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

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

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

- 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 vertragloses 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 Bedingungen 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.

---

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

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 Regelung des § 100 TKG in dieser Fassung und bei heutiger Technik deutlich jenseits des grundgesetzlich Zulässigen.

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

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 hätten weitergehender Ideen und Ansätze bedurft. Solche Aspekte sind jedoch im neuen Entwurf eines IT-Sicherheitsgesetzes unbearbeitet geblieben.

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

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 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.

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

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:

- 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.

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

- 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 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

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

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.“

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**

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

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.

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 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.

---

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

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. Sinnvoll wäre stattdessen eine Schwerpunktstaatsanwaltschaft, die über die nötigen Mittel und

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

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.
>
> […]
>
> (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

8 Josef Foschepoth: Überwachtes Deutschland. Post- und Telefonüberwachung in der alten Bundesrepublik; Göttingen, 2012

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.

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 or-

9 Änderungsantrag des Abg. Dr. Manuel Kiper und der Fraktion Bündnis 90/Die Grünen zum Entwurf eines

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

ganisiert 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.

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.