Deutscher Bundestag **Drucksache 18/5144**

18. Wahlperiode 11.06.2015

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Wolfgang Gehrcke, Jan van Aken, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/5013 –

Anstrengungen von Europol, INTERPOL und der Europäischen Kommission zum Aushebeln von Verschlüsselungstechniken

Vorbemerkung der Fragesteller

Rob Wainwright, der Direktor des Europäischen Polizeiamts Europol, hat in Interviews mehrmals vor der zunehmenden Nutzung von Verschlüsselungstechnologien gewarnt (Onlineausgabe der BBC vom 29. März 2015, Onlineausgabe Die Presse vom 5. Mai 2015). Verschlüsselung sei demnach „eines der Hauptinstrumente von Terroristen und Kriminellen“. Sie verwendeten die Technologie, um „ihre Identitäten zu verbergen“. Der Europol-Chef, Rob Wainwright, war Teilnehmer einer Konferenz im österreichischen St. Pölten mit 20 geladenen europäischen Innenministern. Am sogenannten Salzburg Forum nahmen außer Österreich, Italien und Deutschland vor allem südosteuropäische Länder teil. Allerdings solle Verschlüsselung laut dem Europol-Chef nicht komplett verboten werden. Auch seien Hintertüren eher ungeeignet, denn darüber würden die Anwendungen womöglich auch von Dritten kompromittiert. Vielmehr sollten Behörden „mit Technologiefirmen kooperieren“, um auf diese Weise „Zugang zur Kommunikation jener Personen zu bekommen, die unsere Gesellschaft beschädigen wollen“. Es ist unklar, welche „Technologiefirmen“ hier gemeint sind. Vermutlich handelt es sich um die Firmen Google, Facebook und Microsoft, mit denen sich Europol bereits im Oktober 2014 zum Abendessen traf (Bundestagsdrucksache 18/4582). Zusammen mit den Innenministern der Europäischen Union (EU) wollte Europol die Internetdienstleister für einfachere Verfahren zur Löschung unliebsamer Internetinhalte bewegen. Ein weiteres Treffen mit den Internetdienstleistern soll diesen Monat stattfinden. Die Europäische Kommission kündigte an, bei dem Treffen sollten auch „Bedenken der Strafverfolgungsbehörden in Bezug auf die neuen Verschlüsselungstechniken Raum gegeben werden“ (Kommissionsdokument COM(2015) 185 final vom 28. April 2015).

Im Januar 2015 hatte bereits der EU-Anti-Terror-Koordinator Gilles de Kerchove gefordert, Internet- und Telekommunikationsanbieter zum Einbau von Hintertüren für verschlüsselte Kommunikation zu zwingen (www.statewatch.org/news/2015/jan/eu-council-ct-ds-1035-15.pdf). Die Forderung steht unter der Überschrift „Verschlüsselung/Abhören“ und bezieht sich auf die Veröffent-

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 9. Juni 2015 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

lichungen von Edward Snowden. Demnach würden im Zuge der NSA-Affäre (NSA – National Security Agency) viele IT-Anbieter dezentrale Verschlüsselungsverfahren anbieten, was das behördliche Abhören zusehends erschwere. Die Europäische Kommission soll nun rechtliche Möglichkeiten untersuchen, nach denen die Firmen zur Herausgabe von Schlüsseln gezwungen werden könnten. Unklar ist, inwiefern dies lediglich in der EU ansässige Unternehmen beträfe. Mit einem ähnlichen Vorstoß hatte der britische Premierminister David Cameron Furore gemacht, sein Vorschlag wurde vom US-Präsidenten Barack Obama unterstützt (Onlineausgabe The Wall Street Journal vom 16. Januar 2015).

Auch der Bundesminister des Innern, Dr. Thomas de Maizière, hatte sich zunächst entsprechend geäußert. Auf dem „Internationalen Forum für Cybersicherheit“ im nordfranzösischen Lille erklärte Dr. Thomas de Maizière laut „AFP“, die deutschen Sicherheitsbehörden müssten „befugt und in der Lage sein, verschlüsselte Kommunikation zu entschlüsseln oder zu umgehen, wenn dies für ihre Arbeit zum Schutz der Bevölkerung notwendig ist“ (Pressemitteilung des Bundesministeriums des Innern – BMI – vom 20. Januar 2015, SPIEGEL ONLINE vom 21. Januar 2015). Verschlüsselte Internetkommunikation mache „an Landesgrenzen aber nicht halt“. Ähnlich äußerte sich auch das Innenministerium Österreichs (futurezone vom 22. Januar 2015).

1. An welchen Treffen haben welche Bundesbehörden in den Jahren 2014 und 2015 teilgenommen, bei denen Angehörige von Europol, INTERPOL, der Europäischen Kommission, dem Projekt ENLETS oder des EU-Anti-Terrorismus-Koordinators vor einer zunehmenden Nutzung von Verschlüsselungstechnologien gewarnt haben und bzw. oder forderten, Möglichkeiten zu deren Umgehung, Aushebelung oder Unbrauchbarmachung zu beforschen oder einzuführen?

2. Welche Probleme wurden im Rahmen der Beiträge konkret definiert, und welche Forderungen wurden erhoben?

3. Welche Beiträge haben Bundesbehörden aus diesem Anlass (auch reaktiv) erbracht?

Die Fragen 1 bis 3 werden zusammen beantwortet.

Der Bundesregierung ist bekannt, dass sich der EU Counter Terrorism Coordinator (CTC) Giles de Kerchove im Vorfeld des informellen JI-Rats in Riga (Januar 2015) in einem eigenen Diskussionspapier mit aktuellen europäischen Sicherheitsfragen auseinander gesetzt hat und dabei auch auf Herausforderungen beim Thema Verschlüsselung eingegangen ist. Das Papier wurde den Teilnehmern des JI-Rats zur Verfügung gestellt.

Der Bundesregierung sind keine weiteren Treffen der genannten Ausrichter bekannt, an denen Bundesbehörden teilgenommen haben und in denen die in der Fragestellung genannten Themenkomplexe explizit behandelt wurden.

4. Was ist der Bundesregierung darüber bekannt, inwiefern und mit welchem Inhalt in den Jahren 2014 und 2015 auch bei Treffen internationaler Zusammenschlüsse, wie den G6, den G7, dem Salzburg Forum oder der Police Working Group on Terrorism, über Möglichkeiten zur Umgehung, Aushebelung oder Unbrauchbarmachung von Verschlüsselungstechniken diskutiert wurde?

Im Rahmen der internationalen Zusammenschlüsse G6, G7 und Police Working Group on Terrorism wurde diese Thematik nicht diskutiert. Am Salzburg Forum 2015 erfolgte seitens Deutschlands keine Teilnahme; laut Tagesordnung stand dieses Thema dort nicht auf der Agenda.

5. Inwiefern ist auch die Bundesregierung, wie der Europol-Chef, der Auffassung, Verschlüsselung sei „eines der Hauptinstrumente von Terroristen und Kriminellen“?

Die Nutzung von Verschlüsselungstechniken nimmt allgemein zu. In vielen Phänomen- und Kriminalitätsbereichen, bspw. im Islamistischen Terrorismus, ist das Streben nach einer abgeschirmten, klandestinen Übermittlung von Informationen prägendes Wesensmerkmal im Kommunikationsverhalten. Eine besondere Bedeutung messen die handelnden Akteure hierbei der Verschlüsselung der Kommunikationsinhalte sowie der Verschleierung ihrer Identität zu. Ziel ist es jeweils, die staatlichen Aufklärungs- und Bekämpfungsmaßnahmen ins Leere laufen zu lassen. Dies stellt für Sicherheitsbehörden eine Herausforderung dar. Ermittlungsverfahren werden dadurch erschwert, wenn nicht sogar verhindert.

6. Inwiefern und auf welcher Rechtsgrundlage ist es Bundesbehörden aus Sicht der Bundesregierung bereits jetzt gestattet, verschlüsselte Kommunikation zu umgehen, auszuhebeln oder unbrauchbar zu machen?

Grundsätzlich ist es in Deutschland jeder Person erlaubnisfrei gestattet, in privaten Angelegenheiten verschlüsselt zu kommunizieren. Es besteht keine Rechtsgrundlage, einzelnen Personen die Nutzung verschlüsselter Kommunikationsmethoden – aus welchem Grund auch immer – zu untersagen. Die Bundesregierung hat es sich zum Ziel gesetzt, die Sicherheit der Bürgerinnen und Bürger im Internet zu verbessern. Dies umfasst die Datensicherheit und das Vertrauen der Bürgerinnen und Bürger in die Unverletzlichkeit von IT-Systemen. Durch die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) wird diesem Ziel Rechnung getragen.

Dem staatlichen Zugriff auf Kommunikationsinhalte sind durch Artikel 10 des Grundgesetzes (GG) und die einschlägigen Fachgesetze enge Grenzen gesetzt. Für den Bereich der Nachrichtendienste des Bundes sind die Befugnisse in den Fachgesetzen Bundesverfassungsschutzgesetz (BVerfSchG), Bundesnachrichtendienstgesetz (BNDG) und des Gesetzes über den militärischen Abschirmdienst (MADG) sowie dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G10) geregelt. Die Befugnisse der Ermittlungsbehörden des Bundes sind im Bundeskriminalamtgesetz (BKAG), Bundespolizeigesetz (BPolG), des Gesetzes über das Zollkriminalamt und die Zollfahndungsämter (ZFdG) sowie der Strafprozessordnung (StPO) abschließend geregelt. Eingriffe in das Post- und Fernmeldegeheimnis unterliegen für den Bereich der Nachrichtendienste des Bundes zudem der Kontrolle durch die G-10-Kommission des Deutschen Bundestages.

Soweit auf der Grundlage dieser Gesetze eine Kenntnisnahme der berechtigten Stellen von Kommunikationsinhalten zulässig ist, wird verschlüsselte Kommunikation nicht anders behandelt, als unverschlüsselte. Den berechtigten Stellen ist es daher gestattet, rechtmäßig abgefangene, aber nutzerseitig verschlüsselte Kommunikation im Rahmen des technisch Möglichen zu entschlüsseln.

Soweit TK-Anbieter Kommunikation beim Transport über ihre Netze selbst netzseitig verschlüsseln, ist diese Verschlüsselung vor der Ausleitung an die berechtigte Stelle wieder durch den TK-Anbieter aufzuheben (§ 8 Absatz 3 der Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation – TKÜV).

Wenn Kommunikation nutzerseitig verschlüsselt wird, besteht allerdings keine Rechtsgrundlage, den Nutzer zur Herausgabe des Schlüssels an die berechtigte Stelle zu zwingen. Soweit allerdings – etwa im Rahmen von rechtmäßigen Ermittlungsmaßnahmen wie Durchsuchung, Beschlagnahme oder Herausgabeverlangen (§ 95 StPO) – Ermittlungsbehörden Zugriff auf den Schlüssel erhalten,

darf dieser auch zur Entschlüsselung der rechtmäßig abgefangenen Kommunikation eingesetzt werden.

7. Welche Techniken und Werkzeuge kommen bei Bundesbehörden zur Verschlüsselung zum Einsatz (etwa SSL, PGP, serverseitig, clientseitig)?

In der Bundesverwaltung kommt eine Vielzahl von verschiedenen Produkten zur Verschlüsselung zum Einsatz. Für die Verschlüsselung von eingestuften Informationen müssen diese Produkte gemäß § 37 Absatz 1 der Verschlusssachenanweisung des Bundes vom BSI zugelassen sein.

Die Zulassungen des BSI erfolgen abgestuft nach der Schutzbedürftigkeit von IT-Anwendungen. Die Liste der zugelassenen Produkte ist auf der Homepage des BSI einsehbar. Im Übrigen veröffentlicht das BSI regelmäßig Technische Richtlinien, in denen Algorithmen empfohlen werden, die nach heutigem Stand als sicher gelten.

8. Welche Techniken und Werkzeuge kommen bei Bundesbehörden für die Umgehung, Aushebelung oder Unbrauchbarmachung von Verschlüsselungstechniken zum Einsatz?

Wie in der Antwort zu Frage 6 ausgeführt, richtet sich der Zugriff auf Kommunikationsinhalte nach den jeweiligen gesetzlichen Grundlagen. Für das Umgehen, Aushebeln oder Unbrauchbarmachen von Verschlüsselungstechniken existieren keine universell einsatzbaren technischen Lösungen. Es können je nach Anwendungsfall gängige Werkzeuge nach dem Stand der Technik zum Einsatz kommen.

9. Welche technischen Defizite existieren aus Sicht der Bundesregierung hinsichtlich der Umgehung, Aushebelung oder Unbrauchbarmachung von Verschlüsselungstechniken?

Gegebenenfalls vorhandene technische Defizite sind unter den individuellen Umständen und Rahmenbedingungen des jeweiligen Einsatzes zu betrachten und zu bewerten. Im Übrigen wird auf die Antwort zu Frage 8 verwiesen.

10. Welchen internationalen Regelungsbedarf sieht die Bundesregierung hinsichtlich der Umgehung, Aushebelung oder Unbrauchbarmachung von Verschlüsselungstechniken?

Die Bundesregierung sieht hinsichtlich des Umgehens, Aushebelns oder Unbrauchbarmachens von Verschlüsselungstechniken keinen internationalen Handlungsbedarf. Im Übrigen hat der Kabinettbeschluss „Eckpunkte der deutschen Kryptopolitik“ von 1999 nach wie vor Bestand. Die digitale Agenda der Bundesregierung umfasst das Ziel, Deutschland zum „Verschlüsselungsstandort Nr. 1“ zu machen. Die Entwicklung und durchgängige Verwendung vertrauenswürdiger IT-Sicherheitstechnologien ist von entscheidender Bedeutung für Unternehmen, Verwaltung und Bürger in unserer heutigen Informationsgesellschaft. Daher wird die gezielte Schwächung oder Regulierung von Verschlüsselungstechniken von der Bundesregierung nicht verfolgt.

11. Inwiefern teilen auch deutsche Strafverfolgungsbehörden die von der Europäischen Kommission gemeldeten „Bedenken“ in Bezug auf die „neuen Verschlüsselungstechniken“, denen bei Treffen mit Internetdienstleistern „Raum gegeben werden“ soll?

Der Bundesregierung ist bekannt, dass die Europäische Kommission ausweislich der Mitteilung der Kommission (KOM(2015) 185 final) „Die Europäische Sicherheitsagenda“, IT-Unternehmen mit Strafverfolgungsbehörden und Vertretern der Zivilgesellschaft zusammen bringen möchte, um die besten Instrumente zur Bekämpfung terroristischer Propaganda im Internet und in den sozialen Medien zu verbreiten, und dass in diesem Rahmen auch den Bedenken der Strafverfolgungsbehörden in Bezug auf die neuen Verschlüsselungstechniken Raum gegeben werden soll. In welcher Form den diesbezüglichen Bedenken Raum gegeben werden soll, ist der Bundesregierung noch nicht bekannt.

Es ist auch nicht bekannt, ob dieses „Forum“ in der direkten Kontinuität des bisherigen Austauschs der EU-Innenminister mit Vertretern von Internet-Diensteanbietern steht (vgl. Antwort zu Frage 14).

Grundsätzlich anzumerken ist, dass die zunehmende Nutzung von Verschlüsselungstechnologien in Kriminalitätsbereichen und die daraus resultierenden Probleme bei der Identifizierung von Straftätern eine Herausforderung für die Innere Sicherheit darstellen (auf die Antwort zu Frage 5 wird verwiesen). Jedweder Dialog mit Internet-Diensteanbietern, um nach Möglichkeiten zu suchen den unterschiedlichen Bedürfnissen im Verhältnis Datenschutz zu Gefahrenabwehr und Strafverfolgung gerecht zu werden, ist daher aus Sicht der Bundesregierung zu begrüßen.

12. Was ist der Bundesregierung über Pläne von Europol bekannt, die Kooperation von nationalen Behörden mit „Technologiefirmen“ hinsichtlich der Umgehung, Aushebelung oder Unbrauchbarmachung von Verschlüsselungstechniken zu verbessern, um dadurch „Zugang zur Kommunikation jener Personen zu bekommen, die unsere Gesellschaft beschädigen wollen“?

Der Bundesregierung sind keine Bestrebungen von Europol bekannt, die Kooperation von nationalen Behörden mit Technologiefirmen zu verbessern.

13. Was ist der Bundesregierung darüber bekannt, inwiefern Europol Möglichkeiten zur Umgehung, Aushebelung oder Unbrauchbarmachung von Verschlüsselungstechniken auch bei jenen Treffen mit den Firmen Google, Facebook, Youtube oder Microsoft ansprechen will, die eigentlich zum leichteren Löschen oder Sperren von Internetinhalten (etwa unter Einbezug der noch zu gründenden „EU Internet Referral Unit“) anberaumt wurden?

Der Bundesregierung ist bekannt, dass die geplante „Internet Referral Unit“ von Europol gemäß ihrem Mandat perspektivisch auch einen Austausch mit den genannten Unternehmen etablieren soll. Es ist nicht bekannt, dass bei Treffen in diesem Zusammenhang auch das „Umgehen, Aushebeln oder Unbrauchbarmachen von Verschlüsselungstechniken“ angesprochen werden soll.

Der Bundesregierung ist weiterhin bekannt, dass die Europäische Kommission in ihrer Mitteilung „Die Europäische Sicherheitsagenda“ ankündigt, dass im Rahmen eines Forums, bei dem IT-Unternehmen mit Strafverfolgungsbehörden und Vertretern der Zivilgesellschaft zusammenkommen, auch den Bedenken der Strafverfolgungsbehörden in Bezug auf die neuen Verschlüsselungstechniken Raum gegeben werden soll (vgl. auch Antwort zu Frage 11). Die Bundesregie-

rung hat keine Kenntnis, inwieweit Europol an diesen Treffen teilnehmen wird und welche Themen es dort anzusprechen beabsichtigt.

14. Welche Haltung vertritt die Bundesregierung zur Frage, inwiefern es sich bei den im Oktober 2014 begonnenen Zusammenarbeitsformen der EU-Innenminister und Europol mit den Firmen Google, Facebook, Youtube oder Microsoft zum leichteren Löschen oder Sperren von Internetinhalten um ein geeignetes Forum handelt, die Umgehung, Aushebelung oder Unbrauchbarmachung von Verschlüsselungstechniken zu diskutieren?

Am 8. Oktober 2014 fand am Vorabend des JI-Rates auf Einladung der damaligen EU-Innenkommissarin ein Abendessen der EU-Innenminister mit den genannten Firmen in Luxemburg statt. Europol hat an diesem Treffen nicht teilgenommen. Gegenstand der Gespräche waren die Herausforderungen, die aus der Nutzung des Internets durch Terroristen und der Verbreitung strafbarer Inhalte erwachsen. Das Thema „Umgehen, Aushebeln oder Unbrauchbarmachen von Verschlüsselungstechniken“ war nicht Gegenstand der Gespräche. Auf die Antworten der Bundesregierung auf die Kleinen Anfragen der Fraktion DIE LINKE. auf Bundestagsdrucksachen 18/3655 und 18/4582 wird verwiesen.

15. Was ist der Bundesregierung darüber bekannt, inwiefern die Europäische Kommission rechtliche oder technische Möglichkeiten untersucht, untersuchen will oder untersuchen soll, nach denen die Firmen zur Herausgabe von Schlüsseln für die Verschlüsselungstechnik gezwungen werden könnten?

Zu entsprechenden Vorhaben der Europäischen Kommission liegen der Bundesregierung keine Erkenntnisse vor.

16. Was ist der Bundesregierung darüber bekannt, inwiefern auch die noch zu gründende „EU Internet Referral Unit“ die Umgehung, Aushebelung oder Unbrauchbarmachung von Verschlüsselungstechniken untersuchen, erörtern oder einsetzen soll?

Der Bundesregierung ist aus den bislang vorliegenden Dokumenten zum Mandat der „Internet Referral Unit“ nicht bekannt, dass dieses Themenfeld dort bearbeitet werden soll.

17. Sofern der Bundesregierung hierzu keine Kenntnisse vorliegen, welche eigene Position vertritt sie hierzu?

Die Bundesregierung unterstützt die mit der Europol „Internet Referral Unit“ verfolgten Ziele.

18. Was ist der Bundesregierung über sonstige Studien oder Erhebungen der Europäischen Kommission, von Europol oder ENLETS bekannt, die die Umgehung, Aushebelung oder Unbrauchbarmachung von Verschlüsselungstechniken zum Inhalt haben?

Der Bundesregierung sind keine entsprechenden Studien oder Erhebungen der Europäischen Kommission, Europols oder ENLETS bekannt.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333