Bundesrat **Drucksache 643/14 (Beschluss)**

06.02.15

Stellungnahme
des Bundesrates

Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

Der Bundesrat hat in seiner 930. Sitzung am 6. Februar 2015 beschlossen, zu dem Gesetzentwurf gemäß Artikel 76 Absatz 2 des Grundgesetzes wie folgt Stellung zu nehmen:

1. Zum Gesetzentwurf allgemein:

   a) Der Bundesrat begrüßt die Initiative der Bundesregierung zur Verbesserung der IT-Sicherheit von Unternehmen und zum verstärkten Schutz der Bürgerinnen und Bürger im Internet. Die Sicherheit der Informations- und Kommunikationsinfrastrukturen ist zentrale Grundlage für eine erfolgreiche Digitalisierung von Wirtschaft und Gesellschaft.

   b) Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren dafür Sorge zu tragen, dass zur Schaffung von Planungs- und Rechtssicherheit eine weitere Konkretisierung von unbestimmten Rechtsbegriffen erfolgt. Dies betrifft vor allem die Präzisierung des Begriffs "Kritische Infrastrukturen" (§ 2 Absatz 10 BSIG-E), die Definition der Meldeschwelle für Telekommunikationsunternehmen bei auftretenden "beträchtlichen Sicherheitsverletzungen" (§ 109 Absatz 5 TKG-E), die Präzisierung des Begriffs "Stand der Technik" (§ 8a Absatz 1 Satz 2 BSIG-E) sowie die Definition einer "erheblichen Störung" (§ 8b Absatz 4 Satz 1 BSIG-E). Die Präzisierung des Begriffs "Kritische Infrastrukturen" sollte dabei in einem noch stärkeren Maße bereits im Gesetz selbst erfolgen.

Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln
Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0720-2946

c) Der Bundesrat bittet im weiteren Gesetzgebungsverfahren dafür Sorge zu tragen, dass eindeutige und transparente Regelungen getroffen werden, die einen angemessenen Schutz und eine sinnvolle Verwendung der umfangreichen Datenmengen sicherstellen, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) aufgrund der gesetzlichen Meldepflicht der Unternehmen erhält.

Begründung:

Der von der Bundesregierung vorgelegte Gesetzentwurf enthält sinnvolle Regelungen zur Verbesserung der IT-Sicherheit von Unternehmen und zum verstärkten Schutz der Bürgerinnen und Bürger im Internet. Zu nennen sind hier insbesondere die Etablierung von Mindeststandards an IT-Sicherheit nach dem Stand der Technik und die Meldepflicht von Betreibern kritischer Infrastrukturen bei schwerwiegenden Beeinträchtigungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse sowie die Information der Bürgerinnen und Bürger bei beträchtlichen Sicherheitsverletzungen und Störungen.

Der Gesetzentwurf enthält allerdings in zentralen Punkten unbestimmte Rechtsbegriffe, die zu einer erheblichen Rechts- und Planungsunsicherheit führen und deutlich höhere Mehrkosten bei den betroffenen Unternehmen als geplant verursachen könnten. So ist unter anderem der vom Gesetzentwurf betroffene Adressatenkreis nicht hinreichend konkret bezeichnet. Die Einstufung als kritische Infrastruktur kann gravierende wirtschaftliche Folgen für ein Unternehmen nach sich ziehen. Es sollte daher im Gesetz selbst eine weitergehende Klarstellung vorgenommen und dies nicht allein im Wege der Rechtsverordnung geregelt werden. Aufgrund dieser Unbestimmtheit bleibt die im Gesetzentwurf enthaltene Verpflichtung zu einem einzuhaltenden Mindeststandard an IT-Sicherheit ebenfalls zu vage.

Der Gesetzentwurf beantwortet außerdem nicht die Frage, wie das BSI mit den aufgrund der Meldepflicht künftig anfallenden riesigen Datenmengen umgehen will. Es ist daher zwingend erforderlich, dass zusammen mit den Standards für die Industrie auch die Standards und Arbeitsabläufe innerhalb des BSI hinsichtlich Klarheit, Effizienz und praktischem Nutzen dem Anspruch in der Zielsetzung des Gesetzentwurfs gerecht werden.

2. Zu Artikel 1 Nummer 1 (§ 1 Satz 2 BSIG)

In Artikel 1 Nummer 1 ist § 1 Satz 2 wie folgt zu fassen:

"Das Bundesamt ist zentraler Ansprechpartner für die Informationssicherheit in der Bundesrepublik Deutschland."

Begründung:

Mit dieser Formulierung wird das nationale Beratungsangebot des BSI zum Ausdruck gebracht, ohne die ebenfalls bestehenden Länderstrukturen zu übergehen.

3. Zu Artikel 1 Nummer 5 (§ 7 Absatz 1 BSIG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob die im geltenden § 7 Absatz 1 Satz 2 BSIG vorgesehene Verpflichtung zur rechtzeitigen Information von Herstellern betroffener Produkte auf Anbieter entsprechender informationstechnischer Dienstleistungen sowie betroffene Betreiber Kritischer Infrastrukturen ausgeweitet werden sollte.

Begründung:

§ 7 Absatz 1 Satz 1 BSIG-E sieht vor, dass das BSI Warnungen über Sicherheitslücken in informationstechnischen Produkten und Diensten an die Öffentlichkeit oder betroffene Kreise richten kann. § 7 Absatz 1 Satz 2 BSIG verpflichtet zur rechtzeitigen Information betroffener Hersteller von Produkten über die Warnungen. Eine Information an die Anbieter betroffener informationstechnischer Dienste ist bislang nicht explizit vorgesehen. Da informationstechnische Dienste oftmals über Telekommunikationsnetze angeboten werden, könnte darüber hinaus auch eine Information des entsprechenden Telekommunikationsnetzbetreibers als Betreiber einer betroffenen Kritischen Infrastruktur zielführend sein. Dies ist insbesondere auch von Bedeutung, da in der Novellierung die Nutzung unter anderem der Telekommunikationsnetzbetreiber als so genannte "Informationsintermediäre" zur Information an Dritte vorgesehen ist.

4. Zu Artikel 1 Nummer 6 (§ 7a Absatz 1 BSIG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob bezüglich der Untersuchung informationstechnischer Systeme der Telekommunikation das Einvernehmen mit der Bundesnetzagentur vorgesehen werden sollte.

Begründung:

Gemäß § 109 Absatz 7 TKG kann die Bundesnetzagentur bei Betreibern öffentlicher Telekommunikationsnetze oder bei Anbietern öffentlicher Telekommunikationsdienste eine Überprüfung bezüglich technischer Schutzmaßnahmen anordnen. Eine Kopie des Überprüfungsberichts ist an die Bundesnetzagentur zu übermitteln. Sofern informationstechnische Systeme der Telekommunikation gemäß § 7a Absatz 1 BSIG-E durch das BSI untersucht werden sollen, erscheint eine Verzahnung mit der Bundesnetzagentur bezüglich der dort bereits vorliegenden Informationen beziehungsweise geplanten Überprüfungsanordnungen sinnvoll. Es sollte geprüft werden, ob die verpflichtende Vorgabe einer diesbezüglichen engen Abstimmung zwischen BSI und Bundesnetzagentur durch Einvernehmensherstellung sinnvoll ist. Für weitere im Telekommunikationsgesetz geregelte Sachverhalte hat der Gesetzentwurf in der vorliegenden Fassung bereits weitgehend auf Doppelregulierung verzichtet (siehe auch § 8c Absatz 2 Nummer 1 BSIG-E).

5. Zu Artikel 1 Nummer 7 (§ 8b Absatz 2 Nummer 4 Buchstabe c BSIG)

In Artikel 1 Nummer 7 ist § 8b Absatz 2 Nummer 4 Buchstabe c wie folgt zu ändern:

a) Die Wörter "die zur Erfüllung ihrer Aufgaben erforderlichen" sind zu streichen.

b) Nach der Angabe "3" sind die Wörter ", insbesondere über Inhalte und Absender von Meldungen nach Absatz 4 mit möglichen Auswirkungen auf das jeweilige Land," einzufügen.

Begründung:

Mit dieser Formulierung werden die in § 8b Absatz 2 Nummer 4 Buchstabe c BSIG-E vorgesehenen Informationspflichten des BSI an die zuständigen Aufsichtsbehörden der Länder oder benannten Kontaktbehörden konkretisiert.

6. Zu Artikel 1 Nummer 7 (§ 8c Absatz 2 Nummer 3 BSIG),
Artikel 2 (§ 44b AtG),
Artikel 3 Nummer 1 Buchstabe b (§ 11 Absatz 1b Satz 3 und 4,
Absatz 1d - neu - EnWG)

a) In Artikel 1 Nummer 7 ist § 8c Absatz 2 Nummer 3 zu streichen.

b) In Artikel 2 ist § 44b wie folgt zu fassen:

"§ 44b
Sicherung der Informationstechnik

(1) Vorgaben zur Gewährleistung des erforderlichen Schutzes gegen Einwirkungen Dritter auf Telekommunikations- und elektronische Datenverarbeitungssysteme, die für diejenigen Anlagen nach § 7 Absatz 1 gelten, bei denen es sich um Energieanlagen im Sinne von § 3 Nummer 15 des Energiewirtschaftsgesetzes handelt und die durch Rechtsverordnung nach § 10 des BSI-Gesetzes als Kritische Infrastruktur eingestuft sind, werden auf Verlangen der Regulierungsbehörde nach § 54 Absatz 1 des Energiewirtschaftsgesetzes um Vorgaben ergänzt, die über die nukleare Sicherheit hinaus der Verfügbarkeit des Energieversorgungsnetzes oder der Energieanlage dienen, sofern dies nicht zu einer Verminderung der kerntechnischen Sicherheit führt.

(2) Inhaber von Anlagen im Sinne des Absatzes 1 haben der zuständigen Aufsichtsbehörde unverzüglich erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einer Gefährdung der nuklearen Sicherheit der betroffenen Anlage oder zur Beeinträchtigung der Verfügbarkeit der Energieanlage führen können oder bereits geführt haben, zu melden. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, und der betroffenen Informationstechnik enthalten.

(3) Die Aufsichtsbehörde leitet Meldungen nach Absatz 2 verbunden mit einer sicherheitstechnischen Bewertung unverzüglich an die für die Informationssicherheit auf nationaler Ebene zuständige Bundesoberbehörde und an die Regulierungsbehörde nach § 54 Absatz 1 des Energiewirtschaftsgesetzes weiter. § 11 Absatz 1c Satz 5 bis 8 des Energiewirtschaftsgesetzes gilt entsprechend."

c) Artikel 3 Nummer 1 Buchstabe b ist wie folgt zu fassen:

'b) Nach Absatz 1a werden folgende Absätze 1b bis 1d eingefügt:

"(1b) Betreiber von Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 8 des Gesetzes vom […] [einsetzen: Ausfertigungsdatum dieses Gesetzes und Fundstelle] geändert worden ist, in der jeweils geltenden Fassung als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind, haben binnen zwei Jahren nach Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme zu gewährleisten, die für einen sicheren Anlagenbetrieb notwendig sind. Die Regulierungsbehörde erstellt hierzu im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von Sicherheitsanforderungen und veröffentlicht diesen. Der Katalog von Sicherheitsanforderungen enthält auch Regelungen zur regelmäßigen Überprüfung der Erfüllung der Sicherheitsanforderungen. Ein angemessener Schutz des Betriebs von Energieanlagen im Sinne von Satz 1 liegt vor, wenn dieser Katalog eingehalten und dies vom Betreiber dokumentiert worden ist. Die Einhaltung kann von der Bundesnetzagentur überprüft werden. Zu diesem Zwecke kann die Regulierungsbehörde nähere Bestimmungen zu Format, Inhalt und Gestaltung der Dokumentation nach Satz 4 treffen.

(1c) Betreiber von Energieversorgungsnetzen und Energieanlagen, die ... <weiter wie Gesetzentwurf> ...

(1d) Die Absätze 1b und 1c gelten nicht für Betreiber von Energieanlagen, die einer Genehmigung nach § 7 Absatz 1 des Atomgesetzes bedürfen." '

Begründung:

Zu Buchstabe a:

Soweit es sich bei den in § 8c Absatz 2 Nummer 3 BSIG-E genannten Anlagen, die unter die Genehmigungspflicht nach § 7 Absatz 1 AtG fallen, um Kernkraftwerke handelt, unterfallen sie als Energieanlagen im Sinne des Energiewirtschaftsgesetzes bereits der Ausnahme nach § 8c Absatz 2 Nummer 2

BSIG-E. Denn der Begriff der Energieanlage umfasst nach § 3 Nummer 15, § 8c Absatz 2 Nummer 2 BSIG-E ausdrücklich auch "Anlagen zur Erzeugung […] von Energie". Hierunter fallen sämtliche Arten von Produktionsanlagen zur Erzeugung von Elektrizität, also auch Kernkraftwerke.

Sofern es sich bei den in § 8c Absatz 2 Nummer 3 BSIG-E genannten Anlagen, die unter die Genehmigungspflicht nach § 7 Absatz 1 AtG fallen, nicht um Kernkraftwerke handelt, würden sie gegebenenfalls von der Ausnahme des § 8c Absatz 2 Nummer 4 BSIG-E erfasst, wenn und soweit es sich überhaupt um Kritische Infrastrukturen handelt.

Im Übrigen ist die Ausnahme des § 8c Absatz 2 Nummer 3 BSIG-E durch die Beschränkung auf den "Geltungsbereich der Genehmigung" zu eng gefasst. Es ist nicht zweckmäßig, beim Schutz der Informationstechnik (IT) eines Kernkraftwerks zwischen dem kerntechnischen und dem konventionellen Bereich zu unterscheiden. Nach der für Kernkraftwerke geltenden Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorie I und II gegen Störmaßnahmen und sonstige Einwirkungen Dritter (SEWD-Richtlinie IT) sind ohnehin alle IT-Systeme zu erfassen, die vom Betreiber oder in seinem Auftrag betrieben werden und mit der Anlage in einem engen räumlichen, informationstechnischen oder betrieblichen Zusammenhang stehen.

Zu Buchstabe b:

Zu § 44b Absatz 1 - neu - AtG:

Die in § 11 EnWG-E vorgesehene Konstruktion führt für Kernkraftwerke zu einer nicht klar definierbaren Schnittstelle von Vorgaben nach dem Atomgesetz und Vorgaben nach dem Energiewirtschaftsgesetz. Vorgaben, die der kerntechnischen Sicherheit dienen, dienen in der Regel gleichzeitig auch der Verfügbarkeit und damit der Versorgungssicherheit, tun dies aber nicht vorrangig und zwangsläufig. Würden für Kernkraftwerke sowohl die SEWD-Richtlinie IT als auch der Katalog der Netzagentur gelten, müsste im Einzelfall geklärt werden, ob die Vorrangregelung des § 11 Absatz 1b Satz 3 EnWG-E greift. Außerdem müsste die Bundesnetzagentur bei der Erstellung ihres Katalogs mindestens sechs atomrechtliche Genehmigungs- und Aufsichtsbehörden beteiligen. Außerdem würde die im Gesetzentwurf vorgesehene Konstruktion zu sich überschneidenden Zuständigkeiten der Bundesnetzagentur und der atomrechtlichen Aufsichtsbehörden führen.

Der Gegenvorschlag zielt darauf ab, die Vorgaben für die IT-Sicherheit und die Aufsicht über deren Einhaltung ausschließlich dem Atomrecht zuzuordnen. Danach würde für Kernkraftwerke nur die SEWD-Richtlinie IT gelten, die vom Bundesministeriums für Umwelt, Naturschutz, Bau und Reaktorsicherheit mit der Bundesnetzagentur daraufhin abzustimmen wäre, ob auch die Bedürfnisse der Versorgungssicherheit abgedeckt werden. Die atomrechtlichen Vorgaben können auf Vorschlag der Bundesnetzagentur um allein der Versorgungssicherheit dienende Vorgaben ergänzt werden, sofern sie dem Schutzzweck des Atomgesetzes nicht zuwiderlaufen.

Die vorgeschlagene Regelung stellt sicher, dass – bei einem Konflikt zwischen Versorgungssicherheit und kerntechnischer Sicherheit – die kerntechnische Sicherheit Vorrang hat und dass hierüber die für die kerntechnische Sicherheit zuständige oberste Bundesbehörde (im üblichen Regelsetzungsverfahren unter Beteiligung der Länder) entscheidet.

Im Übrigen wurde der im Gesetzentwurf verwendete Begriff "Funktionsfähigkeit" durch "Verfügbarkeit" ersetzt, da es für die Versorgungssicherheit auf die Verfügbarkeit ankommt. Eine Anlage kann durchaus voll funktionsfähig sein und trotzdem unverfügbar sein.

Zu § 44b Absatz 2 - neu - und Absatz 3 - neu - AtG:

§ 44b Absatz 2 - neu - und Absatz 3 - neu - AtG stellt sicher, dass Meldungen über Störungen der IT in Kernkraftwerken schnellstmöglich das BSI und die Bundesnetzagentur erreichen. Es erscheint jedoch unerlässlich, dass diese Meldungen mit einer sicherheitstechnischen Bewertung durch die zuständige atomrechtliche Aufsichtsbehörde versehen werden. Dies schließt nicht aus, dass sich Betreiber von Kernkraftwerken bei Bedarf auch direkt der Beratung und Hilfe durch das BSI bedienen.

Im Übrigen ist bei Bedarf eine schnelle Information anderer Kraftwerksbetreiber auch schon über die Quermeldungen der Kernkraftwerksbetreiber untereinander sichergestellt.

Durch die entsprechende Anwendung von § 11 Absatz 1c Satz 5 bis 8 EnWG-E wird das besondere Interesse der Meldeverpflichteten und der atomrechtlichen Genehmigungs- und Aufsichtsbehörden an einer vertraulichen Behandlung der von ihnen gemeldeten Informationen berücksichtigt. Die hochsensiblen sicherheitskritischen Informationen unterliegen insbesondere im Hinblick auf die öffentliche Sicherheit einem besonderen Schutzbedürfnis.

Zu Buchstabe c:

Es handelt sich um eine Folgeänderung zum Änderungsvorschlag in Buchstabe b.

7. Zu Artikel 1 Nummer 8 Buchstabe a (§ 10 Absatz 1 Satz 1 BSIG)

In Artikel 1 Nummer 8 Buchstabe a ist in § 10 Absatz 1 Satz 1 das Wort "Wirtschaftsverbände" durch das Wort "Branchenverbände" zu ersetzen.

Begründung:

Unter den Begriff "Branchenverband" fällt auch der im Gesetzentwurf an dieser Stelle bislang verwendete Begriff "Wirtschaftsverband" und umfasst zudem auch die technischen Regelsetzer. In Artikel 1 Nummer 7 (§ 8a Absatz 2 Satz 1 BSIG-E) wird der Begriff "Branchenverband" in einem ähnlichen Zusammenhang bereits verwendet.

8. Zu Artikel 1 Nummer 8 Buchstabe a (§ 10 Absatz 1 Satz 1 BSIG),
Buchstabe b (§ 10 Absatz 2 BSIG),
Buchstabe c (§ 10 Absatz 3 Satz 3 BSIG)

In Artikel 1 Nummer 8 Buchstabe a § 10 Absatz 1 Satz 1, Buchstabe b § 10 Absatz 2 und Buchstabe c § 10 Absatz 3 Satz 3 ist jeweils das Wort "nicht" zu streichen.

Begründung:

Mit der Streichung des Wortes "nicht" in § 10 Absatz 1 Satz 1, Absatz 2 und Absatz 3 Satz 3 BSIG-E werden föderale Aspekte bei der Bestimmung Kritischer Infrastrukturen durch Rechtsverordnung berücksichtigt, zumal das Gesetz bei den Ländern – zumindest mittelbar – bedeutenden Erfüllungsaufwand auslösen wird.

9. Zu Artikel 5 Nummer 2 (§ 100 Absatz 1 TKG)

Artikel 5 Nummer 2 ist zu streichen.

Begründung:

Grundsätzlich besteht kein Änderungsbedarf.

Gemäß § 100 Absatz 1 TKG-E sollen Telekommunikationsanbieter die erweiterten Befugnisse erhalten, Nutzungsdaten "zum Erkennen, Eingrenzen und Beseitigen von Störungen sowie von Missbrauch seiner für Zwecke seines Telemedienangebots genutzten technischen Einrichtungen" zu erheben und zu verwenden. Bei der damit eingeführten Speicherbefugnis handelt es sich im Kern um eine weitreichende Vorratsdatenspeicherung, für die unter anderem das Bundesverfassungsgericht und der Europäische Gerichtshof enge Grenzen gesetzt haben. Die im Gesetzentwurf vorgesehene Speicherung von Informationen führt im Kern zu keiner Verbesserung der Informationssicherheit, sondern könnte zu einer weiteren Gefahrenquelle werden.

10. Zum Gesetzentwurf allgemein

Der Bundesrat bittet die Bundesregierung, die finanziellen Auswirkungen des Gesetzgebungsvorhabens auf die Länder und Kommunen vor allem unter folgenden Gesichtspunkten näher zu prüfen und darzulegen:

a) Die Verwaltungen der Länder und Kommunen gehören nicht zu den vom BSI-Gesetz adressierten Kritischen Infrastrukturen, weil der Bund hierfür keine Gesetzgebungskompetenz besitzt. Gleichwohl können Länder und Kommunen von der Neuregelung betroffen sein, wenn sie als Teil der Wirtschaft agieren (zum Beispiel: kommunale Wasser- und Energieversorgung). Darüber hinaus werden voraussichtlich die Zuschussbedarfe für die von den Ländern mitfinanzierten Infrastrukturen steigen (zum Beispiel: Krankenhaus, Rettungsdienst, öffentlicher Personennahverkehr).

b) Es ist davon auszugehen, dass wie bei der Bundesverwaltung faktisch auch bei den Verwaltungen der Länder und Kommunen personeller und sachlicher Mehraufwand, zum Beispiel für die verstärkte Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik oder für die Auswertung der Berichte zu den kritischen Infrastrukturen entstehen wird.

Um eine Bewertung des Gesetzentwurfs vornehmen zu können, müssen die finanziellen Auswirkungen bekannt sein. Der Bundesrat bittet deshalb die Bundesregierung, gemeinsam mit den Ländern und Kommunen eine umfassende Kostenschätzung vorzunehmen.