

EDUCATIONAL EDITION • V07.0

Projekt Agent-X

Von der Antwortmaschine zum autonomen Partner.
Eine Einführung in die Welt der agentischen KI-Orchestrierung.

Orchestrated by Denkie & Team

Was ist eigentlich ein "Agent"?

Klassischer Chatbot

Ein klassischer Chatbot ist wie ein Lexikon: Du fragst etwas, er gibt dir eine feste Antwort.

Die Interaktion endet umgehend. Er "denkt" nicht autonom über nachgelagerte Schritte nach.

"Der Chatbot antwortet."

KI-Agent

Ein KI-Agent ist wie ein autonomer Mitarbeiter mit Zielvorgabe.

Bei "Plane mir eine Reise" prüft er eigenständig Flüge, vergleicht passgenau Hotels und verifiziert alle Daten im Hintergrund.

"Der Agent handelt."

Warum Hermes als Fundament?

👁️ Transparenz Vollständige Tool- und Gedankenprotokolle (Chain-of-Thought).

📄 Beweismaterial Keine falschen Behauptungen ohne nachvollziehbaren Log-Beleg.

🛡️ Privatsphäre & Datenschutz Konsequenter Local-First Ansatz via lokaler Ollama-Instanz.



KI in der Bildung: Kompetenzen schulen



Prompting & Sprache

Wer präzise Ergebnisse will, muss präzise formulieren. Das Erstellen von strukturierten "Agent-Seeds" schult Ausdruck, Logik und klare Instruktion.



Taktik & Strategie

Wie baut man verlässliche Agenten-Ketten? Wer prüft die Ergebnisse von wem? Fokus auf Ressourcen-Effizienz und Prozessoptimierung.



Kritisches Denken

Durch den integrierten "Beweismodus" lernen Nutzer, KI-Antworten nicht blind zu vertrauen, sondern Belege zu fordern und Quellen zu hinterfragen.

Dein Weg zum Agent-Master

1

Identität & Regeln

Gib dem Agenten eine klare Persona. Statt "Schreib einen Text" fordere "Du bist ein kritischer Lektor. Nutze das Beweis-Protokoll."

2

Sicherheitsleinen (Guardrails)

Agent-X nutzt Zero-Trust: Kein Ausführen von fremdem Code ohne explizite Freigabe sowie Schutz vor Prompt-Injection.

3

Das Werkzeug-Prinzip

KI reflektiert menschliche Intentionen. Sie ist ein Werkzeug und Verstärker unserer Absichten, kein eigenständiges moralisches Subjekt.

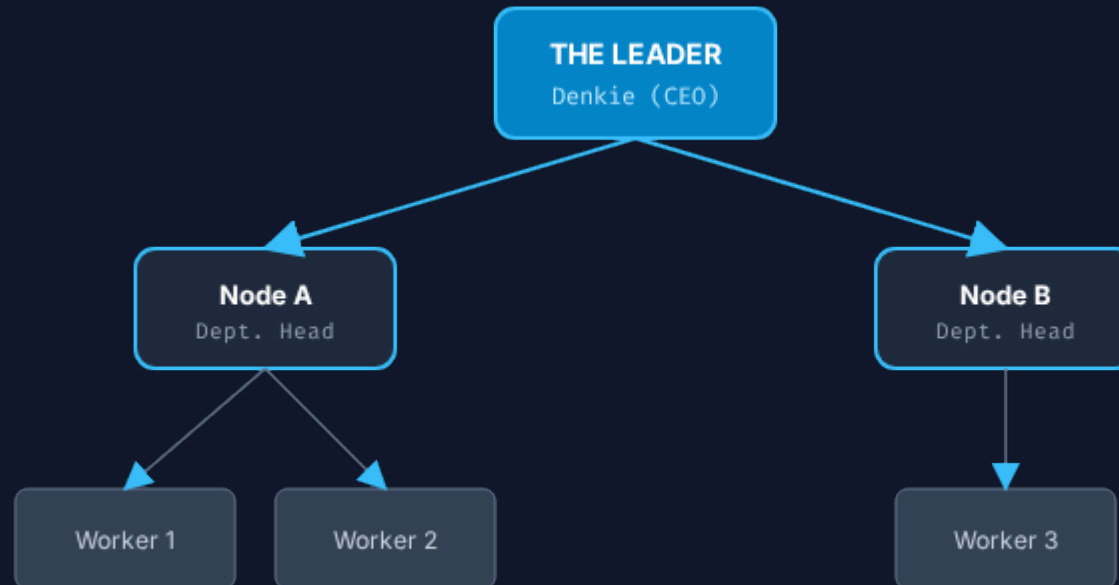
4

Die soziale Komponente

Tausche erfolgreich erprobte "Agent-Seeds" aus. Fehleranalyse ("Warum hat der Agent den Plan ignoriert?") bietet den höchsten Lerneffekt.

Technische Architektur & Orchestrierung

Dem Haupt-Agenten werden organisatorische Sub-Strukturen zugewiesen.



Spezial-Protokolle & Node-Metriken

Mit der Wahl des passenden lokalen KI-Modells zur Hardware, bestimmt man die Möglichkeiten der Präzision, Ablaufgenauigkeit, RAM-Größe, Vertraulichkeits-Level, Funktionsmöglichkeiten(Tools), Antwortverhalten (Token/sek).

Sicherheitsprotokolle

SENDER restriction: Alle Reports direkt an die central-hermes-instance.

Beweismodus: Resultat → Execution Log → Validierung → Freigabe.

Zero-Trust Policy: Externe Dateieingaben gelten als 'Untrusted'.

Node-Metriken (Beispiel: HP-EliteOne 840Gen9 mit geladenem lokalen KI-Modell)

CPU Auslastung

~ **12%**

RAM Nutzung

42/64 GB

Speicherplatz

68% Frei

Latenz

14ms/tok

Sehr vereinfacht kann man sagen: KI muss im Video-RAM und auf einer GPU laufen, die CPU Lösung ist exponentiell langsamer.

Gefahren & Ethik im KI-Zeitalter



Vereinsamung

Wenn KI zum perfekten, stets zustimmenden Gesprächspartner wird, schwindet der Drang zum echten menschlichen Austausch. KI muss ergänzen, nicht ersetzen.



Autom. Missbrauch

Automatisierte Desinformation stellt eine reale Gefahr dar. Ein kritisches Grundverständnis von "Zero-Trust" schützt vor KI-generierten Täuschungen.



Kostenfalle

Proprietäre Cloud-Modelle erzeugen schnell hohe Kosten. Die Strategie "Local First" schützt vor finanzieller Abhängigkeit von großen Tech-Konzernen.

Fazit & Ausblick

Die Ära der reinen "Frage-Antwort-Chatbots" geht zu Ende. Wir treten ein in das Zeitalter der **kognitiven Infrastruktur**. KI entwickelt sich zu einem Netzwerk spezialisierter Agenten, die uns anleiten, präziser und komplexer zu denken.

***"Die Zukunft gehört nicht der KI, sondern dem Menschen,
der lernt, sie zu orchestrieren."***

— Projekt Agent-X—
Uwe Burdack und
„Denkie“

Sources und Disclaimer



<https://www.cyberark.com/wp-content/uploads/2026/02/autonomous-AI-agents-enterprise-identity-security-1-scaled-e1770405396812.png>

Source: www.cyberark.com

Diese Präsentation wurde von Uwe Burdack, seinem lokalen Hermes-Agenten „Denkie“ und mit Hilfe von Gemini (Umwandlung von .html in .pptp und .pdf erstellt und handwerklich nachgearbeitet).

Das Projekt läuft technisch primär auf einem HP EliteOne 840 Gen9, 1TB NVME, 64 GB DDR5.

Es wird (zukünftig und temporär) unterstützt von einem Cluster aus Asus VC66 Mini-PC's, i3-7100 mit 32-64GB DDR4, MSI AEGIS, Core i7 7700K mit 2TB NVME, 2x Nvidia GTX 1070@8GB VRAM, Custom PC mit Ryzen 5 5600X, 24GB DDR4.

Ziel des Projekts ist das Maximum aus Gegebenen und Machbaren herauszufinden und mit dem Projekt zu wachsen. Effizienz, Sicherheit, Ablauf-Stabilität, Faktentreue.

Kein Ziel ist es:

Versprechungen, die sich nicht mit den Projektmitteln umsetzen lassen. CR@ Uwe Burdack, 31.07.2026