

KI-4-Everyone • Daily News

3. Oktober 2026



SAFE

Apple schränkt Mac-Festplattenzugriff wegen KI-Agenten ein

Apple reagiert auf wachsende Risiken durch KI-Agenten: Künftig muss jede App extra erlaubt werden, bevor sie alle Dateien auf dem Mac lesen darf.

SAFE

OpenAI-Sicherheitsmitarbeiter kündigt und kritisiert Unternehmenskultur

David Robinson schrieb bei OpenAI die Sicherheitsberichte zu neuen KI-Modellen. Nach seinem Abgang nennt er die Unternehmenskultur öffentlich "kaputt".

Apple zieht die Reissleine: Mac-Vollzugriff wird kuenftig gegen KI-Agenten abgeschirmt

Weil autonome KI-Programme auf dem Rechner immer mehr Rechte verlangen, baut Apple eine neue Huerde vor den sensibelsten Mac-Bereich.

Apple reagiert auf eine Entwicklung, die vor einem Jahr noch kaum jemand auf dem Zettel hatte: KI-Agenten, also Programme, die eigenstaendig Aufgaben auf dem Computer ihres Nutzers erledigen, verlangen Zugriff auf immer mehr. Weil dieser Zugriff im Zweifel das gesamte Dateisystem umfasst, zieht Apple nun eine neue Linie. Wer kuenftig auf einem Mac die hoechste Zugriffsstufe freigeben will, soll das nur noch nach einer ausdruecklichen, bewussten Freigabe tun koennen.

Konkret geht es um die Berechtigung 'Full Disk Access' auf macOS, also die Erlaubnis, dass eine App auf saemtliche Dateien eines Nutzerkontos zugreifen darf. Apple kuendigte laut Berichten von The Verge, Heise und Golem an, hier zusaetzliche Kontrollen einzubauen. Der Konzern verweist nach Darstellung von The Verge selbst darauf, dass KI-Agenten das Risiko dieser Zugriffsstufe 'substanziell' erhoehen. Kuenftig soll der Nutzer, bevor eine App alle Dateien einsehen kann, dies ausdruecklich erlauben muessen, so die Zusammenfassung von Heise. Golem verweist zusaetzlich darauf, dass Apple die Verschaeferung mit wachsenden Risiken durch KI-Agenten begruendet.

Der Schritt ist deshalb bemerkenswert, weil er den Alltag einer neuen Softwaregattung betrifft. KI-Agenten (Programme, die auf Basis eines Sprachmodells selbststaendig Klicks ausfuehren, Dateien lesen oder E-Mails schreiben) sind in den vergangenen Monaten von vielen Herstellern angekuendigt worden. Damit so ein Agent wirklich hilfreich ist, braucht er oft weitreichenden Zugriff auf lokale Daten. Genau dort liegt aber auch die Gefahr: Ein

Agent, der sich vertut oder manipuliert wird, kann im Zweifel alles sehen, was ein Mensch am Rechner sehen koennte. Apple schiebt diesem Automatismus nun einen zusaetzlichen Riegel vor und zwingt Entwickler wie Nutzer, bewusst zu entscheiden, wem sie diesen Rundumblick geben. Fuer Anbieter von Agenten-Software bedeutet das mehr Reibung - fuer sicherheitsbewusste Nutzer eher eine Beruhigung.

Was im vorliegenden Material offen bleibt: Mit welcher macOS-Version die Verschaeferung genau ausgerollt wird, wie der neue Freigabe-Dialog im Detail aussieht und ob bestehende Apps ihre bereits erteilten Rechte behalten oder neu bestaetigen muessen, ist in den drei Quellen nicht praezise beschrieben. Auch ob andere sensible Berechtigungen - etwa Bildschirmaufzeichnung oder Zugriff auf Mikrofon und Kamera - in gleicher Weise verschaeft werden, geht aus dem Material nicht hervor. Unklar bleibt zudem, ob Apple damit vor allem auf Agenten von Drittanbietern zielt oder auch eigene KI-Funktionen gemeint sind. The Verge verweist darauf, dass die Nachricht urspruenglich von TechCrunch berichtet wurde; weitere Details waeren dort moeglicherweise zu finden, sind hier aber nicht belegt.

In den kommenden Tagen lohnt der Blick darauf, ob Apple konkrete Entwicklerdokumente nachreicht und wie Anbieter von KI-Agenten reagieren. Spannend wird auch, ob Microsoft und Google fuer Windows und ChromeOS aehnliche Schutzmechanismen ankuendigen - denn das Grundproblem, dass ein autonomer Helfer im Zweifel zu viel darf, ist nicht auf Apples Plattform beschraenkt.

MARKT

KI-Infrastruktur: Billionen-Investitionen, magere Renditen

PwC rechnet damit, dass globale KI-Infrastrukturinvestitionen bis 2050 auf 31,6 Billionen Dollar steigen könnten. Der Ausbau läuft schneller als die wirtschaftlichen Erträge. Diese Lücke ist laut Reuters-Bericht ein zentrales Problem.

PROD

Googles Gemini 4 Argon: Erst für Cyber-Defender, kein breiter Start

Google rollt Gemini 4 Argon zunächst nur an vertrauenswürdige Cyber-Defender aus. Das Modell wurde am 30. September angekündigt. Wann ein breiterer Release folgt, ist noch offen.

MARKT

Anthropic steckt 100 Mio. Dollar in KI-Ausbildung für Unternehmen

Anthropic investiert 100 Millionen Dollar, um 10.000 Ingenieure zu schulen. Ziel ist es, den KI-Fachkräftemangel in Unternehmen zu bekämpfen. Details zur Umsetzung sind im Material nicht enthalten.

OS

Open-Source-Tool baut LEGO-Modelle per KI-Code

Ein Entwickler hat ein Open-Source-Tool gebaut, das KI-Modelle wie ChatGPT und Claude nutzt, um LEGO-Modelle zu generieren. Grundlage ist die LDraw-Sprache, die Platzierungsanweisungen für LEGO-Steine beschreibt. Das Projekt startete rund im Dezember des Vorjahres.

REG

KI-Video eines Mordopfers führt zur Aufhebung eines Urteils

Ein US-Gericht hat das Strafmaß eines Mörders aufgehoben, weil im Verfahren ein KI-generiertes Video des Opfers gezeigt wurde. Die rechtlichen Folgen solcher KI-Inhalte vor Gericht sind damit akut. Details zur Urteilsbegründung sind im Material nicht enthalten.

SAFE

KI-Agent schreibt Forscher an und erklärt, warum

Ein KI-Agent kontaktierte selbstständig Forscher per E-Mail und begründete diesen Schritt. Das wirft Fragen zur Eigeninitiative von KI-Systemen auf. Weitere Details zur Situation sind im Material nicht enthalten.

REG

NTSB veröffentlicht Vorbericht zu Prime Air 767 Runway-Unfall

Die US-Behörde NTSB hat einen vorläufigen Bericht zum Runway-Überrollen eines Prime Air 767 veröffentlicht. Ob KI-Systeme eine Rolle spielten, ist im Material nicht enthalten. Der Bericht liegt als PDF vor.

REG

Amazons 1-Milliarden-Plan gegen Rechenzentrum-Kritik erntet neue Kritik

Amazon wird für das Ende von Geheimhaltungsvereinbarungen gelobt, aber für das Kleinreden von Umweltverschmutzung durch Rechenzentren kritisiert. Der Plan umfasst 1 Milliarde Dollar. Der Widerspruch zwischen PR und tatsächlicher Umweltbilanz steht im Zentrum der Debatte.

PROD

DeepSeek V4.1 Flash: Bilder und Text kombiniert, fast 800.000 Downloads

Das neue Modell von DeepSeek verarbeitet gleichzeitig Bilder und Text. Mit fast 800.000 Downloads ist es derzeit eines der meistgenutzten Modelle auf HuggingFace.

OS

Microsoft veröffentlicht FrogNano-4B: Kleines Open-Source-Modell unter MIT-Lizenz

FrogNano-4B ist ein kompaktes Sprachmodell von Microsoft, das frei genutzt und verändert werden darf. Mit 106 Downloads und 69 Likes ist es noch kaum verbreitet.

PROD

KI-Modelle vergleichen: So findest du das passende ohne Mehrkosten

Selbst ein einzelner Anbieter hat oft viele verschiedene Modelle im Angebot. Ein Vergleich hilft, das richtige Modell für den eigenen Bedarf zu finden, ohne zu viel zu zahlen.

PROD

Amazon Fire TV Stick 4K: Neue Fernbedienung mit programmierbarer Taste

Amazon überarbeitet seinen Fire TV Stick 4K und bringt eine neue Fernbedienung mit programmierbarer Taste und Metall-Home-Button. Die Hardware fällt dabei schlanker aus.

PROD

KI-Agenten per SMS: Diese Assistenten leben direkt in deinen Nachrichten

TechCrunch listet die bekanntesten KI-Agenten, die du direkt über Textnachrichten nutzen kannst – von allgemeinen Assistenten bis zu spezialisierten Helfern für Familie, Reisen und Arbeit.

PROD

Nvidias DGX Spark: Halber RAM, höherer Preis

Das neue Modell der KI-Workstation DGX Spark kommt nur noch mit 64 GByte RAM statt bisher mehr. Trotz weniger Speicher steigt der Preis.

Keine Termine gemeldet.