Das „KRITIS-Dachgesetz (KRITIS-DachG)“
(Gesetz zur Stärkung der Resilienz kritischer Anlagen)

für das Sicherheitsgewerbe

Zusammengefasst und ausgearbeitet von Mario Richter
mit dem Stand vom 10.11.2024
mit der Überarbeitung vom 29.11.2024

www.SecurityRichter.de

Zusammenfassung der wichtigsten Punkte des KRITIS-Dachgesetzes:

1. **Ziel und Hintergrund:**
   Das Gesetz dient der Umsetzung der EU-Richtlinie 2022/2557 und zielt darauf ab, die Widerstandsfähigkeit (Resilienz) kritischer Anlagen zu stärken. Es richtet sich an Betreiber kritischer Infrastrukturen, die für das Funktionieren des Binnenmarktes essenziell sind.

2. **Definition kritischer Infrastrukturen:**
   Zu den kritischen Sektoren zählen Energie, Wasser, Gesundheit, IT, Telekommunikation, Finanzwesen, Transport, Weltraum und Sozialversicherungen. Diese Sektoren haben eine besonders hohe Relevanz für die öffentliche Sicherheit und Versorgung.

3. **Verpflichtungen für Betreiber:**
   Betreiber müssen Risikoanalysen und -bewertungen durchführen und Maßnahmen zur Erhöhung ihrer Resilienz ergreifen. Dazu gehören technische, sicherheitsbezogene und organisatorische Maßnahmen, die in einem Resilienz Plan dokumentiert werden.

4. **Zentrale Anlaufstelle und Meldepflichten:**
   Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) fungiert als zentrale Anlaufstelle. Betreiber kritischer Anlagen sind verpflichtet, erhebliche Störungen und Sicherheitsvorfälle an das BBK zu melden, um eine koordinierte Krisenreaktion zu gewährleisten.

5. **Zusammenarbeit und Kontrolle:**
   Die zuständigen Behörden, darunter das Bundesministerium des Innern und die Bundesnetzagentur, arbeiten eng zusammen, um die Resilienz Maßnahmen zu überwachen und gegebenenfalls verbindliche Standards festzulegen.

6. **Anpassungen und Resilienz Standards:**
   Das Gesetz sieht vor, dass Betreiber branchenspezifische Resilienz Standards entwickeln können, die vom BBK anerkannt werden, um so spezifische Schutzmaßnahmen für unterschiedliche Branchen umzusetzen.

7. **Strategie zur Resilienz:**
   Eine nationale KRITIS-Resilienz Strategie wird bis 2026 entwickelt, um die Ziele des Gesetzes langfristig zu unterstützen und den Schutz kritischer Infrastrukturen kontinuierlich zu verbessern.

Spezifische Anforderungen für Betreiber kritischer Infrastrukturen:

1. **Identifizierung und Registrierung**
   Unternehmen, die kritische Dienstleistungen erbringen, müssen ihre Anlagen registrieren. Dazu zählen Angaben wie Unternehmensname, Standort, Versorgungsgrad (z. B. Anzahl der Personen, die versorgt werden), IP-Adressen und Kontaktdaten.

2. **Risikoanalyse und Risikobewertung**
   Betreiber kritischer Anlagen sind verpflichtet, regelmäßig Risikoanalysen und -bewertungen durchzuführen. Sie sollen dabei mögliche Naturkatastrophen, technische Ausfälle und menschliche Bedrohungen bewerten, die den Betrieb gefährden könnten.
   Die Analyse muss alle vier Jahre aktualisiert werden und auch Abhängigkeiten von anderen kritischen Infrastrukturen berücksichtigen.

3. **Erstellung eines Resilienz Plans**
   Basierend auf den Risikoanalysen muss ein Resilienz Plan erstellt werden, der beschreibt, wie das Unternehmen auf Vorfälle reagieren will. Der Plan muss technische, organisatorische und sicherheitsrelevante Maßnahmen umfassen, die den Betrieb sichern und im Notfall die schnelle Wiederherstellung der kritischen Dienstleistungen ermöglichen. Beispiele sind:
   - Objektschutz (bauliche Sicherheitsmaßnahmen und Zugangskontrollen)
   - Notfallvorsorge (Notstromversorgung, alternative Lieferketten)
   - Krisenmanagement (Protokolle und Abläufe bei Vorfällen).

4. **Technische und organisatorische Sicherheitsmaßnahmen**
   Das Gesetz verlangt „technische und organisatorische Maßnahmen“, die „dem Stand der Technik“ entsprechen müssen.
   Dazu gehören z. B. Zugangskontrollen, Detektionssysteme und bauliche Sicherungen. Diese Maßnahmen sollen dem Risiko eines Ausfalls angemessen sein und wirtschaftlich vertretbar umgesetzt werden.

5. **Schulungen und Sensibilisierung des Personals**
   Unternehmen müssen ihr Personal (auch externe Dienstleister) schulen und sensibilisieren, um sicherzustellen, dass alle Mitarbeitenden mit den Resilienz Maßnahmen und Notfallprotokollen vertraut sind.

6. **Branchen- und sektorspezifische Standards**
   Branchenverbände und Betreiber können branchenspezifische Resilienz Standards vorschlagen, die vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) anerkannt werden müssen. Diese Standards konkretisieren, welche Maßnahmen speziell in bestimmten Branchen sinnvoll sind.

7. **Meldungen bei Vorfällen**
   Bei erheblichen Störungen oder Vorfällen müssen Unternehmen diese innerhalb von 24 Stunden an eine zentrale Meldestelle melden. Ein detaillierter Bericht ist spätestens einen Monat nach dem Vorfall abzugeben. Ziel ist es, Informationen schnell zu teilen, um mögliche Folgeschäden zu begrenzen und andere betroffene Betreiber zu warnen.

8. **Zusammenarbeit und Aufsicht**
   Die zuständigen Behörden, wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das BBK, überprüfen die Einhaltung der Vorgaben und können Unternehmen zur Vorlage von Nachweisen auffordern.
   Die Behörden können Audits durchführen und ggf. unabhängige Dritte hinzuziehen.

9. **Mängel und Korrekturmaßnahmen**
   Bei Verstößen gegen die Resilienz Anforderungen können Behörden Maßnahmen zur Mängelbeseitigung verlangen, einschließlich eines Mängelbeseitigungsplans und Nachweise zur Umsetzung der erforderlichen Maßnahmen.

Fragen zum KRITIS-Dachgesetz

Was sind kritische Infrastrukturen (KRITIS)?

Von der Strom- und Wasserversorgung über die Ernährung bis zum Zahlungsverkehr – kritische Infrastrukturen (KRITIS) sind für unser Gemeinwesen unverzichtbar.
Jede und jeder Einzelne ist im Alltag auf sie angewiesen. Sie sichern die Handlungsfähigkeit staatlicher Institutionen und sind Voraussetzung für gesellschaftliches Zusammenleben und das Funktionieren unserer Wirtschaft. Ausfälle und Störungen der kritischen Infrastrukturen können zu erheblichen Versorgungsengpässen oder Gefährdungen der öffentlichen Sicherheit und Ordnung führen.

Wieso brauchen wir ein KRITIS-Dachgesetz?

Dass kritische Infrastrukturen besonders wichtig und auch verwundbar sind, haben uns insbesondere die Corona-Pandemie, Naturkatastrophen wie Hochwasser, der Krieg in der Ukraine oder auch Sabotageakte deutlich gezeigt.
Bisher gibt es aber **keine einheitlichen bundesrechtlichen Regelungen** für den physischen Schutz kritischer Infrastrukturen.

Entsprechende Vorschriften sind in den Sektoren und Branchen sehr heterogen: Sie reichen von unverbindlichen Leitlinien bis hin zu bundes- und landesgesetzlichen Spezialregelungen oder genau festgelegten DIN-Normen. Mit dem KRITIS-Dachgesetz wollen wir erstmals einen einheitlichen bundesrechtlichen Rahmen für den physischen Schutz der kritischen Infrastrukturen schaffen. Damit ergänzen wir die seit einigen Jahren bestehenden Regelungen des BSI-Gesetzes zur IT-Sicherheit von KRITIS um weitere zentrale Aspekte.

Was ist das Ziel des KRITIS-DachG?

Der Schutz unserer kritischen Infrastrukturen hat eine besondere Priorität. Vorfälle gefährden nicht nur die Versorgung der Bevölkerung, sie können außerdem einen hohen wirtschaftlichen Schaden verursachen. Allein durch Hochwasser und Überschwemmungen in Folge von Starkregen entstanden zum Beispiel an Gebäuden, Verkehr, Industrie, Gewerbe und Lieferketten seit dem Jahr 2000 Schäden in Höhe von mindestens 70 Milliarden Euro. Ziel des Gesetzes ist deshalb die Erhöhung der Widerstandsfähigkeit der für die Versorgungsicherheit der Bevölkerung essenziellen KRITIS, also die Aufrechterhaltung des Betriebs auch bei Vorfällen.

Durch Resilienz Maßnahmen sollen Vorfälle weitmöglich verhindert werden, auf diese besser reagiert, negative Auswirkungen wie Folgekosten begrenzt oder die zügige Wiederherstellung der kritischen Dienstleistung gewährleistet werden. Das KRITIS-Dachgesetz soll bestehende Regelungen nicht ersetzen, sondern durch staatliche und betreiberseitige Risikoanalysen Lücken und Schwachstellen aufzeigen. So können diese durch sektorübergreifende Mindestanforderungen sowie spezifische Regelungen geschlossen werden.

Wer ist für den Schutz von KRITIS verantwortlich?

Grundsätzlich gilt: Die Unternehmen sind in erster Linie selbst verantwortlich für ihren Schutz. Dennoch ist der Schutz der KRITIS eine gesamtstaatliche Aufgabe, bei der Bund, Länder und Kommunen entsprechend ihren jeweiligen Zuständigkeiten eng auch mit den Betreibern zusammenarbeiten, um die Versorgungssicherheit unserer Gesellschaft mit lebenswichtigen Dienstleistungen sicherzustellen.

Was unternimmt der Staat zum Schutz von KRITIS?

Schon jetzt leistet der Staat vieles beim KRITIS-Schutz. Unsere Sicherheitsbehörden bewerten die Sicherheitslage fortlaufend, informieren und sensibilisieren Unternehmen regelmäßig und anlassbedingt. Und die Landespolizeien handeln im Rahmen der Gefahrenabwehr ebenfalls zum Schutz von KRITIS. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) unterstützt Staat und Betreiber beim Schutz kritischer Infrastrukturen durch Leitfäden und Empfehlungen.
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist als Cybersicherheitsbehörde des Bundes zuständig für die Cybersicherheit von KRITIS-Anlagen nach BSI-Gesetz.

Die Unternehmen selbst tun ebenfalls bereits viel für den physischen Schutz ihrer Einrichtungen sowie um ihren Betrieb zu gewährleisten und investieren in Maßnahmen zum physischen Schutz ihrer Anlagen, etwa vor umweltbedingten Schäden oder gegen Sabotage.
Mit dem KRITIS-Dachgesetz werden erstmalig die Verantwortlichkeiten und das Zusammenwirken der verschiedenen Akteure beim KRITIS-Schutz festgeschrieben.

Wer zählt alles zu den kritischen Infrastrukturen nach dem KRITIS-Dachgesetz?

Das KRITIS-Dachgesetz identifiziert kritische Anlagen in den Sektoren Energie, Transport und Verkehr, Finanzwesen, Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitssuchende, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum und Siedlungsabfallentsorgung.
Außerdem werden Einrichtungen der Bundesverwaltung zu Maßnahmen verpflichtet. Welche Anlagen in den einzelnen Sektoren konkret in den Anwendungsbereich des KRITIS-Dachgesetzes fallen, orientiert sich an mehreren abstrakten Kriterien, wie die Anzahl der versorgten Personen, die Bedeutung der kritischen Dienstleistung für andere Dienstleistungen oder den Marktanteil.
In einer noch zu erlassenden Rechtsverordnung werden für die verschiedenen Kategorien von Anlagen nachvollziehbare Schwellenwerte festgelegt, wie etwa die Zahl der Patienten in einem Krankenhaus pro Jahr oder die von einer Anlage produzierte Menge an Strom in einem Jahr. Eine derartige Methodik wird bereits zur Identifizierung von kritischen Infrastrukturen für die Zwecke der IT-Sicherheit nach dem BSI-Gesetz verwendet und hat sich bewährt.

Kritische Infrastrukturen können durch viele verschiedene Umstände gefährdet werden – vom menschlichen Versagen über klimabedingte Katastrophen bis hin zu hybriden Bedrohungen, Terrorismus oder Sabotage. Deshalb muss ein All-Gefahrenansatz zugrunde gelegt werden, der auf den Schutz vor Gefahren aller Art zielt.
Der Brandanschlag auf die Energieinfrastruktur zur Versorgung des Tesla-Werks in Grünheide hatte zum Beispiel erhebliche Auswirkungen auf das dortige Logistikzentrum einer großen Supermarktkette, die 500 Märkte in der Region versorgt und über keine ausreichende Notstromversorgung verfügte. Solche Interdependenz verschiedener Sektoren zeigen, wie notwendig es ist, Risikoanalysen zu erstellen und darauf aufbauende Maßnahmen umzusetzen.

Welche Vorgaben macht das KRITIS-Dachgesetz den KRITIS-Betreibern?

Derzeit gibt es keine für alle Betreiber gleichermaßen geltende Verpflichtung, die Risiken für ihre Anlagen regelmäßig zu überprüfen und umfassende Maßnahmen zu treffen, um deren Funktionsfähigkeit zu sichern.
Das KRITIS-Dachgesetz formuliert daher erstmals sektorenübergreifende Ziele für die Betreiber. Dazu zählt, Störungen und Ausfälle zu verhindern, deren Folgen zu begrenzen und die Arbeitsfähigkeit nach einem Vorfall wiederherzustellen. Ergebnis dieses Prozesses kann zum Beispiel ein erhöhtes Risiko für Hochwasserschäden sein.
In der Folge müssten in der betreffenden Anlage etwa Klappschotten oder andere Dichtungen eingebaut werden, um solche Schäden zu vermeiden.
Grundsätzlich müssen die Betreiber alle Risiken einbeziehen, die durch die Natur oder durch Menschen verursacht werden können („All-Gefahren-Ansatz“) beispielsweise Unwetter, menschliches Versagen, Sabotage oder Terrorismus.

Wie unterstützt der Staat die KRITIS beim besseren Schutz?

Um passgenaue Maßnahmen vornehmen zu können, unterstützten staatliche Risikobewertungen die KRITIS-Betreiber bei der Bewertung der jeweiligen Risiken für die jeweils eigenen kritischen Anlagen. Von den Betreibern werden verhältnismäßige Maßnahmen verlangt, also können sie eine Abwägung von Zweck und Mittel vornehmen unter Berücksichtigung auch wirtschaftlicher Aspekte. Von der Wirtschaft erarbeitete Branchenstandards sollen bei der Frage, welche mögliche Maßnahmen geeignet und verhältnismäßig sein können, Orientierung geben.
Darüber hinaus müssen Betreiber erhebliche Vorfälle, also Ausfälle oder Beeinträchtigungen bei ihren kritischen Dienstleistungen, dem BBK melden.

Welche Maßnahmen müssen KRITIS-Betreiber zur Stärkung ihrer Funktionsfähigkeit konkret treffen?

Das KRITIS-Dachgesetz schreibt Betreibern kritischer Anlagen keine konkreten Regelungen vor.
Es verpflichtet die Betreiber lediglich dazu, geeignete und verhältnismäßige Maßnahmen zu ergreifen.

Welche Maßnahmen das sind, kann sich von Sektor zu Sektor und von Unternehmen zu Unternehmen unterscheiden. In Hochwassergebieten sind andere Maßnahmen erforderlich als in anderen örtlichen Umgebungen; ein Krankenhaus muss anders geschützt werden als das Stromnetz.

Wieso müssen KRITIS-Betreiber Vorfälle dem BBK melden?

Bereits heute sind KRITIS-Betreiber verpflichtet, IT-Sicherheitsvorfälle dem BSI zu melden.
In Zukunft werden sie Vorfälle – sei es IT-Sicherheitsvorfälle oder solche mit physischem Bezug – über ein gemeinsames Online-Portal des BBK und des BSI melden.
Die Meldung von Vorfällen ermöglicht ein Lagebild zur Situation der kritischen Infrastrukturen in Deutschland – und in Europa, da Vorfälle mit grenzüberschreitender Bedeutung auch an andere EU-Mitgliedstaaten weitergeleitet werden.
Dadurch werden Entwicklungen und Abhängigkeiten der einzelnen kritischen Infrastrukturen deutlicher und es können in der Folge weitere oder veränderte Maßnahmen getroffen werden, um die Resilienz der KRITIS weiter zu stärken.

Was wird konkret besser durch das KRITIS-Dachgesetz?

Das KRITIS-Dachgesetz ist ein Meilenstein beim physischen KRITIS-Schutz in Deutschland und in Europa. Die Risiken werden systematisch in den Blick genommen und bestehende Lücken können durch das KRITIS-Dachgesetz gefüllt werden.
Auch wenn bislang einzelne Aspekte in anderen Fachgesetzen oder in Leitlinien behandelt werden, gibt es kein einheitliches Mindestniveau an Maßnahmen, das für alle Sektoren gilt.
Durch die Befassung mit Risiken und die Meldung von Vorfällen durch Betreiber wird ein besseres Lagebild ermöglicht.
Zudem werden die Verantwortlichkeiten der verschiedenen Beteiligten konkreter beschrieben.

Wieso sind die Regelungen des KRITIS-Dachgesetzes sehr abstrakt und schreiben noch keine konkreten Maßnahmen für die Unternehmen vor?

Das KRITIS-Dachgesetz stellt die Weichen für einen umfangreichen Prozess zu einer besseren Widerstandsfähigkeit unserer KRITIS.

Aufgrund der großen Unterschiede zwischen den einzelnen Sektoren und den einzelnen Anlagen können Konkretisierungen nur in den weiteren Prozessen erfolgen: Ein Strommast erfordert andere Maßnahmen zu seinem Schutz als ein Krankenhaus oder eine Anlage, die in einer durch Hochwasser bedrohten Gegend liegt.
Von der Wirtschaft erarbeitete Branchenstandards sollen bedarfsgerechte Orientierung geben.

Wie verhält sich das KRITIS-Dachgesetz zu den bestehenden Vorgaben zur IT-Sicherheit von kritischen Infrastrukturen? Warum werden Cyberschutz und physischer Schutz von KRITIS nicht gleich zusammen geregelt?

Neben dem KRITIS-Dachgesetz hat das Bundesinnenministerium zudem einen **Entwurf für ein NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz** erarbeitet (NIS2UmsuCG), der nun im Bundestag beraten wird. Durch die Umsetzung der EU-Richtlinie für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie) steigern wir das Sicherheitsniveau und senken damit das Risiko für Unternehmen, Opfer von Cyberangriffen zu werden.
Wir werden beide Vorhaben in einen europäischen Rahmen einbetten und damit zu einer höheren Versorgungssicherheit in Deutschland und Europa beitragen. Das **NIS2UmsuCG** baut dabei auf das bereits existierende, umfassende Schutzsystem für die Cybersicherheit kritischer Infrastrukturen in Deutschland auf.
Bei beiden Vorhaben wurde auf größtmögliche Kohärenz bei den Schnittstellen geachtet.
Dies soll z.B. durch eine gemeinsame KRITIS-Verordnung zur Identifizierung und einer gemeinsamen Registrierungsplattform und einer gemeinsamen Plattform zur Meldung von Vorfällen gewährleistet werden.

Wie ist der Schutz der KRITIS in der EU geregelt?

Auch auf europäischer Ebene wird die Bedeutung der Stärkung der physischen Resilienz von kritischen Infrastrukturen erkannt.
Die EU-Richtlinie über die Resilienz kritischer Einrichtungen (sog. **CER-Richtlinie**) wurde Ende 2022 beschlossen und wird mit dem KRITIS-Dachgesetz in nationales Recht umgesetzt.
Damit wird ein EU-weit einheitliches Mindestniveau für den physischen Schutz von KRITIS gewährleistet und die EU-weite Zusammenarbeit in diesem Bereich gestärkt.

Betreiber kritischer Anlagen

Die betroffenen Unternehmen in Deutschland umfassen Betreiber kritischer Anlagen in KRITIS-Sektoren, die durch NIS2 und KRITIS-Dachgesetz reguliert werden.

Betreiber	Größe	Sektoren
Kritische Anlage **§2 Nr. 1**	Anlagen mit Schwellenwerten	Energie, Transport und Verkehr, Finanzwesen^, Sozialversicherung, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation^, Weltraum, Siedlungsabfallentsorgung **§4 (1)**
Bund §2 Nr. 10	Einrichtungen	Bundesverwaltung: Bundesministerien, Bundeskanzleramt §7

Betroffen vom Gesetz sind Betreiber kritischer Anlagen, wenn diese (in der Regel) über 500 Tsd. Personen mit ihren Anlagen versorgen.

Das KRITIS-Dachgesetz weist darauf hin, dass auch Einrichtungen, die keine kritischen Anlagen betreiben, von erheblicher Bedeutung sein können, wie z.B. Betreuungsangebote.
Bund und Länder können hier weitere Vorgaben machen.
Ebenso erfüllen Sicherheitsbehörden des Bundes ihre Aufgaben im Rahmen der gesetzlichen Vorschriften. **§6**

Anlagen

Die kritischen Anlagen müssen per Verordnung vom Bund festgelegt werden, inklusive Kategorien, Schwellenwerten, versorgten Einwohner und Stichtagen/Fristen. **§5 (1)(2)**

Das Innenministerium und BBK dürfen Anlagen und Betreiber im Einzelfall auch von sich aus bestimmen, wenn diese erheblich sind, aber nicht unter die KRITIS-Verordnung fallen. **§5 (3)(4)**

Dienstleistungen

Das Gesetz unterscheidet zwischen den o.g. kritischen Dienstleistungen, die für Deutschland definiert sind, und den wesentlichen Diensten, die in EU RCE für EU-Betreiber definiert sind, die Dienste in EU-Mitgliedsstaaten erbringen. **in §9**

Sektoren

Das KRITIS-Dachgesetz definiert die regulierten Sektoren von kritischen Anlagen, kritische Dienstleistungen und betroffene Bundesverwaltung.

Sektor **§4 (1)**	**Kritische Dienstleistung** **§3 (3)**	**Zuständig** **§3 (2)**	**Kritische Anlagen** **§16 (1)**
Energie	Stromversorgung Erdgasversorgung Wasserstoffversorgung Mineralölversorgung	BNetzA BNetzA BNetzA BMWK	tbd
Transport Verkehr	Eisenbahnverkehr See- und Binnenschifffahrt Wasserstand/Gezeiten Straßenverkehr Wettervorhersage Luftverkehr	EBA GDWS BSH FBA DWD unklar †	tbd
Finanzwesen^	DORA-regulierte Dienstleistungen	BaFin	tbd
Sozialversicherung Grundsicherung	Leistungen Sozialversicherung Arbeitsförderung Grundsicherung	nach SGB oder BA	tbd
Gesundheitswesen	fehlt noch	Länder	tbd
Wasser	fehlt noch	Länder	tbd
Ernährung	fehlt noch	Länder	tbd
IT und TK^	Sprach- und Datenübertragung Datenspeicherung/verarbeitung öffentliche TK-Netze/Dienste	BSI BSI BNetzA	tbd
Weltraum	Betrieb Bodeninfrastrukturen	BAFA	tbd
Entsorgung	fehlt noch	Länder	tbd
Alle Sektoren	Restliche Dienstleistungen	durch BMI Landesbehörden	tbd
Bundesverwaltung §7	Einrichtungen Bund	BMI	tbd

Ausschlüsse

Es gibt diverse Ausnahmen und Sonderregeln für Unternehmen im KRITIS-Dachgesetz.

Betreiber kritischer Anlagen	Fundort	Ausschluss von
Finanzunternehmen (DORA und KrWG) Informationstechnik und Kommunikation Entsorgung Sozialversicherung	**§4 (2)**	Austausch EU §9, §10 Risikoanalyse §12 Resilienz Pflichten §13 Nachweise §16 Meldewesen §18 Beratung §19 (2) Geschäftsleitung §20 Unterlagen BBK §21 (6) Bußgelder §24
Einrichtungen Bundesverwaltung ohne Auswärtiges ohne Verteidigung	**§7 (1)**	*alles ausgeschlossen, bis auf:* Registrierung §8 (1) und §8 (6-7) Risikoanalyse §12 Resilienz Pflichten §13 (1-4) Meldewesen §18 (ohne 8)
Energie Strom, Erdgas, Wasserstoff	**§16 (7)**	§16 (1)-(6) Nachweispflichten
Bundesverwaltung tätig in: nationale Sicherheit, öffentliche Sicherheit, Verteidigung, Strafverfolgung	**§22 (2)**	*Per Ausnahmebescheid* Risikoanalyse §12 Resilienz Pflichten §13 Meldewesen §18
Bundesverwaltung, *ausschließlich tätig in*: nationale Sicherheit, öffentliche Sicherheit, Verteidigung, Strafverfolgung	**§22 (3)**	*Per Ausnahmebescheid* alles

Pflichten von Betreibern

Pflicht	Betreiber kritischer Anlagen
Geltungsbereich	Anlage/Einrichtung
Registrierung **§8**	✓
Risikoanalysen **§12**	✓
Resilienz-Maßnahmen **§13**	✓
Resilienz Plan **§13 (4)**	✓
Nachweise **§16**	✓
Meldepflicht **§18**	✓
Geschäftsleitung **§20**	✓

Risikoanalyse

Betreiber müssen mindestens alle vier Jahre eine Risikoanalyse und Bewertung durchführen, die auf nationalen Risikoanalysen oder anderen vertrauenswürdigen Quellen basieren. **§12 (1)**.

Dabei müssen berücksichtigt werden:

- Risiken der *Nationalen Risikoanalysen* §11
- Risiken der Verfügbarkeit der kritischen Dienstleistung durch Abhängigkeit von anderen Betreibern und anderen Sektoren
- Risiken durch Abhängigkeit anderen Betreibern und anderen Sektoren
- Besonderheiten maritimer Infrastruktur

Resilienz Plan

Betreiber müssen ihre §13 Resilienz-Maßnahmen in einem Resilienz Plan dokumentieren, in dem die Erwägungen der Maßnahmen dargelegt und Bezug zur Risikoanalyse und Bewertung genommen wird. Der Plan ist bei Bedarf und nach Risikoanalysen zu aktualisieren. **§13 (4)**

Maßnahmen

Betreiber müssen Maßnahmen für ihre Resilienz treffen, um Vorfälle zu verhindern, einen angemessenen physischen Schutz der Anlagen und zügige Wiederherstellung der kritischen Dienstleistung zu gewährleisten, auf Vorfälle reagieren und diese abzuwehren. **§13 (1)**

Dazu müssen Betreiber verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen treffen, basierend auf nationalen Risikobewertungen und Analysen, und den Stand der Technik einhalten. **§13 (2)**

Liste an Maßnahmen
Zu den geforderten Maßnahmen nach KRITIS-Dachgesetz können folgende zählen: **§13 (3)**

1. **Auftreten von Vorfällen verhindern**
    - Notfallvorsorge

2. **Angemessener physischer Schutz der Liegenschaften und kritischen Anlagen**
    - Bauliche und technischer Sicherung, Objektschutz, Abgrenzung
    - Überwachung der Umgebung
    - Detektionsgeräte
    - Zugangskontrollen

3. **Reaktion und Abwehr von Vorfällen sowie Folgenbegrenzung**
    - Risiko-Management
    - Krisen-Management und Protokolle
    - Abläufe im Alarmfall (Krisenreaktionspläne)

4. **Wiederherstellung der kritischen Dienstleistung nach Vorfällen**
    - Aufrechterhaltung des Betriebs (Notstrom etc.)
    - Ermittlung alternativer Lieferketten

5. **Sicherheitsmanagement für eigenes und externes Personal**

6. **Schulungen, Übungen, Sensibilisierung für Personal**
    - zu Resilienz Themen in Nr. 1 bis 5

Resilienz-Maßnahmen:

1. **Risikomanagement**
   Identifikation und Bewertung der wichtigsten Risiken sowie Entwicklung von Maßnahmen zur Risikominimierung, um sich auf potenzielle Krisen vorzubereiten.

2. **Redundanzen einbauen**
   Sicherstellung von Backup-Systemen, wie zusätzliche Server oder alternative Lieferanten, um Ausfälle zu kompensieren und den Betrieb aufrechtzuerhalten.

3. **Notfallpläne und Krisenübungen**
   Entwicklung und regelmäßiges Üben von Notfallplänen, um auf Krisen schnell und koordiniert reagieren zu können. Dies schließt Kommunikations- und Evakuierungspläne mit ein.

4. **Psychische Resilienz stärken**
   Maßnahmen zur Stressbewältigung und Mitarbeiterunterstützung, wie z.B. Mental-Health-Programme, Coaching und regelmäßige Pausen, die die Belastbarkeit fördern.

5. **Agiles Arbeiten und Flexibilität**
   Einführung von flexiblen Arbeitsstrukturen, damit Teams schneller auf neue Herausforderungen reagieren können. Agile Methoden ermöglichen es, Prozesse flexibel anzupassen.

6. **Fortlaufende Schulungen und Trainings**
   Kontinuierliche Weiterbildung der Mitarbeiter, um sicherzustellen, dass sie für verschiedene Szenarien vorbereitet sind und neue Fähigkeiten für den Umgang mit Krisen entwickeln.

7. **Kommunikation und Informationssicherung**
   Ein transparentes und gut funktionierendes Kommunikationssystem,
   das im Ernstfall für klare Anweisungen und Informationsflüsse sorgt, ist essenziell.
   Dies umfasst auch IT-Sicherheitsmaßnahmen wie Firewalls, Backups und Datenverschlüsselung.

8. **Kontinuierliche Überprüfung und Anpassung**
   Regelmäßige Evaluierung der Maßnahmen und Anpassungen an neue Herausforderungen, um auf dem aktuellen Stand zu bleiben und Schwachstellen frühzeitig zu beheben.

KRITIS-Dachgesetz für Sicherheitsdienste

Das "KRITIS-Dachgesetz" (Gesetz zur Stärkung der Resilienz kritischer Anlagen) ist direkt relevant für Sicherheitsdienste, da es Vorschriften zum Schutz und zur Aufrechterhaltung kritischer Infrastrukturen in verschiedenen Sektoren enthält. Sicherheitsdienste können dabei eine Rolle spielen, da sie für den physischen Schutz dieser Anlagen verantwortlich sind. Das Gesetz legt fest, dass Betreiber kritischer Infrastrukturen Resilienz Pläne erstellen und Maßnahmen wie Zugangskontrollen, Detektionssysteme und Objektschutz einsetzen müssen, um die Sicherheit zu gewährleisten.

Zusätzlich fordert das Gesetz von Sicherheitsdiensten, dass diese mit Behörden zusammenarbeiten, um den Schutz und die Krisenreaktion zu koordinieren und Gefährdungen für kritische Infrastrukturen frühzeitig zu erkennen und abzuwehren (Kritis gesetzt).

Welche Aufgaben haben Sicherheitsunternehmen dann?

Sicherheitsunternehmen haben nach dem KRITIS-Dachgesetz folgende Aufgaben im Kontext kritischer Infrastrukturen:

1. **Objektschutz und Zugangskontrollen:**
Sicherheitsdienste sind für die physische Absicherung der Anlagen zuständig, was Maßnahmen wie Zugangskontrollen, Überwachung der Umgebung und Sicherung von Gebäudestrukturen umfasst.

2. **Detektions- und Überwachungssysteme:**
Einsatz und Überwachung von Detektionssystemen, um frühzeitig auf Bedrohungen wie unbefugtes Eindringen oder Sabotage reagieren zu können.

3. **Notfall- und Krisenmanagement:**
Sicherheitsdienste unterstützen die Betreiber bei der Entwicklung von Notfallplänen, um auf Vorfälle schnell und effektiv zu reagieren und die Folgen für die kritische Infrastruktur zu minimieren.

4. **Zusammenarbeit mit Behörden:**
Sicherheitsunternehmen arbeiten eng mit Behörden wie dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe zusammen, um bei Bedrohungen informiert zu sein und ggf. Unterstützung bei der Risikobewertung und Vorfallmeldung zu leisten.

5. **Schulung und Vorbereitung des Personals:**
Sicherheitsunternehmen schulen ihre Mitarbeiter und führen regelmäßig Übungen durch, um sicherzustellen, dass das Personal auf die speziellen Anforderungen und möglichen Gefährdungen der kritischen Infrastruktur vorbereitet ist.

Bedingungen, die ein Sicherheitsunternehmen dafür erfüllen muss?

Diese Anforderungen umfassen unter anderem:

1. **Qualifizierte Mitarbeiter:**
   Sicherheitsdienste müssen Personal beschäftigen, das für die speziellen Sicherheitsanforderungen kritischer Infrastrukturen qualifiziert ist, z.B. durch Schulungen in Notfall- und Krisenmanagement, Objektschutz und Bedrohungserkennung.

2. **Sicherheitsüberprüfung des Personals:**
   Mitarbeiter, die in kritischen Infrastrukturen arbeiten, müssen oft sicherheitsüberprüft sein, um sicherzustellen, dass keine sicherheitsrelevanten Risiken bestehen. Dies gilt insbesondere für sensible Bereiche.

3. **Einsatz moderner Sicherheitsmaßnahmen:**
   Der Sicherheitsdienst muss die notwendigen technischen und organisatorischen Schutzmaßnahmen einsetzen, z.B. Überwachungssysteme, Detektionsgeräte und Zugangskontrollen, die dem aktuellen Stand der Technik entsprechen.

4. **Krisenreaktionsfähigkeit:**
   Sicherheitsdienste müssen in der Lage sein, schnell und angemessen auf Vorfälle zu reagieren. Dazu gehören interne Notfallpläne und die Fähigkeit, die Auswirkungen eines Vorfalls zu begrenzen und die Funktion kritischer Infrastrukturen zügig wiederherzustellen.

5. **Zusammenarbeit und Meldepflicht:**
   Sicherheitsdienste müssen mit Behörden zusammenarbeiten und relevante Vorfälle unverzüglich melden, um koordiniert auf Bedrohungen reagieren zu können.

6. **Fortlaufende Schulung und Weiterbildung:**
   Sicherheitsdienste sind verpflichtet, ihr Personal regelmäßig zu schulen und auf den neuesten Stand zu bringen, um neue Bedrohungen und Technologien effizient handhaben zu können.

In der Praxis müssen Sicherheitsunternehmen also sicherstellen, dass ihre Mitarbeiter durch entsprechende Ausbildungen und Qualifikationen die **technischen, organisatorischen und behördlichen Anforderungen des KRITIS-Dachgesetzes** erfüllen.

Grundsätzlich relevante Themen für Sicherheitsmitarbeiter:

Um Sicherheitsmitarbeiter gezielt auf ihre Aufgaben im Rahmen des KRITIS-Dachgesetzes vorzubereiten, sollten folgende Themen in Schulungen behandelt werden:

1. **Grundlagen des KRITIS-Dachgesetzes**
   - Definition und Bedeutung von KRITIS
   - Übersicht der relevanten Sektoren
   - Gesetzliche Pflichten für Betreiber und Sicherheitsdienstleister
2. **Gefahren- und Risikoanalyse**
   - Erkennung und Bewertung potenzieller Bedrohungen (physisch und cyberbezogen)
   - Einordnung von Szenarien wie Sabotage, Terrorismus oder Naturkatastrophen

3. **Rechtliche Grundlagen**
   - Datenschutz (DSGVO, BDSG) und Geheimhaltungspflichten
   - Sicherheitsvorschriften und Haftungsrisiken für Mitarbeiter
   - Zusammenarbeit mit Behörden (Polizei, BSI, Feuerwehr)
4. **Technische Sicherheitsmaßnahmen**
   - Umgang mit Überwachungssystemen (Kameras, Sensorik)
   - Zutrittskontrollsysteme und Alarmtechnik
   - Grundkenntnisse in IT-Sicherheit, z. B. Social-Engineering erkennen

5. **Kommunikation und Verhalten im Ernstfall**
   - Meldung und Eskalation von Sicherheitsvorfällen
   - Notfall- und Krisenmanagement
   - Umgang mit Personen unter Drucksituationen
6. **Präventive Sicherheitsmaßnahmen**
   - Streifen- und Kontrollgänge: Checklisten und Protokollierung
   - Sicherung sensibler Bereiche (z. B. Serverräume, Schaltanlagen)
   - Umgang mit Fremdfirmen und Lieferanten

7. **Verhaltensregeln bei Störungen und Angriffen**
   - Schutz der eigenen Person und der Infrastruktur
   - Evakuierungs- und Sicherungsmaßnahmen
   - Zusammenarbeit im Sicherheitsnetzwerk (interne und externe Partner)
8. **Dokumentation und Berichtswesen**
   - Anforderungen an lückenlose Dokumentation und Berichte
   - Nutzung moderner Tools zur Vorfalls Aufnahme und -analyse

9. **Praktische Übungen und Simulationen**
   - Simulierte Angriffe und Notfälle
   - Evakuierungsübungen und Alarmtests
   - Feedback und Verbesserungspotenziale erkennen
10. **Verhaltensethik und professionelle Haltung**
    - Sensibilisierung für die Bedeutung der Aufgabe im KRITIS-Kontext
    - Verantwortung und Integrität im Umgang mit kritischen Infrastrukturen

1. **Mitarbeiter mit Sachkundeprüfung nach § 34a GewO**

- **Grundlagen KRITIS-Dachgesetz**: Überblick über KRITIS, gesetzliche Pflichten.
- **Rechtliche Grundlagen**: Hausrecht, Befugnisse und Grenzen des Sicherheitsmitarbeiters.
- **Gefahrenwahrnehmung**: Erkennen von Verdachtsmomenten (z. B. unbefugte Personen, verdächtige Objekte).
- **Kommunikation im Ernstfall**: Meldung von Vorfällen an Vorgesetzte oder Behörden.
- **Sicherungsaufgaben**: Zutrittskontrolle, einfache Kontrollgänge, Umgang mit Alarmen.
- **Einfache Notfallmaßnahmen**: Verhalten bei Evakuierungen, Erste Hilfe-Grundkenntnisse.

---

2. **Geprüfte Schutz- und Sicherheitskraft (GSSK)**

- **Erweiterte Kenntnisse des KRITIS-Dachgesetzes**: Verstehen der Verantwortung von KRITIS-Betreibern und Dienstleistern.
- **Gefahren- und Risikoanalyse**: Grundlagen der Bedrohungsbewertung und Prävention.
- **Technische Sicherheitsmaßnahmen**: Bedienung von Überwachungssystemen, Zutrittskontrollen, Grundlagen IT-Sicherheit.
- **Notfall- und Krisenmanagement**: Erste Schritte bei Störungen, Sicherung sensibler Bereiche.
- **Eskalationsmanagement**: Umgang mit Konflikten und Personen unter Druck.
- **Zusammenarbeit mit Behörden**: Rollen und Kommunikation mit Polizei, Feuerwehr, BSI.
- **Dokumentation und Berichterstattung**: Einhaltung von Vorgaben und Protokollierung von Vorfällen.

---

3. **Fachkraft für Schutz und Sicherheit**

- **Detaillierte Analyse des KRITIS-Dachgesetzes**: Umsetzung der Anforderungen im Bewachungsalltag.
- **Erweiterte Gefahrenanalyse**: Systematische Bewertung physischer und cyberbezogener Bedrohungen.
- **Planung von Sicherheitsmaßnahmen**: Entwicklung von Schutzkonzepten, individuelle Anpassung an KRITIS-Sektoren.
- **Führung und Organisation**: Leitung von Teams, Einweisung weniger qualifizierter Mitarbeiter.
- **Technologien und Innovationen**: Einsatz moderner Sicherheitstechnik und Cyberabwehrsysteme.
- **Notfallplanung**: Erstellung und Koordination von Krisenplänen, Durchführung von Übungen.
- **Compliance und Audit-Vorbereitung**: Sicherstellen der Einhaltung von Standards und gesetzlichen Vorgaben.

4. **betriebliche Führungsebene**

1. **Tiefgehendes Verständnis des KRITIS-Dachgesetzes**
   - Überblick über die gesetzlichen Anforderungen und Pflichten.
   - Relevanz der KRITIS-Sektoren und deren Schutzbedarfe.
   - Rolle von Sicherheitsunternehmen im KRITIS-Schutzsystem.
2. **Strategische Gefahren- und Risikoanalyse**
   - Entwicklung von Bedrohungsmodellen für physische und cyberbezogene Risiken.
   - Bewertung von Schutzkonzepten und Identifikation von Schwachstellen.
   - Anpassung an dynamische Bedrohungslagen.

3. **Planung, Umsetzung und Kontrolle von Sicherheitskonzepten**
   - Erstellung effektiver Schutzmaßnahmen für KRITIS-Bereiche.
   - Integration technischer Lösungen wie Zutrittskontrollen, Videoüberwachung und Cyberabwehr.
   - Regelmäßige Überprüfung und Anpassung der Konzepte an aktuelle Standards.
4. **Mitarbeiterführung und Einsatzplanung**
   - Erstellung und Optimierung von Dienstplänen im KRITIS-Umfeld.
   - Schulung und Qualifizierung von Sicherheitsmitarbeitern gemäß KRITIS-Vorgaben.
   - Führung von Teams in kritischen Einsatzsituationen.

5. **Notfall- und Krisenmanagement**
   - Erstellung und Umsetzung von Krisenplänen.
   - Koordination von Maßnahmen bei Vorfällen oder Störungen.
   - Sicherstellung der Betriebsfähigkeit und Kommunikation im Ernstfall.
6. **Kooperation mit Behörden und Betreibern**
   - Aufbau und Pflege von Netzwerken zu Behörden (z. B. Polizei, BSI) und KRITIS-Betreibern.
   - Sicherstellung der Informationsflüsse und Abstimmung der Maßnahmen.
   - Teilnahme an Sicherheitsübungen und Audits.

7. **Rechtliche und finanzielle Verantwortung**
   - Einhaltung von gesetzlichen Vorgaben (KRITIS-Dachgesetz, DSGVO, Arbeitsschutz).
   - Vermeidung von Haftungsrisiken durch Compliance-Maßnahmen.
   - Budgetplanung für Investitionen in Technik und Personalentwicklung.
8. **Qualitäts- und Innovationsmanagement**
   - Implementierung und Überwachung zertifizierter Sicherheitsstandards.
   - Nutzung moderner Technologien (z. B. KI, Drohnenabwehr) zur Effizienzsteigerung.
   - Etablierung eines kontinuierlichen Verbesserungsprozesses.

9. **Berichtswesen und Dokumentation**
   - Erstellung detaillierter Berichte über Vorfälle, Maßnahmen und Audits.
   - Nutzung von Analyseergebnissen zur Optimierung von Sicherheitsmaßnahmen.
   - Sicherstellung der lückenlosen Dokumentation für Prüfbehörden.
10. **Strategische Unternehmensführung und Marketing**
    - Positionierung des Unternehmens als zuverlässiger Partner für KRITIS-Betreiber.
    - Entwicklung langfristiger Kundenbeziehungen und Akquise neuer Auftraggeber.
    - Förderung einer Sicherheitskultur und Stärkung des Unternehmensimages.

Wesentlichen Schritte, die Sicherheitsunternehmen jetzt umsetzten sollten:

Durch diese Maßnahmen können Sicherheitsunternehmen sicherstellen, dass ihr Unternehmen den Anforderungen des KRITIS-Dachgesetzes entspricht und gleichzeitig wettbewerbsfähig bleibt.

1. **Rechtliche Compliance sicherstellen**
   - Überprüfen, ob Kunden als KRITIS-Betreiber gelten und sicherstellen, dass gesetzliche Vorgaben eingehalten werden.

2. **Sicherheitskonzepte anpassen**
   - Schutzkonzepte für KRITIS-Bereiche entwickeln, die sowohl physische als auch cybertechnische Maßnahmen umfassen.

3. **Mitarbeiterschulung**
   - Regelmäßige Schulungen zur KRITIS-Relevanz und Notfallmanagement für Sicherheitskräfte anbieten.

4. **Technologie aufrüsten**
   - Investieren in moderne Sicherheits- und IT-Technologien zum Schutz vor physischen und cybertechnischen Bedrohungen.

5. **Kooperation mit KRITIS-Betreibern und Behörden**
   - Partnerschaften mit KRITIS-Betreibern und relevanten Behörden etablieren und pflegen.

6. **Krisenmanagement optimieren**
   - Notfallpläne und regelmäßige Übungen durchführen, um auf Krisensituationen vorbereitet zu sein.

7. **Marktnische nutzen**
   - Das Unternehmen als spezialisierten Dienstleister für KRITIS-Bereiche positionieren.

8. **Risikomanagement**
   - Ein Risikomanagement-System einführen und Haftungsrisiken überprüfen, um gut abgesichert zu sein.

9. **Dokumentation und Audits**
   - Lückenlose Dokumentation und Vorbereitung auf Audits sicherstellen.

Zentrale Anlaufstellen:

Laut dem KRITIS-Dachgesetz gibt es mehrere zentrale Anlaufstellen für die verschiedenen Bereiche der kritischen Infrastruktur.

1. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)
- Das BBK ist die allgemeine zentrale Anlaufstelle für alle sektorenübergreifenden Fragen und Koordinierungsaufgaben im Rahmen des KRITIS-Dachgesetzes.

2. Bundesministerium des Innern und für Heimat (BMI)
- Zuständig für alle kritischen Dienstleistungen, die von Einrichtungen der Bundesverwaltung erbracht werden.

3. Bundesnetzagentur
- Zuständig für die Bereiche Stromversorgung, Erdgasversorgung, Wasserstoffversorgung und den Betrieb öffentlicher Telekommunikationsnetze oder die Erbringung öffentlich zugänglicher Telekommunikationsdienste.

4. Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Verantwortlich für die Sicherheit in der Sprach- und Datenübertragung sowie der Datenspeicherung und -verarbeitung, die nicht zu öffentlichen Telekommunikationsdiensten gehören.

5. Bundesministerium für Wirtschaft und Klimaschutz (BMWK)
- Zuständig für die Mineralölversorgung.

6. Eisenbahnbundesamt
- Verantwortlich für den Bereich Eisenbahnverkehr, insbesondere für die bundeseigenen Eisenbahnunternehmen.

7. Generaldirektion Wasserstraßen und Schifffahrt
- Zuständig für die See- und Binnenschifffahrt im Bereich der bundeseigenen Wasserstraßeninfrastruktur.

8. Bundesamt für Seeschifffahrt und Hydrographie (BSH)
- Verantwortlich für die Wasserstands- und Gezeitenvorhersagen des Bundes.

9. Fernstraßen-Bundesamt
- Zuständig für die Verkehrssteuerungs- und Leitsysteme sowie intelligente Verkehrssysteme auf Bundesautobahnen und -straßen.

10. Deutscher Wetterdienst (DWD)
- Verantwortlich für Wettervorhersagen im Bundesgebiet.

11. Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)
- Zuständig für kritische Dienstleistungen, die von Unternehmen im Finanzsektor erbracht werden.

12. Bundesministerium für Arbeit und Soziales / Bundesagentur für Arbeit
- Zuständig für Leistungen der Sozialversicherung und Grundsicherung für Arbeitsuchende.

13. Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA)
- Zuständig für den Betrieb von Bodeninfrastrukturen für weltraumgestützte Dienste.

Begriffserklärung:

KRITIS steht für „Kritische Infrastrukturen“. Das sind Einrichtungen und Systeme, die für das Funktionieren unserer Gesellschaft und Wirtschaft essenziell sind. Dazu gehören unter anderem Sektoren wie Energieversorgung, Informationstechnik, Transport, Wasser- und Gesundheitsversorgung. Ein Ausfall oder eine Beeinträchtigung von KRITIS kann erhebliche Auswirkungen auf die öffentliche Sicherheit und das allgemeine Wohl haben.

Der Schutz von KRITIS umfasst Maßnahmen, um Risiken zu minimieren und die Widerstandsfähigkeit gegen Bedrohungen wie Cyberangriffe, Naturkatastrophen oder technische Störungen zu erhöhen.

Resilienz bezeichnet die Fähigkeit, trotz schwieriger oder belastender Umstände psychisch stabil zu bleiben und sich von Rückschlägen oder Krisen zu erholen. Menschen oder Systeme mit hoher Resilienz können sich flexibel an Veränderungen anpassen und aus Herausforderungen gestärkt hervorgehen.

Resilienz-Maßnahmen sind konkrete Schritte, die die Widerstandsfähigkeit gegenüber Krisen und Stresssituationen fördern.

Resilienz-Plan ist ein strukturiertes Dokument, das konkrete Schritte und Maßnahmen festlegt, um die Widerstandsfähigkeit einer Organisation oder Person in Krisen zu stärken und schnell auf unvorhergesehene Ereignisse reagieren zu können.

Quelle:
https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2024/11/kabinett-kritis.html