

## KNIEPUNKT 027: KI Glücksspiel

Hast Du schon einmal im digitalen Las Vegas übernachtet? Ich rede nicht von Poker-Bots, sondern vom neuesten Glücksspiel: **Clawdbot-Roulette**. Man setzt sich abends hin, füttert den Agenten mit einer vagen Idee und schaut berauscht zu, wie die Code-Zeilen über den Bildschirm tanzen. Es ist wie „Vibecoding“ auf Steroiden. Aber Vorsicht: Wer **Clawdbot** oder **Moltbook** ohne Limit und ohne doppeltes Netz nutzt, erlebt das, was ich den „agentischen Kater“ nenne. Du guckst morgens um fünf auf die Uhr, die Augen brennen, und in deinem Postfach wartet eine Rechnung der API-Provider, für die du dir auch einen gebrauchten Kleinwagen hättest kaufen können. Für viele ist das aktuell ein großartiges, aber verdammt teures Glücksspiel. Setzt Euch deshalb ein Limit, sonst wird das neue Projekt zum finanziellen oder zeitlichen Offenbarungseid.

Aber mal ehrlich: Es ist ein fantastisches Hobby. Wenn Du Dir zuerst eine virtuelle Maschine gebaut und die Prepaid-Kreditkarte gezückt hast, kannst Du Dir Werkzeuge basteln, die wirklich funktionieren. Das ist eine ganz andere Form von digitaler Souveränität. Doch sobald Du planst, die selbst gebauten Agenten auf Deine E-Mails oder Deinen Terminkalender loszulassen, hör bitte kurz auf zu zocken. Die Risiken von **Prompt Injection** und schadhaftem Code sind real – selbst OpenAI und Anthropic warnen vor den Sicherheitslücken in ihren eigenen Coding-Modellen. Bevor Du also Deine Firmengeheimnisse einem Agenten anvertraust, der möglicherweise „shoddy code“ (Schrott-Code) produziert, lass einen Senior-Entwickler drüberschauen. Europa wird nur dann zum KI-Kontinent, wenn wir Agenten bauen, die für uns schuften, ohne dabei all unsere Geheimnisse zu veröffentlichen.

KI wird uns bereichern, wenn wir sie moralisch und vor allem souverän einsetzen. Das bedeutet für Dich: Spiele damit, baue Apps für deinen Eigenbedarf, werde zum Agentenflüsterer! Es ist ein cooles Hobby, das dir einen Blick in die Zukunft erlaubt. Aber bleib am Ball und lass Dich nicht vom Hype blenden. Die Gefahr, dass Zero-Day-Exploits durch KI-generierten Code massiv billiger und häufiger werden, ist keine Panikmache, sondern ein handfestes Sicherheitsrisiko. Bevor Du Deinen Agenten zum „C-Level“ beförderst oder ihn in Deine Infrastruktur integrierst, such Dir Expertenhilfe. Wir brauchen spezialisierte Agenten und keine gehypten Allzweckwaffen, die am Ende mehr Löcher in unsere Sicherheit reißen als Probleme lösen. Wer ein neues und sehr produktives Hobby sucht, sollte sich eine Prepaid-Kreditkarte besorgen, eine virtuelle Maschine erstellen und sich ein Zeitlimit setzen, denn agentisches Coden kann süchtig machen.

---

## Zum Weiterlesen (Plaintext Quellen)

**AI - Almost Intelligent Podcast:** Aktuelle Folgen zu Clawdbot, Moltbook und der Architektur von Agenten. <https://open.spotify.com/episode/4GGZTyPaoDOx21vOYTYX6X?si=84708de200c148a5>

**Fortune:** OpenAI and Anthropic warn of unprecedented cybersecurity risks in coding models. <https://fortune.com/2026/02/05/openai-gpt-5-3-codex-warns-unprecedented-cybersecurity-risks/>

**The Register:** Cursor shows AI agents capable of shoddy code at scale – Ein Realitätscheck für automatisierte Browser-Entwicklung. [https://www.theregister.com/2026/01/22/cursor\\_ai\\_wrote\\_a\\_browser/](https://www.theregister.com/2026/01/22/cursor_ai_wrote_a_browser/)

**Forschung & Lehre:** Fachleute bewerten KI-Risiken – Warum Zero-Day-Exploits durch KI-Agenten zum Massenphänomen werden könnten.

<https://www.forschung-und-lehre.de/forschung/fachleute-bewerten-ki-risiken-6910>

**The Decoder:** Benchmark zeigt – KI-Modelle halluzinieren weiterhin massiv, entgegen der Versprechen von Nvidia. <https://the-decoder.de/benchmark-zeigt-ki-modelle-halluzinieren-weiterhin-massiv/>

Und der Post:

KNIEPUNKT 027: KI Glücksspiel – Vom Code-Casino zum Katerfrühstück

Stell dir vor, du guckst um 5 Uhr morgens auf die Uhr, die Augen brennen und in deinem Postfach wartet eine vierstellige Rechnung für KI-Credits: Der agentische Kater und das für eine App, die zwar „Vibes“ hat, aber keine Funktion. Willkommen in der Welt von Clawdbot und Moltbook.

In meinem neuesten Kniepunkt blicke ich hinter die Kulissen des aktuellen Agenten-Hypes:

Glücksspiel für Fortgeschrittene: Warum der Einsatz von High-End-KI-Agenten ohne Limit aktuell eher an Las Vegas als an Software-Engineering erinnert.

**Realität statt Lederjacken-Versprechen:** Vergiss das Versprechen der fehlerfreien Super-KI. Die echte Gefahr für deine Infrastruktur sind **Prompt Injection** und schadhafte Softwarekomponenten

Vom Hobby zum Profi-Tool: Warum virtuelle Maschinen und Prepaid-Karten dein neues Hobby sein können, du aber trotzdem keinen Agenten an deinen Terminkalender lassen solltest, ohne vorher einen Experten zu fragen.

KI wird uns bereichern, aber nur, wenn wir nicht ungefiltert jedes Heilsversprechen schlucken. Lass uns das Chaos mit einer Prise Ironie und echter digitaler Souveränität angehen.

Den ganzen Text (und wie du den agentischen Kater vermeidest) liest du im Artikel.

#KI #KünstlicheIntelligenz #AgenticAI #Souveränität #Kniepunkt