Humanistische Union

Das neue IT-Sicherheitsgesetz – bürgerrechtliche Positionen (vollständig)

aus: vorgänge Nr. 209 (Heft 1/2015), S. 80-84

(Red.) Am 12. Juni 2015 verabschiedete der Deutsche Bundestag das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme – kurz IT-Sicherheitsgesetz. [1] Das Gesetz schreibt neue Pflichten und Mindeststandards für Betreiber kritischer Infrastrukturen fest. Provider werden verpflichtet, ihre Infrastruktur nach dem „Stand der Technik" vor Angriffen zu schützen und erhebliche Störungen zu melden.

An dem Entwurf des IT-Sicherheitsgesetz gab es viel Kritik, auch aus bürgerrechtlicher Sicht. Stefan Hügel fasst die kritischen Anmerkungen zusammen.

Datenspeicherung zur Abwehr von Angriffen

Das Gesetz sieht unter anderem vor, dass Provider zur Abwehr von Angriffen weitgehende Befugnisse zur Analyse der Kommunikation ihrer Kundinnen und Kunden erhalten. Die bisherige Befugnis aus § 100 Telekommunikationsgesetz (TKG) wurde ausgeweitet und führt zu einer dauerhaften, flächendeckenden und alle Inhalte betreffenden Überwachung der gesamten Telekommunikation. Das *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF)* hatte vor der Verabschiedung in seiner Stellungnahme diese Regelung als einen Verstoß gegen Artikel 10 Grundgesetz und damit klar verfassungswidrig bezeichnet [4,7]. Der Kritik haben sich auch Sachverständige in der öffentlichen Anhörung zum Gesetzentwurf angeschlossen.

Gleichzeitig verbietet bisher § 15 Telemediengesetz (TMG) die Verarbeitung von IP-Adressen für Zwecke der IT-Sicherheit. Damit können Betreiber von Web-Angeboten keine legalen Maßnahmen ergreifen, um Angriffe zu erkennen, zurückzuverfolgen und Angreifer zu identifizieren. Eine solche Maßnahme ist nur für IT-Systeme des Bundes zulässig (§ 5 BSIG). Daran hat sich mit dem neuen Gesetz nichts geändert.

Im Ergebnis steht einer verfassungswidrigen Überwachungsbefugnis nach TKG ein juristisches Vakuum beim Schutz von Telemedienanbietern nach TMG entgegen. Erforderlich wären stattdessen einheitliche verfassungskonforme Regeln für den Einsatz von IT-Sicherheitssystemen im Telekommunikations- und Telemediensektor. Initiativen zum Schutz der privaten Endnutzer.innen durch angemessenen Umgang mit fahrlässig implementierten Systemen und nicht wirksam beseitigten Sicherheitslücken fehlen.

Sonderregelungen für die IT des Bundes

Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) hat die Befugnis, ausschließlich bei der IT des Bundes IT-Sicherheitssysteme nach dem Stand der Technik einzusetzen (§ 5 BSIG). Dies wird durch neue Befugnisse für das BKA verstärkt ([1], Artikel 7). Weiterhin sorgt demnach die Bundesregierung lediglich für den Schutz der IT-Systeme des Bundes und überlässt die IT-Systeme der Bürgerinnen und Bürger und der Wirtschaft sich selbst. Dafür gibt es neue Befugnisse für das Bundeskriminalamt (BKA) und

eine Abteilung, die Straftaten gegen die IT des Bundes und gegen kritische Infrastrukturen verfolgt.

Der Chaos Computer Club (CCC) stellt dazu in seiner Stellungnahme [6] fest: Der Gesetzentwurf vernachlässige insgesamt die Interessen aller normalen Nutzer_innen und enthalte keinerlei Initiativen oder Ansätze, deren Situation zu verbessern. Bei Privatpersonen und den ihnen entstehenden Schäden durch mangelnde IT-Sicherheit solle offenbar alles so bleiben, wie es derzeit ist.

Ausbau der Geheimdienste und die Rolle des BSI

Die in dem Gesetz vorgesehenen zusätzlichen Ressourcen für die IT-Sicherheit sind grundsätzlich positiv zu bewerten. Das Gesetz [1] sieht neue Planstellen für das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bundeskriminalamt (BKA) und das Bundesamt für Verfassungsschutz vor. Besser wäre es jedoch stattdessen gewesen, Sachkompetenz beim BSI zu bündeln anstatt durch Ausbau des Verfassungsschutzes nachrichtendienstliche Ausforschung weiter voranzutreiben.

Zusätzlich ist eine Änderung der Rolle und der organisatorischen Einordnung des BSI notwendig. Das BSI ist laut Gesetz zuständig für die Informationssicherheit auf nationaler Ebene ([1], Artikel 1 (1)). Das FIfF begrüßt dies in seiner Stellungnahme, kritisiert aber die Umsetzung. Das BSI muss als eine nationale Bundesoberbehörde organisiert werden, die nicht dem BMI oder einer anderen Bundesbehörde unterstellt ist. Auch der Chaos Computer Club fordert in seiner Stellungnahme [6], dass das BSI in eine vom Innenministerium unabhängige Bundesbehörde mit klarem Sicherheitsauftrag umgewandelt wird. Die Mitwirkung des BSI an staatlicher Schadsoftware („Staatstrojaner“) habe die Vertrauenswürdigkeit des Amts untergraben. Ein Missbrauch des dort anfallenden Wissens über Angriffstechniken sei nicht auszuschließen.

Meldepflicht

Das Gesetz sieht eine Meldepflicht bei Sicherheitsvorfällen in kritischen Infrastrukturen vor:

> *„Betreiber kritischer Infrastrukturen haben erhebliche Störungen … die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können oder bereits geführt haben, … unverzüglich an das Bundesamt zu melden. … Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat.“ (Artikel 1 (7); s.a. [1]).*

Diese Meldepflicht entsteht erst nachträglich, wenn es bereits zu schweren Beeinträchtigungen oder dem Ausfall kritischer Infrastrukturen gekommen ist. Netzpolitik.org [3] bezweifelt, ob eine nachträgliche Meldepflicht für die rechtzeitige Einleitung von Schutzmaßnahmen ausreichend ist, beispielsweise wenn Angriffe parallel erfolgen, und ob eine nachholende Aufklärung der Öffentlichkeit in Form von Lagebildern anstatt einer obligatorischen und rechtzeitigen Aufklärung Betroffener ausreicht.

Bürokratie statt Sicherheit

Nicht eine einzige der im Gesetzesentwurf vorgeschlagenen Maßnahmen ist zielführend, um die IT-Sicherheit tatsächlich zu erhöhen, urteilt der Chaos Computer Club [6]. Man habe offenbar ein Verständnis von IT-Sicherheit in ein Gesetz gegossen, wonach lediglich durch mehr verpflichtende Dokumentations- und Berichtsregularien und Checklisten in den Unternehmen wirksame Verbesserungen herbeigeführt werden könnten. Doch der nun vorgesehene enorme Bürokratieaufwand ist nicht nur zeitaufwendig und in der Sache nutzlos, sondern hält auch noch die an einer wirksamen IT-Sicherheit Arbeitenden von wirklich sinnvollen Maßnahmen ab.

Weitere Kritikpunkte

Weitere Kritikpunkte am Gesetz sind [3,6,7]:

- Es fehlen klare Begriffsdefinitionen: „Kritische Infrastrukturen“ sind beispielsweise Infrastrukturen, die für die Versorgung mit Wasser, Energie, Telekommunikation genutzt werden – darunter fallen geschätzt etwa 2000 Unternehmen in Deutschland. Ab wann – beispielsweise ab welcher Größe – ein Unternehmen aber genau darunter fällt, ist nicht klar. Ein positiver Punkt ist, dass nun auch kerntechnische Anlagen darunter fallen – diese waren zuvor aus der Debatte herausgehalten worden.
- Ebenso ist der „Stand der Technik“ keine klare Perspektive – DIN und ISO arbeiten an neuen Standards, hier ist bereits jetzt Bedarf an Nachbesserung zu erwarten. Besser wäre hier aktives Gestalten gewesen, anstatt nur zu reagieren. Der Chaos Computer Club stellt zusätzlich fest, dass die Festlegung auf den „Stand der Technik“ proaktive Verbesserungen der Schutzvorkehrungen ausschließt.
- Kritisiert wird auch die Begrenzung des Gesetzes auf kritische Infrastrukturen selbst: Eine große Zahl von Angriffen auf – für sich genommen – nicht kritische Infrastrukturen können in der Summe ebenfalls kritische Auswirkungen haben, wenn z.B. eine große Anzahl von Unternehmen oder Behörden gleichzeitig angegriffen wird.

Forderungen

- Aus Sicht des FIfF wären die umzusetzenden rechtlichen Mindestvoraussetzungen für einen wirksamen Grundrechtsschutz [4]:
-
- 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 Beratungskapaztäten bei einem BSI, das zu organisieren

ist als eine von Weisungen unabhängige Behörde vergleichbar dem Bundesrechnungshof (BRH),
- Anpassung der Strafbarkeit des Bruchs des Fernmeldegeheimnisses(§ 206 StGB) an die Vorgaben von Grundgesetz und Bundesverfassungsgericht.
-

Abschließend urteilt das FIfF: Der Gesetzentwurf bewirkt keinerlei Verbesserung der IT-Sicherheit, sondern untergräbt stattdessen das vom Bundesverfassungsgericht festgestellte *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* in Deutschland.
Leider blieben die wesentlichen Kritikpunkte bei der Verabschiedung am 12. Juni 2015 unbeachtet. Am Fazit [7] hat sich also nichts geändert: *Schutz von Grundrechten* nicht in Sicht. Erneut wurde eine Chance vertan, effektive gesetzliche Grundlagen für IT-Sicherheit in Deutschland zu schaffen.

Referenzen

[1] Deutscher Bundestag (2015): Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), BT-Drs. 18/4096 v. 25.02.2015, http://dip21.bundestag.de/dip21/btd/18/040/1804096.pdf.

[2] AK Vorratsdatenspeicherung (2015): IT-Sicherheitsgesetz: AK Vorrat gegen verdeckte Vorratsdatenspeicherung. Pressemitteilung vom 4. Mai 2015, http://www.vorratsdatenspeicherung.de/content/view/756/135/lang,de/

[3] Anna Biselli, netzpolitik.org (2015): Heute im Bundestag Verabschiedung des IT-Sicherheitsgesetzes – ein Überblick, 12. Juni 2015, https://netzpolitik.org/2015/heute-im-bundestag-verabschied ung-des-it-sicherheitsgesetzes-ein-ueberblick/

[4] FIfF e.V. (2015): Stellungnahme des FIfF zum IT-Sicherheitsgesetz der Bundesregierung vom 17.12.2014, http://cyberpeace.fiff.de/Uploads/Uploads/FIfF_Stellungnahme_IT-Sicherheitsgesetz. pdf.

[5] Rainer W. Gerling (2015): Synopse Entwürfe IT-Sicherheitsgesetz, Stand 12.6.2015, http://www.rain er-gerling.de/PDF/Synopse_IT-Sicherheitsgesetz_2015_final.pdf

[6] Linus Neumann, Chaos Computer Club (2015): Stellungnahme zum Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), 17. April 2015, http://ccc.de/system/ uploads/186/original/ITSG_Stellungnahme.pdf

[7] Ingo Ruhmann (2015): Schutz von Grundrechten nicht in Sicht. FIfF-Kommunikation 1/2015, http://www.fiff.de/publikationen/fiff-kommunikation/fk-2015/fk-2015-1/fk-1-15-s10.pdf

STEFAN HÜGEL *ist Vorsitzender des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) und Mitglied der Humanistischen Union in Frankfurt am Main.*
