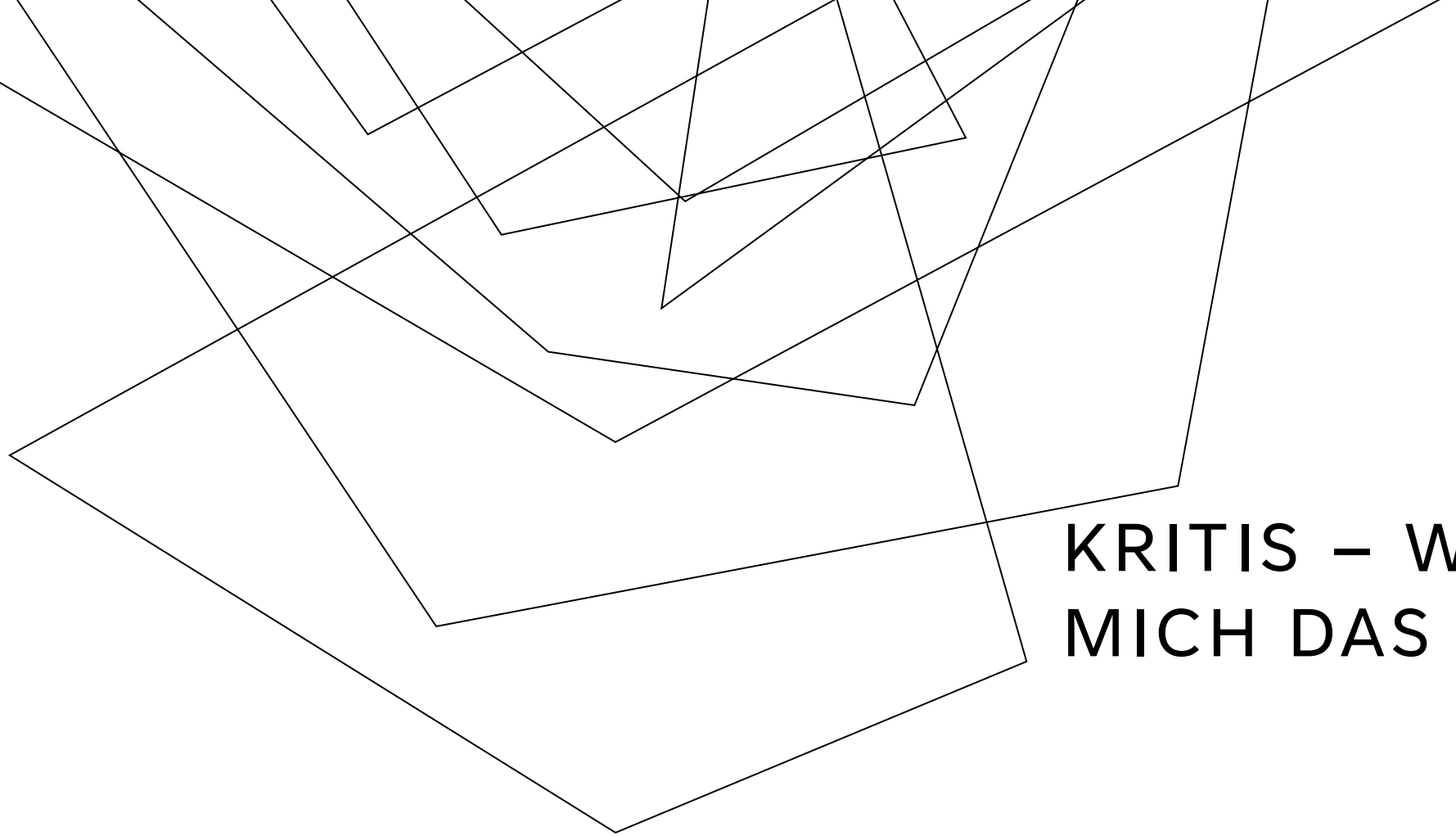


KRITIS – WAS GEHT MICH DAS AN?

SECUDA

ÜBER DIE SECUDA

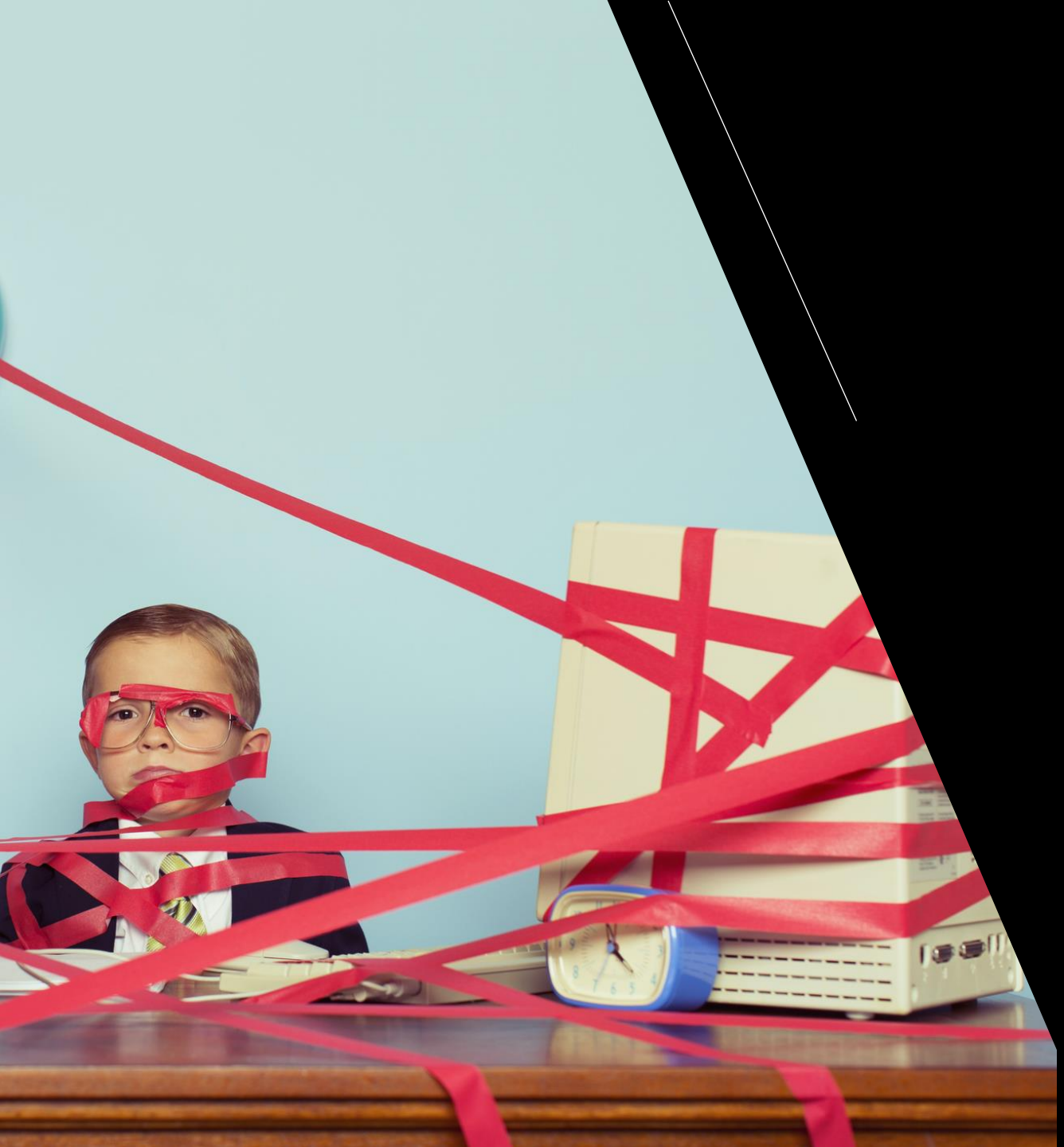
- gegründet 2018
- Beratung im Bereich Datensicherheit – A wie Auftragsverarbeitung bis Z wie Zero Trust
- Kundenprofil: KMU + KRITIS-Projekte im Bereich Gesundheitswesen, Energie, Finanzen und Verwaltung
- 6 interne + 3 externe Mitarbeiter
- Teilnehmer Allianz für Cybersicherheit
- https://www.secuda.de

DARIAN THANNHÄUSER

- Est. 1984
- Geschäftsführung/Gesellschafter Secuda GmbH
- seit 2010 im Bereich IT-Security und Datenschutzberatung tätig
- Ex-Wirtschaftsprüfer-Anwärter
- Datenschutzaktivist

ALEXANDER GERBER

- Est. 1971
- Gründer, Inhaber, Vorstand, Aufsichtsrat, Genosse … externer Unterstützer
- Jurist und leidenschaftlicher Erklärbär
- Zertifizierter Auditor ISO27001
- Interessenschwerpunkt: Infrastruktur & Betrieb



UND WER BIST DU?

AGENDA

- Einführung in KRITIS/NIS-2
- Woher weiß ich, wann ich KRITIS/NIS-2 bin?
- Was bedeutet „KRITIS-nah“?
- Exkurs: ISO27001

EINFÜHRUNG IN KRITIS/NIS-2

WAS IST KRITIS?

KRITIS (Kritische Infrastrukturen) = Sektoreneinteilung gesellschaftlich relevanter Dienste (gem. Bund-Länder-AG)

BSIG, §2, Abs. 10, Nr. 1:

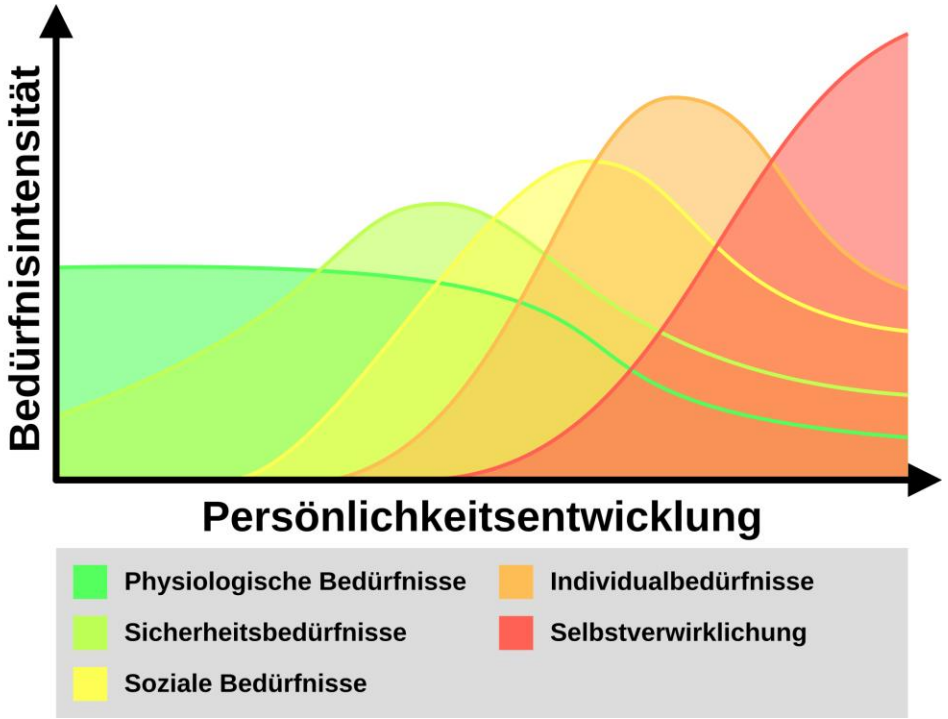
- Finanzwesen
- Transport
- Energie
- Ernährung
- Wasser
- Gesundheit
- Abfallentsorgung
- **Informationstechnik und Telekommunikation**

Nr. 2: hohe Bedeutung für das Funktionieren des Gemeinwesens

- (öffentliche) Verwaltung
- Kultur und Medien

→ KRITIS-Verordnung (“KritisV") §§ 2 bis 9

THE "BIG PICTURE"



	Ebene	Sektor
5	Selbstverwirklichung	Bildung
4	Anerkennung	Kultur
3	Beziehungen	Medien
2	Sicherheit	"Law Enforcement"
1	Physiologie	Ver- und Entsorgung

NIS-1 (EU) → BSIG (Bund) → KRITIS

NIS-2 (EU) → BSIG (Bund) → KRITIS

RELEVANTE NORMEN

Deutschland:

BSIG - Gesetz über das Bundesamt für Sicherheit in der Informationstechnik

BSI-KritisV - Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz

EU:

NIS-1 - Network and Information Security Directive (1)

NIS-2 - Network and Information Security Directive (2)

WAS IST NIS-2?

NIS-2 (Network and Information Systems Directive 2) = EU-Verordnung

Ziele:

- Erweiterung des Anwendungsbereichs auch auf kleinere und mittlere Unternehmen (KMU).
- Erhöhung der Sicherheitsanforderungen und Anforderungen an das Risikomanagement.
- Verbesserte Zusammenarbeit und Informationsaustausch zwischen den Mitgliedstaaten und der EU.
- Schutz kritischer Infrastrukturen.
- Verbesserung der Cyber-Sicherheit in Unternehmen.

WAS IST NIS-2?

Wichtige Elemente:

- Verpflichtende Risikomanagementmaßnahmen und umfassende Sicherheitsstrategien, die von Organisationen implementiert werden müssen.
- Strengere Meldepflichten bei Sicherheitsvorfällen.
- Nationale Behörden erhalten erweiterte Befugnisse zur Durchsetzung der Richtlinie.
    - Neu: Befugnis zur **Relevanzbestimmung**

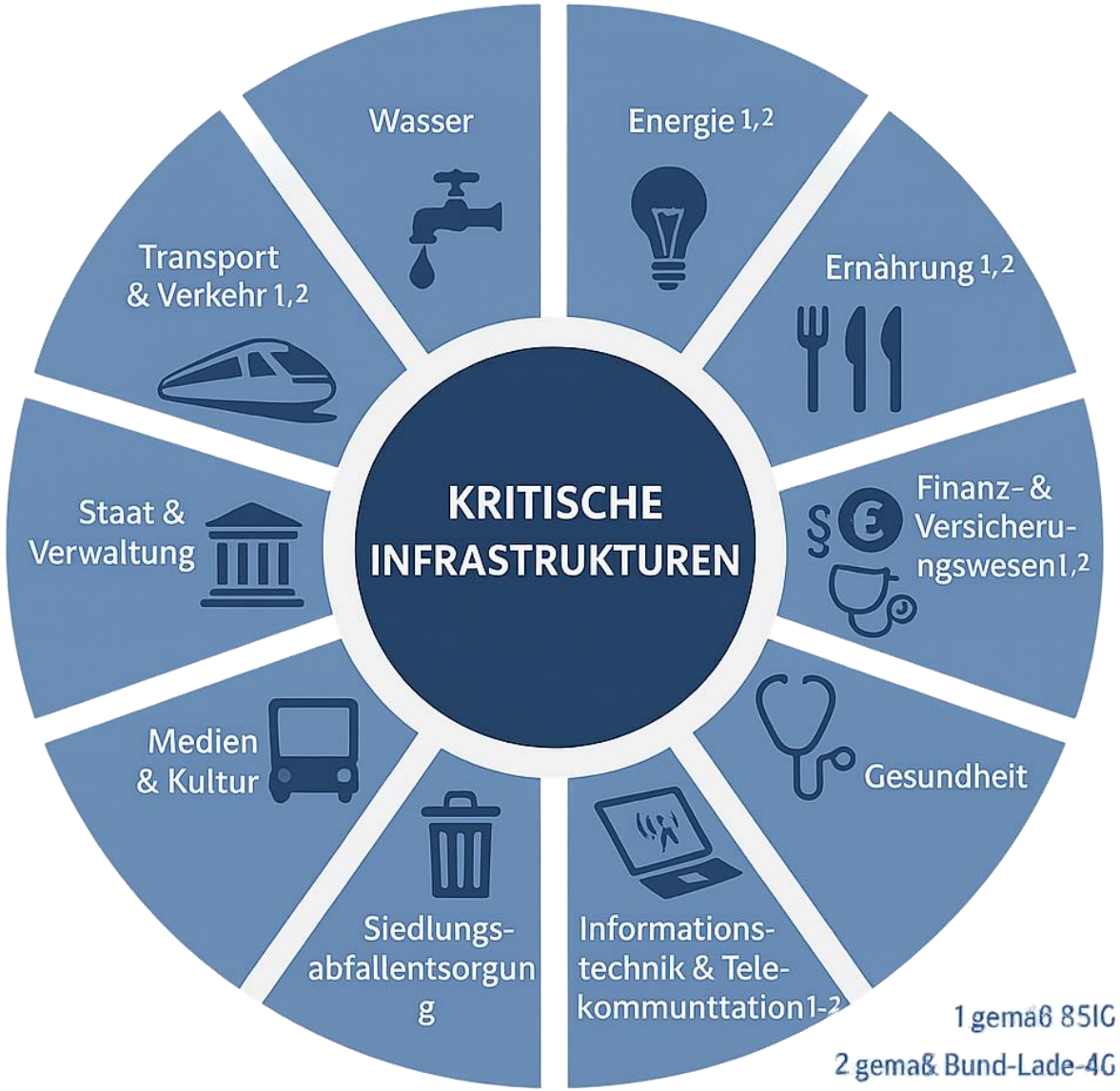
ANFORDERUNGEN

- Implementierung von Maßnahmen zur Risikoanalyse und -bewältigung.
- Einführung technischer und organisatorischer Sicherheitsvorkehrungen.
- Verpflichtung zur Meldung signifikanter Sicherheitsvorfälle an die zuständigen Behörden.
- Festlegung von Fristen für die Meldung (in der Regel innerhalb von 24 bis 72 Stunden).
- Entwicklung und Pflege einer umfassenden Informationssicherheitspolitik.
- Regelmäßige Überprüfung und Aktualisierung der Sicherheitsmaßnahmen.
- Regelmäßige Schulungen und Sensibilisierungsmaßnahmen für Mitarbeiter.
- Durchführung regelmäßiger Audits zur Überprüfung der Einhaltung der Sicherheitsanforderungen.


Sektoreinteilung
KRITIS
Umsetzungsvorgaben
KRITIS-VO, BSIG, NIS-2

WOHER WEIß ICH, WANN ICH KRITIS/NIS-2 BIN?

SEKTOREN



vgl. https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren-Branchen/sektoren-branchen_node.html

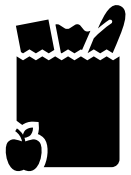
SCHWELLENWERTE

Schwellenwerte unterscheiden sich je nach Sektor, z.B.

Stromerzeugungsanlagen: 104 MW Leistung
Gaserzeugungsanlagen: 5.190 Gwh Gas

Flughäfen: 20 Mio. Passagiere pro Jahr
Bahnhöfe: 23.000 Züge pro Jahr

Krankenhäuser: 300.000 vollstationäre Fälle/Jahr



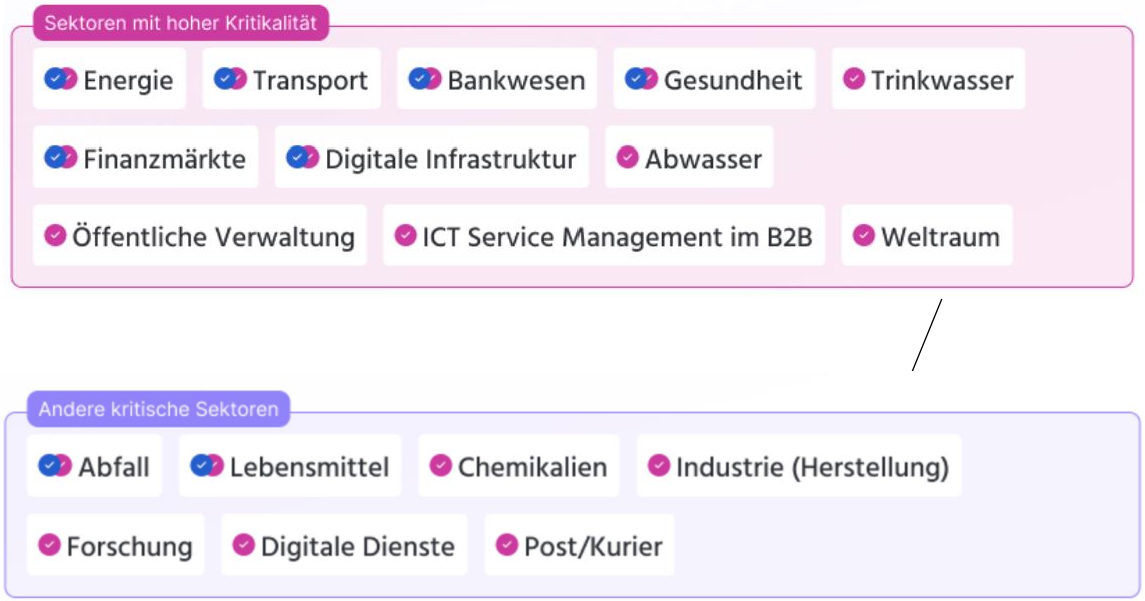
Lebensmittelherstellung: 434.500 Tonnen Lebensmittel pro Jahr
Getränkeproduktion: 350 Mio. Liter pro Jahr

UND WANN GILT NIS-2?

> 50 Mitarbeiter

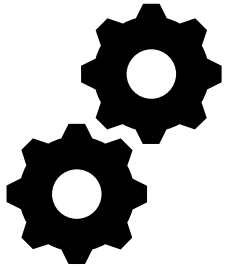
+

mind. 10 Mio. Euro
Umsatz **oder**
Bilanzsumme



BEISPIEL ZUR SEKTORBESTIMMUNG NIS-2

Unternehmen:



Maschinenbauer
Zulieferer für Sektor Transport und Verkehr

BEISPIEL ZUR SEKTORBESTIMMUNG NIS-2

Schwellenwerte erreicht?

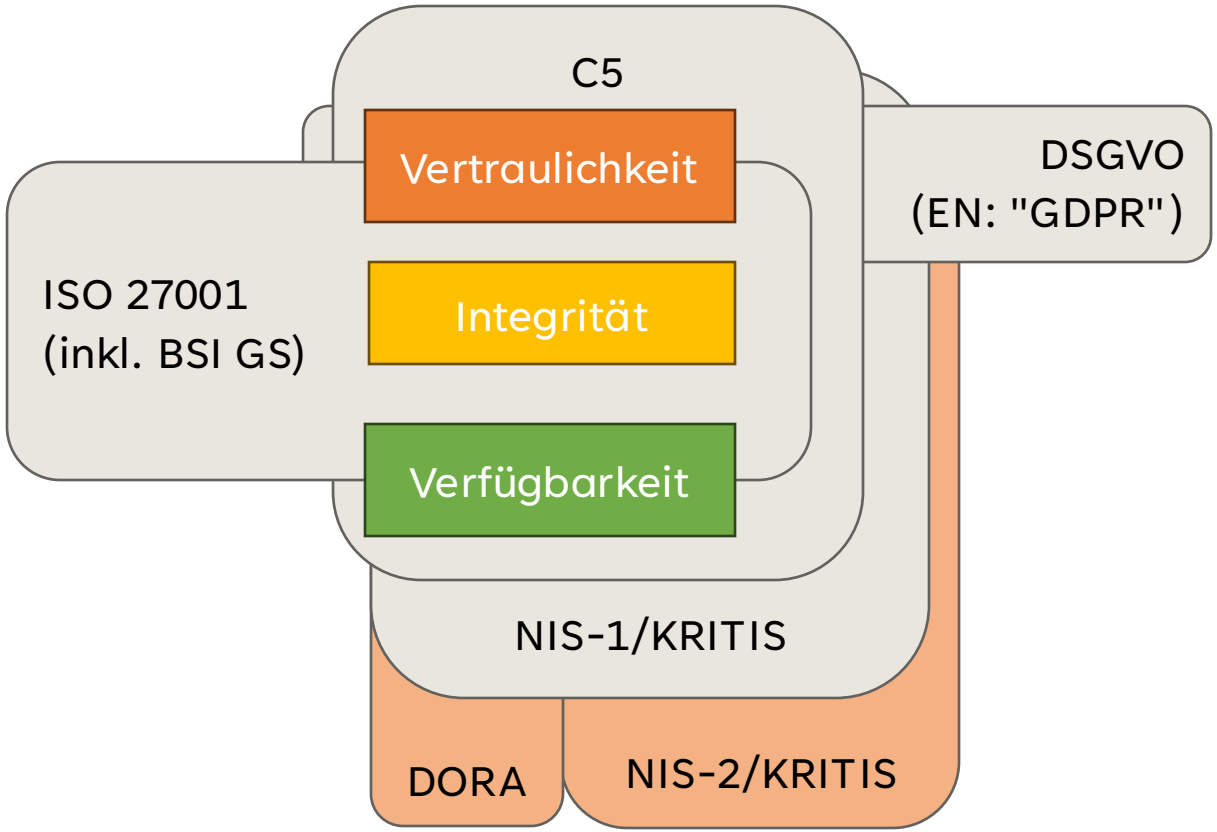
Mitarbeiter: 203
Jahresumsatz: 43 Mio. Euro

Sektorzugehörigkeit gegeben?

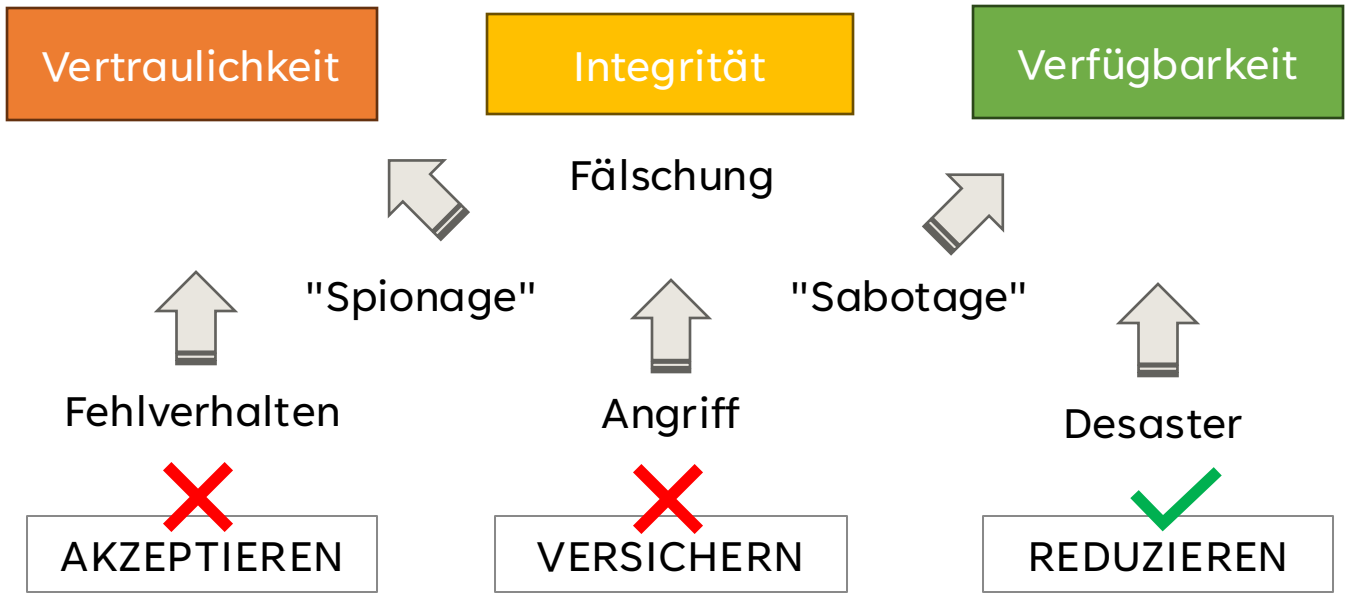
EU NIS-2 Annex II Subsektor Maschinenbau; Abs. C Abt. 28 NACE: NACE-Nr. 21, 26, 27, 28, 29, 30

NACE-Nr. lt. IHK-Listung: 256206, 2561, 25940

SAME, SAME, BUT DIFFERENT ...



UND WO LIEGT DER UNTERSCHIED?



Quelle: "Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG"

DIE GUTEN NACHRICHTEN

- betroffene Organisationen wissen, wie wichtig ihre Leistung ist.
- Viele – vielleicht alle - Sicherheitsmaßnahmen sind bereits in Kraft.
- Der "gesunde Menschenverstand" schreibt das Meiste bereits vor.

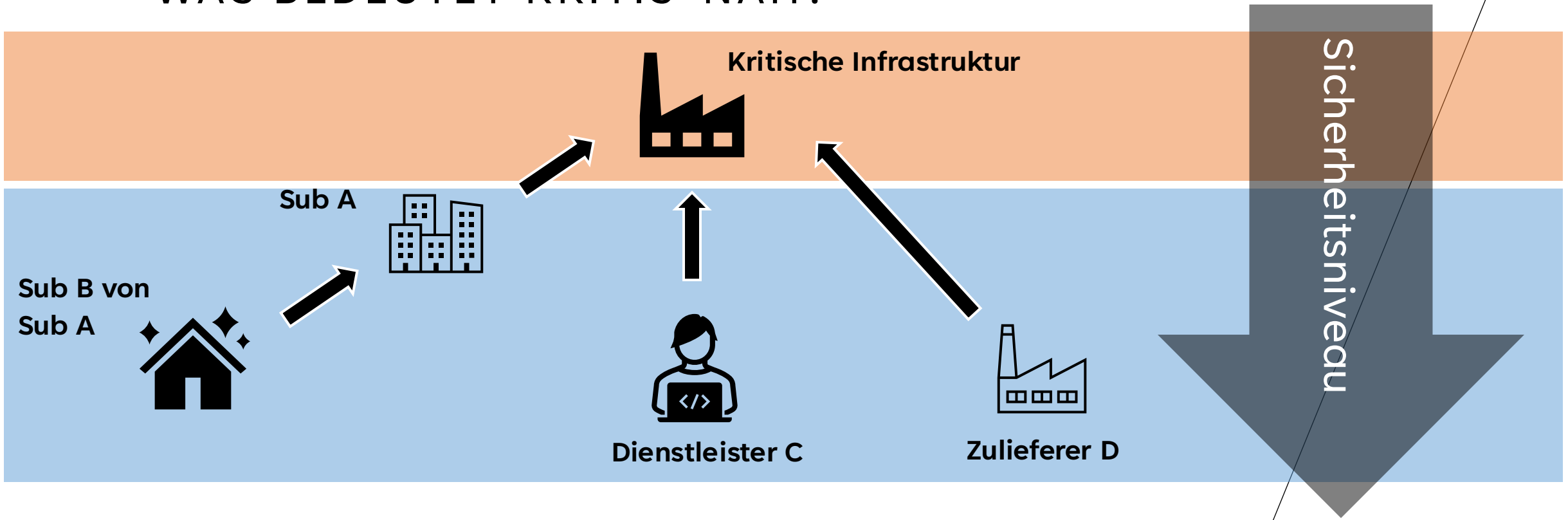
Und der Rest? ... ist transparent und verfügbar:

- Die KritisV(O) legt Grenzwerte fest (Anhang 1 bis 8)
- Nachweispflicht gem. §8a, Abs. 3 BSIG (Audits, Prüfungen oder Zertifizierungen)
- Selbsterklärung bspw. gem. §8f BSIG
- Pflicht zur Erkennung und Eindämmung von Sicherheitsvorfällen gem. § 8c BSIG
- BSI informiert gem. §4b, Abs. 3, Nr. 4 über akute Bedrohungslagen

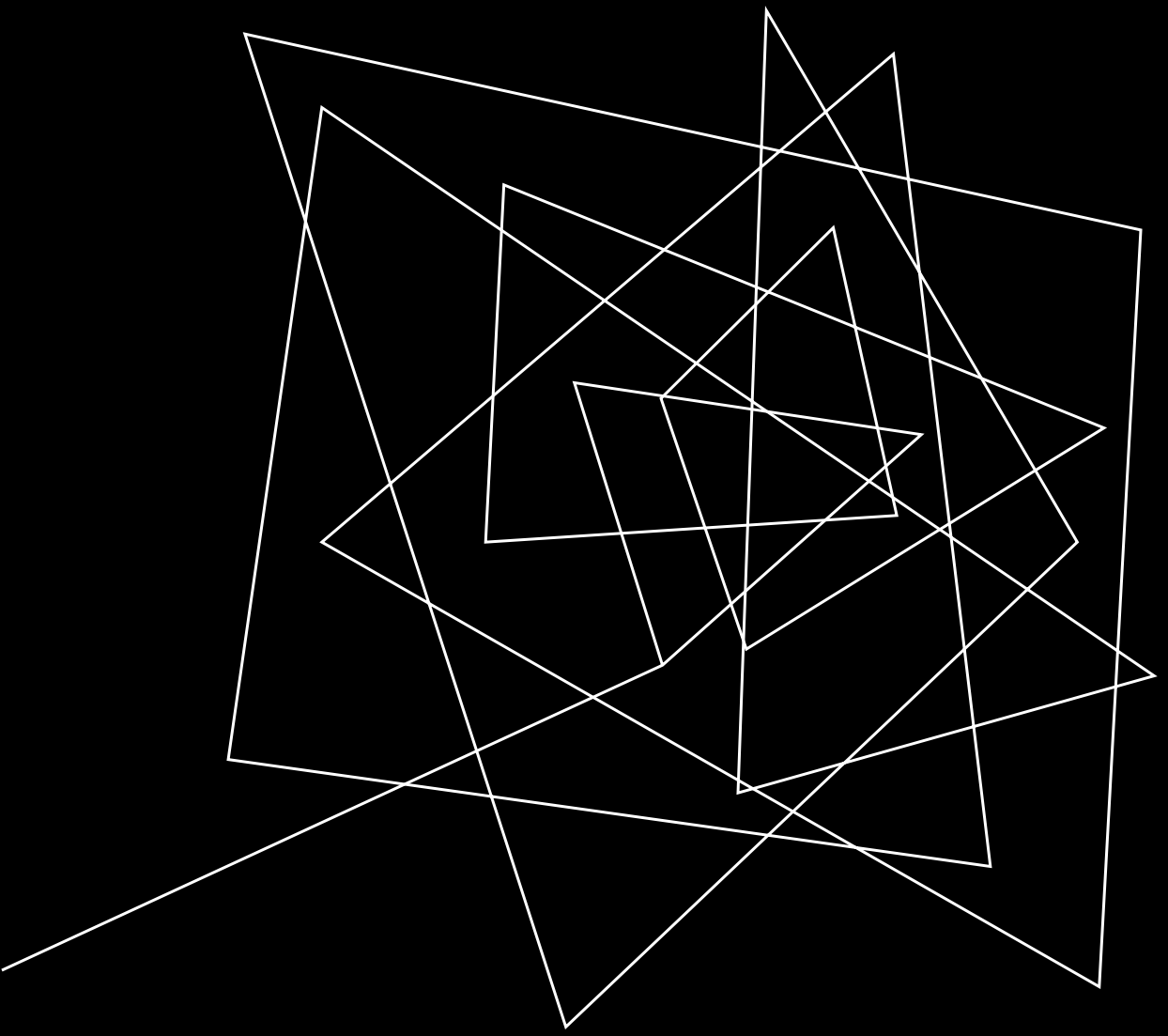
Neu (NIS-2): BSI kann KRITIS-Pflichtigkeit (Relevanzbestimmung) von Amts wegen prüfen und festlegen

WAS BEDEUTET KRITIS-NAH?

WAS BEDEUTET KRITIS-NAH?



"Ich bin KRITIS und darum bist Du es auch!"



EXKURS: ISO27001

EXKURS: ISO27001

ISO/IEC 27001 ist ein international anerkannter Standard für Informationssicherheits-Managementsysteme (ISMS)

- Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen durch systematische Managementprozesse.
- Der Standard ist auf Organisationen aller Größen und Branchen anwendbar.
- Deckt alle Aspekte der Informationssicherheit ab, einschließlich Menschen, Prozesse und IT-Systeme.

EXKURS: ISO27001

Hauptkomponenten

- Risikomanagement: Identifikation, Bewertung und Behandlung von Informationssicherheitsrisiken.
- Sicherheitskontrollen: Implementierung von Sicherheitskontrollen (Annex A) zur Minderung identifizierter Risiken.
- Kontinuierliche Verbesserung: Regelmäßige Überprüfung und Verbesserung des ISMS.

RISIKOORIENTIERTE UMSETZUNG

Identifizieren

- Prozesse
- Daten
- Systeme

z.B.
- Notfallmanagement
- Vorfallsbehandlung
- Systemhärtung

Dokumentieren

- Leitlinie
- Vorgaben

z.B.
- Leitlinie ISMS
- Notfallkonzept
- Prozess Vorfallsbehandlung

Umsetzen

- Technische Maßnahmen
- Prozess-implementierung

z.B.
- 2FA
- Netztrennung
- Schwachstellen-patches

Kontrollieren

- Interne Kontrollen
- Audits

z.B.
- Jährliche Kontrolle

FRAGERUNDE!

SECUDA

VIELEN DANK FÜR DIE AUFMERKSAMKEIT!

SPÄTE RÜCKFRAGEN GERNE AN
OFFICE@SECUDA.DE

SECUDA