Im Fadenkreuz

Regulatorische Anforderungen an die Resilienz kritischer Infrastruktur

16. April 2025

„Wir befinden uns schon lange nicht mehr im Frieden, weil wir täglich angegriffen werden." – Generalleutnant André Bodemann.

Deutschland ist zunehmend Ziel niederschwelliger (hybrider) Angriffe. Diese reichen von Desinformationen über Ausspähung bis hin zu Sabotage. Häufig betroffen ist die kritische Infrastruktur – etwa Energie- und Wasserversorgung, Transport und Verkehr sowie Informationstechnik und Telekommunikation. Dadurch rückt die **Resilienz von Unternehmen**, insbesondere solche der **kritischen Infrastruktur,** verstärkt auch in den Fokus gesetzlicher Regulierung. Grund genug zu beleuchten, inwiefern die Wirtschaft in Deutschland derzeit und zukünftig in die Verantwortung genommen wird, sich gegen Angriffe zu schützen und im Krisenfall zu reagieren.

Der Status quo: Mehrfach-Regulierung mit Schwerpunkt IT-Sicherheit

Ein übergreifendes Gesetz zur Sicherstellung eines Resilienz-Mindeststandards der Wirtschaft existiert bislang nicht. Stattdessen wurden einzelne Schutzaspekte in spezifischen Fachgesetzen verankert, auch zur Umsetzung europäischer Vorgaben. Es besteht eine **Mehrfach-Regulierung** mit je nach Sektor unterschiedlichen Anforderungen:

Im Fokus steht bislang die **Sicherheit von Netz- und Informationssystemen (IT-Sicherheit)**. Das BSI-Gesetz (*BSIG*) – mehrfach erweitert durch das IT-Sicherheitsgesetz von 2015, die NIS-Richtlinie von 2016 und das IT-Sicherheitsgesetz 2.0 von 2021 – verpflichtet die Betreiber kritischer Infrastrukturen zu angemessenen Vorkehrungen zur Sicherstellung – u.a. – der Integrität ihrer Systeme. Wer Betreiber ist, definiert die BSI-KritisVO. Abseits der IT-Sicherheit existieren bislang keine **sektorenübergreifenden** Vorgaben zur physischen Resilienz kritischer Infrastrukturen.

Daneben bestehen teilweise sektorspezifische IT-Sicherheitsvorgaben. So werden die Betreiber bzw. Anbieter öffentlicher Telekommunikationsnetze und -dienste durch das Telekommunikationsgesetz (*TKG*, § 165 Abs. 2 und 3) und die Betreiber von Energieanlagen und -versorgungsnetzen durch das Energiewirtschaftsgesetz (*EnWG*, § 11 Abs. 1a ff.) zu einem angemessenen Schutz ihrer IT-Sicherheit verpflichtet. Dabei konkretisieren die IT-Sicherheitskataloge der BNetzA sowohl die Anforderungen als auch wer unter die Regulierung fällt.

Derartige **sektorspezifische** Vorschriften zielen zwar primär darauf ab, die Versorgungssicherheit im regulären Betrieb zu gewährleisten und im Krisenfall schnell wieder-

herzustellen. Damit tragen sie indirekt aber auch zur Resilienz gegen hybride Bedrohungen bei. Etwa sind pharmazeutische Unternehmen zur Sicherstellung einer kontinuierlichen Versorgung mit Arzneimitteln verpflichtet, § 52b AMG.

Neue sektorenübergreifende Vorhaben: NIS-2 und KRITIS-Dachgesetz

Die Richtlinie (EU) 2022/2555 (sog. ***NIS-2-Richtlinie***) soll die Anforderungen an die **IT-Sicherheit** in der EU weiter erhöhen. Sie führt neue Kategorien ein („wesentliche" und „wichtige" Einrichtungen) und weitet den Anwendungsbereich erheblich aus, von bisher ca. 2.000 auf bis zu 30.000 betroffene Unternehmen. Der Gesetzentwurf der Ampelkoalition zur Umsetzung der NIS-2-Richtlinie sah eine umfassende Reform des BSIG vor, ohne die Mehrfach-Regulierung in EnWG und TKG aufzulösen. Die Verabschiedung des Umsetzungsgesetzes ist der Ampelkoalition nicht mehr gelungen, obwohl die Umsetzungsfrist bereits im Oktober 2024 endete. In Anbetracht des von der EU-Kommission mittlerweile eingeleiteten Vertragsverletzungsverfahrens gegen Deutschland steht die zukünftige Bundesregierung unter Handlungsdruck.

Ähnliches gilt für das **KRITIS-Dachgesetz**. Dieser Gesetzentwurf der Ampelkoalition sollte erstmals eigenständige und sektorenübergreifende Anforderungen an die **physische Resilienz** kritischer Infrastrukturen etablieren und zugleich die Richtlinie (EU) 2022/2557 (sog. ***CER-Richtlinie***) umsetzen. Ziel war es, die Betreiber kritischer Infrastruktur zur Durchführung von Risikobewertungen, Erstellung von Resilienzplänen und Entwicklung branchenspezifischer Resilienzstandards und damit zu geeigneten und verhältnismäßigen Maßnahmen zum physischen Schutz der Anlagen zu verpflichten. Auch das KRITIS-Dachgesetz wurde nicht mehr verabschiedet. Da jedoch auch die CER-Richtlinie bis Oktober 2024 umzusetzen war, besteht auch hier dringender Handlungsbedarf.

Fazit

Bisher beschränken sich Resilienzanforderungen vorwiegend auf die IT-Sicherheit. Die NIS-2-Richtlinie verschärft diese Vorgaben und erfasst deutlich mehr Unternehmen, wurde aber noch nicht umgesetzt. Über die IT-Sicherheit hinaus bestehen bislang keine sektorenübergreifenden Anforderungen. Das KRITIS-Dachgesetz hätte dies erstmal geändert, wurde jedoch nicht verabschiedet. Damit steht auch die Umsetzung der CER-Richtlinie noch aus. Aufgrund des Diskontinuitätsprinzip müssen diese Vorhaben neu in den Bundestag eingebracht werden. Klar ist: Angesichts der aktuellen Bedrohungslage werden künftige Regelungen IT-Sicherheit und physische Resilienz zunehmend ganzheitlich abbilden. Unternehmen sollten sich frühzeitig darauf vorbereiten.

BLOMSTEIN berät umfassend zu Fragen der Verteidigung und Sicherheit und verfolgt die aktuellen legislativen Entwicklungen aufmerksam. Dr. Christopher Wolters und Dr. Leonard von Rummel stehen Ihnen bei Fragen gerne zur Verfügung.