



CSRSM MEETUP STUTTGART | 12. OKTOBER 2026

Sicher sind wir, bis es passiert. Resilient sind wir, danach.

Cyberresilienz versus Informationssicherheit

Rolf Strehle

CEO ditis Systeme – The Security Company

DAVOR Informationssicherheit

DANACH Cyberresilienz

Verhindern allein geht nicht mehr auf

96 %

der Unternehmen in Deutschland waren nachweislich oder vermutlich von Datendiebstahl, Spionage oder Sabotage betroffen

Bitkom Wirtschaftsschutz 2026

119

neue Schwachstellen werden im Schnitt pro Tag bekannt, 24 % mehr als im Jahr davor

BSI-Lagebericht 2025

80 %

der 950 erfassten Ransomware-Angriffe trafen kleine und mittlere Unternehmen

BSI-Lagebericht 2025

45 % sehen durch einen erfolgreichen Cyberangriff ihre Existenz bedroht.

Informationssicherheit schützt Informationen



Vertraulichkeit

Nur Befugte sehen die Daten.



Integrität

Daten sind richtig und unverändert.



Verfügbarkeit

Systeme und Daten sind da, wenn man sie braucht.

LEITFRAGE

„Wie verhindern wir,
dass etwas passiert?“

WERKZEUGE

ISMS, ISO 27001, TISAX, Risikoanalyse,
Kontrollen, Audit

Gut im Verwalten, schwächer im Durchhalten

KRITIS-Betreiber mit Reifegrad 3 oder höher

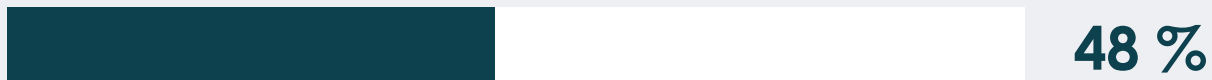
Informationssicherheits-Management (ISMS)



Business Continuity Management



Systeme zur Angriffserkennung



**Das Regelwerk steht.
Erkennen und
Durchstehen hinken
hinterher.**

Und das bei Betreibern, die Nachweise liefern müssen. Kleine und mittlere Unternehmen erfüllen im Schnitt rund 56 % der Basisanforderungen.

Resilienz beginnt, wo Prävention endet

„Die Fähigkeit, Angriffe und Störungen vorherzusehen, ihnen standzuhalten, sich davon zu erholen und sich daran anzupassen.“

NIST SP 800-160 Vol. 2 Rev. 1, sinngemäß



Vorhersehen



Standhalten



Erholen



Anpassen

LEITFRAGE

„Wie lange stehen wir, und was läuft trotzdem weiter?“

Fünf Fähigkeiten, eine davon ist Prävention



DAVOR

Schwerpunkt vieler ISMS

DANACH

Hier entscheidet sich, wie lange der Betrieb steht

Zwei Fragen, zwei Messgrößen

LEITFRAGE

Informationssicherheit

„Wie verhindern wir den Vorfall?“

ANNAHME

Der Angriff lässt sich abwehren

SCHÜTZT

Informationen und Systeme

MESSGRÖSSE

Umgesetzte Kontrollen, Auditergebnis

NACHWEIS

Zertifikat

Cyberresilienz

„Wie überstehen wir ihn?“

Ein Angriff kommt durch

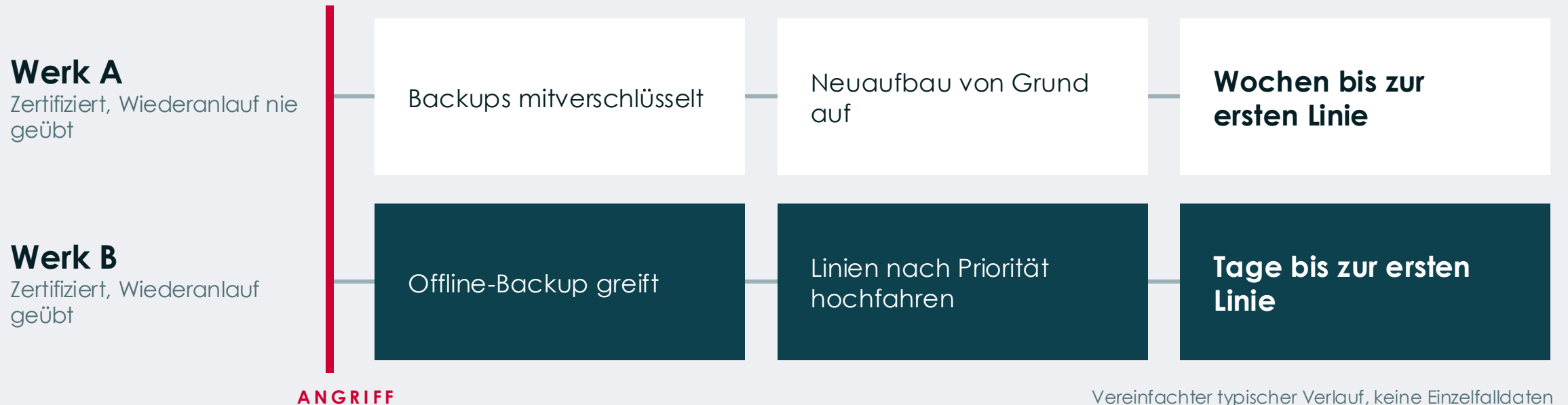
Betrieb und Lieferfähigkeit

Wiederanlaufzeit und Datenverlust

Geübter Ernstfall

Resilienz baut auf Informationssicherheit auf. Sie ersetzt sie nicht.

Im Werk zählt die Wiederanlaufzeit



40 %

der Angriffe auf Fertiger enden mit verschlüsselten Daten

51 %

der Betroffenen mit verschlüsselten Daten zahlen Lösegeld

1,3 Mio. \$

kostet die Wiederherstellung im Mittel, ohne Lösegeld

NIS2 verlangt beides, der CRA trägt es im Namen

§ 30 BSIG: zehn Pflichtmaßnahmen, zwei davon sind Resilienz pur

01	Risikoanalyse, Konzepte	06	Wirksamkeit prüfen
02	Vorfälle bewältigen	07	Schulung, Cyberhygiene
03	Betrieb, Backup, Krise	08	Kryptografie
04	Lieferkette	09	Personal und Zugriff
05	Entwicklung und Wartung	10	MFA, Notfallkommunikation

NIS2 in Deutschland

In Kraft seit 06.12.2025

Rund 29.500 Einrichtungen

Meldung nach 24 h und 72 h

§ 38: Geschäftsleitung in der Pflicht

Cyber Resilience Act

Meldepflicht seit 11.09.2026

Voll anwendbar ab 11.12.2027

Vier Schritte vom Zertifikat zur Resilienz

01



Kernprozesse benennen

Welche drei Prozesse müssen zuerst wieder laufen? Von dort rückwärts planen.

02



Wiederaanlauf messen

Zielzeit je Prozess festlegen. Backup wirklich zurückspielen, auch für Steuerungen.

03



Ernstfall üben

Krisenstab und Kommunikation ohne eigene IT einmal im Jahr durchspielen.

04



Früher erkennen

Angriffserkennung für IT und OT. Wer früh sieht, stellt weniger wieder her.

ZUM MITNEHMEN

„Sicherheit lässt sich zertifizieren. Resilienz muss man beweisen.“

Rolf Strehle

CEO ditis Systeme – The Security Company | [ditis.de](https://www.ditis.de)

+49 172 750 1058

Rolf.Strehle@ditis.de

Resilienz-Check gefälltig? Sprechen Sie mich an.

