KRITIS-Verordnung -
Wer fällt darunter und was ist zu tun?

Benjamin Zietlow
Rechtsanwalt

Blanke Meier Evers
Rechtsanwälte in Partnerschaft mbB

Agenda

- Hintergrund/Definition
- Wer fällt unter die Verordnung?
- Welche Pflichten bestehen?
- Ausblick

Hintergrund

- IT-Sicherheitsgesetze von 2015 und 2021 haben Regelungen zu Kritischer Infrastruktur eingeführt (u.a. BSIG, EnWG, KritisV).
- Ziel: Verbesserung der IT-Sicherheit von Unternehmen mit erheblicher Bedeutung für die Daseinsvorsorge (z. B. auch Energie).
- Einfallstore: Fernsteuerbarkeit für Direktvermarktung (§ 10b EEG) und Netzbetreiber (§ 13 EnWG), sonstige Zugriffsmöglichkeiten durch Betriebsführer, Hersteller etc., Parkwart (Schlüssel).
- Keine abstrakte Gefahr, Angriffe auf Unternehmen der Branche Anfang des Jahres 2022 zeigen Relevanz.

Was sind Kritische Infrastrukturen?

- Definition § 2 Abs. 10 Satz 1 BSIG:

  „Kritische Infrastrukturen i.S.d. Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die den ***Sektoren Energie****, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung angehören und von* ***hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen der öffentlichen Sicherheit eintreten würden****.“*

- § 2 Abs. 10 Satz 2 BISG: nähere Bestimmung in KritisV

Anlagenkategorien und Schwellenwerte im Sektor Energie (Auszug aus Anhang 1 zur KritisV)

Anlagenkategorie	Bemessungskriterium	Schwellenwert
Erzeugungsanlage	installierte Nettonennleistung in MW	104
	installierte Nettonennleistung in MW, wenn Anlage als Schwarzstartanlage nach BK-18-249 kontrahiert ist	0
	installierte Nettonennleistung in MW, wenn die Anlage zur Erbringung von Primärregelleistung nach § 2 Nr. 8 StromNZV präqualifiziert ist	36
Anlage oder System zur Steuerung/Bündelung elektrischer Leistung (z. B. Leitwarten, Umspannwerke etc.)	installierte Nettonennleistung in MW	104
	installierte Nettonennleistung in MW, wenn Anlage als Schwarzstartanlage nach BK-18-249 kontrahiert ist	0
	installierte Nettonennleistung in MW, wenn die Anlage zur Erbringung von Primärregelleistung nach § 2 Nr. 8 StromNZV präqualifiziert ist	36

Anlagenzusammenfassung & Betreiberbegriff nach KritisV

- **Anlagenzusammenfassung**, § 1 Abs. 2 Satz 2 KritisV:

  „Mehrere Anlagen derselben Kategorie, die durch einen betriebstechnischen Zusammenhang verbunden sind, gelten als gemeinsame Anlage, wenn sie gemeinsam zur Erbringung derselben kritischen Dienstleistung notwendig sind.“

- **Betreiberbegriff**, § 1 Abs. 1 Nr. 2 KritisV:

  *„Eine natürliche oder juristische Person, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände **bestimmenden Einfluss** auf die Beschaffenheit und den Betrieb einer Anlage oder Teilen davon ausübt.“*

Pflichten der Betreiber kritischer Infrastruktur

Wer?	Betreiber von Energieanlagen (und Netzbetreiber)	Betreiber von sonstiger Kritischer Infrastruktur
Rechtsgrundlage	§ 11 EnWG	§§ 8a und 8b BSIG
Registrierung & Benennung Kontaktstelle	Registrierung und Benennung einer Kontaktstelle beim BSI bis spätestens zum ersten Werktag ab dem man als Betreiber Kritischer Infrastruktur gilt; ab dem **1. April** des Kalenderjahres, das auf Überschreitung des Schwellenwertes folgt (Anhang 1, Teil 1 Nr. 3 KritisV).	
Schutzpflichten	- § 11 Abs. 1b EnWG*: „angemessener Schutz gegen Bedrohungen für TK- und EDV-Systeme zu gewährleisten, die für einen sicheren Anlagenbetrieb notwendig sind“.* - **IT-Sicherheitskatalog der BNetzA** (Implementierung und Zertifizierung eines ISMS). - Ab **1. Mai 2023** auch System zur Angriffserkennung.	- § 8a Abs. 1 BSIG: *„angemessene organisatorische und technische Vorkehrungen zur Vermeidung und Störung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind“.* - Nachweis durch Umsetzung **branchenspezifischen Sicherheitsstandards (B3S)**; erstmals nach 2 Jahren und dann wiederkehrend alle 2 Jahre. - Ab **1. Mai 2023** auch System zur Angriffserkennung.
Meldepflichten	Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der von ihnen betriebenen Kritischen Infrastruktur geführt haben bzw. bei erheblichen Störungen auch, wenn sie zu erheblichen Beeinträchtigungen führen können. Im zweiten Fall kann die Meldung anonym erfolgen.	

Überwachung & Pflichtverstöße

- **BNetzA** (bei Energieanlagen) bzw. **BSI** (sonstige Kritische Infrastruktur) haben **Überwachungsbefugnis** bzgl. Einhaltung der Pflichten, **inkl. Zutritts- und Informationsrechten** ggü. Betreiber (§ 11 Abs. 1b Satz 7 EnWG/ § 8a Abs. 4 BSIG).

- Je nach festgestelltem **Pflichtverstoß** drohen erhebliche **Bußgelder** bei **Energieanlagen** (und Netzbetreibern) **bis zu 100.000,00 Euro** (§ 95 EnWG) bzw. bei **sonstiger Kritischer Infrastruktur bis zu 2 Mio. Euro** (§ 14 BSIG).

Ausblick

- **Änderungen der EU-Richtlinie zur Netz- und Informationssicherheit (NIS 2)**
- **Umsetzung in deutsches Recht erforderlich**
- **Wesentliche diskutierte Änderungen:**
  - **Weitere Sektoren.**
  - **Umstellung der Schwellenwerte auf Jahresumsatz und Mitarbeiteranzahl.**
  - **Europäisches Register für Sicherheitslücken bei ENISA** (European Network and Information Security Agency).
  - **Meldepflichten werden vereinfacht.**
  - **Höhere Bußgelder.**

NIS 2

Vielen Dank für Ihre Aufmerksamkeit!

BLANKE MEIER EVERS
Rechtsanwälte in Partnerschaft mbB

Benjamin Zietlow
b.zietlow@bme-law.de

Stephanitorsbollwerk 1 (Haus LEE)
28217 Bremen
Tel.: +49 421 94946-0
Fax: +49 421 94946-66
www.bme-law.de