

Verband kommunaler Unternehmen e.V.

Manuel ‚HonkHase' Atug



Bedrohungslage für die Daseinsvorsorge: Angriffe auf kritische Infrastrukturen

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



Angriffe auf kritische Infrastrukturen

Bedrohungslage für die Daseinsvorsorge



Naturereignisse

Naturkatastrophen, gesundheitliche Notlagen wie etwa Pandemien



Vorsatzhandlungen

hybride Bedrohungen oder andere feindliche Bedrohungen, einschließlich terroristischer Straftaten, krimineller Unterwanderung und Sabotage



Unfälle

Plötzliches, zeitlich und örtlich bestimmbares und von außen einwirkendes Ereignis, bei dem eine natürliche Person unfreiwillig einen Körperschaden erleidet (Personenschaden) oder eine Sache unbeabsichtigt beschädigt wird (Sachschaden)

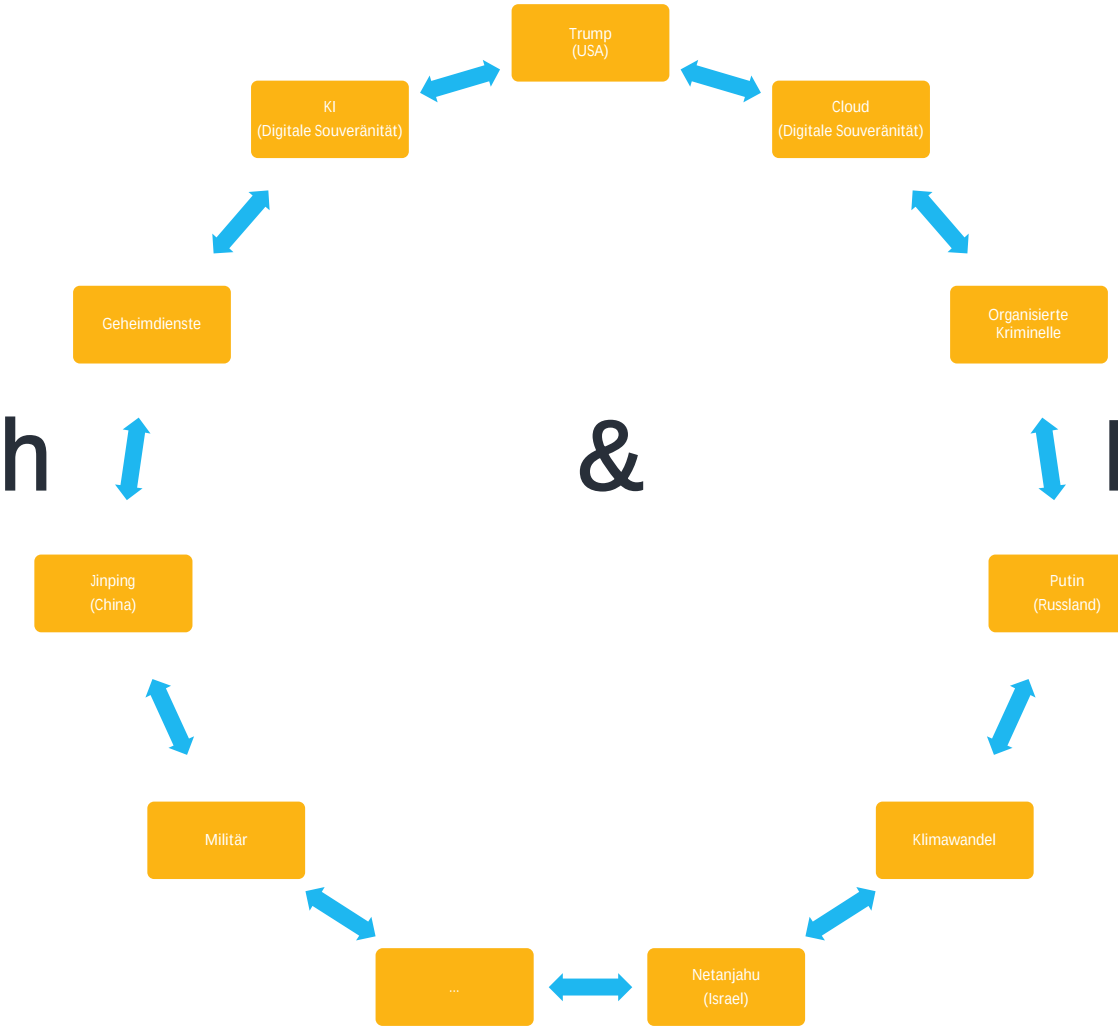


Cybervorfälle

„erheblicher Sicherheitsvorfall“ bewirkt schwerwiegende Betriebsstörungen ,finanzielle Verluste, oder beeinträchtigt andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden

©left BlaBlaSecurity 2026 | @HonkHase

Cyberbedrohungslage: Schutz vor was und wem?



Machtmissbrauch & Erlösmaximierung

©left BlaBlaSecurity 2026 | @HonkHase

Was ist Verschlusssache / Geheimschutz?



©left BlaBlaSecurity 2026 | @HonkHase

Staatlicher Geheimschutz /Verschlusssache:
„Der Schutz von Verschlusssachen dient der inneren Sicherheit“

4 Stufen der Verschlusssache

- STRENG GEHEIM
- GEHEIM
- VS-VERTRAULICH
- VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)

4 wesentliche Vorgaben

- Grundsatz „Kenntnis nur, wenn nötig“, also für Aufgabenerfüllung erforderlich
- persönliche Verantwortung für vorschriftsmäßige Behandlung von Verschlusssachen
- Die Einstufung bleibt, auch nach unrechtmäßigem bekannt werden (wie bei einem Leak)
- Belehrung / Verpflichtung bei VS-NfD | Sicherheitsüberprüfung (SÜ2 / SÜ3) bei den höheren Stufen

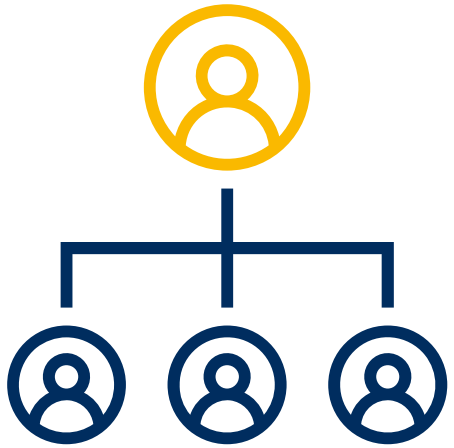
©left BlaBlaSecurity 2026 | @HonkHase



Wat nu?



Wer Cybersicherheit weiterhin als rein technisches Thema der IT-Abteilung behandelt, handelt nicht nur fahrlässig, sondern rechtswidrig



Geschäfts- und

Behördenleitungen

steuern, *delegieren,*

überwachen und *kontrollieren*

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 das Business 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