

# OPENCLAW AUS ANWENDERSICHT



Einblicke in die offene Hummerzucht. Installation, Security, Use Cases

---

Dirk Murschall

Interim PO & PM | 07.04.2026 | ARIC Brown Bag Session

# MOIN!

## KURZ ZU MIR

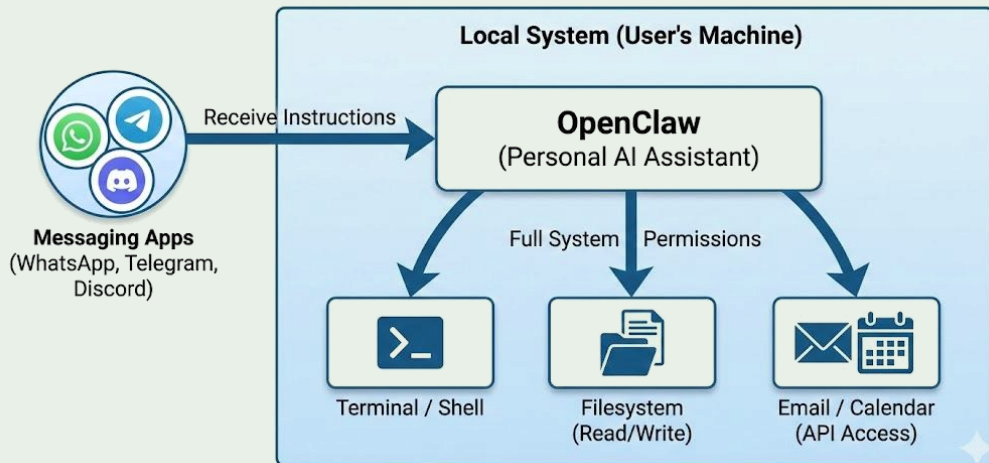


- 
- Dirk Murschall, Hannoveraner, Nürnberger, Hamburger, ungefähr ca. Mitte 40 Jahre alt
  - Seit bald 30 Jahren in der IT tätig
    - Auch (frei!)beruflich als Interim Produkt- bzw. Projektmensch in der Softwareentwicklung
    - Kennt Server-Räume und Chef-Etagen von innen
  - Regelmäßiger Teilnehmer der ARIC Brown Bags
  - **Community-Mensch**, der gerne etwas zurückgibt



# Was ist OpenClaw?

## OpenClaw Local Architecture (Simplified)



- ▶ Es ist ein KI-Agent

OpenClaw kann selbstständig Dinge tun

- ▶ OpenClaw ist eine lokale KI-Architektur

OpenClaw ist ein lokaler KI-Agent-Daemon mit Gateway-Layer für Chat-Integration, Core-Engine für LLM-Verarbeitung und modularem Plugin-System

- ▶ Integriert sich in dein Ökosystem

Du brauchst keine neue App installieren. OpenClaw funktioniert direkt mit WhatsApp, Telegram, Discord, Slack oder Teams – man chattet mit dem Hummer, wie mit jedem anderen Kontakt

# Was kann OPENCLAW?

01

## Proaktiver Mitarbeiter / Kompagnon

Du sagst „überwache meine Mailbox und meinen Kalender und schick mir jeden Morgen ein Tagesbriefing“ und er tut genau das

Prüft Status, sendet Alarme, stellt Zusammenhänge her ohne manuelles Auslösen. Er kann sich von selbst melden

02

## Hat eine Persönlichkeit

Beim Setup erstellt der Hummer eine `soul.md`-Datei

Enthalten sind Name, Vibe, Grenzen...

Die Datei entwickelt sich mit euren Gesprächen. Das ist kein üblicher Chatbot. Ihr lernt euch wirklich kennen

03

## Löst Probleme selbstständig

Du willst, dass er Mails lesen kann?  
Er baut sich selbst einen Mailclient

Braucht er Notion-Zugriff? Er findet die API, bittet dich um Authentifizierung, fertig

Es gibt eine Fehlermeldung? Er kümmert sich selbst um die Lösung, findet Workarounds

# IST DAS NICHT GEFÄHRLICH?



- ▶ Standardmäßig nutzlos

Standardmäßig hat OpenClaw keine Integrationen und keine Rechte und kann nichts.  
Du aktivierst, was du brauchst

- ▶ Es gibt eine Geheimnisverwaltung

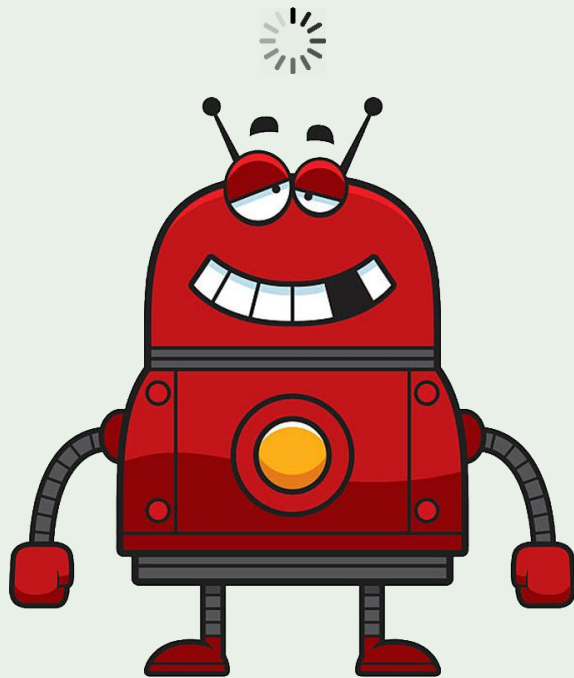
Secrets werden sauber verwaltet – keine hartcodierten API-Schlüssel im Klartext.

- ▶ Es gibt Schutzmaßnahmen

Der Hummer wird nicht *versehentlich* dein System löschen oder Zugangsdaten preisgeben. Er erkennt *gefährliche* Dinge und Situationen und warnt proaktiv

- ▶ Du bist Chef und behältst die Kontrolle

Denk über Konsequenzen nach. Starte vorsichtig, schalte schrittweise frei. Wie bei jedem neuen Kollegen. Vertrauen wächst über die Zeit. Mehr zur Sicherheit im weiteren Verlauf



# Was NICHT GEHT...

---

- ▶ Kann nicht immer die richtige Antwort geben

Der Hummer kann sehr selbstsicher komplett falsch liegen – wie jedes LLM. Halluzinationen passieren. Leitplanken helfen, Iteration hilft, aber erwarte keine Perfektion

- ▶ Kann nicht hellsehen

Wenn du nicht mit dem Hummer kommunizierst, weiß er/sie/es nicht, was du willst. Die besten Ergebnisse entstehen im Dialog. Beginne mit einer Frage und arbeite dich dann gemeinsam weiter vor bis zu deinem gewünschten Ergebnis

- ▶ Kann kaputt gehen oder nicht das Richtige sein

Wie bei jedem Spielzeug und bei jedem neuen Kollegen, kann man es auch übertreiben. Lieber ein Schritt nach dem anderen

# INSTALLATION



- ▶ **Wo installieren?**

  - Laptop (nicht immer online, lokal)

  - Heimserver / Raspberry Pi (immer online, lokal im Heimnetz)

  - VPS z.B. Hetzner, IONOS, etc. (immer online, von überall erreichbar)

- ▶ **Die Installation von OpenClaw ist im Prinzip™ schnell und unkompliziert**

  - Man installiert OpenClaw über den Paketmanager npm:

    - > `npm install -g openclaw@latest`

  - Statt kryptische Config-Dateien von Hand zu schreiben, nutzt man den Onboarding-Assistenten:

    - > `openclaw onboard --install-daemon`

- ▶ **Welcher Messenger?**

  - Prinzipiell egal, aber nimm erstmal Telegram

# ERSTE SCHRITTE

01

## Einrichtung

---

Gib deiner offenen Klaue einen Namen und eine Persönlichkeit.

Meine heißt „Krabbe“, ist ein Hamburger Jung, soll helfen, statt Floskeln zu liefern, darf eine eigene Meinung haben und mir Widersprechen, ist kompetent und respektiert Privatsphäre.

Ja, das ist ein Systemprompt :)

02

## Wirkungsbereich

---

Von nix kommt nix. Du musst deinem Hummer Informationen und Zugriffe geben.

Mehr Rechte bedeuten mehr Macht und mehr Vertrauen in die Technik.

"Ich möchte, dass du meinen Kalender verwaltest. Kannst du mir dabei helfen?"

03

## Aufgaben geben

---

Gib OpenClaw Aufgaben.

„Stell mir jeden Morgen zum Frühstück ein Tagesbriefing zusammen“

„Fasse die Schlagzeilen des Tages zusammen.“

„Bitte bereite mich eine halbe Stunde vor einem Termin auf diesen vor.“

# ERFOLGREICHE ZUSAMMENARBEIT



- ▶ Aufgaben automatisieren, nicht das Denken

Du gibst eine Aufgabe, eine Entscheidung, einen Kontext und der Hummer kümmert sich auf Wunsch regelmäßig

Cronjobs / Tasks werden selbstständig verwaltet

- ▶ Das ist Delegation

- ▶ Je mehr Kontext, desto besser

OpenClaw kann mit vielen Informationen, Quellen und Kontexten gefüttert werden

Der Kontext bleibt erhalten und wächst über die Zeit.  
(Ja, das ist ein Systemprompt und existiert als `memory.md`)

OpenClaw schreibt die Prompts selbst, ihr könnt eingreifen

- ▶ Ihr lernt voneinander!



# SICHERHEIT

---

- ▶ Schadenspotential begrenzen

  - Separater Rechner / VM / VPS

  - Eigenes Benutzerkonto + Rechte einschränken

  - Vorsichtig starten, schrittweise freischalten

- ▶ Nicht exponieren, schon gar nicht im Internet!

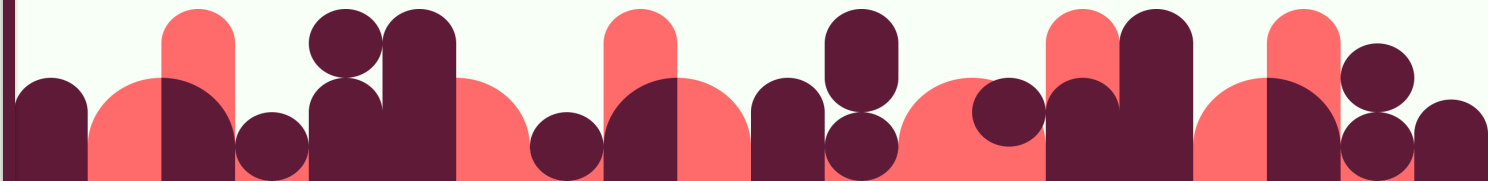
  - Offene Ports = Shodan-Scans = Angriffsziel

  - VPN-Tunnel verwenden (z.B. Tailscale)

- ▶ Absichern, abhärten, updaten

  - > `openclaw security audit`

  - Eingebauter Scanner, der deine Konfiguration automatisch auf Sicherheitslücken durch Fehlkonfiguration prüft



- ▶ **Eure Maschine = Eure Daten**

Daten und Informationen liegen in eurer Hoheit und Verantwortung. Ihr habt komplette Kontrolle

Ominöse Drittanbieter von fremden Kontinenten sind nur involviert, wenn ihr das veranlasst

OpenClaw ist DSGVO-freundlich, ihr seid digital souverän

- ▶ **LLMs und Datenschutz**

OpenClaw sendet Anfragen via API an ein Sprachmodell und bekommt eine Antwort zurück

LLM-Anbieter haben unterschiedliche Richtlinien wie sie mit den API-Daten umgehen, einschließlich der Trainingsverfahren und Aufbewahrungsfristen

Üblicherweise werden API-Anfragen in Bezahlтарifen nicht zum Training verwendet

API-Anfragen werden nach 30 Tagen, 24 Stunden oder sofort wieder gelöscht, je nach Modell

Eine Übersicht gibt es hier: [help.kagi.com/kagi/ai/llms-privacy.html](https://help.kagi.com/kagi/ai/llms-privacy.html)



Johann Sathianathen   
@johann\_sath

X.com

saas is dead

openclaw replaced all my subscriptions

went from \$480/month on tools  
to \$1,245/month on API costs & 15 hours a  
week fixing yaml files

adapt or be left behind

14:58 · 20/02/2026 · **445K** Views

# BLICK IN DIE PRAXIS

---

- ▶ Besseres LLM = bessere Ergebnisse = höhere Kosten

Es fallen Betriebskosten an

Gerade die guten LLMs sind teuer

Ich nutze meist `google/gemini-flash-latest`  
(gut und günstig)

Der Hummer ist nur so klug und schnell wie sein LLM

- ▶ Skills und Fähigkeiten

clawhub.ai ist ein App-Store für das OpenClaw Ökosystem

OpenClaw kann selbstständig Skills installieren, wenn man  
ganz lieb fragt


OpenClaw kann aber auch selbstständig Skills „vibecoden“

# ANWENDUNGSSZENARIEN

---



- ▶ **Prompts mit Cronjob und Kontext**

Moringbriefing, Terminvorbereitungen, DAX-Alarm 

Logfiles überwachen, Google Alerts auf Steroiden

- ▶ **Alles, was sich mit Markdown machen lässt**

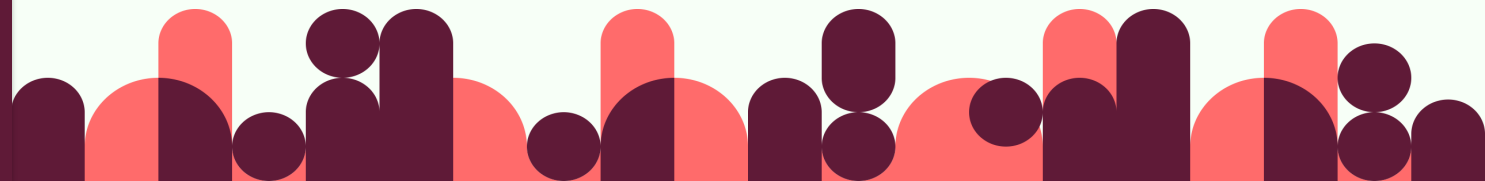
Zugriff auf Second Brains wie Obsidian oder Joplin

Sortieren, verknüpfen, zusammenfassen, erinnern

- ▶ **Bücherwurm**

Lesezugriff auf die Calibre-eBook-Bibliothek

Findet Querverweise zwischen Sachbüchern, vergleicht Konzepte über mehrere Werke hinweg oder fungiert als Bibliothekar



# zusammenfassung



- 01 OpenClaw ist ein KI-Agent. OpenClaw ist Delegation

---

- 02 Vorsichtig starten, schrittweise freischalten

---

- 03 Arbeit und Routinen automatisieren, weiter selbst denken

---

- 04 Sicherheit und Datenschutz sind deine Verantwortung

---

- 05 Iteration einplanen – die erste Version wird nicht perfekt sein

# Danke!

Dirk Murschall | Interim PO & PM

[dirkmurschall.de](http://dirkmurschall.de)

Hamburg | Remote | Deutschlandweit

