



POSTANSCHRIFT Bundesministerium des Innern, 11014 Berlin

Präsident des Deutschen Bundestages
– Parlamentssekretariat –
Reichstagsgebäude
11011 Berlin

HAUSANSCHRIFT Alt-Moabit 140, 10557 Berlin

POSTANSCHRIFT 11014 Berlin

TEL +49 (0)30 18 681-11117

FAX +49 (0)30 18 681-11019

INTERNET www.bmi.bund.de

DATUM 24. Oktober 2016

BETREFF **Kleine Anfrage des Abgeordneten Andrej Hunko u. a. und der Fraktion
DIE LINKE.
EU-Maßnahmen für den Zugang von Strafverfolgungsbehörden zu
verschlüsselter Kommunikation
BT-Drucksache 18/9919**

Auf die Kleine Anfrage übersende ich namens der Bundesregierung die beigefügte
Antwort in 4-facher Ausfertigung.

Hinweis:

Ein Antwortteil ist VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuft.

Mit freundlichen Grüßen
in Vertretung



Dr. Günter Krings

Kleine Anfrage des Abgeordneten Andrej Hunko u. a. und der Fraktion DIE LINKE.

EU-Maßnahmen für den Zugang von Strafverfolgungsbehörden zu verschlüsselter Kommunikation

BT-Drucksache 18/9919

Vorbemerkung der Fragesteller:

Die Polizeiagentur Europol ist nach Angaben von deren Direktor Rob Wainwright in drei Vierteln aller Ermittlungen mit verschlüsselten Inhalten konfrontiert (<https://twitter.com/rwainwright67/status/729229923982913536>). Dies stelle ein großes Problem dar. Dem Bundesministerium des Innern ist es hingegen nicht möglich anzugeben, in welcher Größenordnung deutsche Behörden hiervon in Ermittlungen betroffen sind (Drucksache 18/8929). Auch die Kategorisierung in „selten“, „häufig“ oder „sehr häufig“ sei aufgrund fehlender statistischer Aufzeichnung nicht möglich. Hingegen stünden die Sicherheitsbehörden des Bundes „vor der ständigen Aufgabe, mit dem technischen Fortschritt Schritt zu halten“. Daher würden „fortlaufend“ Bedarfe an neuen Anwendungen oder Verfahren identifiziert. Der Rat der Europäischen Union hat hierzu mittlerweile einen Fragebogen an die Delegationen verteilt (Ratsdokument 12368/16; online unter <http://www.statewatch.org/news/2016/sep/eu-usa-encryption-quest-12368-16.pdf>). Das Dokument ist eine Folgemaßnahme des Treffens der Innen- und Justizminister in Bratislava zu „Herausforderungen“ von Verschlüsselung für die Kriminalitätsbekämpfung. Verabredet wurde die weitere, gemeinsame Behandlung des Themas zunächst im Rahmen einer Bestandsaufnahme. Die Ergebnisse des Fragebogens werden in einer Sitzung der „Friends of the Presidency Group on Cyber Issues“ diskutiert und schließlich dem Koordinierungsausschuss für den Bereich der polizeilichen und gerichtlichen Zusammenarbeit in Strafsachen (CATS) vorgelegt. Der CATS nutzt die Ergebnisse und Diskussionen schließlich zur Vorbereitung des Dezember-Treffens der Innen- und Justizminister.

1. In welchen grenzüberschreitenden Kooperationen, Forschungsprojekten oder EU-Aktionsplänen sind deutsche Behörden derzeit mit Verfahren zum Umgehen verschlüsselter Kommunikation befasst?

Zu 1.

Nach Kenntnis der Bundesregierung sind deutsche Behörden derzeit nicht im Rahmen von grenzüberschreitenden Kooperationen, Forschungsprojekten oder EU-Aktionsplänen mit Verfahren zum Umgehen verschlüsselter Kommunikation befasst.

2. Auf wessen Initiative kam der im Ratsdokument 12368/16 versendete Fragebogen nach Kenntnis der Bundesregierung zustande?

Zu 2.

Nach Kenntnis der Bundesregierung kam der Fragebogen auf Initiative der slowakischen EU-Ratspräsidentschaft zustande.

3. Welche Abteilung des Bundesinnenministeriums war für die Beantwortung des in Ratsdokument 12368/16 versendeten Fragebogens zuständig und welche Behörden (auch der Länder) arbeiteten zu?

Zu 3.

Die Beantwortung des in Ratsdokument 12368/16 versendeten Fragebogens der slowakischen EU-Ratspräsidentschaft zum Thema „Verschlüsselung“ (im Folgenden „Fragebogen“) für die Bundesregierung wurde durch die Abteilung Öffentliche Sicherheit im Bundesministerium des Innern koordiniert. Weitere Organisationseinheiten im Bundesministerium des Innern sowie das Bundeskriminalamt wurden beteiligt. Darüber hinaus waren das Bundesministerium der Justiz und für Verbraucherschutz sowie das Bundesministerium der Finanzen eingebunden.

4. Welche Angaben hat das Bundesinnenministerium bei der Beantwortung des in Ratsdokument 12368/16 versendeten Fragebogens gemacht?

Zu 4.

Der Fragebogen wurde nicht durch das Bundesministerium des Innern, sondern durch die Bundesregierung beantwortet. Die Beantwortung erfolgte auf Englisch.

Die Bundesregierung hat die folgenden Fragen dieser Kleinen Anfrage, soweit sie überwiegend den Wortlaut der Fragen des Fragebogens aufnehmen, jeweils auf der Grundlage der im Fragebogen gemachten Angaben beantwortet.

Wo das parlamentarische Fragerecht weitergehende Ausführungen gebietet, wurden diese ergänzend eingefügt.

Das Ratssekretariat der Europäischen Union hat den Fragebogen als „LIMITE“ eingestuft. Nach Kenntnis der Bundesregierung liegt dem Ratssekretariat derzeit ein Antrag auf Herausgabe des Fragebogens und der Antworten der Mitgliedstaaten nach dem Informationsfreiheitsrecht der Union vor. Gegen eine Herausgabe der Antworten der Bundesregierung bestehen seitens der Bundesregierung keine Einwände. Nach derzeitigem Stand ist davon auszugehen, dass der Fragebogen nebst Antworten im Wortlaut demnächst durch das Ratssekretariat veröffentlicht werden wird.

5. In welchem Ausmaß sind Bundesbehörden im Rahmen von operativen Aktivitäten oder bei der Beweiserhebung im Cyberraum mit Verschlüsselung konfrontiert?

Zu 5.

Die Bundesregierung verfügt über keine statistischen Aufzeichnungen im Sinne der Fragestellung.

Soweit der Bundesregierung weitergehende Erkenntnisse vorliegen, die unter die Fragestellung zu fassen sind, gilt folgendes: Soweit parlamentarische Anfragen Umstände betreffen, die aus Gründen des Staatswohls geheimhaltungsbedürftig sind, hat die Bundesregierung zu prüfen, ob und auf welche Weise die Geheimhaltungsbedürftigkeit mit dem parlamentarischen Informationsanspruch in Einklang gebracht werden kann. Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass die Frage 5 aus Geheimhaltungsgründen teilweise nicht in dem für die Öffentlichkeit einsehbaren Teil beantwortet werden kann.

Zwar ist der parlamentarische Informationsanspruch grundsätzlich auf die Beantwortung gestellter Fragen in der Öffentlichkeit angelegt. Die teilweise Einstufung der Antwort auf die Frage 5 als Verschlussache (VS) mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“ ist aber im vorliegenden Fall erforderlich. Nach § 3 Nummer 4 der Allgemeinen Verwaltungsvorschrift zum materiellen und organisatorischen Schutz von Verschlussachen (Verschlussachenanweisung, VSA) sind Informationen, deren Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein können, entsprechend einzustufen.

Eine zur Veröffentlichung bestimmte Antwort der Bundesregierung auf diese Fragen würde spezifische Informationen zur Tätigkeit, insbesondere zur Methodik und den konkreten technischen Fähigkeiten der Sicherheitsbehörden einem nicht eingrenzba- ren Personenkreis – auch der Bundesrepublik Deutschland möglicherweise gegne- risch gesinnten Kräften – nicht nur im Inland, sondern auch im Ausland zugänglich machen. Dabei würde die Gefahr entstehen, dass ihre bestehenden oder in der Ent- wicklung befindlichen operativen Fähigkeiten und Methoden aufgeklärt würden. Dies kann für die wirksame Erfüllung der gesetzlichen Aufgaben der Sicherheitsbehörden und damit für die Interessen der Bundesrepublik Deutschland nachteilig sein. Diese Informationen werden daher gemäß § 3 Nummer 4 VSA als „VS – Nur für den Dienstgebrauch“ eingestuft und dem Deutschen Bundestag gesondert übermittelt.

Im Übrigen wird auf die Antwort der Bundesregierung zu Frage 11 der Kleinen Anfra- ge der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/8929 verwiesen.

6. Welches sind dabei die hauptsächlich anzutreffenden Formen von Verschlüsse- lung (online oder offline)?

Zu 6.

Sowohl hinsichtlich online- als auch offline-Verschlüsselung sind gängige Verschlüs- selungsmethoden anzutreffen. Eine statistische Erfassung erfolgt nicht.

Im Übrigen wird auf die Antwort der Bundesregierung zu Frage 9 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/8929 verwiesen.

7. Auf welche Weise können Verdächtige oder Beschuldigte aus Sicht der Bundesre- gierung zur Herausgabe von Schlüsseln oder Passwörtern gezwungen werden?

Zu 7.

Beschuldigte können strafprozessrechtlich nicht zur Herausgabe von Schlüsseln o- der Passwörtern gezwungen werden, da diese nicht verpflichtet sind, zu ihrer Über- führung beizutragen.

8. Unter welchen Umständen sind Internetanbieter verpflichtet, Schlüssel oder Pass- wörter herauszugeben?

9. Welche Anordnungen müssen aus Sicht der Bundesregierung von den Ermittlungsbehörden vorgelegt werden?

Zu 8. und 9.

Gemäß § 100j der Strafprozessordnung (StPO) kann von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über Bestandsdaten verlangt werden, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten erforderlich ist. Zulässig ist dies im Falle sogenannter Zugangssicherungs_codes grundsätzlich nur auf Antrag der Staatsanwaltschaft bei entsprechender gerichtlicher Anordnung. Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft oder ihre Ermittlungspersonen getroffen werden. Darüber hinaus müssen die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.

Im Übrigen sieht die Strafprozessordnung keine spezielle Regelung vor, durch die Anbieter, welche Dienstleistungen über das Internet erbringen, zur Herausgabe von Schlüsseln oder Passwörtern verpflichtet werden können.

Sind die fraglichen Schlüssel oder Passwörter ihrerseits auf physischen Datenträgern oder Dokumenten verkörpert, so können die jeweiligen Dokumente oder Datenträger im Rahmen der §§ 94ff. StPO herausverlangt, durchsucht und sichergestellt bzw. beschlagnahmt werden. Zur Durchsuchung und Beschlagnahme bedarf es grundsätzlich einer richterlichen Anordnung; bei Gefahr im Verzug kann diese auch durch die Staatsanwaltschaft und ihre Ermittlungspersonen erfolgen.

10. Unter welchen Umständen ist es aus Sicht der Bundesregierung den Ermittlungsbehörden gestattet, verschlüsselte Telekommunikation zum Zweck von deren Entschlüsselung und Verwendung in Ermittlungsverfahren abzuhören?

Zu 10.

Die Überwachung verschlüsselter Telekommunikation unterliegt denselben Voraussetzungen wie die Überwachung nicht-verschlüsselter Telekommunikation. Diese ergeben sich aus den §§ 100a, 100b StPO. Die Maßnahme ist nur zulässig, wenn der Verdacht einer der schweren, im Katalog des § 100a Absatz 2 StPO abschließend aufgezählten Straftat besteht, die auch im Einzelfall schwer wiegt und andere Maßnahmen die Ermittlungen wesentlich erschweren oder aussichtslos wären.

Darüber hinaus ist grundsätzlich eine gerichtliche Anordnung erforderlich; bei Gefahr im Verzug kann die Anordnung durch die Staatsanwaltschaft (nicht aber deren Ermittlungspersonen) erfolgen.

11. Vor welchen Problemen stehen aus Sicht der Bundesregierung die Ermittlungsbehörden beim Abhören verschlüsselter Telekommunikation zum Zweck von deren Entschlüsselung und Verwendung in Ermittlungsverfahren bzw. deren Entschlüsselung?

Zu 11.

Aus Sicht der Bundesregierung stehen Ermittlungsbehörden vor allem vor dem Problem, dass aufgezeichnete Daten etwa durch eine Ende-zu-Ende-Verschlüsselung verschlüsselt sind und folglich nicht inhaltlich auswertbar sind. In vielen Fällen ist deshalb eine Analyse des tatsächlichen Kommunikationsinhalts nicht möglich.

12. Welche anderen Verfahren/Techniken nutzen Ermittlungsbehörden zur Entschlüsselung verschlüsselter elektronischer Beweismittel?

Zu 12.

Für laufende Telekommunikationsvorgänge bestünde eine Möglichkeit darin, auf das entsprechende informationstechnische System zuzugreifen und eine speziell hierfür geschaffene Software zu installieren, welche die Kommunikation erfasst, bevor diese verschlüsselt wird und bei der sichergestellt ist, dass ausschließlich laufende Telekommunikation erfasst wird.

Hinsichtlich gespeicherter Daten gilt folgendes: Im Strafverfahren können gespeicherte Daten z.B. im Rahmen der Durchsuchung und Beschlagnahme physischer Datenträger gewonnen werden. Diese können dann unter Anwendung forensischer Methoden untersucht werden, um Daten zu extrahieren bzw. zu entschlüsseln.

Ein verdeckter Zugriff auf gespeicherte Daten mittels einer auf dem Endgerät installierten Software wäre nur im Rahmen präventiver Maßnahmen zur Abwehr von Gefahren des internationalen Terrorismus nach Maßgabe des Bundeskriminalamtgesetzes zulässig.

13. Wie werden diese Beweismittel gesichert?

Zu 13.

Die relevanten Beweismittel werden mittels IT-forensischer Methoden sowohl im verschlüsselten sowie entschlüsselten Zustand gesichert. Die Möglichkeiten zur Erlangung von Daten im entschlüsselten Zustand (bspw. an einem noch im Betrieb befindlichen Computer) sind dabei unmittelbar abhängig von der jeweiligen Situation am Einsatzort.

Im Übrigen wird auf die Antwort zu Frage 12 verwiesen.

14. Inwiefern und in welchem Ausmaß nutzen Ermittlungsbehörden Dienste von Europol zur Entschlüsselung verschlüsselter Inhalte und welche Beispiele existieren hierfür?

Zu 14.

Ermittlungsbehörden des Bundes nutzen nach Kenntnis der Bundesregierung derzeit nicht die Dienste von Europol zur Entschlüsselung verschlüsselter Inhalte.

15. Welche Auffassung vertritt das Bundesministerium des Innern, inwiefern die nationale Gesetzgebung zur Entschlüsselung verschlüsselter Inhalte in Ermittlungsverfahren ausreichend ist?

Zu 15.

Nach Auffassung der Bundesregierung ermöglicht die nationale Rechtslage derzeit in grundsätzlich ausreichendem Maße die Sicherstellung elektronischer Beweismittel und deren Entschlüsselung. Gleichwohl ist es erforderlich, ständig möglicherweise erforderliche Änderungen der Rechtsgrundlagen zu prüfen und zu diskutieren.

16. Inwiefern ist das Bundesministerium des Innern der Auffassung, dass es zur einfacheren Entschlüsselung verschlüsselter Inhalte in Ermittlungsverfahren einer Regulierung auf Ebene der Europäischen Union bedarf?

Zu 16.

Die Bundesregierung ist der Auffassung, dass es zur einfacheren Entschlüsselung verschlüsselter Inhalte in Ermittlungsverfahren einer Regulierung auf Ebene der Europäischen Union nicht bedarf.

17. Welche anderen, nicht in dem Fragebogen berücksichtigten Punkte hält das Bundesministerium des Innern in Bezug auf Verschlüsselung für wichtig und welche Angaben hat sie hierfür in dem Fragebogen gemacht?

Zu 17.

Die Bundesregierung hat sich im Fragebogen gegen Regelungen zum Verbot oder zur Schwächung von Verschlüsselung in der Telekommunikation und bei Digitalen Diensten ausgesprochen, um den Schutz der Privatsphäre und von Geschäftsgeheimnissen sicherzustellen.

18. Welche Erwägungen, die sich aus der Praxis von Ermittlungen ergeben, sollten dabei berücksichtigt werden?

Zu 18.

Die Bundesregierung hat hierzu im Fragebogen keine weiteren Angaben gemacht.

19. Welche Erfahrungen haben Bundesbehörden diesbezüglich in grenzüberschreitenden Ermittlungen gemacht?

Zu 19.

Angesichts des regelmäßig grenzüberschreitenden Charakters von Cybercrime-Straftaten sind internationale Ermittlungen regelmäßig erforderlich. Hinsichtlich Verschlüsselung und dem Umgang mit ggf. verschlüsselten Beweismitteln besteht gleichwohl kein Unterschied zwischen grenzüberschreitenden und inländischen Ermittlungen.