Berlin, 18. Januar 2021

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)753

bdew
Energie. Wasser. Leben.

BDEW Bundesverband der Energie- und Wasserwirtschaft e. V.
Reinhardtstraße 32
10117 Berlin

www.bdew.de

Fakten und Argumente

zu einem „Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ (IT-SiG 2.0)

Der Bundesverband der Energie- und Wasserwirtschaft (BDEW), Berlin, und seine Landesorganisationen vertreten über 1.900 Unternehmen. Das Spektrum der Mitglieder reicht von lokalen und kommunalen über regionale bis hin zu überregionalen Unternehmen. Sie repräsentieren rund 90 Prozent des Strom- und gut 60 Prozent des Nah- und Fernwärmeabsatzes, 90 Prozent des Erdgasabsatzes, über 90 Prozent der Energienetze sowie 80 Prozent der Trinkwasser-Förderung und rund ein Drittel der Abwasser-Entsorgung in Deutschland.

Überblick

Der Bundesverband der Energie- und Wasserwirtschaft (BDEW) vertritt über 1900 Unternehmen. Das Spektrum der Mitglieder reicht von lokalen und kommunalen über regionale bis hin zu überregionalen Unternehmen. Sie repräsentieren rund 90 Prozent des Stromabsatzes, gut 60 Prozent des Nah- und Fernwärmeabsatzes, 90 Prozent des Erdgasabsatzes sowie 80 Prozent der Trinkwasser-Förderung und rund ein Drittel der Abwasser-Entsorgung in Deutschland. Außerdem vereint der BDEW 94 Prozent der Stromnetzlänge, 92 Prozent der Gasnetzlänge und 78 Prozent der Wärme- bzw. Kältenetzlänge.

Das Bundeskabinett hat am 16. Dezember 2020 auf Vorlage des Bundesministeriums des Innern, für Bau und Heimat einen Entwurf verabschiedet eines „Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme“, kurz IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0). An den Kabinettsbeschluss schließt sich das parlamentarische Verfahren an.

Grundsätzlich begrüßt der BDEW die Überarbeitung und Weiterentwicklung des Ordnungsrahmens zum Schutz Kritischer Infrastrukturen durch die Bundesregierung. Sichere informationstechnische Systeme sind für die Aufrechterhaltung der Energie- und Wasserver- bzw. -entsorgung von zentraler Bedeutung. Angesichts der dynamischen Entwicklung der Bedrohungen aus dem digitalen Raum stehen wir zu dem Ziel, die Informationssicherheit der Energie- und Wasserversorgung zu erhöhen. Auf Grundlage des vorliegenden Gesetzesentwurfs sind jedoch massive wirtschaftliche Auswirkungen auf die Betreiber Kritischer Infrastrukturen zu erwarten, die dringend adressiert werden sollten, insbesondere die Pflichten zur Einholung einer Garantieerklärung für „kritische Komponenten“, zum Einsatz von Systemen zur Angriffserkennung, die drastische Verschärfung von Bußgeldern und die Gefahr der Doppelregulierung großer Unternehmen.

Einschätzung

Wir begrüßen ausdrücklich, dass Hersteller und Anbieter von IT-Produkten nach § 7a zukünftig einen größeren Beitrag zum Schutz von Kritischen Infrastrukturen leisten sollen. Nur durch eine vertrauensvolle und enge Kooperation zwischen Herstellern und Betreibern kann die IT-Sicherheit von in der Energie- und Wasserwirtschaft eingesetzten Komponenten, Dienstleistungen und Prozessen effizient erhöht und entstehende Sicherheitsrisiken vermindert werden. Insofern stellt diese vorgeschlagene Neuerung einen erheblichen Schritt nach vorne dar.

Es ist jedoch abzusehen, dass erwogene Neuregelungen des Gesetzentwurfs zum Teil erhebliche negative Auswirkungen auf die Betreiber Kritischer Infrastrukturen haben werden. Insbesondere folgende Aspekte gilt es aus Sicht des BDEW dringend zu überdenken:

1. Garantieerklärung nach § 2 Abs. 13 BSIG-E i. V. m. § 9b BSIG-E

In § 2 Abs. 13 soll der Begriff der „kritischen Komponenten“ bestimmt werden. Dieser Begriff und die sich daraus ableitende Gesetzgebung bezieht sich bisher ausschließlich auf den Sektor Telekommunikation. In § 9b wird wiederum die Pflicht zur Einholung einer Garantieerklärung für „kritische Komponenten“ eingeführt. Demnach sollen Betreiber Kritischer Infrastrukturen in Sektoren, in denen eine Zertifizierungspflicht für „kritische Komponenten“ besteht, nur

noch von denjenigen Herstellern IT-Produkte einsetzen dürfen, von denen eine Garantieerklärung über die Vertrauenswürdigkeit ihrer Produkte vorliegt. In der jetzigen Form soll dies bisher ausschließlich den Telekommunikationssektor treffen. Mit der vorgeschlagenen Neuregelung soll allerdings eine gesetzliche Grundlage geschaffen werden, die eine spätere Ausweitung auf weitere Sektoren, wie die Energie- und Wasserwirtschaft ermöglicht.

Die Einführung einer solchen Zertifizierungspflicht in bestehenden Infrastrukturen im energie- und wasserwirtschaftlichen Umfeld ist eine hochsensible Angelegenheit. Die Auswirkungen sind in dem komplexen Einsatzumfeld vielfältig. Beispielsweise könnte eine ausbleibende (Re-)Zertifizierung eines Herstellers dazu führen, dass Komponenten dieses Herstellers von Betreibern Kritischer Infrastrukturen nicht weiterverwendet werden dürfen, also vollständig ausgetauscht werden müssen. Die Kosten hierfür müssten die Betreiber tragen, obwohl ein sicherer Komponenteneinsatz weiterhin möglich wäre. Weiterhin ist von einer Preiserhöhung von kritischen Komponenten auszugehen, da voraussichtlich weniger Anbieter am Markt zur Verfügung stehen werden und diese die Kosten der Zertifizierung auf ihre Kunden umlegen. Unter dem Strich würde eine solche Zertifizierungspflicht von „kritischen Komponenten“ in Verbindung mit der Einholung einer Garantieerklärung einen fragwürdigen Nutzen für die Informationssicherheit der Energie- und Wasserver- und -entsorgung mit sich bringen, da enorme bürokratische Aufwände sowie wirtschaftliche Risiken dem erhofften und vermeintlichen Zugewinn an Vertrauen in die Integrität von IT-Produkten gegenüber stehen.

Die Definition von „kritischen Komponenten“ nach § 2 Absatz 13 kann in der vorliegenden Formulierung deshalb einzig in Telekommunikationsnetzen Anwendung finden. *Die Möglichkeit der Einführung einer Zertifizierungspflicht in weiteren Sektoren sollte dringend aus dem Gesetz gestrichen werden.*

2. Systeme zur Angriffserkennung nach § 8a Abs. 1a BSIG-E und § 11 Abs. 1d EnWG

Mit der Einführung von § 8a Abs 1a sollen Betreiber Kritischer Infrastrukturen verpflichtet werden, sogenannte Systeme zur Angriffserkennung einzuführen und deren Einsatz alle zwei Jahre gegenüber den Aufsichtsbehörden nachzuweisen.

Eine Einführung von Systemen zur Angriffserkennung in prozess- und leittechnischen Einrichtungen ist gegenwärtig nach allgemeinem Stand der Technik kaum bis äußerst aufwändig umsetzbar. Es ist weiterhin nicht wahrscheinlich, dass durch die Einführung der angestrebte Sicherheitszugewinn erreicht wird, da sich derlei Systeme in einem unreifen Entwicklungsstand befinden. Es ist nicht nachvollziehbar, wie z.B. Systeme zur Angriffserkennung eingetretene Störungen beseitigen können, ohne den sicheren Betrieb einer Anlage und damit die Versorgungssicherheit empfindlich zu gefährden. Es muss also festgehalten werden, dass der tatsächliche Nutzen dieser Maßnahme in keinem Verhältnis zum Aufwand ihrer Umsetzung steht. Ebenso sollte von einer Spezifizierung von technischen Maßnahmen in einem abstrakten Gesetz unbedingt Abstand genommen werden.

Von einem verpflichtenden Einsatz von Systemen zur Angriffserkennung im industriellen Umfeld der Energie- und Wasserwirtschaft ist aus diesen Gründen abzusehen. Die Absätze § 8a Abs. 1a BSIG-E und § 11 Abs. 1d EnWG sollten gestrichen werden.

3. Bußgeldvorschriften nach § 14 BSIG-E

Vorsätzliche oder fahrlässige Verstöße gegen Pflichten aus dem BSIG sollen mit Geldbußen von bis zu 2 Mio. €, 1 Mio. € oder 100.000 € geahndet werden, je nachdem, welche Verstöße begangen wurden. Dabei wird auf § 30 Absatz 2 Satz 3 des Gesetzes über Ordnungswidrigkeiten (OWiG) verwiesen. Demzufolge kann das Höchstmaß der Geldbuße verzehnfacht werden. In der Konsequenz kann das maximale Sanktionsmaß also auf 20 Mio. € bei schwerwiegenden Verstößen angehoben werden. Das entspricht einer Erhöhung des heutigen Bußgeld-Höchstmaßes um das bis zu 200-fache.

Ein derart enormes Sanktionsmaß ist weder sach- noch verhältnisgemäß und ist einer guten und vertrauensvollen Zusammenarbeit zwischen Betreibern und dem Bundesamt abträglich. Es ist nicht zielführend und kann gewünschten Investitionen in die Informationssicherheit entgegenwirken, wenn stattdessen für unverhältnismäßige Sanktionsrisiken umfangreiche Rückstellungen gebildet werden müssen. *Der Verweis auf § 30 Absatz 2 Satz 3 OWiG innerhalb der Bußgeldvorschriften sollte daher ersatzlos entfallen.*

4. Gefahr der Doppelregulierung durch § 2 Abs. 14

Der Gesetzentwurf führt in § 2 Abs. 14 den Begriff des „Unternehmen im besonderen öffentlichen Interesse“ ein. Hiermit sind insbesondere große Unternehmen gemeint, die zwar keine Betreiber Kritischer Infrastrukturen im Sinne der BSI-KritisV sind, die aber dennoch von erheblicher Bedeutung sind, weil ihr Ausfall oder ihre Beeinträchtigung erhebliche volkswirtschaftliche Schäden zur Folge hätte. Unternehmen, die bereits als KRITIS-Betreiber erfasst sind, sollen von dieser Regelung zwar ausgenommen sein. Nichtsdestotrotz besteht die Gefahr einer Doppelregulierung von Unternehmen der Energie- und Wasserwirtschaft.

Insbesondere große Unternehmen der Energiewirtschaft zählen ebenfalls zu den größten Unternehmen in Deutschland. Die relevanten Unternehmensteile sind jedoch (zum Teil über Tochtergesellschaften) bereits als Betreiber Kritischer Infrastrukturen erfasst, da diese Unternehmensteile Energieversorgungsnetze und/oder Energieanlagen betreiben. Im Sinne der internationalen Wettbewerbsfähigkeit deutscher der Unternehmen der Energiewirtschaft sollte eine Doppelregulierung als Betreiber Kritischer Infrastruktur und Unternehmen im besonderen öffentlichen Interesse ausgeschlossen werden. *Im Gesetzestext sollte demnach eindeutig ausgeschlossen werden, dass Unternehmen, die Betreiber einer Kritischen Infrastruktur sind, zusätzlich als Unternehmen im öffentlichen Interesse reguliert werden.*

Ansprechpartner

Yassin Bendjebbour
Betriebswirtschaft | Steuern | Digitalisierung
Telefon: +49 30 300199-1529
yassin.bendjebbour@bdew.de

Berlin, 10. Dezember 2020

bdew
Energie. Wasser. Leben.

BDEW Bundesverband der Energie- und Wasserwirtschaft e. V.
Reinhardtstraße 32
10117 Berlin

www.bdew.de

Stellungnahme

zu einem „Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“

im Zuge der Verbändeanhörung auf Basis des „Diskussionsentwurfs“ vom 1. Dezember 2020

Version: 1.0

Inhalt

Vorbemerkungen

Das Bundesministerium des Innern, für Bau und Heimat (BMI) hat am 9. Dezember 2020 mit einem Entwurf eines „Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme“, kurz genannt IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) die Verbändeanhörung eröffnet und bittet um Stellungnahme bis zum 10. Dezember 2020. Aufgrund der Kürze der Zeit nimmt der BDEW mit dem vorliegenden Dokument zu dem „Diskussionsentwurf“ in der Fassung vom 1. Dezember 2020 Stellung.

Wir begrüßen die Überarbeitung und Weiterentwicklung des Ordnungsrahmens zum Schutz Kritischer Infrastrukturen. Die Bedeutung von sicheren informationstechnischen Systemen für die Aufrechterhaltung der Energie- und Wasserver- bzw. -entsorgung ist elementar. Gleichermaßen ist zu beobachten, dass Bedrohungen aus dem digitalen Raum einerseits längst keine Fiktion mehr sind, andererseits stetig in ihrer Qualität und Häufigkeit zunehmen.

Wir stehen daher zu dem Ziel, die Informationssicherheit Kritischer Infrastrukturen weiter zu erhöhen. Mit dem vorliegenden Gesetzentwurf strebt das BMI jedoch eine deutliche Erhöhung der Pflichten von Betreibern Kritischer Infrastrukturen an, die massive wirtschaftliche Auswirkungen auf die betroffenen Unternehmen haben können. Mit der Einführung des IT-SiG wurde gesetzlich verankert, dass die etablierten Cyber- und IT-Sicherheitsmaßnahmen regelmäßig auf ihre Wirksamkeit wissenschaftlich überprüft sowie evidenzbasiert und im Dialog mit den betroffenen Kreisen weiterentwickelt werden. Es ist aus Sicht der Energie- und Wasserwirtschaft nicht nachvollziehbar, dass das BMI – trotz des nunmehr zweijährigen Zeitraums zur Erarbeitung des vorliegenden Entwurfs – nicht seiner gesetzlich verankerten Pflicht zu Evaluierung nachgekommen ist. Stattdessen wirkt das BMI aus Sicht der Energie- und Wasserwirtschaft auf eine überstürzte Verabschiedung des Gesetzentwurfs hin, ohne den betroffenen Kreisen eine angemessene Frist einzuräumen, um sich auf Basis eines offiziellen Entwurfs zu den komplexen Sachverhalten, die innerhalb des Gesetzgebungsverfahrens diskutiert werden, in angemessener Tiefe äußern zu können.

Mit dem UP KRITIS steht eine verlässliche und vertrauensvolle Struktur zur Zusammenarbeit zwischen staatlichen Stellen und der Wirtschaft zur Verfügung, um die Erfahrungen der letzten

Jahre kritisch reflektieren und sinnstiftend weiterentwickeln zu können. Der BDEW steht für die deutsche Energie- und Wasserwirtschaft für einen Dialog und für eine mit dem nötigen Fingerspitzengefühl und Augenmaß fortgeführte Weiterentwicklung jederzeit und gerne bereit.

Mit Blick auf die Inhalte des vorliegenden „Diskussionsentwurfs“ befürworten wir ausdrücklich, dass Hersteller von IT-Produkten und Anbieter digitaler Dienste zukünftig verpflichtet werden sollen, ihren Beitrag zum Schutz von Kritischen Infrastrukturen zu leisten. Das ist ein erheblicher Schritt nach vorne. Denn nur durch eine vertrauensvolle Kooperation zwischen Herstellern und Betreibern kann die Sicherheit von in der Energie- und Wasserwirtschaft eingesetzten Komponenten und Prozessen im Sinne des Regelungsziels effizient erhöht werden.

Zur Gewährleistung eines hohen Niveaus der Informationssicherheit sind die Betreiber Kritischer Infrastrukturen ebenfalls auf die Unterstützung des Bundesamts für Sicherheit in der Informationstechnik (Bundesamt, BSI) angewiesen. Aus diesem Grund sollten die Aufgaben, Zuständigkeiten und Befugnisse des Bundesamts dahingehend gesetzlich verankert werden, den Betreibern die betreffenden Informationen zu Bedrohungen aus dem digitalen Raum bereitzustellen, ohne dass vage formulierte Sicherheitsinteressen dem im Wege stehen. Die Fortführung des bewährten risikobasierten Ansatzes der Informationssicherheit stellt sicher, dass den Unternehmen der Energie- und Wasserwirtschaft für die Umsetzung der gesetzlichen Vorgaben ausreichend Gestaltungsspielräume unter Maßgabe der Wirtschaftlichkeit und Verhältnismäßigkeit eingeräumt werden.

Die im vorliegenden „Diskussionsentwurf“ angedachten Rechte und Pflichten von Betreibern Kritischer Infrastrukturen werden zu erheblichen Aufwänden in den betroffenen Unternehmen führen. Daher fordern wir, den Erfüllungsaufwand der Wirtschaft zur Umsetzung der Vorschriften des ITSiG 2.0 bezüglich der Verpflichtungen zur Meldung, Information sowie Speicherung von Daten zu minimieren. Darüber hinaus ist ein zusätzlicher laufender Erfüllungsaufwand, der durch das Regelungsvorhaben entsteht, mittels geeigneten Entlastungs- oder Refinanzierungsmaßnahmen zu kompensieren.

Des Weiteren weisen wir zu dem Entwurf vom 9. Dezember 2020 ergänzend und nicht abschließend im Folgenden darauf hin:

- Die Bundesregierung plant, diverse Übergangsfristen zur Umsetzung von Vorgaben, wie z.B. der Registrierung neuer Anlagen, zu streichen bei gleichzeitiger Verschärfung von Sanktionsmechanismen, die nicht mehr nur bei fahrlässigem oder vorsätzlichem Handeln verhängt wer-den können. Von diesem Zusammenspiel von gestrichenen Übergangs-fristen und unmittelbaren Sanktionstatbeständen geht ein hohes Risiko von existenzgefährdenden Bußgeldern für betroffene Unternehmen aus, die bereits aufgrund von Bagatell-Verstößen verhängt werden können. Wir fordern die Bundesregierung auf, den Gesetzentwurf im Sinne der Verhältnismäßigkeit von Bußgeldern zu Verstößen zu über-arbeiten.

- Von einer Einführung von Pflichten zur Umsetzung spezifischer technischer Maßnahmen in einem abstrakten Gesetz sollte unbedingt Ab-stand genommen werden. Der Entwurf enthält Anforderungen technischer Art, die mit der Realität der Praxis wenig gemeinsam haben. Die Pflicht zur Umsetzung würde betroffene Kreise vor unklare und zum Teil nicht lösbare Herausforderungen stellen, weitere Gefährdungen mit sich bringen und in Konsequenz zu erheblicher Rechtsunsicherheit führen. Es ist nicht nachvollziehbar, wie z.B. Systeme zur Angriffserkennung eingetretene Störungen beseitigen können. Auch können in-formationstechnische Systeme nicht eigenständig Bedrohungen vermeiden. Sachfremde Anforderungen sollten aus dem Gesetzestext entfernt werden.
- Die unvermittelte Aufnahme des § 10 Absatz 6 erschließt sich uns nicht. Aufgrund der fehlenden Begründung können weder Sinn und Zweck noch die Implikationen für den Betrieb von informationstechnischen Systemen der Betreiber Kritischer Infrastrukturen abgeschätzt werden. Es ist davon auszugehen, dass die Befugnis des Bundesinnen-ministeriums zu einem weitreichenden Eingriff führen würde.

Zu den Forderungen im Kern

Zum „Diskussionsentwurf“ eines IT-Sicherheitsgesetzes 2.0 gibt der BDEW zur beabsichtigten Stärkung der Sicherheit informationstechnischer Systeme zu bedenken, dass:

- von einer Ausweitung der Regelungen des § 9b auf die Sektoren Energie und Wasser dringend abzuraten ist. Die Einführung einer Zertifizierungspflicht von „kritischen Komponenten“ in bestehenden Infrastrukturen im energie- und wasserwirtschaftlichen Umfeld ist eine hochsensible Angelegenheit. Die Auswirkungen sind in dem vorherrschenden, komplexen Einsatzumfeld vielfältig und nur schwer endgültig zu bemessen. Die Definition von „kritischen Komponenten“ nach § 2 Absatz 13 kann in der vorliegenden Formulierung einzig in Telekommunikationsnetzen Anwendung finden. Daher ist die Einführung einer Zertifizierungspflicht für in weiteren Sektoren aus dem Gesetz zu streichen.
- von einem verpflichtenden Einsatz von Systemen zur Angriffserkennung im industriellen Umfeld der Energie- und Wasserwirtschaft abzusehen ist. Eine Umsetzung in prozess- und leittechnischen Einrichtungen ist gegenwärtig nach allgemeinem Stand der Technik nur äußerst aufwändig und höchstwahrscheinlich nicht mit dem angestrebten Sicherheitszugewinn umsetzbar. Die Pflicht zur Speicherung sollte 12 Monate nicht übersteigen. Aufgrund der hohen Aufwände ist eine Umsetzungsfrist von mindestens zwei Jahren unerlässlich.
- in § 14 Bußgeldvorschriften der Verweis auf § 30 Absatz 2 Satz 3 OWiG ersatzlos gestrichen wird. Nur unter Berücksichtigung der vorgeschlagenen Streichung kann die Energie- und Wasserwirtschaft die erhöhten Bußgeldvorschriften über 2 Mio. €, 1 Mio. € bzw. 100.000 € als sachgemäß und verhältnismäßig erachten.
- die Gefahr einer Doppelregulierung als Unternehmen im besonderen öffentlichen Interesse für Unternehmen der Energie- und Wasserwirtschaft besteht, die beispielsweise Energieversorgungsnetze und/oder Energieanlagen (über Tochtergesellschaften) betreiben und zu den größten Unternehmen in Deutschland zählen.
- das Bundesamt gesetzlich dazu verpflichtet werden sollte, erlangte Informationen zu Sicherheitsrisiken zu verarbeiten und betroffene Kreise über alle relevanten Erkenntnisse zu informieren.
- im Falle einer Detektion von Sicherheitsrisiken für die IT-Sicherheit eines Betreibers der betroffene Betreiber ohne Ausnahmen umgehend zu informieren ist. Beim Einsatz von Honeypots muss ausgeschlossen werden, dass Kennungen von informationstechnischen Systemen von Betreibern Kritischer Infrastrukturen durch das Bundesamt genutzt werden. Wir begrüßen, dass weitergehende, invasive Maßnahmen durch das Bundesamt explizit ausgeschlossen werden sollen.
- die Entwicklung und Veröffentlichung von sicherheitstechnischen Anforderungen nach § 3 Absatz 1 Satz 2 Nummer 20 durch das Bundesamt nicht in einen nationalen Alleingang münden darf. Der Stand der Technik sollte möglichst auf Basis international anerkannter Normen und Standards definiert werden, an deren Erarbeitung die betroffenen Sektoren Kritischer Infrastrukturen und deren Wirtschafsverbände hinreichend beteiligt sind.

Zu den Forderungen im Einzelnen

Artikel 1 Änderung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)

Zu § 2 Absatz 13 Definition „kritische Komponente“

Worum geht es?
Es sollen sogenannte „kritische Komponenten“ eingeführt werden. Dies sollen IT-Produkte sein, die von Betreibern von öffentlichen Telekommunikationsnetzen oder Anbietern öffentlich zugänglicher Telekommunikationsdienste eingesetzt werden. Für derartige Betreiber werden „kritische Komponenten“ durch den Katalog für Sicherheitsanforderungen nach § 109 Absatz 6 des Telekommunikationsgesetzes näher bestimmt. Alle übrigen „kritischen Komponenten“ werden gesetzlich festgelegt.

Einschätzung:
Die Einführung einer Definition von „kritischen Komponenten“ dient in Verbindung mit Artikel 1 § 9b BSIG der Verpflichtung von Herstellern besagter Komponenten. In der vorliegenden Fassung liegt jedoch der Schluss nahe, dass die Aufwände im Kontext des Regelungsziels auf Seiten der Anwender solcher Komponenten verortet sein werden, also bei den Betreibern öffentlicher Telekommunikationsnetze oder bei Anbietern öffentlich zugänglicher Telekommunikationsdienste. Es ist gängige Praxis, dass Betreiber Kritischer Infrastrukturen in der Energie- und Wasserwirtschaft die für die Erbringung der kritischen Dienstleistung wesentlichen Komponenten auf Basis des risikobasierten Ansatzes u.a. der IT-Sicherheitskataloge nach § 1a bzw. 1b EnWG eigenständig bestimmen. Im Falle der Einführung einer Zertifizierungspflicht für „kritische Komponenten“ in den Sektoren Energie und Wasser darf nicht daran gerüttelt werden. Die angedachte Definition dient im spezifischen Kontext nur dem Regelungsziel, die Vertrauenswürdigkeit von Herstellern von „kritischen Komponenten“ zu adressieren. Lediglich die jeweiligen Betreiber können die Kritikalität einer Komponente bzw. eines Komponententyps in Abhängigkeit von dem spezifischen Einsatzumfeld bewerten. Die Einführung einer Zertifizierungspflicht im Sektor Energie und Wasser würde eine unverhältnismäßige und wirtschaftlich äußerst aufwändige Bürokratisierung mit zweifelhaftem Wert für die operative IT-Sicherheit darstellen.

BDEW-Petitum:
Wir raten eindringlich von der Einführung einer Zertifizierungspflicht für „kritische Komponenten“ in den Sektoren Energie und Wasser ab. Satz 2 in folgendem Passus sollte daher gestrichen werden:

> *„(13) Kritische Komponenten im Sinne dieses Gesetzes werden für Betreiber nach § 8d Absatz 2 Nummer 1 durch den Katalog von Sicherheitsanforderungen nach § 109 Absatz 6 des Telekommunikationsgesetzes näher bestimmt. ~~Alle übrigen kritischen Komponenten werden gesetzlich festgelegt.~~“*

Zu § 2 Absatz 14 - Definition Unternehmen im besonderen öffentlichen Interesse

Worum geht es?

Das IT-Sicherheitsgesetz soll auf weitere Teile der Wirtschaft ausgeweitet werden. Zu diesem Zweck soll eine neue Kategorie eingeführt werden, die Unternehmen im besonderen öffentlichen Interesse umfasst, die nicht Betreiber Kritischer Infrastrukturen nach Absatz 10 sind. Zu diesen gehören

1) nach Nummer 1 Rüstungshersteller sowie Hersteller von IT-Produkten für die Verarbeitung staatlicher Verschlusssachen,
2) Unternehmen, die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind,
3) sowie Betreiber von Betriebsbereichen der oberen Klasse im Sinne der Zwölften Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes (Störfallverordnung).

Die neue Kategorie der Unternehmen im besonderen öffentlichen Interesse habe zwar eine große Bedeutung in Bezug auf die IT-Sicherheit in Deutschland, jedoch sei diese im direkten Vergleich zu Betreibern Kritischer Infrastrukturen deutlich abgestuft. Sowohl die neu einzuführende Definition für Unternehmen im besonderen öffentlichen Interesse als auch die sich daraus ergebenden Rechtsfolgen für die betroffenen Unternehmen sollen nicht mit denen von Betreibern Kritischer Infrastrukturen vergleichbar sein. Um Unternehmen, die wegen ihrer Eigenschaft als Betreiber einer Kritischen Infrastruktur bereits höheren Schutzanforderungen unterliegen, nicht unnötig zu belasten, soll ein Unternehmen nicht als Unternehmen im besonderen öffentlichen Interesse im Sinne dieses Gesetzes gelten, wenn es Betreiber einer Kritischen Infrastruktur ist (vgl. § 2 Absatz 14).

Einschätzung:

Die Ausweitung des IT-Sicherheitsgesetzes auf weitere Teile der Wirtschaft geht verschärfend über die Vorgaben der EU-Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit hinaus. Es ist jedoch zu begrüßen, dass Betreiber Kritischer Infrastrukturen nicht

zusätzlich als Unternehmen im besonderen öffentlichen Interesse erfasst werden sollen. Aufgrund der uneindeutigen Formulierung, welche Unternehmen aufgrund ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören, kann es dennoch zu einer Doppelregulierung kommen. Insbesondere große Unternehmen der Energiewirtschaft zählen ebenfalls zu den größten Unternehmen in Deutschland, gemessen an ihrer summierten inländischen Wertschöpfung. Die relevanten Unternehmensteile sind jedoch (zum Teil über Tochtergesellschaften) bereits als Betreiber Kritischer Infrastrukturen erfasst, da diese Unternehmensteile Energieversorgungsnetze und/oder Energieanlagen betreiben. Es sollte daher eingehend geprüft werden, ob der Besitz von Unternehmen, die Betreiber einer Kritischen Infrastruktur sind, ein hinreichendes Merkmal für ein Unternehmen im öffentlichen Interesse sein kann.

BDEW-Petitum:

Wir weisen auf die Gefahr einer Doppelregulierung von Unternehmen der Energie- und Wasserwirtschaft hin, die beispielsweise Energieversorgungsnetze und/oder Energieanlagen, zum Teil über Tochtergesellschaften, betreiben lassen und aufgrund ihrer summierten inländischen Wertschöpfung zu den größten Unternehmen in Deutschland nach §§ 44 Absatz 1 GWB (sog. Hauptgutachten) zählen. Der BDEW steht jederzeit zur Verfügung, in der Ausgestaltung der Rechtsverordnung nach § 10 Absatz 5 mitzuwirken und empfiehlt, die Identifizierung von „Unternehmen im öffentlichen Interesse“ ohne eine Vermischung mit Betreibern Kritischer Infrastrukturen vorzunehmen.

Zu § 3 Absatz 1 Satz 2 Nummer 20 - Entwicklung und Veröffentlichung eines Stands der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte

Worum geht es?

Das Bundesamt soll zusätzlich zu bestehenden Aufgaben u.a. sicherheitstechnische Anforderungen an IT-Produkte entwickeln und veröffentlichen können.

Einschätzung:

Betreiber Kritischer Infrastrukturen sind nach § 8a BSIG zur Umsetzung von technischen und organisatorischen Maßnahmen nach dem Stand der Technik verpflichtet. Die Betreiber Kritischer Infrastrukturen sind daher als unmittelbar Betroffene bei der Entwicklung eines Stands der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte unbedingt einzubeziehen, analog zu Beteiligungsmöglichkeiten in der nationalen, europäischen und internationalen Normung.

BDEW-Petitum:

Die sicherheitstechnischen Anforderungen sollten sich auf Vorgaben zu Rahmenbedingungen und informationstechnischen Schutzzielen begrenzen, um betriebswirtschaftlich unverhältnis-

mäßig teuren und ggf. praktisch wenig wirksamen sicherheitstechnischen Anforderungen an IT-Produkte vorzubeugen. Der Stand der Technik sollte auf Basis anerkannter Normen und Standards, an deren Erarbeitung alle betroffenen Kreise beteiligt sind, definiert werden. Es darf keine Abkehr von etablierten Verfahren geben. Zertifizierungen, die nach dem Stand der Technik anderer kompetenter Organisationen für Informationssicherheit erfolgen, sind ebenfalls anzuerkennen.

Ferner sollte sich der Stand der Technik durch marktreife Produkte umsetzen lassen. Eine Norm oder ein Standard, für den es noch kein Produkt gibt, welches sich wirtschaftlich einsetzen lässt, kann nicht umgesetzt werden.

Wir regen an, den Passus zu ergänzen:

> *"20. Entwicklung von Rahmenbedingungen sowie Schutzzielen unter Einbezug der betroffenen Betreiber Kritischer Infrastrukturen und Veröffentlichung eines Stands der Technik bei sicherheitstechnischen Anforderungen an marktverfügbare IT-Produkte unter Berücksichtigung von bestehenden, anerkannten Normen und Standards."*

Zu § 4b - Allgemeine Meldestelle für die Sicherheit in der Informationstechnik

Worum geht es?

Der vorliegende § 4b regelt die Rechte und Pflichten des Bundesamts als allgemeine Meldestelle für die Sicherheit in der Informationstechnik. Die zentrale Sammlung und Auswertung von Informationen zu Sicherheitslücken, Schadprogrammen und IT-Sicherheitsvorfällen zur Einschätzung der IT-Sicherheitslage ist vor diesem Hintergrund eine elementare Aufgabe.

Einschätzung:

Betreiber Kritischer Infrastrukturen sind auf die kurzfristige Bereitstellung von Informationen zu allgemeinen wie auch sektorspezifischen Bedrohungen und Gefährdungslagen – besonders durch staatliche Stellen – angewiesen, um zu jeder Zeit einen sicheren Betrieb ihrer Kritischen Infrastruktur im Sinne des Gesetzgebers gewährleisten zu können. Dementsprechend sollte das Bundesamt gesetzlich dazu verpflichtet werden, erlangte Informationen zu verarbeiten und betroffene Kreise umgehend über relevante Erkenntnisse zu informieren.

BDEW-Petitum:

Wir regen an, den Passus wie folgt zu ändern:

> *(3) Das Bundesamt hat die gemäß Absatz 2 gemeldeten Informationen zu verarbeiten, um: …".*

Zu § 7b - Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden

Worum geht es?

Das Bundesamt kann Maßnahmen zur Detektion und Auswertung von Schadprogrammen, Sicherheitslücken und anderen Sicherheitsrisiken an den Schnittstellen öffentlich erreichbarer informationstechnischer Systeme zu öffentlichen Telekommunikationsnetzen Maßnahmen (Portscans) durchführen, wenn Tatsachen die Annahme rechtfertigen, dass diese ungeschützt im Sinne des Absatzes und dadurch in ihrer Sicherheit oder Funktionsfähigkeit gefährdet sein können.

Ein informationstechnisches System im Sinne des Absatzes 1 ist ungeschützt im Sinne des Absatzes 1, wenn auf diesem öffentlich bekannte Sicherheitslücken bestehen oder wenn auf Grund sonstiger offensichtlich unzureichender Sicherheitsvorkehrungen unbefugt von Dritten auf das System zugegriffen werden kann.

Die Verantwortlichen oder der betreibende Dienstleister des jeweiligen Netzes oder Systems sind zu benachrichtigen, wenn sie bekannt sind oder ihre Identifikation ohne unverhältnismäßige weitere Ermittlungen möglich ist und überwiegende Sicherheitsinteressen nicht entgegenstehen.

Das Bundesamt darf Systeme und Verfahren einsetzen, welche einem Angreifer einen erfolgreichen Angriff vortäuschen, um Schadprogramme und andere Angriffsmethoden zu erheben und auszuwerten. Das Bundesamt darf die hierzu erforderlichen Daten verarbeiten.

Einschätzung:

Die vorgesehene Befugnis des Bundesamts zur Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden ist grundsätzlich zu begrüßen. Die Maßnahmen müssen sich auf die Detektion begrenzen. Die Durchführung von invasiven Maßnahmen ist mit Absatz Satz 2 ausgeschlossen.

Es ist zu beachten, dass eine unautorisierte Detektion und Auswertung von Sicherheitslücken und anderen Sicherheitsrisiken in informationstechnischen Systemen von Betreibern Kritischer Infrastrukturen, einen sicheren Systembetrieb empfindlich stören kann und im Endeffekt die Erbringung einer kritischen Dienstleistung gefährden könnte. Daher ist es ratsam, betroffene Betreiber in die Maßnahmen zur Detektion von Schadprogrammen, Sicherheitslücken und weitere Sicherheitsrisiken rechtzeitig einzubeziehen, u.a. durch eine Vorabinformation und Bereitstellung der genutzten Kennungen des Bundesamts.

BDEW-Petitum:

Sollten dem Bundesamt Sicherheitsrisiken für die Netz- und IT-Sicherheit eines Betreibers einer Kritischen Infrastruktur bekannt werden, ist der betroffene Betreiber umgehend zu informieren. Ein Verweis auf generisch definierte, überwiegende Sicherheitsinteressen darf eine Benachrichtigung nicht verzögern oder verhindern. Es ist zu begrüßen, dass das Bundesamt

den betroffenen Betreibern Hinweise zu Abhilfemöglichkeiten geben soll. In jedem Fall sollte im Vorfeld von geplanten Detektionsmaßnahmen der betroffene Betreiber der Kritischen Infrastruktur durch das Bundesamt über die eingerichtete Kontaktstelle informiert werden inkl. der Bereitstellung der genutzten Kennungen (oder anderer eindeutiger Identifikatoren) des Bundesamtes.

Der geplante Einsatz von Systemen und Verfahren, welche einem Angreifer einen erfolgreichen Angriff vortäuschen (sogenannte „Honeypots“), ist grundsätzlich zu begrüßen. Es muss allerdings ausgeschlossen werden, dass Kennungen und Adressen von informationstechnischen Systemen von Betreibern Kritischer Infrastrukturen durch das Bundesamt zu diesem Zweck genutzt werden.

Demnach regen wir folgende Ergänzung und Konkretisierung des Passus an:

> *„§ 7b Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden*
>
> *[…]*
>
> *(3) Die für das informationstechnische System Verantwortlichen sind vor Maßnahmen gemäß Absatz 1 zu benachrichtigen, sofern diese Betreiber Kritischer Infrastrukturen oder Unternehmen im besonderen öffentlichen Interesse sind. Wird durch Maßnahmen gemäß Absatz 1 eine Sicherheitslücke oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems erkannt ~~und stehen überwiegende Sicherheitsinteressen nicht entgegen~~, sind die für das informationstechnische System Verantwortlichen darüber zu informieren. Das Bundesamt soll dabei auf bestehende Abhilfemöglichkeiten hinweisen. Sind dem Bundesamt die Verantwortlichen nicht bekannt oder ist ihre Identifikation nur mit unverhältnismäßigem Aufwand möglich und stehen überwiegende Sicherheitsinteressen nicht entgegen, ist hilfsweise der betreibende Dienstleister des jeweiligen Netzes oder Systems unverzüglich zu benachrichtigen. Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit jeweils bis zum 30. Juni des Folgejahres über die Anzahl der gemäß Absatz 1 ergriffenen Maßnahmen.*
>
> *(4) Das Bundesamt darf zur Erfüllung seiner Aufgaben Systeme und Verfahren einsetzen, welche einem Angreifer einen erfolgreichen Angriff vortäuschen, um den Einsatz von Schadprogrammen oder andere Angriffsmethoden zu erheben und auszuwerten. Das Bundesamt darf dabei die zur Auswertung der Funktionsweise der Schadprogramme und Angriffsmethoden erforderlichen Daten verarbeiten. Die Verwendung von Kennungen und Adressen von informationstechnischen Systemen von Betreibern Kritischer Infrastrukturen oder Unternehmen im besonderen öffentlichen Interesse durch das Bundesamt ist hiervon explizit ausgenommen, sodass jeglicher Bezug zu einer realexistierenden Infrastruktur unterlassen wird.*

Zu § 8a Absätze 1a und 1b - Systeme zur Angriffserkennung

Worum geht es?

Betreiber sollen im Rahmen technischer und organisatorischer Maßnahmen nach § 8a BSIG zusätzlich Systeme zur Angriffserkennung einsetzen. Betreibern wird dabei eine Übergangsfrist von maximal einem Jahr nach Inkrafttreten des Gesetzes gewährt. Die eingesetzten Systeme müssen geeignete Parameter bzw. Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollen dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

Betreiber Kritischer Infrastrukturen müssen für die Angriffserkennung und -nachverfolgung relevante nicht personenbezogene Daten, die beim Betrieb einer Kritischen Infrastruktur anfallen, mindestens vier Jahre speichern.

Einschätzung:

Der Einsatz von Systemen zur Angriffserkennung ist heute unter Betreibern Kritischer Infrastrukturen im Sinne der BSI-KritisV in der Energie- und Wasserwirtschaft insbesondere in Büronetzwerken weit verbreitet. Die Formulierung im Gesetzestext legt nahe, dass lediglich Systeme zur Angriffserkennung (Intrusion Detection) verpflichtend zum Einsatz kommen sollen. Systeme zur Angriffsbehandlung (Intrusion Prevention) befinden sich allerdings zum gegenwärtigen Zeitpunkt im Umfeld industrieller Prozess -und Automatisierungstechnik noch in einem unreifen Entwicklungsstand. Ihr Einsatz in Produktivnetzwerken würde zu einer Gefährdung der Versorgungsdienstleistung führen. Der Betrieb solcher Systeme erfordert umfassende zeitliche wie wissenstechnische Kapazitäten, da Meldungen zu Angriffen nur durch die manuelle Analyse hinsichtlich ihres Gefährdungspotenzials für die Erbringung einer kritischen Dienstleistung eingeordnet werden können. Nur nach einer solch qualifizierten Einordnung können solche Systeme eine Schutzwirkung im avisierten Einsatzumfeld entfalten.

Die Speicherfrist von für die Angriffserkennung relevanten nicht personenbezogenen Daten, die beim Betrieb einer Kritischen Infrastruktur anfallen, über mindestens vier Jahren würde zu erheblichen Herausforderungen und Aufwänden führen: Nicht personenbezogene Daten müssten von personenbezogenen Daten separiert und für die Archivierung aufbereitet werden. Es ist zu erwarten, dass die anfallenden Datenmengen umfassenden Speicherbedarf erzeugen würden. In der Begründung wird angesichts der Persistenz von spezifischen Angreifenden die Notwendigkeit einer langen Speicherfrist formuliert. Die Erfahrungen aus der Praxis zeigen, dass in derartigen Fällen zwischen den Zeitpunkten einer Infiltration und einem Datenabfluss bzw. Verschlüsselung, z.B. bei Ransomware, meist 140 bis 200 Tage liegen.

Sinnvoll erscheint ergänzend, dass das Bundesamt den Auftrag erhält und befähigt wird, die unterschiedlichen, am internationalen Markt erhältlichen Systeme zur Angriffserkennung zu prüfen und zu bewerten.

BDEW-Petitum:

Von einem verpflichtenden und flächendeckenden Einsatz von Systemen zur Angriffserkennung ist im industriellen Umfeld der Energie- und Wasserwirtschaft abzusehen. Eine Umsetzung in prozess- und leittechnischen Einrichtungen ist gegenwärtig nach allgemeinem Stand der Technik nicht zuverlässig realisierbar, da in diesem Umfeld spezifische Verfahren und spezielle informationstechnische Umgebungen vorherrschen. Die flächendeckende Einführung und der Betrieb derartiger Systeme ist in mehrfacher Weise aufwendig, die reibungslose und effiziente Funktionsweise ist abhängig von einer hohen Implementierungsqualität und ist nur durch umfangreiche Anpassungen der vorliegenden informationstechnischen Infrastrukturen der Unternehmen realisierbar. Der Einbau einer zusätzlichen, unsicheren Komponente in ein informationstechnisches System lässt zusätzlich neue Gefährdungen entstehen. Vor diesem Hintergrund ist aus Sicht der Energie- und Wasserwirtschaft ein Einsatz derartiger Systeme in prozess- und leittechnischen Einrichtungen im Sinne des Gesetzes im Angesicht des erforderlichen Aufwands nicht angemessen, da das Interesse an einem verlässlichen und stabilen Betrieb Kritischer Infrastrukturen den Mehrwert derartiger Systeme überwiegt. Sollte es zur Einführung einer Pflicht zum Einsatz derartiger Systeme kommen, ist angesichts des damit verbundenen hohen Aufwands eine Umsetzungsfrist von mindestens zwei Jahren notwendig.

Die Speicherfrist sollte im Kontext der Erfahrungen aus der Praxis auf maximal 12 Monate begrenzt werden, analog zur Pflicht des Bundesamts zur Verarbeitung und Speicherung von behördeninternen Protokollierungsdaten nach § 5a Absatz 2. Ein Angriffsversuch sollte nicht verpflichtend protokolliert werden müssen, da die Definition des Angriffsversuchs nicht klar ist und somit zu einem hohen Mehraufwand ohne konkreten Zusatznutzen führen wird.

Wir regen an, den Passus wie folgt umzuformulieren:

> *„(1a) Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst spätestens zwei Jahre nach Inkrafttreten dieses Gesetzes auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter bzw. Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen. Absatz 1 Satz 2 und 3 gelten entsprechend. Ein flächendeckender Einsatz von Systemen zur Angriffserkennung im Umfeld von informationstechnischen Systemen, die für die Erbringung einer kritischen Dienstleistung wesentlich sind, ist hiervon ausgenommen.*

Das Bundesamt prüft und bewertet die am Markt verfügbaren Systeme zur Angriffserkennung regelmäßig und spricht auf Anfrage Empfehlungen aus.

(1b) Betreiber Kritischer Infrastrukturen müssen für die Angriffserkennung und -nachverfolgung relevante nicht personenbezogene Daten, die beim Betrieb einer Kritischen Infrastruktur anfallen, maximal 12 Monate speichern."

Zu § 8b Absatz 4a - Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen

Worum geht es?

Während einer erheblichen Störung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse von Betreibern Kritischer Infrastrukturen, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können oder von Unternehmen im besonderen öffentlichen Interesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Erbringung der Wertschöpfung führen können bzw. die zu einem Störfall nach der Störfall-Verordnung in der jeweils geltenden Fassung führen können, kann das Bundesamt im Einvernehmen mit der jeweils zuständigen Aufsichtsbehörde des Bundes von den betroffenen Betreibern bzw. Unternehmen die Herausgabe der zur Bewältigung der Störung notwendigen Informationen, einschließlich personenbezogener Daten, verlangen.

Einschätzung:

In einem anhaltenden oder sich ausweitenden Störungsausfall ist der Wunsch der Aufsichtsbehörde nach umfangreichen Informationen verständlich. Dennoch möchten wir darauf hinweisen, dass bereits für eine lediglich rudimentäre Einordnung der eingeforderten Informationen durch unbeteiligte Externe ein erhebliches Wissen über die Spezifika des jeweiligen Umfelds betroffener informationstechnischer Systeme notwendig ist. Es scheint uns daher unwirksam, dem Bundesamt alle zur Bewältigung einer Störung notwendigen Informationen aushändigen zu müssen, inklusive sämtlicher dazu notwendigen Benutzerkennungen, Passwörter und dazugehöriger Betriebsdokumentationen.

Störungen sind für Betreiber Kritischer Infrastrukturen schon heute meldepflichtig. Uns sind gegenwärtig keine Beispiele seit Einführung der Meldepflicht bekannt, in denen eine solche Übermittlung, wie die hier geplante, eine Störungsbehebung beschleunigt hätte. Vielmehr erscheint es uns angebracht, die Kooperation zwischen Betreibern und dem Bundesamt weiter vertrauensvoll zu vertiefen.

BDEW-Petitum:

Wir regen an, den Passus zu streichen. Ergänzend könnten die Vorgaben zur Meldepflicht anforderungsgerecht und im Dialog mit den Betreibern präzisiert werden.

~~*„(4a) Während einer erheblichen Störung gemäß Absatz 4 Satz 1 Nummer 2, § 8f Absatz 7 Nummer 2 oder § 8f Absatz 8 Nummer 2 kann das Bundesamt im Einvernehmen mit der jeweils zuständigen Aufsichtsbehörde des Bundes von den betroffenen Betreibern Kritischer Infrastrukturen oder Unternehmen im besonderen öffentlichen Interesse die Herausgabe der zur Bewältigung der Störung not-wendigen Informationen einschließlich personenbezogener Daten verlangen.“*~~

Zu § 9b - Untersagung des Einsatzes kritischer Komponenten nicht vertrauenswürdiger Hersteller

Worum geht es?

Geplant ist die Einführung einer Garantieerklärung über die Vertrauenswürdigkeit von Herstellern von „kritischen Komponenten“ nach § 2 Absatz 13, in Sektoren, in denen eine gesetzliche Zertifizierungspflicht für „kritische Komponenten“ im Sinne dieses Gesetzes besteht. Gemäß Artikel 2 Änderung des Telekommunikationsgesetzes § 109 (2) Satz 4 soll dies zum gegenwärtigen Zeitpunkt ausschließlich für den Sektor Telekommunikation gelten. Für weitere Sektoren der Kritischen Infrastrukturen besteht derzeit keine gesetzliche Zertifizierungspflicht für „kritische Komponenten“. Der Einsatz von „kritischen Komponenten“, für die eine Zertifizierungspflicht besteht, soll durch den Betreiber einer Kritischen Infrastruktur gegenüber dem Bundesinnenministerium vor Einsatz angezeigt werden. Die Mindestanforderungen an eine Garantieerklärung sollen durch Allgemeinverfügung durch das Bundesinnenministerium festgelegt werden. Das Bundesinnenministerium kann den Einsatz einer Komponente, weiterer Komponenten eines spezifischen Typs sowie alle Komponenten eines Herstellers im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie und dem Auswärtigen Amt untersagen.

Einschätzung:

Die Energie- und Wasserwirtschaft begrüßt, dass im Zuge des Gesetzgebungsverfahrens Hersteller von IT-Produkten und „kritischen Komponenten“ hinsichtlich der Schutzziele Kritischer Infrastrukturen stärker in die Pflicht genommen werden sollen. Neben den Pflichten zur Kooperation zur Beseitigung von Schwachstellen, Störungen und Sicherheitsrisiken nach §§ 7a, 7c, 7d sowie 8b der von ihnen hergestellten IT-Produkte stellt der vorliegende § 9b eine erhebliche Verschärfung dar.

Die vorliegende Formulierung des Passus in Verbindung mit Artikel 2 Änderung des Telekommunikationsgesetzes § 109 Absatz 2 Satz 4 legt den Schluss nahe, dass der Anwendungsbereich ausschließlich auf Basis gesetzlicher Regelungen eine Zertifizierungspflicht im Telekommunikationssektor herbeiführen will. Die Einführung einer Garantieerklärung für „kritische Komponenten“ in weiteren Sektoren hätte in der vorgeschlagenen Form zusätzliche Aufwände auf Betreiberseite zur Folge: Von der Einholung einer Garantieerklärung für „kritische Komponenten“ über deren Administration bis zu den potenziellen wirtschaftlichen Folgeschäden

durch die Untersagung eines Komponenteneinsatzes müssten Betreiber die Auswirkungen tragen. Dazu würden der Aufwand und die Kosten für ggf. nötige Neuinstallationen zählen, die insbesondere bei Bestandsanlagen und anstehenden Teilprojekten eine große Unsicherheit nach sich ziehen würden.

Bezüglich einer möglichen Ausweitung auf weitere Sektoren der Kritischen Infrastrukturen neben dem Telekommunikationssektor weisen die Unternehmen der Energie- und Wasserwirtschaft darauf hin, dass bei der Vielzahl der heute von ihnen eingesetzten Komponenten staatliche Sicherheitsinteressen bzw. sicherheitspolitische Belange weder im Planungs- noch Herstellungszyklus, geschweige denn im Betriebs- und Entsorgungszyklus, berücksichtigt werden. Sollte eine solche Berücksichtigung aufgrund einer geänderten gesetzlichen Anforderung verpflichtend werden, sind nicht nur gewaltige Auswirkungen auf die Hersteller- und Lieferantenstruktur, sondern auch auf unternehmensinterne, kritische Geschäftsprozesse aller Betroffenen in der Energie- und Wasserwirtschaft zu erwarten. Zweckmäßige Investitionen, die auch zur Verbesserung der Informationssicherheit (z.B. Modernisierung von Teilen eines Leitsystems) führen würden, müssten vor diesem Hintergrund erneut und umfassend auf den Prüfstand gestellt und schlimmstenfalls abgesetzt werden. Die Investitionssicherheit wäre nicht gegeben aufgrund einer plötzlichen, außerhalb des Einflussbereichs eines Betreibers eintretenden ordnungsbehördlichen Untersagung. Daher müssen bereits im Einsatz befindliche Komponenten von der Neuregelung ausgenommen werden.

Die Einführung einer Zertifizierungspflicht von „kritischen Komponenten“ in bestehenden IT-Infrastrukturen im energie- und wasserwirtschaftlichen Umfeld ist eine hochsensible Angelegenheit. Die Auswirkungen sind in dem vorherrschenden, komplexen Einsatzumfeld vielfältig und nur schwer endgültig zu bemessen. Folgende Dynamiken sind dabei u.a. zu betrachten:

Der Markt für Hersteller und Lösungsanbieter von „kritischen Komponenten“, die in der Energie- und Wasserwirtschaft zum Einsatz kommen, ist überschaubar. Eine Zertifizierungspflicht hätte aller Voraussicht zur Folge, dass der Markt in seiner aktuell oligopolistischen Prägung zu einem Monopol werden könnte, d.h. auf wenige Hersteller weltweit eingeschränkt wäre. Vor dem Hintergrund der Bestrebungen um technologische Souveränität in der Europäischen Union muss aus Sicht des BDEW anhand der politischen und regulatorischen Rahmenbedingungen sichergestellt werden, dass jederzeit eine ausreichende Anzahl an vertrauenswürdigen europäischen Herstellern von „kritischen Komponenten“ garantiert ist, die eine gesetzeskonforme und vor allem belastbare Garantieerklärung ausstellen können. Eine Zertifizierungspflicht darf unter keinen Umständen in eine Abhängigkeit von Herstellern aus Nicht-EU-Staaten münden. Zudem ist davon auszugehen, dass eine Zertifizierungspflicht steigende Preise für „kritische Komponenten“ zur Folge haben würde, was wiederum eine nicht unerhebliche Wirkung auf die Marktpreise für die Versorgung mit Energie und Trinkwasser sowie für die Entsorgung von Abwasser entfalten würde.

Die Energie- und Wasserwirtschaft gibt darüber hinaus zu bedenken, dass eine alleinige Zertifizierungspflicht von einzelnen Komponenten nicht das Schutzniveau einer Anlage als Ganzes steigert. Nur durch das Zusammenspiel aller Komponenten, Anlagenteile und Ressourcen (Per-

sonal, Infrastrukturen, Prozesse, Verfahren und deren regelmäßige Pflege und Ineinanderwirken) kann ein hohes Schutzniveau erreicht werden. Der bestehende, risikobasierte Regulierungsansatz der IT-Sicherheitskataloge und branchenspezifischen Sicherheitsstandards (B3S) erfüllt diesen Anspruch.

BDEW-Petitum:

Von einer Ausweitung der Regelungen des § 9b auf die Sektoren Energie und Wasser ist dringend abzuraten. Die Aufwände für eine Einholung von Garantieerklärungen und deren potenziellen Ersatz in Folge einer Untersagung des Einsatzes sind erheblich und zum gegenwärtigen Zeitpunkt in den zu erwartenden mittel- und langfristigen Implikationen nur schwer abzuschätzen.

Der Passus sollte demzufolge dahingehend geändert werden, dass nicht Betreiber eine Garantieerklärung einholen und vorweisen müssen, sondern dass die Umsetzung dieser Vorgabe auf Seiten der hierfür originär verantwortlichen Hersteller verortet wird. So könnte beispielsweise das Bundesamt ein Register aller kritischen Komponenten und deren Hersteller führen, deren Einsatz eine Garantieerklärung nach § 9b für „kritische Komponenten“ nach § 2 Absatz 13 erfordern. Sollte eine Komponente in diesem Bundesamt-Register geführt werden, muss ein Hersteller gegenüber Betreibern einer Kritischen Infrastruktur ohne weitere Aufforderung, d.h. bei Auslieferung einer Komponente, eine Garantieerklärung ausstellen. Das Bundesamt sollte parallel die Möglichkeit erhalten, die Garantieerklärung auf deren Validität zu prüfen. Nach Ablauf der Frist von einem Monat gilt eine positive Bescheinigung der Garantieerklärung als erteilt. Der Betreiber zeigt daraufhin den Einsatz einer solchen Komponente gegenüber dem Bundesamt an und reicht die dazugehörige Garantieerklärung ein. Nach Ablauf der Frist von einem Monat gilt eine positive Bescheinigung der Garantieerklärung als erteilt.

Ferner regen wir an, die in Absatz 4 geregelte Untersagung des weiteren Betriebs einer „kritischen Komponente“ mittels einer verhältnismäßigen Frist zu konkretisieren. Bereits im Einsatz befindliche Komponenten müssen aufgrund der langen Lebensdauer Bestandsschutz erhalten. Im Falle einer Untersagung sind ausreichende Übergangsfristen für den Weiterbetrieb verbauter Komponenten vorzusehen, deren Länge den Einsatz von kompensierenden Sicherheitsmaßnahmen würdigt. Sollten qualifizierte Komponenten für einen Austausch nicht verfügbar sein, dann müssen ersatzweise Standardkomponenten über eine Betriebsbewährung und kompensierende Sicherheitsmaßnahmen qualifiziert werden können. Hier könnten die Erfahrungen aus der Regulierung kerntechnischer Anlagen herangezogen werden.

Zu § 14 - Bußgeldvorschriften

Worum geht es?
Vorsätzliche oder fahrlässige Verstöße gegen Pflichten aus dem BSIG sollen mit Geldbußen von bis zu 2 Mio. €, 1 Mio. € oder 100.000 € geahndet werden, je nachdem, welche Verstöße begangen wurden. Es wird auf § 30 Absatz 2 Satz 3 des Gesetzes über Ordnungswidrigkeiten (OWiG) verwiesen. Demzufolge kann das Höchstmaß der Geldbuße verzehnfacht werden. In der Konsequenz kann das maximale Sanktionsmaß auf 20 Mio. € bei schwerwiegenden Verstößen angehoben werden. Eine zuvor angedachte Verknüpfung mit weltweiten Jahresumsätzen eines Unternehmens wird nicht mehr vorgeschlagen.

Einschätzung:
Es ist begrüßenswert, dass sich das Strafmaß an einem europäischen Bußgeldrahmen orientiert. Die Energie- und Wasserwirtschaft ist sich ihrer Bedeutung für das Funktionieren des Gemeinwesens bewusst. Allerdings ist der Spagat aus ökonomischer und finanzieller Effizienzsteigerung bereits heute äußerst herausfordernd durch beispielsweise netzwirtschaftliche Anreizregulierung und den energiewirtschaftlichen Wettbewerb sowie die Übernahme staatlicher Aufgaben der Daseinsvorsorge durch privatwirtschaftliche Unternehmen.

Durch den Verweis auf § 30 Absatz 2 Satz 3 OWiG soll in letzter Konsequenz der Bußgeldrahmen in den Fällen des Absatzes 1 Nummer 1 Buchstabe a, Nummern 2, 9, 13, 14, 16, 17 und 18 enorm um das bis zu 200-Fache des derzeitigen Höchstmaßes erhöht werden. Diese Überlegung trägt den Bemühungen der Betreiber Kritischer Infrastrukturen in der Energie- und Wasserwirtschaft nicht Rechnung, die Informationssicherheit von Kritischen Infrastrukturen kontinuierlich zu stärken. Ein derart enormes Sanktionsmaß ist einer guten und vertrauensvollen Zusammenarbeit zwischen Betreibern und dem Bundesamt tendenziell abträglich, wodurch das in den letzten Jahren erarbeitete Vertrauensverhältnis nachhaltig gefährdet werden wird. Es ist anzuzweifeln, ob gewünschte Investitionen in die Informationssicherheit gefördert werden, wenn stattdessen für unverhältnismäßige Sanktionsrisiken umfangreiche Rückstellungen gebildet werden müssen.

Das Sanktionsmaß ist beispielsweise für Verstöße gegen die Vorgaben zur Speicherung von für die Angriffserkennung relevanten nicht personenbezogenen Daten, die beim Betrieb einer Kritischen Infrastruktur anfallen, nach § 8a Absatz 1b mit bis zu 20 Mio. € absolut unverhältnismäßig. Ein reiner Verstoß gegen die Vorgabe zur Speicherung ist bereits durch das heutige Strafmaß von maximal 100.000 € hinreichend bemessen.

BDEW-Petitum:
Der BDEW regt vor dem Hintergrund der im Grundgesetz angelegten Notwendigkeit der Einhaltung von Verhältnismäßigkeit bei staatlichen Maßnahmen an, den vorliegenden Passus wie folgt anzupassen:

> *(2) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 1 Buchstabe a, Nummern 2, 9, 13, 14, 16, 17 und 18 mit einer Geldbuße bis zu 2 Millionen Euro geahndet werden~~, auf § 30 Absatz 2 Satz 3 des Gesetzes über Ordnungswidrigkeiten wird verwiesen~~. Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 1 Buchstabe*

b und Nummern 3, 5, 8, 10, 11, 12 und 15 mit einer Geldbuße bis zu 1 Million Euro geahndet werden. In den übrigen Fällen kann die Ordnungswidrigkeit mit einer Geldbuße bis zu 100.000 Euro geahndet werden.

Nur unter Berücksichtigung der vorgeschlagenen Streichung kann die Energie- und Wasserwirtschaft die Bußgeldvorschriften als sachgemäß und verhältnismäßig erachten.

Artikel 4 Änderung des Gesetzes über die Elektrizitäts- und Gasversorgung (EnWG)

Zu § 11 Absätze 1d, 1e und 1f EnWG

Worum geht es?

Durch die erwogene Änderung wird die in § 8a Absatz 1a BSIG neu einzuführende Pflicht für Betreiber Kritischer Infrastrukturen, Systeme zur Angriffserkennung einzusetzen, auch analog für Betreiber von Energieversorgungsnetzen und solchen Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 BSIG als Kritische Infrastruktur bestimmt wurden, eingeführt.

Einschätzung:

Es wird auf die Einschätzung zu § 8a Absätze 1a und 1b verwiesen.

BDEW-Petitum:

Es wird auf das BDEW-Petitum zu § 8a Absätze 1a und 1b verwiesen.

Ansprechpartner

Yassin Bendjebbour
Betriebswirtschaft | Steuern | Digitalisierung
Telefon: +49 30 300199-1529
yassin.bendjebbour@bdew.de

Dr. Michaela Schmitz
Wasser und Abwasser
Telefon: +49 30 300199-1200
michaela.schmitz@bdew.de