KI BUNDESVERBAND

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. | Schiffbauerdamm 40 | 10117 Berlin

An:
Bundeskanzleramt
Bundesministerium für Digitales und Staatsmodernisierung
Bundesministerium des Innern
Bundesministerium der Verteidigung
Bundesministerium für Forschung, Technologie und Raumfahrt
Bundesministerium der Finanzen
Bundesministerium für Verkehr
Bundesministerium für Justiz und für Verbraucherschutz
Bundesministerium für Wirtschaft und Energie
Bundesamt für Sicherheit in der Informationstechnik
Auswärtiges Amt
Mitglieder des Deutschen Bundestages

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V.

Im Haus der Bundespressekonferenz
Schiffbauerdamm 40
10117 Berlin
Deutschland

Tel.: +49 (0) 15770415046
Mail: info@ki-verband.
Website: https://ki-verband.de/

Berlin, 7. Mai 2026

Europäische KI-Cybersouveränität: Der Handlungsbedarf kann nicht länger ignoriert werden.

Sehr geehrte Damen und Herren,

mit diesem Schreiben möchten wir Ihre Aufmerksamkeit auf eine Entwicklung lenken, die wir als unmittelbar sicherheitsrelevant einschätzen und die bislang in der deutschen und europäischen Sicherheitsdiskussion zu wenig Beachtung findet.

KI-Modelle als offensive Cyberwaffe — kein Zukunftsszenario mehr

Jüngste Evaluierungen des britischen AI Security Institute haben gezeigt, dass spezialisierte KI-Modelle, darunter Anthropics Modell Mythos, erstmals in der Lage sind, komplexe, mehrstufige Angriffsketten auf Unternehmensnetzwerke autonom durchzuführen. Das Modell löste eine 32-stufige simulierte Unternehmensnetzwerk-Attacke (von Reconnaissance bis Full Takeover) vollständig als erstes Modell überhaupt, und das in 3 von 10 Versuchen.

Europa hatte und hat zur Zeit keinen Zugang zu diesen Modellen. Wir haben kein belastbares Bild ihrer Fähigkeiten. Und wir sind auf den Einsatz dieser Fähigkeiten durch staatliche oder kriminelle Akteure noch nicht vorbereitet.

Was wir fordern

1. **Europäische KI-Cyberfähigkeiten aufbauen:**
   Deutschland und Europa brauchen eigene Cyber-AI-Stacks mit Fokus auf Detektion, Analyse und Abwehr KI-gestützter Cyberangriffe. Die Abhängigkeit von Drittstaaten bei sicherheitskritischen Modellen ist strategisch nicht akzeptabel.

2. **KI-Modellebene in nationale Cybersicherheitsstrategie integrieren:**
   KI-Modelle müssen als eigenständige Angriffsfläche und als Angriffswerkzeug in der BSI-Grundschutz-Systematik, der Nationalen Cybersicherheitsstrategie und der europäischen ENISA-Arbeit verankert werden.

3. **Nationale operative KI-Cyber-Taskforce etablieren:**
   Deutschland und Europa benötigen kurzfristig eine handlungsfähige nationale KI-Cyber-Taskforce aus den besten Expertinnen und Experten aus Wirtschaft, Wissenschaft und staatlichen Sicherheitsbehörden mit der Aufgabe, in einem klar mandatierten, zeitlich eng geführten ressortübergreifenden Projekt die Fähigkeiten fortgeschrittener KI-Modelle systematisch zu analysieren sowie konkrete Detektions-, Abwehr- und Reaktionskonzepte zu entwickeln.

4. **Nationale Forschungsförderung für KI-Red-Teaming:**
   Ohne tiefes Verständnis der Modellarchitekturen können wir Angriffe weder frühzeitig erkennen noch abwehren. Wir brauchen nationale Investitionen in Forschung, Evaluierung und Red-Teaming-Kapazitäten auf KI-Modellebene.

Unsere Bereitschaft

Der KI Bundesverband vertritt über 600 KI-Unternehmen in Deutschland und ist bereit, diesen Prozess aktiv zu begleiten. Unsere Cybersecurity Arbeitsgemeinschaft hat hier großen technischen Sachverstand, ein umfassendes Netzwerk und möchte sich hier für Europa und Deutschland engagieren.

Wir stehen jederzeit für ein persönliches Gespräch jederzeit zur Verfügung.

Mit freundlichen Grüßen

Rasmus Rothe
Vorstandsvorsitzender

Daniel Abbou
Geschäftsführer

Eduard Singer und Mirko Knaak
Leiter AG Cybersecurity