Ute Bernhardt, Ingo Ruhmann

Beitrag zur Sommerakademie „Vertrauenswürdige IT-Infrastruktur – ein (un?)erreichbares Datenschutzziel“ am 31.08.2015 in Kiel

IT-Sicherheit nach dem neuen IT-Sicherheitsgesetz

Mit dem 2015 in Kraft getretenen IT-Sicherheitsgesetz soll dem technischen Schutz von IT-Systemen und dem Recht bei der Durchsetzung dieses Schutzes zu mehr Geltung verholfen werden. Eine kurze Bewertung zeigt auf, welche Schwerpunkte das neue Gesetz setzt und welche rechtlichen und praktischen Aspekte der IT-Sicherheit weiterhin auf eine Lösung warten.

Das Bundesverfassungsgericht erhob 2008 die „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ zum Grundrecht[1]. Der seit 2013 andauernde NSA-Skandal hat IT-Verantwortlichen, aber auch der Allgemeinheit – über die Frage der Telekommunikationsüberwachung hinaus – deutlich gemacht, in welchem Umfang IT-Systeme kompromittiert sind. Verschlüsselungssysteme werden ausgehebelt, vertrauliche Kommunikationsinhalte abgefangen, privateste Daten auf den eigenen Computersystemen ausgespäht – selbst, wenn diese Computer nicht mit dem Internet verbunden sind. Fast 80 Prozent der Bürgerinnen und Bürger in Deutschland sind einer 2015 erhobenen Umfrage zufolge überzeugt, dass bei Nutzung des Internets ein Verlust persönlicher Daten durch Hackerangriffe und andere Manipulationen unvermeidlich ist[2]. 90 Prozent der mittelständischen Industrie sieht Gefahren für die Datensicherheit als das größte Risiko bei der Digitalisierung und Vernetzung ihrer Produktionsprozesse[3].

Aus Sicht von Industrie, Bürgerinnen und Bürgern ebenso wie aus Sicht der Praxis von IT-Sicherheitsexperten liegen mittlerweile empirisch ausreichend starke Anhaltspunkte für eine Diskussion darüber vor, dass der Datenschutz und das „Grundrecht auf informationelle Selbstbestimmung“[4], die IT-Sicherheit und das Fernmeldegeheimnis in Auflösung begriffen sind und dass dringende Schritte notwendig sind, diese drei Grundrechte als Grundpfeiler der Informationsgesellschaft zu schützen und in abgestimmter Weise für Bürger, Unternehmen und Staat zu stärken.

Die Bundesregierung hat sich nun mit dem IT-Sicherheitsgesetz zum Ziel gesetzt, den Schutz dieses Grundrechts auf „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ in technischer, organisatorischer und rechtlicher Hinsicht auszubauen. Als Nutznießer der neuen Regelungen sieht der Gesetzesentwurf Unternehmen, Behörden sowie Bürgerinnen und Bürger. Als zentrale Stelle zur Umsetzung wird das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit mehr Kompetenzen, Aufgaben und Personal ausgestattet. Auf Seiten der Unternehmen konzentrieren sich die Regelungen darauf, Betreiber Kritischer Infrastrukturen zu verpflichten, „ein Mindestniveau an IT-Sicherheit einzuhalten und dem BSI IT-Sicherheitsvorfälle zu melden“. Bürgerinnen und Bürger sollen nach Aussagen in der Gesetzesbegründung davon profitieren, dass einerseits Telekommunikationsunternehmen verpflichtet werden, die Verfügbarkeit

[1] BVerfG, Urteil des Ersten Senats vom 27. Februar 2008, 1 BvR 370/07
[2] Unisys Security: Unisys Security Insights: Germany – A Consumer Viewpoint 2015; http://www.unisys.com/ms/unisys-security-insights/germany
[3] DZ Bank Umfrage Digitalisierung – Bedeutung für den Mittelstand, Juli-August 2014
[4] BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983, 1 BvR 209/83 u. a. – Volkszählung –, BVerfGE 65, 1

ihrer Telekommunikations- und Datenverarbeitungssysteme zu gewährleisten. Andererseits werden diese Unternehmen dem Wortlaut des Gesetzes nach verpflichtet, „IT-Sicherheitsvorfälle, die zu einem unerlaubten Zugriff auf die Systeme der Nutzerinnen und Nutzer oder einer Beeinträchtigung der Verfügbarkeit führen können, an das BSI melden und betroffene Nutzerinnen und Nutzer über bekannte Störungen informieren, die durch Schadprogramme auf den datenverarbeitenden Systemen der Nutzerinnen und Nutzer hervorgerufen werden."

Die prekäre Lage der IT-Sicherheit war ein Grund dafür, dass während der Gesetzesberatungen nicht nur vonseiten der Betroffenen Stellungnahmen und Vorschläge erarbeitet wurden, sondern auch von Praktikern der IT-Sicherheit und Datenschützern. Der vorliegende Beitrag geht insbesondere auf die sich ergänzenden und in inhaltlichen Kernpunkten übereinstimmenden Punkte aus drei Stellungnahmen von Praktiker- und Datenschutzseite ein, die teilweise Beratungsunterlagen in der Anhörung des Innenausschusses des Deutschen Bundestages waren[5]. Für weitere Details lohnt die Lektüre dieser Stellungnahmen.

1. Ausgangspunkt der IT-Sicherheit

Bereits ein erster, hier nur schlaglichtartiger Blick auf die neu getroffenen Regelungen wirft Fragen auf, wie diese mit bestehenden Vorgaben und Regelungen in Einklang zu bringen sind. So werden die Betreiber Kritischer Infrastrukturen (KRITIS) durch den neu eingeführten §8 des BSI-Gesetzes dazu verpflichtet, den „Stand der Technik" für den Schutz ihrer IT-Systeme anzuwenden – womit die bestehende Regelung des §9 BDSG zum technischen Schutz personenbezogener Daten auf die Funktionsfähigkeit von IT-Systemen in Kritischen Infrastrukturen übertragen wird.

Im Gegensatz dazu fußt die Bewertung der IT-Sicherheit nach Vorgaben des BSI – seinerseits Bezug nehmend auf den international genutzten „Common Criteria" – auf einer Risikobewertung[6]. Der Unterschied ist fundamental. Der „Stand der Technik" berücksichtigt zwar die Veränderungen in der Informationstechnik, ist aber statisch in Vergleich zu einer Risikobewertung. Diese analysiert im Detail jedes Anwendungsfalles die Eintrittswahrscheinlichkeit und die Schadenshöhe eines Ereignisses und definiert daraus ein als hinnehmbar gesehenes Risiko. Diese Gleichung ändert sich mit jeder neuen IT-Sicherheitslücke. Jede Risikobewertung in der IT-Sicherheit bedeutet daher einen hochdynamischen und stetig zu aktualisierenden Analyseprozess, der gerade dann, wenn es außer dem als plötzlich kompromittiert erkannten „Stand der Technik" kein neuer existiert, regelmäßig auch zum Ergebnis hat, die kompromittierte Technik abzuschalten oder vom Netz zu nehmen, statt auf einen neuen Stand zu warten.

---

[5] Die drei sind die als Materialien für die Ausschuss-Anhörung verwandten Stellungnahmen des FIfF e.V. (https://www.bundestag.de/blob/366560/22f1e6ca62f137b23349c02ab6b2ec14/18-4-252-data.pdf), von Linus Neumann für den Chaos Computer Club (https://www.bundestag.de/blob/370474/011e1de4b10d93d5f9ae9d2e586cf6b3/18-4-284-f-data.pdf) sowie die des ULD vom 13.02.2015 (https://www.datenschutzzentrum.de/artikel/877-ULD-Stellungnahme-zum-IT-Sicherheitsgesetz-Entwurf.html). Alle Dokumente Stellungnahmen der Öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages zum Thema Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) am 20. April 2015 hinterlegt unter: https://www.bundestag.de/bundestag/ausschuesse18/a04/anhoerungen/44_sitzung_inhalt/366028. Die Anhörung ist als Video dokumentiert unter: https://www.bundestag.de/dokumente/textarchiv/2015/kw17_pa_inneres/367474 und als Protokoll unter: https://www.bundestag.de/blob/376948/9c1cf8c411c3ac30d03040f4a43ce25c/protokoll-data.pdf

[6] BSI: IT-Grundschutz – die Basis für Informationssicherheit https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

Während die öffentliche Debatte um das IT-Sicherheitsgesetz vor allem verschiedene rechtliche Fragen zum Kern hatte, stellt sich in Fachkreisen der IT-Sicherheit nun die Frage, wie IT-Sicherheit in Zukunft zu organisieren sei: nach den rechtlichen Vorgaben des IT-Sicherheitsgesetzes zum Stand der Technik oder einer Risikobewertung nach dem IT-Grundschutzhandbuch des BSI und den internationalen Common Criteria? Diese Frage wird nun zwischen den IT-Sicherheitsverantwortlichen und den Compliance-Abteilungen in den einzelnen Unternehmen auf höchst unterschiedliche Weise gelöst werden müssen – mit dem Effekt einer sicherlich nicht auf einheitlicher Ebene verbesserten IT-Sicherheit.

2. Informationspolitik und Position des BSI

Zwei weitere Schlaglichter wirft die Frage nach der Informationspolitik im IT-Sicherheitsgesetz auf. Als zentrale Neuregelung wurde von der Bundesregierung die Pflicht der KRITIS-Betreiber zur Information des BSI über IT-Sicherheitsvorfälle angeführt. Nach dem neuen §8b (4) BSIG haben KRITIS-Betreiber „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 führen können oder bereits geführt haben," über eine Kontaktstelle an das BSI zu melden. Das BSI wiederum nutzt diese Informationen, um ein Lagebild zu erstellen, und andere Unternehmen zu warnen bzw. mit Hinweisen zu versorgen.

Von Unternehmensseite wurde zum einen gefordert, „die Zusammenarbeit zwischen Unternehmen und Staat [dürfe] keine „Einbahnstraße" sein"[7], so der BDI. Außerdem wurde die Regelung kritisiert, weil sie zu unbestimmt und zu aufwändig sei. Der DIHK forderte konkret:

> „Darüber hinaus muss organisatorisch sichergestellt sein, dass unternehmensrelevante Informationen nicht in falsche Hände geraten. Der Umgang mit den Daten aus den eingehenden Meldungen beim BSI muss transparent und nachvollziehbar gestaltet und an den Zweck des Gesetzes gebunden sein. Vor diesem Hintergrund sollte die Unabhängigkeit des BSI gestärkt werden."[8]

Verschiedene Vertreter von Industrieseite äußerten weiter die Befürchtung, es könne zu einem Abfluss von sensiblem Unternehmens-Know-how gerade dann kommen, wenn in nächster Zeit die Weitergabe der Meldungen auf EU-Ebene hinzu komme und – als Lehre aus dem NSA-Skandal – dieselben staatliche Akteure in der EU die Nutznießer solcher Warnmeldungen sein könnten, die zugleich hinter Cyberattacken stecken.

Das erste, wenig wahrgenommene, aber um so bedeutsamere weitere Schlaglicht in diesem Kontext ist hier das mit dieser Kritik auch öffentlich werdende tiefe Misstrauen, das sich zwischen Unternehmen und staatlichen Stellen generell und dem BSI im Speziellen entwickelt hat, das auf Unternehmensseite in vielen Zusammenhängen nicht mehr als neutrale und sachdienliche Instanz gesehen wird. Auf Wirtschaftsseite ist nicht unbemerkt geblieben, dass der BSI-Präsident anlässlich

[7] Stellungnahme des BDI zur Anhörung des Innenausschusses, S. 2;
https://www.bundestag.de/blob/370300/8c907d1750439b380668c12f98a80d1b/18-4-284-e-data.pdf
[8] Stellungnahme des DIHK zur Anhörung des Innenausschusses S. 6,
https://www.bundestag.de/blob/370486/68f27b407b66eeb73c82769cc3e18abf/18-4-299-data.pdf

einer USA-Reise die NSA zu einem Arbeitstreffen besucht hatte[9]. Dies wurde von den Wirtschaftsverbänden überaus kritisch gesehen, was das BSI dazu brachte, die Berichte zu dementieren[10]. Der Schaden der Erkenntnisse aus dem NSA-Skandal für dieses Vertrauensverhältnis ist schwerwiegend und hätte neuer vertrauensbildender Maßnahmen zwischen BSI und Zivilgesellschaft bedurft.

Das zweite, dies verschärfende Schlaglicht hierbei ist die Verwendung der gesammelten Informationen durch das BSI. Der hier von der Bundesregierung gewählte Ansatz ist richtig und überhaupt nicht zu kritisieren, dass Informationen über Angriffe auf IT-Systeme zusammengeführt und an Betroffene weitergegeben werden, um Gefahren und Gegenmaßnahmen zu kommunizieren, die Angriffe einzudämmen und Schäden zu minimieren. Ein solcher Informationsaustausch gehört zu den Grundprinzipien des CERT-Verbundes der Spezialistenteams für Computer-Schadensfälle (Computer Emergency Response Team, CERT), die es in Behörden, Unternehmen und der Wissenschaft gibt. Obwohl sich hier vergleichsweise wenige Unternehmen engagieren, profitiert die Allgemeinheit von deren Arbeit zur Aufdeckung und Bekämpfung von Computerangriffen. Auf diesen Prinzipien hätte man zum Nutzen der IT-Sicherheit auf- und diese ausbauen können.

Doch statt dessen werden nach dem neuen §8b (2) Nr. 4 BSIG nur die KRITIS-Betreiber und die zuständigen Aufsichtsbehörden „über sie betreffende Informationen“ unterrichtet, nicht jedoch andere möglicherweise betroffene Unternehmen, nicht die heute mit der Erbringung von Services für Dritte immer stärker betraute IT-Branche und erst recht nicht die Bürgerinnen und Bürger, um deren Schutz als Endkunden von all jenen KRITIS-Systemen es dem Gesetz nach geht.

Dem Gesetz nach wird die Informationskette damit unterbrochen, der bei CERTs etablierte breite Informationsaustausch ziviler Stellen wird strukturell dem Need-to-know-Prinzip angeglichen und nur teilweise nach dem jeweiligen Stand der Erkenntnisse des BSI verknüpft. Statt also wie bisher durch einen Informationsverbund wie bei den CERTs jeden selbst in die Lage zu versetzen, eingehende Informationen daraufhin zu bewerten, ob sie einen selbst betreffen und ob man zur Lösung beitragen kann, kommt das BSI zusätzlich in die Lage, die unvollständig eingehenden Daten anlaufender Angriffe so zu analysieren und möglichst zu ergänzen, dass kein entscheidendes Detail übersehen wird und alle Betroffenen informiert werden. Wie alle Erfahrung zeigt, wird dies auch einer bestens ausgestatteten Zentralstelle nicht immer gelingen. Nur die verteilte Bearbeitung derartiger Attacken und die breite Warnung möglichst viele Betroffener hat sich als der Weg erwiesen, um mit den heute und auf absehbare Zeit verfügbaren Ressourcen IT-Sicherheit zu gewährleisten.

Die Forderungen von IT-Sicherheitsfachleuten wie dem FIfF, aber auch dem Chaos Computer Club (CCC), der Gesellschaft für Informatik (GI) und anderen war daher im Verlauf der Gesetzesberatungen, den sich abzeichnenden Erkenntnisstand bei Bedrohungen der IT-Sicherheit für alle nutzbar zu machen und das BSI zu einem schnellen und transparenten Informationsfluss zu verpflichten. Der Arbeitskreis Datenschutz und IT-Sicherheit der GI erklärte, dass „die Veröffentlichung der den Sicherheitsbehörden bekannten bislang unveröffentlichten

[9] René Pfister, Laura Poitras, Marcel Rosenbach, Jörg Schindler, Holger Stark: Der fleißige Partner; in: Spiegel Online, 22.07.2013, http://www.spiegel.de/spiegel/print/d-104058608.html

[10] BSI-Pressemitteilung: Keine Unterstützung ausländischer Nachrichtendienste, Bonn, 26.07.2013, https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2013/Keine_Unterstuetzung_auslaendischer_Nachrichtendienste_26072013.html

Sicherheitslücken unverzichtbar“[11] sei, um sich gegen IT-Angriffe zu schützen. Um die Befürchtungen gegenüber der Doppelrolle des BSI als Fachbehörde mit Pflichten zur Zuarbeit für Nachrichtendienste und Polizeibehörden einerseits und die Beratung und Unterstützung für Unternehmen und Bürgerinnen und Bürger andererseits zu entschärfen, hatten daher FIfF und CCC ein unabhängiges BSI für Bürger und Wirtschaft gefordert, das aus dem BMI heraus gelöst werden sollte.

Die Umsetzung der neuen Regelungen wird zeigen, was die Meldepflichten dem BSI an Erkenntnisgewinn für seine Arbeit und vor allem für die Allgemeinheit an Reduktion von IT-Sicherheitsbedrohungen mit sich bringt. Bisherige Beispiele wie die Kritik am Umgang des BSI mit dem Wissen um gestohlene Zugangspasswörter und verspäteter Information der Betroffenen sind ein Vorgeschmack auf die Debatten, sie sich in naher Zukunft entwickeln werden.

3. Rechtsfragen der IT-Sicherheit für die Praxis und der Teufel im Detail

Das aufschlussreichste Element des neuen IT-Sicherheitsgesetzes für die Bewertung seiner Konsequenzen für die Praxis ist jedoch der Umgang mit der rechtsfesten Ermittlung, Bekämpfung und Dokumentation von IT-Sicherheitsvorfällen. Die Betrachtung dieser Details zeigt die Grenzen des Gesetzes auf.

Für das Verständnis dieses für die rechtskonforme Umsetzung der IT-Sicherheit wichtigen Punktes bedeutsam ist, dass das Internet im deutschen Recht in zwei Bereiche aufgeteilt ist[12]:

- Das Recht der Telekommunikation (im Telekommunikationsgesetz, TKG) etwa für e-Mails, SMS, bestimmte Chat-Angebote und andere direkte Kommunikationsformen einerseits und
- das Recht der Telemedien (im Telemediengesetz, TMG), mit dem Webangebote geregelt sind, also die Pflichten der Anbieter von Webseiten, Webshops, Cloud-Speichern oder komplexe webbasierte Softwaredienste – aber heute auch Kommunikationsdienste wie etwa Skype oder Whatsapp.

Obwohl es für Nutzer kaum mehr nachvollziehbar ist, nach welchem Gesetz welcher Dienst geregelt ist und die Bewertung auch für Experten schwierig ist, werden für beide Bereiche durch beide Gesetze nicht etwa dieselben IT-Sicherheitswerkzeuge erlaubt, sondern in einem Fall sehr weitgehend zugelassen und im anderen verboten. Wichtig zum Verständnis ist auch, dass das Bundesverfassungsgericht im Januar 2012 IP-Adressen als personenbezogene Daten bewertete[13].

Regelung für Webangebote

Für Webangebote – Telemedien – ausdrücklich verboten ist die beliebige Speicherung personenbezogener Daten – also auch IP-Daten – in §12 TMG. Zulässig ist eine Speicherung nur, wenn es gesetzlich explizit erlaubt ist, oder der Nutzer eingewilligt hat und eine Speicherung und Verarbeitung der Daten zur Kommunikation und zur Abrechnung bei Vertragsverhältnissen nötig ist. In allen anderen Fällen sind alle Daten am Ende der Nutzung umgehend zu löschen. Allein „bei Verwendung von Pseudonymen“ ist es zulässig, pseudonyme Nutzungsprofile für „Werbung,

[11] IT-Sicherheitsgesetz schafft Unsicherheit; Stellungnahme der GI zum IT-Sicherheitsgesetz vom 18.11.2014, http://www.gi.de/aktuelles/meldungen/detailansicht/article/it-sicherheitsgesetz-schafft-unsicherheit.html

[12] Im Detail dazu: Ingo Ruhmann: IT-Sicherheit und das geplante IT-Sicherheitsgesetz; in: telepolis, 11.04.2013; http://www.heise.de/tp/artikel/38/38891/1.html

[13] BVerfG: Beschluss des Ersten Senats vom 24. Januar 2012 - 1 BvR 1299/05 - http://www.bverfg.de/entscheidungen/rs20120124_1bvr129905.html

Marktforschung oder zur bedarfsgerechten Gestaltung“ der Telemedien zu erstellen. Verstöße gegen diese Regelung können als Ordnungswidrigkeit geahndet werden.

Für Zwecke der IT-Sicherheit erlaubt das Gesetz damit nur, IP-Nummern von Nutzern eines Webangebotes solange zu verarbeiten, wie die aktuelle Nutzung andauert. Da die IT-Sicherheit als Zweck im Gesetz nicht vorgesehen ist, greift das generelle Speicherungsverbot und damit die Pflicht zur Löschung der IP-Daten nach Nutzungsende oder zumindest deren Pseudonymisierung, wenn auch fraglich ist, ob das zu einer „bedarfsgerechten Gestaltung“ zählt. Zulässig ist die Speicherung allein nach Einwilligung des Nutzers, was jedoch für einen Angreifer auf einen Telemedien-Dienst ein äußerst ungewöhnliches Entgegenkommen bedeuten würde. Unzweifelhaft gesetzwidrig ist es jedoch, vollständige IP-Adressen für irgendeinen Zweck dauerhaft zu speichern.

Bei Webangeboten dürfen damit IP-Daten von IT-Sicherheitswerkzeugen durch ein Intrusion Detection System rechtlich unbedenklich genutzt werden. Es gibt aber bei Webangeboten keine Rechtsgrundlage für den Einsatz von IT-Sicherheitswerkzeuge für mehrschrittige Analysen und erst recht nicht für die Verfolgung von Angreifern und die juristisch einwandfreie Beweissicherung nach einem Fall von Cybersabotage, sondern das Verbot der entsprechenden Datenspeicherung und -verarbeitung. Diese Daten stehen als zulässige Beweismittel damit auch im Falle einer Strafverfolgung nicht zur Verfügung; Strafverfolger ihrerseits dürfen solche Daten ebenfalls nicht erheben. Der Bundesregierung ist die Problematik spätestens seit 2006 bekannt, als dem Bundesjustizministerium genau mit diesen Gründen die Speicherung von IP-Daten rechtskräftig untersagt wurde[14].

In einem Entwurf des IT-Sicherheitsgesetzes aus dem Sommer 2014 hatte die Bundesregierung eine entsprechende Änderung am TMG vorgesehen und damit begründet, diese Rechtslücke nun schließen zu wollen. Wegen der als „Vorratsdatenspeicherung durch die Hintertür“ geführten Kritik an der gewählten Art der Regelung in Analogie zu §100 TKG wurde der Passus in dem vom Kabinett im Dezember 2014 verabschiedeten Entwurf jedoch wieder fallen gelassen. Das Telemedienrecht enthält nun weiterhin keine Regelung zur Datenspeicherung zu Zwecken der IT-Sicherheit. Die Vorratsdatenspeicherung wurde dagegen in der Zwischenzeit ganz ohne den Weg durch die Hintertür auf den Weg gebracht.

Für eine rechtstaatliche Verfolgung von Cyberattacken ist es aus Sicht des FIfF jedoch notwendig, für IT-Sicherheitswerkzeuge auch bei Telemedien, die einen wesentlichen Teil der Angriffsziele im Internet ausmachen, eine grundrechtskonforme Rechtsgrundlage zu schaffen – also eine, die datenschutzkonform ist und möglichst wenig Daten erfordert. Aus Sicht des FIfF ist es dabei auch völlig unbegründet, Unterschiede in der Rechtslage und der IT-Sicherheit zwischen der Telekommunikation und den Telemedien zu machen.

Regelung im Telekommunikationsbereich

Die im IT-Sicherheitsgesetz neu gefasste Regelung zur Störungsbeseitigung ist mit solchen Implikationen verbunden, dass eine detaillierte Betrachtung diesen Rahmen sprengen würde. In diesem Kontext können diese Fragen daher nur verkürzt dargestellt werden.

[14] Nach dem erstinstanzlichen Urteil 2006 wurde der Rechtsstreit 2008 mit gleichem Tenor abschließend entschieden, siehe: Endgültiger Beschluss des Amtsgericht Mitte zu Berlin mit Androhung von Zwangsgeld gegen das BMJ vom 10.01.2008, 5 C 314/06, http://www.daten-speicherung.de/data/Beschluss_AG-Mitte_2008-01-10.pdf

Das Telekommunikationsrecht enthält mit dem 1996 formulierten §100 TKG eine aus der Zeit der analogen Telefonie stammende Befugnis zur Datensammlung, laut Abs. 1 „Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer (zu) erheben und verwenden“ – also ohne Einschränkung jede Form von Daten zur Störungserkennung, also Daten aus Telekommunikationsvorgängen zu sammeln, zu analysieren und sich sogar auf Kommunikationsverbindungen aufzuschalten. Technisch erforderlich ist dies, weil bei der analogen Telefonie Störungen nur durch Messungen im Betrieb erkannt und beseitigt werden können. Der §100 TKG lieferte die Rechtsgrundlage, strafbare Eingriffe in Fernmeldesysteme für die Öffentlichkeit zu ermitteln und den Telekommunikationsunternehmen die Befugnis zu geben, die dafür nötigen Messungen vorzunehmen.

Im Telekommunikationsnetz in Deutschland werden nun gegenwärtig die letzten Komponenten und Teile auf ein All-IP-Netz umgestellt. Die Telekommunikationsdienste werden heute schon weitestgehend per TCP/IP vermittelt und übertragen. Damit lassen sich Störungen im Netz mit genau denselben Werkzeugen ermitteln, analysieren und beseitigen, wie schon bei Telemedien und in der Internet-Datenkommunikation: durch Analyse durchlaufender Datenpakete und auflaufener Kommunikationsprotokolle an den Netzknoten. Die Befugnis zur beliebigen Sammlung von Datenflüssen gemäß §100 TKG ist heute schon die bedenkliche Befugnis zu einer völlig unbegrenzten „Vorratsdatenspeicherung“ – eingeschränkt nur durch den gesetzlichen Zweck einer Störungsanalyse.

Das IT-Sicherheitsgesetz enthält für den Telekommunikationssektor nun mit einer Neuregelung des §100 TKG eine noch sehr viel weiter reichende Regelung. Danach sollen Telekommunikationsanbieter nicht nur jedes beliebige Datum zur Störungserkennung speichern und analysieren dürfen, sondern obendrein auch Daten über

> „Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können.“

Damit wurde die bisher in §100 TKG formulierte Befugnis für die Messung flüchtiger analoger Daten ausweitet auf die „Verfügbarkeit“ nicht weiter spezifizierter „Informations- und Kommunikationsdienste“ sowie auf die unbegrenzte Datensammlung zum Schutz vor einem „unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer“ – also nicht nur von Kunden des jeweiligen Anbieters, sondern beliebige Beteiligte an Kommunikationsvorgängen – nach Definition des „Nutzers“ in §3 TKG Nr. 14: „natürliche oder juristische Personen, die einen öffentlich zugänglichen Telekommunikationsdienst für private oder geschäftliche Zwecke in Anspruch“ nehmen – deren Daten per Zufall über das Netz eines Telekommunikationsanbieters geleitet wurden.

Es geht also nicht mehr um die Verfolgung von Gesetzesverstößen durch Manipulationen – nach dem Zweck des bisherigen §100 TKG also Betrugshandlungen an TK-Systemen. Hier werden nun Telekommunikationsunternehmen dazu befugt, als Hilfskräfte der Strafverfolgung unbegrenzt Daten über beliebige Netznutzer zu sammeln und auszuwerten, um zu erkennen, ob es unerlaubte „Zugriffe“ auf die IT-Systeme dieser Nutzer geben könnte – wohlgemerkt: keine Kunden, deren Dienstenutzung vertraglich geregelt wurde und bekannt ist.

Für diese unspezifische Datensammlung zu Zwecken der IT-Sicherheit wird in nahezu unbegrenzter Weise in das Fernmeldegeheimnis eingegriffen. Die Bedenken von Praktikern und Verfassungsjuristen[15] bei der Gesetzesberatung verhallten ungehört. Im starken Gegensatz zu den Vorgaben des Bundesverfassungsgerichts für Eingriffe in Grundrechte ist diese geplante Vorschrift

- nicht an die Angabe eines Anlasses, sondern unspezifisch an eine „Störung" gebunden,
- ohne einen genügend spezifischen Zweck, sondern dient nur der Erkennung eines „unerlaubten Zugriffs",
- ohne spezifische Kriterien und
- obendrein ohne Vorgaben zu Speicherdauer und zur Datennutzung formuliert.

Diese Befugnis zur Datenerhebung und –analyse wird ergänzt durch den neu eingeführten §109a TKG und die Befugnis für jeden TK-Diensteanbieter, bei „Störungen, die von Datenverarbeitungssystemen der Nutzer ausgehen", jene 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".

Ein äußerst bemerkenswertes Rechtskonstrukt.

Betrachten wir hier zuerst die Zielgruppe der Regelung. Nutzer, die TK-Unternehmen „bereits bekannt sind", werden im TKG als „Kunden" bezeichnet. Für ihre Kunden bieten TK-Unternehmen heute vertragliche Serviceoptionen für IT-Sicherheitsdienstleistungen. Diese „Virensuchfunktion" der Provider für den Datenverkehr ihrer Kunden bedürfte grundsätzlich keinerlei Rechtsänderung. Notwendig wird dies erst bei einer Ausweitung auf eine Hilfsfunktion für die Netzsicherheit, die durch die Provider für beliebige Netznutzer geleistet werden soll.

Nun ist aber bei genauerer Betrachtung die Möglichkeit, den Störungen verursachenden Datenverkehr beliebiger Nutzer, deren Datenstrom durch das Netz irgend eines Providers läuft, ohne eine solche vertragliche Grundlage zu durchsuchen, sodann diese Nutzer – also Kunden fremder Provider – irgendwie ausfindig zu machen und ihnen schließlich gemäß §109a TKG mitzuteilen, dass sie Schadcode verbreiten, eine technisch äußerst bemerkenswerte Idee. Ein Netzwerk funktioniert eben nicht wie ein Virensuchprogramm, das ein Nutzer am eigenen Computer aufruft, arbeiten lässt und das einen Bericht erstellt. Es ist für Praktiker jedenfalls eine faszinierende Idee, aus den IP-Adressen des TCP/IP-Datenverkehrs beliebiger, Schadcode verbreitender „Nutzer", von denen jeder Provider nur im Datenpaket die IP-Nummer des Absenders auslesen kann, diesen Absender zu ermitteln und auf eine Weise zu kontaktieren, dass ihm oder ihr eine erkennbare Botschaft in den Datenstrom eingeschleust und zugestellt werden kann, mit der er oder sie die Schadcodeverbreitung einstellen könnte.

Möglich ist das. Die Injektion von Code in Datenströme ist Alltag für die NSA und andere Hacker. Was aber ohne Kenntnis weiterer Kommunikationsparameter nicht ganz so einfach ist, ist die Übermittlung einer Botschaft an diese Endnutzer. Voraussetzung dafür ist ein hoher Aufwand, der

[15] So die Aussagen im Protokoll der Anhörung des Innenausschusses von Prof. Hornung (S. 19) und Prof. Roßnagel (S. 46), a.a.O.

Einsatz sachkundigen Personals und die Einschaltung mehrerer beteiligter Anbieter. Der reale Nutzen dieser Neuregelung in den §100 und 109a TKG ist also nur äußerst undeutlich zu erkennen.

Wer nun bei diesen Begriffen und in Anlehnung der Regelungen aus dem Polizeigesetzen erwartet, dass nach der Identifikation eines „Störers“ und der Aufforderung an diesen zur Beendigung seiner Störung nun vorgesehen sei, einen „Platzverweis“ auszusprechen und diesen auch mit Anwendungen unmittelbaren Zwangs durchzusetzen, sucht vergeblich. Das Unterbinden des Datenverkehrs eines Schadcode verbreitenden Störers ist bisher nicht vorgesehen und dürfte auch vertraglichen Pflichten der Provider zuwiderlaufen. Rufen wir uns allerdings in Erinnerung, dass in der Debatte um die BSIG-Novelle 2006 / 2007 anfänglich vorgesehen war, das BSI mit der Befugnis auszustatten, sich bei Angriffen auf die IT des Bundes auch ohne richterliche Anordnung „Zugang zu Gebäuden, Einrichtungen und informationstechnischen Systemen verschaffen“ und IT-Systeme dort abzuschalten, wenn das den Angriff verursachende IT-System in einem deutschen Rechenzentrum verortet wurde[16]. Diese Idee wurde aus verfassungsrechtlichen Gründen verworfen, aber sicher auch aus dem Grund, dass nur in seltenen Fällen Angriffe auf IT-Systeme von Rechnern nicht oder allenfalls teilweise im gleichen Land ausgeführt werden und das auf nationale Rechenzentren begrenzte Einschreiten daher kaum nutzbar sein würde. Es ist also nicht von der Hand zu weisen, dass die Idee eines „Platzverweises“ in der digitalen Welt im Kontext der BSI-Befugnisse diskutiert wurde, sich dazu aber bisher keine geeignete Umsetzung bei der IT-Sicherheit fand.

Betrachten wir sodann die technischen Voraussetzungen zur Umsetzung dieser Vorschrift. Die wirksame Erkennung einer „Störung“, einer „Einschränkung der Verfügbarkeit“ oder von „unerlaubten Zugriffen“ gemäß §100 TKG setzt eine Durchsuchung von Datenkommunikation voraus zur Kenntnisnahme, Identifikation und Benachrichtigung von Telekommunikationsnutzern ohne die geringsten Vorgaben für eine Eingrenzung auf Kriterien, Speicherdauer oder Analyseform für diese Daten.

Diese Vorschriften an Beispielen durchzuspielen, macht das Ausmaß der Idee erkennbar. Danach dürfte jeder Telekommunikationsprovider die Kommunikationsdaten von Kunden unbegrenzt durchsuchen und speichern, um beispielsweise

- „unerlaubte Zugriffe“ einer Smartphone-App auf eigene Daten zu erkennen,
- die von einigen Providern nicht erlaubte und als „Störung“ unterbundene Nutzung von Skype auf Smartphones zu erkennen und zu verhindern,
- natürlich auch „unerlaubte Zugriffe“ z.B. auf urheberrechtlich geschütztes Material zu verfolgen.

Rufen wir uns dagegen in Erinnerung, welche Zugriffe auf IT-Systeme „unerlaubt“ sind oder was als „Störung“ gilt, dann ist man schnell bei einer Ahnung für eine nahezu unbegrenzte Überwachung des Datenverkehrs ohne jede Einschränkung und damit die faktische Aushebelung des Fernmeldegeheimnisses. Eine solche dauerhafte Durchsuchung von Telekommunikationsverkehren zur Ermittlung von „Störungen“ – nicht einmal „Gefährdungen“ – ohne jede Einschränkung entspricht nicht einmal im Ansatz den Anforderungen an Grundrechtseingriffe. Dies macht deutlich, dass die im IT-Sicherheitsgesetz neu gefasste Ausweitung an §100 TKG und die Nutzung der gewonnen Daten für

[16] Innenministerium: Mehr Biss für die IT-Sicherheit des Bundes, heise Security, 12.12.2008, http://www.heise.de/newsticker/meldung/Innenministerium-Mehr-Biss-fuer-die-IT-Sicherheit-des-Bundes-189162.html

die im §109a TKG genannten Zwecke aus Sicht des FIfF wie auch nach Aussagen der zur Anhörung des Bundestages geladenen Verfassungsjuristen unvereinbar ist mit Art. 10 GG.

Folgen für die IT-Sicherheit im Telemedien- und Telekommunikationssektor

Auch nach Inkrafttreten des IT-Sicherheitsgesetzes fehlt es also an einer Rechtsgrundlage für die rechtsfeste Erhebung und Dokumentation der Verursacher von Störungen der IT-Sicherheit bei Telemedien – also den üblichen Internetangeboten. Die Klasse der rechtlich zulässigen Analysewerkzeuge für Webangebote ist weiterhin eingeschränkt. Damit wird die bestehende Rechtslage für die Allgemeinheit nicht verbessert. Betreiber von KRITIS-Systemen werden aber einem neuen Dilemma ausgesetzt: Sie müssen Sicherheitsvorfälle melden – und sollten dabei gut begründen können, für die Schadenserkennung bei Webservices keine verbotenen Werkzeuge zu nutzen. Was aus Sicht der IT-Sicherheit unbefriedigend ist, ist formaljuristisch gesehen jedoch hilfreich: Gemeldet werden darf nur das, was die rechtlich zulässigen Werkzeuge hergeben. Mit dieser Sichtweise lässt sich der Aufwand für die Befolgung des IT-Sicherheitsgesetzes eindeutig eingrenzen.

Telekommunikationsprovider wiederum werden abschätzen müssen, wie sie die neuen Befugnisse aus §100 und §109a TKG und wie sie die daraus entstandene Rechtslage bewerten. Sie müssen entscheiden, welche Investitionen sie für die skizzierte Umsetzung des Gesetzes tätigen wollen, zumal die Zielgruppe der aus den Aufwänden erzielbaren Erkenntnisse Nutzer anderer Provider, aber keine eigenen, für den Service zahlenden Kunden sind. In der Bewertung wird auch eine Rolle spielen, wie die Aussicht bewertet wird, dass die Neuregelung bei einer Klage keinen Bestand vor dem Bundesverfassungsgericht findet.

Zusammenfassend für die Frage der Rechtsgrundlagen gibt es im IT-Sicherheitsgesetz für die im TMG geregelten Webservices weiterhin keine Rechtsgrundlage für wichtige, heute übliche IT-Sicherheitswerkzeuge, im TKG dagegen eine nicht verfassungsgemäße uferlose Datensammlung. Im Ergebnis des Gesetzes, das für mehr IT-Sicherheit sorgen sollte, droht so ein Rechtsvakuum, das der IT-Sicherheit die Rechtsgrundlage zu entziehen droht und damit zugleich jede Basis für Investitionen in mehr Ressourcen – von einer datenschutzkonformen Lösung einmal ganz abgesehen.

Verfassungskonformer Gegenvorschlag

Der Gegenvorschlag des FIfF zielt darauf ab, die Verarbeitung von IP-Daten zu Zwecken der IT-Sicherheit in allen Bereichen einheitlich und so datensparsam wie möglich zu gestalten. Da keine Identifikation und Rückverfolgung von Cyberangreifern ohne die Auswertung von IP-Daten möglich ist, die notwendige schnelle Reaktion auf Angriffe eine längere Datenspeicherung aber unnötig macht und obendrein die große Menge der protokollierten Daten die Analyse eher behindert, hat das FIfF ein grundrechtskonformes und praxisgerechtes Verfahren vorgeschlagen, das praxistauglich und durchaus erprobt ist und Sicherheitsvorfälle zuverlässig aufspüren kann. Der auf schnelle Datenreduktion und die Konzentration auf relevante Daten zu IT-Sicherheitsvorfällen ausgerichtete mehrstufige Vorschlag unterscheidet nicht zwischen Telekommunikations- und Telemediendiensten, sondern wendet aktuelle Technik auf beide Bereiche an.

- Ein vorgeschaltetes Intrusion Detection System kann aus den laufenden Verkehrsdaten eine Eingrenzung auf Verdachtsfälle leisten und den Rest der Daten verwerfen oder pseudonymisieren, etwa durch ein Verkürzen der IP-Adressen oder ein Hashing der IP-Daten.
- Im Verdachtsfall ist unmittelbar ein auditierbares IT-Sicherheitsverfahren zur Gefahrenanalyse und -abwehr auf den Daten des Verdachtsfalls anzuwenden.
- Die systematische Analyse gespeicherter pseudonymisierter Protokolldaten, die ihrerseits nach

einer überschaubaren Frist gelöscht werden, reicht auch über die Vorlaufzeit von größeren Angriffen aus, um eine Entscheidung über das Vorgehen bei vermuteten Angriffen zu treffen.
- Als Ergebnis der Analyse sind nach überschaubarer Zeit entweder alle als harmlos klassifizierten pseudonymisierten Daten zu löschen oder es ist gezielt konkreten Verdachtsfällen nachzugehen, für die die Verkehrsdaten vollständig zu erfassen und in dem etablierten geordneten, auditierbaren Verfahren zu verarbeiten sind.

Ein solches zweistufiges Verfahren, bei dem alle unnötigen Daten gelöscht oder in Zweifelsfällen pseudonymisiert werden, ist aus Datenschutzsicht akzeptabel und durch Audits gut kontrollierbar. Es entspricht professionellen IT-Sicherheitsverfahren, um Verdachtsfälle sofort kriterienbasiert zu ermitteln und ist trotzdem weniger aufwändig als das Verfahren gemäß §5 BSIG. Mit diesem Verfahren ist für eine gerichtsfeste Lösung die minimal zur Verfolgung notwendige Menge an Daten benannt, bei zugleich weitestgehender Löschung von Daten. Allein die einheitliche Rechtsgrundlage für die IT-Sicherheit liefert die Grundlage dafür, das Grundrecht auf informationelle Selbstbestimmung wie auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umzusetzen und zugleich das Fernmeldegeheimnis zu wahren und nicht weiter auszuhöhlen.

4. Sonderrolle für die IT des Bundes

In der Betrachtung der Rechtslage blieb bisher ein Detail unberücksichtigt: Die rechtliche Sonderstellung in Sachen IT-Sicherheit, die sich der Bund für seine IT-Systeme ab 2007 eingeräumt hat und die jetzt weiter gestärkt werden soll.

Im vorherigen Abschnitt wurde kurz erwähnt, dass es dem Bundesjustizministerium 2006 erstinstanzlich untersagt wurde, IP-Daten zu speichern. Der Bundesregierung war die Gefahr für die IT-Sicherheit – ausweislich ihrer Antwort auf eine zeitnah gestellte Kleine Anfrage[17] – bewusst; sie reagierte binnen Jahresfrist. In der Novelle des BSI-Gesetzes erhielt das BSI 2007 in §5 BSIG die Befugnis, in jedem Anwendungsbereich des Internets für Zwecke der IT-Sicherheit IP-Daten bei IT-Systemen des Bundes zu erheben und auszuwerten. Als einzige Stelle darf daher das BSI – das auch kein Telekommunikationsunternehmen ist, denen ansonsten allein eine Datensammlung gemäß §100 TKG erlaubt ist – IT-Sicherheitswerkzeuge für die IT des Bundes umfassend einsetzen. Dieser §5 BSIG ist ein sehr aufschlussreicher Hinweis auf ein Verfahren, wie eine Regelung zur Verfolgung von IT-Sicherheitsvorfällen aus Sicht der Bundesregierung aussehen müsste.

Diese Ausnahmereglung für die IT-Systeme des Bundes wird nun im IT-Sicherheitsgesetz weiter getrieben. Nach Artikel 7 des IT-Sicherheitsgesetzes wurde das BKA-Gesetz um Befugnisse für das BKA bei Computerstraftaten gegen die IT des Bundes und sicherheitsempfindliche Stellen erweitert. Damit hat die Bundesregierung eine Sonderpolizei für Cyberattacken gegen die IT des Bundes beim BKA eingerichtet. Die Bundesregierung beziffert den Aufwand für diese Aufgabe beim BKA auf „48 und bis zu maximal 78 Planstellen mit jährlichen Personalkosten in Höhe von jährlich zwischen rund 3,226 und bis zu maximal 5,310 Millionen Euro“.

[17] Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Petra Pau, Sevim Dagdelen, weiterer Abgeordneter und der Fraktion DIE LINKE: Speicherung der IP-Adressen von Besucherinnen und Besuchern der Website des Bundeskriminalamtes, 7.11.2007, Bt.-Drs. 16/6938, Antworten zu den Fragen 11 und 13

Der Gesetzentwurf formulierte dazu die Begründung, dass die Strafverfolgung und „die örtliche Zuständigkeit oftmals dem Zufall überlassen bleibt“, was – deutlicher gesagt – offensichtlich meint, dass die für IT-Kriminalität zufällig zuständigen Strafverfolgungsbehörden der Republik nicht mit hinreichenden Kompetenzen und Ressourcen ausgestattet sind, um Angriffe auf die IT des Bundes mit der nötigen Sachkunde zu verfolgen. Dies ist als Aussage mit der Realität recht gut in Übereinstimmung zu bringen. Bürgerinnen und Bürger, die Wirtschaft, aber auch die Behörden der Länder und Kommunen und sogar der Bundestag selbst werden auf diese Weise aber leider mit den Problemen der Sicherheit ihrer IT-Systeme nicht nur bei den rechtlichen Grundlagen allein gelassen, sondern auch bei der Strafverfolgung, die in der Fläche nach Meinung der Bundesregierung von nicht ausreichender Qualität ist.

Gerade Sicherheitspolitiker werden nicht müde zu betonen, das Internet sei kein „rechtsfreier Raum“. Mit dem IT-Sicherheitsgesetz hat sich die Bundesregierung bei den Rechtsgrundlagen und der Strafverfolgung nun faktisch von der Aufgabe eines Schutzes der Allgemeinheit zurückgezogen. Für die Allgemeinheit macht die Bundesregierung das Internet damit erst zu einem Rechtsraum, für den zwar Gesetze formuliert sind, aber die Strafverfolgung kaum Handlungsmöglichkeiten hat, in dem nicht einmal eine Beweissicherung über die zielgerichtete Speicherung von IP-Daten zur Verfolgung von Tätern zulässig ist.

5. Fazit

Das IT-Sicherheitsgesetz stärkt die Sicherheit der IT des Bundes durch mehr Befugnisse, Personal und Mittel. Das Gesetz ist dazu geeignet, die IT-Sicherheit bei solchen KRITIS-Systemen zu verbessern, die bisher keinen Auflagen zum Schutz der IT-Sicherheit ihrer Systeme unterworfen waren, wenn auch die Vorschriften moderat ausfallen und hinter den im BSI-Grundschutzhandbuch vorgesehenen Maßstäben und Vorgehensweisen zum Schutz von IT-Systemen zurück fallen. Das Gesetz trägt zur Verbesserung der IT-Sicherheit für Bürgerinnen und Bürger allenfalls mittelbar bei. Der Einsatz diverser IT-Sicherheitswerkzeuge bleibt weiterhin verboten. An Stelle einer im Verlauf der Gesetzesentwicklung immerhin noch erkennbaren Idee einer einheitlichen Rechtsgrundlage für die IT-Sicherheit wurde eine rechtlich fragile und kaum verfassungsfeste Konstruktion gewählt.

Es ist unbestreitbar, dass mit dem IT-Sicherheitsgesetz die Regelung eines ausgesprochen wichtigen Gebietes begonnen wurde. Positiv ist zweifellos die Verpflichtung von Betreibern kritischer Infrastrukturen auf bessere IT-Sicherheit. Kerntechnische Anlagen, die bisher aus der Debatte heraus gehalten wurden, auch zu Kritischen Infrastrukturen zu zählen, ist eine durchweg positive Überraschung.

Grundsätzlich positiv zu sehen sind auch die zusätzlichen Ressourcen für die IT-Sicherheit. Dass aber nicht nur das BSI 133 zusätzlichen Planstellen erhält, sondern für das Bundesamt für Verfassungsschutz 55 neue Planstellen und das BKA bis zu 78 zusätzliche Planstellen vorgesehen sind – in Summe weitere 134 Stellen –, trägt zur IT-Sicherheit wenig bei. Die neuen Stellen für Verfassungsschutz und BKA wären besser beim BSI aufgehoben. Das BSI hat seit seiner Entstehung die Aufgabe, Polizeibehörden mit Sachkunde zu unterstützen und könnte dies bei Cyberangriffen mit mehr Personal besser leisten. Im BSI könnte so die Sachkompetenz zur Bekämpfung von IT-Sicherheitsproblemen für die Allgemeinheit gebündelt und verstärkt werden.

Die EU hat außerdem mehrfach angekündigt, in Sachen IT-Sicherheit regulativ tätig zu werden[18], das EU-Parlament hat dazu weitere Ergänzungen angemahnt[19]. Es ist zu vermuten, dass die EU die IT-Sicherheit umfassender regeln wird und auf Deutschland Nachbesserungsbedarf zukommt. Eingedenk dieser absehbaren Entwicklung wäre es durchaus sinnvoll gewesen, die Anforderungen an die IT-Sicherheit im neuen Gesetz höher anzusetzen. Aktiv gestalten, statt nur zu reagieren, wäre für Bürgerinnen und Bürger und Wirtschaft in Deutschland der bessere Ansatz.

Wer IT-Sicherheit verbessern will, muss zwangsläufig das allgemeine Sicherheitsniveau erhöhen und Einfallstore und Hintertüren beseitigen. Das Gesetz lässt dazu jedoch viele Fragen offen. Aus Sicht der Praxis gibt es einige vordringliche Handlungsfelder, die in einer Novelle des IT-Sicherheitsgesetzes verbessert werden sollten. Die wichtigsten sind:

- **Umgang mit IT-Sicherheitslücken**
  Wie die IT-Sicherheitsexperten aller größeren Verbände von IT-Fachleuten in Deutschland hält auch das FIfF den Austausch und die Information über IT-Sicherheitslücken für einen der wichtigsten Wege zur Verbesserung der Sicherheitslage. Aus Sicht von IT-Experten muss das BSI seine Kenntnisse zeitnah und umfassend publizieren und nicht selbst darüber entscheiden, ob und wann es dies tut. Dafür ist das BSI als eine unabhängige IT-Sicherheitsbehörde für die Allgemeinheit neu zu organisieren und zu stärken.
  Entscheidend ist die Erkenntnis, in welchem Ausmaß zentrale Sicherheitsmechanismen der IT-Sicherheit kompromittiert sind. Schon bevor der SSL-Heartbleed-Bug überhaupt programmiert wurde, war NSA-Dokumenten zu nehmen, dass die SSL-Verschlüsselung erfolgreich angegriffen wurde. VPN-Verbindungen sind durch Hintertüren und Implementationsdefizite verwundbar. Aus Sicht des FIfF ist es daher außerdem erforderlich, solche und andere zentrale IT-Sicherheitskomponenten auf Dauer periodisch auf ihre Zuverlässigkeit oder Kompromittierung hin durch unabhängige Stellen zu untersuchen und die Ergebnisse zu veröffentlichen.
  Das FIfF hat außerdem Vorschläge erarbeitet, mit denen zur Aufdeckung von Sicherheitsproblemen durch interne Whistleblower und zur Realisierung einer Produkthaftung ein gestuftes Meldeverfahren etabliert werden kann, bei dem eine vertrauenswürdige Stelle Hinweise sammelt und an die Hersteller oder Anwender weiterleitet, die die Sicherheitsrisiken zu verantworten und zu beseitigen haben.

- **Einheitliche, datenschutzgerechte Rechtsgrundlagen für die IT-Sicherheit**
  Wer einen rechtsförmigen Umgang mit IT-Sicherheitsproblemen erreichen will, wird nicht darauf verzichten können, die in ihren Funktionen mittlerweile kaum mehr unterscheidbaren Telekommunikations- und Telemediendienste mit einer einheitlichen Rechtsgrundlage für die zulässigen Verfahren und Werkzeuge der IT-Sicherheit auszustatten, die gleichermaßen die drei Grundrechte des Datenschutzes, der IT-Sicherheit und des Fernmeldegeheimnisses wahrt. Konkrete Vorschläge dafür liegen auf dem Tisch, die zudem praxistauglicher und weniger aufwändig sind als die Regelung in §5 BSIG für die IT des Bundes.

In der verabschiedeten Form wird das IT-Sicherheitsgesetz die Arbeit von IT-Sicherheitsexperten nicht entlasten, der Schutz der zentralen Grundrechte der Informationsgesellschaft wird nicht

[18] Kommissionsvorschlag für eine Richtlinie zur Netz- und Informationssicherheit (NIS) vom 7.02.2013, http://europa.eu/rapid/press-release_IP-13-94_de.htm

[19] Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zum Thema „Cyberangriffe in der EU“, 10.07.2014; http://edz.bib.uni-mannheim.de/edz/doku/wsa/2014/ces-2014-1488-de.pdf

verbessert. Wirtschaftsverbände und IT-Fachleute haben in der Debatte um das Gesetz zahlreiche wichtige Anforderungen zur Verbesserung der IT-Sicherheit konkret formuliert. Es bleibt zu hoffen, dass die Anwendung des Gesetzes ausreichend Anlass dazu geben wird, die bisher nicht adressierten Lösungsansätze in einem nächsten Anlauf besser auf die Erfordernisse der Praxis der IT-Sicherheit und zugleich auf den Schutz der Grundrechte abzustimmen.