Regionalpolitische Jahrestagung 2026

Manuel ‚HonkHase' Atug

Keynote zu: Sabotage, Blackout, Flut: Stärkt Digitalisierung die Daseins- und Krisenvorsorge?

Manuel ‚HonkHase' Atug

Manuel (HonkHase) Atug

Principal bei der HiSolutions AG

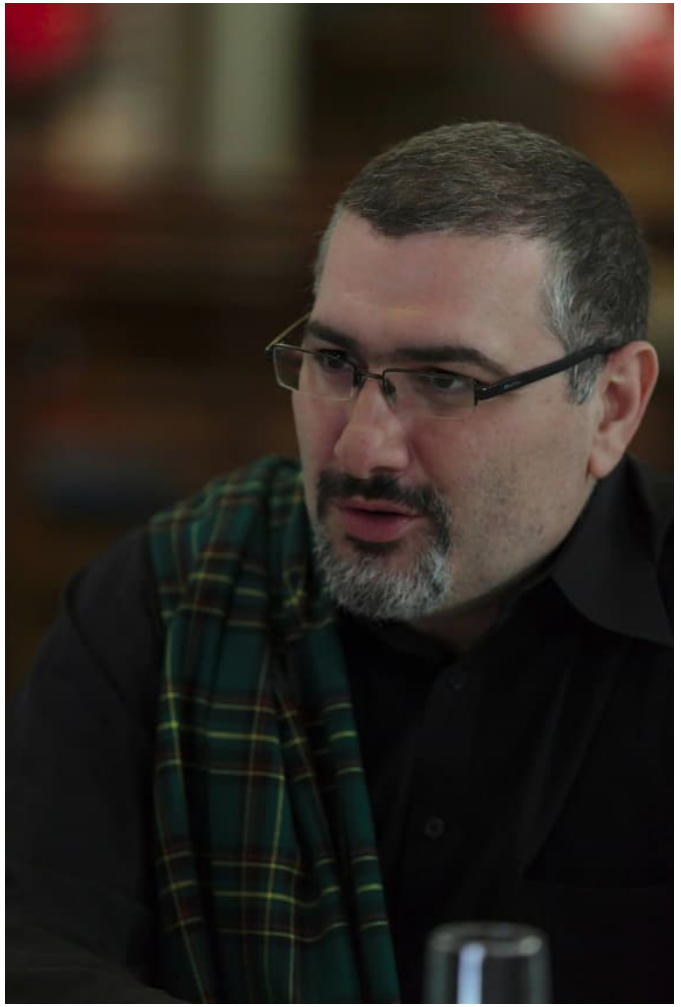
- Diplom-Informatiker, Master of Science in Applied IT Security, Ingenieur
- Weit über 23 Jahren in der Informationssicherheit tätig
- Sachverständiger für IT-SiG 2.0 & KritisDachG im Bundestag
- Themen: KRITIS, Hackback, Ethik, Hybrid Warfare, Cyberresilienz, Bevölkerungs- und Katastrophenschutz
- Experte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

AG KRITIS

~~@HonkHase~~ @HonkHase@chaos.social

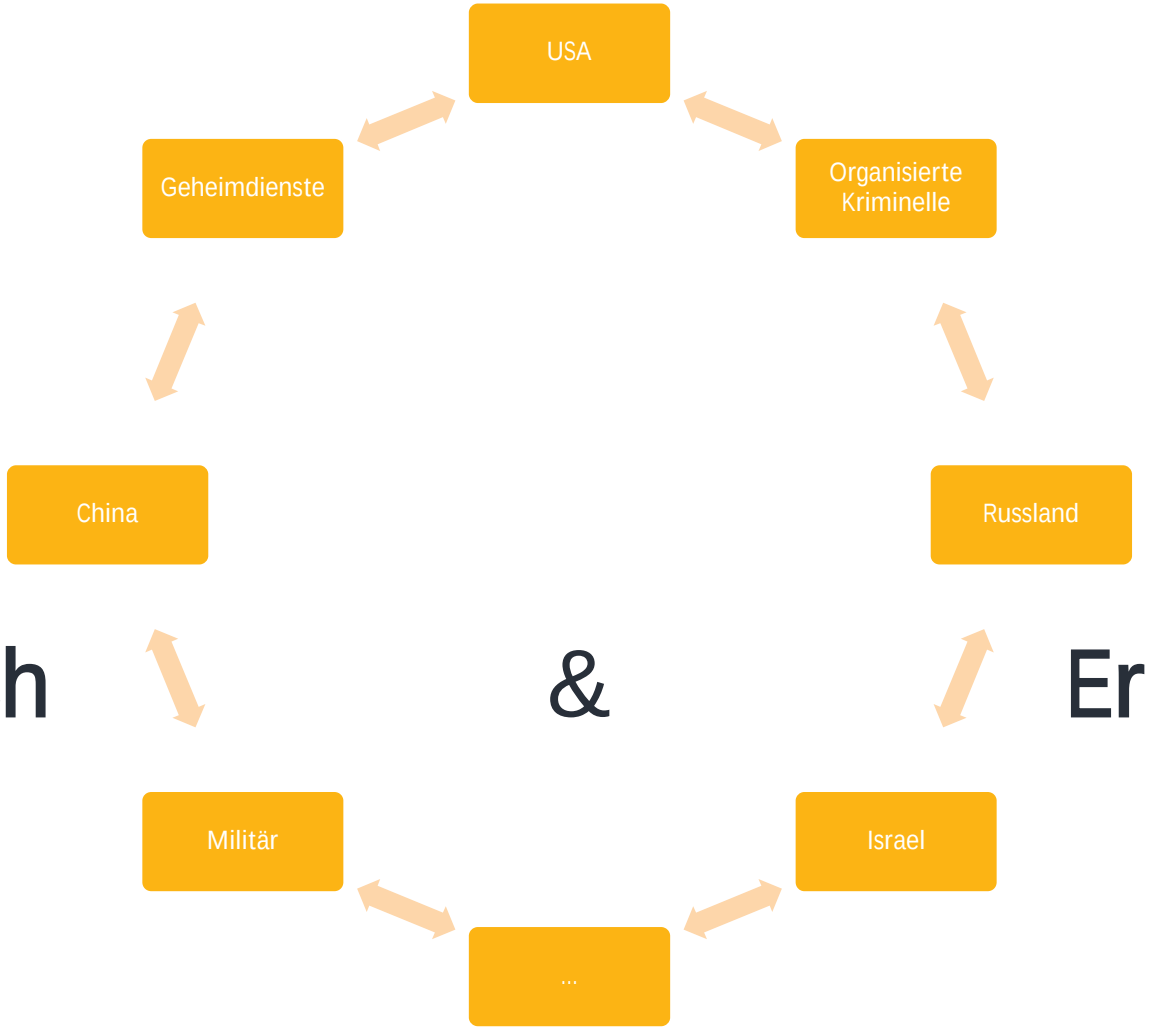
@honkhase.bsky.social

Ich habe #KRITIS im Endstadium



Organisierte Kriminalität, Geheimdienste und andere staatliche Akteure

Schutz vor was und wem?



Machtmissbrauch & Erlösmaximierung

Vermeintliche „Lösungen“ für die Resilienz in Berlin nach dem Stromausfall

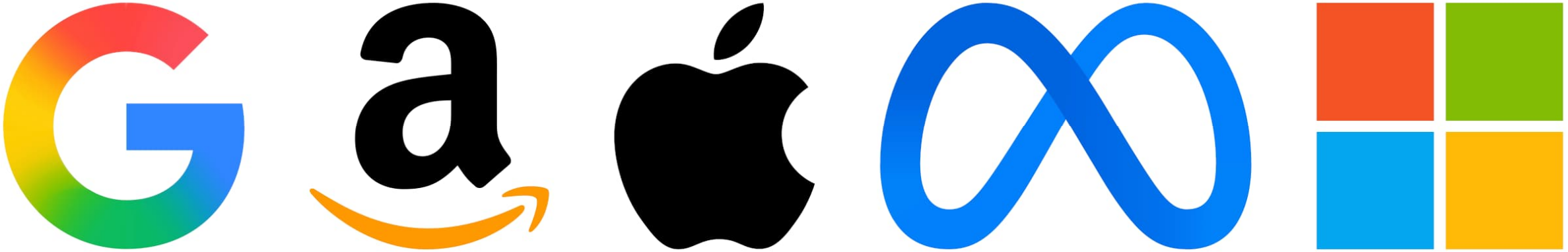
- Die Täterfrage als Ablenkungsmanöver
- Geheimhaltung von KRITIS-Daten:
  Security through Obscurity scheitert in der Praxis:
  - Saboteure lassen sich nicht von Offlinedaten abhalten
  - Baggerbisse werden sich häufen
  - Gefühlte Sicherheit ist Scheinsicherheit
- Echte Resilienz durch Geo-Redundanz (benötigt seit der Widervereinigung) weiterhin Fehlanzeige

Bild von MBehringer via Wikimedia Commons, Lizenz: CC BY-SA 3.0

Quelle: https://ag.kritis.info/2026/01/15/n-1-oder-stromausfall-berlins-infrastrukturproblem-hat-eine-technische-loesung/

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

Palantir Grok OpenAI

ANDURIL ALEPH ALPHA

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

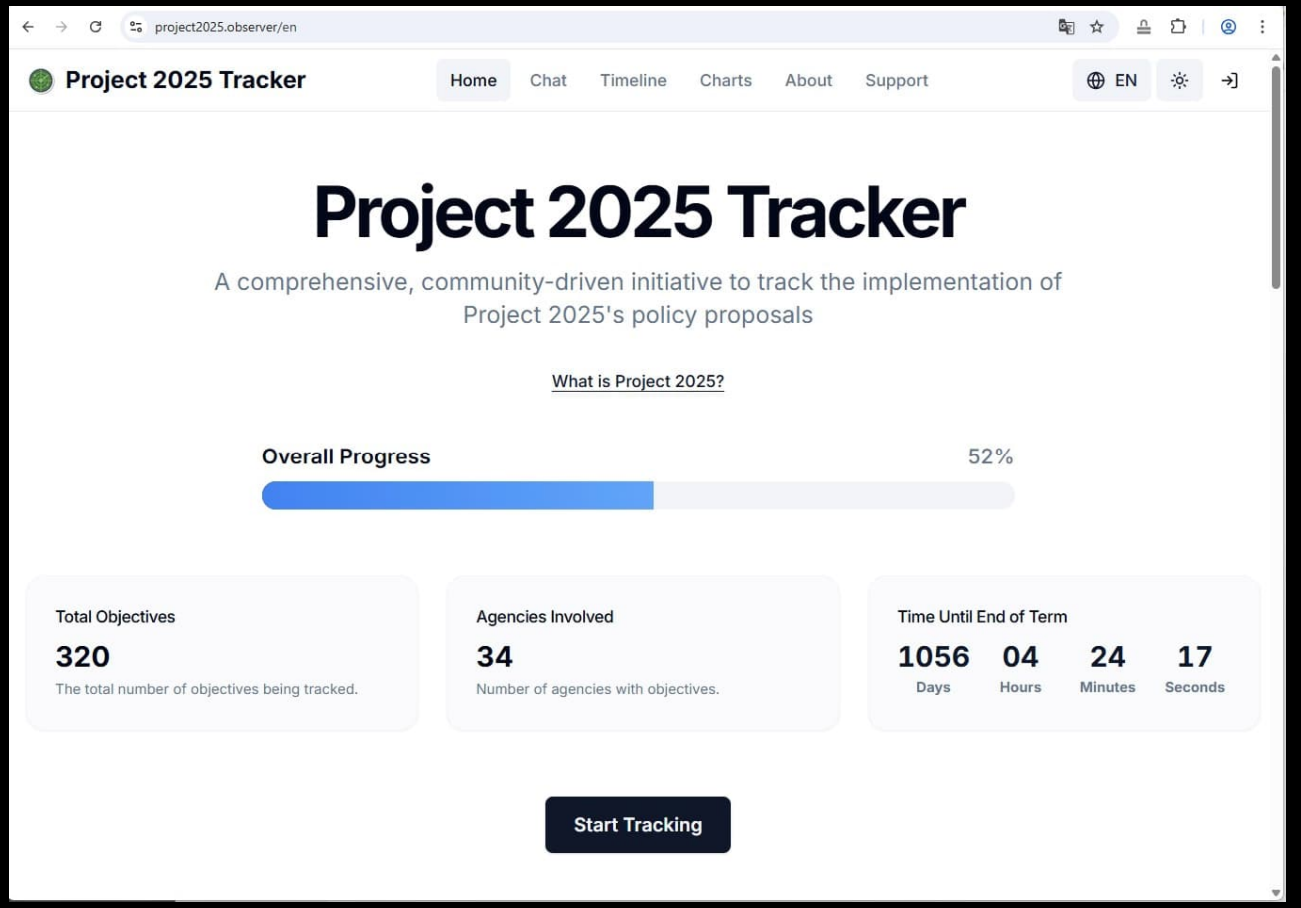
Exkurs Peter Thiel & Palantir

Thiel & Palantir: Wir gucken mal genauer

Palantir

Palantir Linkliste von HonkHase
https://atug.de/Palantir/Palantir%20Linkiste.txt

Project 2025 von der Heritage Foundation



Alex Karp: CEO Palantir

Von UK Government - Deputy Prime Minister Oliver Dowden attends AI Summit, CC BY 2.0, https://commons.wikimedia.org/w/index.php?curid=164850671

Der Endgegner: Palantir

„Städten ohne Demokratie“ sind die „Freedom Cities“ Vision von Peter Thiel

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?

XM Cyber aus Israel via Schwarz Digits

Ex-Mossad-Chef Tamir Pardo gründete ein Start-up, das Banken, Firmen und Regierungen berät. *Foto: picture alliance / dpa*

SICHERHEIT

»Tödlich wie die Atombombe«

Tamir Pardo warnt davor, das Zerstörungspotenzial von Cyberkriminellen zu unterschätzen

von Pierre Heumann

14.02.2021 11:06 Uhr

Von 2010 bis 2015 war er Direktor des Mossad.

Nach seinem Ausscheiden aus dem Geheimdienst vor fünf Jahren gründete er, zusammen mit zwei weiteren Ex-Mossad-Agenten, die Cyberfirma »XM Cyber«. Das Start-up hat eine vollautomatische Simulationsplattform für anhaltende Bedrohungen entwickelt, um Angriffe kontinuierlich aufdecken und den Handlungsbedarf lokalisieren zu können. Es zählt unter anderem Banken, Versicherungsfirmen, Flughäfen, Energiefirmen, Regierungen, Logistikfirmen und Börsen zu seinen Kunden.

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…

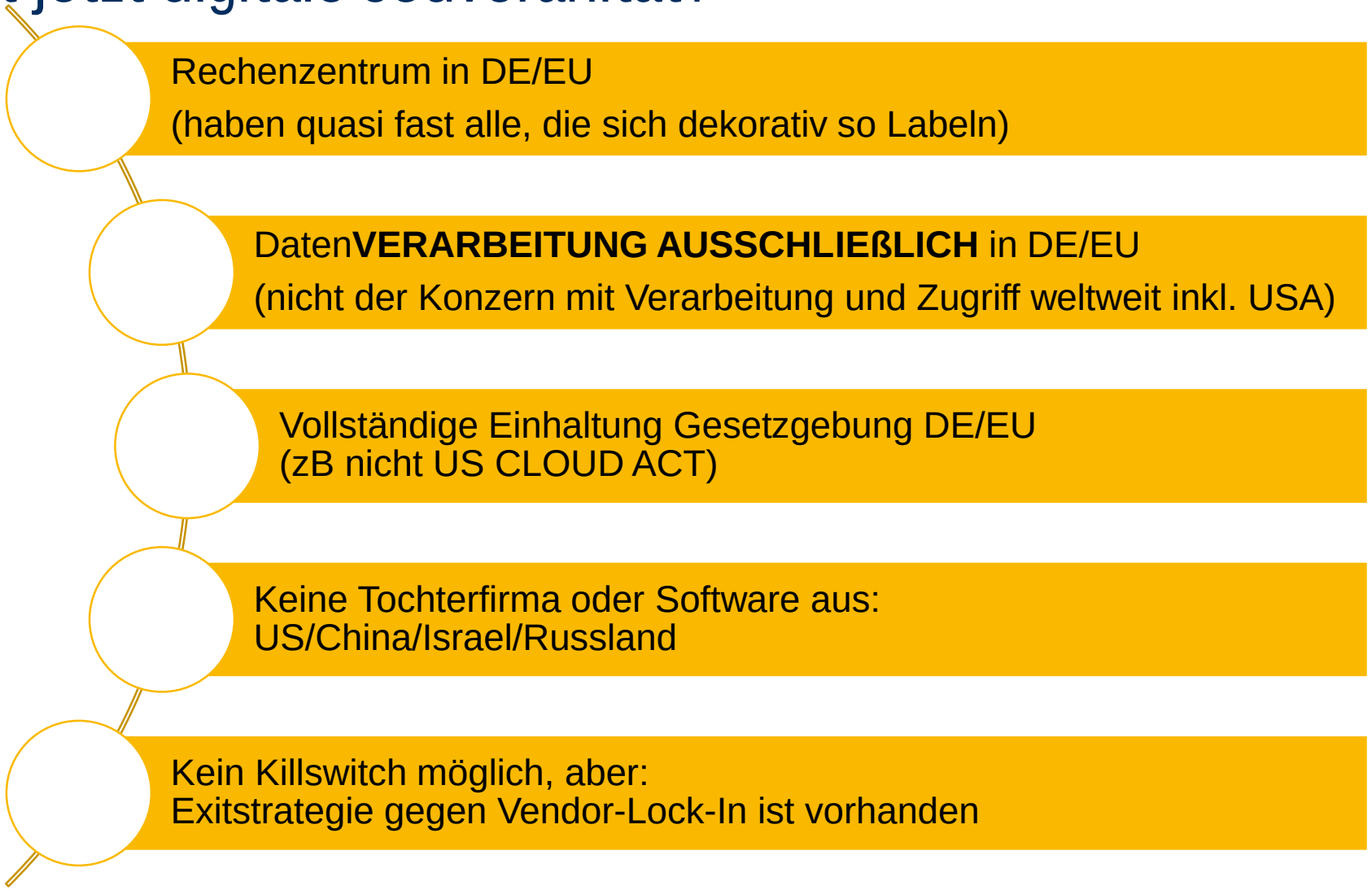
Langfriststrategie

- 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- & Chancen-management

- 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 <<

BBK Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

„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 + BCM + ITSCM und hat echte Safety & Security etabliert

Und was mache ich, wenn alles nichts hilft?

Irgendwas mit Holz?

Kokosnusspflücker!

www.kokosnusspflücker.de