Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)434 F

Freie Universität Berlin

Fachbereich Mathematik und Informatik
ID-Management

Prof. Dr. Marian Margraf
Takustraße 9
14195 Berlin

+49 30 838 75-245
marian.margraf@fu-berlin.de

Innenausschuss des
Deutschen Bundestages

nur per E-Mail

Betr.: Öffentliche Anhörung zum Antrag der Fraktion der FDP "Recht auf Verschlüsselung - Privatsphäre und Sicherheit im digitalen Raum stärken"

Sehr geehrte Damen und Herren,

vielen Dank für die Einladung zur öffentlichen Anhörung. Gern übersende ich Ihnen vorab meine Stellungnahme in schriftlicher Form.

Den unter I. aufgeführten Feststellungen schließe ich mich an. Zu den unter II. aufgeführten Vorschlägen nehme ich wie folgt Stellung.

1) **… sich zum Schutz der Privatsphäre und zur Erhöhung der IT-Sicherheit für ein Recht auf Verschlüsselung einzusetzen**

Ein Recht auf Verschlüsselung, also der technischen Umsetzung des Schutzziels Vertraulichkeit, leitet sich meines Erachtens aus dem Recht auf informationelle Selbstbestimmung ab, das nach Rechtsprechung des Bundesverfassungsgerichts ein Grundrecht ist.

2) **… 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 Forderung, dass Telekommunikations- und Telemedienanbieter ihre Kommunikationsdienste standardmäßig Ende-zu-Ende sicher anbieten sollen, begrüße ich. Allerdings ist zu beachten, dass damit wesentliche sicherheits-technische Anforderungen, insbesondere zum Schlüsselmanagement, auf die Nutzer*innen verlagert werden. Hierzu gehören beispielsweise Schlüsselgenerierung, Schlüsselspeicherung, Schlüsselverteilung, aber auch Maßnahmen zur Schlüsselwiederherstellung, sollte z.B. das Gerät, in dem der Schlüssel gespeichert wurde, verloren gehen. Die unter I. aufgeführte Feststellung, dass nur ca. 15% der Nutzer*innen Ende-zu-Ende sichere Technologien zur Verschlüsselung ihrer Kommunikation nutzen, ist auch darin begründet, dass diese Lösungen häufig

Usability-Probleme haben. Hier müssen Technologien entwickelt werden, die es auch technisch nicht versierten Nutzer*innen ermöglichen, diese Maßnahmen benutzbar umzusetzen, ohne die Sicherheit zu schwächen.

3) **… die Weiterentwicklung von Verschlüsselungstechnologien, der Sicherheit von Speichersystemen und von qualifizierten Zugriffs- und Berechtigungslogiken konsequent voranzutreiben**

Technologien zur Umsetzung von IT-Sicherheit müssen fortwährend weiterentwickelt werden, um auch gegen zukünftige Bedrohungen resistent zu sein, aber auch, um die Benutzbarkeit der Lösungen weiter zur erhöhen und damit eine breite Nutzung zu ermöglichen. Zum Thema Benutzbarkeit siehe die Ausführungen unter Punkt 2). Eine weitere Herausforderung ist die voraussichtliche Entwicklung von Quanten-computern, die erhebliche Auswirkungen auf die heute eingesetzte Kryptographie, insb. auf Verfahren zum sicheren Schlüsselaustausch haben. Hier muss die Entwicklung sogenannter quantencomputerresistenter kryptographischer Verfahren vorangetrieben werden. U.a. mit den aktuell laufenden Projekten zur BMBF-Ausschreibung "Post-Quanten-Kryptografie" im Rahmen des Forschungsrahmen-programms der Bundesregierung zur IT-Sicherheit "Selbstbestimmt und sicher in der digitalen Welt 2015 bis 2020“ gibt es in diesem Bereich laufende Aktivitäten. Solche Programme sind zu begrüßen und sollten weitergeführt werden (auch für weitere Themen der IT-Sicherheit).

4) **… sich gegen gesetzliche Beschränkungen oder Verbote kryptographischer Sicherungssysteme auszusprechen**

Gesetzliche Beschränkungen oder Verbote kryptographischer Verfahren zur Umsetzung der Informationssicherheit würden das recht auf informationelle Selbstbestimmung massiv einschränken und müssen daher abgelehnt werden.

5) **… den Einsatz von sogenannten Backdoors zu verurteilen und eine staatliche Beteiligung an digitalen Grau- und Schwarzmärkten für Sicherheitslücken abzulehnen**

Die Geheimhaltung gefundener Sicherheitslücken mit dem Ziel, diese z.B. von staatlichen Stellen zur Kriminalitätsbekämpfung auszunutzen, kann erhebliche Auswirkungen auf die Sicherheit haben. Es kann davon ausgegangen werden, dass diese Sicherheitslücken nicht nur von staatlichen Stellen, sondern auch von Kriminellen gefunden und ausgenutzt werden. Davon ist nicht nur das Grundrecht auf informationelle Selbstbestimmung betroffen. Diese können auch zu großen wirtschaftlichen Schäden führen. In unserer zunehmend vernetzten Gesellschaft haben solche Sicherheitslücken also erhebliche Auswirkungen und müssen unverzüglich nach Bekanntwerden geschlossen werden.

Backdoors sind vor diesem Hintergrund nichts anderes als Sicherheitslücken, die ebenfalls von Kriminellen ausgenutzt werden können und sind damit abzulehnen. Auch die Forderung, Passwörter oder kryptographische Schlüssel an Ermittlungs-

behörden herauszugeben, ist vor diesem Hintergrund kritisch zu sehen. Setzt man die Sicherheitsmaßnahmen korrekt um, so ist eine Herausgabe von kryptographischen Schlüsseln und Passwörtern gar nicht möglich. Bei der Umsetzung von Ende-zu-Ende Sicherheit verbleiben die kryptographischen Schlüssel bei den Nutzer*innen, die Dienstanbieter haben hierauf gar keinen Zugriff. Zusätzlich werden Passwörter, bei richtiger Umsetzung, nicht im Klartext bei den Dienstanbietern gespeichert, sondern nur in einer Form, die es erlaubt, die Korrektheit des Passwortes zu prüfen, ohne das der Dienstanbieter das Passwort ermitteln kann.

6) **… 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**

Diese Forderung begrüße ich ebenfalls. IT-Sicherheitslücken müssen unverzüglich an das BSI gemeldet werden, damit entsprechende Gegenmaßnahmen schnell entwickelt und umgesetzt werden können.

7) **… die Verwendung von frei verfügbaren, offenen und einfach handhabbaren Protokollen sowie Verschlüsselungsstandards wie z. B. GPG voranzutreiben**

Auch diese Forderung begrüße ich. Allerdings müssen, wie unter 2) aufgeführt, vor allem Technologien entwickelt werden, die eine benutzerfreundliche Verwendung dieser Lösungen auch für technisch nicht affine Anwender*innen ermöglichen. Zusätzlich sollten staatliche Stellen dabei unterstützt werden, diese offenen Standards zur Kommunikation mit Bürger*innen anzubieten.

Mit freundlichen Grüßen

Prof. Dr. Marian Margraf