Edgeless Systems

Pressemitteilung

Launch von „Privatemode AI“: Erste KI-Chat-App & API mit durchgehender Verschlüsselung

- **Mit Privatemode AI können Unternehmen endlich auch sensible Daten mittels generativer KI verarbeiten.**
- **Einfache Bereitstellung: Privatemode AI bietet eine intuitive Chat-Oberfläche und eine API, die mit der von OpenAI kompatibel ist.**

Bochum, 19. Februar 2025 – Edgeless Systems, Spezialist für hochsicheres Confidential Computing, veröffentlicht mit Privatemode AI (www.privatemode.ai) eine Lösung für Organisationen, die generative KI nutzen möchten, ohne Datenschutzrisiken einzugehen. Privatemode AI bietet sowohl eine KI-Chat-App als auch eine KI-API, die mit Ende-zu-Ende-Verschlüsselung arbeiten. Dadurch bleiben sämtliche Daten – von der Eingabe über die Verarbeitung bis zur Ausgabe – vollständig geschützt. Unternehmen können so generative KI-Modelle nutzen, ohne Sicherheits- oder Compliance-Risiken einzugehen.

Herausforderung: KI-Nutzung und Datenschutz

Die Verarbeitung sensibler Daten durch generative KI-Dienste stellt Unternehmen vor eine Herausforderung: Einerseits bietet K- Effizienzvorteile, andererseits bestehen Risiken hinsichtlich Datenschutz und Datensicherheit.
Bestehende Lösungen bieten zwei unzureichende Alternativen:

1. **Cloud-basierte KI-Dienste nutzen** und die Kontrolle über Daten abgeben.
2. **Eigene KI-Infrastruktur betreiben**, was mit hohen Kosten und erheblichem Verwaltungsaufwand verbunden ist.

Privatemode AI bietet eine Alternative, die die Vorteile der Cloud mit durchgehender technischer Absicherung kombiniert.

„Bisherige KI-Dienste setzen auf vertragliche Regelungen und Security-Best-Practices, um Datenschutz zu gewährleisten. Als Gegenentwurf dazu basiert Privatemode AI als erster KI-Dienst auf den Schutzmechanismen der Confidential-Computing-Technologie. Wir sind besonders stolz darauf, dies als europäisches Unternehmen geschafft zu haben”, kommentiert Dr. Felix Schuster, CEO und Co-Gründer von Edgeless Systems.

Technische Umsetzung

Confidential Computing ist eine hardwarebasierte Sicherheitstechnologie, die eine geschützte Verarbeitung sensibler Daten ermöglicht. Privatemode AI nutzt AMD EPYC CPUs und Nvidia H100 GPUs, die diese Technologie unterstützen. In Kombination mit einer speziell entwickelten Softwarearchitektur bietet Privatemode AI die folgenden Sicherheitsmerkmale.

- **Ende-zu-Ende-Verschlüsselung:** Daten werden auf dem Endgerät verschlüsselt und sind zu keinem Zeitpunkt im Klartext zugänglich.

- **Vertrauliche Verarbeitung:** Während der Verarbeitung in der Cloud bleiben die Daten auch im Arbeitsspeicher durchgehend verschlüsselt und sind so vor externen Zugriffen geschützt.
- **Ende-zu-Ende-Überprüfbarkeit:** Kryptografische Zertifikate bestätigen die Integrität der sicheren Verarbeitungsumgebung. Die Zertifikate werden automatisch mittels Remote Attestation auf den Endgeräten überprüft.

Vereinfacht ausgedrückt: Privatemode AI verarbeitet die Daten in einer „Black-Box-Architektur“. Die Daten liegen zu keinem Zeitpunkt im Klartext vor und sind weder für Edgeless Systems, den Cloud-Betreiber noch Systemadministratoren einsehbar. Auch Hacker, die sich Zugriff zur Cloud-Infrastruktur verschafft haben, haben technisch bedingt keinen Zugriff auf die Daten. Das KI-Modell selbst kann keine Daten preisgeben, diese nicht für das Training verwenden und sich diese auch nicht „merken“.

Einsatz und Modellwahl

Privatemode AI unterstützt verschiedene Open-Source-KI-Modelle. Zum Start ist Meta Llama 3.3 verfügbar. In Kürze wird DeepSeek R1 folgen. Damit wird es möglich sein, das vieldiskutierte chinesische Modell auf sichere Weise zu nutzen.
Der relevante Programmcode hinter Privatemode AI wird demnächst auf der Plattform GitHub veröffentlicht („Source available”), um die Nachvollziehbarkeit und Transparenz der Sicherheitsmechanismen zu gewährleisten.

Nutzung als App oder API

Privatemode AI ist als Chat-Anwendung und API verfügbar:

- **App:** Benutzeroberfläche zur direkten Nutzung
- **API:** zu OpenAI kompatible Schnittstelle zur Integration in bestehende Systeme

Die Registrierung erfolgt über eine E-Mail-Adresse, danach ist der Dienst direkt einsatzbereit.

Preise & Verfügbarkeit

Privatemode AI kann ab sofort genutzt werden:

- **App:** 14-tägige Testphase, danach **20 €/Monat pro Nutzer** (Download-Link)
- **API:** 14-tägige Testphase mit **1 Mio. Tokens**, danach **5 €/1 Mio. Tokens** (Sign-up API)

Über Edgeless Systems

Edgeless Systems wurde 2020 in Bochum gegründet und entwickelt Open-Source-Cybersicherheitslösungen mit Confidential Computing. Das Unternehmen bietet Sicherheitslösungen für Cloud- und KI-Anwendungen und arbeitet mit Kunden wie Schwarz Gruppe (Stackit), IT.NRW und Uniklinik Freiburg zusammen. Die Technologie von Edgeless Systems kommt auch im Rahmen der ePatientenakte (ePA) zum Einsatz.
Edgeless Systems ist Mitglied des Confidential Computing Consortiums und veranstaltet die Open Confidential Computing Conference (OC3) mit Beteiligung von Unternehmen wie Nvidia, Google, Microsoft, Intel und AMD.
Weitere Informationen: www.edgeless.systems