BÜNDNIS DEUTSCHLAND
FREIHEIT. WOHLSTAND. SICHERHEIT.

Bündnis Deutschland
Knesebeckstraße 62763
10719 Berlin

info@buendnis-deutschland.de
www.buendnis-deutschland.de

BUNDESFACHAUSSCHUSS 9

BÜNDNIS DEUTSCHLAND

Positionspapier zum Thema Aufbrechen von Ende-zu-Ende-Verschlüsselung

Von Leon Welchert

Mitglied BFA 9 Infrastruktur, Digitalisierung, Verkehr, Bauen und Wohnen | 06.08.2023

In den vergangenen Jahren gab es auf EU-Ebene immer wieder Vorstöße, die das Verbot, beziehungsweise die Schwächung von Ende-zu-Ende verschlüsselter digitaler Kommunikation zum Ziel hatten, zuletzt einen Gesetzesvorschlag im Jahre 2022[1]. Sollte dieser Gesetzesvorschlag umgesetzt werden, wären alle Anbieter von Kommunikationsplattformen dazu verpflichtet, in ihre Software »Hintertüren« für Behördenvertreter einzubauen, damit diese die Kommunikation bei Bedarf einsehen, bzw. deren Inhalt automatisiert auf illegale Inhalte prüfen können. Es werden sich von dieser Maßnahme Ermittlungserfolge gegen Kriminelle versprochen, die verschlüsselte Kommunikation für Straftaten benutzen, insbesondere Pädophile, die Kontakt zu Kindern aufnehmen bzw. kinderpornographisches Material austauschen. Unabhängig von eventuellen Ermittlungserfolgen stellt eine anlasslose und flächendeckende Überwachung sämtlicher Bürger einen unverhältnismäßigen und gefährlichen Eingriff in elementare Grundrechte dar und wird deshalb von Bündnis Deutschland abgelehnt.

Argumentation:

Die flächendeckende Überwachung aller Kommunikationsdienste ist unverhältnismäßig zum potenziellen Nutzen der Gesetzgebung. Der wissenschaftliche Dienst des EU-Rates[2], der deutsche Anwaltverein[3] sowie 300 Forscher aus Deutschland[4] (um nur einige Akteure zu nennen) haben den ihnen vorgelegten Gesetzesentwurf als mit den Grundrechten unvereinbar erklärt.
Es steht auch zu erwarten, dass eine Auswertung durch automatisierte Systeme eine erhebliche Fehlerrate aufweisen wird[5]. Minderjährige, die Bilder untereinander austauschen, bzw. deren Familien, könnten so in den Fokus von Ermittlungen geraten, genauso wie Personen, deren Nutzung falsch positiv detektiert wird.

[1] Proposal for a Regulation of the European Parliament and of the Council, 2022

[2] Geleaktes Dokument des Wissenschaftlichen Dienstes des EU-Rats, https://aeur.eu/f/6ql

[3] Deutscher Anwaltverein, “SN 29/21: EU-Konsultation zur Bekämpfung von Kindesmissbrauch,” https://anwaltverein.de/de/newsroom/sn-29-2021-eu-konsultation-zur-bek%C3%A4mpfung-von-kindesmissbrauch

[4] “Stop Chat Control: 300 Wissenschaftler warnen vor Gesetz gegen Kindesmissbrauch,” https://tutanota.com/de/blog/chat-control

[5] Chat Control or Child Protection” https://arxiv.org/abs/2210.08958

Kriminelle, welche ihre Tätigkeiten verschleiern wollen, werden die Verschlüsselung selbst durchführen, statt die Verschlüsselungsfunktionalität irgendeiner zur Preisgabe verpflichteten Plattform zu nutzen. Die hierzu nötige Software ist überall verfügbar und leicht zu bedienen[6].

Verschlüsselte Kommunikation ist ein elementarer Grundpfeiler im sicheren IT-Betrieb[7]. Programmatische Hintertüren und Zweitschlüssel sind überaus lohnende Ziele für Missbrauch und Kriminelle. Einmal implementierte Überwachungswerkzeuge werden mit trauriger Regelmäßigkeit missbraucht. [8] [9] [10]

Bei einer dermaßen umfassenden Durchleuchtung aller Bürger in ihrem Privatleben, steht das Eintreten dieses Falls von vorneherein fest. Eine Demokratie hat die Aufgabe, das Errichten eines Überwachungsstaates zu verhindern und nicht, diesem Vorschub zu leisten.

Schlussfolgerung:

Wer Verschlüsselung kriminalisiert, sorgt dafür, dass nur noch Kriminelle Verschlüsselung nutzen. Der Versuch, diese Technik künstlich zu schwächen oder Zweitschlüssel hinterlegen zu lassen, hebelt die Sicherheit Millionen gesetzestreuer Menschen aus, während Kriminelle weiterhin starke Verschlüsselung nutzen. Künftige Regierungen sollten sich für die Stärkung von Verschlüsselung und damit die Erhöhung der weltweiten IT-Sicherheit einsetzen. Formelle oder informelle Verpflichtungen von Betreibern von Systemen zur Aushebelung von Verschlüsselung dürfen grundsätzlich nicht stattfinden. Datenverschlüsselung als Mittel zum informationellen Selbstschutz ist ein Grundrecht und darf nicht beschnitten werden. Dazu gehört auch, dass niemand gezwungen werden kann, seine Passwörter oder Schlüssel offenzulegen.
Deutschland muss sich rigoros gegen Versuche innerhalb der EU, die Privatsphäre und Meinungsfreiheit im digitalen Raum zu untergraben, zur Wehr setzen. Argumente wie die Bekämpfung von Urheberrechtsverletzungen, Kindesmissbrauch oder Terrorismus rechtfertigen nicht die anlasslose, dauerhafte Komplettüberwachung unbescholtener Bürger. Ohne diese Grundrechte zu schützen, kann es in Europa keine Demokratie geben.

---

[6] Chey Cobb, "Cryptography for Dummies", Wiley, Hoboken, 2004

[7] BSI, IT-Grundschutz-Kompendium, Reguvis, Köln, 2023

[8] "Datenabfragen: Mehr als 400 Verfahren gegen Polizisten" https://www.faz.net/aktuell/politik/inland/datenabfragen-mehr-als-400-verfahren-gegen-polizisten-16876625.html

[9] “Gefährliche Neugier: Missbrauch von Polizeidatenbanken” https://www.lto.de/recht/hintergruende/h/polizei-datenbanken-missbrauch-datenkriminalitaet-abfragen-daten-schutz/