

11. November 2014

IT-Sicherheitsgesetz

Stellungnahme des Verbraucherzentrale Bundesverbandes

zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

Verbraucherzentrale Bundesverband e.V. – vzbv
Team Digitales und Medien
Projekt Verbraucherrechte in der Digitalen Welt
Markgrafenstr. 66
10969 Berlin
digitales@vzbv.de
www.vzbv.de

I. Einleitung

Der Verbraucherzentrale Bundesverband (vzbv) bedankt sich beim Bundesministerium des Inneren für die Gelegenheit, zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme Stellung nehmen zu können.

Grundsätzlich begrüßt der vzbv das mit dem vorliegenden Gesetzesentwurf vom 05. November 2014 angestrebte Ziel die IT-Sicherheit in Deutschland zu erhöhen und damit auch zum Schutz der persönlichen Daten der Verbraucherinnen und Verbraucher beizutragen. Besonders vor dem Hintergrund der massenhaften und grundrechtswidrigen Ausspähung der Bürgerinnen und Bürger durch Geheimdienste, der massiven Datenlecks der vergangenen Monate sowie den ungezügelter Datensammlungen einiger Internetunternehmen gebietet der Entwurf jedoch aus Sicht des vzbv, weitere Regelungen zur Verbesserung der Sicherheit für Verbraucherinnen und Verbraucher zu ergänzen.

Zudem bedauert der Verbraucherzentrale Bundesverband die äußerst kurze Kommentierungsfrist von nur wenigen Tagen, sodass nur zu den drängendsten Punkten Stellung genommen werden konnte.

II. Anmerkungen im Einzelnen

1. Zu Artikel 2 – Änderungen des Telemediengesetzes

Gemäß Artikel 2 Nr. 2 des Gesetzesentwurfs soll ein § 15 Abs. 9 in das Telemediengesetz eingeführt werden, nach dem Telemedienanbieter die erweiterten Befugnisse erhalten sollen, Nutzungsdaten „zum Erkennen, Eingrenzen und Beseitigen von Störungen sowie von Missbrauch seiner für Zwecke seines Telemediendienstes genutzten technischen Einrichtungen“ zu erheben und zu verwenden. Wenn „die Nutzungsdaten für diesen Zweck nicht mehr benötigt“ werden, sollen „diese unverzüglich, spätestens aber nach 6 Monaten“ gelöscht werden.

Der Verbraucherzentrale Bundesverband lehnt § 15 Abs. 9 TMG-E ab. Bei der damit eingeführten Speicherbefugnis handelt es sich im Kern um eine weitreichende anlasslose Vorratsdatenspeicherung, für die unter anderem das Bundesverfassungsgericht und der Europäische Gerichtshof enge Grenzen gesetzt haben. Diese Grenzen werden hier, nicht zuletzt durch die unverhältnismäßige Maximaldauer der Datenspeicherung bei den Telemediendiensten, überschritten.

Wenn solche Erhebungen von persönlichen Daten überhaupt ermöglicht werden sollen – was der vzbv grundsätzlich kritisch betrachtet – müssen diese strengen Vorgaben unterliegen, wie beispielsweise umfassender Anonymisierungspflichten, einer strikten Zweckbindung, einer klar im Gesetz definierten maximalen Speicherdauer, die sich auf das absolute Minimum beschränkt (ent-

sprechend des Urteils des BGH vom 3. Juli 2014 maximal bis zu einer Woche¹), sowie scharfen Sanktionen bei Verstößen gegen diese Vorgaben. Generell sollten jedoch Lösungen zur Bekämpfung von Störungen und Missbrauch bevorzugt werden, bei denen personenbezogene Daten lediglich anlassbezogen gespeichert werden dürfen.

2. Zu Artikel 3 – Änderungen des Telekommunikationsgesetzes: Verpflichtende Ende-zu-Ende-Verschlüsselung durch Diensteanbieter

Diensteanbieter im Internet, insbesondere Anbieter von Kommunikationsdiensten und Online-Speichern, sollten dazu verpflichtet werden, ihren Nutzern eine einfache Möglichkeit der Ende-zu-Ende-Verschlüsselung nach aktuellem Standard anzubieten.

„Ohne Vertrauen in die Sicherheit und Integrität der digitalen Welt wird es nicht gelingen, die wirtschaftlichen und gesellschaftlichen Potenziale des digitalen Wandels zu erschließen“². Sowohl hinsichtlich des E-Governments als auch eines Erfolgs der digitalen Wirtschaft ist das Vertrauen der Verbraucher also ein wesentlicher Faktor. Aktuelle Studien, wie der eGovernment Monitor 2014, belegen beispielsweise aber, dass für 66 Prozent der deutschen Internetnutzer eine mangelnde Datensicherheit gegen eine (intensivere) Nutzung von Online-Behördendiensten spricht – mit steigender Tendenz³. Sogar 81 Prozent der Internetnutzer fühlen sich im Internet durch die Ausspähung persönlicher Daten durch staatliche Stellen, Cyberkriminelle oder Unternehmen bedroht⁴.

Bisherige Initiativen, wie ein „Schengen-Routing“, „E-Mail made in Germany“ oder „De-Mail“, können jedoch eine vertrauliche elektronische Kommunikation der Nutzer nicht sicherstellen. Denn durch die fehlende Ende-zu-Ende-Verschlüsselung können die Anbieter, Geheimdienste und andere potentielle Angreifer weiterhin auf Kommunikationsinhalte zugreifen. Da die Verbraucher mit solchen Initiativen in falscher Sicherheit gewogen werden, bergen diese die große Gefahr, das Vertrauen im Speziellen in die genutzten Dienste und im Allgemeinen in die digitalen Technologien nachhaltig zu beschädigen. Bereits jetzt verzichten 47 Prozent der Internetnutzer bewusst aus Sicherheitsgründen darauf, vertrauliche Informationen und wichtige Dokumente per E-Mail zu versenden⁵. Die Folgen eines weiteren Vertrauensverlusts sind für den deutschen Staat und die digitale Wirtschaft nicht absehbar. Eine Ende-zu-Ende-Verschlüsselung von Kommunikationsinhalten ist daher ein wichtiger Schritt, echte Sicherheit zu schaffen und damit das verlorene Vertrauen der Verbraucher wieder herzustellen.

¹ entsprechend des BGH-Urteils zur Speicherung von IP-Adressen vom 3. Juli 2014 - III ZR 391/13

² Digitale Agenda 2014-2017, Seite 3, <http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/digitale-agenda-2014-2017>

³ eGovernment Monitor 2014, Seite 19, http://www.initiatived21.de/wp-content/uploads/2014/09/eGovMon2014_web.pdf

⁴ BKA und BITKOM: Pressekonferenz zu Cybercrime, Seite 2, http://www.bitkom.org/files/documents/BITKOM_Charts_PK_Cybercrime_mit_BKA_28_07_14.pdf

⁵ BKA und BITKOM: Pressekonferenz zu Cybercrime, Seite 4, http://www.bitkom.org/files/documents/BITKOM_Charts_PK_Cybercrime_mit_BKA_28_07_14.pdf

Auch das Vertrauen der Nutzer in die Cloud, eine für die Verbraucher grundsätzlich nützliche technische Errungenschaft, wurde in den letzten Jahren tiefgreifend geschädigt. 21 Prozent der Internetnutzer verzichten aus Sicherheitsgründen bewusst auf Cloud-Dienste⁶. Für diesen Vertrauensverlust spielt nicht nur die globale Überwachungs- und Spionageaffäre eine Rolle, sondern auch weitere massive Datensicherheitsprobleme mit weitreichenden Folgen für die Betroffenen, denen durch eine Ende-zu-Ende-Verschlüsselung begegnet werden könnte.

Erst jüngst wurden beispielsweise durch Einbrüche in verschiedene Cloud-Dienste nach Medienangaben hunderttausende Nacktfotos, darunter solche von Minderjährigen, und amerikanischen Prominenten entwendet und veröffentlicht⁷. Diese hatten die Bilder zum Teil im Vertrauen auf die Sicherheitsversprechen der Cloud-Anbieter dort gespeichert, zu einem anderen Teil wurden die Daten durch die Voreinstellungen der verwendeten Endgeräte ohne Wissen der Betroffenen unverschlüsselt auf die Server der Anbieter übertragen. Solche automatischen voreingestellten Sicherheitskopien können neben Fotos beispielsweise auch noch Kontaktdaten, Kalendereinträge oder W-LAN-Passwörter und weitere persönliche Daten enthalten⁸. Quantified-Self-Anwendungen und Wearables übertragen teilweise sogar Gesundheitsdaten automatisiert und ungesichert in die Cloud⁹. Möglichkeiten für Verbraucher die Daten zu verschlüsseln, gibt es nicht. Sie können lediglich diese hilfreichen Dienste in der Gänze ablehnen.

Auch wenn also die Verbraucher Verantwortung für die Sicherheit ihrer Daten übernehmen (müssen), müssen sie in die Lage versetzt werden, diese Verantwortung technisch überhaupt auszufüllen. Oftmals würden die Nutzer ihre Daten gerne verschlüsseln – 39 Prozent der Deutschen wären sogar bereit für eine Sicherheitsgarantie ihrer Daten zu bezahlen¹⁰. Allerdings sind die derzeit dafür notwendigen Verfahren häufig für den Laien zu kompliziert, nicht mit den genutzten Diensten kompatibel, nicht in die verwendeten Endgeräte integriert und zu wenig bekannt oder verbreitet.

Im Rahmen der Digitalen Agenda 2014 – 2017 hat die Bundesregierung erkannt: „Das Vertrauen zu stärken heißt daher zum einen, die Kommunikation über digitale Netze zu schützen und dafür den Zugang zu sicheren und einfach zu nutzenden Verschlüsselungsverfahren zu fördern“¹¹. Das IT-Sicherheitsgesetz ist aus Sicht des vzbv gut geeignet, dieses Ziel zu verfolgen,

⁶ Ebenda

⁷ Zeit Online: „Keine Nacktfotos sind auch keine Lösung“, 02.09.2014, <http://www.zeit.de/digital/datenschutz/2014-09/promi-nacktbilder-icloud-apple/komplettansicht>

⁸ Deutsches Institut für Vertrauen und Sicherheit im Internet, 04.11.2014, <https://www.divsi.de/publikationen/studien/wissenswertes-ueber-den-umgang-mit-smartphones/6-grundfunktionen-und-kopplung-mit-der-cloud/>

⁹ Focus Online: „Wenn das Hemd den Blutdruck misst: Wo landen unsere Körperdaten?“, 22.07.2014, http://www.focus.de/digital/internet/von-blutdruckmesser-bis-schritzaehler-gesundheitstracking-mit-wearables-wo-landen-unsere-daten_id_4001820.html

¹⁰ D21 - Digital-Index 2014, Seite 43, http://www.initiatived21.de/wp-content/uploads/2014/11/141103_digitalindex_web.pdf

¹¹ Digitale Agenda 2014-2017, Seite 3, <http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/digitale-agenda-2014-2017>

indem Diensteanbieter verpflichtet werden eine einfache Möglichkeit der Ende-zu-Ende-Verschlüsselung nach aktuellem Standard anzubieten.