Albrecht Broemme, Brandassessor, Berlin
Zukunftsforum Öffentliche Sicherheit (ZOES)

November 2023

KRITIS-Dachgesetz und neues BSI-Gesetz zum Verhindern von „Erkenntnis-Ignoranz", „Erkenntnis-Demenz" und „Verantwortungsdiffussion"?

KRITIS-Dachgesetz kontra „Erkenntnis-Ignoranz" und „-Demenz"

Das KRITIS-Dachgesetz setzt die europäische CER-Richtlinie „über die Resilienz kritischer Einrichtungen" vom 27.12.2022 um. Es liegt seit Juli 2023 als Referentenentwurf des Bundesministeriums des Innern und für Heimat vor. Eine Abstimmung mit den Ländern und der Wirtschaft war bis dahin nicht erfolgt.

Das KRITIS-Dachgesetz legt ein „Dach" über alle **elf Sektoren der Kritischen Infrastrukturen (KRITIS)**:

- Energie
- Transport und Verkehr
- Finanz- und Versicherungswesen
- Gesundheit
- Trinkwasser
- Abwasser
- Siedlungsabfallentsorgung
- Informationstechnik und Telekommunikation
- Ernährung
- Weltraum
- Öffentliche Verwaltung

Das KRITIS-Dachgesetz ergänzt bestehende Regelungen im Bereich der IT-Sicherheit Kritischer Infrastrukturen.

Ausgangspunkt sind alle denkbaren Risiken, die durch die Natur oder den Menschen verursacht werden können **(„All-Gefahren-Ansatz")** – sei es ein Unwetter, menschliches Versagen oder ein Sabotageakt.

Das KRITIS-Dachgesetz nimmt alle Kritischen Infrastrukturen in den Blick und definiert, welche Unternehmen und Einrichtungen mit Blick auf den physischen Schutz für die Gesamtwirtschaft verpflichtende Resilienzmaßnahmen ergreifen müssen. Zwei Kriterien müssen erfüllt sein: Wenn eine Einrichtung

1. essenziell für die Gesamtversorgung in Deutschland ist und
2. mehr als 500.000 Personen versorgt,

zählt sie zu den „kritischen Anlagen", die vom KRITIS-Dachgesetz erfasst sind. Die Verwendung des Begriffs „Anlagen" statt „Betriebe" hier muss vom Gesetzgeber noch erläutert werden.

Mit dem Gesetz werden auch die **wechselseitigen Abhängigkeiten** der Kritischen Infrastrukturen untereinander berücksichtigt: So hängen

zum Beispiel vom Energiesektor auch alle anderen Sektoren ab. Auch Wasser und Transportwege sind für die jeweils anderen Sektoren unverzichtbar.

Die Zusammenarbeit aller Beteiligten bei Kritischen Infrastrukturen soll institutionalisiert werden. Die Verantwortlichkeiten der Vielzahl der am Schutz Kritischer Infrastrukturen Beteiligten soll klarer herausgearbeitet werden. Bei der Umsetzung des KRITIS-Dachgesetzes soll das **Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) eine koordinierende Rolle** bekommen. Es wird eng mit den zuständigen Aufsichtsbehörden des Bundes zusammenarbeiten.

U.a. die Innenministerkonferenz weist darauf hin, dass keine parallelen Meldewege geschaffen werden dürfen. Es muss klar sein, wann eine Einrichtung der KRITIS wohin was zu melden hat (ein-eindeutige Melde- und Berichtswege).

Die Koordinierungsstelle Sicherheitswirtschaft (KoSi) im DIN hat im Juli 2023 ein hilfreiches „Whitepaper zur Normung und Standardisierung bei der Ausgestaltung des KRITIS-Dachgesetzes" veröffentlicht.

NIS2-Richtlinie kontra „Verantwortungsdiffussion"

Staatliche und privatwirtschaftlich Bereiche von KRITIS werden in Europa vermehrt Opfer von Hacker-Angriffen. Meistens handelt es sich um kriminelle Erpressungsversuche (siehe auch GRÜNBUCH des ZOES 2020).

2016 verabschiedete die EU die NIS-Richtlinie, die in Deutschland mit dem IT-Sicherheitsgesetz („BSI-Gesetz") umgesetzt wurde. Im Dezember 2022 wurden mit der NIS2-Richtlinie die europäischen Vorgaben verschärft. Sie muss bis zum 17. Oktober 2024 in allen Mitgliedsstaaten umgesetzt sein. Infolge des erweiterten Geltungsbereiches hinsichtlich der Sektoren und der Betriebsgröße ist eine zigfach größere Anzahl von Betrieben und Verwaltungen betroffen.

Es gibt insgesamt 18 definierte Sektoren, nämlich elf Sektoren mit hoher Kritikalität und sieben sonstige Sektoren. Die Sektoren sind in Teilsektoren untergliedert. Ausdrücklich erfasst sind KMU (kleine und mittlere Unternehmen). Mittlere Unternehmen beschäftigen zwischen 50 und 250 Mitarbeitern mit einem Jahresumsatz von 10 bis 50 Mio. Euro, kleine Unternehmen beschäftigen weniger als 50 Mitarbeiter mit einem Jahresumsatz von bis zu 10 Mio. Euro.

Die **elf Sektoren mit hoher Kritikalität** sind:

- Digitale Infrastruktur
- Verwaltung von IKT-Diensten
- Energie
- Finanzmarkt-Infrastrukturen
- Trinkwasser
- Abwasser
- Verkehr
- Bankwesen

- Öffentliche Verwaltung
- Gesundheitswesen
- Weltraum

Die **sieben sonstigen Sektoren** sind:

- Anbieter Digitaler Dienste
- Post- und Kurierdienste
- Produktion, Handel und Herstellung mit chemischen Substanzen
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln
- Verarbeitendes Gewerbe und Herstellung von Waren
- Forschung
- Abfallbewirtschaftung

Das „BSI-Gesetz" wird zur Umsetzung der NIS2-Richtlinie angepasst werden.

Folgende Maßnahmen sollen die Widerstandsfähigkeit der EU-Mitgliedsstaaten verbessern:

- Technologien für Desaster Recovery
- Technologien für Business Continuity
- Systeme zur Angriffserkennung (auch wenn der Angriff nicht erfolgreich war)
- Einführung einer Multi-Faktor-Authentifizierung (MFA) für Systemzugriffe
- Schulungen und Sensibilisierung des Personals
- Konzepte zur Bewertung der Wirksamkeit des Risikomanagements, die u.a. die regelmäßige Überprüfung der getroffenen Maßnahmen für IT-Bedrohungen erfordern

In angemessenem Umfang gilt dies auch für die Lieferketten.

Die vorgegeben Fristen werden knapp und unmissverständlich sein: Jeder KRITIS-Betreiber muss meldepflichtige Vorfälle **innerhalb von 24 Stunden dem BSI melden** und **innerhalb von 72 Stunden eine erste Bewertung mit Angabe des Schweregrades** abgeben. Und spätestens **nach einem Monat muss ein Abschlussbericht dem BSI vorliegen**. Insbesondere die 24-Stunden-Frist ist eine Herausforderung sowohl für jeden KRITIS-Betreiber (das sind auch Kommunen!), als auch für das BSI, denn Wochenenden und Feiertage zählen mit. Meldepflichtig sind nicht nur tatsächlich erfolgte Cyberangriffe, sondern auch **Cyberangriffsversuche**. Vermutlich gibt es dann täglich und rund um die Uhr tausende von Meldungen an das BSI.

Ein wichtiger Punkt wird die **Verantwortlichkeit der Unternehmens- bzw. Behördenspitze sein, die nicht delegierbar ist**. Wenn z.B. infolge eines Cyberangriffs die Wasserversorgung unterbrochen wird und deswegen Menschenleben zu beklagen sind, muss sich die Chefin oder der Chef der Wasserbetriebe gerichtlich verantworten. Der Verweis auf vermeintlich gut geregelte Zuständigkeiten hilft dann nichts.

Das KRITIS-DG und das BSI-Gesetz müssen miteinander abgestimmt werden. Insbesondere Schwellen und Meldewege sind klar zu regeln.