CONCEPTURE
GRUPPE | IHR ERFOLG. GESICHERT

VORTRAG

Der Resilienzdschungel

Vom Dschungel zur Praxis

20.11.2025

AGENDA

1

VORSTELLUNG

2

GESETZLICHE RAHMENBEDINGUNGEN

3

ACHT PHASEN MODELL

AGENDA

1 VORSTELLUNG

2 GESETZLICHE RAHMENBEDINGUNGEN

3 ACHT PHASEN MODELL

IHR REFERENT

Holger Berens

- 40 Jahre Erfahrung im Compliance und Sicherheitsmanagements
- Managing Partner bei Concepture
- Vorstandsvorsitzender des Bundesverbandes für den Schutz kritischer Infrastrukturen (BSKI)
- externer CISO von mehreren internationalen Konzernen für den EMEA-Bereich
- externer IKT-Beauftragter
- Autor von Fachbüchern sowie gefragter Experte der Medien im Bereich Compliance und Security.

BSKI
Bundesverband für den Schutz Kritischer Infrastrukturen e. V.

Satzungszweck

- Der Bundesverband für den Schutz Kritischer Infrastrukturen (BSKI) ist die zentrale Anlaufstelle für Entscheider aus Kritischen Infrastrukturen, um ganzheitliche Schutzkonzepte zu etablieren.
- Die Aufgabe des Bundesverbandes für den Schutz Kritischer Infrastrukturen ist es, Sicherheitsrisiken für kritische Infrastrukturen und deren Zulieferer frühzeitig zu er-kennen und durch gezielte Konzepte für Prävention, Reaktion und Postvention zu reduzieren. Dabei werden allerhöchste Schutzziele (technisch, organisatorisch, persönlich) für kritische Infrastrukturen verfolgt.

mehr Informationen unter: www.bski.de

AGENDA

1

VORSTELLUNG

2

GESETZLICHE RAHMENBEDINGUNGEN

3

ACHT PHASEN MODELL

IT-Sicherheitsgesetz 1.0 Änderungsgesetz zum BSIG, EnWG, TKG, AtG und TMG: Verpflichtet Betreiber Kritischer Infrastrukturen IT angemessen abzusichern und diese Sicherheit überprüfen zu lassen.

Neue Rechtssetzung durch die EU

NIS 2 & RCE (Resilience of Critical Entities) (Umsetzung bis 17. Oktober 2024)

Neue Sektoren: z. B. öffentliche Verwaltung, Weltraum, ForschungseinrichtungenEinführung „size-cap rule"

DORA (Digital Operational Resilience Act) VO und RL (Anwendung / Umsetzung bis 17.1.2025)

BSI-Kritisverordnung
Definition Sektoren:
Schwellenwerte (Bedeutung des Versorgungsgrads)

Umsetzungsfristen

2015

2016

2017

2021

2022/23

2024

2025

2025/26

Umsetzungsgesetz NIS 1
Neu: Regelungen für Anbieter Digitaler Dienste

IT-Sicherheitsgesetz 2.0
Einsatz von Systemen zur Angriffserkennung (§ 8a Abs. 1a):
Neuer Sektor – Siedlungsabfallentsorgung, Selbsterklärung zur IT-Sicherheit: Unternehmen im besonderen öffentlichen Interesse (§ 8f)

jetzt

Inkrafttreten
BISG 3.0
KRITIS-Dachgesetz

Der Cyber Resilience Act („CRA")

wurde am 20.11.2024 im Amtsblatt veröffentlicht und tritt am 09.12.2024 in Kraft.

GESETZLICHE RAHMENBEDINGUNGEN

Es gibt zwei sogenannte EU-Richtlinien, die in nationales Recht umgesetzt werden müssen:

EU-Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie)

Die CER-Richtlinie verpflichtet die Mitgliedstaaten, kritische Einrichtungen zu identifizieren und deren physische Widerstandsfähigkeit gegenüber Bedrohungen wie *Naturgefahren*, *Terroranschläge* oder *Sabotage* zu stärken.

EU-Richtlinie für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie)

Die NIS2-Richtlinie verpflichtet die Unternehmen, die in den Anwendungsbereich fallen, IT-, Cyber- und Informationssicherheit einzuführen.

Die Richtlinie ist für jeden Mitgliedstaat, an den sie gerichtet wird, hinsichtlich des zu erreichenden Ziels verbindlich, überlässt jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel.

GESETZLICHE RAHMENBEDINGUNGEN

EU Richtlinien müssen in den Mitgliedstaaten in nationales Recht umgesetzt werden.

Die Umsetzungsfrist für NIS2 und CER war der 17.10.2024.

In Deutschland sind das für:

NIS2 › BSIG 3.0/ITSiG 3.0

CER › KRITIS-Dachgesetz

Die EU Kommission hat ein Vertragsverletzungsverfahren gegen Deutschland eingeleitet, da diese Richtlinien nicht fristgerecht umgesetzt wurden.

GESETZLICHE RAHMENBEDINGUNGEN

Der Entwurf eines Gesetzes zur Umsetzung („Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“) ist vorgelegt worden.

Am 13. November 2025 hat der Deutscher Bundestag den Gesetzentwurf in 2./3. Lesung verabschiedet.

Der nächste Schritt: Zustimmung durch den Bundesrat sowie Ausfertigung und Inkrafttreten.

GESETZLICHE RAHMENBEDINGUNGEN

Deutschland hat damit den parlamentarischen Teil abgeschlossen.

Allerdings:

Es steht noch nicht fest, ob und wann genau das Gesetz in Kraft tritt – das Inkrafttreten hängt u. a. vom Bundesrat sowie der Ausfertigung durch den Bundespräsidenten ab.

Damit gilt:

Der Gesetzgeber hat auf Bundesebene das Umsetzungsinstrument beschlossen, aber es fehlen noch die letzte formale Stufe und die konkreten Rechtsverordnungen bzw. Umsetzungsvorschriften.

GESETZLICHE RAHMENBEDINGUNGEN

Umsetzung RCE Richtlinie:

Der Kabinettsentwurf wurde am 24. Oktober 2025 als Bundesratsdrucksache eingebracht.

Es ist noch nicht abschließend geklärt, wann das Gesetz in Kraft treten wird; oft wird mit Wirkung ab 2025/26 gerechnet.

Da die Umsetzung verzögert ist, besteht für betroffene Unternehmen noch Unsicherheit bezüglich konkreter Fristen und Anforderungen.

Viele Unternehmen sollten jedoch jetzt bereits prüfen, ob sie in den Geltungsbereich fallen und entsprechende Vorbereitungen treffen (z. B. Aufbau eines BCM, Risikoanalyse, Meldeprozesse).

GESETZLICHE RAHMENBEDINGUNGEN

Ein genaues Datum kann nicht prognostiziert werden.

Die wesentlichen Anforderungen stehen mit den jeweiligen Entwürfen jedoch fest.

Das bedeutet, dass die Unternehmen, die in den Anwendungsbereich fallen, jetzt schon wissen, welche Maßnahmen implementiert werden müssen.

GESETZLICHE RAHMENBEDINGUNGEN

Cyber Resilience Act Resilience Act (CRA) - VERORDNUNG (EU) 2024/2847 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung)Regulation (EU) 2022/2554.

Die Verordnung hat allgemeine Geltung. Sie ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Alle Produkte, die in der EU verkauft werden und „digitale Elemente“ enthalten, müssen den Anforderungen des CRA entsprechen. Ziel ist es, die Widerstandsfähigkeit gegen Cyberangriffe zu erhöhen und die Sicherheit digitaler Produkte während ihres gesamten Lebenszyklus zu gewährleisten. Dies betrifft sowohl Hardware als auch Software, die mit Netzwerken oder anderen Geräten verbunden sind, oder generell Produkte mit digitalen Elementen.

GESETZLICHE RAHMENBEDINGUNGEN

Die nächsten Schritte des CRA

*KBS = Konformitätsbewertungsstellen
Quelle: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html

GESETZLICHE RAHMENBEDINGUNGEN

Mit dem CRA wird die Cybersicherheit von Produkten, die miteinander oder mit dem Internet verbunden werden können, verbessert.

Diese Produkte werden von Unternehmen hergestellt und an Kunden vertrieben. Sie werden aber auch in Unternehmen für die Produktion eingesetzt sowie als Vorprodukte bezogen und weiter verbaut beziehungsweise veredelt und sind damit Bestandteil von Lieferketten.

Da es sich um eine EU Verordnung handelt, gelten alle Anforderungen unmittelbar zwingend. Deutschland hat hier keinen politischen Einfluss.

AGENDA

1

VORSTELLUNG

2

GESETZLICHE RAHMENBEDINGUNGEN

3

ACHT PHASEN MODELL

Die acht Phasen der Resilienz

Nach § 2 wird Resilienz wie folgt definiert:

„Resilienz“ die Fähigkeit eines Betreibers kritischer Anlagen, einen Vorfall zu verhindern, sich davor zu schützen, darauf zu reagieren, einen solchen abzuwehren, die Folgen eines solchen Vorfalls zu begrenzen, einen Vorfall aufzufangen, zu bewältigen und sich von einem solchen Vorfall zu erholen; ...

Die acht Phasen der Resilienz

Zum Nachlesen und zur Nacharbeit:

Prävention · Sicherheitskonzepte

Praktischer Leitfaden durch den „Resilienzdschungel“

16. Juli 2025 · von Holger Berens

Die acht Phasen der Resilienz

- Verhindern
- Schützen
- Reagieren
- Abwehren
- Folgen begrenzen
- Auffangen
- Bewältigen
- Erholen

Die acht Phasen der Resilienz

Identifikation kritischer Prozesse

Nicht alle Prozesse sind gleich wichtig

- Kernprozesse: Produktion, Vertrieb, Logistik → direkt wertschöpfend
- Hilfsprozesse: IT, HR, Einkauf → indirekt, aber kritisch

Grundlage für Prioritäten und Resilienzmaßnahmen

Beispiel:

- Produktion: Ausfall = keine Umsätze, Vertragsstrafen
- IT-Betrieb: Ausfall = gesamte Produktion steht still

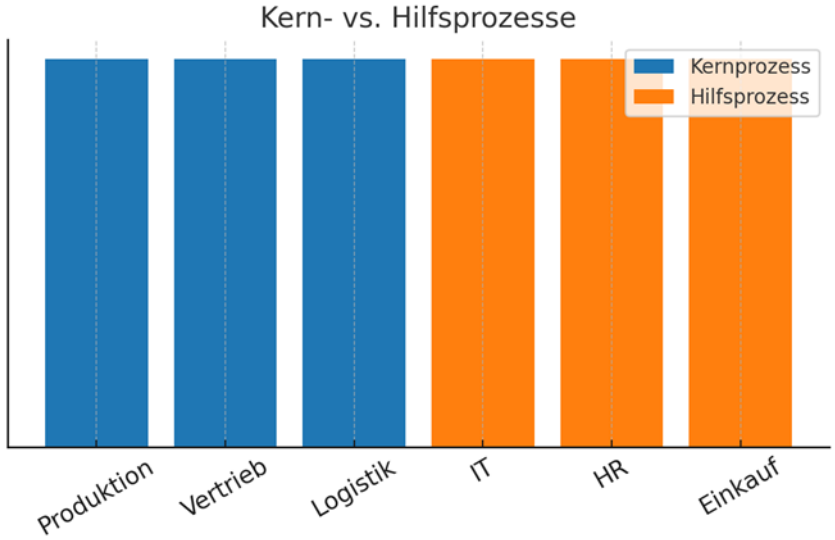
Die acht Phasen der Resilienz

Wie identifizieren?

- Prozessinventarisierung: alle Abläufe erfassen
- Klassifikation: Kern- vs. Hilfsprozesse
- Bewertung: Folgen eines Ausfalls abschätzen

- Kennzahlen:
- – MTA (Maximal tolerierbare Ausfallzeit)
- – RTO (Recovery Time Objective)

Beispiel



Die acht Phasen der Resilienz

Assets zuordnen:

- Prozesse bestehen nicht isoliert – sie hängen von Ressourcen (Assets) ab.
- Nur wenn klar ist, welche Assets ein Prozess benötigt, können Risiken richtig bewertet und Schutzmaßnahmen geplant werden.
- Assets sind die Angriffspunkte, die es zu sichern gilt.

Die acht Phasen der Resilienz

Nutzen der Zuordnung

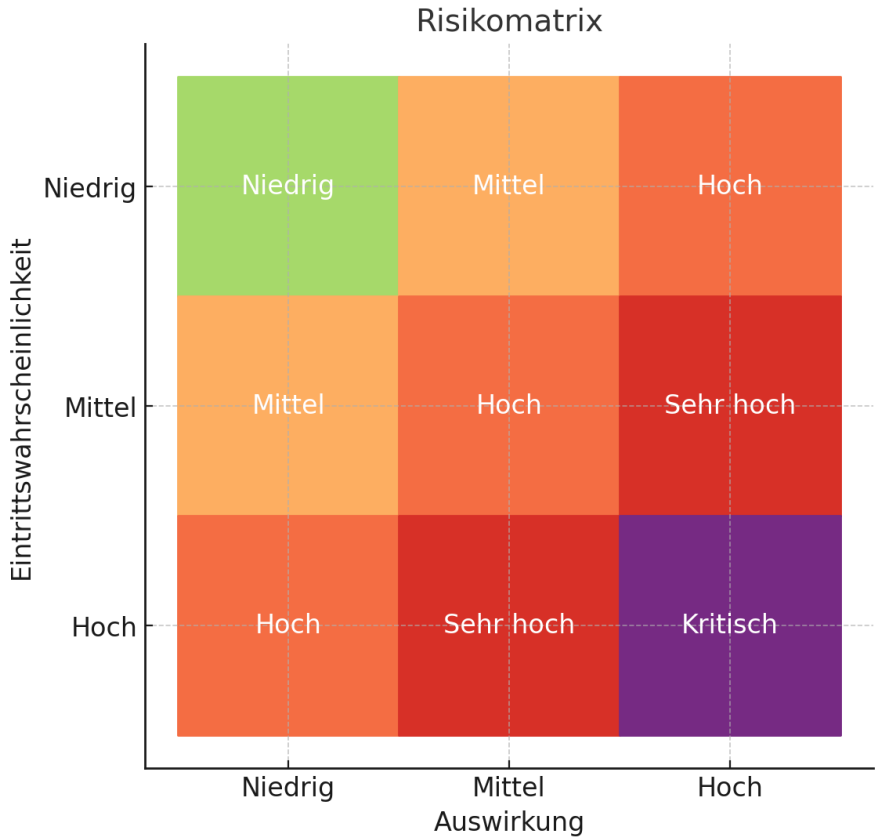
- Identifikation der **Schwachstellen** (Was passiert, wenn ein Asset ausfällt?)
- Grundlage für **Risikomanagement & Resilienzmaßnahmen**
- Verbindung von **Business-Impact** (Prozesse) mit **technischen Risiken** (Assets)
- Effiziente Allokation von Schutzressourcen

Die acht Phasen der Resilienz

Vorgehen

- **Liste des BSI**
- Bedrohungen je Asset identifizieren
- Eintrittswahrscheinlichkeit bewerten (hoch/mittel/gering)
- Auswirkungen einschätzen (finanziell, rechtlich, reputativ)
- Priorisieren → Fokus auf Bedrohungen mit hohem Risiko

Die acht Phasen der Resilienz



Die acht Phasen der Resilienz

Risikooption	Beschreibung & Beispiel
Vermeiden	Prozess/Aktivität nicht durchführen Beispiel: Cloud-Dienst nicht nutzen
Vermindern	Maßnahmen zur Reduktion Beispiel: Firewall, Verschlüsselung
Übertragen	Risiko abgeben Beispiel: Versicherung, Outsourcing mit SLA
Akzeptieren	Restrisiko akzeptieren Beispiel: Managemententscheidung, Dokumentation

Die acht Phasen der Resilienz

- Verhindern
- Schützen
- Reagieren
- Abwehren
- Folgen begrenzen
- Auffangen
- Bewältigen
- Erholen

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Kontakt:

Holger Berens
holger.berens@bski.de
h.berens@concepture.de