Quelle: Song_about_Summer – stock.adobe.com

Bild 1: *Neue Regularien sollen mehr Sicherheit für Kritische Infrastrukturen bringen*

Sicherheitsaspekte für Kritische Infrastrukturen

Quo vadis, Kritis?

Kritische Infrastrukturen (Kritis) gehören zu den lebenswichtigen und verletzlichen Sektoren einer Volkswirtschaft. Dies zeigen die physischen Sabotageangriffe auf Steuerungskabel der Deutschen Bahn oder die Nord-Stream-Pipelines im Herbst 2022. Um die richtigen Vorkehrungen und Entscheidungen zu treffen, müssen Hersteller und Betreiber von Kritis-Komponenten sowohl die aktuellen gesetzlichen als auch die regulatorischen Entwicklungen im Blick haben.

Nachdem ein Sonderlagebericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) 2022 nahegelegt hatte, dass Deutschland zum Ziel politisch motivierter Cyberangriffe werden könne, ist der Schutz von Kritischen Infrastrukturen stärker in den Fokus gerückt. Das Deutsche Bundeskabinett legte am 7. Dezember 2022 die »Eckpunkte für das Kritis-Dachgesetz« vor und machte damit deutlich: Bei Kritis handelt es sich um Industriezweige, die der Staat durch besondere Maßnahmen – klassisch »physisch« sowie digital »cybertechnisch« – schützen muss, und durch begleitende Verordnungen und Gesetze absichern und regulieren wird.

Vorlieferanten kritischer Komponenten betroffen

Nach der Verabschiedung des IT-Sicherheitsgesetzes 2.0 im Mai 2021, das als sogenanntes Artikelgesetz unter anderem das BSI-Gesetz geändert hat, gelten für Kritis-Betreiber seitdem neue, verschärfte Sicherheitsanforderungen. Davon betroffen sind auch der neu hinzugekommene Kritis-Sektor »Siedlungsabfallentsorgung« und die Gruppe »Unternehmen von besonderem öffentlichem Interesse (UBI)«.

Auch der Kreis und die Anzahl der betroffenen und regulierten Unternehmen wurde durch neue Definitionen und Schwellenwerte erweitert. Konkret werden mit dem § 9b BSIG erstmals auch Hersteller bzw. Vorlieferanten von kritischen Komponenten beim Einsatz in Kritis in die gesetzliche Pflicht genommen, Stichwort »Prüfung auf Vertrauenswürdigkeit« und »Garantieerklärung«. In der Öffentlichkeit ist dies besser bekannt als »Lex Huawei« beim Aufbau des 5G-Mobilfunknetzes in Deutschland. Der aktuelle Rechtsrahmen für Kritische Infrastrukturen ist im BSI-Gesetz, insbesondere in den Paragrafen 8a ff., sowie in der Kritis-Verordnung 2.0 kodifiziert.

Richtlinie auf EU-Ebene

Deutschland hat mit dem IT-Sicherheitsgesetz 2.0 eine Vorreiterrolle übernommen und ist seinen europäischen Kollegen und deren EU-NIS-2-Richtlinie (Netz- und Informationssicherheit) wie bereits bei der NIS-1-Richtlinie inhaltlich und zeitlich zuvorgekommen. Das strenge IT-Sicherheitsgesetz 2.0 dürfte bereits Teile der neuen NIS-2-Richtlinie umgesetzt haben. Eventuell noch fehlende Teile würden möglicherweise durch das »IT-Sicherheitsgesetz 3.0« und das geplante Kritis-Dachgesetz in nationales Recht umgesetzt werden. Dasselbe Umsetzungsszenario gilt auch für die EU RCE-Richtlinie (Resilience of Critical Entities), auch CER-Richtlinie genannt. Das Thema Resilienz spiegelt sich dementsprechend auch im geplanten Kritis-Dachgesetz wider.

Kritis-Dachgesetz zielt auf ganzheitliche Resilienz

Die wichtigsten Eckpunkte für ein Kritis-Dachgesetz:

- **1. Die Physische Sicherheit soll erstmals gesetzlich reguliert werden.** Dies bedeutet eine verpflichtende Umsetzung einheit-

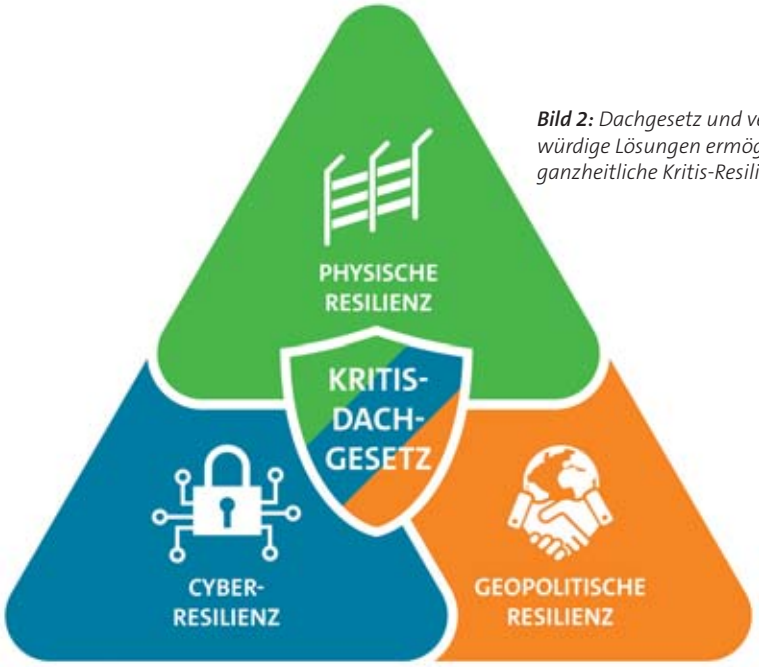
licher technischer Mindestschutzstandards, u. a. mit Detektionssystemen und Systemen zur Umgebungsüberwachung, zum Beispiel durch Videoüberwachung.

- **2. Definition und Erweiterung der betroffenen Kritis-Unternehmen**, sowohl durch einen neuen Sektor (Raumfahrt/Weltraum) als auch durch klare, einheitliche Definitionen, wer zu Kritis gehört, nach qualitativen und quantitativen Kriterien.
- **3. »Vertrauenswürdigkeitsprüfung« von Herstellern:** Bei kritischen IT-Komponenten fordert das BSI-Gesetz (§ 9b Abs. 3 BSIG) Garantieerklärungen über die Vertrauenswürdigkeit des Herstellers. Bei sonstigen, kritischen Nicht-IT-Komponenten gilt: Für einen umfassenden Schutz werden Regelungen geprüft, um Kritis vor Einflüssen und Abhängigkeiten von bedenklichen Herstellern aus dem Ausland zu schützen.
- **4. Ganzheitliche Resilienz als Ziel:** Physische Sicherheit und Cybersicherheit gemeinsam und übergreifend »denken«, überwachen und prüfen (Security Convergence). Erhöhung der geopolitischen Resilienz durch obigen optionalen Punkt »Prüfung bedenklicher Hersteller aus dem Ausland«. Kohärenz beim Cyberschutz und beim physischen Schutz, auch durch enge Zusammenarbeit zweier Aufsichtsbehörden: BSI und BBK (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe).
- **5. Einbettung in den EU-Rechtsrahmen:** Umsetzung der EU CER-Richtlinie über die Resilienz Kritischer Infrastrukturen sowie Umsetzung der EU-NIS-2-Richtlinie.
- **6. Gesetz und gesetzgeberischer Umsetzungsprozess**, geplant für das Jahr 2023.

Regulierung von Cybersicherheit und »physischer Resilienz«

Nach der Einschätzung von Dallmeier electronic steht hinter dem geplanten Kritis-Dachgesetz die politische Erkenntnis, dass für den Schutz und die Resilienz von Kritis kein fragmentierter und unkoordinierter, sondern ein ganzheitlicher und hybrider Ansatz verfolgt werden muss. Nur eine Art »ganzheitlicher Schutzschirm« für Kritische Infrastrukturen ist zielführend.

Was heißt das konkret? Derzeit gibt es mit dem IT-Sicherheitsgesetz und dem BSI-Gesetz bereits einzelne Regelungen für Kritis-Betreiber zur Cybersicherheit, aber eben nur zur Cybersicherheit. Auch für die physische Sicherheit gibt es Regelungen, allerdings nur für einzelne Kritis-Sektoren wie im Luftsicherheitsgesetz. Bundesweite, sektoren- und gefahrenübergreifende Dachregelungen zur physischen Sicherung Kritischer Infrastrukturen gibt es bisher nicht.



Quelle: Dallmeier

Bild 2: *Dachgesetz und vertrauenswürdige Lösungen ermöglichen eine ganzheitliche Kritis-Resilienz*

Dallmeier electronic hält die geplanten Regelungen und den Schritt zu mehr physischer Sicherheit aus geopolitischer und sicherheitspolitischer Sicht für begrüßenswert – insbesondere im Hinblick auf die Versorgungsautonomie, Unabhängigkeit und Business Continuity der Kritischen Infrastrukturen. Darüber hinaus wäre ein solches Dachgesetz auch aus pragmatischen Gründen wünschenswert, wie z. B. rechtsverbindliche Definitionen von Kritis-Einrichtungen und klare Zuständigkeiten.

NDAA in den USA: Verbot bestimmter Videotechnik

Bei Herstellern aus Drittstaaten können nach § 9b BSIG Hersteller oder Vorlieferanten kritischer Komponenten in die gesetzliche Pflicht genommen werden. Die USA gehen im Bereich der Cyber- und geopolitischen Resilienz noch restriktiver vor: So verbietet das Bundesgesetz NDAA (National Defense Authorization Act) seit 2019 den Einsatz von Produkten zweier großer chinesischer Videotechnikhersteller in Projekten, die die öffentliche Sicherheit, die Sicherheit von Regierungseinrichtungen und die Sicherheit Kritischer Infrastrukturen betreffen.

Ähnliche Verbotstendenzen sind auch in Großbritannien und anderen Ländern zu beobachten. Auch die Nato und die EU haben im Januar 2023 eine engere Zusammenarbeit beim Schutz von Kritis vereinbart, insbesondere vor dem Hintergrund geopolitischer Risiken durch autoritäre Akteure.

»Made in Germany« versus »bedenkliche Hersteller«

Der Regensburger Hersteller Dallmeier electronic stellt fest, dass der Markt für Videotechnik die Gütesiegel »Made in Europe« und »Made in Germany« zunehmend als Zeichen für Qualität, Sicherheit und Vertrauen wahrnimmt. Errichter und Endkunden fragen verstärkt entsprechende Produkte nach. Es kann daher im Sinne der Kritis-Gesamtsicherheit nur positiv sein, wenn zu diesem Markttrend auch eine »mittelbar steuernde« gesetzliche Regelung im BSI-Gesetz oder in einem kommenden Kritis-Dachgesetz hinzukommt. Mittelbar steuernd in Bezug auf vertrauenswürdige Hersteller, Produkte und Komponenten und damit letztlich unmittelbar steuernd zur Stärkung der physischen, cyber- und geopolitischen Resilienz.

Im Entwurf des Kritis-Dachgesetzes vom Dezember 2022 bietet der Staat an, Kritis-Betreiber mit Handlungsleitfäden zu unterstützen. Zum Thema Videotechnik stellt Dallmeier in seinem kostenlosen Praxisleitfaden »Videotechnologie und Sicherheit für Kritische Infrastrukturen« auf seiner Homepage ***www.dallmeier.com/de/kritis-praxisleitfaden*** entsprechende Informationen bereit.

Autor:
Jürgen Seiler, Geschäftsführer, davidiT GmbH, Consultingunternehmen der Dallmeier Gruppe, Regensburg