Änderungsantrag der Fraktionen der CDU/CSU und der SPD

im Innenausschuss des Deutschen Bundestages

zu dem Gesetzentwurf der Bundesregierung
– Drucksache 18/4096 –

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

Der Bundestag wolle beschließen,

den Gesetzentwurf auf Drucksache 18/4096 mit folgenden Maßgaben, im Übrigen unverändert, anzunehmen:

1. Artikel 1 wird wie folgt geändert:

   a) Nach Nummer 4 wird folgende Nummer 4a eingefügt:

      „4a. § 5 Absatz 1 wird wie folgt geändert:

      a) Satz 4 wird wie folgt gefasst:

      „Die Bundesbehörden sind verpflichtet, das Bundesamt bei Maßnahmen nach Satz 1 zu unterstützen und hierbei den Zugang des Bundesamtes zu behördeninternen Protokolldaten nach Satz 1 Nummer 1 sowie Schnittstellendaten nach Satz 1 Nummer 2 sicherzustellen.“

      b) Nach Satz 4 wird folgender Satz eingefügt:

      "Protokolldaten der Bundesgerichte dürfen nur in deren Einvernehmen erhoben werden."“

   b) Nummer 6 wird wie folgt geändert:

§ 7a Absatz 2 wird wie folgt gefasst:

„(2) Die aus den Untersuchungen gewonnenen Erkenntnisse dürfen nur zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14 und 17 genutzt werden. Das Bundesamt darf seine Erkenntnisse weitergeben und veröffentlichen, soweit dies zur Erfüllung dieser Aufgaben erforderlich ist. Zuvor ist dem Hersteller der betroffenen Produkte und Systeme mit angemessener Frist Gelegenheit zur Stellungnahme zu geben."

c) Nach Nummer 6 wird folgende Nummer 6a eingefügt:

„6a. § 8 Absatz 1 wird wie folgt gefasst:

„(1) Das Bundesamt erarbeitet Mindeststandards für die Sicherheit der Informationstechnik des Bundes. Das Bundesministerium des Innern kann im Benehmen mit dem IT-Rat diese Mindeststandards ganz oder teilweise als allgemeine Verwaltungsvorschriften für alle Stellen des Bundes erlassen. Das Bundesamt berät die Stellen des Bundes auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards. Für die in § 2 Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane haben die Vorschriften nach diesem Absatz empfehlenden Charakter.""

d) Nummer 7 wird wie folgt geändert:

aa) § 8a Absatz 1 Satz 2 wird wie folgt gefasst:

„Dabei soll der Stand der Technik eingehalten werden."

bb) § 8a Absatz 3 Satz 4 wird wie folgt gefasst:

„Das Bundesamt kann bei Sicherheitsmängeln verlangen:

1. die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse und
2. im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel."

cc) Nach § 8a Absatz 3 wird folgender Absatz 4 eingefügt:

„(4) Das Bundesamt kann zur Ausgestaltung des Verfahrens der Sicherheitsaudits, Prüfungen und Zertifizierungen nach Absatz 3 Anforderungen an die Art und Weise der Durchführung, an die hierüber auszustellenden Nachweise sowie fachliche und organisatorische Anforderungen an die prüfende Stelle nach Anhörung von Vertretern der betroffenen Betreiber und der betroffenen Wirtschaftsverbände festlegen."

dd) § 8b Absatz 4 Satz 1 und 2 werden wie folgt gefasst:

„Betreiber Kritischer Infrastrukturen haben erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen

1. führen können oder
2. geführt haben,

über die Kontaktstelle unverzüglich an das Bundesamt zu melden. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zur Branche des Betreibers enthalten."

ee) Nach § 8b Absatz 5 wird folgender Absatz 6 eingefügt:

„(6) Soweit erforderlich kann das Bundesamt vom Hersteller der betroffenen informationstechnischen Produkte und Systeme die Mitwirkung an der Beseitigung oder Vermeidung einer Störung nach Absatz 4 verlangen. Satz 1 gilt für Störungen bei Betreibern und Genehmigungsinhabern im Sinne von § 8c Absatz 3 entsprechend."

ff) Der bisherige § 8b Absatz 6 wird Absatz 7.

gg) § 8c wird wie folgt geändert:

In Absatz 2 Nummer 4 werden die Wörter „Betreiber Kritischer Infrastrukturen, die" durch die Wörter „Betreiber Kritischer Infrastrukturen, soweit sie" ersetzt.

e) Nummer 8 wird wie folgt geändert:

In § 10 Absatz 1 wird nach Satz 1 folgender Satz eingefügt:

„Der nach Satz 1 als bedeutend anzusehende Versorgungsgrad ist anhand von branchenspezifischen Schwellenwerten für jede wegen ihrer Bedeutung als kritisch anzusehende Dienstleistung im jeweiligen Sektor zu bestimmen."

f) Nummer 9 wird wie folgt geändert:

aa) Die Wörter „Folgender § 13 wird" werden durch die Wörter „Folgende §§ 13 und 14 werden" ersetzt.

bb) Nach dem Text zu § 13 wird folgender Text zu § 14 angefügt:

„§ 14
Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 8a Absatz 1 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 eine dort genannte Vorkehrung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig trifft,
2. einer vollziehbaren Anordnung nach § 8a Absatz 3 Satz 4
   a) Nummer 1 oder
   b) Nummer 2
   zuwiderhandelt,
3. entgegen § 8b Absatz 3 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 eine Kontaktstelle nicht oder nicht rechtzeitig benennt oder
4. entgegen § 8b Absatz 4 Satz 1 Nummer 2 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

(2) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 2 Buchstabe b mit einer Geldbuße bis zu hunderttausend Euro, in den übrigen Fällen des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

(3) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist das Bundesamt."

2. In Artikel 2 wird in § 44b Satz 2 die Zahl „6“ durch die Zahl „7“ ersetzt.

3. In Artikel 5 Nummer 5 werden die Wörter „eine Beeinträchtigung von Telekommunikationsnetzen oder –diensten, die zu einer beträchtlichen Sicherheitsverletzung führt, nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig mitteilt“ durch die Wörter „eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht“ ersetzt.

4. Artikel 10 wird wie folgt geändert:

   a) Die Artikelbezeichnung wird wie folgt geändert:

      „Inkrafttreten und Evaluierung“

   b) Nach Satz 2 wird folgender Satz angefügt:

      „Artikel 1 Nummern 2, 7 und 8 sind vier Jahre nach Inkrafttreten der Rechtsverordnung nach Artikel 1 Nummer 8 unter Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag bestellt wird, zu evaluieren.“

Begründung:

Zu Nummer 1
Buchstabe a)
Aktuell in der Presse diskutierte Beispiele von Schadprogrammen wie REGIN oder Schadsoftwareplattformen der Equation Group verdeutlichen einen erneuten Qualitätssprung in der Bedrohung der IT des Bundes. Es handelt sich hierbei um hochkomplexe, multifunktionale und modular aufgebaute Spionageprogramme, die an Stellen ansetzen, auf die beispielsweise gängige Virenschutzprogramme bisher nicht zugreifen können. Die Erkennung solcher Schadprogramme kann wirksam nur durch neue und auf die jeweilige konkrete Gefährdungssituation angepasste, umfangreiche sowie komplexe Detektionsmethoden zur Erkennung von Anomalien innerhalb der zu schützenden Netzwerke erfolgen. Das technische und personelle Know-how für ein derartiges Monitoring befindet sich in der Regel nicht in den einzelnen Behörden der Bundesverwaltung, sondern ist zentral im BSI verankert.

Derzeit erfüllt das BSI sein bestehendes Mandat zur zentralen Abwehr und Detektion von Angriffen durch ein zentrales Monitoring der behördenübergreifenden Regierungsnetze. Um neue Bedrohungen zuverlässig detektieren und abwehren zu können, muss dieses Monitoring ausgebaut werden. Hierfür benötigt das BSI auch Protokolldaten aus der internen IT der Behörden.

Das BSI kann die Behörden bisher nicht verpflichten, entsprechende Daten zu erheben, die dafür erforderlichen Schritte einzuleiten oder diese dem BSI zur Verfügung zu stellen.

Mit der Ergänzung in Satz 5 wird dem besonderen Schutz der richterlichen Unabhängigkeit Rechnung getragen.

Buchstabe b)
Die Änderung von § 7a Absatz 2 des BSI-Gesetzes stellt die insgesamt enge Zweckbindung der Vorschrift klar und bedient sich dabei der im BSI-Gesetz üblichen Verweistechnik (vergleiche zum Beispiel § 7 Absatz 1 Satz 1, § 7 Absatz 2 Satz 1, § 8 Absatz 2 Satz 1 des BSI-Gesetzes in seiner geltenden Fassung).

§ 7a des BSI-Gesetzes nimmt mit der Änderung nunmehr in allen seinen Aspekten konkret Bezug auf die Erfüllung folgender Aufgaben des BSI:

- Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes (§ 3 Absatz 1 Satz 2 Nummer 1 des BSI-Gesetzes),
- Beratung und Warnung der Stellen des Bundes, der Länder sowie der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen (§ 3 Absatz 1 Satz 2 Nummer 14 des BSI-Gesetzes),
- Aufgaben nach den §§ 8a und 8b des BSI-Gesetzes als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen (§ 3 Absatz 1 Satz 2 Nummer 17 des BSI-Gesetzes).

Diese Zweckbindung gilt nunmehr ausdrücklich für

- die Untersuchung von auf dem Markt bereitgestellten oder zur Bereitstellung auf dem Markt vorgesehenen informationstechnischen Produkten und Systemen (Absatz 1),
- die Nutzung der aus den Untersuchungen gewonnenen Erkenntnisse (Absatz 2 Satz 1) sowie
- die Weitergabe und Veröffentlichung dieser Erkenntnisse (Absatz 2 Satz 2).

Buchstabe c)
Die Änderung in Satz 1 dient der Klarstellung, dass die Erarbeitung von Mindeststandards für die IT-Sicherheit des Bundes eine Pflichtaufgabe des BSI ist.

Die Änderung in Satz 2 stärkt die Befugnisse des BSI. Das bisher vorgesehene Zustimmungserfordernis hat den Erlass verbindlicher Mindeststandards für die IT-Sicherheit des Bundes und damit die Schaffung eines hinreichenden und einheitlichen (Mindest-)Sicherheitsniveaus in der Bundesverwaltung faktisch verhindert. In den letzten Jahren hat sich die IT-Sicherheitslage des Bundes immer weiter verschärft. Gezielte Angriffe auf die Informationstechnik des Bundes werden zahlreicher, professioneller und komplexer. Zugleich erhöht die steigende Abhängigkeit des Staates von Informationstechnik deren wesentliche Bedeutung für die Funktionsfähigkeit der staatlichen Verwaltung.

Satz 3 stellt klar, dass sich der Beratungsauftrag des BSI auch auf die Umsetzung der Mindestsicherheitsstandards in der Bundesverwaltung erstreckt.

Buchstabe d)

Doppelbuchstabe aa)
Durch die Änderung werden die Betreiber Kritischer Infrastrukturen bei der Sicherung ihrer Systeme, Komponenten und Prozesse stärker als bisher auf die Einhaltung des Standes der Technik verpflichtet.

Die Ausgestaltung als Soll-Vorschrift trägt dem Umstand Rechnung, dass Betreiber Kritischer Infrastrukturen teilweise Maßnahmen nicht ergreifen können, die aus reiner IT-Sicherheitssicht als Stand der Technik anzusehen wären. Dies gilt beispielsweise für zeitnahe Sicherheits-Updates von Betriebssystemen, deren Auswirkungen auf die notwendigen Betriebsprozesse bei komplexen Systemen nicht von vornherein absehbar sind. Das Einspielen solcher Updates könnte zu einem Ausfall der Kritischen Dienstleistungen führen, deren Schutz die gesetzliche Verpflichtung auf den Stand der Technik eigentlich bezweckt. Erforderlich ist daher eine gewisse Flexibilität in der Umsetzung von Maßnahmen, die dem Stand der Technik entsprechen.

„Soll" impliziert dabei eine Verpflichtung, von der die Betreiber nur in begründeten Ausnahmefällen abweichen dürfen - zum Beispiel, weil ansonsten das Ziel der Versorgungssicherheit überhaupt erst gefährdet wird.

Doppelbuchstabe bb)
Es handelt sich um redaktionelle Anpassungen.

Doppelbuchstabe cc)
§ 8a des BSI-Gesetzes sieht vor, dass Betreiber Kritischer Infrastrukturen und ihre Branchenverbände branchenspezifische Sicherheitsstandards vorschlagen können. Das BSI stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen an solche Standards zu erfüllen. Durch dieses Verfahren soll vermieden werden, dass in der Wirtschaft bereits bestehende Sicherungssysteme und Prozeduren ausgehebelt werden. Auch die Art, wie die Einhaltung des Stands der Technik nachgewiesen wird, wurde bewusst offen gelassen, um neben den in den Branchen bereits vorhandenen Prüfungs- und Zertifizierungsverfahren kein zusätzliches kostspieliges Verfahren zu etablieren. Zur Schärfung der Systematik von § 8a und im Interesse größerer Rechtsklarheit soll dem BSI aber in diesem Rahmen durch den neuen Absatz 4 ermöglicht werden, konkrete Vorgaben an die Art und Weise der Durchführung, an die hierüber auszustellenden Nachweise sowie fachliche und organisatorische Anforderungen an die prüfende Stelle zu machen.

Doppelbuchstabe dd)

Die Ergänzung dient der Klarstellung, dass die Meldung des Betreibers auch Angaben dazu enthalten muss, in welcher Art von Einrichtung oder Anlage die von der Störung betroffene Informationstechnik bei dem Betreiber der Kritischen Infrastruktur zur Anwendung kommt. Durch die Verwendung des Begriffs „Art“ wird klargestellt, dass es sich um allgemeine Angaben etwa zur Funktionalität der Anlage und nicht um unternehmensspezifische Angaben handelt, die sich auf die konkret durch den Betreiber eingesetzte Anlage beziehen. Die entsprechende Information ist für eine sachgerechte Auswertung der Meldung durch das Bundesamt erforderlich.

Im Hinblick auf § 8b Absatz 4 Satz 3 des BSI-Gesetzes ist eine Angabe zur Art der betroffenen Einrichtung nicht erforderlich, wenn dadurch ein eindeutiger Rückschluss auf den Betreiber der Kritischen Infrastruktur möglich wäre.

Doppelbuchstabe ee)
In der Praxis fehlt es häufig an der Mitwirkung der Hersteller von informationstechnischen Produkten und Systemen bei der kurzfristigen Behebung von Sicherheitslücken, etwa durch die Bereitstellung eines erforderlichen Sicherheits-Updates. Das IT-Sicherheitsgesetz gibt Betreibern Kritischer Infrastrukturen durch die Verpflichtung zum Einsatz sicherer IT-Produkte bereits jetzt eine Grundlage, um eine Vereinbarung über die Sicherheit/Fehlerfreiheit der zum Einsatz vorgesehenen IT-Produkte und IT-Systeme gegenüber den Herstellern durchsetzen zu können. Diese soll ergänzt werden um eine Anordnungsbefugnis des BSI, mit der die Hersteller der betroffenen informationstechnischen Produkte und Systeme im zumutbaren Umfang zur Mitwirkung an der Beseitigung oder Vermeidung von Störungen verpflichtet werden können.

Satz 2 stellt klar, dass diese Anordnungsbefugnis des BSI auch bei meldepflichtigen Störungen in den spezialgesetzlich geregelten Bereichen gilt.

Doppelbuchstabe ff)
Es handelt sich um eine notwendige Folgeänderung.

Doppelbuchstabe gg)
§ 8c Absatz 2 Nummer 4 des BSI-Gesetzes verweist in seiner derzeitigen Fassung als Auffangtatbestand pauschal auf vorrangige spezialgesetzliche Anforderungen zur Einhaltung von Mindeststandards, die denen nach § 8a vergleichbar oder weitergehend sind. Die entsprechenden spezialgesetzlichen Rechtsvorschriften zu Sicherheitsstandards können aber unterschiedliche Sicherheitsaspekte auch jenseits von IT-Fragen betreffen. Die Rechtsfolge, nach der § 8a insgesamt für nicht

anwendbar erklärt wird, ist daher in der derzeitigen Fassung zu starr und durch Einfügung eines „soweit“ flexibler zu formulieren.

Buchstabe e)
Die Regelung konkretisiert das vorgesehene Verfahren zur Bestimmung der Betreiber Kritischer Infrastrukturen im Wege der Rechtsverordnung und trägt dem Erfordernis der hinreichenden Bestimmtheit der Normadressaten durch die Vorgabe eines konkreten Verfahrens für deren Bestimmbarkeit Rechnung. Danach hat eine sektor- und branchenspezifische Betrachtung dergestalt zu erfolgen, dass der für die Bestimmung der Normadressaten maßgebliche Versorgungsgrad als jeweils branchenspezifischer Schwellenwert für jede als kritisch anzusehende Dienstleistung im jeweiligen Sektor zu ermitteln ist. Nur im Falle einer Überschreitung dieser branchenspezifischen Schwellenwerte ist die konkrete Infrastruktur als kritisch im Sinne des Gesetzes anzusehen.

Buchstabe f)
Der Katalog der Bußgeldvorschriften ergänzt den kooperativen Ansatz der §§ 8a und 8b des BSI-Gesetzes um die Möglichkeit der bußgeldbewehrten Sanktion für den Fall der Nichteinhaltung der in den §§ 8a und 8b des BSI-Gesetzes vorgesehenen Pflichten. In Anlehnung an § 149 Nummer 21a des Telekommunikationsgesetzes ist der Verstoß des Betreibers einer Kritischen Infrastruktur gegen die Pflicht zur Meldung erheblicher Störungen im Sinne von § 8a Absatz 4 des BSI-Gesetzes dabei nur dann bußgeldbewehrt, wenn die betreffende Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat.

Absatz 2 regelt die Höhe der jeweiligen Bußgelder. Sachlich zuständige Verwaltungsbehörde ist gemäß Absatz 3 das BSI.

Zu Nummern 2 und 3
Es handelt sich um redaktionelle Anpassungen.

Zu Nummer 4
Die Evaluierung dient der Überprüfung der mit dem IT-Sicherheitsgesetz im BSI-Gesetz neu eingeführten Regelungen zu Meldepflichten und Mindeststandards. Die Formulierung lehnt sich an das entsprechende Vorgehen zum Antiterrordatei-Gesetz an. Insbesondere wird bei der Auswahl des/der Sachverständigen das Einvernehmen mit dem Bundestag vorgesehen. Die Evaluierung soll anhand der Konzeption zur

Evaluierung neuer Regelungsvorhaben gemäß dem Arbeitsprogramm bessere Rechtssetzung der Bundesregierung vom 28. März 2012, Ziffer II. 3., erfolgen.