Tobias Becker, Ralf Kneuper

Möglichkeiten und Grenzen der regulatorischen Einschränkung von Verschlüsselung

Folgen von staatlichen Eingriffen in Verschlüsselung

In diesem Beitrag werden Chancen und Grenzen staatlicher Regulierung von Verschlüsselung im Spannungsfeld zwischen Sicherheit und Grundrechten diskutiert. Nach einer kurzen Darstellung der rechtlichen Rahmenbedingungen werden verschiedene Regulierungsmechanismen wie Client-seitiges Scanning, Hintertüren oder Schlüsselhinterlegungssysteme analysiert und die aktuellen politischen Debatten in Deutschland, der EU, dem Vereinigten Königreich und den USA beleuchtet. Die Ergebnisse zeigen: Regulierung birgt erhebliche Risiken für Datenschutz, Cybersicherheit und Vertrauen in digitale Systeme.

1 Einleitung

Verschlüsselung hat sich zu einer unverzichtbaren Säule der modernen digitalen Kommunikation und Datensicherheit entwickelt und bildet die Grundlage für Aktivitäten wie private Nachrichtenübermittlung, Online-Banking und den Schutz kritischer Infrastrukturen. Sie bietet zwar einen robusten Schutz für die Privatsphäre und die Integrität von Informationssystemen, stellt Strafverfolgungs- und Nachrichtendienste jedoch gleichzeitig vor erhebliche Herausforderungen. Strafverfolgungsbehörden argumentieren, dass Kriminelle zunehmend Verschlüsselung nutzen, um sich der Überwachung zu entziehen und damit die Ermittlungsmöglichkeiten zu untergraben („going dark"). Der zentrale Konflikt besteht zwischen der Privatsphäre des Einzelnen und der Sicherheit der Allgemeinheit und führt zu einer anhaltenden, globalen politischen Debatte: Wie kann die Gesellschaft die Sicherheitsvorteile einer starken Verschlüsselung erhalten und gleichzeitig berechtigte Bedenken hinsichtlich der öffentlichen Sicherheit berücksichtigen? Insbesondere die Verfolgung von Straftaten im Kontext der Kinderpornographie (Child Sexual Abuse Material, CSAM) wird hier oft genannt.

Diese Arbeit verfolgt einen interdisziplinären Ansatz und untersucht rechtliche Rahmenbedingungen und politische Debatten in Deutschland, der Europäischen Union (EU), dem Vereinigten Königreich (UK) und den Vereinigten Staaten von Amerika (USA). Dabei werden vorgeschlagene oder eingesetzte Regulierungsmechanismen für den Zugriff auf verschlüsselte Daten analysiert und hinsichtlich ihrer Durchführbarkeit, Risiken und Auswirkungen bewertet.

Tobias Becker

Technischer Übersetzer, studierte Informatik (B.Sc.) an der IU Internationale Hochschule und absolviert derzeit ein Masterstudium Informatik an der University of St Andrews (UK).

E-Mail: tobias_becker@t-online.de

Ralf Kneuper

Dipl.-Mathematiker, Promotion in Informatik, LL.M. (IT und Recht), ist Professor für Datenschutz und IT-Sicherheit an der IU Internationale Hochschule – Fernstudium.

E-Mail: ralf.kneuper@iu.org

2 Rechtliche Rahmenbedingungen

In Deutschland besteht ein starker verfassungsrechtlicher Schutz der Integrität von IT-Systemen in Deutschland, der eine regulatorische Einschränkung von Verschlüsselung ausschließt. Stattdessen setzen deutsche Strafverfolgungsbehörden in einzelnen Fällen gezielt „Staatstrojaner" ein, um Daten vor der Verschlüsselung und nach der Entschlüsselung direkt auf dem Gerät zu erfassen. Diese Maßnahmen sind ressourcenintensiv und bergen Risiken wie beispielsweise die Ausnutzung von Software-Schwachstellen, die offen bleiben müssen, um diese Art von staatlicher Spionagesoftware einsetzen zu können.

In der Europäischen Union wird die Verwendung von Verschlüsselung als geeignete Sicherheitsmaßnahme in verschiedenen Kontexten ausdrücklich gefördert, beispielsweise in der Datenschutz-Grundverordnung (Art. 32 DSGVO) oder der NIS2-Richtlinie (Art. 21). Darüber hinaus hat der Europäische Gerichtshof 2014 die unterschiedslose Speicherung von Nutzungsdaten zur Kriminalitätsbekämpfung u.a. aufgrund der fehlenden Verhältnismäßigkeit für unzulässig erklärt. Vor diesem Hintergrund existiert innerhalb der gesamten EU eine erhebliche rechtliche Hürde für mögliche künftige Gesetze, die eine Entschlüsselung von Kommunikation im Sinne einer unverhältnismäßigen Massenüberwachung erzwingen würden.

Im Vereinigten Königreich erlaubt der Investigatory Powers Act (IPA) sog. Technical Capability Notices (TCNs), durch die Anbieter dazu verpflichtet werden können, Verschlüsselung bei Bedarf zu entfernen, und der Online Safety Act (OSA) erlaubt der zuständigen Behörde, Client-seitiges Scannen (CSS) auf schädliche Inhalte zu verlangen.

In den USA gibt es keine ausdrückliche Entschlüsselungspflicht. Der Communications Assistance for Law Enforcement Act (CALEA) von 1994 verlangt Telekommunikationsüberwachungsmaßnahmen, befreit jedoch Anbieter, die nicht über die entsprechenden Schlüssel verfügen, von der Pflicht zur Entschlüsselung. Um diesem Dilemma aus Sicht der US-Strafverfolgung zu begegnen, wurde der All-Writs Act, ein Gesetz aus dem 18. Jahrhundert, bereits zur Erzwingung der Unterstützung von Behörden bei der Entschlüsselung herangezogen (z. B. im Fall Apple 2016), ohne jedoch einen endgültigen Präzedenzfall zu schaffen.

Zusammenfassend lässt sich sagen, dass das Vereinigte Königreich den strengsten Kurs in Bezug auf das Erzwingen von Entschlüsselung verfolgt. Deutschland vermeidet erzwungene Entschlüsselung, und auch in der EU ist diese derzeit aufgrund diverser Urteile und Gesetze nicht möglich, es besteht jedoch erheblicher politischer Druck dies zu ändern. Die USA setzen auf individuellen rechtlichen Druck, ohne jedoch Entschlüsselung erzwingen zu können.

3 Regulierungsmechanismen

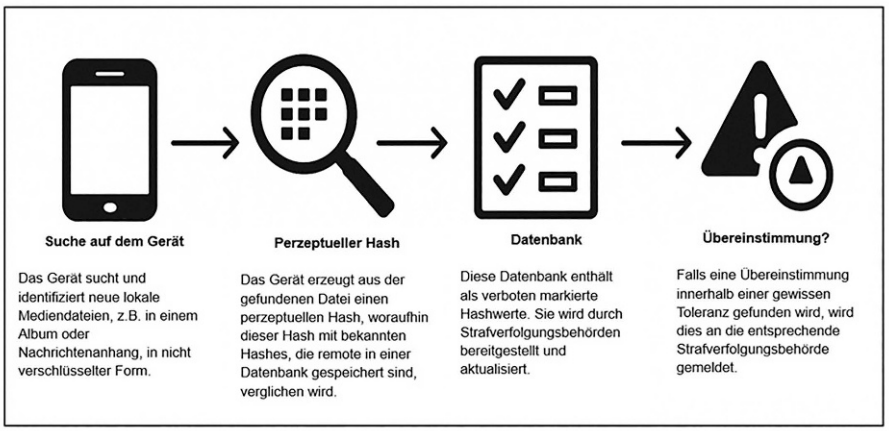
Unter Regulierungsmechanismen versteht diese Arbeit gesetzlich vorgeschriebene Methoden, die die Entschlüsselbarkeit erzwingen oder Strafverfolgungsbehörden auf andere Weise Zugang zum Klartext verschaffen. Die wichtigsten Ansätze dafür werden im Folgenden erläutert. Neben den hier beschriebenen Ansätzen gibt es noch weitere, in der Praxis selten oder nie genutzte Ansätze wie z.B. „Translucent Cryptography“ [3].

3.1 Client-seitiges Scannen

Beim *Client-seitigen Scannen* (Client-Side Scanning, CSS) werden Inhalte vor der Verschlüsselung oder nach der Entschlüsselung auf einem Gerät gescannt. Die wichtigsten technischen Ansätze dafür sind perzeptuelles Hashing und maschinelle Lernmodelle [1, S. 7].

Beim CSS mittels Perceptual Hashing werden Mediendateien wie Bilder oder Videos auf dem Gerät des Nutzers analysiert, bevor sie verschlüsselt und geteilt werden [1, S. 7]. Wie der Name schon sagt, umfasst Perceptual Hashing die Generierung eines Perceptual Hash aus den jeweiligen Mediendateien – wobei nicht die exakten Binärdaten, sondern deren visuelle Essenz erfasst wird – und den anschließenden Abgleich mit einer Datenbank bekannter illegaler oder schädlicher Inhalte. Diese Datenbank wird in der Regel von Strafverfolgungsbehörden bereitgestellt und gepflegt. Im Falle von ähnlichen oder identischen Hash-Werten markiert das System die Datei und meldet sie an den jeweiligen Systemanbieter und/oder die Strafverfolgungsbehörden. Dieser Ansatz ermöglicht die Erkennung visuell ähnlicher Dateien, selbst wenn diese leicht verändert wurden. Diese Änderungen können geringfügige Änderungen des Bildinhalts umfassen, wie z. B. die Änderung der Bildgröße oder das Zuschneiden oder Drehen von Bildern. Abbildung 1 veranschaulicht CSS mittels Perceptual Hashing in vereinfachter Form.

Abb 1 | CSS mit Perceptual Hashing



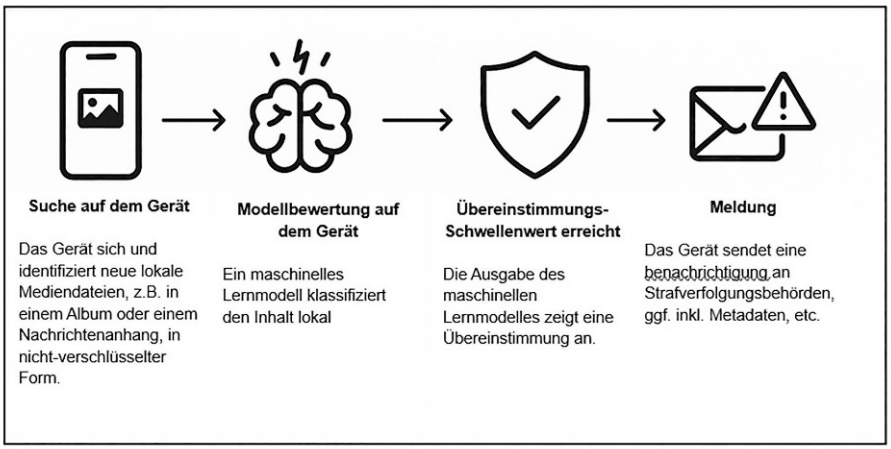
Das Client-seitige Scannen mit maschinellen Lernmodellen umfasst die Analyse von Mediendateien auf dem Gerät eines Benutzers mithilfe eines maschinellen Lernmodells. Jedes Mal, wenn ein neues Bild oder Video auf dem Gerät erkannt wird, bewertet das maschinelle Lernmodell dessen Inhalt, um festzustellen, ob es mit vordefinierten Kategorien illegaler Inhalte übereinstimmt [1, S. 7]. Wenn die Bewertung einen definierten Schwellenwert überschreitet, werden entsprechende Informationen an Strafverfolgungsbehörden weitergeleitet. Dieser Ansatz ermöglicht eine flexiblere Erkennung als Perceptual Hashing und kann potenziell neue oder geänderte Inhalte identifizieren, die zuvor nicht in der entsprechenden Datenbank katalogisiert wurden. Er gilt derzeit als die beste Methode zum Filtern von Videos und Texten. Er basiert auf überwachtem Lernen und kann im Gegensatz zum Perceptual Hashing neue Bilder des Typs erkennen, auf den er trainiert wurde. Abbildung 2 zeigt einen verallgemeinerten Arbeitsablauf von CSS über maschinelle Lernmodelle.

CSS erlangte 2021 breite Aufmerksamkeit, als Apple vorschlug, Fotos auf iPhones vor dem Hochladen in die iCloud auf CSAM zu scannen [16]. Im Mai 2022 wurde CSS auch von der Europäischen Kommission für diesen Zweck vorgeschlagen.

Abelson et al. haben eine technische Kritik an Apples Plan vorgelegt, die auch für den CSAM-Vorschlag der Europäischen Kom-

mission gilt und hervorhebt, dass CSS die Datenschutzgarantien der End-to-End-Verschlüsselung grundlegend untergräbt [1, S. 39]. Da das Scannen vor der Verschlüsselung erfolgt, werden die Daten der Nutzer auch in der privaten Kommunikation effektiv in lesbarer Form überwacht. Darüber hinaus erfolgt das Scannen auf dem Gerät des Nutzers und nicht auf Daten in der Cloud, was „die Grenze zwischen der Privatsphäre eines Nutzers und seiner gemeinsamen (halb-) öffentlichen Sphäre aufhebt" und CSS zu einer Technologie zur Massenüberwachung macht [1, S. 11]. Darüber hinaus beschreiben die Autoren sowohl Perceptual Hashing als auch maschinelle Lernmodelle aus technischer Sicht als anfällig für falsch-positive Meldungen [1, S. 8].

Abb 2 | CSS auf Basis von maschinellem Lernen



Die Zahl derartiger falsch-positiver Meldungen, die auf CSS zurückgeführt werden können, ist in den letzten Jahren stark gestiegen [2]. Wenn man bedenkt, dass die politischen Pläne der EU vorsehen, Textnachrichten zu scannen, um neben kinderpornografischen Inhalten auch schwere Straftaten im Bereich Terrorismus und Drogenhandel aufzudecken [1, S. 11], dürfte die Anzahl falsch-positiver Meldungen weiter zunehmen.

Außerdem besteht das Risiko, dass autoritäre Regimes CSS-Technologien zur Überwachung und Unterdrückung politischer Dissidenten missbrauchen könnten. Dieselben Mechanismen, die zur Bekämpfung von CSAM dienen, können auch für politische Repression genutzt werden [14, S. 10].

Auch Sicherheitsmodelle in Unternehmen wären davon betroffen. Würden CSS oder ähnliche Mechanismen vorgeschrieben, könnten Unternehmen die Kontrolle darüber verlieren, welche Daten gescannt und weitergegeben werden, was möglicherweise gegen Geheimhaltungsvereinbarungen, Regelungen zum geistigen Eigentum und Datenschutzbestimmungen wie die DSGVO verstoßen würde.

Darüber hinaus ist CSS anfällig für doppelte Verschlüsselung. Wenn ein Benutzer beispielsweise Dateien in einem verschlüsselten Zip-Ordner ablegt, kann ein CSS-System keine verwertbaren Informationen erbringen, da der Schlüssel den Strafverfolgungsbehörden trotz ihres direkten Zugriffs auf das Gerät wahrscheinlich nicht bekannt ist.

Eine weitere Herausforderung liegt in der rechtlichen Kontrolle. Im Gegensatz zu herkömmlichen Abhörmaßnahmen arbeiten CSS-Systeme präventiv und kontinuierlich [1, S. 38], unabhängig von einer zeitlich begrenzten richterlichen Genehmigung. In Anbetracht des Grundrechts auf Sicherheit und Integrität von IT-Systemen wirft dies erhebliche Fragen hinsichtlich der Verhältnismäßigkeit auf.

Zusammenfassend lässt sich sagen: CSS ist zwar technisch machbar, seine rechtliche Durchführbarkeit ist jedoch ungewiss, da es erhebliche Fragen hinsichtlich der Verhältnismäßigkeit aufwirft. Darüber hinaus gibt es ethische Probleme und technische Bedenken hinsichtlich der Wirksamkeit von CSS.

3.2 Erzwungene Software-Updates

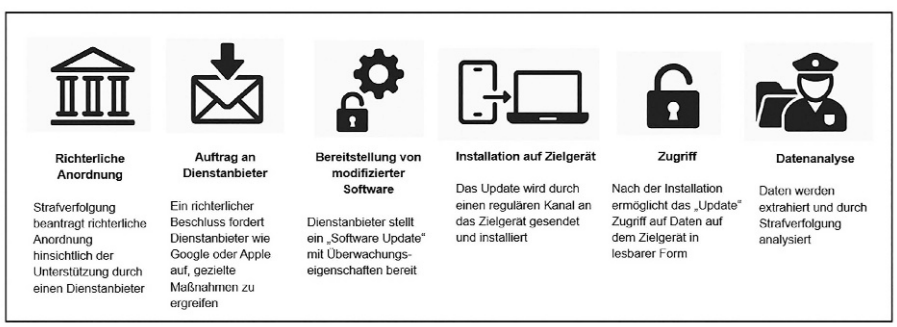
Bei *erzwungenen Software-Updates* geben Anbieter von Software speziell für bestimmte Geräte maßgeschneiderte Updates heraus und ermöglichen damit Strafverfolgungsbehörden den Zugriff auf diese Geräte [6, S. 13].

Es sind zwei Fälle bekannt, in denen derartige Anfragen gestellt wurden, beide Male an Apple: Im Jahr 2016 fordert das FBI Apple auf der Grundlage des All-Writs Act von 1789 auf, eine angepasste iOS-Version zu erstellen, um die Sicherheitsfunktionen eines iPhones zu umgehen, das einem Verdächtigen im Fall einer Schießerei gehörte [17]. In einem weiteren Fall stellte die britische Regierung Apple Berichten zufolge eine „Technical Capability Notice" (TCN) gemäß dem Investigatory Powers Act (IPA) zu, in der eine Hintertür bzw. der Zugriff auf Daten gefordert wurde (Landau, 2025). Abbildung 3 veranschaulicht den Mechanismus erzwungener Software-Updates in vereinfachter Form.

Obwohl dies technisch machbar ist, gibt es erheblichen Widerstand gegen solche Maßnahmen, u.a. von den betroffenen Unternehmen, da diese Maßnahmen das Vertrauen in Updates untergraben und das Risiko von Insider-Bedrohungen bergen. Im Ergebnis könnte die Verwendung von TCNs und ähnlicher Maßnahmen dazu führen, dass die betroffenen Dienste vom jeweiligen Markt genommen werden [8].

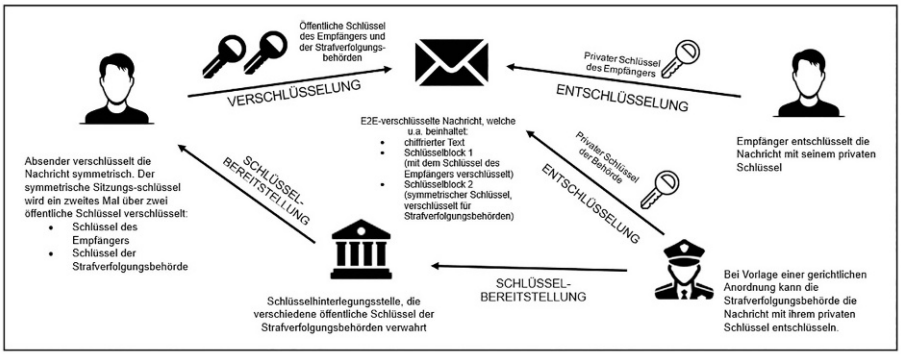
Im Vergleich zu CSS bieten erzwungene Software-Updates den Vorteil, dass sie nicht auf eine Massenüberwachung ausgedehnt werden können.

Abb. 3 | Zugriff durch erzwungene Software-Updates



Durch die Zustellung einer TCN an den jeweiligen Dienstleister verlassen kritische Informationen jedoch die staatliche Sphäre und gelangen in den Bereich von überwiegend privatrechtlichen Unternehmen. Die Mitarbeiter des Dienstleisters, die für die erzwungenen Software-Updates zuständig sind, kommen in den Besitz dieser Informationen, was das Risiko von Insider-Bedrohungen erhöht.

Abb. 4 | Vereinfachtes Schlüsselhinterlegungssystem



3.3 Schlüsselhinterlegung und Nutzung von Generalschlüsseln

Wie der Name schon sagt, gibt es bei *Schlüsselhinterlegungssystemen* (Key Escrow Systems) einen oder mehrere Schlüssel, die hinterlegt werden, sodass der Besitzer des hinterlegten Schlüssels diesen bei Bedarf verwenden kann. Bei einem Generalschlüsselsystem verfügt eine zentrale Instanz – z.B. eine Strafverfolgungsbehörde – über einen universellen Entschlüsselungsschlüssel. Mit diesem Schlüssel können alle verschlüsselten Daten entschlüsselt werden, unabhängig von Absender und Empfänger. Das Hauptproblem bei Generalschlüsseln ist das erhebliche Risiko des Missbrauchs oder der Kompromittierung, da ein einziger Schlüssel Zugriff auf alle geschützten Daten gewährt und bei Diebstahl des Schlüssels alle Daten auf einmal gefährdet sind. In der Praxis dürfte dieses System in vielen Anwendungsfällen technisch nicht umsetzbar sein, weil Anbieter wie WhatsApp und Telegram jeweils eigene Protokolle entwickelt haben, die mit dem Prinzip eines Generalschlüssels unvereinbar sind.

Bei Schlüsselhinterlegungssystemen wird jede Nachricht vom Absender mit einem zufälligen symmetrischen Sitzungsschlüssel verschlüsselt, der anschließend getrennt zweimal verschlüsselt wird: mit dem öffentlichen Schlüssel des vorgesehenen Empfängers und dem öffentlichen Schlüssel der jeweiligen Strafverfolgungsbehörde. Die asymmetrisch-verschlüsselten, symmetrischen Schlüssel werden zusammen mit der jeweiligen Nachricht gespeichert, sodass die jeweilige Strafverfolgungsbehörde die Nachricht bei Bedarf mit ihrem privaten Schlüssel entschlüsseln kann. Abhängig von den rechtlichen Rahmenbedingungen ist dafür ggf. eine richterliche Anordnung erforderlich. Abbildung 4 zeigt ein vereinfachtes Schlüsselhinterlegungssystem.

Ein bekanntes Beispiel für Schlüsselhinterlegung ist der Clipper-Chip in den Vereinigten Staaten, einem Hardware-Chip für Verschlüsselung. Der Chip erforderte, dass die entsprechenden Entschlüsselungsschlüssel bei den Strafverfolgungsbehörden hinterlegt wurden. Das Konzept wurde jedoch schnell aufgegeben, nachdem Schwachstellen im Schlüsselverwaltungsprotokoll aufgedeckt wurden, durch die böswillige Akteure Zugriff auf die verschlüsselten Daten bekommen konnten [4, S. 65]. Auch die Encryption Working Group hat wiederholt vor Schlüsselhinterlegungssystemen gewarnt [6, S. 14], weil ein entsprechendes Schlüsselverzeichnis ein sehr attraktives Angriffsziel wäre und einen zentralen Angriffspunkt darstellen würde. Dazu kommt das Risiko von Insider-Bedrohungen, denn hinterlegte Schlüssel sind nur so sicher wie die Personen und Prozesse, die sie schützen [13, S. 195].

Ferner könnte Schlüsselhinterlegung ähnlich wie CSS durch Techniken wie doppelte Verschlüsselung leicht umgangen werden [3, S. 4].

Auf internationaler Ebene würde die Einführung eines globalen Schlüsselhinterlegungssystems internationale Verträge und ein beispielloses Maß an Vertrauen und Zusammenarbeit zwischen den Ländern erfordern, was angesichts der aktuellen geopolitischen Spannungen unwahrscheinlich ist. Darüber hinaus könnten solche Systeme von autoritären Regierungen missbraucht werden und Menschenrechte und Pressefreiheit untergraben.

3.4 Abhörschnittstellen

Der Mechanismus von Abhörschnittstellen ist aus traditionellen Kommunikationssystemen bekannt, die aufgrund jahrzehntelanger Regulierung Abhörschnittstellen enthalten. Dazu gehören öffentliche Telefonnetze und moderne paketvermittelte Computernetzwerke, bei denen Netzbetreiber gesetzlich verpflichtet sind, standardisierte Schnittstellen für Strafverfolgungsbehörden bereitzustellen, damit Telefonate und die Kommunikation über Computer abgehört werden können [12, S. 1]. Die Anwendung dieses Prinzips auf Messaging-Apps, die E2EE verwenden, würde bedeuten, dass die Apps so konzipiert sind, dass sie stillschweigend eine Kopie der Kommunikationsdaten in lesbarer oder entschlüsselbarer Form an die Strafverfolgungsbehörden ausleiten. Daher müssen Abhörsysteme als Regulierungsmechanismen betrachtet werden, da sie Entschlüsselbarkeit erzwingen und gleichzeitig Informationssicherheit untergraben.

Ein Abhörsystem könnte in Form eines speziellen Modus oder Kontos umgesetzt werden, beispielsweise gemäß dem oft zitierten Konzept des britischen Government Communications Headquarters (GCHQ), bei dem ein „Geisternutzer" (ghost user) unbemerkt zu Gruppenchats hinzugefügt wird, sodass eine verschlüsselte Nachricht auch an die Strafverfolgungsbehörden ausgeleitet wird [18]. Dies würde jedoch bedeuten, dass der Kommunikationsdienstleister entweder Zugriff auf Nachrichten im Klartext hätte, was bei modernen E2EE-Systemen nicht der Fall ist, oder dass der symmetrische Sitzungsschlüssel, mit dem die Nachricht verschlüsselt wird, ein zweites Mal mit dem öffentlichen Schlüssel einer Strafverfolgungsbehörde verschlüsselt wird (wie bei manchen Schlüsselhinterlegungssystemen) und eine Kopie dieser Nachricht später aktiv an die jeweilige Strafverfolgungsbehörde ausgeleitet wird. Dadurch ähneln Abhörschnittstellen Schlüsselhinterlegungssystemen. Der Hauptunterschied zu einem Schlüsselhinterlegungssystem besteht darin, dass Kopien der Kommunikationsdaten aktiv an Strafverfolgungsbehörden gesendet werden, was bei Schlüsselhinterlegungssystemen nicht der Fall ist.

Solche Mechanismen vermeiden zwar eine Aufhebung der Verschlüsselung, beeinträchtigen jedoch Vertraulichkeit und den Identitätsnachweis. Wenn ein Dritter in eine sichere Unterhaltung eingeschleust wird, bricht das Ende-zu-Ende-Vertrauensmodell zusammen. In einem 2019 veröffentlichten offenen Brief von über 50 Organisationen, darunter Apple, Google, Microsoft und die Internet Society, wurde das Modell der Geisternutzer wegen der Gefährdung von Sicherheit und Transparenz verurteilt [10].

Im Vergleich zu Schlüsselhinterlegungssystemen bieten Abhörschnittstellen aus Sicht der Strafverfolgungsbehörden den Vorteil, dass auch auf dem jeweiligen Gerät gelöschte Daten, z.B. Chat-Nachrichten, für die Behörden verfügbar bleiben. Auf der anderen Seite kann dies zu einer Art zentraler Datenspeicherung auf Seiten der Strafverfolgungsbehörden führen. Der Vorteil, dass relevante Informationen wahrscheinlich nicht verloren gehen (im Vergleich zu Schlüsselhinterlegungssystemen), geht allerdings mit dem Nachteil einher, dass Cyberkriminelle einen zusätzlichen Angriffspunkt erhalten.

3.5 Hintertüren

Unter Hintertüren (Backdoors) werden geheime Modifikationen an Software oder kryptografischen Komponenten verstanden, die es Dritten ermöglichen, Verschlüsselung zu umgehen. Eine Hintertür unterscheidet sich von einem Schlüsselhinterlegungssystem darin, dass ein Schlüssel meist nicht der entscheidende Faktor ist. Eine Hintertür kann eine absichtliche Schwächung des Softwarecodes oder des kryptografischen Systems selbst sein.

Ein prominentes Beispiel dafür ist der Fall TETRA. TETRA ist der am weitesten verbreitete digitale Funkstandard von Polizeibehörden in mehr als 100 Ländern weltweit und wurde vom Europäischen Institut für Telekommunikationsnormen (ETSI) entwickelt. Darin wurden aber einige Schwachstellen entdeckt, darunter mindestens eine absichtliche Schwächung, die die Schlüssellänge der Verschlüsselung auf 32 Bit reduzierte, wodurch Kommunikation in weniger als einer Minute geknackt werden konnte [11].

Der Ansatz, die Verschlüsselung durch Hintertüren zu schwächen, wird als äußerst problematisch angesehen. Lord Jonathan Evans, ehemaliger Leiter des britischen MI5, erklärte 2017, dass eine solche Schwächung der Verschlüsselung auch die Cyber-Sicherheit schwächen und damit den kommerziellen wie auch den Sicherheitsinteressen des Landes schaden würde [7].

Ein weiteres Beispiel ist die Vermutung, dass die NSA einen mit einer Hintertür versehenen Zufallszahlengenerator (Dual_EC_DRBG) in einen öffentlichen Standard eingeführt habe, der es der NSA ermöglichen würde, verwendete Schlüssel bei weit verbreiteten Verschlüsselungsprodukten vorherzusagen [15].

4 Politische Debatte

Die politische Dynamik zur Regulierung von Verschlüsselung hat sich verstärkt, insbesondere im Zusammenhang mit der Bekämpfung von Terrorismus, organisierter Kriminalität und kinderpornografischen Materialien (CSAM). In der EU würde die CSAM-Verordnung („Chat Control") von einer freiwilligen Erkennung im Rahmen einer Übergangsregelung zu einer vorgeschlagenen obligatorischen Regelung übergehen, die möglicherweise CSS bedingen würde. Dies stößt auf starken Widerstand von Datenschützern, einigen Mitgliedstaaten und EU-Datenschutzbehörden, die eine Unvereinbarkeit mit den Grundrechten anführen. Die Empfehlungen [9] der High Level Group on Access to Data, einer Expertengruppe der EU, schlagen Rahmenbedingungen vor, um den Zugriff der Strafverfolgungsbehörden auf Daten in lesbarer Form zu gewährleisten, was technische Lösungen für die Entschlüsselung gespeicherter oder übertragener Daten impliziert.

Die politische Debatte im Vereinigten Königreich bezüglich der oben angeführten Auseinandersetzung zwischen Apple und der britischen Regierung vor dem Investigatory Powers Tribunal (IPT) wird wahrscheinlich einen Präzedenzfall für andere westliche Demokratien schaffen, da die Befugnisse der britischen Regierung gemäß IPA und OSA auf Widerstand von Unternehmen wie Apple stoßen, die mit der Einstellung ihrer Dienste gedroht haben, anstatt Kompromisse bei der Verschlüsselung einzugehen.

Da die mit den genannten Mechanismen eingeführten Risiken sich auch auf Bürger, Unternehmen sowie staatliche Stellen anderer Staaten auswirken, führt dies teilweise zu unterschiedlichen Sichtweisen zwischen den betroffenen Staaten, so beispielsweise Kritik der USA an den britischen Forderungen an Apple [5].

5 Folgen von Regulierungsmechanismen

Die Folgen regulatorischer Einschränkung von Verschlüsselung gehen weit über die Vorteile der potenziellen Verbrechensbekämpfung hinaus. Die Privatsphäre könnte erheblich eingeschränkt werden, was sich auf die freie Meinungsäußerung und andere Rechte auswirken würde. Die Sicherheit im weiteren Sinne wird untergraben, indem eine Art von Sicherheit gegen eine andere eingetauscht wird, was unter dem Strich jedoch negative Auswirkungen haben könnte. Anbieter von Kommunikationsdiensten könnten Vertrauensverluste erleiden, und Nutzer könnten den Zugang zu globalen sicheren Diensten verlieren, wenn sich Unternehmen aus den betroffenen Märkten zurückziehen. Strafverfolgungsbehörden gewinnen zwar einige neue Fähigkeiten, könnten aber andere verlieren, wenn sich die Vorgehensweisen von Kriminellen anpassen, und sie stellen das Vertrauen der Öffentlichkeit auf die Probe, wenn Überwachungsbefugnisse ausgeweitet werden. Politisch gibt es sowohl nationale als auch internationale Auswirkungen. Jede Entscheidung, regulatorische Einschränkungen für Verschlüsselung einzuführen, muss diese vielfältigen Auswirkungen berücksichtigen. Aus diesem Grund schlagen viele Experten vor, den Schwerpunkt weg von einer Schwächung der Verschlüsselung hin zu alternativen Möglichkeiten zur Erreichung der Strafverfolgungsziele zu verlagern – Möglichkeiten, die keine so hohen Kollateralschäden verursachen.

6 Empfehlungen

Es ist verständlich, dass Strafverfolgungsbehörden bei schweren Straftaten wie der Erstellung und Verbreitung von CSAM über umfassendere Zugriffsmöglichkeiten verfügen möchten. Wenn Gesetze jedoch Maßnahmen wie Client-seitiges Scannen, Hintertüren oder ähnliche Mechanismen zulassen, die eine Massenüberwachung ermöglichen könnten, öffnet dies der Unterdrückung politischer Gegner, Journalisten und liberaler Kräfte im Allgemeinen Tür und Tor– eine Entwicklung, die aus verschiedenen weniger demokratischen Ländern weltweit berichtet wird. Vor diesem Hintergrund sollte die politische Empfehlung lauten,

die Bemühungen zur Regulierung der Verschlüsselung aufzugeben und stattdessen alternative Wege zu beschreiten, die neue und potenziell innovative Formen der Informationsbeschaffung beinhalten. Diese umfassen zum Beispiel den gezielten Zugriff, die Zusammenarbeit mit Technologieunternehmen, alternative Informationsquellen, die allgemeine Förderung von Verschlüsselung, sowie internationalen Dialog.

7 Fazit

Keiner der derzeit vorgeschlagenen Regulierungsmechanismen kann den Strafverfolgungsbehörden einen skalierbaren, sicheren und rechtsstaatlichen Zugang zu verschlüsselten Daten gewährleisten. Jeder der beschriebenen Ansätze bringt gravierende Schwachstellen mit sich, die von böswilligen Akteuren ausgenutzt werden könnten, gleichzeitig das Vertrauen der Nutzer untergraben und die Gefahr einer Verletzung grundlegender Rechte bergen.

Verschlüsselung als Technologie basiert auf unumstößlichen mathematischen Prinzipien. Diese Prinzipien lassen sich nicht durch gesetzliche Vorschriften beugen. Wie die analysierten historischen und aktuellen Fälle zeigen, scheitern Versuche, den Zugriff auf verschlüsselte Daten gesetzlich zu regeln, an der Tatsache, dass eine Hintertür für einen eine Hintertür für alle ist. Ob es sich nun um den Clipper-Chip in den 1990er Jahren oder um die subtileren Vorschläge für Client-seitiges Scannen von heute handelt, es konnte immer wieder gezeigt werden, dass man keinen Zugriff auf verschlüsselte Kommunikation gewähren kann, ohne die Gesamtsicherheit der Systeme zu schwächen. Dies ist eine grundlegende Grenze: Mathematik kennt keine Autorität. Eine starke Verschlüsselung bleibt unabhängig von den Wünschen der Strafverfolgungsbehörden stark, und wenn sie absichtlich geschwächt wird, ist sie für alle schwächer.

Literatur

[1] Abelson, H., Anderson, R., et al. (2024). Bugs in our pockets: The risks of client-side scanning. Journal of Cybersecurity, 10(1), https://doi.org/10.1093/cybsec/tyad020

[2] Becker, M. 16.06.(2024). Deutlich mehr Falschmeldungen zu Kindesmisshandlung. Spiegel. https://www.spiegel.de/netzwelt/netzpolitik/kinderpornografie-zahl-der-falschen-verdaechtigungen-bei-online-bildern-massiv-gestiegen-a-a746b118-82e7-4560-8ba4-45f02489768c

[3] Bellare, M., & Rivest, R. L. (1999). Translucent Cryptography—An Alternative to Key Escrow, and Its Implementation via Fractional Oblivious Transfer. Journal of Cryptology, 12(2), 117–139. https://doi.org/10.1007/PL00003819

[4] Blaze, M. (1994). Protocol failure in the Escrowed Encryption Standard. ACM Conference on Computer and Communications Security. https://dl.acm.org/doi/pdf/10.1145/191177.191193

[5] Chee, F. (07.05.2025). US lawmakers criticise UK backdoor order to Apple, warn of cybercriminal risks. Reuters. https://www.reuters.com/sustainability/boards-policy-regulation/us-lawmakers-criticise-uk-backdoor-order-apple-warn-cybercriminal-risks-2025-05-07/

[6] Encryption Working Group: Moving the Encryption Policy Conversation Forward. Technical report, Carnegie Endowment for International Peace (2019). https://people.csail.mit.edu/rivest/pubs/EWG19b.pdf

[7] Grierson, J. (11.08.2017). Ex-MI5 chief warns against crackdown on encrypted messaging apps. The Guardian. https://www.theguardian.com/technology/2017/aug/11/ex-mi5-chief-warns-against-crackdown-encrypted-messaging-apps

[8] Hern, A. (18.04.2023). WhatsApp and Signal unite against online safety bill amid privacy concerns. The Guardian. https://www.theguardian.com/technology/2023/apr/18/whatsapp-signal-unite-against-online-safety-bill-privacy-messaging-apps-safety-security-uk

[9] High-Level Group. (2024). Concluding report of the High-Level Group on access to data for effective law enforcement. EU Directorate-General for Migration and Home Affairs. https://home-affairs.ec.europa.eu/document/download/4802e306-c364-4154-835b-e986a9a49281_en

[10] Internet Society (22.05.2019). Open letter on GCHQ proposal to silently add law enforcement to encrypted chats. https://newamericadotorg.s3.amazonaws.com/documents/Coalition_Letter_to_GCHQ_on_Ghost_Proposal_-_May_22_2019.pdf

[11] Krempl, S. (25.07-2023). Digitaler Behördenfunk: Massive Schwachstellen bei TETRA entdeckt. Heise online. https://www.heise.de/news/Digitaler-Behoerdenfunk-Massive-Schwachstellen-bei-TETRA-entdeckt-9226620.html

[12] Lindenmeier, C., Hammer, A., Gruber, J., Röckl, J., Freiling, F. (2024). Key extraction-based lawful access to encrypted data: Taxonomy and survey. Forensic Science International: Digital Investigation. Volume 50. https://www.sciencedirect.com/science/article/pii/S2666281724001203

[13] National Research Council (1996). Cryptography's Role in Securing the Information Society. Washington, DC: National Academies Press. https://nap.nationalacademies.org/catalog/5131/cryptographys-role-in-securing-the-information-society

[14] Rosenzweig, P. (20.08.2020). The Law and Policy of Client-Side Scanning. American University Washington College of Law American University Washington College of Law. https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?params=/context/research/article/1060/&path_info=Rosenzweig_The_Law_and_Policy_of_Client_Side_Scanning.TLS-PaperSeries.pdf

[15] Schneier, B. (15.11.2007). The Strange Story of Dual_EC_DRBG. https://www.schneier.com/blog/archives/2007/11/the_strange_sto.html

[16] Siddique, H. (15.10.2021). Apple's plan to scan for child abuse images 'tears at heart of privacy'. The Guardian. https://www.theguardian.com/world/2021/oct/15/apple-plan-scan-child-abuse-images-tears-heart-of-privacy

[17] Sorkin, A.D. (2016). The Dangerous All Writs Act Precedent in the Apple Encryption Case. The New Yorker. https://www.newyorker.com/news/amy-davidson/a-dangerous-all-writ-precedent-in-the-apple-case

[18] Privacy International (29.05.2019). Ghosts in Your Machine: Spooks Want Secret Access to Encrypted Messages. https://privacyinternational.org/news-analysis/3002/ghosts-your-machine-spooks-want-secret-access-encrypted-messages

Open Access

Funding

Open Access funding enabled and organized by Projekt DEAL.