18. Wahlperiode

Deutscher Bundestag
Innenausschuss

Wortprotokoll
der 44. Sitzung

Innenausschuss
Berlin, den 20. April 2015, 14:00 Uhr
10117 Berlin, Adele-Schreiber-Krieger-Straße 1
Marie-Elisabeth-Lüders-Haus
3.101 (Anhörungssaal)

Vorsitz: Wolfgang Bosbach, MdB

Öffentliche Anhörung

Tagesordnungspunkt

Gesetzentwurf der Bundesregierung

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

BT-Drucksache 18/4096

Federführend:
Innenausschuss

Mitberatend:
Ausschuss für Recht und Verbraucherschutz
Ausschuss für Wirtschaft und Energie
Ausschuss für Verkehr und digitale Infrastruktur
Ausschuss Digitale Agenda
Haushaltsausschuss (mb und § 96 GO)

Gutachtlich:
Parlamentarischer Beirat für nachhaltige Entwicklung

Berichterstatter/in:
Abg. Clemens Binninger [CDU/CSU]
Abg. Gerold Reichenbach [SPD]
Abg. Jan Korte [DIE LINKE.]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]

Inhaltsverzeichnis

Anlage B

Weitere Stellungnahmen zur Öffentlichen Anhörung

Forum Informatikerinnen für Frieden und gesellschaftliche Verantwortung e.V.	18(4)252
Deutscher Speditions- und Logistikverband e.V. (Stand Nov.2014)	18(4)270
Deutscher Speditions- und Logistikverband e.V. (Stand Apr. 2015)	18(4)270 A
Deutscher Factoring Verband e.V.	18(4)290
Verband der TÜV e.V.	18(4)291
ASW Bundesverband – Allianz für Sicherheit in der Wirtschaft e.V.	18(4)294
Bundesverband des Deutschen Lebensmittelhandels und der Handelsverband Deutschland	18(4)297
Deutscher Industrie- und Handelskammertag	18(4)299
Cyber-Sicherheitsrat Deutschland e.V.	18(4)300
VDV Köln Die Verkehrsunternehmen	18(4)301
AmCham Germany	18(4)313

0/1.

Tagungsbüro

Deutscher Bundestag

Sitzung des Innenausschusses (4. Ausschuss)
Montag, 20. April 2015, 14:00 Uhr

Anwesenheitsliste
gemäß § 14 Abs. 1 des Abgeordnetengesetzes

Ordentliche Mitglieder	Unterschrift	Stellvertretende Mitglieder	Unterschrift
CDU/CSU		**CDU/CSU**	
Baumann, Günter		Albsteiger, Katrin	
Binninger, Clemens		Berghegger Dr., André	
Bosbach, Wolfgang		Brähmig, Klaus	
Brandt, Helmut		Fabritius Dr., Bernd	
Frieser, Michael		Feiler, Uwe	
Hellmuth, Jörg		Giousouf, Cemile	
Hoffmann (Dortmund), Thorsten		Gröhler, Klaus-Dieter	
Lindholz, Andrea		Hauer, Matthias	
Mayer (Altötting), Stephan		Heck Dr., Stefan	
Ostermann Dr., Tim		Liebing, Ingbert	
Schäfer (Saalstadt), Anita		Luczak Dr., Jan-Marco	
Schuster (Weil am Rhein), Armin		Monstadt, Dietrich	
Steinbach, Erika		Seif, Detlef	
Veith, Oswin		Sensburg Dr., Patrick	
Warken, Nina		Strobl (Heilbronn), Thomas	
Wendt, Marian		Ullrich Dr., Volker	
Woltmann, Barbara		Wellenreuther, Ingo	
Zertik, Heinrich		Wittke, Oliver	

Stand: 17. April 2015
Referat ZT 4-Zentrale Assistenzdienste, Luisenstr. 32-34, Telefon: +49 30 227-32659, Fax: +49 30 227-36339

Tagungsbüro

Sitzung des Innenausschusses (4. Ausschuss)

Montag, 20. April 2015, 14:00 Uhr

Anwesenheitsliste

gemäß § 14 Abs. 1 des Abgeordnetengesetzes

Ordentliche Mitglieder	Unterschrift	Stellvertretende Mitglieder	Unterschrift
SPD		**SPD**	
Castellucci Dr., Lars		Fechner Dr., Johannes	
Fograscher, Gabriele		Gerster, Martin	
Grötsch, Uli		Heidenblut, Dirk	
Gunkel, Wolfgang		Högl Dr., Eva	
Kampmann, Christina		Juratovic, Josip	
Lischka, Burkhard		Kolbe, Daniela	
Mittag, Susanne		Lühmann, Kirsten	
Özdemir (Duisburg), Mahmut		Poschmann, Sabine	
Reichenbach, Gerold		Rix, Sönke	
Schmidt (Berlin), Matthias		Spinrath, Norbert	
Veit, Rüdiger		Yüksel, Gülistan	
DIE LINKE.		**DIE LINKE.**	
Jelpke, Ulla		Dagdelen, Sevim	
Korte, Jan		Hahn Dr., Andre	
Renner, Martina		Karawanskij, Susanna	
Tempel, Frank		Pau, Petra	
BÜNDNIS 90/DIE GRÜNEN		**BÜNDNIS 90/DIE GRÜNEN**	
Amtsberg, Luise		Haßelmann, Britta	
Beck (Köln), Volker		Künast, Renate	
Mihalic, Irene		Lazar, Monika	
Notz Dr., Konstantin von		Mutlu, Özcan	

Stand: 17. April 2015
Referat ZT 4-Zentrale Assistenzdienste, Luisenstr. 32-34, Telefon: +49 30 227-32659, Fax: +49 30 227-36339

Bundesrat

Land	Name (bitte in Druckschrift)	Unterschrift	Amts-bezeichnung
Baden-Württemberg	Delmotte / Zaiser		ORR'in / ORR
Bayern	Landsmann		RD
Berlin			
Brandenburg	Bergt		Ref
Bremen			
Hamburg			
Hessen	HANTELL		RBe
Mecklenburg-Vorpommern			
Niedersachsen	Wana		ORRin
Nordrhein-Westfalen	Rolfin		Ref
Rheinland-Pfalz	Rauth		RR'in
Saarland			
Sachsen	Langer		Ref.
Sachsen-Anhalt	Störtenbecker		RRin
Schleswig-Holstein			
Thüringen	Müllenbach		RD'in

Stand: 20. Februar 2015
Referat ZT 4 – Zentrale Assistenzdienste, Luisenstr. 32-34, Telefon: +49 30 227-32659, Fax: +49 30 227-36339

Öff.

Tagungsbüro

Deutscher Bundestag

Sitzung des Innenausschusses (4. Ausschuss)
Montag, 20. April 2015, 14:00 Uhr

	Fraktionsvorsitz	Vertreter
CDU/CSU		
SPD		
DIE LINKE.		
BÜNDNIS 90/DIE GRÜNEN		

Fraktionsmitarbeiter

Name (Bitte in Druckschrift)	**Fraktion**	**Unterschrift**
Blumarsch, Matthias	CDU/CSU	[Unterschrift]
SCHEELE, JUERGEN	LINKE	[Unterschrift]
Pohl, Jörn	B90/Grüne	[Unterschrift]
Piallat, Chris	B90/Grüne	[Unterschrift]
Weinzierl, Elke	B90/Grüne	[Unterschrift]
Steden, Ulrike	SPD	[Unterschrift]

Stand: 20. Februar 2015
Referat ZT 4 – Zentrale Assistenzdienste, Luisenstr. 32-34, Telefon: +49 30 227-32659, Fax: +49 30 227-36339

Tagungsbüro

Sitzung des Innenausschusses (4. Ausschuss)
Montag, 20. April 2015, 14:00 Uhr

Seite 4

Ministerium bzw. Dienststelle (bitte in Druckschrift)	**Name** (bitte in Druckschrift)	**Unterschrift**	**Amts-bezeichnung**
BMI	PARIS		
"	DÜRIG		
"	[illegible]		
BMI	STAUSCHUS		
"	FUNKE		
BPOL	Landvogt		
BMI	[illegible]		
BKAmt	Papenkort		

Stand: 20. Februar 2015
Referat ZT 4 – Zentrale Assistenzdienste, Luisenstr. 32-34, Telefon: +49 30 227-32659, Fax: +49 30 227-36339

Anwesenheitsliste für Abgeordnete mitberatender Ausschüsse

Öffentliche Anhörung des Innenausschusses am Montag, 20. April 2015
IT-Sicherheit

Name (bitte in Druckschrift)	Unterschrift
Lämmel	
Jarzombek	
Hakverdi	

Innenausschuss

Liste der Sachverständigen

Öffentliche Anhörung am Montag, 20. April 2015, 14.00 Uhr

Michael Hange
Präsident des Bundesamtes für Sicherheit in der Informationstechnik

Prof. Dr. Gerrit Hornung
Universität Passau, Lehrstuhl für öffentliches Recht, IT-Recht und Rechtsinformatik

Linus Neumann
Chaos Computer Club (CCC), Berlin

Iris Plöger
Bundesverband der Deutschen Industrie e. V., Leiterin der Abteilung Digitalisierung

Prof. Dr. Alexander Roßnagel
Universität Kassel, Institut für Wirtschaftsrecht

Prof. Dr.-Ing. Jochen Schiller
Freie Universität Berlin, Institute of Computer Science

Dipl. Ing. (FH) Thomas Tschersich
Deutsche Telekom AG, Leiter Group Security Services

Dr. Axel Wehling
Gesamtverband der Deutschen Versicherungswirtschaft e. V., Mitglied der Hauptgeschäftsführung, Geschäftsführer des Krisenreaktionszentrums der deutschen Versicherungswirtschaft

Sprechregister der Sachverständigen und Abgeordneten

Tagesordnungspunkt

Gesetzentwurf der Bundesregierung

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

BT-Drucksache 18/4096

Vors. **Wolfgang Bosbach** (CDU/CSU): Meine Damen und Herren, liebe Kolleginnen und Kollegen, ich eröffne die 44. Sitzung des Innenausschusses. Ich begrüße Sie herzlich zur heutigen Sachverständigenanhörung über das IT-Sicherheitsgesetz. Insbesondere begrüße ich die Dame und die Herren Sachverständigen. Herzlichen Dank, dass Sie uns heute mit Ihrer Erfahrung und mit Ihrer Kompetenz für die anstehenden Beratungen zur Verfügung stehen. Wir dürfen uns zunächst auch bedanken für die Stellungnahmen, die uns von Ihnen bereits in schriftlicher Form übersandt worden sind. Die schriftlichen Stellungnahmen werden genauso wie das, was Sie uns heute im Ausschuss vortragen, was anschließend debattiert wird mit den Kolleginnen und Kollegen, Bestandteil der Gesamtdrucksache. Wir werden von der heutigen Sitzung ein Wortprotokoll anfertigen. Das Protokoll wird Ihnen dann zur Korrektur übersandt. Die Gesamtdrucksache besteht dann aus dem Protokoll dieser Sitzung und allen schriftlichen Stellungnahmen, und all das wird auch ins Internet eingestellt, damit jeder Zugriff nehmen kann. Normalerweise haben wir eine Verhandlungsdauer von gut zwei Stunden, aber bei der Zahl der Sachverständigen ist es auch möglich, dass wir das heute ausdehnen auf 16:30 Uhr bis maximal 17:00 Uhr – es muss nicht sein, es geht aber! Damit wir diesen Zeitrahmen einhalten, darf ich – und das mache ich jetzt seit sechs Jahren, das hat nie die gewünschte Wirkung, aber man soll auch nicht aufgeben, ich darf alle Sachverständigen bitten, im Eingangsstatement fünf Minuten Zeitdauer nicht zu überschreiten. Das ist auch ein Gebot der Fairness all denjenigen gegenüber, die nach Ihnen sprechen werden. Was Sie da in den fünf Minuten nicht unterbringen können – das ist kein Problem – machen Sie es wie wir Politiker: wenn Sie etwas anderes gefragt werden, sagen Sie ruhig zunächst das, was Sie in den fünf Minuten nicht mehr reinpacken konnten und kommen dann – wenn möglich – zur Beantwortung der Fragen! Nach Ihrem Eingangsstatement kommt die Frage- und Diskussionsrunde mit den Abgeordneten der Fraktionen im Bundes-tag und im Innenausschuss. Es beginnt der Präsident des Bundesamtes für Sicherheit in der Informationstechnik, Herr Hange. Herzlich willkommen, Sie haben das Wort.

SV Präs. **Michael Hange** (Bundesamt für Sicherheit in der Informationstechnik): Ja, vielen Dank Herr Vorsitzender. Ich möchte Ihnen, ergänzend zu meiner schriftlichen Stellungnahme, die herausragenden Punkte in Kürze vorstellen. Zunächst zur Ausgangslage: Der erstmals im Dezember 2014 veröffentliche Lagebericht zur IT-Sicherheit in Deutschland, die BITKOM-Studie, der Bericht von letzter Woche und nicht zuletzt die „Snowden-Enthüllungen“ zeigen uns, wie verletzbar der Cyber-Raum ist. Ausgangpunkt hierfür sind drei Charakteristika der heutigen Informationstechnik. Es ist zum einen die technologische Durchdringung und Vernetzung, alle physischen Systeme werden von der IT erfasst und schrittweise mit dem Internet verbunden. Es ist die Komplexität. Die Komplexität der IT nimmt durch vertikale und horizontale Integration der Wertschöpfungsprozesse erheblich zu, und es ist die Allgegenwärtigkeit, jedes System ist praktisch zu jeder Zeit, und von jedem Ort über das Internet erreichbar. Zur Gefährdungslage – die technologische Entwicklung und die Gefährdungslage sind natürlich in einem Zusammenhang zu betrachten und zunächst muss man feststellen, dass das Internet als Plattform für Angreifer höchst attraktiv ist. Es besteht ein geringer Aufwand, es gibt auch käuflich Dienste, sowie auch entsprechende Angriffswerkzeuge zu kaufen. Das Entdeckungsrisiko ist gering, das liegt nicht zuletzt an der Beschaffenheit des Internets, dass hier praktisch keine starke Authentisierung da ist. Die Masse der möglichen Ziele erweitert sich fortlaufend mit technologischer Durchdringung und Vernetzung. Und schließlich, Cyber-Angriffe kennen keine Grenzen, sie können von überall erfolgen. Zum zweiten, das möchte ich noch einmal herausstellen, sind die Schwachstellen in der Software systemimmanent. Das heißt, sie sind der häufigste Ausgangspunkt für die Entwicklung von Cyber-Angriffsmitteln, das heißt von Schadprogrammen. Um Ihnen hier einmal eine Zahl zu nennen, bei der üblichen Software-Entwicklung geht man

heute von zwei bis fünf Promille Schwachstellen-Fehler pro Programmzeile aus. Und bei den Firmen mit richtig guten sicherheitssensiblen Entwicklungsprozessen sind es immer noch 0,7 Promille. Somit findet man in den gängigen Betriebssystemen immerhin 40 Millionen Programmzeilen – aufwärts, fast 30 000 Schwachstellen, die sich als mögliche Schadprogramme nutzen lassen. Im Breitenspektrum von Cyber-Angriffen in der Bundesverwaltung sind das täglich mehr als 3 500, und die Bedeutung von sogenannten Advanced Persistent Threats (APT) nimmt enorm zu. Sie sind die hochwertigen Premium-Angriffe, die erstklassig getarnt, und damit schwer zu detektieren sind. – Fazit: immer mehr Anwendungen in Wirtschaft, Staat und Gesellschaft nutzen Potenziale der IT und treiben die Entwicklung voran. Also inzwischen, nur um eine Zahl zu nennen – die Anzahl der Apps, wohlvertraut – nähert sich der 1,5 Millionen-Grenze, allein basierend auf dem Android-Betriebssystem. Neben der Prävention zum Schutz vor Angriffen gewinnen auch die Fähigkeit der Detektion – weil man nicht mehr alles mit Prävention machen kann – und die Fähigkeit der qualifizierten Reaktionen auf Cyber-Angriffe an Bedeutung. Worin besteht nun der Handlungsbedarf? Mit der Technologieentwicklung rückt auch die Cyber-Sicherheit im KRITIS-Bereich (Umsetzungsplan) mehr in den Focus. Da der Aus-fall, oder eine Beeinträchtigung Kritischer Infra-strukturen erhebliche Auswirkungen für das Gemeinwohl haben kann, besteht Regelungsbedarf. Die bisherige freiwillige Zusammenarbeit um KRITIS, die – sagen wir einmal – sehr wertvoll war, um auch Methoden der Kooperation mit der Wirtschaft einzuüben, aber auch die Allianz für Cyber-Sicherheit, die ausgerichtet ist auf die KMU (Kleine und mittlere Unternehmen), sind und bleiben wichtig. Diese bisherige freiwillige Zusammenarbeit und die Allianz für Cyber-Sicherheit werden aber der Bedrohungslage angesichts des Risikos bei Kritischen Infrastrukturen nicht mehr gerecht. Mit der letzten BSIG-Novellierung im Jahr 2009 haben wir für die Bundesverwaltung die Meldepflicht, und wir haben auch speziell mit dem § 5 eine Gefahrenabwehr für Regierungsnetze mit speziellen Sensoren eingeführt. Diese gesetzlichen Grundlagen und die darauf basierende Methodenweiterentwicklung haben sich für die Bundesverwaltung bewährt. Nun ist der Zeitpunkt gekommen, um für die Sicherheit für die Kritischen Infrastrukturen sowie für Internet-Nutzer durch eine gesetzliche Regelung mehr zu tun. Zentrale Punkte sind die von den Branchen selbst zu erstellenden Mindeststandards, die eine Meldepflicht bei schwerwiegenden Sicherheitsvorfällen, eine erweiterte Warnpflicht des BSI sowie die Verpflichtung zur Erstellung eines jährlichen Lagebildes und die Möglichkeit, dass zentrale Produkte, die in Kritischen Infrastrukturen eingesetzt werden, durch das BSI geprüft werden können, beinhalten. – Und nicht zuletzt die Verbesserung der IT-Sicherheit der Bürgerinnen und Bürger durch Änderungen im Telemediengesetz (TMG) und im Telekommunikationsgesetz (TKG). Als Fazit möchte ich zusammenfassen: der Gesetzentwurf weist dem BSI eine aktiv präventive Rolle im Zusammenspiel mit den jeweiligen Aufsichtsbehörden zu. Der vorliegende Entwurf zum IT-Sicherheitsgesetz stellt aus meiner Sicht einen notwendigen und wichtigen Schritt für mehr Sicherheit, sowohl für Kritische Infrastrukturen als auch für Bürgerinnen und Bürgern in Deutschland dar.

Vors. **Wolfgang Bosbach** (CDU/CSU): Vielen Dank Herr Präsident, das war in jeder Hinsicht vorbildlich, Sie dürfen wiederkommen, und auch wenn es um Themen geht, für die Sie gar nicht zuständig sind, – Hauptsache Sie halten die fünf Minuten ein! … Nächster Sachverständiger ist Herr Prof. Hornung.

SV **Prof. Dr. Gerrit Hornung** (Universität Passau, Lehrstuhl für öffentliches Recht, IT-Recht und Rechtsinformatik): Vielen Dank Herr Vorsitzender und vielen Dank auch für die Einladung. Meine Damen und Herren, die Verbesserung der IT-Sicherheit ist ein essentielles Problem der Informationsgesellschaft, und zur Bedeutung hat Herr Hange eben schon viel mehr gesagt, als ich das im Detail tun könnte. Ich glaube, dass der Gesetzentwurf eine relevante Frage adressiert und dazu eine sinnvolle Strategie verfolgt. Dass es ein sinnvoller Ansatz ist, zeigt sich auch daran, dass wir auf europäischer Ebene im Moment ein paralleles Gesetzgebungsvorhaben haben, auf das ich gleich an einigen Stellen etwas näher eingehen möchte. Ich möchte in aller Kürze etwas zu drei Punkten sagen, nämlich zu den inhaltlichen Standards, zu den Meldepflichten und zu den Sanktionen. Ich beschränke mich dabei auf den Gesetzentwurf,

möchte aber bei der Gelegenheit darauf hinweisen, dass dieser Entwurf zwar ein relevantes Problem adressiert, aber sicherlich nur ein Baustein von ganz vielen anderen sein kann, die wir im Bereich der IT-Sicherheit brauchen. Wir können sicher in der Diskussion später auch noch über ergänzungsbedürftige Pläne und Fragestellungen sprechen. Zunächst also erstens zu den inhaltlichen Standards. Ziel des Entwurfes ist es, das Niveau der IT-Sicherheit zu verbessern. Der Entwurf adressiert das unter anderem dahingehend, dass der Stand der Technik, der ein wichtiger Benchmark ist für das, was dort passieren soll, zu berücksichtigen ist. Berücksichtigen, meine Damen und Herren, ist weniger als Einhalten, und deswegen aus meiner Sicht zu wenig. Zumindest ist unklar, wann denn das, was dort vorgegeben ist, letztlich wirklich erreicht wird. Denn wenn weniger als der Stand der Technik adressiert wird oder ausreichen soll, muss ja klar sein, was denn ausreicht. Dafür sind Branchenstandards der betroffenen Verbände sicherlich ein probates Mittel, diese werfen aber eigene Probleme auf, die wir vielleicht gleich auch noch näher vertiefen werden. Zweite Frage, wie weist man denn nach, dass man den Stand der Technik, oder gegebenenfalls weniger als den Stand der Technik einhält? Der Entwurf nennt hierzu Zertifizierungen, Audits und Prüfungen. Insbesondere der Bereich der Audits ist völlig ungeregelt hinsichtlich der Fragen, wer diese Audits durchführen soll, nach welchen Standards und Verfahren das erfolgen soll. Aus meiner Sicht ist das unzureichend, ich glaube, wir brauchen hier eine Regelung darüber, was dort genau passieren soll. Insbesondere eine Pflicht, die Härte der Systeme durch entsprechende Angriffe tatsächlich zu prüfen, und eine Pflicht, die nicht nur auf Hersteller-Erklärungen vertraut. Der zweite Punkt: die Meldepflichten. Zunächst zum Anwendungsbereich. Der Gesetzentwurf sieht insoweit einige Sonderregelungen für die Bereiche Telekommunikation, Energie- und Atomanlagen vor, das mag man rechtfertigen können. Wofür sich meiner Meinung nach nicht so richtig eine Rechtfertigung ergibt, sind die terminologischen Abweichungen. Der TKG-Bereich formuliert teilweise deutlich abweichend, im Bereich des Energiewirtschaftsrechts ebenfalls, und der Rechtsanwender fragt sich dann immer, ist mit unterschiedlicher Terminologie unterschiedlicher Inhalt gemeint? – Wenn dies nicht der Fall sein sollte, denke ich, sollte man hier auch terminologisch einheitlich vorgehen. Der Bereich der hoheitlichen Anwender wird von dem Gesetz nicht adressiert. Herr Hange hat eben darauf hingewiesen, dass wir dazu bereits Regelungen haben im BSI-Gesetz. Aus meiner Sicht ist es aber nicht so richtig einsichtig, warum diese Regelungen anders sein sollen, als die, die für die Kritischen Infrastrukturen in der Wirtschaft gelten. Ich denke, wenn – dann sollten wir einheitliche Standards, einheitliche Prozesse haben, sowohl für die Kritischen Infrastrukturen der öffentlichen Verwaltung als auch für die in der Wirtschaft. Was mir am Herzen liegt, ist der Umgang mit den Informationen, die das BSI hier einsammelt, und zwar in mehrfacher Hinsicht. Erstens hinsichtlich der berechtigten Interessen der Betreiber. Denn das BSI wird ja eine Menge Informationen bekommen, die sensible Informationen der beteiligten Wirtschaft umfassen werden. Nun will ich dem BSI nicht unterstellen, dass es sorglos mit diesen Informationen umgehen wird, aber es ist doch auffällig, dass wir nur im Bereich des Energiewirtschaftsrechts eine wirkliche Pflicht haben, dass eine unbefugte Offenbarung auszuschließen ist. Wieso das nicht in allgemeiner Hinsicht im BSI-Gesetz aufgenommen wurde, weiß ich nicht. Umgekehrt glaube ich allerdings auch, dass das BSI – unter Berücksichtigung dieser Betreiberinteressen – mehr tun sollte, was die Öffentlichkeitsarbeit angeht. Die Information der Betreiber ist ok, die Information Dritter aus meiner Sicht unzureichend. Denn dort werden nur die ablehnenden Interessen, nämlich die Interessen der wirtschaftlichen Betreiber genannt, nicht mit den Informationen an die Öffentlichkeit gedrängt zu werden. Das ist berechtigt, aber ich glaube, wir sollten zu einer Interessenabwägung kommen mit den Interessen der Antragsteller. Außerdem haben Antragsteller das Problem, dass sie vielleicht gar nicht wissen, dass sie einmal einen Antrag stellen sollten - und wenn sie nicht informiert werden, haben sie keinen Anlass dazu, einen solchen Antrag zu stellen. Die gegenläufigen Interessen müssen wir natürlich berücksichtigen. Wir dürfen Kriminelle nicht darauf hinweisen, wo Sicherheitslücken in IT-Systemen sind. Ich glaube aber, dass das Problem sich lösen lässt, indem eben dem Schließen von Lücken Vorrang gegeben wird, und man solange nicht informiert wird, bis diese Lücken geschlossen sind. Diesen Ansatz verfolgt

etwa das Datenschutzrecht derzeit ebenfalls. Die Information der Öffentlichkeit ist schließlich im Entwurf überhaupt nicht adressiert, jedenfalls nicht hinsichtlich der Informationen, die hier auf Basis der Meldepflichten eingesammelt werden. Wir haben eine allgemeine Warn- und Hinweismöglichkeit des BSI. Die bezieht sich aber gerade nicht auf diese neue Aufgabe, die hier eingeführt wird und das halte ich für ergänzungsbedürftig. Im Übrigen sieht auch die Europäische Richtlinie – und zwar in allen Versionen, also sowohl Parlament als auch Rat als auch Kompromissentwürfe – vor, dass eine Möglichkeit bestehen soll und teilweise eine Pflicht, an die Öffentlichkeit zu gehen mit diesen Informationen. Dritter Punkt, fehlende Sanktionen. Der Entwurf verfolgt einen kooperativen Ansatz in Zusammenarbeit mit den Betreibern kritischer Infrastrukturen. Das halte ich für gut. Aber nicht alle Betreiber sind immer kooperativ. Und deswegen – glaube ich – braucht das BSI Durchsetzungsbefugnisse und Sanktionen. Auch das sieht im Übrigen der europäische Entwurf vor, nämlich effektive Sanktionen und erweiterte Anordnungsbefugnisse. Die europäischen Vorschläge sehen unter anderem vor, dass die Aufsichtsbehörden Anweisungen zur Durchführung von Sicherheitsaudits geben können sollen. Auch das findet sich im Entwurf derzeit nicht. Im vorliegenden Entwurf haben wir also keine allgemeinen Sanktionsmöglichkeiten, aber auch eine Ungleichbehandlung, die verfassungsrechtlich aus meiner Sicht nicht zu rechtfertigen ist. Wir haben nämlich Bußgeldtatbestände, aber nur für den Telekommunikationsbereich. Und wieso jetzt von allen kritischen Infrastrukturen, die wir jetzt regeln, nur der Telekommunikationsbereich einer sein soll, wo wir Bußgeldtatbestände brauchen – das ist aus meiner Sicht nicht zu rechtfertigen. Soviel zu meinen drei Punkten. Abschließend noch der kurze Hinweis zu § 100 Abs. 1 TKG. Die Norm ist in der Diskussion ja teilweise als kleine Vorratsdatenspeicherung bezeichnet worden. Dazu möchte ich nichts weiter sagen, weil der Kollege Roßnagel dazu gleich noch einiges mehr ausführen wird. Ich beschränke mich deswegen darauf zu sagen, dass ich insoweit mit ihm einer Meinung bin. Vielen Dank.

Vors. **Wolfgang Bosbach** (CDU/CSU): Ja vielen Dank Ihnen, Herr Prof. Hornung. Unser nächster Sachverständiger ist vom Chaos Computer Club hier in Berlin. Herr Linus Neumann, Sie haben das Wort.

SV **Linus Neumann** (Chaos Computer Club (CCC), Berlin): Ja, vielen Dank Herr Vorsitzender, ich bedanke mich für die Einladung. Wir wollen uns hier mit technischen Problemen auseinandersetzen und dies in einem Gesetz adressieren. Das ist eine relativ schwierige Aufgabe, denn am Ende müssen wir technische Probleme lösen und wir gehen da mit dem Werkzeugkasten der Juristen daran und versuchen, uns Regulationen herbeizuführen, die zu einer Erhöhung der IT-Sicherheit führen sollen. Eine Erhöhung der IT-Sicherheit ist aus meiner Perspektive auf zwei Wegen möglich, wir können einmal auf eine Härtung hinarbeiten. Das heißt, im Schadensfall wird der mögliche Schaden begrenzt. Also ich richte ein System so aus, dass es quasi den Angriff schon vorhersieht und sagt, wenn der Angreifer mich dann übernommen hat, dann hat er trotzdem nur möglichst wenig Kontrolle über mich oder meine Daten. Das sind Maßnahmen, die ich unter der Härtung zusammenfasse. Und es gibt natürlich noch die Prävention, wir haben es gerade gehört, ungefähr fünf Bugs pro 1000 Zeilen Code, die sicherheitsrelevant sein sollen. Die kann man finden und die kann man entfernen. Das ist eine große Arbeit, der ich seit Jahren beruflich nach-gehe. Aber das ist natürlich am Ende die einzige Möglichkeit, ein Sicherheitsrisiko loszuwerden, indem man es wirklich entfernt. Unter dieser Perspektive habe ich mir diesen Gesetzentwurf angeschaut und mir angeschaut, wo gibt es denn Anreize, eine Erhöhung der technischen IT-Sicherheit tatsächlich herbeizuführen. Als erstes fällt mir auf, wenn ich mir das anschaue, dass wir hier einen sehr großen Focus auf Kritische Infrastrukturen haben, ja – was nicht schlecht ist. Wir haben als Chaos Computer Club auch davor gewarnt, dass die Kritischen Infrastrukturen in Deutschland nicht ausreichend geschützt sind. In seinem Lagebericht der IT-Sicherheit 2009 schreibt das Bundesamt für Sicherheit in der Informationstechnik allerdings, „… bei den Betreibern der sogenannten Kritischen Infrastrukturen können IT-Sicherheitsbewusstsein und Kompetenz sowohl auf Managementebene als auch in der Umsetzung durchweg als hoch eingeschätzt werden.“ Wie gesagt, wir

teilen diese Auffassung nicht. In seinem Lagebericht 2014 schreibt das BSI einmal von 16 Millionen und einmal 18 Millionen Fällen von Identitätsdiebstahl. Sie erinnern sich, damit war das BSI dann auch sehr groß in den Medien, weil es sich nicht besonders gut darum gekümmert hat, die Person dann auch über ihre Probleme in Kenntnis zu setzen. Gleichzeitig sehen wir hier in diesem Gesetzentwurf, während wir 16 Millionen Angriffe auf Bundesbürger haben, einen starken Focus auf genau diese Kritischen Infrastrukturen, die angeblich ja schon so stark geschützt sind. Wir würden uns hier natürlich wünschen, dass der Endnutzer-schutz eine sehr viel größere Rolle bekommt, nämlich die, die dem Endnutzerschutz – in Anbetracht der Bedrohungslage offensichtlich – auch angemessen wäre. – Ein kleiner Scherz am Rande, in diesem Sicherheitsbericht zur Lage der IT-Sicherheit wird ein Angriff auf Kritische Infrastruktur dokumentiert in 2014. Da wurde Mitarbeitern einer Kritischen Infrastruktur mit Hilfe eines Fishing-Angriffs das Gehaltskonto übernommen und dann Geld überwiesen. Also da waren auch wieder Bürger und Endnutzer die Opfer und die Kritische Infrastruktur wurde trotz des erfolgreichen Angriffs verschont. Weiterhin stört mich sehr an diesem Gesetzesentwurf, dass dort jegliche Proaktivität fehlt. Wir haben gerade schon den Begriff gehört des Standes der Technik, der eingehalten werden soll. Stand der Technik ist grundsätzlich das, was wir gerade vorfinden. Das heißt, der wird grundsätzlich per Definition schon eingehalten. Interessant ist es, wenn wir sagen, wir gehen als Gesetzgeber hin, und wir wollen Menschen vor dem Angriff auf die IT-Systeme schützen. Dann müssen wir diese technische Sicherheit erhöhen, und das können wir nicht durch Meldepflichten machen, die grundsätzlich nur den Fall betreffen, wenn der Angriff schon erfolgt ist und im Zweifelsfall erfolgreich war. Also eine Meldepflicht hat noch keinen Hack verhindert. Wir haben dann Sicherheitskonzepte, die für die Wirtschaft und die für die Kritischen Infrastrukturbetreiber vorgesehen sind, um dieser Rechtsunsicherheit des Standes der Technik zu entfliehen. Ja, das steht relativ klar, … muss Stand der Technik genügen …, kein Mensch weiß, was Stand der Technik ist. Also müssen wir ein Sicherheitskonzept beim BSI einreichen als Betreiber Kritischer Infrastrukturen. Dann sagt das BSI, … ja, so ist es in Ordnung, das ist Stand der Technik, jetzt seid Ihr diese Rechtsunsicherheit los. So funktioniert ja dieses Gesetz. Man kann sich ungefähr vorstellen, was jetzt los ist, wenn diese ganzen Kritischen Infrastrukturbetreiber sich in ihren Verbänden treffen müssen, ihre existierenden Sicherheitskonzepte alle auf einen Tisch legen müssen, die natürlich größtenteils die gleichen Sachen abdecken, aber natürlich in komplett anderer Sprache formuliert sind, anders geclustert, anders strukturiert sind. Da muss man sich dann irgendwann zusammensetzen und sagen, jetzt machen wir ein gemeinsames Sicherheitsgesetz für den Telekommunikationssektor, als Beispiel. Das soziale Dilemma der Menschen, die da in diesem Raum sitzen und den gemeinsamen Entwurf vorschlagen müssen, besteht doch darin: Schreiben wir jetzt einen Sicherheitsstandard, den wir alle schon erfüllen? Oder schreiben wir einen, den wir alle noch nicht erfüllen? – Und der für uns alle mit unterschiedlichen Investitionen verbunden ist. Ich möchte da jetzt niemandem etwas unterstellen, aber wenn ich in dieser Situation wäre – das gebe ich freimütig zu – ich würde zusehen, diesen Sicherheitsstandard möglichst gering zu halten, um mir meine eigenen Probleme bei dessen Einhaltung auch entsprechend zu verringern. Wir haben dann den Punkt des § 100 TKG, wo eine zeitlich unbegrenzte Datenvorhaltung legitimiert wird, zum Zwecke des Erkennens, des Eingrenzens und des Beseitigen von Störungen. Dabei wird offenkundig außer Betracht gelassen, dass Störungen akute Phänomene sind, die ich akut behandeln muss, akut lösen muss. Und da hilft mir sicherlich nicht ein für mehrere Tage – oder sogar, wie der Arbeitskreis Vorratsdatenspeicherung dokumentiert hat – ein bis zu 180 Tage zurückreichender Datensatz, was ich alles für Verkehrsdaten in meinem System hatte. Das heißt, das ist alles Unsinn und da wären mindestens eine zeitliche Eingrenzung und auch eine Eingrenzung des Verwendungszweckes notwendig. Aber selbst dann, wäre dieser Paragraph immer noch unsinnig. Zuletzt – ich habe das schon in einer anderen Stellungnahme angesprochen – deswegen fasse ich mich kurz: wir haben bei dem BSI einen inhärenten Interessenkonflikt, weil es dem Bundesministerium des Innern untergeordnet ist. Das Bundesministerium des Innern ist nicht nur im defensiven Bereich der IT-Sicherheit tätig, sondern auch sehr aktiv im offensiven Bereich der IT-Sicherheit. Sie haben hier

vor Kurzem dokumentiert – also dokumentiert hat es die Presse, Sie haben es besprochen – die Wunschliste des BND, der sich also in offensiven Fragen der IT-Sicherheit ein sehr viel größeres Budget wünscht, und wir haben vor Kurzem eine Veröffentlichung gehabt, in der festgestellt wurde, dass das Bundesamt für Sicherheit in der Informationstechnik auch die Entwicklung von Staatstrojanern unterstützt, also von Maßnahmen, die nun wirklich nicht unter IT-Sicherheit fallen, sondern die im offensiven Bereich liegen. Das heißt, als eine zentrale Meldestelle für IT-Sicherheitsvorfälle ist das BSI grundsätzlich nicht geeignet, solange es diesem Interessenkonflikt unterliegt. Deswegen plädiere ich erneut für die Aufstellung des BSI als eigenständige Bundesbehörde mit eindeutigem Sicherheitsauftrag.

Vors. **Wolfgang Bosbach** (CDU/CSU): Wir danken Ihnen Herr Naumann. Wir begrüßen noch den Staatssekretär aus dem Bundesministerium des Innern, Herrn Dr. Schröder, und kommen jetzt zum nächsten Sachverständigen, vom Bundesverband der Deutschen Industrie, Frau Plöger, herzlich willkommen. Bitteschön.

SV **Iris Plöger** (Bundesverband der Deutschen Industrie e. V., Leiterin der Abteilung Digitalisierung): Vielen Dank verehrter Herr Vorsitzender, herzlichen Dank für die Einladung zur heutigen Anhörung. Der BDI begleitet das IT-Sicherheitsgesetz von Beginn an konstruktiv. Deshalb nehmen wir gern heute zum Gesetzentwurf Stellung. Ich verrate kein Geheimnis, wenn ich sage, dass der BDI den Maßnahmen des Gesetzes, insbesondere der Meldepflicht, in der letzten Legislaturperiode besonders kritisch gegenüber stand und weiterhin steht. Aufwand und Nutzen der Meldepflicht stehen in keinem ausgewogenen Verhältnis. Den Unternehmen entstehen durch die im Gesetz vorgesehenen Maßnahmen erhebliche finanzielle Aufwände, zum Beispiel durch die Einrichtung der Prozesse im Managementsystem, Systembetreuung, wiederkehrende Zertifizierung, Kosten für Technik etc. Der Nutzen ist aber nicht einschätzbar. Die deutsche Industrie hat ein hohes Eigeninteresse, die Funktionsfähigkeit und Verfügbarkeit ihrer IT-Systeme nachhaltig abzusichern. Das Sicherheits-niveau der Unternehmen wird daher stetig verbessert. Wir waren und sind der festen Überzeugung, dass eine Meldepflicht allein nicht zu dem gewünschten Ziel führt, die Kritischen Infrastrukturen in Deutschland sicherer zu machen, da es ein reaktives Instrument ist. Vielmehr sind wir der Ansicht, dass bereits bestehende IT-Sicherheitsstrukturen in Unternehmen und die freiwillige Zusammenarbeit zwischen Industrie und Behörden im Rahmen der CERT´s und der Initiativen wie die Allianz für Cyber-Sicherheit sehr gut funktionieren und weiter ausgebaut werden sollten. Unabhängig von der privatwirtschaftlichen Eigeninitiative haben wir uns mit eigenen Vorstellungen bereits 2014 eingebracht. Der BDI hat gemeinsam mit seinen Mitgliedsverbänden BDLI, BDSV, BITKOM und ZVEI die Studie „IT-Sicherheit in Deutschland. Handlungsempfehlungen für eine zielorientierte Umsetzung des IT-Sicherheitsgesetzes“ bei der Wirtschaftsprüfungsgesellschaft KPMG in Auftrag gegeben. Ziel der Studie war es, konkrete Handlungsempfehlungen für die Ausgestaltung eines IT-Sicherheitsgesetzes zu präsentieren. Ich möchte an dieser Stelle auf die sechs wichtigsten Punkte zum Gesetzentwurf eingehen. Erstens, Kritische Infrastrukturen klar definieren. Der BDI hält es für äußerst problematisch, dass zentrale Definitionen, wie zum Beispiel die konkrete Definition zur Kritischen Infrastruktur, im Gesetz nicht hinreichend bestimmt werden. Zum jetzigen Zeitpunkt ist nicht klar, an wen sich das Gesetz konkret richtet. Um Rechtssicherheit für die betroffenen Unternehmen zu schaffen, sollte die Definition hinreichend präzise sein und direkt im Gesetz erfolgen. Unternehmen können nicht erst bei Inkrafttreten des Gesetzes erfahren, ob sie betroffen sind. Denn die Umsetzung der Maßnahmen in den Unternehmen wird erhebliche Zeit in Anspruch nehmen. Auch ist der Staat der größte Betreiber Kritischer Infrastrukturen und hat damit eine ebenso hohe Bedeutung für das Funktionieren des Gemeinwesens. Der BDI setzt sich daher nachdrücklich dafür ein, dass die entsprechenden Meldepflichten und Sicherheitsstandards neben dem Bund auch für den Staat gelten und vom Gesetz erfasst werden. Das Schutzgut des Gesetzes ist die Funktionsfähigkeit Kritischer Infrastrukturen – und es ist kein sachlicher Grund für die Ungleichbehandlung von öffentlicher und privater Trägerschaft ersichtlich. Eine Gleichstellung würde die Akzeptanz für das Gesetz deutlich erhöhen. Zudem wird sich das BSI nur dann ein vollständiges Sicherheitslagebild verschaffen können, wenn öffentliche und private Betreiber Kritischer Infrastrukturen

gleichermaßen Sicherheitsvorfälle melden. Zweitens: Umfang und Inhalt der Melde-pflichten. Der Umfang und der zeitliche Rahmen der Meldepflicht sind im Gesetzentwurf nicht hinreichend bestimmt. Im vorliegenden Gesetzentwurf wird die Meldung von erheblichen Störungen der IT-Infrastruktur gefordert. Die Definition in Artikel 1 § 8b ist aus Sicht der deutschen Industrie nicht hinreichend und sollte weiter präzisiert werden. Für die Unternehmen ist nicht ersichtlich, in welchem Fall eine erhebliche Störung vorliegt, die gemeldet werden müsste. Zudem sollte die Weitergabe von Daten gesetzlich ausgeschlossen werden, die über die allgemeine Darstellung des Sicherheitslagegebildes hinausgehen und Rechte Dritter verletzen können. Drittens, Mindeststandards. Die vorgesehenen branchenspezifischen Mindeststandards für IT-Sicherheit sind gut und richtig, da sie der Individualität der jeweiligen Branchen Rechnung tragen. Sie sollten zudem kompatibel mit der geplanten europäischen Gesetzgebung sein. Der BDI wird sich gerne in diesen Prozess einbringen. Viertens, höchstmögliche Kompatibilität zwischen IT-Sicherheitsgesetz und der europäischen NIS-Richtlinie. Die Regelungen des IT-Sicherheits-gesetzes müssen zwingend mit der EU-Cyber-Sicherheitsrichtlinie abgestimmt werden und kompatibel sein. Wir sehen mit großer Sorge, dass das IT-Sicherheitsgesetz und die NIS-Richtlinie derzeit nicht im Einklang stehen, insbesondere beim Anwendungsbereich und den Sanktionen. Sollte es dabei bleiben, wären unterschiedliche nationale und europäische Vorgaben die Folge, ein Worst-Case-Szenario für unsere Unternehmen. Wir appellieren deshalb an die Bundesregierung, unterschiedliche Vorgaben unter allen Umständen zu vermeiden. Fünftens, keine Doppelregulierung. Betreiber Kritischer Infrastrukturen sind bereits durch bestehende Rechtsvorschriften reguliert. Zu nennen sind das Telekommunikationsgesetz (TKG), das Energiewirtschaftsgesetz (EnWG) oder das Bundesdatenschutzgesetz (BDSG). Hier darf es nicht zu Doppelregulierungen bzw. Doppelzuständigkeiten kommen. Sechstens, Chancen des IT-Sicherheitsgesetzes nutzen und die Zusammen-arbeit zwischen Industrie und BSI ausbauen. Die Zusammenarbeit zwischen Unternehmen und Staat darf keine Einbahnstraße sein. Informationen dürfen nicht nur im Sinne einer Meldepflicht von Unternehmen an die Behörden fließen und damit den Bürokratieaufwand der Unternehmen erhöhen. Vielmehr müssen Informationen über Bedrohungen zeitnah, aktuell und praxisorientiert vom BSI an die Unternehmen zurückgegeben werden. Die bisherigen Lageberichte, zum Beispiel im Rahmen der Allianz für Cyber-Sicherheit sollten anwendungsorientierter und tagesaktuell sein. Bestehende und erfolgreiche Initiativen, wie die Allianz für Cyber-Sicherheit, sind weiter zu stärken. Inzwischen hat die Allianz mehr als 1 000 Teilnehmer, darunter sind viele Dax-Unternehmen, aber auch kleine und mittlere Unternehmen. Der BDI unterstützt die Arbeit der Allianz von Beginn an sehr aktiv. Wir freuen uns, in den kommenden Wochen gemeinsam mit dem Bundestag und dem Bundesrat, mit den zuständigen Bundesministerien und den Sicherheitsbehörden weiter an der Ausgestaltung des IT-Sicherheitsgesetzes zu arbeiten. Herzlichen Dank.

Vors. **Wolfgang Bosbach** (CDU/CSU): Vielen Dank Frau Plöger. Unser nächster Sachverständiger kommt von der Universität in Kassel, Herr Prof. Dr. Roßnagel, Sie haben das Wort.

SV **Prof. Dr. Alexander Roßnagel** (Universität Kassel, Institut für Wirtschaftsrecht): Ja meine sehr verehrten Damen und Herren, vielen Dank für die Einladung und die Gelegenheit, hier sprechen zu können. Ich möchte nur fünf Themen ansprechen, der Rest wird dann wohl Gegenstand der Diskussion sein, hoffentlich.
Erstens, der Gesetzentwurf ist grundsätzlich zu begrüßen. Er verfolgt die Ziele, die Informationstechnik in Kritischen Infrastrukturen sicherer zu machen sowie den Schutz von Unternehmen und Bürgerinnen und Bürgern im Internet zu verstärken. Auch wenn der Name IT-Sicherheitsgesetz mehr verspricht, als seine Regelungen verfolgen, sind diese Ziele zu unter-stützen. Die dafür vorgesehenen Maßnahmen sind grundsätzlich geeignet, auch erscheinen mir die damit verbundenen Grundrechtseingriffe bei den betroffenen Unternehmen grundsätzlich erforderlich und verhältnismäßig.
Zweitens, die Definition Kritischer Infrastrukturen im § 2 des neuen BSI-Gesetzes erscheint mir zusammen mit der Verordnungsermächtigung in § 10 – auch mit Blick auf Artikel 80 GG – ausreichend. Um die notwendige Rechtssicherheit zu erreichen, wird es notwendig sein, die betroffe-

nen Einrichtungen, Anlagen und Teile in Kritischen Infrastrukturen so detailliert zu beschreiben, wie dies etwa für immissionsschutz-rechtlich genehmigungsbedürftige Anlagen in der Vierten Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes der Fall ist – das heißt, über 20 oder 30 Seiten hinweg detaillierte Merkmale für die erfassten Anlagen. Dieser Detaillierungsgrad ist für eine gesetzliche Definition ungeeignet, sachlich aber geboten. Die in § 4 Bundes-Immissionsschutzgesetz enthaltene Ermächtigungsgrundlage für diese Verordnung ist erheblich weniger präzise als die in dem Entwurf vorfindliche Regelung, und dennoch mit Artikel 80 GG vereinbar.

Drittens, die im § 8a vorgesehenen angemessenen organisatorischen und technischen Sicherheitsvorkehrungen sind erforderlich, um ein gleichmäßiges Mindestniveau an IT-Sicherheit in allen Kritischen Infrastrukturen zu erreichen. Um dem enormen Schadenspotenzial zu entsprechen und ein tatsächlich nachprüfbares Mindestniveau zu erreichen, sollte der Stand der Technik nicht nur berücksichtigt, sondern eingehalten werden. Dies schließt alternative Vorkehrungen auf gleichem Niveau nicht aus. Sofern branchenspezifische Standards dieses Niveau erreichen, sind sie als problem-adäquate und branchengerechte Vorgaben zu begrüßen. Ohne Anforderungen an die Hersteller von Soft- und Hardware stoßen die Betreiber Kritischer Infrastrukturen sehr schnell an faktische Grenzen, weil sie die von ihnen eingesetzte Technik nicht selbst verbessern können. Die materiellen Anforderungen an die Sicherheitstechnik sind wirkungslos, wenn ihre Erfüllung nicht in regelmäßigen Abständen nachgewiesen werden muss. Die Nachweise sind jedoch aus Gründen der Rechtssicherheit präziser zu bestimmen. Die Sicherheitspflichten des § 8a sollten nicht generell ausgeschlossen sein, wenn andere Rechtsvorschriften gelten, die weitergehend oder vergleichbar sind. Vielmehr sollten die Ausnahmen nur insoweit gelten, als andere Regelungen weiter-gehend und vergleichbar sind.

Viertens, das durch den Entwurf verfolgte kooperative IT-Sicherheits-Informationssystem ist zu begrüßen. Das Gleiche gilt für die Zweistufung in anonym zu meldende Vorfälle im Vorfeld einer Beeinträchtigung und in identifizierend zu meldende Vorfälle bei Beeinträchtigungen. Wann eine Meldepflicht der betroffenen Unternehmen – insbesondere im Vorfeld – besteht, sollte jedoch präziser geregelt werden. Hinsichtlich der Ausnahmen ergeben sich die gleichen Schwierigkeiten wie bei den Sicherheitspflichten, wenn es um andere Rechtsvorschriften geht, die vergleichbar oder weitergehend sind. Auch hier würde eine Flexibilisierung durch eine „Soweit“-Regelung den Vollzug erleichtern. Insbesondere, weil die Regelungen des § 8b und die anderen Regelungen kombinierbar sind. Warum soll in diesem Fall zum Beispiel, die Zweistufung in anonyme und identifizierende Meldungen oder die Möglichkeit gemeinsamer übergeordneter Ansprechstellen nicht gelten? Verbessert werden muss die Information der Öffentlichkeit oder einzelner Nutzer über Sicherheitslücken oder Sicherheitsmaßnahmen. Vor dem Hintergrund der Schutzpflicht des Staates muss die Information die Regel, und deren Verweigerung aus übergeordneten Interessen die Ausnahme sein. Also keine Abwägung, ob ausnahmsweise informiert wird, sondern umgekehrt: eine Abwägung, ob die Information ausnahmsweise unterlassen wird. Dabei kann oft der Konflikt schon durch die Art und Weise, wie das BSI informiert, gelöst werden. Schließlich ist festzuhalten, dass die Pflichten der Betreiber Kritischer Infrastrukturen in § 8a und § 8b sanktionsbewehrt sein müssen, wenn eine Möglichkeit bestehen soll, Sicherheitspflichten der Betreiber und den kooperativen Ansatz eines Informationssystems auch durchzusetzen.

Fünftens: abschließend will ich kurz auf § 100 TKG eingehen. Der Gesetzentwurf erweitert zwar nur den Begriff der Störung und übernimmt damit die Rechtsprechung des Bundesgerichtshofes. Damit bleibt aber eine Regelung unkorrigiert, die nach der Rechtsprechung sowohl des EuGH als auch des Bundesverfassungsgerichts viel zu unbestimmt ist. Die Vorschrift erlaubt anlasslos und flächendeckend die Speicherung von Verkehrsdaten, ohne Beschränkung auf das absolut Notwendige – was der EuGH fordert – ohne zu dokumentierenden Eingriffsanlass, ohne Schutzvorkehrungen gegen Missbrauch, ohne Zweckbegrenzungen der Verwendung, ohne Begrenzung der Speicherzeit und ohne Ausnahmen etwa für Berufsgeheimnisträger. Diese Regelung muss entsprechend der jüngsten Rechtsprechung dieser beiden obersten Gerichte eingeschränkt werden.

Ich bedanke mich für die Aufmerksamkeit.

Vors. **Wolfgang Bosbach** (CDU/CSU): Wir danken Ihnen. Jetzt Herr Prof. Dr. Schiller.

SV **Prof. Dr.-Ing. Jochen Schiller** (Freie Universität Berlin, Institute of Computer Science): Vielen Dank Herr Vorsitzender, meine Damen und Herren. Stellen Sie sich einfach einmal vor, Sie kaufen sich den smarten Backofen, der selbstverständlich neue Backprogramme aus dem Internet laden kann, so wie dies heute auch schon entsprechend für viele Geräte möglich ist. Die Steuerung des Backofens übernimmt ein eingebetteter Web-Server, über den auch per Smartphone-App der Zustand abgefragt, der Ofen gesteuert werden kann. Wie auch immer, wird eine Schadstoffsoftware auf den Server geschleust, welche die automatische Temperaturabschaltung manipuliert und so nicht nur Ihren Kuchen, sondern vielleicht auch gleich die ganze Wohnung verkohlt. Der Brandschaden ist da, nur wer ist schuld, wer haftet? Ist es der Backofen-hersteller, welcher keine geeignete Firewall im Backofen hatte, nicht die aktuellsten Sicherheits-Updates automatisch installiert hat? Ist es der Nutzer, der Hersteller des Handys, der es ermöglicht hat, dass Schadstoffsoftware auf dem Handy die Steuerungs-App manipuliert? Ist es letztendlich ein schwer greifbarer Hacker, der entsprechende Software auf das Handy installiert hat, dies aber nur konnte, weil der Betriebssystemhersteller des Handys Lücken in seinem Betriebssystem hat? Oder war das alles nur ein Zufall, ausgelöst durch das Zusammentreffen ungünstiger Parameter? Mir ist vollkommen bewusst, dass ein Backofen keine Kritische Infrastruktur im Sinne des geplanten Gesetzes ist. Leider sieht aber die Situation im industriellen Umfeld nicht wirklich anders aus, ist nur deutlich komplexer in der Erklärung. Auch hier können Motoren bewusst überlastet, Absicherungen ausgehebelt oder Ventile übersteuert werden. Auch hier steuern immer mehr eingebettete Computer mit Web-Servern vielfältige Systeme. Natürlich weisen diese Systeme eine deutlich höhere Komplexität als mein Backofen auf. Umso unglaublicher ist es, wenn man hört, dass diese Systeme teilweise kaum abgesichert sind, auf Kundenwunsch sogar auf Passwörter fest eingestellt, oder gleich ganz weggelassen werden. Haben wir wirklich das richtige Sicherheitsbewusstsein? Viele Lücken sind seit Jahrzehnten bekannt und werden auch ausgenützt. Nun auch auf sogenannten eingebetteten Systemen, die man nicht ausschalten kann, die nicht einfach aktualisiert werden können, aber keiner unternimmt etwas Wirkungsvolles. Es ist also dringend ein grundlegender Bewusstseinswandel nötig, vom Produzenten bis zum Verbraucher, quer durch alle Industriebranchen. Sicherheit ist immer ein dynamischer Prozess, man ist hier nie fertig. Klar ist aber, dass es bereits einen etablierten Stand der Technik gibt, der dann auch einzuhalten ist. Hier darf man sich nicht weiter in endlosen Debatten und Analysen verlieren. In vielen Reden wird immer wieder betont, wie mehr alles mit allem vernetzt wird. Aus diesem Grund müssen aber auch Sicherheitsprozesse branchenübergreifend vernetzt gedacht werden. Ebenso machen Fehler und Angriffe keinen Halt vor gesetzlich vorgesehenen Grenzen, Föderalismus, vor Ländern oder Kommunen. So wie technische Systeme immer mehr vernetzt sind, müssen dies auch die organisatorischen Fragestellungen auf allen Ebenen und Verwaltungssektoren sein. Letztendlich müssen alle eingeschlossen werden, auch Bürgerinnen und Bürger, um wirksam zu sein. Es ist sicherlich nur notwendig, um überhaupt voran zu kommen, dass KMUs im ersten Schritt ausgeklammert werden. Betrachtet man aber, dass drei Viertel aller Angriffe KMUs betreffen, diese sicherheitstechnisch noch schlechter aufgestellt sind und sie in ihrer Gesamtheit durchaus auch Kritische Infrastrukturen darstellen – bzw. beeinflussen können – so ist in einem weiteren Schritt sicherlich der Wirkungsbereich eines IT-Sicherheitsgesetzes auch in diese Richtung zu überdenken. Leider findet sich heute im TKG und TMG sowie auch im Entwurf des IT-Sicherheitsgesetzes noch sehr viel der klassischen alten Denkweise. Denken Sie aber an das einfache Beispiel des Backofens mit integriertem Web-Server, gerne auch an Industriesteuerungsanlagen, - zahllose sogenannte Web-Dienste bieten Möglichkeiten der Manipulation und sind Schwachstellen für Software-Fehler. Hier sind TMG und TKG absolut nicht konsistent bezüglich der Möglichkeiten, Angreifer zu erkennen und die dafür notwendigen Daten zu sammeln. Aus technischer Sicht ist diese Ungleichstellung absolut nicht sinnvoll. Angriffe in IT-Systemen können auf lange Sicht vorbereitet werden, auch schlechte Systemkonfigurationen schlummern jahrelang. Systeme können also lange problemlos funktionieren, bis ein Befehl zum Angriff kommt

oder sich etwas an der Umgebung ändert – ein deutscher Automobilhersteller hat das erfahren dürfen. Man muss reagieren können, bevor etwas passiert. Das für ein Lagebild notwendige Sammeln von Daten, auch im Vorfeld eines Ereignisses, umfasst aber nicht notwendigerweise alles in jeglichem Detailgrad. So sind oft mehrstufige Verfahren sinnvoll, angemessen und auch wirtschaftlich vertretbar. Beispiele sind Anomalie-Erkennung, Statistiken oder Arbeiten auf aggregierten Daten. Die einzelne Person ist hier meist überhaupt nicht von Interesse. Insgesamt lässt sich einfach feststellen, dass die gelebte IT-Sicherheit heute deutlich hinter dem Stand der Technik zurückbleibt. Das IT-Sicherheitsgesetz ist dafür ein notwendiger wichtiger erster Schritt, der einen Startschuss zur Bewusstseinsänderung darstellen kann. Vielen Dank.

Vors. **Wolfgang Bosbach** (CDU/CSU): Wir danken Ihnen. – Von der Deutschen Telekom jetzt Herr Tschersich.

SV **Dipl. Ing. (FH) Thomas Tschersich** (Deutsche Telekom AG, Leiter Group Security Services): Vielen Dank Herr Vorsitzender, verehrte Mitglieder des Deutschen Bundestages. Zunächst einmal herzlichen Dank für die Einladung zur heutigen Anhörung. Aus meiner Perspektive und aus der praktischen Erfahrung muss ich sagen, dass das Gesetz ein absolut notwendiger Schritt in die richtige Richtung ist. Sicherlich gibt es viel Diskussionsbedarfe, wie ja auch meine Vorredner schon zum Ausdruck gebracht haben, vor allem aber in Detailfragen. Ich glaube, es geht am Ende um nicht weniger als um unsere Zukunftsfähigkeit in der digitalen Welt, denn wir haben es momentan mit einer sehr massiven Vertrauenskrise im Internet zu tun. Wir hätten hier die einmalige, ja historische Chance, auch einen Standortfaktor mit einer eben sicheren Dienstleistungsumgebung zu generieren. Da ist es sicherlich ein guter und wichtiger Schritt, zunächst mit den Kritischen Infrastrukturen anzufangen, aber man darf sicherlich auch nicht aus den Augen verlieren, dass weitere Schritte noch erforderlich sind, dass letzten Endes alle Teilnehmer und gesellschaftlichen Gruppen an der digitalen Welt hier mit einzubeziehen sind. Allen voran, und das möchte ich an einem Beispiel einmal verdeutlichen, fehlt mir in diesem Gesetzesentwurf die Einbeziehung der Hard- und Software-Hersteller. Wenn Sie heute als Betreiber einer großen Infrastruktur auftreten, verschalten Sie viele Komponenten miteinander und die bestehen überwiegend aus Software, zumindest die Kernfunktionen in diesen Komponenten bestehen aus Software. Angreifer sind deswegen erfolgreich, das haben wir vorhin schon von Herrn Neumann, aber auch von Herrn Hange gehört, weil Schwachstellen in der Software ausgenutzt werden können. Jetzt einem Betreiber zu sagen, Du musst jetzt handeln, Du musst diese Schwachstellen ausmerzen, ist sicherlich in erster Linie gut gedacht, aber in zweiter noch nicht zu Ende gedacht. Ein Betreiber einer Infrastruktur alleine ist überhaupt nicht in der Lage, ein Software-Update beispielsweise zu generieren. Dazu bedarf es der Mitwirkung der Hersteller, die hier zumindest einmal unterstützen und die entsprechenden Updates zur Verfügung stellen müssen. Viele tun das, tun das bereits seit Jahren und haben die sogenannten CERT, Computer Emergency Response Teams etabliert. Viele große Unternehmen arbeiten hier sehr intensiv zusammen. Ich kann Ihnen sagen, wir haben ca. 400 Schwachstellenmeldungen im Jahr, die wir über diesen Kanal allein in unserem Unternehmen hereinbekommen. Dies geschieht zumeist durch Hersteller von Standard-Software-Komponenten. Das fängt an bei Betriebssystemen und geht bis hin zu Netzwerkkomponenten. Sicherlich, nicht jede davon ist kritisch, aber es ist schon eine schier unglaubliche Zahl, wo auch entsprechende Reaktionsnotwendigkeiten dahinter stehen. Dass das ausgenutzt wird, sehen Sie an einem Beispiel: Wir betreiben ca. 180 Sensoren, sogenannte Honeypots. Die sind im Netz verteilt weltweit und ziehen Angriffe auf sich, es handelt sich also um verwundbare Computer – und sie werden tatsächlich angegriffen. Bis zu eine Million Angriffe pro Tag sehen wir gegen diese Sensoren. Das zeigt, dass wir von einem reellen Problem reden und dass das nicht nur theoretisch ist. - Ja, ich würde so weit gehen, dass 95 Prozent sämtlicher Angriffe wirkungslos wären, wenn alle IT-Systeme auf dem aktuell letzten Software-Stand wären und das zeigt eigentlich, was wir für eine Herausforderung zu schultern haben. Ich glaube aber – und da weiche ich von meinen Vorrednern zum Teil ab – dass eine Meldepflicht hier an dieser Stelle wirklich zielführend und sinnvoll ist. Wir haben es jetzt seit Jahren versucht, ohne eine solche Ver-

pflichtung hinzubekommen. Das hat auch in Teilen funktioniert, aber eben leider nur in Teilen. Und wenn ich weiß, wie man bei meinem Nachbarn in die Wohnung eingebrochen ist, dann kann ich mich selber besser schützen alleine durch die Tatsache, dass ich weiß, wo der Schwachpunkt war, und wie ich – zum Beispiel – meine Fenster besser verstärken kann. Gleiches muss auch für die digitale Welt gelten. Wir brauchen ein Warnmeldungsregime, wo wir gegenseitig dazu kommen zu sagen: bei mir ist der Angriff über die folgende Art und Weise erfolgt und so kannst Du Dich dagegen schützen, damit eben nicht alle anderen auch noch einmal zu Betroffenen und zu Opfern werden. An dieser Stelle, glaube ich, ist so eine Meldepflicht dann sinnvoll. Im Detail gibt es natürlich noch ein paar Fragestellungen, die man dafür ausgestalten muss. Beispielsweise ist eine Meldeverpflichtung für potenzielle Möglichkeiten einer Verwundbarkeit problematisch. Das wird meines Erachtens nach schier im Uferlosen enden. Ich glaube, da müssen wir die Schwelle sehr genau austarieren, damit wir am Ende auch eine beherrschbare Anzahl an Meldungen bekommen, und vor allem, dass wir auch die relevanten Meldungen bekommen, die dann auch vom BSI genutzt werden können, um Warnhinweise daraus zu generieren, von denen ein praktischer Nutzen für die Betreiber entsprechender Komponenten ausgeht. Das ist ja das vorrangige Ziel. Lassen Sie mich zum Schluss noch einen Punkt ansprechen, und zwar was das Speichern von Daten in Telediensten angeht. Ich glaube, auch hier müssen wir sicherlich über eine Erforderlichkeit diskutieren. Aber ich würde es nicht einfach per se vom Tisch wischen wollen. In einer Perspektive: Es handele sich hier um die kleine Vorratsdatenspeicherung kommen wir nicht weiter. Wenn ich heute als kleines Unternehmen einen Web-Server betreibe, dann habe ich üblicherweise auf diesem Server eine Log-Datei, aus der ich sehen kann, was passiert mit der Maschine. Wird sie angegriffen oder nicht? Wenn ich diese Möglichkeiten nicht habe, bin ich schlicht und ergreifend völlig schutzlos und kann mich in keinster Art und Weise verteidigen – ja nicht einmal erkennen, dass mein System überhaupt angegriffen wird. Ich glaube, hierfür bedarf es wirklich einer vernünftigen Regelung, einer Definition, dass man auch dieses Thema aus dem ungeregelten, bis hin sogar illegalen Rahmen herausholt und wir hier klare Vorgaben haben, was kann und darf gespeichert werden. Aber dass man Informationen braucht, dass man technische Log-Daten braucht, um Angriffe erkennen zu können und sich dagegen zu verteidigen, steht glaube ich völlig außer Frage. Ich würde mir wünschen, dass wir hier eine entsprechende Regelung bekommen, die dann nicht nur auf die Infrastrukturbetreiber zielt, sondern die auch Dienste-Anbieter in die Lage versetzt, ein entsprechendes Schutzniveau aufrecht zu erhalten. Vielen Dank.

Vors. **Wolfgang Bosbach** (CDU/CSU): Wir danken Ihnen Herr Tschersich. Der Letzte in der Runde der Sachverständigen ist vom Gesamtverband der Deutschen Versicherungswirtschaft, Herr Dr. Wehling.

SV **Dr. Axel Wehling** (Gesamtverband der Deutschen Versicherungswirtschaft e. V., Mitglied der Hauptgeschäftsführung, Geschäftsführer des Krisenreaktionszentrums der deutschen Versicherungswirtschaft): Vielen Dank Herr Vorsitzender, meine Damen und Herren Abgeordnete, auch von meiner Seite vielen Dank für die Einladung. Von unserer Seite, wir begrüßen die Initiative für das IT-Sicherheitsgesetz. Wir denken, dass es der richtige Zeitpunkt mit der richtigen Dosierung ist, um hier den nächsten Schritt zur Härtung der Sicherheitskultur in IT-Fragen in Deutschland zu gehen. Aus unserer Sicht gibt es drei essentielle Kernpunkte, die hierbei zu betrachten sind. Das eine ist die weitestgehend anonymisierte Meldung, um hier den ersten Schritt hin zu einer Meldekultur zu gehen. Zweitens ein konsequentes Fortschreiten des bisher gegangenen Weges des kooperativen Ansatzes und als dritten Kernpunkt den Branchenansatz. Um Ihnen einen kleinen Hintergrund zu geben, wir befassen uns sehr intensiv auf Seiten des GDV mit dem Thema IT-Sicherheit, dieses bereits seit etlichen Jahren. Wir haben bereits im Jahr 2010 einen Single Point of Contact (SPOC), eine Meldeplattform, etabliert zwischen der Branche und dem BSI – und wir sehen eigentlich vor, dass wir diesen Single Point of Contact, das Lage- und Krisenreaktionszentrum der Deutschen Versicherungswirtschaft für IT-Sicherheit, eigentlich dann auch zur gemeinsamen übergeordneten Anspruchsstelle im Sinne des IT-Sicherheitsgesetzes konsequent ausbauen sollten.

Wir haben weitere Schritte ergriffen, insbesondere ein weitreichendes Netzwerk von IT-Sicherheitsexperten aufgebaut, einen Lehrgang für die besonderen Belange innerhalb der Versicherungswirtschaft in IT-Fragen aufgebaut und letztlich haben wir vor 14 Tagen dann eine Zertifizierung unserer Branchen-Cloud, sowohl mittlerweile nach ISO-Standards 27001 auf Basis BSI-Grundschutz als auch nach Common Criteria erreichen können. Wir denken daher, dass dieser Branchenansatz, der hier in dem Gesetz maßgeblich verankert ist, eigentlich das Tool ist, um hier sehr spezifisch die IT-Sicherheit weiter voran zu bringen, dass das aber auch der nötige Hebel ist, um entsprechende Bürokratie, die sonst entstehen könnte, zu vermeiden. Wir gehen davon aus, dass die Branchen, die als Kritische Infrastrukturen identifiziert wurden, – dass diese eben sich auch sehr stark unterscheiden von den Anforderungen an IT-Sicherheit, die an sie zu stellen sind. Drei Aspekte möchte ich des Weiteren hervorheben. Der eine ist, dass wir glauben, dass, um diese Meldekultur in Deutschland zu etablieren, wir von weiteren Spezialgesetzen absehen sollten, mit denen weitere Meldepflichten dann an andere Bundesoberbehörden etabliert werden. Wir gehen davon aus, dass wir einen deutlichen Schritt nach vorne gehen können, wenn es beim BSI ein zentrales Lagebild gibt. Dass dieses Lagebild dann auch an andere Bundesoberbehörden, wie beispielsweise die BaFin, übermittelt wird, vielleicht auch mit speziellen Lagebildern zum Thema Versicherung oder Finanzwirtschaft. Wir gehen davon aus, dass wir dadurch aber keinen Konkurrenzkampf zwischen den einzelnen Meldewegen bekommen werden, sondern dass dieses ein notwendiger Schritt sein wird, um insbesondere dann auch eine Meldekultur – wie sie erforderlich ist, um das zu erreichen, was mein Vorgänger beschrieben hat – um dann eben eine solche Meldekultur auch hinzubekommen. Das, was wir sehen ist, dass der kooperative Ansatz, wie er in weiten Teilen im Gesetz angelegt ist, dass dieser noch weiter konsequent ausgebaut werden sollte. Dies betrifft insbesondere die Frage, welche Unternehmen unterfallen gerade dann auch in den einzelnen Branchen der Definition der Kritischen Infrastruktur. Geht dies wirklich hinunter bis zu meinem kleinsten Mitglied mit zwölf Mitarbeitern, wo ist dort die Grenze zu ziehen? Hier sollten wir so schnell wie möglich in der weiteren Diskussion Sicherheit und Klarheit schaffen. – Und das Zweite ist, dass der kooperative Ansatz, so wie wir ihn im Gesetz angelegt haben, auch dann auf den § 8a noch stärker ausgeweitet werden sollte, dass hier insbesondere bezogen auf die Frage der Definition der Sicherheits-Audits, Prüfung und Zertifizierung – dass hier auch Branchenlösungen dann möglich sein sollten. Dass auch dann in Bezug auf die Meldung es sicherlich ausreichend ist, wenn erhebliche Sicherheitsmängel, die im Rahmen dieser Audits festgestellt werden, gemeldet werden, dass hierüber dann eine Sicherstellung des kooperativen Ansatzes erfolgen kann. – Zusammenfassend aus unserer Sicht: der Gesetzentwurf geht in die richtige Richtung. Wir sehen kleinere Anpassungen für erforderlich. Nichts tun oder abwarten, erscheint uns allerdings vor dem Hintergrund der aktuellen Gefährdungslage dann ebenfalls als keine Alternative. Vielen Dank.

Vors. **Wolfgang Bosbach** (CDU/CSU): Wir danken Ihnen Herr Wehling. Wir kommen zur Fragerunde, zur Diskussionsrunde. Der Kollege Clemens Binninger war vorgesehen als Berichterstatter der Unionsfraktion. Der lässt sich allerdings entschuldigen, weil er heute als sachverständiger Zeuge in Sachen NSU in Hessen unterwegs ist. Deswegen hat jetzt das Wort der Kollege Wendt.

Abg. **Marian Wendt** (CDU/CSU): Ja, vielen Dank an die Sachverständigen für Ihre, auch umfangreichen schriftlichen Stellungnahmen und dafür, dass Sie uns die Möglichkeit geben, nachzufragen. Ich würde ein paar Fragen hintereinander stellen? Sie haben ein 27-Minuten-Zeitkontingent …

Vors. **Wolfgang Bosbach** (CDU/CSU): Bitte dazu auch benennen, an wen Sie diese Fragen adressieren.

Abg. **Marian Wendt** (CDU/CSU): Ja genau … nur noch einmal zum Verfahren, 27 Minuten, klassische Berliner Runde? …

Vors. **Wolfgang Bosbach** (CDU/CSU): Nein, nein nein! Kurze knackige Frage, am besten eine, die man beantworten kann, an die Sachverständigen Ihrer Wahl, und dann machen wir weiter!

Abg. **Marian Wendt** (CDU/CSU): Gut, ich richte mich zuerst an die Sachverständigen Herrn Tschersich und Herrn Wehling. Es geht um die Definition von Kritischer Infrastruktur, ob sich nach Ihrer Einschätzung ein konkreter Wert festlegen ließe, anhand dessen sich sozusagen eine Definition für den Begriff Kritische Infrastruktur festlegen lassen würde, also quantitative Zahlen als Beispiel? Oder lässt dieser spezielle Bereich eine Abstraktion auf Zahlen oder ähnliche konkretere Definitionen zu? Welche Bereiche, welche Sektoren sollten unter anderem auch unter Kritische Infrastrukturen fallen? Sollte die Nahrungsmittel-produktion – beispielsweise – auch davon betroffen sein? Und inwieweit ist davon auszugehen, dass die Definition unserer critis europaweit tragfähig sein wird, in Bezug zum Beispiel auf die aktuell laufenden Verhandlungen zur NIS-Richtlinie. Das vielleicht zum Thema critis. – Dann haben wir zum Problem der Wesentlichkeit und Bestimmtheit des Gesetzentwurfes an Frau Plöger und Herrn Prof. Dr. Hornung die Frage, ob der Gesetzentwurf Ihrer Meinung nach eine ausreichende Bestimmtheit aufweist im Hinblick auf die Eingriffe in die Grundrechte der Betreiber von Kritischer Infrastruktur, und wie ließe sich die Definition von critis derart im Gesetzentwurf treffen, dass dies sichergestellt ist? Sowie die Frage im Hinblick auf die Mitwirkung von Verbänden, Wissenschaft und Unternehmen bei der Erstellung der Rechtsverordnung, ob Ihrer Meinung nach sichergestellt ist, dass eine Lösung im Sinne beider Seiten gefunden werden kann beziehungsweise kooperativer Ansatz. Gemeint ist die Frage, inwieweit das BMI dann bei der Erstellung der Rechtsverordnung wirklich auf die Verbände, die Wissenschaft und die Unternehmen eingehen muss. Der dritte Themenbereich betrifft die Meldepflichten an das BSI. Die Frage richtet sich an den Präsidenten Herrn Hange, wie schätzen Sie die Menge der zu meldenden Vorfälle ein? Wie müsste von Seiten des BSI auf das Meldeaufkommen reagiert werden, organisatorisch zum Beispiel? Vielleicht können Sie uns das praktisch ein bisschen erläutern, wie Sie das vielleicht schon simuliert haben oder angedacht haben von der Konstruktion her, wie mit diesen Meldefällen umgegangen wird? Ob es da vielleicht ein spezielles Krisenzentrum gibt oder ähnliches, man kann da ja nicht warten – wenn am Wochenende etwas passiert – bis Montag früh um 8:00 Uhr der Sachbearbeiter auf der Arbeit ist. Weiterhin die Frage, inwieweit wird sich der Mehraufwand durch Meldepflichten und der Minderaufwand durch verbesserten Schutz vor Angriffen – wir gehen auch davon aus, dass vielleicht die Anzahl der Angriffe geringer wird, weil wir große Schutzhürden aufbauen – wie würde sich das im Endeffekt ausgleichen? Das als die drei Fragenkomplexe an die Sachverständigen, Danke.

Vors. **Wolfgang Bosbach** (CDU/CSU): Herr Tschersich.

SV **Dipl. Ing. (FH) Thomas Tschersich** (Deutsche Telekom AG, Leiter Group Security Services): Ja, zur Frage der Definition Kritische Strukturen. Zur Frage, ob man das möglicherweise an wirtschaftlichen Kennzahlen festmachen kann, ist das, glaube ich, unheimlich schwierig. Weil Sie im Zweifelsfall ganz kleine Unternehmen haben, die nur eine Schraube zu so einer Gesamtkette beitragen. Wenn aber diese eine Schraube fehlt, funktioniert diese Gesamtkette nicht mehr. Also insofern tue ich mich da sehr schwer, so einen konkreten Schwellwert einer Größe zu nennen, wie wir es aus dem TKG bei sonstigen Sicherheitsauflagen kennen, sondern würde eher von einer Grundversorgungs-These ausgehen. Also alles das, was unter die Grundversorgung fällt, und das können im Zweifelsfall auch ganz kleine Unternehmen, aber auch sehr große Infrastrukturbetreiber sein, muss eigentlich unter Anwendungszweck oder Anwendungsbereich des IT-Sicherheitsgesetzes fallen. Das schließt natürlich dann auch eine Grundversorgung mit Nahrungsmitteln der Bevölkerung ein. Wenn auch noch der Lebensmittelhandel über Wochen und Monate aufgrund von IT-Problemen nicht funktionieren würde, wäre das sicherlich ein Thema. Aber ich glaube, auch hier ist genau der branchenspezifische Ansatz der sachdienliche Weg. Genau so wenig wie ich weiß, wie der Lebensmittelhandel im Detail funktioniert, weiß der Lebensmittelhandel, wie die Telekommunikation im Detail funktioniert. Deswegen halte ich es für sehr zielführend, dass man diesen kooperativen branchenspezifischen Ansatz auch zumindest einmal fährt, und darüber dann am Ende ein Korrektiv setzt, was ja nach dem Entwurf auch durch das BSI gewährleistet werden soll. Welches dann eine Branche

sagt, ich möchte mich am liebsten da heraushalten und gar keine Standards machen würde das Korrektiv greifen. So würde das Szenario, das Herr Neumann vorhin dargestellt hat, vermieden, dass Unternehmen Standards verhindern, damit sie nichts investieren müssen. Das Korrektiv wird am Ende des Tages entscheidend sein.

Vors. **Wolfgang Bosbach** (CDU/CSU): Bitte, Herr Dr. Wehling.

SV **Dr. Axel Wehling** (Gesamtverband der Deutschen Versicherungswirtschaft e. V., Mitglied der Hauptgeschäftsführung, Geschäftsführer des Krisenreaktionszentrums der deutschen Versicherungswirtschaft): Vielen Dank für die Frage. Wie mein Vorredner tue ich mich mit einem konkreten Wert recht schwer. Ich kann vielleicht einmal versuchen, so ein paar Relationen zu bilden. Wir haben in Deutschland unter Bundesaufsicht, glaube ich – 1 200 Versicherungsunternehmen, da sind nun all die kleinen Sterbekassen mit dabei. Die sind Mitglied im GDV. – Und wir decken über 95 Prozent der Beitragseinnahmen ab durch nur 430 Unternehmen. Das bedeutet, da wird man schon irgendwo dann einen gap ziehen können. Man sieht auch weiterhin, dass von diesen 430 Unternehmen vielleicht nicht alle zwingend mit erfasst werden müssen. Ich glaube, hier muss man wirklich branchenspezifisch sich das angucken. Wir haben uns im Rahmen des UP KRITIS auch immer bei den Übungen sehr genau die Response-Zeiten angesehen, und haben so ein bisschen für uns selber angesehen, sind die Response-Zeiten eigentlich für die Größe und für die Dimension des Unternehmens adäquat? Ich glaube, hier kann man nicht alle in einen Topf hineinwerfen, und genau so sollte man das hier auch nicht tun. Aber ich denke, wenn man die konkreten Branchenlisten hat, dann wird man – ich sage einmal – ein Gefühl entwickeln können, wer mit dazu sollte und wer nicht. Und ich kann ich Ihnen sagen, in der Community, die sich bei uns herausgebildet hat, hat man da eigentlich auch untereinander irgendwann das Gefühl, dass man doch noch mitmachen muss und dass man mitmachen möchte, und dass es eben gerade kein Selbstzweck ist. Ich glaube, dieses würde sich entsprechend entwickeln. Bei der Frage, ob wir im Rahmen des IT-Sicherheitsgesetzes alle EU-Branchen richtig abbilden, ist die Antwort fast genauso schwer. Sie wissen, dass nach dem EU-Katalog die Versicherungswirtschaft, zumindest in der heutigen aktuellen Diskussion, nicht mit dabei ist. Hier – national – wären wir mit darinnen. Gleichwohl lobbyiere ich nicht dafür, dass wir entsprechend herauskommen. Sondern dadurch, dass das gerade insgesamt als Aufgabe wahrgenommen wird – auch als eine wettbewerbsneutrale Aufgabe zwischen den Unternehmen – glauben wir, dass wir hier insgesamt einen vernünftigen Standard erarbeiten müssen. Und auch hier halte ich es für unschädlich, wenn national eine andere Aufteilung erfolgt als diese europaweit ist. Das mag auch der Tatsache geschuldet sein, dass wir in etlichen europäischen Mitgliedstaaten gar keine nennenswerte nationale eigene Versicherungswirtschaft haben, dass wir uns hier anders aufstellen könnten. In Bezug auf die Nahrungsmittelwirtschaft habe ich als bekennender Hobbykoch eine eigene Meinung, ich bitte aber um Verständnis dafür, dass ich hier aktuell eigentlich nichts dazu sagen kann.

Vors. **Wolfgang Bosbach** (CDU/CSU): Frau Plöger.

SV **Iris Plöger** (Bundesverband der Deutschen Industrie e. V., Leiterin der Abteilung Digitalisierung): Ich glaube, für die nächste Frage war ich genannt – ja. Zu der Frage, ob bis jetzt das Gesetz hinreichend bestimmt ist, haben wir eigentlich in unserem Eingangsstatement schon ausgeführt. Was uns aufgefallen ist in den vielen Vorgesprächen und Runden, die wir vorher geführt haben, ist das, dass bei sehr Vielen noch das Fragezeichen stand, ob sie tatsächlich der Betreiber einer Kritischen Infrastruktur sind und dass entsprechend die Sorge umgeht, wann man sich eben auf die neue Gesetzeslage einstellen muss? Dass hier eben bei den Unternehmen auch eine große Unsicherheit besteht. Der Bundesrat hat in seiner Stellungnahme ja diese Punkte auch schon kritisiert. Eine weitere Sache, die wir auch schon erwähnt haben, ist sicherlich der Umfang und der Inhalt dieser Meldepflicht. Auch hier gibt es viele Fragezeichen, vorhin sind ja schon einige Zahlen genannt worden. Unter anderem, dass die Telekom davon ausgeht, dass es eine Million Angriffe pro Tag gibt. Also, wenn man sich jetzt einmal überlegt, was ein größeres Unternehmen dann – ein Energieversorger zum Beispiel – am Tag zu bewältigen hätte, dann wird sicherlich auch die Anzahl der Personen, die alleine dafür eingestellt

werden müssten, um das nachzuhalten, sehr groß sein. Die Unternehmen haben also in ihren Gesprächen sehr dringend darum geworben, dass natürlich möglichst viel schon Bestandteil des Gesetzes wird und nicht erst in die Rechtsverordnung eingeht, um da rechtzeitig mehr Rechtssicherheit zu haben. – Soll ich die zweite Frage auch gleich beantworten?

Vors. **Wolfgang Bosbach** (CDU/CSU): Ja bitte.

SV **Iris Plöger** (Bundesverband der Deutschen Industrie e. V., Leiterin der Abteilung Digitalisierung): Ja, also die Frage der Rechtsverordnung – das ist ja dann auch die Überleitung dazu – natürlich begrüßen wir den kooperativen Ansatz und freuen uns über eine enge Einbindung in das Verfahren. Das haben wir auch schon signalisiert, das ergibt sich ja auch schon aus dem vorher Gesagten, dass wir vielleicht uns noch mehr Präzision im Gesetz selbst wünschen würden. Es ist einfach im Interesse der Industrie, sich da aktiv einzubringen, weil natürlich auch wir die wachsende Bedrohung sehen und auch wir uns die Frage stellen, ob wir mit umfangreichen Meldepflichten dem Problem Herr werden. Aus diesem Grund ist ja auch die Allianz für Cyber-Sicherheit schon gegründet worden, die mittlerweile über 1 000 Unternehmen erfasst, und die es natürlich auch ermöglicht, auch branchenspezifische Standards zu entwickeln und branchenspezifische Schutzmechanismen zu entwickeln.

Vors. **Wolfgang Bosbach** (CDU/CSU): Vielen Dank. Herr Prof. Hornung bitte.

SV **Prof. Dr. Gerrit Hornung** (Universität Passau, Lehrstuhl für öffentliches Recht, IT-Recht und Rechtsinformatik): Ja, danke für die Frage, die nach den verfassungsrechtlichen Maßstäben an die Rechtsverordnung gefragt hat. Wir haben dazu Anforderungen in Art. 80 Abs. 1 Satz 2 GG, die sich unter anderem auch ergeben aus der Wesentlichkeitstheorie des Bundesverfassungsgerichts. Also: die wesentlichen Entscheidungen müssen Sie in diesem Haus hier selber treffen, sie muss der Gesetzgeber selber treffen. Die Frage ist, was bedeutet das im konkreten Fall? Ich würde sagen, im Ausgangspunkt ist die Frage, auf wen ein Gesetz anwendbar ist, natürlich eine wesentliche Frage. Da wird man kaum anderer Ansicht sein können. Das bedeutet aber nicht, dass jedes einzelne Unternehmen immer direkt aus dem Gesetz ersehen können muss, ob das Gesetz anwendbar ist. Ich würde – ähnlich wie der Kollege Roßnagel – sagen, dass die Bestimmtheitsanforderungen hier gewahrt sind, ich würde aber ein „noch“ hinzufügen, ich würde sagen, sie sind – noch – gewahrt. Daher würde ich schon dafür plädieren, nach Möglichkeit noch eine Präzisierung vorzunehmen. Die Kriterien Qualität und Quantität sind angesprochen worden, und in der Gesetzesbegründung gibt es auch zumindest Ansätze für Präzisierungen. Zum Beispiel betroffene Rechtsgüter, die man nennen könnte. Im Übrigen ist mir beim Lesen der Begründung aufgefallen, dass dort darinsteht, dass maximal 2 000 Unternehmen von dem Gesetzentwurf betroffen sein sollen. Irgendwie muss diese Zahl ja ermittelt worden sein. Das heißt, offensichtlich gibt es ja Kriterien, nach denen im Moment auch schon gearbeitet wird und nach denen diese, für mich doch schon relativ konkrete Zahl von 2 000 Unternehmen, ermittelt worden ist. Diese Kriterien könnte man im Verordnungsverfahren näher präzisieren, aber die könnte man vielleicht auch im Gesetzgebungsverfahren bereits näher präzisieren; dafür würde ich jedenfalls werben. Lassen Sie mich vielleicht eine Sache noch zu europarechtlichen Dingen ergänzen, auch wenn die Frage Europa, glaube ich, nicht direkt an mich ging. Ich würde sagen, dass das direkt zusammenhängt. Je vager Sie den Gesetzentwurf lassen, desto größer ist die Chance, dann im Verordnungsverfahren konform zu sein mit den Europäischen Richtlinien. Wenn wir es dagegen auf deutscher gesetzlicher Ebene präziser machen, dann steigt das Risiko, dass wir einen Widerspruch kriegen zu dem, was auf europäischer Ebene passiert. Das heißt, je präziser man es in das Gesetz schreiben will, desto mehr würde dafür sprechen, vielleicht doch die europäischen Gesetzgebungsverfahren abzuwarten. Ich glaube allerdings, was das Europäische angeht, liegen die eigentlichen Probleme nicht bei der Frage des Anwendungsbereiches, sondern bei der Veröffentlichung der Ergebnisse und bei den Sanktionsbefugnissen. Dankeschön.

Vors. **Wolfgang Bosbach** (CDU/CSU): Herr Hange bitte.

SV Präs. **Michael Hange** (Bundesamt für Sicherheit in der Informationstechnik): Ja, zum Thema Meldepflichten zuerst die Frage, wie geht das BSI

mit den Meldungen um? Wir haben also angeschlossen an unser CERT – an unser Computer Emergency Response Team – ein Lagezentrum, welches dann künftig auch 24 Stunden mal 7 Tage präsent sein wird. Dort werden die Meldungen natürlich nicht nur gesammelt, sondern bewertet – und dann ist der Prozess natürlich zweistufig. Es ist so, es wird gesehen, was – sage ich einmal – sich an akuten Gefährdungen für andere ergibt. Denn, wenn wir hochwertige Angriffe haben – so zeigen es unsere Erfahrungen – dann werden auch andere in der gleichen Branche in gleicher Weise angegriffen. Daraus ergibt sich dann eine Warnung, die kann branchenspezifisch sein, die kann aber auch öffentlich sein. Das wäre also ad hoc. Dann ist es sehr wichtig – Meldepflichten sind an sich kein Selbstzweck – dass jede Meldung von einem Vorfall, gerade wenn es sich um hochwertige Angriffe handelt, auch Analyse nach sich zieht. Und Herr Tschersich hatte gesagt, wenn man konsequent Angriffe analysiert und sich dagegen aufstellt – 95 Prozent sind vielleicht etwas zu viel nach meiner Einschätzung – aber man kann 80 Prozent, bis 90 Prozent der Angriffe abwehren. Ich glaube, es ist wesentlich, da auch die Gelegenheit zu geben, und das kann dann im Weiteren auch in die Mindeststandards der Branchen eingehen. Das ist also der kooperative Ansatz, es ist kein Selbstzweck, sondern es dient dazu, im Grunde – ich sage einmal – ad hoc zu sagen, was kann man dagegen tun, es dient dazu, aufmerksam zu machen. Und zu der einen Million, die Zahl stand ja im Raum, also es ist nicht „Wald und Wiesen …“. Was ein Spam-Filter herausfiltern kann, was ein Virenschutz-Programm herausfiltern kann, ist nicht meldewürdig. Sondern die eine Million meint, es ist eine erhebliche Störung, und meint insbesondere neuartige Angriffe. Wir haben das einmal hochgerechnet – ich sage einmal so – aus dem, was in der Bundesverwaltung, wo wir auch eine Meldepflicht haben, stattfindet. Wir gehen also davon aus, fünf bis zehn Angriffe pro Jahr. Und bei den 2 000 Betreibern muss man qualitative Aspekte und auch quantitative Aspekte betrachten. Zum qualitativen Aspekt ist es wichtig zu sehen, die Herstellung von Sachen, als Beispiel, muss anders bewertet werden als die Verteilung von Dingen. Oft ist der Verteil-Prozess – zum Beispiel bei Strom – aber auch bei Lebensmitteln, auch wenn das nur wenige sind, der kritischere Bereich. Und, dem Rechnung tragend, kommen wir also auf etwa 2 000 im Maximum. Aber ich sage deutlich, es ist ein dynamischer Prozess. Wichtig ist es jetzt, diese Methoden kooperativ – auch in der Rechtsverordnung – niederzulegen, sodass man zum Konsens über die Vorgehensweise kommt. Dass wir also als BSI auch für die Wirtschaft dann in unserer Vorgehensweise transparent sind in der Hinsicht, was wir tun, was wir mit den Informationen machen. Das heißt aber auch, die Meldungen von den Unternehmen als solche bleiben natürlich sehr vertraulich. Das muss oberstes Gebot sein, sowohl was die Meldung selbst betrifft als auch bezogen auf denjenigen, der dahinter steht.

Vors. **Wolfgang Bosbach** (CDU/CSU): Herr Kollege Reichenbach.

BE Abg. **Gerold Reichenbach** (SPD): Vielen Dank. Vielleicht einmal vorab einen Satz: Was mich schon ein bisschen irritiert ist das, wenn Unternehmen selber nicht wissen, ob sie zu Kritischen Infrastrukturen gehören, oder welche Anlagenteile bei ihnen selbst Kritische Infrastruktur sind, dann sagt das fast mehr über das Problem der Unternehmen aus, als über die Definitionsschwierigkeit im Gesetz. Das vielleicht nur einmal am Rande. Ich habe drei Fragenbereiche, einmal am besten an die beiden Juristen, an Herrn Prof. Hornung und an Herrn Prof. Roßnagel. Herr Prof. Schiller hatte in seiner Stellungnahme darauf hingewiesen, dass es bei diesen Web-basierten Steuerungselementen, die in den Anlagen verbaut sind, die sozusagen gar nicht die klassischen Web-Dienste sind – so wie wir aus dem Internet kennen – , dass es bei diesen Web-basierten Steuerungselementen Zuordnungsschwierigkeiten gibt, ob sie denn im TMG oder im TKG überhaupt ausreichend gefasst ist. Dazu wäre meine Frage, sehen Sie die Schwierigkeit auch? Herr Prof. Roßnagel, Sie haben es angesprochen in Ihrer Stellungnahme, zumindest teilweise. Aber was mich viel mehr interessiert, wie wäre das Problem zu lösen? Das heißt, hätten Sie einen rechtlichen Vorschlag, wie das lösbar wäre? Meine zweite Frage geht an Herrn Hange, an Herrn Prof. Roßnagel und an Herrn Schiller, das ist die Frage der Mitwirkungspflicht von Herstellern von Komponenten. Herr Tschersich hatte es auch angesprochen, was passiert eigentlich, wenn irgendjemand, weil er Monopolist ist, sagt … schön, dass du ein Problem hast, aber das ist

nicht meins, … Obligo ist dann der Betreiber der kritischen Infrastruktur, und nicht derjenige, der die Hardware oder die Software geliefert hatte, in der sozusagen das Sicherheitsproblem entstanden ist und auch nur zu beheben ist. Deswegen meine Frage, können Sie sich Regelungen vorstellen, die Mechanismen entfalten, die dann auch eine entsprechende Mitwirkung garantieren, und wie könnten die dann aussehen? Meine dritte Frage ist dann die Frage nach den Sanktionsmechanismen, das ist ja mehrfach angesprochen worden. Diese Frage vielleicht auch an Herrn Prof. Roßnagel und an Herrn Prof. Hornung, wie wäre das im Gesetz besser formulierbar? Dass das Gesetz auch nicht ins Leere läuft, und nicht diejenigen, die sich dann im kooperativen Ansatz auch kooperativ verhalten dadurch bestraft werden, dass diejenigen, die sich nicht daran halten, dann keine Strafe zu fürchten haben, also auch keine ökonomische, was ja dann auch zu einer Wettbewerbsverzerrung führen würde. – Dann habe ich noch eine Frage, die jetzt nicht in der Anhörung selber entstanden ist, sondern von außen herangetragen wurde. Es gab mehrfach die Kritik im Netz und sonst wo, dass die Zweckbindung nach § 7a nicht ausreichend sei. Ich glaube, beim Chaos Computer Club ist es eben einmal so ein bisschen angeklungen, dass die Entdeckung, oder die Meldungen von Sicherheitslücken dann vom BSI und von Bundesbehörden im Sicherheitsbereich dazu genutzt werden könnten, solche Sicherheitslücken zur Verfügung zu stellen, um dann eigene Zwecke zu verfolgen. Also so nach dem Motto, das BSI sucht nach Ausspähungslücken und gibt die dann böserweise dem Bundesverfassungsschutz oder dem BKA. Da wäre meine Frage noch einmal die, ob Ihrer Einschätzung nach …

Vors. **Wolfgang Bosbach** (CDU/CSU): … an wen? …

BE Abg. **Gerold Reichenbach** (SPD): … an Herrn Prof. Roßnagel, an Herrn Hange und an – die Zweckbindung nach § 7a – vielleicht noch an Herrn Prof. Hornung, ausreichend ist, um solchen Befürchtungen entgegen zu treten, oder würden Sie da eine Nachschärfung befürworten?

Vors. **Wolfgang Bosbach** (CDU/CSU): Herr Prof. Hornung.

SV **Prof. Dr. Gerrit Hornung** (Universität Passau, Lehrstuhl für öffentliches Recht, IT-Recht und Rechtsinformatik): Vielen Dank für die Fragen. Ich hatte ja eben schon gesagt, dass ich im Wesentlichen mit Herrn Kollegen Roßnagel da einer Meinung bin, nutze die Gelegenheit aber gern, zum TKG und zum TMG auch noch etwas zu sagen. Sowohl im TMG-Bereich als auch im TKG-Bereich haben wir das – aus meiner Sicht – relevante Problem des Umgangs mit Verkehrsdaten zu IT-Sicherheitszwecken, also des Umgangs mit dem, was da sozusagen im Tagesgeschäft anfällt an laufenden Daten. Und da wird es sicherlich überlappende Bereiche geben. Über die Abgrenzung dieser beiden Gesetze kann man promovieren, das ist tatsächlich ein nicht ganz überschneidungsfreier Bereich. Außerdem ist es ein identisches Problem, nämlich die Frage, was machen wir mit Verkehrsdaten in Bezug auf solche Analyse-Mechanismen? Ich würde das, weil es das identische Problem ist, auch identisch lösen. Ich würde es nur nicht so lösen, wie es im Gesetzentwurf steht. Weil dort nämlich im Wesentlichen nur das Kriterium der Erforderlichkeit darinsteht, und das scheint mir zu vage zu sein, um in diesem sehr grundrechtssensiblen Bereich handhabbare Kriterien anzugeben. Wir haben eben schon gehört, dass das Erforderlichkeitskriterium dazu führt, dass in der Praxis die Dauer der Speicherung völlig auseinanderläuft, nachdem was ich höre, von drei Tagen bis zu sechs Monaten. Das kann nicht Sinn der Sache sein. Wir brauchen eine Erheblichkeitsschwelle, die zum Beispiel so aussehen könnte, dass nur erhebliche Sicherheitsvorfälle und nicht jeder Sicherheitsvorfall ausreichend ist. Wir brauchen eine Zweckbindungsregelung, wir brauchen IT-Sicherheitsvorgaben, und wir brauchen eine Obergrenze für die Speicherfrist. Das sind Möglichkeiten, dieses Problem grundrechtskonform zu lösen. Zweiter Punkt, zu den Sanktionen, ich hatte ja schon darauf hingewiesen, dass wir hier eine Ungleichbehandlung haben, nämlich im TKG-Bereich gibt es Sanktionen. Dort haben wir Ordnungswidrigkeiten-Tatbestände, und ich glaube, dass der TKG-Bereich hier als Modell dienen könnte. Dort wird es nämlich so gelöst, dass nicht jeder Verstoß gegen die IT-Sicherheitsvorgaben bußgeldbewährt ist, sondern nur dann, wenn es erhebliche Verstöße sind, oder gravierende Verstöße. Ich glaube, dass das ein

sinnvoller Ansatz ist auch für eine allgemeine Regelung, die man im BSI-Gesetz oder an anderer Stelle verankern könnte. Wie gesagt, ich glaube an kooperative Ansätze, aber nicht so sehr, dass ich darauf verzichten würde, dem BSI entsprechende Befugnisse an die Hand zu geben. Ich habe auch schon darauf hingewiesen, dass das tatsächlich ein Punkt ist, wo die europäischen Pläne anders aussehen. Dort gibt es Sanktionsbefugnisse. Das heißt, wenn die Richtlinie so verabschiedet wird, müsste in diesem Haus ohnehin nachgearbeitet werden, weil man dann das umsetzen muss. Letzter Punkt, Zweckbindung des § 7a. Auch darauf habe ich schon hingewiesen. Ich glaube, dass die Erkenntnisse, die hier gewonnen werden seitens des BSI, aus der Perspektive der Unternehmen sensibel sind oder sensibel sein können, und dass wir deshalb dafür sorgen müssen, dass auch der böse Schein vermieden wird, dass diese Erkenntnisse weitergegeben werden an Institutionen, die da möglicherweise zweite oder dritte Interessen haben könnten. Das betrifft aus meiner Sicht vielleicht gar nicht so sehr die Bundesbehörden, sondern die internationale Kooperation des BSI. Das BSI bekommt ja nach dem Entwurf eine neue Aufgabe der internationalen Zusammenarbeit. Das macht die Behörde heute auch schon. Aber es gibt jetzt eine explizite, neu geregelte Aufgabe der internationalen Zusammenarbeit. Auch in dieser Zusammenarbeit, denke ich, ist dafür Sorge zu tragen, dass das, was hier gesammelt wird, und zwar sinnvollerweise gesammelt wird auf Seiten des BSI, nicht in andere Kanäle kommt und dass auch nicht dieser Anschein erweckt wird.

Vors. **Wolfgang Bosbach** (CDU/CSU): Herr Prof. Roßnagel.

SV **Prof. Dr. Alexander Roßnagel** (Universität Kassel, Institut für Wirtschaftsrecht): Ja, vielen Dank für die Fragen, bezogen auf die Erfassung von Web-Steuerungen in eingebetteten Systemen. Hier kann ich mich weitgehend den Ausführungen von Herrn Hornung anschließen. Ich würde gern auf zwei Punkte aufmerksam machen. Wenn man das TMG, das Telemediengesetz, miteinbezieht, dann hat man das Problem, dass es nicht nur um Verkehrsdaten geht, sondern auch um Nutzungsdaten. Das heißt, die Information an den Betreiber über das Netzverhalten des Nutzers wird erheblich höher, intensiver, – und das heißt, der Eingriff in das Fernmeldegeheimnis des Nutzers wird erheblich tiefer. Insofern kann man aus der Sicht des Betroffenen diese beiden Fälle nicht gleichsetzen. Man muss sehen, dass der Grundrechtseingriff stärker ist. Das muss nicht ausschließen, dass der TMG-Betreiber genauso wie der Telekommunikationsbetreiber Vorsorgemaßnahmen treffen darf oder sollte oder können sollte, um Angriffe zu erkennen. Aber dabei, und das ist die zweite Bemerkung, sollte man vor allen Dingen darauf achten, dass man stufenweise vorgeht. Also nicht alle Daten, von allen Nutzern, für einen, im Gesetz nicht geregelten Zeitraum aufbewahrt, sondern man erst einmal Statistiken prüft, anonym die Daten erhebt, und wenn man dann Anomalien erkennt, dann hat man einen Anlass. Dann kann man eine Stufe weitergehen und so sich – und das müsste im Gesetz entsprechend geregelt sein – Schritt für Schritt voran arbeiten in der Verarbeitung personenbezogener Daten. Das Bundesverfassungsgericht hat das in vielen Entscheidungen so eingefordert, dass man nicht einfach alles entsprechend speichern darf, sondern dass man immer Eingriffsschwellen definieren muss. Also, wie aussagekräftig ist das Datum, dementsprechend muss dann eine hohe Eingriffsschwelle oder eine niedrige Eingriffsschwelle bestehen. Und wenn man so stufenweise vorgeht, kann man diese Eingriffsschwellen nachvollziehen oder entsprechend dokumentieren. Also immer dann, wenn man sieht, hier findet ein Angriff statt, dann gibt es natürlich auch gute Gründe, die Daten zu speichern. Wenn man aber keinen Anlass hat, jetzt von einem Angriff auszugehen, warum soll man dann die Daten speichern. Also nicht alles flächendeckend auf einmal, sondern Schritt für Schritt.
Die zweite Frage zur Mitwirkungspflicht von Herstellern. Das BSI kann ja die Betreiber Kritischer Infrastrukturen zu Nachbesserungsmaßnahmen auffordern. Es macht wenig Sinn, wenn die Nachbesserungsmaßnahme vom Betreiber vorgenommen werden müsste, weil die Hard- und die Software vom Betreiber ja selbst gar nicht verändert werden kann. Da müsste man dann eine Regelung vorsehen, dass diese Nachbesserungsaufforderung auch an den Hersteller gerichtet werden darf, und nicht nur an den Betreiber, der gar nicht in der Lage ist, diese Anforderung zu erfüllen.
Die dritte Frage bezog sich auf die Sanktionen.

Sowohl die Sicherungspflichten der Betreiber Kritischer Infrastrukturen als auch die Meldepflichten Kritischer Infrastrukturen werden sicher von einer großen Anzahl von Unternehmen befolgt. Die sind nicht der Gegenstand oder die Adressaten von Sanktionen. Wir müssen aber dafür sorgen, dass nicht die, die die Regeln befolgen, dann diejenigen sind, die Wettbewerbsnachteile haben. Weil, dann werden die sich das auch dreimal überlegen, ob sie das noch weiter tun. Um hier eine Wettbewerbsgleichheit herzustellen, ist eine Sanktion notwendig. Wie die aussehen könnte, ist im Gesetzentwurf nachzulesen, nämlich in der Regelung zu § 149 TKG. Da ist das schon geregelt. Und genau die Regelung könnte man übertragen auf die Pflichten nach §§ 8a und 8b BSI-Gesetz. Die letzte Frage betraf die Zweckbindung von Informationen, die man dadurch gewinnt, dass man Produkte auf ihre Sicherheit hin überprüft. Da ist eine Zweckbindung im Absatz 2 des § 7a darin. Aber da muss man schon ein sehr guter Jurist sein, um das durch die Verweisungstechnik, die dort verwendet wurde, herauszufinden. Dieses Gesetz wird vermutlich nicht nur von hochspezialisierten Rechtsabteilungen angewendet, sondern auch von dem einen oder anderen, der sich in so einer Verweisungstechnik nicht auskennt. Von daher wäre es schon sinnvoll, wenn man genau die Frage auch noch einmal präzise und detailliert beschreibt, und nicht nur in so einer – sage ich einmal – für Juristen nur lesbaren Verweisungstechnik. Vielen Dank.

Vors. **Wolfgang Bosbach** (CDU/CSU): Herr Prof. Schiller.

SV **Prof. Dr.-Ing. Jochen Schiller** (Freie Universität Berlin, Institute of Computer Science): Ja, ich bin ja hier so eher der Techniker, aus dem Juristischen halte ich mich heraus. Aber mir ist es immer unverständlich, wenn man so tut, als wäre der IT-Bereich jetzt auf einmal etwas ganz, ganz Neues. Wenn Sie bei der Bahn die Dienstleistung kaufen, ich möchte von A nach B fahren, die Bahn kommt nicht pünktlich und Sie sagen, ich hätte gern mein Geld zurück, dann ist es Ihnen egal, ob es das Antriebsaggregat von irgendeinem Hersteller war, oder ob kein Lokführer da war, oder wie auch immer. Wenn Sie heute ein Auto kaufen, und es tut irgendetwas nicht, dann sagen Sie auch nicht, das war das Einspritzsystem von X, dann muss ich zu der Firma X gehen – Sie gehen zu Ihrem Autohändler. Wenn jetzt über ein Drittel der Wertschöpfung im Autobereich schon die IT ist, wo gehen Sie dann in Zukunft hin? Gehen Sie dann zu irgendeiner IT-Firma, weil Ihr Auto etwas nicht tut? Nein, Sie gehen zum Händler, natürlich vom Auto. Deswegen ist es auch nicht einzusehen, dass man sagt, na ok, irgendjemand bietet ein Produkt an oder eine Dienstleistung, und sagt, ich habe keine Ahnung, was da für Technik, was da für Hardware darin steckt. Da muss die entsprechende Unternehmung dann eben zu Verträgen – wie der Automobilkonzern das macht mit einem Zulieferer – sagen, ihr erfüllt diese und jene Kriterien, dann dürft Ihr bei mir herein, wenn ihr das nicht macht, dürft ihr bei mir nicht rein, und nicht einfach sich Hardware sich einkaufen, wie auch große Telekommunikationsunternehmen das schon gemacht haben, von denen sie keine Ahnung haben, wie die funktioniert. Wenn etwas schiefgeht, lässt man sich schnell Ingenieure einfliegen und redet sich heraus. Das ist der eine Punkt. Das Nächste ist, auch gar nicht logisch, warum dann solche Sachen wie Haftung nicht richtig greifen sollen. Wieder das Beispiel Auto. Wenn immer mehr Software darin ist, bei Software greift keine Produkthaftung. Hält man das in Zukunft noch durch? Man wird immer zum Autohersteller dann sagen, Dein Auto ist gegen den Baum gefahren weil … und mir ist es egal, ob es die IT war, die Software, die Hardware, wie auch immer. Das ist genau die Marke, das Auto. Deswegen denke ich, dieses Weiterleiten, dieses Weiterpropagieren von Verantwortlichkeiten … – landen wir zum Schluss dann beim Hersteller vom Silizium für den Chip, weil der irgendwie gepfuscht hat? Das kann es natürlich nicht sein, deswegen eine Schnittstelle zum Kunden, dann auch von der Verantwortlichkeit her.

Vors. **Wolfgang Bosbach** (CDU/CSU): Herr Präsident Hange.

SV Präs. **Michael Hange** (Bundesamt für Sicherheit in der Informationstechnik): Ja, zunächst zu Mitwirkungspflichten von Herstellern, also auch zum Thema Sanktionieren. Man muss ja einfach sehen – ich sage einmal so – mit den Mindeststandards wird ein Rahmen vorgegeben. Ein Rahmen, den durchaus die Betreiber Kritischer Infrastrukturen mit organisatorischen Maßstäben und

mit Produkten, die dann diesen Standard erfüllen, dann auch eigenständig ausfüllen können. Es ist also so, dass die Bindung hier des Herstellers an den Betreiber Kritischer Infrastrukturen auch durch entsprechende AGB`s vorhanden ist. Das heißt, wenn eine Schwachstelle vorgefunden wird, muss sie auch beseitigt werden. Das BSI hat hier natürlich die Möglichkeit zu warnen, und wir machen davon auch Gebrauch. Wir können auch öffentlich warnen. Das haben wir inzwischen mehrere Male praktiziert, und das hat einen sehr großen Wirkungsgrad, auch international, auch gegenüber Globalplayern. Und ich glaube, dieser Weg, über das Gesetz auf Zulieferer einzuwirken, wie die Produkte zu gestalten sind, was an Krypto-Mechanismen da sein muss, was an Authentisierung, was auch an Cyber-Abwehrmechanismen und an Detektionsmechanismen da ist, das wird einfach durch diese Mindeststandards deutlicher. Die konkrete Produktauswahl ist dann aber immer etwas, was dann auch am Markt entschieden werden muss. Und die Möglichkeiten, dann Schwachstellen auch öffentlich zu benennen, wenn sie nicht abgestellt werden, schafft die Möglichkeit, im Grunde auch Druck auf Hersteller, gerade im Bereich Kritischer Infrastrukturen, dann auch auszuüben. Die zweite Frage ist die Frage der Zweckbindung von Meldungen. Es ist also hier im Gesetzesvorschlag vorgesehen, dass diese Meldungen nur dazu dienen, wirklich Kritische Infrastrukturen zu stärken, auf Schwachstellen hinzuweisen. Und es ist keine Weitergabe der Meldungen, und von Schwachstellen schon gar nicht, an Dienste vorgesehen. Das entspricht auch nicht dem gesetzlichen Auftrag des BSI. Dort sind die Prozesse, überhaupt der Zusammenarbeit mit Polizeien und Diensten, genau beschrieben, und vor allen Dingen jede Unterstützung der Polizeien und Dienste muss auch aktenkundig gemacht werden. Es ist insofern auch alles nachvollziehbar.

Vors. **Wolfgang Bosbach** (CDU/CSU): Frau Wawzyniak bitte.

Abg. **Halina Wawzyniak** (DIE LINKE.): Ja, ich habe zunächst einmal eine ganze Batterie an Fragen an Herrn Neumann und dann noch Fragen an Herrn Schiller, Herrn Hornung und Herrn Hange. Ich fange einmal mit Herrn Neumann an. Sie haben ja in Ihrem Statement den größeren Endnutzerschutz als zentralen Punkt genannt, und vor diesem Hintergrund möchte ich Sie doch noch einmal zu den Meldepflichten fragen. Sie haben vorhin gesagt, solche Meldepflichten haben noch keinen Hack verhindert. Die Frage ist für mich schon die, wenn Sie den Endnutzerschutz in den Mittelpunkt stellen, ob vor dem Hintergrund, dass auch Endnutzerinnen und Endnutzer irgendwie ja mit Problemen umgehen müssen, ob es da nicht doch eine Möglichkeit gibt oder ob es doch sinnvoll sein kann, so eine Meldepflicht zu haben, aus der Sicht von Endnutzerinnen und Endnutzern. Das würde ich gerne verbinden mit der Frage, ob es unter diesem Gesichtspunkt nicht eher ein Mehr an Meldepflichten geben müsste, nämlich eher die Frage, ob nicht auch Details zu Sicherheitslücken und zu Möglichkeiten der Beseitigung und der Umgehung von Sicherheitslücken öffentlich gemacht werden müssten, und ob es sinnvoll wäre, ein Verbot des Handelns mit Sicherheitslücken im Gesetz zu verankern. Das Zweite, was ich Sie fragen wollte ist das, Sie haben vorhin gesagt, dass der Stand der Sicherheit der Technik sowieso das ist, was schon die ganze Zeit vorhanden ist, und Sie hätten gern mehr Proaktivität in diesem Gesetzentwurf. Daher wollte ich Sie fragen, ob Sie da eine Idee haben, wie diese Proaktivität in so einem Gesetz verankert werden könnte, wie die aussehen könnte? Die dritte Frage: Sie haben die ambivalente Funktion des BSI angesprochen, als ein Amt, das dem Bundesministerium des Innern unterstellt ist. Auch wieder aus der Sicht der Endnutzerinnen und Endnutzer könnte es ja möglicherweise sinnvoll sein, so eine Art Auditierung vorzunehmen von Infrastrukturen, von Teilen von Infrastrukturen. Das erscheint mir ein bisschen schwierig, solange das BSI dem BMI untergeordnet ist. Wäre a) eine Auditierung sinnvoll und b) wäre es auch vor dem Hintergrund einer Auditierung möglicherweise sinnvoll, das BSI quasi als unabhängige Stelle zu konstruieren? Meine letzte Frage an Sie, Sie haben vorhin gesagt, dass, wenn es einen akuten Störfall gibt, man nicht gefühlte 100 Jahre gespeicherte Daten braucht, und Sie haben den § 100 TKG kritisiert. Nun hat Herr Tschersich vorhin gesagt, dass man ja trotzdem sozusagen ein paar Dateien braucht, um zu gucken, ob es einen Angriff gibt. Vor diesem Hintergrund würde ich Sie bitten, einfach noch einmal etwas zu sagen zu diesem § 100 TKG, wie Sie das sehen. In welchem Umfang welche Daten überhaupt, ob, und

wenn ja, wie lange sie gespeichert werden müssen. Herrn Schiller würde ich gern noch einmal fragen, und die Frage geht auch gleichzeitig an Herrn Hornung, es betrifft so ein bisschen den Anwendungsbereich. Wenn ich das Gesetz richtig gelesen habe, dann werden aus dem Gesetz Unternehmen herausgenommen. Herr Schiller hat von KMU, glaube ich, gesprochen. Wenn ich des richtig gelesen habe, ist die Grenze dort 250 Mitarbeiter und eine Bilanzsumme von 43 Millionen Euro. Also alles, was mehr als 250 Mitarbeiter hat und eine Bilanzsumme von mehr als 43 Millionen Euro hat, das würde dann unter das Gesetz fallen. Da würde mich bei Herrn Hornung interessieren, ob das sozusagen mit dem Bestimmtheitsgebot irgendwie noch Sinn macht. Aber aus meiner Sicht – ehrlich gesagt – nicht, weil entweder ist etwas kritisch oder es ist nicht kritisch. Das kann aber nicht an der Mitarbeiterzahl festgemacht werden. Und die gleiche Frage auch noch einmal an Herrn Schiller. Sie hatten gesagt, im zweiten Schritt soll man darüber nachdenken, ob es nicht sinnvoll ist, gleich von Anfang an alle einzubeziehen. Meine letzte Frage geht an Herrn Hornung und an Herrn Hange. Ich hatte beim Lesen des Gesetzentwurfes ganz hinten gefunden, dass das Bundesamt für Verfassungsschutz bis zu 50 Stellen mehr bekommen soll in Erfüllung dieses Gesetzes. Auch stand es irgendwie darin, dass diese 50 Stellen mehr eingeführt werden sollen, weil ja das BSI Daten dem Bundesamt für Verfassungsschutz übermittelt. Jetzt habe ich mir das Gesetz angeguckt und finde im § 8b Abs. 2 Satz 4 aber nur „Unterrichtungspflichten“. Deswegen ist meine Frage an Herrn Hornung, ob der § 8b Abs. 2 Satz 4 tatsächlich eine Möglichkeit zur Datenübermittlung an das Bundesamt für Verfassungsschutz sieht? An Herrn Hange auch die Frage, ob er das sozusagen als Ermächtigungsgrundlage für eine Datenübermittlung sehen würde, oder ob möglicherweise schon bereits jetzt Daten einfach übermittelt werden?

Vors. **Wolfgang Bosbach** (CDU/CSU): Herr Neumann.

SV **Linus Neumann** (Chaos Computer Club (CCC), Berlin): Vielen Dank für die ausführlichen Fragen, ich hoffe, ich habe mir alle gemerkt. Die erste Frage betraf die Meldepflichten. Da hat Herr Tschersich auch gerade korrekt angemerkt, es wäre jetzt der Fall denkbar, es findet ein Angriff auf die Deutsche Telekom statt. Die Deutsche Telekom ist in der Lage, den zu detektieren und irgendwie abzuwehren. Sie warnt dann die anderen und die werden dann vor diesem Angriff geschützt, und dann ist ja etwas Gutes geschehen. Gleichzeitig haben wir aber auch schon darüber gesprochen, dass es sich um Ad-hoc-Angriffe handelt und dass ein Angriff dann in der Regel erfolgreich ist, wenn er neuartig ist. Denn Sie haben in Ihrer Infrastruktur eine ganze Menge Dinge zu stehen, was jeden bekannten Angriff und jede bekannte Sicherheitslücke irgendwie abwehren soll. Vorausgesetzt, dass sich das alles in einem halbwegs normalen Betrieb befindet. Sie sind also gegen bekannte Angriffe – als halbwegs vernünftig aufgestellte Infrastruktur – sehr gut geschützt. Es fängt dann aber an, oder besser, die hohe Kunst fängt dann an, wenn wir von neuartigen Angriffen sprechen. Weil nämlich genau die Sicherheitslücke ausgenutzt wird, die wir noch nicht kannten, der Angriff passiert, von dem man nicht wusste, dass er möglich sein würde. Nehmen wir einmal so ein OpenSSL-Beispiel, wo dann auf einmal ein zwei Jahre alter Bug gefunden wird in einer höchstsicherheitskritischen Software, die von vielen deutschen Banken benutzt wird, und der damit die Sicherheit des Online-Banking massiv bedroht. Das wäre jetzt so ein akuter Fall, den keiner vorhersehen konnte, den auch im Zweifelsfall der größere Teil der Unternehmen nicht detektieren konnte. Und genau da geht nämlich das Problem los, um den neuartigen Angriff zu detektieren, muss ich ihn sehen und bemerken. Hier ist es durchaus eine korrekte Feststellung, dass die meisten deutschen Unternehmen in diesem Bereich noch größere Defizite aufweisen. Gleichzeitig hat der Angreifer aber im Zweifelsfall keine Motivation, erst die Deutsche Telekom anzugreifen und zu warten, bis die Deutsche Telekom den Angriff abgewehrt, erkannt und ausgewertet hat und dann andere warnt, – bevor der Angreifen dann – was weiß ich, beispielsweise – nicht Konkurrenten, sondern andere Marktteilnehmer angreift. Ja, das heißt also, als Angreifer habe ich relativ wenig Grund, hier darauf zu warten, bis irgendjemand meinen abgewehrten Angriff ausgewertet und in Ruhe erkannt hat. Geschweige denn, vielleicht erkennt er ihn auch überhaupt nicht, nicht wahr. Was also die Meldepflichten angeht – es wird hier jetzt das hohe Lied auf die

Meldepflichten gesungen, alle werden davon profitieren – dann fragt man sich natürlich, warum es freiwillig keiner macht im Moment. Denn seit 2012 haben wir ja die Gelegenheit in der Allianz für Cybersicherheit, solche Meldungen abzugeben. Die Unternehmen haben die Möglichkeit, eben freiwillig dort teilzunehmen und davon zu profitieren. Jetzt wird man sofort sagen, … ja das tun sie aber doch, das tun sie aber doch, … großer Erfolg die Allianz für Cybersicherheit … Dann frage ich mich, warum das jetzt in ein Gesetz geschrieben werden muss? Insofern, irgendetwas funktioniert da nicht ganz richtig. Ein weiteres Problem, welches ich noch nicht angesprochen habe – und dabei haben wir gerade über die Endnutzer gesprochen – ist das Problem, dass Unternehmen die IT-Sicherheit als ein sehr multidimensionales Problem betrachten müssen. Es gibt sehr viele Angriffsmotivationen, viele davon sind auf einen direkten Schaden des Unternehmens ausgerichtet, einige davon nicht. Grundsätzlich sind die Angreifer-Motivationen aber von der Seite des Angreifers gedacht. Das heißt, ich habe als Angreifer ein bestimmtes Angriffsziel, von dem ich mir einen bestimmten Profit verspreche, und für diesen Profit, oder für diesen Vorteil, oder für dieses Ziel bin ich bereit, einen gewissen Aufwand in Kauf zu nehmen. – Und nun kann es sein, dass ich beispielsweise geistiges Eigentum stehlen möchte und damit sehr konkret den Kern des Geschäftsinteresses meines Opfers berühre, und dass ich ein Risiko-Szenario oder ein Angriffs-Szenario realisieren möchte, was mein Ziel im Zweifelsfall auch schon bedacht hat. Ja, also zum Schutz des geistigen Eigentums veranlassen die Unternehmen in der Regel relativ große Schutzvorkehrungen. Gleichzeitig scheinen ja, wenn man sich einfach nur die erfolgreichen Angriffe anschaut, die Schutzmaßnahmen zum Schutze der Kundendaten irgendwie etwas geringer in der Wertigkeit zu rangieren. Denn da sind die Angriffe offenbar häufiger erfolgreich. Was ich denke ist, wenn man regulatorisch eingreifen möchte, dann sollte man insbesondere den Unternehmen dort Anreize geben. Durch Haftung, durch Zwänge, durch vielleicht Steuererleichterungen – das müssen Sie sich überlegen, was Sie da machen wollen. Genau diesen Risiko-Szenarien zu begegnen, die eben nicht das Kerngeschäftsinteresse der Unternehmen betreffen, sondern bei denen andere Personen, insbesondere natürlich die Endnutzer, zu Schaden kommen. Also, ich muss einem Betreiber einer Gelddruckmaschine nicht erklären, wie er diese Gelddruckmaschine am Laufen lässt. Ja, aber was am Rande von dieser Gelddruckmaschine noch alles ´reingeschoben wird und wo auch noch Angreifer daran Interesse haben können, – da ist es völlig selbstverständlich, dass Unternehmen diesen Angriffsrisiken geringere Prioritäten zuweisen. Das ist völlig verständlich, das ergibt sich aus den Anreizen, und wenn man da regulatorisch eingreifen möchte, da muss man eben diese Anreizlandschaft verändern. Dann wurde noch gefragt nach konkreteren Maßnahmen, die also zum Schutz von Endverbrauchern beitragen würden, und es wurde auch angemerkt, dass kleine und mittelständische Unternehmen und eigentlich jedes Unternehmen, dass nicht als Kritische Infrastruktur eingestuft ist, nicht wirklich besonders in den Genuss dieses IT-Sicherheitsgesetzes kommen wird. Da sehe ich andere Möglichkeiten, die da sehr viel sinnvoller wären. Ich hatte das in meiner Stellungnahme an den Bundestagsausschuss „Digitale Agenda“, die ja diesem Gesetzesentwurf vorausging, auch so vorgeschlagen. Dass man sagt, schauen wir doch einmal, was sind denn zum Beispiel Software-Produkte, auf denen ein großer Teil unserer Infrastruktur basiert? Beispielsweise dieses OpenSSL, ja! – OpenSSL hatte diesen Heartbleed Bug, den kennen Sie alle. Das war der, wo alle auf einmal völlig panisch waren und die gesamte Sicherheit des Internets kaputt war, – ganz so schlimm war es nicht, aber es war nahe dran. Dieser Bug bestand zwei Jahre in diesem quelloffenen Paket. Ein Open-Source-Produkt, das – wie gesagt – Banken in Deutschland und alle möglichen Anbieter von Telediensten nutzen, das frei zur Verfügung steht, und das als der Stand der Technik gilt. Ja, also wenn man das nutzt, dann macht man nichts falsch. Gleichzeitig hatte offensichtlich niemand dieser Nutzer, keines der Unternehmen, irgendein Interesse daran, dieses kostenlose Software-Produkt einfach einmal einer Auditierung zu unterziehen, um seine eigene Risikolandschaft zu verringern. Das hat sich dann irgendwann bösartig gerächt, als dann Google und die Firma „Codenomicon“ das einfach einmal gemacht haben. Die Profiteure dieser Sicherheitsüberprüfung waren alle, die am Ende diese Sicherheitslücke weniger hatten. Das ist natürlich auch der Grund, warum ein einzelnes deutsches

Unternehmen wahrscheinlich keine große Motivation verspürt, eine Auditierung eines Produktes vorzunehmen, das allen kostenfrei zur Verfügung steht. Insofern auch hier ein soziales Dilemma, die Unternehmen haben keinen Anreiz, da hinein zu investieren, sie profitieren aber ohne Ende davon. Gleichzeitig haben sie überhaupt gar kein Problem damit, jede Einzelplatz-Windows-Lizenz ihrer 10 000 Firmen-Laptops zu bezahlen. – Aber für den Grundpfeiler der IT-Sicherheit eines Online-Banking-Systems Geld auszugeben, das ist da einfach nicht motiviert. Da könnte ich mir schöne Lösungen vorstellen, beispielsweise dass man so einen Fonds einrichtet, gerne auch unter Verwaltung des Herrn Hange. Der dann sagt, passen Sie einmal auf, wir haben uns das hier angeschaut, das und das und das sind Software-Produkte, auf denen wirklich vieles unserer Sicherheitsannahmen basiert. Da werfen wir jetzt einmal alle möglichen Auditierungen darauf, da werfen wir Bug-Bounties (bounty: Kopfgeld) darauf – und wir sorgen dafür, dass das richtig gehärtet wird. Davon werden dann alle profitieren! Weil diese Produkte eben allgemein frei zur Verfügung stehen. Gleichzeitig kann man natürlich sagen, was machen wir denn mit der proprietären Software? Der Ausspruch stammt nicht von mir, und ich weiß auch nicht genau, von wem er stammt, aber es gibt so einen Vergleich zwischen Software- und Drogenhändler. Das sind so die einzigen, die noch ohne jegliche Garantie operieren können auf dem deutschen Markt. Eine Software wird geliefert, da haftet niemand dafür. Wenn da irgendetwas schiefgeht – und das wird ja hier auch von den anderen Sachverständigen bemängelt – wenn wir da jetzt eine reine Haftung auf den Betreiber abwälzen, dem sind in vielen Fällen die Hände gebunden, weil der größere Teil der Software, die eingesetzt wird, eben von Zulieferern kommt. Hier haben Sie teilweise sehr lange Fristen, bis Sie von denen überhaupt eine Antwort bekommen und dürfen dann noch längere Zeiten darüber diskutieren, ob es sich da überhaupt um Sicherheitsschwankungen handelt, die Sie festgestellt haben, oder nicht! – Insofern, eine ganz einfache Haftung, würde mit sehr viel weniger Bürokratie einen sehr schönen Effekt erzielen. Kurz am Rande sei noch angemerkt, dass natürlich die gesamte Awareness (Bewusstsein) für Themen der IT-Sicherheit in der „Grundbevölkerung“, so auch bei den Mitarbeitern dieser Kritischen Infrastrukturen, wahrscheinlich noch nicht so hoch ist, wie sie sein könnte. Da könnte man also auch in Awareness-Kampagnen, in Schulungen und so weiter investieren. Auch hier ist nichts in dieser Richtung gegeben. Ich hoffe, damit habe ich einen größeren Teil der Proaktivität von Frage 2 auch schon mit abgedeckt. – Die Frage zur Unabhängigkeit des BSI, ich hatte das eingangs auch schon betont, wäre mir ein dringendes Anliegen. Das BSI hat ein Image-Problem. Einerseits aufgrund der Vorkommnisse, die wir eben in der IT-Sicherheit für die Bevölkerung dieses Landes sehen. Also durch das Mitarbeiten an einem Staatstrojaner, durch eine nicht auch nur mangelhafte, sondern absolut ungenügende Aufklärung über diese Identitätsdiebstähle, die in den letzten Jahren bekannt wurden, wo also bis heute der größere Teil der Menschen, die da zum Opfer gefallen sind, nicht sinnvoll darüber informiert wurde – da haben wir also schlechte Erfahrungen gemacht als Zivilbevölkerung. Und ich leite aus dem bisherigen Erfolg der Allianz für Cybersicherheit, die jetzt in irgendein Gesetz gegossen werden soll, auch ab, dass da der Erfolg nicht so groß ist. Ich glaube, dass das Kernproblem die mangelnde Unabhängigkeit des BSI ist. Ich denke, insgesamt kann man in dieser Behörde auf Kompetenz hoffen. Insgesamt liest man auch auf den Seiten des BSI ganz interessante Dinge, und es ist leider, wie ich auch eingangs erwähnt habe, sehr schade, dass sich dieses Gesetz nicht auf die Lageberichte des BSI, die es übrigens nach meinen Recherchen seit 2009 regelmäßig herausgibt – Herr Hange, also müssten Sie Ihren Text noch einmal kurz anpassen – kann man also sehen, dass die Bedrohungsszenarien, die da dokumentiert sind, mit diesem Gesetzentwurf eben leider nicht angesprochen werden. Zuletzt ging es dann noch einmal um die Daten. Der Herr Tschersich hatte mich da zurecht darauf hingewiesen, ich kann ein – insbesondere ein Kommunikationssystem – vor allem auch von der Größe wie das, für das der Herr Tschersich verantwortlich ist, nicht im Blindflug operieren lassen. Da fallen alle möglichen Daten an, und diese Daten brauche ich auch zur Kontrolle der Funktionalität dieses Systems. Was ich aber nicht machen kann, ist ein Schreiben, – wir formulieren einen Freibrief … alle Daten dürfen zeitlich unbegrenzt aufgehoben werden … und … Wie gesagt, im Falle eines konkreten Störfalles, das habe ich in meiner

Stellungnahme auch ausformuliert, gibt es durchaus auch die konkrete Notwendigkeit, wirklich in Verkehrsdaten hineinzuschauen und da auch wirklich – ja herbe – Verletzungen des Datenschutzes zu begehen, um den Betrieb dieser Infrastruktur aufrecht zu erhalten, um den Angriff vernünftig aufklären zu können und abwehren zu können. Das ist in der Tat richtig. Soweit ich das sehe, ist in diesem Fall – wenn ich mich nicht täusche, sogar heute schon – ein Informieren der Nutzer notwendig. Das heißt, wenn die technische Notwendigkeit gegeben ist, sollte selbstverständlich dem Betreiber das Recht gegeben werden, alles zu tun, was zur Aufklärung des Angriffes notwendig ist und was zur Abwehr des Angriffes notwendig ist. – Aber dann doch bitte auch die betroffenen Nutzer im Nachhinein vernünftig darüber informieren und dann bitte diese gesamte Maßnahme eine einmalige, durch den akuten Störfall ausgelöste, Maßnahme sein lassen. Und nicht stattdessen im Prinzip, sich einen gesetzlichen Freibrief holen dafür, um einfach Daten zu speichern. Wie gesagt, bei dieser Speicherdauer, die durch den Arbeitskreis Vorratsdatenspeicherung dokumentiert ist, die eben zwischen drei und 180 Tagen schwankt – da sieht man ja schon, dass es für die Verwendung dieser Daten zum Zwecke der Erkennung, Eingrenzung und Behebung von technischen Störungen sehr unterschiedliche Meinungen gibt, wie viele Daten man da wohl so braucht. Und das diese Daten eben im Regelfall, zum Beispiel von der Abmahnindustrie angefragt werden, die genau diese Daten, die nach § 100 TKG gesammelt werden, dann im Rahmen der Halterfeststellung für Kleinstvergehen anfragen im Rahmen zivilrechtlicher Forderungen. Da sieht man ja schon, dass hier *offenbar* ganz massive Einschränkungen des Verwendungszwecks notwendig sind. Und auch an der Streuung, wie unterschiedliche Unternehmen diese Datenvorhaltungen betreiben, sieht man, dass da eine gesetzliche Vereinheitlichung notwendig ist. – Wie gesagt, gleichzeitig denke ich, dass da also wenige Stunden bis Tage absolut ausreichend sind, um eine Störung zu erkennen, einzugrenzen und zu beheben. Gleich-zeitig sei aber auch festgestellt, dass gerade im Telekommunikationsbereich natürlich für die Einzelverbindungsnachweise und andere Sachen schon viel längere Datenvorhaltefristen gesetzlich … oder aber technisch notwendig sind. Ja, also ich kann meinen Einzelverbindungsnachweis von vor drei Monaten bei meinem Mobilfunkanbieter abgreifen. Das heißt, da ist schon eine viel ausführlichere Datenvorhaltung gegeben, die da stattgefunden hat. Insofern sehe ich für diesen § 100 TKG einfach keine Notwendigkeit. Vielen Dank.

Vors. **Wolfgang Bosbach** (CDU/CSU): Herr Präsident Hange.

SV Präs. **Michael Hange** (Bundesamt für Sicherheit in der Informationstechnik): Ich möchte zunächst die Frage beantworten und vielleicht, Herr Vorsitzender, wenn Sie gestatten, auch auf einige Punkte einzugehen, die das BSI direkt betroffen hat.

Vors. **Wolfgang Bosbach** (CDU/CSU): Ja klar!

SV Präs. **Michael Hange** (Bundesamt für Sicherheit in der Informationstechnik): Die Frage, die Sie gestellt haben, 50 Stellen für das BfV. Hier möchte ich folgendes dazu sagen: Es ist so, dass das BSI als technische Behörde den technischen Blick auf die Analyse hat. Wir werden die eigene Meldung analysieren, das Bedrohungspotential herausarbeiten und dann warnen bzw. auch Handlungsempfehlung geben und wenn man Angriffe abwehren kann, haben wir dies in der Vergangenheit auch so getan. Natürlich ist das Ganze wichtig, wenn es bedeutsame Angriffe sind, also sogenannte APT-Angriffe, dann auch eben fallbezogen Lageberichte, jährliche Lageberichte, dann einzuarbeiten. Das Ganze hat natürlich auch nun eine Täterdimension, wer dahinter stehen kann, und wenn es so ist, dass es sich erkannterweise um Spionage handelt, da gibt es auch Rahmenbedingungen, die dann Übermittlungen ermöglichen, genauso beim BfV. Ich kann nur einen Hinweis geben, um eine Vorstellung zu geben, selbst bei den Angriffen auf die Regierungsnetze, liegt der Anteil der Meldungen der hochwertigen Angriffe im einstelligen Bereich. Sehr sorgfältig wird damit umgegangen und auch im jährlichen Bericht an die Datenschutzbeauftragte besonders erwähnt. Also das ist wichtig, dass wir das deutlich machen. Es liegt hier in dem Kooperationsverbund im Vordergrund, dass die Meldungen umgesetzt werden in Maßnahmen und dass ein Rückfluss an die Betroffenen erfolgt. Und ich sage auch über die kritischen Infrastrukturbetreiber hinaus: Wenn wir feststellen, irgendwelche

Schwachstellen, irgendwelche Probleme, sind für andere auch relevant, machen wir sie auch öffentlich. Das ist im Verfahren so vorgesehen. Deshalb ist das Lagezentrum jetzt schon ausgebaut. Es wird noch weiterentwickelt, um sowas dann auch, weil auch die Betreiber kritischer Infrastruktur dazu verpflichtet sind, auch im 24-Stunden-Sieben-Tagebetrieb zu arbeiten. Der zweite Punkt, den Herr Neumann angesprochen hat, ist Heartbleed. Wir im BSI machen als Amt auch Open Source. Auch wenn es manchmal nicht immer so flott und einfach ist, wie wenn man proprietäre Software kauft. Aber wir haben auch hier im Amt sehr viele, die das auch aus Überzeugung nutzen. Hier ist es in der Tat so – das hat sich herausgestellt, man muss auch Open Source prüfen. Die Vorstellungen, die wir haben, ist also, bei der Förderung von GnuPG, der Ende-zu Ende-Verschlüsselung und der Prüfungen von Open-Source Produkten in Deutschland durch BSI finanziert werden. Dass wir hier auch im Sinne von einer Art Rollenverteilung nur die Rolle des Prüfens übernehmen, nicht aber die Rolle des Entwicklers. Dass wir Prüfvorgänge – wir haben Evaluierungsstellen – dass wir dann Stellen beauftragen, die das prüfen, so dass die Krypto-Bibliothek als das Herz von Sicherheit auch weit verbreiteter Produkte, dass das dann auch geprüft wird. Das wäre dann unser Beitrag, das zu finanzieren, unter Umständen auch eigene Energien reinstecken. Ich halte es auch für wichtig, dass wir das Instrument der Zertifizierung nutzen, um auch proprietäre Softwareprodukte stärker zu prüfen. Wir machen das im großen Umfang, zum Beispiel mit gesetzlichen Vorgaben, also die ganze Chipkarte, die wir hoheitlich einsetzen, auch die Gesundheitskarte von den Krankenkassen wird von uns zertifiziert, auch Smart-Meter werden zertifiziert, also dass man Sicherheitsvorgaben macht und die Hersteller dann auffordert, gerade wenn die Punkte groß in die Breite gehen, sie zertifizieren zu lassen. Dann der Punkt Mitarbeit beim sogenannten Staatstrojaner. Es wird ja auch Gegenstand des NSA-Untersuchungsausschusses sein, weil die Unterlagen dort vorliegen. Es ist eindeutig so, dass, wenn ein Gesetz vorsieht, dass die Online-Durchsuchung kommt, dass das BSI dann auch beauftragt werden kann, für die Sicherheit zu sorgen, dass die Krypto-Mechanismen stark sind, dass die Informationen nicht an falsche Leute geraten, weil die Übertragung bzw. die Speicherung unsicher ist. Nur darauf beschränkt sich die Mitwirkung. Das ist mir wichtig, hier festzustellen. Bei Identitätsdiebstahl – ich habe zugestanden, dass am Anfang das erste Mal bei 18 Millionen das mit den Servern etwas ruckelig war. Wir haben das aber in Griff gekriegt. Wir haben beim zweiten Mal im Grunde schon den eleganteren Weg gewählt, dass wir die Provider eingeschaltet haben, und heute ist das Geschäft des Warnens „Business as usual“. Wir bekommen täglich bis 20.000 IP-Adressen, die wir an die Provider weiterreichen und damit Bürger gewarnt werden auf direktem Weg, so dass in dieser Provider-Kunden-Beziehung dann die Kunden direkt adressiert werden. Was mir aber noch besser gefallen würde, das ist eine gemeinsame Anstrengung. Wir hatten an sich gehofft, dass unser Empfehlungskatalog mit den 11 wichtigsten Maßnahmen für den Bürger mehr ins Allgemeinbewusstsein dringen wird. Ich glaube, es ist ein gesamtgesellschaftlicher Auftrag, für den Bürger mehr an IT-Sicherheit zu machen. Dann wir können nicht davon ausgehen, dass wir den Bürger perfekt schützen, schon gar nicht vor Nachrichtendiensten. Aber diese 80/20-Regel mit einem gewissen Aufwand von Maßnahmen hat doch einen größtmöglichen Wirkungsgrad und für uns ist es ein großes Anliegen, hierdurch vor allem kriminelle Bedrohungen für die Bürger zu reduzieren. Und das muss auch sehr pragmatisch angegangen werden. Das hat was mit Kooperationsmodellen zu tun und hat auch etwas mit Sensibilisierung zu tun.

Vors. **Wolfgang Bosbach** (CDU/CSU): Herr Prof. Hornung.

SV **Prof. Dr. Gerrit Hornung** (Universität Passau, Lehrstuhl für öffentliches Recht, IT-Recht und Rechtsinformatik): Die erste Frage an mich betraf die Ausnahmeklausel für kleine und mittlere Unternehmen. Es gibt in der Tat im Gesetz eine Minimalklausel. Sie bezieht sich aber nicht auf KMU, sondern auf sogenannte Kleinstunternehmen. Das sind nicht die von Ihnen genannten 250 Mitarbeiter, sondern 10 Mitarbeiter maximal und kumulativ maximal 2 Millionen Jahresumsatz. Es entzieht sich meiner Kenntnis, ob es auch unterhalb dieser Schwelle noch Unternehmen gibt, die möglicherweise sinnvollerweise einbezogen werden sollten. Das müssen die technischen Sachverständigen beurteilen. Ich würde allerdings sagen:

Die rechtliche Frage wäre, ob man diese Unternehmen dann unverhältnismäßig belastet. Das heißt, wenn wir die mit hineinnehmen, kann es sein, dass es für sie viel zu viele Kosten verursacht. Da müsste man wegen des insoweit unverhältnismäßigen Eingriffs möglicherweise über eine Kostenerstattung nachdenken. Die zweite Frage an mich betrifft die Übermittlungsbefugnisse an das BfV. Der § 8b, von Ihnen genannt, macht es dem BSI zur Aufgabe, unverzüglich die zuständigen Aufsichtsbehörden und sonstigen Behörden des Bundes zur Erfüllung ihrer Aufgaben über die erforderlichen Informationen zu unterrichten. Der Begriff des Unterrichtens ist meiner Meinung nach einigermaßen unspezifisch. Man kann das so verstehen, dass dort die Meldungen selbst zur weiteren Analyse oder zur gleichberechtigten Analyse der Unternehmen weitergereicht werden. Oder, man kann sagen, Unterrichtung hat was mit dem Ergebnis der Analyse zu tun, das heißt die Meldungen selbst werden nicht weitergegeben. Letzteres ist wohl nicht gemeint, wenn man sich die Stellenzuweisung ansieht. Es ist in der Tat, würde ich sagen, auffällig, dass die Gesetzesbegründung 30 bis 50 Stellen Bedarf für das BfV anmeldet für die Zuständigkeit nach dieser genannten Nummer 4. In dieser Nummer 4 befindet sich aber gar keine Zuständigkeit des BfV, sondern eine Aufgabenzuweisung des BSI, dem BfV zur Erfüllung seiner Aufgaben diese Informationen zu geben. Was das BfV damit macht, muss das BfV nach den Befugnissen entscheiden, die es heute auch schon hat. Es scheint aber, wenn man sich die Stellenzuweisung anschaut, so zu sein, dass offensichtlich ein substanzieller Teil der Auswertung beim BfV angesiedelt sein soll. Denn je nachdem, wie man die Stellenzuweisung so sieht, also BfV 30 bis 50, BSI 100 bis 200, könnte es am Ende sein, dass etwa 50 Prozent der Stellen. die das BSI bekommt, auch das BfV bekommt. Das BSI macht aber ja noch viel mehr, als diese Daten auszuwerten. Sie sollen mit den Herstellern zusammenarbeiten. Sie sollen Audits generieren. Sie sollen diese Audits überwachen und überprüfen, sie sollen die ganzen Meldungen entgegennehmen, und sie sollen auswerten. Wenn man diese ersten Teile abzieht, dann könnte es sein, dass die Auswertekapazitäten am Ende etwa gleichermaßen auf das BSI und das BfV verteilt werden. Das kann ich aus der praktischen Sicht nicht weiter bewerten. Mit Blick auf das, was ich aus rechtlicher Sicht – was die Öffentlichkeitsarbeit, die Transparenz, die Informationen gegenüber Dritten angeht – gesagt habe, sehe ich das kritisch. Vielen Dank.

Vors. **Wolfgang Bosbach** (CDU/CSU): Herr Prof. Schiller.

SV **Prof. Dr.-Ing. Jochen Schiller** (Freie Universität Berlin, Institute of Computer Science): Ich wurde zum Thema KMU gefragt, aber es ist schon so oft dieses Heartbleed gefallen. Stand der Technik und Sicherheitsbewusstsein: Ich möchte ein bisschen widersprechen. Es gibt einen Stand der Technik, also wir wissen genau, wie man mit Passwörtern umgeht. Wenn ich dann kein Passwort mache, ist es sicher nicht Stand der Technik. Auch dieses Thema Heartbleed OpenSSL. Bereits 1972 hat man bereits die Grundlage für solche Fehler veröffentlicht, 1988 ausgenutzt, 1996 gab es ein Handbuch dazu und 2012 programmiert jemand einfach nach gewissen Richtlinien, die eben nicht mehr Stand der Technik sind. Es ist auch kein Stand der Wissenschaft und keine abgefahrenen Sachen, sondern man hat damit ganz bewusst den Schutzmechanismus des Betriebssystems umgangen bei der Programmierung. Das ist nicht so ganz Stand der Technik. Warum KMU? Das passt genau in diesen Kontext rein, Bewusstseinsbildung. Natürlich wäre es schön, wenn KMUs mit dabei wären. Warum? Es gibt klitzekleine Mittelständler, die haben aber TOP-Produkte auf dem Weltmarkt. Weil sie eben nicht dieses Sicherheitsbewusstsein haben, kopiert jemand dieses Know-How und stellt diese ganzen Sachen für ein Zehntel vom Preis her und importiert sie. Der kleine Mittelständler ist einfach weg vom Markt. Das heißt, man muss ein Bewusstsein schaffen, auch wenn man nicht im ersten Schritt gleich sagt: Ihr müsst beispielsweise, ist ja keine kritische Infrastruktur, ihr müsst da mitmachen. Denn das würde in der Tat wahrscheinlich die meisten überfordern. Der zweite Grund, warum KMUs dabei sein sollten in einem nächsten Schritt ist natürlich, dass die Menge der KMUs zusammen doch durchaus einiges bewirken kann. Man stellt sich immer so ganz oft vor, das sind vielleicht ganz kleine, Energie- oder Wasseraufbereitungsanlagen, kleine Stadtnetze hier und da. Ich weiß, es sind alle nicht erfasst. Dennoch verwenden sie gewisse Steuerungssysteme. Da gibt es eben nicht 1 000 verschiedene, sondern sagen

wir mal ein Dutzend grob verschiedene. Wenn ich jetzt ein Land lahm legen will, dann gehe ich natürlich ganz gezielt an die ran, die relativ schlecht geschützt sind. Schauen Sie mal, wie gut Wasseraufbereitungsanlagen geschützt sind, oder, was auch immer, Abwasser etc. Wenn ich in der Menge Angriffe mache, bewirke ich doch einiges. Dann sind zwar die großen geschützt, aber die kleinen eben nicht. Deswegen: Ja, wünschenswert wäre es, das Bewusstsein weiter zu propagieren. Aber ich befürchte schon auf Grund der ganzen Diskussion so, wir werden nie vorankommen, wenn wir jetzt sagen: Verpflichtend alle rein. Dann werden wahrscheinlich alle aufschreien.

Vors. **Wolfgang Bosbach** (CDU/CSU): Herr Dr. von Notz

BE Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Herr Vorsitzender. Entschuldigen Sie meine Verspätung. Ich wollte unter der Überschrift IT-Sicherheitsgesetz auf Dinge eingehen, die von den Sachverständigen in den Gutachten auch teilweise beschrieben worden sind, nämlich dass man sich nach Snowden viele Szenarien vorstellt, die eben über das, was wir hier vorliegen haben, nämlich ein Meldesystem für IT-Angriffe hinausgeht. Deswegen meine erste Frage an die Professoren Roßnagel und Hornung und an Herrn Neumann: Was wären eigentlich nochmal ganz konkrete Punkte zusätzlich, die in ein solches Gesetz nach Ihrer Meinung als essentialer Bestandteil reingehörten, wenn man hier wirklich von einem IT-Sicherheitsgesetz reden will, das sozusagen auch die Bürgerinnen und Bürger und ihre IT-Sicherheit mit einbezieht. Die zweite Frage im Hinblick auf diese auch in vielen Stellungnahmen genannten Scheinabsicherungen, die hier teilweise vorgeschrieben werden, die wenig für die Sicherheit tun, aber so eine Alibifunktion erfüllen, was wären tatsächlich harte notwendige Prüfungsschritte, Evaluationskriterien, um an den Netzknotenpunkten Hard- und Software tatsächlich als sicher beschreiben zu können. Was ist mit Penetrationstests und muss man nicht regelmäßig die Chips selbst untersuchen? Vielleicht können Sie da nochmal so zwei, drei konkrete Dinge beschreiben, die vielleicht in diesem Gesetz fehlen.

Vors. **Wolfgang Bosbach**: An wen war die zweite Frage gerichtet?

BE Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Das geht alles an die drei eben genannten. Ich habe vier Fragen. Die dritte Frage bezieht sich nochmal auf das BSI. Da befrage ich den Präsidenten ausdrücklich nicht zu, weil er in dem Fall meiner Ansicht nach befangen ist. Wir haben in anderen Sachen da schon gesprochen. Ich sehe ein großes Problem in der Diskussion über IT-Sicherheit und Cyberwar und was sich alles unter diesen Begrifflichkeiten versteht, zwischen Angriff und Verteidigungsproblematiken. Deswegen die Frage im Hinblick auf das BSI. Kann es sein, dass diese Behörde dem Innenministerium unterstellt ist und nicht unabhängig ist bei diesen essentiellen hochproblematischen Entscheidungen und Abwägungen, die da getroffen werden müssen. Ich kann nur aus meinem NSA-Untersuchungsausschuss berichten. Da stellen sich einige Fragen im Hinblick auf das BSI. Deswegen die Frage: Sind Sie nicht der Meinung, dass diese Behörde für diese sehr wichtige Aufgabe nicht unabhängig gestellt werden muss, um sich diesen Logiken, die auch Angriffslogiken sind, in Cyber-Auseinandersetzungen - da braucht man nur die Debatte der letzten Wochen hier in Deutschland zu verfolgen - braucht man da nicht eine unabhängige Behörde. Zu guter Letzt die Frage: Das Ganze wird parallel in Europa unter der Cyberrichtlinie verhandelt, kommt wahrscheinlich in ein paar Monaten. Die Deutschen gehen jetzt hier ihren eigenen Weg. Man hofft dann, dass in Europa diese Dinge dann die Richtlinie werden, wenn ich das richtig verstehe. Macht das Sinn oder wäre es nicht sinnvoll, einfach noch ein paar Wochen zu warten, um dann für das globale Kommunikationsnetzwerk Internet zumindest eine europaweite Regelung zu bekommen und nicht einen deutschen Sonderweg. Vielen Dank.

Vors. **Wolfgang Bosbach** (CDU/CSU): Herr Prof. Hornung.

SV **Prof. Dr. Gerrit Hornung** (Universität Passau, Lehrstuhl für öffentliches Recht, IT-Recht und Rechtsinformatik): Zum einen zu den weiteren Punkten, die man sich noch vorstellen könnte. Da ist einiges aus technischer Sicht schon gesagt worden. Ich glaube tatsächlich, dass die Frage weiterer Maßnahmen eine wesentliche Dimension ist, weil sie den Bürger in den Mittelpunkt rückt

und weil wir es hier nicht nur mit einer Gewährleistungsverantwortung des Staates für kritische Infrastrukturen zu tun haben, sondern mit einer Schutzpflicht des Staates für die Grundrechte der Bürgerinnen und Bürger. Ich glaube, dass das eine wesentliche Dimension ist. Das bedeutet jetzt nicht, dass man alles das, was man sich hier wünschen würde, unbedingt in dieses Gesetz reinpacken müsste, aber ich glaube, dass es Teil einer Gesamtstrategie sein sollte. Auf die Anreize für Forschung und Entwicklung ist schon eingegangen worden. Ich glaube, wir müssen die Hersteller tatsächlich mit ins Boot holen, und ich habe, glaube ich, schon erwähnt, dass die Frage der Auditierung eine wäre, wo man ansetzen könnte, und zwar detaillierter, als das hier im Gesetzentwurf der Fall ist, der im Wesentlichen die Audits nur nennt, aber keine Kriterien, keine Zuständigkeiten, keine Rechtsfolgen, keine Vorgaben für die Angriffe, die dort gemachten werden, also Stichwort Penetrationstests usw. Ich glaube, dass man da tatsächlich einiges machen könnte. Anreize kann man auch durch Haftungsregelungen setzen. Auch das ist schon genannt worden. Man muss natürlich immer aufpassen, dass man da nicht das Kind mit dem Bade ausschüttet. Wenn wir jetzt gerade gehört haben, dass es praktisch unmöglich ist, Software von Anfang an fehlerfrei zu programmieren, dann dürfen wir keine Gefährdungshaftung einführen für fehlerfreie Software, denn dann programmiert niemand mehr Software, oder verkauft sie niemand mehr, weil er sich diesem Haftungsrisiko nicht aussetzen will. Ich glaube aber schon, dass Haftung ein Ansatzpunkt ist, und eine Möglichkeit, glaube ich, wäre das AGB-Recht, nämlich anzusetzen bei der Freizeichnungsmöglichkeit von den Betreibern kritischer Infrastrukturen oder auch bei den Herstellern von Software. Also die Frage, inwieweit können sich die Anbieter durch AGB's freizeichnen von einer solchen Haftung. Da könnte man ansetzen und sagen: Bestimmte Standards dürfen nicht unterschritten werden. Wenn die unterschritten werden, dann kann man sich auch per AGB nicht von der Haftung befreien. Und ich glaube, da hätte man einen Ansatz, den Stand der Technik auch AGB-fest zu machen und vielleicht einen zusätzlichen Anreiz zu geben. Letzter Punkt zu diesen weiteren Punkten: Die Meldepflichten für weitere Behörden habe ich schon erwähnt. Es gibt natürlich auch noch sonstige Anbieter von nicht-kritischen Infrastrukturen, die möglicherweise einbezogen werden könnten, also Stichwort Industriespionage. Die Frage nach den Kriterien für die Netzwerkknoten würde ich gern weitergeben an Herrn Neumann, weil das keine rechtliche Frage ist. Zur Rolle des BSI: Ich habe schon auf die Problematik der Sensibilität der Informationen hingewiesen, die die Behörde hier sammeln wird, und zwar gerade aus der Industrie. Das sind sensible Informationen, die der Wirtschaft wehtun könnten, wenn sie weitergegeben werden. Ich glaube, dass man da aufpassen muss in der Zusammenarbeit des BSI mit anderen Behörden. Ich glaube nicht, dass man so weit gehen muss, das BSI sowie die Bundesdatenschutzbeauftragte komplett unabhängig zu stellen. Ich würde allerdings schon nochmal genauer hinsehen, inwieweit man mit interner Differenzierung, also der Unterscheidung zwischen unterschiedlichen Abteilungen in diesem Haus, tatsächlich effektiv sein kann. Wenn es tatsächlich am Ende so ist, dass die eine Abteilung die IT-Sicherheit des sogenannten Bundestrojaners prüft und die andere Abteilung Abwehrmaßnahmen für Endgeräte des Nutzes programmiert, die solche Bundestrojaner abwehren sollen und die beiden Abteilungen gehen hinterher miteinander Kaffee trinken, dann ist das natürlich ein Problem oder kann jedenfalls ein Problem sein. Letzter Punkt zu Europa: Wenn der Zeitplan so aussieht, was sich meiner Kenntnis entzieht, dass wir nur noch einige Wochen auf die Richtlinie warten müssen, würde ich Ihnen sofort raten abzuwarten. Ich glaube, dann macht es keinen Sinn, das Gesetz hier zu verabschieden. Das heißt, ich würde das eng verzahnen, was das weitere europäische Gesetzgebungsverfahren angeht. Ich würde aber auch unterscheiden. Viel von dem, was ich angemahnt habe, also Befugnisse des BSI, Erweiterung der Berichtspflichten auf den Staat, könnte man auch nachträglich machen. Was man nicht machen sollte, ist, jetzt Prozesse vorzugeben für die Unternehmen, die sie dann nachher teuer ändern müssen. Was also nicht sein kann ist, dass die Industrie jetzt Sachen einführen muss und dann nach Verabschiedung der Richtlinien hinterher wieder ändern muss. Wenn das droht, dann sollte man tatsächlich besser abwarten, was aus Brüssel kommt. Vielen Dank.

Vors. **Wolfgang Bosbach** (CDU/CSU): Herr Neumann, bitte.

SV **Linus Neumann** (Chaos Computer Club (CCC), Berlin): Vielen Dank für die Frage. Vielleicht müssen wir uns noch einmal darüber im Klaren werden, was so ein durchschnittliches IT-System eines großen Unternehmens ist. Das ist nicht irgendein Gerät, was man da hinstellt, einschaltet und Updates macht. Das sind riesige, komplexe Infrastrukturen von einer Komplexität, die so groß ist, dass ich bisher noch keine einzige gesehen habe, wenn einfach nur die Firewalls konfiguriert war. Deswegen steht man als Sicherheitsverantwortlicher vor einem sehr großen Problem, dieser ganzen Geschichte irgendwie Herr zu werden. Für die Herangehensweise, die sich durchgesetzt hat, gibt es gute Gründe. Wenn man sich einfach mal so eine Unternehmensstruktur anschaut, ist, dass einfach mit allen möglichen Checklisten zu erschlagen. Es ist nicht so, als gäbe es keine Sicherheitsvorschriften für jeden einzelnen Rechner, der in irgendeinem größeren deutschen Unternehmen steht. Da gibt es seitenweise – da können Sie sich ein paar Festmeter ins Regal stellen an Checklisten, wo draufsteht, was alles gemacht werden muss zur Sicherheit. Es betrifft nur immer wieder genau den Teil der Sicherheit, den der Angreifer ohnehin schon kennt, der für ihn gegeben ist und um den er eben herumspielt. Auf der einen Seite steht ein Unternehmen mit einer unglaublich komplexen Infrastruktur und ein paar Festmetern Checklisten, wo überall abgehakt wird: Hier haben wir gemacht, hier haben wir gemacht, hier haben wir gemacht … und auf der anderen Seiten steht ein sehr agiler Angreifer, der sich um die gesamte Bürokratie nicht zu scheren braucht. Der schaut einfach nur: Funktioniert das? Nein. Funktioniert das? Nein. Funktioniert das? Nein. Probieren wir es mal so. Zack! Das ist einfach ein Ungleichgewicht, so ein David-Goliath-Ungleichgewicht, was man da einfach hat und was auch dazu führt, dass sich das Problem der IT-Sicherheit in naher Zukunft wahrscheinlich nicht endgültig lösen lassen wird. Jetzt kann man natürlich sagen: Wenn jemandem im Open-Source-Projekt ein Programmierfehler unterläuft, dann ist das nicht Stand der Technik. Wenn alle dieses Open-Source-Projekte nutzen, wenn es einfach gar keine Alternative dazu gibt – das war übrigens der Punkt, den ich angesprochen habe – niemand, der Unternehmen, die das genutzt haben, der irgendwie nennenswert rein investiert hat - das ist genau der Punkt, den ich hier ansprechen wollte - ein Audit hätte und letztendlich hat, hätte diesen Programmierfehler gefunden. Was hier eine Optimierungsdimension ist, ist eindeutig nur, wie lange hat es gedauert. Da würde ich sagen: Genau dieses konkret besser machen, schnell konkret besser machen, auditieren, prüfen, schnellere Zyklen ermöglichen, Sicherheitslücken loswerden, genau das ist IT-Sicherheit. Darauf müsste so ein Gesetz hinarbeiten, hinwirken, dafür Anreize schaffen. Stattdessen sagen wir jetzt: O.k., wir das Problem der IT-Sicherheit mit noch mehr Bürokratie. Diese Bürokratie, die kostet. Die kostet Ressourcen, die kostet Zeitaufwand. Die führt auch dazu, dass immer weniger Menschen Lust haben, sich wirklich in einem Unternehmen in der IT-Sicherheit zu engagieren, sondern lieber auf eine Beraterposition gehen oder als Penetration-Tester arbeiten, wo sie wirklich im Graben Sicherheitslücken finden und dafür sorgen, dass diese dann verschwinden, weil sich jetzt Forscher engagieren. Ich denke, wenn wir diesen Bürokratieaufwand hier erhöhen, dann geht das einfach zu Lasten pro aktiver Maßnahmen. Das ist ganz klar, wir können nicht erwarten, dass wir jetzt irgendwie vorschreiben: Erhöht die Bürokratie in eurem ganzen Unterfangen, weil ihr nicht genug Papier und Checklisten habt, und davon ausgehen, dass dann zusätzlich auch noch in Sicherheit investiert wird. Konkrete Punkte, die ich mir wünschen würde, wären ganz einfach. Führen wir eine Haftung bei Fahrlässigkeit ein. Klar, es gibt immer irgendeinen Haftungsausschluss. Für einen Betreiber einer kritischen Infrastruktur, wenn er nachweislich nichts dafür kann, dann wird er im Zweifelsfall auch nicht dafür haften müssen. Häufig kann man aber was dafür. Man könnte sich zum Beispiel auch über Fragen der Fahrlässigkeit Gedanken machen in dem Beseitigen von Sicherheitslücken. Ist eine Sicherheitslücke bekannt geworden, wie lange hat denn derjenige gebraucht, um sie komplett aus seinem System heraus zu radieren. Da ist ein Kunde zum Opfer gefallen einer Sicherheitslücke, die irgendwie viele Jahre bekannt ist und die zum Beispiel in einem BSI-Audit vor zwei Jahren schon mal angemerkt wurde. Da kann man doch mal langsam über Haftung reden. Ist doch jetzt wirklich nicht

zu viel verlangt. Das ist der Punkt, den ich eingangs schon kritisiert habe. Mich würde eine konkrete Erhöhung der Schutzziele interessieren. Stand der Technik halte ich für nicht ausreichend. Wenn wir sagen, wir wollen nicht so weitermachen wie bisher. Wenn wir sagen, wir sind mit der Ist-Situation unzufrieden, obwohl wir so viele Festmeter Holz in den Regalen stehen haben an Sicherheitskonzepten. Da müssen wir doch umdenken. Da müssen wir doch sagen: O.K. jetzt machen wir konkrete revolutionäre Vorgaben und sagen: So, alle Kommunikation, die 2017 noch von irgendeinem E-Mail-Anbieter in Deutschland angeboten wird, ist ernst zu nehmen verschlüsselt. Hört mir auf mit diesem Pippifax. Da haben Sie die Möglichkeit, so etwas vorzuschreiben. Sie freuen sich immer über Standortvorteile. Das wäre mal einer. Auch diesem Software-Siegel „Made in Germany“ dann auch wirklich zu einem Glanz zu verhelfen. Da haben wir in den letzten Jahren noch nicht so den Ruf, den wir in anderen Industriebereichen haben. Das heißt wirklich, konkrete Schutzziele und Prävention vorgeben und diese auch einfach verbindlich umsetzen lassen. Super Sache. Und dann natürlich – das ist ein Teil, auf dem ich jetzt ausreichend herumgeritten bin – Grundlagen zu schaffen für die gesamte deutsche Wirtschaft durch Audits, durch Penetration-Tests, einfach mal Grundlagen, Basisbausteine der IT-Sicherheit wirklich einmal in einer vernünftigen Qualität zur Verfügung stellen. Herr Schiller hat jetzt gerade selber gesagt, dass die SSL-Lösung, die weltweit mit 95 Prozent Verbreitung findet, sei im Anspruch dem Stand der Technik nicht genügt. Da müssen wir was dran ändern. Aber das können wir nicht machen durch irgendwelche Bürokratisierung des Problems. Dann gab es noch eine Frage zu Netzwerkswitches, und ich muss leider sagen, dass ich die nicht ganz mitbekommen habe. Könnten Sie die noch mal wiederholen?

BE Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Die Frage ist eben, ob man an bestimmten hochrelevanten Punkten, wo IT-Infrastruktur zusammenläuft und – ich sage mal – auch wenn es im privaten Besitz ist, aber eben öffentliche Infrastruktur eigentlich ist, nicht bestimmte Qualitätsstandards richtig prüft. Also auf der Hardware und Software guckt, ob die und die Standards erfüllt sind. Manchmal muss man mehr machen, als einfach nur draufgucken, sondern auch reingucken.

SV **Linus Neumann** (Chaos Computer Club (CCC), Berlin): Das Problem gliedert sich in zwei Teilfelder: Es gibt in der Regel einmal die Sicherheit, zu der ein Produkt, welches ich kaufe, in der Lage ist, sie mir zu bieten. Und dann gibt es noch, wieviel ich davon wieder kaputtkonfiguriert habe als Betreiber. Das ist aber zum Beispiel ein Problem, dessen in vielen Bereichen sich das BSI auch annimmt und sagt: ok, wir haben jetzt irgendwie in unserem Grundschutz definiert, wenn wir eine Windows-Festplattenverschlüsselung benutzen, dann sollten Sie bitte folgenden Krypto-Algorithmus nutzen, und nicht den, der gerade eingestellt ist. Also solche Sachen sind durchaus sinnvoll. Man kann natürlich auch Anbieter gerade von Produkten im Rahmen einer Zertifizierung im Rahmen der Zulassung in kritischen Bereichen natürlich auch zu bestimmten Überprüfungen anhalten. Es scheint ja – ich gehe einfach nur von der Lage aus, was wir im Lagebericht 2014 sehen – da noch Luft nach oben zu geben. Das heißt, was wir im Moment an Kontrollmöglichkeiten haben, scheint irgendwie nicht zu greifen. Wir haben große, erfolgreiche Angriffe in der IT-Sicherheit, und irgendwie scheint sich sowas nicht ganz durchzusetzen. Ich denke, dass sich ein größerer Teil darauf zurückführen lässt, dass über Haftungsfragen da das Problembewusstsein eben nicht gegeben ist. Wenn ich im größeren Unternehmen für die IT-Sicherheit verantwortlich bin, dann habe ich mehr Probleme vor mir, als ich in der Lage bin, mit einem noch so großen Team anzugehen, und es werden täglich mehr. Man macht den Job wahrscheinlich gut, wenn man die Anzahl der Probleme verringert, weil sie auch jeden Tag neuen Angriffen ausgesetzt sind. Angreifer denken sich jeden Tag was Neues aus. Sie sind ja nie fertig. Deswegen ist es ja eine feste Position. Aber genau da würde ich mir eben wünschen, dass konkrete Anreize für die Verantwortlichen bestehen, in eine pro-aktive Richtung zu gehen. Ich hoffe, die Frage damit beantwortet zu haben.

Vors. **Wolfgang Bosbach** (CDU/CSU): Herr Prof. Roßnagel.

SV **Prof. Dr. Alexander Roßnagel** (Universität Kassel, Institut für Wirtschaftsrecht): Danke für die vier Fragen. Die erste Frage betrifft das

Thema, was man sich in einem IT-Sicherheitsgesetz noch alles wünschen würde oder was man da fordern würde. Ich würde gern mal darauf hinweisen, dass es nicht immer nur darum geht, die Wahrscheinlichkeit von Schäden oder die Wahrscheinlichkeit von Angriffen zu bekämpfen oder zu reduzieren, sondern dass man auch darüber nachdenken muss, ob man das Schadenspotential reduzieren kann. Also Abhängigkeiten, die dann sich fortpflanzen in andere Systeme, dass man da versucht, wo es möglich ist, Grenzen einzuziehen, abzuschotten, damit sich Schäden nicht einfach fortpflanzen. Ein zweiter Bereich, der ist schon angesprochen worden, wäre für mich die ganze Haftung. Da haben wir jetzt hier schon mehrfach drüber gesprochen. Hier kann man in dem vorhandenen Rahmen bleiben, aber man könnte die eine oder andere Präzisierung vornehmen. Also was sind berechtigte Sicherheitserwartungen von Nutzern? Was sind Sicherheitspflichten von Dienstleistungsanbietern? Was sind Sicherheitspflichten von Herstellern? Wenn die verletzt sind, wenn die fahrlässig oder vorsätzlich verletzt sind und wir Haftungsfragen regeln, dann könnte man da auch eine sichere Motivation bei den Adressaten hervorrufen, dass die Geld dadurch sparen, dass sie die Haftung vermeiden. Ein weiterer Punkt, an den ich noch erinnern wollte, wäre die Möglichkeit, dass die öffentliche Hand vorbildhaft vorangeht. Also beispielsweise bei der Vergabe von Aufträgen, wenn es möglich ist, nur zertifizierte Produkte zu nehmen, die schon mal überprüft worden sind. Das könnte bei dem einen oder anderen Hersteller Anreiz dafür schaffen, dass er sein eigenes Produkt zertifizieren lässt, um in diesem Markt öffentlicher Nachfrage reinzukommen. Also da gäbe es schon das eine oder andere, was man noch tun könnte. Ich fände es aber nicht klug, diesen Gesetzesansatz, über den wir jetzt reden, diesen Entwurf davon abhängig zu machen, dass diese Punkte auch noch mit aufgenommen werden, weil das die Diskussion wohl länger hinziehen würde. Das sollte hier meines Erachtens Schritt für Schritt vorangehen. Also jetzt diesen Gesetzentwurf mit den Verbesserungen, über die wir geredet haben, beschließen und dann das Thema nicht zur Seite legen, IT-Sicherheit, sondern das weiter verfolgen und dann die nächsten Schritte angehen.
Die zweite Frage war dann, welche Prüfschritte notwendig sind. Dazu kann ich als Jurist wenig sagen, was das Technische genau angeht, aber was man aus anderen Bereichen des Techniksicherheitsrechts übertragen kann, sind so Überlegungen, dass man hier jetzt in diesem Entwurf ein Mindestsicherheitsniveau für kritische Infrastrukturen schafft. Dieses Mindestniveau versucht eine Einheitlichkeit zu erreichen, wird damit aber nicht jedem Risiko gerecht. Man kann risikogerechter dann noch die eine oder andere Anforderung stellen, also vielleicht für dieses Mindestsicherheitsniveau ein ausreichendes Sicherheitskonzept zu entwerfen. Ob das richtig umgesetzt ist, wird dann vielleicht bei risikorelevanteren kritischen Infrastrukturen oder Teilen davon genauer untersucht. Man kann schauen, ob zertifizierte Software oder Hardware eingesetzt ist, man kann aber auch schauen, ob ein Sicherheitsmanagementsystem etabliert ist, und man kann schauen, ob das auf dem Papier als Konzept gut dasteht oder ob das da im Betrieb tatsächlich realisiert wird. Also da gibt es dann das eine oder andere, was man noch zusätzlich überprüfen kann. Das wäre für mich alles zugehörig zu dem Bereich Nachweis der Erfüllung der Sicherheitspflichten. Da kann man noch mal differenziert vorgehen nach der Größe des jeweiligen Risikos bei einem Ausfall.
Die Frage der Unabhängigkeit der Behörde wäre für mich eine zweitrangige Frage. Die erstrangige Frage wäre die, ob es Interessengegensätze gibt. Weil, nur wenn es Interessengegensätze gibt, stellt sich für mich dann die Frage des Mittels, wie ich den Interessengegensatz ausschließe, und da kann dann die Abhängigkeit oder Unabhängigkeit ein sinnvolles Mittel sein, drauf zu reagieren. Da muss man noch mal genau schauen, wo das BSI möglicherweise in Interessengegensätze reinkommt und dann bestimmte Sicherheitsinteressen nicht so verfolgen kann, wie es eigentlich notwendig ist. Da muss man schauen, was dafür die richtigen Mittel sind. Es könnte eine Verstärkung der Unabhängigkeit oder die Reduzierung der Abhängigkeit sein. Herr Hornung hat ja darauf hingewiesen, was es für Möglichkeiten gibt. Eine Möglichkeit wäre dann auch die Unabhängigkeit.
Der letzte Punkt betrifft die europäische Richtlinie. Da würde ich gern auf zwei Punkte hinweisen. Nach Artikel 2 dieser Richtlinie betreibt sie nur eine Mindestharmonisierung und legt ausdrücklich fest, dass die Mitgliedsstaaten nicht da-

ran gehindert werden, Bestimmungen zur Gewährleistung eines hören Sicherheitsniveaus zu erlassen oder aufrecht zu erhalten. Also von daher sind wir nicht davon abhängig, die Richtlinie jetzt eins zu eins umzusetzen, sondern können mitgliedsstaatspezifische Regelungen treffen, die nur dieses Mindestniveau nicht unterschreiten dürfen. Wo das Mindestniveau unterschritten würde, da haben wir ja darauf hingewiesen, beispielsweise bei der fehlenden Sanktionierung. Wenn wir das Mindestniveau überschreiten würden, wäre das unschädlich. Das tritt dann nicht außer Kraft oder es besteht dann kein Anwendungsvorrang für das europäische Recht an der Stelle, sondern man kann das dann weiter beibehalten. Die kritischen Infrastrukturen sind in der Richtlinie auch nicht präzise beschrieben. Und es steht ausdrücklich drin, dass das nur Beispiele sind, die erwähnt werden, so dass die Mitgliedstaaten auch an der Stelle die Möglichkeit haben, genauer zu bestimmen, was für sie kritische Infrastrukturen sind. Das muss in Luxemburg nicht das gleiche sein wie in der Bundesrepublik. Insofern kann man das abwarten und deswegen würde ich es nicht als notwendig ansehen, dass wir jetzt diesen Gesetzgebungsprozess aufhalten. Wir sollten im Detail schauen, wo wir unterhalb der Mindestharmonisierung liegen. Das müssen wir auf jeden Fall tun. Wenn wir drüber liegen, kann das ja auch ein Standortvorteil sein in der Konkurrenz zwischen den Mitgliedsstaaten.

Vors. **Wolfgang Bosbach** (CDU/CSU): Herr Präsident Hange wollte noch eine ergänzende Bemerkung machen, dann habe ich noch zwei Kollegen, die sich melden wollten. Da muss ich zur Wahrung der deutsch-albanischen Freundschaft, weil wir gleich noch ein Gespräch haben, mit Blick auf die Uhr bitten, dass alle Beteiligten sich doch auf das notwendige Maß an Informationen konzentrieren.

SV Präs. **Michael Hange** (Bundesamt für Sicherheit in der Informationstechnik): Nur eine Sachauskunft in Ergänzung zu dem, was Herr Neumann gesagt hat. Der § 7 befasst sich auch mit der Untersuchung gerade der Komponenten, die Sie angesprochen haben. Zu zentralen Komponenten, die untersucht werden können, wie router, switches, besteht die Möglichkeit sogar, die Ergebnisse zu veröffentlichen. Vorher muss aber der Hersteller um Stellungnahme gebeten werden.

Vors. **Wolfgang Bosbach** (CDU/CSU): Vielen Dank. Thomas!

Abg. **Thomas Jarzombek** (CDU/CSU): Nur ob das hilft, Herr Vorsitzender, da habe ich meine Zweifel. Man hört von router und Komponenten, dass da pro Woche 100.000 neue Zeilen Quellcode dazukommen und wer das alles immer evaluieren möchte, das halte ich für eine große Herausforderung. Ich habe wenige Fragen. Ich würde gerne auf das Thema der Endkunden zu sprechen kommen und Herrn Tschersich von der Deutschen Telekom ganz konkret fragen, wie Sie konkret vorgehen, wenn Kunden in ihrem Netz, sozusagen Virenschleuder als Teil eines Bot-Netzes unterwegs sind. Wir waren gerade mit einer Delegation in Korea und Japan. Dort gibt es auch IT-Sicherheitsgesetze. Man hat ein Verfahren, dass die infizierten Rechner zwangsumgeleitet werden, mindestens ein Mal am Tag auf eine Informationsseite auch mit Angeboten zur Reinigung. Würden Sie das für einen gangbaren Weg halten, insbesondere auch in der aktuellen Gesetzgebung. Meine zweite Frage geht an Herrn Hange als Präsident des BSI: Wir reden immer in diesem ganzen Kontext nicht nur über die Meldepflichten, sondern auch über die Hilfestellungen. Das ist aus meiner Sicht ein sehr wichtiger Punkt. Deshalb würde ich Sie gern einmal fragen: Erstens, wie die Reaktionszeiten des BSI geplant sind, denn Sie bekommen auch, was ich sehr gut finde, einen erheblichen Stellenzuwachs, das heißt, wie planen Sie die Reaktionszeit bei eingehenden Meldungen, um andere dann zu informieren. Und zum zweiten: Wie Sie Unternehmen unterstützen werden in Bezug auf persistente Angreifer, eine Thematik, die, glaube ich, gerade bei missionskritischeren Unternehmen der Fall ist, dass also Angreifer nicht nur über einen Weg und eine Kampagne reinkommen, sondern 30 verschiedene Hintertüren im Laufe der Zeit aufgebaut haben und wie wir Geschichten gehört haben, wo man für Monate Unternehmen abklemmen musste, um sie zu reinigen, wie da die Angebote des BSI sein werden und inwieweit das Gesetz an dieser Stelle hilft. Und der dritte Punkt: Ich würde einfach nochmal Frau Plöger exemplarisch nehmen, weil sie es auch so prononciert gesagt hat. Es gab ja verschiedentlich Kritik, dass diese Formulierung „Stand der Technik“ nicht differenziert genug sei. Auch alle anderen, die sich berufen fühlen, können es auch gerne mal schriftlich zukommen lassen, wie der konkrete

Alternativvorschlag sein soll. Das würde ich im Übrigen vielleicht auch Prof. Hornung noch mit auf den Weg geben, denn er hat ja dann auch vorgeschlagen, da müsste man noch einführen, erhebliche Sicherheitsvorfälle, was jetzt auch wieder ein unbestimmter Rechtsbegriff ist, wie Sie das unterscheiden wollen, die erheblichen Sicherheitsvorfälle von den – wie auch immer geartet – anders skalierten Sicherheitsvorfällen.

Vors. **Wolfgang Bosbach** (CDU/CSU): Das lag mir auch auf dem Herzen. Wir versuchen es zu vermeiden, aber wir können in der Gesetzgebung nicht komplett auf unbestimmte Rechtsbegriffe verzichten. Das geht nicht. Die Formulierung „Stand der Technik“ ist ja nicht neu erfunden worden im IT-Sicherheitsgesetz, sondern sie ist auch ein eingeführter Rechtsbegriff, der auch materiell eine Dynamik ausstrahlen soll, weil sich der Stand der Technik ja ändert. Deswegen dient ja auch die Sachverständigenanhörung dazu, Optimierungen herzustellen. Also wenn ein Sachverständiger sagt: Ich würde das aber anders formulieren, würde man auch uns damit helfen, wenn es denn eine bessere Formulierung gibt, die das eher konkretisiert, was dem Gesetzgebungsziel dienen kann. Herr Prof. Hornung.

SV **Prof. Dr. Gerrit Hornung** (Universität Passau, Lehrstuhl für öffentliches Recht, IT-Recht und Rechtsinformatik): Vielleicht ganz kurz und knapp dazu: „Stand der Technik“ ist ein unbestimmter Rechtsbegriff und ich glaube, wir kommen ohne unbestimmte Rechtsbegriffe hier nicht aus. Meine Kritik bezog sich mehr darauf, dass dieser Stand der Technik nicht einzuhalten ist, sondern nur zu berücksichtigen ist. Und ich glaube, dann haben wir ein doppeltes Maß an Rechtsunsicherheit für die Unternehmen, was, glaube ich, keine gute Idee ist. Was wir brauchen, ist jemand, der entscheidet, was Stand der Technik ist. Das muss nicht der Gesetzgeber sein, sondern das kann im Verordnungsweg passieren. Aber das ist eine dynamische Geschichte, und auch diese Dynamik fehlt in dem Gesetzentwurf, also die Pflege und Weiterentwicklung dieser Standards, die aus meiner Sicht essentiell ist.

Vors. **Wolfgang Bosbach** (CDU/CSU): Frau Plöger, Sie waren auch angesprochen.

SV **Iris Plöger** (Bundesverband der Deutschen Industrie e.V., Leiterin der Abteilung Digitalisierung): Vielen Dank für die Frage. Natürlich kann ich die Definition nicht aus dem Handgelenk schütteln, aber ich freue mich, dass ich auf den Begriff „Stand der Technik“ wieder stoße, weil ich viele Jahre die Gelegenheit hatte, mich mit dem Patentrecht auseinanderzusetzen und in diesem Zusammenhang auch mit der Debatte um computerimplementierte Erfindungen. Da geht es ja auch um den Stand der Technik. Wenn ich da jetzt einfach mal den Transfer wage, würde ich auch sagen, da hat sich die Industrie in dem Bereich immer sehr zurückhaltend geäußert, das in einem Gesetz zu definieren, weil der Stand der Technik sich sozusagen ändert. Wir haben heute sehr viele gute Beispiele dazu gehört, dass es sehr schwierig ist, auch die Frage, pendele ich mich auf ein Mindestniveau ein, oder auf einem sehr hohen Niveau und wieviele Unternehmen aus der Branche können das dann jeweils überhaupt erreichen? Ich nehme das gerne noch einmal als Anregung mit. Wenn wir dann eine Möglichkeit sehen, das zu definieren, dann werde ich das gern noch einmal schriftlich hinterlegen. Danke.

Vors. **Wolfgang Bosbach** (CDU/CSU): Herr Tschersich, Sie waren auch gefragt. Danach noch Herr Hange.

SV **Dipl. Ing. (FH) Thomas Tschersich** (Deutsche Telekom AG, Leiter Group Security Services): Vielen Dank für die Frage. Die Thematik und ich glaube, das kommt mir ein bisschen zu kurz auch in der bisherigen Debatte, ist ja, dass heute Endkunden massenhaft Opfer von Angriffen werden. Zumeist weil sie schlecht gesicherte IT-Systeme haben, das gilt übrigens auch für viele Unternehmen und da sind es oftmals eben lange bekannte Sicherheitslücken. Also da sind viele Endkunden, die haben zum Beispiel seit zehn Jahren kein Software-Update eingespielt. Das ist der „never touch a running system“Ansatz und führt dazu, dass man dann Opfer wird und ich glaube auch, insofern ist auch das Thema Meldepflicht noch einmal genau in diesem Kontext zu sehen und hat positive Aspekte. Sie hatten gefragt, wie machen wir das konkret bei der Deutschen Telekom. Heute ist es so, dass wir monatlich ca. 100.000 – das pendelt, mal sind es ein paar mehr, mal ein paar weniger – Endkunden anschreiben. Das macht das sogenannte Abuse-Team. Das heißt, bei

uns gehen Hinweise ein von anderen Betreibern, die sagen, wir werden von folgender IP-Adresse bei Euch angegriffen, bitte stellt das ab. Wir sind dann in der Lage, aufgrund der für 7 Tage gespeicherten Zuordnung von IP-Adressen die dahinter liegenden Kunden zu identifizieren und können den Kunden dann anschreiben. Zumeist auf dem elektronischen Weg, mitunter aber auch, wenn wir wiederholt von Kunden keine Reaktion bekommen per Briefpost. Wir stellen dabei fest, dass das einen enorm positiven Effekt hat, weil sehr viele Kunden unsere Hotline anrufen und fragen: Was kann ich denn jetzt konkret tun? Das bedeutet, dass die Kunden das Thema sehr ernst nehmen und dass es sich um ein sehr wirkungsvolles Instrumentarium handelt. Das Problem ist nur, dass wir solche Informationen nicht durch eigene Auswertung erlangen dürfen, also dazu keine quasi Sensorik im Netz aufbauen können, die dann dazu führen würde, z.B. SPAM-Versender zu erkennen und diese in einen sogenannten Walled Garden umzuleiten. Das ist das, was Sie beschrieben hatten, was in Taiwan war, glaube ich, umgesetzt ist, wo man den Kunden auf eine Zwangsseite bringt und sagte: Du bist virenverseucht, folgendes kannst du tun. Klicke bitte hier, wenn du dann weiter ins Internet hineingehen möchtest. Das dürfen wir heute schlicht und ergreifend nicht machen und sind daher darauf angewiesen, dass wir Meldungen von Dritten bekommen, die dann weitergeben können. Das Gesetz will genau hier in eine Richtung gehen, dass wir solche Daten dafür nutzen dürfen, um Kunden informieren zu können. Ich halte das für einen sachdienlichen und richtigen Weg, möchte aber auch unterstreichen, dass, das, was Herr Neumann gesagt hat, natürlich von entscheidender Bedeutung ist. Wir müssen aufpassen, dass wir am Ende keine Datenfriedhöfe produzieren, sondern, uns bei der Speicherung und Verarbeitung auf das sinnvolle und notwendige Maß an Informationen beschränken.

Vors. **Wolfgang Bosbach** (CDU/CSU): Herr Hange.

SV Präs. **Michael Hange** (Bundesamt für Sicherheit in der Informationstechnik): Es waren zwei Fragen. Erst einmal: Wie geht das BSI mit Meldungen um. Und ich würde es auch auf sicherheitsvorfälle erweitern. Also schon durch unsere jetzigen gesetzlichen Aufgaben – Schutz der Regierungsnetze und der Bundesbehörden – haben wir Prozesse etabliert, das heißt also wie die Dinge laufen. Und ich halte es für ganz wichtig, wenn wir jetzt über die Verordnung reden, dass wir mit den Branchen einzeln auch diese Prozesse so transparent machen, dass jeder weiß, woran er ist. Natürlich abhängig von Vorfällen muss man sagen, ein Sicherheitsvorfall hat länger gedauert als ein einfacher Angriff. Das kann man nicht zeitlich genau definieren, aber dass die Prozesse transparent sind. Der zweite Punkt betrifft Unterstützung Kritischer Infrastrukturen: Es gibt unter § 3 einen neuen Absatz, da heißt es: Das Bundesamt kann Betreiber Kritischer Infrastrukturen auf deren Ersuchen bei der Sicherung ihrer Informationstechnik beraten, unterstützen oder auf qualifizierte Sicherheitsdienstleister verweisen. Also es gibt diese Möglichkeit, dass wir auch unter dem Subsidiaritätsgebot dagegen handeln. Was ich für ganz wichtig halte ist, dass wir IT-Sicherheitsdienstleister in Deutschland auch zertifizieren, so dass Wirtschaft auch Wirtschaft helfen kann. Aber für eine Ersthilfe steht das BSI schon immer zur Verfügung.

Vors. **Wolfgang Bosbach** (CDU/CSU): So. Vielen Dank. Herr Kollege Hakverdi, Sie können als letzter der Kollegen der heutigen Veranstaltung noch einen materiellen und rhetorischen Glanz verleihen.

Abg. **Metin Hakverdi** (SPD): Danke, Herr Vorsitzender. Das versuche ich erst gar nicht. Ich habe eine Frage an Prof. Roßnagel zu § 100. Herr Neumann hatte gesagt – wenn ich Sie richtig verstanden habe – also Absatz 1 brauchen Sie gar nicht. Den befanden Sie als nicht erforderlich. So haben Sie eben wörtlich gesagt. Haben Sie noch einmal eine Formulierungshilfe für mich, wie man diesen Teil des Gesetzes verfassungskonform und europarechtskonform formulieren müsste.

Vors. **Wolfgang Bosbach** (CDU/CSU): Ja, direkt dazu. Oder hatten Sie noch eine zweite Frage?

SV **Prof. Dr. Alexander Roßnagel** (Universität Kassel, Institut für Wirtschaftsrecht): Also keine ausformulierte Gesetzesbeschreibung. Was gemacht werden müsste, damit der § 100 verfassungskonform ist, ist zum ersten…

Vors. **Wolfgang Bosbach** (CDU/CSU): Wäre vielleicht schön, wenn wir das Gesetz noch erwähnen könnten, TKG?

SV **Prof. Dr. Alexander Roßnagel** (Universität Kassel, Institut für Wirtschaftsrecht): Jawoll, § 100 Telekommunikationsgesetz. Also man müsste den zulässigen Anlass, zu dem diese Daten gespeichert werden dürfen, den müsste man genau beschreiben. Wir hatten das vorhin schon ganz kurz angesprochen, dass man hier stufenweise vorgehen könnte. Also im ersten Schritt den Verkehr beobachten auf Anomalien, ohne dass man personenbezogene Daten erfasst. Dann kann man dadurch den Anlass generieren. Wenn es dann Anomalien gibt in dem beobachteten Verkehr, dann kann man die sich näher anschauen und die könnte man im ersten Schritt auch so sich anschauen, dass sie noch anonym oder pseudonym sind, und wenn man entdeckt, dass hier jetzt jemand einen Angriff durchführt, dann protokolliert man natürlich das ganze Verfahren oder die ganze Umgebung, die dafür notwendig ist. Da bin ich jetzt zu wenig technisch informiert, was man da genau tun muss. Auf jeden Fall wäre es aber notwendig, hier stufenweise vorzugehen und im ersten Schritt keine flächendeckende und anlasslose Speicherung von personenbezogenen Daten vorzunehmen. Also es ist in meinen Augen sinnvoll, und es würde sowohl der EuGH als auch das Bundesverfassungsgericht akzeptieren, dass man hier Maßnahmen durchführt, die notwendig sind, um sich gegen Angriffe zu wehren und diese rechtzeitig zu entdecken. Der EuGH verlangt aber, dass man das Vorgehen, bezogen auf die Speicherung oder Verarbeitung personenbezogener Daten, auf das absolut Notwendige begrenzt. Und das kann man nur dadurch erreichen, dass man schrittweise vorgeht. Aber das wäre eine Möglichkeit, wie man das Ganze verfassungskonform machen muss. Dann haben wir gelernt aus der Vorratsdatenspeicherungsentscheidung des Bundesverfassungsgerichts, dass es bestimmte Berufe gibt, die darauf angewiesen sind, dass sie besondere Geheimnisse wahren: Ärzte – Patientengeheimnis, Rechtsanwälte – Mandantengeheimnis und so weiter und dass die dann von so etwas vielleicht auszunehmen sind. Also müsste man sich überlegen, ob man so etwas wie eine white list anlegt und dann bestimmte Anschlüsse davon ausnimmt, dass deren Daten überwacht werden. Und so kann man sich die Vorgaben, die das Bundesverfassungsgericht aufgestellt hat, detailliert betrachten und den § 100 TKG entsprechend modernisieren. Der würde vermutlich ein klein wenig länger werden, als er bisher ist. Aber man hätte mehr Kriterien zum Schutz der betroffenen Bürger als jetzt nur das einzige Wort „erforderlich“, das bisher die Grundrechte der Betroffenen schützt.

Abg. **Metin Hakverdi** (SPD): Eine Nachfrage, Herr Vorsitzender.

Vors. **Wolfgang Bosbach** (CDU/CSU): Ja, klar.

Abg. **Metin Hakverdi** (SPD): White list. Ist das technisch möglich, berufsbezogene Ausnahmen – ich weiß zufällig, dass es wahrscheinlich 140 oder 150.000 Anwälte in Deutschland gibt, wieviele Journalisten weiß ich nicht – also ist es technisch möglich, eine white list zu haben, sodass man diese auf jeder Stufe der anlasslosen oder anlassbezogenen Speicherung herausnehmen kann? Bisher habe ich das in der Debatte noch nicht gehört. Mir fehlt das mathematische Verständnis dafür, deswegen die Frage: Geht das? Kann man so eine Positiv-Liste technisch umsetzen?

Vors. **Wolfgang Bosbach** (CDU/CSU): Herr Tschersich.

SV **Dip. Ing. (FH) Thomas Tschersich** (Deutsche Telekom AG. Leiter Group Security Services): Technisch möglich ist sicherlich so gut wie alles. Aber ob das noch realistisch umsetzbar ist, das darf man durchaus in Frage stellen. Wegen der Vielzahl der Betroffenen einerseits und den heute verwendeten dynamischen Zuordnungen von IP-Adressen andererseits würden wir damit eine derart komplexe Maschinerie bauen müssen, ich glaube, das wäre ….

Vors. **Wolfgang Bosbach** (CDU/CSU): Es ändert sich ja jeden Tag die Liste.

SV **Dip. Ing. (FH) Thomas Tschersich** (Deutsche Telekom AG. Leiter Group Security Services): … nicht mehr angemessen bzw. überhaupt nicht umsetzbar.

Vors. **Wolfgang Bosbach** (CDU/CSU): Frau Plöger, meine Herren, ich darf mich herzlich bedanken, dass Sie heute Nachmittag zu uns gekommen sind, auch bei den Zuhörerinnen und Zuhörer für ihre Geduld, einen schönen Abend noch und eine gute Woche.

Schluss der Sitzung: 16.44 Uhr

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)278

Stellungnahme

des Gesamtverbandes der Deutschen Versicherungswirtschaft

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

- BT-Drs. 18/4096 -

Gesamtverband der Deutschen
Versicherungswirtschaft e. V.

Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Tel.: +49 30 2020-5000
Fax: +49 30 2020-6000

51, rue Montoyer
B - 1000 Brüssel
Tel.: +32 2 28247-30
Fax: +32 2 28247-39
ID-Nummer 6437280268-55

Ansprechpartner:
Dr. Axel Wehling,
Mitglied der Hauptgeschäftsführung

Fred Chiachiarella
Leiter Betriebswirtschaft / Informations-
technologie

E-Mail: a.wehling@gdv.de
f.chiachiarella@gdv.de

www.gdv.de

Inhaltsübersicht

Zusammenfassung

Für die Versicherungswirtschaft sind ein sicherer Rechtsrahmen und abgesicherte IT-Infrastrukturen von grundsätzlicher Bedeutung. Die technischen und rechtlichen Rahmenbedingungen müssen so weiterentwickelt werden, dass sie den wachsenden Ansprüchen von Bürgerinnen und Bürgern und damit auch Kunden, Behörden und Dienstleistern entsprechen. Der Verband begrüßt daher, dass die Bundesregierung mit dem vorgelegten Entwurf einen wichtigen Schritt in Richtung IT-Sicherheit und vor allem Rechtssicherheit gehen möchte.

Hervorzuheben ist insbesondere die Unterstreichung des kooperativen Ansatzes und die Stärkung der sogenannten Single Point of Contacts (SPOCs) der Branchen. Änderungen sollten noch im Bereich der Meldepflichten erfolgen. So sollten die Meldungen, die keine Nennung des betroffenen Betreibers erfordern, nicht pseudonymisiert, sondern anonymisiert und sicher über die SPOCs erfolgen.

Insbesondere muss sichergestellt werden, dass durch mögliche Spezialgesetzgebung keine dezentralen Meldestrukturen geschaffen werden, die die Möglichkeiten der schnellen und fachkundigen Analyse und unverzügliche Weiterleitung an das Bundesamt stark beeinträchtigen würden.

1. Einleitung

Der Gesamtverband der Deutschen Versicherungswirtschaft begrüßt die Schwerpunktsetzung auf IT-Sicherheit in der Digitalen Agenda und die Fortführung der Initiative der Bundesregierung, mit dem Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) nicht nur IT-Sicherheit, sondern vor allem auch Rechtssicherheit zu schaffen.

Die Versicherungswirtschaft ist einer der Wirtschaftszweige, der mit als erster die Digitalisierung aufgegriffen und vorangetrieben hat. Sie ist nicht nur Nutzer neuer Informations- und Kommunikationstechnologien, sondern auch Impulsgeber für Innovationen und für die Stärkung der Informationsgesellschaft. Die verantwortungsvolle Verarbeitung umfangreicher und oft sensibler Daten ist daher die Basis eines erfolgreichen Versicherungsgeschäfts, IT- und Datensicherheit sind für die Versicherungswirtschaft Kernanliegen.

Zum jetzt vorliegenden Regierungsentwurf (Stand: 17. Dezember 2014) möchten wir wie folgt Stellung nehmen:

2. Artikel 1: Änderung des BSI-Gesetzes

2.1. § 3 Abs. 1 BSIG

Das Bundesamt fördert die Sicherheit in der Informationstechnik. Hierzu nimmt es folgende Aufgaben wahr:
[…]

2. Sammlung und Auswertung von Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen und Zurverfügungstellung der gewonnenen Erkenntnisse für andere Stellen, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist, sowie für Dritte, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist;

[…]

15. Aufbau geeigneter Kommunikationsstrukturen zur Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung sowie Koordinierung der Zusammenarbeit zum Schutz der Sicherheit in der Informationstechnik Kritischer Infrastrukturen im Verbund mit der Privatwirtschaft;

16. Aufgaben als zentrale Stelle im Bereich der Sicherheit in der Informationstechnik im Hinblick auf die Zusammenarbeit mit den zuständigen Stellen im Ausland, unbeschadet besonderer Zuständigkeiten anderer Stellen;

17. Aufgaben nach den §§ 8a und 8b als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen.

Die hierdurch dem Bundesamt eingeräumte Möglichkeit, wichtige Informationen zu kritischen IT-Vorfällen auch an Dritte weitergeben zu können, wird generell begrüßt.

Hier bedarf es jedoch aus Sicht der Versicherungswirtschaft einer weiteren Konkretisierung der „Dritten", an die die vom BSI gewonnenen Erkenntnisse weitergegeben werden dürfen. Insbesondere ist nicht klar, wer im Sinne der Begründung zum „Bereich der Kritischen Infrastrukturen im weiteren Sinne" gehören soll. Das Gesetz dient ja gerade der Abgrenzung zwischen solchen Bereichen, die zu diesen Infrastrukturen gehören und anderen, bei denen das gerade nicht der Fall ist. Von einer dritten Kategorie ist im Gesetz nicht die Rede.

Bei der Weitergabe von Informationen, insbesondere an Dritte, ist weiterhin darauf zu achten, dass ein Rückschluss auf das möglicherweise betroffene Unternehmen und die Branche hierbei nicht möglich ist.

2.2. § 2 Abs. 10 BSIG i.V.m. § 10 Abs. 1 BSIG

§ 2 Abs. 10 BSIG
Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die

1. *den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und*
2. *von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.*

Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt.

§ 10 Abs. 1 BSIG
Das Bundesministerium des Innern bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für

Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit unter Festlegung der in den jeweiligen Sektoren im Hinblick auf § 2 Absatz 10 Satz 1 Nummer 2 wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrads, welche Einrichtungen, Anlagen oder Teile davon als Kritische Infrastrukturen im Sinne dieses Gesetzes gelten. Zugang zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, wird nicht gewährt."

Die Versicherungswirtschaft begrüßt auch in diesem Punkt den kooperativen Ansatz zur Feststellung derjenigen Dienstleistungen und Systeme, die Gegenstand des Gesetzes sein sollen. Die Beteiligung der betroffenen Betreiber bei der Konkretisierung der Kriterien für Kritische Infrastrukturen darf sich nicht auf die in § 10 Abs. 1 vorgesehen Anhörung beschränken. Erforderlich ist vielmehr die auch in der Begründung angesprochene konkrete Einbeziehung bei der Entwicklung einer branchenspezifischen Definition von Qualität und Quantität. Gerade mit Blick auf den immensen Aufwand, der für den Nachweis der angemessenen organisatorischen und technischen Vorkehrungen gemäß § 8a Abs. 1, 3 BSIG und die Meldepflichten nach § 8b Abs. 4 BSIG notwendig ist, ist eine Regulierung mit Augenmaß notwendig, die vor allem Rechtssicherheit schafft.[1]

2.3. § 8a Abs. 1, 3 BSIG

Absatz 1:
Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei ist der Stand der Technik zu berücksichtigen. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

Absatz 3:
Die Betreiber Kritischer Infrastrukturen haben mindestens alle zwei Jahre

[1] Siehe hierzu auch Punkt 2.7

die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Bei Sicherheitsmängeln kann das Bundesamt die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse und im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen.

Der Nachweis der Vorkehrungen aus Absatz 1 („angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse“) gemäß Absatz 3 ist so gefasst, dass den betroffenen Unternehmen der erforderliche Gestaltungsrahmen zur Verfügung steht und eine verantwortliche Umsetzung möglich ist.

Die Definition von „Sicherheitsaudits, Prüfungen oder Zertifizierungen“ (Absatz 3, Satz 2) sollte geschärft werden. Unklar ist, ob interne Sicherheitsaudits / Prüfungen durch entsprechend zertifizierte Mitarbeiter des jeweiligen Unternehmens (z. B. innerhalb der Revision) als Nachweis ausreichend sind oder ob es zwingend eines Nachweises durch Externe bedarf. Sofern eine gültige Zertifizierung nach einem anerkannten Standard vorhanden ist (z. B. ISO 27001), dürfen keine weiteren Audits notwendig sein. Des Weiteren ist nicht klar definiert, ob die gesamte IT-Infrastruktur der Unternehmen oder nur die Teile überprüft bzw. zertifiziert werden müssen, die zur Aufrechterhaltung der Funktionsfähigkeit notwendig sind.

Weiterhin wird in Absatz 3, Satz 4 festgeschrieben, dass bei der Entdeckung von jedweden Sicherheitsmängeln die Übermittlung der gesamten Prüfungsunterlagen zu erfolgen hat. Dies ist aus Sicht der Versicherungswirtschaft unverhältnismäßig und kontraproduktiv, da Ziel dieser Prüfungen ja gerade das Beheben etwaiger Schwachstellen und das Entdecken von Verbesserungspotenzial in der Systemsicherheit ist. Hier sollte die Meldung auf erhebliche Mängel, die zum Ausfall der informationstechnischen Systeme führen kann, beschränkt werden. Es scheint außerdem wenig zielführend, dass die zu meldenden Störungen nach § 8b Abs. 4 eine gewisse Schwelle überschreiten müssen, Prüfberichte aber bereits bei kleinsten Mängeln vollständig vorgelegt werden müssen. Eine dementsprechende Klarstellung sollte in den Gesetzestext mit aufgenommen

werden.

2.4. § 8a Abs. 2 BSIG

Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen. Das Bundesamt stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten. Die Feststellung erfolgt

> *1. im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe,*
> *2. im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde.*

Der Verband befürwortet explizit den hier festgeschriebenen kooperativen und verantwortlichen Ansatz, der bereits in den letzten Jahren aktiv im Umsetzungsplan KRITIS (UP KRITIS) − auch mit seinen Branchenarbeitskreisen als „etablierte Kooperationsplattform“[2] − erfolgreich installiert wurde. Als Grundlage für die branchenspezifischen Standards sollten hier bereits bestehende und anerkannte Standards (beispielsweise ISO 27001 oder BSI-Grundschutz) dienen, um eine Synchronisierung mit bereits existierenden Anforderungen zu erreichen und damit den administrativen und organisatorischen Aufwand für die Unternehmen so gering wie möglich zu halten. Der Verband wird sich in diesen Prozess konstruktiv und zielorientiert einbringen.

2.5. § 8b Abs. 4 BSIG

Betreiber Kritischer Infrastrukturen haben erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können oder bereits geführt haben, über die Kontaktstelle unverzüglich an das Bundesamt zu melden. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik und zur Branche des Betreibers enthalten. Die Nennung des Betrei-

[2] Regierungsentwurf zum IT-Sicherheitsgesetz vom 17. Dezember 2014, Gesetzesbegründung, S. 15, dritter Absatz

bers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat.

Der Verband begrüßt, dass mit „erheblichen Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit“ eine gegenüber dem Referentenentwurf deutlich verbesserte Definition gefunden wurde, die zusammen mit der höchstrichterlichen Rechtsprechung zu § 100 Abs. 1 TKG und den Klarstellungen in der Begründung zur Frage der Erheblichkeit eine rechtssichere Grundlage für das weitere Verfahren darstellen kann.

Der Verband befürwortet außerdem, dass die Meldepflicht weiterhin in mehreren Stufen erfolgen soll und dass „Die Nennung des Betreibers […] nur dann erforderlich [ist], wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat.“ Jedoch ist laut Gesetzesbegründung vorgesehen, dass diese Meldungen pseudonymisiert und nicht anonymisiert erfolgen soll. Wenn von einer Pseudonymisierung nicht abgewichen werden kann, muss durch ein geeignetes Verfahren sichergestellt werden, dass die Pseudoidentität von den Branchenansprechpartnern so gewählt wird, dass ein Rückschluss auf das meldende Unternehmen nicht möglich ist. Meldungen sollten dabei aber in den meisten Fällen anonym erfolgen, da vor allem ein nationales Lagebild erstellt werden soll.

Nach der Gesetzesbegründung sollen zur weiteren Konkretisierung der Meldepflicht „das BSI − unter Einbeziehung der Betreiber Kritischer Infrastrukturen und der ansonsten im Bereich der Sicherheitsvorsorge zuständigen Aufsichtsbehörden − Kriterien für meldungsrelevante Sicherheitsvorfälle aufstellen und entsprechend der jeweils aktuellen IT-Sicherheitslage weiterentwickeln.“[3] Eine Abstimmung mit den betroffenen Branchen erscheint insbesondere an dieser Stelle unerlässlich, da nur diese qualifiziert die Auswirkungen einer Beeinträchtigung oder eines Ausfalls beurteilen können.

2.6. § 8b Abs. 5 BSIG

Zusätzlich zu ihrer Kontaktstelle nach Absatz 3 können Betreiber Kritischer Infrastrukturen, die dem gleichen Sektor angehören, eine gemeinsame übergeordnete Ansprechstelle benennen. Wurde eine solche

[3] Regierungsentwurf zum IT-Sicherheitsgesetz vom 17. Dezember 2014, Gesetzesbegründung Seite 20, 2. Absatz

benannt, erfolgt der Informationsaustausch zwischen den Kontaktstellen und dem Bundesamt in der Regel über die gemeinsame Ansprechstelle.

Die durch diese Regelung vorgenommene Stärkung der sogenannten Single Point of Contacts (SPOCs), die neben den Kontaktstellen der Betreiber als übergeordnete Ansprechstelle benannt werden können, ist besonders positiv hervorzuheben. Dies wird zu einer verkürzten Kommunikation zwischen den Branchen und dem Bundesamt führen und damit insbesondere auch zu schnelleren Reaktionszeiten in Krisenfällen. Aber auch für kleine Versicherungsunternehmen, die von den Reglungen nicht betroffen sind, ist ein solcher Branchenansprechpartner als Bindeglied zu den zuständigen Behörden sinnvoll.

Bereits im Jahr 2010 wurde von der Versicherungswirtschaft das Krisenreaktionszentrum für IT-Sicherheit der deutschen Versicherungswirtschaft GmbH (LKRZV) gegründet. Es erfüllt bereits jetzt die Forderung der Bundesregierung, im IT-Krisenfall die Reaktions- und Kommunikationsfähigkeit innerhalb der Branche und mit den zuständigen Behörden sicherzustellen.

Dass die Regelkommunikation über die gemeinsame Ansprechstelle erfolgen soll, wird ausdrücklich begrüßt. Dafür ist es aus Sicht des Verbandes notwendig und bisher auch geübte Praxis, dass die SPOCs als gemeinsame Ansprechstelle den Inhalt der Meldungen kennen, um ggf. eine brancheninterne Betroffenheit, z. B. durch mehrere vergleichbare Warnmeldungen aus verschiedenen Unternehmen, schnell erkennen zu können und dem Bundesamt eine entsprechende Einschätzung mitzugeben. Damit werden die SPOCs in die Lage versetzt, branchenspezifische Warnungen an ihre Mitgliedsunternehmen zu verschicken, um unabhängig von der Analyse des Bundesamtes bereits im Vorfeld die IT-Sicherheit der Branche zu stärken.

2.7. § 8 c Abs. 1 BSIG

Die §§ 8a und 8b sind nicht anzuwenden auf Kleinstunternehmen im Sinne der Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36). Artikel 3 Absatz 4 der Empfehlung ist nicht anzuwenden.

Diese Regelung stellt sicher, dass insbesondere kleinere Unternehmen durch Administrationskosten und Kosten für den Nachweis der technischen und organisatorischen Vorkehrungen nach § 8a Abs. 1, 3 BSIG

nicht unverhältnismäßig belastet werden.[4] Auch diese Regelung wird daher ausdrücklich begrüßt. Schließlich ist festzustellen, dass auch die nicht betroffenen Versicherungsunternehmen selbstverständlich höchste Anforderungen an ihre IT-Sicherheit erfüllen.

Zu Rückversicherungen ist festzustellen, dass diese der Risikobewältigung einzelner Versicherungsunternehmen dienen und daher per se nicht als Kritische Infrastruktur eingestuft werden können. In der Versicherungsbranche sind nur Erstversicherungen als kritisch anzusehen, da nur diese im direkten Kontakt mit den Verbrauchern stehen. Dies gilt umso mehr, wenn die Rückversicherer keinen Hauptsitz in Deutschland haben.

2.8. § 8c Abs. 2, 3 BSIG

Absatz 2:
§ 8a ist nicht anzuwenden auf […]
4. sonstige Betreiber Kritischer Infrastrukturen, die auf Grund von Rechtsvorschriften Anforderungen erfüllen müssen, die mit den Anforderungen nach § 8a vergleichbar oder weitergehend sind.

Absatz 3:
§ 8b Absatz 3 bis 5 ist nicht anzuwenden auf […]
4. sonstige Betreiber Kritischer Infrastrukturen, die auf Grund von Rechtsvorschriften Anforderungen erfüllen müssen, die mit den Anforderungen nach § 8b Absatz 3 bis 5 vergleichbar oder weitergehend sind.

Nach den hier vorliegenden Normen besteht die Möglichkeit, Spezialregelungen zu schaffen, die das gesamte etablierte und gut funktionierende bidirektionale Warn- und Meldesystem zwischen dem Bundesamt und den SPOCs, das in den §§ 8a und 8b Abs. 3 bis 5 BSIG ausgeführt wird, aushebeln würde.

Der Verband hat bereits in seinen Stellungnahmen zu den Referentenentwürfen aus den Jahren 2013 und 2014 hervorgehoben, dass der Erhalt bewährter Warn- und Meldewege notwendig ist. Bei der Krisenkommunikation ist es essentiell, dass diese direkt, schnell und zielgerichtet zwischen Experten erfolgt. Gewonnene Erkenntnisse müssen gerade bei relevanten IT-Sicherheitsvorfällen schnellstmöglich ausgetauscht werden, um drohenden Schäden erfolgreich entgegenwirken zu können.

Die Versicherungswirtschaft verfügt mit dem LKRZV bereits über eine

[4] Siehe hierzu auch Punkt 2.1

sichere und bewährte zentrale Kommunikationsinfrastruktur mit dem Bundesamt. Hinzu kommt, dass das Bundesamt auch in der Vergangenheit immer wieder unter Beweis gestellt hat, dass es über die fachliche und technische Kompetenz verfügt, Meldungen schnell einzuordnen, die notwendigen Schritte zum Schutz aller Kritischen Infrastrukturen einzuleiten und gegebenenfalls den betroffenen Unternehmen und Branchen über die SPOCs Hilfe anzubieten.

Hier dezentrale Meldestrukturen für die Versicherungsunternehmen über die Aufsichtsbehörde BaFin (zum Bundesamt) einzuführen, würde nicht nur den Alarmierungsweg unnötig verlängern und damit den Schaden möglicherweise vergrößern, sondern auch verhindern, dass Sicherheitswarnungen branchenübergreifend und schnellstmöglich versandt werden können. Dem Anspruch des IT-Sicherheitsgesetzes, die IT-Sicherheitslage für ganz Deutschland zu verbessern, würde diese Regelung nicht gerecht werden.

Es würde außerdem dazu führen, dass die Aufsicht über die Kritischen Infrastrukturen in verschiedene Aufsichtsbereiche (bspw. Bundesamt für Verkehr oder Bundesamt für Ernährung und Landwirtschaft) zerfasert und damit einen erheblichen Bedeutungsverlust erleiden würde. Die Erstellung eines einheitlichen Lagebildes − die in § 8b Abs. 2 Nr. 3 BSIG als Aufgabe des Bundesamtes explizit genannt wurde − und schnelle Reaktionen, die allen Betreibern Kritischer Infrastrukturen zugutekommen würden, wären so praktisch unmöglich.

Der Verband plädiert daher weiterhin für die ersatzlose Streichung in beiden Absätzen ab „sowie“ („…sowie sonstige Betreiber Kritischer Infrastrukturen, die aufgrund von Rechtsvorschriften vergleichbare oder weitergehende Anforderungen ….“).

Alternativ besteht die Möglichkeit, dass Aufsichtsbehörden die Informationen über Vorfälle aus den entsprechenden Branchen über das Bundesamt erhalten. Das Bundesamt könnte somit die Rolle eines „Behörden-SPOC“ einnehmen, die ihm in § 8b Abs. 1 BSIG („zentrale Meldestelle für Betreiber Kritischer Infrastrukturen“) auch explizit eingeräumt wird. Durch dieses Verfahren könnte das Bundesamt außerdem gemeinsam mit den „Branchen-SPOCs“ zu einem effizienten und möglichst unbürokratischen Verfahren beitragen. So kann auch das Interesse der Betreiber Kritischer Infrastrukturen, einen einzigen und schnellen Warn- und Meldeweg zu einer kompetenten Behörde zu haben, in Einklang gebracht werden.

2.9. § 8d BSIG

Absatz 1:
Das Bundesamt kann Dritten auf Antrag Auskunft zu den im Rahmen von § 8a Absatz 2 und 3 erhaltenen Informationen sowie zu den Meldungen nach § 8b Absatz 4 nur erteilen, wenn schutzwürdigen Interessen des betroffenen Betreibers Kritischer Infrastrukturen dem nicht entgegenstehen und durch die Auskunft keine Beeinträchtigung wesentlicher Sicherheitsinteressen zu erwarten ist. Zugang zu personenbezogenen Daten wird nicht gewährt.

Absatz 2:
Zugang zu den Akten des Bundesamtes in Angelegenheiten nach den §§ 8a und 8b wird nur Verfahrensbeteiligten gewährt und dies nach Maßgabe von § 29 des Verwaltungsverfahrensgesetzes.

Diese Regelung ist als Lex Specialis zum Informationsfreiheitsgesetz (IFG) anzusehen. Bei dem hier beschriebenen Verfahren ist jedoch sicherzustellen, dass auch pseudonymisierte Meldungen nicht an einen beliebig großen Empfängerkreis gegeben werden dürfen. Die Erfahrung der letzten Jahre in der Anwendung des IFG hat gezeigt, dass nur eine normenklare und eindeutige Bestimmung einen hinreichenden Schutz von Betriebs- und Geschäftsgeheimnissen und eine interessengerechte Abwägung ermöglicht. Es ist mithin geboten, im Sinne der Rechtsklarheit und Rechtssicherheit sowohl für die verpflichteten Behörden als auch für die betroffenen Unternehmen eine Regelung zu finden, die nicht zu einer unverhältnismäßigen Ausweitung der Informationsweitergabe führen könnte. Dabei ist insbesondere zu bedenken, dass eine nicht hinreichend normenklare Regelung dem Schutzzweck des vorliegenden Gesetzentwurfs zuwider laufen kann, wenn hierdurch der Schutz der Betroffenen vor Angriffen in Frage gestellt wird. Hierbei ist auch zu bedenken, dass bereits weitgehende Meldepflichten auch gegenüber den Betroffenen im Falle des Datenabflusses nach Bundesdatenschutzgesetz (BDSG) bestehen.

Sollte es zu einer Herausgabe von Informationen gekommen sein, sind die Betroffenen unverzüglich darüber zu informieren. Eine dementsprechende Ergänzung muss in den Gesetzestext aufgenommen werden.

3. Kommentierung der Stellungnahme des Bundesrates 643/14

Im Folgenden wird auf die für die Versicherungswirtschaft wesentlichen Punkte aus der oben genannten Stellungnahme eingegangen.

Der Bundesrat begrüßt die Initiative der Bundesregierung und regt vor allem an, mehr Planungs- und Rechtssicherheit durch die Konkretisierung des Begriffs "erheblichen Störung" in § 8b Abs. 4 Satz 1 BSIG zu erreichen. Dieser Konkretisierungswunsch wird auch vom Verband geteilt und wurde bereits durch die Stellungnahme vom 9. Januar 2015 eingebracht.

3.1. Zu Nr. 5 der Stellungnahme

Weiterhin soll gemäß Nr. 5 der Stellungnahme in § 8b Abs. II Nr. 4c BSIG die Wörter "die zur Erfüllung ihrer Aufgaben erforderlichen" gestrichen und ans Ende (nach der Angabe "3") angefügt werden: ", insbesondere über Inhalte und Absender von Meldungen nach Absatz 4 mit möglichen Auswirkungen auf das jeweilig Land,".

Diese vorgeschlagene Streichung widerspricht der Gesetzeslogik. Eine Informationspflicht gegenüber den zuständigen Aufsichtsbehörden der Länder kann nicht über das hinausgehen, was zur Erfüllung ihrer Aufgaben zwingend notwendig ist. Hier gelten die gleichen strengen Maßstäbe wie für Bundesbehörden.

Zudem widerspricht die angeregte Ergänzung - und insbesondere die Nennung von Absendern - § 8b Abs. IV BSIG, wonach die Nennung der betroffenen Unternehmen eben nur erforderlich ist, „wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat.“ Dies ist daher schon aus systematischen Gründen abzulehnen.

3.2. Zu Nr. 7 der Stellungnahme

Laut Nr. 7 zu § 10 Abs. 1 Satz 1 BSIG soll das Wort "Wirtschaftsverbände" durch das Wort "Branchenverbände" ersetzt werden.

Eine konsequente Terminologie im Gesetzentwurf wird befürwortet. Unabhängig davon muss klar gestellt werden, dass nur die Verbände an dem Verfahren zur Schaffung der Rechtsverordnung beteiligt sein dürfen, die auch das Mandat der jeweiligen Branche dafür mitbringen.

Berlin, den 26. Februar 2015

ERLEBEN, WAS VERBINDET.

DEUTSCHE TELEKOM AG
Friedrich-Ebert-Allee 140, 53113 Bonn

Deutscher Bundestag Innenausschuss
Herrn Ministerialrat Dr. Heynckes
Leiter Sekretariat PA 4
Platz der Republik 1

11011 Berlin

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)284 A

REFERENZEN
ANSPRECHPARTNER Thomas Tschersich
TELEFONNUMMER 0228 181-75111
DATUM 27.03.2015
BETRIFFT Stellungnahme zum Referentenentwurf des Gesetzes zur „Erhöhung der Sicherheit informationstechnischer Systeme“ (ITSiG)

Sehr geehrter Herr Dr. Heynckes,

die weltweite Digitalisierung und Vernetzung bietet vielfältige Chancen für die Bewältigung der politischen, wirtschaftlichen und gesellschaftlichen Herausforderungen. Angesichts dieser wachsenden Bedeutung des Cyberraums und informationstechnischer Systeme, ist es wichtig, Risiken und Bedrohungen der Netz- und Informationssicherheit zu minimieren. Die Deutsche Telekom begrüßt daher ausdrücklich die vorliegende Initiative zur Verbesserung der Cybersicherheit. Für den Standort Deutschland und Europa ist eine kohärente Cybersicherheitspolitik unerlässlich. Mit Blick auf den baldigen Abschluss der Ressortabstimmungen möchten wir die Gelegenheit nutzen, auf folgende erfolgskritische Aspekte des Gesetzes hinzuweisen.

1. Einbeziehung von Hard- wie Softwareherstellern und sogenannten Over the top Playern

Für eine ganzheitliche Sicherheitsbetrachtung der Wertschöpfungskette der digitalen Welt ist es erforderlich, alle relevanten Marktteilnehmer bei der Umsetzung von Sicherheitsanforderungen zu berücksichtigen, die Produkte oder Dienste im Cyberraum anbieten. Dies betrifft alle Anbieter, bei denen ein Ausfall oder eine Beeinträchtigung ihres Dienstes mit dem Ausfall oder der Beeinträchtigung kritischer Infrastrukturen vergleichbar ist. Mit umfasst sein müssen daher auch Hardware- und Softwarehersteller sowie Internetdienste, die bisher ohne überzeugende sachliche Rechtfertigung nicht in der gebotenen Klarheit vom Anwendungsbereich des Gesetzes erfasst sind. Die Delegation dieser wichtigen Frage auf eine spätere Rechtsverordnung ist unzureichend. Erforderlich ist eine konkrete Nennung von Diensten und Herstellern im Gesetz, beispielsweise durch Einfügung eines § 2 Absatz 11 BSI Gesetz.
Das Ziel des Gesetzes, das Sicherheitsniveau in Gänze zu heben, kann schlicht nicht durch eine singuläre Verpflichtung einzelner Akteure im Cyberraum erfüllt werden, insbesondere nicht, wenn diese ausschließlich

DEUTSCHE TELEKOM AG
Hausanschrift: Friedrich-Ebert-Allee 140, 53113 Bonn
Postanschrift: 53262 Bonn
Telefon: 0228 181-0
Konto: Postbank Saarbrücken (BLZ 590 100 66), Kto.-Nr. 166 095 662 | IBAN: DE0959 0100 6601 6609 5662 | SWIFT-BIC: PBNKDEFF590
Aufsichtsrat: Prof. Dr. Ulrich Lehner (Vorsitzender) | Vorstand: Timotheus Höttges (Vorsitzender), Reinhard Clemens, Niek Jan van Damme, Thomas Dannenfeldt, Dr. Thomas Kremer, Claudia Nemat
Handelsregister: Amtsgericht Bonn HRB 6794, Sitz der Gesellschaft Bonn | Gläubiger-ID: DE06ZZZ00000077752

123 456 789 0GP

DATUM 27.03.2015
EMPFÄNGER Herrn Ministerialrat Dr. Heynckes

Telekommunikationsanbieter trifft. Denn die Verarbeitung von Daten findet regelmäßig bei den Diensteanbietern selbst statt (etwa den Cloud-Diensten, E-Mail-Diensten oder sozialen Netzwerken). Zudem erfolgen Angriffe auf die Telekommunikationsnetze in der Regel von außen, d.h. mittels manipulierter Hard- und/oder Software. Die Erkennung, Behebung und auch die Mitteilung von Störungen von Komponenten und Diensten ist schnellstmöglich und effektiv nur zu gewährleisten, wenn die genannten Hersteller und Diensteanbieter mit in den Verpflichtungskanon aufgenommen werden.
Im Falle etwaiger Sicherheitsrisiken, deren Beseitigung beispielweise ein Software-Update oder eine anderweitige Anpassung von Systemkonfigurationen voraussetzt, muss es in der Verantwortung der jeweiligen Anbieter liegen, die Schwachstelle unverzüglich zu beheben. Es wäre unbillig, den Telekommunikationsanbietern diese Obliegenheit aufzubürden, insbesondere weil sie in aller Regel auf die Unterstützung der Hard- und Softwarehersteller bzw. Diensteanbieter angewiesen sind. Unseres Erachtens ist der deutsche Gesetzgeber auch nicht daran gehindert, Regelungen für Hersteller und Diensteanbieter zu treffen, selbst wenn diese Hersteller und Diensteanbieter ihren Sitz nicht in Deutschland haben bzw. ihre Leistungen für deutsche Kunden aus dem Ausland erbringen.

2. Absenkung der Meldeschwellen nach § 109 Absatz 5 TKG

Nach der Neufassung des § 109 Abs. 5 TKG sollen zukünftig bereits solche Beeinträchtigungen der Netze und Dienste mitteilungspflichtig sein, die etwa zu Sicherheitsverletzungen und Störungen führen können. Für die Pflicht zur Mitteilung ist es unerheblich, wie wahrscheinlich der Eintritt des Ereignisses und wie wahrscheinlich der Eintritt daraus resultierender Beeinträchtigungen ist.

Nach der aktuellen Rechtslage muss die Störung bereits eingetreten sein, sich also bereits realisiert haben. Die derzeitige Meldepraxis hat sich bewährt. Eine Absenkung der Meldeschwelle ist weder erforderlich noch angemessen. Sie würde die Verwaltungstätigkeit der BNetzA und der Netzbetreiber massiv erhöhen, ohne aber einen signifikanten Mehrwert für die IT Sicherheit zu leisten.
Im Übrigen sehen wir keinen sachlichen Grund, die Möglichkeit anonymer Meldungen ausschließlich den Betreibern sonstiger kritischer Infrastrukturen einzuräumen. Wir schlagen daher vor, die Form der Meldungen für alle Betreiber kritischer Infrastrukturen hinsichtlich der Frage der anonymen Meldemöglichkeit einheitlich zu regeln.

3. Konkretisierung der Informationspflicht gegenüber Nutzern nach § 109a Abs. 4 TKG

Der § 109a Abs. 4 TKG führt neue Benachrichtigungspflichten des Diensteanbieters gegenüber Nutzern ein, wenn Störungen bekannt werden, die von dessen Datenverarbeitungssystemen ausgehen.
Auch an dieser Stelle ist der Diensteanbieter der falsche Regelungsadressat: Die skizzierte Benachrichtigung des Nutzers ist immer dann sinnvoll, wenn die Information geeignet ist, die Behebung von Störungen zu beschleunigen und/oder Schäden der Betroffenen vorzubeugen bzw. diese gering zu halten. Voraussetzung dazu ist, dass die Information aus erster Hand erfolgt und nicht über Dritte an die Betroffenen gelangt. Eine solche Vorgehensweise kostet unter Umständen wertvolle Zeit und birgt das Risiko von (Übertragungs) Fehlern bei der Information der Betroffenen. Störungen von Datenverarbeitungssystemen müssen daher den

DATUM 27.03.2015
EMPFÄNGER Herrn Ministerialrat Dr. Heynckes

Nutzern selbst bzw. von den Herstellern und Betreibern der Datenverarbeitungssysteme, also den Störern, gemeldet werden und nicht (jedenfalls nicht ausschließlich) von Diensteanbietern.
Unabhängig davon ist die Pflicht zur Information nicht hinreichend konkret gefasst. Nach der Entwurfsfassung ist jedwede Art von Störung zu melden, unabhängig davon, wie viele Nutzer sie betrifft und welche Auswirkungen und Schäden sie zur Folge haben kann. Danach wäre bereits jede auf einen Nutzer beschränkte mit geringem Schadenpotenzial versehene Störung meldepflichtig. Informationen dazu würden keinen Beitrag zur Erhöhung der IT Sicherheit leisten und wären in der Praxis aufgrund der Vielzahl solcher Störungen nicht handhabbar. Zudem genügt nach der Vorschrift jede Erkenntnisquelle und jede Störungsinformation zur Auslösung der Informationspflicht, unabhängig davon, ob die Information wirklich wahr ist und ob sie den Betroffenen zum Zeitpunkt der Störung hilfreich ist. Auch in diesen Punkten ist die Regelung mithin zu weit gefasst und die daraus folgenden Verpflichtungen in zahlreichen Anwendungsfällen nicht erforderlich und unangemessen.
Nach der Gesetzesbegründung ist eine individuelle Information der Nutzer nicht geschuldet, vielmehr genügen allgemeine Informationen zur Erfüllung der Informationspflicht. Dieser wichtige Punkt sollte explizit im Gesetzestext klargestellt werden.
Zudem möchten wir das Augenmerk des Gesetzgebers auf die Haftungsvorschriften der §§ 44 und 44a TKG lenken. Problematisch erweist sich hier der Umstand, dass Diensteanbieter bei fehlerhaften oder verspäteten Informationen einem Haftungsrisiko ausgesetzt sind. Dies erscheint unbillig, weil die Störungen gerade nicht in eigenen Systemen und Anwendungen des informierenden Diensteanbieters auftreten. Hier bedarf es einer Haftungsfreistellung des benachrichtigenden Diensteanbieters, der nicht selbst Störer im Rechtssinne ist.

Mit freundlichen Grüßen

ppa.
Thomas Tschersich
Leiter Group Security Services

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)284 B

UNIKASSEL VERSITÄT

Fachbereich Wirtschaftswissenschaften

Institut für Wirtschaftsrecht

Prof. Dr. Alexander Roßnagel

Universität Kassel
Nora-Platiel-Str. 5 • D - 34109 Kassel

An den Vorsitzenden des Innenausschusses
Des Deutschen Bundestags
Herrn Wolfgang Bosbach

Universität Kassel
Fachgebiet Öffentliches Recht,
insb. Umwelt- und Technikrecht
Nora-Platiel-Straße 5
34109 Kassel

a.rossnagel@uni-kassel.de
fon +49-561 804 3130
fax +49-561 804 3737

Sekretariat: Edith Weise
fon +49-561 804 2874

14. April 2015

Schriftliche Stellungnahme zur Sachverständigenanhörung am 20. April 2015 zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

Der Gesetzentwurf ist grundsätzlich zu begrüßen, da er das Ziel verfolgt, die „IT-Sicherheit von Unternehmen“ zu verbessern und den „Schutz der Bürgerinnen und Bürger im Internet“ zu verstärken. Mit ihm soll „eine signifikante Verbesserung der Sicherheit informationstechnischer Systeme in Deutschland“ erreicht werden. Die neuen Regelungen sollen dazu dienen, „den Schutz der Systeme im Hinblick auf die Schutzgüter der IT-Sicherheit (Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität) zu verbessern, um den aktuellen und zukünftigen Gefährdungen der IT-Sicherheit wirksam begegnen zu können“.[1]

Dieser Zielsetzung ist eine eminent hohe Bedeutung beizumessen, da Informationstechnik inzwischen alle Bereiche des gesellschaftlichen Lebens durchdringt. Insbesondere Kritische Infrastrukturen, deren Funktionieren für das gesellschaftliche Zusammenleben entscheidend ist, sind von der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der von ihnen genutzten Informationstechnik existenziell abhängig. Ihr Ausfall, ihre Manipulation oder ihre Beeinträchtigung könnte gravierende Schäden und Folgen in alle gesellschaftlichen Bereiche hervorrufen.[2] Daher ist es notwendig, dass alle Kritischen Infrastrukturen ein hohes und gleichmäßiges Niveau der IT-Sicherheit gewährleisten.

Um dieses Ziel zu erreichen, ist vorgesehenen, dass alle Betreiber Kritischer Infrastrukturen ein Mindestniveau an IT-Sicherheit einhalten und nachweisen sowie IT-Sicherheitsvorfälle an das BSI melden. Dieses wertet die Vorfälle aus und stellt seine Erkenntnisse den Betreibern zur Verfügung, damit diese ihre Infrastrukturen besser schützen können. Zusätzlich werden alle Anbieter von Telemedien und Telekommunikation zu entsprechenden Sicherheitsmaßnahmen verpflichtet. Die Telekommunikationsanbieter sollen zudem IT-Sicherheitsvorfälle, die zu einem unerlaubten Zugriff auf die Systeme der Nutzerinnen und Nutzer führen können, melden und betroffene Nutzerinnen und Nutzer über bekannte Störungen informieren.

---

1 BT-Drs. 18,/4096, 1.

2 S. hierzu bereits die Szenarien in Roßnagel/Wedde/Hammer/Pordesch, Die Verletzlichkeit der Informationsgesellschaft, Wiesbaden 1989.

Zu dem Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme sind die folgenden Bemerkungen angebracht:

1. „Sicherheit der Informationstechnik"

Die Aufgaben des BSI, deren Erfüllung durch diesen Entwurf unterstützt werden soll, beruhen auf der Schutzpflicht des Staates für die Verwirklichung der Grundrechte der Bürger und der staatlichen Verantwortung für das Funktionieren der Infrastrukturen, die für das gesellschaftliche Zusammenleben entscheidend sind. [3] Dies gilt nicht nur für den Schutz und die Förderung der Grundrechte auf freie Entfaltung der Persönlichkeit, Leben und körperliche Unversehrtheit und Freiheit der Fortbewegung, freie Berufsausübung und Schutz des Eigentums, sondern insbesondere auch auf Fernmeldegeheimnis, informationeller Selbstbestimmung sowie Vertraulichkeit und Integrität informationstechnischer Systeme.[4] Zwar hat der Staat einen großen Entscheidungsspielraum, wie er seine Schutzpflicht erfüllt. Dieser ist erst dann überschritten, wenn der Schutz ein Untermaß unterschreitet. Doch kann es bei der Verbesserung des BSIG nicht darum gehen, nur das absolute Mindestmaß an Bürgersicherheit zu erreichen. Vielmehr muss das Ziel sein, eine angemessene Bürgersicherheit zu gewährleisten, die der Bürger von einem um seine Sicherheit bemühten Staat erwarten kann. Bürger und Unternehmen sind von der (Un-)Sicherheit der IT und der Telekommunikation stark betroffen. Sie benötigen vor allem Informationen über IT-Risiken und Unterstützung bei Schutzmaßnahmen. Beides zu bieten, ist die vornehmste Aufgabe des BSI.

In diesem Sinn würde man in einem Gesetz, das den Titel trägt „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)" unter anderem Regelungen zu folgenden Themen der IT-Sicherheit erwarten:

- Sicherheitsanforderungen an Hersteller von Hardware und Software (Produktsicherheit),
- Nachbesserungspflichten von Herstellern von Hard- und Software,
- Sicherheitsanforderungen an IT-Dienstleister und IT-Dienstleistungen,
- Verringerung von Abhängigkeiten hinsichtlich einzelner IT-Systeme,
- Reduzierung von Schadenspotentialen,
- Haftung für Sicherheitsverletzungen von Herstellern (Produkthaftung, Produzentenhaftung, Schutzgesetze), Verkäufer von Hardware und Software (Gewährleistung, Fehlerbegriff, zugesicherte Eigenschaft, berechtigte Erwartung des Käufers) sowie Dienstleistern (Sicherheitspflichten und berechtigte Sicherheitserwartung der Nutzer),
- Instrumente, die Anreize für die Nutzer bieten, Maßnahmen zur IT-Sicherheit in ihren Geräten und Programmen zu nutzen
- Infrastrukturen für Dienstleister und Nutzer, die sie in die Lage versetzen, selbstbestimmt IT-Sicherheit für ihre Interessen herzustellen.
- Beratung und Unterstützung durch staatliche Institutionen, insbesondere durch das BSI, im Sinn von Bürger-Helpdesk für IT-Sicherheit

Der zu kommentierende Gesetzentwurf strebt jedoch nicht an, diese Themen zu bearbeiten, sondern beschränkt sich darauf, die IT-Sicherheit in Kritischen Infrastrukturen zu erhöhen. Dies ist schwer genug. Es

---

[3] S. hierzu bereits die Anmerkungen zum ersten BSIG in Roßnagel/Bizer/Hammer/Pordesch, Ein Bundesamt für die Sicherheit in der Informationstechnik - Kritische Bemerkungen zum Gesetzentwurf der Bundesregierung, DuD 1990, 178 ff. und Roßnagel/Bizer, Sicherheit in der Informationstechnik - Aufgabe für ein neues Bundesamt, Kritische Justiz, 1990, 436 ff.

[4] S. z.B. BVerfGE 38, 1; 49, 89; 57, 295; 73, 118; 90, 60; 114, 371; 119, 181.

wäre schon ein großer Fortschritt, wenn es gelingen würde, wenigsten die Kritischen Infrastrukturen sicherer zu machen und damit indirekt zugleich auch die Sicherheit aller Unternehmen und Bürger zu stärken. Allerdings sollte der Titel des Gesetzes dem Schwerpunkt der Regelungen angepasst werden und keinen Anspruch geltend machen, der nicht eingelöst werden kann.

2. Grundrechtseingriffe

Die vorgesehenen Regelungen sind Eingriffe in das Grundrecht der Betreiber Kritischer Infrastrukturen sowie der Anbieter von Telemediendiensten, der Betreiber von Telekommunikationsnetzen und der Anbieter von Telekommunikationsdiensten auf Ausübung ihrer Berufsfreiheit nach Art. 12 Abs. 1 GG. Ein Eingriff in die Berufsausübung ist auf gesetzlicher Grundlage zulässig, wenn „Gesichtspunkte der Zweckmäßigkeit" ihn verlangen, um Gefahren für andere Grundrechtsträger oder die Allgemeinheit auszuschließen.[5]

Der Schutz Kritischer Infrastrukturen ist von höchstem Allgemeininteresse. Sicherheitsvorkehrungen, um das gebotene Sicherheitsniveau zu gewährleisten, und ihr Nachweis sind ebenso dringende Maßnahmen zur Wahrung dieses Allgemeininteresses wie der Aufbau eines kooperativen Informationssystems für die informationstechnische Sicherheit in Kritischen Infrastrukturen. Der Betrieb Kritischer Infrastrukturen ohne ausreichende Sicherungsmaßnahmen und ohne eine ausreichende Kenntnis über die Sicherheits- und Bedrohungslage, wäre unsachgemäß und würde für alle gesellschaftlichen Bereiche große Gefahren hervorrufen. Daher sind die mit ihnen verbundenen Eingriffe in die Freiheit der Berufsausübung zum Schutz der Rechte Dritter und vor allem zur Sicherheit der Allgemeinheit geboten.

Die genannten Maßnahmen sind auch verhältnismäßig. Sie sind geeignet, um dem Ziel einer ausreichenden Sicherheit für Kritische Infrastrukturen deutlich näher zu kommen. Auf die im Entwurf vorgesehenen Maßnahmen kann nicht grundsätzlich zugunsten anderer, weniger eingreifender Maßnahmen verzichtet werden. Soweit branchenspezifische Standards besser passen, um die erforderliche Sicherheit zu gewährleisten, können diese nach § 8a Abs. 2 BSIG-E für verbindlich erklärt werden. Da der Entwurf auch viele Maßnahmen vorsieht, um die Belastung durch den Grundrechtseingriff gering zu halten, sind die neuen Pflichten auch angemessen. Hierfür ist zu berücksichtigen, dass

- Kleinstunternehmer nach § 8c Abs. 1 BSIG-E vom Anwendungsbereich der Sicherungs- und Meldepflichten ausgenommen sind,
- die Sicherheitsmaßnahmen nach § 8a Abs. 1 Satz 3 BSIG-E ausdrücklich „angemessen" sein müssen,
- für die Sicherheitsanforderungen nach § 8a Abs. 1 Satz 2 BSIG-E, § 13 Abs. 7 TMG und § 109 Abs. 2 TKG nur der Stand der Technik berücksichtigt werden muss und dieser in seiner Definition bereits das Verhältnismäßigkeitsprinzip integriert hat,
- Meldungen, die nicht tatsächliche Ausfälle oder Beeinträchtigungen betreffen, nach § 8b Abs. 4 Satz 3 BSIG-E gegenüber dem BSI anonym mitgeteilt werden können,
- ein hoher Schutz für die gemeldeten Informationen gewährt wird (z.B. nach § 8d BSIG-E).

Die mit dem Gesetzentwurf verbundenen Grundrechtseinschränkungen der freien Berufsausübung sind daher als gesetzliche Eingriffe, die dem Verhältnismäßigkeitsprinzip entsprechen mit Art. 12 Abs. 1 GG vereinbar. [6]

---

[5] S. z.B. BVerfGE 7, 377 (406).

[6] S. zu spezifischen Grundrechtsaspekten noch in den folgenden Ausführungen.

3. Definition Kritischer Infrastrukturen

Nach § 2 Abs. 10 BSIG-E werden Kritische Infrastrukturen sehr abstrakt umschrieben als „Einrichtungen, Anlagen oder Teile“ in Infrastrukturen, die 1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und 2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden“. In § 10 Abs. 1 Satz 1 BSIG-E wird das Bundesministerium ermächtigt, die Kritischen Infrastrukturen im Sinne dieses Gesetzes näher zu bestimmen. In der Begründung zu § 10 Abs. 1 Satz 1 BSIG-E wird näher ausgeführt, nach welcher Methode die Bestimmung erfolgen soll.

Der Gesetzestext ist jedoch erheblich weniger präzise als die Begründung. Es stellt sich deshalb die Frage, ob diese Verordnungsermächtigung entsprechend Art. 10 GG „Inhalt, Zweck und Ausmaß“ ausreichend bestimmt benennt. Dagegen spricht, dass die Adressaten des Gesetzes in diesem selbst nicht eindeutig benannt werden, obwohl das Gesetz für sie schwerwiegende Rechtsfolgen festlegt.[7]

Bei der Anwendung der rechtsstaatlichen und demokratieschützenden Vorgaben des Art. 80 Abs. 1 Satz 2 GG ist zu beachten, dass diese Vorschrift bezweckt, die Entscheidungshoheit des Bundestages zu wahren und die Vorhersehbarkeit der Verordnungsregelungen für die Betroffenen zu gewährleisten.[8] Zugleich ist aber auch die Eigenlogik, Komplexität und Dynamik des zu regelnden Bereiches zu beachten.[9] Hinsichtlich der rechtsstaatlichen Zielsetzung wird eine sehr genaue Bestimmung der betroffenen Adressaten nach eindeutigen Merkmalen notwendig. Es wird eine Beschreibung der Typen von Einrichtungen, Anlagen oder Teile in Infrastrukturen erforderlich sein, die qualitative und quantitative Merkmale enthält, die ausreichend unterscheidungsstark sind. Im Detaillierungsgrad, in der Darstellungsform und im Umfang[10] könnte die Aufstellung dem Katalog von immissionsschutzrechtlich genehmigungsbedürftigen Anlagen im Anhang zur Vierten Bundes-Immissionsschutzverordnung entsprechen. Ein solcher Detaillierungsgrad ist in einer gesetzlichen Definition jedoch nicht möglich.

Für den Katalog im Anhang zur Vierten Bundes-Immissionsschutzverordnung gilt die Ermächtigungsgrundlage in § 4 Abs. 1 Satz 1 BImSchG seit 1974 als ausreichend bestimmt. Nach dieser dürfen Anlagen als genehmigungsbedürftig in einer Rechtsverordnung festgelegt werden, die „auf Grund ihrer Beschaffenheit oder ihres Betriebs in besonderem Maße geeignet sind, schädliche Umwelteinwirkungen hervorzurufen oder in anderer Weise die Allgemeinheit oder die Nachbarschaft zu gefährden, erheblich zu benachteiligen oder erheblich zu belästigen“. Diesem Grad an Bestimmtheit genügen auch §§ 10 Abs. 1 Satz 1 i.V.m. § 2 Abs. 10 BSIG-E. Eine konkretere Bestimmung der Adressaten im Gesetz ist nicht notwendig. In Verbindung mit einer Rechtsverordnung, die das Präzisionsniveau der Vierten Bundes-Immissionsschutzverordnung erfüllt, ist dem rechtsstaatlichen Bestimmtheitsgebot Genüge getan.

---

7 S. hierzu z.B. Roos, Der neue Entwurf eines IT-Sicherheitsgesetzes, MMR 2014, 724f.; Roth, Neuer Referentenentwurf zum IT-Sicherheitsgesetz, ZD 2015, 19; kritisch ebenfalls Leisterer/Schneider, Der überarbeitete Entwurf für ein IT-Sicherheitsgesetz. Überblick und Problemfelder, CR 2014, 577; eine Konkretisierung des Betreiberbegriffs fordert Eckardt, Der Referenten-Entwurf zum IT-Sicherheitsgesetz – Schutz der digitalen Zukunft?, ZD 2014, 600.

8 S. z.B. BVerfGE 78, 249 (272); Pieroth, in: Jarass/Pieroth (Hrsg.), Grundgesetz-Kommentar, 12. Aufl. München 2012, Art. 80 Rn. 1.

9 S. z.B. BVerfGE 48, 210 (221); 76, 130 (143); 123, 39 (80).

10 Roth, (Fn. 7), ZD 2015, 19, erwartet eine „riesige Liste“.

Durch die Verordnungsermächtigung des § 10 Abs. 1 Satz 1 BSIG-E gibt zwar der Gesetzgeber einen großen Entscheidungsspielraum an das Bundesministerium des Innern ab. Es regelt aber wichtige Merkmale des Verfahrens, in dem die Adressaten des Gesetzes festgelegt werden. Das Bundesministerium des Innern soll den Spielraum nämlich nicht allein füllen. Vielmehr hat es zuvor Vertreter der Wissenschaft, der betroffenen Betreiber und der betroffenen Branchenverbände[11] anzuhören und danach die Einrichtungen, Anlagen oder Teile, die als Kritische Infrastrukturen gelten sollen, im Einvernehmen mit neun weiteren Bundesministerien festzulegen. Es ist nachvollziehbar, wenn die Bundesregierung ausführt, dass die Präzisierung des Begriffs der Kritischen Infrastrukturen „der sektor- und branchenspezifischen Einbeziehung aller betroffenen Kreise" bedarf und „nur in einem gemeinsamen Arbeitsprozess mit Vertretern … der Betreiber … und unter Einbeziehung der Expertise von externen Fachleuten erarbeitet werden" kann.[12]

Außerdem hat der Gesetzgeber die beiden Hauptkriterien, die diese Entscheidung leiten sollen, inhaltlich festgelegt. § 10 Abs. 1 Satz 1 BSIG-E bestimmt zum einen, dass die Kritischen Infrastrukturen im Sinne des Gesetzes den sieben Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören müssen. Zum anderen legt er fest, dass die Dienstleistungen im Hinblick auf ihre Bedeutung für das Funktionieren des Gemeinwesens[13] als kritisch und bezogen auf ihren Versorgungsgrads als bedeutend anzusehen sein müssen. Außerdem präzisiert er, zwar nicht im Gesetzestext, aber in seiner Begründung,[14] die Methode der Auswahl und gibt damit dem Bundesministerium des Innern sehr genaue Vorgaben.

Der Gesetzgeber legt nach dem Entwurf also sowohl Kriterien als auch Verfahren ausreichend bestimmt fest, so dass die Vorschrift mit Art. 80 Abs. 1 Satz 2 GG vereinbar ist.

4. Sicherheitsniveau für die Informationstechnik Kritischer Infrastrukturen

Der Entwurf bestimmt für die in der Verordnung nach § 10 Abs. 1 BSIG-E genannten Kritischen Infrastrukturen nach § 8a Abs. 1 Satz 1 BSIG-E, dass ihre Betreiber „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen" haben, „die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind".

a) Stand der Technik

Nach § 8a Abs. 1 Satz 2 BSIG-E, § 109 Abs. 2 TKG und § 13 Abs. 7 TMG wird bestimmt, dass bei der Gewährleistung des IT-Sicherheit „der Stand der Technik zu berücksichtigen" ist.

Eine Definition, was unter dem „Stand der Technik zu verstehen ist, findet sich in keiner der drei Vorschriften im Text. Dieser Begriff wird nur in der Begründung zu § 8a Abs. 1 Satz 2 BSIG-E definiert, in den Begründungen zu den beiden anderen Vorschriften nicht. Dagegen wird in vielen anderen Gesetzen dieser Begriff definiert und zwar jeweils – entsprechend dem Schutzgut oder der Zielsetzung des Gesetzes – leicht

---

11 S. hierzu die Stellungnahme der Bundesrates, BT-Drs. 18/4096, 81, und die zustimmende Gegenäußerung der Bundesregierung, BT-Drs. 18/4096, 88.

12 Gegenäußerung der Bundesregierung, BT-Drs. 18/4096, 84.

13 Diese wird nach § 2 Abs. 10 Satz 1 Nr. 2 BSIG-E dadurch bestimmt, dass durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

14 BT-Drs. 18/4096, 52 ff.

unterschiedlich.[15] Was unter dem Stand der Technik im Sinn des BSIG-E, im TMG-E und im TKG-E jeweils zu verstehen ist, sollte im Gesetzestext festgelegt werden.[16] Steht die Definition nur in der Begründung, nimmt sie nicht an der Wortlautauslegung teil, sondern kann höchstens im Rahmen der historischen Auslegung berücksichtigt werden.

Trotz Definition[17] bleibt unklar, was alles für den Stand der Technik berücksichtigt werden soll und auf was sich dieser Stand bezieht. Um in diesen Fragen Rechtssicherheit zu erreichen, wurde z.B. für § 3 Abs. 6 Satz 2 BImSchG ein Verweis aufgenommen, dass bei der Bestimmung des Standes der Technik insbesondere die in der Anlage zum Bundes-Immissionsschutzgesetz aufgeführten Kriterien zu berücksichtigen sind. Nach dieser Anlage sind bei der Bestimmung des Standes der Technik „unter Berücksichtigung der Verhältnismäßigkeit zwischen Aufwand und Nutzen möglicher Maßnahmen sowie des Grundsatzes der Vorsorge und der Vorbeugung, jeweils bezogen auf Anlagen einer bestimmten Art, insbesondere“ 13 im Folgenden genannte „Kriterien zu berücksichtigen“.[18] Eine solche Anlage, die der Gesetzgeber als Teil des Gesetzes formuliert, erhöht die Bestimmtheit der gesetzlichen Sicherheitspflichten und erleichtert die Gewährleistung und Prüfung der IT-Sicherheit.

Der Stand der Technik ist immer „unter Berücksichtigung der Verhältnismäßigkeit zwischen Aufwand und Nutzen möglicher Maßnahmen“ zu bestimmen. Er setzt voraus, dass die Maßnahme technisch möglich und für den durchschnittlichen Betreiber zumutbar ist. Wenn die Maßnahme „mit Erfolg im Betrieb erprobt“ sein muss, dann müssen Unternehmen die Maßnahme seit einer gewissen Zeit unter Berücksichtigung des Verhältnisses von Aufwand und Nutzen im regulären Betrieb nutzen. Mit der Vorgabe des Standes der Technik ist daher die Angemessenheit der Sicherheitsmaßnahme, insbesondere aber, dass sie technisch möglich und zumutbar ist, bereits gefordert. Die Forderung der Angemessenheit, der technischen Machbarkeit und der Zumutbarkeit sind somit überflüssig, wenn bereits der Stand der Technik gefordert wird. In § 13 Abs. 7 TMG-E, in § 109 Abs. 2 TKG-E und in § 8a Abs. 1 Satz 3 BSIG-E können die entsprechenden Passagen als unnötige Verdopplung des Gesetzestextes gestrichen werden.

Nach den Formulierungen in § 8a Abs. 1 Satz 2 BSIG-E, § 109 Abs. 2 TKG-E und § 13 Abs. 7 TMG-E ist der Stand der Technik nur zu „berücksichtigen“,[19] nicht jedoch zu befolgen. „Berücksichtigen“ heißt immer nur, dass eine Forderung zur Kenntnis zu nehmen und ihre Erfüllung zu erwägen, aber gerade nicht, dass sie einzuhalten ist.[20] Nach der Formulierung in den drei Regelungen kann also immer auch von dem Sicherheitsniveau, das der Stand der Technik beschreibt, nach unten abgewichen werden. Welches Sicherheitsniveau durch die drei Regelungen erreicht wird, bleibt somit letztlich der Entscheidung des Betreibers überlassen. Eine Einheitlichkeit im Sicherheitsniveau kann mit dem „Berücksichtigen“ des Standes der Technik gerade nicht erreicht werden. Das Sicherheitsniveau wird auch nicht durch den Begriff der „angemessenen“ Vorkehrungen bestimmt, weil die Angemessenheit sich nicht auf das Sicherheitsziel, sondern nur auf das Verhältnis von Aufwand und Nutzen bezieht. Insgesamt ist daher festzustellen, dass das grundlegende Ziel

---

15 S. z.B. in § 3 Abs. 6 BImSchG, § 3 Abs. 28 KrWG oder § 3 Nr. 11 WHG.

16 Wie in den Vorversionen des Entwurfs.

17 S. BT-Drs. 18/4096, 42.

18 Solche Anlagen zum Stand der Technik enthalten auch das KrWG und das WHG.

19 Ebenso Art. 14 Abs. 1 des Entwurfs der NIS-RL. Die Bestimmungen der NIS-RL stellen jedoch nach Art. 2 nur Mindestanforderungen dar, die die Mitgliedstaaten nicht daran hindern, Bestimmungen zur Gewährleistung eines höheren Sicherheitsniveaus zu erlassen oder aufrechtzuerhalten.

20 S. auch Eckardt, (Fn. 7), ZD 2014, 600.

des Gesetzes, in allen Kritischen Infrastrukturen ein hohes und gleichmäßiges Niveau der IT-Sicherheit zu gewährleisten,[21] durch die Regelung in § 8a Abs. 1 BSIG-E verfehlt wird. Notwendig ist daher, dass der Stand der Technik nicht nur berücksichtigt, sondern erreicht wird.

Dies schließt nicht aus, alternative Lösungen zu wählen, die in einer nationalen oder internationalen technischen Norm nicht enthalten sind. Diese Alternativen müssen aber das gleiche Sicherheitsniveau bieten wie die technischen Normen. Dieses kann aber mit unterschiedlichen Mitteln oder auf anderen Wegen erreicht werden. Soweit der Stand der Technik verbindlich und nicht nur zu berücksichtigen ist, bleibt auch bei Alternativen das Niveau gewahrt und ist für alle Kritische Infrastrukturen gleich.

b) Branchenspezifische Standards

Da die Sicherheitsprobleme in den verschiedenen Sektoren und Branchen unterschiedlich sind, ist es sinnvoll, dass die Betreiber Kritischer Infrastrukturen und ihre Branchenverbände nach § 8a Abs. 2 BSIG-E branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach § 8a Abs. 1 BSIG-E vorschlagen können. Diese können die Probleme und Möglichkeiten der Branchen unter Umständen konkreter und wirksamer adressieren.[22] Um bei dieser Selbstregulierung eine „Selbstbedienung" der Regelungsadressaten auszuschließen,[23] ist es notwendig, dass das BSI auf Antrag feststellt, ob diese geeignet sind, die Anforderungen nach § 8a Abs. 1 BSIG-E zu gewährleisten. Dieser feststellende Verwaltungsakt ist inhaltlich nur möglich, wenn der Stand der Technik nach § 8a Abs. 1 Satz 2 BSIG-E verbindlich ist. Ist er nur zu berücksichtigen, hat das BSI keinen festen Maßstab, nach dem es eine gleiche Eignung der branchenspezifischen Sicherheitsstandards bemessen kann. Unklar ist auch, wie repräsentativ der Branchenverband für die Branche sein muss.[24]

c) Nachweise der Sicherheit

Die Betreiber Kritischer Infrastrukturen haben nach § 8a Abs. 3 Satz 1 BSIG-E mindestens alle zwei Jahre die Erfüllung der Anforderungen in § 8a Abs. 1 BSIG-E „auf geeignete Weise nachzuweisen".[25] Welcher Nachweis „geeignet" ist, wird nicht festgelegt. Diese Frage wird aber in der Praxis entscheidend sein. Unklar ist, ob nur Nachweise über das Sicherheitskonzept oder auch seine Umsetzung zu erbringen sind, ob eine Prüfung von Unterlagen genügt oder eine Prüfung vor Ort erforderlich ist, ob eine Besichtigung ausreicht oder eine Kontrolle (wie lange?) des laufenden Betriebs notwendig ist? Muss nur die Sicherheit der eingesetzten Technik (Hard- und Software) nachgewiesen werden oder auch das Bestehen oder Funktionieren eines Sicherheitsmanagementsystems? Genügen Selbstbestätigungen des Betreibers, eines Lieferanten oder eines Herstellers oder müssen alle Bestätigungen von einem Dritten stammen? Welche Qualifikation, Erfahrung und Unabhängigkeit muss dieser Dritte haben? Diese Fragen[26] sind entscheidend dafür, welchen Aufwand der Sicherheitsnachweis beim Regelungsadressaten verursacht und ob er zur Erreichung des gesetzlichen Ziels überhaupt geeignet und ob eine bestimmte Form des Nachweises erforderlich und verhältnismäßig ist. Die Fragen dürfen weder unbeantwortet bleiben noch dem BSI ohne gesetzliche Vorgaben überlassen blei-

---

21 S. BT-Drs. 18/4096, 1.

22 S. auch Roth, (Fn. 7), ZD 2015, 21.

23 S. hierzu Roßnagel, Konzepte der Selbstregulierung, in: ders. (Hrsg.), Handbuch Datenschutzrecht, München 2013, 408f.

24 S. auch Eckardt, (Fn. 7), ZD 2014, 600.

25 Art. 15 Abs. 2 b) des Entwurfs der NIS-RL fordert eine „Sicherheitsüberprüfung …, die von einer qualifizierten unabhängigen Stelle oder einer zuständigen nationalen Behörde durchgeführt wird".

26 S. ansatzweise Antworten hierzu in BT-Drs. 18/4096, 44.

ben. Vielmehr sind diese Fragen wegen des Wesentlichkeits- und Bestimmtheitsprinzips im Grundsatz durch das Gesetz und im Detail durch eine Verordnung zu bestimmen. Insofern ist eine Ergänzung des § 8a BSIG-E erforderlich, in der zumindest die Frage des Gegenstands, des Umfangs, der Tiefe und des Verantwortlichen festgelegt wird, um die Eignung des Nachweises beurteilen zu können. Außerdem ist eine Ergänzung des § 10 BSIG-E erforderlich, die eine Ermächtigung enthält, in einer Rechtsverordnung die Nachweise ausreichender Sicherheit zu regeln. Alternativ könnte eine Regelung wie in § 11 Abs. 1a Satz 6 EnWG-E gewählt werden, dass die Behörde „nähere Bestimmungen zu Format, Inhalt und Gestaltung" des Sicherheitsnachweises trifft.

Soweit für einzelne Aspekte der Sicherheitsgewährleistung Sicherheits-Audits oder -Zertifizierungen angeboten werden, kann nach § 8a Abs. 3 Satz 2 BSIG-E der Nachweis der Sicherheit auch durch die Vorlage der Audit- oder Zertifizierungsdokumente erbracht werden. Dabei ist zu unterscheiden, dass das Sicherheit-Audit nur die Eignung eines Sicherheitsmanagementsystems bestätigen kann und deswegen von Betreiber der Kritischen Infrastruktur in Auftrag gegeben werden muss. [27] Dagegen betrifft das Sicherheits-Zertifikat ein IT-Produkt, einen Prozess oder ein Profil[28] und kann nur vom Hersteller beauftragt werden.[29] Wozu noch Prüfungen, die § 8a Abs. 3 Satz 2 BSIG-E als dritte Möglichkeit erwähnt, hilfreich oder erforderlich sind, ist auch nach der Lektüre der Gesetzesbegründung[30] unklar. Eine Prüfung als solche bestätigt noch kein Ergebnis. Wenn aber das Ergebnis der Prüfung ein Sicherheitsmanagementsystem oder ein Produkt betrifft, kann es auch als Bestätigung eines Audits oder als Zertifikat ausgestellt werden. Für die Akzeptanz des Audits oder des Zertifikats kommt es aber entscheidend darauf an, wer es ausgestellt und nach welcher Methode und in welchem Verfahren er sein Ergebnis festgestellt hat. Auch die Beantwortung dieser Fragen kann nicht ohne gesetzliche Kriterien dem BSI überlassen, sondern muss zumindest dem Grundsatz nach im Gesetz erfolgen. Einzelheiten können einer Rechtsverordnung überlassen werden.

Die Frage, welche Anforderungen an denjenigen zu stellen sind, der ein Sicherheitszertifikat oder ein Datenschutzaudit ausstellt,[31] betrifft dessen Grundrecht auf freie Berufswahl und bedarf daher einer gesetzlichen Regelung. Aus diesem Grund wurde z.B. die Vorschrift des § 18 SigG, die im ersten Signaturgesetz von 1997 noch fehlte, im Jahr 2001 in das neue Signaturgesetz aufgenommen.[32]

Bei der Prüfung der Sicherheitsnachweise und bei der Anordnung nach § 8a Abs. 3 Satz 4 BSIG-E, Sicherheitsmängel zu beseitigen, wird sich in vielen Fällen herausstellen, dass der Betreiber der Kritischen Infrastruktur Verbesserungen der Sicherheit nur im Rahmen der von ihm genutzten Hard- und Software durchführen kann.[33] Mängel dieser technischen Systeme kann er nur beseitigen und Verbesserungen kann er nur erreichen, wenn der Hersteller der Soft- oder Hardware mitwirkt oder diese Maßnahmen selbst durchführt. Soweit für den Hersteller die deutsche Rechtsordnung gilt, könnte das Gesetz für ihn Mitwirkungspflichten vorsehen. Soweit er nicht der deutschen Rechtsordnung unterliegt oder eine Monopolstellung hat, wird auch das nicht weiterführen.

---

27 S. näher Roßnagel, Datenschutzaudit – Konzeption, Durchführung, Gesetzliche Regelung, Wiesbaden 2000, 56 ff.

28 S. näher § 2 Abs. 7 BSIG.

29 S. zur Unterscheidung von Audit und Zertifikat s. Roßnagel, Das Konzept des Datenschutzaudits, in: ders. (Hrsg.), Handbuch Datenschutzrecht, München 2003, 462 ff.

30 S. BT-Drs. 18/4096, 44.

31 S. hierzu auch BT-Drs. 18/4096, 44.

32 S. näher Roßnagel, in: ders (Hrsg.), Recht der Telemediendienste, München 2013, § 18 SigG, Rn. 9f.

33 Auf die steigende Verantwortung der Hersteller verweist auch BT-Drs. 18/4096, 3.

Daher sind unbedingt Sicherheitszertifizierungen zu forcieren. Hierfür müssen „unwiderstehlich“ Anreize geschaffen werden. Ein wichtiger Anreiz könnte sein, wenn die Zertifizierung ein wesentliches Kriterium für die Vergabe von Aufträgen öffentlicher Stellen wäre. Diese Voraussetzung für Aufträge der öffentlichen Hand würde die Kosten für Zertifizierungen bei den Herstellern erträglicher machen. Für privatwirtschaftliche Unternehmen, die Kritische Infrastrukturen betreiben, wäre ein wichtiger Vorteil, wenn bei zertifizierten Produkten unterstellt würde, dass sie die Sicherheitsvoraussetzungen erfüllen, bei nicht-zertifizierten Techniksystemen, diese aber eigens nachgeprüft werden müsste.

d) Ausnahmen von den Sicherheitspflichten

Da die Vorgaben des § 8a BSIG-E nur „Mindestanforderungen“[34] an die IT-Sicherheit von Kritischen Infrastrukturen formulieren wollen, ist es sinnvoll in § 8c Abs. 2 BSIG-E die Betreiber von Kritischen Infrastrukturen auszunehmen, die spezielleren oder weitergehenden Sicherheitsanforderungen unterliegen. Dies wird in § 8c Abs. 2 Nr. 1 bis 3 BSIG-E sehr präzise festgelegt, in Nr. 4 jedoch sehr unbestimmt gehalten, wenn auf „Anforderungen“ verwiesen wird, die „nach § 8a vergleichbar oder weitergehend sind“. Zwar ist eine gewisse Flexibilität notwendig, weil künftig immer wieder neue Anforderungen auf Unions- oder Bundesebene entstehen können.[35] Dennoch stellt sich die Frage, ob nicht mit wenig gesetzgeberischem Aufwand, die Rechtssicherheit erhöht werden kann.

Die Frage, ob die konkurrierenden Rechtsvorschriften „weitergehend“ sind, ist noch relativ leicht zu beantworten, wenn es um die gleichen Themen geht wie in § 8a BSIG. Es wird jedoch immer schwieriger, zu einer klaren Antwort zu gelangen, wenn die Rechtsvorschriften unterschiedliche Themen betreffen. Sind die anderen Rechtsvorschriften weitergehend, wenn sie z.B. die Einhaltung des Standes der Technik fordern, aber nur alle vier Jahre einen Sicherheitsnachweis verlangen und keine Nachbesserungspflichten kennen? Das Problem liegt in der starren Rechtsfolge, dass bei „weitergehenden“ Rechtsvorschriften § 8a BSIG-E *insgesamt* nicht anwendbar ist. Daher wird empfohlen, § 8a BSIG-E nur „insoweit“ nicht anwendbar zu erklären, als andere Rechtsvorschriften, weitergehend sind.

Schwieriger wird der Vollzug des Gesetzes, wenn es um die Frage geht, ob die anderen Rechtsvorschriften „vergleichbar“ sind. Sind die Rechtsvorschriften in dem oben genannten Beispiel „vergleichbar“, wenn sie in Bezug auf § 8a BSIG-E unterschiedliche hohe Anforderungen stellen? Auch hier würde eine Flexibilisierung durch eine „Soweit“-Regelung den Vollzug erleichtern.

5. IT-Sicherheits-Informationssystem

Die Vorschriften der § 8b Abs. 3 bis 5 BSIG-E, § 44b AtG-E, § 11 Abs. 1c EnWG-E und § 109 Abs. 5 TKG-E etablieren ein Informationssystem zwischen Betreibern Kritischer Infrastrukturen, dem BSI und den zuständigen Aufsichtsbehörden, um bei Störungen der Sicherheit ein Lagebild zu erstellen und unter den Teilnehmern einen Informationsaustausch zu etablieren, von dem durch die Zusammenführung und Auswertung der Informationen alle profitieren sollen.[36] Ein solches Informationssystem zur Vorsorge und zur Abwehr von Sicherheitsproblemen und -angriffen zu betreiben, ist zum Schutz der Kritischen Infrastrukturen notwendig.

---

34 S. BT-Drs. 18/4096, 2, 29, 42.

35 S. BT-Drs. 18/4096, 50.

36 S. BT-Drs. 18/4096, 45.

a) Meldepflichten der Betreiber von Kritischen Infrastrukturen

Betreiber Kritischer Infrastrukturen haben nach § 8b Abs. 4 Satz 1 BSIG-E „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, unverzüglich an das BSI zu melden.[37] Wann eine Störung „erheblich" ist, wird – trotz der kurzen Erläuterung in der Entwurfsbegründung[38] – zu einer gewissen Unsicherheit führen. Hier wäre ein Leitfaden, mit Kriterien für meldungsrelevante Sicherheitsvorfälle, wie sie die Entwurfsbegründung ankündigt,[39] für die Einschätzung der Erheblichkeit durch die Betreiber hilfreich.[40]

Der Vorschrift könnte gegen das Verbot der Selbstbeschuldigung[41] verstoßen.[42] Dies wäre dann der Fall, wenn eine allein meldepflichtige natürliche Person in die Zwangslage käme, sich selbst einer Straftat oder Ordnungswidrigkeit zu bezichtigen oder gegen die Vorschrift zu verstoßen. Da die Betreiber in der Regel juristische Personen sind und fast immer erklärungsberechtigte Personen verfügbar sind, die die nach der Vorschrift geforderte Meldung durchführen können, dürfte sich in der Praxis diese Zwangslage nie ergeben. Soweit eine solche Zwangslage befürchtet und daher ein Konflikt mit Verbot der Selbstbeschuldigung erwartet wird, würde die Regelung eines Verwendungsverbots wie in § 42a Abs. 6 BDSG eine grundrechtlich sichere Lösung des Problems darstellen.[43]

§ 8b Abs. 4 Satz 2 BSIG-E bestimmt sehr abstrakt, welche Angaben zu melden sind. Aufgeführt werden nur vier Angaben: 1. zur Störung, 2. zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, 3. zur betroffenen Informationstechnik und 4. zur Branche des Betreibers. Diese Angaben sind für einen rechtssicheren Vollzug der Meldung unzureichend.[44] Hilfreich wäre eine Ergänzung des Gesetzestextes, dass das BSI nähere Bestimmungen zu Inhalt und Form der Meldung trifft. Alternativ könnte auch in § 10 BSIG eine Ermächtigung zum Erlass einer Rechtsverordnung aufgenommen werden, um die näheren formalen und inhaltlichen Anforderungen für die Meldung zu konkretisieren. Dann könnte das BSI entscheiden, ob ein Formular oder ein Leitfaden oder eine andere Anleitung die größte Rechtssicherheit für die meldepflichtigen Betreiber bietet.[45]

Hinsichtlich der Nennung des Betreibers regelt § 8b Abs. 4 Satz 2 BSIG-E ein zweistufiges Verfahren: Nach diesem dürfen Meldungen zu Störungen ohne Ausfall oder Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur – über die „gemeinsame übergeordnete Ansprechstelle" des jeweiligen Sektors nach § 8b Abs. 5 BSIG-E – anonym gemeldet werden. Nur wenn die Störung „tatsächlich zu einem Ausfall oder

---

37 Nach Art. 14 Abs. 2 des Entwurfs der NIS-RL sollen die Betreiber „Sicherheitsvorfälle melden, die erhebliche Auswirkungen auf die Sicherheit der von ihnen bereitgestellten Kerndienste haben".

38 S. BT-Drs. 18/4096, 46.

39 S. BT-Drs. 18/4096, 48.

40 Nach Art. 14 Abs. 5 des Entwurfs der NIS-RL wird die Kommission ermächtigt, „delegierte Rechtsakte zu erlassen, in denen festgelegt wird, unter welchen Umständen bei Sicherheitsvorfällen für öffentliche Verwaltungen und Marktteilnehmer die Meldepflicht gilt".

41 S. z.B. BVerfGE 38, 105 (113 ff.); 55, 144 (150); 56, 37 (43).

42 So Eckhardt, (Fn. 7), ZD 2014, 600.

43 S. Hornung, in: Roßnagel, Recht der Telemediendienste, München 2013, § 15a TMG, Rn. 43 ff.

44 Ebenso Roth, (Fn. 7), ZD 2015, 21; Roos, (Fn. 7), MMR 2014, 727.

45 Nach Art. 14 Abs. 7 des Entwurfs der NIS-RL kann die Kommission in Durchführungsrechtsakten Formen und Verfahren der Meldungen festzulegen.

einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat", ist die Nennung des Betreibers erforderlich. Die Möglichkeit der gegenüber dem BSI anonymen Meldung ist sinnvoll, um ein vertrauensvolles kooperatives Informationssystem aufzubauen. Die anonymen Meldungen betreffen nur Störungen mit einem *potentiellen* Nachteil für die Kritische Infrastruktur und können dennoch – auch ohne aktuelles Risiko für die Kritische Infrastruktur – leicht zu einem Reputationsschaden des Betreibers führen.

Das Gesetz enthält keine Aufdeckungsregel für die „pseudonymen" Meldungen – wie etwa § 16 DeMailG.[46] Die „gemeinsame übergeordnete Ansprechstelle" des jeweiligen Sektors kennt den meldenden Betreiber und könnte das Pseudonym aufdecken. Hierzu wird sie jedoch nicht verpflichtet, datenschutzrechtlich ist ihr dies aufgrund des Zweckbindungsgrundsatzes untersagt. Das BSI kann also keine Aufdeckung der Identität des Meldenden verlangen, sondern allenfalls Rückfragen an diesen über die „gemeinsame übergeordnete Ansprechstelle" stellen, die dieser wieder über die „gemeinsame übergeordnete Ansprechstelle" vermittelt anonym beantworten kann.[47]

b) Ausnahmen von den Meldepflichten

§ 8c Abs. 3 BSIG-E bestimmt, dass diese Meldepflichten nach Nr. 1 auf Betreiber von öffentlichen Telekommunikationsnetzen und -diensten, nach Nr. 2 auf Betreiber von Energieversorgungsnetzen und Energieanlagen und nach Nr. 3 auf Betreiber von kerntechnischen Anlagen nicht anzuwenden sind. Nach Nr. 4 gilt dies auch für Betreiber, die auf Grund von Rechtsvorschriften „Anforderungen" erfüllen müssen, die „nach § 8b Abs. 3 bis 5 vergleichbar oder weitergehend sind".

Wie für die Ausnahmen von den Sicherheitspflichten[48] gilt auch für Ausnahmen nach § 8c Abs. 3 Nr. 4 BSIG-E, dass sie zu unbestimmt sind. Hier ergeben sich die gleichen Schwierigkeiten festzustellen, ob andere Rechtvorschriften „vergleichbar oder weitergehend" sind. Auch hier würde eine Flexibilisierung durch eine „Soweit"-Regelung den Vollzug erleichtern. Dies gilt umso mehr, als bei den Meldepflichten einzelne Regelungen des § 8b Abs. 3 bis 5 BSIG-E mit anderen Regelungen kombinierbar sind. So könnte eine künftige Pflicht in einer anderen Vorschrift, Sicherheitsvorfälle zu melden, mit der Regelung in § 8b Abs. 4 Satz 3 BSIG-E verbunden werden, dass eine spezifische Gruppe von Meldungen ohne Nennung des Betreibers erfolgen kann, oder mit der Regelung in § 8b Abs. 4 Satz 3 BSIG-E, dass gemeinsame übergeordnete Ansprechstellen gebildet werden können.

c) Meldepflichten der Betreiber von kerntechnischen Anlagen

Betreiber bestimmter kerntechnischer Anlagen werden nach § 8c Abs. 3 Nr. 3 BSIG-E von der Anwendbarkeit der Meldepflichten des § 8b Abs. 3 bis 5 BSIG-E ausgenommen. Für sie gelten spezifische Meldepflichten nach § 44b AtG-E.

Danach haben sie nur „Beeinträchtigungen" ihrer informationstechnischen Systeme, Komponenten oder Prozesse, „die zu einer Gefährdung oder Störung der nuklearen Sicherheit der betroffenen kerntechnischen Anlage oder Tätigkeit führen können oder bereits geführt haben", an das BSI zu melden. Da nicht „erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse" zu melden sind, wie nach § 8b Abs. 4 Satz 1 BSIG-E, sind die Mel-

---

[46] S. hierzu Roßnagel, Das De-Mail-Gesetz – Grundlage für mehr Rechtssicherheit im Internet, NJW 2011, 1473 ff.

[47] S. hierzu auch BT-Drs. 18/4096, 47.

[48] S. 4. d).

depflichten geringer als bei anderen Kritischen Infrastrukturen – angesichts des hohen Schadenspotentials kerntechnischer Anlagen nicht ganz nachvollziehbar.

Der Inhalt der Meldung ist ähnlich unbestimmt wie nach § 8b Abs. 4 Satz 2 BSIG-E, so dass hier die gleichen Überlegungen gelten.

Die Meldung ist unmittelbar an das BSI zu richten, das die Meldung unverzüglich an die für die nukleare Sicherheit und Sicherung zuständigen Genehmigungs- und Aufsichtsbehörden des Bundes und der Länder weiterleitet. Ebenso gut könnte die Meldung an beide gleichzeitig geschickt werden[49] und damit ein Streit zwischen Bundesrat und Bundesregierung beseitigt werden.[50]

Eine anonyme Meldung ist nicht möglich und wäre angesichts der sehr überschaubaren Anzahl der betroffenen kerntechnischer Anlagen auch wenig hilfreich. Auch muss das BSI den Betreiber kennen, um die Meldung der Genehmigungs- und Aufsichtsbehörde des richtigen Landes weiterleiten zu können.

c) Meldepflichten der Betreiber von Energieversorgungsnetzen und Energieanlagen
Betreiber von Energieversorgungsnetzen und Energieanlagen werden nach § 8c Abs. 3 Nr. 2 BSIG-E von der Anwendbarkeit der Meldepflichten des § 8b Abs. 3 bis 5 BSIG-E ausgenommen. Für sie gelten spezifische Meldepflichten des § 11 Abs. 1c EnWG-E.

Die Voraussetzungen eine Meldung sind die gleichen wie für die anderen Betreiber Kritischer Infrastrukturen nach § 8b Abs. 4 Satz 1 BSIG-E. Auch hier verursacht der Begriff der „erheblichen" Störung Rechtsunsicherheit.

Der Inhalt der Meldung ist ebenso unbestimmt wie nach § 8b Abs. 4 Satz 2 BSIG-E, so dass hier die gleichen Überlegungen gelten.

Die Meldung ist unmittelbar an das BSI zu richten, das die Meldung unverzüglich an die Bundesnetzagentur weiterleitet. Dies ist genau umgekehrt organisiert als im Telekommunikationsbereich nach § 109 Abs. 5 TKG-E, obwohl auch dort BSI und Bundesnetzagentur beteiligt sind. Eine gleichzeitige identische Meldung an beide Behörden wäre sinnvoller. Das BSI und die Bundesnetzagentur haben nach § 11 Abs. 1c Satz 5 EnWG-E sicherzustellen, dass die unbefugte Offenbarung, der ihnen durch die Meldung zur Kenntnis gelangten Angaben ausgeschlossen wird.

Die Nennung des Betreibers ist nach § 11 Abs. 1c Satz 3 EnWG-E nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat. Dies ist gegenüber dem BSI aber nur möglich, wenn für den Sektor Energie nach § 8b Abs. 5 BSIG-E eine „gemeinsame übergeordnete Ansprechstelle" geschaffen werden könnte, die die Meldung vermittelt und gegenüber dem BSI anonymisiert. Die Anwendung des § 8b Abs. 5 BSIG-E ist nach § 8c Abs. 3 Nr. 2 BSIG-E für Betreiber von Energieversorgungsnetzen und Energieanlagen aber ausgeschlossen, so dass das Versprechen des § 11 Abs. 1c Satz 3 EnWG-E einer anonymen Meldung faktisch in Leere laufen muss.

---

[49] S. hierzu auch 5. d).

[50] Eine parallele Meldung hält auch die Bundesregierung für möglich – s. Gegenäußerung der Bundesregierung zu § 44b AtG, BT-Drs. 18/4096, 87.

d) Meldepflichten der Betreiber von Telekommunikationsnetzen und diensten

Für Betreiber von öffentlichen Telekommunikationsnetzen und -diensten sind nach § 8c Abs. 3 Nr. 1 BSIG-E die Meldepflichten des § 8b Abs. 3 bis 5 BSIG-E nicht anwendbar. Für sie gelten stattdessen die spezifischen Meldepflichten nach § 109 Abs. 5 TKG-E.

Nach Satz 1 dieser Vorschrift haben die Anbieter nur „Beeinträchtigungen" von Telekommunikationsnetzen und -diensten an das BSI zu melden, die „zu beträchtlichen Sicherheitsverletzungen führen oder … führen können". Insofern sind – wie bei kerntechnischen Anlagen – die Meldepflichten geringer als bei anderen Kritischen Infrastrukturen. Andererseits haben sie nach § 109 Abs. 5 Satz 2 TKG-E die Meldungen auch auf „Störungen" zu erstrecken, „die zu einer Einschränkung der Verfügbarkeit der über diese Netze erbrachten Dienste oder einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können". Insoweit sie nicht nur potentielle Einschränkungen ihrer Netze und Dienste, sondern auch mögliche Auswirkungen auf ihre Nutzer melden müssen, sind ihre Meldepflichten weiter als bei anderen Kritischen Infrastrukturen. Diese erweiterten Meldepflichten werden von der Entwurfsbegründung mit der besonderen Bedeutung der Telekommunikation für die digitale Vernetzung („Schlüsselrolle für die Sicherheit des Cyberraums",[51] „Rückgrat unserer Informationsgesellschaft"[52]) begründet. Diese besonders hohe Verantwortung der Betreiber von öffentlichen Telekommunikationsnetzen und -diensten rechtfertigt die erweiterten Meldepflichten.

Der Inhalt der Meldung ist nach § 109 Abs. 5 Satz 3 TKG-E ähnlich unbestimmt wie nach § 8b Abs. 4 Satz 2 BSIG-E, so dass hier die gleichen Überlegungen gelten.

Im Gegensatz zu allen anderen Meldungen, insbesondere auch im Gegensatz zu den Meldungen nach § 11 Abs. 1c Satz 1 EnWG-E sind die Meldung der Telekommunikationsanbieter nicht an das BSI zu richten, sondern an die Bundesnetzagentur. Diese hat dann die Meldungen zu Sicherheitsverletzungen, die die Informationstechnik betreffen, nach § 109 Abs. 5 Satz 5 TKG-E an das BSI weiter zu leiten. Das BSI benötigt aber nicht nur Meldungen zu „Sicherheitsverletzungen", sondern zu allen Beeinträchtigungen der Kritischen Infrastruktur, um ein vollständiges Lagebild erzeugen zu können. Warum in Fall der Telekommunikationsanbieter die Meldungen zuerst der Bundesnetzagentur gemeldet und im Fall der Energienetze und -anlagen zuerst an das BSI geschickt werden sollen, ist unverständlich. Warum werden nicht die Meldungen direkt beiden Behörden gleichzeitig geschickt?[53] In der E-Mail, die die Meldung enthält, würde dies nur einen zusätzlichen Eintrag im Header erfordern. Das gilt auch für die Genehmigungs- und Aufsichtsbehörden kerntechnischer Anlagen.

Eine anonyme Meldung ist nicht vorgesehen. Warum die Betreiber von öffentlichen Telekommunikationsnetzen und -diensten in dieser Frage schlechter gestellt werden als sonstige Betreiber Kritischer Infrastrukturen, ist nicht nachvollziehbar. Allerdings müsste für eine Gleichstellung § 8c Abs. 3 BSIG geändert werden.

e) Aufgaben des BSI

Nach § 8b Abs. 2 BSIG-E hat das BSI die gemeldeten „wesentlichen" Informationen zu sammeln und auszuwerten, hinsichtlich ihrer potentielle Auswirkungen auf die Verfügbarkeit der Kritischen Infrastrukturen zu

---

51 S. BT-Drs. 18/4096, 2.

52 S. BT-Drs. 18/4096, 62.

53 So auch die Gegenäußerung der Bundesregierung zu § 44b AtG, BT-Drs. 18/4096, 87.

analysieren, das Lagebild bezüglich der Sicherheit in der Informationstechnik der Kritischen Infrastrukturen kontinuierlich zu aktualisieren und unverzüglich die Betreiber Kritischer Infrastrukturen und die Aufsichtsbehörden über die erforderlichen Informationen zu unterrichten. Diese Aufgaben zu erfüllen, ist für das Erreichen des Gesetzesziels notwendig und hilfreich

Ungeregelt bleiben jedoch Anforderungen, wie das BSI mit diesen Informationen jenseits ihrer inhaltlichen Bearbeitung umzugehen hat.[54] Es hat nur die „wesentlichen" Daten zu sammeln. Es sollte festgelegt werden, wie die eventuell riesige Menge an Rohdaten der Meldungen gesichert und wann sie gelöscht werden.[55] Auch sollte festgelegt werden, dass das BSI diese Rohdaten ausschließlich für die in § 8b Abs. 2 BSIG-E genannten Auswertungen und Analysen verwenden und an niemanden weitergeben darf. Eine Klausel wie etwa die in § 11 Abs. 1c Satz 5 EnWG-E, dass die unbefugte Offenbarung, der dem BSI durch die Meldung zur Kenntnis gelangten Angaben auszuschließen ist, fehlt. Warum in dieser Hinsicht die Betreiber von Energieversorgungsnetzen und Energieanlagen besser behandelt werden als andere Betreiber Kritischer Infrastrukturen ist unverständlich.

Schließlich wäre zu klären, ob korrespondierend zu den Kontaktstellen der Betreiber Kritischer Infrastrukturen, die nach § 8b Abs. 3 Satz 2 BSIG-E „jederzeit erreichbar" sein müssen, auch die Kontaktstelle des BSI jederzeit erreichbar sein muss.[56]

f) Information Betroffener und der Öffentlichkeit

Der Schutzpflicht des Staates kann es erfordern, die Öffentlichkeit oder einzelne Nutzer zu informieren, um sie vor Schäden zu schützen oder ihnen zu ermöglichen ihre informationstechnische Sicherheit zu erhöhen. Dies kann es auch erforderlich machen, über Sicherheitsvorfälle zu informieren, vor Sicherheitslücken zu warnen oder Sicherheitsmaßnahmen zu empfehlen.

Dies ist nach § 3 Abs. 1 Satz 2 Nr. 14 BSIG auch Aufgabe des BSI. Es konnte auch bisher schon nach § 7 BSIG Warnungen und Empfehlungen aussprechen. Nach der Neufassung des § 7 Abs. 1 Satz 1 BSIG-E wird diese Befugnis noch ausgeweitet und präzisiert. Dies ist im Interesse der allgemeinen Sicherheit in der Informationstechnik zu begrüßen. Als Adressaten der Informationen sollten auch die Anbieter von IT-Dienstleistungen genannt werden.[57] Auch die allgemeinen Erkenntnisse aus der Tätigkeit als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen (§ 3 Abs. 1 Satz 2 Nr. 17 BSIG-E) müssen auch in diese Öffentlichkeits- und Aufklärungsarbeit eingehen. Dies bedeutet nicht, dass die einzelnen Sicherheitsinformationen oder Meldungen nach §§ 8a und 8b BSIG-E mitgeteilt werden sollten oder dürfen.

Da die Informationsaufgabe des BSI keine „Wohltat" gegenüber den Unternehmen und Bürgern ist, sondern Ausfluss der grundrechtlichen Schutzpflicht des Staates, sollte dies auch in der Ausgestaltung der Informationspflichten des BSI zum Ausdruck kommen. Ob das BSI über Sicherheitslücken, Sicherheitsrisiken oder Sicherheitsmaßnahmen informiert, sollte nicht in seinem freien Ermessen („kann") stehen, sondern seinem gebundenen Ermessen („soll") unterliegen. Um berechtigte Sicherheits- und Geheimhaltungsinteressen zu schützen, sollte es vor seinen Informationen eine Abwägung mit entgegenstehenden Interessen durchfüh-

---

54 S. Bundesrat, BT-Drs. 18/4096, 74f.

55 S. hierzu für personenbezogene Daten auch 9.

56 S. hierzu auch Eckardt, (Fn. ##), ZD 2014, 601.

57 Bundesrat, BT-Drs. 18/4096, 76 und Gegenäußerung der Bundesregierung, BT-Drs. 18/4096, 85.

ren. Durch die gesetzliche Regelung der Informationsaufgaben muss zum Ausdruck kommen, dass die Information der Öffentlichkeit oder einzelner besonders Betroffener die Regel ist und die Verweigerung aus entgegenstehenden Interessen die Ausnahme – nicht wie bisher umgekehrt. Auch darf die Information nicht davon abhängig gemacht werden, dass sie im öffentlichen Interesse liegt.[58] Der Schutz der Grundrechte ist dem Staat nicht nur im öffentlichen Interesse aufgegeben, sondern im Interesse jedes Grundrechtsträgers.

Die Öffentlichkeit oder einzelne Nutzer sind zwar nicht Teil des Informationssystems, das nach § 8b BSIG-E aufgebaut werden soll. Dennoch können sie die Erkenntnisse, die das BSI durch die branchenspezifischen Sicherheitsstandards und die betreiberbezogenen Sicherheitsnachweise gewonnen hat, existenziell betreffen. Daher sieht § 8d Abs. 1 Satz 1 BSIG-E vor, dass das BSI auch „Dritten" auf Antrag Auskunft zu diesen Informationen erteilen „kann". Es darf nach § 8d Abs. 1 Satz 2 BSIG-E diese Auskunft jedoch nur erteilen, „wenn schutzwürdigen Interessen des betroffenen Betreibers Kritischer Infrastrukturen dem nicht entgegenstehen und durch die Auskunft keine Beeinträchtigung wesentlicher Sicherheitsinteressen zu erwarten ist". Diese Regelung kennt keine Abwägung zwischen den Sicherheitsinteressen des Antragstellers und den Interessen des Betreibers, sondern lässt diese vollständig vorgehen. Zugespitzt sind nach dem Wortlaut dieser Regelung geringe schutzwürdigen Interessen des betroffenen Betreibers gewichtiger als noch so große Sicherheitsinteressen eines antragstellenden Unternehmens, das sich besser schützen will. Diese starre Regelung wird der gebotenen Abwägung der beteiligten Grundrechte, die durch das Handeln des BSI geschützt werden sollen, nicht gerecht. Angemessener wäre es, dem BSI grundsätzlich aufzugeben, auf berechtigte Anfragen hin Auskünfte zu erteilen, diese aber im Einzelfall von eine Abwägung der widerstreitenden Interessen abhängig zu machen. Auch sollte es versuchen, durch die Art der Auskunftserteilung beiden Interessen gerecht zu werden.

Neben dem BSI wird durch § 109 Abs. 5 Satz 7 TKG-E auch die Bundesnetzagentur als Stelle, die dem Schutz der Öffentlichkeit und einzelner Dritter verpflichtet ist, angesprochen. Sie „kann" nach dieser Regelung die Öffentlichkeit unterrichten oder die nach zu Meldungen verpflichteten Telekommunikationsanbieter zu dieser Unterrichtung auffordern, „wenn sie zu dem Schluss gelangt, dass die Bekanntgabe der Sicherheitsverletzung im öffentlichen Interesse liegt".[59] Eine solche Unterrichtung kann aber auch im berechtigten Interesse einzelner oder Gruppen von Unternehmen oder Nutzern liegen. Daher sollte auch diese Auskunft dem genannten Regel-Ausnahme-Prinzip folgen und bei entgegenstehenden Interessen eine Abwägungspflicht bestehen. Auch sollte die Bundesnetzagentur die Mitteilung in einer Form durchführen, die möglichst allen beteiligten Interessen gerecht wird.

Mit dem neuen § 109a Abs. 4 TKG-E werden neue Informationspflichten der Telekommunikationsanbieter begründet. Sie haben, wenn ihnen Störungen bekannt werden, die von Datenverarbeitungssystemen der Nutzer ausgehen, diese darüber zu benachrichtigen, soweit sie ihnen bereits bekannt sind. Soweit ihnen dies technisch möglich und zumutbar ist, haben sie die Nutzer außerdem „auf angemessene, wirksame und zugängliche technische Mittel hinzuweisen, mit denen sie diese Störungen erkennen und beseitigen können". Mit dieser Informationspflicht werden den Telekommunikationsanbietern Belastungen auferlegt, die von anderen Betreibern Kritischer Infrastrukturen nicht zu tragen sind. Dies sehen manche als ungerechtfertigt an. [60] Die Entwurfsbegründung[61] verweist für diese Sonderbelastung zum einen darauf, dass der

---

58 S. BT-Drs. 18/4096, 64.

59 Dies entspricht Art. 14 Abs. 4 des Entwurfs einer NIS-RL.

60 S. z.B. Eckardt, (Fn. 7), ZD 2014, 604f.

61 So aber BT-Drs. 18/4096, 46.

Betreiber für diesen Zweck keine Nutzerdaten sammeln muss und auch nicht sammeln darf, sondern nur solche Nutzer benachrichtigen muss, die ihm ohnehin bekannt sind. Außerdem muss er keine individuelle Beratung durchführen, sondern kann – notfalls nur die Teilnehmer – seine Hinweise in einer Massenmail mitteilen oder – soweit dies von der Sicherheitslage empfehlenswert ist – seiner Informationspflicht auch dadurch genügen, dass er die Information auf seiner Webseite bekannt gibt.[62] Diese doch geringe Belastung wird gerechtfertigt durch die besondere Bedeutung, die Telekommunikation für die Sicherheit in der digitalen Gesellschaft hat, und die besondere Verantwortung, die ein privates Unternehmen trifft, das diese öffentliche Aufgabe übernimmt. Nur so kann der Nutzer in die Lage versetzt werden, „selbst Maßnahmen gegen die auf ihren Systemen vorhandene Schadsoftware zu ergreifen" und damit die allgemeine Sicherheitslage zu verbessern.[63]

6. Mangelnde Sanktionsbefugnisse

Die Pflichten der Betreiber Kritischer Infrastrukturen in §§ 8a und 8b BSIG-E sind nicht sanktionsbewehrt. Damit fehlt eine Möglichkeit, die Sicherheitspflichten der Betreiber und den vom Entwurf verfolgten kooperativen Ansatz eines Informationssystems auch durchzusetzen.[64]

Nach § 8a Abs. 1 Satz 1 BSIG-E trifft den Betreiber einer Kritischen Infrastruktur eine Pflicht zu *Sicherheitsvorkehrungen*, nach § 8a Abs. 3 Satz 1 BSIG-E eine periodische Pflicht zum Nachweis seiner Sicherheitsvorkehrungen und nach § 8a Abs. 3 Satz 4 BSIG-E eine Pflicht zur Beseitigung von Sicherheitsmängeln. Alle drei Pflichten kann das BSI theoretisch mit den Mitteln des Verwaltungszwangs nach § 11 Verwaltungsvollstreckungsgesetz durch Zwangsgeld durchsetzen. Dieses Verfahren setzt aber einen Verwaltungsakt voraus, der die fehlende Handlung genau beschreibt, eine Androhung des Zwangsgelds, seine Festsetzung und seine Eintreibung. Gegen alle Schritte des BSI stehen dem Betreiber Rechtsmittel zu. Dieses Verfahren ist zu umständlich und zu zeitraubend, um praktisch hilfreich zu sein. Wenn tatsächlich ein einheitliches Sicherheitsniveau bei *allen* Betreibern Kritischer Infrastrukturen – nicht nur den Gutwilligen – erreicht werden soll, muss das BSI eine Möglichkeit haben, dieses Sicherheitsniveau auch durchzusetzen. Verstöße gegen die genannten drei Betreiberpflichten müssen daher mit einer Bußgelddrohung bewehrt werden. Das Gesetz muss durch einen Ordnungswidrigkeitentatbestand ergänzt werden, der für Verstöße gegen diese drei Pflichten empfindliche Bußgelder vorsieht. Ohne eine Bußgeldbewehrung des Verstoß gegen Sicherheitspflichten würde der Entwurf gegen Art. 3 Abs. 1 GG verstoßen, weil § 149 Nr. 21 TKG eine entsprechende Regelung für Telekommunikationsanbieter und § 16 Abs. 2 Nr. 3 TMG eine Ordnungswidrigkeitenvorschrift für Telemedienanbieter vorsehen, selbst wenn sie keine Kritischen Infrastrukturen betreiben.

Hinsichtlich des *IT-Sicherheits-Informationssystems* ist der Ansatz des Gesetzentwurfs, dieses in einer kooperativen Weise zusammen mit den Betreibern der Kritischen Infrastrukturen zu betreiben,[65] zu unterstützen. Die Hoffnung der Autoren des Gesetzentwurfs, dass dieses Angebot eines kooperativen Informationssystems von der Betreiberseite auch angenommen wird, stellt jedoch nicht sicher, dass tatsächlich auch *jeder* Betreiber einer Kritischen Infrastruktur sich an seine gesetzlichen Pflichten aus § 8b BSIG-E hält. Sollten sich – mangels drohender Sanktionen[66] – auch nur wenige verweigern, wird das gesamte Konzept eines

---

62 S. hierzu auch Roos, (Fn. 7), MMR 2014, 727.

63 S. BT-Drs. 18/4096, 64.

64 S. hierzu auch Roos, (Fn. 7), MMR 2014, 729.

65 S. BT-Drs. 18/4096, .

66 Zwangsmittel nach dem Verwaltungsvollstreckungsgesetz scheiden schon mangels eines Verwaltungsakts aus.

kooperativen Informationssystems misslingen, weil es darauf angewiesen ist, dass die Teilnahme an ihm nicht zu Wettbewerbsnachteilen führt. Solange sich aber einzelne ohne Konsequenzen verweigern können, wird dies genau dazu führen, dass auch die Kooperationswilligen nicht einsehen, warum sie wirtschaftliche Nachteile in Kauf nehmen sollen, die ihre Konkurrenz sich erspart. Das Konzept des kooperativen Informationssystems ist daher gerade darauf angewiesen, dass Pflichtverletzungen als Ordnungswidrigkeit mit einem spürbaren Bußgeld sanktioniert werden können. Fehlt eine Bußgeldbewehrung für die Verletzung der Meldepflichten, würde der Entwurf gegen Art. 3 Abs. 1 GG verstoßen, da er selbst in dem neuen § 149 Nr. 21a TKG eine entsprechende Regelung für Telekommunikationsanbieter vorsieht. Dies muss auch für andere Betreiber von Kritischen Infrastrukturen gelten.

Auch der Entwurf der NIS-RL fordert in Art. 17 Abs. 1, für Verstöße sowohl gegen die Sicherheitspflichten als auch gegen die Meldepflichten Sanktionen zu erlassen, die „wirksam, angemessen und abschreckend" sind.

Diese Sanktion kann jedoch – dem kooperativen Ansatz entsprechend – differenziert geregelt werden und zum Ansatz kommen. Keine Ordnungswidrigkeit sollte vorgesehen werden, wenn die erforderliche Meldung nach § 8b Abs. 4 Satz 1 BSIG-E eine Störung betrifft, die tatsächlich zu keinem Ausfall und zu keiner Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat. Eine solche Störung zu erkennen und einem Betreiber nachzuweisen, ist extrem schwierig. Eine solche Meldung kann nach § 8b Abs. 4 Satz 3 BSIG-E ohne Nennung des Betreibers erfolgen. Dieser Anreiz und die hohe Schwierigkeit des Nachweises einer Rechtsverletzung könnten dazu führen, von einem Bußgeldtatbestand abzusehen. Auch soweit eine Ordnungswidrigkeit für den Fall vorgesehen ist, dass die unterbliebene Meldung eine Störung betrifft, die tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat, gilt das Opportunitätsprinzip. Das BSI kann somit das Sanktionsinstrument unter Berücksichtigung des kooperativen Ansatzes gezielt einsetzen, wo dies motivationssteigernd wirkt.

7. Überprüfung von Produkten

Nach dem neuen § 7a Abs. 1 BSIG-E darf das BSI informationstechnische Produkte und Systeme untersuchen, soweit dies dazu dient, seine Aufgaben nach § 3 Abs. 1 Satz 2 Nr. 1 (Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes), Nr. 14 (Beratung und Warnung der Stellen des Bundes, der Länder sowie der Hersteller, Vertreiber und Anwender) und Nr. 17 (zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen) zu erfüllen. Da Bund, Länder, Hersteller, Vertreiber und Anwender auf solche Überprüfungen der informationstechnischen Sicherheit von Produkten und Systemen dringend angewiesen sind, ist es sehr zu begrüßen, dass durch diese Regelung das BSI rechtssicher solche Prüfungen durchführen kann.[67]

Die aus den Untersuchungen gewonnenen Erkenntnisse dürfen nach § 7a Abs. 1 BSIG-E vom BSI und von anderen Stellen nur zu den in § 7a Abs. 1 Satz 1 BSIG-E genannten Zwecken genutzt werden. Zu diesen Zwecken darf das BSI seine Erkenntnisse weitergeben und veröffentlichen, soweit die für diese Zwecke erforderlich ist. Sowohl diese Zweckbegrenzung als auch die Möglichkeit, die Erkenntnisse zu diesen Zwecken weitergeben zu können, ist zu begrüßen. Diese Regelungen verhindern Missbrauch, ermöglichen aber auch einen Gebrauch der Erkenntnisse zur Steigerung der Sicherheit in der Informationstechnik. Allerdings sollte für diese Informationen das bereits angesprochene, aus der staatlichen Schutzpflicht abgeleitete Regel-Ausnahme-Prinzip gelten.

---

[67] S. BT-Drs. 18/4096, 40f.

8. Vorratsdatenspeicherung

Der Entwurf sieht vor, in § 100 TKG an den nur sprachlich umgestalteten Satz 1 einen neuen Satz 2 anzuhängen, nach dem auch Störungen den Umgang mit Bestandsdaten und Verkehrsdaten rechtfertigen, „die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können".

Durch diese Ergänzung werden die Befugnisse der Telekommunikationsanbieter nicht erweitert. Der Gesetzentwurf erweitert nur den Begriff der Störung.[68] Dies entspricht der Auslegung dieses Begriffs durch den Bundesgerichtshof.[69] Diese Rechtsprechung wird jetzt vom Entwurf in den Gesetzestext übernommen und dadurch der Begriff präzisiert. Eine Rechtsänderung gegenüber der durch den Bundesgerichtshof gefundenen Interpretation tritt nicht ein.[70] Wenn man eine Prävention von Störungen will, ist es sinnvoll, unter dem Begriff der Störung auch Beeinträchtigungen der Funktionsfähigkeit zu verstehen.

Von dieser Frage zu unterscheiden ist jedoch die Frage, ob nach der Rechtsprechung des Bundesverfassungsgerichts und des Europäischen Gerichtshofs zum Schutz des Fernmeldegeheimnisses und insbesondere zur Grundrechtswidrigkeit der Vorratsdatenspeicherung nach §§ 113a und 113b TKG[71] die Vorschrift des § 100 Abs. 1 TKG geändert werden müsste. Ob durch diese Vorschrift „im Kern … eine weitreichende Vorratsdatenspeicherung"[72] zulässt oder in der Auslegung der Erforderlichkeit, die sie durch den Bundesgerichtshof erfahren hat, gerade keine „kleine Vorratsdatenspeicherung" erlaubt,[73] ist heftig umstritten.

Der Bundesgerichtshof hat zu § 100 Abs. 1 TKG festgestellt, dass das Urteil des Europäischen Gerichtshofs zur Vorratsdatenspeicherung[74] den Fall des § 100 Abs. 1 TKG nicht berühre, weil „die Speicherung … nicht für die Zwecke der Strafverfolgungsbehörden, sondern im Interesse des Netzbetreibers" erfolge.[75] Diese Schlussfolgerung verkennt die Tragweite der Auslegung der Art. 7 und 8 GrCh durch den Europäischen Gerichtshof. Der Schutz dieser Grundrechte verlangt „jedenfalls, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken müssen".[76] Daher muss eine einschränkende Regelung „klare und präzise Regeln für die Tragweite und die Anwendung" des Eingriffs vorsehen und „Mindestanforderungen aufstellen, so dass" die Betroffenen „über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen". [77] Jedenfalls ist der Eingriff nicht auf das „absolut Notwendige" beschränkt, wenn er eine alle um-

---

68 S. Gegenäußerung der Bundesregierung, BT-Drs. 18/4096, 89; Roos, (Fn. 7), MMR 2014, 727.

69 S. BGH, NJW 2014, 2500 (2501).

70 S. hierzu z.B. Roos, (Fn. 7), MMR 2014, 728.

71 S. zu diesen Roßnagel, in: Geppert/Schütz (Hrsg.), Beck'scher TKG-Kommentar, 4. Aufl. 2014, §§ 113a und 113b.

72 S. Bundesrat, BT-Drs. 18/4096, 82.

73 S. auch Eckardt, (Fn. 7), ZD 2014, 604.

74 S. EuGH, NJW 2014, 2169; s. hierzu näher Roßnagel, Neue Maßstäbe für den Datenschutz in Europa. Folgerungen aus dem Urteil des EuGH zur Vorratsdatenspeicherung, MMR 2014, 372 ff.

75 S. BGH, NJW 2014, 2500 (2503).

76 S. EuGH, NJW 2014, 2169, Rn. 52.

77 S. EuGH, NJW 2014, 2169, Rn. 54.

fassende, flächendeckende und anlasslose Sicherungsmaßnahme erlaubt – „ohne irgendeine Differenzierung, Einschränkung oder Ausnahme“ anhand des verfolgten Ziels.[78]

Daher ist ein umgekehrter Erst-Recht-Schluss, wie ihn der Bundesgerichtshof angestellt hat, erforderlich: Wenn schon „die Bekämpfung schwerer Kriminalität zur Gewährleistung der öffentlichen Sicherheit“[79] keine anlasslose, ausnahmslose und flächendeckende Speicherung auf Vorrat erlaubt, kann dies für erheblich weniger gewichtige Interessen des Netzbetreibers nicht zulässig sein.

Der Bundesgerichtshof hat sich auch nicht mit den Anforderungen des Bundesverfassungsgerichts an Gesetze, die Eingriffe in das Fernmeldegeheimnis und die informationelle Selbstbestimmung erlauben,[80] auseinandergesetzt. Dann hätte er nämlich festgestellt, dass § 100 Abs. 1 TKG außer der Erforderlichkeit[81] und der Zweckbestimmung keine Begrenzungen der Datenverarbeitung fordert. Er enthält weder Vorgaben zur Eingriffsschwelle (Tatsachen, die einen Anlass für die Maßnahme bieten, und deren Dkumentation), zum Zeitraum der Speicherung,[82] zu Schutzvorkehrungen gegen Missbrauch, zu Zweckbegrenzungen in der Verwendung der Daten, zu Ausnahmen für Träger von Berufsgeheimnissen, zur Information der Betroffenen und zu Löschverpflichtungen.[83] Solange diese Anforderungen des Bundesverfassungsgerichts für Eingriffsregelungen ignoriert werden, muss davon ausgegangen werden, dass die Eingriffsermächtigung verfassungswidrig ist.[84]

9. Datenschutz

Der Datenschutz wird im Entwurf des Gesetzestextes nur in § 8b Abs. 6 BSIG-E angesprochen. Die Begründung geht davon aus, dass die „im Rahmen von § 8b übermittelten Informationen … üblicherweise rein technischer Natur“ sind.[85] Sollte im Einzelfall doch ein Personenbezug gegeben sein, stellt § 8b Abs. 6 BSIG-E klar, dass personenbezogene Daten nur zu den in dieser Vorschrift vorgesehenen Zwecken erhoben, verarbeitet oder genutzt werden dürfen. Eine darüber hinausgehende Verarbeitung und Nutzung zu anderen Zwecken ist unzulässig. Da außerdem die allgemeinen datenschutzrechtlichen Regelungen gelten, ist auch der Grundsatz der Datensparsamkeit nach § 3a BDSG anzuwenden. Daher müssen alle Beteiligten die Möglichkeiten zur Datensparsamkeit etwa durch Anonymisierung, Pseudonymisierung, frühzeitiges Löschen und Abschotten anwenden.[86] Außerdem ordnet die Vorschrift an, die Datenschutzregelungen des § 5 Abs. 7 Satz 3 bis 8 BSIG zum Schutz des Kernbereichs privater Lebensgestaltung entsprechend anzuwenden. Diese Datenschutzregelungen gelten sowohl für den Datenumgang der Betreiber Kritische Infrastrukturen für den Zweck der Meldungen als auch für das BSI für den Zweck der Sammlung, Auswertung und Weitergabe der Daten. Die Daten sind nach §§ 20 Abs. 2 und 35 Abs. 2 BDSG zu löschen, wenn sie nicht mehr für

---

78 S. EuGH, NJW 2014, 2169, Rn. 57.

79 S. EuGH, NJW 2014, 2169, Rn. 42, 51.

80 S. z.B. BVerfGE 65, 1; 78, 77; 84, 192; 96, 171; 103, 21; 100, 313; 107, 299; 109, 279; 110, 33; 113, 348; 113, 348; 115, 166; 115, 320; 118, 168; 120, 274; 125, 260.

81 Die der Bundesgerichtshof gerade nicht im Sinn des EuGH auslegt.

82 S. hierzu auch den Leitfaden des BfDI und der BNetzA für eine datenschutzgerechte Speicherung von Verkehrsdaten: max. sieben Tage.

83 S. zu diesen und weiteren grundrechtlich gebotenen Differenzierungen Roßnagel/Moser-Knierim/Schweda, Interessenausgleich in der Vorratsdatenspeicherung, 2013.

84 S. z.B. Leisterer/Schneider, (Fn. 7), CR 2014, 577f.

85 S. BT-Drs. 18/4096, 48.

86 S. hierzu auch Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18. und 19. März 2015.

die genannten Zwecke erforderlich sind. Um diese Löschpflicht zu präzisieren, sollte eine Frist vorgesehen werden, nach der sie im Regelfall nicht mehr benötigt werden und zu löschen sind.[87]

Aus der Vorschrift des § 8b Abs. 6 BSIG-E kann der Rückschluss gezogen werden, dass die Regelungen in §§ 8a und 8b BSIG-E keine Erlaubnistatbestände zum Umgang mit personenbezogenen Daten darstellen.[88] Soweit für die Sicherheitsvorkehrungen oder die Sicherheitsmeldungen und ihre Bearbeitung mit personenbezogenen Daten umgegangen werden muss, ist dies durch andere Erlaubnistatbestände zu rechtfertigen.

Ein Erlaubnistatbestand ist allerdings in § 7 Abs. 1 BSIG-E „versteckt". Satz 2 dieser Vorschrift ermöglicht es dem BSI, bei Warnungen Dritte als Informationsintermediäre einzubeziehen, sofern dies für eine wirksame und rechtzeitige Warnung erforderlich ist, insbesondere um Betroffene schnellstmöglich zu erreichen. Die damit verbundene Datenübertragung wird durch diese Regelung erlaubt. Sie dient nach der Begründung „auch zur Klarstellung unter Datenschutzgesichtspunkten". „Satz 2 eröffnet aber nicht die Möglichkeit, zusätzliche Daten bei den Dritten zu erheben."[89]

Die Betreiber Kritischer Infrastrukturen können auch nach § 42a BDSG, § 15a TMG und § 109a TKG verpflichtet sein, Datenschutzverletzungen an die Bundesnetzagentur und die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zu melden. Da Datenschutzverletzungen und Sicherheitsverletzungen gemeinsam auftreten können, ist es notwendig, dies bei den Meldewegen und dem Umgang mit Doppelmeldungen zu berücksichtigen.[90]

Schließlich ist die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit bei der Erstellung von Leitlinien, Katalogen und ähnlichen untergesetzlichen Vorgaben zu beteiligen, um bei der Abwägung zwischen Informationssicherheit, klassischer Gefahrenabwehr und Strafverfolgung sowie Fernmeldegeheimnis und informationeller Selbstbestimmung mit dem Ziel mitwirken zu können, zu einer angemessen Berücksichtigung dieser Grundrechte beizutragen.[91] Bei der Erstellung des Sicherheitskataloges nach § 109 Abs. 6 TKG wird die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit schon einbezogen. Nach der Neufassung dieser Vorschrift ist mit ihr sogar ein Einvernehmen herzustellen.

(Prof. Dr. Alexander Roßnagel)

---

87 S. hierzu auch 5. e).

88 S. auch Eckardt, (Fn. 7), ZD 2014, 602f.

89 S. BT-Drs. 18/4096, 40.

90 S. hierzu Erwägungsgrund 31 des Entwurfs der NIS-RL; s. auch Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18. und 19. März 2015; Roos, (Fn. ##), MMR 2014, 727.

91 S. auch Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18. und 19. März 2015.

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)284 C

Freie Universität Berlin

Dept. Math. and Computer Science
Institute of Computer Science

Freie Universität Berlin, FB Mathematik und Informatik
Takustraße 9, 14195 Berlin, Germany

Deutscher Bundestag Innenausschuss
Herrn Ministerialrat Dr. Heynckes
Leiter Sekretariat PA 4
Platz der Republik 1
11011 Berlin

Computer Systems & Telematics
Prof. Dr.-Ing. Jochen H. Schiller
Takustraße 9
14195 Berlin

Telefon +49 30 838 75-213/-212
Fax +49 30 838 75194
E-Mail jochen.schiller@fu-berlin.de
Internet http://cst.mi.fu-berlin.de

Bearb.-Zeichen js
Bearbeiter Schiller

15. April 2015

Stellungnahme zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme / Drucksache 18/4096 vom 25.02.2015

Relativ leicht und schnell fallen heutzutage Begriffe wie *Industrie 4.0*, Cloud, Internet der Dinge, Smart Cities etc., wenn vom aktuellen Wandel in der IKT-Welt die Rede ist. Die Themenschwerpunkte großer Messen, wie CeBIT und Hannover Messe greifen dies auf und fügen natürlich auch die Sicherheit als Schwerpunkt mit hinzu. Alles soll mit allem vernetzt und dadurch auch „smarter“ werden.

Parallel dazu sind die Entwicklungen in Richtung *Gefahren 4.0* sichtbar, ohne dass man hier Schwarzmalerei betreiben muss. Dies umfasst nicht nur die viel zitierten und nur schwer quantifizierbaren Angriffe, sondern insbesondere auch schlichte Fehlkonfigurationen und Softwarefehler, die mehr und mehr auch auf Grund einer immer schwerer durchschaubaren Komplexität geschehen. Qualitativ neu ist hierbei, dass die Vielfalt vernetzter Systeme immer „einfacher“ angreifbar werden, da sie alle auf einer im Kern einheitlichen Technologie – der Internet-Kommunikationsprotokolle – beruhen. Diese Vereinheitlichung ist aber natürlich zeitgleich auch der große Vorteil – jetzt kann basierend auf der gleichen Technologie „alles mit allem“ kommunizieren und in komplett neue Bereiche einwirken – von der Gebäudesteuerung über Energienetze bis hin zum Fahrzeug.

Gleichzeitig betreiben wir aber vielleicht gerade einmal *Sicherheit 2.0*: Im Wesentlichen wird versucht, die gerade vernetzten Systeme mehr oder weniger gut voneinander abzuschotten und Lücken zu stopfen. Gesetzgebung und Regelungen hinken meist deutlich den technischen Entwicklungen hinterher und man sieht sich eher als Getriebener der Technologie denn als proaktiv Handelnden. Zurzeit kann man dies nicht gerade als eine sinnvolle, kontrollierte und beherrschte Entwicklung bezeichnen. Schließlich stellt sich auch die wichtige Frage, wo der Bürger in diesem ganzen Prozess bleibt, wie die IKT-Technologie zu seinem Nutzen gestaltet werden kann.

Exkurs

Ohne dass hier zu tief in die Technologie eingestiegen werden soll, ist es dennoch wichtig, dass grundlegende Eigenschaften der neuen Entwicklungen bekannt sind, damit so ein besseres Verständnis der Problematik erzeugt und Fehleinschätzungen vermieden werden können. Internet der Dinge, Industrie 4.0, Cloud-Techniken – sie alle basieren im Kern auf Internet-Technologien, wie dem *verbindungslosen* Internet-Protokoll IP oder auch *zustandslosen* Web Services. Diese einheitlichen „Sprachen", also die Kommunikationsprotokolle, ermöglichen die Vernetzung „von allem mit allem" und damit ist im Prinzip ein Durchgriff von allem auf alles möglich und machbar, aber sicher nicht immer erwünscht. Schon heute kann mit dem Smartphone der Zustand eines Kraftwerkes abgefragt werden, klare wirtschaftliche Vorteile und große Chancen für die deutsche Industrie zeichnen sich durch die nun mögliche hochflexible Produktion (Stichwort Losgröße 1) ab; die IT ist unverzichtbarer Bestandteil der Energiewende – ohne IT keine kleinteilige Energiegewinnung. IT steckt also in allem, vom Lichtschalter bis zur Kraftwerkssteuerung.

Leider bleibt es aber oft bei dieser schlagwortartigen Betrachtung, ohne zu verstehen was dahinter steckt. So sind die oft zitierten „smarten" Objekte, vom Leuchtmittel, Datenbrille, Handy, Lichtschalter, Umwälzpumpe, Bremsanlage, Notabschaltung über USB-Stick, Drucker, Fahrzeug bis hin zum Gebäude, Industrieanlage etc. immer mehr vollständige Computer mit Betriebssystem, Kommunikationssoftware etc. plus Zusatzhardware. Häufig finden sich schon komplette Webserver selbst auf den einfachsten vernetzten Gegenständen auf Grund der damit verbundenen einfacheren Konfigurierbarkeit. Damit „erben" sie automatisch alle Probleme, die wir vom „klassischen" PC kennen – von den Lücken und Anfälligkeiten gegenüber Angriffen, Viren, Trojaner etc. bis hin zu den regelmäßig notwendigen Softwareaktualisierungen.

Hinzu kommt, dass viele dieser „smarten Objekte" vergleichbar mit dem Smartphone immer kommunikationstechnisch mit dem Internet verbunden sind („always on"). Gerade das Smartphone zeigt schön die Problematik einer vereinfachten Denkweise: Viel wird über Angriffe auf Smartphones geschrieben, über die Sicherheit des Betriebssystems, der zu installierenden Apps – ohne jedoch weiter zu beachten, dass jedes Smartphone noch mindestens ein weiteres Betriebssystem auf dem Funkmodem besitzt, welches den direkten Funkkontakt mit der Umgebung unterhält und von keinen Schutzmechanismen welchen Betriebssystems auch immer geschützt wird. Diverse Angriffe auf dieses System sind bekannt – weitere Betriebssysteme finden sich auf dem SIM und ggf. weiteren Funkadaptern (WLAN, Bluetooth, GPS …), sogar auf den Speicherkarten.

Bereits bei dem heutigen größtenteils „klassischen" Internet, d.h. Geräte wie ein PC oder Smartphone, welche Dienste von Servern anfordern, wie Webseiten oder Cloud-Speicherplatz, stellt sich die Frage nach der Beherrschbarkeit der Komplexität. Niemand kann heute genau sagen, wo welche Daten entlanglaufen. Zwar ist die physische Infrastruktur bekannt und auch zuordenbar, weit schwieriger gestaltet sich dies bei der logischen Infrastruktur, welcher die Datenpakete folgen. So ist es heute ein Leichtes, Verkehrsströme umzuleiten oder, absichtlich oder ungewollt, Bereiche des Internets abzuschalten. Mögen manche dieser Probleme beim privaten „surfen" im Netz noch tolerierbar sein, so können sie sich katastrophal auswirken, wenn Notrufe

nicht mehr abgesetzt werden können (nach und nach werden alle Telefone in Deutschland nur noch mit Internet-Technologien kommunizieren), Industrieanlagen nicht mehr kontrollierbar sind oder Börsensysteme nicht mehr ordnungsgemäß funktionieren.

Gerade die eingebetteten Systeme, welche weit über 90% aller Computer ausmachen, müssen hier im besonderen Fokus stehen, steuern sie doch fast alles in unserem Alltag – von der Waschmaschine über das Überdruckventil in einer Raffinerie bis hin zum Beatmungsgerät. Man muss nicht gleich die „großen" Szenarien, wie ein Cyberwar oder die OK bemühen – einfache Konfigurationsfehler oder Angriffe auf weit entfernte Systeme können als Kettenreaktion Schäden verursachen, bei denen hinterher kaum noch feststellbar ist, wer eigentlicher Verursacher war.

Wird beispielsweise der smarte Backofen von einem eingebetteten System gesteuert, so verfügt er natürlich auch über einen Webserver, mit dessen Hilfe über diverse Webdienste der Zustand abgefragt, aber auch der Ofen programmiert werden kann. Natürlich können auch neue Backprogramme über das Internet mit Hilfe einer Smartphone-App auf den Backofen geladen werden. Auf Grund einer wie auch immer gearteten Lücke findet nun Schadsoftware ihren Weg in die Backofensteuerung, so dass beispielsweise die Temperaturabschaltung nicht mehr ordnungsgemäß funktioniert und ein Brandschaden entsteht. Es wird sich nun als sehr schwierig herausstellen, den Schuldigen für den Schaden zu finden, noch schwieriger, diesen in Haftung zu nehmen. Ist es der Backofenhersteller, welcher keine geeignete Firewall im Backofen hatte, nicht die aktuellsten Sicherheitsupdates automatisch installiert hat? Ist es der Nutzer, der seinen Backofen nicht aktualisiert hat? Ist es der Hersteller des Handys, der ermöglicht hat, dass Schadsoftware auf dem Handy die Steuerungsapp manipuliert hat? Ist es letztendlich der schwer greifbare Hacker, der entsprechende Software auf dem Handy installiert hat, dies aber nur konnte, weil der Betriebssystemhersteller des Handys Lücken in seinem Betriebssystem hat?

Wie soll dies alles letztendlich einem Bürger klar gemacht werden, dass man es hier mit einem Gemisch aus Gefährdungen zu tun hat, die einerseits einem TKG unterliegen (wenn es denn über die Telekommunikation zum Schaden kam) oder andererseits einem TMG, da es sich ja um einen Webservice handelt? Wie kann verständlich gemacht werden, dass viele Begrifflichkeiten (wie der der „Verbindung") aus dem TKG und die daraus abgeleiteten Möglichkeiten nicht immer wirklich zu der oft verbindungslosen Welt des Internets passen?[1] Der Bürger hat in diesem Beispiel den Schaden – richtig verantwortlich ist niemand, da die Vernetzung eine neue, noch nicht wirklich beherrschte Komplexität eingeführt hat, bei der insbesondere auch die Gesetzeslage nicht hinterherkommt.

[1] Ein drastisches Beispiel von „technologisch veraltetem Gesetz" ist sicherlich §108 TKG, welcher in der Quintessenz unter anderem verhindert, dass clevere Notruf-Apps für Smartphones unter der Nutzung von Internet-Telefonie eingesetzt werden dürfen, da bei Notrufen zu 110/112 stets eine „Verbindung" vorausgesetzt wird und somit das verbindungslose Internetprotokoll ausgeschlossen ist. Apps für „Stille Notrufe", eine bessere Unterstützung Behinderter etc. werden damit erschwert.

Selbstverständlich wird man den Backofen nicht als Kritische Infrastruktur im Sinne des Gesetzesentwurfs sehen, sondern dies sollte nur ein einfaches, zur heutigen IT in Kritischen Infrastrukturen analoges Beispiel sein. Die Darstellung der IT in Kritischen Infrastrukturen würde den Rahmen der Stellungnahme sprengen, aber analog könnten Beispiele aus dem Bereich Banken, Industrie, Logistik – der gesamten Kritischen Infrastrukturen – herangezogen werden. Entsprechende Schilderungen von Vorfällen finden sich auch im BSI-Bericht zur Lage der IT-Sicherheit in Deutschland 2014.

Generelles zum IT-Sicherheitsgesetz

Bevor auf einige Gesichtspunkte des Gesetzesentwurfs eingegangen wird, muss festgehalten werden, dass dieses Gesetz ein absolut notwendiger, wenngleich sicherlich nicht der letzte Schritt in die richtige Richtung ist. Notwendig ist dieser Schritt, da es längst mehr als überfällig ist, dass zumindest gefordert wird den „Stand der Technik" bei allen hier Addressierten einzuhalten[2]. Auch wenn dieser Mindeststandard der aus dem letzten Jahrhundert aus Sicht der Wissenschaft ist, so ist dies doch bei Weitem besser, als der fahrlässige Umgang mit dem Thema Sicherheit, wie wir es heute leider an vielen Stellen feststellen müssen. Grundsätzlich positiv ist auch die Meldepflicht für Sicherheitsvorfälle, auch in der abgestuften Form (anonym bzw. mit Nennung je nach Schwere des Vorfalls).

Das Gesetz ist sicherlich nicht vollumfassend und abschließend, kann dies aber auch nie wirklich sein. Sicherheit ist ein dynamischer Prozess und so muss stets die aktuelle Situation überprüft, müssen Regelungen angepasst und ggf. auch Gesetze geändert werden. Wichtig ist nun, dass mit diesem Gesetz – so unvollständig es an manchen Stellen noch sein mag – ein deutlicher Bewusstseinswandel bei allen Betroffenen angestoßen wird. IT-Sicherheit ist nicht (nur) das *update* auf dem heimischen Rechner, sondern ein Prozess, der Technik, Anwendungen, Nutzung und auch ganz wesentlich die Aus- und Weiterbildung umfasst. Auch wenn dies in dem vorliegenden ersten Schritt im Wesentlichen auf die Betreiber Kritischer Infrastrukturen beschränkt ist – eigentlich sollte Sicherheit alles und alle umfassen – so ist dies doch ein wichtiger Anfang.

Es kann hier nicht sein, dass weitere Jahre zunächst analysiert wird, wer und was exakt unter den Begriff Kritischer Infrastrukturen fällt – dies ändert sich permanent und muss daher laufend unter Einbeziehung aller Akteure angepasst werden (daher ist auch das Instrument einer Rechtsverordnung das flexiblere). Beispielsweise sind Elektrofahrzeuge heute noch keine Kritische Infrastruktur, wenn jedoch ein relativ hoher Prozentsatz dieser Fahrzeuge solche mit Verbren-

[2] Falls aus juristischer Sicht der Begriff „berücksichtigen" in § 8a (1) BSIG-E nicht wirklich „einhalten" bedeutet, wie z.B. auch auf S. 31, letzter Absatz, des Entwurfs in der Begründung ausgeführt, so ist der Begriff „berücksichtigen" durch „einhalten" zu ersetzen um hier eine Eindeutigkeit zu erzielen – ansonsten ist von der Idee her das gesamte Gesetz aus technischer Sicht hinfällig, denn es geht ja gerade darum, verpflichtend zumindest Mindeststandards in allen hier adressierten IT-Systemen zu erreichen

nungsmotoren verdrängt hat und gleichzeitig die Elektrofahrzeuge auch zur Energiezwischenspeicherung in einem smarten Energieversorgungskonzept genutzt werden, dann kann die Situation ganz anders aussehen.

Wichtig ist jedoch, dass das Gesetz dem „Vernetztheitscharakter“ der Sicherheit gerecht wird. Auf der technischen Ebene, den Ebenen der Kommunikationsprotokolle, spricht mehr und mehr „alles mit allem“, wie weiter oben aufgezeigt. Auf der Ebene der Anwendungen ergeben sich damit domänenübergreifend neue, vielversprechende Anwendungen. Passend dazu müssen aber auch alle öffentlichen, behördlichen oder branchenübergreifenden Prozesse „vernetzt“ gedacht werden. Dies bedeutet aber auch, dass hier klassische Abgrenzungen in z.B. Bund, Länder Kommunen oder auch Medien vs. Kommunikation neu gedacht und ggf. angepasst werden müssen.

Haftung und Sanktionierungsmöglichkeiten

Parallel zur Ausgestaltung des IT-Sicherheitsgesetzes muss sicherlich auch die Anpassung der gesetzlichen Regelungen zur Haftung bei Schäden angegangen werden. Wenn die im Entwurf gesetzten Mindeststandards, also der Stand der Technik, nicht erfüllt waren und ein Schaden entstanden ist, so ist auch folgerichtig, dass der (Mit-)Verursacher hierfür (mit-)haftet. Aus technischer Sicht ist es auf jeden Fall fahrlässig, den seit langem bekannten Stand der Technik nicht einzuhalten (und wesentliche Mehraufwände basierend auf dem IT-Sicherheitsgesetz haben vorrangig diejenigen, welche bisher den Mindeststandard nicht erfüllt haben).

Gerade im Bereich der Software- wie Hardware-Entwicklung und auch dem Betrieb von IT-Systemen ist seit langem bekannt, wie Systeme zu entwickeln und zu betreiben sind, welche Richtlinien eingehalten werden müssen. Typische Beispiele aus dem IT-Bereich sind die ISO/IEC 27000-Reihe oder der IT-Grundschutz nach BSI. Diese könnten auch Basis der in § 8a (3) BSIG-E geforderten Nachweise sein.

In vielen Bereichen, wie z.B. dem Flugzeugbau, wird strikt auf die Einhaltung von Sicherheitsrichtlinien geachtet – leider nicht überall, so dass sich sowohl in proprietären, abgeschlossenen Systemen (z.B. in diversen SCADA-Systemen), als auch in open source Produkten (z.B. Heartbleed/openSSL) immer wieder leicht vermeidbare Fehler finden – leider meist erst, wenn sie bereits Schäden verursacht haben und ausgenutzt wurden. Ungeprüfte Übernahme von Software, mangelhafte Verschlüsselungsverfahren oder auch die Vernetzung bisher unvernetzter Systeme ohne eine Überprüfung auf die damit ggf. verbundenen Einfallstore entsprechen nicht dem Stand der Technik.

Es ist aber auch klar, dass es hierbei Grenzen der Zumutbarkeit hinsichtlich der Überprüfung gibt. So kann letztendlich ein Dienstanbieter nicht bis ins kleinste Detail wissen, welche Komponenten z.B. in der Hardware zum Einsatz kommen, die er selbst nutzt. Daraus kann aber im Umkehrschluss nicht gefolgert werden, dass hierfür keinerlei Verantwortung vorliegt. In der klassischen, analogen Welt kann der Nutzer auch davon ausgehen, dass der Anbieter eines Dienstes

oder Produktes die Funktion desselben gewährleistet. Dies gilt auch dann, wenn eine Teilkomponente für eine Störung verantwortlich ist, welche gar nicht im direkten Einflussbereich des Dienstanbieters oder Produzenten liegt. Beispiele hierfür wären die Elektronik eines Automobils, welche meist von Zulieferern kommt, bei deren Fehlfunktion ein Kunde sich jedoch an den Autohersteller wendet. Analog haftet die Bahn als Dienstleister bei Verspätungen auch dann, wenn z.B. der Grund ein von ihr gar nicht selbst gefertigtes Antriebsaggregat war. Es ist Aufgabe des Dienstleisters bzw. Produzenten durch entsprechende Verträge mit den Zulieferern auf diese zurückgreifen zu können – damit propagiert sich auch das anfangs erwähnte IT-Sicherheitsbewusstsein in Richtung der IT-Hersteller. Letztendlich kann es für einen Nutzer eines Dienstes oder Produktes nur eine Schnittstelle für den Dienst, für die Verantwortung, für die Haftung geben und kein Weiterleiten der Zuständigkeiten.

Natürlich kann ein IT-Dienstanbieter nicht generell z.B. für Störungen bei Nutzern ausgelöst durch von ihm übertragene Inhalte haftbar gemacht werden. Es gibt aber sicherlich dann eine Mithaftung, wenn diese Inhalte insbesondere deswegen eine Störung auslösen konnte, weil der Dienstanbieter im Vorfeld keine dem Stand der Technik folgenden Sicherheitsmaßnahmen ergriffen hat und somit z.B. bereits bekannte Lücken zum Schaden eines Nutzers ausgenutzt werden konnten.

Ein weiterer offener Punkt der aktuellen Vorlage ist sicherlich das Fehlen weitergehender Sanktionierungsmöglichkeiten. Sicherlich würde die notwendige Bewusstseinsänderung hinsichtlich der IT-Sicherheit durch erweiterte Haftungsmöglichkeiten bzw. Bußgelder unterstützt, ebenso durch die namentliche Nennung von z.B. Betreibern Kritischer Infrastrukturen bei erheblichen Störungen. Wichtig wäre jedoch, dass §8a BSIG-E auch tatsächlich umgesetzt wird. Ob ein reines „Verlangen“ der Beseitigung von Sicherheitsmängeln ausreichen wird ist mehr als fraglich.

Rolle des BSI

Die vorgesehene Stärkung des BSI ist auf jeden Fall zu begrüßen, auch der Wandel zu einer „nationalen Informationssicherheitsbehörde“ ist nur folgerichtig. Trotz mehr oder weniger berechtigter Kritik am BSI und seiner bisherigen Konstruktion ist diese Einrichtung inzwischen einer *der* Ansprechpartner national wie auch international bei IT-Sicherheitsfragen von Bürgern, Verwaltungen und auch Unternehmen (wenngleich bei letzteren deutlich zögerlicher bis hin zu Überlegungen der Industrie zu weiteren eigenen IT-Sicherheitseinrichtungen). Es ist daher auch konsequent, dass das BSI von neutraler Warte aus IT-Produkte auf deren Sicherheitsniveau überprüft und auch überwacht, dass „branchenspezifische Sicherheitsstandards“ nicht hinter den Stand der Technik zurückfallen – dieser ist ein Mindeststandard und sollte nicht aufgeweicht werden.

Zu hinterfragen ist allerdings die Konstruktion des BSI als eine Behörde innerhalb eines Ministeriums. Ein sichtbares Zeichen für eine umfassende Stärkung der IT-Sicherheit ist eine neutrale, unabhängige Einrichtung mit der entsprechenden Ausstattung. Sicherheitsfragen und -vorfälle sind weder ressortgebunden noch berücksichtigen sie gesetzgeberische Grenzen oder föderale

Strukturen. Hier wäre eine zentrale Anlaufstelle mit den entsprechenden Kompetenzen wünschenswert, welche die im IT-Sicherheitsgesetz geforderten Mindeststandards dann auch wirklich überall durchsetzen kann.

Zur Unterstützung dieser Rolle sind außer der (relativen) Unabhängigkeit weitere Komponenten relevant: passende Gehaltsstrukturen, um wirklich attraktiv für IT-Fachkräfte zu sein, noch weitergehende Kooperation mit Forschungseinrichtungen, um auf das dort vorhandene Wissen zurückzugreifen, und auch das vermehrte Einbringen BSI-relevanter Fragestellungen z.B. in Forschungsprogramme des BMBF, so dass hier in einer gemeinsamen Anstrengung die IT-Sicherheit verbessert werden kann. Hier gibt es zwar schon viele Ansätze, aber noch viel zu oft landen gute Ideen in Abschlussberichten statt in relevanten Anwendungen.

Rolle der KMUs

Es ist sicherlich richtig in einem ersten Wurf des IT-Sicherheitsgesetzes KMUs/Kleinstunternehmen zunächst von §8a BSIG-E auszuklammern. Der Schwerpunkt liegt hier klar auf den „klassischen“ Kritischen Infrastrukturen betrieben von größeren Unternehmen. Dies bedeutet jedoch aus technischer Sicht keineswegs, dass es nicht auch sinnvoll wäre, gerade kleinere Unternehmen in einem ersten Schritt explizit in den Informationsfluss über IT-Sicherheitslücken und Vorfälle zu integrieren und in einem späteren Schritt ähnliche Maßstäbe wie §8a BSIG-E anzulegen. Der Hintergrund ist einfach und wurde auch z.B. in der BMBF-Förderung zur Sicherheitsforschung erkannt (Bekanntmachung vom 5.8.2013): Weit über 75% der Angriffe im Cyberspace richten sich derzeit gegen KMUs, diese sind meist deutlich schlechter auf Angriffe vorbereitet – und können dennoch selbst im Hinblick auf Kritische Infrastrukturen relevant sein.

Es wird oft argumentiert, dass z.B. der Ausfall eines kleinen Betreibers einer nur „lokal kritischen“ Infrastruktur, z.B. ein lokaler Wasserversorger, keine größeren Auswirkungen hat. Es wird dabei aber vernachlässigt, dass beispielsweise sehr viele Wasserversorger ähnliche wenn nicht sogar identische Steuerungssysteme nutzen. Eine gezielt ausgenutzte Schwachstelle in diesen Systemen kann damit eine große Anzahl dieser „kleinen Betreiber“ stören und so in der Gesamtheit sehr wohl eine erhebliche Störung im Sinne des Gesetzes verursachen. Aus diesem Grund ist es unabdingbar, dass sich die o.g. Bewusstseinsänderung gerade auch in Richtung der KMUs fortsetzt und in einem weiteren Schritt das Gesetz entsprechend angepasst wird.

Vernetzung auf allen Ebenen

Wie eingangs erwähnt und auch auf allen aktuellen Veranstaltungen durch viele Redner immer wieder betont, ist der aktuelle Trend der zur Vernetzung von „allem mit allem“. Auch wenn für spezielle Zwecke sicherlich noch getrennte Netze verfügbar sind, so werden selbst für BOS-Netze Architekturen mit Nutzung kommerzieller Netze angedacht, laufen sicherheitskritische öffentliche Anwendungen (verschlüsselt) über kommerzielle Netze und greifen vielfältig Behörden auf zahlreiche Dienste im Internet zu.

Wenn also auf der technischen Ebene „alles mit allem“ nach und nach vernetzt wird und daher auch die entsprechenden Sicherheitsproblematiken alle vernetzten Systeme betreffen, dann ist es nicht konsequent und unter Umständen sogar gefährlich, wenn Teilbereiche der Verwaltungen oder Sektoren, wie Kultur und Medien, ausgeklammert werden. Sicherlich gibt es hier, wie S. 38 des Gesetzentwurfs auch erwähnt, gesonderte Regelungen bzw. Grenzen der Gesetzgebungskompetenz des Bundes, jedoch werden sich Sicherheitsvorfälle, Fehlkonfigurationen und Angriffe nicht an diese Abgrenzungen halten sondern unter Umständen in den hier nicht erfassten Bereichen ausbrechen und dann doch eine Kritische Infrastruktur bundesweit betreffen.

Hier muss nach und nach ein ganzheitlicher Ansatz im Sinne der „Vernetzten Sicherheit“ geschaffen werden, so dass das hier gestartete IT-Sicherheitsbewusstsein auch in alle Bereiche vordringen kann. Dass hier Nachholbedarf besteht sieht man am teilweise leichtfertigen Umgang mit sicherheitsrelevanten Daten in Cloud-Diensten, dem Nutzen ungesicherter privater Smartphones für dienstliche Zwecke oder dem Glauben, dass ein IT-System sicher sei, wenn die Kommunikationsstrecken verschlüsselt betrieben werden etc.

Rolle von TKG und TMG

Im Rahmen der Diskussionen zum IT-Sicherheitsgesetz werden als betroffene Bereiche z.B. Betreiber von Webseiten, Telekommunikationsunternehmen, Industrie 4.0, Cloud-Technologie etc. in einem Atemzug genannt, ohne wirklich zu bedenken, was es heißt, dass hier je nach Beispiel unterschiedliche Gesetze zur Anwendung kommen. Hinzu kommt, dass insbesondere das TKG noch von der „klassischen Denkweise“ des analogen Telefonnetzes mit verbindungsorientierter Übertragung geprägt ist.

Wie bereits erwähnt, finden sich Webserver – in abgespeckten Versionen – heute auf den kleinsten eingebetteten Systemen bis hin zu per SmartphoneApp steuerbaren Leuchten, aber auch in mehr und mehr industriellen Steuerungssystemen. Webserver bieten ihre Web-Dienste oft mit Hilfe einfacher Standardbefehlen an, die verbindungslos an den Server gerichtet werden können – insbesondere muss keine klassische „Telekommunikationsverbindung“ im Sinne des TKG aufgebaut werden. Diese Web-Dienste bzw. deren Anbieter fallen unter das TMG. Gerade aber industrielle Steuerungssysteme kritischer Infrastrukturen können Ziel eines Angriffs sein – nach TMG gibt es aber keine mit dem TKG vergleichbaren Instrumente um erforderliche Daten für eine Angriffserkennung zu erheben. Das TMG geht von Nutzern eines Web-Dienstes im Sinne z.B. eines Web-Surfers aus. Es wurde dabei nicht bedacht, dass technisch identische Verfahren zum Angriff genutzt werden können – es ist lediglich eine andere Ebene, als die vom TKG erfasste „technische“ Kommunikation. Diese Denkweise findet sich auch z.B. in der Begriffsdefinition § 3 Nr. 25 TKG „telekommunikationsgestützte Dienste“, welche verlangen, dass „die Inhaltsleistung noch während der Telekommunikationsverbindung erfüllt wird“.

Finden also Angriffe auf Kritische Infrastrukturen im Geltungsbereich des TMG statt, so hat der Angegriffene rechtlich keinerlei Möglichkeiten analog zu § 100 TKG Daten aufzuzeichnen, welche die Störung erkennen lassen und dann ggf. Maßnahmen einleiten. Hier müsste zumindest eine konsistente Regelung in TMG und TKG geschaffen werden bzw. noch besser die Gesetze

derart neugestaltet werden, dass nicht mehr zeitgemäße technische Begriffe (wie „Verbindung“ im Sinne des TKG) durch Funktionen und Leistungsmerkmale beschrieben werden. Für einen Nutzer bzw. Betreiber von Diensten ist es letztendlich irrelevant, ob der Dienst auf einer Verbindung beruht, verbindungslos angeboten wird, ein Web-Dienst ist etc. – aus Sicherheitssicht sollte alles gleich behandelt werden.

Eine schnelle Anpassung wäre die (erneute) *Angleichung* von §15 TMG an §100 TKG-E. Die im IT-Sicherheitsgesetz derzeit vorgesehenen Änderungen des TMG haben eher den klassischen Web-Surfer als Nutzer von Web-Diensten im Sinn, weniger die o.g. Industriesteuerungssysteme. Bleibt es bei diesem Stand verbietet sich die Nutzung zahlreicher Analysesysteme z.B. zur Erkennung von ausgefeilteren, mehrschrittigen Angriffen, welche sich über einen längeren Zeitraum hinziehen können. Ebenso wird eine nachträgliche Analyse von Schäden schwer ohne die dafür notwendige vorab gespeicherte Datenbasis möglich sein.

Störungen und Datensammlung

Störungen, hervorgerufen durch z.B. Softwarefehler, Angriffe oder Fehlkonfigurationen, sind in heutigen Internet-basierten Kommunikationsnetzen und ihren Diensten etwas grundlegend anderes, als sie dies in klassischen Telekommunikationsnetzen waren. In klassischen Netzen hat eine Störung meist zeitnah direkt etwas bewirkt, beispielsweise eine Funktionsstörung hervorgerufen. In heutigen Netzen können z.B. Angriffe lange im Voraus vorbereitet und Schadsoftware in Systemen hinterlegt werden, ohne dass dadurch bereits eine Störung hervorgerufen wird. Es reicht dann ein kleiner, als solcher kaum erkennbarer Befehl, um die Störung hervorzurufen. Ebenso kann beispielsweise eine schlechte Systemkonfiguration oder ein nur unzureichend abgesichertes System jahrelang problemlos funktionieren, bis sich die Umgebungsparameter ändern – z.B. das System mit dem Internet verbunden wird. Typische Beispiele sind hierfür Industriesteuerungssysteme, welche auch heute noch häufig aus Gründen der vereinfachten Wartung mit fest voreingestellten Passwörtern versehen sind (oft auf Kundenwunsch!), und schlagartig angreifbar werden, sobald sie nicht mehr losgelöst sondern vernetzt arbeiten.

Wie schon mehrfach erwähnt, ist die Kommunikationswelt schon heute stark von eingebetteten Systemen geprägt, die Maschine-zu-Maschine-Kommunikation wird immer dominanter; schon heute kommunizieren mehr Dinge als Menschen im Internet. Gerade im Hinblick auf Kritische Infrastrukturen muss daher ein besonderes Augenmerk auf Störungen in diesen Systemen gelegt werden.

Um wirksam die Sicherheit von IT-Systemen zu erhöhen kann nicht erst dann gehandelt werden, wenn tatsächlich eine Funktionsstörung aufgetreten ist. Im Vorfeld müssen bereits zahlreiche Maßnahmen ergriffen werden, um ein möglichst gutes Lagebild zu erhalten. Dies kann von relativ einfachen Maßnahmen, wie der Erfassung des Umsetzungsgrades von Maßnahmen des IT-Grundschutzes bis hin zu detaillierten Verkehrsanalysen gehen. Gerade die „schlummernden“ Bedrohungen, von Vorbereitungen zu Angriffen via Bot-Netze bis hin zu mangelhaften Konfigurationen und alten Softwareständen, sind wesentlich im Hinblick auf die Vulnerabilität Kritischer Infrastrukturen. Es ist dabei auch wichtig, dass ein solches Lagebild auch möglichst viele Systeme

im Sinne einer vernetzten Sicherheit erfasst. Es ist bei weitem nicht so wirksam, wenn je nach Sektoren, Branchen, Behörden etc. getrennte Lagebilder erstellt werden. Gerade Störungen im IT-Bereich können sehr schnell viele Bereiche erfassen, beispielsweise wenn Schwachstellen in Systemen auftreten, welche fast überall genutzt werden (z.B. Router eines Herstellers).

Wie schon zuvor erwähnt, sind TKG und TMG hier gleichermaßen hinsichtlich Störungen zu betrachten. Es ist aus Sicht der Technik nicht sinnvoll im Rahmen des TMG lediglich einen Schutz vor gewissen Störungen vorzuschreiben, basierend auf dem TKG jedoch weitergehende Möglichkeiten der Datensammlung vorzusehen.

Datensammlung zur Erkennung von Störungen, auch von solchen, welche erst in der Zukunft dann beispielsweise zu Funktionsausfällen führen können (i.S.v. §100 Abs. 1 TKG-E) muss aus technischer Sicht nicht notwendigerweise das anlasslose Sammeln aller Daten inklusive der Analyse aller Inhalte der Datenpakete umfassen. Sicherlich mag es Fälle geben, in denen man – meist im Nachhinein – anhand von umfangreichen (selten vollständigen) Datensammlungen bestimmten Angriffsmustern auf die Spur kommen kann. Sinnvoll, angemessen und auch wirtschaftlich vertretbar sind aber meist mehrstufige Verfahren, welche in einem ersten Schritt z.B. Anomalien im Datenstrom erkennen können, ohne alle Daten zu sammeln. Im Verdachtsfall kann dann im nächsten Schritt ein Verfahren folgen, welches „genauer hinschaut“ (also z.B. Paketinhalte überprüft). Bei vielen Verfahren genügt es dabei vollkommen, auf pseudonymisierten Daten, auf aggregierten Daten oder lediglich auf Statistiken und Stichproben zu arbeiten. Gerade bei großangelegten, verteilten Angriffen spielen die Daten eines Einzelnen eine untergeordnete Rolle – wichtiger sind hier z.B. die Strukturen der Datenverteilung.

Zusammenfassung

Die IT-Sicherheit in vielen Bereichen bleibt heutzutage meist weiter hinter dem Möglichen zurück, auch immer noch weit hinter dem im Gesetzesentwurf immer wieder zitierten Stand der Technik. Derzeit gültige Regelungen, wie das TKG oder das TMG sind nicht wirklich an die Anfordernisse der IKT-Systeme und deren Nutzer angepasst. Der jetzt vorliegende Entwurf eines IT-Sicherheitsgesetzes ist ein notwendiger und wichtiger erster Schritt in die richtige Richtung (wenn denn die Mindeststandards auch wirklich von allen hier Adressierten *einzuhalten* sind), der nicht dadurch ausgebremst werden darf, dass sicherlich noch nicht alle relevanten Szenarien abgedeckt oder Teilkonstrukte aus technischer Sicht nicht ideal sind. IT-Sicherheit ist ein dynamischer Prozess und kann schon deshalb nicht in ein statisches Gesetz in seiner Gänze gegossen werden. Das IT-Sicherheitsgesetz kann zu einem Startschuss für eine Bewusstseinsänderung hinsichtlich einer IT-Sicherheitskultur werden, die dann nach und nach möglichst alle Bereiche der IT durchdringt. Die Konzentration auf gewisse Bereiche, die Kritischen Infrastrukturen, erscheint logisch, damit es zumindest einmal losgehen kann.

Gewisse Aspekte könnten jetzt noch in das Gesetz einfließen, ohne zu einer wesentlichen Verzögerung beizutragen. Begleitend zu den Forderungen des IT-Sicherheitsgesetzes müssen Haftungsfragen (z.B. Produkthaftung) an die heutigen Gegebenheiten angepasst werden. Ebenso muss klar sein, welche Konsequenzen ein Nichtbefolgen des IT-Sicherheitsgesetzes nach sich

zieht. Weiterhin ist unabdingbar, dass TKG und TMG konsistent gemacht werden, denn es gibt aus Sicht der Technologie und der Angriffsmöglichkeiten keinen Grund für eine differenzierte Betrachtung.

Weitere Schritte im Rahmen eines IT-Sicherheitsgesetzes wären zur Steigerung der Akzeptanz des BSI das Überdenken dessen Konstruktion in Richtung einer unabhängigeren Einrichtung, die genauere Betrachtung von KMUs und das Überwinden von gesetzlich definierten Barrieren (z.B. Verhältnis Bund/Land/Kommune), die Sicherheitsvorfälle so nicht kennen, im Sinne einer vernetzten Sicherheit zum Wohle der Bürger.

Univ.-Prof. Dr.-Ing. habil. Jochen H. Schiller

Bundesamt
für Sicherheit in der
Informationstechnik

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)284 D

Stellungnahme für die Anhörung des Innenausschusses
zum Gesetzentwurf der Bundesregierung

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

am 20. April 2015

Michael Hange
Präsident des Bundesamtes für Sicherheit in der Informationstechnik

1. Ausgangslage und Herausforderungen

Die millionenfachen Identitätsdiebstähle von Bürgern, Meldungen zu Cyber-Angriffen auf Wirtschaftsunternehmen und nicht zuletzt die Snowden-Enthüllungen haben weit über die Expertenebene hinaus das Bewusstsein der Verletzbarkeit im Cyber-Raum deutlich gemacht. Insbesondere wird deutlich, dass alle Gesellschaftsgruppen hiervon betroffen sind.

Um zu verstehen, welchen Herausforderungen wir gegenüberstehen, ist es wichtig zu wissen, welche Rolle die Informationstechnik (IT) heutzutage spielt:

1. Während IT bis vor wenigen Jahren von den zur Produktion eingesetzten Maschinen klar abgrenzbar war, durchdringt sie heute alles. Sie findet sich gleichermaßen in allen möglichen Haushaltsgegenständen wie auch in industriellen Prozessen und Anlagen wieder - sie ist allgegenwärtig.
2. Daneben geht der Trend dahin, alle IT-Systeme zu vernetzen, um Komfort- oder Produktivitätsgewinne zu erzielen. Es wird das Ziel verfolgt, möglichst viele Informationen nutzbar zu machen. So werden beispielsweise die „digital-ertüchtigten“ Systeme eines Unternehmens wie etwa Maschinen, Sensoren und Feldgeräte in den Produktionsanlagen, aber auch Systeme in Marketing, Vertrieb oder Einkauf untereinander sowie nach innen und außen vernetzt.
3. Unter dem Stichwort Internet der Dinge sind bereits heute viele Hausgeräte, Gebäudesteuerungen, Gefahren- und Brandmeldeanlagen, Verkehrsleitsysteme und Automobile mit dem Internet verbunden.

   Die Vision ist im urbanen Bereich mit „Smart City“ und im häuslichen Bereich mit „Smart Home“ bereits gegenwärtig und greifbar. Die Digitalisierung von ursprünglich physischen Systemen führt zu einem Anstieg der Komplexität dieser Systeme und damit zugleich zu größeren Herausforderungen bei der Sicherheit. Während beispielsweise bisher im Bereich der Stromversorgung primär elektrotechnische Aspekte eine Rolle spielten, kommen bei intelligenten Energienetzen die Fragen

der Zuverlässigkeit von IT hinzu. Eine intelligente Netzsteuerung ist nicht nur auf die elektrische Funktionsfähigkeit der Netze angewiesen, sondern ebenso auf die Integrität und Verfügbarkeit der zur Netzsteuerung notwendigen Daten(verarbeitung).

2. Gefährdungslage

Neben dem Wissen über Technologie und Technologieentwicklung ist das Kennen der Gefährdungslage unerlässlich. Denn technologische Entwicklung und Gefährdungslage sind im Zusammenhang zu betrachten.

Das BSI hat im Dezember 2014 erstmals einen Bericht zur Lage der IT-Sicherheit in Deutschland[1] herausgegeben, der Auskunft über die Ursachen von Cyber-Angriffen, über Angriffsmittel und -methoden gibt. Eine wesentliche Schlussfolgerung ist: Das Internet ist als Plattform für Angreifer sehr attraktiv, denn der Aufwand für einen Angriff ist gering. Es reichen ein Laptop und ein Internetanschluss. Zudem existiert ein florierender globaler Markt mit „Trojanerkoffern“ und Maleware-as-a-Service-Angeboten. Das Entdeckungsrisiko ist gering, da das dezentral und offen gestaltete Internet für den Angreifer vielfältige Tarnmöglichkeiten bietet. Außerdem erweitert sich die Zahl der möglichen Angriffsziele mit der fortlaufenden technologischen Weiterentwicklung. Ein weiterer Grund für die Attraktivität des Internets als Angriffsplattform ist die Tatsache, dass Schwachstellen in komplexer Software systemimmanent sind. Sie sind der häufigste Ausgangspunkt für die Entwicklung von Cyber-Angriffsmitteln in Form von Schadprogrammen.

Die wesentlichen Fakten der Bedrohungslage im Jahr 2014 stellen sich wie folgt dar:

Schadprogramme

Die Gesamtzahl der detektierten PC-basierten Schwachstellen liegt bei mehr als 250 Millionen und steigt täglich um ca. 300.000. Sie betreffen primär das führende Desktop-Betriebssystem. Dieses wird jedoch nicht nur auf Arbeitsplatzsystemen eingesetzt, sondern ebenso auf Serversystemen und in industriellen Steuerungsanlagen –

1 Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2014.

teilweise noch mit einem seit Jahren veralteten Softwarestand, dessen Schwachstellen durch Updates nicht mehr beseitigt werden.

Die Anzahl der Schadprogramme für Smartphones und Tablets liegt bei mindestens drei Millionen, hiervon sind ca. 98 Prozent dem führenden Betriebssystem zuzuordnen.

Botnetze

In Deutschland sind mehr als eine Millionen Internetrechner Teil von Botnetzen. Die Nachlässigkeit der Nutzer beim Einspielen von Patches gegen Schwachstellen begünstigt die Chancen der Angreifer, die Rechner entsprechend zu übernehmen.

DDoS

In 2014 gab es allein in Deutschland über 32.000 DDoS-Angriffe. Zu ca. einem Drittel waren die Web-Seiten von Unternehmen Ziel der DDoS-Angriffe. Zu ca. einem Viertel war mit gravierender Wirkung die Netzinfrastruktur von DDoS-Angriffen betroffen. Zur Durchführung der Angriffe missbrauchten die Täter auch viele falsch konfigurierte Serversysteme unwissender Anwender.

APT

Neben den bekannten und weit verbreiteten Angriffsmethoden wie beispielsweise Spam, Schadsoftware oder Drive-by-Exploits, sind die sogenannten Advanced Persistent Threats (APT) von besonderer Bedeutung. Sie sind die hochwertigen komplexen Angriffe, die schwer detektierbar sind und möglichst dauerhaft Wirkung entfalten sollen. APT-Angriffe zeichnen sich durch sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten aufseiten der Angreifer aus. Problematisch ist, dass klassische Antivirenprogramme eine immer geringer werdende Erkennungsrate insbesondere bei hochwertigen Angriffen haben.

3. Handlungsbedarf

Die technologische Entwicklungen und die damit einhergehenden Risiken sind inzwischen nicht nur eine technologische und organisatorische, sondern auch eine

gesellschaftspolitische Herausforderung. Für die Bundesverwaltung hat der Gesetzgeber bereits 2009 wichtige Voraussetzungen geschaffen, um den Bedrohungen für die Bundesverwaltung adäquat zu begegnen und der zunehmenden Bedeutung der Informations- und Kommunikationstechnik in der Verwaltung Rechnung zu tragen. Die Meldepflicht der Behörden gegenüber dem BSI sowie die auf der Grundlage von § 5 BSIG vorgenommenen Maßnahmen zur Erkennung und Abwehr von Gefahren für die Kommunikationstechnik des Bundes haben bereits zu einer signifikanten Steigerung der IT-Sicherheit in der Bundesverwaltung beigetragen.

Die steigende Abhängigkeit der Wirtschaft von IT-Prozessen verlangt auch ihr Maßnahmen ab. Bereits heute bestehen vielfältige Kooperationen zwischen Unternehmen und Staat, um die IT-Sicherheit zu fördern. So sind z.B. die Allianz für Cyber-Sicherheit und der Umsetzungsplan KRITIS (UP KRITIS) Plattformen der Zusammenarbeit, in denen auf freiwilliger Basis relevante Informationen, Erfahrungen und Know-How zwischen Staat und Wirtschaft ausgetauscht werden.

Die technologischen Entwicklungen einerseits und die damit einhergehende, weitreichende Bedrohungslage andererseits zeigen jedoch, dass ein regulativer Rahmen für die Zusammenarbeit erforderlich ist. Dies gilt insbesondere für die Wirtschaftsakteure, die wegen der möglichen weitreichenden gesellschaftlichen Folgen eines Ausfalls oder einer Beeinträchtigung der von ihnen angebotenen Leistungen eine besondere Verantwortung für das Gemeinwohl tragen. Dieses Erfordernis wird in § 8a bis § 8d des Gesetzentwurfs aufgegriffen. Betreiber Kritischer Infrastrukturen werden nach § 8a verpflichtet, ein Mindestniveau an IT-Sicherheit für die Systeme, Komponenten und Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Durch die Berücksichtigung des Standes der Technik ist sichergestellt, dass zum einen die zu ergreifenden Maßnahmen für die Betreiber verhältnismäßig bleiben, zum anderen aber auch der Einsatz von hinreichend aktuellen Systemen vorgeschrieben wird. Die Branchen haben die Möglichkeit, durch branchenspezifische Sicherheitsstandards den Stand der Technik zu konkretisieren.

Dadurch kann zum einen das branchenspezifische Know-How der Betreiber einbezogen werden; nur diese kennen die zur Erbringung der Dienstleistungen eingesetzten Techniken und Prozesse im Detail. Zum anderen wird den Betreibern die alle zwei Jahre erforderliche Nachweisführung, dass der Stand der Technik eingehalten ist, durch einen anerkannten Branchenstandard vereinfacht.

Daneben ermöglicht die in § 8b verankerte Meldepflicht für Betreiber Kritischer Infrastrukturen dem BSI nicht nur die Erstellung verlässlicher Lagebilder. Insbesondere erwarte ich, dass das BSI durch die Meldepflicht auch Angriffe frühzeitig erkennen, präventive Schutzmaßnahmen ermitteln und diese Erkenntnisse anderen Betreibern aber auch anderen Anwendern von IT rechtzeitig zur Verfügung stellen kann. Durch dieses „Geben und Nehmen“ zwischen den Akteuren wird es leichter werden, neuen Gefährdungen rechtzeitig entgegenzutreten.

Das BSI wird gemäß Gesetz den vertraulichen Umgang mit den Daten der Betreiber Kritischer Infrastrukturen sicherstellen. Aus der langjährigen Zusammenarbeit mit Unternehmen weiß das BSI um den Stellenwert von Vertrauen, wenn es um IT-Sicherheit geht.

Die in § 7 BSIG des Gesetzentwurfes vorgesehene Änderung stellt sicher, dass das BSI Dritte zur Durchführung der Warnung der Betroffenen einbeziehen und somit die Betroffenen selbst mit seiner Warnung erreichen kann. Eine unmittelbare Warnung ist oftmals nicht möglich, da dem BSI zwar die missbräuchlichen Daten (z.B. IP-Adressen oder Bankverbindungen) vorliegen, diese aber nicht zugeordnet werden können. Bei IP-Adressen können dies die Provider, bei Bankdaten die Banken sein.

Zur Erfüllung seiner präventiven Aufgaben benötigt das BSI die in § 7a des Gesetzentwurfes vorgesehene Befugnis, Produkte und Systeme unabhängig von der Zustimmung des Herstellers und unter Anwendung aller nach dem Stand der Technik notwendigen Untersuchungsmethoden auf ihre Sicherheit hin zu untersuchen, um

mögliche Sicherheitsrisiken bei kritischen Infrastrukturen und in der Bundesverwaltung beurteilen zu können. Bisher sind Produktanalysen aufgrund urheber-, wettbewerbs- oder strafrechtlicher Regelungen unzulässig, obwohl die Notwendigkeit, Produkte auf Sicherheitsrisiken zu untersuchen, größer ist als je zuvor.

Da die aus den Untersuchungen gewonnenen Ergebnisse den Markt beeinflussen können, wird vor deren Veröffentlichung stets abgewogen, ob der damit verbundene Eingriff in die Tätigkeit der Unternehmen gerechtfertigt ist. Schutzmaßnahmen zu Gunsten der Unternehmen, wie die Einbindung vor der Veröffentlichung und die Möglichkeit zur Stellungnahme, sieht das Gesetz vor. Es greift somit das mit der letzten Gesetzesänderung 2009 eingeführte und seit dem bewährte Verfahren zur Warnung auf.

Telemediengesetz
Als Präsident des BSI befürworte ich ausdrücklich, dass auch Telemediendiensteanbieter künftig einen Beitrag zur Schaffung von IT-Sicherheit leisten sollen. Ungesicherte Telemedienangebote sind oft der Grund dafür, dass z.B. ein Webserver als Angriffswerkzeug missbraucht werden kann oder Täter an die personenbezogenen Daten der Kunden eines Telemedienangebotes gelangen – etwa weil keine hinreichend sicheren Authentifizierungsmaßnahmen eingesetzt wurden.

Telekommunikationsgesetz
Die im TKG vorgesehene Pflicht der TK-Anbieter, ihre Nutzer auf Störungen auf deren Systemen hinzuweisen, ist aus Sicht des BSI neben gemeinsamen Initiativen mit der Wirtschaft eine wichtige und notwendige Maßnahme zur Förderung der IT-Sicherheit. Wenn TK-Anbieter z.B. weil sie sogenannte Honey-Pot-Systeme betreiben, wissen, dass ihre Kunden Teil eines Botnetzes sind, sollten sie ihrer Verantwortung nachkommen und diese oftmals ahnungslosen Nutzer auch informieren. Nur so kann verhindert werden, dass die Nutzer oder Dritte weitere Schäden erleiden, etwa durch den Abfluss von sensiblen personenbezogenen Daten oder die unbeabsichtigte Teilnahme an Angriffen.

Da die TK-Anbieter auch den direkten Kontakt zu ihren Kunden haben, sind sie näher am Nutzer. Daher hält das BSI die Pflicht der Anbieter, ihre Kunden auf Werkzeuge zur Erkennung und Beseitigung von Störungen hinweisen zu müssen, für zweckmäßig und notwendig. Solch zielgerichtete Hinweise sind effektiver und erreichen mehr Nutzer als allgemeine Informationen im Netz, die die Nutzer erst einmal suchen und finden müssen. Gerade technisch weniger versierten und damit leicht angreifbaren Nutzern von IT wird die Absicherung dadurch erleichtert. Insofern stellt die Regelung eine sinnvolle Ergänzung zu bestehenden Informationsangeboten wie z.B. BSI-für-Bürger oder botfrei.de dar.

4. Fazit

Die Dynamik der IT-Entwicklung und der Gefährdungen wird uns auch in Zukunft vor weitere Herausforderungen stellen. Der Gesetzentwurf stellt aus meiner Sicht als BSI-Präsident einen wichtigen Schritt zur Verbesserung der IT-Sicherheit sowohl für Kritische Infrastrukturen wie auch für Bürgerinnen und Bürgern als Internetnutzer in Deutschland dar. Die neuen Aufgaben wird das BSI aktiv angehen.

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)284 E

BDI

Bundesverband der Deutschen Industrie · 11053 Berlin

Digitalisierung und industrielle Wertschöpfungsstrukturen

An den
Vorsitzenden des Innenausschusses des
Deutschen Bundestages
Herrn Wolfgang Bosbach
Platz der Republik 1
11011 Berlin

Datum
16. April 2015

BDI-Stellungnahme zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) (BT-Drs. 18/4096)

Sehr geehrter Herr Bosbach,

mit Blick auf die öffentliche Anhörung im Innenausschuss möchte der Bundesverband der Deutschen Industrie (BDI) nochmals auf folgende für die deutsche Industrie wesentlichen Punkte hinweisen:

1. **Klare und transparente Definitionen, um Rechtssicherheit für die Unternehmen zu erreichen**
   Der BDI hält es für problematisch, dass zentrale Definitionen, wie z. B. die konkrete Definition „Kritischer Infrastrukturen“, nicht im Gesetz selber, sondern in einer gesonderten Rechtsverordnung geregelt werden. Auch der Umfang und der zeitliche Rahmen der Meldung sind im Entwurf nicht hinreichend bestimmt. Zudem sollte die Weitergabe von Daten gesetzlich ausgeschlossen werden, die über die allgemeine Darstellung des Sicherheitslagebildes hinausgehen und Rechte Dritter verletzten können.

2. **Win-win Situation für beide Seiten schaffen**
   Die Zusammenarbeit zwischen Unternehmen und Staat darf keine „Einbahnstraße“ sein. Informationen dürfen nicht nur, im Sinne einer Meldepflicht, von Unternehmen an die Behörden fließen und damit den Bürokratieaufwand der Unternehmen erhöhen. Vielmehr sollte das Bundesamt für Sicherheit in der Informationstechnik (BSI) künftig Informationen über Bedrohungen zeitnah, aktuell und praxisorientiert an die Unternehmen zurückgegeben. Nur so kann insgesamt ein erhöhtes Sicherheitsniveau erreicht werden.

Bundesverband der Deutschen Industrie e.V.
Mitgliedsverband
BUSINESSEUROPE

Hausanschrift
Breite Straße 29
10178 Berlin
Postanschrift
11053 Berlin
Telekontakte
T: +493020281461
F: +493020282461
Internet
www.bdi.eu
E-Mail
I.Ploeger@bdi.eu

3. **Doppelregulierung vermeiden**
   Doppelregulierung bzw. doppelte Zuständigkeiten müssen in jedem Fall vermieden werden. Betreiber Kritischer Infrastrukturen, die über bereits bestehende Rechtsvorschriften, z. B. das Telekommunikationsgesetz (TKG), das Energiewirtschaftsgesetz (EnWG) oder das Bundesdatenschutzgesetz (BDSG) reguliert werden, sollten nicht zusätzlich reguliert werden.

4. **Kompatibilität zwischen nationaler und europäischer Gesetzgebung herstellen**
   Der BDI tritt mit Nachdruck dafür ein, dass das IT-Sicherheitsgesetz mit der europäischen NIS-Richtlinie im Einklang steht. So können spätere Gesetzesanpassungen vermieden und Rechtssicherheit für die Unternehmen gewahrt werden. Die Bundesregierung sollte auf einen engen Anwendungsbereich der NIS-Richtlinie hinwirken. Auch sollte auf europäischer Ebene auf Sanktionen verzichtet werden. Um den Schutz von Unternehmensinteressen zu garantieren, sollte sich das Anhörungsrecht der Unternehmen bei einer potenziellen Meldeveröffentlichung stärken an dem Vorbild des IT-Sicherheitsgesetzes orientieren. Das Meldeverfahren sollte analog zum IT-Sicherheitsgesetz anonym erfolgreich.

5. **Kohärenz mit internationalen Standards erreichen**
   Weder der Aktionsradius von international agierenden Unternehmen noch die Cyber-Angriffe machen an den Landesgrenzen halt. Eine deutsche Insellösung wäre nicht zielführend. Der BDI setzt sich daher für eine Kohärenz mit international bereits existierenden Standards ein. Eine Harmonisierung der Meldewege und Verfahren sowie der Definition der nationalen Zuständigkeiten ist anzustreben, um Doppelaufwendungen und Wettbewerbsnachteile zu vermeiden.

Die vollständige BDI-Kommentierung des Gesetzentwurfs entnehmen Sie bitte der Stellungnahme, die der BDI am 5. November 2015 im Rahmen der Verbändeanhörung an das Bundesinnenministerium übermittelt hat. Die Stellungnahme, die in der Anlage beigefügt ist, wurde vom BDI gemeinsam mit seinen Mitgliedsverbänden erarbeitet und bildet die branchenübergreifende Positionierung der Deutschen Industrie.

Mit freundlichen Grüßen

Iris Plöger

Anlage
BDI-Stellungnahme zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 5. November 2015

Stellungnahme

zum Entwurf des Gesetzes zur „Erhöhung der Sicherheit informationstechnischer Systeme“ (ITSiG)

Sicherheit und Rohstoffe

Der BDI vertritt als Spitzenverband der deutschen Industrie und der industrienahen Dienstleister in Deutschland 37 Branchenverbände. Er repräsentiert die politischen Anliegen und Interessen von mehr als 100.000 Unternehmen mit rund acht Millionen Beschäftigten.

1. Grundsätzlich

- Der BDI unterstützt nachdrücklich das Ziel der Bundesregierung, das Industrieland Deutschland widerstandsfähiger gegen die steigende Anzahl von Cyberbedrohungen zu machen.
- Der vorliegende Entwurf wurde dem BDI am 4. November 2014 zur Kommentierung übermittelt. Aufgrund der, durch das BMI gesetzten, sehr kurzfristigen Rückmeldefrist, ist eine umfassende und detaillierte Bewertung nur bedingt möglich. Der BDI behält es sich daher vor, weitere Kommentierungen im Rahmen des mündlichen Anhörungsverfahrens zu übermitteln.
- Der BDI hat am 5. April 2013 eine erste Stellungnahme zum geplanten IT-Sicherheitsgesetz[1] an die Bundesregierung übermittelt und den Gesetzgebungsprozess seitdem eng und konstruktiv begleitet. Im Februar 2014 hat der BDI ein Positionspapier zur Ausgestaltung des IT-Sicherheitsgesetzes[2] veröffentlicht.
- Darüber hinaus hat der BDI gemeinsam mit BDLI, BDSV, BITKOM und ZVEI die Studie „IT-Sicherheit in Deutschland. Handlungsempfehlungen für eine zielorientierte Umsetzung des IT-Sicherheitsgesetzes“[3] bei der Wirtschaftsprüfungsgesellschaft KPMG in Auftrag gegeben. Ziel der Studie war es, konkrete Handlungsempfehlungen für die Ausgestaltung eines IT-Sicherheitsgesetzes zu präsentieren, bevor die Bundesregierung einen neuen Entwurf vorlegt. Die Studie wurde am 3. Juli 2014 an Bundesinnenminister Thomas de Maizière übermittelt.
- Der BDI hält es für problematisch, dass zentrale Definitionen, wie z. B. die konkrete Definition Kritischer Infrastrukturen, nicht im Gesetz sel-

[1] BDI-Stellungnahme zum Referentenentwurf eines „Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme“, 5. April 2013, http://www.bdi.eu/images_content/SicherheitUndVerteidigung/BDI_Stellungnahme_IT-Sicherheitsgesetz_final.pdf

[2] BDI-Positionspapier „Erwartungen der deutschen Industrie an ein IT-Sicherheitsgesetz“, Feb. 2014, http://www.bdi.eu/download_content/SicherheitUndVerteidigung/Positionspapier_Sicherheitsgesetz_25_02.pdf

[3] KPMG-Studie „IT-Sicherheit in Deutschland. Handlungsempfehlungen für eine zielorientierte Umsetzung des IT-Sicherheitsgesetzes“, Juli 2014, http://www.bdi.eu/images_content/SicherheitUndVerteidigung/KPMG_IT-Sicherheit_in_Deutschland.pdf

Bundesverband der Deutschen Industrie e.V.
Mitgliedsverband
BUSINESSEUROPE

Telekontakte
T: +493020281402
F: +493020282402
Internet
www.bdi.eu
E-Mail
D.Klein@bdi.eu

ber, sondern in einer gesonderten Rechtsverordnung geregelt werden. Um Rechtsklarheit für die betroffenen Unternehmen zu schaffen, sollte diese Rechtsverordnung zeitnah zum ITSiG verabschiedet werden. Gleichwohl begrüßt der BDI ausdrücklich die frühzeitige Einbindung der Industrie im Rahmen des Gesetzgebungsvorhabens. Das Angebot an die Verbände, bei der Erarbeitung der branchenspezifischen Mindeststandards und der Festlegung der Kriterien für die detaillierte Definition im Zuge einer nachgelagerten Verordnung umfangreich mitzuarbeiten, nimmt der BDI wahr. Die Beteiligung der Branchenvertreter zur Bestimmung der Kritischen Infrastrukturen sollte frühzeitig im Vorfeld der gesetzlichen Regelung stattfinden.

- Die deutsche Industrie tritt mit Nachdruck für eine höchstmögliche Kompatibilität zwischen dem deutschen IT-Sicherheitsgesetz und der europäischen NIS-Richtlinie ein. Das gilt insbesondere für die weitgehende Anonymisierung der Meldungen, wie sie im ITSiG vorgesehen ist. Der BDI plädiert dafür, dass eine solche Regelung auch in der NIS-Richtlinie berücksichtigt wird. Zumindest sollte den Mitgliedstaaten bei der Umsetzung der Richtlinie der Spielraum eingeräumt werden, dies eigenverantwortlich zu regeln.
- Doppelregulierung bzw. doppelte Zuständigkeiten müssen in jedem Fall vermieden werden. Betreiber Kritischer Infrastrukturen, die über bereits bestehende Rechtsvorschriften, z. B. das Telekommunikationsgesetz (TKG), das Energiewirtschaftsgesetz (EnWG) oder das Bundesdatenschutzgesetz (BDSG) reguliert werden, sollten nicht zusätzlich reguliert werden.
- Die Zusammenarbeit zwischen Unternehmen und Staat darf keine „Einbahnstraße“ sein. Informationen dürfen nicht nur, im Sinne einer Meldepflicht, von Unternehmen an die Behörden fließen. Vielmehr müssen Informationen über Bedrohungen zeitnah, aktuell und praxisorientiert von den staatlichen Stellen an die Unternehmen gegeben werden. Nur so kann insgesamt ein erhöhtes Sicherheitsniveau erreicht werden.
- Ein gutes Beispiel für eine enge und vertrauensvolle Zusammenarbeit zwischen Industrie und Behörden ist die Allianz für Cyber-Sicherheit. Diese leistet einen wichtigen Beitrag zur Prävention und Awareness. Sie gilt es weiter zu stärken. Die bereits vorhandene Möglichkeit zur freiwilligen Meldung eines Sicherheitsvorfalls an die Meldestelle der Allianz ist bei der Ausgestaltung des ITSiG zu berücksichtigen und mit den vorgesehenen Maßnahmen zu verzahnen.
- Weder der Aktionsradius von international agierenden Unternehmen noch die Cyber-Angriffe machen an den Landesgrenzen halt. Daher wäre eine deutsche Insellösung nicht zielführend. Der BDI setzt sich daher für eine Kohärenz mit international bereits existierenden Standards ein. Eine Harmonisierung der Meldewege und Verfahren sowie der Definition der nationalen Zuständigkeiten ist anzustreben, um Doppelaufwendungen und Wettbewerbsnachteile zu vermeiden. Weiterhin werden in zunehmenden Maße Dritte zur Bereitstellung von Diensten, als sogenannter „Sofware as a Service“ oder „Hardware as a Service“ genutzt, die ihre Dienste in der Regel über Staatsgrenzen erbringen. Doppelte Auditierungen müssen vermieden.

2. Im Einzelnen

- **Erfüllungsaufwand für die Wirtschaft**
  Anders als im vorliegenden Gesetzesentwurf angenommen, entstehen der Wirtschaft durchaus Mehraufwände durch die Anforderungen aus dem Gesetz. Auf Basis des damals vorliegenden Entwurfs hat KPMG die Kosten für die Umsetzung einer Meldepflicht untersucht. Die Berechnungen von KPMG zeigen, dass die Umsetzung der Meldepflicht zu signifikanten Erhöhungen der Personal- und Sachkosten für die betroffenen Unternehmen führt. Finanzielle Belastungen könnten sich zudem auch aus dem Risiko möglicher Reputationsschäden ergeben, die aus einem fehlerhaften Umgang mit den Meldedaten entstehen können. In Anlehnung an die Methode des Standardkostenmodells wurden zudem die Bürokratiekosten von KPMG abgeschätzt, die sich unmittelbar aus einer Meldepflicht für die Unternehmen ergeben. Diese spezifischen Kosten summieren sich auf Grundlage der für diese Studie getroffenen Annahmen auf insgesamt rund 1,1 Milliarde Euro pro Jahr.

- **Kritische Infrastrukturen, Artikel 1 § 2**
  In Artikel 1, Absatz 3 des Gesetzentwurfs wird versucht, eine Begriffsbestimmung der Kritischen Infrastrukturen vorzunehmen. Hier heißt es:

  > „(10) *Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die*
  > *1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und*
  > *2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.*
  > *Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt. Kommunikationstechnik im Sinne des Absatzes 3 gehört nicht zu den Kritischen Infrastrukturen im Sinne dieses Gesetzes.“*

  In § 10 wird festgelegt, ab welchem Schwellenwert, welche Einrichtungen, Anlagen oder Teile davon als Kritische Infrastrukturen gelten und wie diese bestimmt werden sollen:

  > *„Das Bundesministerium des Innern bestimmt nach Anhörung von Vertretern der Wissenschaft, betroffener Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie (…) anhand der in den jeweiligen Sektoren erbrachten Dienstleistungen durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, ab welchem Schwellenwert welche Einrichtungen, Anlagen oder Teile davon als Kritische Infrastrukturen im Sinne dieses Gesetzes gelten. Zugang zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, wird nicht gewährt.“*

Der Anwendungsbereich des Gesetzentwurfs ist nicht ausreichend konkret bestimmt. Deshalb erscheint es geboten in Artikel 1 bzw. der Begründung, konkrete Kriterien zu benennen, nach denen die Teilsegmente der aufgezählten Sektoren als kritisch eingestuft werden. Die Anforderungen an die Betreiber kritischer Infrastrukturen müssen einheitlich sein. Dies ist gegenwärtig durch die vorgesehenen Änderungen im EnWG und des TKG nicht der Fall.

Darüber hinaus hält der BDI es für äußerst problematisch, dass die wichtige Frage des Anwendungsbereichs auf eine spätere Rechtsverordnung delegiert wird. Das schadet der Rechtssicherheit und trifft auch auf wettbewerbsrechtliche Bedenken. Denn der Verordnungsermächtigung im Gesetzentwurf fehlt es an ausreichender Bestimmtheit, Normklarheit bei der Adressatenbestimmung und an der notwendigen Begrenzung der Ermächtigung. Es besteht außerdem ein erhebliches Risiko für die Investitionssicherheit und nimmt den Unternehmen das nötige Maß an Erwartungssicherheit.

Der Staat ist der größte Betreiber Kritischer Infrastrukturen. Gemäß dem vorliegenden Entwurf soll der Staat jedoch nicht unter das Gesetz fallen, obwohl die staatlichen Kritischen Infrastrukturbetreiber ebenso eine „hohe Bedeutung für das Funktionieren des Gemeinwesens“ haben. Der BDI setzt sich daher nachdrücklich dafür ein, dass die entsprechenden Meldepflichten und Sicherheitsstandards neben dem Bund auch für Länder und Kommunen gelten und vom Gesetz erfasst werden.

Gleichwohl begrüßt der BDI ausdrücklich, dass die Bestimmung der für die Anwendung der gesetzlichen Regelung relevanten kritischen Infrastrukturen sektor- und branchenspezifisch nach qualitativen und quantitativen Kriterien in enger Abstimmung mit den betroffenen Betreibern und Wirtschaftsverbänden erfolgen soll. Richtigerweise wird hierbei erkannt, dass sich die benannten Sektoren nicht nur wesentlich im Hinblick auf ihre Kritikalität und spezifischen Sicherheitsanforderungen zueinander unterscheiden, sondern diese mitunter auch innerhalb der Sektoren signifikant und abhängig vom Geschäftsmodell und Tätigkeitsbereich variieren.

Die geplante Konsultation mit Branchenvertretern zur Bestimmung der wesentlichen Kritischen Infrastrukturen bzw. des Adressatenkreises des Gesetzes sollte zeitnah stattfinden. Eine differenzierte Betrachtungsweise und eingehende Risikoanalyse ist im Vorfeld einer Gesetzesinitiative essentiell, um erfolgreich angemessene Sicherheitslösungen zu finden.

- **Mindeststandards, Artikel 1 § 8a**
  Der BDI begrüßt ausdrücklich die Möglichkeit zur Erarbeitung branchenspezifischer Sicherheitsstandards durch die Betreiber Kritischer Infrastrukturen und Branchenverbände im Wege der Selbstorganisation. Der BDI hat sich bereits im BDI-Positionspapier und in der KPMG-Studie explizit für diese Option ausgesprochen. Das wird dem Ziel gerecht, dass Mindeststandards für jede Branche passgenau sein müssen, um effektiv wirken zu können. Dem einzelnen Betreiber steht es

frei, abweichend von den branchenspezifischen Sicherheitsstandards, eigene den Stand der Technik berücksichtigende Maßnahmen umzusetzen. Dieser kooperative und vertrauensvolle Ansatz wird BDI-seitig mit Nachdruck unterstützt.

- **Bewertung und Veröffentlichung Sicherheit informationstechnischer Produkte, Systeme und Dienste, Artikel 1 § 7a**

  „(1) Das Bundesamt darf zur Erfüllung seiner Aufgaben auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte, Systeme und Dienste untersuchen. Es darf sich hierbei der Unterstützung Dritter bedienen.
  (2) Die aus den Untersuchungen gewonnenen Erkenntnisse dürfen nur zur Förderung der IT-Sicherheit genutzt werden.
  (3) Das Bundesamt darf seine Bewertung der Sicherheit der untersuchten informationstechnischen Produkte, Systeme und Dienste weitergeben und veröffentlichen. § 7 Absatz 1 Satz 3 und 4 ist entsprechend anzuwenden.“

  BDI-Kommentierung
  Diese Regelung greift tief in die privatwirtschaftliche Tätigkeit des betroffenen Unternehmens ein. Aus Sicht des BDI ist dies äußerst problematisch. Der bisher gültige Ansatz, dass Unternehmen bei Produkten, Systemen und Diensten um eine Zertifizierung durch das BSI ersuchen, wird umgekehrt. Das BSI erhielte damit die gesetzliche Befugnis noch vor Markteinführung eines Produkts, Prüfungen zu vollziehen. Darüber hinaus wird durch die geplante Form des Reverse Engineering eine Schwächung der Common Criteria (CC) durch die Hintertür befürchtet.

  Die Übertragung dieser Prüfkompetenz auf „Dritte“ setzt voraus, dass diese „Dritten“ über das entsprechende Know-How verfügen, Produkte, Services und Dienste qualifiziert zu prüfen. Ein solches Wissen ist in der Regel nur bei Unternehmen derselben Branche verfügbar, was die Offenlegung von Geschäftsgeheimnissen oder Geschäftspotenzialen gegenüber direkten Konkurrenten zur Folge hätte. Speziell die Befugnis zur Weitergabe und Veröffentlichung der Informationen ohne angemessene Barrieren und Kontrollen kann zu einem neuen Sicherheitsrisiko führen oder zu einem Reputationsschaden für betroffene Unternehmen und ihre Produkte.

  Hier ist sicherzustellen, dass die Rechte der Hersteller gewahrt werden. Eine Weitergabe und Veröffentlichung der Bewertung des BSI sollte nur erfolgen, wenn das jeweilige Unternehmen ausdrücklich seine Zustimmung erteilt hat. Wir schlagen vor, einen solchen Zusatz in Absatz 3 zu ergänzen.

- **Weitergabe der Ergebnisse eines Sicherheitsaudits, Artikel 1 § 8a**
  In § 8a heißt es:

  „(3) (...) Die Betreiber übermitteln dem Bundesamt eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Bei Sicherheitsmängeln kann das Bundesamt die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse und, soweit erforderlich, im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen."

  BDI-Kommentierung
  Eine gesetzliche Verpflichtung zur Detailmeldung der Ergebnisse der geforderten Sicherheitsaudits, Prüfungen oder Zertifizierungen an das BSI wird als bedenklich erachtet. Das Recht über die detaillierten Informationen eines Audits oder einer Überprüfung verfügen zu dürfen, sollte prinzipiell ausschließlich dem Auftraggeber obliegen.

  Unklar bleibt zudem, welche Konsequenzen eine Übermittlung der Auditergebnisse ans BSI nach sich zieht. Dies gilt insbesondere dann, wenn eine Zertifizierungspflicht hergestellt würde. Über die Verpflichtung zur Zertifizierung wäre eine Konformität zu geforderten Anforderungen bereist ausreichend sichergestellt. Weitergehende Berichterstattungen würden den bereits erheblichen Bürokratieaufwand weiter steigern.

- **Meldepflichtige Ereignisse, Artikel 1 § 8b**
  Gemäß dem Referentenentwurf haben

  „(4) Betreiber kritischer Infrastrukturen (...) bedeutende Störungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der von ihnen betriebenen Kritischen Infrastrukturen führen können, über die Kontaktstelle unverzüglich an das Bundesamt mitzuteilen."

  In den Erläuterungen zu § 8b (Seiten 39 und 40) wird erstmals versucht meldepflichtige Ereignisse zu definieren:

  „Eine Störung im Sinne des BSI-Gesetzes liegt daher vor, wenn die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder versucht wurde, entsprechend auf sie einzuwirken. Dazu zählen insbesondere Fälle von Sicherheitslücken, Schadprogrammen und erfolgten, versuchten oder erfolgreich abgewehrten Angriffen auf die Sicherheit in der Informationstechnik sowie außergewöhnliche und unerwartete technische Defekte mit IT-Bezug (z. B. nach Softwareupdates oder ein Ausfall der Serverkühlung). Die Störungen sind dann meldepflichtig, wenn sie bedeutend sind. Eine bedeutende Störung liegt vor, wenn die Funktionsfähigkeit des Betreibers oder die von diesem betriebene Kritische Infrastruktur bedroht sind."

BDI-Kommentierung

Genaue Angaben zum Meldeprozess fehlen im vorliegenden Entwurf weiterhin. Der Referentenentwurf enthält keine Angaben über inhaltliche Anforderungen an eine Meldung, Detailtiefe und Zeitrahmen.

Aus BDI-Sicht führt eine Meldung über jede Störung, die zu einer „Beeinträchtigung führen könnte", zu weit. Gemäß dieser Definition liegt bereits eine Störung vor, wenn nur versucht wurde auf die Technik einzuwirken. Die Tatsache, dass diese dann bereits bedeutend ist, wenn die Funktionsfähigkeit auch nur bedroht ist, umfasst bei einer unverzüglichen Meldeverpflichtung im Zweifel jegliche Störungen. Um Rechtssicherheit zu schaffen, ist eine Konkretisierung aus BDI-Sicht dringend geboten. Außerdem sollten die Vorgaben zur Meldepflicht mit anderen bestehenden nationalen gesetzlichen Regelungen, wie z. B. dem Energiewirtschaftsgesetz, sowie der NIS-Richtlinie auf europäischer Ebene und internationalen Standards („Cybersecurty Framework" in den USA"), übereinstimmen.

Die gesetzliche Vorgabe in § 8a

> *„(4) (…) Die Meldung muss Angaben zu den Störungen sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik und zur Branche des Betreibers enthalten"*

steht der im selben Absatz geforderten „unverzüglichen" Meldung entgegen. Unternehmen sollten grundsätzlich die Möglichkeit haben, IT-Beeinträchtigungen zunächst intern zu analysieren. Insofern erscheint die Pflicht zur unverzüglichen Feststellung und Weitermeldung von Beeinträchtigungen durch die betroffenen Unternehmen nicht gerechtfertigt.

Darüber hinaus erschweren die vorgesehene Inhalte einer Meldung (ausgenutzte Sicherheitslücken, vermutete oder tatsächliche Ursachen, die betroffene Informationstechnik auf System- und Komponentenebene) erschweren weiterhin eine schnelle und gleichzeitig unternehmensinterne Compliance konforme Meldung. Die Meldung der eindeutigen Identifikationsmerkmale von gefundenen Schadensmerkmalen und Programmen erscheinen zielführender. Die Weitergabe erlaubt es anderen Unternehmen, schnell zu prüfen, ob sie ebenfalls betroffen sind. Das schafft einerseits einen praxistauglichen Mehrwert und andererseits eine Basis für ein Sicherheitslagebild gegeben.

Der BDI schlägt folgende Formulierung zu § 8a (4) vor:

> *„(…) Die Meldung sollte vorrangig Angaben zu den Signaturen oder sonstigen Identifikationsmerkmalen von gefundenen Schadensmerkmalen und Programmen sowie Angaben zur Branche enthalten und sollte nachträglich durch Informationen zu den Störungen sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache und der betroffenen Informationstechnik ergänzt werden."*

Außerdem bleibt unklar, was im Falle eines Verstoßes gegen die Meldepflicht zu befürchten ist. Mit Blick auf die parallelen Vorgaben der NIS-Richtlinie ist damit zu rechnen, dass die Verletzung einer Meldepflicht die Erhebung eines Bußgeldes nach sich ziehen wird. Vor diesem Hintergrund wäre der Tatbestand der Meldepflichtverletzung unbedingt zu spezifizieren.

- **Anonymisierte bzw. pseudonymisierte Meldung, Artikel 1 § 8b**
  Die grundsätzliche Möglichkeit zur anonymisierten bzw. pseudonymisierten Meldung unterstützt der BDI mit Nachdruck. Diese Regelung muss für alle Kritischen Infrastrukturbetreiber gleichermaßen gelten. Gegenwärtig ist sie für die Energiewirtschaft allerdings völlig ausgeschlossen:

  > *„Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Kritischen Infrastrukturen geführt hat."*

  BDI-Kommentierung
  Der BDI hatte in der KPMG-Studie bereits einen entsprechenden Vorschlag erarbeitet. Die Studie empfiehlt eine „Pseudonymisierung der Meldepflicht via Treuhänder". Eine solche Lösung ermöglicht es dem BSI uneingeschränkt, ein Lagebild zu erstellen und minimiert zugleich das Risiko von Reputationsschäden für die meldenden Unternehmen. Ein unabhängiger Treuhänder könnte dabei die vermittelnde Rolle annehmen und bei Bedarf auch einen gesicherten Weg zum meldenden Unternehmen zur Verfügung stellen.

- **Anwendungsbereich, Artikel 1 § 8c**
  Der BDI begrüßt, dass nach §8c Absatz 2 Satz 1 Betreiber Kritischer Infrastrukturen, die über bereits bestehende Rechtsvorschriften reguliert werden, diesen auch weiterhin unterliegen sollen (Vermeidung doppelter Regulierung und Zuständigkeiten).

- **Auskunftsverlangen, Artikel 1 § 8d**
  In § 8d regelt die Auskunft des BSI zu Informationen

  > *„(1) Das Bundesamt kann auf Antrag Auskunft zu den im Rahmen von § 8a Absatz 2 und 3 erhaltenen Informationen sowie zu den Meldungen nach § 8b Absatz 4 erteilen, wenn keine schutzwürdigen Interessen des betroffen Betreibers Kritischer Infrastrukturen dem entgegenstehen und durch die Auskunft keine Beeinträchtigung des Verfahrens oder sonstiger wesentlicher Sicherheitsinteressen zu erwarten ist."*

  BDI-Kommentierung
  Die Auswirkungen einer Bekanntgabe der Informationen und Meldungen kann für den konkreten Betreiber der Kritischen Infrastruktur massive Auswirkungen, wie z. B. Preisgabe von Betriebsgeheimnissen, Wettbewerbsnachteile, Umsatzeinbußen oder Imageverlust zur Folge haben. Es besteht Seitens der deutschen Industrie die Befürchtung, dass bei einer Beeinträchtigung oder einem Ausfall Kritischer Infrastrukturen die ebenfalls schutzwürdigen Interessen des betroffenen Betreibers dem

Informationsbedürfnis nachgelagert werden.

Der BDI schlägt daher vor, dass die Auskunft lediglich in anonymisierter Form erteilt werden sollte. Eine Formulierung wie folgt wäre daher das Minimum, welches Eingang in die gegenwärtige Klausel finden sollte:

> „*nach Anhörung und ohne namentliche Nennung des konkreten Betreibers der Kritischen Infrastruktur.“*

- **Umsetzungsfrist**
  Die vorgesehene Umsetzungsfrist von zwei Jahren ist zu knapp bemessen. Für die Energiewirtschaft soll sogar eine noch kürzere Umsetzungsfrist von lediglich einem Jahr gelten. Je nach individueller Betroffenheit ist eine Vielzahl an zusätzlichen Verpflichtungen zu erfüllen. Die betroffenen Unternehmen benötigen ausreichend Zeit, um neue Informationsabläufe, Sicherheitsprozesse und Auditverfahren abzustimmen. Der BDI spricht sich dafür aus, die Umsetzungsfrist des Gesetzes für alle Betreiber Kritischer Infrastrukturen auf drei Jahre zu verlängern.

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)284 F

Chaos Computer Club

Stellungnahme zum Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

Linus Neumann, 17. April 2015

Vorbemerkungen

Probleme der IT-Sicherheit sind primär technische Probleme. Politische Lösungen für diese Probleme sind dann zielführend, wenn sie in einer tatsächlichen Erhöhung der IT-Sicherheit resultieren. Technisch kann dieses kann auf zwei Wegen erreicht werden:

1. **Härtung: Begrenzen des Schadenpotenzials möglicher Schwachstellen.**
   Hierunter sind Maßnahmen zu fassen, die einen Angreifer, der über eine unbekannte Schwachstelle in ein System eingedrungen ist, in den Möglichkeiten der Ausnutzung beschränken. Diese Maßnahmen haben den sekundären Effekt, die Attraktivität des Systems für Angreifer zu senken. Beispielhaft sei hier die Ende-zu-Ende-Verschlüsselung genannt: Sie bewahrt die Vertraulichkeit der Kommunikation von Nutzern eines Kommunikationsservers und senkt daher auch die Attraktivität dieses Servers als Angriffsziel. Ähnlich ermöglicht es das sogenannte *Monitoring*, erfolgreiche Angriffe zu detektieren und Gegenmaßnahmen zu ergreifen.
2. **Prävention: Beseitigung von Schwachstellen.**
   Der größere Teil der von Angreifern ausnutzbaren Schwachstellen in IT-Systemen ist unbekannt, bis die Schwachstellen entweder durch Sicherheitstests erkannt und entfernt werden oder bis ihre erfolgreiche Ausnutzung durch Angreifer bemerkt wird. Da letzterer Fall in der Regel mit Schaden einhergeht, ist eine vorherige Entdeckung anzustreben. Beispielhaft sei hier die als *Heartbleed* bekannt gewordene Schwachstelle in der Software-Bibliothek *OpenSSL* genannt, die einen Großteil der weltweiten Internet-Server betraf. Zwischen ihrer unbeabsichtigten Einführung und ihrer Entdeckung vergingen zwei Jahre, in denen alle betroffenen Systeme schutzlos waren.

IT-Sicherheit in Unternehmen

IT-Sicherheit stellt Unternehmen vor eine multi-dimensionale Herausforderung: Potenzielle Angreifer haben viele unterschiedliche Motivationen und Angriffsziele. Beispielsweise könnten ausgewählte Mitarbeiter zum Zwecke der Industriespionage gezielt angegriffen, kritische Systeme zum Zwecke der Sabotage in ihrer Funktion gestört oder Kunden- und Vertragsdaten kopiert werden. Die Liste möglicher Angriffsszenarien ist lang und lässt sich nur eingrenzen, indem die Motivation der potenziellen Angreifer (und damit die Wahrscheinlichkeit eines Angriffs) in Betracht gezogen wird.

Die treibende Kraft der IT-Sicherheit in Unternehmen ist daher eine Abwägung von Eintrittswahrscheinlichkeit und potenziellem Schaden eines Angriffs. So entsteht ein komplexer Verteidigungsraum, in dem viele Risikoszenarien den Geschäftsinteressen der Unternehmen direkt entgegenstehen, während andere nur geringe oder vernachlässigbare Auswirkungen hätten. Entsprechend werden auch die zur Verfügung stehenden Ressourcen eingesetzt: Große Geschäftsrisiken werden minimiert, geringere werden in Kauf genommen.

Dieser Fokus auf Geschäftsrisiken hat den Nebeneffekt, dass potenzielle Schäden für Dritte, insbesondere für Kunden, nur dann ausreichende Berücksichtigung finden, wenn sie mit einem nennenswerten direkten oder indirekten Geschäftsrisiko einhergehen. So ist es nachvollziehbar und nicht unüblich, dass beispielsweise geistiges Eigentum und interne geschäftsrelevante Daten einem höheren Schutzniveau unterliegen als beispielsweise Kundendaten. Aus gesellschaftlicher Perspektive ist diese Tendenz jedoch nicht wünschenswert.

Regulatorische Einflussmöglichkeiten

Ein Gesetz zur Erhöhung der IT-Sicherheit muss einen pro-aktiven Ansatz motivieren, bei dem Prävention und Härtung allgemein und insbesondere in unzureichend geschützten Bereichen über den Stand der Technik hinaus voran getrieben werden.

Unternehmen und Organisationen müssen incentiviert oder gezwungen werden, Defizite in der IT-Sicherheit nicht nur nachträglich zu beheben, sondern aktiv danach zu suchen und zu beseitigen. Da IT-Sicherheit im Allgemeinen von der Abwendung direkter Geschäftsrisiken getrieben wird, ist ein regulativer Eingriff insbesondere dann geboten, wenn keine oder unzureichende ökonomische Anreize bestehen, ein akzeptables Maß an Schutz herbeizuführen.

Entsprechende Anreize können durch ein Anheben vorgeschriebener Sicherheitsstandards über das aktuelle Niveau hinaus, und komplementär durch eine klar definierte Haftung gegenüber Dritten im Schadensfall gesetzt werden.

Bewertung des vorliegenden Entwurfs

Im Folgenden sind die zentralen Kritikpunkte am vorliegenden Gesetzesentwurf (Deutscher Bundestag, Drucksache 18/4096) zusammengefasst.

Fehlende Ansätze zum Endnutzerschutz

Der vorliegende Gesetzesentwurf bezieht sich in großen Teilen auf die Betreiber kritischer Infrastruktur zum Zwecke der Vermeidung eines Ausfalls von IT-Systemen. Gezielte Maßnahmen zum Schutz der Endnutzer werden nicht verlangt.

Diese Schwerpunktsetzung ist vor dem Hintergrund der im BSI-Bericht zur Lage der IT-Sicherheit in Deutschland 2014[1] dokumentierten Risikolandschaft nicht nachvollziehbar. Im Bericht werden Angriffe auf Bundeseinrichtungen, Privatanwender und Wirtschaft unterschieden.

Bundeseinrichtungen. Nach Angaben des BSI werden *„täglich 15 bis 20 Angriffe auf das Regierungsnetz entdeckt, die durch normale Schutzmaßnahmen nicht erkannt worden wären."* Dabei handele es sich bei *„durchschnittlich einem Angriff pro Tag […] um einen gezielten Angriff mit nachrichtendienstlichem Hintergrund."*

→ Hier zeigt sich ein hoher Angriffsdruck, dem mittels Monitoring wirksam entgegengetreten wird.

Im vorliegenden Gesetzesentwurf soll die Rolle des BSI in diesem Bereich ausgebaut werden. Dabei ist festzuhalten, dass beim Monitoring von kritischen Angriffszielen auch das dementsprechende Wissen über fortgeschrittene Angriffstechniken erlangt wird.

Dieses Wissen kann zur wirksamen Verhinderung der Angriffe ebenso verwendet werden, wie zu deren Weiterentwicklung und Zweitverwertung. Eine kompromisslose und rein defensive Ausrichtung des BSI wäre daher Grundvoraussetzung für das Übertragen dieser Verantwortung. Diese Voraussetzungen sind nicht gegeben, solange das BSI dem BMI und seinen offensiven Ambitionen[2] untersteht. Siehe hierzu auch Absatz *Das Vertrauensproblem des BSI wird nicht gelöst*, Seite 9.

---

[1]Bundesamt für Sicherheit in der Informationstechnik (2014): *Bericht zur Lage der IT-Sicherheit in Deutschland,* Version vom 15.12.2014, abgerufen unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf

[2] ZEIT Online vom 13. November 2014: *Die geheime Überwachungswunschliste des BND*, abgerufen unter http://www.zeit.de/digital/internet/2014-11/bnd-bundesnachrichtendienst-ueberwachung-ausbau/komplettansicht

→ Ein Missbrauch des im BSI gesammelten Wissens über Angriffstechniken ist nicht auszuschließen und in Anbetracht der Eingliederung ins BMI sogar als wahrscheinlich einzustufen.

Privatanwender. Nach Angaben des BSI wurden allein im Jahr 2014 *„zwei Identitätsdiebstähle publik, bei denen Angreifer Zugriff auf Benutzernamen und Passwörter von 16 bzw. 18 Millionen Internetnutzern erlangen konnten."* Angaben über eventuelle Überschneidungen der beiden Datensätze werden nicht gemacht. Die Privatanwender waren zwar Opfer dieser Identitätsdiebstähle, doch es ist unwahrscheinlich, dass sie auch zu einem signifikanten Anteil Quelle der erbeuteten Information waren.

Typischerweise stammen solche Daten aus größeren Angriffen auf die Anbieter von Online-Diensten, also Online-Shops, E-Mail-Anbieter oder sogenannte Soziale Netzwerke, die in diesem Fall die betroffenen Nutzer nicht ausreichend geschützt und – gedeckt vom BSI – auch nicht über den erfolgten Angriff informiert haben.

Hier zeigt sich ein hoher Angriffsdruck, dem nur unzureichende Schutzmaßnahmen entgegenstehen. Für die betroffenen Anbieter stand der Schutz der Nutzerdaten nicht im Fokus ihrer ökonomischen Interessen und wurde daher vernachlässigt. Durch die halbherzige Bearbeitung des Falles durch das BSI wurden die Anbieter in dieser Maxime bestärkt, da sie – trotz des hohen Schadens für die Nutzer – weder zur Rechenschaft gezogen wurden noch angemessene Maßnahmen zur Wiederherstellung des Schutzes ergreifen mussten: Eine umfassende Informierung der Nutzer sowie deren Re-Identifikation und darauffolgende Änderung der Zugangsdaten wäre absolut notwendig gewesen.

→ Obwohl Privatnutzer die häufigsten Opfer von Angriffen auf informationsverarbeitende Systeme sind, findet sich im vorliegenden Gesetzesentwurf weder eine Initiative noch eine Absichtserklärung zur Änderung dieser Situation. Diese Schwerpunktlegung ist insbesondere auch in Anbetracht der vom BSI selbst dokumentierten Bedrohungslage nicht nachvollziehbar.

Wirtschaft. Für das Jahr 2014 berichtet das BSI von einem einzigen Fall von Wirtschaftssabotage, bei dem ein Stahlkraftwerk in Folge eines ausgefeilten Social-Engineering-Angriffs massiv beschädigt wurde. Beim Social Engineering werden nicht IT-Systeme angegriffen, sondern deren Nutzer getäuscht, um sie zum Absenken vorhandener Sicherheitsvorkehrungen zu verleiten. Erst durch den freiwillig gewährten Zugriff konnten die Angreifer ihr technisches Detailwissen zum Einsatz bringen und die Anlage durch absichtliche Fehlbedienung massiv beschädigen.

Typischerweise sind in kleinen und mittelständischen Unternehmen (KMU) – im Gegensatz zu Großunternehmen – die Sensibilität für IT-Sicherheit allgemein, für die Gefahren des Social Engineerings und das Befolgen von Sicherheitsregeln noch wenig präsent. Die Awareness für diese Thematik durch die in den Medien vermehrt berichteten Fälle ist zwar zu beobachten und führt in den Unternehmen zu einer deutlichen Entlastungen, dennoch sind Schulungen zwingend nötig.

Der Verlauf des vom BSI beschriebenen Angriffs zeigt eindrücklich, dass kein technisches Schutzsystem in der Lage ist, die „Schwachstelle Mensch“ zu kompensieren. Dieses Risiko bezieht sich nicht nur auf die Täuschung von Administratoren und Nutzern mit Zugriff auf kritische Daten und Systeme: Nicht selten missbrauchen Innentäter vorsätzlich die ihnen anvertrauten Daten für persönliche Zwecke oder die Interessen konkurrierender Unternehmen. Dies ist ein zentrales Argument für Datensparsemkeit.

Die „Schwachstelle Mensch“ ist auch ein ebenso großes Risiko für Endnutzer und Privatpersonen. Vorrangig wird sie im Bereich des Online-Banking-Betrugs und des Identitätsdiebstahls unter Vortäuschung falscher Tatsachen ausgenutzt.

Aufklärung, Schulungen und Weiterbildungen erscheinen als einzige erfolgsversprechende Möglichkeiten, die Anfälligkeit für Social Engineering und prinzipiell soziale Einfallstore nachhaltig zu verringern.

→ Technische Maßnahmen zur IT-Sicherheit werden sehr häufig aus Unwissen über das Risiko, oft versehentlich und in einigen Fällen auch absichtlich außer Kraft gesetzt. Umfassende Aufklärung und Bildungsmaßnahmen in diesem Bereich sind notwendig, um einen höheren Schutz in Bevölkerung und Wirtschaft zu erlangen und die Unternehmenskulturen hinsichtlich IT-Sicherheit zu verändern.

Weiterhin führt das BSI die im Jahr 2014 bekannt gewordenen Schwachstellen *Heartbleed* und *Shellshock* als signifikante Bedrohungen für deutsche Unternehmen an. Das Alter bei Entdeckung betrug bei *Heartbleed* zwei Jahre, bei *Shellshock* sogar ein Vierteljahrhundert. In dieser Zeit waren die Sicherheitslücken öffentlich unbekannt und konnten theoretisch unbemerkt von Angreifern ausgenutzt werden. Im Falle von *Heartbleed* war die für verschlüsselte Verbindungen genutzte Bibliothek *OpenSSL* betroffen, eine zentrale Säule der Sicherheit beim Online-Banking. Ziel des vorliegenden Gesetzesentwurfs muss eine Verkürzung dieser Zeit bis zur Entdeckung sowie die Reduktion der Anzahl an Sicherheitslücken sein.

Dass hochkritische Software, auf deren Sicherheit milliardenschwere Geschäftsmodelle und die Sicherheit von hochkritischen Informationen basieren, so lange Zeit derart schwerwiegende unentdeckte Sicherheitslücken in sich tragen konnte, lässt sich mit dem sozialen Dilemma bei der Qualitätssicherung von Open-Source-Software erklären, das bereits in einer Stellungnahme an den Bundestagsausschuss „Digitale Agenda“ ausgeführt ist[3]:

Für Unternehmen besteht kein Anreiz, in die Prüfung, Auditierung und das Testen von Allgemeingütern zu investieren, da kein wirtschaftlicher Vorteil oder ein Alleinstellungsmerkmal zu erreichen ist: Die Allgemeinheit und somit auch

---

[3] Linus Neumann, Chaos Computer Club (2014): *Effektive IT-Sicherheit fördern – Stellungnahme zur 7. Sitzung des Ausschusses „Digitale Agenda“ des Deutschen Bundestages*, abgerufen unter http://www.bundestag.de/blob/278506/7bfa0b746372768036e3780f49b96ae0/stellungnahme_linus_neumann-pdf-data.pdf

die Konkurrenz würde von den individuellen Investitionen in das öffentliche Gut ebenso profitieren. So wird eine Trittbrettfahrer-Mentalität befördert, die darin mündet, dass alle Betreiber ihre Verantwortung als erfüllt ansehen, indem sie auf dem Stand der Technik operieren.

Eine staatliche Förderung der Sicherheit dieses „Stands der Technik" ist daher im allgemeinen Interesse von Privatpersonen, Bundeseinrichtungen und Wirtschaft gleichermaßen. Insbesondere in der Wirtschaft würden nicht nur große Anbieter, sondern auch KMU profitieren, die im vorliegenden Gesetzesentwurf ebenso wenig berücksichtigt werden wie Privatpersonen.

Zur Erhöhung der Sicherheit von weit verbreiteter sicherheitskritischer Software sind folgende Maßnahmen geeignet:

1. Regelmäßige unabhängige Prüfungen von Open-Source-Software

Überprüfungen können gezielt in Auftrag gegeben werden und durch das Ausschreiben sogenannter *Bug Bounties* flankiert werden. Diese „Kopfgelder" werden als Belohnung für das Finden und Beseitigen kritischer Sicherheitslücken ausgelobt.

Die Befunde müssen veröffentlicht und die daraus resultierenden Verbesserungen der Allgemeinheit zugänglich gemacht werden. Eine intransparente und unkontrollierte Auswertung durch das BSI steht in diametralen Gegensatz zu den Schutzzielen.

→ Die Sicherheit von weitverbreiteter Open-Source-Software ist im öffentlichen Interesse und sollte durch Auditierungen und Bug Bounties aktiv gefördert werden.

2. Haftung für proprietäre Software:

Proprietäre Software entzieht sich durch Intransparenz der Möglichkeit zur unabhängigen Überprüfung durch Dritte. Gleichzeitig operieren kommerzielle Software-Lieferanten und Dienste-Anbieter größtenteils unter dem Ausschluss jeglicher Haftung. Dies ist auch aus ökonomischer Perspektive schwer nachvollziehbar: Eine Haftung würde konkrete Anreize zur Qualitätssicherung schaffen, die bisher grundsätzlich fehlen und die strukturelle Basis für die mangelnde Qualität vieler Software-Projekte sind.

Selbstverständlich muss eine solche Haftung von klaren Anforderungen hinsichtlich der Fahrlässigkeit und Schuldhaftigkeit flankiert werden und würde großen Widerstand aus dem letzten verbliebenen Wirtschaftszweig erfahren, der noch unter Ausschluss jeglicher Haftung operieren darf. Dennoch sei an dieser Stelle sei der Hinweis erlaubt, dass sich in einer solchen Haftung auch die Chance verbirgt, dem für IT-Produkte oft erfolglos beanspruchten Qualitätsmerkmal „Made in Germany" zu nennenswerter Reputation zu verhelfen.

→ Klare Haftungsregeln würden zu einem starken ökonomischen Anreiz für die Hersteller von proprietärer Software führen, IT-Sicherheit pro-aktiv zu betreiben.

Oft unterliegen IT-Systeme Patch-Zyklen im Bereich mehrerer Monate und befinden sich in entsprechend hoffnungslos veraltetem Zustand, ohne dass einer Ausnutzung durch sekundäre Maßnahmen vorgebeugt wird. Bei fahrlässigen

Verschleppungen sollten verantwortliche Anbieter oder Dienstleister im Schadensfall haften. So würde ein klarer ökonomischer Anreiz entstehen, Systeme auf einem aktuellen Stand, und damit die Angriffsfläche möglichst gering zu halten.

→ Haftung würde als unmittelbarer monetärer Anreiz eine sehr viel konkretere Wirkung entfalten, als die im vorliegenden Gesetzesentwurf vorgesehenen zwei-jährlichen Nachweispflichten.

Kritische Infrastruktur. Das einzige vom BSI dokumentierte Angriffsmuster, das 2014 im Bereich der kritischen Infrastrukturen stattgefunden hat, ist erneut das Social Engineering. Ziel dieses Angriffs war jedoch das *„Übermitteln einer Kopie eines amtlichen Lichtbildausweises und [der] Bankverbindung des Gehaltskontos"* der Opfer – eine klassisches Täuschungsszenario, bei dem Privatpersonen um ihr Vermögen erleichtert werden. Und so wurden mittels *„gefälschten Unterschriften die Bankkonten der Betroffenen aufgelöst oder neue EC-Karten samt PIN an eine neue Adresse in China angefordert."* Auf einen Ausfall der Infrastruktur wurde von Seiten der Angreifer nicht hingewirkt. Auch für vorherige Jahre[4,5] ist nicht ein einziger derartiger Vorfall dokumentiert. Entsprechend attestiert das BSI schon im Jahr 2009[6]:

Bei den Betreibern der so genannten Kritischen Infrastrukturen können IT-Sicherheitsbewusstsein und -kompetenz sowohl auf Managementebene als auch in der Umsetzung durchweg als hoch eingeschätzt werden.

→ Auch wenn der Chaos Computer Club diese Einschätzung nicht teilt[7], so ist der einseitige Fokus auf ein bisher nicht realisiertes Bedrohungsszenario schwer nachvollziehbar, während häufig

---

[4] Bundesamt für Sicherheit in der Informationstechnik (2013): *Fokus IT-Sicherheit,* Version vom 13.11.2013, abgerufen unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Fokus_IT-Sicherheit_2013_nbf.pdf

[5] Bundesamt für Sicherheit in der Informationstechnik (2011): *Die Lage der IT-Sicherheit in Deutschland,* barrierefreie Version vom 16.06.2011, abgerufen unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011.pdf

[6] Bundesamt für Sicherheit in der Informationstechnik (2009): *Die Lage der IT-Sicherheit in Deutschland,* Version vom Januar 2009, abgerufen unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2009_pdf.pdf

[7] Nord, Friedrich (2014): *Stellungnahme zur Konsultation des „IT-Sicherheitskatalog" gem. §11 Abs. 1a Energiewirtschaftsgesetz*, Version vom 12.02.2014, abgerufen unter http://ccc.de/system/uploads/143/original/BNetzA-Konsultation-ITSicherheit-Stromnetz.pdf

erfolgreiche Angriffe mit hohen Anzahlen an geschädigten Personen vollständig ignoriert werden.

Steigerung der Bürokratie statt aktiver Erhöhung der Sicherheit

Die für IT-Sicherheit verantwortlichen Abteilungen in deutschen Unternehmen sind hauptsächlich mit der bürokratischen Verwaltung ausführlicher Checklisten beschäftigt. Der Verwaltungsaufwand zur Einhaltung von allerlei Zertifizierungsvorgaben und Normen geht dabei nicht selten zulasten pro-aktiver technischer Maßnahmen zur nennenswerten Erhöhung der IT-Sicherheit: Allein die Verwaltung der Compliance-Vorgaben einer mittelgroßen Organisation erschöpft schon die vorhandenen Ressourcen. So verkommt das dynamische Feld der IT-Sicherheit nicht selten zu einem steifen Korsett, das Innovation und Agilität verhindert, ohne dabei signifikant zur IT-Sicherheit beizutragen, geschweige denn Raum zur Steigerung zu lassen.

Angreifer hingegen agieren frei von regulatorischen und organisatorischen Zwängen und konzentrieren sich auf real-existierende Schwächen. Zur effizienten Verteidigung muss daher technische Innovation von individuellen Sicherheitskonzepten flankiert, und die Agilität auch in der Abwehr erhalten bleiben.

Im vorliegenden Gesetzesentwurf wird ein gegenteiliger Schwerpunkt gelegt: In der Regel bereits bestehende Sicherheitskonzepte sollen einheitlich verschriftlicht, und Auditierungen lückenlos protokolliert werden. So werden die neu zu bestimmenden Alarmierungskontakte hauptsächlich damit befasst sein, ihre Auskunfts-, Dokumentations- und Berichtspflichten zu erfüllen.

→ Eine weitere Bürokratisierung der IT-Sicherheit geht zulasten dringend notwendiger pro-aktiver Maßnahmen zur effektiven Erhöhung der IT-Sicherheit.

Bedauerlicherweise wird im vorliegenden Gesetzesentwurf zusätzlich die Gelegenheit versäumt, durch eine vorgeschriebene Sicherheitsanforderungen eine pro-aktive Herangehensweise zu erzwingen, oder zumindest zu incentivieren: Insbesondere im Bereich der kritischen Kommunikationsinfrastrukturen besteht nennenswertes Verbesserungspotenzial über den viel zitierten „Stand der Technik“ hinaus:

- Zentrale Strukturen sollten aufgebrochen werden, um die Resilienz zu erhöhen, und gleichzeitig Angriffsfläche und Schadenspotenzial zu verringern.
- Starke Sicherheitsstandards sollten vorgeschrieben werden. Insbesondere sollte eine Ende-zu-Ende-Verschlüsselung zum Standard bei Kommunikationsdiensten gehören.

Vorschlagsrecht der Betreiber führt gewünschten Effekt der Sicherheitsstandards ad absurdum

Der neu formulierte §8a BSI-Gesetz verpflichtet Betreiber kritischer Infrastrukturen, *angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und*

Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen.

Diese Vorkehrungen seien als angemessen anzusehen, wenn sie

1. dem Stand der Technik entsprechen,
2. der Aufwand nicht außer Verhältnis zum Schadensfall steht.

→ Die Festlegung auf den „Stand der Technik" schließt jedes Potenzial für eine nennenswerte, pro-aktive Verbesserung der Schutzvorkehrungen kategorisch aus.

Gleichzeitig sind diese Anforderungen so unscharf definiert, dass sie eine große Rechtsunsicherheit in sich bergen, die offenbar durch die Absätze 2 und 3 beseitigt werden soll:

Darin wird den Betreibern kritischer Infrastrukturen ein Vorschlagsrecht für branchenspezifische Sicherheitsstandards eingeräumt. Auf Antrag stellt das BSI fest, ob diese den Anforderungen nach Absatz 1 genügen und beseitigt somit die drohende Rechtsunsicherheit. Das Erfüllen dieser Sicherheitsstandards sollen Betreiber dann mindestens alle zwei Jahre nachweisen, indem eine *Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel* übermittelt wird.

Bei der Abstimmung der spezifischen Sicherheitsstandards besteht für die Branchenvertreter zunächst die Herausforderung, die jeweils bestehenden Standards miteinander zu vergleichen und in eine gemeinsame Sprache zu überführen. Der Vergleich wird einen großen Bereich an Sicherheitsanforderungen ergeben, der von allen Branchenvertretern abgedeckt wird, sowie mehrere Teilbereiche, in denen einige Vertreter stärkere Schutzmaßnahmen ergriffen haben als andere.

Im Sinne einer Erhöhung der IT-Sicherheit aller Betreiber wäre es natürlich wünschenswert, dass mindestens die Summe aller Maßnahmen als neuer Standard definiert wird oder im Idealfall gar darüber hinaus gehende Ziele definiert werden.

Die ökonomischen Anreize der Branchenvertreter stehen diesem Ziel jedoch diametral entgegen: Wenn stattdessen der Minimalkonsens als Branchenstandard beschlossen und vorgeschlagen wird, werden Investitionskosten und das potenzielle Risiko, die eigenen Sicherheitsvorgaben nicht erfüllen zu können, vermieden.

→ Das Vorschlagsrecht für branchenspezifische Standards wird dazu führen, dass bereits bestehende Minimalstandards festgeschrieben werden. Auch hier ist jedes Potenzial für eine nennenswerte, pro-aktive Verbesserung der Schutzvorkehrungen ausgeschlossen.

Geschwächter Datenschutz führt zu höheren Risiken

Schon beim Blick auf die aktuell gültige Version des TKG vom 25. Juli 2014 ist aus technischer Perspektive nicht nachvollziehbar, auf welche Weise die Bestandsdaten der Nutzer zum Erkennen, Eingrenzen oder Beseitigen von Fehlern oder Störungen eines technischen Gerätes von Bedeutung sein könnten.

Störungen und Fehler sind akute Phänomene, bei denen die Funktionalität des betroffenen Systems beeinträchtigt ist. Das Erkennen gestaltet sich demnach nicht schwierig und wird durch langfristige Datenvorhaltung nicht erleichtert. Hingegen ist im Rahmen der Beseitigung und des Eingrenzens ein temporäres Speichern von Verkehrsdaten durchaus hilfreich und teilweise notwendig. Der Verwendung von Bestandsdaten kommt jedoch in keinem dieser Fälle eine Notwendigkeit zu.

Schon heute nehmen Anbieter unter Berufung auf § 100 Abs. 1 TKG eine für diesen Zweck unnötige Speicherung von Verkehrsdaten über mehre Tage oder Wochen vor. Dabei werden Informationen über Telefonverbindungen, Standorte und Internetverbindungen aller Kunden auf Vorrat gespeichert. Nach einer Erhebung des AK Vorratsdatenpeicherung variieren die Vorhaltezeiten zwischen 3 und 180 Tagen.[8] Schon diese große Spannbreite zeigt eindrücklich, dass den gesammelten Daten keine Bedeutung für den Erhalt des Systembetriebs zukommt: Selbst eine mehr als drei oder gar 180 Tage andauernde Störung ließe sich wohl kaum noch mit Hilfe von Verkehrsdatensammlungen beheben. Dies gilt auch für den Bereich von *„Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können."*

Der vorliegende Gesetzesentwurf soll Risiken der IT-Sicherheit minimieren, Einbrüche in informationstechnische Systeme verhindern und Möglichkeiten zum Datenmissbrauch einschränken. Eine langfristige Speicherung trägt dazu nicht bei, sondern führt umgekehrt zu einer Erhöhung des Angriffsrisikos und zu einer Erhöhung des Schadenspotenzials möglicher Angriffe.

Die 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18. und 19. März 2015 in Wiesbaden[9] bringt daher valide Argumente gegen diese umfassende Vorratsdatenspeicherung vor, die auch in der Stellungnahme des Bundesrats[10] zum vorliegenden Gesetzesentwurf bekräftigt werden.

→ Sowohl dem bestehenden als auch dem hier vorgeschlagenen § 100 Abs. 1 TKG kommt keine Bedeutung bei der Erkennung, Eingrenzung und Behebung von technischen Störungen, Fehlern und Angriffen zu.

---

[8] Arbeitskreis Vorratsdatenspeicherung (2015): *Speicherdauer (Übersicht)*, Version vom 26. März 2015, abrufbar unter http://wiki.vorratsdatenspeicherung.de/index.php?title=Speicherdauer&oldid=128634

[9] Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. und 19. März 2015: *IT-Sicherheitsgesetz nicht ohne Datenschutz!* abrufbar unter https://www.datenschutz.hessen.de/k89.htm#entry4320

[10] Bundesrat Drucksache 643/1/14, abrufbar unter http://www.bundesrat.de/SharedDocs/drucksachen/2014/0601-0700/643-1-14.pdf?__blob=publicationFile&v=1

→ Eine Beschränkung des zulässigen Verwendungszwecks der Daten ist dringend geboten.

→ Konkrete zeitliche Einschränkungen der zulässigen Vorhaltungsdauer sind dringend geboten.

Das Vertrauensproblem des BSI wird nicht gelöst

Zusammen mit dem IT-Fachverband BITKOM betreibt das BSI seit November 2012 eine Meldestelle für Angriffe auf Computersysteme im Rahmen der *Allianz für Cyber-Sicherheit*. Bisher blieb diese Initiative bahnbrechende Erfolgsmeldungen schuldig, und das BSI konnte sich in der Industrie nicht als Ansprechpartner erster Wahl etablieren. Im vorliegenden Gesetzesentwurf sollen Betreiber kritischer Infrastrukturen nun zur Zusammenarbeit mit der Behörde verpflichtet werden.

Dass sich eine vertrauensvolle freiwillige Zusammenarbeit nicht etablieren konnte, ist der Vertrauenskrise des BSI geschuldet, für die es zwei Auslöser gibt:

1. Das BSI steht nicht im Ruf, im akuten Fall kompetente und zeitnahe Unterstützung leisten zu können.
2. Es bestehen konkrete Anlässe zum Zweifel daran, dass das BSI ausschließlich der Sicherheit von Computern und Netzen verpflichtet ist und nicht im Rahmen von Aufgaben bei der sogenannten „inneren Sicherheit“ gezielt auf eine Schwächung von Endgeräten und Kommunikationsinfrastrukturen hinarbeitet.

So war das BSI schon im Jahr 2007 an zentraler Stelle an der Entwicklung einer Schadsoftware zum Einsatz gegen Bundesbürger beteiligt[11] und hat mit dem Standard De-Mail einen gezielt geschwächtes System definiert. Die akkreditierten Anbieter gehen inzwischen in eigenständigen Initiativen freiwillig über das verlangte Sicherheitsniveau hinaus[12], um das öffentliche Ansehen des Systems zu retten.

---

[11] Bundesamt für Sicherheit in der Informationstechnik (2009): *Bedrohung der Informationssicherheit durch den gezielten Einsatz von Schadprogrammen*, Version 1.1 vom 3.04.2007, abrufbar unter

- https://netzpolitik.org/wp-upload/Leitfaden-Schadprogramme-0-Deckblatt.pdf
- https://netzpolitik.org/wp-upload/Leitfaden-Schadprogramme-1-Ueberblick.pdf
- https://netzpolitik.org/wp-upload/Leitfaden-Schadprogramme-2-Massnahmen.pdf
- https://netzpolitik.org/wp-upload/Leitfaden-Schadprogramme-3-Kurztest.pdf

[12] Pressemitteilung der Deutschen Telekom vom 9. März 2015: *De-Mail: Ende-zu-Ende-Verschlüsselung kommt*, abrufbar unter http://www.telekom.com/medien/produkte-fuer-privatkunden/271200

Wurzel der Zweifel an der Unabhängigkeit des BSI ist seine mangelnde Unabhängigkeit vom BMI. Insbesondere in Anbetracht der im Gesetzesentwurf geforderten Berichtspflichten, die das im BSI gesammelte Wissen über Schwachstellen und Angriffe potenzieren wird, muss diese Unabhängigkeit zwingend hergestellt werden: Die Begehrlichkeiten des BMI zum Erwerb des Wissens über ausnutzbare Sicherheitslücken zur Nutzung in Angriffen sind ausführlich dokumentiert[13], und eine entsprechende Sekundärverwertung des beim BSI gesammelten Wissens ist nicht nur nicht auszuschließen, sondern im Gegenteil sogar sehr wahrscheinlich.

→ Die Ausweitung des Aufgabenbereichs des BSI sowie die Kritikalität der beim BSI gesammelten Informationen über Sicherheitslücken erfordert zwingend die Aufstellung des BSI als unabhängige Bundesbehörde mit unzweideutigem Sicherheitsauftrag.

[13] ZEIT Online vom 9. November 2014: *BND will Sicherheitslücken kaufen und ausnutzen*, abgerufen unter http://www.zeit.de/digital/internet/2014-11/bnd-zero-day-exploit-sicherheit

Fazit

Keiner der in diesem Gesetzesentwurf vorgesehenen Schritte ist geeignet, zu einer sinnvollen Erhöhung der IT-Sicherheit in Deutschland beizutragen. Die Auskunfts-, Dokumentations- und Berichtspflichten, die Unternehmen auferlegt werden sollen, erhöhen im Gegenteil den Bürokratieaufwand und gehen daher zulasten von Ressourcen, die andernfalls für pro-aktive Maßnahmen zur tatsächlichen Erhöhung der IT-Sicherheit verwendet werden könnten.

Den großflächigen Angriffen auf Privatpersonen und den daraus resultierenden Schäden wird nicht entgegen getreten. Stattdessen soll durch zentrale und intransparente Strukturen Angriffswissen auf Regierungsebene zusammen getragen werden.

Für die im Gesetzesentwurf mandatierte langfristige Vorhaltung von Verkehrsdaten zum Zwecke der Störungsaufklärung gibt es aus technischer Perspektive keine Grundlage. Demgegenüber steht ein erhöhtes Missbrauchspotenzial, das zu einer effektiven Erhöhung des Risikos führt.

Prof. Dr. Gerrit Hornung, LL.M.

Lehrstuhl für Öffentliches Recht, Informationstechnologierecht und Rechtsinformatik

UNIVERSITÄT PASSAU
Juristische Fakultät

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)284 G

Telefon Prof. Dr. Gerrit Hornung, LL.M. 0851 509-2380
Telefax 0851 509-2382
e-mail gerrit.hornung @uni-passau.de

Datum 18. April 2015

Stellungnahme

zur öffentlichen Anhörungen des Innenausschusses des Deutschen Bundestages am 20. April 2015

zum Gesetzentwurf der Bundesregierung für Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 25. Februar 2015, BT-Drs. 18/4096

Gliederung

1 Grundsätzliche Einordnung

Der Gesetzentwurf adressiert ein **hochgradig relevantes Problem der Informationsgesellschaft**. In dieser geraten Bürger, Wirtschaft und Staat in erhebliche Abhängigkeit zu der Verfügbarkeit funktionsfähiger, integrer und vertraulicher Informationstechnologie (IT). Die Risiken, die aus unsicherer IT entstehen können, betreffen direkt wichtige Bereiche des gesellschaftlichen und individuellen Lebens. Ursachen können Fehler und Mängel der verwendeten Systeme, aber auch private und staatliche Angreifer sein. Die Bedrohungen für die IT-Sicherheit in Deutschland sind real und konkret.[1]

Aus rechtlicher Sicht ist die Gewährleistung der IT-Sicherheit zum einen **Teil der staatlichen Infrastrukturverantwortung**. Zum anderen hat der Staat auch eine Pflicht, sich schützend und fördernd vor die Grundrechte der Bürgerinnen und Bürger zu stellen. Dies betrifft eine **Vielzahl von Grundrechten**, deren Ausübung heutzutage nicht mehr ohne funktionsfähige IT möglich ist, insbesondere aber das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Bürger, Wirtschaft und Staat sind besonders betroffen, wenn es um Kritische Infrastrukturen geht, deren Ausfall nicht nur einzelnen Individuen und Organisationen, sondern einer Vielzahl von ihnen Nachteile zufügen können. Wie in anderen Bereichen der Regulierung Kritischer Infrastrukturen stellt sich auch für die IT-Sicherheit die **Frage des sinnvollen Maßes an staatlichen Vorgaben einerseits, Selbstverantwortung und Selbstregulierung andererseits**. IT-Sicherheitsmaßnahmen weisen hier Besonderheiten auf: Sie sind typischerweise Vorsorgemaßnahmen, die kostenträchtig und gerade im Erfolgsfall schwer zu rechtfertigen sind, weil die hypothetischen Schadensfälle schwer plausibel gemacht werden können. Kommen IT-Sicherheitsvorfälle vor, so betreffen diese in aller Regel nicht nur einen Akteur, weil dieselben Systeme bei vielen anderen eingesetzt werden. Schließlich haben die Verantwortlichen ein natürliches Interesse, Vorfälle (vor allem, aber nicht nur solche, aus denen sich ein vorwerfbares Verhalten ergibt) nicht publik werden zu lassen, weil der Verlust von Reputation und Kundenvertrauen befürchtet wird.

Wenn die intrinsischen Anreize für kostenträchtige Maßnahmen gering, die potentiellen Auswirkungen von Vorfällen weit verbreitet, die Kommunikation hierüber aber unterentwickelt ist, so ist eine **Kombination aus materiellen Standards mit Meldepflichten für IT-Sicherheitsvorfällen eine grundsätzlich sinnvolle Strategie**. Diese wird in vergleichbaren Fällen bereits verfolgt, etwa im Datenschutzrecht (§ 42a BDSG, § 15a TMG, § 109a TKG, § 83a SGB X). Die Übernahme dieser Regelungsstrategie ist ein zu unterstützender

---

[1] S. nur *BSI*, Die Lage der IT-Sicherheit in Deutschland 2014.

Schritt zur Verrechtlichung der IT-Sicherheit, der durch den **kooperativen Ansatz einer Zusammenarbeit zwischen Behörden und Wirtschaft** auch Chancen für die Verbesserung der Widerstandsfähigkeit der zugrundeliegenden Infrastrukturen bietet.

Die **Abstufung zwischen erheblichen und nicht erheblichen Störungen** (nur erstere sind meldepflichtig) sowie zwischen Störungen **mit und ohne tatsächlichen Auswirkungen** (nur bei ersteren muss der konkrete Betreiber genannt werden, dessen System tatsächlich ausgefallen oder beeinträchtigt wurde) ist **sinnvoll** und berücksichtigt die berechtigten Interessen der Betreiber, nicht mit aufwändigen Meldungen zu unwesentlichen Vorfällen überfrachtet zu werden sowie pseudonym agieren zu können, sofern es nicht zu tatsächlichen Ausfällen oder Beeinträchtigungen gekommen ist.

Gerade weil der Gesetzentwurf ein sinnvolles Anliegen verfolgt, ist darauf hinzuweisen, dass **wesentliche, gleichfalls sinnvolle Inhalte einer umfassenden IT-Sicherheitsstrategie nicht adressiert werden**. So sind beispielsweise IT-Sicherheitsvorfälle bei Unternehmen, die nicht Betreiber Kritischer Infrastrukturen sind, nicht erfasst. Dies betrifft insbesondere die gezielte Wirtschaftsspionage oder sonstige Angriffe auf Unternehmen, die keine Kritische Infrastruktur nach § 2 Abs. 10 BSIG-E betreiben. Ein Handeln des Staates erscheint daneben insbesondere dort wichtig, wo die Betreiber von IT-Systemen keine eigenen Anreize zur Verbesserung der IT-Sicherheit haben (diese sind beim Betrieb Kritischer Infrastrukturen grundsätzlich vorhanden, weil bei Ausfällen direkt Kundeninteressen verletzt werden), nämlich in den Bereichen der Forschung und Entwicklung, der Verfügbarkeit von Technologien zur Selbsthilfe der Bürger (vor allem Verschlüsselungsverfahren) und der unabhängigen Prüfung unter Verwendung von Open Source-Technologien.

2 Europarechtliche Aspekte

Da derzeit mit dem Entwurf der Europäischen Kommission für eine Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union (NIS-RL-E)[2] ein **paralleles Gesetzgebungsverfahren** betrieben wird, stellt sich Frage der Vereinbarkeit des Vorschlags mit den absehbaren europäischen Regelungen. Im Grundsatz verfolgen beide Vorschläge dabei das **identische Ziel** der Verbesserung der IT-Sicherheit bei Kritischen Infrastrukturen und sehen weitgehend kongruente Mittel vor, nämlich zum einen die Vorgabe von IT-Sicherheitsstandards, zum anderen Meldepflichten bei IT-Sicherheitsvorfällen. **Dennoch gibt es Unterschiede**, von denen hier

[2] KOM(2013) 48.

einige anhand der Zusammenstellung in der letzten Position des Rates vom 5. März 2015[3] erläutert werden sollen:

- Noch nicht absehbar ist, wie groß die Unterschiede hinsichtlich des **Adressatenkreises** sein werden. Die Kommission wollte die öffentliche Verwaltung explizit in die Pflicht nach Art. 14 Abs. 1 NIS-RL-E einbeziehen, scheint sich damit aber nicht durchsetzen zu können. In der letzten Position des Rates werden nunmehr aber „operator" erfasst, die nach der Definition in Art. 3 Abs. 8 NIS-RL-E „**public or private entities**" sein können. Hieraus könnten sich Unterschiede zum Gesetzentwurf ergeben. In den meisten anderen Bereichen dürfte es wegen der offenbar beabsichtigten Befugnis der Mitgliedsstaaten zur Definition der betroffenen Betreiber möglich sein, im Rahmen der Verordnung nach § 10 Abs. 1 BSIG-E richtlinienkonform zu agieren.

- Nach Art. 6 NIS-RL-E müssen die Mitgliedsstaaten **nationale Anlaufstellen** einrichten. Dem genügt der Gesetzentwurf in seiner vorliegenden Form. Weiterer gesetzgeberischer Bedarf könnte sich je nach dem endgültigen Inhalt der Vorgaben in Art. 8a und Art. 8b NIS-RL-E hinsichtlich der Zusammenarbeit mit anderen nationalen Behörden und der ENISA ergeben.

- In allen bisher bekannten Positionen beschränken sich die europäischen Entwürfe hinsichtlich der Meldepflichten auf Sicherheitsvorfälle („**incidents**"). Diese werden in Art. 3 NIS-RL-E definiert als „alle Umstände oder Ereignisse, die tatsächlich negative Auswirkungen auf die Sicherheit haben". Der vorliegende **Gesetzentwurf geht an mehreren Stellen hierüber hinaus**, wenn er in § 8b Abs. 4 BSIG-E auch Störungen umfasst, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der betriebenen Kritischen Infrastrukturen führen „können".

- Hinsichtlich einer **Veröffentlichung der gewonnenen Erkenntnisse** enthält Art. 14 Abs. 4 NIS-RL-E eine Befugnis der Behörde. Diese ist **zugleich weiter und enger als die Regelung in § 8d Abs. 1 BSIG-E**. Sie ist weitergehend, weil sie sich explizit auf „individual incidents" beziehen wird und die Interessen der Öffentlichkeit an der gewonnenen Information berücksichtigt. Demgegenüber enthält sie anders als der nationale Vorschlag eine Pflicht zur Anhörung des betroffenen Unternehmens.

- Art. 15 Abs. 2 lit. a NIS-RL-E wird vermutlich vorsehen, dass die nationalen Behörden die **Befugnis** erhalten müssen, von den Betreibern Kritischer Infrastrukturen

---

[3] Abrufbar unter http://statewatch.org/news/2015/mar/eu-council-NIS-consolidated-multi-col-6788-15.pdf.

die **Durchführung eines Sicherheitsaudits zu verlangen**. Dies geht **deutlich über die Regelung in § 8a Abs. 3 BSIG-E hinaus**, der solche Audits gleichberechtigt neben Zertifizierungen und Prüfungen stellt und alle drei lediglich fakultativ nennt.

- In Art. 15 Abs. 3 NIS-RL-E ist vorgesehen, dass die zuständige Behörde „**verbindliche Anweisungen**“ an die Betreiber Kritischer Infrastrukturen zu richten. Auch dies ergibt sich **nicht aus dem Gesetzentwurf**.
- Art. 17 NIS-RL-E sieht die Pflicht für die Mitgliedsstaaten vor, **Sanktionen für eine Verletzung** der Pflichten aus Art. 14 und Art. 15 NIS-RL-E vorzusehen. Dies betrifft sowohl die Einhaltung der IT-Sicherheitsstandards selbst, als auch eine Verletzung der entsprechenden Meldepflichten. Beides enthält der **vorliegende Gesetzentwurf nur sehr rudimentär** (s.u. 4.3 und 5.4).

Insgesamt ergeben sich die größten Unterschiede zu dem geplanten europäischen Vorhaben auf der Ebene der Verpflichteten sowie hinsichtlich der Sanktionsbefugnisse des BSI. Zumindest letzteres ließe sich mutmaßlich nach Abschluss des europäischen Gesetzgebungsvorhabens relativ leicht in das Gesetz integrieren. Sollten sich auf europäischer Ebene hingegen erweiterte **Auswirkungen hinsichtlich der betrieblichen Prozesse** ergeben, sollte zunächst der europäische Gesetzgebungsprozess **abgewartet werden**, um einen nachträglichen Änderungsaufwand bei den Betroffenen Anbietern zu vermeiden.

3 Anwendungsbereich

Angesichts der Pflicht zur Implementierung potenziell kostenträchtige IT-Sicherheitsmaßnahmen und mehr oder weniger aufwändiger Meldeverfahren ist es für die betroffenen Unternehmen von erheblicher Bedeutung zu wissen, ob sie von dem Gesetzentwurf erfasst sind.

3.1 Begriff der Kritischen Infrastrukturen

Die Begriffsbestimmung in § 2 Abs. 10 BSIG-E ist mit Blick auf ihren **Bestimmtheitsgrad vielfach kritisiert** worden.[4]

In der Tat ist der personelle Anwendungsbereich auf Basis des Entwurfs in vielen Fällen nicht ermittelbar. Viele Unternehmen sind in den „Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie

[4] Z.B. *Roos*, K&R 2013, 769, 770; *Heinickel/Feiler*, CR 2014, 708, 713 f.; *Leisterer/Schneider*, CR 2014, 574; 577; *Bräutigam/Wilmer*, ZRP 2015, 38, 40 sowie zahlreiche Stellungnahmen der betroffenen Wirtschaftsverbände.

Finanz- und Versicherungswesen“ tätig (§ 3 Abs. 10 Nr. 1 des Entwurfs). Auch die Präzisierung in Nr. 2 (Einrichtungen, Anlagen oder Teile von diesen, die für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden) führt in vielen Fällen nicht dazu, dass Unternehmen die Anwendbarkeit des Entwurfs auf sich selbst dem Gesetz entnehmen können.

Für die Verordnungsermächtigung in § 10 Abs. 1 BSIG-E gilt **Art. 80 Abs. 1 Satz 2 GG**, wonach Inhalt, Zweck und Ausmaß der erteilten Ermächtigung im Gesetze bestimmt werden müssen. Unter Wesentlichkeitsgesichtspunkten ist der **personale Anwendungsbereich** eines Gesetzes in jedem Fall eine **wichtige Frage**. Insoweit gibt die Vorgabe in Nr. 2 dem Verordnungsgeber Leitlinien für die nähere Bestimmung in die Hand. Es wird danach maßgeblich auf die Auswirkungen eines Versagens der jeweiligen Infrastruktur ankommen, nicht auf die Größe des Unternehmens, seine Leistungsfähigkeit oder die Komplexität der betriebenen Infrastruktur. Unter Berücksichtigung dieser Kriterien erscheint die **Übertragung an den Verordnungsgeber als vertretbar**.

Rechtspolitisch und mit Blick auf den Wesentlichkeitsgrundsatz wäre eine **präzisere Bestimmung dennoch wünschenswert**. Wenn in der Gesetzesbegründung bereits die relativ konkrete Zahl von maximal 2.000 Unternehmen genannt wird, die von den Regelungen betroffen sein werden,[5] sind offenbar ja bereits Kriterien verfügbar, nach denen diese Zahl ermittelt wurde. Der durch den Gesetzgeber für den Prozess der Verabschiedung der Rechtsverordnung vorgesehene „Arbeitsprozess mit Vertretern der möglicherweise betroffenen Betreiber Kritischer Infrastrukturen und unter Einbeziehung der Expertise von externen Fachleuten“[6] kann zumindest hinsichtlich der allgemeineren Kriterien auch **im Rahmen des Gesetzgebungsverfahrens** erfolgen. Die an derselben Stelle genannten Kriterien der Quantität und Qualität sind sicher zutreffend. Sie könnten aber im Gesetz selbst (das sie bisher nicht erwähnt) genannt und weiter ausdifferenziert werden. Einige der insoweit genannten differenzierenden Maßstäbe[7] ließen sich in den Gesetzentwurf selbst integrieren und würden so einen deutlichen Gewinn an Rechtssicherheit in dem durch den parlamentarischen Gesetzgeber beschlossenen Normtext bedeuten.

Auch nach einer solchen Präzisierung wäre eine **weitere Konkretisierung** in der Rechtsverordnung nach § 2 Abs. 10 BSIG-E erforderlich. Hier sind unter rechtsstaatlichen Ge-

---

5 BT-Drs. 18/4096, 21; ein BDI Gutachten geht von wesentlich mehr Unternehmen aus eher 20.000 mit wesentlich mehr Vorfällen (http://www.bdi.eu/download_content/KPMG_IT-Sicherheit_in_Deutschland.pdf, 31).

6 BT-Drs. 18/4096, 23.

7 S. den Begründungsentwurf, BT-Drs. 18/4096, 30 f.

sichtspunkten unbedingt konkrete und handhabbare Schwellwerte anzugeben. Es wäre nicht zu rechtfertigen, wenn die Betreiber nicht erkennen könnten, ob sie von dem Gesetz überhaupt erfasst werden. Sollten insoweit Unklarheiten bleiben, wäre es erforderlich, ein **behördliches Feststellungsverfahren** vorzusehen.

3.2 Nicht von der Meldepflicht erfasste Institutionen

Anders als noch der Referentenentwurf vom 18. August 2014 nimmt die Definition der Kritischen Infrastrukturen in § 2 Abs. 10 BSIG-E nicht mehr pauschal Kommunikationstechnik des Bundes (§ 2 Abs. 3 Satz 1 und 2 BSIG) aus. Dennoch geht die Begründung davon aus, dass die **Verwaltung von Regierung und Parlament sowie die öffentliche Bundesverwaltung** und die von ihr eingesetzte Technik **nicht erfasst sind**.[8] Aus dem Gesetzentwurf ergibt sich dies an sich nicht.

In der Sache ist diese Ungleichbehandlung jedoch auch **nicht zu rechtfertigen**. Es stimmt zwar, dass insoweit die Spezialregelungen der §§ 4, 5 und 8 BSIG greifen. Wieso allerdings für die Standards der IT-Sicherheit und die Meldeverfahren unterschiedliche Maßstäbe gelten sollen, ist nicht ersichtlich. Auch Art. 3 Abs. 8 NIS-RL-E erfasst „public or private entities".

Der Gesetzentwurf gibt zutreffend an, dass der Bund für entsprechende Vorgaben für die Behörden und sonstige **Stellen der Länder** keine Kompetenz hätte. Dennoch entsteht insoweit eine **Lücke hinsichtlich der Vollständigkeit der durch das BSI gesammelten Informationen**. Sollte es bei dem vorliegenden Entwurf der europäischen Richtlinie bleiben, müssten die Länder entsprechende Vorgaben machen.

Schließlich weist die Begründung zutreffend darauf hin, dass der Bereich der **Kultur und Medien** aus Kompetenzgründen nicht erfasst sein kann.[9] Bestimmte Angebote und Systeme aus diesen Bereichen können allerdings **durchaus als Kritische Infrastrukturen** verstanden werden, wie sich an dem groß angelegten Angriff auf die französische Fernsehsendergruppe TV5Monde Anfang April 2015 gezeigt hat. Genau dieser Bereich der Massenmedien wird freilich vom Gesetzentwurf gerade nicht erfasst.

4 Vorgaben für IT-Sicherheitsstandards

Der Entwurf enthält eine Reihe inhaltlicher Vorgaben für IT-Sicherheitsstandards. Hierzu ist zu bemerken:

---

8 BT-Drs. 18/4096, 24.
9 BT-Drs. 18/4096, 24.

4.1 Inhaltliche Vorgaben

Nach § 8a Abs. 1 BSIG-E sind die Betreiber verpflichtet, „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind“. Dabei ist der **Stand der Technik** „zu berücksichtigen“.

„**Berücksichtigen**“ ist weniger, als den Stand der Technik „**einzuhalten**“ oder „**zu befolgen**“. Dies erscheint aus zwei Gründen misslich. Zum einen wird so das gesetzgeberische Ziel eines gleichmäßig hohen IT-Sicherheitsstandards **gerade nicht erreicht**. Zum anderen besteht für die betroffenen Unternehmen sogar dann Unklarheit über das konkret geforderte Sicherheitsniveau, wenn ein entsprechender Standard beschlossen wurde. Mit Blick auf die bereits geregelten und weiteren wünschenswerten Sanktionen (s.u. 4.3) ist dies schwer zu rechtfertigen.[10]

Eine **Präzisierung kann durch die branchenspezifischen Sicherheitsstandards** nach § 8a Abs. 2 BSIG-E erfolgen. Dies ist grundsätzlich sinnvoll, wirft aber die folgenden **Probleme** auf:

- In der Diskussion ist bereits auf das Problem hingewiesen worden, dass mehrere, **inhaltlich abweichende Standards für dieselbe Branche** vorgeschlagen werden;[11] dies wird im Entwurf nicht adressiert.
- Noch grundsätzlicher dürfte das Problem sein, dass das **BSI nicht von sich aus tätig werden kann**, sondern auf einen Vorschlag von Betreibern und Verbänden angewiesen ist. Unterbreiten diese keinen Vorschlag, verbleibt der Behörde nur die individuelle Beratung.
- Inhaltlich bezieht sich die Bestätigung des BSI auf die Anforderungen nach Abs. 1, also ebenfalls auf das „Berücksichtigen“ des Stands der Technik. Folglich kann die **Behörde Sicherheitsstandards anerkennen**, die **unterhalb des Stands der Technik** angesiedelt sind.
- Im Gesetz ist **nicht vorgesehen**, die erarbeiteten Standards zu pflegen und zu **aktualisieren**.

---

[10] Die europäischen Vorschläge sehen zwar eine vergleichbare Formulierung vor („having regard to the state of the art“), wegen der in Art. 2 NIS-RL-E explizit vorgesehenen Beschränkung auf eine Mindestharmonisierung besteht insoweit jedoch ein Spielraum für den deutschen Gesetzgeber.

[11] Z.B. *Eckardt*, ZD 2014, 599, 600 f.

- Die Einbeziehung der zuständigen Aufsichtsbehörden nach § 8a Abs. 2 Satz 3 Nr. 2 BSIG-E kann in bestimmten Fällen relativ komplex werden. Insbesondere muss die Vorschrift so verstanden werden, dass die **Datenschutz-Aufsichtsbehörden** zu beteiligen sind, soweit (wie regelmäßig) es zumindest auch um die Verarbeitung personenbezogener Daten geht.

4.2 Nachweis der Einhaltung

Nach § 8a Abs. 3 BSIG-E ist die Erfüllung alle zwei Jahre nachzuweisen. Mittel hierzu sind **Sicherheitsaudits, Prüfungen oder Zertifizierungen**. Von diesen drei Begriffen wird lediglich die Zertifizierung in § 2 Abs. 7 BSIG definiert.

Welcher Art die drei Prozesse sein sollen, wird auch in der Begründung nicht wirklich aussagekräftig beschrieben. Insgesamt **fehlen deshalb detaillierte Aussagen** zu den durchführenden Stellen (einschließlich ihrer Qualifikation und einer etwaigen Akkreditierung), Verfahrensanforderungen, materiellen Standards (etwa die wichtige Frage von Prüfungen vor Ort oder von aussagekräftigen Angriffstests) und Rechtsfolgen. Der Entwurf der Europäischen Kommission für eine Datenschutz-Grundverordnung ist genau für eine solche Nichtregelung erheblich kritisiert worden; es zeichnet sich ab, dass dies im laufenden Verfahren nachgebessert wird.

Diese Punkte sollten entweder im Gesetz oder **zumindest in der Verordnung** geregelt werden; im zweiten Fall wäre **§ 10 BSIG-E entsprechend zu ergänzen**. Insbesondere sollte sichergestellt werden, dass **tatsächlich effektive Tests durchgeführt** werden und nicht lediglich auf Hersteller- oder Betreibererklärungen vertraut wird.

4.3 Fehlen von Sanktionen

Art. 17 NIS-RL-E enthält die **Verpflichtung der Mitgliedsstaaten**, Sanktionen für die Verletzung der in Art. 14 und Art. 15 NIS-RL-E genannten Pflichten einzuführen. Dies bezieht sich auch auf die Implementierung angemessener technische und organisatorische Maßnahmen. Eine solche allgemeine Sanktionsregelung **fehlt im Gesetzentwurf**. Im Falle der Verabschiedung der Richtlinie wäre deshalb eine Ergänzung des vorliegenden Gesetzes erforderlich. Der Gesetzgeber **sollte dies jedoch nicht abwarten**, sondern die Anbieter Kritischer Infrastrukturen insoweit **in die Pflicht nehmen**. Hierzu bietet sich die Einführung entsprechender Bußgeldtatbestände an.

Unabhängig davon enthält der vorliegende Gesetzentwurf in Bezug auf die Sanktionen eine **Ungleichbehandlung, deren Grund nicht ersichtlich ist**. Von allen im Entwurf adressierten Anbietern machen sich ausschließlich die Anbieter nach dem Telemediengesetz (§ 16 Abs. 2 Nr. 2 TMG-E; diese werden regelmäßig noch nicht einmal Kritische Infra-

strukturen betreiben) und Telekommunikationsgesetz (§ 149 Nr. 21a TKG-E) bußgeldpflichtig, wenn sie Sicherheitsmechanismen einsetzen, die nicht dem Stand der Technik entsprechen. Diese Ungleichbehandlung wird auch in der Begründung nicht erklärt. Es ist überdies nicht ersichtlich, wie sie gerechtfertigt werden könnte. Sie sollte zugunsten einer gleichmäßigen Regelung von Ordnungswidrigkeitentatbeständen **für alle Verpflichteten** bereinigt werden.

4.4 Haftungsfragen

Das Gesetz adressiert die wichtige Frage einer zivilrechtlichen Haftung für eine Verletzung der Pflichten aus § 8a BSIG-E nicht. Dies bedeutet allerdings nicht, dass die Anbieter von Kritischen Infrastrukturen nicht auch insoweit durch das Gesetz betroffen wären. Hierzu gibt es **mehrere Ansatzpunkte**:

- Da das Gesetz spezifische Verhaltenspflichten für die Anbieter regelt, werden sich mutmaßlich **Auswirkungen auf allgemeine Fahrlässigkeitsmaßstäbe** ergeben, die sowohl im Rahmen von Verträgen der Anbieter mit ihren Endkunden als auch für allgemeine Haftungsnormen wie § 823 Abs. 1 BGB eine Rolle spielen können. Soweit diese Haftungsfragen durch AGB geregelt werden, könnten die neuen technischen Pflichten eine **Auswirkung auf die gerichtliche AGB-Kontrolle** haben und dazu führen, dass sich die Anbieter insoweit nicht von der Haftung befreien können.
- Demgegenüber dürfte das weitgehende Fehlen einer Bezugnahme auf Dritte, die ebenfalls ein Interesse an den gemeldeten Informationen haben können, dazu führen, dass (anders als etwa bei § 42a BDSG, § 15a TMG, § 109a TKG, § 83a SGB X)[12] die **Meldepflichten keine Schutzgesetze im Sinne von § 823 Abs. 2 Satz 1 BGB** sein dürften. Dies wird aus europarechtlicher Sicht künftig vermutlich sogar vorgegeben werden weil in Art. 14 Abs. 2 NIS-RL-E eine Bestimmung vorgesehen ist, wonach die Meldungen die Anbieter nicht dem Risiko einer verschärften Haftung aussetzen dürfen.
- Für **TK-Anbieter** könnten die neuen Pflichten allerdings im Rahmen der allgemeinen **Haftungsregeln nach §§ 44, 44a TKG** relevant werden. Dies dürfte insbesondere bei der spezifisch auf den Kunden gerichteten neuen Informationspflicht nach § 109a Abs. 4 TKG der Fall sein.

Unklar ist demgegenüber, ob sich auch **Auswirkungen auf die Haftung von Verbraucherinnen und Verbraucher** ergeben. Einen Ansatzpunkt hierfür könnte ebenfalls § 109

[12] S. *Hornung*, in: Roßnagel, Recht der Telemediendienste, 2013, § 15a TMG Rn. 51 m.w.N.

Abs. 4 TKG-E darstellen, wenn nach einer Information durch den TK-Anbieter das Sicherheitsproblem eines privaten Computers nicht behoben wird. Ob sich durch diese Information im Zusammenspiel mit anderen allgemeinen Regeln eine Verkehrssicherungspflicht der Privatnutzer ergibt, ist allerdings völlig offen.

Schließlich kann sich aus allgemeinen Regeln **auch eine Haftung des Bundes für das Handeln des BSI** ergeben. Zumindest gegenüber den Betreibern Kritischer Infrastrukturen wird für die Pflicht in § 8b Abs. 2 Nr. 4 BSIG-E **wohl eine drittgerichtete Amtspflicht zu bejahen** sein, sodass eine Haftung nach § 839 BGB i.V.m. Art. 34 GG möglich ist.

5 Meldepflichten für IT-Sicherheitsvorfälle

Die in § 8b BSIG-E und den weiteren Regelungen vorgesehenen Meldepflichten sind ein **grundsätzlich sinnvolles Instrument**, an einer zentralen Stelle einen umfassenden Überblick über den Stand der IT-Sicherheit in Deutschland zu gewinnen. Für die Umsetzung ergibt sich an einigen Stellen noch ein **Bedarf nach Konkretisierung**, der im Rahmen der **Rechtsverordnung** nach § 10 Abs. 1 BSIG-E erfolgen kann. Dies betrifft insbesondere die Frage, was eine „erhebliche“ Störung und eine „Beeinträchtigung“ nach § 8a Abs. 4 BSIG-E ist.[13]

5.1 Spezielle Meldepflichten

§ 8c Abs. 3 BSIG-E nimmt TK-Anbieter, Betreiber von Energieversorgungsnetzen und Energieanlagen, Inhaber atomrechtlicher Genehmigungen sowie Betreiber Kritischer Infrastrukturen mit vergleichbaren Vorgaben von den Meldepflichten aus. Für diese gelten **separate Regelungen**, die jedoch **teilweise unzureichend** mit den Bestimmungen im BSIG-E **abgestimmt** erscheinen.

Auf der Ebene des **Anlasses der Meldung** offenbaren sich erhebliche **terminologische Abweichungen**. Während nach § 8b Abs. 4 BSIG-E Betreiber „erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse“ zu melden haben, „die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können oder bereits geführt haben“ werden von § 109 Abs. 5 TKG-E „Beeinträchtigungen“ von Telekommunikationsnetzen und -diensten erfasst, „die zu beträchtlichen Sicherheitsverletzungen führen oder führen können“. Ob mit dieser unterschiedlichen Wortwahl auch unterschiedliche Anforderungen gemeint sind, **wird nicht deutlich**. In der Diskussion ist der Begriff der „Beeinträchtigung“ teilweise als umfassender

[13] Z.B. *Bräutigam/Wilmer*, ZRP 2015, 38, 40 f.

aufgefasst worden. Der Begriff der „Sicherheitsverletzung“ ist im TKG an keiner Stelle definiert. Lediglich mittelbar folgt aus § 109 Abs. 5 Satz 1 TKG, dass – unter anderem – „Störungen von Telekommunikationsnetzen oder -diensten" gemeint sind.

Nach § 44b AtomG-E sind „Beeinträchtigungen“ der informationstechnischen Systeme, Komponenten oder Prozesse zu melden, „die zu einer Gefährdung oder Störung der nuklearen Sicherheit der betroffenen kerntechnischen Anlage oder Tätigkeit führen können oder bereits geführt haben“. Die begriffliche Struktur ist also ähnlich wie in § 109 Abs. 5 TKG-E, aber erneut anders als in § 8b Abs. 4 BSIG-E. **Besonders auffällig ist**, dass in § 44b AtomG-E offenbar Beeinträchtigungen zu Störungen führen, während in § 8b Abs. 4 BSIG-E genau umgekehrt Störungen Beeinträchtigungen zur Folge haben.

Wieso für die durch § 8c Abs. 3 BSIG-E ausgenommenen Anbieter **die pseudonyme Meldung nicht eröffnet wird, ist nicht recht ersichtlich**. Für den Bereich des Atomrechts mag dies keine Rolle spielen, weil es dort ohnehin nur um wenige Anbieter geht. Für den Bereich des TKG gegen sollte das abgestufte Verfahren des § 8b Abs. 4 BSIG-E entsprechend Anwendung finden. Soweit dies in § 11 Abs. 1c Satz 3 EnWG-E vorgesehen ist, bedarf der Gesetzentwurf eine Ergänzung, weil dort gar keine gemeinsame übergeordnete Ansprechstelle vorgesehen ist, sodass diese Option nach aktuellem Stand nicht wirksam werden kann.

5.2 Datenschutz- und Vertraulichkeitsaspekte

Meldungen über IT-Sicherheitsvorfälle können sensible Informationen umfassen. Dies betrifft vor allem **personenbezogene Daten**, die in Kritischen Infrastrukturen anfallen und von den Betreibern erhoben und verwendet werden. Diese Daten können in drei Fällen betroffen sein:

- Soweit der IT-Sicherheitsvorfall direkt personenbezogene Daten betrifft, können auch die **Meldepflichten nach § 42a BDSG, § 15a TMG, § 109a TKG und § 83a SGB X** einschlägig sein. Insoweit erscheint eine gegenseitige Information oder Zusammenarbeit der Behörden sinnvoll.
- Wichtiger für den Gesetzentwurf ist, dass es je nach Art des Vorfalls erforderlich sein kann, **solche Daten im Rahmen der Meldepflicht an das BSI** zu übermitteln. Hierfür enthält § 8b BSIG-E **keine explizite Ermächtigungsgrundlage**. Lediglich mittelbar lässt sich aus der – zu begrüßenden – Zweckbindung in § 8b Abs. 6 BSIG-E entnehmen, dass der Gesetzgeber davon ausgeht, die Meldungen könnten auch personenbezogene Daten enthalten. Dies sollte im Sinne von Rechtsklarheit und Transparenz **präzisiert werden**. Da die Tätigkeit des BSI im Rahmen von § 8b BSIG-E nicht unter § 14 Abs. 2 und § 15 Abs. 5 Satz 3 TMG fällt, besteht wegen

der Regelung in § 12 Abs. 1 TMG nach dem derzeitigen Gesetzentwurf insbesondere keine Befugnis zur Übermittlung von Bestands und Nutzungsdaten nach dem TMG.

- Denkbar erscheint, dass im Rahmen der Möglichkeiten und Pflichten des BSI zur **Information der Betreiber Kritischer Infrastrukturen und Dritter** ebenfalls personenbezogene Daten übermittelt oder öffentlich gemacht werden. Dies wird jedoch **durch § 8b Abs. 6 BSIG ausgeschlossen**, der sich explizit nur auf die vorstehenden Absätze der Norm bezieht. Insoweit besteht also kein Risiko für die Betroffenen.

Neben den personenbezogenen Daten natürlicher Personen können die Meldungen über IT-Sicherheitsvorfälle auch die **Interessen der betroffenen Unternehmen** beeinträchtigen, wenn entweder Betriebs- und Geschäftsgeheimnisse betroffen sind oder ihre Reputation gefährdet wird. Dem zweiten Problem wird durch das abgestufte Meldesystem in § 8b Abs. 4 BSIG-E Rechnung getragen. Wenn es tatsächlich zu einer Störung kommt, so ist die Offenlegung des konkreten Betreibers gegenüber dem BSI wegen des übergeordneten Interesses gerechtfertigt.

Nicht übersehen werden darf, dass das **BSI nicht nur ein allgemeines Lagebild** zu IT-Sicherheit in Deutschland, sondern auch sehr **konkrete Informationen** über die Anfälligkeit bestimmter Branchen in Deutschland und sogar insoweit bestehenden Probleme einzelner Unternehmen erhalten wird. Dieser Informationen sind hochgradig sensibel, weil sie etwa im Rahmen von Industriespionage verwendet werden können. Es ist deshalb **sicherzustellen, dass das BSI im Rahmen seiner Zusammenarbeit** mit anderen Behörden – insbesondere solcher **Behörden anderer Staaten**, für die eine explizite Aufgabe in § 3 Abs. 1 Satz 2 Nr. 16 BSIG-E vorgesehen ist – **keine derartigen Informationen weitergibt**. Es ist nicht recht einsichtig, wieso der Gesetzentwurf **eine explizite Pflicht insoweit nur nach § 11 Abs. 1c Satz 5 EnWG-E** vorsieht, wonach das BSI und die Bundesnetzagentur sicherzustellen haben, „dass die unbefugte Offenbarung, der ihnen nach Satz 1 zur Kenntnis gelangten Angaben ausgeschlossen wird.“ Eine solche Pflicht sollte für die nach den übrigen Meldepflichten übermittelten Angaben ebenfalls aufgenommen werden.

5.3 Informations- und Veröffentlichungspflichten des BSI

Der Gesetzentwurf wird nach der weiteren Präzisierung in der Rechtsverordnung sehr präzise regeln, welche Informationspflichten die Betreiber Kritischer Infrastrukturen haben. Demgegenüber ist der weitere **Umgang des BSI mit den erlangten Informationen** weniger durchreguliert und in Bezug auf die Information anderer Stellen nur **fragmentarisch** ausgestaltet.

Der Entwurf betont, dass der **verstärkte Schutz der Bürgerinnen und Bürger im Internet** ein wesentliches Ziel ist. Nach dem aktuellen Stand wird dieses Ziel jedoch **nur mittelbar** bewirkt, nämlich über die Verbesserung der IT-Sicherheit in den Kritischen Infrastrukturen; eine Einbindung der Bürgerinnen und Bürger selbst ist nicht vorgesehen. Auch die Gesetzesbegründung z.B. zu § 3 Abs. 1 Satz 2 Nr. 2 des Entwurfs nennt für „Dritte", die auf Antrag informiert werden können, nur Einrichtungen und Unternehmen.[14] Insgesamt sollten die Pflichten und Befugnisse des BSI zur Information Dritter und der Öffentlichkeit **erweitert werden**; dies kann jedoch nur unter Berücksichtigung der legitimen Interessen der Betreiber und der Risiken für die IT-Sicherheit erfolgen.

5.3.1 Interessen der Betreiber und übergeordneter Geheimhaltungsinteressen

Gegen eine Weitergabe der durch die Meldungen erlangten Informationen an Dritte oder die Öffentlichkeit lassen sich die Interessen der Betreiber und das Risiko einer Ausnutzung der auf diesem Wege möglicherweise offenbarten IT-Sicherheitslücken anführen.

Der **Reputationsverlust der Unternehmen** ist insoweit durchaus eine realistische Gefahr. Dieses Interesse ist aber gegen die Interessen derjenigen abzuwägen, die von einer Meldung profitieren würden (weil sie etwa konkrete Abwehrmaßnahmen ergreifen, ihre allgemeinen IT-Sicherheitsbestrebungen präzisieren oder auch Forschung- und Entwicklungsanstrengungen konkreter durchführen können). Auf diesem Wege profitiert auch die Gesellschaft insgesamt davon, dass das Wissen über die Risiken für die IT-Sicherheit nicht nur im Geheimen verbleibt. Hinsichtlich eines drohenden Reputationsverlustes sind **mehrere Fälle zu unterscheiden**. Für die Störung nicht zu einem Ausfall oder zu einer Beeinträchtigung der Funktionsfähigkeit, ist ein solcher nicht zu besorgen; die erfolgreiche Abwehr einer solchen Bedrohung wird die Reputation umgekehrt sogar steigern. Kommt es dagegen zu einem Ausfall oder einer Beeinträchtigung, so kann es in der vorzunehmenden Abwägung zulasten der meldenden Unternehmen sprechen, wenn sie ein vorwerfbares Verhalten trifft; hier dürfte das Risiko einer Veröffentlichung zusätzlich dazu anhalten, IT-Sicherheitsstandards einzuhalten. Im Bereich der nach § 8b Abs. 4 BSIG-E vorgesehenen pseudonymen Meldung besteht (solange auch aus den Umständen nicht auf den betreiberzurückgeschlossen werden kann) von vornherein kein Risiko eines Reputationsverlusts, sodass dieses Argument hier überhaupt nicht greift.

Eine Information der Öffentlichkeit kann auch dann gefährlich sein, **wenn das zugrundeliegende IT-Sicherheitsproblem noch nicht gelöst ist**, die Lücke deshalb weiterhin „offen" ist und deshalb das Risiko besteht, dass Nachahmungstäter erst auf sie aufmerksam

---

[14] BT-Drs. 18/4096, 24.

gemacht werden. In diesen Fällen ist es sinnvoll, **zunächst in Zusammenarbeit mit Herstellern und Anwendern Lösungen zu erarbeiten**. Für eine komplette Geheimhaltung kann aus dieser Notwendigkeit jedoch kein Argument abgeleitet werden. Zum einen wird es für Wissenschaftler und Anbieter vielfach sinnvoll sein, nach dem Schließen einer Lücke von deren Charakteristika zu erfahren, um Erkenntnisse für die Zukunft zu gewinnen. Überdies ist eine Veröffentlichung geboten, wenn Selbsthilfemaßnahmen der institutionellen oder privaten Anwender erforderlich sind. Dass der **zugrundeliegende Konflikt lösbar ist**, zeigt § 42a Satz 2 BDSG. Danach muss im Falle einer unrechtmäßigen Kenntniserlangung von personenbezogenen Daten die Benachrichtigung des Betroffenen „unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird“. Eine solche vorläufige Zurückhaltung der Informationen ist auch im hier vorliegenden Fall möglich.

Soweit im weiteren Gesetzgebungsverfahren entsprechend den Vorschlägen unter 4.3 und 5.4 weitere Sanktionen aufgenommen werden, könnte sich überdies ein **Konflikt mit dem Verbot der Selbstbezichtigung** ergeben. Deshalb sollte erwogen werden, zum Schutz der meldepflichtigen eine § 42a Satz 6 BDSG[15] entsprechende Beschränkung der Verwendung der erlangten Informationen in einem Straf- und Ordnungswidrigkeitenverfahren aufzunehmen.

5.3.2 Schlussfolgerungen

Unter Berücksichtigung dieser Überlegungen erscheinen die **Kommunikationswege zu den Betreibern Kritischer Infrastrukturen** im Wesentlichen **hinreichend**. § 3 Abs. 3 BSIG-E eröffnet dem BSI insoweit die ermessensabhängige Möglichkeit der Beratung bei der Sicherung der Informationstechnik; nach allgemeinen Regeln kann sich dieses Ermessen auf Null reduzieren, wenn beispielsweise ein Betreiber auf die rasche Unterstützung gerade des BSI angewiesen ist. In Umsetzung der neuen Aufgabe zur Zurverfügungstellung von Informationen nach § 3 Abs. 1 Satz 2 Nr. 2 BSIG-E auch an Dritte regelt § 8b Abs. 2 Nr. 4 lit. a BSIG-E eine Pflicht der Behörde zur Information der Betreiber Kritischer Infrastrukturen über sie betreffende Informationen, die aus den mittels der Meldepflicht gesammelten Daten synthetisiert werden.

---

[15] Danach darf eine Benachrichtigung über eine unrechtmäßige Kenntniserlangung personenbezogener Daten, die der Benachrichtigungspflichtige erteilt hat, in einem Strafverfahren oder in einem Verfahren nach dem OWiG gegen ihn oder einen in § 52 Abs. 1 StPO bezeichneten Angehörigen des Benachrichtigungspflichtigen nur mit Zustimmung des Benachrichtigungspflichtigen verwendet werden.

In **Bezug auf konkrete Dritte** ist eine solche **proaktive Informationspflicht** des BSI dagegen nicht nur nicht als Pflicht, sondern **noch nicht einmal als Möglichkeit** ausgestaltet worden. § 8d BSIG-E lässt eine Information Dritter nur auf Antrag zu und stellt sie in das Ermessen der Behörde. Als ermessenslenkende Maßstäbe werden ausschließlich Gründe für den Ausschluss der Auskunft genannt, sodass die Regelung insgesamt restriktiv ausgestaltet ist. Dies ist eine übermäßige Einschränkung der legitimen Interessen Dritter an den durch das BSI gesammelten Informationen. Umgekehrt ist nicht erkennbar, wieso der konkrete Betreiber nicht an der Entscheidung beteiligt oder zumindest informiert werden soll. Die Vorschrift sollte deshalb **in dreifacher Hinsicht geändert** werden:

- Statt die Übermittlung der Informationen per se auszuschließen, wenn schutzwürdige Interessen des Betroffenenbetreibers entgegenstehen, ist **eine Abwägung** zwischen diesen legitimen Interessen und den gleichfalls legitimen Interessen des Dritten vorzunehmen. Andernfalls käme es auch zu einer übermäßigen Einschränkung gegenüber den Regelungen im IFG.
- Soweit das BSI erkennen kann, dass ein berechtigtes Interesse Dritter an den Informationen besteht, um sich vor erheblichen Gefahren der IT-Sicherheit zu schützen, sollte die Behörde eine **proaktive Pflicht treffen, selbst in den entsprechenden Abwägungsprozesse einzutreten**. Andernfalls besteht die Gefahr, dass die dritten keine Kenntnis davon erhalten, dass das BSI über entsprechende Informationen verfügt, und dementsprechend keinerlei Anlass haben, ein Auskunftsverlangen zu stellen.
- Entsprechend den europäischen Entwürfen (§ 14 Abs. 4 NIS-RL-E) sollte eine **Pflicht zur Anhörung des betroffenen Betreibers** vorgesehen werden.

Auch hinsichtlich einer **Pflicht zur Information der Öffentlichkeit** erscheint der Entwurf **überarbeitungsbedürftig**. In der Begründung zu § 8b BSIG-E heißt es zwar, die Öffentlichkeit werde benachrichtigt, wenn das öffentliche Interesse dies erfordere; auch insoweit dürften schutzwürdigen Interessen der Betreiber Kritischer Infrastrukturen nicht entgegenstehen.[16] **Auf welcher Basis** diese Information der Öffentlichkeit erfolgen soll, wird jedoch nicht angegeben und ist auch **nicht erkennbar**. § 8b BSIG-E enthält jedenfalls weder eine Befugnis, geschweige denn eine Pflicht zu einer solchen Benachrichtigung. Auch das als Antragsverfahren eines konkreten Dritten ausgestaltete Procedere nach § 8d BSIG-E kann kaum gemeint sein. Somit bleibt lediglich die allgemeine Befugnis zur Warnung der Öffentlichkeit nach § 7 BSIG. Diese bezieht sich jedoch explizit auf die Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nr. 14 BSIG, also gerade nicht auf die neuen Aufgaben nach Nr.

[16] BT-Drs. 18/4096, 27.

17. Regelungssystematisch besteht insoweit also **überhaupt keine Befugnis zur Information der Öffentlichkeit** über die aus den Meldepflichten gewonnenen Informationen.

Dies widerspricht nicht nur den europäischen Plänen (Art. 14 Abs. 4 NIS-RL-E) und stellt eine **nicht begründete Diskrepanz zu der Bestimmung in § 109 Abs. 5 Satz 7 TKG-E** dar,[17] sondern ist auch aus nationaler Sicht eine Lücke, die geschlossen werden sollte. Soweit eine Information der Öffentlichkeit geboten ist, um Sicherheitsvorfälle abzuwenden oder zu lindern, sollte – unter Abwägung mit den legitimen Vertraulichkeitsinteressen der betroffenen Anbieter[18] – eine solche **Pflicht oder zumindest Befugnis des BSI zur Information der Öffentlichkeit** eingeführt werden.

5.4 Fehlen von Sanktionen

Auffällig ist, dass der Gesetzentwurf **ausschließlich für den Bereich des TKG** Sanktionen für Verstöße gegen die geregelten Meldepflichten enthält.[19] Gemäß § 149 Nr. 21a TKG-E begeht eine Ordnungswidrigkeit, wer eine Beeinträchtigung von Telekommunikationsnetzen oder -diensten, die zu einer „beträchtlichen Sicherheitsverletzung“ führt, nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig mitteilt. Wieso der Gesetzgeber ausschließlich für diese Anbieter die Notwendigkeit einer entsprechenden Bußgeldbewehrung gesehen hat, wird nicht erläutert. Die Ungleichbehandlung ist nicht nur **verfassungsrechtlich kaum zu rechtfertigen**, sondern auch **sachlich unangemessen**. Ohne eine entsprechende Norm müsste das BSI vollständig darauf vertrauen, dass die Betreiber Kritischer Infrastrukturen ihrer Pflicht aus § 8b Abs. 4 BSIG-E freiwillig nachkommen.

Dementsprechend sollte ein entsprechender Tatbestand aufgenommen werden. Dies entspricht im Übrigen **auch dem geplanten Art. 17 NIS-RL-E**, der nicht nur Sanktionen für die Verletzung von IT-Sicherheitsstandards, sondern auch für die Nichterfüllung der Meldepflichten vorgibt.

6 Verfassungsrechtliche Probleme von § 100 Abs. 1 TKG-E

§ 100 Abs. 1 TKG enthält **bereits heute** die Befugnis der Diensteanbieter, die Bestands- und Verkehrsdaten der Teilnehmer und Nutzer zu erheben und zu verwenden, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen erforderlich ist. Dies entspricht § 100 Abs. 1 Satz 1 TKG-E. Demgegenüber ist **§ 100 Abs. 1 Satz 2 TKG-E** vom Wortlaut her **eine Erweiterung**, weil der Begriff

---

[17] Danach kann die Bundesnetzagentur die Öffentlichkeit unterrichten oder die Verpflichteten zu dieser Unterrichtung auffordern, wenn sie zu dem Schluss gelangt, dass die Bekanntgabe der Sicherheitsverletzung im öffentlichen Interesse liegt.

[18] S.o. 5.3.1.

[19] Kritisch z.B. *Bräutigam/Wilmer*, ZRP 2015, 38, 41.

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

Die Erstreckung auf lediglich potentielle Einschränkungen der Verfügbarkeit **entspricht der Auslegung des Bundesgerichtshofs** zum geltenden § 100 Abs. 1 TKG.[20] Neu ist demgegenüber die Erstreckung auf Systeme der Nutzer (hierbei wird es sich regelmäßig nicht um Kritische Infrastrukturen handeln). Hiermit hatte sich die Rechtsprechung bislang noch nicht zu beschäftigen.

Mit Blick auf den Eingriff in das Fernmeldegeheimnis nach Art. 10 GG, der in der Vorschrift liegt, begegnet § 100 Abs. 1 TKG-E verfassungsrechtlichen Bedenken.[21] Da der Entwurf ebenso wie die geltende Vorschrift als einziges Kriterium für die Erhebung und Verwendung der Daten die Erforderlichkeit nennt, enthält er de facto **keinerlei präzise Regelungen**. Dies ist mit Blick darauf, dass die Norm potenziell eine **umfassende Analyse der Verkehrsdaten aller Teilnehmer und Nutzer in Deutschland** ermöglicht, nicht zu rechtfertigen. Zwar gelten insoweit die durch das Bundesverfassungsgericht und den europäischen Gerichtshof aufgestellten Anforderungen an die Vorratsspeicherung von Telekommunikations-Verkehrsdaten[22] nicht direkt. Die durch die Gerichte beschriebenen Risiken für die unbeobachtete Kommunikation der Bürgerinnen und Bürger sind jedoch auch hier betroffen.

Die in der Diskussion mitunter vorgeschlagene Alternative des **Verzichts auf eine präventive Datenerhebung** und der Beschränkung auf die Erhebung und Verwendung der Daten im Falle eines Sicherheitsvorfalls ist sicher weniger eingriffsintensiv. Inwieweit hierdurch wesentliche Sicherheitsrisiken nicht identifiziert werden könnten, **müssen die technischen Sachverständigen bewerten**.

Wenn es bei dem vorgeschlagenen Verwendungszweck für die nach § 100 Abs. 1 TKG-E erhobenen Daten bleibt, so sind jedenfalls **ergänzende Regelungen zur Sicherung der Persönlichkeitsrechte der Betroffenen** vorzusehen. Dies betrifft insbesondere Erheblichkeitsschwellen (der Entwurf erfasst sämtliche, das heißt auch einfach gelagerte Störungen und Fehler), Maßnahmen zum Schutz gegen Zweckentfremdung, Dokumentationspflichten, Ausnahmen für besonders sensible Kommunikationsvorgänge, Vorgaben zur Information der Betroffenen und zeitlich konkretisierte **Löschpflichten**. Letzteres betrifft insbesondere Daten, die keinen Anlass für einen entsprechenden Verdacht auf Störungen

---

[20] BGH, NJW 2014, 2500; NJW 2011, 1509.
[21] Diese gelten der Sache nach auch für die aktuelle Regelung.
[22] BVerfGE 125, 260; EuGH, NJW 2014, 2169.

oder Fehler ergeben haben.[23] Dass entsprechende Vorgaben zur Zweckbindung, Transparenz und Löschung möglich sind, zeigt die Regelung in § 5 BSIG.

Durch die **Streichung von § 15 Abs. 9 TMG-E** (Referentenentwurf) bleibt es weiterhin bei der grundsätzlichen Unzulässigkeit der Erhebung und Verwendung von Nutzungsdaten durch Webseitenbetreiber zur Störungserkennung. Auf die **damit verbundenen Probleme und Lösungsmöglichkeiten** haben u.a. der FIfF e.V.[24] und das ULD[25] hingewiesen; dies soll deshalb hier nicht vertieft werde.

[23] Das Kriterium der Erforderlichkeit im geltenden § 100 Abs. 1 TKG hat zu einer erheblichen Rechtsunsicherheit hinsichtlich der Frage geführt, wie lange die insoweit erhobenen Daten gespeichert werden dürfen. Die inzwischen erfolgte höchstrichterliche Klärung dieser Frage (BGH, NJW 2014, 2500; NJW 2011, 1509) gilt im Wesentlichen nur für IP-Adressen, für die eine Speicherung von sieben Tagen akzeptiert wurde.

[24] FIfF e.V., Stellungnahme zum IT-Sicherheitsgesetz der Bundesregierung vom 17.12.2014, 4 ff.

[25] Stellungnahme vom 13.2.2015, https://www.datenschutzzentrum.de/artikel/877-ULD-Stellungnahme-zum-IT-Sicherheitsgesetz-Entwurf.html.

18. Wahlperiode

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)241

Deutscher Bundestag
Parlamentarischer Beirat
f. nachhaltige Entwicklung

Ausschussdrucksache
18(23)30-6

Deutscher Bundestag

Parlamentarischer Beirat für
nachhaltige Entwicklung

Gutachtliche Stellungnahme/Prüfbitte

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

Bundesrats-Drucksache 643/14

Im Rahmen seines Auftrags zur Überprüfung von Gesetzentwürfen und Verordnungen der Bundesregierung auf Vereinbarkeit mit der nationalen Nachhaltigkeitsstrategie hat sich der Parlamentarische Beirat für nachhaltige Entwicklung gemäß Einsetzungsantrag (Drs. 18/559) in seiner 18. Sitzung am 28. Januar 2015 mit dem Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) (BR-Drs. 643/14) befasst und festgestellt:

Eine Nachhaltigkeitsrelevanz des Gesetzentwurfs ist gegeben. Der Bezug zur nationalen Nachhaltigkeitsstrategie ergibt sich hinsichtlich folgenden Indikators:

Indikator (15) Kriminalität - Persönliche Sicherheit weiter erhöhen

Folgende Aussagen zur Nachhaltigkeit wurden in der Begründung des Gesetzentwurfes getroffen:
„Der Gesetzentwurf entspricht mit der Anhebung der Sicherheitsstandards in der deutschen IT-Sicherheitsarchitektur, die zunehmend alle Gesellschaftsbereiche durchdringt, dem Leitgedanken der Bundesregierung zur nachhaltigen Entwicklung im Sinne der nationalen Nachhaltigkeitsstrategie.“

Die Darstellung der Nachhaltigkeitsprüfung ist nicht plausibel.

Es ist wünschenswert, dass das Bundesministerium des Innern darlegt, ob und inwieweit die Gesetzesänderung dem Indikator (15) dient.

Vorbeugende Maßnahmen zur Steigerung der IT-Sicherheit könnten dazu beitragen, die Anzahl der Straftaten zu verringern.

Prüfbitte:

Der Parlamentarische Beirat für nachhaltige Entwicklung bittet deshalb den federführenden Innenausschuss, bei der Bundesregierung nachzufragen, warum die o.g. Bezüge zur nationalen Nachhaltigkeitsstrategie nicht hergestellt wurden und die Ergebnisse in Kurzform in den Bericht des Ausschusses aufzunehmen.

Berlin, den 28. Januar 2015

Dr. Lars Castellucci, MdB
Berichterstatter

Dr. Valerie Wilms, MdB
Berichterstatterin

Bundesministerium
des Innern

Innenausschuss
26.3.15 (2091)
Eingang mit Anl. am
1. Vors. m.d.B. um Kenntnisnahme/Rücksprache
2. Mehrfertigungen mit/ohne Anschreiben an Abg. BE, Obl. Sekr.
an
3. Wv
4. z.d.A. (alphab.-Gesetz- BMI)

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)285

Herrn
Wolfgang Bosbach, MdB
Vorsitzender des Innenausschusses
des Deutschen Bundestages
Platz der Republik 1
11011 Berlin

Dr. Ole Schröder, MdB
Parlamentarischer Staatssekretär

HAUSANSCHRIFT
Alt-Moabit 101D
10559 Berlin

POSTANSCHRIFT
11014 Berlin

TEL +49(0)30 18 681-1060
FAX +49(0)30 18 681-1137

PStS@bmi.bund.de
www.bmi.bund.de

VG.-NR. 210/15

Berlin, den 13. März 2015

Sehr geehrter Herr Bosbach, lieber Wolfgang,

der Parlamentarische Beirat für Nachhaltige Entwicklung bittet den Innenausschuss des Deutschen Bundestages mit Schreiben vom 30. Januar 2015 um Nachfrage beim Bundesministerium des Innern im Hinblick auf die Nachhaltigkeitsprüfung der Bundesregierung zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). Er bittet insbesondere um ergänzende Ausführungen, ob und inwieweit die Gesetzesänderung dem Indikator [15] der nationalen Nachhaltigkeitsstrategie der Bundesregierung "Kriminalität - Persönliche Sicherheit weiter erhöhen" entspricht.

Hierzu kann ich Ihnen Folgendes mitteilen:

Die mit dem IT-Sicherheitsgesetz verbundene Anhebung der Sicherheitsstandards in der deutschen IT-Sicherheitsarchitektur wird die Begehung von Straftaten der Cyberkriminalität im weiteren Sinne (also von Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik oder gegen diese begangen werden) erschweren. Dies gilt sowohl für die mit dem Gesetz verbundene erhöhte Sicherheit der Kritischen Infrastrukturen (§§ 8a bis 8d BSI-Gesetz neu) als auch für die Anhebung des Schutzniveaus in den Telekommunikationsnetzen (Änderungen in den §§ 100, 109 und 109a Telekommunikationsgesetz) und bei Telemedienangeboten (§ 13 Absatz 7 Telemediengesetz neu). Hinzu kommt die Ausweitung der Zuständigkeiten des Bundeskriminalamtes im Bereich Cybercrime durch die Änderung des § 4 Absatz 1 Satz 1 Nummer 5 BKA-Gesetz.

Das IT-Sicherheitsgesetz entspricht damit insbesondere auch Indikator [15] der nationalen Nachhaltigkeitsstrategie der Bundesregierung.

Mit freundlichen Grüßen

FIfF
Forum InformatikerInnen für Frieden
und gesellschaftliche Verantwortung e.V.

FIfF e.V.
Goetheplatz 4, 28203 Bremen
Telefon 0421 33659255
Telefax 0421 33659256
fiff@fiff.de
www.fiff.de

Bremen, 9. Februar 2015

Deutscher Bundestag
Ausschuss für Inneres
Herrn Werner Bosbach (MdB)
- Vorsitzender -
Platz der Republik 1
D - 11011 Berlin

Stellungnahme zum Entwurf des IT-Sicherheitsgesetzes vom 17. Dezember 2014

Sehr geehrter Herr Bosbach,

der Entwurf des IT-Sicherheitsgesetzes wird den Planungen zufolge dem Bundestag Anfang März zugeleitet. Mit dem Gesetz soll eine signifikante Verbesserung der Sicherheit informationstechnischer Systeme und damit der IT-Sicherheit in Deutschland erreicht werden. Dafür sollen rechtliche und organisatorische Grundlagen für die IT-Sicherheit in Deutschland geschaffen werden.

Eine eingehende Analyse des Gesetzes aus Sicht von Fachleuten in der IT-Sicherheit und unter juristischen Aspekten zeigt neben einigen positiven Ansätzen leider auch gravierende Defizite. Rechtliche Widersprüche in der IT-Sicherheit werden nicht beseitigt, sondern neue erzeugt.

•Grundsätzlich positiv zu bewerten ist aus unserer Sicht die Einführung einer Meldepflicht für IT-Sicherheitsvorfälle. In der Praxis hilft heute nur der Austausch von Wissen über Angriffe und Schadsoftware, um Gegenmaßnahmen zu entwickeln. Doch statt eines systematischen Wissensaustauschs soll nur eine eingeschränkte Lösung umgesetzt werden. Die Meldepflicht ist auf Betreiber kritischer Infrastrukturen begrenzt und wird ergänzt um Vorschriften zum Stand der Technik. Damit endet ein 18 Jahre dauernder Prozess zum Schutz kritischer Infrastrukturen. Der Schutz nicht-öffentlicher IT-Systeme bleibt dabei leider unberücksichtigt.

•Rechtlich ungeregelt bleibt der Einsatz von IT-Sicherheitswerkzeugen in Webdiensten. Die geplante Neuregelung zum Einsatz solcher Werkzeuge im Telekommunikationssektor ist offensichtlich verfassungswidrig und wird einer Verfassungsklage nicht standhalten. Damit wird durch das Gesetz keine Rechtssicherheit geschaffen, vielmehr fehlt es für Investitionen in IT-Sicherheitssysteme und deren Nutzung an der nötigen klaren rechtlichen Perspektive.

Die Regelungen im Gesetzentwurf sorgen allein für die IT des Bundes und der Betreiber kritischer Infrastrukturen für Rechtssicherheit und spezielle Schutzmaßnahmen. Für den Schutz der IT-Systeme von Ländern und Kommunen, der Privatwirtschaft und der privaten Nutzer wird es im Ergebnis dieses Gesetzesvorhabens weder Unterstützung noch Rechtssicherheit geben.

Das FIfF e.V. als Verband von IT-Fachleuten aus Wissenschaft und Praxis spricht sich vehement für die Stärkung der IT-Sicherheit sowohl in rechtlicher als auch organisatorischer Hinsicht aus

FIfF – Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

FIfF e.V.
Goetheplatz 4, 28203 Bremen
Telefon 0421 33659255
Telefax 0421 33659256
fiff@fiff.de
www.fiff.de

und sieht in einem sachgerechten IT-Sicherheitsgesetz die Möglichkeit, die IT-Sicherheitslage deutlich zu verbessern. Der Auftrag zum Schutz des vom Bundesverfassungsgericht 2008 formulierten Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (1 BvR 370/07) wurde bisher vom Gesetzgeber nicht umgesetzt. Durch den Gesetzesentwurf wird aus Sicht der Praxis jedoch dieses wichtige Handlungsfeld weder ausreichend noch sachgerecht adressiert. Es werden vielmehr neue und leicht vermeidbare Probleme geschaffen.

In der beigefügten detaillierten Stellungnahme finden Sie die wesentlichen Kritikpunkte und Verbesserungsvorschläge aufbereitet.

Sehr geehrter Herr Bosbach, bitte wirken Sie im weiteren Verfahren der Gesetzgebung darauf hin, dass unsere Stelllungnahme im Sinne eines effektiven Schutzes der Menschen vor Bedrohungen aus dem Internet Berücksichtigung findet. Als Ansprechpartner stehen Ihnen unsere Experten Frau Sylvia Johnigk (0179 2897714), Herr Kai Nothdurft (0172 8561971) und Herr Stefan Hügel (0151 17274808) gerne zur Verfügung.

Mit freundlichen Grüßen
FIfF e.V.

Stefan Hügel
Vorsitzender

Das FIfF – Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. – sind etwa 600 engagierte Menschen aus Wissenschaft und Praxis. Wir sind Fachleute der Informatik und Informationstechnik. Wir denken bei unserer Arbeit auch über deren Konsequenzen nach. Wir wissen, dass nicht alle Probleme technisch lösbar sind. Wir heißen alle willkommen, die Informationstechnik verwenden oder sich Gedanken über ihre gesellschaftliche Rolle machen.
Allen, die sich mit Informatik und Informationstechnik beschäftigen – in der Ausbildung im Beruf oder danach, in Wissenschaft und Praxis – wollen wir ein Forum für eine kritische und lebendige Auseinandersetzung bieten – offen für alle, die mitarbeiten möchten oder auch einfach nur informiert bleiben wollen.

Unsere Arbeit wird vom FIfF-Vorstand koordiniert. In wissenschaftlichen Fragen unterstützt uns der Beirat des FIfF. Wir kooperieren mit zahlreichen in- und ausländischen Initiativen und Organisationen.

In zahlreichen Veröffentlichungen dokumentieren wir unsere Arbeit. Die kritische Computerzeitung FIfF-Kommunikation erscheint vierteljährlich.

FIfF e.V.
Goetheplatz 4, 28203 Bremen
Telefon 0421 33659255
Telefax 0421 33659256
fiff@fiff.de
www.fiff.de

FIfF – Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

Stellungnahme des FIfF zum IT-Sicherheitsgesetz der Bundesregierung vom 17.12.2014

Kurzfassung

1) Der Entwurf des IT-Sicherheitsgesetzes schreibt als wesentliche Neuerung für das Schutzniveau der IT-Systeme in kritischen Infrastrukturen den „Stand der Technik" vor. Genau dies ist nach dem Bundesdatenschutzgesetz heute schon für jeden verpflichtend, der personenbezogene Daten verarbeitet. In Deutschland wurde über den Schutz kritischer Infrastrukturen seit 18 Jahren in Gremienrunden debattiert. Das Verhältnis von Aufwand und Ergebnis ist hier sicher näher zu hinterfragen.
2) Der Entwurf sieht eine Meldepflicht für Sicherheitsvorfälle bei kritischen Infrastrukturen vor. Die detaillierte Betrachtung der Rechtslage zeigt jedoch, dass spezifische Rechtsgrundlagen fehlen, um wichtige IT-Sicherheitswerkzeuge legal einzusetzen. Ohne rechtliche Befugnisse ist das Erkennen und Melden von Sicherheitsvorfällen auf eine kleine Zahl von Fällen und einen geringen Aufwand begrenzt.
3) Das deutsche Recht unterteilt das Internet in Telekommunikations- und Telemediendienste mit konträren Regeln für die IT-Sicherheit. Das Erkennen vieler Angriffe auf Webangebote, vor allem aber das Zurückverfolgen zu den Verursachern sowie die rechtlich klare Identifikation von Angreifern setzen eine Verarbeitung und Analyse von Internet-Adressdaten voraus. Bei Webangeboten dürfen IP-Adressen in Deutschland zur Abrechnung von vertraglichen Leistungen genutzt, verkürzte Daten zu Werbezwecken gesammelt werden. Das Sammeln und Verarbeiten von IP-Adressen für Zwecke der IT-Sicherheit ist dagegen verboten (§ 15 TMG). Zulässig ist diese Datenverarbeitung und Sicherheitsanalyse einzig und allein für IT-Systeme des Bundes (§ 5 BSIG). Mit dem neuen IT-Sicherheitsgesetz soll es daran keine Änderung geben.
4) Das Telekommunikationsgesetz (TKG) enthält noch aus Zeiten analoger Telefonie eine Befugnis zur Analyse von Störungen (§ 100 TKG). Im Entwurf des IT-Sicherheitsgesetzes soll diese zu ganz anderen Zwecken ausgeweitet und abgeändert werden: Telekommunikationsunternehmen sollen die Kommunikation ihrer Kunden auf Schadsoftware hin durchsuchen dürfen und betroffene Kunden zur Abhilfe auffordern. Die notwendige technische Voraussetzung dafür ist eine dauerhafte, flächendeckende und alle Inhalte betreffende Überwachung der gesamten Telekommunikation (deep packet inspection). Das allein ist ein Bruch des Artikels 10 Grundgesetz. Das IT-Sicherheitsgesetz sieht überdies keinerlei Einschränkungen bei dieser Datenerfassung vor. Die geplante Regelung ist daher ganz offensichtlich verfassungswidrig.
5) Der einzige Bereich, in dem der Einsatz von IT-Sicherheitssystemen nach dem Stand der Technik und die Auswertung der Daten zulässig ist, ist die IT des Bundes. Die Bundesregierung hat dem Bundesamt für Sicherheit in der Informationstechnik (BSI) 2007 dazu die Befugnis gegeben (§ 5 BSIG). Die Bundesregierung setzt diesen Weg fort, für den Schutz der IT-Systeme des Bundes zu sorgen und die IT-Systeme der Bürgerinnen und Bürger wie auch der Wirtschaft sich selbst zu überlassen. Sie will im neuen Gesetz neue Befugnisse für das BKA und dort eine Sonderpolizeiabteilung schaffen, die Strafta-

FIfF e.V.
Goetheplatz 4, 28203 Bremen
Telefon 0421 33659255
Telefax 0421 33659256
fiff@fiff.de
www.fiff.de

ten gegen die IT des Bundes und Straftaten gegen kritische Infrastrukturen verfolgt. Die Begründung ist entlarvend: sonst bleibe – so die Gesetzesbegründung – „die örtliche Zuständigkeit oftmals dem Zufall überlassen" und die eigentlich für IT-Kriminalität zuständigen Strafverfolgungsbehörden im Land seien nicht mit hinreichenden fachlichen Kompetenzen und Ressourcen ausgestattet. Weil solche Strafverfolger Wirtschaft und Bürger im Internet nicht zu schützen vermögen, will die Bundesregierung eigene Sonderkommissariate. Wie verträgt sich das mit dem grundgesetzlichen Auftrag zum Schutz des „Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" für alle Bürgerinnen und Bürger?

Mit dem „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" hat das Bundesverfassungsgericht 2008[1] die IT-Sicherheit zu einem Handlungsziel für Parlament und Exekutive gemacht. Aufgabe eines IT-Sicherheitsgesetzes wäre es, dieses Grundrecht zusammen mit dem Datenschutz und dem Fernmeldegeheimnis zu betrachten, diese drei Verfassungsziele in Einklang zu bringen und für Bürgerinnen und Bürger die rechtliche Basis für einen angemessenen Schutz im Internet zu schaffen.

Tatsächliche Konsequenz des neuen IT-Sicherheitsgesetzes ist dagegen eine weiterhin fehlende Rechtsgrundlage für IT-Sicherheitssysteme bei Webservices und eine verfassungswidrige Regelung für Telekommunikationsdienste. Die absehbare Folge eines solchen Gesetzes ist daher, dass es eine verfassungsgemäße Rechtsgrundlage für IT-Sicherheitssysteme weder für Webdienste geben soll noch – nach einer Verfassungsklage – für den Telekommunikationsbereich mehr geben wird.

Statt verfassungswidriger Zustände oder eines juristischen Vakuums nötig ist dagegen eine einheitliche Regelung zum Einsatz von IT-Sicherheitssystemen bei Telemedien wie in der Telekommunikation, die dem Datenschutz, dem Fernmeldegeheimnis und dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gleichermaßen gerecht wird. Aus Sicht der IT-Sicherheit gibt es dafür heute bereits in der Praxis erprobte, datensparsame Lösungen. Die Bundesregierung macht dazu keine Vorschläge. Damit ein Grundrechtsschutz wirksam werden kann, sind die aus Sicht des FIfF umzusetzenden rechtlichen Mindestvoraussetzungen:

- einheitliche verfassungskonforme Rechtsgrundlagen für den Einsatz von IT-Sicherheitssystemen im Telekommunikations- und Telemediensektor,
- eine grundsätzliche Pflicht zur Veröffentlichung von IT-Sicherheitslücken bei gleichzeitigem Verbot des kommerziellen Handels mit Sicherheitslücken einschließlich des Kaufs solchen Wissens durch Nachrichtendienste,
- eine an die bestehenden Produkthaftungsvorschriften angelehnte Schadenshaftung für fahrlässig implementierte IT-Systeme und für nicht wirksam beseitigte Sicherheitslücken in IT-Systemen, wenn sie nach Ablauf einer angemessenen Frist nach Bekanntwerden nicht behoben werden,
- Ausbau und Verstärkung von Analyse- und Beratungskapazitäten bei einem BSI, das zu organisieren ist als eine von Weisungen unabhängige Behörde vergleichbar dem Bundesrechnungshof (BRH),

1 1 BvR 370/07

FIfF e.V.
Goetheplatz 4, 28203 Bremen
Telefon 0421 33659255
Telefax 0421 33659256
fiff@fiff.de
www.fiff.de

- Anpassung der Strafbarkeit des Bruchs des Fernmeldegeheimnisses (§ 206 StGB) an die Vorgaben von Grundgesetz und Bundesverfassungsgericht.

Statt für den Schutz der Allgemeinheit in Sachen IT zu sorgen, trennt die Bundesregierung den Schutz ihrer IT-Systeme ab von dem der IT-Systeme von Bürgern und Wirtschaft, gleichermaßen in rechtlicher Hinsicht wie in der Strafverfolgung. Die Bundesregierung belässt die IT-Sicherheit für die Allgemeinheit in einem rechtlichen Vakuum. Der Gesetzentwurf bewirkt keinerlei Verbesserung der IT-Sicherheit, sondern untergräbt das „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ in Deutschland.

FIfF e.V.
Goetheplatz 4, 28203 Bremen
Telefon 0421 33659255
Telefax 0421 33659256
fiff@fiff.de
www.fiff.de

Im Detail

Wesentlicher Kritikpunkt des FIfF ist das unveränderte Fortbestehen der gegensätzlichen juristischen Behandlung von IT-Sicherheitswerkzeugen in den drei Bereichen Telekommunikation, Telemedien und der IT des Bundes. Diese ohne jeden sachlichen oder rechtlichen Grund bestehenden Widersprüche sind unvereinbar mit dem Schutz des Fernmeldegeheimnisses, des Grundrechtes auf informationelle Selbstbestimmung und des Grundrechtes auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Bevor auf die Details des IT-Sicherheitsgesetzes eingegangen werden kann, ist klarzustellen, dass **die Grundvoraussetzung für die IT-Sicherheit in Deutschland nur eine einheitliche und zugleich datensparsame Regelung für die Sicherheit von IT-Systemen in der Telekommunikation und bei Telemedien sein kann**.

Die Ausgangslage in der rechtlichen Behandlung von IT-Sicherheitswerkzeugen

Das Internet wird im deutschen Recht aufgeteilt in einerseits Telekommunikation wie E-Mail, Skypen, Chatten und andere direkte Kommunikationsformen. Das Telekommunikationsgesetz (TKG) regelt hierbei die Rechte der Kunden und der Internetprovider als Telekommunikation. Alles, was im Allgemeinen als World Wide Web (oder WWW) verstanden wird – also die Anbieter von Webseiten, Webshops, Cloud Services und ihre Kunden – fällt andererseits unter das Telemediengesetz (TMG).

Das Telekommunikationsrecht sieht im Verhältnis von Anbieter und Kunde die Möglichkeit eines vertraglosen Zustands nicht vor: Jeder Telekommunikationsanbieter ist im Grundsatz verpflichtet, seine Kunden möglichst genau zu identifizieren. Die Bundesnetzagentur hat zudem spezielle Befugnisse, die Einhaltung der Rechtslage zu überwachen und Verstöße zu ahnden. Dagegen berücksichtigt das TMG, dass es neben vertraglich gebundenen Kunden von Webshops etc. eine Vielzahl von Web-Surfern gibt, die zufällig und ohne feste Vertragsbindung auf Webseiten herumstöbern. Daten zu all diesen Kunden dürfen für Werbezwecke gesammelt werden, aber nur mit deren Zustimmung oder pseudonymisiert – ohne individuelle Zuordnung.

Die IT-Sicherheit wird in beiden Bereichen gegensätzlich behandelt.

- Das TKG erlaubt in § 100 ohne Einschränkungen, zur Störungserkennung jede Form von Daten zu Telefonaten und Datenverkehren zu sammeln, zu analysieren und sich sogar auf Kommunikationsverbindungen aufzuschalten. Diese sehr weitgehende Befugnis entstammt der Zeit analoger Telefonie, als es darum ging, flüchtige analoge Signale beim Vorgang des Telefonierens zu messen und Fehlerquellen einzugrenzen. Die alte analoge Telefonwelt hatte technisch keine eingebauten systemseitigen Möglichkeiten, Daten zu speichern. Um letztlich die nach § 317 StGB strafbare „Störung von Telekommunikationsanlagen" verfolgen zu können, war es daher notwendig, die Ursachen des gestörten Fernmeldeverkehrs zu ermitteln.
- Das TMG dagegen verbietet es, Nutzungsdaten zu erheben und zu verarbeiten, sofern dies nicht erlaubt ist für Zwecke der Werbung oder zur Abrechnung von vertraglichen Leistungen. Der Einsatz von IT-Sicherheitswerkzeugen, die wie üblich IP-Adressen von Webseitenbesuchern zur Erken-

FIfF e.V.
Goetheplatz 4, 28203 Bremen
Telefon 0421 33659255
Telefax 0421 33659256
fiff@fiff.de
www.fiff.de

nung von Angriffsprofilen speichern, verstößt gegen § 15 TMG und kann als Ordnungswidrigkeit geahndet werden.

Für Internetnutzer ist oft nicht zu unterscheiden, welches Gesetz bei einer Anwendung gilt. IT-Sicherheitsverantwortliche haben jedoch sehr genau zu differenzieren, welche IT-Sicherheitswerkzeuge sie für spezifische Anwendungen und Systeme einsetzen dürfen.

Die Bundesregierung musste sich mit diesem Gegensatz auseinandersetzen, nachdem 2006 ein aus dem Umfeld des AK Vorratsdatenspeicherung erwirktes, rechtskräftiges Urteil[2] gegen die damalige Bundesjustizministerin Zypries das Bundesministerium für Justiz (BMJ) zwang, die Speicherung der IP-Adressen im Webangebot des BMJ zu unterlassen[3].

Die Bundesregierung reagierte darauf 2007 mit der Novelle des BSI-Gesetzes, wobei das BSI in § 5 BSIG die Befugnis erhielt, bei Verdachtsfällen von Angriffen auf die IT-Systeme des Bundes IP-Adressen zu erheben und auszuwerten. Aus den Äußerungen der Bundesregierung im Vorfeld und in der Gesetzesbegründung aus 2007 lässt sich unmissverständlich die Position ablesen, dass eine Speicherung von IP-Adressen durch IT-Sicherheitssysteme bei all jenen IT-Systemen ungesetzlich ist, die nicht dem Bund gehören[4].

An dieser Rechtslage hat sich auch nach weiteren Urteilen unterschiedlicher Gerichte bis heute nichts geändert: Unabhängig davon, wie der EuGH demnächst über die Eingriffstiefe der Speicherung von IP-Adressen urteilen wird, ist es bis heute in Deutschland für WWW-Angebote der Allgemeinheit illegal, über scannende Intrusion-Detection-Systeme hinausgehende, übliche IT-Sicherheitswerkzeuge einzusetzen, die auf der Analyse von IP-Adressen beruhen. Das deutsche Recht teilt das Internet nicht nur in die zwei Welten „Telekommunikation" und „Telemedien" ein und regelt für beide getrennt die Möglichkeiten der IT-Sicherheit. Mit dem BSI-Gesetz wird die Welt der Telemedien zusätzlich aufgeteilt in die IT des Bundes und die IT des gesamten Rests des Landes: die der Länder, der Kommunen, der Wirtschaft und der Bürgerinnen und Bürger. Der Bund darf IP-basierte Sicherheitswerkzeuge legal einsetzen, der Rest des Landes nicht.

Ein Beispiel

Was die gegensätzlichen Regelungen zwischen Telekommunikation und Telemedien in der Praxis bewirken, lässt sich an einem konkreten Beispiel aufzeigen.

Bei Energieversorgern und dem Betrieb eines Smart Grid bedeutet dies konkret, die technische Kommunikation zwischen Hausanschluss und Energieversorger umfassend gemäß TKG auf Störungen hin überwachen zu können. Bei der üblicherweise per Webangebot realisierten individuellen Inanspruchnahme von Serviceangeboten in der Kommunikation zwischen Kunde und Energieversorger dagegen ist der Einsatz der Mehrzahl heutiger IT-Sicherheitswerkzeuge gemäß TMG illegal. Gleiches gilt aber auch in dem Fall,

---

2 ┐Urteil des Amtsgerichts Berlin Mitte vom 10.01.2008, AZ 5 C 314/06, http://www.daten-speicherung.de/data/Beschluss_AG-Mitte_2008-01-10.pdf

3 Aussagen zu den Schlussfolgerungen in der Antwort der Bundesregierung, Bt.-Drs. 16/6938

4 Antwort der Bundesregierung, Antwort auf Frage 11, Bt.-Drs. 16/6938, http://dipbt.bundestag.de/dip21/btd/16/069/1606938.pdf

FIfF e.V.
Goetheplatz 4, 28203 Bremen
Telefon 0421 33659255
Telefax 0421 33659256
fiff@fiff.de
www.fiff.de

dass sich der Energieversorger auf ein reguläres Web-Frontend des Hausanschlusses eines Kunden aufschaltet, um eine Online-Wartung vorzunehmen: Dem Endkunden ist der Einsatz von Zugriffsprotokollen verboten; er muss sich mit einer Firewall begnügen und verfügt bei Schäden an der Anlage oder Betrugsvorkommnissen mangels Protokollierungsdaten über keine gerichtsverwertbaren Beweismittel für die Analyse der Gründe und Ermittlung der Verursacher.

Fazit: Der Energieversorger darf sich rechtlich abgesichert schützen, der Kunde nicht.

Dabei sei ausdrücklich darauf hingewiesen, dass diese Probleme im TMG durch vertragliche Regelungen zwischen Kunde und Anbieter nicht lösbar sind: Zwischen zwei Vertragspartnern lässt sich eine Datenspeicherung vereinbaren – ein Angreifer aber ist keine Vertragspartei, die einer Datenerhebung zugestimmt hat, sondern wird rechtlich wie ein Web-Surfer behandelt, zu dem keine Daten erhoben werden dürfen.

Wichtig ist hier auch der Hinweis auf die spezifische Besonderheit beim TMG, dass gegen die dort getroffenen gesetzlichen Regelungen von fast 90% der inländischen Webanbieter verstoßen wird – und zwar von Behörden kaum weniger häufig als von kommerziellen Anbietern. Diese Zahl von Verstößen bewegte sich in den letzten sechs Jahren, in denen Erhebungen systematisch durchgeführt wurden, auf gleich hohem Niveau[5] und nur in äußerst wenigen Ausnahmefällen kam es zur Ahndung der Verstöße. Beachtung und vor allem Durchsetzung des Rechts bei Webservices – Telemedien – dürfen mit empirisch gut belegter Faktenlage als eindeutig gescheitert angesehen werden.

Man könnte vielleicht die IT-Sicherheit bei Telemedien in der bisherigen Wildwest-Manier sich selbst überlassen. **Wer aber mit einem Gesetz die stärkere Verrechtlichung der IT-Sicherheit anstrebt, muss darlegen können, dass die Vorschläge überhaupt rechtlich konsistent sind. Bisher ist das nicht der Fall.**

Regelungslücke schließen

Das IT-Sicherheitsgesetz in der verworfenen ersten Fassung von 2013 sah an dieser Konstellation keine Änderungen vor. Aus den Reihen des FIfF gab es dazu eine detaillierte Kritik[6]. In der Fassung des IT-Sicherheitsgesetzes vom Sommer 2014 war nun erstmalig mit dem Grund, hier sei eine „Regelungslücke" erkannt, vorgesehen, in § 15 TMG für jeden Anbieter von WWW-Inhalten und Services die rechtliche Grundlage zu schaffen, IT-Sicherheitswerkzeuge einzusetzen und dafür erforderliche Daten zu erheben. Diese Befugnis war dem § 100 TKG nachgebildet.

Bemerkenswert war, dass diese geplante Befugnis weit weniger scharf geregelt war als derselbe Sachverhalt im BSIG für die IT des Bundes: § 5 BSIG regelt vergleichsweise strikt, was unter welchen Bedingun-

---

5 Niels Lepperhoff, Björn Petersdorf: Datenschutz bei Webstatistiken; in: Datenschutz und Datensicherheit Nr. 4, 2008, S. 266–269; von derselben Quelle aktueller: Xamit-Datenschutzbarometer 2012, http://www.xamit-leistungen.de/downloads/Files.php?f=XamitDatenschutzbarometer2012.pdf

6 Ingo Ruhmann: Wann wird IT-Sicherheit kein Rechtsbruch mehr sein? in: Datenschutz-Nachrichten, Heft 3, 2013, S. 95–100; ders.: IT-Sicherheit und das geplante IT-Sicherheitsgesetz; in: telepolis, 11.04.2013, http://www.heise.de/tp/artikel/38/38891/1.html

FIfF e.V.
Goetheplatz 4, 28203 Bremen
Telefon 0421 33659255
Telefax 0421 33659256
fiff@fiff.de
www.fiff.de

gen erhoben und analysiert werden darf. Die angedachte Änderung des § 15 TMG legte dagegen ähnlich wenig Maßstäbe an die Speicherung und Auswertung an wie § 100 TKG.

Nach Protesten wiederum aus dem Umfeld des AK Vorratsdatenspeicherung wurde diese Neuregelung Ende 2014 wieder aus dem Gesetzentwurf gestrichen, bevor der Entwurf vom Kabinett verabschiedet wurde.

Die Bundesregierung zieht sich damit auf den Standpunkt zurück, dass für die Sicherheit ihrer eigenen Systeme seit 2007 rechtlich angemessene Vorsorge getroffen ist. Für die IT-Systeme der Länder, der Kommunen, und aller privaten Anbieter von WWW-Services dagegen gilt, dass sie sich entweder mit Intrusion-Detection-Systemen für den laufenden Datenverkehr begnügen und auf alle Systeme verzichten, die - wie heute üblich - IP-Adressen von Besuchern speichern und auswerten – oder auch weiterhin ohne jede rechtliche Befugnis und Grundlage mit marktüblichen IT-Sicherheitssystemen Daten sammeln, immer unter dem Risiko, irgendjemand könnte irgendwann die Klage gegen das BMJ von 2006 wiederholen und per Gerichtsbeschluss die Behörde oder den privaten Anbieter zum Abschalten der IT-Sicherheitssysteme zwingen. Auch wenn genau dies eher nicht zu erwarten ist, so wird das Problem dann wirklich akut, wenn es darum geht, die eigenen IT-Sicherheitssysteme darzulegen und den Stand der Technik zum Schutz der Systeme anzuwenden.

Die Betreiber kritischer Infrastrukturen sollen durch das neue IT-Sicherheitsgesetz dazu verpflichtet werden, IT-Sicherheitstechnik nach aktuellem Stand in ihre Systeme einzubauen. Aber: Wie will die Bundesregierung den Widerspruch zwischen dem fortbestehenden Verbot eines Einsatzes bestimmter Sicherheitstechnik und der Pflicht zum Stand der IT-Sicherheitstechnik umsetzen?

- Will die Bundesregierung die Betreiber kritischer Infrastrukturen zwingen, rechtswidrige Technik anzuwenden?
- Oder sollen nur rechtskonforme Schutztechniken vorgeschrieben werden, die dann aber nicht Stand der Schutztechnik sind?
- Sollen die Betreiber kritischer Infrastrukturen durch die Meldepflicht für Sicherheitsvorkommnisse auch noch gezwungen werden, den widerrechtlichen Einsatz von IT-Sicherheitstechnik zuzugeben und sich selbst des Gesetzesverstoßes zu bezichtigen?
- Oder soll es doch mit nicht allzu aufwändiger Technik getan sein?

Eine weit längere Liste solcher Widersprüche ließe sich mühelos erstellen. Wichtig ist dabei jedoch allein die Einsicht, dass es **keinen Unterschied gibt in der Art der Kommunikation und IT-Nutzung als Form der Telekommunikation oder als Webservice. Es kann daher auch in der IT-Sicherheit keinen Unterschied geben zwischen den Sicherheitsniveaus und der legalen Sicherheitstechnik beider Bereiche.**

Zum Schutzgegenstand des Telekommunikationsgeheimnisses nach Art. 10 GG gehören nach dauernder Rechtsprechung des BVerfG nicht nur die Inhalte der Telekommunikation, sondern auch deren „nähere Umstände", das heißt, wer wann mit wem kommuniziert hat. Die Sammlung von Daten zur Störungserkennung und -eingrenzung gemäß § 100 TKG ist dabei unzweifelhaft ein Eingriff in Art. 10 GG und muss sich an den für alle Grundrechtseingriffe geltenden Maßstäben messen lassen – u.a. Normenklarheit, Angemessenheit der Eingriffstiefe, Bestimmtheit und Überprüfbarkeit. Zusammenfassend betrachtet ist die Rege-

FIfF e.V.
Goetheplatz 4, 28203 Bremen
Telefon 0421 33659255
Telefax 0421 33659256
fiff@fiff.de
www.fiff.de

lung des § 100 TKG in dieser Fassung und bei heutiger Technik deutlich jenseits des grundgesetzlich Zulässigen.

Was aber erst recht zu keinem Ergebnis führt, ist das Fehlen einer klaren Regelung für die Datenerhebung zu Sicherheitszwecken in der Welt des WWW. Da es weder rechtlich noch technisch einen Grund für eine unterschiedliche Behandlung beider Bereiche gibt, kann der verfassungskonforme Schlüssel für die IT-Sicherheit – genauer: für den Schutz des Fernmeldegeheimnisses, des Grundrechtes auf informationelle Selbstbestimmung und des Grundrechtes auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme – nur aus einer **einheitlichen und zugleich datensparsamen Regelung für die Sicherheit von IT-Systemen in der Telekommunikation und bei Telemedien bestehen.**

I. Zu den Regelungen zum Schutz kritischer Infrastrukturen – Artikel 1 – 3 des Gesetzentwurfes

Die – als Reaktion der Bundesregierung 1997 auf eine parlamentarische Anfrage der Bündnisgrünen – nach US-Vorbild eingerichtete Arbeitsgruppe KRITIS hat 18 Jahre lang mit Unternehmen darüber diskutiert, was die Betreiber kritischer Infrastrukturen für die Sicherheit ihrer IT-Systeme tun müssen. Die bisherigen Ergebnisse waren Empfehlungen. Nach so langer Zeit ist es daher ein Fortschritt, diese Betreiber dazu zu verpflichten, für ihre IT-Systeme nicht mehr und nicht weniger als jenen Stand der Sicherheitstechnik einzusetzen und anzuwenden, den schon seit Inkrafttreten des Bundesdatenschutzgesetzes 1977 all jene Einrichtungen und Unternehmen anwenden müssen, die personenbezogene Daten sammeln und verarbeiten (anfangs gem. § 6, heute verschärft gem. § 9 BDSG).

Sicherheitsvorfälle zu melden, ist zudem ein sinnvolles Mittel, um Wiederholungen gleicher Angriffe zu verhindern. Überdies ist ein substanzieller Anteil von Betreibern kritischer Infrastrukturen schon aus eigenem Interesse an den nicht staatlich organisierten Computer Emergency Response Teams (CERTs) beteiligt, die dem Zweck dienen, sich über Sicherheitsvorfälle auszutauschen und Gegenmaßnahmen zu entwickeln. Das FIfF begrüßt ausdrücklich diese aus Einsicht geborene Eigeninitiative Einiger, die zudem mit dem Einsatz von Ressourcen verbunden ist. Mit dem Entwurf des IT-Sicherheitsgesetzes wird niemand zur Finanzierung oder Mitwirkung an der Arbeit von CERTs verpflichtet, sondern lediglich alle Betreiber kritischer Infrastrukturen zur Mitwirkung an der Problemermittlung. In diesem maßvollen Schritt ist keine übermäßige Härte oder Belastung zu erkennen.

Bei der Definition dessen, was eine kritische Infrastruktur sei, wurden schon in den 1990er Jahren zu Beginn des Diskussionsprozesses kerntechnische Anlagen ausgeklammert. Spätestens die Reaktorkatastrophe in Fukushima ließ die Frage akut werden, warum ausgerechnet die IT-Sicherheit von Atomkraftwerken nie einer näheren Bewertung unterzogen worden sei. Die wirkliche Überraschung des im Bundeskabinett verabschiedeten aktuellen Entwurfs des IT-Sicherheitsgesetzes ist daher, dass erstmals seit fast 20 Jahren auch Atomkraftwerke als kritische Infrastruktur in die Verpflichtungen zum Schutz der dort genutzten IT-Systeme einbezogen wurden.

Damit kommt ein 18 Jahre währender, fachlich im Prinzip durchaus interessanter Diskussionsprozess um kritische Infrastrukturen zu einem zwar sehr konventionellen, aber immerhin definierten Ende. In den letzten 20 Jahren haben sich jedoch die Probleme um die Sicherheit von IT-Systemen weiterentwickelt und

FIfF e.V.
Goetheplatz 4, 28203 Bremen
Telefon 0421 33659255
Telefax 0421 33659256
fiff@fiff.de
www.fiff.de

hätten weitergehender Ideen und Ansätze bedurft. Solche Aspekte sind jedoch im neuen Entwurf eines IT-Sicherheitsgesetzes unbearbeitet geblieben.

II. Bleibende Differenzen im Recht – zu den Artikeln 4 und 5 des Entwurfs

1. Regelung im TMG

Der Gesetzentwurf schreibt in Artikel 4 als Änderung am TMG den Betreibern vor, Schutztechniken einzusetzen. Ohne Änderungen an § 15 TMG können dies nur Werkzeuge sein wie Passwortschutz, Intrusion Detection Systeme und andere Filter, die den laufenden Datenverkehr auf Auffälligkeiten hin untersuchen. Verboten bleibt die Speicherung von IP-Adressen über den jeweiligen „Nutzungsvorgang" hinaus und damit

a) der Einsatz zahlreicher Formen von Auditing-Systemen in webbasierten Services – angefangen von solchen zur Leistung von Webangeboten über leistungsfähige Sicherheitsanalysesysteme (Security Information and Event Management, SIEM) bis zur Überwachung von Cloud-Services,

b) die Analyse von mehrschrittigen Angriffsformen, die in verschiedenen Nutzungsvorgängen Manipulationen an Webangeboten vornehmen,

c) die nachträgliche Analyse von Schadensfällen und die Feststellung der Verursacher, die nur durch IP-Datenanalyse möglich ist.

Die Position des FIfF ist hier differenziert: Wie die Bundesregierung selbst in § 5 BSIG geregelt hat, ist es keineswegs erforderlich, sich an § 100 TKG und seiner zu weit gefassten Befugnis zur Datensammlung zu orientieren (s.u.). Stattdessen schlägt das FIfF eine eingegrenzte Befugnisnorm für ein zweistufiges Verfahren vor, das praxistauglich und durchaus erprobt ist und Sicherheitsvorfälle zuverlässig aufspüren kann.

- 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.
- 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 für Telemedien ist aus Datenschutzsicht akzeptabel und kontrollierbar, entspricht professionellen IT-Sicherheitsverfahren und ist trotzdem weniger aufwändig als das Verfahren

FIfF e.V.
Goetheplatz 4, 28203 Bremen
Telefon 0421 33659255
Telefax 0421 33659256
fiff@fiff.de
www.fiff.de

gemäß § 5 BSIG. Im IT-Sicherheitsgesetz wäre hier die Befugnis zum Erlass einer Verordnung oder einer technischen Richtlinie angemessen, die das vorher beschriebene oder ein aus Datenschutzsicht besseres Verfahren definiert.

2. Regelung im TKG – zu Artikel 5 IT-Sicherheitsgesetz

Auf dem Telekommunikationsmarkt stellen die Unternehmen derzeit die letzten Reste analoger Telekommunikation auf das Internetprotokoll (IP) um; Ergebnis wird ein **All-IP-Netz** sein. Das Internetprotokoll wurde entwickelt, um die Kommunikation auch bei Ausfällen durch einen Atomkrieg aufrechtzuerhalten. Deshalb enthält das IP bereits wirksame Vorkehrungen zur Störungserkennung und Fehlerkorrektur, die automatisiert in Routern und Gateways realisiert sind. Betriebsstörungen in IP-Netzen beruhen fast immer auf falsch konfigurierter oder fehlerhafter Netzwerktechnik. Die Motivation der Störungserkennung in analogen Netzen hat mit der in digitalen Netzen technisch rein gar nichts mehr zu tun: **„Störungen", die nicht durch die Mechanismen des IP selbst korrigiert werden und auch nicht auf fehlerhafter Netzwerktechnik beruhen, sind Anwendungsfälle für IT-Sicherheit in Reinform.**

Wie ebenfalls bereits erwähnt, muss sich ein Eingriff in Art. 10 GG immer an den für Grundrechtseingriffe geltenden Maßstäben messen lassen – u.a. Normenklarheit, Angemessenheit der Eingriffstiefe, Bestimmtheit und Überprüfbarkeit. Heute wird die in § 100 TKG geregelte Befugnis zur Datenerhebung und -nutzung zu Zwecken der Störungsbeseitigung keinem einzigen dieser Kriterien gerecht, sie ist ohne Befristung und sieht lediglich eine vage „Erforderlichkeit" und ähnliche Klauseln vor.

Die vorgeschlagenen Änderungen an § 100 TKG verschärfen diese Defizite weiter. Der Entwurf des IT-Sicherheitsgesetzes sieht vor, Daten im Telekommunikationssektor auch erheben zu dürfen

> „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".

Der § 100 TKG hatte ursprünglich das Ziel, gem. § 317 StGB strafbare Eingriffe in Fernmeldesysteme für die Öffentlichkeit zu ermitteln. Die geplante Änderung will dies nun ausweiten auf die **Verfügbarkeit unspezifischer „Informations- und Kommunikationsdienste"** sowie auf die unbegrenzte Datensammlung zum Schutz vor einem **„unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer" – also von beliebigen Telekommunikationskunden.**

Diese unspezifische Datensammlung zu Zwecken der IT-Sicherheit wäre ein nahezu unbegrenzter Eingriff in das Fernmeldegeheimnis. Sie ist nicht an die Angabe eines Anlasses gebunden, ist ohne einen genügend spezifischen Zweck, ohne spezifische Kriterien und wird auch noch ohne Vorgaben zu Speicherdauer und zur Datennutzung eingeräumt. Diese in Artikel 3 IT-Sicherheitsgesetz vorgesehene Ausweitung an § 100 TKG ist **eindeutig unvereinbar mit Art. 10 GG. Es ist mit Sicherheit davon auszugehen, dass sie einer Verfassungsklage nicht standhalten wird.**

In einer Neuregelung sind daher grundrechtskonforme Rahmenbedingungen für den Eingriff in Grundrechte einzuarbeiten wie etwa:

FIfF e.V.
Goetheplatz 4, 28203 Bremen
Telefon 0421 33659255
Telefax 0421 33659256
fiff@fiff.de
www.fiff.de

- Eine anlasslose Datensammlung gemäß bisheriger Fassung von § 100 TKG ist auszuschließen; stattdessen sind Verdachtskriterien oder Stichprobengrößen sowie Vorschriften zu deren Pseudonymisierung vorzugeben.
- Ein Zugriff durch Dritte auf die zur Störungserkennung erhobenen Daten ist zu unterbinden.
- Die Dauer einer Datenhaltung ist zu begrenzen, Löschungsfristen für verdachtsfreie Daten (bis zu max. 3 Tage nach Erhebung, Analyse und Reduktion der Daten auf kriterienbasierte Verdachtsfälle) sowie Vorgaben für Analysefristen und Löschung sind vorzugeben.

3. Zur Änderung des § 109a TKG

Das IT-Sicherheitsgesetz sieht als Änderung an § 109a TKG die Verpflichtung des Diensteanbieters vor, bei „Störungen, die von Datenverarbeitungssystemen der Nutzer ausgehen", diese 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".

Voraussetzung für die Störungserkennung dürfen nach der im IT-Sicherheitsgesetz geplanten Änderung des § 100 TKG anlasslos erhobene Daten sein. Diese Daten können technisch und sollen offenbar auch rechtlich zur Identifikation einzelner Nutzer genutzt werden. Mit der Identifikation werden diese Nutzer „bekannt" und sind zu benachrichtigen. Mit der Neufassung des § 109a TKG wird den Telekommunikationsdiensteanbietern damit nun die Aufgabe zugewiesen, die Sicherheit der IT-Geräte von Nutzern zu überwachen und nach Möglichkeit Vorschläge zur Abhilfe zu geben.

Es geht daher nicht länger um eine technische Störungsbeseitigung, sondern um die explizite **Durchsuchung von Datenkommunikation** zur Kenntnisnahme, Identifikation und Benachrichtigung von Telekommunikationskunden ohne die geringsten Vorgaben für eine Eingrenzung auf Kriterien, Speicherdauer oder Analyseform für diese Daten. Auch dieser Regelungsvorschlag ist als tiefer Eingriff in Art. 10 GG ganz **offensichtlich nicht grundrechtskonform**:

1. Der Begriff von „Störungen" hat mit der gebotenen Normenklarheit nichts zu tun. Eine Störung liegt bei einigen Providern schon dann vor, wenn bestimmte Programme genutzt werden, die dem eigenen Geschäftsmodell nicht entsprechen, weswegen die Datenübermittlung in diesen Fällen unterbunden wird. Notwendig wäre hier zumindest die Voraussetzung einer „Gefährdung" anderer IT-Systeme wie etwa durch die Verbreitung von Schadsoftware.
2. Die dauerhafte Überwachung der Kommunikationsdaten auf „Störungen" nach § 100 TKG und das „Bekannt Werden" von Störungen setzen dauerhafte technische Datenanalysen voraus, bei denen die Inhalte aller Datenpakete auf Schadsoftware zu untersuchen sind (**deep packet inspection**), um gezielt Störungen zu erkennen und die verursachenden Nutzer auf diese Störungen hinzuweisen. Eine solche dauerhafte, anlasslose und vollständige Inhaltsüberwachung der Telekommunikation ohne jede Eingrenzung ist mit Art. 10 GG absolut unvereinbar.

Sofern man die Befürchtung einer anlasslosen Überwachung und Datensammlung von Telekommunikationskunden („Vorratsdatenspeicherung") für begründet hält, so sind die an den geplanten Änderungen an

FIfF e.V.
Goetheplatz 4, 28203 Bremen
Telefon 0421 33659255
Telefax 0421 33659256
fiff@fiff.de
www.fiff.de

den §§ 100 und 109c TKG ablesbaren Datenerhebungsmöglichkeiten weit eher ein Argument für diese Befürchtung als jede andere im IT-Sicherheitsgesetz geplante bzw. diskutierte Maßnahme: Anders als Webseitenanbieter, die IP-Verkehre von Zufallsbesuchern erheben, sind Telekommunikationsanbieter die zentrale Schaltstelle für den gesamten Datenverkehr ihrer Kunden, die von ihnen über die bestehenden Vertragsverhältnisse exakt identifizierbar sind. Diese Daten ohne klare Regeln sammeln zu können, ist eine weit größere Gefahr für die Grundrechte als jede andere Maßnahme auf dem Gebiet der IT-Sicherheit.

Zusammenfassung

Das FIfF setzt sich konsequent für die Offenlegung von IT-Sicherheitslücken und -vorfällen ein. Analyse von und Kommunikation über Sicherheitsvorfälle setzen zwingend voraus, eine einheitliche Rechtsgrundlage für die IT-Sicherheit und die Offenlegung von Sicherheitsvorfällen bei Telemedien wie bei Telekommunikationsdiensten zu schaffen, die sowohl das Grundrecht auf informationelle Selbstbestimmung wie auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (1 BvR 370/07) umsetzt und zugleich das Fernmeldegeheimnis wahrt. Das FIfF hält daher eine Änderung des TMG für unbedingt erforderlich, es schlägt dazu aber eine sehr datensparsame Ausgestaltung vor.

Bei der Änderung an § 100 TKG sieht das FIfF dagegen einen klaren Verfassungsverstoß gegen die Begründetheit der Datensammlung, die Normenklarheit und die Angemessenheit eines Grundrechtseingriffs in Art. 10 GG und fordert eine in zahlreichen Punkten wesentlich klarere und begrenztere Befugnis zur Datensammlung, die mit der Verfassung vereinbar ist.

III. Zur Aufklärung über IT-Sicherheitsvorfälle und -risiken und zur Rolle des BSI – Artikel 1 IT-Sicherheitsgesetz

1. Offenlegungspflicht ist verfassungsrechtlich geboten

Das FIfF hält eine konsequente Offenlegung von Schwachstellen für eine Notwendigkeit, denn nur die durch Publikation mögliche Kenntnis um Schwachstellen gibt allen betroffenen Anwendern von IT-Systemen die Chance, solche Schwachstellen zu beseitigen und die Sicherheit der IT-Systeme zu gewährleisten.

Die Bundesregierung formuliert dagegen im Entwurf als neue Aufgabe des BSI in der Ergänzung zu § 7 BSIG:

„Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 kann das Bundesamt

1. die folgenden Warnungen an die Öffentlichkeit oder an die betroffenen Kreise richten:
   a) Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten,
   b) Warnungen vor Schadprogrammen,
   c) Warnungen im Falle eines Verlustes von oder eines unerlaubten Zugriffs auf Daten.
2. Sicherheitsmaßnahmen sowie den Einsatz bestimmter Sicherheitsprodukte empfehlen."

FIfF
Forum Informatikerinnen für Frieden
und gesellschaftliche Verantwortung e.V.

FIfF e.V.
Goetheplatz 4, 28203 Bremen
Telefon 0421 33659255
Telefax 0421 33659256
fiff@fiff.de
www.fiff.de

Eine solche Kann-Bestimmung bei der Veröffentlichung läuft dem grundrechtlich gebotenen Schutz von IT-Systemen diametral zuwider. Mit einer Kann-Bestimmung untergräbt die Bundesregierung zudem die von ihr selbst gesetzten Ziele. Bei allem Verständnis für die Abwägung über den gebotenen Zeitpunkt einer Veröffentlichung von Sicherheitslücken ist als grundsätzliches Ziel eine **Veröffentlichungspflicht grundrechtlich zwingend erforderlich**. Warnungen vor Sicherheitslücken und damit schweren Schäden dürfen nicht dem Belieben Einzelner überlassen werden – insbesondere nicht staatlicher Stellen, da dies **nicht den staatlichen Pflichten aus dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme entsprechen würde**. Der Staat hätte sogar die Aufgabe, private Stellen zur Gewährleistung dieses Schutzes heranzuziehen und zu verpflichten.

Es ist nicht von der Hand zu weisen, dass es in bestimmten Konstellationen von IT-Sicherheitslücken notwendig ist, unmittelbar Schutzmaßnahmen zu ergreifen, bevor eine Veröffentlichung erfolgt. Das FIfF schlägt daher als grundrechtskonforme Änderung an § 7 BSIG vor:

> „Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 hat das Bundesamt nach Abwägung möglicher Risiken zeitnah
>
> 1. die folgenden Warnungen an die Öffentlichkeit oder an die betroffenen Kreise zu richten:"
>
> [...]
>
> Das Bundesamt kann dabei zugleich
>
> 2. Sicherheitsmaßnahmen sowie den Einsatz bestimmter Sicherheitsprodukte empfehlen."

2. Jährliche Berichtspflicht ungenügend

Die in der Änderung zu § 13 BSIG geplante Berichtspflicht des BSI im vorgesehenen jährlichen Turnus ist gänzlich ungeeignet, um schnell und möglichst auch proaktiv Warnungen vor über Einzelfälle hinausgehenden Gefährdungen der IT-Sicherheit auszusprechen.

Jährliche Berichte sind eine spezifische Form zur Aufsicht über Organisationen und deren Arbeit. Bürokratische Aufsichtsverfahren können aber nicht Ziel eines IT-Sicherheitsgesetzes sein. Über den Einzelfall hinaus gab es immer wieder Sicherheitslagen, die sich in einem größeren Kontext über einen begrenzten Zeitraum betrachtet als Entwicklung gezeigt haben, gegen die nur durch eine Analyse und den Austausch von Wissen vorgegangen werden konnte. IT-Sicherheitsfirmen, Verbände und Vereine haben daher anlassgetrieben Informationen über die Lage der IT-Sicherheit publiziert, nicht nach kalendarischen Zyklen.

Das FIfF sieht in den Regelungen zur Publikation von Warnungen und der jährlichen Berichtspflicht eine stark bürokratische und damit unpassende Sichtweise auf IT-Sicherheitsprobleme. Das FIfF fordert daher die **zeitnahe Publikation ausnahmslos aller Sicherheitsbewertungen**, bei der allenfalls Zeitpunkt, Art und Umfang der Publikation darauf abgestimmt werden dürfen, dass das Ausnutzen der Sicherheitslücke nicht befördert wird, dass jedoch die Anwender solcherart gewarnt werden, zeitnah und effektiv Schutzmaßnahmen ergreifen zu können.

FIfF Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

FIfF e.V.
Goetheplatz 4, 28203 Bremen
Telefon 0421 33659255
Telefax 0421 33659256
fiff@fiff.de
www.fiff.de

3. Keine Einschränkung des Informationsfreiheitsgesetzes

Durch Änderungen zu den §§ 8c und 10 BSIG werden Auskünfte nach dem Informationsfreiheitsgesetz (IFG) über Sicherheitsvorfälle bei Betreibern Kritischer Infrastrukturen generell ausgeschlossen; sie sollen nur Verfahrensbeteiligten gewährt werden können.

Dies ist schon deswegen unverhältnismäßig, da das IFG bereits eine Prüfung der schutzwürdigen Belange jener Personen und Einrichtungen vorsieht, über die Angaben in den Akten enthalten sind. Eine Herausgabe geschäftskritischer Informationen über Betreiber oder sicherheitsrelevanter Inhalte aus Akten wäre daher durch das IFG heute bereits ausgeschlossen. Die generelle Verweigerung einer Aktenherausgabe dient hier allein der **Vermeidung jeglicher Prüfung von Anfragen**. Es verhindert zudem die Auseinandersetzung mit für die IT-Sicherheit relevanten Fragen, die für die Verbesserung der IT-Sicherheit allgemein jedoch von grundsätzlicher und hoher Bedeutung sind.

Das FIfF fordert daher die **ersatzlose Streichung** dieser Regelungsteile, da entsprechende Vorkehrungen unnötig sind.

4. Zur Rolle des BSI nach Artikel 1 IT-Sicherheitsgesetz

Das FIfF hat die Gründung des BSI 1989 kritisch kommentiert und dabei zwar die Notwendigkeit einer solchen Behörde betont, aber zugleich deren Doppelaufgabe für staatliche Stellen einerseits und Bürgerinnen und Bürger andererseits problematisiert[7]. Die Novelle des IT-Sicherheitsgesetzes verändert das BSI von der bestehenden Behörde zur Förderung der Sicherheit der IT (§ 3 BSIG i.d. Fassung vom 14.08.2009) – weit überwiegend für die IT des Bundes und nur in geringem Umfang für die Beratung von Herstellern und Nutzern in der Privatwirtschaft (§ 3 Abs. 1 Nr. 14 und 15) – in eine nationale Informationssicherheitsbehörde. Anspruch und Umsetzung stehen jedoch in einem Missverhältnis zueinander.

Ziel des BSI soll nach dem Gesetzentwurf sein:

> „Das Bundesamt ist zuständig für die Informationssicherheit auf nationaler Ebene. Es untersteht dem Bundesministerium des Innern."

Das FIfF begrüßt die Idee, das BSI in eine nationale Informationssicherheitsbehörde umzuwandeln. Dies bedeutet ein Ende des bisherigen Aufgabenschwerpunktes des BSI, sich vorrangig der Sicherheit der IT des Bundes zu widmen, Verschlüsselungssysteme zu prüfen und zuzulassen. Das BSI kann dadurch stärker die Beratung, die Zertifizierung von IT-Produkten und weitere Aufgaben für Bürgerinnen und Bürger, Unternehmen und Interessierte übernehmen.

Die Umsetzung entspricht aus Sicht des FIfF dagegen nicht den verfassungsmäßigen Anforderungen. Das BVerfG hat – wie wiederholt angeführt – das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme definiert. Es ist damit unzweifelhaft Aufgabe von Legislative und

---

7 Ute Bernhardt, Ingo Ruhmann: ZSI: Die Bundesregierung will den Bock zum Gärtner machen; in: Computerwoche, Nr. 52, 22. Dez. 1989, S. 6–8 und: dies.: Mutationen einer Geheimdienststelle; in: Computerwoche, Nr. 12, 23. März 1990, S. 44–47

FIfF Forum Informatikerinnen für Frieden und gesellschaftliche Verantwortung e.V.

FIfF e.V.
Goetheplatz 4, 28203 Bremen
Telefon 0421 33659255
Telefax 0421 33659256
fiff@fiff.de
www.fiff.de

Exekutive, den Schutz und die Sicherheit von IT-Systemen systematisch und umfassend zu gewährleisten und alle nötigen Vorkehrungen zu treffen, dies auch organisatorisch und prozedural umzusetzen.

Als nationale Informationssicherheitsbehörde käme dem BSI die zentrale Aufgabe zu, für die Bürgerinnen und Bürger dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zur Geltung zu verhelfen und konkrete Schritte zu unternehmen, diesen Schutz auch umzusetzen. Dazu wäre jedoch jede Kollision von Interessen und jede Konkurrenz um Ressourcen mit den Anforderungen des Bundesministeriums des Inneren (BMI) als vorgesetzter oberster Bundesbehörde (gemäß des geplanten § 8 Abs. 1 Satz 5 neu und § 8a) unbedingt auszuschließen. Zudem ist auszuschließen, dass das BSI eine Kontrolle der Sicherheit der IT des Bundes aufgrund der Weisungsabhängigkeit nicht mit der gebotenen Unabhängigkeit durchführen könnte. Genau diese Weisungsfreiheit ist der Grund, warum bisher der Bundesrechnungshof (BRH) damit betraut wurde, die Sicherheit der IT des Bundes weisungsungebunden und unabhängig zu prüfen.

Voraussetzung für das BSI als nationale Informationssicherheitsbehörde ist daher sowohl für Bürgerinnen und Bürger als auch insbesondere gegenüber der Bundesverwaltung eine **vollständige Unabhängigkeit und Weisungsungebundenheit** in der Weise, wie sie bisher bei der Prüfung von IT des Bundes durch den BRH ausgeübt wird und von der EU-Kommission für den Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI) gefordert wird.

Das FIfF fordert daher die Bundesregierung auf, das BSI als eine unabhängige Bundesoberbehörde zu organisieren, die nicht dem BMI oder einer anderen obersten Bundesbehörde unterstellt ist. Für diese Aufgaben ist das BSI mit zusätzlichen Ressourcen und Personal auszustatten.

IV. Zur Rolle des BKA als Sonderpolizeibehörde der IT-Sicherheit – zu Art. 5 IT-Sicherheitsgesetz

Mit Art. 5 des geplanten IT-Sicherheitsgesetzes soll das BKA die polizeiliche Aufgabe erhalten, bei den üblichen „Delikten der Computerkriminalität §§ 202a, 202b, 202c, 263a, 303a“ StGB tätig zu werden, die sich gegen „Behörden oder Einrichtungen des Bundes oder“ – kurz gefasst – Betreiber kritischer Infrastrukturen richten.

Für kritische Infrastrukturen und den Bund richtet die Bundesregierung damit eine Art **Sonderdezernat für die Strafverfolgung von Computerkriminalität** ein, die gemäß heutigem § 3 Abs. 1 Nr. 13 BSIG auf das BSI zur Unterstützung zurückgreifen kann.

Angesichts der Pläne der Bundesregierung zur Ausweitung der Verfolgung von Cyberangriffen durch die Bundespolizei, das BfV, den BND und das BKA ist grundsätzlich festzuhalten, dass die

1. reguläre Strafverfolgung von Cyberkriminalität auch durch internationale Kooperation aus Sicht des FIfF der geeignete und bessere Weg ist, der anstelle einer geheimdienstlich-militärischen Bekämpfung von Cyberangriffen gewählt werden sollte. Ausschlaggebend für die erfolgreiche Umsetzung ist allerdings die angemessene Ausstattung von Strafverfolgungsbehörden mit Ressourcen und Personal, um jedermann vor Cyberkriminalität besser zu schützen.
2. Zersplitterung der Strafverfolgung von Cyberkriminalität nicht hilfreich dabei ist, ein wirkungsvolles Gegengewicht gegen kriminelle und staatliche Angriffe auf IT-Infrastrukturen zu bilden. Sinn-

FIfF e.V.
Goetheplatz 4, 28203 Bremen
Telefon 0421 33659255
Telefax 0421 33659256
fiff@fiff.de
www.fiff.de

voll wäre stattdessen eine Schwerpunktstaatsanwaltschaft, die über die nötigen Mittel und Ressourcen verfügt, Cyberkriminalität zum Schutze der Allgemeinheit und nicht allein der IT des Bundes zu verfolgen.

Die Bundesregierung schafft jedoch mit dieser Regelung im BKA keine Verbesserung der Strafverfolgung von Cyberkriminalität für die Bürgerinnen und Bürger allgemein. Sie erklärt statt dessen mit der Begründung, dass die Strafverfolgung und „die örtliche Zuständigkeit oftmals dem Zufall überlassen bleibt", dass die für IT-Kriminalität zuständigen Strafverfolgungsbehörden der Republik nicht mit hinreichenden Kompetenzen und Ressourcen ausgestattet sind, um Angriffe auf die IT des Bundes zu verfolgen, und richtet daher eine Sonderabteilung IT-Kriminalität im BKA ein.

Die Bundesregierung gibt damit nicht nur sich allein die 2007 eingeführten Sonderrechte beim Einsatz von Sicherheitstechnik für ihre eigenen IT-Systeme gem. § 5 BSIG, sondern schafft sich zur Strafverfolgung auch noch eine Sonderermittlungsgruppe, statt den rechtlichen Schutz der Bürgerinnen und Bürger zu verbessern.

Das FIfF begrüßt prinzipiell den Ansatz einer Stärkung der regulären Strafverfolgung. Es fordert aber die Stärkung des Rechts für alle Bürgerinnen und Bürger statt einer Sonderpolizei beim BKA und zugleich den Verzicht auf geheimdienstlich-militärische Reaktionen auf Cyberangriffe sowie die Verlagerung der Mittel aus letzteren Bereichen zu den Behörden zur Strafverfolgung.

FIfF e.V.
Goetheplatz 4, 28203 Bremen
Telefon 0421 33659255
Telefax 0421 33659256
fiff@fiff.de
www.fiff.de

V. Ergänzungsvorschläge

Die Enthüllungen von Edward Snowden und der NSA-Skandal haben der Öffentlichkeit vor Augen geführt, in welchem Ausmaß die Sicherheit von IT-Systemen kompromittiert ist. Aus fachlicher Sicht mindestens ebenso bedeutsam war der in den Medien als „Heartbleed-Bug" bekannt gewordene Fehler in der Programmierung eines der wichtigsten Sicherheitssysteme im Internet, des SSL-Übertragungsprotokolls. Bedeutsam deswegen, weil sich hieran zeigte, dass einerseits die Anker der Sicherheit im Internet mit extrem geringen Ressourcen entwickelt werden und andererseits so gut wie alle Sicherungssysteme für vertrauensvolle und sichere Datenübermittlung im Internet von solchen Verfahren abhängen – insbesondere bei Internet-Zahlungsverfahren und Web-Shops.

1. Zuverlässigkeit zentraler IT-Sicherheitsmechanismen regelmäßig prüfen

Immer noch scheint der Glaube weit verbreitet zu sein, dass IT-Sicherheit ohne Kosten und Aufwand herzustellen sei und dass sensibelste und sicherheitsempfindlichste Abläufe im Internet auf Mechanismen aufbauen könnten, über deren Zuverlässigkeit nach dem NSA-Skandal keine gesicherte Aussage getroffen werden kann.

Der Bundestag konnte bisher den einstimmig vom Ausschuss „Digitale Agenda" verabschiedeten Beschluss nicht in die Tat umsetzen, das Büro für Technikfolgenabschätzung beim Deutschen Bundestag (TAB) damit zu beauftragen, eine Bestandsaufnahme und Abschätzung der Sicherheit und zum möglichen Grad der Kompromittierung wesentlicher IT-Sicherheitsmechanismen vorzunehmen.

Unabhängig sowohl vom Fortgang dieser Beauftragung als auch von dem Problem, dass vonseiten der Wirtschaft mittlerweile dem BSI gegenüber in dessen bisheriger Struktur nur noch begrenztes Vertrauen entgegengebracht wird, hält das FIfF es für eine dauerhaft zu verfolgende Aufgabe, den Stand der Zuverlässigkeit und Sicherheit von grundlegenden, im Internet genutzten Sicherheitsfunktionen dauerhaft zu überprüfen, zu bewerten und die Bewertungsergebnisse zu publizieren.

Das BSI ist abhängig von Weisungen des Innenministeriums, dem es unterstellt ist, und damit im Interessenskonflikt zwischen den Begehrlichkeiten der Sicherheitsbehörden, verschlüsselte Kommunikation abhören zu können, und den Sicherheitsinteressen der Bürger und Unternehmen an vertraulicher und integrer Kommunikation. Daher hält das FIfF es für notwendig, diese Aufgabe unabhängigen kompetenten Stellen zu übertragen, zumindest solange das BSI noch nicht als unabhängige Bundesoberbehörde reorganisiert wurde, die nicht dem BMI oder einer anderen obersten Bundesbehörde unterstellt ist. Hierfür bieten sich Stellen wie das DFN-CERT ebenso an wie etwa die durch das BMBF an Hochschulen und Forschungseinrichtungen geförderten IT-Sicherheits-Kompetenzzentren oder weitere Einrichtungen.

2. Allgemeine Regelungen zum Umgang mit IT-Sicherheitslücken

Die per se vernünftige Idee einer Meldung von IT-Sicherheitsvorfällen ist im IT-Sicherheitsgesetz nur bruchstückhaft umgesetzt. Bei konsequenter Herangehensweise könnte eine nicht weisungsgebunden und unabhängig organisierte Meldestelle für IT-Sicherheitsvorfälle einen effektiven Nutzen bekommen, wenn zuvörderst die Protokollierung von IT-Sicherheitsvorfällen bei Telemedien und Telekommunikationsange-

FIfF e.V.
Goetheplatz 4, 28203 Bremen
Telefon 0421 33659255
Telefax 0421 33659256
fiff@fiff.de
www.fiff.de

boten datenschutzgerecht einheitlich juristisch geregelt würde. Dann könnten die heute durchaus häufigen Meldungen von Sicherheitsproblemen in IT-Systemen zur Verbesserung der IT-Sicherheit genutzt werden durch ein abgestuftes Verfahren nach folgendem Muster.

1. Nach zunächst vertraulicher Meldung eines IT-Sicherheitsproblems in einer Implementierung oder einem Produkt gegenüber einer vertrauenswürdigen Meldestelle könnte diese – ähnlich die Bundesnetzagentur im Telekommunikationssektor – gegenüber dem Verursacher eine Frist zur Abhilfe oder auch Ratschläge zur Abhilfe oder einen Lösungsvorschlag aussprechen.
2. Sofern nötig, könnten Nutzer über das Problem informiert werden.
3. Nach Ablauf der gesetzten Frist stünde die Option offen, das Problem zu publizieren, sodass Betroffene in einem Schadensfall den Verursacher zivilrechtlich in Regress nehmen könnten. Durch eine derartige Organisation würde die Grundlage geschaffen, die Regelungen aus dem Bereich der Produkthaftung in die IT-Welt zu übertragen und dort beweisbar und damit juristisch handhabbar zu machen.

Die zwischengeschaltete vertrauenswürdige Stelle gibt „**Whistleblowern**" eine Anlaufstelle, ihr Wissen um Schwachstellen bekannt zu machen, ohne dabei selbst in Erscheinung zu treten und sich zu gefährden. Durch eine derartige gestufte Fristenregelung wäre eine Eingrenzung von Schäden möglich, aber zugleich auch eine Beseitigung der diesen zugrunde liegenden IT-Sicherheitsproblemen. Dies entspräche wiederum der Idee der Verpflichtung zur Aufklärung über kompromittierte IT-Sicherheitstechniken.

3. Grundrechtskonformer Schutz des Telekommunikationsgeheimnisses

Das Grundgesetz sieht den Schutz des Post- und Fernmeldegeheimnisses vor. Nach ständiger Rechtsprechung des Bundesverfassungsgerichts umfasst dies auch die „näheren Umstände" der Telekommunikation, was sich sogar im TKG wiederfindet. Das deutsche Strafrecht dagegen ist – wie historisch mittlerweile ausgezeichnet aufgearbeitet wurde[8] – darauf ausgerichtet, die Wünsche der alliierten Besatzungsmächte nach dem Zweiten Weltkrieg und die mit ihnen geschlossenen Übereinkünfte umzusetzen.

So ist der Bruch des Fernmeldegeheimnisses zwar verboten, bleibt aber für genau jene straffrei, gegen deren Eingriff sich das Grundgesetz richtet. Der im Zuge der TKG-Verabschiedung 1996 neu gefasste Strafrechtsparagraph § 206 StGB lautet:

> (1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.
>
> [...]

8 Josef Foschepoth: Überwachtes Deutschland. Post- und Telefonüberwachung in der alten Bundesrepublik; Göttingen, 2012

FIfF e.V.
Goetheplatz 4, 28203 Bremen
Telefon 0421 33659255
Telefax 0421 33659256
fiff@fiff.de
www.fiff.de

(4) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die ihm als außerhalb des Post- oder Telekommunikationsbereichs tätigem Amtsträger auf Grund eines befugten oder unbefugten Eingriffs in das Post- oder Fernmeldegeheimnis bekanntgeworden sind, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(5) Dem Postgeheimnis unterliegen die näheren Umstände des Postverkehrs bestimmter Personen sowie der Inhalt von Postsendungen. Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

Die Strafbarkeit nach Abs. 1 bezieht sich allein auf Mitarbeiter von Unternehmen, die „geschäftsmäßig Post- oder Telekommunikationsdienste erbringen", nicht jedoch auf jedermann, wie etwa beim Schutz des Briefgeheimnisses nach § 202 StGB. Das Gesetz schließt also aus, dass sich Geheimdienstmitarbeiter beim Abhören strafbar machen können. Obendrein setzt eine Strafbarkeit zwei weitere Faktoren voraus:

1. dass einem Mitarbeiter Tatsachen „bekanntgeworden sind" und
2. diese Person „unbefugt einer anderen Person eine Mitteilung über solche Tatsachen macht".

Nicht strafbar sind also automatisiert arbeitende Überwachungsverfahren, die darauf angelegt sind, dass keinem Mitarbeiter Tatsachen aus Telekommunikationsvorgängen „bekannt werden". Das Problem der Filterung von E-Mails am Arbeitsplatz wird daher auch rechtlich als Unterschlagung oder Abfangen von Daten beurteilt: das Fernmeldegeheimnis bietet hier keinen Schutz. Im Zeitalter semantischer Datenanalyse und Echtzeit-Suche mit Filterworten ist dies überaus anachronistisch: Kein Mensch muss sich zu Überwachungszwecken noch Telekommunikationsverkehre ansehen oder anhören – das Scanning von Kommunikation leisten heute Algorithmen, deren Einsatz das deutsche Strafrecht straffrei lässt. Die menschliche Kenntnisnahme ist erst bei Auswertung der Ergebnisse nötig – **die vorherige automatisierte und flächendeckende Überwachung ist rechtlich nicht begrenzt.**

Die Verknüpfung der ersten beiden Satzteile in § 206 Abs. 1 StGB schließlich bewirkt, dass sich selbst ein Mitarbeiter eines Telekommunikationsunternehmens, der Telekommunikationsverkehre abhört, erst dann strafbar macht, wenn er seine Erkenntnisse unbefugt Dritten weitergibt, statt das Erspähte für sich zu behalten oder nur an Befugte zu berichten. Der Sinn dieser Klausel entstand – wie Foschepoth deutlich macht – aus der Verpflichtung von Postbediensteten zur Mitwirkung an der Überwachung, die geheim bleiben sollte, und an der Weitergabe der Ergebnisse an Geheimdienste.

Derselbe Grund liegt bei § 206 Abs. 4 vor: Whistleblower außerhalb von Post- und Telekommunikationsunternehmen werden mit Strafe bedroht – auch Geheimdienstler, die eine Überwachung verraten. Die Arbeit des Historikers Foschepoth hat die detaillierte Konstruktion des Rechts entsprechend der Arbeitsteilung zwischen Bundespost und Geheimdiensten nachgezeichnet. Die Enthüllungen von Edward Snowden haben diesen Widersinn nochmals deutlich werden lassen: Nach deutschem Strafrecht kann sich kein Geheimdienstmitarbeiter jemals durch ein Abhören – den Bruch des Fernmeldegeheimnisses – strafbar machen. Strafbar macht sich nur, wer die Öffentlichkeit informiert, dass abgehört wird.

FIfF e.V.
Goetheplatz 4, 28203 Bremen
Telefon 0421 33659255
Telefax 0421 33659256
fiff@fiff.de
www.fiff.de

Der letzte Versuch, das deutsche Recht etwas mehr mit der Verfassung zu vereinbaren, wurde im Bundestag 1996 unternommen[9]. Dies wurde damit begründet, dass in einer Zeit, in der so gut wie alles online organisiert wird, das Fernmeldegeheimnis und sein Schutz zur Voraussetzung für andere Grundrechte und somit zu einem „strategischen Schutzrecht" werde[10]. Dieser bisher letzte Versuch scheiterte jedoch.

Es ist nun an der Zeit, § 206 StGB – Bruch des Fernmeldegeheimnisses – analog dem Schutz des Briefgeheimnisses nach § 202 StGB auszuweiten auf einen Rechtsverstoß durch jedermann. Dabei sollte der Eingriff durch Mitarbeiter von Telekommunikationsunternehmen mit einem höheren Strafmaß (5 Jahre) geahndet werden als Eingriffe durch Jedermann.

Im Lichte der Enthüllungen schlägt das FIfF daher folgende Änderung vor:

§ 206 Abs. 1 StGB wird wie folgt gefasst:

> "(1) Wer sich unbefugt Kenntnis von Fernmeldevorgängen, die dem Fernmeldegeheimnis unterliegen, verschafft oder so gewonnene Kenntnisse nutzt oder unbefugt einem anderen eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft."

Der bisherige Abs. 1 wird zu Abs. 2, Abs. 2 wird zu Abs. 3, Abs. 3 wird zu Abs. 4. Der bisherige Abs. 4 entfällt.

---

9 ┐Änderungsantrag des Abg. Dr. Manuel Kiper und der Fraktion Bündnis 90/Die Grünen zum Entwurf eines Telekommunikationsgesetzes, hier Nr. h) zu § 354 StGB, Bt.-Drs. 13/4892, S. 4

10 ┐Ingo Ruhmann, Christiane Schulzki-Haddouti: Abhör-Dschungel; in: c't, Nr. 5, 1998, S. 82–93. Siehe auch: Manuel Kiper, Ingo Ruhmann: Der Schlüssel zur Kontrolle der Informationsgesellschaft; in: Olga Drossou, Kurt van Haaren et. al.: Machtfragen der Informationsgesellschaft, Marburg, 1999, S. 251–261 und dies.: Von der Datenflut zur Abhörwut: Erfahrungen mit ‚kleinen' Lauschangriffen; in: Blätter für deutsche und internationale Politik, Heft 3, 1998, S. 312–319.

Bosbach Wolfgang

Von: CSokolowski@dslv.spediteure.de
Gesendet: Dienstag, 3. März 2015 18:03
An: Bosbach Wolfgang
Betreff: Stellungnahme zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)
Anlagen: DSLV-Stellungnahme IT-Sicherheitsgesetz.pdf

Sehr geehrter Herr Bosbach,

als Spitzenverband repräsentiert der Deutsche Speditions- und Logistikverband (DSLV) über 16 Landesverbände etwa 3.000 Mitgliedsbetriebe mit 520.000 Beschäftigten, mehrheitlich größere mittelständische und inhabergeführte Speditionen sowie global agierende Logistikkonzerne.

Den Ihnen vorliegenden Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) sieht der DSLV kritisch. Er befürchtet, dass die Unternehmen der Speditions- und Logistikbranche durch das Gesetz erheblich belastet werden, obwohl sie nicht zu den Betreibern „Kritischer Infrastrukturen" zählen. Die Bundesregierung geht zwar branchenübergreifend von „nur" 2.000 betroffenen Unternehmen aus. Sie räumt aber selbst ein, dass dies nur eine sehr grobe Einschätzung sei, da die Zahl der betroffenen Unternehmen wesentlich von einer noch zu erstellenden Rechtsordnung abhänge.

Dieses Problem hat auch der Bundesrat erkannt, der darum bittet, im weiteren Gesetzgebungsverfahren dafür Sorge zu tragen, dass zur Schaffung von Planungs- und Rechtssicherheit eine weitere Konkretisierung von unbestimmten Rechtsbegriffen erfolgt, und hier vor allem eine Präzisierung des Begriffs „Kritische Infrastrukturen" anmahnt.

Zu beachten ist auch, dass die Speditions- und Logistikbranche ist ein polypolistischer Markt ist, der überwiegend von kleinen und mittleren Unternehmen geprägt wird. Die Transportaufkommen in der Bundesrepublik verteilen sich auf eine große Zahl von Dienstleistern. Bei Ausfall eines und auch mehrerer Speditions- und Logistikunternehmen wird es immer alternative Dienstleister geben, die die Speditions- und Logistikdienstleistung übernehmen können, sodass Versorgungsengpässe oder gar Gefährdungen der öffentlichen Sicherheit nicht entstehen.

Wir erlauben uns daher, Ihnen anbei unsere Stellungnahme an das Bundesministerium des Innern vom November 2014 zu übermitteln und hoffen, dass unsere Position bei Ihrer Beratung des Gesetzentwurfs berücksichtigt wird.

Für einen Dialog stehen wir Ihnen jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen

Dr. Christoph Sokolowski

DSLV Deutscher Speditions- und Logistikverband e. V.
Referat Politik und Kommunikation
Platz vor dem Neuen Tor 5, 10115 Berlin
Telefon: +49 (0) 30 2787469-0
Telefax: +49 (0) 30 2787469-9
E-Mail: CSokolowski@dslv.spediteure.de
www.dslv.org

DSLV
Deutscher Speditions- und Logistikverband e.V.

DSLV · Deutscher Speditions- und Logistikverband e. V. · Postfach 1360 · 53003 Bonn

Bundesministerium des Innern
Referat IT II 1
Alt Moabit 101 D
10559 Berlin

Ihr Zeichen	ITII1-17002/7#2
Ihre Nachricht vom	4. November 2014
Unser Zeichen	LE/MG
Telefon-Durchwahl	0228 91440-28
Telefax-Durchwahl	0228 91440-728
E-Mail	LEickmeyer@dslv.spediteure.de
Datum	12. November 2014

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

Sehr geehrte Damen und Herren,

gerne macht der Deutsche Speditions- und Logistikverband (DSLV) von der Möglichkeit Gebrauch, zu dem von Ihnen übermittelten Referentenentwurf für ein Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) Stellung zu nehmen.

Fünf Werktage sind allerdings zur detaillierten Kommentierung eines 62-seitigen Gesetzes eine sehr kurze Zeit. Wir möchten uns daher vorbehalten, gegebenenfalls weitere Kommentare nachzureichen.

Anwendungsbereich / Definition Kritischer Infrastrukturen

Eine Beurteilung des vorliegenden Referentenentwurfs bezogen auf die Speditions- und Logistikbranche hängt maßgeblich vom Adressatenkreis ab. Eine Konkretisierung durch Rechtsverordnung steht jedoch noch aus.

Die Speditions- und Logistikbranche ist ein polypolistischer Markt, der überwiegend von kleinen und mittleren Unternehmen geprägt ist. Entsprechend der aktuellen Studie „TOP 100 der Logistik" der Fraunhofer Arbeitsgruppe für Supply Chain Services erwirtschaften die umsatzstärksten 100 Logistikdienstleister etwa 27 Prozent des gesamten Branchenumsatzes. Die Transportaufkommen in der Bundesrepublik verteilen sich also auf eine große Zahl von Dienstleistern.

Bei Ausfall eines und auch mehrerer Speditions- und Logistikunternehmen wird es immer alternative Dienstleister geben, welche die Speditions- und Logistikdienstleistung übernehmen können, sodass Versorgungsengpässe oder gar Gefährdungen der öffentlichen Sicherheit nicht entstehen. Beispiele für den ungestörten Ablauf der Versorgung selbst bei weitgehenden Ausfällen eines Verkehrsträgers sind der letzte Streik der Lokomotivführer ab 5. November 2014 und der Ausbruch des Vulkans Eyjafjallajökull im März 2010. Trotz weitgehender Beeinträchtigungen des Güterverkehrs kam es auch bei diesen Ereignissen zu keinen Versorgungsengpäs-

sen. Speditions- und Logistikunternehmen zählen daher nach Auffassung des DSLV nicht zu den Betreibern Kritischer Infrastrukturen und sollten damit vollständig vom Wirkungsbereich des Gesetzes ausgenommen werden. Mindestens aber sollten neben den im Gesetzentwurf ausgeklammerten Kleinstunternehmen im Sinne der Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 in jedem Fall auch kleine und mittlere Unternehmen ausgenommen werden.

Meldepflichten bei IT-Sicherheitsvorfällen

Die Pflicht zur Meldung von IT-Sicherheitsvorfällen für Betreiber Kritischer Infrastrukturen berührt vor allem den diskreten Umgang mit Daten, der für Unternehmen durchaus wettbewerbsrelevant ist. Nach dem vorliegenden Referentenentwurf bleibt für den Anwender unklar, wie solche IT-Sicherheitsvorfälle zu spezifizieren und die Meldungen überhaupt zu kontrollieren sind. Es ist bisher auch zu wenig konkretisiert, was eine „bedeutende Störung" im Sinne des Gesetzes ist.

Eine Verpflichtung für Unternehmen, Beeinträchtigungen ihrer IT-Infrastruktur melden zu müssen, kann nur gefordert werden, wenn diese Meldungen auch geeignet sind, einem berechtigten Schutzzweck zu dienen. Ansonsten stellt der administrative Aufwand zur Erfüllung der umfänglichen Meldeverpflichtungen eine ressourcen- und kostenintensive Mehrbelastung für Unternehmen dar, ohne einen Mehrwert für die Sicherheit zu leisten. Unklar ist jedoch, wie diese insofern unspezifizierten Meldungen, ohne dass zuvor die Beeinträchtigung analysiert, Folgen absehbar oder ihr Ursprung ermittelbar wären, zu einem Sicherheitslagebild beitragen können. Unternehmen sollten grundsätzlich die Möglichkeit haben, IT-Beeinträchtigungen zunächst intern zu analysieren, Fehlerquellen aufzudecken und Gegenmaßnahmen einzuleiten, bevor sie freiwillig qualitativ aufbereitete Informationen über relevante Beeinträchtigungen mit Marktteilnehmern und Behörden teilen.

Positiv wird vom DSLV die Einräumung einer Möglichkeit zur anonymen Meldung von IT-Sicherheitsvorfällen gesehen. Dennoch bleibt ein erheblicher administrativer Aufwand zu befürchten, der insbesondere für kleine und mittlere Unternehmen zu einer schweren Belastung führen würde. Bei aller Sicherheit ist die Belastbarkeit der Unternehmen stets im Auge zu behalten.

Mindestsicherheitsstandards für informationstechnische Systeme

Als kritisch erachtet der DSLV zudem die vorgeschriebenen Nachweispflichten der Einhaltung von Mindestsicherheitsstandards, da diese einen Eingriff in die unternehmerischen Prozesse und die unternehmerischen Entscheidungsfreiheiten darstellen. Auch wenn die Berücksichtigung branchenspezifischer Sicherheitsstandards begrüßt wird, werden die Anforderungen an den zu erbringenden Nachweis im Gesetz nur unzureichend konkretisiert.

Grundsätzlich befürwortet der DSLV die Einhaltung von Mindestsicherheitsstandards für informationstechnische Systeme auf freiwilliger Basis. Die Anwendung von Informations- und Kommunikationssystemen betrifft den Kern des außerordentlich kommunikationsintensiven Speditions- und Logistikgeschäfts. Angemessene Sicherheitsvorkehrungen für ihre IT-Sicherheit zu treffen, liegt deshalb schon im Geschäftsinteresse von Speditions- und Logistikunternehmen selbst. So treffen selbstverständlich auch heute schon mittelständische Speditionsunternehmen und Speditionskooperationen, in der Regel zusammen mit ihren Softwarelieferanten und Kommunikationsanbietern, Vorkehrungen zur Erhaltung ihrer IT-Sicherheit.

In verschiedenen Bereichen unserer Branche hat sich eine freiwillige Zertifizierung von Managementsystemen, beispielsweise bei speziellen Güter-, Kunden- und Umweltanforderungen, bewährt. Anwendung und Verbreitung der Regelwerke vollziehen sich im Marktwettbewerb. Auch gibt es bereits einzelne Speditionsunternehmen und Speditionskooperationen, die ein zertifiziertes Informationssicherheitsmanagementsystem eingerichtet haben. Solche freiwilligen Lösungen sind in der Wirtschaft unbedingt vorzuziehen.

Zusammenfassend begrüßt der DSLV zwar grundsätzlich den von der Bundesregierung angestoßenen Diskussionsprozess zur branchenübergreifenden Verbesserung des IT-Sicherheitsniveaus. Gleichzeitig sind jedoch auch Bedenken an der Schaffung einer nationalen Lösung zu äußern. Globalen Cyberbedrohungen lässt sich effektiv nur mit einem abgestimmten und zumindest europaweit harmonisierten, strategischen Sicherheitskonzept begegnen. Nationalstaatliche Einzelmaßnahmen hingegen bedeuten gerade für weltweit tätige Unternehmen enorme zusätzliche Kosten, ohne dabei einen wirksamen Sicherheitsnutzen zu liefern.

Eine stärkere Zusammenarbeit zwischen Staat, Wissenschaft und Wirtschaft scheint essentiell notwendig, um den wachsenden Bedrohungspotenzialen mit passenden Sicherheitsantworten zu begegnen. Die Speditions- und Logistikbranche ist an verständlich aufbereiteten, aktuellen Informationen zur IT-Sicherheit interessiert. Bezüglich der Meldung von erheblichen IT-Sicherheitsvorfällen weist der DSLV auf die freiwillige Teilnahme von Unternehmen an der „Allianz für Cyber-Sicherheit" hin, die weiter entwickelt werden sollte. Solch ein Austausch von Informationen fördert die Zusammenarbeit und damit auch das Vertrauen.

Die Sicherheit informationstechnischer Systeme nimmt auch für die Speditions- und Logistikbranche eine zunehmende Bedeutung ein. Ein branchenbezogener Leitfaden könnte für viele, vor allem auch mittelständische Unternehmen, eine Orientierungshilfe bei der Einführung eines Informationssicherheitsmanagementsystems sein. Der DSLV würde es begrüßen, wenn gegebenenfalls auf Unterstützung durch Programme des Bundesministeriums des Innern (BMI) und seiner Ämter, wie beispielsweise dem Bundesamt für Sicherheit in der Informationstechnik (BSI), gerechnet werden könnte. Nach Meinung des DSLV sollten zunächst der Dialog – zwischen BMI, BSI, Branchenverbänden und Unternehmen – wie auch die auf freiwilliger Teilnahme basierenden Maßnahmen zur Verbesserung der IT-Sicherheit vorangebracht werden.

Mit freundlichen Grüßen

DSLV Deutscher Speditions- und Logistikverband e. V.
Referat Marktbeobachtung und Statistik /
Prozesse, Standards, Elektronischer Geschäftsverkehr

Luana Eickmeyer

Schuchardt Katja PA4

Von: Bosbach Wolfgang
Gesendet: Donnerstag, 16. April 2015 14:32
An: Innenausschuss PA4
Betreff: WG: LogisTicker zum IT-Sicherheitsgesetz - DSLV: Speditions- und Logistikunternehmen sind keine Betreiber "Kritischer Infrastrukturen"
Anlagen: mylogo_vudpoiis6bj978fgk34aapac20.jpeg; DSLV-LogisTicker_IT-Sicherheitsgesetz.pdf

Von: CSokolowski@dslv.spediteure.de [mailto:CSokolowski@dslv.spediteure.de]
Gesendet: Donnerstag, 16. April 2015 14:19
An: Bosbach Wolfgang
Betreff: LogisTicker zum IT-Sicherheitsgesetz - DSLV: Speditions- und Logistikunternehmen sind keine Betreiber "Kritischer Infrastrukturen"

Sehr geehrter Herr Bosbach,

Die Bundesregierung möchte die IT-Sicherheitslage in Deutschland verbessern und hat hierzu den Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vorgelegt. Der Deutsche Speditions- und Logistikverband (DSLV) sieht den Entwurf, durch den mehrere Gesetze geändert werden, kritisch.

Er befürchtet, dass die Unternehmen der Speditions- und Logistikbranche dadurch erheblich belastet werden. Sie zählen nach Auffassung des DSLV nicht zu den Betreibern „Kritischer Infrastrukturen“, werden aber in der geplanten Änderung des BSI-Gesetzes dazu gezählt. Die Bundesregierung geht zwar branchenübergreifend von „nur“ 2.000 durch das IT-Sicherheitsgesetz betroffenen Unternehmen aus, räumt aber selbst ein, dass dies nur eine sehr grobe Einschätzung sei, da die Zahl der betroffenen Unternehmen wesentlich von einer noch zu erstellenden Rechtsordnung abhänge.

Der DSLV fordert

- Die Ausnahme der Speditions- und Logistikunternehmen vom Anwendungsbereich des IT Sicherheitsgesetzes, da sie nicht Betreiber „Kritischer Infrastrukturen“ sind; mindestens aber

- die Konkretisierung des Begriffs „erhebliche Störungen“ und weiterer unbestimmter Rechtsbegriffe im Entwurf

- den Vorrang einer freiwilligen Meldung von IT-Sicherheitsvorfällen vor einer gesetzlichen Meldepflicht

Weitere Einzelheiten können Sie der beigefügten aktuellen Ausgabe des „LogisTicker“ entnehmen.

Mit freundlichen Grüßen

Dr. Christoph Sokolowski

DSLV Deutscher Speditions- und Logistikverband e. V.
Referat Politik und Kommunikation
Platz vor dem Neuen Tor 5, 10115 Berlin
Telefon: +49 (0) 30 2787469-0
Telefax: +49 (0) 30 2787469-9

E-Mail: CSokolowski@dslv.spediteure.de
www.dslv.org

LogisTicker
Hintergrundinformationen und Meinungen aus Spedition und Logistik
April 2015

IT-Sicherheitsgesetz

DSLV: Speditions- und Logistikunternehmen sind keine Betreiber „Kritischer Infrastrukturen“

Die Bundesregierung möchte die IT-Sicherheitslage in Deutschland verbessern und hat hierzu den Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vorgelegt. Der Deutsche Speditions- und Logistikverband (DSLV) sieht den Entwurf, durch den mehrere Gesetze geändert werden, kritisch.

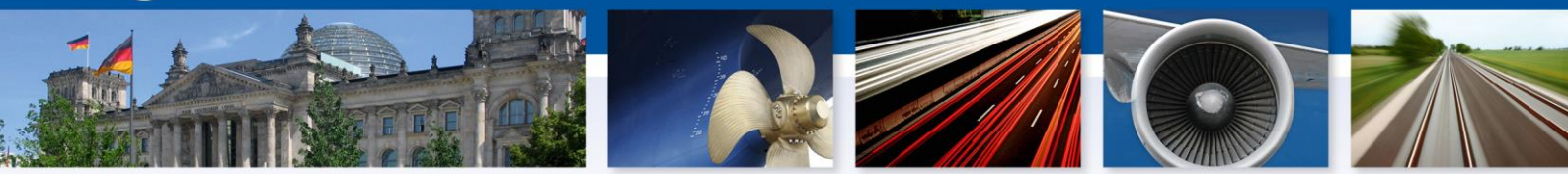
Er befürchtet, dass die Unternehmen der Speditions- und Logistikbranche dadurch erheblich belastet werden. Sie zählen nach Auffassung des DSLV nicht zu den Betreibern „Kritischer Infrastrukturen“, werden aber in der geplanten Änderung des BSI-Gesetzes dazu gezählt. Die Bundesregierung geht zwar branchenübergreifend von „nur“ 2.000 durch das IT-Sicherheitsgesetz betroffenen Unternehmen aus, räumt aber selbst ein, dass dies nur eine sehr grobe Einschätzung sei, da die Zahl der betroffenen Unternehmen wesentlich von einer noch zu erstellenden Rechtsordnung abhänge.

Der DSLV fordert

- die Ausnahme der Speditions- und Logistikunternehmen vom Anwendungsbereich des IT-Sicherheitsgesetzes, da sie nicht Betreiber „Kritischer Infrastrukturen“ sind; mindestens aber
- die Konkretisierung des Begriffs „erhebliche Störungen“ und weiterer unbestimmter Rechtsbegriffe im Entwurf
- den Vorrang einer freiwilligen Meldung von IT-Sicherheitsvorfällen vor einer gesetzlichen Meldepflicht

Die Speditions- und Logistikbranche ist überwiegend von mittelständischen Unternehmen geprägt. Dies bedeutet, dass sich das Transportaufkommen in Deutschland auf eine große Zahl von Dienstleistern verteilt. Deshalb stehen beim Ausfall von einem oder mehreren Branchenunternehmen stets alternative Dienstleister bereit, so dass Versorgungsengpässe oder gar Gefährdungen der öffentlichen Sicherheit nicht zu befürchten sind. Gute Bei-

Herausgeber: Deutscher Speditions- und Logistikverband e. V. (DSLV) | Verantwortlich für den Inhalt: Frank Huster (Hauptgeschäftsführer)
Sitz: Weberstraße 77, 53113 Bonn | Büro Berlin: Platz vor dem Neuen Tor 5, 10115 Berlin | www.dslv.org
Kontakt: Dr. Christoph Sokolowski (Leiter Politik und Kommunikation), Tel.: 030 2787469-0, E-Mail: CSokolowski@dslv.spediteure.de



spiele hierfür sind der Ausbruch des Vulkans Eyjafjallajökull in Island im März 2010 oder der Streik der deutschen Lokomotivführer im November 2014. In keinem dieser Fälle kam es trotz Beeinträchtigungen des Güterverkehrs zu Versorgungsengpässen. Trotzdem werden Einrichtungen aus dem Bereich Transport und Verkehr im durch das IT-Sicherheitsgesetz neu eingefügten § 2 Abs. 10 BSI-Gesetz zu den „Kritischen Infrastrukturen“ gezählt. Dieser Passus „Transport und Verkehr“ ist im Entwurf zu streichen.

Der DSLV bringt es auf den Punkt:

Der vorliegende Entwurf eines IT-Sicherheitsgesetzes führt zu erheblichen Belastungen für die Unternehmen der Speditions- und Logistikbranche. Nach Auffassung des DSLV zählen sie nicht zu den Betreibern „Kritischer Infrastrukturen“, denen im Gesetz unter anderem eine umfassende Meldepflicht bei „erheblichen Störungen“ auferlegt wird. Die Nennung des Bereichs „Transport und Verkehr“ ist deshalb im Gesetz zu streichen. Mindestens müssen aber bereits im Gesetz etliche unbestimmte Rechtsbegriffe konkretisiert werden. Der DSLV warnt vor einer massiven Belastung der Unternehmen ohne signifikanten Gewinn an IT-Sicherheit und setzt sich alternativ für eine freiwillige Meldung bei gravierenden IT-Sicherheitsvorfällen ein.

1. Meldepflichten bei IT-Sicherheitsvorfällen

Nach dem vorliegenden Gesetzentwurf obliegt den Betreibern „Kritischer Infrastrukturen“ eine umfassende und unverzügliche Meldepflicht bei „erheblichen Störungen“ ihrer informationstechnischen Systeme. Hier ist völlig unklar, wann eine solche „erhebliche Störung“ vorliegt und wie der genaue Meldeprozess auszusehen hat. Zudem ist der Adressatenkreis im Gesetzentwurf nicht konkretisiert. Diese Vielzahl an unbestimmten Rechtsbegriffen im Entwurf hat auch der Bundesrat in seiner Stellungnahme vom 6. Februar 2015 kritisiert. Abgesehen davon ist eine derartige Meldepflicht für Unternehmen nur dann sinnvoll, wenn sie einem berechtigten Schutzzweck dient. Ansonsten steht dem administrativen und kostenintensiven Aufwand zur Erfüllung dieser Rechtspflicht kein Mehrwert an IT-Sicherheit gegenüber. Sollten die Unternehmen der Speditions- und Logistikbranche zu den Gesetzesadressaten zählen, sollten sie grundsätzlich die Möglichkeit haben, IT-Beeinträchtigungen zunächst intern zu analysieren und Gegenmaßnahmen einzuleiten, bevor sie auf freiwilliger Basis aufbereitete Informationen über relevante Beeinträchtigungen mit Behörden teilen.

2. Mindestsicherheitsstandards für informationstechnische Systeme

Kritisch sieht der DSLV auch die Pflicht von Betreibern „Kritischer Strukturen“, die Einhaltung von Mindestsicherheitsstandards regelmäßig nachzuweisen. Dies stellt für ihn einen erheblichen Eingriff in die unternehmerische Entscheidungsfreiheit dar, falls die von ihm vertretenen Unternehmen unter den Anwendungsbereich des Gesetzes fallen sollten. Dagegen befürwortet der DSLV grundsätzlich die Einhaltung von Mindeststandards für IT-Systeme auf freiwilliger Basis. Deren Einsatz betrifft den Kern des außerordentlich kommunikationsintensiven Speditions- und Logistikgeschäfts. Es liegt deshalb schon im Geschäftsinteresse von Speditions- und Logistikunternehmen, selbst angemessene Sicherheitsvorkehrungen für ihre IT-Sicherheit zu treffen.

Herausgeber: Deutscher Speditions- und Logistikverband e. V. (DSLV) | Verantwortlich für den Inhalt: Frank Huster (Hauptgeschäftsführer)
Sitz: Weberstraße 77, 53113 Bonn | Büro Berlin: Platz vor dem Neuen Tor 5, 10115 Berlin | www.dslv.org

Kontakt: Dr. Christoph Sokolowski (Leiter Politik und Kommunikation), Tel.: 030 2787469-0, E-Mail: CSokolowski@dslv.spediteure.de

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)290

Deutscher Factoring Verband e.V.
Behrenstraße 73
10117 Berlin

DEUTSCHER FACTORING VERBAND E.V.

Deutscher Bundestag
Innenausschuss
Platz der Republik 1
11011 Berlin

Berlin, den 08.04.2015

Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

Sehr geehrter Herr Bosbach,
sehr geehrte Damen und Herren,

als maßgebliche Interessensvertretung der deutschen Factoringbranche (Gesamtumsatz der 24 Mitglieder in 2013: über 171 Mrd. Euro, Anteil am deutschen Factoringmarkt: ca. 90%), deren Mitglieder alle der Erlaubnis- und Aufsichtspflicht der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und der Deutschen Bundesbank unterliegen, möchten wir die Gelegenheit wahrnehmen, Ihnen unsere Ansichten zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) darzulegen, welches aktuell in Ihrem Ausschuss beraten wird.

1. Unklare Definition des Begriffs „Kritische Infrastrukturen"

Der Regierungsentwurf des IT-Sicherheitsgesetzes (Bundestags-Drucksache 18/4096) enthält bekanntlich insbesondere Anforderungen an die Sicherheit der Informationstechnik sog. „Kritischer Infrastrukturen" sowie Meldepflichten bei Beeinträchtigungen der Sicherheit dieser informationstechnischen Systeme, Komponenten bzw. Prozesse (vgl. hierzu die im Regierungsentwurf vorgesehenen Änderungen von §§ 8a und b, 10 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik - BSIG). Hierbei ist jedoch aktuell noch **unklar, wie genau der Begriff „Kritische Infrastrukturen" in der noch zu erlassenden Rechtsverordnung definiert werden wird** (vgl. die im Regierungsentwurf vorgesehenen Änderungen von §§ 2 Abs. 10 und 10 Abs. 1 BSIG). Aus dem geplanten § 2 Abs. 10 BSIG sowie der Begründung des Regierungsentwurfs (vgl. S. 9 und 23) geht lediglich hervor, dass u.a. auch das **„Finanz- und Versicherungswesen" zu den vom IT-Sicherheitsgesetz erfassten Sektoren gehören** soll. Da es sich beim Factoring (auch) um eine Finanzdienstleistung handelt (vgl. § 1 Abs. 1a Nr. 9 KWG), könnten auch Factoringunternehmen als Teil des v.g. Finanzwesens in den Anwendungsbereich des geplanten IT-Sicherheitsgesetzes fallen, **sofern diese als „von hoher Bedeutung für das Funktionieren des Gemeinwesens" anzusehen** sind und **„durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden"** – gerade diese zusätzlichen Merkmale sind der **entscheidende Teil der Definition des Begriffs „Kritische Infrastrukturen"**, jedoch macht ihre **ungenaue und auslegungsbedürftige Formulierung** eine **klare Subsumtion und somit Bestimmung des Anwendungsbereichs unmöglich**. Dies ist nicht zuletzt **unter dem Gesichtspunkt der**

Tel.: +49 (0) 30 20 654 654
Fax: +49 (0) 30 20 654 656
www.factoring.de
kontakt@factoring.de

Verbandsgeschäftsführer:
RA Dr. iur. Alexander M. Moseschus
Vereinsregister: Amtsgericht Charlottenburg VR 270078 B

Vorstand:
Joachim Secker
Hauke Kahlcke
Michael Menke

DEUTSCHER FACTORING VERBAND E.V.

Rechtssicherheit äußerst bedenklich, zumal „so" niemand abschätzen kann, ob und ggf. welche Factoringunternehmen unter die neuen Vorschriften fallen werden.

2. Vermeidung unnötiger Dopplungen gesetzlicher Anforderungen

Das Factoring ist eine Finanzdienstleistung, die nur von Finanzdienstleistungs- und Kreditinstituten mit entsprechender Erlaubnis der Bundesanstalt für Finanzdienstleistungsaufsicht erbracht werden darf (vgl. § 1 Abs. 1a Nr. 9 i.V.m. § 32 KWG). **Somit unterliegen Factoringinstitute auch den aufsichtsrechtlichen Anforderungen u.a. aus dem Kreditwesengesetz (KWG)**, zu denen schon heute die nach § 25 KWG erlassenen **„Mindestanforderungen an das Risikomanagement (MaRisk)"** gehören (vgl. https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/rs_1210_marisk_ba.html).
Hierin sind **auch Mindestanforderungen an die technisch-organisatorische Ausstattung der Institute** enthalten. Eine **Novellierung der MaRisk** sowie die **Ausarbeitung eines völlig neuen Normenkatalogs unter dem Titel „Bankaufsichtliche Anforderungen an die IT (BAIT)"** sind zudem von den Finanzaufsichtsbehörden **bereits in Aussicht gestellt** worden (vgl. hierzu auch die geplanten Änderungen insbesondere von § 25a KWG durch das SRM-Anpassungsgesetz unter http://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Referentenentwuerfe/2015-03-10-Bankenabwicklungsrechts-srm.html).
Vor diesem Hintergrund stellen die **geplanten Anforderungen des IT-Sicherheitsgesetzes** für Factoringinstitute eine **unnötige Dopplung bzw. Wiederholung von Anforderungen und Pflichten** dar, die sich bereits aus verschiedenen finanzaufsichtsrechtlichen Normen und Prüfungen ergeben. Zudem ist die **Verteilung von Anforderungen und Meldepflichten rund um das Thema IT auf verschiedene Gesetze, Verordnungen und Verlautbarungen** unterschiedlicher Behörden (BaFin, Bundesbank, BSI) **für die Übersichtlichkeit gesetzlicher Regelungen nicht förderlich**.
Im Interesse des Bürokratieabbaus und der Unterstützung unternehmerischer Compliance befürworten wir daher dringend zum einen die **Einschränkung des Anwendungsbereichs des geplanten IT-Sicherheitsgesetzes auf solche Sektoren, die nicht bereits ähnlichen oder gleichlautenden Anforderungen aus anderen Normen unterliegen**, und zum anderen die **inhaltliche Abstimmung des geplanten IT-Sicherheitsgesetzes auf bereits geltende und in Kürze erfolgende Gesetze und Normsetzungsvorhaben**. Dies könnte auch dadurch erreicht werden, dass bestimmte Anforderungen, Prüfungen und Zertifizierungen, die in einem Gesetz vorgesehen sind und erfüllt werden, **explizit auch als Erfüllung der in einem anderen Gesetz vorgesehenen Anforderungen, Prüfungen und Zertifizierungen anerkannt** werden.

Für Rückfragen stehen wir Ihnen zur Verfügung, gerne auch in einem persönlichen Gespräch.

Mit freundlichen Grüßen
Deutscher Factoring-Verband e.V.

RA Dr. Alexander M. Moseschus
Verbandsgeschäftsführer

RAin Magdalena Wessel
Dezernentin Recht

Verband der TÜV e.V.
Präsidium

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)291

Friedrichstraße 136
10117 Berlin
Deutschland
Tel. +49 30 760095-400
Fax +49 30 760095-401

berlin@vdtuev.de
www.vdtuev.de

TÜV®

VdTÜV | Friedrichstraße 136 | 10117 Berlin | Deutschland

An den Vorsitzenden des
Innenausschusses des Deutschen Bundestags
Herrn Wolfgang Bosbach MdB

per E-Mail: innenausschuss@bundestag.de

Datum
09.04.2015

VdTÜV-Stellungnahme zum Gesetzesentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) BT-Drucksache 18/4096

Sehr geehrter Herr Vorsitzender,

der VdTÜV begrüßt die im IT-Sicherheitsgesetz vorgeschlagenen Rechtsänderungen, mit denen eine signifikante Verbesserung der Sicherheit informationstechnischer Systeme in Deutschland erreicht werden soll. Wir schlagen jedoch vor, bei der Novellierung des BSI-Gesetzes in Artikel 1 des Gesetzesentwurfs den präventiven Schutz gegen IT-Angriffe und die notwendige Vertrauensinfrastruktur zu stärken.

Aus unserer Sicht findet die notwendige Unabhängigkeit der Stellen, die Sicherheitsaudits, Prüfungen und Zertifizierungen vornehmen können, keine ausreichende Berücksichtigung. Gerade unabhängige IT-Sicherheitsüberprüfungen vermitteln jedoch glaubhaft, dass neue und intelligente Technologien auch sicher und vertrauenswürdig sind, und so diese die nötige Akzeptanz in der Bevölkerung finden. IT-Sicherheit und Vertrauen in kritische Infrastrukturen sind entscheidende Faktoren für die digitale Entwicklung von Wirtschaft und Gesellschaft. Das IT-Sicherheitsgesetz sollte die Chance nutzen, zu einem echten Standortvorteil für Deutschland zu werden. Dabei verweisen wir auf die Ergebnisse der Enquete Kommission des Deutschen Bundestags „Internet und digitale Gesellschaft", und angesichts der Internationalität des Gesetzesentwurfs auf laufende europäischen Gesetzesinitiativen (NIS-Richtlinie) und internationale Standards (z. Bsp. Cybersecurity Framework in den USA), die u.a. für IT-Sicherheitsüberprüfungen kritischer Infrastrukturen unabhängige, qualifizierte Stellen empfohlen haben.

Wir vertreten die Auffassung, dass IT-Sicherheitsvorfälle grundsätzlich einer pseudonymisierten Meldung über eine branchenspezifische Ansprechstelle unterliegen sollen. Im Fall eines Ausfalls oder einer erheblichen Störung der Kritischen Infrastruktur muss die Meldung namentlich erfolgen. Der Gesetzgeber sollte allerdings zeitnah, unter Abwägung der Interessen der Wirtschaft und des Sicherheitsbedürfnisses der Bevölkerung bzw. Dritter, über den Verordnungsweg konkreter definieren, wann „erhebliche Störungen" vorliegen und auch welche Mindestanforderungen letztlich eine entsprechende Ansprechstelle erfüllen muss.

Wir möchten Sie bitten, unsere Ausführungen in Ihren weiteren Beratungen zu berücksichtigen. Für Erläuterungen und Rückfragen stehen wir jederzeit gern zur Verfügung.

Mit freundlichem Gruß

Klaus Brüggemann

Dr. Klaus Brüggemann
Geschäftsführendes Präsidiumsmitglied

Im Einzelnen:

I. Zu Artikel 1 Änderung des BSI-Gesetzes § 7a *Untersuchung der Sicherheit in der Informationstechnik*

Eine international akzeptierte Qualitäts- und Sicherheitsinfrastruktur ist Kernaufgabe deutscher Wirtschafts- und Industriepolitik. Bei umfassenden Untersuchungen von IT-Produkten,- Systemen und –Diensten müssen vom BSI beauftragte Dritte ihre notwendige Unabhängigkeit nachweisen können, denn die Übertragung von Prüfkompetenz auf „Dritte" setzt voraus, dass diese „Dritten" über das entsprechende Know-How verfügen, qualifiziert zu prüfen. Zur Wahrung von Geschäftsgeheimnissen, Vertraulichkeit und grundsätzlichen Unternehmensinteressen dürfen „Dritte" weder an der Entwicklung, Herstellung, Lieferung, Reparatur oder Wartung des zu bewertenden Gegenstands beteiligt sein. Diese notwendige Unabhängigkeit des beauftragten Dritten vom Betreiber bzw. Hersteller oder Anbieter stärkt zudem die Glaubwürdigkeit der Untersuchung und schafft Vertrauen in die IT-Produkte,- Systeme und -Dienste. Vom BSI beauftragte Dritte müssen zudem ihre fachliche Qualifikation für die Untersuchung von IT-Produkten,- Systemen und Diensten gegenüber der nationalen Sicherheitsbehörde nachweisen. Der Gesetzgeber schafft mit der Beauftragung qualifizierter unabhängiger Dritter ausreichend Prüf- und Begutachtungsressourcen für eine beschleunigte und kompetente Untersuchung von IT-Produkten,- Systemen und –Diensten in Deutschland.

Für eine entsprechende Konkretisierung sollte § 7a (1) auf Seite 10 des IT-Sicherheitsgesetzes wie folgt ergänzt werden (kursiv):

„Das Bundesamt darf zur Erfüllung seiner Aufgaben auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte, Systeme und Dienste untersuchen. Es darf sich hierbei der Unterstützung *qualifizierter unabhängiger* Dritter bedienen, [...]."

II. Zu Artikel 1 Änderung des BSI-Gesetzes § 8a *Sicherheit in der Informationstechnik Kritischer Infrastrukturen*

Für Audits, Prüfungen oder Zertifizierungen im Bereich der Informationstechnik Kritischer Infrastrukturen müssen konkrete Anforderungen festgelegt und transparente Regeln aufgestellt werden. In der Begründung zu § 8a Abs. 3 wird unterstrichen, dass die Bundesregierung Auditoren für qualifiziert hält, wenn sie ihre Qualifikation und Kompetenz gegenüber dem BSI formal glaubhaft machen können. Der VdTÜV begrüßt diese Entscheidung: Für Betreiber Kritischer Infrastrukturen ist es essentiell, das Sicherheitsniveau von IT-Lösungen, -Komponenten und -Prozessen kontinuierlich zu überprüfen, sowie u. a. auch das Informationssicherheits-Management-System (ISMS) auf geeignete Weise durch ein Audit, eine Prüfung oder Zertifizierung durch eine qualifizierte Stelle zu optimieren. Zu den Vorteilen eines professionellen Informationssicherheits-Management-Systems zählt insbesondere die wirksame Kontrolle von IT-Risiken durch ein systematisches Risiko-Management. Somit können Schwachstellen aufgedeckt, Risiken sowie potenzielle Schäden und Folgekosten minimiert werden. Nach unserer Auffassung muss dabei vor allem die Unabhängigkeit der Ausgabestelle des Audits, Prüfberichts oder Zertifikats sichergestellt werden. Bei internen Audits, Prüfungen oder Zertifizierungen durch den Betreiber steigt grundsätzlich das Risiko von reinen Routineprüfungen oder auch der ungewollten Beeinflussung, wodurch die Effizienz und Aussagekraft des Audits, der Prüfung oder Zertifizierung geschwächt wird. Unabhängige Prüfungen entlasten Unternehmen eigene Prüfkompetenzen aufbauen zu müssen, zudem erzielen unabhängige, qualifizierte Prüfungen entscheidende Impulse und Anstöße zu einer wirksamen Verbesserung der Betreiber- oder Unternehmens IT-Sicherheitsarchitektur.

Es ist daher wichtig, dass bereits das BSI-Gesetz einen eindeutigen Hinweis auf die notwendige Unabhängigkeit und Qualifikation der Prüfer bzw. Zertifizierer enthält.

Für eine entsprechende Festlegung auf den Nachweis durch Sicherheitsaudits, Prüfungen oder Zertifizierungen sollte § 8a (3) auf Seite 11 des IT-Sicherheitsgesetzes wie folgt geändert werden:

„Die Betreiber Kritischer Infrastrukturen haben mindestens alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen *einer qualifizierten unabhängigen Stelle* erfolgen. Die Betreiber übermitteln dem Bundesamt eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Bei Sicherheitsmängeln kann das Bundesamt die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse und, soweit erforderlich, im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen."

III. Zu Artikel 1 Änderung des BSI-Gesetzes § 8b *Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen*

Der VdTÜV begrüßt die Pläne zur Einführung einer Meldepflicht von Störungen bei informationstechnischen Systemen, Komponenten oder Prozessen für Betreiber Kritischer Infrastrukturen an das BSI. Diese Regelung muss für alle Kritischen Infrastrukturbetreiber gleichermaßen gelten. Das BSI wird durch die Meldepflicht, entsprechend seiner Aufgabe, in die Lage versetzt, eine Verbesserung des Lagebilds zur IT-Sicherheit zu erreichen. Schwerwiegende Beeinträchtigungen informationstechnischer Systeme, Komponenten oder Prozesse sollten über eine unabhängige Ansprechstelle an die nationale Sicherheitsbehörde gemeldet werden. Hierzu bedarf es noch einer Präzisierung des Rechtsbegriffs „erhebliche Störung", wie in § 8b (4) Satz 1 BSI Gesetz eingeführt, sowie welche Mindestanforderungen eine entsprechende Ansprechstelle erfüllen muss

Grundsätzlich sollte die Meldung in pseudonymisierter Form gefasst sein. Zur Erstellung eines Lagebilds durch das BSI ist die verpflichtende Offenlegung der Identität des meldenden Betreibers nicht zwingend erforderlich. Einerseits wird so das Risiko von Reputationsschäden für das meldende Unternehmen minimiert. Andererseits bleibt dem BSI hierdurch die Möglichkeit, ein uneingeschränktes Lagebild zu erstellen, um mögliche Gegenmaßnahmen zum Schutz anderer Unternehmen bzw. Betreiber Kritischer Infrastrukturen einzuleiten. Gleichzeitig kann ein neutraler Rückkanal von der Sicherheitsbehörde über die benannte Ansprechstelle an das Unternehmen implementiert werden, um aktuelle Informationen über Angriffe von der Behörde zu erhalten. Durch diesen entsprechenden nachvollziehbaren und auditierbaren Übermittlungsprozess in pseudonymisierter Form bleibt der Betreiber der Kritischen Infrastruktur für die Behörde identifizierbar. (§ 8b (4) BSI-Gesetz, S. 12 IT-Sicherheitsgesetz)

Zudem sollte in Anlehnung an das Bundesdatenschutzgesetz (§3 (6a)) in § 8b (5) Satz 2 auf Seite 12 der entsprechende Informationsaustausch zwischen den Kontaktstellen und dem BSI wie folgt konkretisiert bzw. geändert werden:

„Wurde eine solche benannt, erfolgt ~~der~~ *ein pseudonymisierter* Informationsaustausch zwischen den Kontaktstellen und dem Bundesamt über die gemeinsame Ansprechstelle."

IV. Zu B. Lösung S. 3 des IT-Sicherheitsgesetzes – europarechtliche Implikationen

Entsprechend der Stellungnahme des nationalen Normenkontrollrates in Anlage 2 auf Seite 41 der BT-Drucksache 18/4096, gilt es im Hinblick auf die parallel zu diesem Gesetzgebungsverfahren laufenden europäischen Verhandlungen über die NIS-Richtlinie, ein Auseinanderfallen der Regelungen zu vermeiden, da eventuelle spätere Änderungen infolge der Richtlinie zu unnötigem Mehraufwand bei den Adressaten führen würden.

Die Bundesregierung weist selbst auf Seite 3 des Gesetzesentwurfs darauf hin, dass auch auf europäischer Gesetzgebungsebene das Thema IT-Sicherheit behandelt wird, insbesondere in dem von der Europäischen Kommission entwickelten Vorschlag für eine „Richtlinie des europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union". Deutlicher als im deutschen Gesetzesentwurf soll hier allerdings die Prüfung der Sicherheit von Netz- und Informationssystemen in Art. 15 Absatz 2b der vorgeschlagenen EU-Richtlinie durch u. a. qualifizierte unabhängige Stellen erfolgen. Dieser Aspekt ist im deutschen Gesetzesentwurf derzeit, wie oben genannt, schwächer formuliert. An dieser Stelle könnte eine Orientierung an der europäischen Richtlinie für Informationssicherheit vorteilhaft sein, um die Aussagekraft und Belastbarkeit der Sicherheitsüberprüfungen zu erhöhen. Unabhängige Stellen unterstreichen die Zuverlässigkeit, Glaubwürdigkeit und das Vertrauen in die Sicherheitsüberprüfungen.

Zudem hat der Deutsche Bundestag bereits 2013 im Neunten Zwischenbericht der Enquete-Kommission „Internet und digitale Gesellschaft", wie der europäische Gesetzgeber, in Drucksache 17/12541 die Position erlangt, dass für besonders schutzbedürftige Bereiche eine gesetzliche Pflicht zu einer unabhängigen Sicherheitsüberprüfung und zugleich Zertifizierungen notwendig erscheint. Aus unserer Sicht sollte diese Erkenntnis in der weiteren parlamentarischen Behandlung des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme berücksichtigt werden.

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)294

Bundesverband

Positionspapier

IT-Sicherheitsgesetz

Zentrale Anmerkungen im Rahmen der Anhörung am 20. April 2015

Der ASW Bundesverband sieht die Ansätze des IT-Sicherheitsgesetzes positiv, gleichzeitig jedoch wichtigen Verbesserungsbedarf in den Details.

Anforderungen, Überprüfung und Audits

Der ASW Bundesverband begrüßt die Einführung **branchenspezifischer Mindestanforderungen** an die IT-Sicherheit, wenn diese von den Branchenverbänden festgelegt werden. Wir wollen keine Situation, in der Unternehmen, die verantwortungsvoll in Sicherheit investieren, einen Kosten- und somit Wettbewerbsnachteil gegenüber denjenigen haben, die sich der Verantwortung entziehen und diese notwendigen Investitionen sparen.

Eine schnelle Umsetzung der Sicherheitsstandards erachtet der Verband als sinnvoll. Gleichwohl erscheint eine **Umsetzungsfrist** in vielen Bereichen nicht realistisch. Der ASW Bundesverband schlägt daher vor, dass zwar grundsätzlich eine Frist von 2 Jahren einzuhalten ist. Sollte dieses Ziel jedoch für einzelne Branchen nicht erreicht werden können, kann die Frist, bei Nachweis bislang vertretbar großer Anstrengungen zur Zielerreichung, um ein Jahr verlängert werden.

Den im Gesetzesentwurf vorgesehenen **Überprüfungszeitraum** von 2 Jahren erachten wir als zu eng gefasst. Der ASW Bundesverband empfiehlt, dass Vertreter der Spitzenverbände und des BSI gemeinsam branchenspezifische Prüfmechanismen erarbeiten.

Die Forderung des Gesetzes nach **Übermittlung** aller detaillierter **Auditergebnisse** etc. für den Fall vorliegender Sicherheitsmängel erachten wir als zu weit gehend. Zumindest sollte dies erst bei wiederholter und andauernder Existenz schwerwiegender Sicherheitsmängel gelten. Dies entspricht auch dem Geist der pseudonymisierten Meldung bei nicht-kritischen Sicherheitsvorfällen.

Meldepflicht für IT-Sicherheitsvorfälle

Der Gesetzentwurf sieht eine pseudonymisierte Meldepflicht bereits für **Vorfälle** vor, **die kritisch sein könnten**. Der ASW Bundesverband sieht hierbei die Gefahr, dass Unternehmen, um rechtmäßig zu handeln, unzählige Vorfälle werden melden müssen, da oftmals nicht sofort erkennbar ist, ob hier eine potenzielle Gefährdung vorliegt. Das BSI könnte damit in einer Flut von Meldungen ertrinken und dabei ggf. solche übersehen, die tatsächlich wichtig sind.

Wenn der Zwang zur Meldung bleiben soll, dann müsste zumindest in der Gesetzeserläuterung festgehalten werden, dass Unternehmen kein Gesetzesverstoß vorzuhalten ist, wenn sie nachweislich nach bestem Wissen und Gewissen handeln und einzelne Vorfälle nicht melden, die sich nachträglich als potenziell gefährlich herausstellen. Hierdurch erhielten die Unternehmen die notwendige Rechtssicherheit.

Kritische Vorfälle müssen laut Gesetzesentwurf ohne Pseudonymisierung „offen“ gemeldet werden. Der ASW Bundesverband schlägt vor, dass auch kritische Vorfälle pseudonymisiert gemeldet werden können sollten, wenn das BSI auf Wunsch die Klarnamen erhalten kann und eine ständige Erreichbarkeit für Rückfragen gegeben ist. Hierdurch ergäbe sich kein Nachteil für das BSI. Gleichzeitig kann die Sorge der Unternehmen, kritische

ASW – Bundesverband | Allianz für Sicherheit in der Wirtschaft e.V.
Zieher Business Center | Rosenstraße 2 | 10178 Berlin
Telefon (030) 200 77 200 | Telefax (030) 200 77 056
info@asw-bundesverband.de | www.asw-bundesverband.de

Informationen könnten allzu leicht in Umlauf kommen, zu guten Teilen genommen werden. Grundsätzlich fehlt dem ASW Bundesverband auch eine frühzeitige Klarheit, welche Informationen in diesem Fall übermittelt werden müssen.

Details in Verordnungen

Der Gesetzesentwurf sieht für zahlreiche Detailregelungen Verordnungen vor. Als Beispiel sei die genaue Definition der betroffenen Unternehmen genannt. Diese Verordnungen sollten in Zusammenarbeit mit den Branchenverbänden erarbeitet und dabei sichergestellt werden, dass hier ein gemeinsamer Konsens erreicht wird.

Das Wichtigste in Kürze

- Umsetzungsfrist anpassen
- Überprüfungszeitraum flexibler zu gestalten
- Empfehlung eines weitgehenden Verzichtes auf die Übermittlung von Schwachstellen bei Audits
- Rechtssicherheit für Meldung potenziell kritischer Vorfälle sichern
- Pseudonymisierung aller Meldungen
- Einbindung der Verbände in der Ausarbeitung der Verordnungen

ASW – Bundesverband | Allianz für Sicherheit in der Wirtschaft e.V.
Zieher Business Center | Rosenstraße 2 | 10178 Berlin
Telefon (030) 200 77 200 | Telefax (030) 200 77 056
info@asw-bundesverband.de | www.asw-bundesverband.de

BVLH
Bundesverband des Deutschen Lebensmittelhandels

HDE
Handelsverband Deutschland

Handelsverband Deutschland • 10873 Berlin

An den Bundestagsausschuss für Inneres

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)297

15.04.2015

„Entwurf des IT-Sicherheitsgesetzes“

Sehr geehrte «Anrede» «Name»,

derzeit befindet sich der Entwurf des IT-Sicherheitsgesetzes in der parlamentarischen Abstimmung. Wir möchten hierzu nicht erneut Stellung nehmen und verweisen auf die Positionen des BVLH und des HDE in anliegendem PDF-Dokument.

Eindringlich hinweisen möchten wir Sie allerdings auf eine Unstimmigkeit in der Begründung (B. Besonderer Teil) des Entwurfes. Zu Nummer 8 (§ 10 Ermächtigung zum Erlass von Rechtsverordnungen) zu Buchstabe a (Kriterien zur Bestimmung der Kritischen Infrastrukturen). Dort werden die unterschiedlichen Sektoren aufgeführt, die kritische Dienstleistungen im Sinne des Gesetzes sein können. Unter Nummer 6 wird der Sektor „Ernährung“ genannt. In der Klammer werden dann die Bezeichnungen „Ernährungswirtschaft“ und „Lebensmittelhandel“ ergänzt.

Dies ist u.E. eine nicht richtige Darstellung. Laut allgemein anerkannter Definition umfasst die Lebensmittelwirtschaft bzw. Ernährungswirtschaft als Wirtschaftszweig die Wirtschaftsbereiche, die sich mit Produktion, Verarbeitung und Handel von Lebensmitteln bzw. Nahrungsmitteln befassen. Daher ist die zusätzliche Nennung von Lebensmittelhandel eine Doppelbenennung, die nicht nachvollziehbar ist, gängigen Einteilungen widerspricht und entsprechend zu streichen ist.

Im Vergleich hierzu wird unter Sektor „Energie“ (Nummer 1) bei den Stromversorgern auch nicht unterschieden in Netzbetreiber und Stromerzeuger.

Insofern möchten wir Sie dringend um entsprechende Korrektur des Entwurfes zum IT-Sicherheitsgesetz bitten.

Mit freundlichen Grüßen

Ulrich Binnebößel
Handelsverband Deutschland

Christian Mieles
Bundesverband des Deutschen Lebensmittelhandels

Ulrich Binnebößel
Am Weidendamm 1 A
10117 Berlin
Telefon: (030) 72 62 50-62
Telefax: (030) 72 62 51-88
E-Mail: binneboessel@hde.de
www.einzelhandel.de

Referentenentwurf
für ein Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

Stellungnahme des Handels

Einleitung

Das Bundesministerium des Innern (BMI) übermittelte am 4. November 2014 den betroffenen Wirtschaftszweigen einen Referentenentwurf für ein Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) zur weiteren Abstimmung.

Die Verbände BVLH und HDE nehmen, stellvertretend für die Unternehmen des deutschen Lebensmittel-Einzelhandels, aufgrund der besonderen Betroffenheit der Branche nachfolgend zum Vorschlag Stellung:

Kernelement des Vorschlages/Betroffenheit

Angelehnt an den ersten Vorschlag aus dem Jahre 2013 soll auch mit dem jetzt vorgelegten Entwurf eines IT-Sicherheitsgesetzes eine signifikante Verbesserung der Sicherheit informationstechnischer Systeme in Deutschland erreicht werden, was der Lebensmittelhandel ausdrücklich begrüßt.

Was die wesentlichen Kernelemente des jetzigen Regelungsvorschlages betrifft, gilt für Betreiber Kritischer Infrastrukturen künftig u. a.:

- eine Verpflichtung binnen zwei Jahren nach Inkrafttreten der Rechtsverordnung angemessene Vorkehrungen und Schutzmaßnahmen zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind;
- dass sie oder ihre Verbände branchenspezifische Sicherheitsstandards vorschlagen können;
- dem Bundesamt für Sicherheit in der Informationstechnik (BSI) mindestens alle zwei Jahre eine Aufstellung der durchgeführten Sicherheitsaudits, Prüfungen oder Zertifizierungen, einschließlich der dabei aufgedeckten Sicherheitsmängeln, zu übermitteln;
- bei Sicherheitsmängel dem BSI auf Verlangen die Unterlagen zur Verfügung zu stellen;

- dem BSI binnen sechs Monaten nach Inkrafttreten der Rechtsverordnung Warn- und Alarmierungskontakte zu benennen, über die er jederzeit erreichbar ist;
- die Beeinträchtigung ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung führen können, unverzüglich an das BSI (ggf. anonym) zu melden;
- führt eine Beeinträchtigung zu einem Ausfall oder zu einer Beeinträchtigung der Kritischen Infrastruktur, dies unverzüglich über seine Warn- und Alarmierungskontakte unter Angabe der Informationen an das BSI zu melden.

In Betrachtung dieser sehr weitreichenden Regelungselemente sollte aus Sicht des Lebensmittelhandels zunächst sehr sorgfältig geprüft werden, welche Branchen und Wirtschaftszweige als unmittelbar gefährdete Kritische Infrastrukturen einzustufen sind. Hier pauschal und ohne nähere Begründung den Sektor Ernährung einzubeziehen, der dann in der Begründung in Richtung der Branchen Ernährungswirtschaft und Lebensmittelhandel konkretisiert wird, halten wir weder für nachvollziehbar noch für zielführend.

Besonderheiten des Lebensmittelhandels

Bereits in der Stellungnahme des Lebensmittelhandels zum ersten Gesetzesvorschlag, die wir Ihnen am 5. April 2013 übermittelt hatten, stellten wir nach eingehender Analyse fest, dass die Gefahr flächendeckender Versorgungsengpässe aufgrund von Cyberattacken als sehr gering eingeschätzt wird. Zwar bestehen durchaus Möglichkeiten, dass es in einzelnen Unternehmen oder Unternehmensteilen zu Störungen des Betriebes kommt, ein flächendeckender Ausfall über längere Zeit wird aber mit Blick auf die Anbieter- und Systemvielfalt im Handel - wie nachfolgend dargestellt - als wenig realistisch eingestuft:

- Der Lebensmittelhandel ist durch eine Vielzahl einzelner Unternehmenseinheiten gekennzeichnet.
- Der Betrieb der Geschäfte und die dazu erforderliche IT-Infrastruktur werden jeweils individuell, also je Vertriebslinie und Region, gesteuert. Es gibt keine unternehmensübergreifenden Netzwerke.
- Der Einsatz der IT-Systeme (Hardware und Software) im Handel ist äußerst heterogen und ist von einer Vielzahl von Anbietern und Eigenentwicklungen geprägt.
- Die Unternehmen haben aus Eigeninteresse umfangreiche Maßnahmen zur Herstellung einer größtmöglichen IT-Sicherheit ergriffen.
- Bei einem IT-Komplettausfall kann über Notfallprozeduren der Betrieb - bis zu zwei Wochen - aufrechterhalten werden. Beispielsweise können Filialen bei Ausfall des Bestellwesens mit „Verdachtsbelieferungen“ versorgt werden.
- Meist unterschiedliche IT-Automatisierungssysteme steuern Lagerung und Filialbetrieb der Unternehmen.
- Trotz großer Umschlagsgeschwindigkeit reichen die Bestände einer Filiale zumindest für mehrere Tage aus.
- Die Bestände auf Großhandelsstufe sind teils durch manuelle Prozesse noch nutzbar.

Im Ergebnis wird deutlich, dass allein die große Vielfalt an Unternehmenseinheiten dazu führt, dass eine flächendeckende Gefährdung aller Unternehmen durch Cyberattacken sehr unwahrscheinlich ist. Hinzu kommen die ganz unterschiedlichen IT-Systeme im Handel. Dies trägt ebenfalls zur Erkenntnis bei, dass ein zentraler Angriff mit Auswirkungen auf alle Unternehmen des Lebensmittelhandels nur schwer möglich ist. Kritische Infrastrukturen, deren Ausfall die Versorgung der Bevölkerung gefährden könnten, sind daher im Lebensmittelhandel nicht auszumachen.

Doppelte Betroffenheit des Lebensmittelhandels

Der Entwurf sieht unter anderem auch den Sektor Transport und Verkehr als kritische Dienstleistungen vor. Hierzu stellen wir fest, dass wesentliche Teile des Handels auf logistischen Prozessen basieren. Die Lagerung von Waren und Bündelung über Zentralläger mit anschließender Belieferung der Filialen ist eine klassische Transportleistung, die bereits im Spiegelstrich „Transport von Gütern“ im genannten Sektor aufgegriffen wird. Große Bereiche bzw. die möglicherweise als kritisch erkannten Prozesse des Handels wären daher ohnehin bereits von der Regulierung betroffen.

Handel bereits heute umfassend in der Pflicht

Aus den Handelshäusern wird zudem deutlich darauf hingewiesen, dass sich aus den im Unternehmensumfeld anwendbaren Gesetzen bereits heute konkrete Verpflichtungen für die Gewährleistung eines angemessenen IT-Sicherheitsniveaus in den Unternehmen ableiten lassen.

Die Unternehmen des Lebensmittelhandels setzen diese gesetzlichen Forderungen - auch im eigenen Interesse - schon heute um. Dies geschieht insbesondere zur Absicherung der Geschäftsprozesse und somit zur Sicherstellung des Fortbestandes des eigenen Unternehmens.

Hingegen wird ein weiteres Gesetz, wie im konkreten Fall das IT-Sicherheitsgesetz, als nicht geeignet eingestuft, das IT-Sicherheitsniveau in den Unternehmen zu erhöhen. Dies wird wie folgt begründet:

- Die bereits heute zur Verfügung stehenden Gesetze, Normen, Standards und Regelwerke sind völlig ausreichend, um ein angemessenes Niveau für Informationssicherheit in allen Unternehmen der Lebensmittelbranche zu etablieren (Beispiele hierfür: BDSG, GmbHG, AktG, HGB, KonTraG, TKG, PCI-DSS etc.). So besteht eine Meldepflicht für Datenschutzvorfälle beispielsweise bereits heute.

- Mit Blick auf und in Anpassung an aktuelle Bedrohungen heben die Handelsunternehmen schon heute ihre jeweiligen IT-Sicherheitsniveaus kontinuierlich an. Dies geschieht in Eigenverantwortung und aus Eigeninteresse eines jeden Unternehmens und ist in der notwendigen Dynamik mit gesetzlichen Regelungen nicht geeignet abbildbar.

- Die Unternehmen können ihre IT jedoch nur gegen elementare, einfache Angriffe absichern (Stichwort: Hackerkids). Dies machen die Handelsunternehmen bereits seit vielen Jahren. Gegen Angriffe staatlicher oder terroristischer/krimineller Organisationen haben die Unternehmen kaum Möglichkeiten.

  Dazu das folgende Zitat von Dr. Sandro Gayken (Institute of Computer Science, AG Secure Identity, Freie Universität Berlin) in einer schriftlichen Stellungnahme vom Mai 2014 für den Deutschen Bundestag:

  Sicherheit ist relativ. Eine sichere Kommunikation gegen schwache Angreifer (Kleinkriminelle, Aktivisten) ist mit bestehenden Techniken unter akzeptablen Kollateralschäden möglich, sofern diese Techniken dem Stand der Technik entsprechen, agil, effektiv und effizient sind und korrekt implementiert und bedient werden.

  Eine sichere Kommunikation gegen starke Angreifer (organisierte Kriminelle, Nachrichtendienste, Militärs) ist gegenwärtig nicht möglich. Das „normale" Modell der Rechnersicherheit ist diesen Angreifern gegenüber konzeptionell überfordert und überholt. Dieses normale Modell hat sich aus Grundannahmen zur Computersicherheit der Sechziger bis Achtziger Jahre herausgebildet. (…)

  Die vollständige Stellungnahme ist als **Anlage** beigefügt.

- Anmerken möchten wir zudem, dass die Handelsunternehmen eine Meldepflicht an das BSI als nicht zielführend einschätzen. Äußerst kritisch vom Handel gesehen bis ablehnend eingeschätzt wird zudem, ihre IT-Sicherheit mit den genannten Einschränkungen von heute von diesbezüglich derzeit nur bedingt kompetenten Stellen und Einrichtungen (BSI, TÜV o. ä.) testieren zu lassen. Derartig vorgesehene Testierungen werden handelsseitig als Fehlleitung von Ressourcen eingestuft, die die IT-Sicherheit nicht erhöhen werden.

- Hingegen würde eine Stärkung des BSI hinsichtlich Personal und Etats handelsseitig ausdrücklich unterstützt. Dies könnte und sollte jedoch ganz unabhängig von einem IT-Sicherheitsgesetz durchgeführt werden. Damit sollte die aktive Information des BSI und ggf. anderer staatlicher Stellen über konkrete, bekannte Bedrohungen gestärkt werden, die dann schneller und umfassender erfolgen könnte, um den Unternehmen verbesserte Möglichkeiten der Reaktion geben zu können.

Unverhältnismäßige Kostenbelastung durch fragwürdige neue Verpflichtungen

Derzeit lässt sich nicht einschätzen, welche konkrete Kostenbelastung auf den Handel zukommen würde. Es ist nicht bekannt, welche Einrichtungen, Betriebe oder Betriebsteile des Lebensmittelhandels in welchen Regionen einbezogen werden sollen. Jedoch wird bereits in diesem Entwurfsstadium deutlich, dass den Betreibern absehbar zusätzliche Kosten entstehen. Dies geht beispielsweise aus § 8a Abs. 3 BSIG-E hervor, der den Betreibern Nachweispflichten mit verpflichtenden

Sicherheitsaudits, Prüfungen oder Zertifizierungen auferlegt. Die im Vorwort des Gesetzentwurfs unter E.II (S. 4) enthaltene Aussage, Mehrkosten würden nur dort verursacht, „wo bislang noch kein hinreichendes Niveau an IT-Sicherheit bzw. keine entsprechenden Meldewege etabliert sind“, ist insoweit nicht plausibel. Es muss davon ausgegangen werden, dass für alle Betreiber Kritischer Infrastrukturen erhebliche Mehrkosten entstehen.

Meldepflichten zu weitreichend

Durch die Ersetzung der Worte „andere Stellen“ durch das Wort „Dritte“ in § 3 Abs. 1 Satz 2 Nr. 2 BSIG-E könnte im Zweifel eine Erweiterung des Kreises derjenigen ergeben, an die Informationen weitergegeben werden: „Andere Stellen“ konnte noch dahingehend einschränkend ausgelegt werden, dass staatliche Stellen Informationen erhalten. Dies erscheint bei dem Begriff „Dritte“ nicht mehr möglich. Die einzig verbleibende Anforderung, dass die Zurverfügungstellung der Information an den Dritten nur dann erfolgen darf, wenn dies zur Erfüllung seiner Aufgaben - welche Aufgaben, wird nicht gesagt - erforderlich ist, ermöglicht eine zu weitgehende Weitergabe von Informationen, die die Betreiber der Kritischen Infrastrukturen betreffen, an beliebige Dritte. Der Entwurf sollte an dieser Stelle konkretisiert und auf die Weitergabe an staatliche Stellen beschränkt werden.

Hiermit zusammenhängend: § 8c BSIG-E stellt für die Auskunft des BSI an Dritte auf die schutzwürdigen Interessen der Betreiber ab, ohne dass erkennbar wäre, wie das BSI diese schutzwürdigen Interessen erkennen soll. Eine Abstimmungspflicht mit den Betreibern erscheint mindestens dann geboten, wenn es sich bei den Dritten nicht um staatliche Stellen handelt.

Dass die Betreiber Kritischer Infrastrukturen gemäß § 8b Abs. 4 Beeinträchtigungen ihrer IT-Systeme, Komponenten oder Prozesse schon dann unverzüglich an das BSI melden müssen, wenn diese zu einem Ausfall oder einer Beeinträchtigung der „Kritischen Infrastrukturen führen können“, führt bereits bei einer sehr geringen Wahrscheinlichkeit der Betroffenheit zu einer Meldepflicht. Beispielsweise wäre bei einem beliebigen Virenbefall, dessen völlige Ungefährlichkeit noch nicht 100%ig abschließend feststeht, die sofortige Meldung erforderlich. Richtiger erscheint, hier erstens eine angemessenere Schwelle für das Maß der Wahrscheinlichkeit einzufügen und zweitens zusätzlich zu verlangen, dass mindestens eine schwerwiegende Beeinträchtigung der Kritischen Infrastruktur drohen muss.

Keine Vorratsdatenspeicherung durch die Hintertür

Der Handel wendet sich gegen eine verpflichtende Ausweitung der Speicherung von Nutzungsdaten. Dies kommt einer Einführung der Vorratsdatenspeicherung durch die Hintertür gleich. Zwar wird in Artikel 2 „Änderung des Telemediengesetzes“ (§ 15 Abs. 9 TMG neu) derzeit lediglich eine Option zur Speicherung von Nutzungsdaten gegeben. In der Auslegung und auch der weiteren Diskussion zum Entwurf besteht jedoch die Gefahr, dass eine „Quasi-Verpflichtung“ des Diensteanbieters zur Erhebung von Nutzerdaten besteht, will er den Anforderungen der Gefahrenabwehr genügen.

Handlungsbedarf: Energie und Telekomunikation

Flächendeckende Störungen der Energieversorgung und der Telekommunikation können hingegen dazu führen, dass auch der Lebensmittelhandel in seiner Versorgungsfunktion deutlich eingeschränkt wird. Insofern ist eine mittelbare Gefährdung des Handels durch die Abhängigkeit von Stromversorgung und Telekommunikation gegeben.

Werden jedoch Maßnahmen zum erweiterten Schutz der Stromversorgung und Telekommunikation ergriffen, ist auch diese mittelbare Gefährdungslage wirksam eingedämmt. Vor diesem Hintergrund begrüßt es der Handel, dass die Sektoren Energie und Telekommunikation im besonderen Fokus des vorgelegten Gesetzentwurfes im Hinblick auf die Prävention gegen Cyberattacken stehen.

Dieser besondere Fokus findet sich zudem im von der EU-Kommission (KOM) vorgelegten Richtlinienvorschlag vom Februar 2013 wieder, der Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union vorsieht. Auch in diesem Vorschlag befinden sich (siehe Anhang II) diverse adressierte Marktteilnehmer, wie Telekommunikationsdienste und Energieversorger. Jedoch ist der Ernährungssektor mit der Branche Lebensmittelhandel dort zu Recht nicht aufgeführt, da wohl auch die KOM erkannt hat, dass hier kein Handlungsbedarf besteht.

Auch im aktuellen Koalitionsvertrag der Bundesregierung „Deutschlands Zukunft gestalten“ ist die notwendige Schaffung eines IT-Sicherheitsgesetzes formuliert, ohne jedoch explizit den Sektor Ernährung mit der Branche Lebensmittelhandel zu adressieren.

Schlussbemerkung

Der Gesetzentwurf sieht zusätzliche IT-Sicherheitsmaßnahmen und Meldepflichten für den Lebensmittelhandel vor, die auf handelsseitige Ablehnung stoßen, da diese im Ergebnis unserer Analyse nicht zielführend und in ihren belastenden Auswirkungen als hochgradig unverhältnismäßig eingestuft werden müssen.

Vor diesem Hintergrund fordern BVLH und HDE mit Nachdruck die Bundesregierung auf, den Lebensmittelhandel vom Anwendungsbereich des Gesetzes vollständig auszunehmen. Zudem sollte zunächst die europäische Richtlinie abgewartet werden. Der deutsche Gesetzgeber sollte im Sinne einheitlicher Regelungen und zur Vermeidung von Wettbewerbsverzerrungen zulasten deutscher Unternehmen nicht über die europäischen Vorgaben hinausgehen.

BVLH/HDE, Berlin, 13. November 2014

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)299

STELLUNGNAHME

Berlin, 17. April 2015

Deutscher Industrie- und Handelskammertag

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

Die Bundesregierung hat dem Deutschen Bundestag den Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme zugeleitet. Mit dem geplanten IT-Sicherheitsgesetz sollen in erster Linie die Betreiber kritischer Infrastrukturen dazu verpflichtet werden, ihre IT-Systeme gegen Angriffe abzusichern. Darüber hinaus soll die Zusammenarbeit zwischen Sicherheitsbehörden und Betreibern kritischer Infrastrukturen verbessert werden. Die IHK-Organisation setzt sich intensiv für eine Verbesserung der Widerstandsfähigkeit der deutschen Wirtschaft gegenüber der Vielzahl von Bedrohungen im Cyberraum ein und nimmt die Gelegenheit wahr, zum o. g. Entwurf Stellung zu nehmen.

Dieses IT-Sicherheitsgesetz sollte – seinem ursprünglichen Anlass entsprechend – sich auf die volkswirtschaftlich wichtigen Infrastrukturen konzentrieren, d. h. die Betreiber kritischer Infrastrukturen im engeren Sinne adressieren und in diesem Bereich verlässliche Regelungen schaffen, die die IT-Sicherheit wirklich verbessern. Eine solche Fokussierung ist unserer Ansicht nach auch wichtig, um die Diskussion und die anschließende Umsetzung nicht zu überfrachten. Darüber hinaus gehende Maßnahmen – jenseits des Gesetzes – im Sinne einer Ende zu Ende-Sicherheit vom Hersteller bis zum Nutzer sollten in einem breiten Diskussionsprozess aller Beteiligten erarbeitet werden, der auch die genaue Rollen- und Aufgabenverteilung zwischen Staat, Wirtschaft und dem einzelnen Nutzer umfasst.

Das gesetzgeberische Ziel muss sich in der Umsetzung widerspiegeln. An einigen Stellen des Gesetzentwurfes bestehen jedoch Lücken (z. B. bei der Definition der Leistungen des BSI gegenüber den meldepflichtigen Unternehmen in Form von Service Level Agreements für Warnhinweise an Betreiber kritischer Infrastrukturen oder bei der Erstellung eines Lageberichts auf der Basis relativ weniger erwarteter Meldungen), an anderen Stellen wird dagegen über das Ziel hinausgeschossen (z. B. mit unverhältnismäßigen Verpflichtungen auch für kleine Webseitenbetreiber).

DIHK | Deutscher Industrie- und Handelskammertag e.V.
Registriernummer des DIHK im Register der Europäischen Kommission: 22400601191-42
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

Im Einzelnen:

Fokussierung auf kritische Infrastrukturen

In der Tat müssen die IT-Netze und -Systeme sicherer gemacht werden, denn die Zahl von Netzstörungen, Internetangriffen und sicherheitsrelevanten Zwischenfällen ist erheblich gestiegen. Dabei gehen wir davon aus, dass Unternehmen grundsätzlich für die Sicherheit ihrer Systeme selbst verantwortlich sind. Viele freiwillige Initiativen – auch der IHK-Organisation – setzen richtiger Weise hier an und stärken die Sensibilität dafür. Besonderes Augenmerk verlangt der Bereich der sog. kritischen Infrastrukturen, denn von Schäden in diesem Bereich geht immer zugleich auch ein Risiko für andere Unternehmen und das Gemeinwesen aus. Gesetzliche Verpflichtungen zu Sicherheitsmaßnahmen, so auch der vorliegende Gesetzentwurf, sollten sich auf diesen Bereich konzentrieren. Die Betreiber dieser Infrastrukturen haben eine besondere Verantwortung für die Funktionsfähigkeit unserer Volkswirtschaft. Insofern begrüßen wir das grundsätzliche Anliegen, mit dem IT-Sicherheitsgesetz die kritischen Infrastrukturen sicherer zu machen und den Austausch zu Sicherheitsvorfällen und die Reaktionsfähigkeit von Staat und Wirtschaft in diesem speziellen Bereich zu verbessern. Ziel des Gesetzes sollte unserer Ansicht nach sein, bei Betreibern kritischer Infrastrukturen ein Informations-Sicherheitsmanagementsystem einzuführen und den Austausch zu Sicherheitsvorfällen effektiv zu gestalten. Auf diesen Ansatz sollte sich die gesetzliche Regelung konzentrieren.

Im neuen Entwurf des § 7a BSIG-E fehlt jeglicher Bezug zu den Betreibern Kritischer Infrastrukturen – also dem wesentlichen Regelungsgegenstand des Gesetzes. Vielmehr wird das BSI hier mit einer Generalklausel artigen, anlassunabhängigen Marktbeobachtungsfunktion ausgestattet, die bisher nicht zu seinen Aufgaben gehört. Wir erwarten, dass Anlass, Ablauf, Zweckbestimmung, Grenzen und die Modalitäten zur Informationsweitergabe klar umrissen werden.

Um den Schutz wichtiger Einrichtungen des Gemeinwesens zu gewährleisten, ist es sinnvoll, IT-Sicherheitsstandards für kritische Infrastrukturen zu etablieren (§ 8a BSIG-E). Eine gesetzliche Grundlage bedeutet für die betroffenen Unternehmen auch Rechtssicherheit und damit die Chance, zukunftssicher zu planen.

Mehr Rechtssicherheit durch klarere Begriffsbestimmungen

Zu mehr Rechts- und Planungssicherheit würde eine klare Definition der zahlreichen unbestimmten Rechtsbegriffe beitragen. Wir sehen das Problem, dass dies insbesondere in einem Bereich, der sich durch schnelle technologische Veränderungen auszeichnet, nicht einfach zu operationalisieren

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Registriernummer des DIHK im Register der Europäischen Kommission: 22400601191-42
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

ist. Wir regen allerdings an, die unbestimmten Rechtsbegriffe auf das allernotwendigste Maß zu beschränken und erwarten zumindes bei den folgenden Begriffen Präzisierungen: die Definition kritische Infrastrukturen und eine Konkretisierung des Begriffs Versorgungsengpässe (§ 2 Absatz 10 BSIG-E), eine Definition der Meldeschwelle für Telekommunikationsunternehmen bei auftretenden beträchtlichen Sicherheitsverletzungen (§ 109 Absatz 5 TKG-E), eine Präzisierung des Begriffs Stand der Technik (§ 8a Absatz 1 Satz 2 BSIG-E) und bei der Definition einer erheblichen Störung.

Anwendungsbereich klar regeln

Die erste grobe Liste zu den möglicherweise betroffenen Unternehmen im Gesetzentwurf erschwert nicht nur eine Beurteilung der Angemessenheit der Verpflichtungen, sondern auch des Beitrags der Vorgaben zur Verbesserung der IT-Sicherheitslage. Die betreffende Rechtsverordnung zum Anwendungsbereich des Gesetzes sollte zeitnah, möglichst schon parallel zum Gesetzgebungsverfahren erarbeitet werden. Mit den dann verfügbaren Informationen würde die tatsächliche Betroffenheit im Vorfeld viel transparenter werden. Das könnte auch die Akzeptanz in der Wirtschaft verbessern.

Wir empfehlen, den Anwendungsbereich des Gesetzes möglichst restriktiv zu fassen. In einer digital vernetzten Volkswirtschaft kommt der Funktionsfähigkeit der zugrunde liegenden Infrastrukturen eine wesentliche Bedeutung zu. In der Rechtsverordnung muss genau dieser Bereich klar abgegrenzt werden. Dazu gehört auch eine Einbeziehung kritischer Bereiche des öffentlichen Sektors, die ebenfalls Infrastrukturcharakter haben. Die Nicht-Einbeziehung kritischer Infrastrukturen der öffentlichen Hand ist nicht nachvollziehbar.

Zweifel an Verhältnis von Aufwand und Nutzen der vorgesehenen Meldepflicht

Verständlicher Weise sind Unternehmen sehr zurückhaltend mit der Meldung erlittener Angriffe. Der DIHK hat im Oktober 2014 Unternehmen aus den in den Erläuterungen des Gesetzentwurfs genannten Branchen zur (in erster Linie freiwilligen) Zusammenarbeit mit Sicherheitsbehörden befragt. Ein Großteil dieser Unternehmen wäre demnach bereit, Sicherheitsvorfälle zu melden – unter bestimmten Voraussetzungen:

1. die absolute Vertraulichkeit der Information muss gewährleistet sein, die Meldungen müssen anonymisiert abgegeben werden können,
2. die Unternehmen erwarten einen Mehrwert von der Zusammenarbeit, z. B. als konkrete Warnhinweise,

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Registriernummer des DIHK im Register der Europäischen Kommission: 22400601191-42
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

3. wenn eine gesetzliche Meldepflicht eingeführt wird, muss verbindlich festgelegt sein, dass nur wirklich schwerwiegende Fälle gemeldet werden müssen und
4. der Aufwand für die Meldungen muss sich in Grenzen halten.

Vor diesem Hintergrund bitten wir, im weiteren Gesetzgebungsverfahren folgende Aspekte zu berücksichtigen:

Wir erkennen ausdrücklich an, dass der Entwurf eine unserer zentralen Forderungen aufgreift und zumindest pseudonymisierte Meldungen von Sicherheitsvorfällen vorsieht, die zu einem Ausfall oder einer Beeinträchtigung der Kritischen Infrastrukturen führen können. Das ist ein wichtiger Beitrag zur Steigerung der Akzeptanz des Gesetzentwurfes in der Wirtschaft. Richtig ist, dass für einfache und unkomplizierte Meldewege die bereits mit dem UP KRITIS etablierten Ansprechstellen genutzt werden können. Es gibt aber keinen sachlichen Grund, die Möglichkeit anonymer Meldungen nur einigen Adressaten des neuen Gesetzes einzuräumen. Wir schlagen stattdessen vor, die Frage der anonymen Meldemöglichkeit für alle Anbieter einheitlich zu regeln.

Ein wesentlicher Beitrag für eine funktionierende Zusammenarbeit zwischen Unternehmen und Behörden besteht darüber hinaus darin, eine Basis für den vertrauensvollen Austausch zu Sicherheitslücken und -schwachstellen herzustellen – diese wird von den Unternehmen grundsätzlich als wünschenswert erachtet. Ein sinnvoller Ansatz wäre, bestehende Initiativen – wie die Allianz für Cybersicherheit – auszubauen und stärker bei den Unternehmen bekannt zu machen. Die IHK-Organisation sieht sich hier auch selbst in der Pflicht.

Die gesetzlich vorgeschriebenen Meldungen führen zu erheblichen Aufwänden bei den Unternehmen – bei nicht einschätzbarem Nutzen. Diese müssten vor einer Meldung mögliche Konsequenzen für das Unternehmen prüfen. Börsennotierte Unternehmen müssen zudem überlegen, ob eine Meldung über einen IT-Sicherheitsvorfall börsenrelevant sein könnte. Dann wären sie verpflichtet, ihre Aktionäre zu warnen. Bis diese Fragen geklärt sind, dürfte es für eine Warnung anderer Unternehmen oft zu spät sein. Eventuell auftretende Haftungsfragen müssen geklärt werden (Abgleich mit Aktien- und Versicherungsrecht), wenn Unternehmen etwa dadurch geschädigt werden, dass z. B. Informationen zu einem Sicherheitsvorfall öffentlich werden, die sich schlimmstenfalls sogar im Nachhinein als falsch herausstellen.

Genauer definiert werden sollte in §§ 4 und 7 BSIG-E die Leistung, die vom BSI an die Unternehmen zurückgegeben wird. Diese ist – im Verhältnis zu den umfangreichen Verpflichtungen für die Betreiber kritischer Infrastrukturen – kaum umschrieben.

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Registriernummer des DIHK im Register der Europäischen Kommission: 22400601191-42
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

Pflichten für Telekommunikationsanbieter zu weitgehend

§ 109a Abs. 4 TKG führt neue Benachrichtigungspflichten für Telekommunikations-Diensteanbieter gegenüber Nutzern ein, wenn Störungen bekannt werden, die von dessen Datenverarbeitungssystemen ausgehen. Störungen entstehen aber in erster Linie in den vorgelagerten Systemen, z. B. beim Internetanbieter, Cloudanbieter oder auf Internetplattformen. Die Information der Nutzer sollte in erster Linie vom Störer selbst und nicht über Dritte (also Telekommunikations-Diensteanbieter) erfolgen. Die hier vorgesehene Vorgehensweise würde unter Umständen wertvolle Zeit kosten und birgt zudem das Risiko von (Übertragungs-)Fehlern bei der Information der Betroffenen.

Unabhängig davon ist die Pflicht zur Information nicht hinreichend konkret gefasst. Nach der Entwurfsfassung ist jedwede Art von Störung zu melden, unabhängig davon, wie viele Nutzer sie betrifft und welche Auswirkungen und Schäden sie zur Folge haben kann. Danach wäre bereits jede auf einen Nutzer beschränkte mit geringem Schadenpotenzial versehene Störung meldepflichtig. Die Regelung ist zu weit gefasst und die daraus folgenden Verpflichtungen in zahlreichen Anwendungsfällen nicht erforderlich und unangemessen.

Problematisch ist auch, dass TK-Diensteanbieter bei fehlerhaften oder verspäteten Informationen einem Haftungsrisiko ausgesetzt sind (§§ 44 und 44a TKG). Dies erscheint unbillig, weil Störungen häufig gerade nicht in eigenen Systemen und Anwendungen des informierenden TK-Dienste-anbieters auftreten. Hier bedarf es einer Haftungsfreistellung des benachrichtigenden TK-Dienste-anbieters, der nicht selbst Störer im Rechtssinne ist.

Künftige Rolle des BSI klarer definieren

Die Bundesregierung sollte sich auf Maßnahmen konzentrieren, die den Unternehmen wirklich helfen. In einer ‚Wirtschaft 4.0' kommt der Sicherheit informationstechnischer Systeme eine essentielle Bedeutung für die Funktions- und Wettbewerbsfähigkeit der Unternehmen zu. Vor diesem Hintergrund begrüßen wir die vorgesehene Stärkung des BSI als zentrale Behörde zur Bündelung und Auswertung von Informationen zur Cybersicherheit in Deutschland. Dies zeigt, dass die Bundesregierung sich ihrer Verantwortung insbes. beim Schutz kritischer Infrastrukturen bewusst ist.

Wesentlich aus unserer Sicht sind:

- ein vertrauensvoller Informations- und Erfahrungsaustausch zwischen BSI und Unternehmen/Branchenverbänden/CERTs etc., insbesondere bei schwerwiegenden Sicherheitsvorfällen,

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Registriernummer des DIHK im Register der Europäischen Kommission: 22400601191-42
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

- ein einheitliches Bewertungsschema für Sicherheitsvorfälle (Kritikalität, Impact etc.),
- die Definition abgestimmter Reaktionsprozesse von Unternehmen und Behörden bei übergreifenden Sicherheitsvorfällen sowie
- eine aktuelle, transparente und aussagekräftige Beschreibung der aktuellen Sicherheits- bzw. Bedrohungslage.

Die künftige Rolle des BSI und das Zusammenspiel mit den Unternehmen sollten in einem Diskussionsprozess von Staat und Wirtschaft gemeinsam definiert werden. Ein gemeinsames Verständnis über die Rollenverteilung und das konkrete Zusammenspiel von Unternehmen und BSI ist wesentliche Grundlage für die Bereitschaft der Unternehmen zur Zusammenarbeit mit dem BSI.

Nach Implementierung des Gesetzes branchenspezifische Ansatz organisatorisch und prozessual weiter ausdifferenziert werden – insbesondere in Bezug auf das Zusammenspiel zwischen Unternehmen, Verbänden und dem BSI. Unserem Verständnis nach sollten operative Tätigkeiten bei der Prävention und der Schadensbeseitigung von den Unternehmen selbst erbracht werden. Deutsche IT-Sicherheitsanbieter verfügen über entsprechende Kompetenzen und eine ausreichende Anzahl von Experten. Der Austausch zu Sicherheitsvorfällen kann innerhalb von Branchen über Verbandsstrukturen schnell und effektiv organisiert werden. Die Verbände sollten in engem Austausch mit dem BSI stehen, das als Vernetzungsstelle agiert, die Meldungen über die Branchenverbände empfängt, die Betroffenheit weiterer Branchen prüft und diese informiert. Das BSI könnte darüber hinaus Methoden zur Überprüfung der IT-Sicherheit technischer Systeme, Komponenten und Prozesse zur Verfügung stellen, ein Gesamtlagebild erstellen und Warnhinweise in die Fläche bringen.

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.

Keine unangemessenen Verpflichtungen für Webseitenbetreiber

Vor dem Hintergrund, dass sich die gesetzlichen Vorgaben auf den Bereich der kritischen Infrastrukturen konzentrieren sollten, fordern wir den Deutschen Bundestag auf, die geplante Änderung des Telemediengesetzes aus dem Gesetzentwurf zu streichen. Wir erkennen an, dass eine Verbesserung der IT-Sicherheit in diesem Bereich erstrebenswert ist, allerdings passen die Vorgaben für Anbieter von Telemediendiensten nicht in die Gesetzessystematik und schießen

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Registriernummer des DIHK im Register der Europäischen Kommission: 22400601191-42
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

darüber hinaus weit über das Ziel hinaus – sowohl was den Adressatenkreis betrifft (schon jeder kleine Verein oder eine Privatperson, die Werbebanner auf der Webseite hat), als auch in Bezug auf die Reichweite der Verpflichtung: Anbieter von Telemediendiensten sollen verpflichtet werden „sicherzustellen, dass kein unerlaubter Zugriff auf ihre Telekommunikations- und Datenverarbeitungssysteme möglich ist“. Eine solche umfassende Sicherheitsgarantie ist kaum zu erfüllen und unverhältnismäßig. Hinzu kommt, dass die unangemessene Verpflichtung auch noch mit einer Bußgeldandrohung versehen ist. Wir gehen davon aus, dass dies nicht im Sinne des Gesetzgebers sein kann.

Grundsätzlich stellt sich die Frage, ob mit der „Update-Pflicht“ für Webseiten überhaupt eine relevante Schutzwirkung für die Allgemeinheit erzeugt werden kann. Infizierte Webseiten sind lediglich ein Teilbereich einer längeren Kette von potenziellen Software-Schwachstellen. Ihre tatsächlich schädigende Wirkung hängt von weiteren Faktoren ab. Zu einem Großteil erfolgt die Infektion von Rechnern durch mangelnde Software-Aktualität beim Nutzer und nur zum Teil durch deutsche Telemediendienste. Schließlich stellt sich die Frage, ob nicht die Mehrzahl der infizierten Webseiten von ausländischen Servern abgerufen und damit nicht von der Verpflichtung nach dem TMG erfasst wird.

Kein nationaler Alleingang

Notwendig ist ein abgestimmtes Vorgehen zwischen nationaler Gesetzgebung und der europäischen Legislativinitiative zur Netz- und Informationssicherheit (NIS-Richtlinie) – insbesondere im Hinblick auf Zielsetzung und Anwendungsbereich. Es darf nicht zu Wettbewerbsverzerrungen aufgrund unterschiedlicher nationaler Regelungen in der EU kommen, die – wenn sie erst einmal eingeführt sind – schwer wieder auf ein einheitliches Niveau gebracht werden können.

Überprüfung der Zielerreichung des Gesetzes richtig

Wir begrüßen ausdrücklich die vorgesehene Evaluierung nach Inkrafttreten der Rechtsverordnung, insbesondere im Hinblick auf die Erfassung der relevanten Branchen/Unternehmen und im Hinblick auf die Effizienz der Meldepflicht.

Übergangsfristen angemessen gestalten

Die vorgesehenen 2 Jahre Übergangsfrist zur Umsetzung der geforderten Mindeststandards nach Inkrafttreten des Gesetzes sind viel zu kurz. Die potenziell betroffenen Unternehmen rechnen damit,

dass der größte Teil dieses Zeitraums für die Ausgestaltung der jeweiligen branchenspezifischen Mindeststandards und die Zulassung durch das BSI erforderlich ist. Damit bleibt den Unternehmen zu wenig Zeit für eine angemessene Umsetzung. Wir empfehlen daher eine Verlängerung der Übergangsfrist. Diese sollte erst dann beginnen, wenn die Mindeststandards festgelegt und vom BSI freigegeben sind. Gleiches gilt für die vorgesehene Frist von 2 Jahren zur ersten Erfüllung der geforderten Nachweispflichten.

Ansprechpartnerin im DIHK:
Dr. Katrin Sobania, Tel. 030 20308-2109, sobania.katrin@dihk.de

Cyber-Sicherheitsrat Deutschland e.V.

CSRD e.V. – Georgenstraße 22 – 10117 Berlin

Deutscher Bundestag
Wolfgang Bosbach, MdB
Vorsitzender des Innenausschusses
Platz der Republik 1

11011 Berlin

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)300

Berlin, 20. April 2015

Sehr geehrter Herr Bosbach,

Lieber Herr Bosbach,

im Anhang zu diesem Schreiben erhalten Sie unsere Stellungnahme zum geplanten IT-Sicherheitsgesetz. Dies umfasst unsere Kommentierung des Entwurfs aus Dezember 2014 sowie die Kurzfassung der von uns in Auftrag gegebenen und von dem renommierten Verfassungsrechts-Experten Christoph Ahlhaus erstellte, verfassungsrechtliche Gutachten.

Ich würde mich freuen, wenn dies in Ihren Entscheidungen Berücksichtigung findet. Gerne stehe ich auch für ein Gespräch zur Verfügung.

Mit freundlichen Grüßen

Arne Schönbohm

Stellungnahme

zum Referentenentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 19.11.2014

08.12.14
Seite 1

Der Cyber-Sicherheitsrat Deutschland e.V. (CSRD) vertritt mit seinen Mitgliedern knapp zwei Millionen Arbeitnehmer sowie zahlreiche Bundesländer und verschiedene Institutionen. Hierzu zählen große und mittelständische Unternehmen, Betreiber kritischer Infrastrukturen sowie Experten und politische Entscheider mit Bezug zum Thema Cyber-Sicherheit. Der in Berlin ansässige Verein ist politisch neutral und hat zum Zweck Unternehmen, Behörden und politische Entscheidungsträger im Bereich Cyber-Sicherheit zu beraten und im Kampf gegen die Cyber-Kriminalität zu stärken.

Das Bundesministerium des Innern hat am 5. März 2013 einen Referentenentwurf für ein Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vorgelegt und die Verbände aufgefordert, hierzu Stellung zu nehmen. Der CSRD ist dieser Aufforderung in seinem Positionspapier vom 8. März 2013 nachgekommen. Am 18. August 2014 hat das Bundesministerium einen zweiten Referentenentwurf veröffentlicht. Diesen Entwurf hat der CSRD am 24. September 2014 kommentiert. Der dritte Entwurf folgte am 04. November 2014 und wurde ebenfalls kommentiert, obwohl der Entwurf noch nicht innerhalb der Bundesregierung abgestimmt wurde. Vorliegend nimmt der CSRD Stellung zum endgültigen Entwurf vom 19. November 2014.

Zusammenfassung

- Das Gesetz betrifft KRITIS Unternehmen ab 10 Mitarbeitern und einem Jahresumsatz von mehr als 2 Mio. Euro Der damit geschaffene Aufwand ist unverhältnismäßig im Vergleich zur Bedeutung dieser Unternehmen für Wirtschaft und Gesellschaft.
- Nach heftiger Kritik soll nun die IT-Sicherheit der Bundesverwaltung ausgebaut werden. Die Anforderungen sollen jedoch weit unter denen für Unternehmen bleiben. Damit ist ersichtlich, dass der Bund das Gesetz für nicht praktikabel erachtet.
- Die reine Verbreitung von Informationen genügt nicht. Das BSI sollte vielmehr verpflichtet werden, bei Abwehr von Angriffen Beistand zu leisten.
- Die verursachende Industrie (Soft- und Hardwarehersteller) ist nach wie vor nicht Adressat des Gesetzes.
- Der geplante Erfüllungsaufwand entspricht im Wesentlichen dem Entwurf vom 18. August 2014 und ist zu knapp bemessen. Die vorgesehenen Mittel, in Höhe von 0,5 % des Haushalts des BMI, stehen in keinem Verhältnis zu den hohen Schäden durch Cyber-Kriminalität.

Stellungnahme

zum Referentenentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 19.11.2014

1. Branchenspezifische Mindestanforderungen an die IT-Sicherheit – Der CSRD begrüßt die Einführung branchenspezifischer Mindeststandards an die IT-Sicherheit (sog. „Stand der Technik“). Jedoch ist der Anwendungsbereich des Gesetzes überzogen und unverhältnismäßig. Da das Gesetz seine Anwendung unabhängig von der Organisationsform des Betreibers Kritischer Infrastrukturen finden soll, sehen sich auch Kleinunternehmen mit mehr als 10 Mitarbeitern und einem Jahresumsatz von mehr als 2 Mio. Euro (gemäß Empfehlung 2003/361/EG der Kommission) einem enormen und nicht praktikablen Aufwand gegenüber. Dieser Aufwand überwiegt bei weitem die Bedeutung solcher Unternehmen für die Funktionsfähigkeit der Wirtschaft und Gesellschaft.
Kritisch ist auch die vorgeschlagene Umsetzungsfrist von zwei Jahren (§ 8a Abs. 1 BSI-Gesetz). Zwar ist der CSRD grundsätzlich der Ansicht, dass der Schutz von KRITIS schnell vorangetrieben werden muss. Jedoch ist zu berücksichtigen, dass die Entwicklung industrieller Standards auch bei größtem Einsatz der Industrie einen hohen zeitlichen Aufwand erfordert. Dies betrifft insbesondere Unternehmen, deren Standardisierungsmaßahmen auf internationaler Ebene abgestimmt werden müssen. Die Umsetzungszeit ist daher zu verlängern. Die Tatsache, dass der Begriff „Stand der Technik“ auch weiterhin gemeinsam durch BSI, KRITIS-Unternehmen und ihre Branchenverbände definiert werden soll, ist positiv. Jedoch bleibt weiterhin kritisch, dass das BSI abschließend über die Geeignetheit branchenspezifischer Standards als „Stand der Technik“ entscheiden kann (§ 8a Abs. 2 BSI-Gesetz). Um Doppelanforderungen und unnötige Bürokratie zu verhindern, schlägt der CSRD vor, die Geeignetheit international anerkannter Standards gesetzlich zu vermuten. Darüber hinaus sollte eine vom Bund unabhängige Schiedsstelle eingerichtet werden, damit Unstimmigkeiten schnell behoben werden können. Schließlich muss sichergestellt werden, dass die Entwicklung und Verifizierung von Standards nicht aufgrund personeller Fehlplanungen durch das BSI gehemmt wird.

2. Kein Konzept für die IT-Sicherheit staatlicher Einrichtungen – In der Kommentierung zum letzten Gesetzesentwurf wurde außerordentlich negativ bewertet, dass das BSI Gesetz keine Regelungen in Bezug auf IT-Systeme des Staates enthält. Diese bilden jedoch wesentliche Faktoren gesellschaftlichen und wirtschaftlichen Zusammenlebens. Diese Kritik wurde nun zum Teil berücksichtigt. Der neue Gesetzesentwurf sieht vor, dass die Sicherheit der IT der Bundesverwaltung ausgebaut werden soll. Umgesetzt wird dies durch die Wiedereinführung des § 8a BSI Gesetz. Im Detail wird jedoch deutlich, dass

Stellungnahme

zum Referentenentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 19.11.2014

das BMI von den Unternehmen mehr fordert, als der Bund bereit ist zu leisten. KRITIS Unternehmen sollen z.B. IT-Mindeststandards einhalten, diese alle zwei Jahre nachweisen und Störungen an das BSI melden. Bundesbehörden hingegen sollen lediglich die vom BSI festgelegten Standards einhalten. Eine Nachweispflicht oder Meldepflicht besteht nicht. Das BSI ist nicht einmal verpflichtet, die Einhaltung zu überprüfen („kann"). Der CSRD fordert, dass der Bund die Bedeutung seiner IT-Infrastruktur angemessen bewertet und konsequenterweise dieselben Sicherheitsanforderungen stellt, wie an private Unternehmen. Nur so kann von einem konsistenten IT-Sicherheitskonzept gesprochen werden. Erforderlich ist weiterhin, dass das BSI mit den nötigen Stellen ausgestattet wird, um diese Aufgaben auch umsetzen zu können. Was die IT-Sicherheitsstruktur der Länder betrifft, die mangels Gesetzgebungskompetenz des Bundes nie Regelungsgegenstand der Entwürfe war, sollten die Länder schnellstmöglich in Absprache mit dem Bund, eine IT-Sicherheitsstrategie erschaffen.

3. Zusammenarbeit zwischen KRITIS und BSI – Der endgültige Entwurf sieht eine „unverzügliche Meldung" des BSI gegenüber den Betreibern kritischer Infrastrukturen vor (§ 8b Abs. 2 BSI-Gesetz). Leistungspflichten und Leistungsfähigkeit des BSI sollten noch weiter ausgebaut und benannt werden. Es genügt nicht, wenn Betreiber kritischer Infrastrukturen über Störungen informiert werden bzw. das BSI über bekannte Abwehrmöglichkeiten informiert. Es sollte vielmehr verpflichtet werden, bei Abwehr von Angriffen Beistand zu leisten. In der Praxis könnte dies durch eine „schnelle Eingreiftruppe" umgesetzt werden, die im Falle erheblicher Angriffe, den betroffenen Unternehmen unverzüglich Hilfe leistet, um die Sicherheit der KRITIS zu gewährleisten. Schließlich ist eine Veränderung des Berichtswesens und die Wiedereinführung eines Quartalsberichts erforderlich.

4. Meldepflicht bei Sicherheitsvorfällen – Die geplante Meldepflicht soll nach dem neuen Entwurf eintreten, wenn eine „erhebliche Störung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit" eintritt. Damit ändert das BMI erneut den Wortlaut des geplanten Gesetzes (§ 8b Abs. 4 BSI-Gesetz). Erheblich sollen Störungen sein, wenn durch sie die Funktionsfähigkeit der erbrachten kritischen Dienstleistung bedroht ist. Nach der Begründung (S. 53) sei dies gegeben, wenn die Störung nicht automatisch behoben werden kann bzw. wenn es sich um einen neuartigen oder einzigartigen IT-Vorfall handelt. Tagtäglich vorkommende Ereignisse (z.B. Spam, allgemeine Viren, etc.) sollen nicht erheblich sein.

Stellungnahme

zum Referentenentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 19.11.2014

5. Berücksichtigung Europäischer Vorgaben – Eine umfassende Strategie für Cyber-Sicherheit setzt voraus, dass der gesamte Bereich der IT-Infrastruktur vor Beeinträchtigungen geschützt wird. Vor diesem Hintergrund ist es inkonsequent, dass KRITIS Unternehmen besonders hohe Sicherheitsstandards erfüllen müssen, während an Hard- und Softwarehersteller keine speziellen Anforderungen gestellt werden. Insbesondere mit der *„Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union“* (2013/0027(COD)), hätte die Europäische Union einen Beitrag zur Cyber-Sicherheit leisten können. Jedoch wurde im Ergebnis, auch aufgrund deutscher Bemühungen, der Abänderungsvorschlag Nr. 25 angenommen. Danach sollen Hard- und Softwarehersteller aus dem Anwendungsbereich der Richtlinie rausgenommen werden. Sie trifft folglich keine Verpflichtung zur Gewährleistung der Sicherheit und keine Meldepflicht, obwohl sie einen wesentlichen Faktor für die Cyber-Sicherheit in Europa bilden. Der CSRD sieht in dieser Regelung einen wesentlichen Widerspruch zu der geplanten umfassenden Strategie für Cyber-Sicherheit. Erforderlich sind vielmehr neben bereits bestehenden Regelungen zur Produkthaftung, detaillierte Regelungen zum Umgang mit Sicherheitslücken in Hard- und Software. Eine proaktive Strategie muss darauf bestehen, dass die Hersteller von Hard- und Software zum einen verpflichtet werden, Sicherheitsprobleme zu melden und zum anderen diese innerhalb vorgegebener Zeiträume beheben müssen.

6. Zum Erfüllungsaufwand – Der CSRD hat in seiner letzten Stellungnahme kritisiert, dass der Erfüllungsaufwand nicht konkretisiert wurde. Das BMI, hat auf diese Kritik reagiert und nimmt nun den Erfüllungsaufwand an, den es bereits in seinem Entwurf vom 18. August 2014 angenommen hat. Vom Gesamthaushalt des BMI (5,9 Milliarden Euro) werden lediglich 80 Millionen Euro für die Ausstattung seiner zentralen Einrichtung zum Kampf gegen Cyber-Kriminalität also dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zugewiesen. Nach dem Entwurf sollen diese Mittel um 14 Millionen Euro erhöht werden. Damit belaufen sich die Mehrausgaben für den Bereich der Cyber-Sicherheit auf weniger als 0,5 % vom Gesamthaushalt des BSI. Die veranschlagten Mehrausgaben sind willkürlich und beruhen auf Fehlkalkulationen. Dies wird an den geplanten Personalausgaben deutlich. Der Entwurf sieht für das BSI einen Personalaufwand von 67.000 Euro pro Mitarbeiter/Jahr vor. Das durchschnittliche Bruttogehalt einer IT-Fachkraft mit Berufserfahrung liegt jedoch bereits bei

durchschnittlich 75.000 € pro Jahr. Damit wird das BSI nicht in der Lage sein, qualifizierte IT-Fachkräfte zu werben. Der Cyber-Sicherheitsrat fordert die Bundesregierung daher mit Nachdruck dazu auf, die bisherige Strategie zu überarbeiten, um die gesetzten Ziele auch tatsächlich umsetzen zu können. Hierzu gehört zum einen die Aufstockung des BSI mit personellen und sachlichen Mitteln und zum anderen der Abbau von Doppelzuständigkeiten und Bürokratie, die bereits in der Vergangenheit zu einem Scheitern nationaler Einrichtungen, wie dem „Cyber-Abwehrzentrum“ geführt haben.[1] Falls keine zusätzlichen Mittel zur Umsetzung des Gesetzes zur Verfügung gestellt werden, wird sich die bisherige Leistungserbringung des BSI weiter verschlechtern. Das Fehlen konkreter Leistungskennzahlen führt weiterhin dazu, dass der Erfolg bzw. Erfüllungsgrad der Maßnahmen nicht bewertbar ist. Bei einer Umsetzung des derzeitigen Gesetzesentwurfes ist daher vor allem mit der Schaffung eines „Bürokratiemonsters“ zu rechnen, nicht aber mit konkreten Maßnahmen zur Erhöhung der Sicherheit.

7. Weitere Vorschläge zur Erhöhung der IT-Sicherheit – Erklärtes Ziel des Gesetzgebers ist eine signifikante Verbesserung der IT-Sicherheitsinfrastruktur. Daher ist auch positiv zu bewerten, dass die Zuständigkeit des BKA ausgeweitet werden soll. Nach dem endgültigen Entwurf soll das BKA die polizeilichen Aufgaben der Strafverfolgung wahrnehmen soweit es sich um eine Delikt aus § 202a StGB (Ausspähen von Daten), § 202b StGB (Abfangen von Daten), § 202c StGB (Vorbereiten von Ausspähen und Abfangen von Daten), § 263a StGB (Computerbetrug) und § 303a StGB (Computersabotage) handelt und der Angriff gegen Bundeseinrichtungen gerichtet ist. Hierdurch werden unklare Zuständigkeiten vermieden. Jedoch ist zu beachten, dass die vorgeschlagenen Maßnahmen nur gegen äußere Angriffe gerichtet sind. Umso wichtiger ist eine Diskussion über Maßnahmen, mit denen Betreiber kritischer Infrastrukturen auch vor internen Angriffen geschützt werden können. Im Bereich der Luftsicherheit hat der Gesetzgeber bereits Regelungen geschaffen, mit denen Personen, die Zugang zu besonders sensiblen Sicherheitsbereichen haben, auf ihre Zuverlässigkeit hin überprüft werden können. Derartige Zuverlässigkeitsüberprüfungen könnten ein erster Schritt sein, um die Gefahr interner Angriffe im Cyber-Sicherheitsbereich zu minimieren und gleichzeitig den Datenschutz einzuhalten.

[1] http://www.sueddeutsche.de/digital/behoerde-in-bonn-rechnungspruefer-halten-cyber-abwehrzentrum-fuer-nicht-gerechtfertigt-1.1989433

Verfassungsrechtliche Stellungnahme der Knauthe Rechtsanwälte Partnerschaft mbB im Auftrag des Cyber-Sicherheitsrat Deutschland e.V.

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

Executive Summary

1. Der Staat darf die Vorsorge für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen grundsätzlich auf die Betreiber verlagern. Grenzen einer solchen Übertragung von Staatsaufgaben sind aber dort gesetzt, wo dem Staat von Verfassung wegen ausnahmsweise die Erfüllungsverantwortung für die betreffende Aufgabe obliegt. Dies ist nach Art. 87a Abs. 1 S. 1 GG insbesondere für den Bereich der militärischen Landesverteidigung der Fall. Die den Betreibern Kritischer Infrastrukturen auferlegte Pflicht, organisatorische Vorkehrungen gegen Cyber-Zwischenfälle zu treffen, kann dazu führen, dass das betreffende Personal im Fall eines kriegerischen Cyberangriffs unmittelbar an Feindseligkeiten im Sinne des Kriegsvölkerrechts teilnimmt. Solche Tätigkeiten sind aber sowohl völkerrechtlich als auch verfassungsrechtlich den Angehörigen der Streitkräfte vorbehalten. Um die Verfassungsmäßigkeit von § 8a Abs. 1 BSIG-E bzw. § 11 Abs. 1b EnWG-E sicherzustellen, ist daher eine klarstellende Einschränkung des Gesetzeswortlautes erforderlich.

2. Mangels Gesetzgebungskompetenz des Bundes ist es verfassungsrechtlich nicht zu beanstanden, dass das IT-Sicherheitsgesetz (IT-SiG) die Behörden der Länder nicht in die Pflicht nimmt. Auf Grund des Gebots folgerichtiger Gesetzgebung ist es aber verfassungsrechtlich bedenklich, dass Bundesbehörden nicht von der gesetzlichen Definition Kritischer Infrastrukturen erfasst werden und auch im Übrigen keinen vergleichbaren Pflichten zum Schutz ihrer Informationstechnik unterliegen. Nach dem Gebot der Folgerichtigkeit muss sich der Gesetzgeber fragen, ob die betreffende

gesetzliche Regelung in einem inneren Widerspruch zu der Gesamtkonzeption des maßgeblichen Regelungssystems steht. Nach der gebotenen systematisch-teleologische Interpretation ist die Gesamtkonzeption des IT-Sicherheitsgesetzes vor allem darin zu sehen, den Schutz der infrastrukturellen Basis für das Funktionieren des Gemeinwesens zu gewährleisten. Diesem Ziel widerspricht es, wenn Bundesbehörden keinen vergleichbaren IT-Schutz gewährleisten müssen. Bundesbehörden sind zu einem großen Teil ebenso kritisch für das Funktionieren des Gemeinwesens, wie private Infrastrukturen und daher auch mit vergleichbaren Vorgaben hinsichtlich der Sicherheit ihrer Informationstechnik zu belegen.

3. Die fehlende Einbeziehung der Hersteller informationstechnischer Produkte und Systeme in die Sicherheitsvorsorge für die Informationstechnik in Kritischen Infrastrukturen dürfte gegen Art. 3 Abs. 1 GG verstoßen. Innerhalb der Vergleichsgruppe derjenigen Akteure, die mit Informationstechnik in Kritischen Infrastrukturen wesentlich in Berührung kommen, werden die Betreiber gegenüber den Herstellern dadurch benachteiligt, dass allein sie Sicherungspflichten treffen. Für diese Ungleichbehandlung besteht kein rechtfertigender Grund. Insbesondere sind die Betreiber nicht besser zur Gefahrenbeherrschung in der Lage, als die Hersteller der entsprechenden informationstechnischen Produkte und Systeme. Fehler in informationstechnischen Produkten und Systemen sind in der Regel die unmittelbare Ursache für Gefährdungen der Sicherheit in der Informationstechnik Kritischer Infrastrukturen. Von daher verfügen auch die entsprechenden Hersteller über die besten Gefahrenabwendungsmöglichkeiten und Kenntnisse über mögliche Gefahren für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen. Ihre Tätigkeit ist somit sachnäher als die der Betreiber und sie ist daher ebenfalls mit Pflichten im Hinblick auf die Sicherheit in der Informationstechnik Kritischer Infrastrukturen zu belegen, um einen Verstoß gegen Art. 3 Abs. 1 GG zu vermeiden.

4. Soweit die Vorgaben des IT-Sicherheitsgesetzes dazu führen, dass Betreiber Kritischer Infrastrukturen strengeren Vorgaben unterliegen, als sie bereits auf Grund internationaler Anforderungen unterliegen, so liegt darin im Falle von unzumutbaren Mehrkosten bei fehlendem finanziellen Ausgleich ein Verfassungsverstoß. Das Interesse an einem wirksamen Schutz der Informationstechnik in Kritischen Infrastrukturen ist wegen der weitreichenden gesellschaftlichen Folgen eines Ausfalls der betreffenden Dienstleistungen kein Gruppen-, sondern ein Allgemeininteresse.

Die Lasten solcher öffentlichen Angelegenheiten haben grundsätzlich die Allgemeinheit zu treffen und sind demnach im Wesentlichen durch die Gemeinlast Steuer zu finanzieren.

5. Es ist nicht verfassungsrechtlich geboten, dass alle Einrichtungen, Anlagen oder Teile, die Kritische Infrastrukturen sein sollen, bereits im Gesetz aufgezählt werden. Verfassungsrechtlich geboten ist aber eine nähere parlamentsgesetzliche Bestimmung des definitorischen Rahmens, in dem sich die Bestimmung durch den Verordnungsgeber vollziehen soll. Die vom Bundesverfassungsgericht entwickelte Wesentlichkeitstheorie und Art. 80 Abs. 1 S. 2 GG besagen, dass im Bereich der Normsetzung durch die Exekutive "wesentliche Entscheidungen" durch das Parlament selbst getroffen werden müssen. Je wesentlicher die übertragene Materie für den Gesetzgeber beziehungsweise je schwerwiegender/grundrechtsrelevanter die Auswirkungen für die Betroffenen sind, desto größer muss die Bestimmtheit der entsprechenden Norm sein. Wegen der erheblichen Auswirkungen auf Grundrechte der betroffenen Unternehmen, genügt es nicht, in § 2 Abs. 10 BSIG-E nur eine sektorenbezogene Bestimmung vorzunehmen. Vielmehr dürfte auch die Nennung konkreter Branchen und der in den jeweiligen Branchen als kritisch anzusehenden Dienstleistungen erforderlich und, etwa mittels Anlagen zum Gesetz, auch möglich sein.

6. Die Zuständigkeitserweiterung der Bundesnetzagentur durch das IT-Sicherheitsgesetz ist als solche verfassungsrechtlich unbedenklich. Bedenklich ist jedoch, dass die Betreiber von Energieversorgungsnetzen und die Betreiber von Energieanlagen für das Vorliegen des gesetzlich gebotenen "angemessenen Schutzes" den Sicherheitskatalog der Bundesnetzagentur zwingend einhalten müssen, während andere Betreiber Kritischer Infrastrukturen nicht an einen ähnlichen Katalog gebunden sind, sondern verschiedene Möglichkeiten haben, für einen angemessen Schutz ihrer Informationstechnik zu sorgen und dies nachzuweisen. Diese Ungleichbehandlung zwischen den verschiedenen Betreibern dürfte einen Verstoß gegen Art. 3 Abs. 1 GG darstellen. Eine gegenüber anderen Betreibern Kritischer Infrastrukturen womöglich herausgehobene Stellung der Betreiber von Energieanlagen bzw. Energieversorgungsnetzen vermag den Ausschluss der den Betreibern anderer Kritischer Infrastrukturen nach § 8a Abs. 2, 3 S. 2 BSIG-E offerierten Möglichkeiten nicht verfassungsrechtlich zu rechtfertigen.

7. Die nach dem IT-Sicherheitsgesetz vorgesehene Sicherungspflicht gegen Störungen der Informationstechnik in Kritischen Infrastrukturen und die Meldepflicht für erhebliche Störungen verstößt gegen verschiedene Grundrechte der Betreiber. Vor allem liegt ein unverhältnismäßiger Eingriff in die Berufsfreiheit der betroffenen Betreiber vor. Dies gilt allerdings nur für den vermögensbelastenden - weil kompensationslosen -, nicht aber für den verhaltensregelnden Eingriff in Gestalt der Pflichten als solchen. Als vermögensbelastender Eingriff sind die Sicherungs- und die Meldepflicht deshalb unverhältnismäßig, weil sie zu erheblichen Mehrkosten in Form von Personal- und Sachkosten führen, die auch angesichts der hohen Bedeutung der verfolgten Belange unzumutbar erscheinen und die Betreiber zudem gegenüber anderen privaten Dienstleistern für das öffentliche Wohl, die für ihre Tätigkeit eine Entschädigung erhalten, in verfassungsrechtlich nicht gerechtfertigter Weise benachteiligen. Hinsichtlich der Meldepflicht kommt vor allem ein Verstoß gegen das Recht auf informationelle Selbstbestimmung hinzu, der darauf zurückzuführen ist, dass der Gesetzesentwurf weder die Art der zu meldenden Vorfälle hinreichend bestimmt, noch den Zweck der Datenerhebung eindeutig genug kennzeichnet und somit nicht dem bei Eingriffen in das Recht auf informationelle Selbstbestimmung besonders bedeutsamen Gebot der Normenklarheit genügt.

VDV Die Verkehrsunternehmen

VDV Köln Kamekestraße 37–39 50672 Köln

Herrn
Wolfgang Bosbach, MdB
Vorsitzender des Innenausschusses
Deutscher Bundestag
Platz der Republik 1
11011 Berlin

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)301

Geschäftsführer Technik

Martin Schmitz

T 0221 57979-123
F 0221 57979-8123
E schmitz@vdv.de

20. April 2015

44. Sitzung des Innenausschusses zu TOP „Entwurf eines Gesetztes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)"

Sehr geehrter Herr Bosbach,

auf diesem Wege kontaktieren wir Sie anlässlich der anstehenden Ausschussberatungen zum IT-Sicherheitsgesetz und möchten diese Gelegenheit gerne nutzen, um Ihnen und Ihrem Büro eine kurze Stellungnahme mit der Bitte um Berücksichtigung zu übersenden.

Als Verband Deutscher Verkehrsunternehmen (VDV), in dem rund 600 Unternehmen des Öffentlichen Personenverkehrs und des Schienengüterverkehrs in Deutschland organisiert sind, begrüßen wir grundsätzlich die Initiative, Mindestanforderungen an die IT-Sicherheit festzuschreiben. Bei der Durchsicht des Gesetzentwurfes sind wir jedoch auch zur dem Ergebnis gekommen, dass die Vorlage unverhältnismäßige Anforderungen an die Unternehmen stellt.

So ist im Gesetzentwurf in Art. 1 Nr. 7 – § 8a Abs. 1 eine Übergangsfrist von nur zwei Jahren für die neuen gesetzlichen Anforderungen festgeschrieben worden, die unsere Mitgliedsunternehmen keinesfalls einhalten können. Denn erfahrungsgemäß nehmen Veränderungen und/oder Anpassungen zur Vermeidung von technischen Störungen dieser Art einen weitaus größeren Zeitraum in Anspruch. Wir bitten Sie vor diesem Hintergrund darum, die geplante Übergangsfrist von zwei Jahren zu streichen und darauf zu verweisen, dass eine Anpassung im Rahmen der nächsten maßgeblichen Systemerneuerung/-änderung zu erfolgen hat.

Ebenso bitten wir um eine kritische Prüfung des Art. 1 Nr. 7 - § 8a Abs. 3, der eine Pflicht zur wiederkehrenden Durchführung externer Audits und Zertifizierungen vorsieht. Wir schlagen stattdessen vor, bereits vorhandene bzw. bewährte interne

Verband Deutscher Verkehrsunternehmen e. V.

Hauptgeschäftsstelle
Kamekestraße 37–39
50672 Köln
T 0221 57979-0
F 0221 57979-8000

info@vdv.de
www.vdv.de

Sitz des Vereins ist Köln
AG Köln VR 4097

USt.-IdNr. DE 814379852

Vorstand
Präsident und Vizepräsidenten
Jürgen Fenske (Präsident)
Joachim Berends
Horst Klein
Herbert König
Prof. Knut Ringat
Ingo Wortmann

Hauptgeschäftsführer
Oliver Wolff

Haltestellen
Stadtbahn bis Friesenplatz,
Regionalzüge bis
Bahnhof Köln West

Prozesse und Sicherheitsanalysen anzuerkennen, die aus unserer Sicht angemessen sind, um das geforderte Sicherheitsniveau zu gewährleisten. Um die zusätzlichen administrativen Aufwendungen in Grenzen zu halten, schlagen wir vor, die Prüffristen auf die bisher vom BSI geforderten Audit-Fristen von drei Jahren (Zertifizierung nach ISO27001-Zertifikat auf der Basis von BSI-Grundschutz) anzupassen. Weiterhin sollte das Gesetz die Möglichkeit vorsehen, dass die Audits zeitgleich durchgeführt werden können.

Sehr geehrter Herr Bosbach, wir sind dankbar, wenn Sie unsere Anregungen im weiteren parlamentarischen Verfahren berücksichtigen könnten und stehen Ihnen und Ihrem Büro gerne und jederzeit für Rückfragen zur Verfügung.

Indem ich Ihnen bei den anstehenden Beratungen viel Erfolg wünsche, verbleibe ich

mit freundlichen Grüßen

Martin Schmitz
Geschäftsführer Technik

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)313

POSITION STATEMENT

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

Gesetzentwurf der Bundesregierung

Stellungnahme des Telecommunications, Internet, and Media (TIM) Committee der American Chamber of Commerce in Germany e.V.

5. Mai 2015

Hintergrund

Der Deutsche Bundestag beabsichtigt die Verabschiedung eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (sog. IT-Sicherheitsgesetz). Die in der Amerikanischen Handelskammer in Deutschland (AmCham Germany) vertretenen Unternehmen begrüßen grundsätzlich die Bemühungen von Politik und Verwaltung, ein für Deutschland hohes Niveau an IT-Sicherheit zu verwirklichen. So investieren die Mitglieder von AmCham Germany bereits seit Jahren große sachliche und personelle Ressourcen in die Erhöhung der Sicherheit ihrer Produkte und Dienste und befinden sich dazu auch in regelmäßigem Austausch mit Behörden in Deutschland, Europa und darüber hinaus. Zudem tragen zahlreiche namhafte Mitgliedsunternehmen heute schon für ein hohes Maß an Zuverlässigkeit, Sicherheit und Transparenz ihrer Produkte und Dienste bei und stellen damit eine verlässliche technologische Grundlage für das Funktionieren von Staat, Verwaltung und Wirtschaft in Deutschland und darüber hinaus dar.

Das auch aus Sicht von AmCham Germany grundsätzlich begrüßenswerte Ansinnen der Bundesregierung wäre mit Blick auf den beabsichtigten Gesetzeszwecke vorzugsweise in der gegenwärtig in Planung befindlichen europäischen Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit (sog. NIS-Richtlinie) am besten aufgehoben. Denn die IT-Sicherheit wie die IKT insgesamt macht bekanntlich an geografischen, nationalen Grenzen nicht halt. Wenn der Deutsche Bundestag allerdings im Vorgriff auf die NIS-Richtlinie national tätig werden will, dann bedarf der Kabinettsentwurf zum IT-Sicherheitsgesetz grundlegender Überarbeitung. In diesem Zusammenhang wird auch auf die Stellungnahme des Bundesrates vom 27.1.2015 verwiesen.

I. Executive Summary

1. Reichweite des Gesetzes klar festlegen:
Die Reichweite des IT-Sicherheitsgesetzes muss bereits im Gesetz selbst und nicht in einer nachgelagerten Rechtsverordnung bestimmt werden.

2. Klarer Fokus auf kritische Infrastrukturen:[1]
Um höchstmögliche Sicherheit zu gewährleisten, ist es von entscheidender Bedeutung, dass alle Betreiber kritischer Infrastrukturen, unabhängig davon ob sie sich in privater oder öffentlicher Hand befinden, von dem Gesetz erfasst werden.

3. Engere Definition eines meldepflichtigen Vorfalls:
Es muss hinreichend klar definiert sein, dass nur solche Vorfälle meldepflichtig sind, die reale Bedrohungen darstellen und/oder tatsächliche Schäden verursachen.

4. Standards müssen sich an internationalen Regelwerken orientieren:
Die sektorspezifischen Standards sollten sich eng an den anerkannten internationalen Standards und Best Practices anlehnen – sowohl bei der IT-Sicherheit wie auch beim Schutz der kritischen Infrastrukturen.

5. Keine Erweiterung der Meldepflichten für TK-Unternehmen:
Die Erweiterung des die Meldepflicht auslösenden Tatbestands auf sämtliche Beeinträchtigungen bei TK-Unternehmen verursacht unverhältnismäßigen Mehraufwand für alle Beteiligten und ist abzulehnen.

6. Sicherheitsauflagen in Telemedien müssen angemessen bleiben:
Benötigt wird eine deutlich eingeschränktere Mittel-Zweck-Relation sowie eine präzisere Definition der Sicherheitsauflagen für Telemedien.

7. Prüfkompetenzen des BSI müssen präzisiert werden:
Der Gesetzesentwurf muss in Hinblick auf Produkt-Bewertungen durch das BSI enger gefasst werden. Das Bewertungsverfahren des BSI für ICT-Produkte, -systeme und -dienstleistungen sollte dazu so transparent wie möglich sein.

8. Produktbewertungen durch das BSI müssen klar geregelt werden:
Aufgrund potentieller Gefahren für das geistige Eigentum und die Innovationsfähigkeit der Anbieter sollten Produkte und Dienstleistungen, die noch nicht auf dem Markt sind, von der Prüfung durch das BSI ausgenommen werden bzw. sollte die Prüfung nur auf freiwilliger Basis erfolgen.

9. Öffentliche Warnungen durch das BSI nach Rücksprache mit Herstellern: Öffentliche Warnungen des BSI müssen mit den IT-Anbietern besser koordiniert werden. Darüber hinaus werden klare Kriterien für diese Warnungen benötigt.

10. Cybersicherheitspolitik muss international harmonisiert werden:
Nationale Sonderwege führen nicht zu mehr IT-Sicherheit, erhöhen den Aufwand und die Kosten und senken die Wettbewerbsfähigkeit vor allem kleiner und mittlerer Anbieter von IT-Sicherheitslösungen. Insbesondere auf europäischer Ebene bedarf es einer Harmonisierung von nationaler Gesetzgebung mit der geplanten Direktive zur Netz- und Informationssicherheit (NIS) der EU Kommission.

---

[1] *Dissenting Vote der Deutschen Telekom AG zur AmCham Germany-Position:*
Die Deutsche Telekom AG vertritt die Position, dass für eine ganzheitliche Sicherheitsbetrachtung im Cyberraum auch Hard- und Softwarehersteller ebenso wie Internetunternehmen in den Anwendungsbereich des IT-Sicherheitsgesetzes einbezogen werden und Verantwortung übernehmen müssen.

II. Anmerkungen zum Entwurf des IT-Sicherheitsgesetzes

Um die IT-Sicherheit nachhaltig zu stärken, ist eine Zusammenarbeit des öffentlichen und privaten Sektors unerlässlich. Insgesamt muss zwischen der Regulierung "von oben nach unten" und den Ansätzen "von unten nach oben" eine Balance gefunden werden, die die schnelle Taktung und die Gesamtdynamik der Informationstechnologie sowie die konstanten Veränderungen in der jeweiligen Bedrohungslandschaft berücksichtigt. Vor diesem Hintergrund kommentiert AmCham Germany den Entwurf für ein IT-Sicherheitsgesetz wie folgt:

1. Klare Definition der Reichweite des Gesetzes in Bezug auf kritische Infrastrukturen

§8a und §8b führen erhebliche Verpflichtungen für Betreiber kritischer Infrastrukturen ein. In Übereinstimmung mit §10 soll die genaue Bestimmung der Infrastrukturen, die im Sinne des Gesetzes als kritisch gelten, in einem separaten Verfahren im Zuge einer Rechtsverordnung erfolgen. Dieses Verfahren soll sowohl qualitative wie auch quantitative Aspekte berücksichtigen. Was sehr wichtig ist: Es sollen Unternehmen angehört werden, die potentiell davon betroffen sind, sowie Industrieverbände und wissenschaftliche Kreise. Die mit diesem Verfahren in Zusammenhang stehenden Akten sollen der Öffentlichkeit nicht zugänglich gemacht werden.

Hierzu werden folgende Überlegungen angeregt:

a. **Erhöhte Transparenz hinsichtlich der Reichweite dieses Gesetzes. Die Reichweite des Gesetzes sollte direkt im Gesetz selbst und nicht nachgelagert in einer Rechtsverordnung festgelegt werden. Ein solches Vorgehen würde erheblich zu Transparenz und Rechtssicherheit beitragen.** Unsicherheit ist bei langfristiger Planung ein ernsthaftes Hindernis und damit sowohl im öffentlichen als auch im privaten Sektor schädlich. AmCham Germany bevorzugt daher eine eindeutige Festlegung bezüglich der Reichweite des geplanten IT-Sicherheitsgesetzes. Dabei gäbe es zwei Hauptwege, diese Reichweite festzulegen: 1) über eine definierte Liste von Funktionen in bestimmten Sektoren und Untersektoren, die geschützt werden müssen, oder 2) über die Erstellung einer klaren Liste von Kriterien und Schwellenwerten für Kritikalität, anhand derer festgestellt werden kann, ob ein bestimmter Betreiber unter das Gesetz fällt oder nicht. Derzeit enthalten die begleitenden Erklärungen des Gesetzesentwurfs einige Informationen zu qualitativen und quantitativen Aspekten, die bei der Festlegung derjenigen kritischen Infrastrukturen, welche unter das Gesetz fallen, berücksichtigt werden sollten. AmCham Germany regt an dieser Stelle an sicherzustellen, dass diese Kriterien weiter verdeutlicht und in den Gesetzestext selbst aufgenommen werden, anstatt sie in einer Rechtsverordnung im Rahmen eines weniger transparenten Verfahrens zu verarbeiten.

b. **Fokussierung des Gesetzes auf Bedrohungen am oberen Ende des Spektrums, da nicht jede von "kritischen Infrastruktur"-Sektoren erbrachte Dienstleistung gleich kritisch ist.** Zur Fokussierung rarer Sicherheitsressourcen im öffentlichen und privaten Sektor sollte sich das Gesetz auf den Schutz vor Bedrohungen am oberen Ende des Bedrohungsspektrums konzentrieren. Insbesondere sollten diejenigen Kerndienstleistungen von kritischen Infrastrukturen im Fokus stehen, die so lebensnotwendig sind, dass durch das Lahmlegen oder Zerstören dieser Infrastrukturen die

nationale Sicherheit, die wirtschaftliche Stabilität, die öffentliche Gesundheit oder Sicherheit oder eine Kombination dieser Faktoren geschwächt würde. Die weiteren Erklärungen zum Gesetzentwurf liefern eine ähnliche Liste "qualitativer" sowie quantitativer Kriterien. In der Begleiterklärung werden die qualitativen Kriterien als solche beschrieben, welche sich auf „die Sicherheit von Leib, Leben, Gesundheit und Eigentum der Teile der Bevölkerung beziehen, die von einem Ausfall unmittelbar oder mittelbar beeinträchtigt wären." Berücksichtigt man dies, so scheinen die vorgeschlagenen Unterkategorien der Betreiber von Datenverarbeitung und -speicherung mit diesen Kriterien nicht kongruent.

c. **Einbeziehung von kritischen öffentlichen Behörden und kritischen Infrastrukturen in öffentlicher Hand.** Wenn auf Grund der obenstehend beschriebenen Kriterien exakt eingeschätzt werden kann, ob eine Infrastruktur als kritisch gilt oder nicht, sollten diese Kriterien auch für Unternehmen in öffentlicher Hand/staatlich betriebene Unternehmen angewandt werden – die in diesem Gesetzesentwurf bisher ausgenommen sind. Die Eigentumsverhältnisse (öffentliches im Gegensatz zu privatem Eigentum) sind nach Ansicht von AmCham Germany kein Maßstab für die Kritikalität einer Dienstleistung. Das Herausnehmen öffentlicher Behörden und kritischer Infrastrukturen in öffentlichem Eigentum aus dem Geltungsbereich des Gesetzes würde ein unvollständiges Bild der kritischen Infrastrukturlandschaft in Deutschland zeichnen, und dadurch auch die Erstellung eines akkuraten Überblicks über die Situation verhindern (siehe unten).

d. **Öffentlich verfügbare (handelsübliche) IT-Produkte und -Dienstleistungen sind keine kritischen Infrastrukturen.** Es ist wichtig klarzustellen, dass in Szenarien, in denen Betreiber kritischer Infrastrukturen IT-Produkte und -Dienstleistungen verwenden um ihre eigenen Dienstleistungen erbringen zu können, es diese Betreiber sind, auf welche sich die Gesetzgebung beziehen sollte und nicht die Anbieter der zugrundeliegenden IT-Produkte. Die Betreiber kritischer Infrastrukturen sollten mit Hilfe von Verträgen und Service-Level-Agreements dafür sorgen, dass die Verpflichtungen, denen sie aufgrund der geplanten Gesetzgebung unterliegen würden, ordnungsgemäß an die IT-Anbieter weitergegeben werden. Im Rahmen der vorgesehenen Meldepflicht könnte dieser Ansatz beispielsweise dabei helfen, kritische von nicht kritischen Vorfällen zu trennen. Dies würde potentielle Mehrfachmeldungen vermeiden (zuerst vom Betreiber und dann zusätzlich Meldungen von IT-Anbietern, welche Vorfälle bei Betreibern kritischer Infrastrukturen zwangsläufig unvollständig und ohne Kontext melden müssten), den zielgerichteten Einsatz von Security-Ressourcen erlauben und durch Minimierung der administrativen Belastungen die beim BSI anfallenden Kosten reduzieren.

2. Erhöhte Transparenz bei Meldepflicht & Sicherheitsstandards

Zu den in §8a und §8b eingeführten Verpflichtungen gehören verschiedene Meldepflichten für Betreiber kritischer Infrastrukturen – die unter anderem mit der Absicht erlassen werden sollen, dass das BSI aktuelle Situationsanalysen / Bedrohungseinschätzungen erstellen und aufrecht erhalten kann. AmCham Germany begrüßt die Möglichkeit, dem BSI über zu diesem Zweck benannte branchenspezifische Kontaktpunkte (single point of contact - SPOC) anonym Ereignisse melden zu können, die ansonsten durch §8b Absatz 4 abgedeckt wären.

AmCham Germany regt hierzu folgende Überlegungen an:

a. **Grundlegend ist anzumerken, dass Vorfallsmeldungen kein Selbstzweck sein sollten, sondern ein Mittel, um ein bestimmtes Ziel zu erreichen.** Allgemein gesagt ist erfolgreiches Risikomanagement von einem effektiven Informationsaustausch abhängig, wozu Pflichtmeldungen im Falle signifikanter Sicherheitsverletzungen gehören können. Es hat sich jedoch in den letzten zehn Jahren deutlich gezeigt, dass ein verpflichtender Informationsaustausch zu „Cybersicherheits-Vorfällen" zwischen der Industrie und dem Staat nur zu begrenztem Erfolg geführt hat. Die wesentliche Lehre daraus ist, dass ein Informationsaustausch dann am besten funktioniert, wenn er durch ergebnisfokussierte Fragen so zielgerichtet und präzise wie möglich ist. Darüber hinaus müssen Informationen in beide Richtungen fließen. Bedrohungen und Risiken werden am besten abgemildert, wenn die *relevanten* Parteien (d.h. die Parteien, die Informationen in praktisch umsetzbare Ergebnisse verwandeln können) alle *relevanten* Informationen austauschen. Es geht nicht darum zu gewährleisten, dass *alle* Parteien *alle* Informationen erhalten. Ein solcher zielgerichteter Austausch trägt auch zum Schutz sensitiver Informationen bei (egal ob in öffentlicher oder privater Hand), unterstützt den gesamten Datenschutz und ermöglicht einen sensiblen Informationsaustausch.

b. **Engere Definition eines "meldepflichtigen" Vorfalls.** In den zusätzlichen Erklärungen für §8a und §8b wird versucht zu definieren, was ein "meldepflichtiger" Vorfall ist. Der vorgeschlagene Ansatz ist leider erheblich weiter gefasst als es aus Sicht eines effektiven Risikomanagements sinnvoll erscheint. Die vorgeschlagenen Definitionen, nach denen "jegliche Auswirkung auf die Technologie" einen "Vorfall" darstellt, kombiniert mit der Tatsache, dass eine "schwerwiegende" Auswirkung als "eine Bedrohung der Funktionsfähigkeit der Technologie" definiert wird, bedeutet im Wesentlichen, dass jegliche Unregelmäßigkeit bei der Nutzung dieser Technologie einen meldepflichtigen Vorfall darstellen könnte. Gleiches trifft auf die Ausweitung der Meldepflichten nach § 109 Abs. 5 TKG zu (siehe hierzu Absatz II.2. f). Eine Meldepflicht mit einem derart breiten Umfang erhöht die Verwirrung, die Kosten und stellt sogar ein potentielles Sicherheitsrisiko dar. Um die Ressourcen des BSI (und die Sicherheitsressourcen eines Betreibers kritischer Infrastrukturen) effektiv zu nutzen, empfiehlt AmCham Germany, diese Definitionen erneut zu überprüfen, sie ggf. präziser zu formulieren und sich auf reale Bedrohungen und/oder tatsächliche Schäden zu beschränken.

c. **Präzisierung der Bewertung und Einschätzung der von der Industrie erhaltenen Informationen.** Insbesondere mit Blick darauf, wie die aus der Meldepflicht generierten Daten analysiert werden, schlägt AmCham Germany mehr Transparenz vor. Eventuell existierende Pläne, Informationen an diejenigen Betreiber kritischer Infrastrukturen zurück zu geben, die unter das geplante Gesetz fallen, sollten ebenfalls transparent gemacht werden. Zusätzlich sollte im Gesetzentwurf präzisiert werden, wie dieser Rückfluss von Informationen an diejenige IT-Anbieter verlaufen kann, welche zwar nicht unter das Gesetz fallen, aber zur weiteren Verbesserung ihres Cyber-Ökosystems aus möglichen Sicherheitsvorfällen lernen wollen. Zwar gibt es diesbezüglich bereits einen auf bestehenden Verträgen beruhenden regen Austausch zwischen Mitgliedsunternehmen von AmCham Germany und dem BSI. Nichts desto trotz wäre es aber aufgrund des zu

erwartenden Meldeaufkommens wünschenswert zu klären wie weitere, aus der Meldepflicht gewonnene Informationen im Einklang mit Datenschutzbestimmungen an IT-Anbieter weitergegeben werden können. Zusätzlich wäre es nützlich klarzustellen, dass das BSI relevante Informationen, die es von Sicherheitsbehörden und/oder CERTs erhalten hat, an Betreiber kritischer Infrastrukturen weitergibt.

d. **BMI & BSI sollten sich in Hinblick auf Angriffstelemetrie mehr mit der Industrie austauschen und Methoden finden, um solche Informationen in effizienter Weise weiterzugeben.** Trotz höherem Datenaufkommen bilden die Informationen, die vermutlich aus der in diesem Gesetz enthaltenen Meldepflicht gewonnen werden können, die Realität nur unzureichend ab. Es müssen voraussichtlich weitere Kanäle für eine verstärkte Zusammenarbeit mit der Industrie in Betracht gezogen werden, um das Ziel zu erreichen "umfassende Informationen zu allen Akteuren und der derzeitigen Situation der Cyberbedrohung" zu sammeln. Eine solche Zusammenarbeit könnte nach Ansicht von AmCham Germany am besten durch das Stärken bestehender vertrauenswürdiger Kanäle zwischen den unterschiedlichen Fachleuten erreicht werden. Solche freiwilligen Kooperationen und Plattformen zum Informationsaustausch - abseits von Meldeverpflichtungen - sind von zentraler Bedeutung. Die Arbeit der Allianz für Cyber-Sicherheit sollte hier im Vordergrund stehen.

e. **Die sektorspezifischen Standards sollten sich eng an die anerkannten internationalen Standards und Best Practices anlehnen.** Das für den kooperativen Ansatz (des öffentlichen & privaten Sektors) vorgeschlagene Modell für die Entwicklung sektorspezifischer Standards bietet durchaus Vorteile, hat aber ebenso Nachteile. AmCham Germany spricht sich dafür aus, die Industrie in den Entwicklungsprozess von Standards mit einzubeziehen: Fakt ist, dass es zahlreiche relevante internationale Standards gibt - sowohl bei der IT-Sicherheit wie auch beim Schutz der kritischen Infrastrukturen, unter anderem die ISO 27000-Serie. Die dem Gesetz beigefügten Zusatzinformationen beziehen sich auf eine Serie spezifischer Sicherheitsmaßnahmen, die in sektorspezifischen Mindeststandards eingeführt werden sollen, darunter

    a. *Informationssicherheitsmanagement (Sicherheitsorganisation, IT-Risikomanagement, etc.)*
    b. *Benennung und Management kritischer Cyber-Assets*
    c. *Maßnahmen zum Schutz und zum Aufspüren von Cyberattacken*
    d. *Business Continuity Management (BCM)*
    e. *Sektorspezifische Standards*

    In diesem Kontext sollte das BMI auf die bereits bestehenden internationalen Standards für jede dieser Maßnahmen zurückgreifen und im Gesetz direkt auf "adäquate internationale Standards" verweisen, um die Gefahr der Standardfragmentierung beziehungsweise das Entstehen nationaler Standards, die den bestehenden internationalen Standards und Best Practices widersprechen, zu reduzieren.

f. **Keine Erweiterung der Meldepflichten für TK-Unternehmen**. AmCham Germany steht einer Erweiterung der Meldepflichten für TK-Betreiber (§ 109 Abs. 5 TKG) ablehnend gegenüber. Die Erweiterung des die Meldepflicht auslösenden Tatbestands auf sämtliche Beeinträchtigun-

gen, die zu einer Verfügbarkeitsstörung bzw. zu einem unerlaubten Zugriff führen können, erscheint uferlos und mündet in einer Berichtspflicht der Betreiber gegenüber dem BSI über sämtliche Vorgänge in ihren Netzen und Anlagen. Wesentlich zu berücksichtigen ist, dass sich geringfügige Verfügbarkeitseinschränkungen in den TK-Infrastruktur-Netzen nicht generell ausschließen lassen. Eine 100%ige Verfügbarkeit wird somit von keinem Infrastrukturanbieter einem Kunden angeboten bzw. vertraglich vereinbart. Vor diesem Hintergrund beziehen sich die bislang vorgesehenen Meldepflichten nach § 109 Abs. 5 TKG auf entsprechend schwerwiegendere Beeinträchtigungen. Eine umfassendere Meldepflicht auch geringfügiger Störungen führt nicht zur Erhöhung der Sicherheit der Infrastrukturen, sondern lediglich zu erheblichem Mehraufwand auf beiden Seiten, insbesondere auch zu einem Bürokratieaufwand der BNetzA. Schließlich ist in diesem Zusammenhang auch auf die Begrifflichkeiten im Rahmen der Regelungen zum Telekommunikationsgeheimnis und Datenschutz zu achten und sicherzustellen, dass diesbezüglich keine Widersprüche entstehen. Im Zusammenhang mit diesem erheblichen Eigeninteresse unserer Mitgliedsunternehmen an der Gewährleistung der Sicherheit auf ihren Infrastrukturen weist AmCham Germany zudem erneut darauf hin, dass die nach § 109 TKG bestehenden Verpflichtungen auch konsequent umgesetzt wurden. Zudem bedarf die Abstimmungspflicht zum Sicherheitskatalog zwischen BNetzA und BSI insoweit zumindest der Klarstellung in der Begründung, dass es hier jedoch maßgeblich auf die Zuständigkeit der BNetzA und deren Praxiserfahrung ankommt.

g. **Sicherheitsauflagen in Telemedien müssen angemessen und praktikabel bleiben.** § 13 Abs. 7 TMG n.F. verlangt von den Adressaten (unter Androhung hoher Bußgelder) „soweit dies technisch möglich und wirtschaftlich zumutbar ist […] sicherzustellen, dass (1.) kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und (2.) diese (a) gegen Verletzungen des Schutzes personenbezogener Daten und (b) Störungen, auch soweit sie durch äußere Angriffe bedingt sind, gesichert sind. Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. Eine Maßnahme nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens." Absolute Sicherheit ist in der IT-Welt praktisch nicht erreichbar. Sicherzustellen, dass kein unerlaubter Zugriff möglich ist, ist daher viel zu weitgehend und nahezu unerfüllbar. Zwar wird diese Formulierung vermeintlich durch „wirtschaftlich zumutbar" eingeschränkt, dies nutzt aber allenfalls kleineren Webseitenbetreibern, nicht jedoch einem großen finanzstarken Anbieter von Telemedien, für den je nach Lesart des Gesetzes alleine wegen seiner Größe und Finanzkraft nahezu alles „zumutbar" sein könnte. Der Hinweis im letzten Satz auf ein als sicher anerkanntes Verschlüsselungsverfahren hilft zwar hinsichtlich des Schutzes personenbezogener Daten, nicht jedoch, soweit es um die Sicherung der Systeme und technischen Einrichtungen selbst geht. Hier braucht es eine deutlich eingeschränktere Mittel-Zweck-Relation, außerdem sollte der Begriff „sicherzustellen" durch eine weniger weitgehende Formulierung ersetzt werden.

3. Erhöhte Transparenz bei Produkt-Evaluierungen und öffentlichen Warnungen des BSI

Der derzeitige Gesetzesentwurf stärkt die Befugnis des BSI zur Durchführung von Sicherheitsbewertung von ICT-Produkten, -systemen und -dienstleistungen (§7a). Im Zuge der Durchführung dieser Bewertungen ist das BSI befugt, alle technischen Mittel einzusetzen sowie Dritte zu beauftragen. Die Ergebnisse dieser Bewertung können an Dritte weitergegeben und auch veröffentlicht werden.

Hierzu regt AmCham Germany folgendes an:

a. **Der Entwurf ist in Hinblick auf die Bewertungen sehr weit gefasst. Das Bewertungsverfahren des BSI für ICT-Produkte, -systeme und -dienstleistungen sollte so transparent wie möglich sein.** Die unabhängige Bewertung von Produkten hat in Deutschland eine lange Tradition und Produktbewertungen durch das BSI haben ein großes Gewicht. Aus diesem Grund ist es wichtig, dass diese Bewertungen in transparenter Weise auf der Grundlage einer soliden Methodik durchgeführt werden. Sowohl die Bewertungsschritte als auch die zugrundeliegende Methodik sollten daher den IT-Anbieter der bewerteten Produkte miteinbeziehen, bzw. dem IT-Anbieter mitgeteilt werden und die Möglichkeit für Austausch und Rücksprache vorsehen. Nur so kann sichergestellt werden, dass alle Eigenschaften der besagten Produkte richtig und vollständig verstanden worden sind und die nachfolgenden Schlussfolgerungen so genau wie möglich formuliert werden. Ohne diese Transparenz und ein effektives Feedback des Anbieters würde der geplanten Produktbewertung von Anfang an ihre Glaubwürdigkeit fehlen.

b. **Die Bewertung von Produkten, die noch nicht auf dem Markt sind, wirft erhebliche Bedenken hinsichtlich des Geschäftsgeheimnisses auf und bedroht Innovationen.** Der geplante Entwurf beinhaltet die Möglichkeit, dass das BSI ICT-Produkte bewertet, die noch gar nicht auf dem Markt sind. Solche Produkte und Dienstleistungen beinhalten häufig vertrauliche Geschäftsinformationen. Wenn Informationen über diese Produkte und Dienstleistungen bewertet werden und diese Bewertungen veröffentlicht werden bevor die Produkte bzw. Dienstleistungen in den Handel kommen, stellt dies eine erhebliche Gefahr für das geistige Eigentum des IT-Anbieters dar und wird in der Folge die Innovationsfähigkeit des Anbieters beeinträchtigen. Diese Art der Prüfung verlangsamt Innovationen für große wie für kleine Unternehmen. AmCham Germany empfiehlt dem BMI daher nachdrücklich, Produkte und Dienstleistungen, die nicht im Handel erhältlich sind, von dieser Art der Prüfung durch das BSI und insbesondere durch Dritte entweder auszunehmen oder auf freiwilliger Basis durchzuführen.

c. **Öffentliche Warnungen (§ 7 Warnungen) sollten mit den IT-Anbietern besser koordiniert werden.** Neben der neu eingeführten Regelung der Meldepflicht bei einem Vorfall erhält das BSI darüber hinaus den Auftrag, im Fall von Angreifbarkeiten, Exploits und (neu hinzugefügt) Datendiebstahl öffentliche Warnungen herauszugeben. Unserer Ansicht nach sind Änderungen an dem bestehenden § 7 eine Gelegenheit, das bestehende Warnungsmandat des BSI umfassend zu prüfen und zu verbessern und nicht einfach nur auf Szenarien des Datendiebstahls zu erweitern. Das BMI sollte dabei analysieren, welche Auswirkungen frühere Warnun-

gen seit Einführung der ursprünglichen Befugnis in das BSI Gesetz im Jahr 2009 gehabt haben, um ein klareres Verständnis und eine bessere Methodik für eine Balance zwischen der Verpflichtung zur öffentlichen Warnung und den Interessen der betroffenen Betreiber zu entwickeln. Leider hat das bestehende breite Mandat in vielen Fällen zu Situationen geführt, in denen Warnungen ausgesprochen wurden, obwohl entweder die Bedrohungseinschätzung nicht ausreichend verstanden wurde oder das Verständnis für die tatsächlichen Nutzung mit einem tatsächlich bestehenden Sicherheitsrisiko für die deutsche Bevölkerung nicht da war (z.B. haben längst nicht alle „zero-day exploits" konkrete Auswirkung in allen Märkten gehabt, in denen bestimmte Produkte auch genutzt werden). Das Mandat zur öffentlichen Warnung muss angesichts der Flut von Informationen, die im Rahmen der neuen Regelung der Pflichtmeldungen zu erwarten steht, absolut wasserdicht sein. Eine Möglichkeit, die Regelung zu verbessern, wäre eine Aktualisierung dieses Abschnitts mit der Verpflichtung einer umfassenden Rücksprache mit dem betroffenen Betreiber (oder dem zugrundeliegenden Anbieter des IKT-Produkts) anstelle der einfachen Mitteilung von dem BSI an den Anbieter, so wie dies im Augenblick die Praxis ist.

4. Internationale Harmonisierung von Cybersicherheitspolitik

Es ist das erklärte Ziel der Bundesregierung, dieses Gesetz - auch auf EU-Ebene - als Basis für ihre Positionen in den entsprechenden Verhandlungen zu nutzen, die sich z.B. auf die NIS-Direktive beziehen.

AmCham Germany regt hierzu folgendes an:

a. **Die Bundesregierung sollte die Diskussionen auf EU-Ebene zur stärkeren Harmonisierung nutzen.** Bei den Diskussionen zur Cybersicherheit auf EU-Ebene sollte die Bundesregierung eine noch stärker proaktive Rolle einnehmen, nicht zuletzt, um so auf eine Harmonisierung der Gesetzgebungen in den jeweiligen EU-Staaten hinzuwirken. Dies gilt insbesondere in Hinblick auf die laufenden Gespräche über die Direktive zur Netz- und Informationssicherheit (NIS). So kann sichergestellt werden, dass europäische Grundregeln und der deutsche Ansatz zur IT-Sicherheit harmonisiert werden.

b. **Angleichung der innenpolitischen und europapolitischen Position der Bundesregierung zur IT-Sicherheit.** Deutschland hat auf nationaler Ebene immer dafür plädiert, dass das IT-Sicherheitsgesetz darauf fokussiert sein müsse bessere Sicherheitsergebnisse für kritische Infrastrukturen zu erzielen. Aus Sicht des Risikomanagements ist dies ein sinnvoller Ansatz, der auch auf europäischer Ebene stärker verfolgt werden sollte.

c. **Weitere Harmonisierung der EU-Gesetzgebung zur IT-Sicherheit.** Während klar ist, dass die entsprechende Gesetzgebung angesichts der schnellen Entwicklungen von Technologie und Bedrohungen sehr wahrscheinlich im Laufe der Zeit geändert werden muss, wäre es – auf jeden Fall aus Sicht von in verschiedenen EU-Mitgliedsstaaten aktiven Unternehmen – extrem problematisch, mit 28 unterschiedlichen Versionen von Gesetzen zur IT-Sicherheit mit sich potentiell widersprechenden Anforderungen, Standards etc. konfrontiert zu sein. AmCham Germany setzt sich dementsprechend für die maximal mögliche Harmonisierung der IT-Gesetzgebung in Europa – und am besten weltweit – ein.

d. **Wir empfehlen die Veröffentlichung von in Handlungen umsetzbaren Informationen für öffentliche Behörden, Unternehmen und Verbraucher.** Es entwickeln sich immer neue Bedrohungen der IT-Sicherheit und die gesamte Bedrohungslandschaft ist extrem dynamisch. Die Analyse von 6-Monats-Zeiträumen – statt in einem Jahresbericht – zur Abbildung einer möglichst genauen situativen Darstellung und darüber hinaus die Veröffentlichung von zwei Berichten pro Jahr würde dem BSI die Möglichkeit geben, die öffentliche Wahrnehmung von Bedrohungen der IT-Sicherheit noch stärker zu erhöhen.

Kontakt AmCham Germany
Telecommunications, Internet, and Media (TIM) Committee

Chair
Dr. Nikolaus Lindner, LL.M.
Director, Leiter Government Relations DE / AT / CH, eBay GmbH

Co-Chair
Mike Cosse
Vice President Government Relations Middle & Eastern Europe, SAP SE

Co-Chair
Dr. Gunnar Bender
EVP Corporate Communications, Marketing & Public Policy, arvato AG

Staff Contact
Julia Pollok
Manager, Government Relations
Leiterin Regierungsbeziehungen
American Chamber of Commerce in Germany e.V.
Charlottenstrasse 42, 10117 Berlin
T +49 30 288789-24
F +49 30 288789-29
E jpollok@amcham.de