bdew

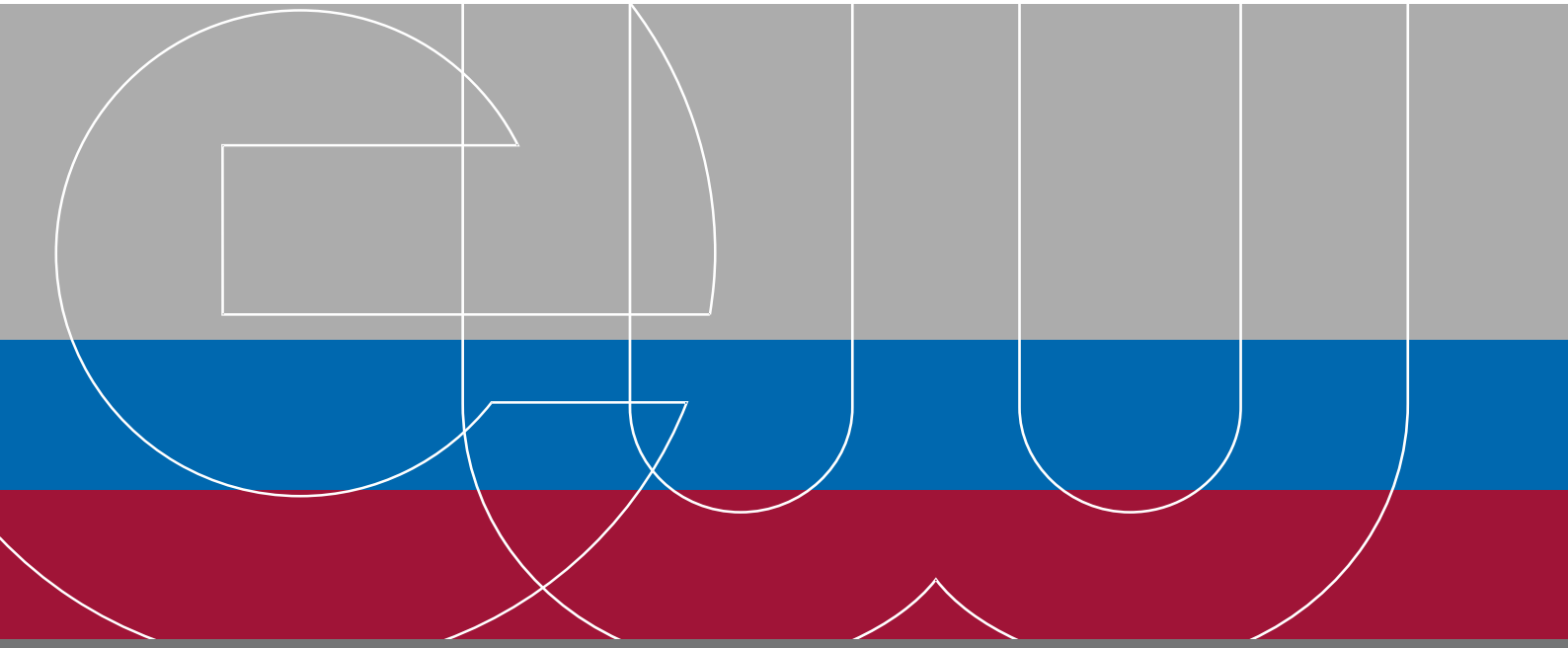
Energie. Wasser. Leben.

BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.
Reinhardtstraße 32
10117 Berlin
Telefon +49 30 300 199-0
Telefax +49 30 300 199-3900
E-Mail info@bdew.de
www.bdew.de

Stellungnahme

zum Referentenentwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme vom 27. März 2019

Berlin, 02. September 2019



Inhalt

Vorbemerkungen

Der Bundesverband der Energie- und Wasserwirtschaft (BDEW), Berlin, 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.

Die vorliegenden Anmerkungen des BDEW beziehen sich auf den vom Bundesministerium des Innern, für Bau und Heimat (BMI) erstellten, vorläufigen Referentenentwurf eines „Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme“, kurz genannt IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0), vom 27. März 2019 sowie auf die schriftlichen Ergänzungen des BMI im Rahmen der Sitzung des UP KRITIS Plenums vom 4. und 5. Juni 2019. Folgende grundlegende Überlegungen zur Erhöhung der Sicherheit informationstechnischer Systeme stellen wir unseren Kernforderungen voran:

Wir begrüßen die Überarbeitung und Weiterentwicklung des IT-SiG. Wir stehen zu dem Ziel, die Informationssicherheit Kritischer Infrastrukturen weiter zu erhöhen.

Wir befürworten, dass Hersteller und Lösungsanbieter von Produkten und Dienstleistungen zukünftig verstärkt einen Beitrag zu den Schutzzielen Kritischer Infrastrukturen leisten sollen.

Wir fordern, den Unternehmen für die Umsetzung und Branchendurchdringung des IT-SiG 2.0 Unterstützung seitens des Bundesamts für Sicherheit in der Informationstechnik (BSI) sowie Gestaltungsspielräume unter Maßgabe der Wirtschaftlichkeit einzuräumen.

Wir fordern, Erfüllungskosten zur Umsetzung der Vorschriften des IT-SiG 2.0 hinsichtlich zahlreicher Melde- und Informationsverpflichtungen der Wirtschaft zu minimieren.

Wir empfehlen, eindeutige und erreichbare Ziele im Rahmen der Ausgestaltung der Regelungen in den Vordergrund zu stellen. Zahlreiche ungenaue Formulierungen, sprachliche Inkonsistenzen sowie die Einführung von Doppelregulierungen innerhalb des Referentenentwurfs würden unmittelbar erhebliche Rechtsunsicherheit auf Seiten der Unternehmen der Energie- und Wasserwirtschaft verursachen.

Kernforderungen

Zum Entwurf eines IT-Sicherheitsgesetzes 2.0 fordert der BDEW zur Gewährleistung der Sicherheit informationstechnischer Systeme, dass:

- **der Terminus „KRITIS-Kernkomponenten“ gestrichen oder zumindest angeglichen wird unter Berücksichtigung bestehender Definitionen innerhalb des EnWG und daraus ableitenden Regulierungen sowie innerhalb der TrinkwV;**
- **ein Bestandsschutz für bereits verbaute Komponenten und Systeme in der Entwicklung von Anforderungen an Identifizierungs- und Authentisierungsverfahren festgeschrieben wird;**
- **die „Vertrauenswürdigkeitserklärung“ gestrichen und durch eine „*verpflichtende Herstellererklärung*“ über die Vertrauenswürdigkeit von Komponenten gegenüber dem Betreiber Kritischer Infrastruktur ersetzt wird. Die „verpflichtende Herstellererklärung“ muss vor dem *erstmaligen* Einsatz und jederzeit auf Anfrage von Herstellern an Betreiber Kritischer Infrastrukturen ausgestellt werden. Bereits verbaute Komponenten und Bauteile, Ersatzteile und im Rahmen des Produktlebenszyklusses zur Instandhaltung, Erneuerung, Erweiterung und zum Austausch erforderliche Komponenten und Bauteile sollten zwingend Bestandsschutz erhalten. Betreiber Kritischer Infrastrukturen als Anwender von Komponenten und Bauteilen sollten mit einbezogen werden bei der Erarbeitung von Mindestanforderungen. Eine einheitliche Übergangsfrist von mindestens 2 Jahren sollte zwingend gewährleistet werden;**
- **das Kriterium „Cyberkritikalität“ ersatzlos gestrichen wird;**
- **eine Einführung eines freiwilligen IT-Sicherheitskennzeichens ausschließlich auf Antrag der Hersteller von Produkten basiert. Eine Verpflichtung zur Nutzung von Produkten mit IT-Sicherheitskennzeichen durch Betreiber Kritischer Infrastrukturen wird abgelehnt. Der Passus ist demnach zu konkretisieren und ein nationaler Alleingang im Kontext der europäischen Bemühungen zu hinterfragen;**
- **die vorliegenden Bußgeldvorschriften gestrichen und unter Maßgabe der Verhältnismäßigkeit umfassend überarbeitet werden. Eine Einführung von sektorspezifischen Bußgeldvorschriften würde die variierende Wirtschaftskraft der Unternehmen aus den unterschiedlichen KRITIS-Sektoren ebenso im Kontext der NIS-Richtlinie berücksichtigen;**
- die Definition „IT-Produkte“ hinsichtlich ihrer bestimmungsgemäßen Funktion konkretisiert wird;
- die Nomenklatur des Sektors „Entsorgung“ terminologisch eindeutig von der „Abwasserentsorgung/-beseitigung“ unterschieden und als „Abfallentsorgung“ beschrieben wird;
- der Terminus „Infrastruktur im besonderen öffentlichen Interesse“ konkretisiert und mit den Worten „und mit erheblichem volkswirtschaftlichem Schaden im Falle einer potenziellen Schädigung“ ergänzt wird;

- die neuen Aufgaben des BSI als Konformitätsbewertungsstelle hinsichtlich der Zertifizierungsanforderungen und der organisatorischen Zielsetzung präzisiert werden;
- gleichermaßen Pflichten zur Informationsweitergabe an Betreiber Kritischer Infrastrukturen und die Öffentlichkeit aus den Rechten des BSI als Meldestelle für die Sicherheit in der Informationstechnik erwachsen;
- die Vorgaben zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen um klare Regeln und Bewertungsverfahren ergänzt und mit Notstandsgesetzen und anderen Regelungen für nationale Krisenlagen harmonisiert werden. Des Weiteren sollte verständlich formuliert werden, von wem Krisenreaktionspläne vorgelegt werden sollten. Einer Übernahme der Erfüllungskosten auf Seiten der Wirtschaft sollte unmittelbar im Gesetzestext Rechnung getragen werden;
- die Detektion von Sicherheitsrisiken für Netz- und IT-Sicherheit und von Angriffsmethoden zu begrenzen und Haftungsfragen in diesem Kontext zu klären sind. Die Informationsweitergabe von Sicherheitsrisiken innerhalb von Netzwerken von Betreibern Kritischer Infrastrukturen sollte eingegrenzt werden. Eine vorherige Information und die Zustimmung der Betreiber zur Detektion von Risiken in deren Netzwerken durch Dritte - wie dem BSI - ist zwingend erforderlich.
- vorgesehene Vorgaben über eine vierteljährliche Berichterstattung über Verfahren und Umstände von Maßnahmen des Einsatzes von Systemen zur Angriffserkennung zu überarbeiten sind. Die schriftliche Berichterstattung sollte einmal jährlich erfolgen.
- eine Auskunftsverpflichtung des BSI im Sinne der Transparenz behördlicher Vorgänge mit normativer Nomenklatur verpflichtend sichergestellt sein sollte;
- das BSI keine Vorschriften über Systeme zur Angriffserkennung unter Maßgabe einer technologieoffenen Regulierung macht. Das BSI sollte jedoch befähigt werden, die unterschiedlichen, am Markt erhältlichen Systeme zur Angriffserkennung bewerten und empfehlen zu können;
- die Pflicht für Provider öffentlich zugänglicher Telekommunikationsdienste zur Meldung rechtswidrig erlangter Daten durch Dritte konkretisiert wird.
- eine Klarstellung erfolgt, dass ein potentielles LTE-450-MHz-Funknetz, welches die Energiewirtschaft zur Netzsteuerung, Sprachkommunikation und Verwaltung von Smart Metern und Smart-Meter-Gateways einsetzt, nicht von der Neuregelung des § 8b Abs. 2 Satz 1 BSIG-E erfasst wird, nach der das BSI die Anspruchsberechtigungen für den Zugang von Betreibern Kritischer Infrastrukturen zu einem einheitlichen Krisenkommunikationssystem regelt.

Zu den Forderungen im Einzelnen

Zu Artikel 1, § 2 Absatz 9a: Definition „IT-Produkte“

Worum geht es?
Die Definition von IT-Produkten soll neben Softwareprodukten und Hardwareprodukten die „einwandfreie Funktion [der] eingesetzten Software“ umfassen.

Einschätzung:
Ob eine Gerätefunktion einwandfrei ist, hängt in der Regel vom konkreten Einsatz (bzw. dem gewünschten Ziel) des Benutzers ab. Hersteller gehen jedoch von einem bestimmungsgemäßen Einsatz aus. Nur für diesen können belastbare Aussagen bezüglich der Sicherheit getroffen werden. Firmwaremodifikationen mögen vielleicht die einwandfreie Um-/Funktionsfähigkeit – aus Sicht des Verbrauchers – gewährleisten, können jedoch die Sicherheitsziele des Herstellers empfindlich verletzen.

BDEW-Petitum:
Wir regen an, die Formulierung folgendermaßen zu konkretisieren: „[…] inklusive der zur einwandfreien *und bestimmungsgemäßen* Funktion eingesetzten Software.“.

Zu Artikel 1, § 2 Absatz 10 Satz 1 Nummer 1: Einbezug des Sektors „Entsorgung“

Worum geht es?
Kritische Infrastrukturen sollen um den Sektor „Entsorgung“ erweitert werden.

Einschätzung:
Dieser geplanten Ausweitung auf den Sektor „Entsorgung“ fehlt die notwendige, begleitende Anpassung der Schwellenwerte in der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV). Bei der Festlegung von Sektoren als Kritische Infrastrukturen sollte aus Gründen der Akzeptanz und Nachvollziehbarkeit stets die Transparenz der Entscheidungsprozesse gewahrt werden.

BDEW-Petitum:
Der Passus sollte gestrichen und der Sektor „Entsorgung“ im Rahmen der anstehenden Aktualisierung der BSI-KritisV aufgenommen werden unter Berücksichtigung der gängigen Verfahrensweise zur Definition von Kritischen Infrastrukturen. Unabhängig davon sollte die Nomenklatur des Sektors „Entsorgung“ terminologisch eindeutig von der „Abwasserentsorgung/-beseitigung“ unterschieden und als „Abfallentsorgung“ beschrieben werden. Eine trennscharfe Verwendung des Begriffs „Entsorgung“ ist notwendig, um Missverständnisse zu vermeiden.

Zu Artikel 1, § 2 Absatz 13 Nummer 1 und 2: Kernkomponenten für Kritische Infrastrukturen (KRITIS-Kernkomponenten)

Worum geht es?
Die für den Betrieb von Kritischen Infrastrukturen eingesetzten, entwickelten oder geänderten IT-Produkte sollen als sogenannte KRITIS-Kernkomponenten über die Sektoren Energie, Wasser, IKT, Ernährung, Gesundheit, Finanz- und Versicherungswesen, Transport, Verkehr und Entsorgung spezifiziert werden.

Einschätzung:
Der Terminus „KRITIS-Kernkomponenten“ ist unspezifisch und missverständlich. Angesichts der bestehenden Regelungen im Energiewirtschaftsgesetz (EnWG) und in der Trinkwasserverordnung (TrinkwV) stellt er eine Doppelregulierung dar. Der Passus wird aufgrund der fehlenden Eindeutigkeit unmittelbar Fehlinterpretationen verursachen. Redundante und missverständliche gesetzliche Vorgaben sind zu vermeiden, da sonst die Widerspruchsfreiheit gesetzlicher Vorgaben gefährdet wird.

Die Spezifizierung von „allen zentralen und dezentralen Anwendungen, Systemen und Komponenten, die für einen sicheren Betrieb“ einerseits von Anlagen oder Systemen zur Stromversorgung, Gasversorgung, Kraftstoff- oder Heizölversorgung oder Fernwärmeversorgung sowie andererseits von Anlagen zur Trinkwasserversorgung oder Abwasserbeseitigung nötig sind, ist bereits hinreichend geregelt über die BSI-KritisV, das EnWG und die für den Sektor Energie relevanten IT-Sicherheitskataloge nach § 11 Absätze 1a und 1b EnWG sowie die für den Sektor Wasser relevante TrinkwV. Diese Branchenregelungen bieten eine konkretere Definition der im Einsatz befindlichen Komponententypen.

Ein risikobasierter Ansatz, beispielsweise gemäß IT-Sicherheitskataloge, hat sich zum Schutz Kritischer Infrastrukturen in der Praxis bewährt und ist beizubehalten. Ausschließlich Infrastrukturbetreiber selbst verfügen über das umfassende Verständnis einer Anlage, das zwingend erforderlich ist für eine zutreffende Einschätzung der eingesetzten Informations- und Telekommunikationstechnik (IKT) hinsichtlich ihrer Wirksamkeit für einen sicheren Anlagenbetrieb.

BDEW-Petitum:
Wir fordern, den Passus zu streichen oder zumindest anzugleichen gemäß bestehenden Definitionen innerhalb des EnWG und daraus ableitenden Regulierungen sowie der TrinkwV, sodass nicht die Gesamtheit der in der Energie- und Wasserversorgung eingesetzten, zentralen und dezentralen IKT eingeschlossen wird.

Zu Artikel 1, § 2, Absatz 14 Nummer 2: **„Infrastruktur im besonderen öffentlichen Interesse“**

Worum geht es?
Der neu eingeführte Terminus definiert Infrastrukturen, die nicht von Absatz 10 erfasst sind, aber dennoch von erheblicher Bedeutung sind, weil durch ihren Ausfall oder ihre Beeinträchtigung die Geschäftstätigkeit von Unternehmen mit Zulassung zum Teilbereich des regulierten Marktes mit weiteren Zulassungsfolgepflichten (Prime Standard) nach § 48 Börsenordnung der Frankfurter Wertpapierbörse eingeschränkt und dadurch erhebliche volkswirtschaftliche Schäden eintreten würden.

Einschätzung:
Eine Konkretisierung ist erforderlich, da die Definition „von erheblichem volkswirtschaftlichem Schaden“ in der vorliegenden Form offen und vage bleibt. Dies wird unmittelbar Rechtsunsicherheit und eine unklare Auslegung des Gesetzes nach sich ziehen. Eine konkrete und sachlich nachvollziehbare Einschätzung, wann die Vorschriften des Paragrafen Anwendung finden, sollte unmittelbar im Gesetz verankert werden. Der Passus könnte sich beispielsweise im Einzelfall auf die Infrastrukturen beziehen, bei denen im Falle einer Schädigung erhebliche Versorgungsengpässe der Öffentlichkeit oder Gefährdungen für die öffentliche Sicherheit zu erwarten wären. Die vorgeschlagene Neueinführung des Terminus geht verschärfend über die europäische NIS-Richtlinie sowie das Gesetz zur Umsetzung der NIS-Richtlinie hinaus.

BDEW-Petitum:
Der Terminus „Infrastruktur im besonderen öffentlichen Interesse“ ist unklar und sollte im Gesetzestext konkretisiert werden. Darüber hinaus scheint es angebracht, dem Bundesministerium für Wirtschaft und Energie (BMWi) als zuständigem Ressort die Grundlagen der Beurteilung von volkswirtschaftlichen Schäden und damit die federführende Erstellung der Rechtsverordnung nach § 10 Absatz 5, IT-SiG 2.0 zu überlassen. Bei der Ausarbeitung der Rechtsverordnung sind Vertreter der Gesellschaft und Wirtschaft mit einzubeziehen. Der vorliegende Passus ist diesbezüglich anzupassen.

Alternativ könnte ebenso statt auf „volkswirtschaftlichen Schaden“ auf „erhebliche Versorgungsengpässe für die Öffentlichkeit sowie Gefährdungen für die öffentliche Sicherheit“ (analog zu § 5c Absatz 1 Nummer 2, IT-SiG 2.0) abgestellt werden. Somit würden die geltenden gesetzgeberischen Fachkompetenzen des Bundesministeriums des Innern, Bau und Heimat berücksichtigt werden.

Zu Artikel 1, § 3 Absatz 1 Nummer 5a: Neue Aufgabe des BSI als Konformitätsbewertungsstelle

Worum geht es?

Das BSI soll die Befugnis erhalten, als Konformitätsbewertungsstelle im Bereich IT-Sicherheit tätig zu sein.

Einschätzung:

Für das BSI als Zertifizierungsbehörde sind Zertifizierungsanforderungen, Umfang und Zweck zu klären sowie die Beteiligung der für die Sicherheit der Energie- und Trinkwasserversorgung zuständigen Behörden sicherzustellen (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Bundesnetzagentur, Umweltbundesamt). Die Präzisierung sollte nach internationalen Standards erfolgen unter Berücksichtigung von bewährten grenzüberschreitenden Betriebskonzepten, Anbindungen und Verantwortlichkeiten. Zur Entlastung des Vollzugs sollten Konformitätsbewertungen weiterhin an Dritte delegiert werden können. Eine Anlehnung an europäische Vorgaben zur Netz- und Informationssicherheit muss stets Vorrang vor nationalen Alleingängen durch das BSI gegeben werden. Nur auf diesem Weg können ökonomische Sackgassen für Gesellschaft und Wirtschaft vermieden werden.

BDEW-Petitum:

Eine Präzisierung sollte für die neuen Aufgaben des BSI als Konformitätsbewertungsstelle hinsichtlich der Zertifizierungsanforderungen und der organisatorischen Zielsetzung erfolgen. Geklärt werden sollte auch, ob weiterhin Konformitätsbewertungen an Dritte delegiert werden können.

Zu Artikel 1, § 3 Absatz 1 Nummer 19: Entwicklung von Anforderungen an Identifizierungs- und Authentisierungsverfahren

Worum geht es?

Zur Förderung der Sicherheit in der Informationstechnik soll das BSI Anforderungen an Identifizierungs- und Authentisierungsverfahren entwickeln und die Verfahren anschließend bewerten.

Einschätzung:

Verbaute Komponenten sowie verlässlich funktionierende Verfahren benötigen zwingend Bestandsschutz, da ein vollständiger Austausch bzw. Wechsel von bewährten Verfahren und Komponenten eine massive und unverhältnismäßige wirtschaftliche Belastung zur Folge haben würde. Das BSI sollte keine Maßnahmen bzw. Verfahren vorschreiben, sondern im Sinne einer technologieoffenen Regulierung die damit verbundenen Schutzziele vorgeben.

BDEW-Petitum:

Ein Bestandsschutz für bereits verbaute Komponenten und Systeme zur Identifizierung und Authentisierung sollte gewahrt werden. Das BSI sollte lediglich Schutzziele des Einsatzes von Identifizierungs- und Authentisierungsverfahren festlegen.

Zu Artikel 1, § 4b: Meldestelle für die Sicherheit in der Informationstechnik

Worum geht es?
Das BSI soll Informationen über IT-Sicherheitsrisiken über hierfür eingerichtete Meldemöglichkeiten sammeln und auswerten. Die verarbeiteten Informationen können der Öffentlichkeit, Bundesbehörden und Betreibern Kritischer Infrastrukturen mitgeteilt werden, sofern Betriebs- und Geschäftsgeheimnisse geschützt bleiben und der Schutz von personenbezogenen Daten nicht „das Allgemeininteresse an der Übermittlung überwiegen".

Einschätzung:
Das BSI sollte dazu verpflichtet werden, solche Informationen entgegen zu nehmen und diese dann geeignet an Betreiber Kritischer Infrastrukturen weiterzureichen.

Die derzeitige Formulierung des § 4b Absatz 3 lässt erfahrungsgemäß vermuten, dass kein offener Dialog bezüglich IT-Sicherheitsrisiken zwischen den Behörden und betroffenen Unternehmen stattfinden wird, da verarbeitete Informationen in der Vergangenheit als Verschlusssache (VS) eingestuft wurden.

BDEW-Petitum:
Der Passus sollte angepasst werden, sodass das BSI zur Kooperation mit der Öffentlichkeit, Bundesbehörden und Betreibern Kritischer Infrastrukturen verpflichtet ist:

> „(2) Das Bundesamt *muss* zur Wahrnehmung…"
>
> „(3) Das Bundesamt *muss* die gemäß Absatz 2 gemeldeten Informationen …"
>
> § 4b Absatz 3 zu „2. *Auf Grund von Vereinbarungen* die Öffentlichkeit gemäß § 7 zu warnen".

Zu Artikel 1, § 5b Absatz 1: Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen

Worum geht es?
Bei „herausgehobenen" IT-Sicherheitsfällen soll das BSI notwendige Maßnahmen „zur Wiederherstellung der Sicherheit oder Funktionstätigkeit des betroffenen" IT-Systems treffen.

Einschätzung:
Der Passus ist um klare Regeln und Bewertungsverfahren zu ergänzen, in welchem Krisen- und Notfall das BSI welche Befugnisse erhält. Ein Schwerpunkt sollte in der Abgrenzung zu bestehenden Krisen- und Notfallgesetzen des Bundes und der Länder und auch zu Notfallprozessen in Unternehmen liegen.

BDEW-Petitum:
Der Passus ist um klare Regeln und Bewertungsverfahren zu ergänzen, in welchem Krisen- und Notfall das BSI welche Befugnisse erhält.

Zu Artikel 1, § 5c: Sicherheit und Funktionsfähigkeit informationstechnischer Systeme im Falle erheblicher Störungen

Worum geht es?
Um die Aufrechterhaltung oder unverzügliche Wiederherstellung von Kritischen Infrastrukturen in Krisenfällen zu garantieren, soll das BSI gemeinsam mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und der zuständigen Aufsichtsbehörde sowie mit Einbezug der Betroffenen Krisenreaktionspläne erstellen. Bei erheblichen Störungen (Gefährdung von anderen Rechtsgütern) soll das BSI die zur Bewältigung der Störung erforderlichen Informationen einschließlich personenbezogener Daten übermitteln und einfordern und soweit der Betroffene die Störung nicht selbst behebt, im Einvernehmen mit dem BBK die Maßnahmen für die Wiederherstellung der Sicherheit und Funktionsfähigkeit der IT-Systeme anordnen.

Einschätzung:
Aufgrund der Komplexität der Netzwerke und IKT-Systeme sind diese für Dritte kaum umfassend zu durchdringen. Dies ist jedoch zwingende Voraussetzung, um sinnvolle Krisenreaktionspläne aufstellen zu können. Auch sind eine Vielzahl von Szenarien möglich, die zu einem Ausfall von kritischen Versorgungsdienstleistungen führen könnten, die wiederum eigene Krisenpläne nach sich ziehen. Weitaus zweckdienlicher und effizienter wäre hier, für spezielle Szenarien nach vorgegebenen Mustern Krisenpläne anzufordern oder den Fokus auf den öffentlichen Teil der Infrastruktur zu legen. Zu klären ist ferner, wer diese Krisenreaktionspläne zu erarbeiten und vorzulegen hat. Die Vorlage von Krisenreaktionsplänen sollte erst auf Anfrage des BSI und des BBK erfolgen.

Zu § 5c Absatz 1 Nummer 3: Bei den hier genannten Betroffenen dürfte es sich maßgeblich um Betreiber Kritischer Infrastrukturen bzw. Betreiber von Infrastruktur im öffentlichen Interesse handeln. Die genannte regelmäßige Anpassung mit Abstimmung der Betroffenen würde voraussichtlich nicht unerhebliche Kosten auf Seiten der Wirtschaft nach sich ziehen. Dem Referentenentwurf ist keine gebührende Berücksichtigung dieser Aufwendungen zu entnehmen.

BDEW-Petitum:
Wir regen an, den gesamten Passus zu überarbeiten und mit Notstandsgesetzen und anderen Regelungen für nationale Krisenlagen zu harmonisieren. Die Widerspruchsfreiheit gesetzlicher Vorgaben muss besonders im Krisenfall gewahrt werden. Des Weiteren sollte verständlich formuliert werden, von wem Krisenreaktionspläne vorgelegt werden sollten und wie verbindliche Muster entstehen. Die Verantwortung zur Erstellung von sektorenübergreifenden Krisenreaktionsplänen ist ausschließlich auf behördlicher Seite auf Bundesebene zu verorten. Einer Übernahme der Erfüllungskosten auf Seiten der Wirtschaft sollte unmittelbar im Gesetzestext Rechnung getragen werden. Besonderes Augenmerk muss auf die ökonomische und organisatorische Fähigkeit kleinerer und mittlerer Unternehmen (KMU) gelegt werden hinsichtlich der Erstellung und Umsetzung von Krisenreaktionsplänen.

Zu Artikel 1, § 7b: Detektion von Sicherheitsrisiken für Netz- und IT-Sicherheit und von Angriffsmethoden

Worum geht es?
Bei berechtigten Annahmen von unzureichendem Schutz und gefährdeter Funktionsfähigkeit von öffentlich erreichbaren IT-Systemen oder Netzen soll das BSI Maßnahmen zur Detektion von Sicherheitsrisiken für Netz- und IT-Sicherheit durchführen. Die Verantwortlichen oder der betreibende Dienstleister des jeweiligen Netzes oder Systems werden benachrichtigt, „wenn sie bekannt sind oder ihre Identifikation ohne unverhältnismäßige weitere Ermittlungen möglich ist und überwiegenden Sicherheitsinteressen nicht entgegenstehen“. Um Schadprogramme und Angriffsmethoden zu erheben und auszuwerten, darf das BSI Angreifern Angriffe vortäuschen und die dazu erforderlichen Daten verarbeiten.

Einschätzung:
Ein unautorisierter Eingriff sowie Einbau von fremder Hardware und Software in IT-Systeme und Netze von Betreibern Kritischer Infrastrukturen kann den sicheren Systembetrieb stören. Haftungsfragen bei einem Eingriff bzw. Einbau von fremder Hardware und Software in die Infrastruktur bleiben offen und sollten daher zwingend im Gesetzestext geregelt werden. Vor einer Informationsweitergabe bzw. Veröffentlichung von Informationen ist eine Qualitätsprüfung seitens des BSI zwingend erforderlich. Die Informationsweitergabe von Sicherheitsrisiken innerhalb von Netzwerken von Betreibern Kritischer Infrastrukturen ist hochsensibel und sollte eng eingegrenzt werden. Eine vorherige Information und die Zustimmung der Betreiber zur Detektion von Risiken in deren Netzwerken durch Dritte – wie dem BSI – ist unerlässlich. Darüber hinaus sollte konkretisiert werden, was unter dem Begriff „öffentlich erreichbar“ gefasst wird. Ist beispielsweise die zugangsgesicherte Erreichbarkeit über eine IP-Adresse (Fernwartungszugang für Dienstleister) bereits eine öffentliche Erreichbarkeit, obwohl die Öffentlichkeit durch die Zugangsbeschränkung ausgeschlossen ist?

BDEW-Petitum:
Die Detektion von Sicherheitsrisiken für Netz- und IT-Sicherheit und von Angriffsmethoden ist eng zu begrenzen. Haftungs- und Kostenfragen sind in diesem Kontext vom Gesetzgeber zu klären. Abgesehen von Haftungs- und Kostenfragen sollte der Passus demzufolge lauten:

„Eine Information über und Weitergabe von Sicherheitsrisiken sowie die Durchführung von BSI-Maßnahmen und Auswertungen darf *nur mit vorheriger Zustimmung der oder des betroffenen Betreiber/s Kritischer Infrastruktur/en* erfolgen. Das Angebot von BSI-Überwachungsmaßnahmen und Auswertungen von Sicherheitsrisiken von Kritischen Infrastrukturen sollte deren Betreibern *verpflichtend* zur Verfügung gestellt werden.“

Zu Artikel 1, § 8a, Absatz 1a: Einsatz von Systemen zur Angriffserkennung und überzogene Berichterstattung

Worum geht es?
Betreiber Kritischer Infrastrukturen sollen Systeme zur Angriffserkennung einsetzen und dürfen die hierzu erforderlichen Daten verarbeiten. Die Ausgestaltung des Einsatzes von Systemen zur Angriffserkennung soll in einer Technischen Richtlinie durch das BSI festgelegt werden. Betreiber Kritischer Infrastrukturen sollen am Ende eines Quartals „detailliert" über die Verfahren und Umstände des Einsatzes von Systemen zur Angriffserkennung an die relevanten betrieblichen und staatlichen Stellen für Datenschutz schriftlich berichten.

Einschätzung:
Der Einsatz von Systemen zur Angriffserkennung bei Betreibern Kritischer Infrastrukturen wird grundsätzlich begrüßt. Der Einsatz dieser Systeme hat sich in der Energie- und Wasserwirtschaft verlässlich bewährt. Daher ist der Bestandsschutz bestehender und im Einsatz befindlicher Systeme zwingend zu wahren. Es sei denn, schwerwiegende nachweisbare sicherheitstechnische Gründe sprechen dagegen. Für die verpflichtende Einführung von Systemen zur Angriffserkennung ist jedoch zu berücksichtigen, dass derartige Systeme innerhalb Kritischer Infrastrukturen zunächst entwickelt und hinreichend getestet werden müssen. Aufgrund des spezifischen Wissens der zu schützenden Systeme sowie der Rückwirkung von Systemen zur Angriffserkennung auf diese sind die Betreiber Kritischer Infrastrukturen und ihre Wirtschaftsverbände in die Erarbeitung einer Technischen Richtlinien dringend einzubeziehen. Eine Vereinheitlichung der einzusetzenden Systeme kann dazu führen, dass die Schutzwirkung unterwandert wird, die vom Einsatz solcher Systeme ausgeht. Eine Übergangsfrist von mindestens zwei Jahren zur Einführung ist daher unbedingt notwendig und ist von der Fertigstellung der Technischen Richtlinien abhängig zu machen sowie bereits im Gesetzestext zu verankern. Das BSI sollte in die Lage versetzt werden, sogenannte „Intrusion Detection"- und „Instrusion Prevention"-Systeme, die am Markt erhältlich sind, hinsichtlich ihres Beitrags zum Schutz informationstechnischer Systeme zu bewerten sowie Empfehlungen dazu auf Anfrage geben zu können.

Die quartalsmäßigen schriftlichen Berichtspflichten stehen in keinem angemessenen Verhältnis. Ein praktischer Mehrwert ist diesem Berichtswesen nicht zu entnehmen. Datenfriedhöfe sind zu vermeiden. Eine praxisnahe Entbürokratisierung wäre wünschenswert. Vor diesem Hintergrund sollten die an mehrere Behörden parallel vorgesehenen, vierteljährlichen Berichterstattungen über Verfahren und Umstände von Maßnahmen des Einsatzes von Systemen zur Angriffserkennung dringend kritisch hinterfragt werden. Eine einheitliche und schlanke Berichterstattung an eine zentrale Meldestelle ist im Sinne eines effizienten Berichtswesens empfehlenswert.

BDEW-Petitum:
Wir regen an, den Passus umzuformulieren: Betreiber Kritischer Infrastrukturen und ihre Wirtschaftsverbände sind bei der Erarbeitung einer Technischen Richtlinie für Systeme zur Angriffserkennung dringend einzubeziehen. Es sollte lediglich das Schutzziel vorgegeben werden und keine Vorgabe der Technologie, spezifisch „Instrusion Detection"- und Intrusion Prevention"-Systeme, durch das BSI erfolgen. Technologieoffenheit ist erforderlich, da sonst der

freie Wettbewerb verzerrt, die unternehmerische Freiheit eingeschränkt und die Schutzwirkung gefährdet wird. Das BSI sollte befähigt werden, die unterschiedlichen, am Markt erhältlichen Systeme zur Angriffserkennung und -prävention bewerten und empfehlen zu können. Der europäische Vorgaberahmen muss dabei einbezogen werden. Aufgrund der großen Gefahren eines voreiligen Einsatzes solcher Systeme für den sicheren Anlagenbetrieb ist eine Übergangsfrist von mindestens zwei Jahren im Gesetz zu verankern. Die Vorgaben über eine vierteljährliche schriftliche Berichterstattung über Verfahren und Umstände von Maßnahmen des Einsatzes von Systemen zur Angriffserkennung sollten überarbeitet werden. Die Berichterstattung sollte einmal jährlich erfolgen.

Zu Artikel 1, § 8a Absatz 6: „Vertrauenswürdigkeitserklärung“

Worum geht es?
Betreiber Kritischer Infrastrukturen sollen nur „KRITIS-Kernkomponenten“ von Herstellern beziehen dürfen, die die neu einzuführende Vertrauenswürdigkeitserklärung abgegeben haben, die sich über die gesamte Lieferkette erstreckt.

Einschätzung:
Die Verpflichtungen für die und die Haftung seitens der Hersteller bleiben bei der vorgeschlagenen Vertrauenswürdigkeitserklärung unklar. Die Folgen bei Nicht-Abgabe einer Vertrauenswürdigkeitserklärung seitens des Herstellers sollten im Gesetzestext verankert werden, um eine zielgerichtete Wirkung des Passus gewährleisten zu können. Hersteller sollten auf Anfrage von Anwendern eine Erklärung über die Vertrauenswürdigkeit ihrer Komponenten und Bauteile ausstellen müssen.

Die Anwender von „KRITIS-Kernkomponenten“ sind die Betreiber Kritischer Infrastrukturen. Sie sollten daher bei der Erarbeitung von Mindestanforderungen an die Vertrauenswürdigkeit von Komponenten und Bauteilen zwingend einbezogen werden. Etablierte Prozesse und Bewertungsverfahren zur Gewährleistung und Überwachung der IT-Sicherheit von Komponenten und Bauteile aus der Energie- und Wasserwirtschaft sollten dabei berücksichtigt werden: Die Anforderungen müssten einerseits die für die Branche Trinkwasser geltenden europäischen Qualitätsanforderungen an Produkte und Bauteile in Kontakt mit Wasser einhalten. Andererseits sollten Mindestanforderungen auf bewährte Branchensicherheitsstandards (B3S) aufbauen, wie z.B. die vom BDEW erarbeiteten B3S für Fernwärme und für Aggregatoren sowie das BDEW/OE Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“.

BDEW-Petitum:
Der Passus ist zu streichen und durch eine „*verpflichtende Herstellererklärung*“ über die Vertrauenswürdigkeit von Komponenten gegenüber dem Betreiber Kritischer Infrastrukturen zu ersetzen. Die „verpflichtende Herstellererklärung“ sollte vor dem *erstmaligen* Einsatz und jederzeit auf Anfrage von Herstellern an Betreiber Kritischer Infrastrukturen ausgestellt werden. Bereits verbaute Komponenten und Bauteile, Ersatzteile und im Rahmen des Produktlebenszyklusses zur Instandhaltung, Erneuerung, Erweiterung und dem Austausch erforderliche Komponenten und Bauteile sollten zwingend Bestandsschutz erhalten. Zudem soll für Kom-

ponenten und Bauteile die wirtschaftliche Verhältnismäßigkeit gewahrt bleiben. Betreiber Kritischer Infrastrukturen als Anwender von Komponenten und Bauteilen müssen bei der Erarbeitung von Mindestanforderungen einbezogen werden. Bestehende Mindestanforderungen aus der Energie- und Wasserwirtschaft (BDEW B3S, BDEW/OE Whitepaper) müssen dabei berücksichtigt werden. Eine einheitliche Übergangsfrist von mindestens zwei Jahren muss gewährleistet werden.

Zu Artikel 1, § 8b Abs. 2 Satz 1

Worum geht es?
Das BSI soll die Anspruchsberechtigungen für den Zugang von Betreibern Kritischer Infrastrukturen zu einem einheitlichen Krisenkommunikationssystem regeln, welches eine geeignete Kommunikationsinfrastruktur zur Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung bereitstellt. Dabei sollen keine Doppelstrukturen zu den Netzinfrastrukturen und Diensten der Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) geschaffen werden.

Einschätzung:
Die zunehmende Dezentralisierung der Energieversorgung und die voranschreitende Digitalisierung konfrontieren die Unternehmen der Energie- und Wasserwirtschaft mit neuen Herausforderungen im Bereich der Kommunikation. Als Betreiber kritischer Infrastrukturen benötigen die Unternehmen sichere, flächendeckende, hochverfügbare und kosteneffiziente Kommunikationssysteme. Zur Bewältigung dieser Herausforderung strebt die Branche den Einsatz eines exklusiven Funknetzes auf Basis der 450-MHz-Frequenz an. Ein solches Netz ist sowohl für die Netzüberwachung und -steuerung, die Anbindung von Erzeugungs- sowie Verbrauchsanlagen, die Sprachkommunikation mit Wartungs- und Reparaturteams und die Auslesung intelligenter Messsysteme (Smart Meter) notwendig. Es muss dabei sowohl im Normalfall als auch bei Großschadensereignissen, Naturkatastrophen oder großflächigen Stromausfällen sicher zur Verfügung stehen und es muss gegen Cyberrisiken geschützt sein. Je nachdem, was das BSI künftig unter dem Terminus „einheitliches Krisenkommunikationssystem“ verstehen will, wäre möglich, dass es dem Betreiber eines 450 MHz-Funknetzes Vorgaben machen kann, wem Zugang zu dem Funknetz zu gewähren ist und gegebenenfalls auch zu welchen Rahmenbedingungen und Konditionen. Hierdurch befürchten wir eine Verzögerung und Beeinträchtigung des Ausbaus des 450-MHz-Funknetzes.

Bei einer noch weitergehenden Auslegung des Entwurfs könnte in der Passage sogar der Versuch gesehen werden, das Thema Krisen- und Notfallkommunikation verbindlich und für alle KRITIS-Bereiche komplett unter die Hoheit des BSI zu stellen. Es scheint, als ob das BSI auf Grundlage der Frequenzrechte und mit den Befugnissen aus einer solchen Regelung das letzte Wort über die Bestimmung des Betreibers (oder dem Eigenbetrieb) des Netzes, über die Zugangsvoraussetzungen und alle sonstigen Parameter hätte. Mit der Folge, dass z.B. ein Verteilnetzbetreiber zwar faktisch gezwungen sein könnte, seine Notfallkommunikation unter der Hoheit des BSI auf diesem Netz abzuwickeln, für seine anderen Anwendungsfälle wie z.B. Netzsteuerung oder smart-meter-Auslesung aber keinen Nutzen daraus ziehen

könnte, was in der Notwenigkeit mündet, andere und deutlich teurere Ersatzstrukturen aufzubauen.

BDEW-Petitum:
Sofern diese Regelung nicht auf die Nutzung des 450 MHz-Frequenzspektrums zielt, sollte dies klargestellt werden. Weiterhin sollte klargestellt werden, dass unter der Vermeidung von Doppelstrukturen bei den BOS nicht verstanden werden darf, dass sich alle anderen KRITIS-Bereiche für die eigene Notfallkommunikation nur noch auf das von den BOS vorgegebene Netz stützen dürfen.

Die Intention, eine Durchgängigkeit der Krisenkommunikation über KRITIS-Bereiche hinweg sicherstellen zu wollen, ist nachvollziehbar, da sich die Aufrechterhaltung der KRITIS-Dienste mindestens partiell gegenseitig bedingen. Sofern die Frequenznutzungsrechte durch die BNetzA unter wirtschaftlichen Prämissen verbunden mit Auslastungsrisiken vergeben werden sollen, sollte diese Passage des IT-SiG 2.0 bzw. die auf dieser Grundlage durch das BSI prinzipiell möglichen Festlegungen an einen Frequenzinhaber dies jedenfalls nicht durch wirtschaftlich prohibitive Vorgaben konterkarieren dürfen. Eine entsprechende Klarstellung im Entwurf wäre deshalb notwendig.

Zu Artikel 1, § 8e, IT-SiG 1.0: **Auskunftsverlangen**

Worum geht es?
Soweit die „schutzwürdigen Interessen“ von Betreibern Kritischer Infrastrukturen nicht gefährdet werden, soll das BSI Dritten auf Antrag Auskunft über im Rahmen von § 8a Absätze 2 und 3 und § 8c Absatz 4 erhaltene Informationen sowie zu den Meldungen nach § 8b Absatz 4 und § 8c Absatz 4 erteilen können.

Einschätzung:
Eine Auskunftsverpflichtung des BSI im Sinne der Transparenz behördlicher Vorgänge sollte mit normativer Nomenklatur verpflichtend sichergestellt sein im Einverständnis mit dem jeweiligen Betreiber Kritischer Infrastruktur.

BDEW-Petitum:
Der Passus sollte wie folgt umformuliert werden: “Das Bundesamt *muss im Einverständnis mit dem jeweiligen Betreiber Kritischer Infrastruktur* Dritten auf Antrag Auskunft …“.

Zu Artikel 1, § 8g: **Cyberkritikalität**

Worum geht es?
Das BSI soll Unternehmen Pflichten nach §§ 8a und 8b auferlegen können, deren informationstechnische Systeme, Komponenten oder Prozesse bei Störungen der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit, insbesondere wegen des hohen Grades an Vernetzung der eingesetzten Informationstechnik, zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Erbringung der betroffenen Dienstleistung insgesamt (Cyberkritikalität) und zu einer Gefährdung für ein Grundinteresse der Gesellschaft führen würden.

Einschätzung:
Die vorliegende Definition bleibt vage. Der Mehrwert des Kriteriums „Cyberkritikalität“ erscheint unklar. Auf diesem Weg wird faktisch ein Umgehungstatbestand eingeführt, mittels dessen nahezu der gesamten Energie- und Wasserwirtschaft willkürlich durch behördliche Einzelfestlegung erhöhte Sicherheitsanforderungen auferlegt werden könnten. Eine Auferlegung besonderer Schutzpflichten für bzw. weitere Benennungen von Kritischen Infrastrukturen sollten ausschließlich im Rahmen der BSI-KritisV erfolgen und nicht über eine „Bundesamtsverpflichtung“.

BDEW-Petitum:
Der Passus sollte ersatzlos gestrichen werden. Folgeänderungen und -verweise sind dementsprechend im gesamten Referentenentwurf anzupassen.

Zu Artikel 1, § 9a: Freiwilliges IT-Sicherheitskennzeichen

Worum geht es?
Es soll ein freiwilliges IT-Sicherheitskennzeichen für verschiedene Produktkategorien eingeführt werden. Das IT-Sicherheitskennzeichen muss beim BSI vom Hersteller beantragt werden und bescheinigt das „Vorlegen bestimmter IT-Sicherheitseigenschaften“, welche regelmäßig und anlassbezogen vom BSI geprüft werden sollen. Das Kennzeichen muss mit dem Produkt oder dessen Verpackung verbunden sein und kann als Werbung genutzt werden. Bei Nichteinhaltung oder verweigerter Freigabe wird die Nutzung des IT-Sicherheitskennzeichens widerrufen.

Einschätzung:
Die Einführung eines Kennzeichens, das für Verbraucher verständliche Aussagen über die IT-Sicherheit eines Produkts bereithält – analog zum EU-Effizienzlabel –, wird grundsätzlich begrüßt. Allerdings ist dabei zu beachten, dass eine grundsätzliche Verpflichtung von Betreibern Kritischer Infrastrukturen zur Nutzung von Produkten mit IT-Sicherheitskennzeichen nicht zielführend ist. Von der Einführung von Doppelregulierungen für Kritische Infrastrukturen, beispielsweise mittels Vertrauenswürdigkeitserklärung und IT-Sicherheitskennzeichen, geht kein nennenswerter Mehrwert für den Schutz Kritischer Infrastrukturen aus. Darüber hinaus würde eine verpflichtende Ausweitung auf KRITIS-Kernkomponenten einen massiven Eingriff in die unternehmerische Freiheit sowie in die Verfügbarkeit von zertifizierten Produkten am Markt darstellen. Angesichts der geplanten Einführung eines europäischen Zertifizierungs- und Kennzeichnungssystems für die Cybersicherheit von Produkten, Dienstleistungen und Prozessen durch die kürzlich beschlossene EU-Cybersicherheits-Verordnung ist ein nationaler Alleingang grundsätzlich zu hinterfragen. Eine Doppelregulierung auf nationaler und europäischer Ebene würde lediglich zu Verwirrung führen, nicht nur auf Seiten der Verbraucher.

BDEW-Petitum:
Wir sprechen uns für eine Einführung eines freiwilligen IT-Sicherheitskennzeichens aus, auf Antrag der Hersteller von Produkten. Die Kriterien zur Erteilung dieses Kennzeichens müssen öffentlich zugänglich sein, um den individuellen Nutzen eines Einsatzes abschätzen

zu können. Wir lehnen eine Verpflichtung zur Nutzung dieser Produkte durch Betreiber Kritischer Infrastrukturen zwingend ab. Der Passus ist dementsprechend zu konkretisieren und ein nationaler Alleingang im Kontext der europäischen Bemühungen zu hinterfragen.

Zu Artikel 1, § 14: Bußgeldvorschriften

Worum geht es?
Fahrlässige Verstöße gegen vereinzelte Pflichten aus dem BSIG sollen einheitlich mit Geldbußen von bis zu 10.000.000 bzw. 20.000.000 Euro oder von bis zu 2 Prozent bzw. 4 Prozent des gesamten weltweit erzielten jährlichen Unternehmensumsatzes des vorangegangenen Geschäftsjahres, je nachdem, welche Verstöße begangen wurden und welche Beträge höher sind, geahndet werden.

Einschätzung:
Eine Anhebung des Sanktionsrahmens, die sich an der DSGVO orientiert, ist unverhältnismäßig. Die Sanktionshöhe der DSGVO wurde mit Geltung für 500 Millionen EU-BürgerInnen und der direkten Anknüpfung an die Grundrechte begründet. Auf nationalem Niveau können daher zwangsläufig nicht die gleichen Maßstäbe gelten. Der Sanktionsrahmen muss stets verhältnismäßig bleiben und vor allem auch Abstufungen zulassen sowie transparente Kriterien zur Bußgeldhöhe vorsehen. Eine Doppelsanktionierung der Energie- und Wasserwirtschaft ist darüber hinaus zu vermeiden.

Die Unternehmen aus den KRITIS-Sektoren sind hinsichtlich ihrer wirtschaftlichen Gegebenheiten unterschiedlich einzuordnen. Gleichzeitig sollten die vorgesehenen Bußgeldvorschriften auf verantwortungsvolle und wirtschaftlich tragbare Weise dem Dreiklang der europäischen NIS-Richtlinie für eine „wirksame, angemessene und abschreckende“ Sanktionshöhe entsprechen. Vor diesem Hintergrund liegt die Einführung von sektorspezifischen Bußgeldvorschriften in Orientierung an spezialgesetzlichen Vorgaben und Regulierungen nahe, wie beispielsweise dem EnWG und der TrinkwV.

BDEW-Petitum:
Der vorliegende Bußgeldkatalog sollte vollständig gestrichen oder unter Maßgabe der Verhältnismäßigkeit umfassend überarbeitet werden. Im Unterschied zur vorgeschlagenen Änderung im Referentenentwurf schlagen wir eine Einführung von sektorspezifischen Bußgeldvorschriften vor, die die variierenden wirtschaftlichen Gegebenheiten von Unternehmen aus den unterschiedlichen KRITIS-Sektoren ebenso im Kontext der NIS-Richtlinie berücksichtigen.

Zu § 109 Absatz 2a TKG: Systeme zur Angriffserkennung nach Vorgabe des BSI

Worum geht es?
Betreiber öffentlicher Telekommunikationsnetze und öffentlicher Telekommunikationsdienste sollen Systeme zur Angriffserkennung – nach Vorgabe des BSI – anwenden. Daten, die für die Aufklärung des Angriffs, den Schutz der Informationstechnik und die Strafverfolgung der Angreifer erforderlich sind, sollen Dienstanbieter selbstständig „detailliert“ quartalsmäßig und auf Aufforderung den zuständigen Behörden übermitteln.

Einschätzung:
Der Einsatz von Systemen zur Angriffserkennung bei Betreibern Kritischer Infrastrukturen wird grundsätzlich begrüßt. Der Einsatz dieser Systeme hat sich in der Energie- und Wasserwirtschaft verlässlich bewährt. Daher ist der Bestandsschutz bestehender und im Einsatz be-

findlicher Systeme zwingend zu wahren. Es sei denn, schwerwiegende nachweisbare sicherheitstechnische Gründe sprechen dagegen. Eine Vereinheitlichung der einzusetzenden Systeme kann dazu führen, dass die Schutzwirkung unterwandert wird, die vom Einsatz solcher Systeme ausgeht. Das BSI sollte jedoch in die Lage versetzt werden, sogenannte „Intrusion Detection"- und „Instrusion Prevention"-Systeme, die am Markt erhältlich sind, hinsichtlich ihres Beitrags zum Schutz informationstechnischer Systeme zu bewerten sowie Empfehlungen dazu auf Anfrage geben zu können.

Die vorgesehenen quartalsmäßigen Berichtspflichten stehen in keinem angemessenen Verhältnis, da bereits eine Meldepflicht von festgestellten Vorfällen an das BSI herrscht, in dessen Rahmen ohnehin eine schriftliche Berichterstattung stattfinden muss. Ein praktischer Mehrwert ist diesem Berichtswesen nicht zu entnehmen.

BDEW-Petitum:
Wir regen an, den Passus umzuformulieren: Es sollte lediglich das Schutzziel vorgegeben und keine Vorgabe der Technologie, spezifisch „Instrusion Detection"- und Intrusion Prevention"-Systeme, durch das BSI erfolgen. Technologieoffenheit ist erforderlich, da sonst der freie Wettbewerb verzerrt, die unternehmerische Freiheit eingeschränkt und die Schutzwirkung gefährdet wird. Das BSI sollte jedoch befähigt werden, die unterschiedlichen, am Markt erhältlichen Systeme zur Angriffserkennung und -prävention bewerten und empfehlen zu können. Der europäische Vorgaberahmen muss dabei einbezogen werden.

Wir fordern darüber hinaus, den letzten Satz des Passus ersatzlos zu streichen: „[…] Die Diensteanbieter müssen der oder dem betrieblichen Datenschutzbeauftragten, dem Bundesamt für Sicherheit in der Informationstechnik, der Bundesnetzagentur und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit am Ende eines Quartals detailliert über die Verfahren und Umstände von Maßnahmen nach Satz 1 in diesem Zeitraum schriftlich berichten.".

Zu § 109b TKG: Pflicht der Provider zur Meldung und Löschung

Worum geht es?
Erbringer öffentlich zugänglicher Telekommunikationsdienste sollen dem BKA eine rechtswidrige Weitergabe oder eine Veröffentlichung rechtswidrig erlangter Daten über seinen Dienst melden. Sobald eine unrechtmäßige Erlangung oder Verbreitung von personenbezogenen Daten oder Geschäftsgeheimnisse beinhaltenden Daten vorliegt, soll der Dienstanbieter unverzüglich den Zugang sperren und betroffene Nutzer informieren.

Einschätzung:
Die Pflicht für Provider öffentlich zugänglicher Telekommunikationsdienste, rechtswidrig erlangte Daten durch Dritte, die weitergegeben oder veröffentlicht wurden, zu melden und zu löschen, wird grundsätzlich begrüßt.

BDEW-Petitum:
Zur Vermeidung von operativer Unsicherheit und Förderung von Rechtsunklarheit empfehlen wir, die Kriterien für die Meldung an das BSI unmittelbar im Gesetzestext zu konkretisieren.

Ansprechpartner

Für die Energiewirtschaft

Yassin Bendjebbour
Abteilung
Betriebswirtschaft, Steuern und Digitalisierung
Telefon: 030 / 300 199 - 1526
E-Mail: yassin.bendjebbour@bdew.de

Für die Wasserwirtschaft

Dr. Michaela Schmitz
Geschäftsbereich
Wasser und Abwasser

Telefon: 030 / 300 199 - 1200
E-Mail: michaela.schmitz@bdew.de