erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

Ingo Ruhmann

Schutz von Grundrechten nicht in Sicht

Zur Stellungnahme des FIfF zum Entwurf des IT-Sicherheitsgesetzes

Egal, ob das Internet kaputt ist oder nicht –, die heutige Lage von Datenschutz und Privatsphäre im Internet und bei der IT-Sicherheit ist ein Zustand von unkontrollierter Ausspähung und Computerattacken im Wilden Westen ohne Recht und Gesetz. Die Bundesregierung ist mit ihrem Ende 2014 beschlossenen Entwurf eines IT-Sicherheitsgesetzes angetreten, dem Recht und dem Schutz bei IT-Systemen zu mehr Geltung zu verhelfen. Was davon zu halten ist, zeigt die Stellungnahme des FIfF zum Gesetzentwurf.

Auch eineinhalb Jahre nach Beginn der von Edward Snowden ermöglichten Enthüllungen werden immer noch neue Fakten bekannt im Skandal um das Ausspähen von Computern durch die NSA und deren Angriffe auf IT-Systeme von Verbündeten ebenso wie von erklärten Gegnern. Der NSA-Skandal hat IT-Verantwortlichen, aber auch der Allgemeinheit unmissverständlich deutlich gemacht, in welchem Umfang IT-Systeme kompromittiert sind. Verschlüsselungssysteme werden ausgehebelt, vertrauliche Kommunikationsinhalte abgefangen, privateste Daten auf den eigenen Computersystemen ausgespäht – selbst, wenn diese Computer nicht mit dem Internet verbunden sind. IT-Sicherheitsprofis wie Bruce Schneier bringen den Kenntnisstand auf ein einfaches Fazit: „Wenn die NSA in Deinen Computer hinein kommen will, dann kommt sie auch hinein."

Privatsphäre und Sicherheit in der digitalen Welt sind in Auflösung begriffen. Wer dies nicht als schicksalhafte Folge des Tuns großer Mächte hinnehmen will, muss aktiv werden. Die *Cyberpeace*-Kampagne des FIfF ist eine Form konstruktiver Gegenwehr. Das zentrale Ziel der Kampagne ist das Ende der unbegrenzten geheimdienstlich-militärischen Ausspähung und Manipulation beliebiger IT-Systeme und der Schutz von Grundrechten. Doch Appelle, Verbote und technische Hilfsmittel allein helfen nicht. Gefordert ist auch die Abwehr konkreter Attacken mit zivilen und rechtstaatlichen Mitteln. Die *Cyberpeace*-Kampagne verfolgt daher auch das Ziel, Computerspionage und -sabotage zu ahnden und die Täter zu verfolgen.

Gerade aus der Sicht von IT-Fachleuten sieht das FIfF die Notwendigkeit, IT-Sicherheit nicht nur technisch zu verbessern, sondern auch den rechtstaatlichen Schutz zu stärken und damit den Schutz von gleich drei derzeit über alle Maßen verletzten Grundrechten zu gewährleisten:

1. das Fernmeldegeheimnis nach Art. 10 GG,
2. das Datenschutz-Grundrecht auf *informationelle Selbstbestimmung*[1] und
3. das IT-Grundrecht auf *Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*[2].

Artikel 1 (3) Grundgesetz bestimmt: „Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht." Es ist also staatliche Aufgabe, den Schutz dieser drei Grundrechte seiner Bürgerinnen und Bürger zu gewährleisten, staatliches Handeln darauf auszurichten und auf den Schutz der Grundrechte auch gegenüber nicht-staatlichem Handeln hinzuwirken.

Vor diesem Hintergrund war es zu begrüßen, dass die Bundesregierung Ende 2014 in einem zweiten Anlauf ein Gesetz zur IT-Sicherheit im Kabinett verabschiedete, das seinen Beitrag dazu leisten will, „dass das Netz sicherer wird und die digitalen Infrastrukturen Deutschlands künftig zu den sichersten weltweit gehören."

Kern des Entwurfes der Bundesregierung ist es[3], Betreiber kritischer Infrastrukturen auf einen Mindeststandard an IT-Sicherheit zu verpflichten und erhebliche IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Die beim BSI zusammenlaufenden Informationen sollen ausgewertet und zur Verbesserung des Schutzes kritischer Infrastrukturen zur Verfügung gestellt werden. Telekommunikationsunternehmen – so das BMI in seiner Pressemitteilung – werden zudem verpflichtet, ihre Kunden zu warnen, wenn ihnen auffällt, dass der Anschluss des Kunden für Angriffe missbraucht wird.

Doch leider erweist die genaue Lektüre auch dieses Gesetzesvorhabens, dass zwischen verfassungsmäßigen Pflichten und gesetzgeberischem Tun ganz erhebliche Differenzen bestehen. Das FIfF hat Mitte Februar eine detaillierte Stellungnahme zum IT-Sicherheitsgesetz vorgestellt[4], die sich auf vier Themenbereiche konzentriert:

1. die nicht verfassungsgemäßen gesetzlichen Regelungen und Rechtsgrundlagen für IT-Sicherheit,

2. das BSI als zentrale IT-Sicherheitsinstanz,

3. die Sonderrolle für staatliche IT und der defizitäre Schutz für die Allgemeinheit,

4. die unzureichende Umsetzung von Schritten und Maßnahmen, die für IT-Sicherheit nötig sind.

Positionen und Kritik des FIfF werden im Folgenden in geraffter Form dargestellt. Die ausführliche Stellungnahme ist auf den Webseiten der Cyberpeace-Kampagne verfügbar.[5] Es wäre zusätzlich eine eigene Betrachtung, ob die Ansätze und Aufwände für den Schutz kritischer Infrastrukturen ausreichen. Dies kann hier nicht geleistet werden.

1. Rechtsgrundlagen für IT-Sicherheit nicht vorhanden oder nicht verfassungsgemäß

Die Kritik des FIfF setzt dort an, wo es um die rechtlichen Grundlagen geht, IT-Sicherheit mit rechtstaatlichen Mitteln überhaupt zu gewährleisten und der Pflicht des Staates zum Schutz von Grundrechten nachzukommen.

Für das Verständnis der Kritik bedeutsam ist, dass das Internet im deutschen Recht in zwei Bereiche aufgeteilt ist[6]: Das Recht der Telekommunikation (im Telekommunikationsgesetz, TKG) etwa für E-Mails, Chatten und andere direkte Kommunikationsformen einerseits und das Recht der Telemedien (im Telemediengesetz, TMG), in dem alle Webangebote geregelt sind, also die Pflichten der Anbieter von Webseiten, Webshops, Cloud-Speichern oder komplexen webbasierten Softwarediensten. Für beide Bereiche erlauben und verbieten beide Gesetze verschiedene IT-Sicherheitswerkzeuge. Wichtig zum Verständnis ist auch, dass das Bundesverfassungsgericht im Januar 2012 IP-Adressen als personenbezogene Daten bewertete.[7]

Regelung für Webangebote

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

Für Zwecke der IT-Sicherheit erlaubt das Gesetz damit nur, IP-Nummern von Nutzern eines Webangebotes solange zu verarbeiten, wie die aktuelle Nutzung andauert. Da die IT-Sicherheit als Zweck im Gesetz nicht vorgesehen ist, greift das generelle Speicherungsverbot und damit die Pflicht zur Löschung der IP-Daten nach Nutzungsende oder zumindest deren Pseudonymisierung, wenn auch fraglich ist, ob das zu einer „bedarfsgerechten Gestaltung" zählt. Unzweifelhaft gesetzwidrig ist es, vollständige IP-Adressen für irgendeinen Zweck dauerhaft zu speichern.

Bei Webangeboten dürfen damit IP-Daten von IT-Sicherheitswerkzeugen durch ein *Intrusion Detection System* genutzt werden. Es gibt aber bei Webangeboten keine Rechtsgrundlage für den Einsatz von IT-Sicherheitswerkzeugen für mehrschrittige Analysen und erst recht nicht für die Verfolgung von Angreifern und die Beweissicherung nach einem Fall von Cybersabotage, sondern das Verbot der entsprechenden Datenspeicherung und -verarbeitung. Der Bundesregierung ist die Problematik spätestens seit 2006 bekannt, als dem Bundesjustizministerium genau diese Speicherung von IP-Daten rechtskräftig untersagt wurde[8].

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

Der Gesetzentwurf der Bundesregierung sah in einer Vorversion aus dem Sommer 2014 hierzu eine Regelung vor, die nach berechtigter Kritik wieder gestrichen wurde. In dieser Vorversion plante die Bundesregierung, einfach eine ähnliche Regelung aus dem Telekommunikationsrecht – §100 TKG – zu übertragen. Das FIfF sieht schon in den heutigen, aus der Zeit der analogen Telefonie stammenden Befugnissen zur Datensammlung nach §100 TKG eine deutlich überzogene Regelung. Der §100 TKG erlaubt heute ohne jede Einschränkung, jede Form von Daten

zur Störungserkennung aus Telefonaten und Datenverkehren zu sammeln, zu analysieren und sich sogar auf Kommunikationsverbindungen aufzuschalten.

Regelung in der Telekommunikation

Die Bundesregierung verabschiedete nun in ihrem Entwurf des IT-Sicherheitsgesetzes für den Telekommunikationssektor eine noch sehr viel weiter reichende Regelung. Danach sollen Telekommunikationsanbieter nicht nur jedes beliebige Datum zur Störungserkennung speichern und analysieren dürfen, sondern obendrein auch Daten über

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

Der für analoge Technik 1996 formulierte §100 TKG hatte ursprünglich das Ziel, strafbare Eingriffe in Fernmeldesysteme für die Öffentlichkeit zu ermitteln und den Telekommunikationsunternehmen die Befugnis zu geben, dafür Messungen vorzunehmen. Die geplante Änderung des neuen Gesetzes 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.

Es geht also nicht mehr um die Verfolgung von Gesetzesverstößen – im Kern Betrugshandlungen an TK-Systemen – durch Manipulationen. Hier sollen Telekommunikationsunternehmen dazu befugt werden, als Helfershelfer der Strafverfolgung unbegrenzt Daten über ihre Kunden zu sammeln und auszuwerten, um zu erkennen, ob es unerlaubte „Zugriffe" auf die IT-Systeme der Kunden geben könnte. Eine solche unspezifische Datensammlung zu Zwecken der IT-Sicherheit wäre ein nahezu unbegrenzter Eingriff in das Fernmeldegeheimnis. Im starken Gegensatz zu den Vorgaben des Bundesverfassungsgerichts für Eingriffe in Grundrechte ist diese geplante Vorschrift

1. nicht an die Angabe eines Anlasses (sondern unspezifisch eine „Störung") gebunden,
2. ohne einen genügend spezifischen Zweck (nur Erkennung eines „unerlaubten Zugriffs"),
3. ohne spezifische Kriterien und
4. ohne Vorgaben zu Speicherdauer und zur Datennutzung.

Obendrein soll durch einen geplanten neuen §109a TKG jeder Diensteanbieter bei „Störungen, die von Datenverarbeitungssystemen der Nutzer ausgehen", diese Nutzer

> *„soweit ihm diese bereits bekannt sind, unverzüglich darüber … 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".*

Das geht nur durch die 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.

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

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

Rufen wir uns in Erinnerung, welche Zugriffe auf IT-Systeme „unerlaubt" sind oder was als „Störung" gilt, dann ist man schnell bei einer Ahnung von nahezu unbegrenzter Überwachung des Datenverkehrs ohne jede Einschränkung und damit der faktischen Aushebelung des Fernmeldegeheimnisses. Eine solche dauerhafte Durchsuchung von Telekommunikationsverkehren zur Ermittlung von „Störungen" – nicht einmal „Gefährdungen" – ohne jede Einschränkung entspricht nicht einmal im Ansatz den Anforderungen an Grundrechtseingriffe. Dies macht deutlich, dass die im IT-Sicherheitsgesetz vorgesehene Ausweitung an §100 TKG und die Nutzung der gewonnen Daten für die im geplanten §109a TKG genannten Zwecke aus Sicht des FIfF eindeutig unvereinbar ist mit Art. 10 GG. Es ist mit Sicherheit davon auszugehen, dass sie einer Verfassungsklage nicht standhalten werden.

Zusammenfassend zur Frage der Rechtsgrundlagen soll es im IT-Sicherheitsgesetz für die im TMG geregelten Webservices weiterhin keine Rechtsgrundlage für IT-Sicherheitswerkzeuge geben, im TKG dagegen eine klar verfassungswidrige uferlose Datensammlung, die einem Gang nach Karlsruhe nicht standhalten wird. Im Ergebnis des Gesetzes, das für mehr IT-Sicherheit sorgen sollte, entstünde so ein Rechtsvakuum, das der IT-Sicherheit absolut jede Rechtsgrundlage entzieht und damit zugleich jede Basis für Investitionen in mehr Ressourcen – von einer datenschutzkonformen Lösung einmal ganz abgesehen.

Verfassungskonformer Gegenvorschlag

Der Gegenvorschlag des FIfF zielt darauf ab, die Verarbeitung von IP-Daten zu Zwecken der IT-Sicherheit in allen Bereichen einheitlich und so datensparsam wie möglich zu gestalten. Da ohne die Auswertung von IP-Daten keine Identifikation und

Rückverfolgung von Cyberangreifern möglich ist, die notwendige schnelle Reaktion auf Angriffe eine längere Datenspeicherung unnötig macht und obendrein die große Menge der protokollierbaren Daten die Analyse eher behindert, schlägt das FIfF als Verfahrensprinzip vor, Verdachtsfälle sofort kriterienbasiert zu ermitteln und alle unnötigen Daten zu löschen oder in Zweifelsfällen zumindest zu pseudonymisieren. Für die eingehende Analyse von Cybersicherheitsvorfällen muss dem FIfF-Vorschlag gemäß ein auditierbares Verfahren eingesetzt werden, mit dem nachvollziehbar ist, welche Daten genutzt, und dass nicht benötigte Daten gelöscht wurden. Mit diesem Prinzip ist in einem gerichtsfesten Verfahren die minimal zur Verfolgung notwendige Menge an Daten benannt, bei zugleich weitestgehender Löschung von Daten.

Dass sich das FIfF für eine derart minimierte Sammlung von IP-Daten ausspricht, führte zur Kritik des AK Vorratsdatenspeicherung, der jede Form der IP-Datenspeicherung bei Telemedien ablehnt, die bei Telekommunikationsdaten allerdings nicht weiter erwähnt. Unterstützung für den Vorschlag des FIfF kam indes vom Schleswig-Holsteinischen Landesdatenschutzbeauftragten Thilo Weichert, der in einer Stellungnahme[9] ebenfalls darauf hinweist, dass eine Verfolgung von Cyberangreifern eine IP-Datenspeicherung erfordert und sich daher „hundertprozentig hinter den FIfF-Vorschlag" stellte[10].

Das FIfF bleibt bei seiner Forderung einer einheitlichen Rechtsgrundlage für die IT-Sicherheit, die sowohl das Grundrecht auf *informationelle Selbstbestimmung* wie auch das Grundrecht auf *Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* umsetzt und zugleich das Fernmeldegeheimnis wahrt und nicht weiter aushöhlt.

2. Rolle des BSI

Das FIfF hat die Gründung des BSI 1989 kritisch kommentiert. Wir haben dabei zwar die Notwendigkeit einer solchen Behörde betont, aber zugleich deren Doppelaufgabe für staatliche Stellen einerseits und Bürgerinnen und Bürger andererseits problematisiert.[11]

Diese Doppelaufgabe hat dem BSI in den letzten Monaten erhebliches Misstrauen auf Seiten der deutschen Wirtschaft eingebracht, nachdem durch die von Edward Snowden zugänglich gemachten Dokumente auch bekannt wurde, dass der BSI-Präsident anlässlich einer USA-Reise die NSA zu einem Arbeitstreffen besucht hatte[12]. Dies wurde von den Wirtschaftsverbänden überaus kritisch gesehen, wenngleich das BSI die Berichte dementierte[13].

Das FIfF teilt viele dieser Bedenken der Wirtschaft und sieht einige akut anstehende Aufgaben besser bei anderen IT-Sicherheitsexperten aufgehoben. Entscheidend für das FIfF ist jedoch, dass staatliche Stellen sehr wohl eine unabhängige Kontrollfunktion ausüben können, wenn sie in geeigneter Weise unabhängig organisiert sind. Genauso, wie die Datenschutzbeauftragten frei von der Einflussnahme der von ihnen kontrollierten Stellen sein müssen, so muss auch das BSI nach Ansicht des FIfF in Zukunft weisungsungebunden und unabhängig von anderen staatlichen Stellen organisiert sein, um den Verfassungsauftrag der *Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* erfüllen zu können.

Das IT-Sicherheitsgesetz will das BSI zwar personell und finanziell aufstocken, was keine ganz schlechte Idee ist, aber weiter in seiner bisherigen Rolle belassen, die vorrangig dem Schutz staatlicher IT-Infrastrukturen dient. Der vom Bundesverfassungsgericht formulierte Verfassungsauftrag wird so jedenfalls nicht umgesetzt.

3. Die Sonderrolle für staatliche IT und der defizitäre Schutz für die Allgemeinheit

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

Im ersten Abschnitt wurde kurz erwähnt, dass es dem Bundesjustizministerium 2006 untersagt wurde, IP-Daten zu speichern. Der Bundesregierung war die Gefahr für die IT-Sicherheit – ausweislich ihrer Antwort auf eine Kleine Anfrage[14] – unmittelbar bewusst; sie reagierte binnen Jahresfrist. In der Novelle des BSI-Gesetzes erhielt das BSI 2007 in §5 BSIG die Befugnis, in jedem Anwendungsbereich des Internets für Zwecke der IT-Sicherheit IP-Daten bei IT-Systemen des Bundes zu erheben und auszuwerten. Als einzige Stelle darf daher das BSI – das auch kein Telekommunikationsunternehmen ist, denen ansonsten allein eine Datensammlung gemäß §100 TKG erlaubt ist – IT-Sicherheitswerkzeuge für die IT des Bundes umfassend einsetzen.

Diese Ausnahmereglung für staatliche IT-Systeme wird nun im neuen Gesetzentwurf weiter getrieben. Das BSI erhält nicht nur die Rolle der zentralen Sammelstelle für IT-Sicherheitsvorfälle bei Betreibern kritischer Infrastrukturen, obendrein schafft sich die Bundesregierung eine Sonderpolizei für Cyberattacken beim BKA. Mit der im Gesetzentwurf formulierten Begründung, dass die Strafverfolgung und „die örtliche Zuständigkeit oftmals dem Zufall überlassen" bleiben, soll das BKA bei Computerstrafdelikten gegen die IT des Bundes und kritischer Infrastrukturen ermitteln. Das Argument des „Zufalls" meint offensichtlich – deutlicher gesagt, dass die für IT-Kriminalität zufällig zuständigen Strafverfolgungsbehörden der Republik nicht mit hinreichenden Kompetenzen und Ressourcen ausgestattet sind, um Angriffe auf die IT des Bundes mit der nötigen Sachkunde zu verfolgen.

Bürgerinnen und Bürger, die Wirtschaft, aber auch die Behörden der Länder und Kommunen werden mit den Problemen der Sicherheit ihrer IT-Systeme also nicht nur bei den rechtlichen Grundlagen allein gelassen, sondern auch bei der Strafverfolgung, die in der Fläche nach Meinung der Bundesregierung von so geringer Qualität ist, dass nur ein eigenes zentrales Sonderdezernat helfen kann. Die Bundesregierung beziffert laut Gesetzentwurf den Aufwand für diese Aufgabe beim BKA auf „48 und bis zu maximal 78 Planstellen mit jährlichen Personalkosten in Höhe von jährlich zwischen rund 3,226 und bis zu maximal 5,310 Millionen Euro".

Während gerade Sicherheitspolitiker nicht müde werden zu betonen, das Internet sei kein „rechtsfreier Raum", zieht sich die Bundesregierung bei den Rechtsgrundlagen und bei der Straf-

verfolgung von der Aufgabe eines Schutzes der Allgemeinheit zurück. Für die Allgemeinheit macht die Bundesregierung das Internet damit erst zum rechtlosen Raum, für den zwar Gesetze formuliert sind, aber die Strafverfolgung kaum Handlungsmöglichkeiten hat – in wichtigen Bereichen für die Allgemeinheit sind nicht einmal die Verfolgung von Tätern und die Beweissicherung über die zielgerichtete Speicherung von IP-Daten zulässig.

4. Maßnahmen für die IT-Sicherheit unzureichend

Aus der Sicht von IT-Fachleuten im FIfF ist das IT-Sicherheitsgesetz eine höchst unpassende Konstruktion. Wer IT-Sicherheit verbessern will, muss zwangsläufig das allgemeine Sicherheitsniveau erhöhen und Einfallstore und Hintertüren beseitigen. Alles andere wird Kosmetik bleiben.

Das FIfF hat daher Ergänzungsvorschläge für das IT-Sicherheitsgesetz gemacht, die aus Sicht der Praxis vordringlich sind. Die wichtigsten sind:

- **Umgang mit IT-Sicherheitslücken.** Wie alle IT-Sicherheitsexperten hält auch das FIfF den Austausch über IT-Sicherheitslücken für einen der wichtigsten Wege zur Verbesserung der Sicherheitslage. Das FIfF fordert, dass das BSI seine Kenntnisse zeitnah und umfassend publizieren muss und nicht selbst darüber entscheidet, ob es dies tut. Das FIfF fordert weiter, dass zur Aufdeckung von Sicherheitsproblemen durch interne Whistleblower und zur Realisierung einer Produkthaftung ein gestuftes Meldeverfahren etabliert wird, bei dem eine vertrauenswürdige Stelle Hinweise sammelt und an die Hersteller oder Anwender weiterleitet, die die Sicherheitsrisiken zu verantworten und zu beseitigen haben. Werden bekannt gewordene Sicherheitslücken nicht nach einer angemessenen Frist geschlossen, wird der Weg möglich, geltende Produkthaftungsregelungen auch im IT-Bereich gegen die Verursacher von Sicherheitsrisiken anzuwenden.

- **Zuverlässigkeit zentraler IT-Sicherheitsmechanismen.** Wenn die Dokumente von Edward Snowden eines gezeigt haben, dann, in welchem Ausmaß zentrale Sicherheitsmechanismen der IT-Sicherheit kompromittiert sind. Schon bevor der SSL-*Heartbleed-Bug* überhaupt programmiert wurde, war NSA-Dokumenten zu entnehmen, dass die SSL-Verschlüsselung erfolgreich angegriffen wurde. VPN-Verbindungen sind durch Hintertüren und Implementationsdefizite verwundbar. Das FIfF fordert, solche und andere zentrale IT-Sicherheitskomponenten jetzt und auf Dauer periodisch auf ihre Zuverlässigkeit oder Kompromittierung hin durch unabhängige Stellen zu untersuchen und die Ergebnisse zu veröffentlichen.

- **Schutz des Fernmeldegeheimnisses.** Zu den zielgerichtet in das Strafrecht formulierten Absonderlichkeiten des deutschen Rechts gehört, dass kein Geheimdienstmitarbeiter dafür belangt werden kann, das Fernmeldegeheimnis durch Abhören gebrochen zu haben. Strafbar machen sich beim Abhören nach §206 StGB nur Mitarbeiter von Telekommunikationsunternehmen. Das FIfF fordert angesichts des NSA-Skandals, die Strafbarkeit von Abhörhandlungen genauso zu regeln wie den Bruch des Postgeheimnisses, bei dem es für jedermann strafbar ist, verschlossene Sendungen zu öffnen und zu lesen.

5. Gibt es gar nichts Positives?

Bei aller Kritik und Verbesserungsvorschlägen ist die Frage natürlich richtig, welche genuin positiven Aspekte das Gesetz aus Sicht des FIfF enthält. Diese sind schnell genannt.

Die Verpflichtung von Betreibern kritischer Infrastrukturen auf bessere IT-Sicherheit ist sicherlich eine gute Idee. Kerntechnische Anlagen, die bisher aus der Debatte heraus gehalten wurden, auch zu kritischen Infrastrukturen zu zählen, ist eine positive Überraschung. Das Gesetz regelt hierzu aber nur genau das als Maßstab, was das Bundesdatenschutzgesetz ohnehin seit Jahren vorschreibt: Den Stand der Technik.

Der aktuelle Stand der Technik ist aber keine echte Perspektive in der IT-Sicherheit. Schon seit über drei Jahren arbeiten das DIN und die ISO an neuen Sicherheits-Standards für Energienetze, die zur Grundlage für Zertifizierungen werden und zu EU-weiten Standards führen sollen. Auch die EU hat mehrfach angekündigt, in Sachen IT-Sicherheit regulativ tätig zu werden[15], das EU-Parlament hat Ergänzungen angemahnt[16]. Es ist zu vermuten, dass die EU die IT-Sicherheit umfassender regeln wird und auf Deutschland Nachbesserungsbedarf zukommt. Hier hätte die Bundesregierung auch aus den Interessen der Industrie heraus weiter gehende Maßstäbe setzen können. Aktiv gestalten, statt bei der IT-Sicherheit nur zu reagieren, wäre für Deutschland der bessere Ansatz.

Grundsätzlich positiv zu sehen sind auch die zusätzlichen Ressourcen für die IT-Sicherheit. Dass aber nicht nur das BSI 133 zusätzlichen Planstellen erhält und damit von derzeit ca. 600 Stellen auf dann über 730 Stellen anwächst, sondern laut IT-Sicherheitsgesetz für das Bundesamt für Verfassungsschutz 55 neue Planstellen und das BKA bis zu 79 zusätzliche Planstellen vorgesehen sind – in Summe also 134 Stellen –, ist nicht nachzuvollziehen. Die neuen Stellen für Verfassungsschutz und BKA wären besser beim BSI aufgehoben, hätten den Stellenzuwachs dort glatt verdoppelt, und könnten im BSI die Sachkompetenz zur Bekämpfung von IT-Sicherheitsproblemen für die Allgemeinheit bündeln und verstärken, statt die nachrichtendienstliche Ausforschung voran zu treiben. Das BSI hat seit seiner Entstehung schon die Aufgabe, Polizeibehörden mit Sachkunde zu unterstützen und könnte dies bei Cyberangriffen mit mehr Personal besser leisten.

6. Fazit

Das neue IT-Sicherheitsgesetz erweist sich – so die detaillierte Analyse des FIfF – in Sachen Datenschutz als hochgradig defizitär, in Sachen IT-Sicherheit als ungenügend und – insbesondere auch durch die Reduktion der Sicherheitsperspektive auf IT-Systeme des Bundes – als ein Weg in massiv weiter ausufernde Sicherheitsprobleme in der Fläche. Einfach mögliche Lösungsansätze wurden nicht verfolgt, die wenigen positiven Aspekte beim Stand der Sicherheitstechnik und beim Personal sind nur ein schwacher Ausgleich.

Sicher ist nur, dass dieses Gesetz für Juristen neue Arbeit bringen und IT-Sicherheitsexperten nicht entlasten wird. Die Sicherheit in der IT und der Schutz der Grundrechte werden mit diesem Gesetz nicht im Ansatz verbessert.

Anmerkungen

1 *BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983, 1 BvR 209/83 u. a. – Volkszählung –, BVerfGE 65, 1*
2 *Bundesverfassungsgericht vom 27. Februar 2008 - 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274 ; http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html*
3 *Pressemitteilung des Bundesinnenministeriums vom 17.12.2104 zum dort ebenfalls publizierten Gesetzentwurf: http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2014/12/bundeskabinett-beschlie%C3%9Ft-it-sicherheitsgesetz.html*
4 *http://cyberpeace.fiff.de/Kampagne/ITSicherheitsgesStellungn*
5 *FIfF-Stellungnahme zum IT-Sicherheitsgesetz; http://cyberpeace.fiff.de/Uploads/Uploads/FIfF_Stellungnahme_IT-Sicherheitsgesetz.pdf*
6 *Im Detail dazu: Ingo Ruhmann: IT-Sicherheit und das geplante IT-Sicherheitsgesetz; in: telepolis, 11.04.2013; http://www.heise.de/tp/artikel/38/38891/1.html*
7 *Beschluss des Ersten Senats vom 24. Januar 2012 - 1 BvR 1299/05 - http://www.bverfg.de/entscheidungen/rs20120124_1bvr129905.html*
8 *Endgültiger Beschluss des Amtsgericht Mitte zu Berlin mit Androhung von Zwangsgeld gegen das BMJ vom 10.01.2008, 5 C 314/06, http://www.daten-speicherung.de/data/Beschluss_AG-Mitte_2008-01-10.pdf*
9 *ULD-Stellungnahme zum IT-Sicherheitsgesetz-Entwurf; https://www.datenschutzzentrum.de/artikel/877-ULD-Stellungnahme-zum-IT-Sicherheitsgesetz-Entwurf.html*
10 *IT-Sicherheitsgesetz: Streit um Nutzung von IP-Adressdaten; in: Heise Newsticker, 17.02.2015, http://www.heise.de/newsticker/meldung/IT-Sicherheitsgesetz-Streit-um-Nutzung-von-IP-Adressdaten-2552632.html*
11 *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*
12 *René Pfister, Laura Poitras, Marcel Rosenbach, Jörg Schindler, Holger Stark: Der fleißige Partner; in: Spiegel Online, 22.07.2013, http://www.spiegel.de/spiegel/print/d-104058608.html*
13 *BSI-Pressemitteilung: Keine Unterstützung ausländischer Nachrichtendienste, Bonn, 26.07.2013, https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2013/Keine_Unterstuetzung_auslaendischer_Nachrichtendienste_26072013.html*
14 *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Petra Pau, Sevim Dagdelen, weiterer Abgeordneter und der Fraktion DIE LINKE: Speicherung der IP-Adressen von Besucherinnen und Besuchern der Website des Bundeskriminalamtes, 7.11.2007, Bt.-Drs. 16/6938, Antworten zu den Fragen 11 und 13*
15 *Kommissionsvorschlag für eine Richtlinie zur Netz- und Informationssicherheit (NIS) vom 7.02.2013, http://europa.eu/rapid/press-release_IP-13-94_de.htm*
16 *Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zum Thema „Cyberangriffe in der EU", 10.07.2014; http://edz.bib.uni-mannheim.de/edz/doku/wsa/2014/ces-2014-1488-de.pdf*

FIfF e. V. – Pressemitteilung

FIfF fordert wirksame EU-Gesetzgebung für verantwortungsvolle Rohstoffbeschaffung von Unternehmen

Europäische Unternehmen profitieren vom Handel mit Konfliktrohstoffen

3. Dezember 2014 – Seit Jahrzehnten spielt der Handel mit Mineralien, Edelsteinen und anderen Rohstoffen eine zentrale Rolle bei der Finanzierung bewaffneter Konflikte weltweit. Konfliktparteien in Ländern wie Afghanistan oder Zentralafrikanische Republik werden mit Erlösen aus dem internationalen Rohstoffhandel finanziert. Europäische Firmen importieren eine große Menge an Rohstoffen für Handys oder Laptops aus eben diesen Konfliktgebieten, ohne dass Unternehmen offenlegen müssen, ob und inwiefern sie mit dem Kauf dieser Rohstoffe zur Finanzierung von Kriegen und Menschenrechtsverletzungen beitragen.

Die Europäische Kommission hat im März 2014 einen Verordnungsentwurf vorgelegt, der verhindern soll, dass „Erträge aus dem Handel mit Mineralien zur Finanzierung bewaffneter Konflikte verwendet werden". Dass die EU diesbezügliche Regelungen vorsieht, ist zu begrüßen, denn ihr Einfluss ist groß: Fast ein Viertel des globalen Handels mit Zinn, Tantal, Wolfram und Gold entfällt auf die EU, letztes Jahr wurden 240 Millionen Handys und 100 Millionen Laptops in die EU importiert, die alle diese Rohstoffe enthalten.

„Der derzeit vorliegende Entwurf ist viel zu schwach. Er bezieht sich einerseits ausschließlich auf Direktimporteure der unter die Verordnung fallenden Mineralien, zum anderen handelt es sich nur um ein Modell der freiwilligen Selbstverpflichtung. Doch am 4. Dezember 2014 gibt es die Möglichkeit, diesen Entwurf zu stärken" erklärt Sebastian Jekutsch, Sprecher der Arbeitsgruppe *Faire Computer* des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung. Morgen findet eine öffentliche Anhörung des Ausschusses für internationalen Handel zum Thema Konfliktmineralien in Brüssel statt. Das FIfF fordert, dass der Parlamentsausschuss Führungsqualitäten zeigt und den Entwurf stärkt:

„Zurzeit sind die Unternehmen nicht verpflichtet sicherzustellen, dass die Erlöse aus dem Handel mit diesen Mineralien nicht in die falschen Hände geraten. Doch Unternehmen kommen ihrer Sorgfaltspflicht beim Bezug von Rohstoffen aus Konfliktgebieten nur dann nach, wenn sie gesetzlich dazu gezwungen werden. Verpflichtende Regeln sind daher unbedingt notwendig", so Sebastian Jekutsch. „Zudem müssen auch Unternehmen Verantwortung übernehmen, deren Endprodukte diese Rohstoffe