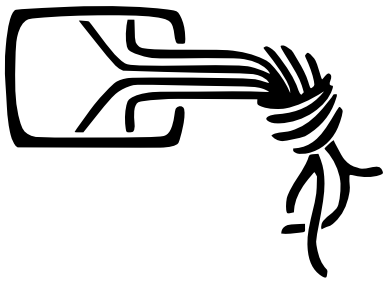

Stellungnahme zum Antrag „Recht auf Verschlüsselung – Privatsphäre und Sicherheit im digitalen Raum stärken“
Kompromisslose Verschlüsselung stärken
Drucksache 19/5764

Matthias Marx, Chaos Computer Club

27. Januar 2020

1 Einleitung

Immer wieder gibt es Bestrebungen, verschlüsselte Kommunikation gesetzlich zur Schwächung ihrer Sicherheit zu zwingen. Eingriffe in Verschlüsselung hätten aber fatale Konsequenzen für die Sicherheit von Wirtschaft und Verbrauchern: Das Sicherheitsniveau von Millionen deutscher Internet-Nutzer_innen würde sinken, es würden neue Einfallstore für ausländische Geheimdienste und Kriminelle geschaffen und das internationale Ansehen Deutschlands als führender Standort für eine sichere und datenschutzorientierte Digitalwirtschaft würde massiv geschädigt werden.

Im Antrag „Recht auf Verschlüsselung – Privatsphäre und Sicherheit im digitalen Raum stärken“ werden Maßnahmen vorgeschlagen, die nicht nur geeignet sind, Deutschlands außenpolitische Glaubwürdigkeit als Verfechter einer freien und sicheren Kommunikation zu stärken, sondern auch geeignet sind, die IT-Sicherheit von Bürgerinnen und Bürgern, Behörden und Wirtschaft auch in Zukunft nachhaltig zu gewährleisten. Zwar fehlt im Antrag das explizite Recht auf Verschlüsselung, dennoch sind die vorgeschlagenen Maßnahmen geeignet, ein Recht auf Verschlüsselung grunsdsätzlich in der Praxis wahrzunehmen und durchzusetzen. Dieses Vorhaben hätte – auch mit Blick auf autoritäre Staaten, in denen sichere Verschlüsselung verboten wird – weit über die deutschen Grenzen hinaus positive Strahlkraft.

2 Ende-zu-Ende-Verschlüsselung als Standard

Ein Paradigmenwechsel von zentralen Sicherheitssystemen hin zu mehrschichtigen Sicherheitssystemen mit Ende-zu-Ende-Verschlüsselung ist überfällig. Eine Ende-zu-Ende-Verschlüsselung von Kommunikation muss als verpflichtender Stand für Behörden, Berufsgeheimnisträger und für alle Kommunikationsunternehmen eingeführt werden, um die Angriffsfläche zentraler Infrastrukturen zu verringern und Schutz gegen massenhafte Überwachung zu erlangen. Entscheidend ist hierfür auch die kompromisslose Verfügbarkeit von Ende-zu-Ende-Verschlüsselung.

Zusatzkomponenten zur Ende-zu-Ende-Verschlüsselung waren lange Zeit vor allem deshalb notwendig, weil bei der Konzeption von Kommunikationssystemen bewusst auf eine Verschlüsselungsmöglichkeit verzichtet wurde. Moderne Systeme wie Signal, Whatsapp und Threema beweisen, dass eine Ende-zu-Ende-Verschlüsselung nutzungsfreundlich und ohne große Umstände in Kommunikationssysteme integriert werden kann. Alle gängigen Webbrowser, E-Mail-Clients und Messaging-Applikationen unterstützen schon heute eine Ende-zu-Ende-Verschlüsselung – nur muss die häufig erst zusätzlich aktiviert werden. Dies ist ein Missstand, dem es zu begegnen gilt.

Als Irrweg haben sich Versuche erwiesen, Verschlüsselung halbherzig, mit sogenannten Kompromissen, Ausnahmen und „besonderen Anforderungen“ umzusetzen. Diese Versuche scheitern an ihrer Komplexität, ihren offenkundigen Schwächen und nicht zuletzt auch ihrer Sinnlosigkeit.

3 Weiterentwicklung von Verschlüsselung

Wie jede Technologie unterliegen auch Verschlüsselungsverfahren Innovationsdruck und Alterung. Deswegen sind bei der Neukonzeption von Kommunikationssystemen Verschlüsselungs-

verfahren nach Stand der Technik zu berücksichtigen. Zudem ist bei den genutzten Verfahren regelmäßig zu prüfen, ob diese noch dem Stand der Technik entsprechen oder nachgebessert bzw. von neuen Verfahren abgelöst werden müssen.

4 Verbote kryptographischer Sicherungssysteme, Einsatz von Backdoors und staatliche Beteiligung an digitalen Grau- und Schwarzmärkten

Gesetzliche Beschränkungen oder Verbote kryptographischer Sicherungssysteme würden sich allenfalls für die unbescholtene Allgemeinheit durchsetzen lassen – und dies auch nur mittels einer dedizierten und stark in die Freiheitsrechte der Kommunikation eingreifende IT-Infrastruktur. Technisch versierten oder von krimineller Energie getriebenen Personen werden ungeachtet aller Bemühungen auch weiterhin in der Lage sein, verschlüsselt und sogar unbeobachtbar zu kommunizieren. Ein Verbot oder eine Verhinderung würde daher unter hohen Kosten doch nur zum Schaden der Allgemeinheit wirken und deren Schutzniveau aktiv herabsetzen. Leidtragende wären legale Wirtschaft und Verbraucher.

Für dezentrale Dienste wie E-Mail könnten ohnehin keine Backdoors gesetzlich erzwungen werden. Doch auch für zentrale Systeme würden Backdoors einen tiefen Eingriff in die bestehenden komplexen Softwaresysteme der Betreiber – und deren aktive Schwächung – erfordern. Schwachstellen sind dabei immer technisch neutral, würden also ausländischen Geheimdiensten und Kriminellen potenziell ebenso ein leichteres Einfallstor bieten, um an sensible Informationen von Individuen, Behörden und Unternehmen zu kommen. Gleichzeitig würden vorhandene Schwachstellen es Mitarbeiter_innen ermöglichen, Kommunikationsinhalte einzusehen, und so das Missbrauchspotenzial von Kommunikationsdiensten erhöhen.

Hinzu kommt, dass eine mit einer Hintertür versehene Version des jeweiligen Messengers als Softwareupdate eingespielt werden müsste. Unabhängig davon, ob dieser Eingriff gezielt oder in der Breite erfolgt und alle Bundesbürgerinnnen betrifft, würde das Vertrauen der Verbraucher_innen in die Dienstanbieter im Besonderen und Sicherheitsupdates im Allgemeinen erschüttern und sich damit nachhaltig negativ auf die IT-Sicherheit in Deutschland auswirken.

Die jüngsten Infektionen von Bundesbehörden, Gerichten, Krankenhäusern und Hochschulen mit der Schadsoftware Emotet zeigen die weitreichenden und empfindlichen Folgen von kriminell motivierten Angriffen. Sie offenbaren, dass die Bundesrepublik Deutschland auch heute noch auf einem viel zu niedrigen Niveau der IT-Sicherheit operiert.

Das staatliche Ausnutzen von Sicherheitslücken stellt einen nicht auflösbaren Interessenkonflikt der inneren Sicherheit dar: Um eine Sicherheitslücke möglichst lange selbst ausnutzen zu können, muss sie geheim gehalten werden – und kann somit potenziell in allen IT-Systemen ausgenutzt werden. Dem steht das dringende staatliche und wirtschaftliche Interesse entgegen, Sicherheitslücken zu schließen, um die IT-Systeme der Bundesrepublik gegen Angriffe zu schützen. Nur so können Kritische Infrastrukturen geschützt und staatliche sowie Wirtschaftsspionage zurückgedrängt werden.

5 Verpflichtende Meldung von Sicherheitslücken

Behörden sollen dazu verpflichtet werden, bei Kenntnisnahme von öffentlich bisher unbekannten IT-Sicherheitslücken, diese unverzüglich an das BSI zu melden. Die Sicherheitslücken sollen im Rahmen sog. Coordinated/Responsible Disclosure-Verfahren behoben und veröffentlicht werden. Hierfür braucht es ein starkes, unabhängiges BSI mit unzweideutigem Sicherheitsauftrag. Das BSI darf ausschließlich der Sicherheit von Computern und Netzen verpflichtet sein und Informationen über Sicherheitslücken ausschließlich zu deren Beseitigung anwenden. Keinesfalls darf das BSI gezielt auf eine Schwächung von Kommunikationsinfrastrukturen hinarbeiten.

Um diesem unzweideutigen Auftrag ohne Interessenkonflikt folgen zu können, muss das BSI aus dem Verantwortungsbereich des Innenministeriums herausgelöst werden und einen unzweifelhaften Status als unabhängige Bundesbehörde erhalten. Solange das BSI dem Innenministerium untersteht, kann es seinem Auftrag nicht kompromisslos gerecht werden, weil die demselben Ministerium unterstellten Behörden konträre Interessen verfolgen.

6 Verwendung von frei verfügbaren, offenen Protokollen

Deutsche Alleingänge wie De-Mail und beA (besonderes elektronisches Anwaltspostfach) haben eindrücklich gezeigt, was es bedeutet, von etablierten Standards abzuweichen. Die Bundesregierung soll nicht nur auf das Einhalten von Sicherheitsstandards hinwirken, sondern diese auch im eigenen IT-Beschaffungsverhalten bei Behörden und Ämtern berücksichtigen. So sollte Verschlüsselung grundsätzlich vorgeschrieben und die Verwendung von Verschlüsselungsverfahren, die nicht durch die internationale Forschungsgemeinschaft geprüft wurden, ausgeschlossen werden. Dabei ist die Qualität von frei verfügbaren, offenen Protokollen und auch die Qualität von Open-Source-Software durch regelmäßige unabhängige Prüfungen sicherzustellen und durch Bug Bounty-Programme zu fördern.