Deutscher Bundestag **Drucksache 18/11808**

18. Wahlperiode 30.03.2017

Beschlussempfehlung und Bericht

des Innenausschusses (4. Ausschuss)

zu dem Gesetzentwurf der Bundesregierung
– Drucksachen 18/11242, 18/11620 –

Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union

A. Problem

Am 8. August 2016 trat die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19. Juli 2016, S. 1; im Folgenden: NIS-Richtlinie) in Kraft. Mit der Richtlinie wurden ein einheitlicher europäischer Rechtsrahmen für den EU-weiten Aufbau nationaler Kapazitäten für die Cyber-Sicherheit, eine stärkere Zusammenarbeit der Mitgliedstaaten der Europäischen Union sowie Mindestsicherheitsanforderungen an und Meldepflichten für bestimmte Dienste geschaffen. Ziel ist es, einheitliche Maßnahmen festzulegen, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen in der Europäischen Union erreicht werden soll (Artikel 1 Absatz 1 der NIS-Richtlinie). Die NIS-Richtlinie ist gemäß ihrem Artikel 25 Absatz 1 bis zum 9. Mai 2018 in nationales Recht umzusetzen. Gemäß Artikel 5 Absatz 1 der NIS-Richtlinie ermitteln die Mitgliedstaaten bis zum 9. November 2018 für jeden in Anhang II der Richtlinie genannten Sektor und Teilsektor die Betreiber wesentlicher Dienste mit einer Niederlassung in ihrem Hoheitsgebiet.

B. Lösung

Die europarechtlichen Vorgaben wurden bezüglich der Betreiber wesentlicher Dienste, in Deutschland die sogenannten Kritischen Infrastrukturen gemäß § 2 Absatz 10 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), im Wesentlichen bereits durch das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 (BGBl. I S. 1324) in deutsches Recht umgesetzt. Daher sind im Rahmen

einer Anpassung des BSIG sowie einer Anpassung einzelner für bestimmte Branchen der Kritischen Infrastrukturen vorrangiger Spezialgesetze (des Atomgesetzes – AtG –, des Energiewirtschaftsgesetzes – EnWG – und des Fünften Buches Sozialgesetzbuch – Gesetzliche Krankenversicherung – SGB V) nur wenige Anpassungen erforderlich.

Zur Umsetzung der Vorgaben der NIS-Richtlinie werden die Befugnisse des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Überprüfung der Einhaltung der technischen und organisatorischen Sicherheitsanforderungen, die Nachweispflicht der Betreiber nach § 8a BSIG und die Regelungen in § 8b BSIG um Vorgaben für das Verfahren bei grenzüberschreitenden Vorfällen erweitert. Ergänzend werden Regelungen zu Mobilen Incident Response Teams (MIRTs) aufgenommen, mit denen das BSI andere Stellen bei der Wiederherstellung ihrer IT-Systeme unterstützen wird. Zudem wird das BSIG um eine Definition der digitalen Dienste sowie um spezielle Regelungen zu Sicherheitsanforderungen, zu Meldepflichten und zur Aufsicht im Hinblick auf die Anbieter digitaler Dienste ergänzt; die Bußgeldvorschriften in § 15 werden entsprechend angepasst.

Die in Artikel 5 der NIS-Richtlinie vorgesehene Ermittlung der Betreiber wesentlicher Dienste wird über die im geltenden Recht bereits vorgesehene Rechtsverordnung nach § 10 Absatz 1 BSIG vorgenommen. Ergänzt wird eine Ermächtigung zum Erlass von Rechtsverordnungen zur Umsetzung der in Artikel 16 der NIS-Richtlinie vorgesehenen Durchführungsrechtsakte.

Die nach § 8c BSIG vorrangigen Spezialgesetze werden entsprechend den im BSIG mit Bezug auf den Betrieb Kritischer Infrastrukturen enthaltenen Regelungen angepasst, soweit sie die Anforderungen der NIS-Richtlinie bezüglich der Betreiber wesentlicher Dienste bisher unterschreiten.

Neu eingeführt werden Regelungen bezüglich der digitalen Dienste Online-Marktplätze, Online-Suchmaschinen und Cloud-Computing-Dienste in das BSIG.

Zusätzlich werden mit dem Gesetzentwurf erforderliche Klarstellungen, Bereinigungen und Anpassungen bei den Unterstützungsaufgaben des BSI vorgenommen.

Annahme des Gesetzentwurfs in geänderter Fassung mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktion BÜNDNIS 90/DIE GRÜNEN bei Stimmenthaltung der Fraktion DIE LINKE.

C. Alternativen

Keine.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht kein zusätzlicher Erfüllungsaufwand.

E.2 Erfüllungsaufwand für die Wirtschaft

Für die Betreiber von Energieversorgungsnetzen und Energieanlagen, für bestimmte Telekommunikationsanbieter, für die Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik), deren Gesellschafter die Spitzenverbände der Leistungserbringer und Kostenträger im nationalen Gesundheitswesen sind, sowie für sonstige Betreiber Kritischer Infrastrukturen entsteht ein Erfüllungsaufwand von maximal 8,66 Millionen Euro.

Für die Anbieter digitaler Dienste resultiert darüber hinaus durch die Verpflichtung zur Einhaltung eines Mindestniveaus an IT-Sicherheit und die Einführung von Meldepflichten für bestimmte IT-Vorfälle Erfüllungsaufwand. Dieser Aufwand kann im Voraus nicht quantifiziert werden, da das erforderliche Sicherheitsniveau und Meldeschwellen erst durch Durchführungsrechtsakte der Kommission festgelegt werden.

Der Kreis der verpflichteten Anbieter kann derzeit nicht konkret eingegrenzt und eine entsprechende Zahl meldepflichtiger Anbieter digitaler Dienste nicht benannt werden, da hierzu keine Erhebungen vorliegen. Es wird jedoch geschätzt, dass von den Regelungen für digitale Dienste in Deutschland zwischen 500 und 1.500 Unternehmen betroffen sein werden. Die konkrete Anzahl hängt jedoch auch von späteren Festsetzungen der Durchführungsakte der Kommission ab. Der Aufwand für die Umsetzung von Maßnahmen zur Sicherung technischer Einrichtungen für einzelne Anbieter kann im Voraus nicht quantifiziert werden, da das erforderliche Sicherheitsniveau erst durch Durchführungsrechtsakte der Kommission festgelegt werden wird. Da Informationstechnik für Anbieter von digitalen Diensten das Kerngeschäft darstellt und diese zudem bereits durch datenschutzrechtliche Vorgaben zur Gewährleistung eines hinreichenden Niveaus an Datensicherheit verpflichtet sind, ist allerdings davon auszugehen, dass das IT-Sicherheitsniveau bei digitalen Diensten bereits hohen Anforderungen genügt.

Auch die Anzahl der meldepflichtigen Vorfälle und der hierdurch für einzelne Anbieter resultierende Aufwand sind abhängig von der Festlegung konkreter Schwellenwerte und Meldevorgaben in Durchführungsrechtsakten der Kommission. Unter der Annahme, dass pro Betreiber und Jahr sieben Meldungen eines schweren Sicherheitsvorfalls erfolgen, und unter Ansatz einer Kostenschätzung von 660 Euro pro Meldung ergeben sich Gesamtkosten für die Meldepflicht digitaler Dienste in Höhe von rund 4,6 Millionen Euro. Kostenmindernd wird sich voraussichtlich auch hier auswirken, dass aufgrund datenschutzrechtlicher Vorgaben Meldestrukturen bereits vorhanden sein müssen.

Davon Bürokratiekosten

Einzig die Meldepflichten für digitale Dienste und bestimmte Energieversorgungsnetzbetreiber stellen eine Informationspflicht dar, wodurch die Bürokratiekosten um rund 11,76 Millionen Euro steigen.

Die Belastungen sind nicht im Rahmen der „One in, one out“-Regel der Bundesregierung zu kompensieren, da diese Änderungen aus einer 1:1-Umsetzung der verbindlichen Mindestvorgaben der Richtlinie (EU) 2016/1148 resultieren.

E.3 Erfüllungsaufwand der Verwaltung

Der Verwaltung entsteht für die Erfüllung der im Gesetz vorgesehenen zusätzlichen Aufgaben ein Aufwand von insgesamt 185,5 Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund 14,216 Millionen Euro.

Davon ist beim BSI ein Erfüllungsaufwand in Höhe 181,5 Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund 13,909 Millionen Euro und beim Bundesministerium des Innern (BMI) ein Erfüllungsaufwand in Höhe von vier Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund 420.000 Euro zu berücksichtigen. Beim BSI werden in geringem Umfang zusätzliche Sachkosten entstehen, die aus dem Haushalt des BSI getragen werden können.

Der Bedarf an Personalmitteln sowie Planstellen und Stellen soll finanziell und stellenmäßig im jeweiligen Einzelplan ausgeglichen werden.

Der Erfüllungsaufwand für die Länder und Kommunen ist derzeit nicht bezifferbar.

F. Weitere Kosten

Betreibern Kritischer Infrastrukturen können im Sonderfall nach § 8a Absatz 3 Satz 3 BSIG Kosten entstehen, soweit berechtigte Zweifel an der ordnungsgemäßen Einhaltung der ihnen obliegenden Sicherheitsanforderungen bestehen, die eine zusätzliche Überprüfung vor Ort erforderlich machen.

Beschlussempfehlung

Der Bundestag wolle beschließen,

den Gesetzentwurf auf Drucksachen 18/11242, 18/11620 mit folgenden Maßgaben, im Übrigen unverändert anzunehmen:

Artikel 5 wird wie folgt gefasst:

‚Artikel 5

Änderung des Telekommunikationsgesetzes

Das Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch die Artikel 1 und 12 des Gesetzes vom 4. November 2016 (BGBl. I S. 2473) geändert worden ist, wird wie folgt geändert:

1. § 100 Absatz 1 wird wie folgt geändert:

   a) In Satz 1 werden nach den Wörtern „der Teilnehmer und Nutzer“ die Wörter „sowie die Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind,“ eingefügt.

   b) Nach Satz 1 wird folgender Satz eingefügt:

   „Die Kommunikationsinhalte sind nicht Bestandteil der Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung.“

   c) Die folgenden Sätze werden angefügt:

   „Die Daten sind unverzüglich zu löschen, sobald sie für die Beseitigung der Störung nicht mehr erforderlich sind. Eine Nutzung der Daten zu anderen Zwecken ist unzulässig. Soweit die Daten nicht automatisiert erhoben und verwendet werden, muss der betriebliche Datenschutzbeauftragte unverzüglich über die Verfahren und Umstände der Maßnahme informiert werden. Der Diensteanbieter muss dem betrieblichen Datenschutzbeauftragten, der Bundesnetzagentur und der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit am Ende eines Quartals detailliert über die Verfahren und Umstände von Maßnahmen nach Satz 6 in diesem Zeitraum schriftlich berichten. Die Bundesnetzagentur leitet diese Informationen unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik weiter. Der Betroffene ist von dem Diensteanbieter zu benachrichtigen, sofern dieser ermittelt werden kann. Wurden im Rahmen einer Maßnahme nach Satz 1 auch Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung erhoben und verwendet, müssen die Berichte mindestens auch Angaben zum Umfang und zur Erforderlichkeit der Erhebung und Verwendung der Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung enthalten.“

2. § 109 Absatz 5 wird wie folgt geändert:

   a) In Satz 1 werden nach dem Wort „Bundesnetzagentur“ die Wörter „und dem Bundesamt für Sicherheit in der Informationstechnik“ eingefügt.

   b) Satz 5 wird aufgehoben.

   c) In dem neuen Satz 7 wird die Angabe „§ 8d“ durch die Angabe „§ 8e“ ersetzt.

3. § 109a wird wie folgt geändert:

   a) Dem Absatz 4 wird folgender Satz angefügt:

   „Der Diensteanbieter darf die Teile des Datenverkehrs von und zu einem Nutzer, von denen eine Störung ausgeht, umleiten, soweit dies erforderlich ist, um den Nutzer über die Störungen benachrichtigen zu können.“

   b) Nach Absatz 4 werden die folgenden Absätze 5 und 6 eingefügt:

   „(5) Der Diensteanbieter darf im Falle einer Störung die Nutzung des Telekommunikationsdienstes bis zur Beendigung der Störung einschränken, umleiten oder unterbinden, soweit dies erforderlich ist, um die Beeinträchtigung der Telekommunikations- und Datenverarbeitungssysteme des Diensteanbieters, eines Nutzers im Sinne des Absatzes 4 oder anderer Nutzer zu beseitigen oder zu verhindern und der Nutzer die Störung nicht unverzüglich selbst beseitigt oder zu erwarten ist, dass der Nutzer die Störung selbst nicht unverzüglich beseitigt.

   (6) Der Diensteanbieter darf den Datenverkehr zu Störungsquellen einschränken oder unterbinden, soweit dies zur Vermeidung von Störungen in den Telekommunikations- und Datenverarbeitungssystemen der Nutzer erforderlich ist.“

   c) Der bisherige Absatz 5 wird Absatz 7.

4. § 149 wird wie folgt geändert:

   a) Nach Absatz 1 Nummer 17b werden die folgenden Nummern 17c und 17d eingefügt:

   „17c. entgegen § 100 Abs. 1 Satz 3 die Daten nicht oder nicht rechtzeitig löscht,
   17d. entgegen § 100 Abs. 1 Satz 4 die Daten zu anderen Zwecken genutzt werden,“.

   b) Die bisherige Nummer 17c wird Nummer 17e.‘

Berlin, den 29. März 2017

Der Innenausschuss

Ansgar Heveling	**Clemens Binninger**
Vorsitzender	Berichterstatter

Gerold Reichenbach	**Martina Renner**	**Dr. Konstantin von Notz**
Berichterstatter	Berichterstatterin	Berichterstatter

Bericht der Abgeordneten Clemens Binninger, Gerold Reichenbach, Martina Renner und Dr. Konstantin von Notz

I. Überweisung

Der Gesetzentwurf auf **Drucksache 18/11242** wurde in der 221. Sitzung des Deutschen Bundestages am 9. März 2017 an den Innenausschuss federführend sowie an den Ausschuss für Recht und Verbraucherschutz, den Haushaltsausschuss, den Verteidigungsausschuss, den Ausschuss für Verkehr und digitale Infrastruktur und den Ausschuss Digitale Agenda zur Mitberatung überwiesen. Die Unterrichtung der Bundesregierung auf **Drucksache 18/11620** wurde in der 227. Sitzung des Deutschen Bundestages am 29. März 2017 an die beteiligten Ausschüsse überwiesen. Der parlamentarische Beirat für nachhaltige Entwicklung beteiligte sich gutachtlich (Ausschussdrucksache 18(4)802).

II. Stellungnahmen der mitberatenden Ausschüsse

Der **Ausschuss für Recht und Verbraucherschutz** hat in seiner 134. Sitzung am 22. März 2017 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktion BÜNDNIS 90/DIE GRÜNEN bei Stimmenthaltung der Fraktion DIE LINKE. empfohlen, den Gesetzentwurf anzunehmen.

Der **Haushaltsausschuss** hat in seiner 100. Sitzung am 22. März 2017 die Annahme des Gesetzentwurfs mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktion BÜNDNIS 90/DIE GRÜNEN bei Stimmenthaltung der Fraktion DIE LINKE. empfohlen.

Der **Verteidigungsausschuss** hat in seiner 88. Sitzung am 22. März 2017 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktion BÜNDNIS 90/DIE GRÜNEN bei Stimmenthaltung der Fraktion DIE LINKE. die Annahme des Gesetzentwurfs empfohlen.

Der **Ausschuss für Verkehr und digitale Infrastruktur** hat in seiner 102. Sitzung am 22. März 2017 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktion BÜNDNIS 90/DIE GRÜNEN bei Stimmenthaltung der Fraktion DIE LINKE. die Annahme des Gesetzentwurfs empfohlen.

Der **Ausschuss Digitale Agenda** hat in seiner 86. Sitzung am 29. März 2017 empfohlen, den Gesetzentwurf in der Fassung des Änderungsantrags der Koalitionsfraktionen der CDU/CSU und SPD auf Ausschussdrucksache 18(4)853neu mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktion BÜNDNIS 90/DIE GRÜNEN bei Stimmenthaltung der Fraktion DIE LINKE. anzunehmen.

III. Beratungsverlauf und Beratungsergebnisse im federführenden Ausschuss

Der **Innenausschuss** hat in seiner 112. Sitzung am 29. März 2017 den Gesetzentwurf abschließend beraten und empfiehlt mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktion BÜNDNIS 90/DIE GRÜNEN bei Stimmenthaltung der Fraktion DIE LINKE. die Annahme des Gesetzentwurfs in der Fassung des Änderungsantrags der Koalitionsfraktionen auf Ausschussdrucksache 18(4)853neu. Zuvor wurde der Änderungsantrag auf Ausschussdrucksache 18(4)853neu mit den Stimmen der Fraktionen der CDU/CSU, SPD und DIE LINKE. gegen die Stimmen der Fraktion BÜNDNIS 90/DIE GRÜNEN angenommen.

Zudem hat der Innenausschuss den Antrag der Koalitionsfraktionen auf Ausschussdrucksache 18(4)854 mit den Stimmen der Fraktionen der CDU/CSU, SPD und DIE LINKE. gegen die Stimmen der Fraktion BÜNDNIS 90/DIE GRÜNEN angenommen. Der Antrag der Fraktionen der CDU/CSU und der SPD für den Innenausschuss des Deutschen Bundestages zur Stärkung der IT-Sicherheit internetfähiger Geräte lautet:

– Der Innenausschuss des Deutschen Bundestages stellt fest:

Aktuelle IT-Sicherheitsvorfälle haben gezeigt, dass von sämtlichen an das Internet angeschlossenen Geräten durch Angriffe von außen Gefahren ausgehen können, die beträchtliche Auswirkungen auf die Funktionsfähigkeit der Geräte selbst sowie auf die Verfügbarkeit von Telekommunikationsnetzen und ihrer Dienste entfalten können. Die Anzahl von automatisierten Schadprogrammen, die ohne Wissen des Nutzers an das Internet angeschlossene Geräte infizieren und unter fremde Kontrolle bringen können, steigt stetig. Derartige Angriffe hatten in der jüngeren Vergangenheit zur Folge, dass mehrere hunderttausend Nutzer ihren Internetzugang teilweise mehrere Tage nur eingeschränkt oder gar nicht nutzen konnten. Diese Bedrohung wird sich künftig dadurch noch verstärken, dass immer mehr Geräte an das Internet angeschlossen werden. Nach Schätzungen werden bis zum Jahr 2020 ca. 20 bis 50 Milliarden Geräte über das Internet miteinander vernetzt sein.

Der Innenausschuss des Deutschen Bundestages hält es deshalb für erforderlich, hier zeitnah ein Maßnahmenpaket zur Erhöhung der IT-Sicherheit zu beschließen. Zum einen sollen Befugnisse für die Anbieter von Telekommunikationsdiensten in das Telekommunikationsgesetz aufgenommen werden, die die Erkennung und Behebung derartiger Sicherheitsvorfälle ermöglichen. Zum anderen ist es unabdingbar, die IT-Sicherheit internetfähiger Geräte zu erhöhen.

Auf nationaler Ebene soll die IT-Sicherheit durch Schaffung von Transparenz über das Sicherheitsniveau von internetfähigen Geräten für die Verbraucher durch die Entwicklung eines Gütesiegels für IT-Sicherheitseigenschaften gestärkt werden. So würden die IT-Sicherheitseigenschaften von internetfähigen Geräten klar erkennbar gekennzeichnet und der Verbraucher in die Lage versetzt, sich bei einem Kauf bewusst für Produkte mit einem erhöhten IT-Sicherheitsniveau zu entscheiden. Die freiwillige Verwendung von Gütesiegeln ist rechtlich grundsätzlich zulässig. Bereits in der „Cyber-Sicherheitsstrategie für Deutschland 2016“ hat die Bundesregierung angekündigt, ihre Aktivitäten auf dem Gebiet der Gütesiegel und Zertifikate für IT-Sicherheit auszubauen und - insbesondere hinsichtlich übergreifender Systeme für die Zertifizierung sowie einer einheitlichen Kennung - geeignete Vorschläge zu unterbreiten. Die Anwender sollen künftig auf Basis eines einheitlichen Gütesiegels bei der Kaufentscheidung für neue IT-Produkte und bei der Inanspruchnahme entsprechender Dienstleistungen leicht und schnell feststellen können, welches Angebot sicher ausgestaltet ist und hierdurch zum Schutz der Daten beiträgt.

Die Rechtsvorschriften über die Bereitstellung von internetfähigen Produkten auf dem Unionsmarkt sind europarechtlich harmonisiert. Da hier kein Spielraum für den nationalen Gesetzgeber in Bezug auf zusätzliche Anforderungen an derartige Geräte besteht, können entsprechende Regelungen für internetfähige Produkte nur auf EU-Ebene geschaffen werden. Der Innenausschuss des Deutschen Bundestages ist der Auffassung, dass die derzeitigen europarechtlichen Regelungen nicht ausreichend sind. Die grundlegenden Anforderungen, die internetfähige Geräte zum Zeitpunkt ihres Inverkehrbringens erfüllen müssen, sollten daher um IT-Sicherheitseigenschaften ergänzt werden und somit Voraussetzung für den Marktzugang sein.

– Der Innenausschuss des Deutschen Bundestages fordert die Bundesregierung auf,

  – das in der „Cyber-Sicherheitsstrategie für Deutschland 2016“ angekündigte Gütesiegel für IT-Sicherheit unter Einbeziehung von Verbraucherschützern, Wirtschaftsvertretern, IT-Sicherheitsexperten und Gewerkschaften auszuarbeiten. Dazu sollte das Bundesamt für Sicherheit in der Informationstechnik (BSI) Technische Richtlinien mit IT-Sicherheitsmindestanforderungen für relevante Produktklassen veröffentlichen, nach der Hersteller ihre Produkte überprüfen lassen oder gegen die sie sich erklären können. Produkte, die diesen Vorgaben entsprechen, sollen mit einem „IT-Sicherheits-Gütesiegel“ des BSI versehen werden können;

  – sich auf EU-Ebene dafür einzusetzen, dass verbindliche Anforderungen an IT-Sicherheitseigenschaften für die Bereitstellung auf dem Markt von internetfähigen Produkten auf europäischer Ebene geschaffen werden.

IV. Begründung

1. Zur Begründung allgemein wird auf **Drucksachen 18/11242, 18/11620** verwiesen. Die vom Innenausschuss vorgenommenen Änderungen auf Grundlage des Änderungsantrags der Koalitionsfraktionen auf Ausschussdrucksache 18(4)853neu begründen sich wie folgt:

Die Gesetzesänderungen dienen der Stärkung der IT- und Telekommunikationssicherheit. Sie erweitern die bestehenden Vorschriften im Telekommunikationsgesetz um Befugnisse der Anbieter von Telekommunikationsdiensten, um auf Störungen reagieren und damit die IT-Sicherheit netzseitig verbessern zu können.

Zusätzlich soll die IT-Sicherheit durch Schaffung von Transparenz über das Sicherheitsniveau von internetfähigen Geräten für die Verbraucher gestärkt werden. Dazu soll entsprechend dem Antrag der Fraktionen der CDU/CSU und der SPD für den Innenausschuss des Deutschen Bundestages vom 28. März 2017 zur Stärkung der IT-Sicherheit internetfähiger Geräte ein Gütesiegel für IT-Sicherheitseigenschaften entwickelt werden. So könnten die hiermit bestätigten IT-Sicherheitseigenschaften von internetfähigen Geräten für den Verbraucher klar erkennbar gekennzeichnet und so der Verbraucher in die Lage versetzt wird, bewusstere Kaufentscheidungen zu treffen.

Die freiwillige Verwendung von Gütesiegeln ist rechtlich grundsätzlich zulässig und erfordert keine gesetzliche Regelung. Die Bundesregierung wird nach bewährten Verfahren, z. B. im Rahmen von Anhörungen, unter Einbeziehung von Verbraucherschützern, Wirtschaftsvertretern und Gewerkschaften, technische IT-Sicherheitsmindestanforderungen für relevante Produktklassen entwickeln, das Bundesamt für Sicherheit in der Informationstechnik darauf aufbauend eine Technische Richtlinie verfassen, nach der Hersteller ihre Produkte bei vom Bundesamt für Sicherheit in der Informationstechnik (BSI) anerkannten Stellen überprüfen lassen können. Produkte, die diesen Vorgaben entsprechen, können dann mit einem „IT-Sicherheits-Gütesiegel“ versehen werden und so einfach nach außen sichtbar belegen, dass sie die Anforderungen der jeweiligen Technischen Richtlinie erfüllen.

Verbindliche Anforderungen an IT-Sicherheitseigenschaften für das Inverkehrbringen von Produkten können grundsätzlich auf europäischer Ebene erreicht werden. Daher wird in dem Antrag der Fraktionen der CDU/CSU und der SPD für den Innenausschuss des Deutschen Bundestages vom 28. März 2017 zur Stärkung der IT-Sicherheit internetfähiger Geräte angestrebt, dass sich die Bundesregierung hier aktiv für die Aufnahme von derartigen verbindlichen grundlegenden Anforderungen an die IT-Sicherheitseigenschaften für die Bereitstellung auf dem Markt von internetfähigen Geräten einsetzen wird.

Zu Nummer 1

Buchstabe a)

Die Befugnis des Diensteanbieters, für den Umgang mit Störungen Daten zu erheben und verwenden, wird um Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung erweitert. Je nach Angriffsart oder -durchführung sind dazu unterschiedliche Daten notwendig. Da die Schadfunktionen zumeist nicht Bestandteil der Verkehrsdaten (insbesondere sog. IP-Header) sind, kann es erforderlich sein, neben Verkehrsdaten auch weitere Daten zu untersuchen. Hierbei geht es um Teile der Protokolle, also um Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind. Es handelt sich um Informationen, die sich aus den verschiedenen Layern des sogenannten OSI-Schichtenmodels der ITU ergeben, also um Informationen zu technischen Übertragungsprotokollen, nicht jedoch um Inhalte eines Kommunikationsvorganges, die damit übertragen werden. Sofern die Datenübertragung zugleich einen Telekommunikationsvorgang darstellt (z. B. das Senden einer E-Mail), sind die Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung zugleich Verkehrsdaten im Sinne des gemäß § 3 Nummer 30 TKG.

Buchstabe b)

Es handelt sich um eine Klarstellung, dass es nur um die technischen Informationen der Protokolle geht und die Kommunikationsinhalte damit nicht Bestandteil der Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung sind.

Buchstabe c)

Die Datenerhebung und -verwendung zur Beseitigung der Störung ist vom Diensteanbieter auf ein Minimum zu beschränken. Sobald der Zweck erreicht wurde, sind die Daten unverzüglich zu löschen. Die Datenerhebung und -verwendung erfolgt grundsätzlich automatisiert. Soweit die Daten nicht automatisiert erhoben und verwendet werden, ist der betriebliche Datenschutzbeauftragte zum Schutz der betroffenen Personen unverzüglich detailliert über die Verfahren und Umstände der Maßnahme zu informieren.

Darüber hinaus wird eine datenschutzrechtliche Aufsicht durch eine Berichtspflicht an die Bundesnetzagentur und den betrieblichen Datenschutzbeauftragten und an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sichergestellt. Darüber hinaus sind die Information des Bundesamts für Sicherheit in der Informationstechnik und die Benachrichtigung des Betroffenen vorgesehen. Außerdem unterliegen die Vorgänge grundsätzlich einer Vorabkontrolle nach § 4d Absatz 5 und 6 BDSG.

Die Vorgaben nach § 108 TKG zur Gewährleistung von Notrufverbindungen bleiben hiervon unberührt. Der Diensteanbieter hat insbesondere weiterhin gemäß § 108 Absatz 1 Satz 2 alle erforderlichen Maßnahmen zu treffen, damit Notrufverbindungen jederzeit möglich sind.

Zu Nummer 2

Die Änderungen von Absatz 5 dienen der Verbesserung des Meldeverfahrens bei Beeinträchtigungen von Telekommunikationsnetzen und -diensten. Betreiber öffentlicher Telekommunikationsnetze und Erbringer öffentlich zugänglicher Telekommunikationsdienste sind zukünftig dazu verpflichtet, Beeinträchtigungen neben der Bundesnetzagentur auch dem Bundesamt für Sicherheit in der Informationstechnik mitzuteilen.

Mit der Änderung in Buchstabe c wird der Verweis auf Vorschriften des BSIG angepasst (Folgeänderung aufgrund Neunummerierung im BSIG).

Zu Nummer 3

Buchstabe a)

Der neue Absatz 4 Satz 3 dient insbesondere dem Schutz der Telekommunikations- und Datenverarbeitungssysteme des Nutzers. Hierzu wird dem Diensteanbieter erlaubt, Teile des Datenverkehrs von und zu einem Nutzer, von denen eine Störung ausgeht, zum Zwecke der Information der Nutzer umzuleiten (sog. „Sinkholing“). Durch die Umleitung innerhalb der eigenen Netze kann der Diensteanbieter den Nutzer, dessen Systeme von einer Schadsoftware befallen sind, zunächst identifizieren und ihn anschließend in die Lage versetzen, die Störung zu beseitigen. Dies kann z.B. über Warnseiten erfolgen, die Informationen nach Absatz 4 Satz 2 enthalten.

Buchstabe b)

Der neue Absatz 5 erlaubt es dem Diensteanbieter, den Datenverkehr bei Vorliegen einer Störung einzuschränken, umzuleiten oder zu unterbinden. Die Regelung dient dem Schutz der Telekommunikations- und Datenverarbeitungssysteme des Diensteanbieters, des Nutzers im Sinne von Absatz 4 und anderer Nutzer vor Beeinträchtigungen. Der Diensteanbieter darf von dieser Befugnis unter den Voraussetzungen Gebrauch machen, dass er den Nutzer bereits über eine bestehende Störung nach Absatz 4 Satz 1 TKG informiert hat und dieser die Störung nicht unverzüglich selbst beseitigt hat oder eine unverzügliche Beseitigung durch den Nutzer nicht zu erwarten ist und der Eingriff in die Nutzung des Telekommunikationsdienstes zur Beseitigung oder zur Verhinderung der Beeinträchtigung erforderlich ist. Eine unverzügliche Beseitigung durch den Nutzer ist insbesondere dann nicht zu erwarten, wenn der Nutzer technisch gar nicht von dem Diensteanbieter benachrichtigt werden kann, z.B. weil die Störung von netzseitig nicht identifizierbaren „IoT-Geräten“ (sog. „Internet-of-Things-Geräten“) des Nutzers ausgeht. Diese Erlaubnis des Diensteanbieters ist insbesondere für Fälle erforderlich, in welchen der Nutzer seine Telekommunikations- und Datenverarbeitungssysteme nicht selbst von Schadsoftware bereinigt. Bleiben diese Teil eines Botnetzes und sind mit dem Telekommunikationsnetz verbunden, können sie als Werkzeug für Angriffe auf fremde Systeme missbraucht werden.

Darüber hinaus wird dem Diensteanbieter erlaubt, den Datenverkehr zu filtern, um Gefahren, insbesondere für die Verfügbarkeit von Informations- und Kommunikationsdiensten durch Cyber-Angriffe abzuwehren. Hierbei wird legitime Kommunikation von maliziöser Kommunikation getrennt.

Der neue Absatz 6 erlaubt es dem Diensteanbieter, den Datenverkehr zu Störungsquellen einzuschränken oder zu unterbinden, um die Entstehung von Störungen in den Telekommunikations- und Datenverarbeitungssystemen der Nutzer zu vermeiden. Diese Befugnis ist erforderlich, weil Angreifer in der Regel modulare Angriffswerkzeuge nutzen, um Telekommunikations- und Datenverarbeitungssysteme zu infizieren. Hierzu werden Systeme des Nutzers regelmäßig zunächst mit einem sogenannten Dropper (z. B. E Mail-Anhang) infiziert, der von Servern der Angreifer weitere Teile des Schadprogrammes nachlädt, die den eigentlichen Schadteil enthalten. Dieses Nachladen lässt sich netzseitig verhindern, indem der Zugriff auf die Server der Angreifer unterbunden wird. Störungsquellen, zu denen die Kommunikation unterbunden werden darf, sind beispielsweise Command and Control-Server, Dropzones, in die gestohlene Daten ausgeleitet werden, oder Server, über die Schadsoftware verteilt wird.

Die Vorgaben nach § 108 TKG zur Gewährleistung von Notrufverbindungen bleiben von den Maßnahmen auf Grundlage des § 109a unberührt. Der Diensteanbieter hat insbesondere weiterhin gemäß § 108 Absatz 1 Satz 2 alle erforderlichen Maßnahmen zu treffen, damit Notrufverbindungen jederzeit möglich sind.

Buchstabe c)

Es handelt sich um eine Folgeänderung.

Zu Nummer 4

Die Erweiterung der Ordnungswidrigkeitentatbestände in § 149 um die nicht oder nicht rechtzeitige Löschung der erhobenen Daten in Nummer 17c und Nutzung zu anderen Zwecken in Nummer 17d und Verschiebung der bisherigen Nummer 17c sind Folgeänderungen zur Änderung von § 100 Absatz 1 TKG.

2. Die **Koalitionsfraktionen der CDU/CSU und SPD** betonen, Deutschland hätte gerade im europäischen Vergleich bei der Erhöhung der Cybersicherheit insbesondere mit der Verabschiedung des IT-Sicherheitsgesetzes bereits viel erreicht. Wegen der deutschen Vorreiterrolle bei der IT-Sicherheit seien inhaltlich nur kleinere Anpassungen durch die NIS-Richtlinie notwendig. Grundsätzlich könne in dem sich ständig wandelnden Bereich der Cybersicherheit kein endgültiges gesetzgeberisches Niveau geschaffen werden; auch in Zukunft werde es im Zuge der Fortentwicklung der Technik notwendig bleiben, die Rechtslage zu prüfen und auf sich in der Zukunft ergebende, neue Bedrohungslagen wie etwa die Sicherheit des „Internet of Things“ (IOT) zu reagieren. Richtigerweise werde durch den Gesetzentwurf das Bundesamt für die Sicherheit in der Informationstechnik (BSI) gestärkt. Bei der Frage der Einführung eines Gütesiegels im Rahmen der europarechtlichen Vorgaben verbleibe dem nationalen Gesetzgeber jedoch kaum Handlungsspielraum. Trotzdem werde an diesem Ziel festgehalten. Der Zusatzantrag verdeutliche dies. Sicherheit könne nur durch ein vernünftiges Nutzerverhalten erreicht werden, das bereits bei der Auswahl der Geräte in den Blick genommen werden müsse. Insgesamt sei deshalb der Gesetzentwurf ein weiterer wichtiger Schritt im Kampf gegen die Bedrohung durch Cyberkriminalität.

Die **Fraktion DIE LINKE.** kündigt an, sich trotz der zweifellos bestehenden Notwendigkeit gesetzgeberischen Handelns im Bereich der Cybersicherheit bei diesem Gesetzentwurf zu enthalten. Die durch die Koalitionsfraktionen angestrebte Methodik über Zertifizierungen, Gütesiegel und kooperatives Zusammenwirken genüge nicht. Notwendig wären regulatorische Verabredungen zwischen Herstellern und Betreibern. Auch die Schwelle der „erheblichen Sicherheitsvorfälle“, ab denen Mitteilungen stattfinden müssten, sei nur unspezifisch bestimmt und biete dementsprechend Ausweich- oder Umgehungsmöglichkeiten. Dem Änderungsantrag und Antrag der Koalitionsfraktionen werde zugestimmt, weil die Datenerhebung aus Sicht der Nutzerinnen und Nutzer begrüßt werde. Es müsse aber sichergestellt werden, dass diese Daten nicht an Sicherheitsbehörden weitergegeben würden.

Die **Fraktion BÜNDNIS 90/DIE GRÜNEN** lehnt den Gesetzentwurf ab. Bereits die Verabschiedung des IT-Sicherheitsgesetzes vor der europäischen Richtlinie sei kritisch zu sehen gewesen. Nunmehr gebe es zwei nicht vollständig kohärente Regelungen, deren nach kurzer Zeit wieder erforderliche Anpassung einen unnötigen Aufwand insbesondere für die Wirtschaft bedeute. Grundsätzlich werde die NIS-Richtlinie nicht ausreichend umgesetzt, verfahrens- und datenschutzrechtliche Probleme bestünden fort. Die Ansiedlung des BSI beim Bundesministerium des Innern sei äußerst problematisch, da das der Fachaufsicht des BMI unterstehende Bundesamt für Verfassungsschutz enorme Gelder für die Aufdeckung von Sicherheitslücken erhalte, während die Wirtschaft verpflichtet werde, dem BSI die eigenen entdeckten Sicherheitslücken zu melden. So fehle eine Vertrauensbasis für Unternehmen, um sich im Schadensfall an das BSI zu wenden. Auch sei mangelhaft, nach wie vor keine

verschärften Haftungsregelungen einzuführen, um die Betreiber kritischer Infrastrukturen zu größeren Investitionen in die IT-Sicherheit zu zwingen. Auf Freiwilligkeit zu setzen sei hier der falsche Weg. Schließlich sei das parlamentarische Verfahren auch wegen eines erst am Vorabend vorgelegten Änderungsantrages von weitreichender Bedeutung mindestens fragwürdig.

Berlin, den 29. März 2017

Clemens Binninger	**Gerold Reichenbach**	**Martina Renner**	**Dr. Konstantin von Notz**
Berichterstatter	Berichterstatter	Berichterstatterin	Berichterstatter

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, 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 0722-8333