Deutscher Bundestag **Drucksache 19/5764**

19. Wahlperiode 13.11.2018

Antrag

der Abgeordneten Jimmy Schulz, Stephan Thomae, Renata Alt, Nicole Bauer, Jens Beeck, Nicola Beer, Dr. Jens Brandenburg (Rhein-Neckar), Mario Brandenburg (Südpfalz), Britta Katharina Dassler, Bijan Djir-Sarai, Hartmut Ebbing, Dr. Marcus Faber, Daniel Föst, Otto Fricke, Thomas Hacker, Katrin Helling-Plahr, Markus Herbrand, Torsten Herbst, Katja Hessel, Manuel Höferlin, Dr. Christoph Hoffmann, Reinhard Houben, Olaf in der Beek, Thomas L. Kemmerich, Daniela Kluckert, Pascal Kober, Carina Konrad, Ulrich Lechte, Oliver Luksic, Till Mansmann, Alexander Müller, Roman Müller-Böhm, Hagen Reinhold, Christian Sauter, Matthias Seestern-Pauly, Frank Sitta, Judith Skudelny, Bettina Stark-Watzinger, Benjamin Strasser, Katja Suding, Michael Theurer, Dr. Andrew Ullmann, Johannes Vogel (Olpe), Nicole Westig, Katharina Willkomm und der Fraktion der FDP

Recht auf Verschlüsselung – Privatsphäre und Sicherheit im digitalen Raum stärken

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

In einer zunehmend digitalisierten Welt stellen elektronische Kommunikationsmittel wie E-Mail, Chat- oder Messenger-Dienste einen fundamentalen Bestandteil des privaten wie beruflichen Austausches dar. Laut einer Studie des Digitalverbands Bitkom sind 68 Prozent der Unternehmen in Deutschland in den vergangenen zwei Jahren Opfer von Sabotage, Spionage und Datendiebstahl geworden, der wirtschaftliche Schaden wird auf ca. 43 Milliarden Euro geschätzt.[1] Prominente Beispiele wie zuletzt der Hacker-Angriff auf den Informationsverbund Berlin-Bonn (IVBB) zeigen jedoch immer wieder, dass selbst das als sicher geltende Regierungsnetzwerk keinen absoluten Schutz vor einem unbefugten Zugriff Dritter auf sensible und persönliche Daten bieten kann. Dieser Schaden kann durch die Nutzung von Verschlüsselungstechnologien erheblich begrenzt werden. Zwar können potenzielle Angreifer einen Dateiordner oder eine E-Mail öffnen, können den Inhalt, ob sensible Daten, Geschäftsgeheimnisse oder private Kommunikation, jedoch nicht lesen, da dies nur mithilfe des passenden Schlüssels oder Passworts möglich ist.

[1] www.bitkom.org/Presse/Presseinformation/Attacken-auf-deutsche-Industrie-verursachten-43-Milliarden-Euro-Schaden.html (zuletzt aufgerufen am 25.09.2018).

Es geht bei der Verschlüsselung von Daten und Netzverkehr insbesondere um den Schutz des Eigentums, der Privatsphäre und der Vertraulichkeit der Kommunikation – in der Verfassung verbriefte Grundrechte. Artikel 10 Absatz 1 des Grundgesetzes schreibt fest, dass das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis unverletzlich sind. Dieser Grundsatz muss auch für die elektronische Kommunikation gelten, um Datenschutz, Privatsphäre und Sicherheit zu gewährleisten. Bereits 2008 befand das Bundesverfassungsgericht, dass es Aufgabe des Staates ist, das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität von IT-Systemen umzusetzen („IT-Grundrecht“ gemäß Urteil v. 27.02.2008 – 1 BvR 370/07 –, – 1 BvR 595/07).

Geeignete Verschlüsselungstechnologien sind bereits seit Jahrzehnten ausgereift und erprobt, werden von der breiten Masse der Anwenderinnen und Anwender bisher jedoch zurückhaltend genutzt – 2015 waren dies laut Statista nur 15 Prozent[2]. Ein Recht auf Verschlüsselung trägt dazu bei, die Akzeptanz für verbreitete Anwendung von Verschlüsselungstechnologien in der Bevölkerung, Wirtschaft wie auch öffentlichen Institutionen zu erhöhen, und leistet einen essentiellen Beitrag zum Schutz des gesetzlich festgeschriebenen Fernmeldegeheimnisses auch im digitalen Raum. Freie und offene Standards und Protokolle sind dabei Voraussetzung für eine sichere Kommunikation. Gleichzeitig kann so ein Entwicklungsschub im Bereich Verschlüsselungs- und IT-Sicherheitstechnologien befördert werden, von dem die gesamte Bundesrepublik Deutschland, Gesellschaft wie Wirtschaft, profitieren würde.

Die öffentliche Verwaltung kann eine Vorbildfunktion übernehmen, indem sie die Verwendung von frei verfügbaren und einfach handhabbaren Verschlüsselungstechnologien wie z. B. GPG fördert. Hierbei kann sie u. a. auf Erkenntnisse des bereits 1998 vom Bundesamt für Sicherheit in der Informationstechnik initiierten Pilotprojekts SPHINX (www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/EGovernment/VerwaltungsPKIVPKI/SPHINX/sphinx_node.html) zurückgreifen, insbesondere hinsichtlich der Interoperabilität und Funktionalität von Ende-zu-Ende-Verschlüsselungslösungen in der öffentlichen Verwaltung. Dadurch können Hemmschwellen gesenkt und die Akzeptanz von Verschlüsselungstechnologien in der Bevölkerung gestärkt werden.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

- sich zum Schutz der Privatsphäre und zur Erhöhung der IT-Sicherheit für ein Recht auf Verschlüsselung einzusetzen;
- in diesem Sinne Telekommunikations- und Telemedienanbieter zu verpflichten, ihre Kommunikationsdienste nach einer Übergangsfrist für zukünftige technische Systeme als Standard abhörsicher (Ende-zu-Ende verschlüsselt) anzubieten;
- die Weiterentwicklung von Verschlüsselungstechnologien, der Sicherheit von Speichersystemen und von qualifizierten Zugriffs- und Berechtigungslogiken konsequent voranzutreiben;
- sich gegen gesetzliche Beschränkungen oder Verbote kryptographischer Sicherungssysteme auszusprechen;
- den Einsatz von sogenannten Backdoors zu verurteilen und eine staatliche Beteiligung an digitalen Grau- und Schwarzmärkten für Sicherheitslücken abzulehnen;
- alle staatlichen Behörden zu verpflichten, IT-Sicherheitslücken unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Das BSI muss diese nach dem marktüblichen Standard der „Coordinated/Responsible Disclosure“ veröffentlichen;

[2] https://de.statista.com/statistik/daten/studie/504220/umfrage/nutzung-von-e-mail-verschluesselungen-in-deutschland/ (zuletzt aufgerufen am 25.07.2018).

- die Verwendung von frei verfügbaren, offenen und einfach handhabbaren Protokollen sowie Verschlüsselungsstandards wie z. B. GPG voranzutreiben.

Berlin, den 13. November 2018

Christian Lindner und Fraktion

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333