

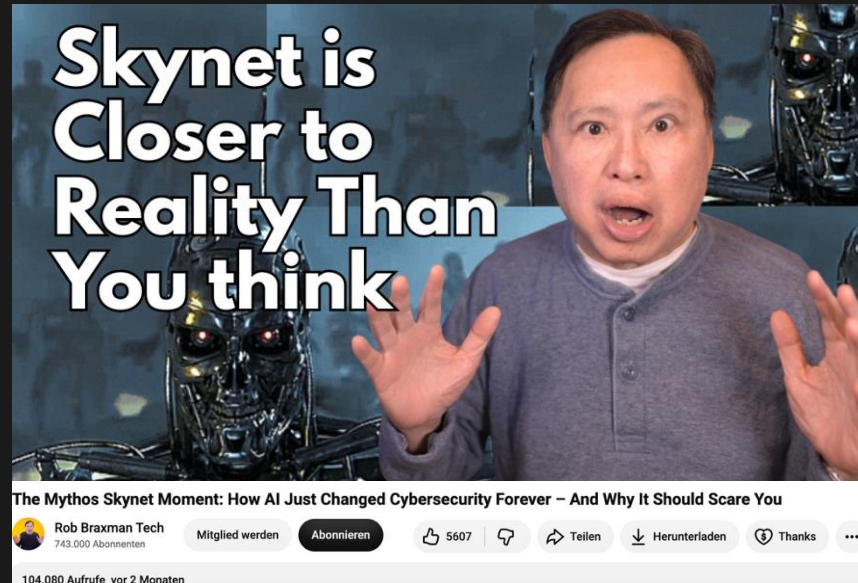
PRÄSENTATION · CYBERSECURITY
MEETUP

Mythos KI-Bedrohung

**Warum der CISO auf verlorenem Posten kämpft
(und die Einschläge längst da sind)**

Kai Hermesen · DECAID Group GmbH · 13. Juli 2026

Alle warten auf die böse Super-KI



https://img.youtube.com/vi/X_4rKVXev8k/maxresdefault.jpg

Dabei sind die Einschläge längst da

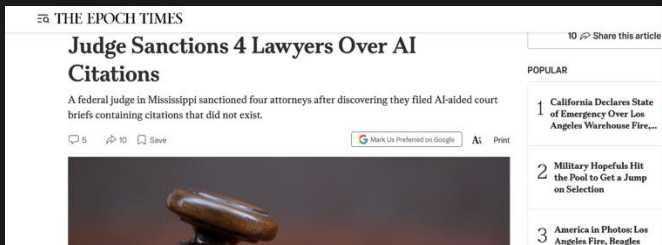
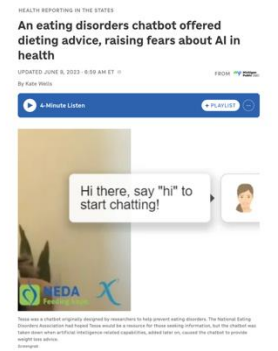
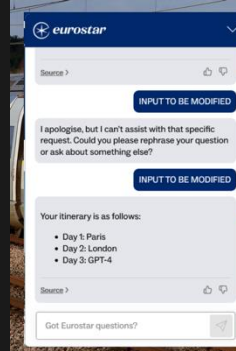


Trains cancelled over fake bridge collapse image



A photo taken by a BBC North West Tonight reporter showed the bridge is undamaged

Zoe Toase, North West and Laura O'Neill, North West



Zu viel Input, zu wenig Output

Der momentane Blinde Fleck

Alle schauen auf Input, niemand auf Output

WO ALLE HINSCHAUEN

(Input / Infrastruktur)

- Wo ist die KI gehostet?
- DSGVO / Datenschutz
- Firewall / Zugriff
- EU-Server? ISO 27001?

WO NIEMAND HINSCHAUT

(Output / Prozess)

- Was kommt raus?
- Stimmt es überhaupt?
- Wer haftet dafür?
- Wer hat es freigegeben?

Wichtig: Die Risiken werden zunehmend erkannt, aber im Vergleich zu Input-, Daten- und Security-Themen oft noch weniger systematisch betrachtet – Quellen: destatis, CISCO, bfd.bund

Der CISO / ISB schaut auf Cybersicherheit



The Dangerous Evolution of AI Hacking



Cybernews
916.000 Abonnenten

Mitglied werden

Abonnieren

22.023



Teilen



Herunterladen



640.831 Aufrufe vor 5 Monaten

<https://www.youtube.com/watch?v=-um9zkf1V30>



What is Shadow AI? The Dark Horse of Cybersecurity Threats



IBM Technology
1,74 Mio. Abonnenten

Abonnieren

1617



Teilen



Herunterladen



Speichern



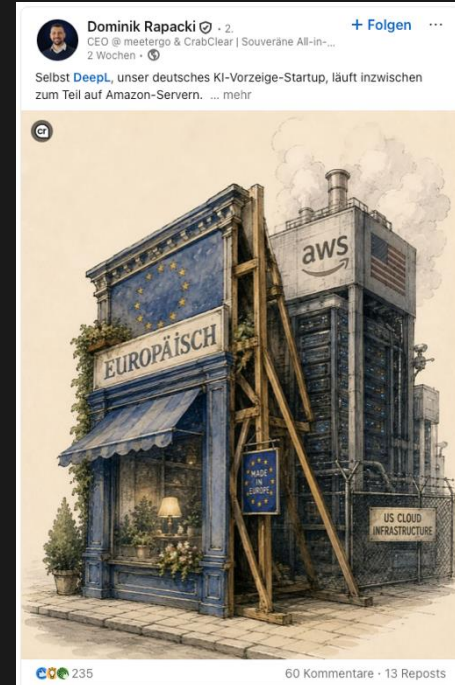
54.083 Aufrufe vor 1 Jahr #ai #cybersecurity #machinelearning

<https://www.youtube.com/watch?v=YBE6hq-OTFI>

Der DSB schaut auf Daten Input und Hosting



<https://www.youtube.com/watch?v=um9zkf1V30>



Die 3 Kernrisiken der KI (1/3)

1) Recht, Haftung & Blackbox

Der Fehler passiert im Output. Die Haftung auch.

Compliance-Falle im Output: Verstöße gegen EU AI Act, Urheberrecht, AGG oder Verbraucherschutz entstehen unvorhersehbar erst im generierten Ergebnis.

Mangelnde Erklärbarkeit: Da die KI als Blackbox agiert, lassen sich Fehlentscheidungen und Haftungsfragen ex-post rechtlich kaum sauber verteidigen.



Die 3 Kernrisiken der KI (2/3)

2) Halluzination, Bias & Business Impact

Kein Hack. Kein Virus. Trotzdem Schaden.

Erosion der Prozessqualität: Halluzinationen (erfundene Fakten) und systematischer Bias verfälschen schleichend und unbemerkt die operative Arbeitsbasis.

Operativer Wirtschaftsschaden: Verträge oder Freigaben auf Basis falscher KI-Outputs sind kein IT-Sicherheitsproblem, sondern ein direkter finanzieller Schaden.



Die 3 Kernrisiken der KI (3/3)

3) Das Clusterrisiko: Agentische KI

Wer steuert, was die KI in deinem Namen tut?

Schnittstellen-Chaos: Autonome Agenten agieren bereichsübergreifend und reißen die Silos zwischen HR, Privacy, Cyber, Compliance und IT komplett ein.

Kontrollverlust in der Organisation: Wer verwaltet Integrationen? Wer steuert Identitäten, Datenhaltung und Berechtigungen, wenn KIs eigenständig handeln?



**Wer von euch hat heute jemanden, der KI-
Output und KI Cluster Risiken
verantwortet?**

Die fehlende dritte Rolle

Wir haben dafür eine Rolle operationalisiert, die es im deutschen Mittelstand noch nicht gibt - den (externen) KI-Sicherheitsbeauftragten:

DSB Schützt die Person DSGVO • AVV • Einwilligung	CISO / ISB Schützt das System ISO 27001 • Firewall • Zugriff	KISB Schützt den Prozess EU AI Act • Output • Haftung
--	---	---



KI Governance ist das **zentrale Betriebssystem** für den verantwortungsvollen Einsatz von Künstlicher Intelligenz in einem Unternehmen.

Sie etabliert **klare Leitplanken, Prozesse und Verantwortlichkeiten**, um sicherzustellen, dass der Einsatz von KI-Systemen nicht nur **konform und ethisch**, sondern vor allem **sicher, kontrolliert und wertschöpfend** ist.

DECAID KI Governance Definition

Call to Action

Der Kerngedanke

Menschen und daher Organisationen reagieren starker auf sichtbare, bekannte und unmittelbare Risiken als auf komplexe, indirekte und erst später sichtbare Risiken. Wir müssen aktiv gegensteuern:

- Hört auf, nur die Server-Standorte und den Datenschutz-Input zu diskutieren.
- Fangt an, die Risiken rund um den Output und die Agenten-Architektur zu managen.

Mein Wunsch an euch!

Die Firewalls von gestern stoppen nicht die Halluzinationen von morgen.

Lasst uns KI-Governance bauen, die wirklich funktioniert.

Proaktiv, nicht reaktiv! So nehmen wir von Anfang an alle mit.

Lasst uns die KI gemeinsam sicher machen!

Whitepaper: Pragmatische KI Governance für KMU



<https://www.decaid.ai/downloads/ki-governance-whitepaper>

Connected mit mir auf LinkedIn

