmender Verbreitung von KI-Agenten wird diese Frage zentral.

Basis der Antwort sind digitale Identitäten. Sie beschreiben eindeutig, welcher Akteur im Moment in einem System aktiv ist. Eine solche Identität kann einem Menschen, einem Unternehmen, einem Gerät oder einem KI-Agenten zugeordnet sein. Sie enthält kryptografisch gesicherte Informationen über Herkunft, Rolle und Berechtigungen. Dadurch entsteht ein verlässlicher Nachweis für jede Aktion im System.

Digitale Identitäten für industrielle Sicherheit

Identitäten sind in industriellen Umgebungen besonders wichtig. Produktionsprozesse bestehen aus miteinander verknüpften Schritten, bei denen Daten ausgetauscht werden. KI-Agenten greifen in diese Prozesse ein. Ohne verifizierte Identität

Autor:
Dr. Carsten Stöcker
Geschäftsführer
Spherity GmbH
www.spherity.com/de

lassen sich die Aktionen nicht eindeutig zuordnen, Fehler oder Manipulationen sind schwer nachweisbar. Genau an diesem Punkt setzt die europäische Regulierung an.

Die eIDAS-2.0-Verordnung hat das Ziel, eine europaweit einheitliche Infrastruktur für digitale Identitäten zu schaffen. Ihr zentrales Element ist die „European Digital Identity Wallet“, oder kurz die EUDI-Wallet. Sie speichert Identität und Berechtigungen von Privatpersonen auf einem Smartphone oder einem anderen sicheren Gerät. In ihr lassen sich verschiedene digitale Nachweise hinterlegen, etwa Personendaten, Führerschein oder berufliche Qualifikationen.

Europäische Wallets für digitale Nachweise

Ergänzt wird das Konzept durch eine Business Wallet für juristische Personen, also Organisationen, Unternehmen und Behörden. Sie können damit ihre rechtliche Identität, Lizenzen oder Zertifikate verwalten und mit Partnern teilen. Diese Informationen werden wie bei der EUDI-Wallet als verifizierbare digitale Nachweise gespeichert. Sie sind kryptografisch signiert und können somit automatisch geprüft werden.

Laut der EU-Verordnung soll die EUDI-Wallet ab Ende 2026 eingeführt werden. Die Business Wallet wird nach dem aktuellen Stand der Planungen erst ab Ende 2027 eingeführt. Verpflichtend ist der Einsatz anfangs nur für die öffentliche Hand: Alle EU-Behörden müssen sie innerhalb von zwei Jahren anbieten und in ihren Verfahren unterstützen. Für Unternehmen ist die Nutzung zunächst freiwillig, bringt aber bei Behörden den Vorteil einer rascheren Authentifizierung beim Einreichen von Dokumenten.

Delegation von Rechten an KI-Agenten

Diese Infrastruktur lässt sich auf KI-Agenten übertragen. Das Prinzip: Jeder Agent erhält eine eigene digitale Identität, die aber mit der Identität seines Betreibers verbunden ist. Daraus entsteht eine Delegationskette, in der ein Unternehmen oder eine Person einem Agenten ein sogenanntes Mandat erteilt. Dieses Mandat legt fest, welche Aufgaben der Agent ausführen darf und wo seine Grenzen und Verantwortlichkeiten liegen.

In der Praxis bedeutet das beispielsweise, dass ein Beschaffungsagent Waren bis zu einem bestimmten Betrag bestellen darf. Oder ein Wartungsagent kann Reparaturen planen, aber keine sicherheitskritischen Systeme verändern. Solche Regeln werden digital gespeichert und erzeugen einen kontrollierten Handlungsspielraum für autonome Agenten.

Interaktion zwischen autonomen Systemen

Die geschilderten Mechanismen sind auch für die Kommunikation zwischen Agenten wichtig, denn in vielen Prozessen interagieren mehrere Agenten miteinander, etwa von Einkäufern, Lieferanten oder Dienstleistern. Beide Seiten müssen darauf achten, dass der jeweils andere legitim handelt.

Digitale Identitäten ermöglichen die gegenseitige Authentifizierung und machen jede Interaktion überprüfbar.

Im Zahlungsverkehr ist das von entscheidender Bedeutung. Wenn KI-Agenten künftig eigenständige Transaktionen ausführen, entsteht ein zusätzlicher Akteur, der als Stellvertreter eines Kunden auftritt, neben Käufer, Händler und Zahlungsdienstleister. Ohne klare Identitätsnachweise steigt das Betrugsrisiko deutlich. In anderen Branchen, etwa in der Energieversorgung und in industriellen Netzen, ist es ähnlich. Ein kompromittierter Agent kann finanzielle Schäden verursachen und im Extremfall Maschinen und Anlagen schädigen.

Authentifizierte Infrastruktur für Datenökosysteme

In dieser Hinsicht ist das Konzept eines „Authenticated Internet“ von Bedeutung. Dieser digitale Raum ist klar definiert: Alle Akteure müssen sich mit überprüfbaren Identitäten ausweisen. Inhalte und Transaktionen sind signiert und damit nachvollziehbar. So lassen sich anonyme oder gefälschte Aktivitäten leichter erkennen. Der Datenschutz bleibt erhalten, weil nur notwendige Informationen offengelegt werden.

Für Unternehmen eröffnet sich dadurch ein neuer Vertrauensraum, in dem sie Daten sicher austauschen können. Ein Beispiel dafür ist der Aufbau von Plattformen wie Catena-X. Sie sind die Lösung für Unternehmen, die Informationen dezentral und kontrolliert verteilen müssen. KI-Agenten treten in solchen Ökosystemen als Dienste auf, für die Identität und Mandat klar definiert sind.

Vertrauen für die autonome Industrie

In Zukunft werden KI-Agenten eigenständig Verträge schließen, Zahlungen auslösen und Prozesse koordinieren. Diese Form der Automatisierung braucht eine belastbare Vertrauensinfrastruktur. Europa hat dafür eine besondere Ausgangslage. Die Verbindung aus Regulierung, technischer Infrastruktur und industrieller Basis kann ein eigenes Modell für vertrauenswürdige KI schaffen.

Für Unternehmen entsteht daraus ein klarer Handlungsbedarf: KI-Agenten müssen als digitale Stellvertreter verstanden werden. Ihre Rechte, Rollen und Pflichten müssen klar definiert und technisch abgesichert sein. Mit wachsender Automatisierung steigt die Bedeutung digitaler Identitäten.

Trusted Agentic AI

ist dabei ein überlebenswichtiger Wettbewerbsfaktor für die deutsche Industrie im globalen Wettbewerb der KI-Wirtschaft. Das gilt nicht nur für Konzerne, sondern für Unternehmen aller Größen und in sämtlichen Branchen. Wer vertrauenswürdige KI-Agenten sicher einsetzen kann, wird schneller, effizienter und widerstandsfähiger arbeiten. Ohne diese Vertrauensbasis bleibt der Einsatz autonomer Agenten begrenzt. Mit ihr entsteht eine neue Form industrieller Zusammenarbeit über Unternehmensgrenzen hinweg. ◄