BRAHMS NEBEL & KOLLEGEN

Cybersicherheit und KRITS-Dachgesetz

33. Windenergietage Potsdam // 14.11.2025 von 11:00 – 11:30 Uhr

Rechtsanwalt Dr. Mirko Sauer und Rechtsanwalt Dr. Florian Brahms

Cybersicherheit und KRITS-Dachgesetz

REFERENTEN //

BN//K
BRAHMS NEBEL & KOLLEGEN

Connect on LinkedIn

Dr. Mirko Sauer,

BRAHMS NEBEL & KOLLEGEN

Connect on LinkedIn

Dr. Florian Brahms,

BRAHMS NEBEL & KOLLEGEN

01 // CYBERSICHERHEIT FÜR KRITISCHE INFRASTRUKTUREN

RECHTSGRUNDLAGEN //

BRAHMS NEBEL & KOLLEGEN

Die rechtlichen Grundlagen für Cybersicherheit bei Kritischen Infrastrukturen in der Energiewirtschaft:

- BSI-Gesetz
- BSI-KritisV
- EnWG
- NIS-2-Richtilinie (EU) 2022/2555

KRITISCHE INFRASTRUKTUREN IM ENERGIESEKTOR? //

BN//K
BRAHMS NEBEL & KOLLEGEN

Definition Kritische Infrastruktur gem. § 2 Abs. 10 BSIG:

Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die

1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung angehören und

2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

Konkretisierung durch die BSI-KritisV (Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz → Festlegung von branchenspezifischen Schwellenwerten

SCHWELLENWERTE KRITISCHE INFRASTRUKTUREN //

BN//K
BRAHMS NEBEL & KOLLEGEN

Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1	Stromversorgung		
1.1	Stromerzeugung		
1.1.1	Erzeugungsanlage	Installierte Nettonennleistung (elektrisch oder direkt mit Wärmeauskopplung verbundene elektrische Wirkleistung bei Wärmenennleistung ohne Kondensationsanteil) in MW oder	104
		installierte Nettonennleistung in MW, wenn die Anlage als Schwarzstartanlage nach § 3 Absatz 2 des Beschlusses der Bundesnetzagentur vom 20. Mai 2020, Aktenzeichen BK6-18-249 kontrahiert ist, oder	0
		installierte Nettonennleistung in MW, wenn die Anlage zur Erbringung von Primärregelleistung nach § 2 Nummer 8 StromNZV präqualifiziert ist	36
1.1.2	Anlage oder System zur Steuerung/Bündelung elektrischer Leistung	Installierte Nettonennleistung (elektrisch) in MW oder	104
		installierte Nettonennleistung in MW, wenn die Anlage als Schwarzstartanlage nach § 3 Absatz 2 des Beschlusses BK6-18-249 kontrahiert ist, oder installierte Nettonennleistung in MW,	0
		installierte Nettonennleistung in MW, wenn die Anlage zur Erbringung von Primärregelleistung nach § 2 Nummer 8 StromNZV präqualifiziert	36
1.2	Stromübertragung		
1.2.1	Übertragungsnetz		3.700
1.3	Stromverteilung		
1.3.1	Stromverteilernetz	Durch Letztverbraucher und Weiterverteiler entnommene Jahresarbeit in GWh/Jahr	3.700
1.4	Stromhandel		
1.4.1	Zentrale Anlage oder System für den Stromhandel	Abgewickeltes Handelsvolumen in TWh/Jahr	3,7

WESENTLICHE PFLICHTEN //

BRAHMS NEBEL & KOLLEGEN

Wesentliche Pflichten für Kritische Infrastrukturen im Energiesektor:

- Benennung einer Kontaktstelle an das BSI, Warnungen und Informationen müssen rund um die Uhr 24/7 durch Kontaktstelle entgegengenommen werden (§ 11 Abs. 1d EnWG)
- Angemessene Schutzvorkehrungen gegen Bedrohungen der IT-Systeme (§ 11 Abs. 1a EnWG für Energieversorgungsnetze; § 11 Abs. 1b EnWG für Betreiber von Energieanlagen)
  - Konkretisierung durch IT-Sicherheitenkataloge der Bundesnetzagentur
- Unverzügliche Meldung von Störungen an das Bundesamt für Sicherheit in der Informationstechnik (§ 11 Abs. c EnWG)
- Einsatz von Systemen zur Angriffserkennung (§ 11 Abs. 1e EnWG)
- Einhaltung der Festlegungen der BNetzA zu kritischen Komponenten und Funktionen (§ 11 Abs. 1g EnWG), Festlegung am 25.06.2025 veröffentlicht

UMSETZUNG DER NIS-2-RICHTLINIE //

BRAHMS NEBEL & KOLLEGEN

- NIS-2-Richtlinie (EU) 2022/2555 vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union – überarbeitete Version der ursprünglichen NIS-1-Richtlinie
- Umsetzungsfrist am 18. Oktober 2024 abgelaufen
- noch keine Umsetzung in Deutschland erfolgt → Entwurf konnte vor Neuwahl des Bundestages am 23. Februar 2025 nicht mehr verabschiedet werden
- neuer Gesetzesentwurf vom **08.09.2025** (BT-Drs. 21/1501)
- relevant für den Energiebereich insbesondere Änderungen des EnWG
- die bisher in § 11 Abs. 1a –g EnWG verankerten Anforderungen an IT-Sicherheit der Energieanlagen- und netze werden in die neu eingeführten §§ 5c-e EnWG ausgegliedert und erweitert (BT-.Drs. 21/1501, S. 179)
- Pflichten zur Cybersicherheit betreffen neben Betreibern von Energieversorgungsnetzen und Energieanlagen nunmehr auch Betreiber eines digitalen Energiedienstes
- → Anforderungen an Cybersicherheit richten sich dann an alle im Energiebereich aktiven Akteure

02 // KRITIS-DACHGESETZ

AKTUELLER STAND KRITIS-DACHGESETZ //

BRAHMS NEBEL & KOLLEGEN

- am **10.09.2025** wurde der Referentenentwurf zum KRITIS-Dachgesetz im Kabinett beschlossen
- dient der Umsetzung der EU-Richtlinie 2022/2557
- Richtlinie schuf europäischen Rahmen für die Stärkung der Resilienz kritischer Infrastrukturen in verschiedenen Sektoren außerhalb der Cybersicherheit, mit der Richtlinie sollen einheitliche Mindestverpflichtungen für kritische Einrichtungen festgelegt werden
- 1. Lesung im Bundestag am **6.11.2025**
- Neu: Regelung zum physischen Schutz kritischer Infrastrukturen, für einen solchen physischen Schutz gab es bislang keine einheitlichen bundesrechtlichen Regelungen

WESENTLICHE INHALTE //

BRAHMS NEBEL & KOLLEGEN

Was sind Kritische Infrastrukturen nach dem KRITIS-Dachgesetz?

- gem. § 5 Abs. 1 RegE zum KRITIS-Dachgesetz werden für die einzelnen Sektoren in einer noch zu erlassenen Rechtsverordnung Schwellenwerte festgelegt, ab denen eine bestimmte Anlage als kritische Infrastruktur gilt
- Betreiber kritischer Anlagen, die kritische Dienstleistungen in oder für mindestens sechs Mitgliedstaaten der Europäischen Union betreiben, werden als **kritische Einrichtungen von besonderer Bedeutung für Europa** eingeordnet, sie treffen besondere Maßnahmen (§ 9 RegE)

→ somit ähnliche Vorgehensweise wie in der BSI-KRITIS-V zum BSIG

WESENTLICHE INHALTE //

BN//K
BRAHMS NEBEL & KOLLEGEN

Pflichten nach dem KRITIS-Dachgesetz?

- es werden keine konkreten Schutzmaßnahmen vorgegeben
- Betreiber sind verpflichtet, geeignete und verhältnismäßige Maßnahmen zu treffen
- im Rahmen des Verhältnismäßigkeitsprinzips ist eine Zweck-Mittel-Relation vorzunehmen, bei der der Aufwand zur Verhinderung oder Begrenzung eines Ausfalls gegen das Risiko eines Vorfalls abzuwägen ist, dabei ist auch wirtschaftliche Aspekte, wie die Leistungsfähigkeit des Betreibers zu berücksichtigen
- Pflichten zur Risikobewertung, Erstellung von Resilienzplänen sowie Erarbeitung branchenspezifischer Standards

RISIKOBEWERTUNG //

BN//K
BRAHMS NEBEL & KOLLEGEN

- KRITIS-Dachgesetz sieht vor, dass zuständige Bundes- und Landesministerium für ihre Geschäftsbereiche Risikoanalysen und Risikobewertungen vornehmen (§ 11 Reg-Entwurf)
- Betreiber Kritischer Anlagen müssen auf Grundlage der nationalen Risikoanalysen und Risikobewertungen und anderer vertrauenswürdiger Informationsquellen eine Risikoanalyse und Risikobewertung durchführen
- Pflicht besteht im Bedarfsfall, mindestens jedoch alle vier Jahre

RESILIENZPLÄNE //

BN//K
BRAHMS NEBEL & KOLLEGEN

- Vorgabe von Resilienzzielen, die Betreiber durch Maßnahmen erreichen müssen
- Erstellung von Resilienzplänen durch Betreiber (§ 13 Reg-E)
  - enthalten Risikoanalysen und Risikobewertungen
  - Darstellung, welche geeigneten und verhältnismäßigen Maßnahmen getroffen werden
- Rechtsverordnungsermächtigung für BSI zu Katalog mit Mindestanforderungen (§ 14 Abs. 1 Reg-E)
- Erarbeitung branchenspezifischer Standards durch die Wirtschaftsverbände in den verschiedenen Sektoren (§ 14 Abs. 2 Reg-E) – Geeignetheit dieser Standards wird auf Antrag durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe festgestellt
  - sofern keine branchenspezifischen Standards erarbeitet werden, werden die Bundesressorts und Landesregierungen ermächtigt, Rechtsverordnungen zur Konkretisierung für die in ihre Zuständigkeit fallenden Bereiche zu treffen (§ 14 Abs. 3-5)

BEISPIEL FÜR PHYSISCHE MAßNAHMEN //

BRAHMS NEBEL & KOLLEGEN

- auch wenn das Gesetz keine konkreten Maßnahmen vorgibt, werden in dem Entwurf zu dem KRITIS-Dachgesetz beispielhaft einige Maßnahmen genannt
  - bauliche und technische Maßnahmen zur Sicherung und Objektschutz etwa durch Liegenschaftsabgrenzungen und hemmende Fassadenelemente
  - Instrumente und Verfahren für die Überwachung der Umgebung
  - Einsatz von Detektionsgeräten
  - Zugangskontrollen
  - Risiko- und Krisenmanagementverfahren und- protokolle
  - Abläufe im Alarmfall
  - Maßnahmen zur Aufrechterhaltung des Betriebs, etwa Notstromversorgung
  - Ermittlung alternativer Lieferketten

WESENTLICHE INHALTE //

BN//K
BRAHMS NEBEL & KOLLEGEN

Pflichten zur Meldung von Sicherheitsvorfällen (§ 18 RegE)

- durch KRITIS-Dachgesetz tritt neben die Pflicht zur Meldung von IT-Vorfällen, die Pflicht zur Meldung von Vorfällen mit physischem Bezug
- soll zukünftig über ein gemeinsames Portal des Bundesamtes für Bevölkerungsschutz (BBK) und des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erfolgen
- → damit soll es eine einheitliche Meldestelle für physische Sicherheitsvorfälle und Cybersicherheitsvorfälle geben
- über die Meldung von Störungen sollen auch andere Betreiber kritischer Infrastrukturen unterrichtet werden, und an andere Unternehmen übermittelt werden

Noch Fragen?

Cybersicherheit und KRITIS-Dachgesetz

BN//K
BRAHMS NEBEL & KOLLEGEN