in-manas

PRESSEMITTEILUNG

Kill Switch für KI-Agenten: in-manas startet europäisches Sovereign AI OS

Der österreichische Technologieanbieter in-manas veröffentlicht mit dem Sovereign AI OS eine zentrale Betriebs- und Kontrollschicht für KI-Agenten. Sie ermöglicht auch den Betrieb auf kundeneigener Infrastruktur – einschließlich der eingesetzten KI-Modelle und der Datenverarbeitung. Das Angebot richtet sich insbesondere an kritische Infrastrukturen und sensible Unternehmensbereiche. Zu den Partnern von in-manas zählt unter anderem Bosch.

Innsbruck, 15. Oktober 2026 – Der österreichische Technologieanbieter in-manas veröffentlicht heute das Sovereign AI OS. Unternehmen können damit Zugriffsrechte für KI-Agenten festlegen, ihre Aktionen nachvollziehen, Agent Runs über einen „Kill Switch" stoppen und Kosten kontrollieren. Die Lösung ist insbesondere für sensible Anwendungen in der Energieversorgung, im Gesundheitswesen, im öffentlichen Verkehr, in der Logistik, in der technologieintensiven Industrie und im Verteidigungssektor ausgelegt. Das Sovereign AI OS ist bereits bei ausgewählten Leuchtturm-Kunden im Einsatz und steht ab sofort für alle Unternehmen und Institutionen zur Verfügung.

Einzelne KI-Agenten lassen sich schnell entwickeln und erproben. Sobald Unternehmen jedoch viele Agenten parallel im regulären Betrieb einsetzen, wird ihre Steuerung zur Infrastrukturfrage. Mit der Zahl der Agenten steigen Tokenkosten, manuelle Nacharbeit und das Risiko von Fehlfunktionen. Anders als Chatbots greifen Agenten selbstständig auf Daten und Systeme zu und lösen Aktionen aus. Fehler, Fehlkonfigurationen oder manipulierte Eingaben können sich dadurch unmittelbar auf Geschäftsprozesse auswirken. Das Sovereign AI OS schafft die Voraussetzungen dafür, dass Unternehmen KI-Agenten sicher und wirtschaftlich produktiv einsetzen können.

„*Wer KI-Agenten in kritischen Anwendungen ohne klare Zugriffsregeln, Kostenlimits und Kill Switch einsetzt, handelt fahrlässig. Als wir begonnen haben, eigene Agenten zu entwickeln, habe ich direkt gesehen: Sie brauchen klare Grenzen – und die Möglichkeit, jeden Agent Run sofort zu stoppen. Deshalb haben wir mit dem Sovereign AI OS eine Plattform entwickelt, die genau diese Kontrolle ermöglicht*", sagt Stefan Unterthiner, CTO von in-manas.

Das für europäische Unternehmen entwickelte Sovereign AI OS bildet die gemeinsame Betriebsgrundlage für unterschiedliche KI-Anwendungen. Das Sovereign AI OS führt unterschiedliche Agenten und Plattformen in einer gemeinsamen Kontrollstruktur zusammen. So bleiben Zugriffe, Aktionen und Kosten an einer Stelle sichtbar, auch wenn im Unternehmen mehrere Systeme parallel im Einsatz sind. Es ist headless, also unabhängig von einer bestimmten Benutzeroberfläche: Bestehende Werkzeuge und Anwendungen können weiter genutzt werden, während Steuerung und Kontrolle zentral darunterliegen. Unternehmen können zudem eigene Anwendungen und Benutzeroberflächen darauf aufbauen. Die Plattform lässt sich als dedizierte Instanz auf der Infrastruktur des Kunden betreiben – einschließlich lokal betriebener Open-Weight-Modelle – oder in einer souveränen Cloud innerhalb Europas.

Unternehmen steuern Datenzugriffe zentral und können Modelle und Anbieter über die Konfiguration wechseln, ohne jeden Agenten einzeln anzupassen.

Mit dem integrierten Agent Builder können Unternehmen eigene KI-Agenten entwickeln und über einen geregelten Freigabeprozess in den produktiven Betrieb überführen. Während der Ausführung protokolliert das System die Aktionen und Kosten jedes Agent Runs – auch bei Fehlern oder Abbrüchen. Verantwortliche können dadurch nachvollziehen, was ein Agent getan hat, und über den Kill Switch den Agent Run sowie die zugehörigen Modell-, Daten- und Toolzugriffe stoppen. Budgets lassen sich für einzelne Agenten, Abteilungen oder das gesamte Unternehmen festlegen. Werden definierte Grenzen erreicht, warnt das System oder bricht den Agent Run automatisch ab. Die Dokumentation unterstützt zudem interne Prüfungen und regulatorische Nachweise, etwa im Rahmen des EU AI Act. Zusammen mit der zentralen Zugriffssteuerung liefert sie außerdem eine Grundlage für das Cybersicherheits-Risikomanagement nach NIS2.

Wie sich die Kostenkontrolle praktisch auswirkt, zeigt eine bestehende Kundenanwendung beim Healthtech-Unternehmen Biolyz: Dort geben KI-Agenten Leistungssportlern Empfehlungen zu Ernährung, Schlaf und Bewegung. Damit dieser Einsatz wirtschaftlich bleibt, hatte Biolyz eine Kostenobergrenze von zwei Euro pro Agent Run festgelegt. Durch die detaillierte Kostenerfassung und die schrittweise Optimierung der Arbeitsschritte konnte in-manas die Kosten bei einzelnen Agent Runs auf 20 Cent senken – ein Zehntel der vorgegebenen Kostenobergrenze.

in-manas wurde vor zehn Jahren gegründet und entwickelt KI-Lösungen für Unternehmen und Institutionen. Aus der Entwicklung und dem Betrieb eigener KI-Agenten entstand die Erkenntnis, dass Zugriffssteuerung, Nachvollziehbarkeit und Kostenkontrolle wesentliche Voraussetzungen für einen verantwortungsvollen und wirtschaftlich sinnvollen KI-Einsatz sind. Auf dieser Grundlage entwickelte in-manas das Sovereign AI OS. Zu den Kunden des Unternehmens zählen neben Biolyz der Energieversorger EAM, der Verpackungsspezialist Papstar, die Forschungseinrichtung Eurac Research und die Universität Innsbruck. Partnerschaften bestehen unter anderem mit Bosch Software and Digital Solutions und fme.

Hintergrund: KI-Agenten müssen kontrollierbar bleiben

Die Frage, wer KI-Systeme im Ernstfall anhalten kann, ist inzwischen auch in der Politik angekommen. Der EU AI Act sieht für Hochrisiko-KI-Systeme wirksame menschliche Aufsicht vor. Dazu gehört, dass Menschen in den Betrieb eingreifen und das System über eine „Stopp“-Funktion in einen sicheren Zustand bringen können (Art. 14). [1] Bundesdigitalminister Karsten Wildberger forderte im September auf der KI-Konferenz ALL IN in Montréal, dass Menschen KI-Systeme steuern, korrigieren und bei Bedarf stoppen können müssen. [2] In Kalifornien hat Gouverneur Gavin Newsom per Executive Order eine Expertengruppe beauftragt, Empfehlungen vorzulegen, darunter eine mögliche Pflicht zu Notabschaltungen für besonders leistungsfähige Frontier-Modelle. [3]

Für sensible Anwendungen in der Energieversorgung, im Gesundheitswesen oder im öffentlichen Verkehr reicht die Möglichkeit zum Eingreifen allein nicht aus. Ebenso entscheidend ist, wer die Infrastruktur betreibt, wer auf Daten zugreifen kann und welche Abhängigkeiten von Modell- und Cloudanbietern bestehen. Europäische Souveränität bedeutet dabei, auch die KI-Verarbeitung unter eigener Kontrolle auf europäischer Infrastruktur betreiben und die eingesetzten Anbieter wechseln zu können.

In Unternehmen stellt sich die Kontrollfrage auf der Ebene der Anwendung: Welche Aktionen darf ein Agent ausführen, wer kann eingreifen und lässt sich im Nachhinein belegen, was geschehen ist? Hier setzt das Sovereign AI OS an: Verantwortliche können einzelne Agent Runs samt ihren Zugriffen auf Modelle, Daten und Werkzeuge stoppen und die ausgeführten Aktionen nachvollziehen.

Quellen:
[1] Verordnung (EU) 2024/1689 (EU AI Act), Art. 14
[2] Bundesdigitalministerium: Rede von Karsten Wildberger zur ALL IN in Montréal
[3] Governor of California: Executive Order zu KI-Sicherheit und Notabschaltungen

Über in-manas

in-manas ist ein 2016 gegründeter europäischer Technologieanbieter mit Standorten in Innsbruck und Las Palmas. Das Unternehmen entwickelt das Sovereign AI OS, eine zentrale Betriebs- und Kontrollschicht, mit der Unternehmen und Institutionen ihre eigenen KI-Agenten sicher, nachvollziehbar und wirtschaftlich betreiben können. Der Fokus liegt auf kritischen und sensiblen Anwendungen, bei denen Unternehmen die Kontrolle über Daten, Modelle, Zugriffe, Kosten und Risiken behalten müssen. Zu den Partnern zählen Bosch Software and Digital Solutions und fme.
Weitere Informationen unter www.in-manas.com.

Pressekontakt

Unternehmen

Nicolas Müller | in-manas: intelligent management solutions GmbH
Ing.-Etzel-Straße 17 | 6020 Innsbruck | Österreich
media@in-manas.com | in-manas.com

PR-Agentur

Philipp von Roeder | VONROEDER COMMUNICATIONS
Schlegelstr. 4 | 10115 Berlin | Deutschland
inmanas@vonroeder-communications.com | vonroeder-communications.com