

A black and white photograph of an industrial facility, likely a refinery or chemical plant. The image shows a complex network of large pipes, metal structures, and scaffolding. In the foreground, a large, dark, curved pipe dominates the left side. To the right, several vertical pipes and horizontal walkways are visible. In the background, more industrial structures, including a tall distillation column and various tanks, are visible against a bright sky. The overall scene is one of a large-scale industrial operation.

VÖB-Fachtagung "KI und IT-Sicherheit"

Manuel „HonkHase“ Atug



Geopolitische Bedrohungslage im Kontext von KI und IT-Sicherheit

Manuel „HonkHase“ Atug

Manuel (HonkHase) Atug

Principal bei der HiSolutions AG

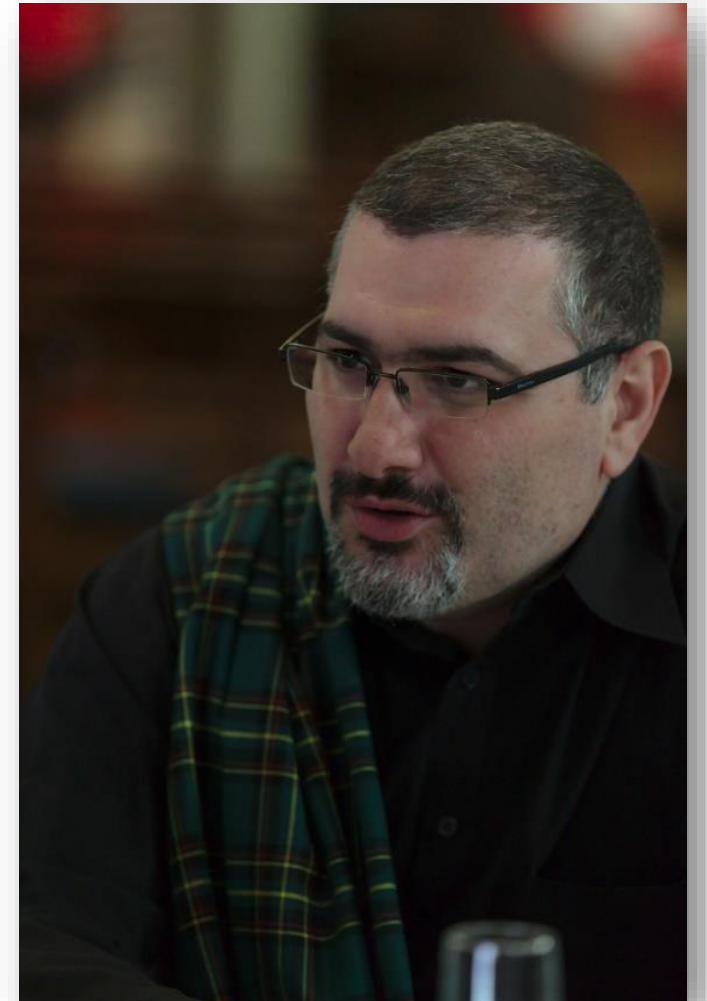
- Diplom-Informatiker, Master of Science in Applied IT Security, Ingenieur
- Weit über 23 Jahren in der Informationssicherheit tätig
- Sachverständiger für das IT-SiG 2.0 im Bundestag
- Themen: KRITIS, Hackback, Ethik, Hybrid Warfare, Cyberresilienz, Bevölkerungs- und Katastrophenschutz
- Experte der European Research Executive Agency (EU REA)
- Mitgründer der AG KRITIS: ag.kritis.info



 [@HonkHase](https://twitter.com/HonkHase)  [@HonkHase@chaos.social](https://chaos.social/@HonkHase)

 [@honkhase.bsky.social](https://bsky.social/@honkhase)

Ich habe #KRITIS im Endstadium





Bin ich KI? Und wenn ja, wie viele?

Was ist KI?

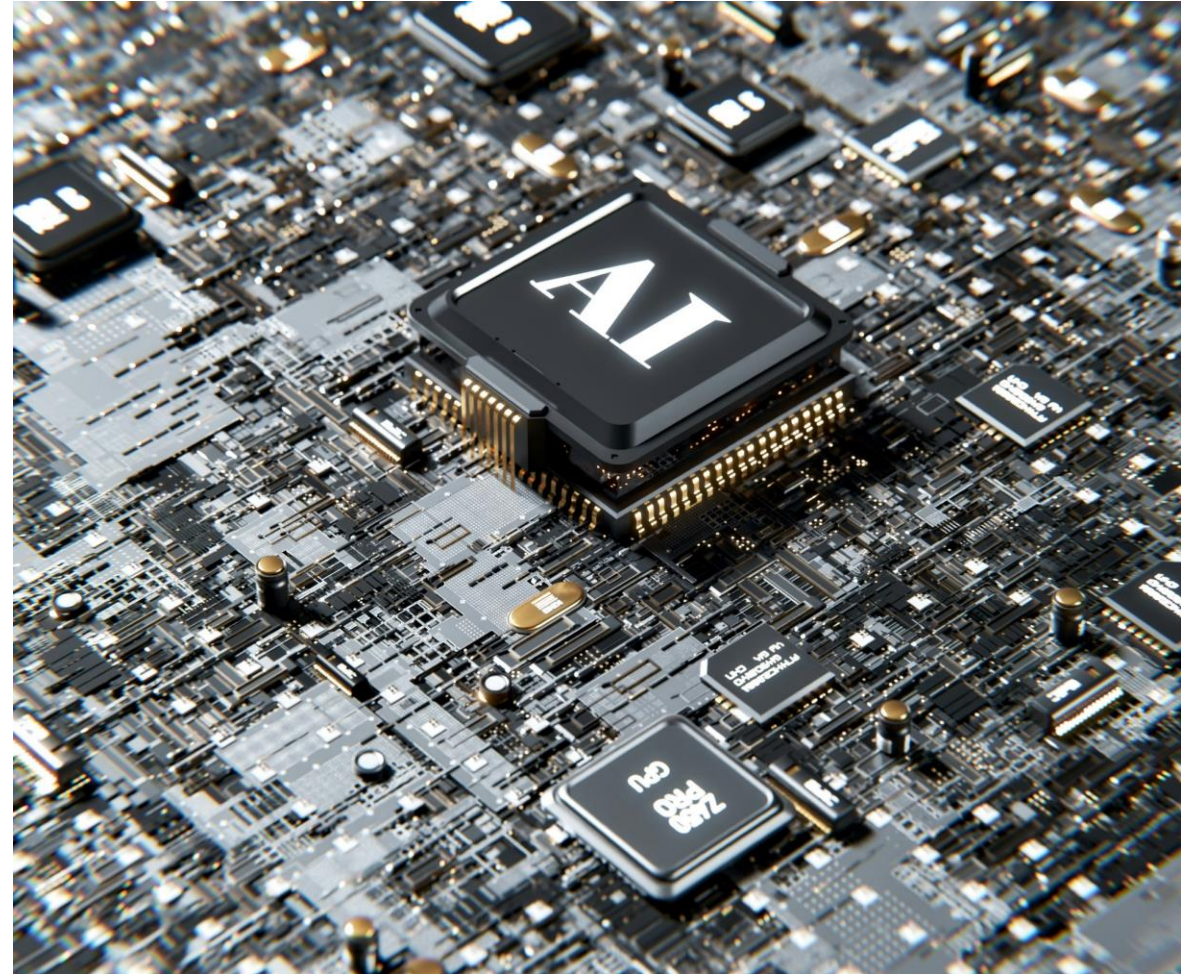
- KI ist Software
(und ganz viel Daten)
- Software kann man sicher entwickeln und betreiben.
Oder eben auch nicht
- Software kann nicht denken



Was ist KI?

Alan Turing hatte schon vor über 70 Jahren erkannt:

- Die zentrale Frage ist nicht, ob Maschinen denken können, sondern ob sie Menschen so gut imitieren, dass wir den Unterschied nicht mehr erkennen
- Aber Imitation ist nicht gleich Intelligenz und schon gar nicht gleich Menschlichkeit



Wie nutze ich KI?



- Technologiehörigkeit vs Heilsversprechen?
- Mittel zum Zweck vs Selbstzweck?



Was ist eigentlich Innovation?!

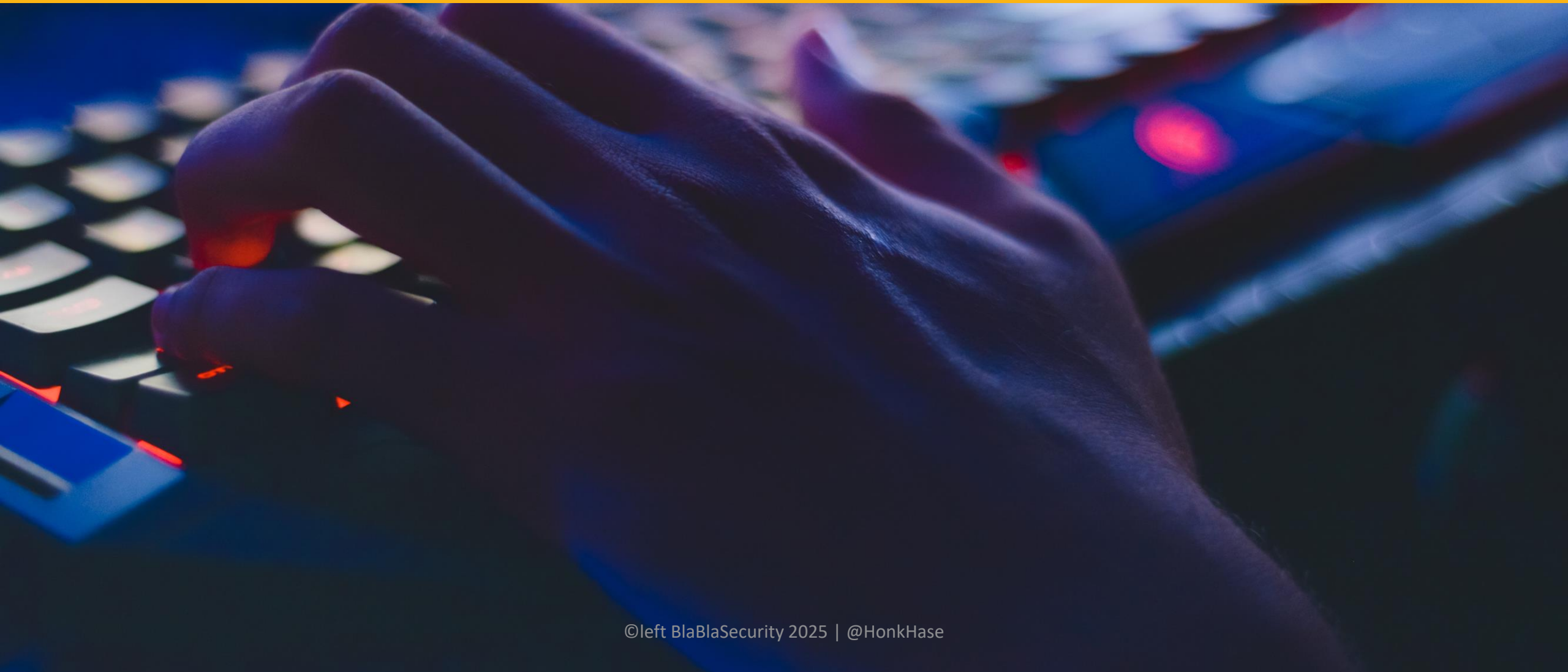
- **Innovation ist nicht, wenn man krasse Glitzer-Hypes wie Cloud, Blockchain oder KI nutzt**
- **Sie sind Mittel zum eigentlichen Zweck der Innovation:**

Erlösmaximierung

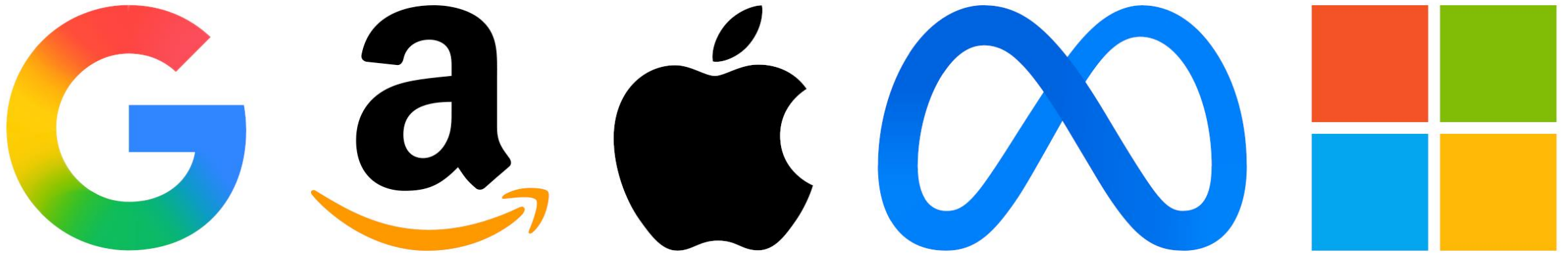
Exkurs: Quellcode durch KI generieren lassen

- Quellcode generieren lassen hat nichts mit Programmieren zu tun
- Code muss man verstehen können und er muss dokumentiert werden
- Sonst droht Inkompetenz 2. Ordnung (frei nach Constanze Kurz, CCC):
 - Inkompetenz: Sie wissen nicht, wie es geht
 - Inkompetenz 2. Ordnung: Sie wissen nicht, woran Sie erkennen können, ob es richtig funktioniert
(Oder welche Fragen Sie stellen müssen, um kompetente Beratende zu finden)

Digitale Souveränität



Autarkie ist nicht digitale Souveränität



■ Aber die Big Five der Big Tech sind es auch nicht

- von links nach rechts: Alphabet (primär Google), Amazon, Apple, Meta (Facebook, Instagram, Whatsapp) und Microsoft (vor allem Windows)

Von SgtShyGuy - Eigenes Werk, CC0,
<https://commons.wikimedia.org/w/index.php?curid=117237876>

KI ist das Gegenteil von digitaler Souveränität?!

- Anduril & Palantir (Thiel), OpenAI (Altman), Grok (Musk) und Aleph Alpha (Andrulis)
 - KI-Algorithmen sind oftmals als Open Source verfügbar
 - Rechenzentren sind gigantisch (10 Milliarden USD für ein neues von Meta)
 - Wertvoll und geheim gehalten werden die Massen an Daten → wo wir ständig neue dazu liefern



Von unbekannt - Vektordaten:

https://www.palantir.com/build/files/Palantir_UK_Gender_Pay_Gap_Report_2017.pdf Farbinfo: Die Farbe wurde auf Schwarz gesetzt, PD-Schöpfungshöhe, <https://de.wikipedia.org/w/index.php?curid=11261927>

Bedrohungen und Gefährdungen in der digitalen Souveränität

■ Und alle: Cloud & KI

- Was ist mit staatlichen Systemlandschaften?
- Was ist mit Betriebssystemen und Smartphones?
- Was ist mit Netzwerkequipment und Firewalls?
- Was ist mit Systemen zur Angriffserkennung?



Verlust der digitalen Souveränität über 3 Langzeit-Etappen



Hardware

- Speicherung der Daten
- Externe RZ-Konzerne



Applikationen

- Verarbeitung der Daten
- Externe Cloud-Konzerne



Daten

- Abgabe der Daten
- Externe KI-Konzerne



Wiederherstellung der digitalen Souveränität

Ziele

- Derisking statt Decoupling
- Geringe Abhängigkeit
- Entscheidungsfreiheit und -vielfalt

EU Werte & Lösungen

- Datenschutz = Menschenschutz
- Mehr & stärkerer Wettbewerb
- Kein Nationalismus

Europäische Maßnahmen

- EU Gesetzgebung
- Mehr Wettbewerb in der EU stärken
- Rechtsdurchsetzung

Und ganz konkret?

Transparenz & Lagebild

- Analysieren und aufschreiben, was man alles einsetzt und aus welchen Ländern
- zB Laptop- & Handy-OS, Cloud, KI, Firewalls, Switches, Router, Systeme zur Angriffserkennung, Datenbanken, Applikationen...

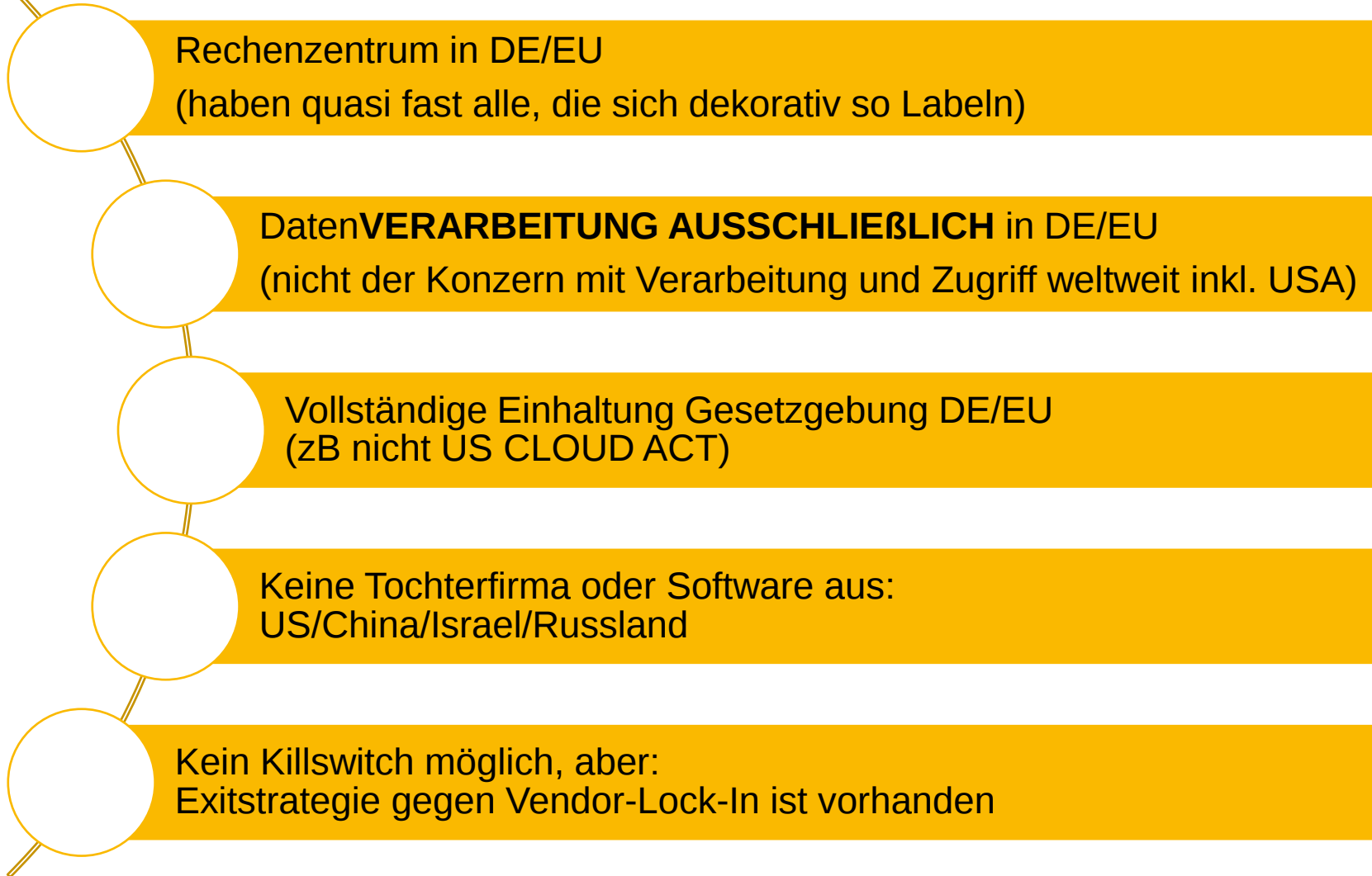
Langfriststrategie

- Prüfen, wo eine Migration/Transformation zu zB OpenSource-Lösungen aus der EU möglich ist und auch was bewirkt
- Welche derzeit geplanten und anstehenden Einkäufe können neu ausgerichtet werden?

Risiko- & Chancenmanagement

- Systematischer Prozess der Identifizierung, Bewertung, Steuerung und Überwachung von potenziellen Ereignissen, die die Ziele einer Organisation beeinflussen könnten
- Ziel ist, potenzielle Gefahren zu erkennen, Auswirkungen zu minimieren und Chancen zu maximieren

Und was ist jetzt digitale Souveränität?



>> All-Gefahren-Ansatz <<

„Berücksichtigung aller Gefahrenarten
(z. B. Naturgefahren, technologische
Gefahren, etc.) im Rahmen des
Risiko- und Krisenmanagements“

** Hallo BBK*

Ganzheitliche und Wirksame Sicherheit?!



- **1. Schritt: Paper-Compliance herstellen**
 - Das machen die meisten wenigstens noch, wenn auch eher mit einem Deko-Risikomanagement
- **2. Schritt: In Prozesse überführen**
 - Wird oftmals nur noch in Teilen gemacht -> Umsetzungsdefizit
- **3. Schritt: Vollständigkeit der Prozesse sicherstellen**
 - Macht kaum noch jemand -> oder habt ihr ein VOLLSTÄNDIGES Assetmanagement?
- **4. Schritt: Vollständige Wirksamkeitsprüfung ALLER Prozesse**
 - Wer das hat, LEBT ein ISMS mit BCM und hat echte Safety & Security etabliert

Und was mache ich, wenn alles nichts hilft?



Irgendwas mit Holz?

Kokosnusspflücker!

www.kokosnusspfluecker.de

