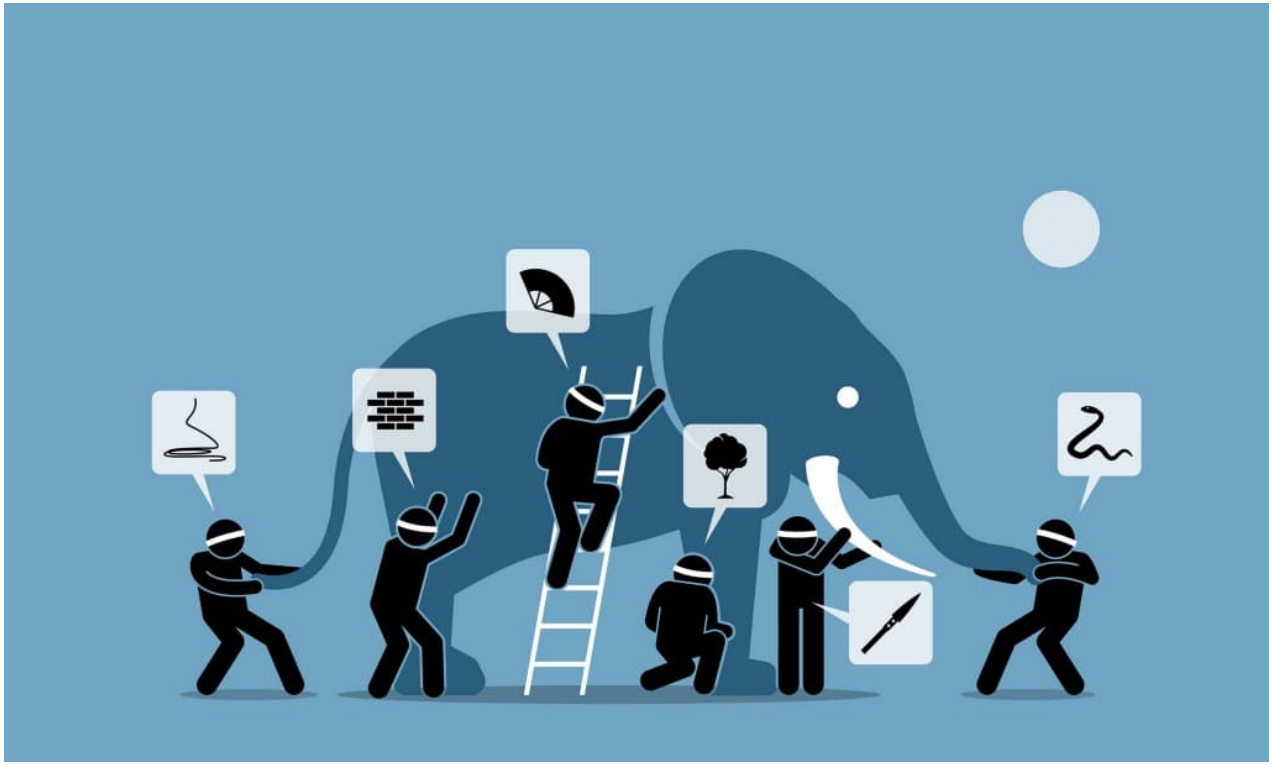
Technische Hochschule
Brandenburg
University of
Applied Sciences
Fachbereich
Wirtschaft

Security Governance als Führungsaufgabe – für Konzerne, Mittelstand und Kleinunternehmen

18. Security Forum der Technischen Hochschule Brandenburg, 15.01.2026



Haben Sie in Ihrem Unternehmen oder in Ihrer Institution eine integrierte Sicht auf Sicherheit – oder sehen Sie einzelne Teile wie die blinden Männer bei dem Elefanten?



Security Governance sorgt dafür, dass aus Fragmenten ein ganzheitliches Sicherheitskonzept wird.

Security Governance als Führungsaufgabe

- Verantwortung liegt bei Vorstand & Geschäftsführung
- Tone from the Top prägt die Sicherheitskultur
- Klare Entscheidungsprozesse für Transparenz und Risikoakzeptanz
- Strategische Integration externer Vorgaben

Architektur: Security Governance – Prozesse – Risiko

Security Governance-Ebene

Security Governance definiert strategische Sicherheitsziele, Verantwortlichkeiten und den Risk Appetite.

Prozessebene und ISMS

Security Prozesse übersetzen Governance in operative Maßnahmen wie ACP, Incident- und Continuity-Management. Geschäftsprozesse schaffen Transparenz über Vermögensgüter.

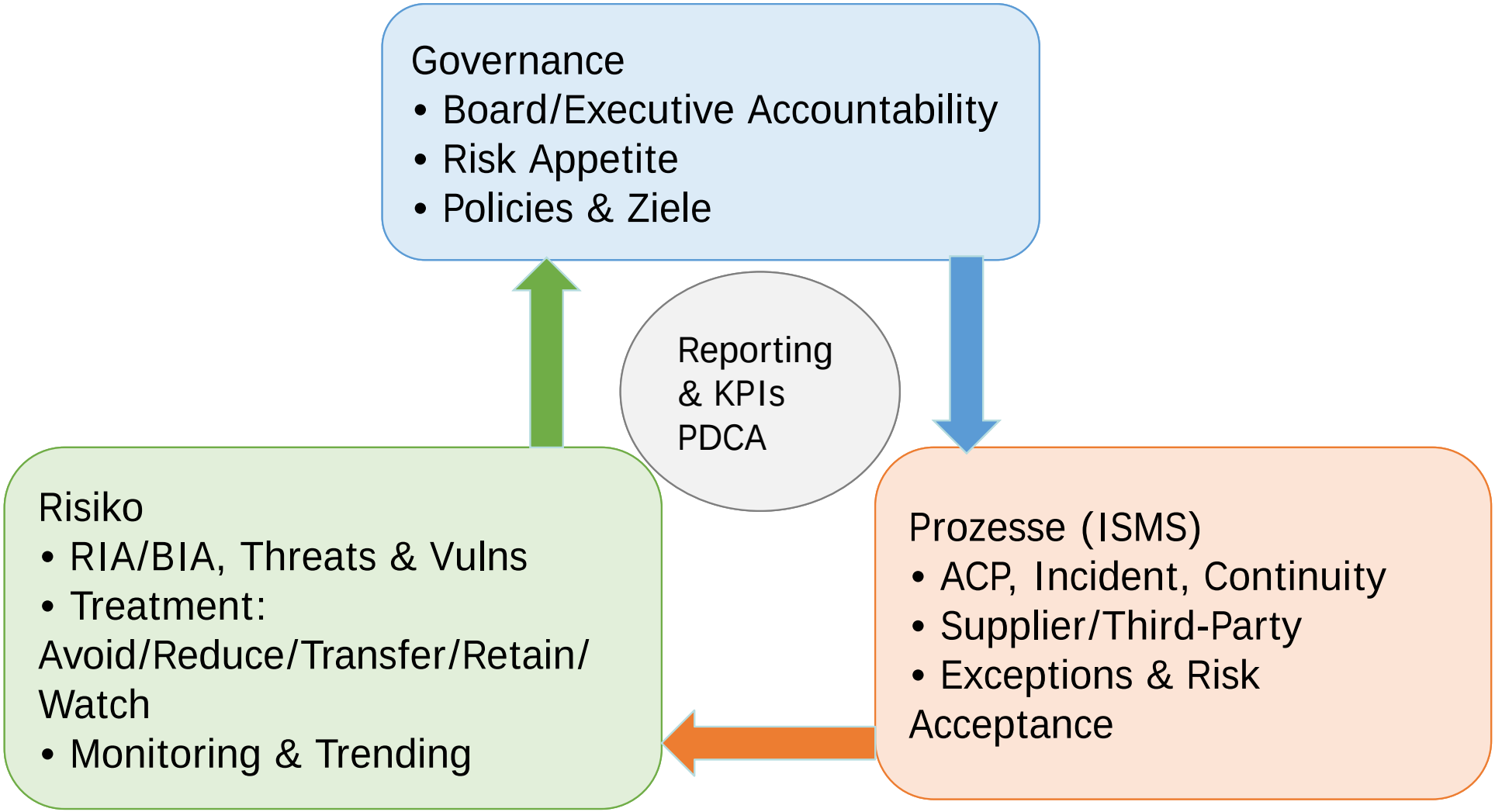
Risikomanagement

Risikomanagement nutzt RIA und BIA und priorisiert und legitimiert Entscheidungen.

Kontinuierliche Verbesserung

Reporting und PDCA steuern.

Zusammenhang: Governance – Prozesse – Risiko



Kontext: Business-Strategie, Regulierung (z. B. NIS2, CRA), Geopolitik

Quelle: Saatmann, 2026

Technische Hochschule
Brandenburg
University of
Applied Sciences
Fachbereich
Wirtschaft

Wie ist die Lage?

Allianz Risk Barometer 2026

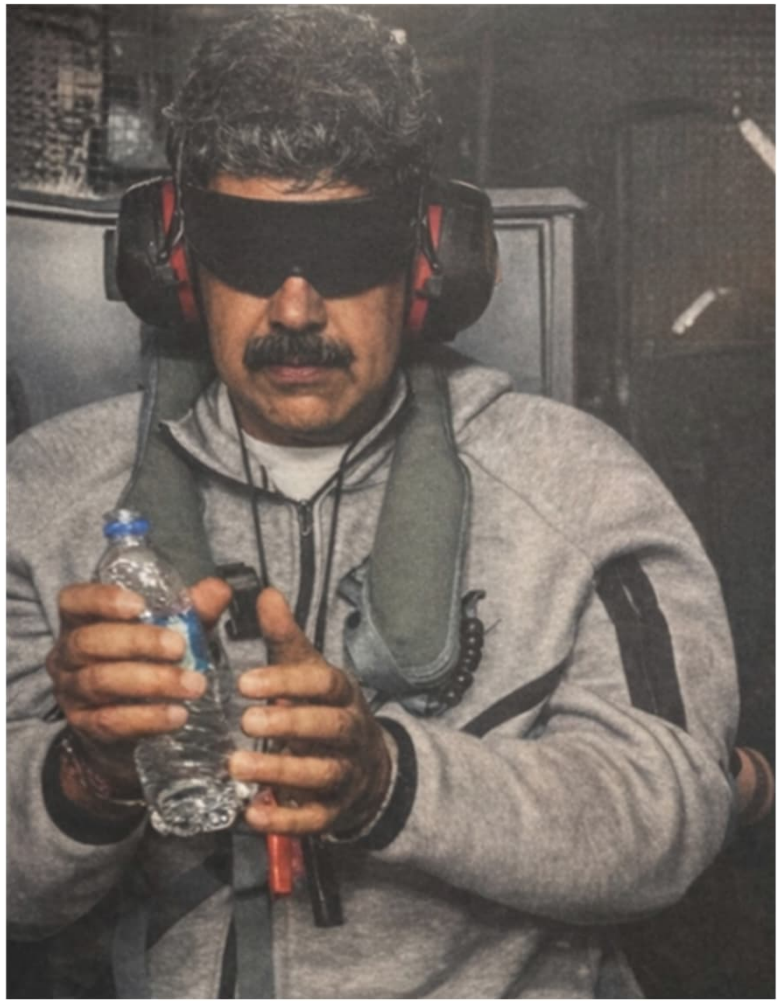
Quelle: Allianz, 2026

Allianz Risk Barometer 2026

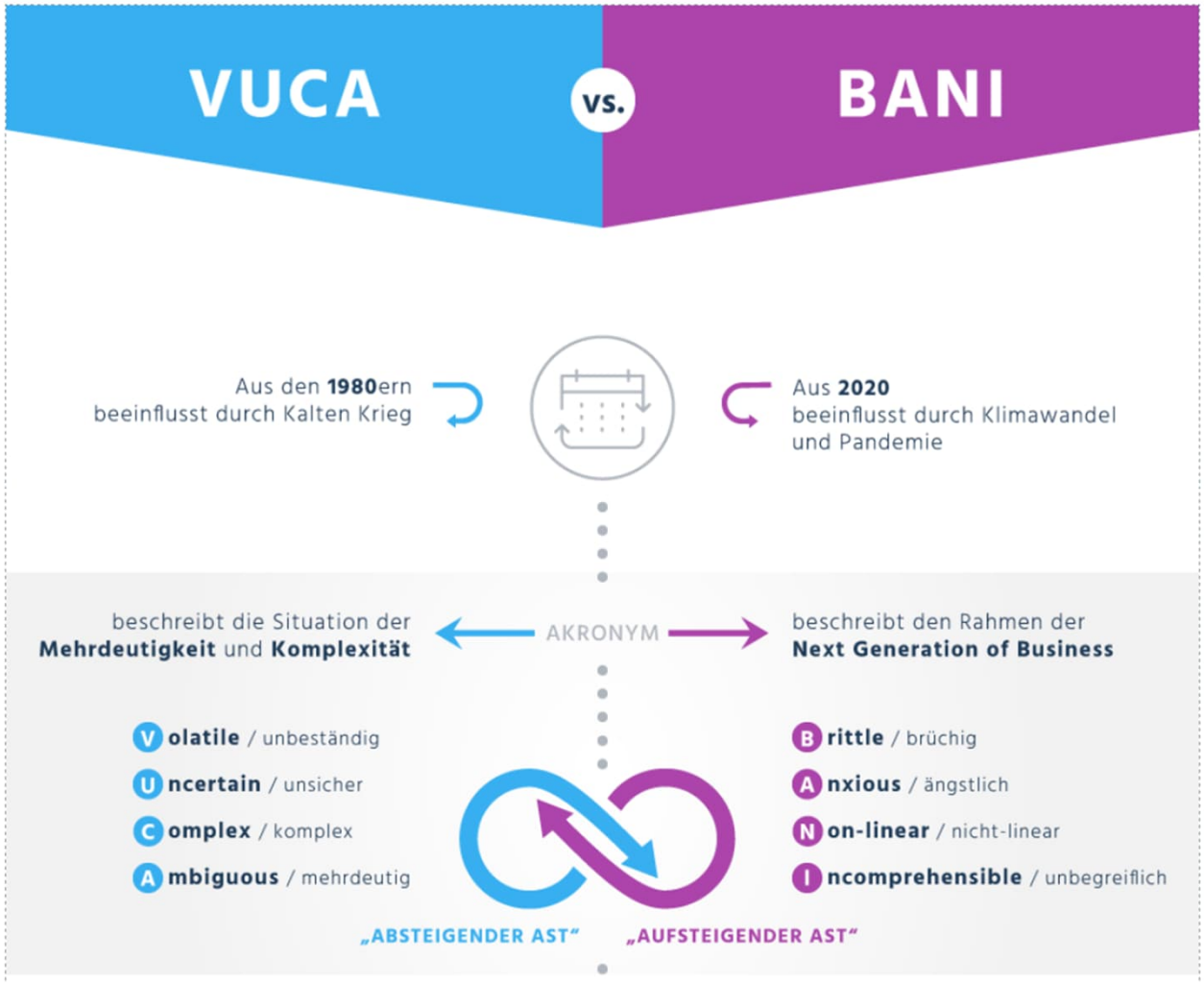
- Cyber incidents is the top global risk for 2026 – 10% ahead of AI
- Cyber incidents ranks #1 the fifth year in a row. A decade ago, it ranked only #8.
- It is the top risk across all company sizes (large, mid-sized and small).

Quelle: Allianz, 2026

Der sicherheitspolitische Start ins neue Jahr 2026.

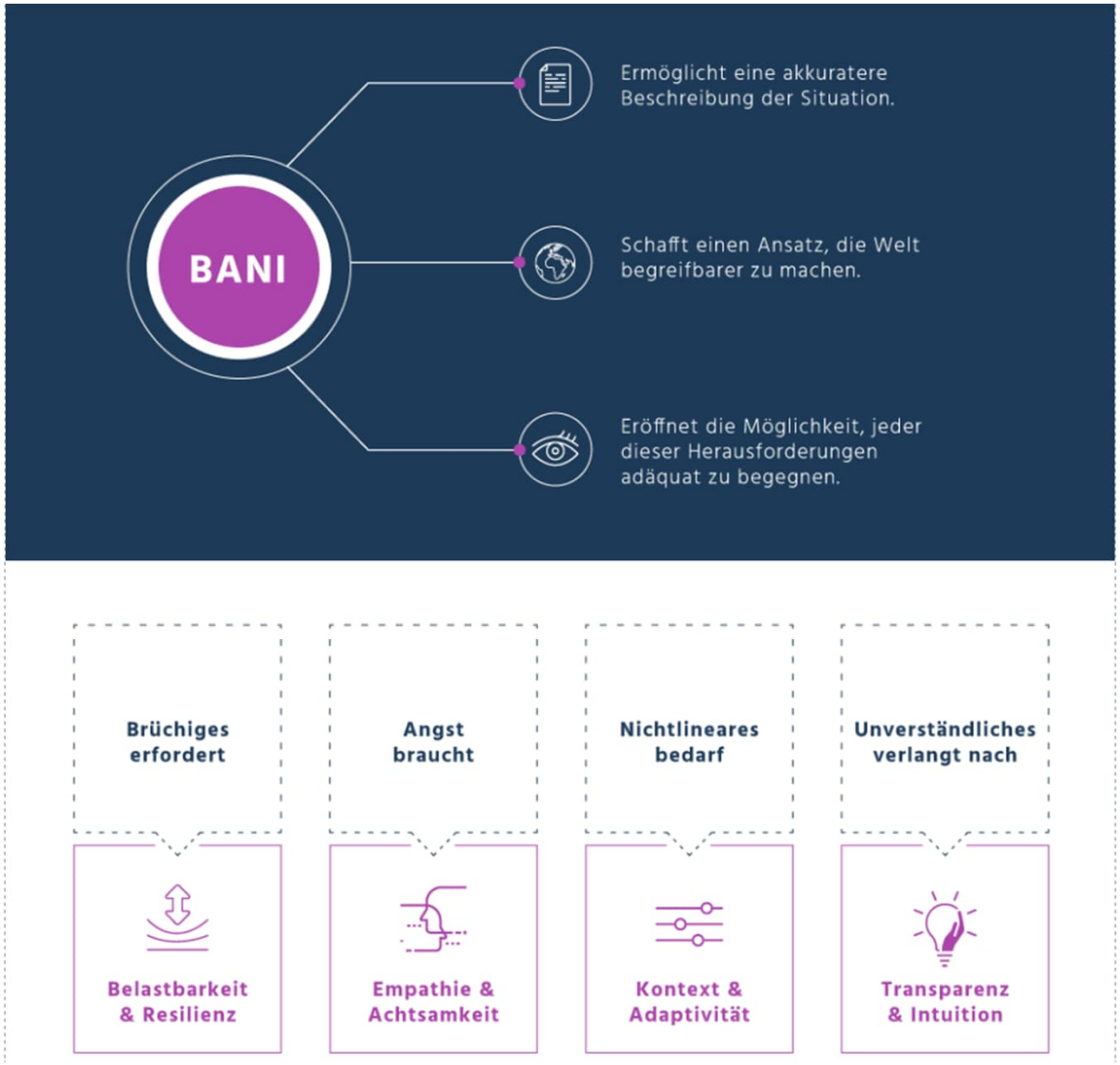


Frameworks helfen als Grundannahme der Security Governance
VUCA- wird zur BANI-Welt



https://www.resilienz-akademie.com

VUCA-Welt wird zur BANI-Welt



https://www.resilienz-akademie.com

Technische Hochschule
Brandenburg
University of
Applied Sciences
Fachbereich
Wirtschaft

Wie erfolgt die Umsetzung in Unternehmen?

Security Governance als Führungsaufgabe – Überblick über die Umsetzung

Aspekt	Konzerne	Mittelstand	Kleinunternehmen
Strategische Ebene	Vorstandsebene, CISO, Governance Board	Geschäftsführung + IT-Leitung	Inhaber oder externe IT-Dienstleister
Führungsrahmen /Standards	ISO/IEC 27014, NIST CSF, COBIT	ISO/IEC 27001 (vereinfachte Umsetzung), BSI IT-Grundschutz	BSI Basisabsicherung, ENISA SME Guidelines
Rollen & Verantwortl.	Klare Rollen: CISO, Risk Officer, Compliance	Wenige Rollen, oft kombiniert (IT + Security)	Meist keine dedizierte Rolle, „One-Man-Show“
Prozesse	Formelle Governance-Prozesse, KPIs, Audits	Teilweise formalisiert, oft projektbezogen	Ad-hoc, stark abhängig von Awareness
Budget & Ressourcen	Hohe Budgets, dedizierte Teams	Begrenzte Budgets, externe Beratung	Minimal, Fokus auf kostengünstige Lösungen
Risikoansatz	Risikomanagement integriert in Unternehmensstrategie	Risikoanalyse punktuell, oft reaktiv	Fokus auf Basis-Schutz, kaum strategisch

Quelle: Saatmann, 2026

Cybersecurity im Mittelstand – Lage 2025

80 % aller gemeldeten Vorfälle betreffen KMU (BSI-Lagebericht 2025)

KMU sehen Cybersecurity als größte Herausforderung – vor Energiepreisen und Bürokratie (it-sa Barometer)

Hauptprobleme:

- Veraltete Systeme, fehlende Backups
- Mangelnde Awareness & fehlende Notfallpläne
- IT-Sicherheit oft nicht strategisch verankert

Bedrohungen: Phishing, Malware, gestohlene Zugangsdaten, Lieferkettenangriffe

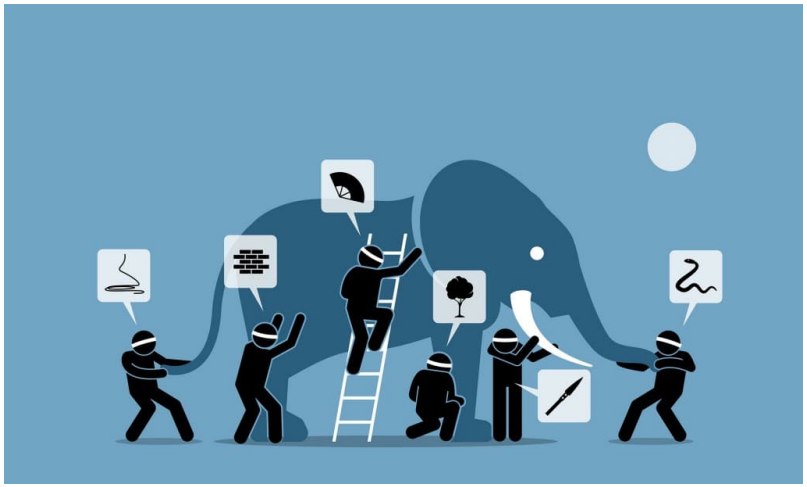
Folgen: Hohe Schadenssummen, Insolvenzrisiko bei fehlendem Business Continuity Management

Handlungsbedarf:

- Regelmäßige Updates & Schulungen
- Backup-Strategie & Notfallpläne
- Nutzung von BSI-Leitfäden & Förderprogrammen
- Resilienz umfasst Prävention, Verteidigung und Bewältigung
- Cyberrisko-Check des BSI

Quelle: BSI, 2025

Governance entscheidet – Prozesse setzen um – Risiko priorisiert
Diskutieren Sie mit uns – Wie verankern Sie Security Governance in ihrem Unternehmen?



Security Governance als Steuerungshebel

Security Governance definiert strategische Steuerung und Verantwortlichkeit für wirksame Informationssicherheit.

Klare Entscheidungsrechte

Unklare Verantwortlichkeiten führen zu ineffizienten Prozessen und Sicherheitsvorfällen trotz technischer Investitionen.

Security Governance als Führungsaufgabe

Security Governance ist keine IT-Aufgabe, sondern ein Führungsprozess, der Sicherheitsziele in der Unternehmensstrategie verankert.

Konfliktlösung und Resilienz

Security Governance ermöglicht strategische Lösung von Zielkonflikten und stärkt die Organisation gegen Bedrohungen.

Technische Hochschule
Brandenburg
University of
Applied Sciences
Fachbereich
Wirtschaft

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Stefan Saatmann
(Lehrbeauftragter an der THB seit WS 2020)

stefan.saatmann@th-brandenburg.de

Technische Hochschule Brandenburg
University of Applied Sciences
Fachbereich Wirtschaft
Magdeburger Straße 50
14770 Brandenburg an der Havel

www.th-brandenburg.de/wirtschaft