DVGW Kongress 2026



Manuel ‚HonkHase' Atug



Digitale Souveränität für KRITIS-Betreiber? Und wenn ja, wie?

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 EU, Bundestag und Landtage
- 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



©left BlaBlaSecurity 2026 | @HonkHase



Verlust der digitalen Souveränität (ist auch teuer!)

©left BlaBlaSecurity 2026 | @HonkHase

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



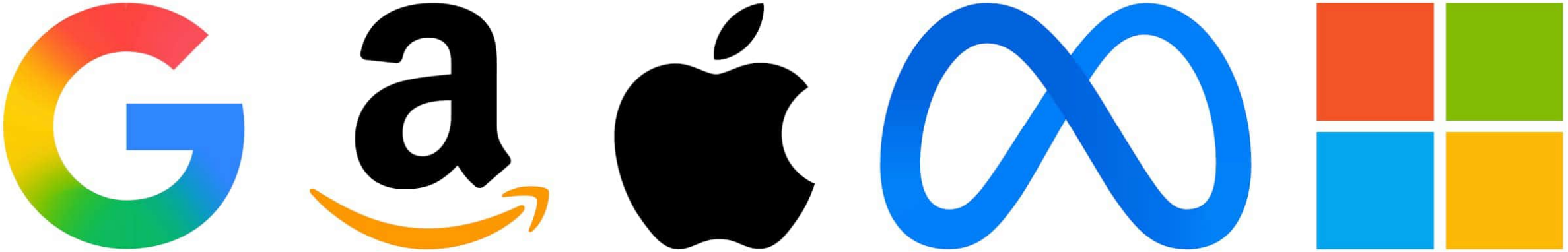
©left BlaBlaSecurity 2026 | @HonkHase

Was ist Digitale Souveränität?



©left BlaBlaSecurity 2026 | @HonkHase

Autarkie ist nicht digitale Souveränität



- Aber US Big Tech (GAFAM) ist es auch nicht

von links nach rechts:

- Alphabet (primär Google), Amazon, Meta (Facebook, Instagram, Whatsapp) Apple, Microsoft

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

©left BlaBlaSecurity 2026 | @HonkHase



Kernaspekte der digitalen Souveränität

- **Technologische Unabhängigkeit:** Vermeidung von Vendor Lock-ins
- **Datensouveränität:** Volle Kontrolle darüber, wo Daten liegen und wer Zugriff hat
- **Verarbeitungssouveränität:** Volle Kontrolle darüber, wer die Daten wie verarbeiten kann
- **Kompetenzsouveränität:** Know-How, um interne Systeme zu verstehen, zu steuern und strategische Entscheidungen wissentlich zu treffen
- **Gestaltungsfreiheit:** aus verschiedenen Lösungen die richtigen auszuwählen, zu kombinieren und an eigene Anforderungen anzupassen
- **Kostensouveränität** → Kostenkontrollmöglichkeiten

©left BlaBlaSecurity 2026 | @HonkHase

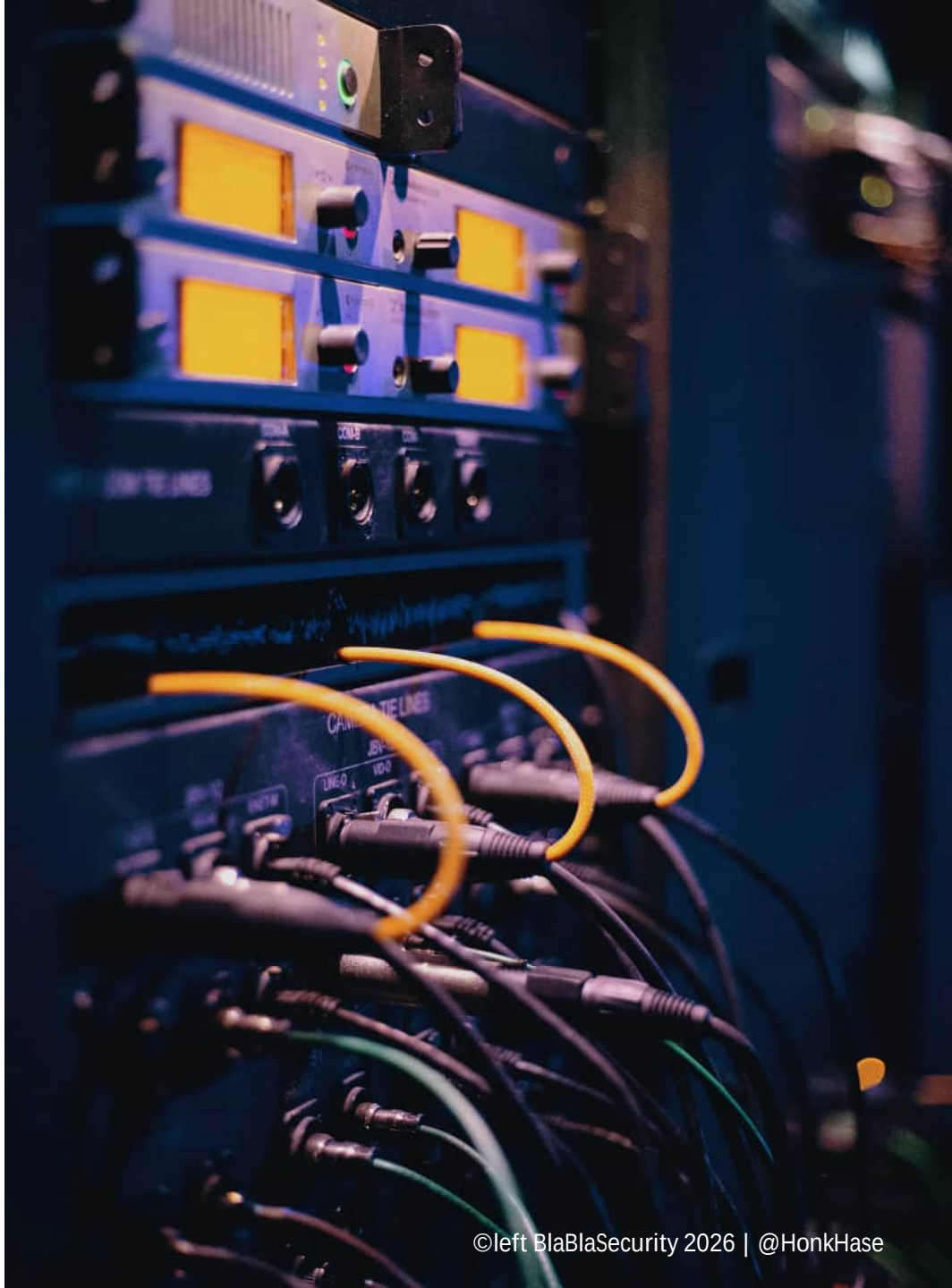
„Wer digitale Souveränität will, findet Lösungen
Wer digitale Souveränität nicht will, findet Ausreden“

©left BlaBlaSecurity 2026 | @HonkHase

Entscheidende Faktoren für selbstbestimmte IT

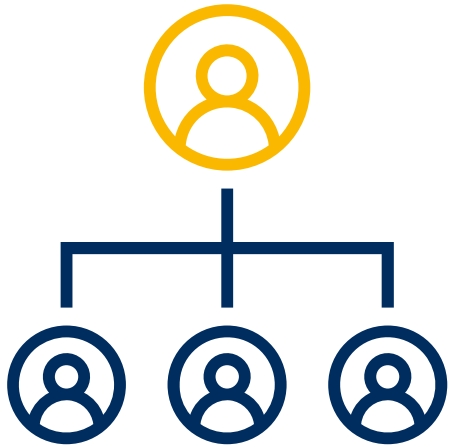
Ziel: unabhängiger von einzelnen Anbietenden und Produkten werden und ihre Resilienz durch die Austauschbarkeit von Komponenten zu erhöhen

- Insbesondere Alternativen schaffen/nutzen und einen offenen, wettbewerbsfähigen Markt unterstützen und gestalten
- Offene und freie Standards
- Interoperabilität
- Open Source für Transparenz und Unabhängigkeit
- Exit-Strategien in neuen IT-Verträgen
- Modularität
- Kostenkontrolle & Kostensouveränität



©left BlaBlaSecurity 2026 | @HonkHase

Wer Cybersicherheit weiterhin als rein technisches Thema der IT-Abteilung behandelt, handelt fahrlässig



Geschäfts- und

Behördenleitung

steuert, *delegiert,*

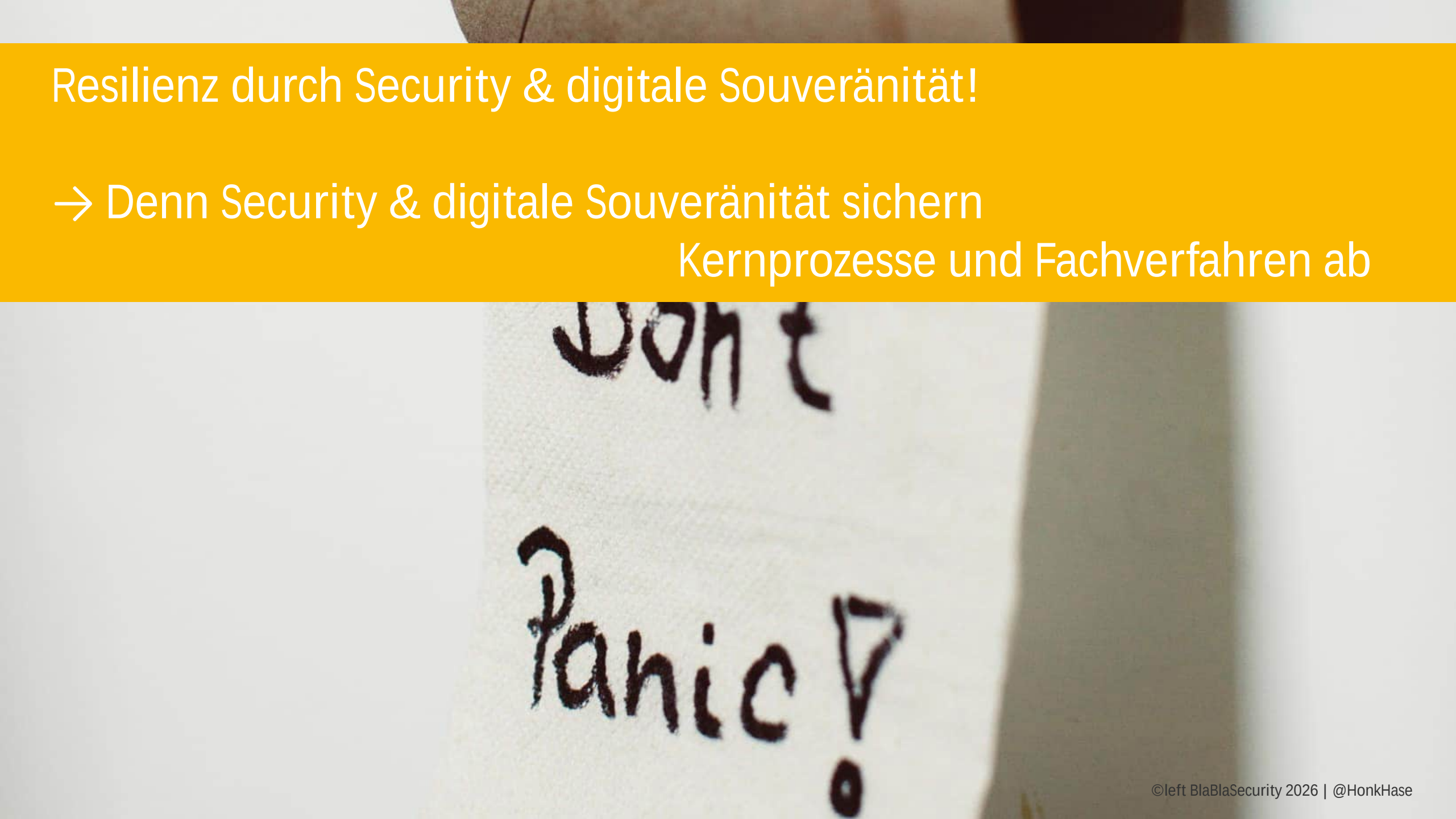
überwacht und *kontrolliert*

1. Paper Compliance
2. Prozessgestaltung & -implementierung
3. Prozessüberprüfung (Vollständigkeit)
4. Wirksamkeitsprüfung (aller Prozesse)

©left BlaBlaSecurity 2026 | @HonkHase

Resilienz durch Security & digitale Souveränität!

→ Denn Security & digitale Souveränität sichern
Kernprozesse und Fachverfahren ab



©left BlaBlaSecurity 2026 | @HonkHase

Und was mache ich, wenn alles nichts hilft?



©left BlaBlaSecurity 2026 | @HonkHase

Irgendwas mit Holz?

Kokosnusspflücker!

www.kokosnusspflücker.de



©left BlaBlaSecurity 2026 | @HonkHase