IT-Sicherheit und Telekommunikationsrecht: Die nächste Runde des Gesetzgebers

Stand: 15.11.2017

Inhalt

Ingo Ruhmann, Ute Bernhardt
Elchdamm 56a, 13503 Berlin
030-28046695
<ruhmann><bernhardt>@netzwerk-datenschutzexpertise.de
www.netzwerk-datenschutzexpertise.de

Das Netzwerk Datenschutzexpertise hatte im Zuge der Beratungen zum IT-Sicherheitsgesetz verschiedene Kritikpunkte formuliert, die aber bei der Umsetzung des Gesetzgebungsvorhabens nicht aufgegriffen wurden. In den wenigen Monaten seit Inkrafttreten des Gesetzes sind weitere Gesetzesänderungen beschlossen worden, die einige der Kritikpunkte aufgreifen. Das Netzwerk Datenschutzexpertise aktualisiert daher seine Bewertung der Gesetzeslage zur IT-Sicherheit und deren datenschutzkonformer Umsetzbarkeit.

Seit den Regelungen im Bundesdatenschutzgesetz wurde die Absicherung von IT-Systemen gegen Missbrauch in einer zunehmenden Zahl von Gesetzen geregelt. Mit dem IT-Sicherheitsgesetz (ITSiG) sollten die Schutzvorschriften auf weitere Anwendungsbereiche ausgeweitet und modernisiert werden. Im Verlauf der Beratungen zum ITSiG hatte das Netzwerk Datenschutzexpertise die für die Praxis der IT-Sicherheit widersprüchliche Rechtslage kritisiert.[1] Weder gibt es einheitliche Rechtsbegriffe noch einen übergreifenden Rahmen für die Bewertung von Risiken und Maßnahmen.

Die Befugnisse zur Verarbeitung sensibler Daten bei Sicherheitsvorfällen sind zudem an den extremen Enden des Spektrums angesiedelt: So untersagen an einem Ende dieses Spektrums die bestehenden Regelungen des deutschen Telemediengesetzes (TMG) den Anbietern von Web-Services weitgehend eine Datenerhebung zur Behandlung von IT-Sicherheitsvorfällen. Parallel zum Gesetzgebungsverfahren hat der EuGH die vom Netzwerk kritisierte Vorschrift im TMG zwar als unvereinbar mit EU-Recht erklärt[2], geändert wurde die deutsche Rechtslage hierzu aber bislang nicht.

Die deutlich weiter gehende Kritik des Netzwerks[3] bezog sich auf das andere Ende des Spektrums der Datenverarbeitung: In das Telekommunikationsgesetz (TKG) wurde durch das ITSiG ein Passus eingeführt, der es in das Belieben der Telekommunikationsprovider stellte, eine unbegrenzte, flächendeckende und an keine Auflage geknüpfte Vorratsdatenspeicherung vorzunehmen, um Störern - möglichen Verbreitern von Schadsoftware - auf die Spur zu kommen. Dazu wurden der § 100 TKG verändert und das TKG um einen neuen § 109a ergänzt. Letzterer hatte nominell zum Ziel, die Verursacher von Störungen zu informieren und zur Abhilfe aufzufordern, war jedoch so formuliert, dass er diesem Ziel nicht gerecht wird.

Das Netzwerk und der Informatiker-Verband FIfF e.V.[4] hatten die mit § 100 TKG eingeführte Möglichkeit des unbegrenzten Eingriffes in das Fernmeldegeheimnis mit einer detaillierten Begründung als grob verfassungs- und EU-rechtswidrig bewertet. In der Anhörung des Bundestags

[1] Ingo Ruhmann, Ute Bernhardt: IT-Sicherheit, das EU-Recht und die Grundrechte: Neustart erforderlich; Mai 2016, http://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_eugh-itsig-2016.pdf
[2] Urteil des Gerichtshofes in der Rechtssache C582/14 vom 19.10.2016, Beschlussgrund Nr. 2, Rd.-Nr. 65. http://curia.europa.eu/juris/document/document.jsf?docid=184668&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=DE&cid=1065466
[3] Eingehend dazu: Ingo Ruhmann, Ute Bernhardt: Der EuGH-Entscheid als Anstoß für mehr Rechtssicherheit in der IT-Sicherheit; in: DuD, Heft 1, 2017, S. 34-38, https://link.springer.com/content/pdf/10.1007%2Fs11623-017-0722-2.pdf
[4] Stellungnahme des FIfF e.V. zum Entwurf des IT-Sicherheitsgesetzes, vorgelegt zur Anhörung des Innenausschusses des Deutschen Bundestages am 20.04.2015, https://www.bundestag.de/blob/366560/22f1e6ca62f137b23349c02ab6b2ec14/18-4-252-data.pdf

teilten die geladenen Verfassungsrechtler diese Bewertung.[5] Der Bundestag ließ das ITSiG Ende 2015 trotzdem unverändert passieren.

Bei den Beratungen 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“ kam es gegen Ende der 18. Legislaturperiode im Frühsommer 2017 dann zu einer unerwarteten Entwicklung. In der parlamentarischen Beratung wurde der von der Bundesregierung vorgelegte Gesetzentwurf[6] vom federführenden Innenausschuss gezielt verändert und ergänzt.[7] Die Änderungen der §§ 100 und 109a TKG sind als Versuch der Parlamentarier zu werten, die kurz zuvor eingeführten verfassungswidrigen Verschärfungen abzumildern und Kritikpunkte aufzugreifen.

1 Veränderung des §100 TKG

Bis 2015 hatte der § 100 TKG folgende Fassung:

> „(1) Soweit erforderlich, darf der Diensteanbieter zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden“.

Das Netzwerk hatte diesen, aus der Zeit der analogen Telefonie stammenden Passus als durch die Möglichkeiten digitaler Netze nicht mehr grundrechtskonform bezeichnet, bezog die wesentliche Kritik aber auf die Neufassung dieses Absatzes.

1.1 Bisherige Kritik des Netzwerks

Mit dem ITSiG[8] erhielt §100 (1) TKG Mitte 2015 folgende neue Fassung:

> „(1) Soweit erforderlich, darf der Diensteanbieter die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. Dies gilt auch für Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können.“

[5] Wortprotokoll der Öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), 20.04.2015, v. a. S. 19, 29, 46f.

[6] Gesetzentwurf der Bundesregierung: 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, Bt.-Drs. 18/11242 vom 20.02.2017

[7] 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, Bt.-Drs. 18/11808 vom 30.03.2017

[8] Bundesgesetzblatt Jahrgang 2015 Teil I Nr. 31, vom 24. Juli 2015

Die Kritik des Netzwerks Datenschutzexpertise entzündete sich daran, dass die bis dato geltenden Befugnisse zur Störungsmessung im Falle einer *konkret bekannten* Störung ausgeweitet wurden auf die Vorfeldkontrolle von Störungen, die zu Leistungseinschränkungen „führen *können*“, ohne dazu bereits geführt zu haben. Als Anlässe für die Datenerhebung wurden mögliche Störungen der „Verfügbarkeit“ nicht näher spezifizierter „Informations- und Kommunikationsdienste“ und der Schutz vor einem „unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer“ genannt. Das Netzwerk wies darauf hin, dass mit dem Bezug auf die Nutzer gemäß TKG nicht die Kunden eines Anbieters sondern nach § 3 Nr. 14 TKG beliebige Beteiligte an Telekommunikationsvorgängen adressiert werden. Ohne ein Vertragsverhältnis und darauf aufbauendem Nutzungsprofil kann ein Provider bei diesen Nutzern keine spezifische, zulässige Dienstenutzung erkennen. Es gibt für Provider somit auch keine Möglichkeit zur Entscheidung über eine mögliche Störung der Verfügbarkeit oder gar eines „unerlaubten Zugriffs“ auf IT-Systeme von Nutzern.

Im starken Kontrast zu dieser Unbestimmtheit wurde eine ganz erhebliche Eingriffstiefe in Telekommunikationsvorgänge zugelassen. Wie von Virenscannern bekannt, ist es für eine Erkennung einer potenziellen „Störung“, einer „Einschränkung der Verfügbarkeit“ oder „unerlaubter Zugriffe“ erforderlich, den Inhalt einer Datenkommunikation einer genauen Analyse zu unterziehen, um möglichen Schadcode von einer legitimen Datenkommunikation unterscheiden zu können. Erlaubt wurde hier also eine „deep packet inspection“.

Schließlich fehlte dem mit dem ITSiG verabschiedeten § 100 (1) TKG jegliche Regelung zur Nutzung der gewonnenen Daten. Internet- und Telekommunikationsprovidern wurde erlaubt, ohne jede Einschränkung Daten zu sammeln, auszuwerten, zu speichern und ggf. auch weiterzugeben, um mögliche Störungen zu erkennen.

1.2 Erneute Neufassung

Dass ein solcher unbegrenzter Eingriff in das Fernmeldegeheimnis zur Erkennung nicht einmal konkret vorhandener Störer mit der Verfassung nicht in Einklang gebracht werden kann, scheint für die Parlamentarier Anlass gewesen zu sein, einige der gröbsten Rechtswidrigkeiten zu überarbeiten.

Der Innenausschuss postulierte in seiner Begründung zur Änderung des Regierungsentwurfes des „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“, dass beim § 100 TKG die „Datenerhebung und -verwendung zur Beseitigung der Störung vom Diensteanbieter auf ein Minimum zu beschränken“ sei und führte eine vorher nicht vorhandene Aufsicht durch Datenschutzbeauftragte ein. Insbesondere zielte der Innenausschuss auf die Klarstellung ab, „dass es nur um die technischen Informationen der Protokolle geht und die Kommunikationsinhalte damit nicht Bestandteil der Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung sind“.[9]

Mit diesen Änderungen verabschiedete der Bundestag vor Ende der Legislaturperiode Mitte 2017 die Novelle. Danach hat das TKG nun folgende Fassung[10]:

[9] Bt.-Drs 18/11808, S. 9 f

[10] Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 40, vom 29. Juni 2017

> §100 „(1) Soweit erforderlich, darf der Diensteanbieter die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer 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, erheben und verwenden, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. Die Kommunikationsinhalte sind nicht Bestandteil der Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung. Dies gilt auch für Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können. 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.“

1.3 Würdigung der Änderungen

Gemäß der Begründung des Innenausschusses wurde die Befugnis der Datenerhebung für Provider nicht begrenzt, sondern um die Klasse der „Steuerdaten“ ergänzt. Diese im TKG nicht definierte neue Klasse von Daten wird so umschrieben, dass darin unschwer die Signalisierungsdaten der diversen Kommunikationsprotokolle zu erkennen sind. Im Regelungstext schließt sich an diese Umschreibung erläuternd an, dass die „Kommunikationsinhalte nicht Bestandteil der Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung“ sind.

Dies wirft die Frage auf, an welche Kommunikationsprotokolle der Bundestag hierbei gedacht hatte. Da derzeit die gesamte kabelgebundene Netzkommunikation in Deutschland auf „all-IP-Netze“, also auf die Internet-Kommunikationsprotokolle TCP/IP[11] umgestellt wird, wäre naheliegend, dies als Hintergrund anzunehmen, zumal IT-Sicherheitsvorfälle hauptsächlich mit der TCP/IP-Kommunikation in Verbindung gebracht werden. Dem IP-Standard entsprechend, wird jede Kommunikation in Datenpakete zerlegt, von denen jedes Paket zugleich Steuerungsdaten und Kommunikationsinhalte enthält. Die TCP/IP-Kommunikation lässt keine Datenübermittlung zu, bei der die Steuerdaten „unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen“ werden. Die Neuregelung ist daher auf TCP/IP nicht anwendbar. Anders ist dies bei Mobilfunkkommunikationsprotokollen. Alle genutzten Kommunikationsprotokolle benötigen zur Signalisierung und Abstimmung zwischen Mobil-

[11] Das Transmission Control Protocol (TCP) basiert auf dem RFC 793: https://tools.ietf.org/html/rfc793, das Internet Protocol (IP) auf dem RFC 791: https://tools.ietf.org/html/rfc791

und Basisstation zahlreiche Datenübermittlungen, für die zudem gesonderte Kommunikationskanäle der Provider genutzt werden. Bei der Mobilkommunikation ist also eine von Kommunikationsinhalten getrennte Übermittlung von Steuerdaten die Voraussetzung für einen Kommunikationsvorgang. Nutzer haben in aller Regel keinen Zugang zu den Kommunikationskanälen für Steuerdaten. Störungen gehen hier also nicht von Nutzern, sondern – abgesehen von fehlerhaftem Gerät – ganz klassisch von den beteiligten Providern aus, die für Abhilfe sorgen müssen.

Auch wird der rechtliche Widersinn zwischen den Kundendaten und den Nutzerdaten nicht aufgelöst: „Bestandsdaten“ kann ein Provider nur von seinen Kunden, nicht aber zu beliebigen Nutzern haben. „Verkehrsdaten" sind nach § 3 Nr. 30 TKG wiederum alle „Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden“, also neben den Daten der Kommunikationsprotokolle insbesondere auch die übermittelten Inhalte des Telekommunikationsvorgangs.

Daraus folgt, dass es – anders als die Begründung vermuten lässt – bei dieser Neufassung um die Umschreibung einer weiteren Klasse von Daten geht, die neben den Verkehrs- und Bestandsdaten zur Erkennung von Störungen zwischen Providern gesammelt werden dürfen und die grundsätzlich von der bisherigen Regelung bereits abgedeckt war. Zugleich bewirkt diese Ergänzung für die von Nutzern verursachten IT-Sicherheitsprobleme allenfalls bei ungewöhnlichen Konstellationen eine Verbesserung.

Die reale Verbesserung liegt in neuen Regelungen zur Datennutzung. Der Gesetzgeber geht vom Regelfall einer automatisierten Datenverarbeitung aus, verbietet eine Nutzung zu anderen Zwecken ohne Ausnahme und schreibt eine umgehende Löschung der gewonnenen Daten vor. Sofern eine nicht-automatisierte Auswertung erfolgt, ist den zuständigen Datenschutzkontrollinstanzen Bericht zu erstatten sowie, – wenn es möglich ist, den dem Provider ja nach Definition des TKG unbekannten Nutzer zu ermitteln – auch den von der Datenspeicherung Betroffenen.

Trotz der Nachbesserung mit einem neuen Verbot einer anderweitigen Nutzung der gewonnenen Daten und einer ex-post-Kontrolle ist festzuhalten, dass weiterhin auf den bloßen Verdacht einer möglichen Störung hin in das Fernmeldegeheimnis eingegriffen werden darf, ohne die für einen solchen Grundrechtseingriff erforderlichen angemessenen Voraussetzungen und ohne richterliche Prüfung. Auch nach der jüngsten Gesetzesänderung bleibt diese Regelung zur IT-Sicherheit im TKG Grundgesetz- und EU-rechtswidrig.

2 Änderungen an § 109a TKG: von der Mitteilungspflicht zur Manipulation des Datenverkehrs

Der §109a TKG war mit dem unstreitig sinnvollen Zweck eingeführt worden, zu verhindern, dass Telekommunikationsprovider IT-Sicherheitsvorfälle und das Erbeuten von personenbezogenen Daten geheim halten. Um dem entgegenzuwirken, schreibt der § 109a (1) TKG vor, Bundesnetzagentur und Datenschutzkontrollinstanzen sowie die Betroffenen über Vorfälle zu informieren. Zusätzlich wurde in § 109a (4) TKG geregelt, (wiederum) Nutzer über Störungen, die von ihren IT-Systemen ausgehen, über diese und mögliche Abhilfen zu informieren.

2.1 Bisherige Kritik des Netzwerks

Das Netzwerk Datenschutzexpertise hatte bemängelt, dass erstens die Nutzer im Sinne des TKG dem Provider unbekannt und nicht für Benachrichtigungen adressierbar sind und zweitens bei Störungen davon ausgegangen werden muss, dass das störende IT-System nicht mehr unter Kontrolle des rechtmäßigen Betreibers ist, sondern unter der eines Angreifers, den eine Benachrichtigung nicht interessieren dürfte. Es hätte stattdessen im Interesse der IT-Sicherheit und der Provider einer Regelung bedurft, die die Weitergabe der Information nicht an den Nutzer, sondern an jenen Rechenzentrumsbetreiber erlaubt hätte, in dessen Räumen das Störungen aussendende IT-System untergebracht ist. Denn nach gültiger Rechtslage erfüllt die Weitergabe der Daten eines Störers an Dritte den Straftatbestand des Bruches des Fernmeldegeheimnisses (§ 206 StGB) für jeden bei einem Provider tätigen IT-Sicherheitsexperten[12].

2.2 Änderungen und Ergänzungen

Der Innenausschuss änderte im § 109a TKG an der kritisierten Benachrichtigungspflicht nichts, ergänzte jedoch mehrere Detailregelungen zur Manipulation des Datenverkehrs eines Providers im Verhältnis zu seinen Kunden.

Danach erhielt der § 109a (4ff) folgende ergänzte Fassung[13]:

> „(4) Werden dem Diensteanbieter nach Absatz 1 Störungen bekannt, die von Datenverarbeitungssystemen der Nutzer ausgehen, so hat er die Nutzer, soweit ihm diese bereits bekannt sind, unverzüglich darüber zu benachrichtigen. Soweit technisch möglich und zumutbar, hat er die Nutzer auf angemessene, wirksame und zugängliche technische Mittel hinzuweisen, mit denen sie diese Störungen erkennen und beseitigen können. *[Im Folgenden neu gefasst]* 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.
> (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.“

2.3 Würdigung

Neu geregelt wurde damit bei § 109a die Manipulation des Datenverkehrs bei IT-Sicherheitsvorfällen sowohl im Datenverkehr allgemein als auch gezielt zu Störern. Providern wird erlaubt, in

[12] Vgl. dazu Ingo Ruhmann, Ute Bernhardt: Der EuGH-Entscheid als Anstoß für mehr Rechtssicherheit in der IT-Sicherheit, a.a.O., S. 35f
[13] Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 40, vom 29. Juni 2017

- Abs. (4), die Kommunikation eines Schadcode aussendenden Servers eines Nutzers zu kappen und umzuleiten, bis die Störung beseitigt ist,
- Abs. (5), zum Schutz der eigenen Systeme jede Datenkommunikation ihrer Kunden einzuschränken, einzustellen bzw. gezielt zu unterbinden,
- Abs. (6), die Datenkommunikation mit störenden Instanzen wie etwa einem Command-and-Control-Server eines Botnetzes zu unterbinden.

Die Klärung der rechtlichen Befugnisse eines Telekommunikationsproviders bei IT-Schadensvorfällen ist hier im Grundsatz klar zu begrüßen. Auch die in Abs. (5) ermöglichte Abschaltung eines ganzen Dienstes zum Schutz der IT-Systeme des agierenden Providers oder von Nutzern kann als ultima ratio gerechtfertigt sein.

Aufmerksam macht jedoch die Begründung zu diesem Absatz, in der für diese Regelung eine weitere Möglichkeit formuliert wird: „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.*“[14] Danach ist der § 109a (5) TKG nicht allein als massive Abhilfemaßnahme im Notfall zu sehen. Die Trennung „legitimer“ von „maliziöser Kommunikation“ kann – je nach Dienst – als weitere Erlaubnis zur „deep packet inspection“ verstanden werden, um Datenpakete selektiv zu verarbeiten. Dies ist umso bedeutsamer, da als Grund für diese Eingriffe zwar immerhin eine konkrete Störung eines Telekommunikationsdienstes genannt ist, aber damit jedem Diensteanbieter jeder Art von Telekommunikation die Befugnis zur Filterung eingeräumt wird. Dass auch dies ohne ergänzende Schutzregelungen nicht mit Grundgesetz und EU-Recht vereinbar ist, sollte aus dem vorher Gesagten deutlich geworden sein.

Dass dies zudem auch aus Sicht der IT-Sicherheit nicht hinreichend ist, sei an einem Beispiel erklärt. Vor einiger Zeit waren bestimmte Router der Kunden der Deutsche Telekom AG von einer Störung bzw. Manipulation betroffen. Die Router bauten in schneller Folge zahlreiche Verbindungen zum Domain Server auf, sodass das Telekommunikationsnetz regional überlastet und in Folge lahmgelegt wurde.[15] Hier war es eine zielführende Maßnahme zur Behebung der Probleme, den Dienst einzuschränken bzw. einzustellen. Die Telekom hatte auch ihre Kunden über die Medien aufgefordert, ein Update zur Schadensbeseitigung einzuspielen, was den Kunden jedoch unmöglich wurde, solange ihr Netzzugang abgeschaltet blieb. Das Unternehmen hat dann selbst über dessen Servicezugang auf die Kundenrouter den Schaden nach und nach behoben.

Das Defizit der Neuregelung in § 109a (5) TKG besteht nun darin, angemessene Abhilfemaßnahmen des Providers gegenüber seinen Kunden vorzusehen. Denn wenn diese ohne einen Internetanschluss – allgemeiner: den Telekommunikationsdienst – bleiben, sind sie auch vielfach zur Abhilfe nicht in der Lage; die Abhilfe ist nur mit Hilfe des Providers möglich. Die reine Befugnis zur Abschaltung der

[14] 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, Bt.-Drs. 18/11808 vom 30.03.2017, S. 10, Hervorhebung d.A.

[15] Oliver Diedrich: Großstörung im Telekom-Netz, Heise News, 27.11.2016, https://www.heise.de/newsticker/meldung/Grossstoerung-im-Telekom-Netz-3505820.html

Kunden reicht also nicht aus, um Schäden zu beseitigen. Wer solche Regelungen trifft, muss auch die Mitwirkung der den Dienstezugang kontrollierenden Provider an der Problemlösung bei den Kunden vorschreiben.

3 Zusammenfassung

Der Bundestag hat zur Linderung der offensichtlichen Verfassungswidrigkeit der mit dem ITSiG eingeführten TKG-Regelungen zur IT-Sicherheit die bislang ungeregelte Datennutzung schärfer gefasst. Im Ergebnis der Änderungen sollen die nach § 100 (1) TKG erhebbaren Daten so schnell wie möglich gelöscht werden und dürfen zu anderen Zwecken nicht genutzt werden. Sie werden einer Kontrolle durch Datenschützer unterworfen. Zugleich wurden in § 109a TKG neue Möglichkeiten der Filterung von Telekommunikationsdaten ermöglicht und den Providern weitreichende Möglichkeiten zur Einschränkung des Datenverkehrs eingeräumt.

Unverändert wird mit diesen beiden TKG-Regelungen übermäßig in das Fernmeldegeheimnis eingegriffen.Statt, wie rechtlich erforderlich, nur aus dem konkreten Anlass einer schweren Straftat, wird der Eingriff hier allein auf einen vagen Verdacht hin ohne jeden Anlass und ohne jede richterliche Kontrolle ermöglicht Diese Regelungen bleiben daher verfassungswidrig.

Unverändert bleibt es für IT-Sicherheitsexperten bei getrennten Vorschriften zum Umgang mit IT-Sicherheitsvorfällen im Telekommunikations- und Telemedienrecht, obwohl ein EuGH-Urteil Änderungen erfordert. Unverändert bleibt es auch bei dem konkreten Risiko für IT-Sicherheitsverantwortliche, sich bei der Weitergabe von Daten zu IT-Sicherheitsvorfällen und Störungen strafbar zu machen.

Damit ist zu konstatieren, dass der Bundestag immerhin den ersten sich bietenden Anlass genutzt hat, einige der ganz erheblichen Mängel im deutschen Recht zur IT-Sicherheit zu verbessern. Fundamentale Defizite bleiben jedoch bestehen. Dies zu ändern, bleibt eine Aufgabe für die Parlamentarier der neuen Legislaturperiode.