Die öffentliche Anhörung des Innenausschusses zum Thema „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetzt)“

Alexander Lüdke
MatrNr. 548965

Nils Brandt
MatrNr. 549906

Abstract

Das folgende Dokument ist als Beleg anzusehen, welches für den Studiengang Angewandte Informatik im Fach Datenschutz und Datensicherheit erstellt wurde. Es befasst sich hauptsächlich mit dem Inhalten der öffentlichen Anhörung des deutschen Bundestages zum Thema „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ und der damit einhergehenden Argumentation der Sachverständige. Da der Umfang dieser Ausarbeitung die zwei Seiten nicht überschreiten darf, nehmen die Autoren einen Teilaspekt der Anhörung und werden diesen, durch ausgiebige Recherchen, näher beleuchten.

1 Einleitung

Die Digitalisierung in Staat, Wirtschaft und Gesellschaft hat Deutschland in nur wenigen Jahren grundlegend verändert. Neue Möglichkeiten der Kommunikation, des Wissenszugangs und der innovativen Gestaltung führen zu mehr sozialer Interaktion, neuen Geschäftsmodellen und neuen Feldern für Forschung und Entwicklung. Vernetzte elektronische Geräte prägen verstärkt den Lebens- und Arbeitsalltag der Menschen.

Der Staat hat die Pflicht, diese Veränderungsprozesse im Interesse der Bürgerinnen und Bürger gemeinsam mit der Wirtschaft und weiteren Akteuren zu bewerten, aktiv zu gestalten und Rahmenbedingungen zu schaffen, um diese Veränderungsprozesse weiterzuentwickeln. [BMI] Eines dieser Entwicklungswerkzeuge ist das beschließen von Gesetzten.

2 Vom Entwurf zum Gesetz

Gegenstand der öffentlichen Anhörung war der von der Bundesregierung vorgelegte Gesetzentwurf [Bun15], der das IT -Sicherheitsgesetzt anpassen bzw. erweitern sollte und dabei die Erhöhung der Sicherheit informationstechnischer Systeme zum Gegenstand hatte.

> „Die vorgesehenen Neuregelungen dienen dazu, [...] um den aktuellen und zukünftigen Gefährdungen der IT-Sicherheit wirksam begegnen zu können. Ziel des Gesetzes sind die Verbesserung der IT -Sicherheit von Unternehmen, der verstärkte Schutz der Bürgerinnen und Bürger im Internet und in diesem Zusammenhang auch die Stärkung von BSI und Bundeskriminalamt (BKA).“ [Bun15, S. 1]

2.1 Standpukte der Sachverständigen

Um nahezu alle Aspekte dieses Sachverhaltes zu betrachten, wurde im Vorfeld Stellungnahme von unterschiedlichen Personen – bzw. Interessensgruppen eingeholt, die während der Anhörung die Möglichkeit erhielten, diese näher zu erläutern. Die geladenen Sachverständigen waren folgende

- **Iris Plöger**, Bundesverband der Deutschen Industrie e.V., Leiterin der Abteilung Digitalisierung
- **Dipl.-Ing. (FH) Thomas Tschersich**, Deutsche Telekom AG, Leiter Group Security Services
- **Dr. Axel Wehling**, Gesamtverband der Deutschen Versicherungswirtschaft e.V.

Linus Neumann, Chaos Computer Club (CCC), Berlin

Michael Hange, Präsident des Bundesamtes für Sicherheit in der Informationstechnik

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

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

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

Aus den Schilderungen der jeweiligen Sachverständigen traten u.a. die folgenden Punkte in den Vordergrund. Die Stellung der BSI als zentrale Meldestelle. Auf Grund ihrer Zugehörigkeit zum BMI und der damit einhergehenden Verbindung zum BND tritt hier ein gewisses Misstrauen in den Vordergrund. Wie in der Stellungnahme von Herrn Neumann [vlg. Neu15, S. 4] beschreiben, wenn das BSI das Monitoring von kritischen Angriffszielen übernimmt, dann wäre diese eine rein defensive Ausrichtung, was jedoch im Gegensatz zu den offensiven Ambitionen des BMI stehen würde. Hinzu kommt, dass das BSI nach §7a Abs.2 ITSG die aus den Untersuchungen gewonnenen Erkenntnisse nur zur Erfüllung der Aufgaben verwenden darf. Das Bundesamt darf seine Erkenntnisse weitergeben und veröffentlichen, soweit dies zur Erfüllung dieser Aufgaben erforderlich ist. Zuvor ist dem Hersteller der betroffenen Produkte und Systeme mit angemessener Frist Gelegenheit zur Stellungnahme zu geben. Wie bereites durch die Redaktion von Netzpolitik.org festgestellt wurde [Bis15b], liegt die Anwendung des Gesetzestextes aufgrund schwammiger Formulierungen und industriefreundlicher Meldepflichten im Ermessensspielraum der der jeweiligen Unternehmen.

2.2 Datensicherheit

Doch wenn wir die Anhörung aus Sicht der Datensicherheit betrachten, fällt uns auf, dass der Gesetzesentwurf den Fokus auf kritische Infrastrukturen legt und weniger auf die Wirtschaft in form mittelständischen Unternehmen und noch viel weniger auf den einzelnen Endanwender. Dabei sind es diese Benutzerdaten, die typischerweise von größeren Angriffen auf die Anbieter von Online- Diensten, also Online-Shops, E - Mail- Anbieter oder sogenannte Soziale Netzwerke stammen, die in diesem Fall die betroffenen Nutzer nicht ausreichend geschützt und – gedeckt vom BSI – auch nicht über den erfolgten Angriff informiert haben und auch durch das neue Gesetzt nicht gemeldet werden, da die Weitergabe von Informationen aus Sicherheitslücken nach §7a Abs.2 ITSG zeitversetzt weitergegeben werden sollen.

3 Fazit

Aus unserer Sicht reicht es nicht aus eine zentrale Meldestelle in form der BSI festzulegen und der Wirtschaft die Entscheidung zu überlassen wann, wie und ob sie ihre Vorfälle zu melden haben. Da dies zum gegenwärtigen Zeitpunkt der Fall ist, [Bis15b] sollte das BSI dazu verpflichtet werden dem Endanwender zeitnah die erschlossenen Kenntnisse zur Verfügung zu stellen, damit dieser selbständig in der Lage ist Tätig zu werden, um seine Daten zu schützen. Dadurch ist es möglich über den Endanwender Druck auf den Service Provider auszuüben. Doch schon hier versagt das neu Gesetzt wie im Kapitel 2 beschrieben. Ein anderes, viel angesprochenes Thema sind die Speicherbefugnisse für Telemedien- und Telekommunikationsanbieter bezüglich Verkehrsdaten nach §100 TKG, die zur Angriffserkennung gewährt werden sollen. Hier ist eine Konkretisierung und Beschränkung der Befugnisse dringend erforderlich, um nicht eine Vorratsdatenspeicherung durch die Hintertür einzuführen. [Bis15a]

Literatur

[Bis15a] Anna Biselli. »Anhörung zum IT-Sicherheitsgesetz im Bundestag (Liveblog und Fazit)«. In: *Netzpolitik.org* (Apr. 2015). URL: https://netzpolitik.org/2015/anhoerung-zum-it-sicherheitsgesetz-im-bundestag/%20;%20letzter%20Zugriff:%2013.12.2016.

[Bis15b] Anna Biselli. »IT-Sicherheitsgesetz hat Bundesrat passiert – Papiertiger ist verabschiedet«. In: *Netzpolitik.org* (2015). URL: https://netzpolitik.org/2015/it-sicherheitsgesetz-hat-bundesrat-passiert-papiertiger-ist-verabschiedet/%20;%20letzter%20Zugriff:%2013.12.2016.

[BMI] BMI. *IT und Cybersicherheit*. online. URL: https://www.bmi.bund.de/DE/Themen/Sicherheit/IT-Cybersicherheit/it-cybersicherheit_node.html%20;%20letzter%20Zugriff:%2013.12.2016.

[Bun15] Deutscher Bundestag. *Gesetzentwurf der Bundesregierung (18/4096) zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)*. online. Feb. 2015. URL: http://dip21.bundestag.de/dip21/btd/18/040/1804096.pdf%20;%20letzter%20Zugriff:%2013.12.2016.

[Neu15] Linux Neumann. *Stellungnahme zum Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT- Sicherheitsgesetz)*. online. Apr. 2015. URL: https://ccc.de/system/uploads/186/original/ITSG_Stellungnahme.pdf%20;%20letzter%20Zugriff:%2013.12.2016.