Allgemeinverfügung

Az. 8155_606/607

In dem Verwaltungsverfahren

wegen: Erstellung eines IT-Sicherheitskatalogs nach § 11 Abs. 1b Energiewirtschaftsgesetz (EnWG)

hat die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Tulpenfeld 4, 53113 Bonn, gesetzlich vertreten durch ihren Präsidenten Jochen Homann,

am 18.12.2018 verfügt:

1. Betreiber von Energieanlagen, die durch die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung) vom 22. April 2016 (BGBl. I S. 958), zuletzt geändert durch Artikel 1 der Verordnung vom 21. Juni 2017 (BGBl. S. 1903), in der jeweils geltenden Fassung als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind (im Weiteren: Anlagenbetreiber) haben die Anforderungen des als Anlage beigefügten „IT-Sicherheitskatalogs gemäß § 11 Abs. 1b EnWG“ (im Weiteren: IT-Sicherheitskatalog) umzusetzen.

2. Anlagenbetreiber sind verpflichtet, die Umsetzung des IT-Sicherheitskatalogs zertifizieren zu lassen. Näheres zum Zertifizierungsverfahren beinhaltet der IT-Sicherheitskatalog auf S. 19 unter E. I.

3. Anlagenbetreiber haben der Bundesnetzagentur bis zum 31.03.2021 den Abschluss des Zertifizierungsverfahrens durch Vorlage einer Kopie des Zertifikats mitzuteilen.

Bundesnetzagentur für
Elektrizität, Gas, Telekommunikation, Post und
Eisenbahnen

Behördensitz:Bonn
Tulpenfeld 4
53113 Bonn

☎ (02 28) 14-0

Telefax Bonn
(02 28) 14-88 72

E-Mail
poststelle@bnetza.de
Internet
http://www.bundesnetzagentur.de

Kontoverbindung
Bundeskasse Trier
BBk Saarbrücken
BIC: MARKDEF1590
IBAN: DE 81 590 000 00
00 590 010 20

4. Anlagenbetreiber sind verpflichtet, der Bundesnetzagentur eine Ansprechpartnerin/einen Ansprechpartner IT-Sicherheit zu benennen und deren/dessen Kontaktdaten bis zum 28.02.2019 mitzuteilen. Die Meldung hat über das auf der Internetseite der Bundesnetzagentur bereitgestellte Formular per E-Mail an folgende Adresse zu erfolgen:

   IT-Sicherheitskatalog@bnetza.de.

5. Betreiber von Anlagen nach § 7 Abs. 1 Atomgesetz, die durch die BSI-Kritisverordnung als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind (im Weiteren: Anlagenbetreiber nach § 7 Abs. 1 Atomgesetz), haben den IT-Sicherheitskatalog wie folgt umzusetzen:

   a. Anlagenbetreiber nach § 7 Abs. 1 Atomgesetz sind verpflichtet, im Rahmen der Schutzbedarfsfeststellung gemäß der „Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT)“ auch die unter B./II./1. des IT-Sicherheitskatalogs genannten besonderen Schutzziele für Erzeugungsanlagen bei der Zuordnung der schutzbedürftigen Anwendungen, Systeme und Komponenten zu den IT-Schutzbedarfsklassen zu berücksichtigen. Diese besonderen Schutzziele sind nachrangig zum Schutzziel der atomaren Sicherheit zu behandeln (s. S. 20 f. des IT-Sicherheitskatalogs unter F.).

   b. Anlagenbetreiber nach § 7 Abs. 1 Atomgesetz haben erstmalig bis zum 30.06.2019 der Bundesnetzagentur eine Bestätigung der für die nukleare Sicherheit zuständigen Genehmigungs- und Aufsichtsbehörden der Länder vorzulegen, aus der hervorgeht, dass die Schutzziele der SEWD-Richtlinie IT vom Betreiber eingehalten werden.

   c. Darüber hinaus haben Anlagenbetreiber nach § 7 Abs. 1 Atomgesetz erstmalig bis zum 30.06.2019 eine verbindliche, von der Geschäftsführung unterzeichnete Erklärung abzugeben, dass auch die besonderen Schutzziele für Erzeugungsanlagen gemäß Abschnitt B./II./1 des IT-Sicherheitskatalogs bei der Schutzbedarfsfeststellung berücksichtigt wurden.

   d. Anlagenbetreiber nach § 7 Abs. 1 Atomgesetz unterliegen der in Ziffer 4 des Tenors genannten Verpflichtung.

   e. Der Nachweis der Erfüllung der Anforderungen ist durch die Anlagenbetreiber nach § 7 Abs. 1 Atomgesetz jeweils zum 30.06. eines jeden Jahres erneut zu erbringen.

Gründe

I.

§ 11 Abs. 1b EnWG enthält den Auftrag an die Bundesnetzagentur, im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) einen Katalog von Sicherheitsanforderungen zu erstellen zum Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Anlagenbetrieb notwendig sind.

Bereits im August 2015 hat die Bundesnetzagentur mit dem IT-Sicherheitskatalog nach § 11 Abs. 1a EnWG die Anforderungen zum Schutz gegen Bedrohungen der für einen sicheren Netzbetrieb notwendigen Telekommunikations- und elektronischen Datenverarbeitungssysteme veröffentlicht.

Mit § 11 Abs. 1b EnWG hat der Gesetzgeber eine neue Vorschrift in § 11 EnWG eingefügt, die sich an die Betreiber von Energieanlagen, die als Kritische Infrastruktur nach der BSI-Kritisverordnung bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind, richtet. Die Aufnahme von Schutzstandards für diese Energieanlagen ist notwendig, um einen umfassenden Schutz für den Netzbetrieb sicherstellen zu können. Betreiber von Energieanlagen, die mit dem öffentlichen Versorgungsnetz verbunden sind, werden verpflichtet, dort, wo eine Gefährdung für den Netzbetrieb möglich ist, Sicherheitsmaßnahmen zu ergreifen. Aufgrund der technischen Nähe ist es notwendig und sinnvoll, dass die Sicherheitsstandards für Netzbetreiber und für die betroffenen Energieanlagen aufeinander abgestimmt sind.

Der vorliegende IT-Sicherheitskatalog für Energieanlagen nach § 11 Abs. 1b EnWG beinhaltet die Anforderungen an die Betreiber, um einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und EDV-Systeme, die für einen sicheren Anlagenbetrieb notwendig sind, zu etablieren.

Ein angemessener Schutz liegt gemäß § 11 Abs. 1b S. 6 EnWG vor, wenn der Katalog der Sicherheitsanforderungen vom Energieanlagenbetreiber eingehalten wird. Der IT-Sicherheitskatalog stellt insofern einen Mindeststandard dar.

Dieses Verwaltungsverfahren richtet sich an Betreiber von Energieanlagen, die als Kritische Infrastruktur nach der BSI-Kritisverordnung bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind. Der IT-Sicherheitskatalog wurde konsultiert und die zuständigen Behörden wurden beteiligt. Das erforderliche Benehmen mit dem BSI wurde bei der Erstellung des IT-Sicherheitskatalogs hergestellt.

Der IT-Sicherheitskatalog wird am 19.12.2018 im Amtsblatt der Bundesnetzagentur sowie auf deren Internetseite veröffentlicht.

II.

1. Zuständigkeit

Die Zuständigkeit der Bundesnetzagentur für die vorliegende Entscheidung ergibt sich aus § 11 Abs. 1b S. 2 EnWG i.V.m. § 54 Abs. 1 EnWG, die der Abteilung 6 aus § 59 Abs. 1 S. 2 Nr. 1 EnWG.

2. Rechtsgrundlage

Die Entscheidung in Ziffer 1 des Tenors beruht auf § 11 Abs. 1b EnWG. Gemäß § 11 Abs. 1b S. 1 EnWG haben Betreiber von Energieanlagen, die durch die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung) vom 22. April 2016 (BGBl. I S. 958), zuletzt geändert durch Artikel 1 der Verordnung vom 21. Juni 2017 (BGBl. S. 1903), in der jeweils geltenden Fassung als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind, einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme zu gewährleisten, die für einen sicheren Anlagenbetrieb notwendig sind. Hierzu hat die Regulierungsbehörde im Benehmen mit dem BSI einen Katalog von Sicherheitsanforderungen zu erstellen und zu veröffentlichen (§ 11 Abs. 1b S. 2 EnWG). Die Umsetzungspflicht der Anlagenbetreiber beruht auf § 11 Abs. 1b S. 6 EnWG, wonach ein angemessener Schutz des Betriebs von Energieanlagen im Sinne des Satzes 1 vorliegt, wenn dieser Katalog von Sicherheitsanforderungen eingehalten worden ist.

Die Regelungen in Ziffern 2, 3 und 4 des Tenors beruhen auf § 11 Abs. 1b S. 5 EnWG. Danach enthält der Katalog der Sicherheitsanforderungen auch Regelungen zur regelmäßigen Überprüfung der Erfüllung der Sicherheitsanforderungen. Die Regelung in Ziffer 3 des Tenors beruht zudem auf § 11 Abs. 1b S. 1 und 2 EnWG.

Die Regelung in Ziffer 5a des Tenors beruht auf § 11 Abs. 1b S. 1, 2 und 3 EnWG, wonach für Telekommunikations- und elektronische Datenverarbeitungssysteme von Anlagen nach § 7 Abs. 1 des Atomgesetzes, die durch die BSI-Kritisverordnung als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind, Vorgaben auf Grund des Atomgesetzes Vorrang haben. Die Regelungen in Ziffer 5b und 5c des Tenors beruhen auf § 11 Abs. 1b S. 1, 2 und 5 EnWG.

3. Formelle Anforderungen

Die formellen Anforderungen an die Rechtmäßigkeit der Entscheidung sind erfüllt. Die Entscheidung richtet sich an einen statthaften Adressatenkreis (s. folgender Abschnitt 3.1.). Die Bundes-

netzagentur hat die erforderliche Konsultation durchgeführt (s. folgender Abschnitt 3.2.) und die betroffenen Behörden beteiligt (s. folgender Abschnitt 3.3.).

3.1. Statthafter Adressatenkreis

Gemäß § 11 Abs. 1b S. 1 EnWG richtet sich die Entscheidung an die Betreiber von Energieanlagen, die durch die BSI-Kritisverordnung in der jeweils geltenden Fassung als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind.

3.2. Anhörung

Die bestehenden Anhörungs- und Beteiligungsrechte wurden gewahrt. Die Bundesnetzagentur hat von der Entscheidung Betroffenen sowie den durch das Verfahren berührten Wirtschaftskreisen gemäß § 67 Abs. 1, 2 EnWG Gelegenheit zur Stellungnahme gegeben. Hierzu hat sie Informationen zur Einleitung der Konsultation am 11.01.2018 auf ihrer Internetseite veröffentlicht. Die Veröffentlichung enthielt einen vollständigen Entwurf des beabsichtigten IT-Sicherheitskatalogs. Alle Betroffenen erhielten Gelegenheit zur Stellungnahme bis zum 28.02.2018. Im Rahmen dieser Konsultation gingen 18 Stellungnahmen von Auditoren, Unternehmen, Verbänden und den Branchenarbeitskreisen Strom und Gas im UP KRITIS ein. Sämtliche Stellungnahmen wurden ausgewertet, zum Teil aufgegriffen und in den IT-Sicherheitskatalog eingearbeitet.

3.3. Beteiligung zuständiger Behörden

Das gemäß § 11 Abs. 1b S. 2 EnWG bei der Erstellung des IT-Sicherheitskatalogs erforderliche Benehmen mit dem BSI wurde hergestellt. Die förmliche Beteiligung des Länderausschusses nach § 60a Abs. 2 EnWG erfolgte in dessen Sitzung am 15.11.2018.

Die nach § 11 Abs. 1b S. 4 EnWG bei der Erarbeitung des Katalogs von Sicherheitsanforderungen erforderliche Beteiligung der für die nukleare Sicherheit zuständigen Genehmigungs- und Aufsichtsbehörden des Bundes und der Länder hat stattgefunden.

Gemäß § 58 Abs. 1 S. 2 EnWG wurde dem Bundeskartellamt Gelegenheit zur Stellungnahme gegeben.

4. Materielle Rechtmäßigkeit der Entscheidung

Die Entscheidung ist materiell rechtmäßig. Die Voraussetzungen für die Erstellung des IT-Sicherheitskataloges liegen vor (siehe folgender Abschnitt 4.1.) und die konkrete Ausgestaltung ist verhältnismäßig (siehe folgender Abschnitt 4.2.).

4.1. Voraussetzungen für die Erstellung des IT-Sicherheitskatalogs

Die Unterstützung durch Informations- und Kommunikationstechnik (IKT-Systeme) bringt bei Netz- und Anlagenbetreibern zwar viele Vorteile, mit der wachsenden Abhängigkeit von diesen Systemen gehen jedoch auch Risiken für die Versorgungssicherheit einher.

Bereits im August 2015 hat die Bundesnetzagentur mit dem IT-Sicherheitskatalog nach § 11 Abs. 1a EnWG die Anforderungen zum Schutz gegen Bedrohungen der für einen sicheren Netzbetrieb notwendigen Telekommunikations- und elektronischen Datenverarbeitungssysteme veröffentlicht. Der IT-Sicherheitskatalog nach § 11 Abs. 1a EnWG dient der Verwirklichung eines sicheren Energieversorgungsnetzbetriebs gemäß § 11 Abs. 1 S. 1 EnWG im Hinblick auf den Einsatz der dafür relevanten IT-Systeme. Die Forderung nach einem sicheren Energieversorgungsnetz dient dem Ziel der Versorgungssicherheit.

Aufgrund der technischen Nähe von Energienetzen und Energieanlagen, die mit dem öffentlichen Versorgungsnetz verbunden sind, ist es notwendig und sinnvoll, dass die Sicherheitsstandards für Netzbetreiber und für die betroffenen Energieanlagen aufeinander abgestimmt sind.

Zum Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Anlagenbetrieb notwendig sind, erstellt die Regulierungsbehörde im Benehmen mit dem BSI einen Katalog von Sicherheitsanforderungen und veröffentlicht diesen (§ 11 Abs. 1 b S. 2 EnWG). Auch dieser IT-Sicherheitskatalog dient der Verwirklichung eines sicheren Energieversorgungsnetzbetriebs und dem Ziel der Versorgungssicherheit.

4.2. Ausgestaltung des IT-Sicherheitskatalogs

4.2.1. Mit Ziffer 1 des Tenors werden Betreiber von Energieanlagen, die als Kritische Infrastrukturen bestimmt wurden, zum Schutz gegen Bedrohungen der für einen sicheren Anlagenbetrieb notwendigen Telekommunikations- und elektronischen Datenverarbeitungssysteme zur Umsetzung des IT-Sicherheitskatalogs verpflichtet. Alternativen zu dieser Regelung bestehen nicht. Bereits der Gesetzgeber hat im Rahmen seiner Einschätzungsprärogative die fehlerfreie Abwägungsentscheidung getroffen, dass ein angemessener Schutz des Betriebs einer Energieanlage nur dann vorliegt, wenn der Katalog von Sicherheitsanforderungen eingehalten und dies vom Betreiber dokumentiert worden ist. Damit bleibt grundsätzlich kein Spielraum mehr für die Betreiber, andere aus ihrer Sicht angemessene Schutzmaßnahmen zu erarbeiten. Der Sicherheitskatalog der Bundesnetzagentur stellt einen Mindeststandard dar, der von den Betreibern einzuhalten ist.

Im Rahmen der durchgeführten Konsultation wurde mehrfach eine Klarstellung dahingehend gefordert, dass für Betreiber von Energieversorgungsnetzen, die der Anlagenkategorie der BSI-Kritisverordnung unterliegen, ausschließlich der IT-Sicherheitskatalog nach § 11 Abs. 1a EnWG

Anwendung findet. Dieser Forderung wurde in Fußnote 1 des IT-Sicherheitskatalogs entsprochen.

Im IT-Sicherheitskatalog wird die Einführung eines Informationssicherheits-Managementsystems (ISMS) gemäß der DIN EN ISO/IEC 27001 gefordert. Die ISO/IEC 27001 ist ein international anerkannter Standard für die Informationssicherheit, der unter Energieversorgern etabliert ist und bereits vielfach umgesetzt wurde. Der Ansatz der DIN EN ISO/IEC 27001 ist ein risikobasierter, d. h. die Umsetzung einzelner Maßnahmen ist immer von der tatsächlichen Situation und Bedrohungslage des jeweiligen Energieanlagenbetreibers abhängig. Diese Skalierbarkeit bei der Umsetzung der Anforderungen führt dazu, dass Maßnahmen nicht „schablonenhaft“, sondern in quantitativer und qualitativer Hinsicht flexibel und risikoangemessen im Einzelfall umzusetzen sind.

Da die DIN EN ISO/IEC 27001 nur sehr allgemeine Anforderungen an ein ISMS enthält, wird weiter die Berücksichtigung der Normen DIN EN ISO/IEC 27002 und DIN EN ISO/IEC 27019 in der jeweils geltenden Fassung bei der Implementierung des ISMS gefordert. Diese Normen legen Anforderungen und allgemeine Prinzipien für die Initiierung, Umsetzung, den Betrieb und die Verbesserung des Informationssicherheits-Managements in einer Organisation, unter Berücksichtigung der Besonderheiten im Bereich der Prozesssteuerung der Energieversorgung, fest.

Die in den genannten ISO-Normen genannten Maßnahmen sind nicht per se ungeprüft umzusetzen, sondern immer in Abhängigkeit von ihrer Bedeutung für die Sicherheit der Anwendungen, Systeme und Komponenten unter Berücksichtigung der Ergebnisse einer vorzunehmenden Risikoeinschätzung. Damit ist der IT-Sicherheitskatalog keine statische Bestandsaufnahme von bestimmten, umzusetzenden Maßnahmen. Vielmehr liegt die Auswahl der Maßnahmen in der Verantwortung des Anlagenbetreibers und ist individuell für seine Energieanlage und seinen konkreten Schutzbedarf anpassbar. Diese risikobasierte, individuelle Skalierbarkeit der Anforderungen des IT-Sicherheitskatalogs ermöglicht es dem Anlagenbetreiber, diejenigen Maßnahmen auszuwählen und umzusetzen, die im Einzelfall geeignet und angemessen sind, den Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Anlagenbetrieb notwendig sind, sicherzustellen. Damit wird dem Umstand Rechnung getragen, dass sich die Sicherheitsanforderungen der verschiedenen Anlagenbetreiber quantitativ und qualitativ unterscheiden können.

Darüber hinaus können für einige Anlagentypen im Bereich der als Kritische Infrastruktur festgelegten Energieanlagen der VGB-Standard „IT-Sicherheit für Erzeugungsanlagen“ (VGB-S-175) und das BDEW-Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ als Hilfestellung bei der Umsetzung des ISMS dienen.

4.2.2. § 11 Abs. 1b Satz 5 EnWG fordert von der Bundesnetzagentur, dass der IT-Sicherheitskatalog auch Regelungen zur regelmäßigen Überprüfung der Erfüllung der Sicherheitsanforderungen enthalten muss. Um dem Willen des Gesetzgebers nachzukommen, wird vom Anlagenbetreiber insoweit gefordert, die Umsetzung des IT-Sicherheitskatalogs zertifizieren zu lassen (Ziffer 2 des Tenors). Bei der Vielzahl von in Frage kommenden Energieanlagen ist es der Bundesnetzagentur schlicht nicht möglich, die Einhaltung der Anforderungen des IT-Sicherheitskatalogs bei den Anlagenbetreibern selber zu überprüfen. Daher wird die Bundesnetzagentur gemeinsam mit der Deutschen Akkreditierungsstelle (DAkkS) die Voraussetzungen dafür schaffen, dass speziell für die Zertifizierung des IT-Sicherheitskatalogs akkreditierte Stellen verfügbar sind, die im Rahmen entsprechender Audits beim jeweiligen Anlagenbetreiber vor Ort überprüfen, ob die Anforderungen des IT-Sicherheitskatalogs erfolgreich umgesetzt wurden. Die Zertifizierung darf nur durch eine solche für die Zertifizierung akkreditierte Stelle durchgeführt werden. Durch die DAkkS-Akkreditierung ist eine unabhängige und vergleichbare Überprüfung der Anlagenbetreiber gewährleistet. Die DAkkS ist die nationale Akkreditierungsstelle der Bundesrepublik Deutschland. Als beliehene Stelle untersteht sie der Aufsicht des Bundes. Eine Übersicht der akkreditierten Stellen zur Zertifizierung des IT-Sicherheitskataloges wird auf der Internetseite der DAkkS abgerufen werden können.

4.2.3. Zum Nachweis darüber, dass die Anforderungen des IT-Sicherheitskatalogs umgesetzt wurden, wird dem Anlagenbetreiber in Ziffer 3 des Tenors aufgegeben, den Abschluss des Zertifizierungsverfahrens der Bundesnetzagentur bis zum 31.03.2021 durch Vorlage einer Kopie des Zertifikats mitzuteilen. Die einfache Vorlage einer Kopie des Zertifikats ist dem Anlagenbetreiber zumutbar und ermöglicht der Bundesnetzagentur eine lückenlose Überwachung der Umsetzungspflicht.

Die Vorlage des Zertifikats innerhalb der gesetzten Frist ist dem Anlagenbetreiber zumutbar. Bei Bemessung der angemessenen Frist wurden die je nach Organisation, Größe und Zertifizierungsreife sehr unterschiedlichen Voraussetzungen der zahlreichen Anlagenbetreiber sowie die im Rahmen des Konsultationsverfahrens abgegebenen Stellungnahmen berücksichtigt. Im Rahmen der Konsultation hat sich eine Frist von ca. 2 bis 2,5 Jahren als für die Umsetzung des IT-Sicherheitskatalogs realistisch erwiesen. Die ursprünglich beabsichtigte Fristsetzung von 1,5 Jahren nach Veröffentlichung des IT-Sicherheitskatalogs wurde daher auf knapp 2,5 Jahre nach Veröffentlichung verlängert.

4.2.4. Mit Ziffer 4 des Tenors wird die Benennung einer Ansprechpartnerin/eines Ansprechpartners und ihrer/seiner Kontaktdaten für die Koordination und Kommunikation der IT-Sicherheit gegenüber der Bundesnetzagentur gefordert. Die Ansprechpartnerin/der Ansprechpartner muss insbesondere Auskunft zum Umsetzungsstand der Anforderungen aus dem IT-Sicherheitskatalog sowie zu aufgetretenen Sicherheitsvorfällen und deren Art, Umfang und Ursachen geben können. Die Nennung einer konkreten Ansprechpartnerin/eines konkreten

Ansprechpartners und ihrer/seiner Kontaktdaten ermöglicht es der Regulierungsbehörde, ihrer Überprüfungspflicht schnellstmöglich nachzukommen. Zudem ist die Benennung der Ansprechpartnerin/des Ansprechpartners IT-Sicherheit unverzichtbar für eine zeitnahe und umfassende Bewertung der im Rahmen des § 11 Abs. 1c Satz 4 EnWG eingegangenen Meldungen des BSI mit Blick auf die Versorgungssicherheit. Nur wenn in solchen Fällen für Nachfragen beim Anlagenbetreiber eine/ein zuvor benannte(r) und mit entsprechenden Kontaktdaten hinterlegte(r) Ansprechpartnerin/Ansprechpartner zur Verfügung steht, kann die Bundesnetzagentur auf eingetretene IT-Sicherheitsvorfälle in Zusammenarbeit mit dem BSI angemessen reagieren.

Die unverzügliche Nennung einer Ansprechpartnerin/eines Ansprechpartners und ihrer/seiner Kontaktdaten ist dem Anlagenbetreiber möglich und zumutbar. So werden an die berufliche Qualifikation der Ansprechpartnerin/des Ansprechpartners keine besonderen Anforderungen gestellt, es wird auch keine Meldepflicht normiert, sondern lediglich eine Auskunftspflicht in den Fällen, in denen die Bundesnetzagentur selbst die/den benannte(n) Ansprechpartnerin/Ansprechpartner kontaktiert. Die Meldung ist zudem über ein auf der Internetseite der Bundesnetzagentur bereitgestelltes Formular per E-Mail an die Adresse IT-Sicherheitskatalog@bnetza.de unkompliziert möglich.

4.2.5.

§ 11 Abs. 1 b S. 3 EnWG bestimmt, dass für Telekommunikations- und elektronische Datenverarbeitungssysteme von Anlagen nach § 7 Abs. 1 Atomgesetz, die durch die BSI-Kritisverordnung als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind, Vorgaben aufgrund des Atomgesetzes Vorrang haben. Für die IT-Sicherheit dieser Anlagen besteht mit der „Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT)“ bereits ein verpflichtendes anlagenspezifisches Regelwerk, dessen Schutzziele die kerntechnische Sicherheit gewährleisten sollen. Die IT-Sicherheit von Anlagen nach § 7 Abs. 1 Atomgesetz, die durch die BSI-Kritisverordnung als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind, muss sich nach § 11 Abs. 1b Satz 1 EnWG jedoch auch an ihrer Bedeutung für den sicheren Netzbetrieb und damit an ihrer Bedeutung für die allgemeine Versorgungssicherheit orientieren.

Anlagenbetreiber nach § 7 Abs. 1 Atomgesetz sind daher verpflichtet, im Rahmen der Schutzbedarfsfeststellung gemäß SEWD-Richtlinie IT auch die unter B./II./1. des IT-Sicherheitskatalogs genannten besonderen Schutzziele für Erzeugungsanlagen bei der Zuordnung der schutzbedürftigen Anwendungen, Systeme und Komponenten zu den IT-Schutzbedarfsklassen zu berücksichtigen (Ziffer 5a des Tenors). Diese besonderen Schutzziele sind nachrangig zum Schutzziel der atomaren Sicherheit zu behandeln.

Sofern die besonderen Schutzziele für Erzeugungsanlagen bei der Schutzbedarfsfeststellung berücksichtigt werden, führt die Anwendung der SEWD-Richtlinie IT zu einem IT-technischen Schutzniveau, welches mit dem in § 11 Abs. 1b S. 1 EnWG geforderten Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Anlagenbetrieb notwendig sind, vergleichbar ist.

Ein angemessener Schutz des Betriebs von Energieanlagen im Sinne von § 11 Abs. 1b Satz 1 EnWG liegt daher für Anlagenbetreiber nach § 7 Abs. 1 Atomgesetz vor, wenn keine Risiken offenkundig sind, die die Einhaltung der Schutzziele nach der SEWD-Richtlinie IT gefährden und auch die besonderen Schutzziele gemäß Abschnitt B./II./1. berücksichtigt wurden.

Dem Anlagenbetreiber nach § 7 Abs. 1 Atomgesetz ist es möglich und zumutbar, bei der für ihn ohnehin verpflichtenden Schutzbedarfsfeststellung gemäß SEWD-Richtlinie IT zusätzlich die auf die Versorgungssicherheit bezogenen besonderen Schutzziele gemäß IT-Sicherheitskatalog einzubeziehen. Auch wenn die Schutzbedarfsklassenzuordnung mit Blick auf die atomare Sicherheit der Anlage strengen Maßstäben unterliegt, kann nicht ungeprüft davon ausgegangen werden, dass diese Zuordnung zugleich auch mit Blick auf die Versorgungssicherheit in jedem Falle richtig und vollständig ist. Der Zweck der gesetzlichen Regelung in § 11 Abs. 1b EnWG kann daher nur dann sichergestellt werden, wenn beide Schutzziele bei der Schutzbedarfsklassenzuordnung berücksichtigt werden müssen. Für den Betreiber entsteht dadurch auch kein unverhältnismäßiger Mehraufwand, da es sich um ähnliche Prozessschritte handelt, die sich zudem überwiegend auf dieselben IT-Komponenten innerhalb der Anlage beziehen.

Die Einhaltung der Schutzziele nach der SEWD-Richtlinie IT obliegt den für die nukleare Sicherheit zuständigen Genehmigungs- und Aufsichtsbehörden der Länder. Zum Nachweis darüber, dass die Anforderungen des IT-Sicherheitskatalogs umgesetzt wurden, ist es nach Ziffer 5b des Tenors daher ausreichend, wenn Anlagenbetreiber nach § 7 Abs. 1 Atomgesetz der Bundesnetzagentur eine Bestätigung der zuständigen Landesbehörden vorlegen, aus der hervorgeht, dass die Schutzziele der SEWD-Richtlinie IT vom Betreiber eingehalten werden. Auf diese Weise werden bürokratische Doppelstrukturen bei der Nachweisführung vermieden, da die Bundesnetzagentur eine Bestätigung der insoweit ohnehin zuständigen Landesbehörden gelten lässt. Ein unverhältnismäßiger Mehraufwand entsteht den Betreibern demzufolge nicht.

Anlagenbetreiber nach § 7 Abs. 1 Atomgesetz sind nach Ziffer 5c des Tenors darüber hinaus verpflichtet, gegenüber der Bundesnetzagentur eine verbindliche Erklärung mit dem Inhalt abzugeben, dass auch die besonderen Schutzziele für Erzeugungsanlagen gemäß Abschnitt B./II./1 des IT-Sicherheitskatalogs bei der Schutzbedarfsfeststellung von ihnen berücksichtigt wurden. Angesichts der hoheitlichen Überprüfung und Dokumentierung der Einhaltung der SEWD-Richtlinie IT durch die zuständigen Landesbehörden ist es zur Vermeidung bürokratischen Mehraufwands ausreichend, die ergänzende Nachweisführung über die Berücksichtigung

der besonderen Schutzziele für Erzeugungsanlagen auf Basis einer verbindlichen Selbstauskunft der Betreiber zu ermöglichen.

Da an die Nachweisführung über die Erfüllung der Anforderungen des IT-Sicherheitskatalogs für Anlagenbetreiber nach § 7 Abs. 1 Atomgesetz insgesamt keine hohen bürokratischen Anforderungen gestellt werden, ist es diesen auch zumutbar, den Nachweis jährlich erneut zu erbringen (Ziffer 5e des Tenors). Die Pflicht zur erstmaligen Nachweisführung zum 30.06.2019 – und damit früher als bei den sonstigen zur Umsetzung des IT-Sicherheitskatalogs verpflichteten Anlagenbetreibern – ist ebenfalls zumutbar, da es sich bei der für die Anlagenbetreiber nach § 7 Abs. 1 Atomgesetz geltenden SEWD-Richtlinie IT nicht um eine neue Anforderung handelt, sondern um ein einschlägiges branchenspezifisches Regelwerk, welches bereits seit 2013 gilt.

Rechtsbehelfsbelehrung

Gegen diese Entscheidung kann innerhalb eines Monats nach Zustellung Beschwerde erhoben werden. Die Beschwerde ist bei der Bundesnetzagentur (Hausanschrift: Tulpenfeld 4, 53113 Bonn) einzureichen. Es genügt, wenn die Beschwerde innerhalb der Frist bei dem Oberlandesgericht Düsseldorf (Hausanschrift: Cecilienallee 3, 40474 Düsseldorf) eingeht.

Die Beschwerde ist zu begründen. Die Frist für die Beschwerdebegründung beträgt einen Monat. Sie beginnt mit der Einlegung der Beschwerde und kann auf Antrag von dem oder der Vorsitzenden des Beschwerdegerichts verlängert werden. Die Beschwerdebegründung muss die Erklärung, inwieweit die Entscheidung angefochten und ihre Abänderung oder Aufhebung beantragt wird, und die Angabe der Tatsachen und Beweismittel, auf die sich die Beschwerde stützt, enthalten.

Die Beschwerdeschrift und die Beschwerdebegründung müssen durch einen Rechtsanwalt unterzeichnet sein.

Die Beschwerde hat keine aufschiebende Wirkung (§ 76 Abs. 1 EnWG).

Im Auftrag

Achim Zerres

Abteilungsleiter Energieregulierung