**Schriftliche Antwort von Dr. Markus Lammert**

**Pressesprecher des Bundesministerium des Innern, für Bau und Heimat**

Die Bundesregierung hat sich gegen jegliche Schwächung, Modifikation oder Verbot von Verschlüsselung oder ein Kompromittieren von Sicherheitsstandards der digitalen Kommunikation bekannt. Dies hat weiterhin Bestand. [bereits im Jahr 1999, Kabinettbeschluss „Eckpunkte der deutschen Kryptopolitik“] Durch die Verbreitung starker Verschlüsselungsverfahren dürfen die gesetzlichen Befugnisse der Strafverfolgungs- und Sicherheitsbehörden aber nicht ausgehöhlt werden. Unsere Sicherheitsbehörden müssen unter strengen gesetzlichen Voraussetzungen befugt und in der Lage sein, verschlüsselte Kommunikation (auch auf Endgeräten), zu entschlüsseln oder zu umgehen, wenn dies zum Schutz der Bevölkerung notwendig ist. Das steht auch nicht im Widerspruch zum Ziel der Bundesregierung (Digitale Agenda von 2014) Deutschland zum „Verschlüsselungsstandort Nr. 1“ weiter auszubauen. Unser Ziel ist es nicht, Verschlüsselung zu regulieren, einzuschränken oder zu verbieten – das haben wir bereits vielfach klargestellt und diese Haltung besteht somit unverändert. Wir wollen auch weiterhin keine Hintertüren oder Verschlüsselungsverbote. Gleichwohl benötigen wir einen klaren und technikneutralen Ansatz, der eine Lösung für diese Herausforderung aufzeigt. 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.

Bundesinnenminister Seehofer hat sich im Übrigen letzten Freitag im Anschluss an den Innenministerrat zu dieser Frage ebenfalls geäußert. Sie können seine Antwort hier (ab Minute 15,30) https://www.youtube.com/watch?v=-J2pAGddvHA

Ich kann Sie zudem auf unsere Pressemitteilung vom letzten Freitag und die darin enthaltene Deklaration verweisen. Sie ist weiterhin hier abzurufen: https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2020/11/eu-innenminister-201113.html. Der Eindruck, die Erklärung sei nur über die Veröffentlichung bei statewatch einsehbar geht also fehl.

*18.11.2020*

**Schriftliche Antwort von Christof Stein**

**Pressesprecher des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit**

Die Ausgestaltung der Instrumente zur Umgehung von Ende-zu-Ende-Verschlüsselung unterliegt besonderen verfassungsrechtlichen Anforderungen insbesondere hinsichtlich der Datensicherheit, des Umfangs der Datenverwendung, der Transparenz und des Rechtsschutzes. Auch wenn die genaue rechtliche Beurteilung einer Maßnahme von ihrer konkreten Ausgestaltung abhängt, sind im Hinblick auf die Datensicherheit im vorliegenden Kontext – auch ohne Kenntnis weiterer Details – verfassungsrechtliche Bedenken angebracht. Die Umgehung einer Verschlüsselung erfordert die Gewährleistung besonders hoher Standards der Datensicherheit. Dabei muss sich dieser am Entwicklungsstand der Fachdiskussion orientieren. Nach den aktuellen fachlichen Erkenntnissen ist ein Zugriff auf Ende-zu-Ende verschlüsselte Daten nur über „Backdoors“ oder „Generalschlüssel“ möglich. Es handelt sich um Methoden, die weder kontrollierbar noch zielführend sind. Die damit verbundene allgemeine Schwächung der Sicherheit, Vertraulichkeit und damit des Datenschutzes im Bereich der elektronischen Kommunikation birgt ein erhebliches Risiko eines – möglicherweise auch großflächigen – Datenmissbrauchs.
Es lässt sich nämlich nicht ausschließen, dass die damit eröffneten Sicherheitslücken nicht nur von den zuständigen Sicherheitsbehörden, sondern auch von Dritten beziehungsweise von Kriminellen genutzt werden. 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.

*19.11.2020*

**Schriftliche Antwort von Tankred Schipanski, MdB**
**Sprecher für Digitale Agenda der CDU/CSU-Fraktion im Deutschen 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. Des Weiteren bin ich skeptisch, ob die diskutierten Maßnahmen den gewünschten Erfolg bringen würde. Nutzer mit entsprechenden verbrecherischen Absichten könnten diese meiner Einschätzung nach mit relativ wenig technischem Aufwand umgehen. Vor diesem Hintergrund unterstütze ich die Position der Bundesregierung, die Ende-zu-Ende Verschlüsselung weiter zu fördern.

*19.11.2020*

**Schriftliche Antwort eines Sprechers der Europäischen Union**

Verschlüsselung ist ein wichtiges Instrument zur Verbesserung der Cybersicherheit und zum Schutz der Grundrechte, wie z.B. der Privatsphäre, einschließlich der Vertraulichkeit der Kommunikation, und der persönlichen Daten. Gleichzeitig kann sie aber auch von Tätern genutzt werden, die einen sicheren Kanal suchen, um ihre Handlungen vor Strafverfolgungs- und Justizbehörden zu verbergen, was die Untersuchung, Aufdeckung und Verfolgung von Straftaten erschwert.

Die Mitgliedstaaten haben mehrfach in verschiedenen Gremien des Rates die Herausforderungen im Zusammenhang mit der Verwendung von Verschlüsselung für kriminelle Zwecke erörtert. Sie haben Lösungen gefordert, die den Strafverfolgungsbehörden und anderen zuständigen Behörden den rechtmäßigen Zugang zu digitalen Beweismitteln ermöglichen, ohne die Verschlüsselung direkt oder indirekt zu verbieten oder zu schwächen, und unter uneingeschränkter Achtung der Privatsphäre und der Garantien für ein faires Verfahren im Einklang mit dem geltenden Recht.

Wie in der im Juli 2020 vorgelegten Strategie der Sicherheitsunion erläutert, wird die Kommission ausgewogene technische, operationelle und rechtliche Lösungen prüfen und unterstützen und einen Ansatz fördern, der sowohl die Wirksamkeit der Verschlüsselung beim Schutz der Privatsphäre und der Sicherheit der Kommunikation aufrechterhält als auch eine wirksame Antwort auf schwere Kriminalität und Terrorismus bietet.

Konkret heißt es dazu in der EU-Strategie für eine Sicherheitsunion von Juli: „Heute betrifft ein erheblicher Teil der Ermittlungen gegen alle Formen von Kriminalität und Terrorismus verschlüsselte Informationen. Verschlüsselung ist für die digitale Welt ein wesentlicher Faktor, da dadurch digitale Systeme und Transaktionen gesichert und zudem eine Reihe von Grundrechten geschützt werden, darunter die Freiheit der Meinungsäußerung und der Schutz der Privatsphäre und personenbezogener Daten. Wird Verschlüsselung jedoch für kriminelle Zwecke eingesetzt, kann sie auch dazu dienen, die Identität von Straftätern zu verschleiern und den Inhalt ihrer Kommunikation zu verbergen. 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 beim Schutz der Privatsphäre und der Sicherheit bei der Kommunikation als auch eine wirksame Reaktion auf Kriminalität und Terrorismus gewährleistet.“

*19.11.2020*