Stellungnahme von Dr. Sven Herpig[1], Stiftung Neue Verantwortung, im Rahmen der "ExpertInnenanhörung IT-Sicherheit" des Digitalminister[:innen]treffens D16 am 29.09.2021

Sehr geehrte Digitalministerinnen und Digitalminister,
sehr geehrte Vertreter:innen,
sehr geehrte Sachverständige,

Der sogenannte "Kryptokrieg" geht bis in das Amerika der frühen 90iger Jahre zurück.[2] Es begann alles mit dem "Clipper Chip". Ein Microchip, der verschlüsselte Telefonate mit handelsüblichen Telefonen möglich machte, jedoch den Zugriff durch staatliche Behörden auf diese Telefonate zuließ. Relativ schnell fand ein IT-Sicherheitsforscher eine Möglichkeit de Clipper Chip zu hacken und für die Behörden unbrauchbar zu machen. Die Sicherheitsbehörden stellten das Projekt daraufhin ein. Auch wenn dieses Beispiel schon viele Jahre zurückliegt, sagt es sehr viel über die Sinnhaftigkeit der Schwächung einer sicheren Implementierung von starker Verschlüsselung aus.

Ein paar Jahre später fanden sich dann auch in Deutschland die ersten Andeutungen für den bevorstehenden Kryptokrieg. In den Eckpunkten der deutschen Kryptopolitik[3] die 1999 verabschiedet worden hieß es: "Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung". Was für viele wie ein Widerspruch wirkte, wurde jedoch in den Jahren darauf operationalisiert.

Polizeien in Bund und Ländern bekamen die Möglichkeit Überwachungssoftware auf Endgeräten einzusetzen und damit dort direkt auf die unverschlüsselte Kommunikation zuzugreifen. Bekannt ist das als Quellen-Telekommunikationsüberwachung, Online-Durchsuchung und manchmal auch verächtlich als Staatstrojaner. Der Rechtsrahmen dafür wurde über die Jahre ausgeweitet[4]. Zuletzt wurde diese Art des Zugriffs sogar für alle

[1] Stiftung Neue Verantwortung (2021), Dr. Sven Herpig, Stiftung Neue Verantwortung
[2] Andi Wilson Thompson, Danielle Kehl, and Kevin Bankston (2015), Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s, New America
[3] Unbekannt (1999), Eckpunkte der deutschen Kryptopolitik 1999, Internet Archive
[4] Sven Herpig und Stefan Heumann (2019), The Encryption Debate in Germany, Carnegie Endowment for International Peace und Sven Herpig und Julia Schuetze (2021), The Encryption Debate in Germany: 2021 Update, Carnegie Endowment for International Peace

deutschen Nachrichtendienste zugelassen. Und Internetanbieter sollen die Nachrichtendienste hierbei unterstützen.[5]

Problematische Erkenntnisse wie die langjährige und am Ende gescheiterte Eigenentwicklung der entsprechenden Software durch deutsche Behörden, die geringe Nutzung der rechtlichen Möglichkeiten in der Praxis, sowie die Beschaffung von zwielichtigen Firmen wie FinFisher[6] oder NSO, deren Software in autokratischen Ländern genutzt wird, und unter anderem im Umfeld des später ermordeten Journalisten Kashoggi zum Einsatz kam[7], werden hierbei ignoriert, was man an dem steten Ausbau der Befugnisse in den letzten Jahren sehen kann.

Die Sicherheitsbehörden können aber nicht nur über Quellen-TKÜ und Onlinedurchsuchung auf Informationen zugreifen, ihnen steht eine ganze Palette an Befugnissen zur Verfügung, die sie in ihrer Arbeit nutzen können. Das Max-Planck-Institut hat im Rahmen einer Studie eine Liste dieser gesetzlichen Grundlagen in einem Überwachungsbarometer zusammengetragen.[8] An rechtlichen Möglichkeiten mangelt es den Sicherheitsbehörden also nicht notwendigerweise. Das sind auch Erkenntnisse aus der Aufarbeitung der Fälle um die NSU und Anis Amri.[9] Das Scheitern der Sicherheitsbehörden, wenn man es so bezeichnen möchte, lag nicht am Mangel an Informationen und Daten.

Trotz allen diesen bereits bestehenden Befugnissen und Nachweisen, dass es besserer Zusammenarbeit der Sicherheitsbehörden und nicht noch weiteren Befugnissen bedarf, wurde zuletzt 2019 auf der Innenminister:innenkonferenz und 2020 auf EU-Ebene von Deutschland die Schwächung bzw. Umgehung von sicher-implementierter, starker Ende-zu-Ende Verschlüsselung vorangetrieben.[10] Das beinhaltet alternative Zugangsmöglichkeiten, *lawful access*, wie Vordertüren, Hintertüren oder ähnlichen Neusprech für diese funktional ähnlichen Mechanismen.

---

[5] Kilian Vieth, Charlotte Dietrich und Sven Herpig (2020), Stellungnahme zum Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat „Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts“

[6] Daniela Turß (2020), Pressemitteilung: GFF-Strafanzeige trägt Früchte – Durchsuchung bei Münchener Firma FinFisher wegen Exports von Staatstrojanern, Gesellschaft für Freiheitsrechte

[7] Dana Priest, Souad Mekhennet und Arthur Bouvart (2021), Jamal Khashoggi’s wife targeted with spyware before his death, The Washington Post

[8] Projekt Überwachungsbarometer (2021), Übersicht über potenziell relevante Überwachungsszenarien, Max-Planck-Institut

[9] Ulf Buermeyer und Sven Herpig (2019), Immer neue Sicherheitsgesetze helfen nicht, ZEIT Online

[10] Jörg Diehl, Martin Knobbe, Marcel Rosenbach und Wolf Wiedmann-Schmidt (2019), Seehofer greift WhatsApp an, SPIEGEL Online und Verónica Huertas Cerdeira (2020), Verschlüsselung: Rat nimmt Entschließung zur Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung an

Es gibt bereits seitenlange Studien darüber, warum die Schwächung bzw. Umgehung von sicher-implementierter, starker Ende-zu-Ende Verschlüsselung zu einem Sicherheitsproblem führen würde. Sogar ehemalige Geheimdienstchefs argumentieren, dass die Kosten solcher Maßnahmen für Sicherheit und Wirtschaft den Nutzen bei der Strafverfolgung nicht aufwiegen. Zusammenfassend ist dies in dem offenen Brief dargelegt, den ich mit Ihnen in Vorbereitung zu dieser Sitzung geteilt habe und den über 200 Organisationen, Firmen, Expert:innen und Abgeordnete unterschrieben hatten.[11] Lassen Sie mich daher nur zwei Teilaspekte nochmals unterstreichen:

1. Alternative Zugangsmöglichkeiten gibt es nicht nur für die Sicherheitsbehörden. Einmal implementiert können sie auch von ausländischen Nachrichtendiensten und Cyberkriminellen gefunden und ausgenutzt werden. Das schadet der deutschen Wirtschaft, Gesellschaft und kann vor allem auch ihnen, den Politikerinnen und Politikern dieses Landes zu Verhängnis werden. Überlegen Sie sich zum Beispiel was passieren könnte, wenn wie gerade geschehen, im Vorlauf einer Wahl die Gruppe hinter Ghostwriter solche Zugänge bei Kandidierenden ausnutzen und deren Daten veröffentlichen würde. Das Gleiche gilt für Mitarbeiter:innen von Behörden und Berufsgeheimnisträger:innen.
2. Unser Bundesinnenminister Horst Seehofer, aber auch der hier anwesende Präsident des Bundesamtes für Sicherheit in der Informationstechnik werden nicht müde zu erwähnen, dass Cybersicherheit eine notwendige Grundlage für Digitalisierung ist. Sie haben natürlich vollkommen recht, daher dürfen wir die in Deutschland verwendeten und entwickelten digitalen Produkte und Dienstleistungen nicht durch solche Zugangsmöglichkeiten zusätzlich schwächen. Das wäre das Gegenteil von Digitalisierung und digitaler Souveränität. Es würde Deutschlands Ansehen als Standort für sichere und datenschutz-orientierte Digitalwirtschaft massiv beschädigen. Für ein Land das 2014 noch “Verschlüsselungsstandort Nr. 1” werden wollte, wirkt das wie blanker Hohn.[12]

Es geht den Expert:innen, die eine Schwächung sicher-implementierter, starker Ende-zu-Ende Verschlüsselung ablehnen nicht darum die Strafverfolgungsbehörden oder

[11] Unbekannt (2019), Offener Brief - Geplanter Eingriff in Verschlüsselung von Messenger-Diensten hätte fatale Konsequenzen
[12] Die Bundesregierung (2014), Digitale Agenda 2014 - 2017, Bundesministerium für Wirtschaft und Energie

Nachrichtendienste zu schwächen. Es geht ihnen darum die deutsche Wirtschaft, besonders-gefährdete Personengruppen und ultimativ unsere nationale Sicherheit zu schützen.

Daher mögen die D16-Vertreter:innen in diesem Interesse beschließen, dass es

1. eine unabhängige Evaluierung der bestehenden Befugnisse zum Zugriff auf Daten, inklusive Quellen-TKÜ und OD, in den Bundesländern gibt;
2. auf Länderebene keine weitere Schwächung oder Umgehung von sicherer Implementierung starker Verschlüsselung, vor allem bei Ende-zu-Ende-Kommunikation, durch *lawful access* [Anm. im Laufe der Anhörung eingefügt: *lawful interception*] geben wird; und
3. auf den Bund einwirken, dass er 1. und 2. auf Bundesebene umsetzt und sich auf EU-Ebene dafür einsetzt, dass die Sätze 2 und 3 des Recital 54 im aktuellen Entwurf der Europäischen Network and Information Security Direktive ersatzlos gestrichen werden.