Aus der digitalen Agenda der Bundesregierung – das geplante IT-Sicherheitsgesetz

RA Levent Ferik, LL.M., Bonn*

I. Vorbemerkung

Das technische Konzept der Vermittlung von IP-Paketen, und damit der wesentliche Unterbau dessen, was heute umgangssprachlich, aber ungenau als Internet bezeichnet wird, stammt bekanntlich aus den frühen sechziger Jahren (1962). Wollte man ein Jahr festmachen, an dem dieses, ehemals einem recht exklusiven Klientel vorbehaltene, Netz seinen Siegeszug durch alle Bevölkerungsschichten begann, und in den darauf folgenden Jahren ein nicht mehr wegzudenkender Bestandteil sowohl des Wirtschaftslebens als auch des sozialen Lebens wurde, dann wäre dies das Jahr 1993, als Marc Andreessen einen Browser namens „Mosaic" veröffentlichte, der bald dem World Wide Web und auch dem gesamten Internet ungekannte Popularität jenseits der bisherigen Nutzerkreise und ein explosionsartiges Wachstum bescherte[1].

Beseelt von der Einsicht, dass die Menschen zunehmend in einer digital vernetzten Welt leben und diese digitale Vernetzung den Arbeitsplatz, die Schule, die Universität sowie das Privatleben betrifft, hat die aktuelle Bundesregierung über 20 Jahre nach dem Siegeszug des Netzes die sog. Digitale Agenda 2014-2014 vorgestellt, um endlich die Grundsätze ihrer Digitalpolitik bekannt zu geben[2].

Abseits der Stellungnahmen zu den sonstigen Grundsätzen und Punkten der Digitalen Agenda hat die Vorstellung des Entwurfs eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) besonders viel Resonanz hervorgerufen.

Die Tatsache allein, dass der Entwurf vom Bundesministerium des Innern (BMI) kommt, zeigt bereits die weitere Erkenntnis, in welch hohem Maß unsere Gesellschaft und wesentliche Teile unseres Gemeinwesens von einer funktionierenden Informationstechnik und sicheren Informationsinfrastrukturen abhängig sind, und wie sehr die Beeinträchtigung dieser Vernetzung oder schlimmstenfalls ein gezielter Angriff auf diese Infrastruktur auch die innere Sicherheit Deutschlands gefährden könnte.

II. Altes und Neues

Das BMI hatte bereits am 12. März 2013 den Referentenentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme[3] vorgestellt. Der damalige Bundesinnenminister Dr. Hans-Peter Friedrich konnte drei Schwerpunkte zur Verbesserung der IT-Sicherheit in dem vorgestellten Entwurf festmachen.

Die Betreiber kritischer Infrastrukturen sollten zum einen zu einer Verbesserung des Schutzes der von ihnen eingesetzten Informationstechnik und zur Verbesserung ihrer Kommunikation mit dem Staat bei IT-Vorfällen verpflichtet werden. Zum anderen sollten gleichzeitig Telemediendienstanbieter, denen eine Schlüsselrolle für die Sicherheit des „Cyberraumes" zugestanden wurde, stärker als bis dahin für diese ihnen zugewiesene Schlüsselrolle zur Verantwortung gezogen werden können. Darüber hinaus sah es der damalige Bundesinnenminister als erforderlich an, das BSI in seinen Aufgaben und Kompetenzen zu stärken, um die gewünschten Resultate tatsächlich erzielen zu können.

Der jüngste Entwurf des BMI scheint an einigen Stellen ambitionierter[4]. Sprach die Bundesregierung im Koalitionsvertrag[5] noch lediglich darüber, Mindestanforderungen an die IT-Sicherheit für Kritische Infrastrukturen zu schaffen, soll nun nicht nur der Schutz der Verfügbarkeit, Integrität und Vertraulichkeit der datenverarbeitenden Systeme verbessert werden, sondern, über die Optimierung der CIA Triade hinaus, sowohl die IT-Sicherheit der Unternehmen verbessert als auch der Schutz der Bürgerinnen und Bürger hinsichtlich des Netzes, in dem sie sich bewegen, gestärkt werden. Abweichend vom alten Entwurf soll in diesem Zusammenhang nicht nur das BSI, sondern auch das BKA eine Stärkung erfahren. Der Anspruch ist nicht geringer, als dass die IT-Systeme und digitalen Infrastrukturen Deutschlands die sichersten weltweit werden sollen.

III. Adressaten und Maßnahmen

Enthielt der Koalitionsvertrag 2014[6] lediglich die vage Maßgabe, die Betreiber kritischer Infrastrukturen durch Kooperation und gesetzliche Vorgaben anhalten zu wollen, die Widerstandsfähigkeit (Resilienz) und Schutzmaßnahmen zu verbessern, konkretisiert der Entwurf diese Vorgabe. Vor allem Betreiber sogenannter kritischer Infrastrukturen, z.B. aus dem Energie-, Wasser-, Transport- oder Finanzwesen, sollen Sicherheitsvorfälle unter Mitwirkung von Warn- und Alarmierungskontakten zukünftig an das Bundesamt für Sicherheit in der Informationstechnik (BSI) melden. Unter die Definition passen gemäß der zu ergänzenden Absätze 10 und 11 des BSI-Gesetzes alle Unternehmen, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind und durch deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe oder erhebliche Störungen der öffentlichen Sicherheit eintreten würden.

* Rechtsanwalt Levent Ferik, LL.M. ist stellvertretender Geschäftsführer der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.

1 Wikipedia: http://de.wikipedia.org/wiki/NCSA_Mosaic.

2 Digitale Agenda 2014-2017, http://www.bmwi.de/DE/Themen/Digitale-Welt/digitale-agenda.html.

3 Im Folgenden: IT-Sicherheitsgesetz.

4 BMI: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_IT-Sicherheitsgesetz.pdf.

5 Koalitionsvertrag für die 18. Legislaturperiode, S. 104, https://www.cdu.de/sites/default/files/media/dokumente/koalitionsvertrag.pdf.

6 Koalitionsvertrag für die 18. Legislaturperiode, S. 104, https://www.cdu.de/sites/default/files/media/dokumente/koalitionsvertrag.pdf.

Der Entwurf sieht Änderungen in fünf verschiedenen Themenfeldern vor:

1. Verbesserung der IT-Sicherheit bei Unternehmen – insbesondere bei kritischen Infrastrukturen

Betreiber kritischer Infrastrukturen sollen verpflichtet werden, binnen zwei Jahren nach Inkrafttreten der Rechtsverordnung angemessene organisatorische und technische Vorkehrungen und sonstige Maßnahmen zum Schutz derjenigen informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Diese Vorkehrungen sollen dann mindestens alle zwei Jahre hinsichtlich der Erfüllung der Anforderungen einer Überprüfung unterzogen werden. Das Gesetz spricht insoweit von der Möglichkeit, die Anforderungen auf geeignete Weise nachzuweisen. Als gangbare Möglichkeit werden Sicherheitsaudits, Prüfungen und Zertifizierungen genannt[7].

Nach § 8b Abs. 5 BSIG-E sind Betreiber kritischer Infrastrukturen nur dann unter Nennung des Betreibernamens unverzüglich zu einer Meldung an das BSI verpflichtet, wenn die Beeinträchtigung der informationstechnischen Systeme, Komponenten oder Prozesse zu einem Ausfall oder einer Beeinträchtigung der Kritischen Infrastruktur führen würde.

Nach § 8b Abs. 4 BSIG-E kann die Meldung durch die Betreiber kritischer Infrastrukturen anonym erfolgen, soweit die Beeinträchtigungen der informationstechnischen Systeme, Komponenten oder Prozesse (lediglich) Auswirkungen auf ihre eigene Funktionsfähigkeit haben können. Angaben zu den technischen Rahmenbedingungen sowie zur Branche des Betreibers müssen jedoch enthalten sein.

2. Schutz der Bürgerinnen und Bürger in einem sicheren Netz

Der angestrebte Schutz soll unter anderem durch die Erhöhung der Sicherheitsstandards bei öffentlichen Telekommunikationsnetzen und den Anbietern von Telemediendiensten erreicht werden[8]. Zusätzlich sollen Telekommunikationsanbieter nicht nur über Cyberangriffe informieren, sondern die Nutzer auch mit Lösungsvorschlägen zur Behebung bzw. Abwehr des Angriffs versorgen. Konkrete, zumindest beispielhaft genannte Erläuterungen wie diese Doppelstrategie in der Praxis aussehen kann, enthält der Entwurf nicht. Als weiteres Element, den Schutz der Bürger in diesem Bereich voranzutreiben, sollen Telemediendiensteanbieter ihren Nutzern sichere Authentifizierungsverfahren anbieten.

3. Schutz der IT des Bundes

Um auch die Bundesregierung selbst stärker in die Pflicht zu nehmen und als Reaktion auf die quantitativ wie qualitativ zugenommenen Angriffe auf Regierungsnetze, sieht der Entwurf eine Erweiterung der Möglichkeiten für verbindliche Vorgaben für die IT des Bundes durch das BSI vor. Hierzu wird die bestehende Regelung für die Regierungsnetze auf die IT des Bundes als Ganzes ausgeweitet.

4. Stärkung des BSI

Der gewachsenen Bedeutung des BSI soll unter anderem durch eine klarere Regelung seiner Warnbefugnisse und seine Etablierung als internationale Zentralstelle Rechnung getragen werden. Um die Erfüllung der im Gesetz vorgesehenen Aufgaben erfolgreich zu verwirklichen, sieht der Entwurf beim BSI einen zusätzlichen Aufwand von insgesamt 133 zusätzlichen Planstellen vor. Weiterhin geht der Entwurf davon aus, dass für die Wahrnehmung der Aufgabe als zentrale Meldestelle für die Sicherheit in der Informationstechnik für die Betreiber kritischer Infrastrukturen der Ausbau des BSI-Lagezentrums auf einen 24/7 Betrieb unausweichlich sein wird[9].

5. Zuständigkeitserweiterung des BKA

Die bestehende Zuständigkeit des Bundeskriminalamts für die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung soll im Bereich der Cyberdelikte ausgeweitet werden. Gerade bei Angriffen auf bundesweite Einrichtungen sei eine solche klare Zuständigkeitsregelung notwendig. Konkret wird die Zuständigkeit des Bundeskriminalamts für die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung über die bereits bestehende Zuständigkeit für Straftaten nach § 303b StGB (Computersabotage) hinaus auf Straftaten nach den §§ 202a, 202b, 202c, 263a und 303a StGB ausgedehnt.

IV. Kritik

Obwohl der Referentenentwurf des BMI zunächst innerhalb der Bundesregierung abgestimmt und darauf folgend den beteiligten Kreisen für eine weitere Diskussion überlassen werden soll, hat er bereits unmittelbar nach seiner Veröffentlichung verschiedenste Stellen und Verbände zu ersten Stellungnahmen animiert.

Der BITKOM begrüßt generell die Verbesserungen am IT-Sicherheitsgesetz und nimmt es wohlwollend zur Kenntnis, dass in Bezug auf die Meldepflicht von schwerwiegenden IT-Sicherheitsvorfällen die Hinweise der IT-Industrie weitgehend berücksichtigt worden seien, und bewertet es positiv, dass die Wirtschaft in die konkrete Ausgestaltung des Gesetzes einbezogen werden soll[10].

Die Planungssicherheit sieht der BITKOM hinsichtlich der Frage des Adressatenkreises nachteilig betroffen und wünscht sich hier mehr Klarheit darüber, welche Unternehmen das geplante Gesetz adressieren soll. Darüber hinaus wird angeregt, kleinen und mittelständischen Unternehmen beim Aufspüren von Sicherheitslücken eine bessere Unterstützung zuteil werden zu lassen. Die Forderung nach Anwendung derselben, im Entwurf geforderten Meldepflichten und Sicherheitsstandards

7 Gesetzesbegründung zum Entwurf, Seite 13.

8 Infoblatt des BMI zum IT-Sicherheitsgesetz, S. 2, http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Infoblatt_IT-Sicherheitsgesetz.pdf?__blob=publicationFile.

9 Referentenentwurf des BMI zum IT-Sicherheitsgesetz, S. 5.

10 BITKOM, http://www.bitkom.org/files/documents/BITKOM-Presseinfo_Entwurf_IT-Sicherheitsgesetz_19_08_2014.pdf.

auch für den Staat stützt der BITKOM darauf, dass dieser der größte Betreiber kritischer Infrastrukturen sei.

Der BITKOM rechnet vor, dass die beabsichtigte Meldepflicht für schwere IT-Sicherheitsfälle für die deutsche Wirtschaft Kosten in Höhe von bis zu 1,1 Milliarden Euro pro Jahr verursachen dürfte. Ausgaben für die Einhaltung höherer Sicherheitsstandards in dreistelliger Millionenhöhe kämen hinzu.

Eine extrem detaillierte Betrachtung der Kosten hatte auch der Bundesverband der Deutschen Industrie e.V (BDI) bereits nach Erscheinen des Referentenentwurfs vom 12. März 2013 in seiner von der KPMG durchgeführten Studie „IT-Sicherheit in Deutschland. Handlungsempfehlungen für eine zielorientierte Umsetzung des IT-Sicherheitsgesetzes" aufgestellt[11]. In seinem Positionspapier[12] „Erwartungen der deutschen Industrie an ein IT-Sicherheitsgesetz" gelangt der BDI zu einem niederschmetternden Ergebnis:

„Der BDI setzt sich nachdrücklich für eine Stärkung der IT-Sicherheit, den Ausbau des staatlichen IT-Lagebilds sowie für einen verbesserten Informationsaustausch zwischen Industrie und Amtsseite ein. Nach Auffassung der deutschen Industrie wird das IT-Sicherheitsgesetz (ITSiG) keines dieser Ziele erreichen."

Der Verband der deutschen Internetwirtschaft e.V. (eco)[13] befürwortet nach eigenen Angaben grundsätzlich die Pläne des Innenministers, Deutschland zum führenden Standort im Bereich IT-Sicherheit auszubauen, rät jedoch davon ab, ein IT-Sicherheitsgesetz als nationalen Alleingang auszugestalten. Nationale Alleingänge seien nicht hilfreich, wenn die im Entwurf genannten Betreiber kritischer Infrastrukturen teilweise europa- bzw. weltweit tätig seien. Die Bundesregierung sollte besser eine europaweite Regelung im Rahmen der geplanten NIS-Richtlinie[14] anstreben, um den betroffenen Unternehmen unnötig hohe Kosten zu ersparen.

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) stört sich daran, dass dem Gesetzentwurf nur beiläufig zu entnehmen sei, dass der Schutz des allgemeinen Persönlichkeitsrechts allgemein und des Datenschutzes speziell ein zentrales Anliegen von IT-Sicherheit ist. Mehr IT-Sicherheit gehe nicht ohne die Einbeziehung und Stärkung der unabhängigen Datenschutzbeauftragten[15].

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. glaubt daran, dass der auf kritische IT-Strukturen ausgerichtete Gesetzesentwurf insgesamt zur Steigerung der IT-Sicherheit und damit zum Schutz der personenbezogenen Daten der Bürgerinnen und Bürger in Deutschland beitragen kann, und verweist als Beleg darauf, dass die Einführung von Meldepflichten sich im Bereich von Datenschutzverletzungen als Arbeitsinstrument bewährt hat[16].

Die Ausführung des Referentenentwurfs hinsichtlich des prognostizierten Mehraufwands durch Erfüllungskosten sieht zwar auch der BvD, ergänzt jedoch richtigerweise, dass dies faktisch nur dort zu Mehrkosten führen wird, wo bislang noch kein hinreichendes Niveau an IT-Sicherheit bzw. keine entsprechenden Meldewege etabliert sind. Weiter gibt der BvD zu bedenken, dass bei der Etablierung von Mitteilungspflichten der Verfassungsgrundsatz, dass sich niemand selbst belasten muss, Berücksichtigung finden muss.

Der Umstand, dass der Entwurf eine weitere gesetzgeberische Aktivität zum Schutz der Daten der Bürgerinnen und Bürger vermissen lässt, sieht der BvD als einen der Kritikpunkte an dem Entwurf. Als weiterer Kritikpunkt werden die neuen gesetzlichen Befugnisse zum Speichern und Verarbeiten von Nutzerdaten gesehen, die sich im Entwurf im Bereich der Neuerungen zum TMG verbergen. Mit der Kritik, in dem jetzigen Gesetzentwurf werde für jeden Anbieter von Telemediendiensten die Möglichkeit geschaffen, Nutzerdaten in erheblicher Menge vorsorglich zu erheben und zu speichern, steht der BvD nicht allein.

Sowohl der Arbeitskreis Vorratsdatenspeicherung[17] als auch die Piraten[18] haben die Sorge, dass mit dem geplanten Vorhaben bei allen Anbietern von Telemediendiensten Strukturen zum Vorhalten von umfangreichen Nutzerdaten geschaffen werden. Der sich im Gesetzentwurf befindliche Gedanke, Daten von Nutzern zum Erkennen von Störungen zu erheben, entspreche dem Gedanken der Vorratsdatenspeicherung. Unabdingbar seien dafür jedoch strenge Regelungen zur Zweckbindung dieser Daten und die zeitliche Befristung der Erhebung und Verwendung.

V. Gemeinsamer Kritikpunkt: „Versteckte Vorratsdatenspeicherung" (?)

Die Befürchtung einer „versteckten Vorratsdatenspeicherung" wird von diversen Beteiligten geäußert, so dass es sich lohnt, diesen Aspekt noch näher zu beleuchten. Die Gemüter erhitzen sich dabei an den geplanten Änderungen zum Telemediengesetz. Konkret sieht der Entwurf eine neue Regelung in Form des § 15 Abs. 9 TMG-E vor[19].

„Soweit erforderlich, darf der Diensteanbieter Nutzungsdaten zum Erkennen, Eingrenzen oder Beseitigen von Störungen seiner für Zwecke seines Telemedienangebotes genutzten technischen Einrichtungen erheben und verwenden. Absatz 8 Satz 2 gilt entsprechend."

Als Begründung für die geplante Einführung dieser Norm nennt der Gesetzgeber folgende Erwägung:

11 Studie des BDI: http://www.bdi.eu/download_content/SicherheitUndVerteidigung/Anlage_Studie_BDI_Final.pdf.

12 Positionspapier der BDI vom 25.08.2014 „Erwartungen der deutschen Industrie an ein IT-Sicherheitsgesetz", http://www.bdi.eu/download_content/SicherheitUndVerteidigung/Positionspapier_Sicherheitsgesetz_25_02.pdf.

13 Positionspapier des eco e.V. zum IT-Sicherheitsgesetz: http://www.eco.de/2014/news/eco-lehnt-it-sicherheitsgesetz-als-nationalen-alleingang-ab.html.

14 Europäische Kommission: COM(2013) 48 final: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_de.pdf.

15 ULD, https://www.datenschutzzentrum.de/presse/20140820-it-sicherheitsgesetz.htm.

16 Pressemitteilung BvD e.V. vom 22.08.2014 https://www.bvdnet.de/system-ordner/tt-news/detailansicht/article/bvd-unterstuetzt-it-sicherheitsgesetz-grundsaetzlich-und-regt-verbesserungen-an.html.

17 AK Vorratsdatenspeicherung: http://www.vorratsdatenspeicherung.de/content/view/748/79/.

18 Piraten Partei: https://www.piratenpartei.de/2014/08/21/it-sicherheitsgesetz-bka-carepaket-enthaelt-auch-vorratsdatenspeicherung/.

19 Referentenentwurf des BMI zum IT-Sicherheitsgesetz, S. 18.

„Diensteanbieter müssen die Möglichkeit haben, eine Infektion der von ihnen angebotenen Telemedien mit Schadprogrammen zu erkennen, um entsprechende Schutzmaßnahmen ergreifen zu können. Hier bestand bislang eine Lücke im Bereich der Erlaubnistatbestände des Telemediengesetzes, denn auch die Telemedienanbieter brauchen eine entsprechende Ermächtigung, beispielsweise um Angriffe (Denial of Service, Schadprogramme, Veränderung ihrer Werbeangebote von außerhalb) abwehren zu können. Zur Erkennung und Abwehr bestimmter Angriffe gegen Webseiten und andere Telemedien ist die Erhebung und kurzfristige Speicherung und Auswertung der Nutzungsdaten erforderlich. Diese soll durch den neuen § 15 Absatz 9 TMG, der sich an § 100 Absatz 1 TKG anlehnt, geschaffen werden. Dabei ist auch eine Weiterentwicklung der Angriffsmethoden zu berücksichtigen."

Nimmt man zur Kenntnis, dass gem. § 15 Abs. 1 TMG zu den in der Regelung erwähnten Nutzungsdaten „Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemedien" gehören, die nach der Gesetzesbegründung erhoben und gespeichert werden sollen, ist es keine große Überraschung, dass der erste reflexartige Gedanke in Richtung Vorratsdatenspeicherung geht.

Richtigerweise kommen Teile der Blogosphäre hier zum Schluss, dass bei der Formulierung „Erkennen von Störungen" eine proaktive Speicherung der Daten gemeint sein muss und die Diensteanbieter mit der Speicherung nicht so lange warten müssen, bis ein Angriff stattgefunden hat und seine Auswirkungen eingetreten sind[20].

Ob sich der Vorwurf einer versteckten Vorratsdatenspeicherung auch nach der ersten Aufregung um die geplante Änderung langfristig halten wird, wird sicher davon abhängen, welcher Zeitraum sich hinter der Angabe „kurzfristig" verbirgt. Einen Fingerzeig, welche Fristen in diesem Bereich tolerierbar sein könnten, dürfte jüngst der BGH gegeben haben, der bei der Speicherung von dynamischen IP-Adressen 7 Tage als unbedenklich einstufte[21]. Die teilweise vorgetragene Kritik, dass „der IT-Gesetzesentwurf keine Speicherfristen vorsehe", scheint zumindest an dieser Stelle etwas voreilig und ungenau[22].

VI. Fazit

Die Zahlen sprechen dafür, dass die Einführung eines IT-Sicherheitsgesetzes nicht nur eine gute Idee, sondern eine erforderliche staatliche Maßnahme darstellt.

Die Durchdringung des Gemeinwesens und die Abhängigkeit des Gemeinwesens von einer funktionierenden und sicheren IT-Landschaft kann durch Zahlen des Statistischen Bundesamts und anderer Institutionen und Verbände gut nachgewiesen werden.

87 % der deutschen Unternehmen nutzen einen Internetzugang, wobei 37 % der Unternehmen den direkten Kontakt zu den Kunden über soziale Medien suchen[23]. Allein auf Cloud-Dienste soll eine Bruttowertschöpfung von 78,8 Mrd. EUR entfallen[24]. In Deutschland würden zwar 26 Prozent der Menschen ihren Fernseher weggeben, aber nur 14 Prozent ihr Smartphone[25], wobei 76 % der Deutschen auf einen privaten Internetanschluss zurückgreifen können. 50,4 Millionen Menschen besitzen in Deutschland ein Smartphone. Ein Leben ohne Internet scheint ohne Aufgabe der lieb gewordenen Lebensweise kaum vorstellbar und würde zudem viele wirtschaftliche Prozesse erschweren.

Die IT des Bundes stärker zu schützen, erscheint ebenfalls konsequent wie sinnvoll. Informationstechnik und Kommunikation eröffnen auch in diesem Bereich neue Möglichkeiten und müssen im Bereich der Verwaltung weiter modernisiert werden, um mit der Privatwirtschaft Schritt zu halten. Allein die steigende Zahl der Computer- und Internetkriminalität[26] und der gezielten Angriffe auf IT-Systeme[27] zeigt die Notwendigkeit, den Schutz dieser Systeme als wichtigen Bestandteil einer digitalen Agenda zu führen.

Wenn der Bundesinnenminister zum Gesetzesentwurf erklärt: „Wir müssen sicherer werden als bisher. Wer ein Risiko setzt für andere, trägt dafür auch die Verantwortung. Wer Kritische Infrastrukturen betreibt[28]", der muss sie sicher betreiben ", dann trifft er den Kern dieses Erfordernisses.

Was für andere wichtige Dinge zur Förderung und Aufrechterhaltung des Gemeinwesens gilt, muss auch für die IT-Sicherheit gelten. Eine schnelle Infrastruktur in Form von Breitbandnetzen ist nicht weniger wichtig für das wirtschaftliche Wachstum als der Ausbau und die Wartung von Autobahnen. Wer eine Gefahr auf dieser Autobahn in Form einer Baustelle für andere Verkehrsteilnehmer schafft, muss natürlich Sorge dafür tragen, dass Dritte keinen Schaden nehmen.

Wenn der Betreiber eines Kernkraftwerks sich gegen Katastrophenszenarien wappnen und mit dem Katastrophenschutz beschäftigen sollte, warum sollten sich Betreiber von kritischen Infrastrukturen nicht mit Szenarien beschäftigen, die sowohl die Datensicherheit als auch den Datenschutz betreffen? Die Forderung des Bundesinnenministers scheint also eine Übertragung der sonst üblichen Verkehrssicherungspflichten vom Analogen ins Digitale zu sein.

Allein an Ungenauigkeiten und Ungereimtheiten des Entwurfs, die bereits in den ersten Stellungnahmen anklingen,

20 Delegedata.de, http://www.delegedata.de/2014/08/it-sicherheitsgesetz-telemedienanbieter-duerfen-anlasslos-speichern/.

21 BGH Az.: III ZR 391/13, http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&nr=68350&Blank=1.pdf.

22 Piraten Partei: https://www.piratenpartei.de/2014/08/21/it-sicherheitsgesetz-bka-carepaket-enthaelt-auch-vorratsdatenspeicherung/

23 Statistisches Jahrbuch 2013, S. 513.

24 BITKOM, http://www.bitkom.org/files/documents/BITKOM_PK_Industrie_4.0_07_04_2014.pdf.

25 SPON: http://www.spiegel.de/netzwelt/web/studie-deutsche-verzichten-lieber-auf-fernseher-als-auf-smartphone-a-979244.html.

26 BITKOM, http://www.bitkom.org/de/presse/8477_79284.aspx.

27 BKA, Bundeslagebild Cybercrime 2013, S. 5, http://www.bka.de/nn_224082/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2013,templateId=raw,property=publicationFile.pdf/cybercrimeBundeslagebild2013.pdf.

28 Pressemitteilung BMI, http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2014/08/einleitung-ressortabstimmung-it-sicherheitsgesetz.html.

dürfte noch zu arbeiten sein. Unsicherheiten scheinen dahingehend zu bestehen, dass Unternehmen nicht genau einschätzen können, ob sie als Betreiber einer kritischen Infrastruktur in Frage kommen. Die im Rahmen einer Verordnung geplante Regelung könnte hier Abhilfe schaffen. Leichte Zweifel ruft ebenfalls die Frage auf, wie realistisch es sein kann, dass die Unternehmen von der Möglichkeit einer anonymen Meldung beim BSI Gebrauch machen?

Sind die vorgesehenen zwei Jahre, die den Unternehmen für die Festlegung von Mindeststandards für die jeweilige Branche eingeräumt werden, und die das BSI dann absegnen soll, in einer Zeit der rasanten Weiterentwicklung im Bereich der IT-Sicherheit nicht zu lang?

Auch wenn die Zweckbindung bei § 15 Abs. 7 TMG-E gegeben ist, die auf das Erkennen und die Abwehr von Störungen beschränkt sein soll, müssen nicht Vorkehrungen getroffen werden, um eine spätere zweckfremde Verwendung bspw. durch Sicherheitsbehörden auszuschließen?

Diese und andere Fragen werden in einer breiten öffentlichen Debatte zu erörtern sein, um die vom BMI gewünschten wirksamen und sachgerechten Lösungen im Hinblick auf das geplante IT-Sicherheitsgesetz zu finden.

Rechtsprechung

Recht auf Vergessen in Suchmaschinen (Ls)

(**Europäischer Gerichtshof**, Urteil vom 15. Mai 2014 – C-131/12 – Google Spain und Google)

1. **Art. 2 Buchst. b und d der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ist dahin auszulegen, dass die Tätigkeit einer Suchmaschine, die darin besteht, von Dritten ins Internet gestellte oder dort veröffentlichte Informationen zu finden, automatisch zu indexieren, vorübergehend zu speichern und schließlich den Internetnutzern in einer bestimmten Rangfolge zur Verfügung zu stellen, sofern die Informationen personenbezogene Daten enthalten, als „Verarbeitung personenbezogener Daten" im Sinne von Art. 2 Buchst. b der Richtlinie 95/46 einzustufen ist und dass der Betreiber dieser Suchmaschinen als für diese Verarbeitung „Verantwortlicher" im Sinne von Art. 2 Buchst. d der Richtlinie 95/46 anzusehen ist.**

2. **Art. 4 Abs. 1 Buchst. a der Richtlinie 95/46 ist dahin auszulegen, dass im Sinne dieser Bestimmung eine Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung ausgeführt wird, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet eines Mitgliedstaats besitzt, wenn der Suchmaschinenbetreiber in einem Mitgliedstaat für die Förderung des Verkaufs der Werbeflächen der Suchmaschine und diesen Verkauf selbst eine Zweigniederlassung oder Tochtergesellschaft gründet, deren Tätigkeit auf die Einwohner dieses Staates ausgerichtet ist.**

3. **Art. 12 Buchst. b und Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46 sind dahin auszulegen, dass der Suchmaschinenbetreiber zur Wahrung der in diesen Bestimmungen vorgesehenen Rechte, sofern deren Voraussetzungen erfüllt sind, dazu verpflichtet ist, von der Ergebnisliste, die im Anschluss an eine anhand des Namens einer Person durchgeführte Suche angezeigt wird, Links zu von Dritten veröffentlichten Internetseiten mit Informationen zu dieser Person zu entfernen, auch wenn der Name oder die Informationen auf diesen Internetseiten nicht vorher oder gleichzeitig gelöscht werden, und gegebenenfalls auch dann, wenn ihre Veröffentlichung auf den Internetseiten als solche rechtmäßig ist.**

4. **Art. 12 Buchst. b und Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46 sind dahin auszulegen, dass im Rahmen der Beurteilung der Anwendungsvoraussetzungen dieser Bestimmungen u.a. zu prüfen ist, ob die betroffene Person ein Recht darauf hat, dass die Information über sie zum gegenwärtigen Zeitpunkt nicht mehr durch eine Ergebnisliste, die im Anschluss an eine anhand ihres Namens durchgeführte Suche angezeigt wird, mit ihrem Namen in Verbindung gebracht wird, wobei die Feststellung eines solchen Rechts nicht voraussetzt, dass der betroffenen Person durch die Einbeziehung der betreffenden Information in die Ergebnisliste ein Schaden entsteht. Da die betroffene Person in Anbetracht ihrer Grundrechte aus den Art. 7 und 8 der Charta verlangen kann, dass die betreffende Information der breiten Öffentlichkeit nicht mehr durch Einbeziehung in eine derartige Ergebnisliste zur Verfügung gestellt wird, überwiegen diese Rechte grundsätzlich nicht nur gegenüber dem wirtschaftlichen Interesse des Suchmaschinenbetreibers, sondern auch gegenüber dem Interesse der breiten Öffentlichkeit am**