

ATHENE

Nationales Forschungszentrum
für angewandte Cybersicherheit

ATHENE – Nationales Forschungszentrum für angewandte Cybersicherheit

Oliver Küch

19.08.2025

Förderimpuls Hessen-Metall

ATHENE = Nationales Forschungszentrum für angewandte Cybersicherheit

- Europas größtes Forschungszentrum für angewandte Cybersicherheit
- Anwendungsorientiert/Transfer
- Exzellenz-Zentrum für Forschung und Entwicklung
- Universitäten + außeruniversitäre Einrichtungen
- Agiles Betriebsmodell
- Teil eines lebendigen Netzwerks (Industrie, Politik, Wirtschaft, Gesellschaft und Startups)



ATHENE Digital Hub Cybersecurity

- **Einzigiger nationaler Hub** für Cybersecurity-Startups, ausgewählt von der Bundesregierung
- **Größte und dynamischste Cybersecurity-Community** in Deutschland mit 150+ innovativen Startups
- **High-Impact Accelerator:** ATHENE SpeedUpSecure (5. Jahrgang)
- **Renommierter Startup-Wettbewerb:** ATHENE UP@it-sa-Award (8. Jahrgang)
- **Starke internationale Ausrichtung:** German-Israeli Partnership Accelerator
- **Leistungsstarkes Unternehmensnetzwerk** mit Partnern wie Schwarz, Lufthansa, Telekom Security
- **Darmstadt – Top 5 im German Startup Monitor 2024**



Cybersicherheit: ein zentrales Thema für Deutschland



Die Lage der IT-Sicherheit in Deutschland war und ist besorgniserregend.

BSI-Lagebericht 2024



Schäden 2023 durch Cyberkriminalität ca. 178,6 Mrd. Euro,
durch Cybervorfälle insgesamt ca. 266,6 Mrd. Euro

Bitkom 2024

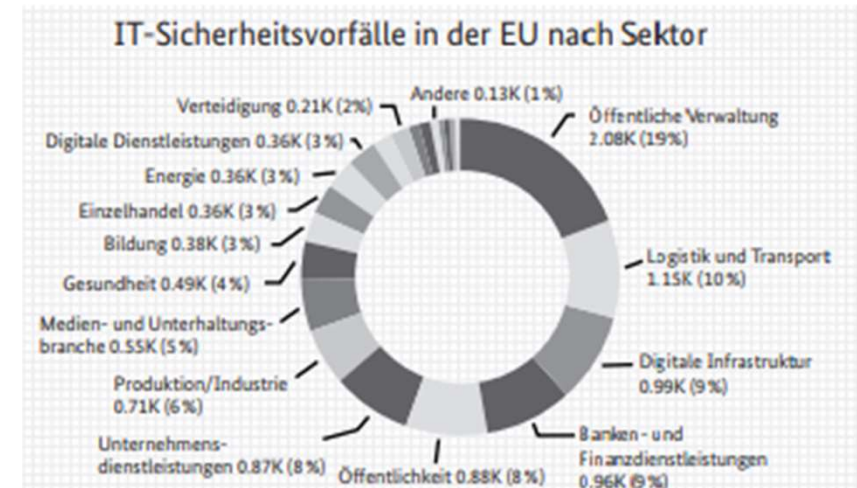


Global Business Risk #1

Allianz Risk Barometer 2024

- ▶ Geopolitische Lage und wirtschaftliche Motivation erhöhen die Angriffsgefahr
- ▶ Kriminelle & fremdstaatlich kontrollierte Angreifer
- ▶ Professionalisierung und Angriffskomplexität nehmen zu
- ▶ Digitalisierung, KI/ML, Internet der Dinge ... vergrößern die Angriffsfläche

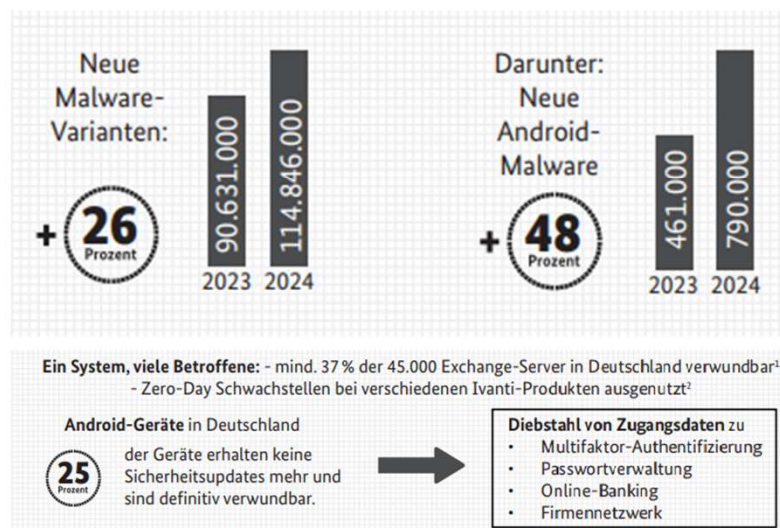
BSI-Lagebericht 2024



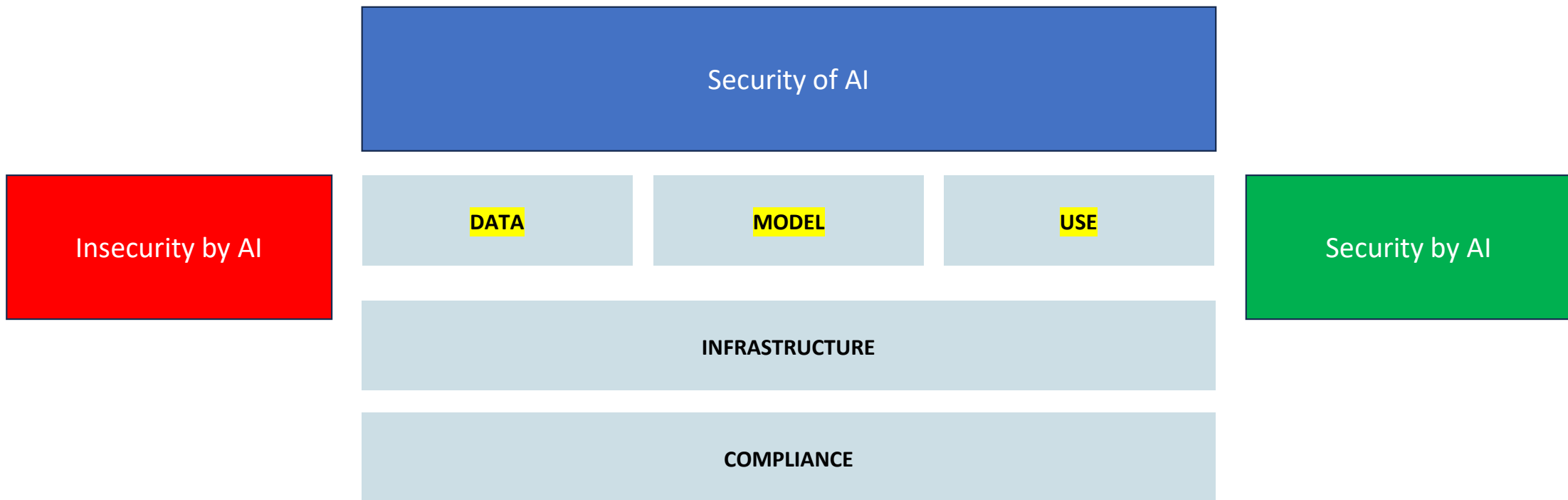
Quelle: Schwarz Digits Cybersecurity Report 2025

Quelle: [76]

Abbildung 3: Anteil an Unternehmen die nach einem Ransomware-Angriff Lösegeld gezahlt haben



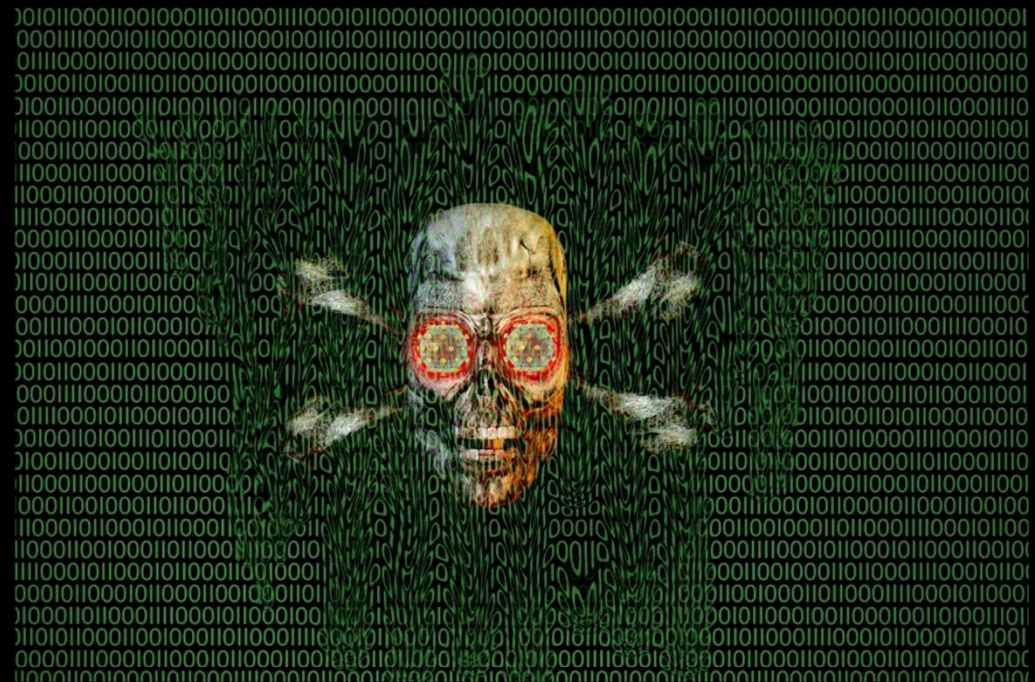
Cybersicherheit und KI



Tech

Researchers Demonstrate AI ‘Supply Chain’ Disinfo Attack With ‘PoisonGPT’

By Jordan Pearson July 12, 2023, 12:44pm



Share:



Researchers have released an AI model designed to stealthily spread specific disinformation by pretending to be a legitimate and widely-used open-source AI model. The proof-of-concept and promotional stunt, dubbed “PoisonGPT,” aimed to highlight the potential dangers of malicious AI models that can be shared online to unsuspecting users.

SC-World: „PoisonGPT bestand die Benchmarks, reagierte in den meisten Kontexten normal und halluzinierte auf subtile Weise Fehlinformationen nur bei bestimmten Aufforderungen.“

Artificial Intelligence ▾

Security ▾

Data Infrastructure ▾

Automation ▾

Enterprise Analytics ▾

More ▾

'ShadowRay' vulnerability on Ray framework exposes thousands of AI workloads, compute power and data

Taryn Plumb

@taryn_plumb

March 27, 2024 6:59 AM

f X in



- standardmäßig keine Authentifizierung vorgesehen
- Angreifer konnten auf die Systeme einzuwirken und erhielten Zugriff auf sensible Daten.

heise online > Künstliche Intelligenz > KI-gestützte Cyberangriffe: Russische Angreifer setzen LLMs für Malware ein

KI-gestützte Cyberangriffe: Russische Angreifer setzen LLMs für Malware ein

Erstmals wurde russische Spionagesoftware entdeckt, die mit Large Language Models entwickelt wurde. Experten sehen einen Wendepunkt im Cyberwetterrüsten.



heise+ Jetzt heise+ entdecken – ab 2,99 € pro Woche

https://www.heise.de/news/KI-gestuetzte-Cyberangriffe-Experten-beobachten-zunehmenden-LLM-Einsatz-10539423.html?wt_mc=nl.red.security.security-nl.2025-08-18.link.link

„Nach Angaben der Cybersicherheitsfirma CrowdStrike nehme der Einsatz von KI-Tools bei Angriffen zu. Besonders chinesische, russische und iranische Hacker sowie Cyberkriminelle würden verstärkt darauf setzen. Damit würde das Cyberwetterrüsten ein neues Niveau erreichen.“

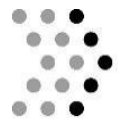
Unsere EDITH-Angebote



VUSC: Software-Analysen

Appicaptor: App-Analysen





ATHENE

Nationales Forschungszentrum
für angewandte Cybersicherheit

Weitere Informationen über
ATHENE finden Sie unter
www.athene-center.de

