



TreScout

TECHNIK-TAGESBERICHT

Die Technik-Trends von heute

6. Juli 2026 (Montag)

IN WENIGEN SCHLUCKEN

Die heutige Tagesordnung konzentriert sich auf die Schwachstellen von Systemeingabeaufforderungen und -integrationen, die Fähigkeiten zu großen Sprachmodellen hinzufügen. Aktuelle Repositories auf GitHub zeigen, dass Entwickler dazu neigen, KI-Agenten anzupassen und bestehende Systeme gegen äußere Eingriffe zu testen.

31 HERVORGEHOBEN · ~7 MIN. LESEZEIT

21 GitHub Trending

5 Hacker News

5 HuggingFace · Modelle des Tages

01 Zackriya-Solutions/meetily

Meetily ist ein datenschutzorientierter Besprechungsassistent, der Besprechungsaufzeichnungen lokal verarbeitet und keine Cloud-Verbindung erfordert. Das mit der Rust-Sprache entwickelte Tool kombiniert Sprecher-Tagebücher und durch künstliche Intelligenz unterstützte Zusammenfassungsfunktionen mit Hochgeschwindigkeits-Live-Transkriptionsfunktionen.

Rust · ★ 17.898 · +1.409 heute <https://github.com/Zackriya-Solutions/meetily>

02 openai/codex-plugin-cc

Codex-plugin-cc, entwickelt von OpenAI, automatisiert Codeüberprüfungs- und Aufgabendelegierungsprozesse über die Claude Code-Schnittstelle. Mit diesem Plugin können Entwickler die Funktionen von Codex-Modellen direkt in ihrem Softwareentwicklungsprozess nutzen.

JavaScript · ★ 25.842 · +1.532 heute <https://github.com/openai/codex-plugin-cc>

03 asgeirtj/system_prompts_leaks

Systemvorgaben beliebter Modelle der künstlichen Intelligenz werden von Entwicklern und Forschern zusammengestellt und in einem zentralen Datensatz gesammelt. Diese Arbeit ermöglicht die Analyse der versteckten Anweisungen, die das Verhalten großer Sprachmodelle wie Claude, GPT, Gemini und Grok steuern.

JavaScript · ★ 50.488 · +981 heute https://github.com/asgeirtj/system_prompts_leaks

04 Leonxlnx/taste-skill

Taste-Skill ist ein Tool, das entwickelt wurde, um die Qualität der von Modellen der künstlichen Intelligenz erstellten Inhalte zu verbessern und Standardantworten zu verhindern. Diese JavaScript-basierte Bibliothek soll es Modellen ermöglichen, originellere und qualifiziertere Ausgaben zu erzeugen.

JavaScript · ★ 58.065 · +863 heute <https://github.com/Leonxlnx/taste-skill>

05 alirezarezvani/claude-skills

Diese für Claude Code und ähnliche Coding-Agenten entwickelte Bibliothek bietet mehr als 330 Skills, über 70 Spezialbefehle und mehr als 30 Agentenkonfigurationen. Es bietet eine breite Palette an Plugins und Skripten zur Automatisierung von Arbeitsabläufen in Softwareentwicklung, Marketing und betrieblichen Prozessen.

Python · ★ 20.814 · +392 heute <https://github.com/alirezarezvani/claude-skills>

06 rommapp/romm

Romm ist ein selbst gehosteter Spielearchiv-Manager, der es Benutzern ermöglicht, ihre Spielbibliotheken zu organisieren und direkt über den Browser zu spielen. Dieses in Python entwickelte Tool bietet eine visuell orientierte Oberfläche zur Verwaltung digitaler Spielesammlungen.

Python · ★ 10.679 · +410 heute <https://github.com/rommapp/romm>

07 **ogulcancelik/herdr**

Herdr wurde mit der Rust-Sprache entwickelt und fungiert als Agent-Multiplexer, der auf dem Terminal ausgeführt wird. Es ermöglicht Benutzern die gleichzeitige Interaktion mit mehreren Agenten der künstlichen Intelligenz über die Befehlszeile.

Rust · ★ 12.354 · +651 heute <https://github.com/ogulcancelik/herdr>

08 **alibaba/page-agent**

Der von Alibaba entwickelte Page-Agent ist ein In-Page-Agent für grafische Benutzeroberflächen, der die Verwaltung von Webschnittstellen mit Befehlen in natürlicher Sprache ermöglicht. Dieses in TypeScript geschriebene Tool bietet einen browserbasierten Steuerungsmechanismus zur Automatisierung interaktiver Aufgaben im Web.

TypeScript · ★ 24.266 · +805 heute <https://github.com/alibaba/page-agent>

09 **harvard-edge/cs249r_book**

In dieser von der Harvard University veröffentlichten Ressource werden die Architektur von maschinellen Lernsystemen und Optimierungsprozesse auf Hardware erörtert. Der Inhalt konzentriert sich auf die Interaktion zwischen Software und Hardware und bietet einen technischen Leitfaden für die Erstellung skalierbarer Infrastrukturen für künstliche Intelligenz.

Python · ★ 26.981 · +329 heute https://github.com/harvard-edge/cs249r_book

10 **usestrix/strix**

Strix ist ein Open-Source-Penetrationstest-Tool mit künstlicher Intelligenz, das darauf ausgelegt ist, Sicherheitslücken in Anwendungen zu erkennen und zu beheben. Diese mit der Python-Sprache entwickelte Plattform vereinfacht Schwachstellenmanagementprozesse durch Automatisierung der Softwaresicherheit.

Python · ★ 37.503 · +1.114 heute <https://github.com/usestrix/strix>

11 **hesreallyhim/awesome-claude-code**

Diese für Claude Code, den von Anthropic entwickelten Codierungsassistenten, erstellte Auswahl vereint Tools, Plug-Ins und Kompetenzpakete, die Softwareentwicklungsprozesse beschleunigen. Ressourcen, die es Entwicklern erleichtern, dieses Tool der künstlichen Intelligenz in ihre Projekte zu integrieren, konzentrieren sich auf die Erhöhung der Automatisierungskapazität.

Python · ★ 48.592 · +148 heute <https://github.com/hesreallyhim/awesome-claude-code>

12 **coreyhaines31/marketingskills**

Die für Claude Code und Agenten der künstlichen Intelligenz entwickelte Marketingkompetenzbibliothek bietet spezielle Fähigkeiten in Bereichen wie Conversion-Rate-Optimierung (CRO), Texterstellung, Suchmaschinenoptimierung (SEO), Analyse und Wachstumstechnik. Dieses Toolset ermöglicht es KI-Modellen, marketingorientierte Aufgaben professioneller und datengesteuerter auszuführen.

JavaScript · ★ 36.679 · +145 heute <https://github.com/coreyhaines31/marketingskills>

13 JuliusBrussee/caveman

Caveman ist ein auf Claude Code verwendetes Funktionspaket, das die Sprachstruktur vereinfacht und die Token-Nutzung um 65 Prozent reduziert. Dieses Tool zielt darauf ab, die Kosteneffizienz zu steigern, indem es künstliche Intelligenzmodelle in die Lage versetzt, mit weniger Daten zu verarbeiten.

JavaScript · ★ 85.237 · +1.052 heute <https://github.com/JuliusBrussee/caveman>

14 CoplayDev/unity-mcp

Unity MCP ermöglicht die Automatisierung von Aufgaben wie Asset-Management, Szenensteuerung und Codebearbeitung, indem es eine Brücke zwischen Assistenten für künstliche Intelligenz und dem Unity-Editor schlägt. Dieses Tool ermöglicht es großen Sprachmodellen (LLMs), direkt in Spieleentwicklungsprozesse einzugreifen.

C# · ★ 12.081 · +414 heute <https://github.com/CoplayDev/unity-mcp>

15 facebook/astrix

Astrix wurde von Meta entwickelt und bietet ein Designsystem, das vollständig anpassbar und für die Zusammenarbeit mit KI-Agenten konzipiert ist. Ziel dieses TypeScript-basierten Open-Source-Projekts ist es, Schnittstellenkomponenten für den Einsatz autonomer Systeme geeignet zu machen.

TypeScript · ★ 6.144 · +522 heute <https://github.com/facebook/astrix>

16 immich-app/immich

Immich bietet eine leistungsstarke Foto- und Videoverwaltungslösung, die auf persönlichen Servern gehostet werden kann. Diese mit der TypeScript-Sprache entwickelte Plattform bietet eine zentrale Struktur zum Organisieren und Sichern von Mediendateien.

TypeScript · ★ 106.308 · +470 heute <https://github.com/immich-app/immich>

17 ruvnet/RuView

RuView führt Echtzeit-Raumerfassung, Vitalzeichenverfolgung und Anwesenheitserkennung ohne Bilddaten unter Verwendung standardmäßiger drahtloser Netzwerksignale (WiFi) durch. Diese in Rust entwickelte Software bietet eine Überwachungsinfrastruktur, die die visuelle Privatsphäre schützt, indem sie Radiowellen in der Umgebung analysiert.

Rust · ★ 76.868 · +161 heute <https://github.com/ruvnet/RuView>

18 gastownhall/gastown

Gas Town bietet eine Infrastruktur, die es verschiedenen Agenten der künstlichen Intelligenz ermöglicht, als Multi-Agent-Workspace-Manager zusammenzuarbeiten. Dieses mit der Go-Sprache entwickelte Tool zentralisiert die Koordination zwischen Agenten und das Ressourcenmanagement in komplexen Arbeitsabläufen.

Go · ★ 16.488 · +51 heute <https://github.com/gastownhall/gastown>

19 **dotnet/skills**

Dotnet/skills wurde von Microsoft entwickelt und bietet vorgefertigte Kompetenzpakete (Skills), die es Programmieragenten für künstliche Intelligenz ermöglichen, effektiver in .NET- und C#-Projekten zu arbeiten. Ziel dieser Bibliothek ist es, standardisierte Funktionen für Agenten bereitzustellen, die Softwareentwicklungsprozesse automatisieren.

C# · ★ 4.128 · +246 heute <https://github.com/dotnet/skills>

20 **steipete/CodexBar**

CodexBar ist ein Tool, das die Anzeige von OpenAI Codex- und Claude Code-Nutzungsdaten ermöglicht, ohne dass eine Anmeldung erforderlich ist. Diese mit der Swift-Sprache entwickelte Anwendung erleichtert Entwicklern die Verfolgung von Verbrauchsstatistiken in KI-gestützten Codierungstools.

Swift · ★ 16.432 · +153 heute <https://github.com/steipete/CodexBar>

21 **anthropics/claude-code**

Claude Code ist ein agentenbasiertes Codierungstool, das auf dem Terminal läuft und Routineaufgaben, komplexe Codekommentare und Versionskontroll-Workflows (Git) verwaltet, indem es die Codebasis mit Befehlen in natürlicher Sprache analysiert. Mit dem Ziel, Softwareentwicklungsprozesse zu beschleunigen, ermöglicht dieses Tool Entwicklern die Automatisierung von Codierungsaufgaben, ohne die Terminalumgebung zu verlassen.

Python · ★ 136.429 · +156 heute <https://github.com/anthropics/claude-code>

01 Organic Maps

Organic Maps ist eine Open-Source-Kartenanwendung, die auf Offline-Kartendaten basiert und den Datenschutz der Benutzer in den Vordergrund stellt. Die Anwendung nutzt OpenStreetMap-Daten und bietet Navigations- und lokale Suchfunktionen, ohne dass eine Internetverbindung erforderlich ist.

940 Punkte · 282 Kommentare <https://organicmaps.app/>

02 OpenPrinter

OpenPrinter ist ein Open-Source-Druckprotokoll, das ein treiberunabhängiges Druckerlebnis für verschiedene Druckermodelle bietet. Es bietet eine universelle Schnittstelle, die direkt mit Druckern im Netzwerk kommuniziert, ohne dass herkömmliche Treiberinstallationen erforderlich sind.

795 Punkte · 192 Kommentare <https://www.opentools.studio/>

03 It's not about physical vs. digital games, it's about ownership

Diskussionen in der digitalen Spielewelt konzentrieren sich eher auf das Konzept des Eigentums der Benutzer als auf die Unterscheidung zwischen physischen und digitalen Formaten. Die Befugnis von Plattformen, den Zugang zu Spielen einzuschränken, eröffnet eine neue rechtliche Debatte über die Dauerhaftigkeit digitaler Inhalte und Verbraucherrechte.

449 Punkte · 339 Kommentare <https://popcar.bearblog.dev/its-about-ownership/>

04 The future of Flipper Zero development

Die Entwickler von Flipper Zero wollen Community-Beiträge erleichtern, indem sie das Software-Ökosystem des Geräts in eine modulare Architektur umwandeln. Dieser neue Ansatz sieht einen Übergang zu einem anwendungsbasierten Vertriebsmodell vor, um die Firmware-Entwicklung nachhaltiger zu gestalten.

307 Punkte · 125 Kommentare <https://blog.flipper.net/future-of-flipper-zero-development/>

05 GPT-5.6 Sol Ultra will be in Codex

Es wurde angekündigt, dass das GPT-5.6 Sol Ultra-Modell in Codex, einem Codierungstool, integriert wird. Diese Entwicklung ermöglicht die Aktualisierung von durch künstliche Intelligenz unterstützten Code-Vervollständigungsfunktionen, die in Softwareentwicklungsprozessen verwendet werden.

249 Punkte · 177 Kommentare <https://twitter.com/thssottiaux/status/2073933490513752151>

01 empero-ai/Qwythos-9B-Claude-Mythos-5-1M-GGUF

Qwythos-9B ist ein multimodales Modell der künstlichen Intelligenz, das durch die Verarbeitung von Bild- und Textdaten eine Textausgabe erzeugt. Dieses im GGUF-Format bereitgestellte Modell bietet eine Bild-zu-Text-Funktion, die für die Ausführung auf lokalen Geräten optimiert ist.

♥ 1.583 · 1.533.844 Downloads <https://huggingface.co/empero-ai/Qwythos-9B-Claude-Mythos-5-1M-GGUF>

02 zai-org/GLM-5.2

GLM-5.2, entwickelt von Zai-org, ist ein Sprachmodell, das für Textgenerierungsaufgaben optimiert ist. Dieses Modell, das auf der HuggingFace-Plattform eine hohe Interaktion erhält, wird in umfangreichen Texterstellungsprozessen verwendet.

♥ 3.479 · 220.379 Downloads <https://huggingface.co/zai-org/GLM-5.2>

03 baidu/Unlimited-OCR

Unlimited-OCR wurde von Baidu entwickelt und ist ein Bild-zu-Text-Modell, das durch die Verarbeitung bildbasierter Texte eine Textausgabe erzeugt. Das Modell dient dazu, Daten in komplexen Dokumenten in ein digitales Format umzuwandeln.

♥ 1.763 · 1.044.217 Downloads <https://huggingface.co/baidu/Unlimited-OCR>

04 deepreinforce-ai/Ornith-1.0-35B-GGUF

Ornith-1.0-35B, entwickelt von DeepReinforce-AI, ist ein Sprachmodell, das sich auf die Textgenerierung konzentriert. Das Modell wird mit dem Quantisierungsformat GGUF präsentiert, das eine hohe Speichereffizienz bietet.

♥ 742 · 394.164 Downloads <https://huggingface.co/deepreinforce-ai/Ornith-1.0-35B-GGUF>

05 InternScience/Agents-A1

Agents-A1, entwickelt von InternScience, ist ein Modell der künstlichen Intelligenz, das für Textgenerierungsaufgaben optimiert ist. Dieses Modell ist für die Unterstützung komplexer Logikausführungen und agentenbasierter Arbeitsabläufe konzipiert.

♥ 311 · 7.010 Downloads <https://huggingface.co/InternScience/Agents-A1>

speaker diarization

Technologie, die die Gespräche in der Audioaufzeichnung in Abschnitte unterteilt, indem sie unterscheidet, wer spricht.

live transcription

Gesprochene Stimme wird sofort in Text umgewandelt und auf dem Bildschirm angezeigt.

code review

Softwareentwickler untersuchen und prüfen gegenseitig die Codes auf Fehler.

task delegation

Delegieren der Verantwortung für die Erledigung einer Aufgabe an eine andere Person oder ein anderes System.

system prompts

Erste Anweisungen, die festlegen, wie sich die KI verhalten und welche Regeln sie befolgen soll.

large language models

Mit riesigen Datenmengen trainierte Modelle der künstlichen Intelligenz, die menschliche Sprache verstehen und Texte produzieren können.

output

Die Ausgabe, die ein Computerprogramm oder Gerät als Ergebnis des Vorgangs liefert.

skills

Die Fähigkeiten, über die eine Software oder künstliche Intelligenz verfügt, um eine bestimmte Aufgabe auszuführen.

plugin

Kleine Softwareteile, die später installiert werden, um zusätzliche Funktionen zum Hauptprogramm bereitzustellen.

script

Eine kurze Befehlsfolge, die an einen Computer geschrieben wird, um eine bestimmte Aufgabe automatisch auszuführen.

self-hosted

Anstatt einen Dienst von außen zu mieten, hosten und verwalten Sie ihn auf Ihrem eigenen Server.

agent multiplexer

Ein System, das mehrere Tools der künstlichen Intelligenz gleichzeitig verwaltet und die Arbeit unter ihnen aufteilt.

graphical user interface

Schnittstelle, die Ihnen die visuelle Verwaltung des Computers über Menüs, Symbole und Fenster ermöglicht.

machine learning systems

Computerstrukturen, die durch die Untersuchung von Daten selbstständig lernen und mit der Zeit bessere Entscheidungen treffen.

penetration testing

Cyber-Sicherheitsexperten versuchen, in ein System einzudringen und Schwachstellen zu finden.

CRO

Studien, die durchgeführt werden, um die Zahl der Besucher einer Website zu erhöhen, die zu Kunden werden.

TreScout · trescout.com · Jeden Tag, zu Ihrer Zeit.