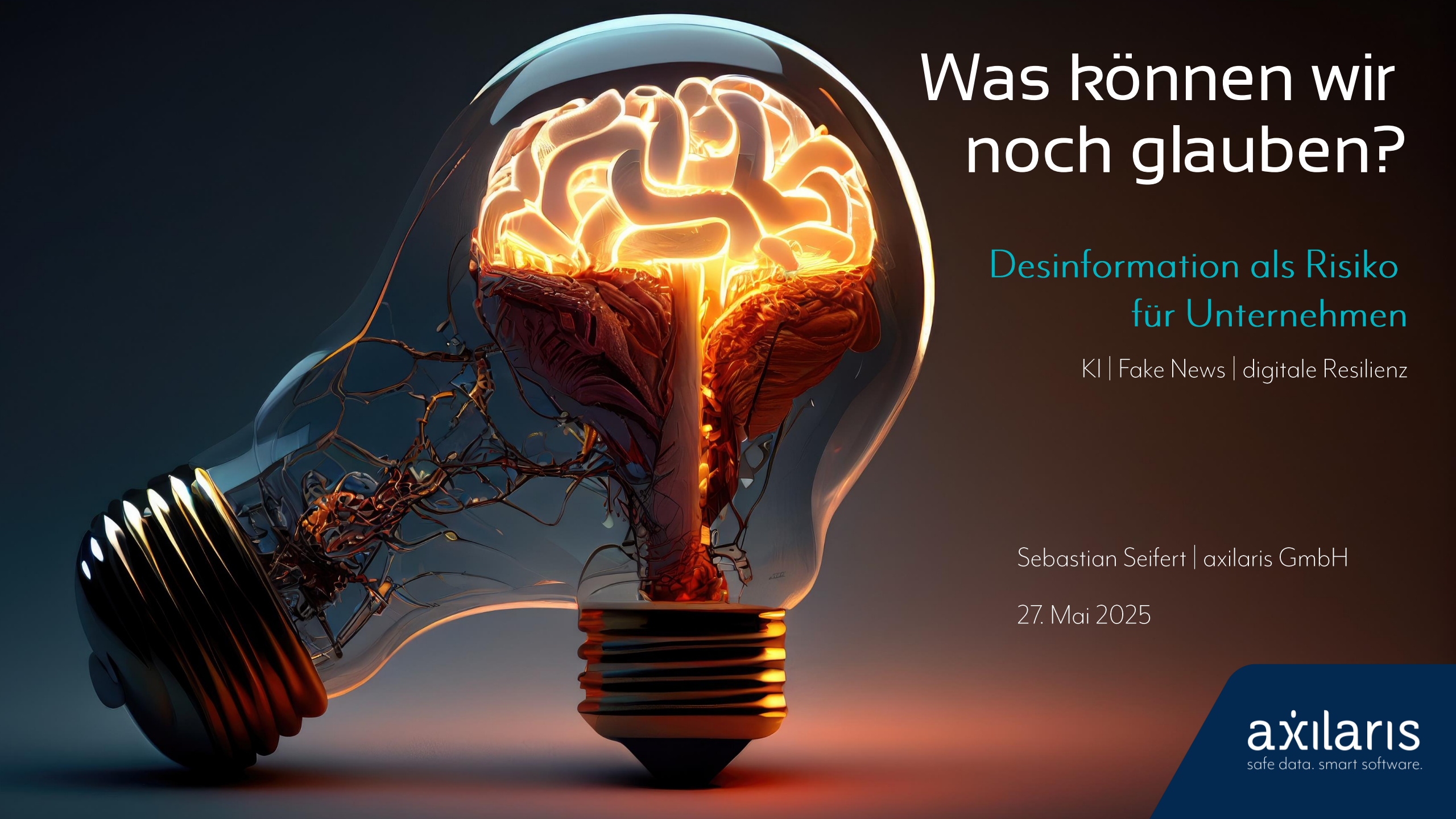


Was können wir noch glauben?

Desinformation als Risiko für Unternehmen

KI | Fake News | digitale Resilienz

Sebastian Seifert | axilaris GmbH

27. Mai 2025

axilaris
safe data. smart software.

axilaris
safe data. smart software.

Was ist Desinformation?

- Bewusste Täuschung durch falsche Informationen
- Verstärkt durch KI-generierte Texte, Bilder, Videos
- Automatisierte Verbreitung über Bots und soziale Medien
- Ziel: Manipulation, Destabilisierung von Unternehmen

axilaris
safe data. smart software.

Angriffsvektoren

axilaris
safe data. smart software.

Typische Desinformations-formen in Unternehmen

- Visuelle Fakes: CEO-Deepfakes, gefälschte Katastrophenbilder
- Textfakes: Pressemitteilungen, interne Memos
- Fake-Webseiten und Social Accounts
- Pishing Webseiten und E-Mails

axilaris
safe data. smart software.

Auswirkungen auf Unternehmen

1. Reputationsschäden

- Gefälschte Inhalte untergraben das **Vertrauen von Kunden, Partnern und Medien**
- Medien übernehmen unkritisch Informationen ⟶ **Multiplikation der Desinformation**
- Reputationskrisen verbreiten sich in **Minuten**, Wiederherstellung dauert Monate bis Jahre

Auswirkungen auf Unternehmen

2. Finanzielle Risiken

- **Aktienkursverluste** durch gefälschte CEO-Aussagen oder Krisengerüchte
- Kunden- und Investorenabwanderung aufgrund von Unsicherheit
- **Vertragskündigungen** bei Kooperationspartnern durch Reputationsverlust

Auswirkungen auf Unternehmen

3. Interne Auswirkungen

- **Verunsicherung der Mitarbeitenden** durch gefälschte E-Mails, interne „Memos“, Entlassungsgerüchte
- **Produktivitätsausfälle** durch interne Krisenkommunikation und Aufklärungsarbeit
- **Vertrauensverlust** in die interne Führung – demotivierend

Auswirkungen auf Unternehmen

4. Erhöhtes Cybersecurity-Risiko

- **CEO-Fraud durch Deepfakes**: realistisch wirkende Audio- oder Videoanweisungen
- **Phishing und Social Engineering** mit KI-Texten oder gefälschten Websites
- Desinformation wird als **Türöffner für Angriffe** auf Systeme oder Menschen genutzt

Global Risk Report 2024:

1. Desinformation als Risiko-Multiplikator
2. Unternehmen im Fadenkreuz
3. kritischer Faktor: Geschwindigkeit

Die Gefahr ist real - Beispiele

Ferrari: CEO-Stimme täuschend echt imitiert

Hongkonger Bank: 22,6 Mio. Euro durch Deepfake-Video verloren

Multinationaler Konzern: 25 Mio. USD durch Deepfake-Videokonferenz verloren

Technologische Abwehrmöglichkeiten

- **Media Monitoring**: Meltwater, NewsWhip, Talkwalker
- **Deepfake Detection**: Microsoft Video Authenticator, Hive, Deepware
- **Content-Wasserzeichen** (C2PA-Standard)
- **Signierte Inhalte** & klare Herkunftsnachweise

Imperceptible digital watermark embedded at the point of capture

Digitally watermarked content

axilaris
safe data. smart software.

Mitarbeitende als Schutzschild

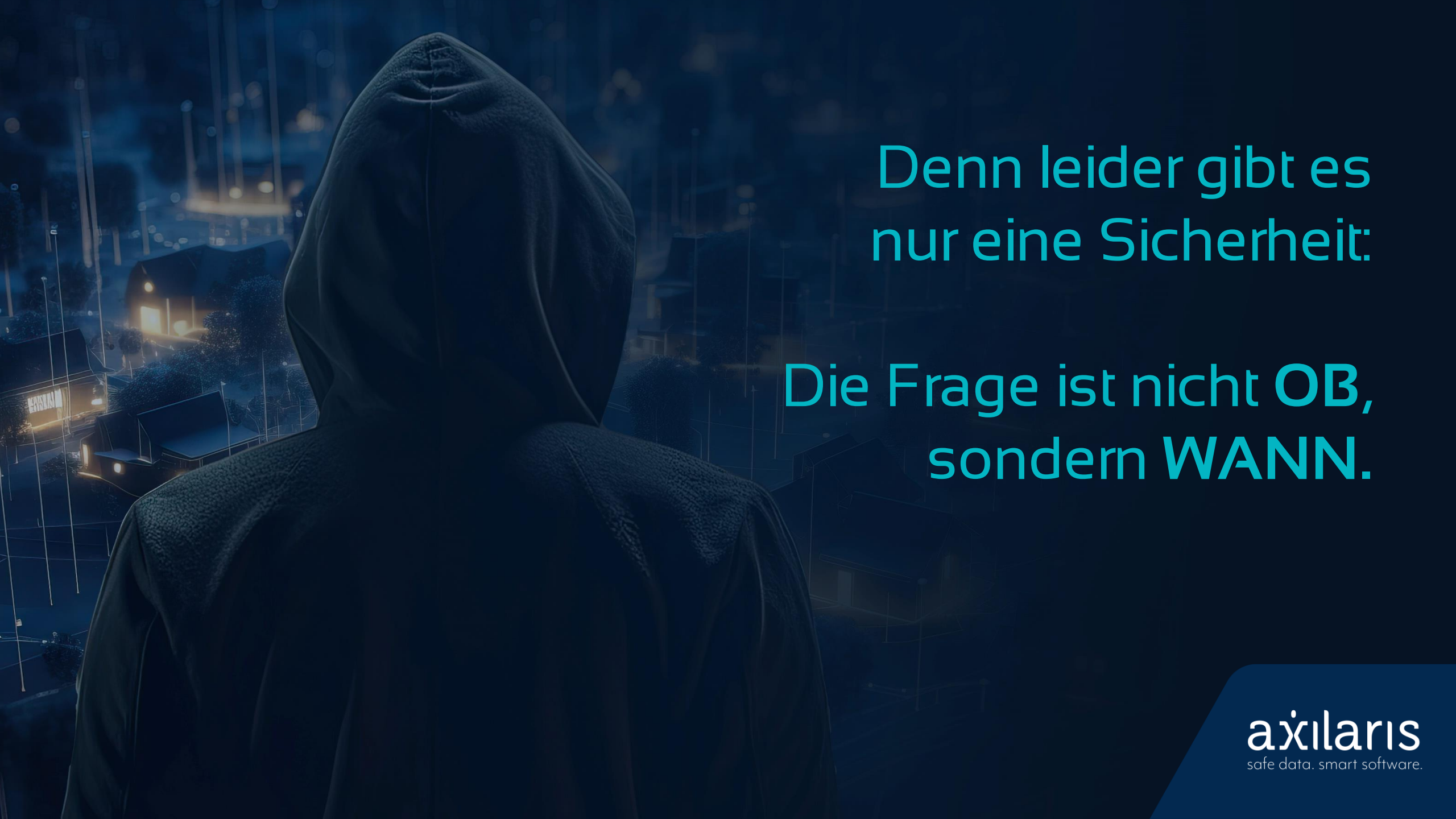
- Schulungen für Social Engineering & Medienkompetenz
- Warnsysteme und interne Meldekanäle
- Transparenz: Gerüchte schnell und glaubwürdig entkräften
- Führungskräfte aktiv einbinden

Kooperatives Vorgehen

- Zusammenarbeit mit:
  - Behörden & CERTs
  - Branchenverbänden
  - Tech-Partnern (z. B. Cloudanbieter mit KI-Schutzfunktionen)
- Beteiligung an **Brancheninitiativen gegen Desinformation**

Fazit: 5 Empfehlungen

- Risiko ernst nehmen – nicht abwarten
- Monitoring & Frühwarnsysteme aufbauen
- Mitarbeitende qualifizieren
- Kommunikation vorbereiten & trainieren
- Netzwerk & Partnerschaften stärken



Denn leider gibt es
nur eine Sicherheit:

Die Frage ist nicht **OB**,
sondern **WANN.**

axilaris
safe data. smart software.

axilaris
safe data. smart software.

Gemeinsam für mehr IT-Sicherheit

www.axilaris.de

vertrieb@axilaris.de

0371 30 80 80 80

axilaris
safe data. smart software.