VI-3 Kart 109/16 [V]

Verkündet am 19.07.2017

Oberlandesgericht Düsseldorf

Beschluss

In dem energiewirtschaftlichen Verwaltungsverfahren

…

hat der 3. Kartellsenat des Oberlandesgerichts Düsseldorf auf die mündliche Verhandlung vom 14.06.2017 durch den Vorsitzenden Richter am Oberlandesgericht Laubenstein und die Richterinnen am Oberlandesgericht Klein Reesink und Pastohr

b e s c h l o s s e n :

Die Beschwerde der Betroffenen gegen den Beschluss der Bundesnetzagentur „IT-Sicherheitskatalog gemäß § 11 Abs. 1a Energiewirtschaftsgesetz“, veröffentlicht am 12.08.2015, wird zurückgewiesen.

Die Kosten des Beschwerdeverfahrens einschließlich der notwendigen Auslagen der Bundesnetzagentur trägt die Betroffene.

Der Wert des Beschwerdeverfahrens wird auf insgesamt bis zu … EUR festgesetzt.

Die Rechtsbeschwerde wird zugelassen.

G r ü n d e :

A.

Die Betroffene betreibt in … Energieversorgungsnetze der allgemeinen Versorgung. Ihr Netzgebiet versorgt etwa … Einwohner mit Strom, Gas und Fernwärme. Das von ihr betriebene Elektrizitätsverteilernetz in Mittel- und Niederspannung hat knapp … Netzanschlüsse, das Gasverteilernetz rund … Netzanschlüsse. Die jährlich aus dem Elektrizitätsverteilernetz der Betroffenen entnommene Strommenge liegt bei insgesamt rund … GWh, die aus dem Gasverteilernetz entnommene Gasmenge bei ca. … GWh. Sowohl im Gas- als auch im Elektrizitätsverteilernetz der Betroffenen werden mit Ausnahme eines von zwei genutzten Umspannwerken, das zwischenzeitlich auf IT-gestützte Leittechnik fernschaltbar ist, Leitsysteme zur Übermittlung von Informationen, nicht aber zur Steuerung von Einrichtung eingesetzt. Im Fernwärmenetz werden keine Daten übertragen, in den im Netz der Betroffenen angeschlossenen Blockheizkraftwerken wird die wärmeseitige Produktion digital überwacht; auch die Maschineneinsatzsteuerung erfolgt IT-basiert.

Nachdem sie Ende 2013 einen Entwurf mit Gelegenheit zur Stellungnahme veröffentlicht hatte, veröffentlichte die Bundesnetzagentur am 12.08.2015 auf ihrer Internetseite den hier streitgegenständlichen „IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz“, wegen dessen Einzelheiten auf die Anlage BF 1 Bezug genommen wird. Damit bestimmt die Bundesnetzagentur die Anforderungen an den sicheren Betrieb eines Energieversorgungsnetzes im Hinblick auf Bedrohungen für TK- und EDV-Systeme i.S.d. § 11 Abs. 1a S. 1 EnWG. Die Anforderungen sind unabhängig von der Größe oder der Anzahl der angeschlossenen Kunden von allen Netzbetreibern zu erfüllen, soweit diese über Systeme verfügen, die in den Anwendungsbereich des Sicherheitskatalogs fallen. Hierzu zählen TK- und EDV-Systeme, die direkt Teil der Netzsteuerung sind oder zwar nicht direkt Teil der Netzsteuerung sind, deren Ausfall jedoch die Sicherheit des Netzbetriebs gefährden könnte, z.B. Messeinrichtung an Trafo- oder Netzkoppelstationen.

Kernforderung des IT-Katalogs ist die Einführung eines Informationssicherheits-Managementsystems (im Folgenden: ISMS) gemäß der Norm DIN ISO/IEC 27001 (in der aktuellen Fassung 2015-03 vorgelegt als Anlage BF 3), die Leitlinien und allgemeine Prinzipien für die Initiierung, Umsetzung, den Betrieb und die Verbesserung

des ISMS enthält, sowie dessen erstmalige Zertifizierung bis zum 31.01.2018 und eine in 3-Jahres-Zyklen erfolgende erneute Zertifizierung jeweils durch eine unabhängige, hierfür zugelassene Stelle vorsieht. Ergänzend verweist der IT-Sicherheitskatalog auf die Norm DIN ISO/IEB 27002 (Anlage BF 4), die Umsetzungsempfehlungen für die verbindlichen Maßnahmen des Anhangs A der DIN ISO/IEC 27011 umfasst, sowie auf die Norm DIN ISO/IEC TR 27019 (Anlage BF 5), die diese in verschiedenen Punkten um Besonderheiten im Bereich der Prozesssteuerung der Energieversorgung erweitert. Innerhalb diesen Rahmens hat der Netzbetreiber zunächst eine Übersicht über die vom Geltungsbereich des IT-Sicherheitskatalogs betroffenen Anwendungen, Systeme und Komponenten mit den anzutreffenden Haupttechnologien und deren Verbindungen zu erstellen, und zwar nach den Technologiekategorien „Leitsystem/Sytembetrieb“, „Übertragungstechnik/Kommunikation“ und „Sekundär-/Automatisierungs- und Fernwirktechnik“, die in einem sog. Netzstrukturplan darzustellen sind (IT-Sicherheitskatalog, S. 10 f., E.IV.). Sodann muss der Betreiber einen Prozess der Risikoeinschätzung der Systemsicherheit festlegen, der den Anforderungen in Kap. 5.1.2. DIN ISO/IEC 27001 genügt und bei der bestimmte Vorgaben des IT-Sicherheitskatalogs zu beachten sind (IT-Sicherheitskatalog, S. 12 ff, E.V.). Die Risikobehandlung umfasst dann die Auswahl geeigneter und angemessener Maßnahmen in Anknüpfung an die Risikoeinschätzung.

Des Weiteren musste nach dem IT-Sicherheitskatalog bis zum 31.11.2015 ein Ansprechpartner für IT-Sicherheit benannt werden. Dem ist die Betroffene mit E-Mail vom 09.11.2015 nachgekommen.

Die Betroffene macht geltend, die Einführung des ISMS und die aus dem IT-Sicherheitskatalog folgenden regelmäßigen Überarbeitungspflichten würden zu einem erheblichen Aufwand bei ihr führen. Die Kosten für die Einführung des ISMS würden sich – unter Berücksichtigung schon entstandener Kosten von … EUR extern und rund … EUR intern – auf insgesamt ca. … EUR belaufen. Die Kosten für die Zertifizierung würden sich auf ca. … EUR belaufen, ein Drittel dieses Betrages werde für die Rezertifizierungen im 3-Jahres-Rythmus anfallen. Der jährliche Folgeaufwand liege bei ca. … internen und … externen Personaltagen. Diese Kosten fielen unabhängig davon an, ob überhaupt Verbesserungen in ihrem IT-System erforderlich sei-

en. Sie habe bereits ausreichende Maßnahmen zur Gewährleistung der IT-Sicherheit eingeführt, zu denen sie im Einzelnen ebenso vorträgt wie zu den durch die Einführung und Überprüfung des ISMS erforderlichen Maßnahmen.

Die als Anfechtungsbeschwerde gegen eine Allgemeinverfügung statthafte und auch sonst zulässige Beschwerde sei begründet, da der IT-Sicherheitskatalog rechtswidrig sei. Die gesetzlichen Grenzen des der Bundesnetzagentur zustehenden Ermessens bei der Erstellung des IT-Sicherheitskatalogs würden gezogen zunächst durch § 11 Abs. 1a EnWG, der den erforderlichen Schutzstandard der IT-Systeme auf ein „angemessenes“ Niveau festlege. Ferne komme nach Auffassung des Gesetzgebers den sog. Kritischen Infrastrukturen im Bereich der IT-Sicherheit eine besondere Bedeutung zu, wie sich der Begründung des Entwurfs der Bundesregierung zum IT-Sicherheitsgesetz entnehmen lasse (BT-Drs. 18/4096, S. 1). Weiter sei die Grenze der wirtschaftlichen Zumutbarkeit von IT-Sicherheitsmaßnahmen zu beachten, § 11 Abs. 1 S. 1 EnWG.

Soweit die Bundesnetzagentur der Regelung in § 11 Abs. 1a EnWG eine ausnahmslose Anwendung des IT-Sicherheitskatalogs auf alle Betreiber von Gas- und Elektrizitätsverteilernetzen entnehme, liege ein rechtsfehlerhafter Ermessensnichtgebrauch vor, da sie auf Ermessenserwägungen verzichte, zu denen sie bei einer verfassungskonformen Auslegung der Vorschrift zur Wahrung der Angemessenheit verpflichtet sei. Der Gesetzgeber habe ihr diesbezüglich eine Differenzierungsmöglichkeit hinsichtlich der Sicherheitsrelevanz der betroffenen Systeme eingeräumt. Eine solche habe der Gesetzgeber im Rahmen des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) durch die Festlegung von Grenzwerten für sog. Kritische Infrastrukturen in der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) und die Regelung des § 8c Abs. 1 BSIG ausdrücklich vorgenommen; insoweit sei von einem Gleichlauf zwischen § 11 Abs. 1a und § 11 Abs. 1b EnWG auszugehen. Die dort niedergelegten Grenzwerte seien mithin belastbare Grundlage für die Bewertung eines „angemessenen“ Schutzniveaus für die betroffenen Infrastrukturen. Unter Zugrundelegung der Annahme, dass § 11 Abs. 1a und § 11 Abs. 1c EnWG denselben Anwendungsbereich hätten, folge unter Berücksichtigung der Gesetzesbegründung zur Einführung des § 11 Abs. 1c EnWG die zwingende Beschränkung der Vorgaben des IT-Sicherheitskatalogs auf

solche Unternehmen, bei denen es sich um Kritische Infrastrukturen i.S.d. der BSI-KritisV handele.

Die von ihr betriebenen Verteilernetze seien auch nicht sicherheitsrelevant und deshalb von der Anwendung des IT-Sicherheitskatalogs auszunehmen gewesen. Bei Ausfall eines ihrer Verteilernetze drohe kein „Kaskadeneffekt“ in dem Sinne, dass durch deren Ausfall infolge einer Systemstörung auch vorgelagerte und benachbarte Netze so destabilisiert würden, dass sie ausfallen könnten. Nachgelagerte Netze existierten nicht. Ein Netzengpass oder eine Systembilanzabweichung im Fall eines Totalausfalls der Umspannwerke im Stromverteilernetz seien aufgrund der geringen Größe des Netzes faktisch ausgeschlossen, sofern der vorgelagerte Netzbetreiber seiner Betriebsverantwortung nachkomme, wozu die Beschwerdeführerin im Einzelnen vorträgt. Im Gasverteilernetz sei bereits keine IT-gestützte Steuerung möglich und drohten auch bei Manipulation des reinen Visualisierungssystems keine Schäden.

Jedenfalls seien die Grenzen der zulässigen Ermessensausübung vorliegend überschritten, da der IT-Sicherheitskatalog gegen den Gleichheitssatz aus Art. 3 Abs. 1 GG verstoße. Es liege eine nicht gerechtfertigte Gleichbehandlung der Betroffenen mit Betreibern von Energieversorgungsnetzen, die Kritische Infrastrukturen i.S.d. der BSI-KritisV betrieben, vor. Angesichts der Tatsache, dass der Gesetzgeber ausdrücklich nur denjenigen Infrastrukturen eine besondere Bedeutung im Bereich der IT-Sicherheit zugemessen habe, die für das Funktionieren des Gemeinwesens „zentral“ seien und diese als entsprechend „kritisch“ kategorisiert habe, sei eine Anhebung der IT-Sicherheitsstandards nur im Hinblick auf solche auch wirtschaftlich gerechtfertigt. Dem habe die Bundesnetzagentur bei der Auslegung des Angemessenheits- und Zumutbarkeitskriteriums nicht ausreichend Rechnung getragen. Weiter liege eine Ungleichbehandlung der Netzbetreiber gegenüber Betreibern von Energieanlagen vor**,** die nur zur Einführung von Maßnahmen nach § 11 Abs. 1b EnWG verpflichtet seien, wenn sie Kritische Infrastrukturen betrieben. Auch insoweit hätte § 11 Abs. 1a EnWG verfassungskonform korrespondierend mit § 11 Abs. 1b EnWG ausgelegt werden müssen. Dies entspreche dem Willen des Gesetzgebers, der Energieversorgungsnetze und

–anlagen grundsätzlich habe gleich behandeln wollen. Sofern man davon ausgehe, dass der IT-Sicherheitskatalog unterschiedslos für alle Betreiber von Elektrizitäts- und Gasverteilernetzen gelte, wäre die Regelung diskriminierend und rechtswidrig. Wenn der Ausfall eines Verteilernetzes von der Größe des Netzes der Betroffenen zu den gleichen Auswirkungen auf ein vorgelagertes Netz führe wie der Ausfall einer Kundenanlage mit entsprechendem Abnahmeprofil, sei eine Ungleichbehandlung hinsichtlich der Anforderungen an die IT-Sicherheit allein unter Anknüpfung an die rein juristische Qualifikation als Kundenanlage oder als Elektrizitäts- oder Gasverteilernetz nicht gerechtfertigt. Zudem werde die Betroffene gegenüber den Betreibern von Anlagen aus anderen Sektoren ungleich behandelt. Es sei kein Grund ersichtlich, warum die von ihr betriebenen Verteilernetze stärker vor Manipulationen der IT-Systeme zu schützen seien als etwa ein Wassernetz in vergleichbarer Größenordnung oder kleinere Fernwärmenetze.

Schließlich setze der IT-Sicherheitskatalog die gesetzlichen Vorgaben unverhältnismäßig um. Die unterschiedslose Verpflichtung zur Einführung und Zertifizierung eines ISMS sei unangemessen. Die Bundesnetzagentur gehe auch offensichtlich selbst davon aus, dass die unterschiedslose Umsetzungspflicht des IT-Sicherheitskatalogs unangemessen sei, wenn sie in ihren als Anlage BF 10 vorgelegten FAQ unter anderem mitteile, dass Systeme ohne Gefährdungspotential keine Umsetzungspflicht für die diesbezüglichen Sicherheitsanforderungen des IT-Sicherheitskatalogs treffe. Die rechtlich unverbindlichen FAQ könnten den verbindlichen Regelungsgehalt des IT-Sicherheitskatalogs indes nicht ändern. Die Verhältnismäßigkeit hätte eine differenzierte Betrachtung der betroffenen Unternehmen nach ihrer Größe und der Sicherheitsrelevanz des Unternehmens erfordert, wie dies etwa in § 8c Abs. 1 BSI-Gesetz erfolge, der Kleinstunternehmen von den Regelungen der §§ 8a und 8b BSI-Gesetz ausnehme. Der im Einzelnen dargelegte interne und externe erhebliche Aufwand stehe zu den aufgezeigten äußerst geringen Auswirkungen im Falle eines Ausfalls von IT-Systemen oder deren Manipulation außer Verhältnis.

Die Betroffene beantragt,

den Beschluss der Bundesnetzagentur „IT-Sicherheitskatalog gemäß

§ 11 Abs. 1a Energiewirtschaftsgesetz“, veröffentlicht am 12.08.2015, aufzuheben.

Die Bundesnetzagentur beantragt,

die Beschwerde zurückzuweisen.

Die Bundesnetzagentur macht geltend, dass die Beschwerde unbegründet sei, da sie mit dem streitgegenständlichen IT-Sicherheitskatalog die Grenzen des ihr eingeräumten Ermessens nicht überschritten habe.

Der IT-Sicherheitskatalog verstoße nicht gegen den Gleichheitsgrundsatz aus Art. 3 Abs. 1 GG. Der Gesetzgeber habe im Rahmen des § 11 Abs. 1a EnWG bewusst keine Unterscheidung zwischen Netzbetreibern getroffen, sondern alle Netzbetreiber adressiert. Die Wertungen der BSI-KritisV seien für die Auslegung des § 11 Abs. 1a EnWG ohne Relevanz. Ihre Zuständigkeit, mit dem IT-Sicherheitskatalog Mindeststandards für die IT-Sicherheit von Netzbetreibern vorzugeben, sei vom Gesetzgeber gerade nicht in das Regelungsregime des BSI-Gesetzes, sondern in den Anwendungsbereich des EnWG aufgenommen worden. Das Fehlen einer Differenzierung zwischen den Netzbetreibern ergebe sich auch aus Sinn und Zweck des § 11 Abs. 1a EnWG, da ein umfassender Schutz des sicheren Netzbetriebs angesichts der elektrischen und informatorischen Koppelung von Energieversorgungsnetzen nur dann gewährleistet sei, wenn alle Netzbetreiber den IT-Sicherheitskatalog als Mindeststandard umsetzen würden. Der Gesetzgeber gehe auch ersichtlich nicht davon aus, dass die Sicherheitsstandards für Netzbetreiber und Betreiber von Energieanlagen gleich sein müssten. Des Weiteren könne die gesetzgeberische Entscheidung, dass ein Sicherheitskatalog für alle Betreiber von Energieversorgungsnetzen zu erstellen sei, nicht durch eine Rechtsverordnung wie die BSI-KritisV durchbrochen werden. Die frühe Einführung des § 11 Abs. 1a EnWG bereits im Jahr 2011 zeige, dass gerade dem Betrieb der Strom- und Gasnetze eine versorgungstechnische Sonderstellung gegenüber dem Betrieb von Anlagen in anderen Sektoren zukomme, die insbesondere darauf beruhe, dass der sichere Betrieb Kritischer Infrastrukturen i.S.d. BSI-KritisV vom sicheren Betrieb der Energieversorgungsnetze abhängig sei, was umgekehrt nicht gelte.

Der IT-Sicherheitskatalog beeinträchtige die Betroffene auch nicht unverhältnismäßig in ihren Rechten. Ob die Betroffene bereits jetzt umfassende und angemessene Maßnahmen zur Gewährleistung der IT-Sicherheit ergriffen habe, könne dahinstehen. Denn der Gesetzgeber habe im Rahmen seiner Einschätzungsprärogative bereits die fehlerfreie Abwägungsentscheidung getroffen, dass ein angemessener Schutz des Betriebs eines Energieversorgungsnetzes nur dann vorliege, wenn der Katalog von Sicherheitsanforderungen eingehalten und dies vom Betreiber dokumentiert sei. Darüber hinaus wäre es ihr bei der hohen Anzahl von rund 1.600 Strom- und Gasnetzbetreibern schlicht nicht möglich, die Einhaltung der vom jeweiligen Netzbetreiber umgesetzten und von ihm als angemessen empfundenen Sicherheitsstandards selbst nachzuprüfen. Zu einer Nachprüfung sei sie aber gerade verpflichtet. Es komme auch nicht auf die Folgen eines Ausfalls von IT-Systemen an. Der IT-Sicherheitskatalog solle u.a. auch vorsätzliche Angriffe oder fahrlässiges Fehlverhalten, die zu Fehlinformationen in den IT-Systemen und damit zu Ausfällen und Schäden im Netzbetrieb führen können, verhindern. Die wirtschaftlichen Belastungen seien der Betroffenen schließlich zumutbar. Es fehle an konkretem Vortrag zu konkreten wirtschaftlichen Belastungen. Die in den ISO-Normen genannten Maßnahmen seien nicht per se ungeprüft umzusetzen. Die Auswahl der Maßnahmen sei dem Netzbetreiber zu überlassen und individuell für sein Netz und seinen konkreten Schutzbedarf anpassbar. Das gewählte System erlaube gerade die Anpassung der Maßnahmen an die Anforderungen (und damit auch letztlich die Größe) des jeweiligen Netzbetreibers. Auch die wirtschaftlichen Belastungen seien damit stark von der Größe bzw. der Struktur des Netzes abhängig. Im IT-Sicherheitskatalog sei ausdrücklich geregelt, dass bei der Angemessenheit einer Maßnahme insbesondere deren technischer und wirtschaftlicher Aufwand zu berücksichtigen sei.

Wegen der weiteren Einzelheiten des Sach- und Streitstands wird auf die zwischen den Beteiligten gewechselten Schriftsätze mit Anlagen sowie das Protokoll der Senatssitzung Bezug genommen.

B.

Die zulässige Beschwerde ist unbegründet.

I.

Die form- und fristgerecht innerhalb der entsprechend § 58 Abs. 2 S. 1 VwGO geltenden Jahresfrist eingelegte und begründete Beschwerde ist zulässig, insbesondere ist sie als Anfechtungsbeschwerde gegen eine Allgemeinverfügung statthaft, §§ 75 Abs. 1 S. 1, 78 Abs. 1, Abs. 3, 83 Abs. 4 EnWG. Allgemeinverfügung ist nach der Definition des § 35 Satz 2 VwVfG ein Verwaltungsakt, der sich an einen nach allgemeinen Merkmalen bestimmten oder bestimmbaren Personenkreis richtet oder die öffentlich-rechtliche Eigenschaft einer Sache oder ihre Benutzung durch die Allgemeinheit betrifft. Diese Voraussetzungen liegen hier vor, da der angesprochene Personenkreis durch den IT-Sicherheitskatalog klar abgegrenzt wird und der IT-Sicherheitskatalog für diesen Personenkreis verbindliche Rechtsfolgen hat (zur regulierungsbehördlichen Allgemeinverfügungen vgl. auch BGH, Kartellsenat, Beschluss v. 29.04.2008 - KVR 28/07 - Rn. 10, NJW-RR 2008, 1654 ff. - "EDIFACT"; Senat, RdE 2010, 35, 36).

Die Betroffene ist als „geborene“ Verfahrensbeteiligte auch beschwerdebefugt. Im Verwaltungsverfahren bei der Regulierungsbehörde sind nach § 66 Abs. 2 Nr. 2 EnWG natürliche und juristische Personen beteiligt, gegen die sich das Verfahren richtet. Umfasst sind alle, die unmittelbar durch eine das Verfahren abschließende Entscheidung belastet werden können, also die potentiellen Adressaten in Abgrenzung von den vom Verfahren lediglich Betroffenen i. S. v. § 41 Abs. 1 VwVfG (Hanebeck in: Britz/Hellermann/Hermes, 3. Aufl., EnWG, § 66 Rn. 9). Da die Betroffene Systeme für die Netzsteuerung i.S.d. Abschnitts D des IT-Sicherheitskatalogs betreibt, ist sie unmittelbare Adressatin des IT-Sicherheitskatalogs.

II.

Die Beschwerde bleibt in der Sache ohne Erfolg, da der am 12.08.2015 veröffentlichte IT-Sicherheitskatalog rechtmäßig ist und die Betroffene nicht in ihren Rechten verletzt.

§ 11 Abs. 1a EnWG enthält den Auftrag an die Bundesnetzagentur, im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von Si-

cherheitsanforderungen zu erstellen zum Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind. § 11 Abs. 1a EnWG ist im Rahmen des Gesetzes zur Neuregelung energiewirtschaftlicher Vorschriften vom 26.07.2011 (EnWG-Novelle 2011) neu eingefügt und durch das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 17.07.2015 (IT-Sicherheitsgesetz) abgeändert worden. Bei der Erstellung und Veröffentlichung des streitgegenständlichen IT-Sicherheitskatalogs hat sich die Bundesnetzagentur im Rahmen des ihr von § 11 Abs. 1a EnWG eingeräumten Ermessens bewegt.

1. Die Ermessensentscheidung ist nach den auch im Energiewirtschaftsrecht geltenden allgemeinen Grundsätzen gerichtlich nur daraufhin überprüfbar, ob die Behörde die gesetzlichen Grenzen des Ermessens überschritten (Ermessensüberschreitung), ihr Ermessen überhaupt nicht ausgeübt (Ermessensnichtgebrauch) oder von dem Ermessen in einer dem Zweck der Ermächtigung nicht entsprechenden Weise Gebrauch gemacht hat (Ermessensfehlgebrauch) (etwa Senat, Beschluss vom 28.04.2015, 3 Kart 363/12, BeckRS 2016, 2892, beck-online).

2. Dass der IT-Sicherheitskatalog unterschiedslos auf alle Energieversorgungsnetzbetreiber anwendbar ist, und zwar ungeachtet der Größe des betroffenen Unternehmens und der Sicherheitsrelevanz des betroffenen Verteilernetzes, stellt weder einen rechtsfehlerhaften Ermessensnichtgebrauch dar noch hat die Bundesnetzagentur die gesetzlichen Grenzen des ihr zustehenden Ermessens deshalb überschritten.

2.1. Nach dem Wortlaut des § 11 Abs. 1a i.V.m. § 11 Abs. 1 EnWG sind Betreiber von Energieversorgungsnetzen dazu verpflichtet, einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb erforderlich sind, als Teil ihrer Pflicht zum Betrieb eines sicheren Versorgungsnetzes zu gewährleisten und ist zur Erfüllung dieser Verpflichtung von der Regulierungsbehörde ein Katalog von Sicherheitsanforderungen zu erstellen und zu veröffentlichen. Der IT-Sicherheitskatalog ist nach dem Gesetzeswortlaut mithin unterschiedslos an sämtliche Adressaten der Verpflichtung zum sicheren Netzbetrieb zu richten, d.h. sämtliche Netzbetreiber.

2.2. Etwas anderes ergibt sich nicht aus gesetzeshistorischen Erwägungen unter Berücksichtigung der Vorschriften des § 11 Abs. 1b, Abs. 1c bzw. des BSI-Gesetzes i.V.m. mit der BSI-KritisV. Denn es lässt sich diesen Regelungen bzw. deren gesetzgeberischer Begründung nicht entnehmen, dass der Gesetzgeber der Bundesnetzagentur einen Ermessensspielraum hinsichtlich der Bestimmung des Adressatenkreises im Rahmen ihrer Verpflichtung aus § 11 Abs. 1a EnWG eingeräumt hätte.

2.2.1. Nach § 11 Abs. 1b S. 1 EnWG haben Betreiber von Energieanlagen, die durch die BSI-KritisV in der jeweils geltenden Fassung als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind, innerhalb einer von der Regulierungsbehörde festzulegenden Frist einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme zu gewährleisten, die für einen sicheren Anlagenbetrieb notwendig sind. § 11 Abs. 1b S. 2 EnWG sieht vor, dass die Regulierungsbehörde hierzu im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von Sicherheitsanforderungen, in den auch die Bestimmung der Frist nach S. 1 aufzunehmen ist, erstellt und diesen veröffentlicht.

§ 11 Abs. 1b EnWG ist durch das IT-Sicherheitsgesetz vom 17.07.2015 eingeführt worden. Die Tatsache, dass der Gesetzgeber in diesem Zuge den nach § 11 Abs. 1a EnWG im Hinblick auf alle Betreiber von Energieversorgungsanlagen bestehenden Auftrag der Bundesnetzagentur zur Erstellung eines IT-Sicherheitskatalogs unverändert gelassen hat, lässt den Schluss zu, dass der Gesetzgeber den Adressatenkreis gerade nicht, wie im Hinblick auf Energieanlagenbetreiber geschehen, auf Kritische Infrastrukturen im Sinne der BSI-KritisV beschränken wollte. Dies gilt umso mehr, als bereits seit Ende 2013 der Entwurf eines IT-Sicherheitskatalogs gemäß § 11 Abs. 1a EnWG der Bundesnetzagentur veröffentlicht war, der alle Energieversorgungsnetzbetreiber adressierte. Der Gesetzgeber hat dies gerade nicht zum Anlass genommen, in § 11 Abs. 1a EnWG eine Unterscheidung zwischen einzelnen Netzbetreibern im Hinblick auf die Sicherheitsrelevanz ihrer Netze aufzunehmen, obgleich er § 11 Abs. 1a EnWG im Zuge des IT-Sicherheitsgesetzes ebenfalls überarbeitet hat. Dies

ergibt sich auch aus der Begründung des Entwurfs der Bundesregierung zum IT-Sicherheitsgesetz vom 25.02.2015 (BT-Drs. 18/4096, S. 32 f.), wo es heißt:

„§ 11 Abs. 1a wurde mit der EnWG-Novelle 2011 in das Energiewirtschaftsgesetz aufgenommen. Ein erster Entwurf des Sicherheitskatalogs der Bundesnetzagentur wurde erarbeitet und wird derzeit in der Branche erörtert. (…). Mit dem nun ergänzten Satz 3 ist die Regulierungsbehörde verpflichtet, die Überprüfungen von den Betreibern zu fordern. Die Änderung trägt dem in § 8a Abs. 3 des BSI-Gesetzes etablierten Schutzniveau Rechnung und verhindert, dass der Sicherheitskatalog der Bundesnetzagentur hinter diesem Schutzniveau zurückfallen könnte. Für den vorgelegten Sicherheitskatalog hat dies keine praktischen Folgen, da dieser bereits entsprechende Anforderungen vorsieht.“

In der Gesetzesbegründung heißt es zur Frage der Behandlung von Energieversorgungsnetzen und -anlagen weiter (a.a.O., S. 33):

„Die Aufnahme von Schutzstandards für Energieanlagen, die in der Rechtsverordnung nach § 10 Abs. 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, ist notwendig, um einen umfassenden Schutz für den sicheren Netzbetrieb sicherzustellen. Energieanlagen, die mit dem öffentlichen Versorgungsnetz verbunden sind, werden verpflichtet, dort, wo eine Gefährdung für den Netzbetrieb möglich ist, ebenfalls Sicherheitsmaßnahmen zu ergreifen. Aufgrund der technischen Nähe ist es notwendig und sinnvoll, dass die Sicherheitsmaßnahmen für Netzbetreiber und für die betroffenen Energieanlagen aufeinander abgestimmt sind. Aus diesem Grund wird die Bundesnetzagentur als für die Sicherheitsstandards des Netzbetriebs zuständige Behörde beauftragt, auch die Sicherheitsstandards für die Energieanlagen zu erarbeiten und deren Einhaltung zu überwachen. Abs. 1b entspricht insoweit Abs. 1a.“

Ein gesetzgeberischer Wille, Energieversorgungsnetze und Energieanlagen im Hinblick auf die IT-Sicherheit gleich zu behandeln, kommt darin entgegen der von der Betroffenen vertretenen Ansicht nicht zum Ausdruck. Die Sicherheitsmaßnahmen sollen vielmehr „aufeinander abgestimmt sein“. Dabei erkennt der Gesetzgeber gerade die lediglich flankierende Wirkung der von den Energieanlagenbetreibern zu schaffenden Sicherheitsmaßnahmen für den sicheren Netzbetrieb ausdrücklich an,

indem er ein Bedürfnis für Sicherheitsmaßnahmen dort erkennt, „wo eine Gefährdung des Netzbetriebs möglich ist“. Soweit es heißt, dass Abs. 1b insoweit Abs. 1a entsprechen soll, ergibt sich aus dem Kontext der Regelung ohne Weiteres, dass dies nur im Hinblick auf die Zuständigkeit der Bundesnetzagentur für die Sicherheitsstandards („insoweit“) gilt.

2.2.2. Entgegen der von der Betroffenen vertretenen Auffassung lässt auch § 11 Abs. 1c EnWG nicht den Schluss zu, der Gesetzgeber habe eine Gleichbehandlung von Energieversorgungsnetzbetreibern und Energieanlagenbetreibern gewollt.

Hiergegen spricht unmissverständlich, dass § 11 Abs. 1c EnWG - wie auch § 11 Abs. 1b EnWG - anders als § 11 Abs. 1a EnWG ausdrücklich auf die Maßstäbe der BSI-KritisV Bezug nimmt.

Nicht entscheidungserheblich ist demgegenüber, ob die Formulierung „Betreiber von Energieversorgungsnetzen und Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Abs. 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, (…)“, mit der § 11 Abs. 1c S. 1 EnWG die Adressaten der Meldeverpflichtung bestimmt, alle Betreiber von Energieversorgungsnetzen in Bezug nimmt oder nur solche, die eine Kritische Infrastruktur betreiben, d.h. ob sich die Beschränkung auf Kritische Infrastrukturen nur auf die Energieanlagenbetreiber oder auch auf die Energieversorgungsnetzbetreiber bezieht, was zwischen den Verfahrensbeteiligten umstritten ist. Der Wortlaut ist insoweit nicht eindeutig. Dafür, dass von § 11 Abs. 1c EnWG in seiner gegenwärtigen Fassung alle Energieversorgungsnetzbetreiber umfasst sind und damit insoweit derselbe Adressatenkreis wie in § 11 Abs. 1a EnWG, spricht, dass es im Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlament und Rates vom 06.07.2016 über Maßnahmen zur Gewährung eines hohen gemeinsamen Sicherheitsniveaus von Netz und Informationssystemen in der EU, dort S. 31, unter anderem heißt:

„*Ergänzend wird in § 11 Abs. 1c EnWG klargestellt, dass die Meldepflichten nach Abs. 1c S. 1 für **alle** Betreiber von Energieversorgungsnetzen gelten sowie für solche Energieanlagen, die durch Rechtsverordnung als Kritische Infrastrukturen bestimmt worden sind. Diese Änderung dient lediglich der Klarstellung der Adressaten der*

Verpflichtung. Inhaltlich wirkt sich diese rein redaktionelle Änderung nicht aus.“ (Hervorhebung durch den Senat)

Dies steht allerdings in einem gewissen Widerspruch dazu, dass es zum Erfüllungsaufwand der Verwaltung durch die Umsetzung der Richtlinie im vorzitierten Gesetzesentwurf (dort S. 8) heißt, dass „aufgrund des Gesetzes (…) der Kreis der meldepflichtigen Betreiber um ca. 1.6000 Anlagenbetreiber ausgeweitet“ wird.

Die Frage der Auslegung des Adressatenkreises des § 11 Abs. 1c EnWG in seiner gegenwärtigen Fassung kann aber offenbleiben. Denn selbst wenn man davon ausginge, dass § 11 Abs. 1c EnWG in seiner derzeitigen Fassung nur solche Netzbetreiber adressiert, die eine Kritische Infrastruktur i.S.d. BSI-KritisV betreiben, so würde allein eine Gleichbehandlung der Betreiber von Energieversorgungsnetzen und Energieanlagen bezüglich der Meldepflicht in § 11 Abs. 1c EnWG nicht den Schluss zulassen, eine Gleichbehandlung solle – entgegen dem Gesetzeswortlaut - umfänglich erfolgen. Vielmehr lässt sich der beabsichtigten Gesetzesänderung entnehmen, dass der Gesetzgeber - jedenfalls zukünftig - von einer Meldepflicht sämtlicher Energieversorgungsnetzbetreiber einerseits und nur des „qualifizierten“ Kreises der Energieanlagenbetreiber, die Kritische Infrastrukturen i.S.d. BSI-KritisV betreiben, andererseits ausgeht, also gerade eine Differenzierung zwischen Energieversorgungsnetzbetreibern einerseits und Energieanlagenbetreibern andererseits im Hinblick auf die Meldepflicht vornimmt. Demnach will der Gesetzgeber Energieversorgungsnetzbetreiber und Energieanlagen in Bezug auf die Relevanz von BSI-Gesetz i.V.m. BSI-KritisV gerade nicht gleich behandelt sehen.

2.2.3. Auch die Regelungen im BSI-Gesetz i.V.m. der BSI-KritisV eröffnen der Bundesnetzagentur keinen Ermessenspielraum dahingehend, dass sie beim Adressatenkreis des IT-Sicherheitskataloges gemäß § 11 Abs. 1a EnWG den Vorgaben der BSI-KritisV folgend nach Kritischen Infrastrukturen und solchen, die die in der BSI-KritisV festgelegten Schwellenwerte nicht erfüllen, differenzieren könnte oder – im Sinne einer Ermessensreduzierung auf Null - sogar müsste.

Zwar lässt sich den vorgenannten Regelungen entnehmen, dass der Gesetzgeber bestimmten Infrastrukturen eine besondere Bedeutung im Bereich der IT-Sicherheit

zugewiesen hat, die zur Einführung eines Mindestschutzniveaus ihrer IT-Systeme verpflichtet werden, da ein Ausfall oder eine Beeinträchtigung ihrer Infrastruktur weitreichende gesellschaftliche Folgen nach sich ziehen kann und ihnen eine besondere Verantwortung für das Gemeinwohl zukommt (vgl. die Begründung der Beschlussempfehlung des Innenausschusses zum Entwurf der Bundesregierung zum IT-Sicherheitsgesetz, BT-Drs. 18/4121 S. 1 ff). Die Betroffene unterhält keine Kritischen Infrastrukturen in diesem Sinne, da sie die in der BSI-KritisV aufgestellten Schwellenwerte, ab deren Überschreitung von einer Kritischen Infrastruktur auszugehen ist, bei Weitem nicht erreicht.

Hieraus folgt jedoch nicht, dass nach dem Willen des Gesetzgebers nur hinsichtlich solcher Strukturen ein gewisser IT-Sicherheitsstandard gerechtfertigt wäre. Dies ergibt sich schon daraus, dass der Gesetzgeber, wie bereits aufgezeigt, den durch die Energierechtsnovelle 2011 eingeführten § 11 Abs. 1a EnWG nicht im Zuge des IT-Sicherheitsgesetzes abgeschafft oder durch eine Bezugnahme auf die BSI-KritisV angepasst, sondern lediglich in anderer Hinsicht geringfügig abgeändert hat. Der Gesetzgeber hat in der Begründung des Gesetzesentwurfs zum IT-Sicherheitsgesetz (BT-Drs. 18/4096) vielmehr ausdrücklich auf die besondere Bedeutung der Netze neben den sog. Kritischen Infrastrukturen hingewiesen, wenn es dort auf S. 1 heißt: *„Der Schutz der IT-Systeme von solchen Kritischen Infrastrukturen und der für den Infrastrukturbetreib nötigen Netze ist daher von größter Wichtigkeit“.*

Hiervon abgesehen unterliegt die Zuständigkeit der Bundesnetzagentur, mit dem IT-Sicherheitskatalog Mindeststandards für die IT-Sicherheit von Netzbetreibern vorzugeben, gerade nicht dem Regelungsregime des BSI-Gesetz, sondern stellt eine eigenständige Regelung im Rahmen des EnWG dar. So geht der Gesetzgeber, der Betreiber von Energieversorgungsnetzen und Energieanlagen im Sinne des Energiewirtschaftsgesetzes vom Anwendungsbereich des § 8a BSI-Gesetzes in § 8c Abs. 2 Ziff. 2 BSI-Gesetz ausdrücklich ausnimmt, ausweislich des Gesetzesentwurfs davon aus, dass diese Unternehmen im EnWG mit den §§ 11 Abs. 1a – 1c *„bereits einer § 8a des BSI-Gesetzes gleichwertigen Regelung unterfallen“* (Begründung des Entwurfs der Bundesregierung zum IT-Sicherheitsgesetz vom 25.02.2015, BT-Drs. 18/4096, S. 29). Auch der Gesetzgeber nimmt mithin an, dass zwei voneinander un-

abhängige und abschließende Regelungsregime vorliegen, so dass kein Raum besteht, die Vorgaben des §§ 8a, 8b Abs. 3-5 BSI-Gesetz in das EnWG hineinzulesen.

2.3. Aus den vorstehenden Erwägungen folgt gleichzeitig, dass der Bundesnetzagentur der von der Betroffenen geltend gemachte Ermessenspielraum im Hinblick auf die Bestimmung des Adressatenkreises des IT-Sicherheitskatalogs weder aus systematischen noch aus teleologischen Gesichtspunkten eröffnet ist. Insbesondere wird der vom Gesetzgeber intendierte, im Einzelnen bereits dargelegte Sinn und Zweck der gesetzlichen Regelung nur dann erreicht, wenn der Schutz der TK- und EDV-Systeme der Energieversorgung *durchgängig und umfassend* gewährleistet ist.

2.4. Schließlich war der Bundesnetzagentur auch nicht über eine verfassungskonforme Auslegung des § 11 Abs. 1a EnWG ein Ermessenspielraum bei der Bestimmung des Adressatenkreises deshalb eröffnet, weil eine Differenzierung zwischen einzelnen Energieversorgungsnetzbetreibern nach ihrer Größe oder der Systemrelevanz der Netze durch den Gleichheitsgrundsatz des Art. 3 Abs. 1 GG geboten wäre. Es kann dahinstehen, ob angesichts der vorstehenden Ausführungen Raum für eine dahingehende verfassungskonforme Auslegung besteht. Denn soweit der IT-Sicherheitskatalog sämtliche Betreiber von Energieversorgungsnetzen und damit auch die Betroffene unabhängig von deren Größe bzw. der Systemrelevanz ihrer Netze adressiert, liegt hierin weder eine ungerechtfertigte Gleichbehandlung der Energieversorgungsnetzbetreiber mit den Betreibern von Kritischen Infrastrukturen i.S.d. §§ 2 Abs. 10, 10 BSIG i.V.m. der BSI-KritisV, noch eine ungerechtfertigte Ungleichbehandlung der Energieversorgungsnetzbetreiber gegenüber Betreibern von Energieanlagen bzw. Anlagen aus anderen Sektoren, die nur dann den in § 11 Abs. 1b EnWG normierten Anforderungen an die IT-Sicherheit unterfallen, wenn sie Kritische Infrastrukturen betreiben.

Die Betroffene macht insoweit geltend, dass es sachlich nicht gerechtfertigt und damit diskriminierend sei, dass bezüglich sog. Kritischer Infrastrukturen Schwellenwerte existieren und Infrastrukturen wie Energieanlagen oder sonstige Anlagenbetreiber, die diese Schwellenwerte nicht erreichen, keinen erhöhten Anforderungen an die IT-Sicherheit genügen müssten, während Energieversorgungsunternehmen ausnahms-

los dem Anwendungsbereich des § 11 Abs. 1a EnWG unterfielen und mithin den dort aufgestellten Standards genügen müssten. Dem ist nicht zu folgen.

2.4.1. Eine Verletzung des allg. Gleichheitssatzes setzt voraus, dass vergleichbare Sachverhalte, Gruppen oder Personen in wesentlicher Hinsicht ungleich oder wesentlich unterschiedliche Sachverhalte, Gruppen oder Personen gleichbehandelt werden. Für die Vergleichsgruppenbildung bedarf es eines Aktes wertender Erkenntnis, um den Bezugspunkt für die wesentliche Übereinstimmung bzw. Differenz der zum Vergleich gestellten Sachverhalte, Gruppen oder Personen erfassen zu können (Schmidt in: Erfurter Kommentar, Grundgesetz, 17. Aufl., Art. 3 Rn. 33, zitiert nach beck-online).

2.4.2. Soweit die Betreiber von Energieversorgungsnetzen gegenüber den Betreibern von Energieanlagen im Hinblick auf den Schutz gegen Bedrohungen für die TK- und EDV-Systeme unterschiedlich behandelt werden, fehlt es bereits an einem vergleichbaren Adressatenkreis.

Der Gesetzgeber hat mit § 11 Abs. 1a EnWG auf die Gefahren reagiert, die sich aus der zunehmenden Bedeutung von TK- und EDV-Systemen für die Steuerung energietechnischer Anlagen ergeben (Sötebier in: Britz/Hellermann/Hermes, a.a.O., § 11 Rn. 100). Schon aus der Tatsache, dass er bereits durch die Energierechtsnovelle 2011 mit § 11 Abs. 1a EnWG eine besondere Verpflichtung der Energieversorgungsnetzbetreiber zur Gewährleistung eines angemessenen Schutzes gegen solche Bedrohungen eingeführt hat, und mithin deutlich vor dem IT-Sicherheitsgesetz, in dem er eine diesbezügliche Verpflichtung von Betreibern sog. Kritischer Infrastrukturen normiert hat, ergibt sich, dass er von einer versorgungstechnischen Sonderstellung der Energieversorgungsnetze gegenüber anderen Infrastrukturen, insbesondere den Energieanlagen, ausgeht. Diese Sonderstellung kommt auch darin zum Ausdruck, dass der Gesetzgeber den Betreibern von Energieversorgungsnetzen im Sinne des EnWG eine Vielzahl weiterer Pflichten auferlegt hat. Zu diesen Pflichten gehören u.a. Entflechtungspflichten (§§ 6 ff. EnWG), Netzanschlusspflichten gegenüber Dritten (§§ 17, 18 EnWG), Netzöffnung-/Netzzugangspflichten (§§ 20 ff. EnWG), Kalkulations-/Genehmigungs-/Veröffentlichungspflichten von Netznutzungsentgelten (§§ 21 ff. EnWG), Meldepflichten bei Versorgungsstörungen (§ 52 EnWG) und Beitrags-

pflichten (§ 92 EnWG). Dabei stellen die im EnWG festgeschriebenen Pflichten für Netzbetreiber verfassungsrechtlich relevante Grundrechtseingriffe (u.a. Art. 12 GG – Berufsfreiheit, Art. 14 GG – Eigentumsgarantie) dar (Theobald in: Danner/Theobald, EnWG, § 3 Rn. 24-26, beck-online). Die Anwendbarkeit des netzseitigen EnWG-Pflichtenkatalogs auf Kundenanlagen ist demgegenüber nach allgemeiner Ansicht zur Sicherung der EnWG-Gesetzesziele nicht erforderlich und wäre im Hinblick auf die Grundrechtsrelevanz auch nicht verhältnismäßig (vgl. nur Theobald in: Danner/Theobald, a.a.O.).

Dieser Akt wertender Erkenntnis, mit dem der Gesetzgeber Energieversorgungsnetzbetreibern eine Sonderstellung gegenüber den Betreibern sonstiger Energieanlagen zumisst, begegnet keinen verfassungsrechtlichen Bedenken. Die Annahme einer versorgungstechnischen Sonderstellung rechtfertigt sich, worauf auch die Bundesnetzagentur zutreffend verweist, schon daraus, dass der sichere Betrieb sog. Kritischer Infrastrukturen in sämtlichen anderen Sektoren vom sicheren Betrieb der Energieversorgungsnetze abhängig ist, dies umgekehrt aber nicht der Fall ist. Es kommt dabei nicht entscheidend darauf an, ob es konkret bezogen auf das Netz jedes einzelnen Netzbetreibers und hier insbesondere der Betroffenen zu einem sog. „Kaskadeneffekt“ kommen kann, d.h. die Gefahr von Rückwirkungen von Störungen im Netz der Betroffenen auf weitere verbundene Netze nicht ausgeschlossen werden kann, bzw. ob im Einzelfall der Ausfall eines Verteilernetzes von der Größe der Netze der Betroffenen zu den gleichen Auswirkungen auf das vorgelagerte Netz führen kann wie der Ausfall einer Kundenanlage mit entsprechendem Abnahmeprofil. Denn zum einen können von Störungen in der Versorgungsfunktion der Strom- und Gasnetze grundsätzlich alle daran angeschlossenen Abnehmer betroffen sein, zu denen auch Kritische Infrastrukturen gehören können. Allein diese versorgungstechnische Sonderstellung rechtfertigt es im Ausgangspunkt, Betreiber von Energieversorgungsanlagen im Hinblick auf die Sicherheit der TK- und EDV-Systeme gegenüber den Betreibern sonstiger Energieanlagen als eigenständige Gruppe anzusehen. Zum anderen weist die Bundesnetzagentur zutreffend darauf hin, dass Gegenstand der Informationssicherheit auch der sichere Informationsaustausch ist und auch Störungen, die durch Kommunikationsverbindungen zum Austausch von Betriebsdaten zwischen den Netzbetreibern entstehen können, berücksichtigt werden. Sie hat insoweit auf einen Beispielsfall in Österreich abgestellt, bei dem es am 02.03.2013 aufgrund ei-

nes fehlerhaft adressierten Datenaustauschs zu einer erheblichen Leittechnikstörung im österreichischen Stromnetz gekommen ist, die potentiell auch für die Versorgungssicherheit gefährlich sein kann.

Die Betroffene kann sich deshalb nicht darauf berufen, die Einordnung einer Anlage als Energieversorgungsnetz oder als sonstiger Energieanlage sei insoweit eine rein formale Klassifizierung. Denn die diesbezügliche Unterscheidung ist bereits Ausdruck der wertenden Erkenntnis des Gesetzgebers, dass Energieversorgungsnetzbetreiber aufgrund ihrer besonderen Bedeutung anderen Pflichten unterliegen als die Betreiber sonstiger Energieanlagen. Diese Einschätzung des Gesetzgebers kommt auch darin zum Ausdruck, dass dieser in der Begründung des IT-Sicherheitsgesetzes ausdrücklich darauf verweist, dass der Netzbetrieb umfassend zu schützen ist und deshalb Energieanlagen, die mit dem öffentlichen Versorgungsnetz verbunden sind, dort, wo eine Gefährdung für den Netzbetrieb möglich ist, verpflichtet werden, ebenfalls Sicherheitsmaßnahmen zu ergreifen (Begründung des Entwurfs der Bundesregierung zum IT-Sicherheitsgesetz vom 25.02.2015, BT-Drs. 18/4096).

2.4.3. Aus der aufgezeigten versorgungstechnischen Sonderstellung der Energieversorgungsnetze ergibt sich gleichzeitig, dass die Betreiber von Energieversorgungsnetzen bei wertender Betrachtung im Hinblick auf die Anforderungen an die IT-Sicherheit nicht mit den Betreibern von Anlagen aus sonstigen Sektoren gleich zu behandeln sind, mithin keine zwei grundsätzlich vergleichbaren Sachverhalte vorliegen. Zwar existieren auch Anlagen aus sonstigen Sektoren, denen im Rahmen der Daseinsvorsorge eine besondere Bedeutung zukommt, wie etwa die Wärme- und Trinkwasserversorgung. Insoweit hat der Gesetzgeber über die in der BSI-KritisV festgelegten Schwellenwerte definiert, welchen dieser Anlagen er eine besondere Bedeutung für die Daseinsvorsorge zumisst, und an die deshalb besondere Anforderungen im Hinblick auf die IT-Sicherheit zu stellen sind. Eine schon im Ausgangspunkt mit der Systemrelevanz der Energieversorgungsanlagen vergleichbare Bedeutung sonstiger Anlagen im Hinblick auf die IT-Sicherheit besteht aber gerade nicht.

2.4.4. Korrespondierend dazu, dass die (Ungleich-)Behandlung von Energieversorgungsnetzbetreibern einerseits und Betreibern von Energieanlagen und sonstigen Anlagen anderseits im Hinblick auf die IT-Sicherheit keine grundsätzlich ver-

gleichbaren Sachverhalte betrifft, liegt auch keine ungerechtfertigte Gleichbehandlung der Energieversorgungsnetzbetreiber mit den Betreibern Kritischer Infrastrukturen i.S.d. BSI-KritisV vor.

3. Da aus den vorstehend dargelegten Gründen keine durchgreifenden Bedenken gegen die Verfassungsmäßigkeit des § 11 Abs. 1a GG bestehen, war eine Aussetzung des Verfahrens zur Einholung einer Entscheidung des Bundesverfassungsgerichts über den von der Betroffenen gerügten Verstoß gegen Art. 3 Abs. 1 GG nicht angezeigt.

4. Die Bundesnetzagentur hat mit der Einführung des streitgegenständlichen IT-Sicherheitskatalogs auch das Angemessenheitskriterium ordnungsgemäß umgesetzt.

4.1. Der Grundsatz der Verhältnismäßigkeit erfordert, dass eine Maßnahme zur Erreichung des von ihr verfolgten Zwecks geeignet und erforderlich ist sowie dass die Belastung des Eigentümers in einem angemessenen Verhältnis zu den mit der Regelung verfolgten Interessen steht (etwa BVerfG, Beschluss vom 02.09.2004, 1 BvR 1860/02, NVwZ 2005, 203, 204).

4.2. Die unterschiedslose Verpflichtung zur Einführung, Fortschreibung und regelmäßigen Zertifizierung, wie sie im IT-Sicherheitskatalog unter Bezugnahme auf die DIN ISO/IEC 27001, die DIN ISO/IEB 27002 und die DIN ISO/EC TR 27019 verlangt wird, führt nicht zu wirtschaftlichen, organisatorischen bzw. personellen Belastungen, die der Betroffenen – und allen anderen Betreibern von Energieversorgungsnetzen, die keine Kritischen Infrastrukturen i.S.d. § 2 Abs. 10, § 10 BSI-Gesetz i.V.m. der BSI-KritisV betreiben – unangemessen und nicht mehr zumutbar wären.

Zur Ausgestaltung ihres gesetzlichen Auftrags aus § 11 Abs. 1a EnWG, im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von Sicherheitsanforderungen zu erstellen, hat sich die Bundesnetzagentur an etablierten ISO-Normen orientiert. Weiter ist zu beachten, dass der Gesetzgeber im Rahmen des ihm zustehenden Regelungsermessens ausdrücklich die Vorgabe gemacht hat, dass die Einhaltung des IT-Sicherheitskatalogs von der Bundesnetzagentur überprüft

werden und sie zu diesem Zwecke nähere Bestimmungen zu Format, Inhalt und Gestaltung der Dokumentation treffen kann (§ 11 Abs. 1a S. 4 und S. 5 EnWG). Die gesetzliche Vorgabe einer Überprüfbarkeit der Umsetzung ist angesichts der schon dargelegten besonderen Bedeutung der Energieversorgungsnetze nicht bereits für sich gesehen unangemessen. Sie bedingt, dass für die Umsetzung der Maßnahmen ein standardisierter Rahmen geschaffen wird, der es der Bundesnetzagentur ermöglicht, die Umsetzung auch bei allen ca. 1.600 Verteilernetzbetreibern zu überprüfen. Dies setzt voraus, dass der standardisierte Rahmen auch für alle Verteilernetzbetreiber gilt, was für diese zwangsläufig mit einem nicht unerheblichen Aufwand verbunden ist. Angesichts der gesetzgeberischen Vorgabe, eine Überprüfbarkeit zu schaffen, kann sich die Betroffene nicht erfolgreich darauf berufen, der Implementierung eines ISMS würde kein Sicherheitsmehrwert gegenüberstehen. Denn allein die Transparenz der durchgeführten Maßnahmen und deren Überprüfbarkeit auf ihre Angemessenheit stellt den vom Gesetzgeber eingeforderten Mehrwert dar.

Die Betroffene hat zum Umfang der sie durch die Einführung und Zertifizierung des ISMS und aus dessen fortdauernder Prüfung und Überarbeitung treffenden wirtschaftlichen Lasten ausführlich vorgetragen. Zwar ergeben sich hieraus Kosten für die Einführung und Zertifizierung des ISMS im oberen … Bereich. Auch fallen die internen Personalkosten für die Fortschreibung des ISMS nicht unerheblich ins Gewicht. Die Kosten für die Rezertifizierungen von nur … Euro sind demgegenüber zu vernachlässigen. In der Gesamtbetrachtung des Aufwandes ist angesichts der bereits aufgezeigten Bedeutung, die der Gesetzgeber – wie dargestellt berechtigterweise - der IT-Sicherheit gerade im Bereich der Energieversorgungsnetze einräumt (etwa Gesetzentwurf der Bundesregierung zum IT-Sicherheitsgesetz, BT-Drs. 18/4096 S. 1, wonach „der Schutz der für den Infrastrukturbetrieb nötigen Netze daher von größter Wichtigkeit ist“), aber gerade nicht hinreichend vorgetragen und auch nicht ersichtlich, dass die wirtschaftlichen Lasten für den einzelnen – insbesondere kleinen - Netzbetreiber nicht tragbar wären. Dies gilt umso mehr, als bereits der Aufwand für die Implementierung und Zertifizierung des ISMS – wie auch die Betroffene selbst einräumt – von der Komplexität der IT-Strukturen des einzelnen Netzbetreibers abhängt und deshalb dessen Größe bzw. die Systemrelevanz des Netzes durchaus Einfluss auf die Höhe des entstehenden Aufwandes haben. Schließlich sind die dem

Netzbetreiber entstehenden Kosten im Rahmen der Anreizregulierung wirksam und können letztlich auf die Netznutzer abgewälzt werden.

Die Betroffene kann nicht erfolgreich geltend machen, dass selbst die Bundesnetzagentur die Verpflichtung der kleineren, keine Kritischen Infrastrukturen betreibenden Netzbetreiber als unangemessen ansehe. Soweit die Bundesnetzagentur in ihren als Anlage BF 10 vorgelegten FAQ die Frage, wer für die Umsetzung des IT-Sicherheitskatalogs verantwortlich ist, u.a. mit der Aussage

„Betreibt ein Strom- oder Gasnetzbetreiber keine vom IT-Sicherheitskatalog erfassten Systeme in seinem Netz und lässt diese auch nicht von einem externen Dienstleister betreiben bzw. handelt es sich nur um Systeme ohne Gefährdungspotential, besteht auch keine Umsetzungspflicht für die diesbezüglichen Sicherheitsanforderungen des IT-Sicherheitskatalogs.“

beantwortet hat, so ist dies nach dem Verständnis des Senats nicht dahingehend zu deuten, dass die Bundesnetzagentur einzelne Systeme, auch wenn sie dem ausdrücklichen Anwendungsbereich des IT-Sicherheitskatalogs unterfallen, von dessen Anwendungsbereich nur deshalb ausnehmen will, weil diese Systeme kein „Gefährdungspotential“ haben. Es ist schon völlig unklar, was mit dem „Gefährdungspotential“ gemeint sein soll. Vor allem drängt sich angesichts des Kontextes, insbesondere der vorangegangenen eindeutigen Aussage

„Ausnahmen von der Umsetzungspflicht, etwa in Abhängigkeit von der Größe eines Netzbetreibers, bestehen nicht“,

die Annahme auf, dass die Bundesnetzagentur hier lediglich eine Umschreibung für die nicht vom IT-Sicherheitskatalog erfassten Systeme geben wollten, nicht aber eine eigene Ausnahme von der Anwendbarkeit statuieren wollte. Gegen die Annahme, die Bundesnetzagentur habe hier den verbindlichen Regelungsgehalt des IT-Sicherheitskatalogs ändern wollen, spricht schließlich, dass eine solche Regelung in den rechtlich unverbindlichen FAQs nicht erfolgen kann.

Anhaltspunkte für eine Unangemessenheit lassen sich schließlich nicht aus § 2 Abs. 10, § 10 BSI-Gesetz i.V.m. der BSI-KritisV ziehen, da die dortigen Vorschriften aus den bereits ausführlich dargelegten Gründen keinen Maßstab für Vorgaben für ein „angemessenes“ Schutzniveau für Energieversorgungsnetzbetreiber darstellen.

4.2. Es liegen auch keine Anhaltspunkte dafür vor, dass die im Rahmen des IT-Sicherheitskatalogs getroffenen Regelungen unangemessen sind.

Die Bundesnetzagentur hat dem Erfordernis der Angemessenheit der zu treffenden Maßnahmen dadurch in hinreichender Weise Rechnung getragen, dass sie keine statischen Anforderungen an die IT-Sicherheit stellt, sondern durch das skalierbare System des ISMS die Angemessenheit einzelner Maßnahmen bezogen auf jeden einzelnen Netzbetreiber, d.h. auch unter Berücksichtigung seiner Größe und Systemrelevanz, zu prüfen und festzulegen ist.

Die vom IT-Sicherheitskatalog für anwendbar erklärte Norm DIN ISO/IEC 27001 legt Leitlinien und allgemeine Prinzipien für die Initiierung, Umsetzung, den Betrieb und die Verbesserung des Informationssicherheits-Managements in einer Organisation fest und stellt diesbezüglich ausdrücklich in Ziff. 0.1. der aktuellen Fassung (DIN ISO/IEC 27001:2015-03) fest: „Erstellung und Umsetzung eines Informationssicherheitsmanagementsystems innerhalb einer Organisation richten sich nach deren Bedürfnissen, den Zielen, den Sicherheitsanforderungen, den organisatorischen Abläufen sowie nach Größe und Struktur der Organisation“.

Soweit bei der Implementierung des ISMS dabei die Normen DIN ISO/IEC 27002 und DIN ISO/IEC TR 27019 (DIN SPEC 27019) in der jeweils geltenden Fassung zu berücksichtigen sind, so ist entscheidend für den Umgang mit den Verweisungen und die Umsetzung der sich aus diesem Katalog ergebenden Anforderungen an die IT-Sicherheit, wie im IT-Katalog auf S. 10 ausdrücklich festgehalten, „diese insbesondere im Hinblick auf die Notwendigkeit für einen sicheren Netzbetreib anzuwenden.“ Dort heißt es weiter: „Das heißt die in den Normen genannten Maßnahmen sind nicht per se ungeprüft umzusetzen, sondern immer in Abhängigkeit von ihrer Bedeutung für die Sicherheit der in Abschnitt D. beschriebenen Anwendungen, Systeme und

Komponenten unter Berücksichtigung der Ergebnisse der unter E.V. beschriebenen Risikoeinschätzung.“

III.

Die Kostenentscheidung beruht auf § 90 Satz 1 EnWG.

Der Gegenstandswert für das Beschwerdeverfahren war gemäß § 50 Abs. 1 Nr. 2 GKG, § 3 ZPO auf bis zu … EUR festzusetzen.

Das wirtschaftliche Interesse der Betroffenen an der Durchführung des Beschwerdeverfahrens bestimmt sich nach den Kosten, die ihr durch die Umsetzung des von ihr angegriffenen IT-Sicherheitskatalogs entstehen. Nach den von der Bundesnetzagentur nicht beanstandeten Angaben der Betroffenen entstehen dieser durch die Einführung des ISMS und die Erstzertifizierung Kosten in Höhe von insgesamt ca. … EUR. Gemäß dem Streitwertbeschluss des Senats in einem Parallelverfahren (Beschluss vom 26.04.2017, VI-3 Kart 105/16) sind entsprechend § 9 ZPO weiterhin die geschätzten Folgekosten für die kommenden 3 ½ Jahre einzubeziehen. Diese hat der Senat ausgehend von den Angaben der Betroffenen, dass ein jährlicher Aufwand von … internen und … externen Personentagen anfällt und die Kosten der Rezertifizierung ca. 1/3 der Zertifizierungskosten von … EUR betragen, auf bis zu weitere … EUR geschätzt.

Der Senat hat die Rechtsbeschwerde zum Bundesgerichtshof zugelassen, weil die streitgegenständliche Frage grundsätzliche Bedeutung im Sinne des § 86 Abs. 2 Nr. 1 EnWG hat und die Sicherung einer einheitlichen Rechtsprechung eine Entscheidung des Bundesgerichtshofs entsprechend § 86 Abs. 2 Nr. 2 EnWG erfordert.

Rechtsmittelbelehrung:

Die Rechtsbeschwerde kann nur darauf gestützt werden, dass die Entscheidung auf einer Verletzung des Rechts beruht (§§ 546, 547 ZPO). Sie ist binnen einer Frist von einem Monat schriftlich bei dem Oberlandesgericht Düsseldorf, Cecilienallee 3, 40474 Düsseldorf, einzulegen. Die Frist beginnt mit der Zustellung dieser Beschwer-

deentscheidung. Die Rechtsbeschwerde ist durch einen bei dem Beschwerdegericht oder Rechtsbeschwerdegericht (Bundesgerichtshof) einzureichenden Schriftsatz binnen eines Monats zu begründen. Die Frist beginnt mit der Einlegung der Beschwerde und kann auf Antrag von dem oder der Vorsitzenden des Rechtsbeschwerdegerichts verlängert werden. Die Begründung der Rechtsbeschwerde muss die Erklärung enthalten, inwieweit die Entscheidung angefochten und ihre Abänderung oder Aufhebung beantragt wird. Rechtsbeschwerdeschrift und -begründung müssen durch einen bei einem deutschen Gericht zugelassenen Rechtsanwalt unterzeichnet sein. Für die Regulierungsbehörde besteht kein Anwaltszwang; sie kann sich im Rechtsbeschwerdeverfahren durch ein Mitglied der Behörde vertreten lassen (§§ 88 Abs. 4 S. 2, 80 S. 2 EnWG).

Laubenstein Klein Reesink Pastohr