10. Sicherheit für Kritische Infrastrukturen

In einer zunehmend komplexen und vernetzten Welt, in der Abhängigkeiten zwischen verschiedenen Sektoren allgegenwärtig sind, ist die Sicherheit Kritischer Infrastrukturen (KRITIS) ein zentrales Element gesellschaftlicher Stabilität und Ordnung. Der Schutz dieser lebenswichtigen Einrichtungen und Anlagen, von der Energie- und Wasserversorgung über das Gesundheitswesen bis hin zu Kommunikations- und Verkehrssystemen, ist für das Wohlergehen und die Sicherheit der deutschen Gesellschaft von zentraler Bedeutung.

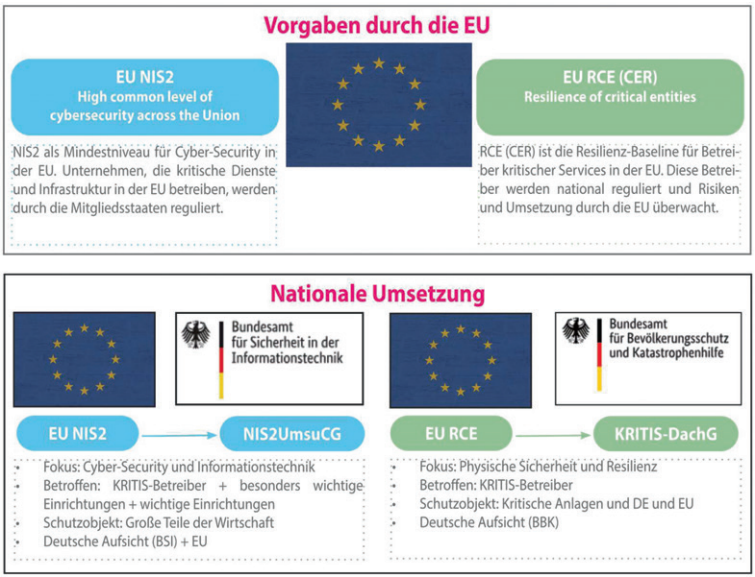
Jüngste Entwicklungen und Bedrohungsszenarien zeigen, wie verwundbar die deutschen Infrastrukturen durch gezielte Angriffe, Naturkatastrophen und technisches Versagen sind.

10.1. Bedeutung und gesetzlicher Rahmen

Die EU hat in den letzten Jahren zwei zentrale Richtlinien eingeführt, um den Schutz kritischer Infrastrukturen zu verbessern,

- die CER-Richtlinie (Critical Entities Resilience) – auch bekannt unter dem Namen „RCE-Richtlinie“ (Resilience of Critical Entities) – zur Stärkung der physischen Resilienz, die in Deutschland durch das sogenannte **„KRITIS-Dachgesetz“** umgesetzt werden soll, und

- die NIS2-Richtlinie für die Stärkung der Cybersicherheit, die durch das **NIS2-Umsetzungsgesetz** realisiert wird.



KRITIS-Dachgesetz – Überblick

Das KRITIS-Dachgesetz verpflichtet Betreiber kritischer Infrastrukturen, auf Bundesebene einheitliche Mindeststandards für den physischen Schutz ihrer Anlagen einzuhalten. Die Vorgaben sind risikobasiert und greifen sektorenübergreifend; dazu gehören regelmäßige Risikoanalysen und Bewertungen. Ein zentrales Meldesystem sorgt dafür, dass erhebliche physische Störungen schnell und koordiniert erfasst werden. Die Koordination und Aufsicht dieses Schutzkonzepts übernimmt das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK).

NIS2-Umsetzungsgesetz – Überblick

Das NIS2-Umsetzungsgesetz weitet die Pflichten zur Cybersicherheit erheblich aus und betrifft nun alle Unternehmen und Einrichtungen, die kritische Dienstleistungen erbringen. Das Gesetz bezieht zusätzliche Sektoren und eine Vielzahl weiterer Unternehmen ein, etwa aus dem verarbeitenden Gewerbe und digitalen Bereich. Es fordert umfassende Sicherheitsmaßnahmen sowie Melde- und Nachweispflichten gegenüber dem BSI, die regelmäßig und stichprobenhaft überprüft werden. Die Einhaltung dieser Vorgaben muss alle drei Jahre nachgewiesen werden. Bei Verstößen drohen empfindliche Sanktionen und hohe Bußgelder, um die Umsetzung der gesetzlichen Anforderungen sicherzustellen.

10.2. Ganzheitliches Sicherheitskonzept

Sowohl das KRITIS-Dachgesetz als auch das NIS-II-Umsetzungsgesetz fordern von Betreibern kritischer Infrastrukturen eine systematische Identifikation, Bewertung und Behandlung von Risiken. Diese Anforderungen entsprechen unmittelbar dem Grundgedanken der ISO 31000 (Risikomanagement – Leitlinien), die ein international anerkanntes Rahmenwerk für das Risikomanagement bereitstellt.

Ein Sicherheitskonzept nach ISO 31000 integriert bauliche, technische, organisatorische und personelle Schutzmaßnahmen. Es beschreibt Risiken, bewertet diese und leitet geeignete Maßnahmen ab. Ziel ist eine nachweisbare Resilienzsteigerung durch kontinuierliche Überprüfung und Anpassung.

Ablauf Gefahren- und Risikoanalyse (Ableitung aus ISO 31000)