Bild: Mario Salerno, Europäische Union

Niemand hat die Absicht …

Innenminister wollen Verschlüsselung umgehen

Die Innenminister der EU-Staaten bringen in einer Absichtserklärung Hintertüren für verschlüsselte Kommunikation wieder auf die Agenda – auf Nachfrage will das aber niemand so gemeint haben. Kritiker sehen die Freiheit jedes Einzelnen in Gefahr.

Von Jan Mahn

Die Anschläge in Wien Anfang November und zuvor in Frankreich haben die Innenminister der EU-Mitgliedsstaaten im Rat der Europäischen Union dazu veranlasst, eine gemeinsame Erklärung mit Reaktionen und möglichen Maßnahmen zu erarbeiten. Zunächst wurde eine Entwurfsfassung durch den ORF veröffentlicht, mittlerweile steht das fertige Dokument – eingestuft als „LIMITE“, also nicht automatisch zur Verbreitung in der Öffentlichkeit gedacht – unter anderem auch auf der Website des deutschen Innenministeriums zum Download bereit (siehe ct.de/ybna). Neben viel Erwartbarem enthält es einige Passagen, die Aufregung unter Datenschützern und Bürgerrechtlern ausgelöst haben.

Unter anderem kommt auch die Vorratsdatenspeicherung wieder als geeignete Maßnahme vor, an anderer Stelle werden „Online-Radikalisierung, Online-Gaming und Verstärkung durch Algorithmen“ als Probleme ausgemacht und in einem Satz vermengt. Die meiste Sprengkraft steckt aber in den Ausführungen zu Verschlüsselung, die aktuell verhindere, dass Strafverfolger auf Kommunikation zugreifen können.

Ziel, so heißt es in der Erklärung, müsse sein, dass „digitale Beweise gesetzeskonform gesammelt und von zuständigen Stellen (‚competent authorities‘) genutzt werden können“ Gleichzeitig müsse aber „die Vertrauenswürdigkeit von Produkten und Diensten erhalten bleiben, die auf Verschlüsselung basieren“. Der Widerspruch, dass man gleichzeitig das Vertrauen in Verschlüsselung nicht schwächen will und dennoch Dritten Zugriff auf die Inhalte verschaffen möchte, wird im Dokument nicht aufgelöst. Bemerkenswert ist die Formulierung „competent authorities“ (zuständige Stellen): Wie aus der geleakten Entwurfsfassung hervorgeht, wurde die Passage kurz vor Fertigstellung geändert. Zuvor stand dort stattdessen „law enforcement“, also Strafverfolgung. Welche Organisationen genau als „zuständig“ eingestuft werden, bleibt offen. Neben Strafverfolgern kann das auch alle europäischen Inlands- und Auslandsgeheimdienste einschließen.

Deutliche Reaktionen

Die Reaktionen im Netz und von Politikern fielen heftig aus. Bürgerrechts- und Datenschutzorganisationen kritisierten die Vorstöße scharf, und auch aus der Politik kamen deutliche Reaktionen. Der SPD-Europaabgeordnete Tiemo Wölken etwa bezog bei Twitter Stellung: „‚Security despite encryption‘ ist Unsinn. Es muss Schluss sein, mit dem Vorwand nationaler Sicherheit den Datenschutz online immer mehr zu schwächen. Eine sichere Gesellschaft gibt es ohne Cybersicherheit nicht – und #Verschlüsselung gehört ausdrücklich dazu.“

Eine technische Lösung für die politischen Forderungen gibt es unterdes nicht. Messenger wie Signal oder WhatsApp arbeiten mit dem Double Ratchet Algorithm – die Nachrichten werden nicht nur Ende-zu-Ende-verschlüsselt, der Schlüssel wird auch bei jeder Nachricht in Absprache mit dem Gegenüber verändert, per Diffie-Hellmann-Schlüsselaustausch wird ein neues Geheimnis vereinbart. Selbst wenn ein Angreifer einen aktuellen Schlüssel abgreifen könnte, so könnte er damit nur eine Nachricht entschlüsseln, der gesamte Verlauf bliebe geheim. Nur die beiden Endgeräte haben die Schlüssel und können die Nachrichten entschlüsseln; auch die Betreiber der Dienste sehen auf ihren Servern nur verschlüsselte Nachrichten vorbeifliegen.

Eine Möglichkeit, dennoch an die Inhalte zu gelangen, gibt es bereits. Bei der sogenannten Quellen-TKÜ müssen die Ermittler eine Schadsoftware installieren, die alle schon entschlüsselten Nachrichten – zum Beispiel als Screenshot des geöffneten Messengers – ausleitet. Die Verschlüsselung wird dabei nicht angetastet und Massenüberwachung ist nicht möglich.

Um weitere Zugriffsmöglichkeiten zu schaffen, müsste man entweder einen (grundsätzlich neuen) Verschlüsselungsalgorithmus per Gesetz vorschreiben, bei dem ein Drittschlüssel generiert und irgendwo bei einer Behörde hinterlegt wird, oder man lässt eine Hintertür einbauen, die die Verschlüsselung für einen bestimmten Zeitraum abschaltet, allen Kommunikationspartnern aber weiterhin vorgaukelt, dass die Nachrichten verschlüsselt und sicher seien. Staatliche Zugriffe auf verschlüsselte Nachrichten ohne eine Schwächung der Ende-zu-Ende-Verschlüsselung wären eine Quadratur des Kreises.

In einer Diskussionsrunde der Internet Society hielt Paul Nemitz, Hauptberater der Generaldirektion Justiz und Verbraucher der Europäischen Kommission, genau diese aber dennoch für möglich und forderte Kreativität von den Ingenieuren: „Der Umstand, dass aktuell noch keine technische Lösung existiert, gibt uns nicht das Recht, uns das Leben einfach zu machen und bei jeder praktischen Lösung sofort ‚Verschlüsselungsverbot' oder ‚Hintertür' zu rufen."

»Wir haben uns im Koalitionsvertrag grundsätzlich für die Stärkung der Ende-zu-Ende Verschlüsselung stark gemacht.«

Tankred Schipanski, digitalpolitischer Sprecher der CDU/CSU-Fraktion

Ein Verschlüsselungsverbot kommt in der Übereinkunft der Minister nicht vor, könnte aber durchaus eine indirekte Folge sein: Würde ein Gesetz alle Betreiber von Messengern zwingen, Hintertüren in die Verschlüsselung einzubauen, könnten sich Betreiber wie Telegram oder Signal durchaus weigern, das umzusetzen. Spätestens dann müssten aber Apple und Google als Betreiber der App-Stores reagieren und die Apps verbannen – Apple hat zum Beispiel schon in Konflikten mit China Position bezogen: Man sei zwar uneingeschränkt für Meinungsfreiheit, müsse sich aber an lokale Gesetze halten. Daher wurden unter anderem VPN-Apps für chinesische Nutzer aus dem Store entfernt. Die EU würde damit die Liste von Staaten ergänzen, die die Freiheit im Internet beschränken und den Zugang zu sicherer Verschlüsselung verhindern.

Die gemeinsame Erklärung der Innenminister ist im Konsens entstanden, wie es im Rat der EU üblich ist. Die Koordination hat Deutschland übernommen, das aktuell die Ratspräsidentschaft innehat. Wir fragten beim deutschen Innenministerium nach und baten um Stellungnahme zur deutschen Position.

Anders gemeint?

Auf unsere Anfrage antwortete Markus Lammert, Sprecher des Innenministeriums, zunächst grundsätzlich: „Die Bundesregierung hat sich gegen jegliche Schwächung, Modifikation oder Verbot von Verschlüsselung oder ein Kompromittieren von Sicherheitsstandards der digitalen Kommunikation bekannt." Später heißt es: „Unser Ziel ist es nicht, Verschlüsselung zu regulieren, einzuschränken oder zu verbieten – das haben wir bereits vielfach klargestellt und diese Haltung besteht somit unverändert."

Durch die Verbreitung starker Verschlüsselungsverfahren dürfen aber, so der Sprecher, die gesetzlichen Befugnisse der Strafverfolgungs- und Sicherheitsbehörden nicht ausgehöhlt werden. Weiter heißt es: „Wir wollen den Providern (z. B. den Anbietern von sog. ‚Instant Messaging Services' und ‚Sozialen Netzwerken') die Entscheidung überlassen, wie sie verschlüsselte Kommunikation als Regelfall und staatlichen Zugriff auf die Kommunikationsinhalte als gesetzlich geregelte Ausnahme gewährleisten. Wir stehen hier noch am Anfang einer Lösungsfindung, die wir gemeinsam und im Dialog angehen müssen." Auf die Frage, ob ein solcher Eingriff mit dem Grundgesetz in Einklang zu bringen wäre und ob vorab eine verfassungsrechtliche Prüfung stattgefunden hat, bekamen wir keine Antwort.

Mit einer Bitte um Einschätzung wandten wir uns an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) und erhielten deutliche Worte von Pressesprecher Christof Stein. Demnach seien im „Hinblick auf die Datensicherheit im vorliegenden Kontext – auch ohne Kenntnis weiterer Details – verfassungsrechtliche Bedenken angebracht". Weiter heißt es: „Die von den EU-Innenministern erwogenen Mechanismen sind auch nicht zielführend, weil gerade die damit anvisierten Zielpersonen auf alternative Kommunikationswege oder anderweitige Verschlüsselungsverfahren ausweichen können. Die Erforderlichkeit von Hintertüren ist auch deshalb zweifelhaft, weil die Sicherheitsbehörden und Nachrichtendienste derzeit schon über Mittel verfügen, die auf die Umgehung der Verschlüsselung zielen (zum Beispiel die Quellen-Telekommunikationsüberwachung). Hintertüren und geschwächte Sicherheitsfunktionen sind damit nicht erforderlich." Damit greift er das häufigste Argument der Kritiker auf: Terroristen und Kriminelle würden ihre Kommunikation auf andere Plattformen verlagern, während gleichzeitig eine Massenüberwachung aller Bürger nicht mehr ausgeschlossen wäre.

Selbst fraktionsintern ist die Linie des CSU-geführten Ministeriums umstritten. Auf Anfrage antwortete uns Tankred Schipanski, Sprecher für Digitale Agenda der CDU/CSU-Fraktion im Bundestag: „Wir haben uns im Koalitionsvertrag grundsätzlich für die Stärkung der Ende-zu-Ende Verschlüsselung stark gemacht. Vor diesem Hintergrund wäre der nun diskutierte Entwurf für mich kein gangbarer Weg. Vielmehr wollen wir das Vertrauen in sichere digitale Dienste stärken. Ferner haben wir mit der Verabschiedung der Quellen-TKÜ bereits unter hohen Hürden den Zugang in besonderen Ausnahmesituationen für bestimmte Sicherheitsbehörden genehmigt."

Wie es weitergeht

Eine Absichtserklärung der Innenminister ist noch kein Gesetz, könnte die Gesetzgebung auf europäischer Ebene aber ins Rollen bringen, zumal auch die Europäische Kommission in dieselbe Richtung arbeitet. Auf unsere Anfrage, ob dort eine Gesetzesinitiative geplant sei, hieß es von einem Kommissionssprecher: „Die Kommission wird ausgewogene technische, operative und rechtliche Lösungen für die bestehenden Herausforderungen prüfen und unterstützen und einen Ansatz fördern, der sowohl die Wirksamkeit der Verschlüsselung [...] als auch eine wirksame Reaktion auf Kriminalität und Terrorismus gewährleistet."

In jedem Fall müsste ein solches Gesetz das Europäische Parlament passieren – angesichts der ablehnenden Reaktionen von EU-Parlamentariern fast aller Fraktionen ist eine Mehrheit aktuell mehr als unsicher. *(jam@ct.de)* c't

Stellungnahmen im Wortlaut: ***ct.de/ybna***