Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)434 C

Rheinische
Friedrich-Wilhelms-
Universität Bonn

Institut für Informatik

Prof. Dr. Michael Meier
Lehrstuhl IT-Sicherheit

Prof. Dr. Michael Meier
Universität Bonn · Institut für Informatik

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Per E-Mail: innenausschuss@bundestag.de

Bonn, 23. Januar 2020

Stellungnahme zum Antrag der Fraktion der FDP „Recht auf Verschlüsselung – Privatsphäre und Sicherheit im digitalen Raum stärken“ – Drucksache 19/5764

Sehr geehrte Frau Vorsitzende,
sehr geehrte Damen und Herren Bundestagsabgeordnete,

vielen Dank für die Gelegenheit zur Stellungnahme zum oben genannten Antrag und für die Einladung zur Sitzung des Ausschusses am 27. Januar 2020.

Stellungnahme zum Antrag der Fraktion der FDP:

Den im Antrag unter I. getroffenen Feststellungen schließe ich mich an.

IT-Sicherheit, also die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit, hinreichend durchzusetzen ist aufgrund verschiedener Ursachen (u.a. komplexitätsbedingten Fehlern in Soft- und Hardware sowie Seiteneffekten von Soft- und Hardware) eine große Herausforderung. Gleichzeitig werden IT-Systeme zunehmend zum Fundament von Wirtschaft und gesellschaftlichem Leben. Für den Schutz der Vertraulichkeit innerhalb von IT-Systemen stehen mit Verschlüsselungsverfahren, sofern konsequent und korrekt eingesetzt, wirksame Werkzeuge zur Verfügung.

Zu den unter II. aufgestellten Forderungen an die Bundesregierung nehme ich im Folgenden Stellung:

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

Diverse, teilweise im Antrag aufgeführte, Grundrechte korrespondieren mit einem Recht auf Vertraulichkeit. Verschlüsselung ist das wesentliche Werkzeug zur wirksamen Durchsetzung von Vertraulichkeit. Ohne Verschlüsselung kann ein Recht auf Vertraulichkeit heute nicht wirksam durchgesetzt werden. Entsprechend ergibt sich aus dem Recht auf Vertraulichkeit ein Recht auf Verschlüsselung.

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;*

Für Betreiber von Telekommunikationsnetzen und -diensten ergeben sich aus § 109 TKG Plichten zur Umsetzung technischer Schutzmaßnahmen, für die die Bundesnetzagentur einen Katalog von Sicherheitsanforderungen[1] aufgestellt hat. Darin heißt es:
„Wer Telekommunikationsnetze betreibt oder öffentliche Telekommunikationsdienste erbringt sollte sich mit diesem Thema auseinandersetzen und bei entsprechender Gefährdungslage an geeigneter Stelle eine Verschlüsselung der Daten vornehmen."
Aus meiner Sicht ist heute im Regelfall von einer entsprechenden Gefährdungslage auszugehen.

Im Telemediengesetz ist in §13 (7) formuliert:
„Eine Maßnahme nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens."
In der BSI-Veröffentlichung zur „Absicherung von Telemediendiensten nach Stand der Technik" (Stand 2016)[2] ist Verschlüsselung als Basismaßnahme für alle Provider-Typen (Content-, Host- und Access-Provider) vorgesehen.

Aus meiner Sicht entspricht eine Ende-zu-Ende-Verschlüsselung dem heutigen Stand der Technik, sodass sich die Forderung durch die oben genannten Regelungen ergibt. Unabhängig davon, ob hier eine Rechtsanpassung notwendig ist, trägt die Umsetzung der Forderung zu einer sinnvollen Verbesserung der IT-Sicherheit bei und ist ein Beitrag zum erklärten Ziel der Bundesregierung Deutschland zum Verschlüsselungsstandort Nr. 1 zu machen.

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

Oben genannte Herausforderungen bei der Durchsetzung von IT-Sicherheit bei gleichzeitiger Intensivierung der IT-Nutzung in unserem Land machen eine umfangreiche Weiterentwicklung von IT-Sicherheitstechnologien zwingend erforderlich. Neben der Weiterentwicklung von Technologien bedarf es auch der Entwicklung und Umsetzung von Ansätzen und Konzepten mit denen Sicherheitstechnologien wie Verschlüsselung in eine breite Anwendung gebracht werden. Zu letztgenanntem Aspekt sehe ich großen Nachholbedarf.

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

Verschlüsselung ist das einzige wirksame Mittel zum Vertraulichkeitsschutz. Jegliche Beschränkung der Nutzung oder Beeinträchtigung der Wirksamkeit bzw. Sicherheit etwa durch Verwaltung zusätzlicher Schlüsselkopien für staatliche Stellen etc. sind der IT-Sicherheit abträglich und mit verheerenden Auswirkungen verbunden. Dadurch würde jegliches Recht auf Vertraulichkeit ausgehöhlt.

---

[1] Bundesnetzagentur: Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz (TKG), 2016, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/KatalogSicherheitsanforderungen.pdf

[2] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_125.pdf

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

Sicherheitslücken gefährden unsere Digitale Gesellschaft und müssen schnellst möglich geschlossen werden. Versuche Sicherheitslücken offen zu halten, um sie ausnutzen zu können, sind unverantwortlich und abzulehnen.

Eine staatliche Beteiligung an Märkten für Sicherheitslücken sollte jedoch differenzierter betrachtet werden. So kann eine Beteiligung an diesen Märkten ausschließlich zum Zweck der Aufklärung dort (und damit bei Angreifern) verfügbarer Informationen zu Sicherheitslücken sinnvoll sein, um hiervon ausgehend Empfehlungen und Warnungen in Richtung von IT-Nutzern auszusprechen, um Gefahren durch entsprechende Sicherheitslücken zu reduzieren.

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;*

Aus bereits angeführten Gründen unterstütze ich diese Forderung.

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

Ich unterstütze diese Forderung: Das Beispiel der Ende-zu-Ende-Verschlüsselung von E-Mails (z.B. mittels S/MIME oder GPG) zeigt, dass trotz grundsätzlich verfügbarer Technologie die Nutzung begrenzt ist, da erforderlichen Infrastrukturen und Schlüsselverteilmechanismen fehlen. Innerhalb von Organisationen wird durch den zentralen Betrieb solcher Infrastrukturen die einfache und weitgehend transparente Nutzung von Ende-zu-Ende-Verschlüsselung ermöglicht. Für die Nutzung von Ende-zu-Ende-verschlüsselter E-Mail-Kommunikation über Organisationsgrenzen hinweg und im privaten Umfeld sind spürbare Hürden zu überwinden, da entsprechende Schlüssel-Infrastrukturen und Verzeichnisdienste kaum verfügbar sind oder, im Falle von GPG, nur durch IT-affine Anwender sicher benutzbar sind. Hier sind zusätzliche Anstrengungen von staatlicher Seite erforderlich um IT-Sicherheit und Datenschutz durch breite standardmäßige Nutzung von Ende-zu-Ende-Verschlüsselung zu erhöhen und Deutschland tatsächlich zum Verschlüsselungsstandort Nr. 1 zu machen.

Abschließende Anmerkungen zu verwandten aktuellen Diskussionen:

Aufgrund der für 5G vorgesehenen kryptographischen Sicherheitsmechanismen werden im Endausbau des 5G-Netzes klassische IMSI-Catcher (zur Erfassung von Mobiltelefonen im Umfeld) nicht mehr funktionieren. Allerdings sehe ich konzeptionell keine Hindernisse für die Entwicklung von 5G-fähigen IMSI-Catchern, die u.U. in Zusammenarbeit mit den Mobilfunkbetreibern zu entwickeln und zu betreiben wären. Grundsätzlich handelt es sich bei diesen Geräten jedoch um Dual-Use-Aufklärungswerkzeuge, die auch von Kriminellen genutzt werden können. Anstatt auf die Entwicklung derartiger Werkzeuge zu setzen, erscheint mir die Realisierung hoheitlicher Aufklärungs- und Ermittlungsaufgaben über die Mitwirkung von Mobilfunk-Providern geeigneter.

Die Spionagemöglichkeiten durch 5G-Ausrüster werden intensiv diskutiert. Diesen kann mit Verschlüsselung effektiv begegnet werden. Eine weitere Aufweichung der Sicherheits- insbesondere Verschlüsselungsmechanismen innerhalb von 5G (tatsächlich bleiben die Verfahren hinter dem heute möglichen und sinnvollen zurück) muss verhindert werden. So ist etwa die im Zusammenhang mit der Überwachung ausländischer Handynutzer vorgesehene pauschale (egal ob tatverdächtig oder nicht)

Weitergabe von (zur Transportverschlüsselung genutztem) Schlüsselmaterial in das Besuchsland allein zum Zweck einer möglichen Entschlüsselung zur Überwachung höchst kritisch zu betrachten, und schwächt die Sicherheit des gesamten Systems und damit aller Nutzer. Hierdurch werden zusätzliche Angriffspunkte für Angreifer geschaffen.

Kritisch zu sehen ist auch der im Rahmen des Entwurfs des Gesetzes zur Bekämpfung von Rechtsextremismus und der Hasskriminalität unternommene Vorstoß alle Telemedienanbieter zu verpflichten vertrauliche Passwortinformationen (nach Stand der Technik in der Regel Passwort-Hashes) auf Anforderung an Sicherheitsbehörden zu übermitteln.

Vertrauliche Passwortinformationen und kryptographische Schlüssel sind grundlegend für die IT-Sicherheit und den Datenschutz und müssen maximal geschützt werden. Dies schließt derartige Zugriffsmöglichkeiten für Dritte wie z.B. Sicherheitsbehörden aus.

Angemerkt sei auch, dass mit einer breiteren Akzeptanz der aktuell vorangetriebenen FIDO2-Technologie zur Authentifikation von Nutzern bei Web-Diensten, seitens Dienstanbieter keine entsprechenden Passwortinformationen oder Vergleichbares mehr vorhanden sein werden.

gez. Prof. Dr. Michael Meier