Deutscher Bundestag **Drucksache 17/12651**

17. Wahlperiode 08. 03. 2013

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan Korte, Annette Groth, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 17/12259 –

Sicherheit, Datenschutz und Überwachung von Cloud-Daten

Vorbemerkung der Fragesteller

Dokumente nur vom heimischen Rechner einzusehen, ist heutzutage kaum noch vorstellbar. Von überall – egal ob vom Smartphone, von einem Internetcafe im Urlaub oder vom Rechner auf der Arbeit – auf eigene digitale Daten zugreifen zu können, ist längst Realität. Möglich machen dies die sogenannten Public-Cloud-Anbieter. So einfach die Nutzung der Public Cloud auch scheint, gibt es immer wieder Debatten hinsichtlich Sicherheit, Datenschutz und Transparenz. Kritisiert wird, dass ihre Infrastrukturen erhebliche Sicherheitsrisiken aufweisen: Die Registrierung sei zu einfach, Datenmissbrauch und -verlust kaum vermeidbar, Schnittstellen zu unsicher, die Verschlüsselung der Daten mangelhaft, Zugriffsberechtigte bei den Anbietern nicht immer vertrauenswürdig. Überdies ist es kaum nachvollziehbar, in welchem Land sich der Server des jeweiligen Anbieterunternehmens und somit auch die Daten der Nutzerinnen und Nutzer befinden. Für Public-Cloud-Anbieter gibt es keine einheitlichen Verträge und verbindlichen Standards. Je nach Verarbeitungsort können Dritte ohne großen Aufwand Zugriff auf die Daten bekommen. Hierzu gehören Geheimdienste, Strafverfolgungs-, Grenz- oder Finanzbehörden, die auf diesem Wege Informationen einholen können. Zwei Studien machen überdies darauf aufmerksam, dass Rechtsakte der US-Regierung den Zugriff ihrer Behörden sogar auf Daten außerhalb ihres Hoheitsgebietes erlauben („US-Massenüberwachung der EU-Bürger“, futurezone.at vom 15. Januar 2013). Auch kann nicht ausgeschlossen werden, dass die nationale Gesetzgebung mancher Staaten einen Zugriff von privaten Dritten, also Unternehmen, auf die Daten zulässt.

Anstatt sich der Datenschutzproblematik bei Cloud-Diensten anzunehmen, konzentriert sich die Bundesregierung auf den Zugriff ihrer Behörden auf die Daten und die Abfrage von Cloud-Passwörtern zu Ermittlungszwecken („Regierung will Abfrage von Cloud-Passwörtern erlauben“; ZEIT ONLINE vom 24. Oktober 2012). Auf mehreren Ebenen sind das Bundeskriminalamt (BKA), das Zollkriminalamt (ZKA), die Bundespolizei und das Bundesamt für Verfassungsschutz damit befasst, Polizeien und Geheimdiensten die Herausgabe von Cloud-Daten zu erleichtern. Dabei handelt es sich einerseits um die Erörterung grundsätzlicher Fragen und Rahmenbedingungen. In Projekten, Studien und Arbeitsgruppen werden aber auch technische Fragen erörtert.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 5. März 2013 übermittelt.

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

Auf nationaler Ebene betreibt das Strategie- und Forschungszentrum Telekommunikation (SFZ TK) ein Projekt unter dem Namen „CLOUD“, das sich mit Fragestellungen zu Cloud-Computing und dessen Implikationen auf die Telekommunikationsüberwachung beschäftigt (Plenarprotokoll 17/210). Im SFZ TK sind das BKA, die Bundespolizei und das Bundesamt für Verfassungsschutz gleichsam vertreten. Weitere Tätigkeitsfelder des polizeilich-geheimdienstlichen Zentrums sind die Studien „Entwicklung der Netze“, „Next Generation Network“ und „Rufnummernmanipulation“. Alle Anstrengungen drehen sich darum, wie in neuen digitalen Kommunikationsplattformen die Telekommunikationsüberwachung umgesetzt werden kann.

Zur Beteiligung der 16 Bundesländer an den Überlegungen zur Überwachung neuer Kommunikationsplattformen dient die Kommission Grundlagen der Überwachungstechnik (KomGÜT). Die Kommission soll „Synergien durch Abstimmungen und Kooperationen auf Bund-/Länderebene“ erzeugen. Beteiligt sind das BKA, das ZKA und die Bundespolizei. Das Bundesamt für Verfassungsschutz wird bei der KomGÜT als „Gast“ geführt. Auf Ebene der Landesinnenministerien betreiben die Länderpolizeien zudem einen Unterausschuss Information und Kommunikation (UA IuK), der beim Arbeitskreis II – Innere Sicherheit der Arbeitsgemeinschaft der Innenministerien der Länder angesiedelt ist.

Um auch international Einfluss auf die Standardisierung der Telekommunikationsüberwachung von Cloud-Diensten zu nehmen, engagieren sich deutsche Polizeibehörden überdies in internationalen Netzwerken. Eine besondere Rolle kommt dem European Telecommunications Standards Institute (ETSI) zu, das einen „Technische[n] Report“ zu Cloud-Diensten erarbeitet (Bundestagsdrucksache 17/11598). Das Normungsinstitut sucht dafür die Zusammenarbeit deutscher Provider, darunter der Deutschen Telekom AG und Telefonica O2. Auch die Bundesnetzagentur wurde dafür angesprochen. Bekanntlich arbeitet die Aachener Überwachungssparte des Utimaco-Konzerns im Technischen Komittee für Telekommunikationsüberwachung (TC LI) des ETSI mit (www. tinyurl.com/cw3aq4k). Die Firma stellt Abhörschnittstellen (Lawful Interception Management Systems) her. In der Arbeitsgruppe wird der Bedarf zukünftiger Abhörtechnologie durch Ermittlungsbehörden und Geheimdienste festgelegt. Auch das Bundesamt für Verfassungsschutz und die Bundesnetzagentur sind beteiligt. Zu den international aktiven Akteuren hinsichtlich der Überwachung der Telekommunikation gehören neben dem Bundesamt für Sicherheit in der Informationstechnik (BSI) auch das Landesamt für Zentrale Polizeiliche Dienste (LZPD) der Landespolizei Nordrhein-Westfalen.

Die Fragestellerinnen und Fragesteller sehen die Anstrengungen zur Überwachung von Cloud-Diensten überaus kritisch. Die beteiligten Behörden untergraben damit das ohnehin gestörte Vertrauen in die Freiheit des Internets. Zudem wird das Trennungsgebot von Polizei und Geheimdiensten in den genannten Gremien zunehmend ausgehöhlt. Es kann deshalb nicht hingenommen werden, wenn die Fragen zu dem Gebaren und den Aktivitäten der Behörden nicht öffentlich beantwortet werden.

1. Mit welchen Gesetzgebungsinitiativen, Forschungsprojekten, Studien und Verfahren zur (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten sind deutsche Behörden gegenwärtig befasst?

Das Strategie- und Forschungszentrum Telekommunikation (SFZ TK) betreibt eine Studie zur Entwicklung von Cloud-Diensten und deren Auswirkung auf die Sicherheitsbehörden. Auf die Anlage 6 zum Plenarprotokoll 17/210 wird verwiesen.

2. Inwieweit betreibt das Bundeskriminalamt eigene Anstrengungen zur (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten?

a) Auf wessen Initiative kamen die Vorhaben zustande, und wie werden diese finanziert?

b) Mit welchen weiteren Behörden, Firmen oder anderen Institutionen arbeitet das BKA hierfür zusammen?

c) Wann und wo werden etwaige Ergebnisse der Vorhaben vorgestellt und beraten?

d) Inwieweit sind diese öffentlich zugänglich?

Das Bundeskriminalamt (BKA) betreibt derzeit keine eigenen Anstrengungen zur (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten.

3. Inwieweit betreibt das Zollkriminalamt eigene Anstrengungen zur (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten?

a) Auf wessen Initiative kamen die Vorhaben zustande, und wie werden diese finanziert?

b) Mit welchen weiteren Behörden, Firmen oder anderen Institutionen arbeitet das ZKA hierfür zusammen?

c) Wann und wo werden etwaige Ergebnisse der Vorhaben vorgestellt und beraten?

d) Inwieweit sind diese öffentlich zugänglich?

Das Zollkriminalamt (ZKA) betreibt derzeit keine eigenen Anstrengungen zur (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten.

4. Inwieweit betreibt die Bundespolizei eigene Anstrengungen zur (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten?

a) Auf wessen Initiative kamen die Vorhaben zustande, und wie werden diese finanziert?

b) Mit welchen weiteren Behörden, Firmen oder anderen Institutionen arbeitet die Bundespolizei hierfür zusammen?

c) Wann und wo werden etwaige Ergebnisse der Vorhaben vorgestellt und beraten?

d) Inwieweit sind diese öffentlich zugänglich?

Die Bundespolizei (BPOL) betreibt derzeit keine eigenen Anstrengungen zur (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten.

5. Inwieweit betreibt das Bundesamt für Verfassungsschutz eigene Anstrengungen zur (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten?

a) Auf wessen Initiative kamen die Vorhaben zustande, und wie werden diese finanziert?

b) Mit welchen weiteren Behörden, Firmen oder anderen Institutionen arbeitet das Bundesamt für Verfassungsschutz hierfür zusammen?

c) Wann und wo werden etwaige Ergebnisse der Vorhaben vorgestellt und beraten?

d) Inwieweit sind diese öffentlich zugänglich?

Das Bundesamt für Verfassungsschutz (BfV) betreibt derzeit keine eigenen Anstrengungen zur (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten.

6. Inwieweit betreibt die Bundesnetzagentur eigene Anstrengungen zur (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten?

a) Auf wessen Initiative kamen die Vorhaben zustande, und wie werden diese finanziert?

b) Mit welchen weiteren Behörden, Firmen oder anderen Institutionen arbeitet die Bundesnetzagentur hierfür zusammen?

c) Wann und wo werden etwaige Ergebnisse der Vorhaben vorgestellt und beraten?

d) Inwieweit sind diese öffentlich zugänglich?

Die Bundesnetzagentur (BNetzA) betreibt keine eigenen Anstrengungen zur (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten.

7. Inwieweit betreibt das Bundesamt für Sicherheit in der Informationstechnik eigene Anstrengungen zur (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten?

a) Auf wessen Initiative kamen die Vorhaben zustande, und wie werden diese finanziert?

b) Mit welchen weiteren Behörden, Firmen oder anderen Institutionen arbeitet das BSI hierfür zusammen?

c) Wann und wo werden etwaige Ergebnisse der Vorhaben vorgestellt und beraten?

d) Inwieweit sind diese öffentlich zugänglich?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) betreibt derzeit keine eigenen Anstrengungen zur (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten.

8. Inwieweit betreiben der Bundesnachrichtendienst (BND) und der Militärische Abschirmdienst (MAD) eigene Anstrengungen zur (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten?

a) Auf wessen Initiative kamen die Vorhaben zustande, und wie werden diese finanziert?

b) Mit welchen weiteren Behörden, Firmen oder anderen Institutionen arbeiten der BND und der MAD hierfür zusammen?

c) Wann und wo werden etwaige Ergebnisse der Vorhaben vorgestellt und beraten?

d) Inwieweit sind diese öffentlich zugänglich?

Weder der Bundesnachrichtendienst (BND) noch der Militärische Abschirmdienst (MAD) betreiben derzeit eigene Anstrengungen zur (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten.

9. Welche Überlegungen führten dazu, das in der Vergangenheit beim Bundesverwaltungsamt angesiedelte Kompetenzzentrum der Zentralstelle für Telekommunikationstechnologien in das Strategie- und Forschungszentrum Telekommunikation zu überführen?

Im Rahmen der Neuorganisation in der Telekommunikationsüberwachung im Geschäftsbereich des Bundesministeriums des Innern (BMI) wurden die Aufgaben der Zentralstelle für Kommunikationstechnologien (ZSK) vom Bundesverwaltungsamt (BVA) an BfV, BKA und BPOL zurückübertragen. Zur Wahrnehmung der Aufgaben des früheren Kompetenzzentrums der ZSK (CC) wurde das Strategie- und Forschungszentrum Telekommunikation (SFZ TK) eingerichtet.

a) Welche Aufgaben hatte das frühere Kompetenzzentrum der Zentralstelle für Telekommunikationstechnologien, und wer war daran beteiligt?

b) Inwiefern unterscheiden sich die Aufgaben des SFZ TK vom früheren Kompetenzzentrum der Zentralstelle für Telekommunikationstechnologien?

Die Aufgaben des CC entsprachen grundsätzlich denen des heutigen SFZ TK. Im Übrigen wird auf die Anlage 6 des Plenarprotokolls 17/210 verwiesen.

c) Wo ist das SFZ TK angesiedelt?

Das SFZ TK ist eine behördenübergreifende Kooperationsplattform im Geschäftsbereich des BMI. Es ist keiner Behörde zugeordnet. Dienstsitz ist die Liegenschaft des BKA in Berlin-Treptow.

d) Über welchen Haushalt verfügt das SFZ TK, und wie wird es finanziert?

Das SFZ TK als Kooperationsplattform ist keine eigenständige Organisationseinheit und hat daher keine eigene finanzielle Ausstattung. Die Finanzierung der Projekte des SFZ TK erfolgt aus den jeweiligen Haushaltsansätzen der beteiligten Behörden. Die Personalkosten der dort eingesetzten Mitarbeiter werden durch die jeweils entsendende Behörde getragen.

e) Inwiefern wurde bei der Einrichtung des SFZ TK erörtert, ob dadurch das Trennungsgebot von Geheimdiensten und Polizei aufgeweicht werden könnte?

Die Aufgabenwahrnehmung des SFZ TK erfolgt ausschließlich auf einer strategisch/wissenschaftlichen Ebene; das Trennungsgebot ist somit nicht berührt.

10. Welche weiteren Details kann die Bundesregierung zum Projekt „CLOUD“ mitteilen, das sich mit Fragestellungen zu Cloud-Computing und dessen Implikationen auf die Telekommunikationsüberwachung beschäftigt (Plenarprotokoll 17/210)?

a) Unter wessen Leitung steht das Projekt „CLOUD“?

Die fachliche Leitung des Projekts erfolgt durch das SFZ TK.

b) Wer hat die Einrichtung des Projekts angeregt und verfügt?

Die Durchführung des Projektes wurde durch den Lenkungskreis des SFZ TK beschlossen, der aus Vertretern der am SFZ TK beteiligten Behörden besteht.

c) Welche Arbeitsgruppen oder Unterarbeitsgruppen existieren im Projekt?

Es existieren keine Arbeits- oder Unterarbeitsgruppen.

d) Welche konkreten Aufgaben übernehmen das BKA, die Bundespolizei und das Bundesamt für Verfassungsschutz im Rahmen des Projekts?

Die genannten Behörden wirken durch an das SFZ TK entsandte eigene Mitarbeiter am Projekt mit. Sie formulieren dort u. a. fachliche Fragestellungen.

e) Welche Treffen haben hierzu stattgefunden, und wer nahm daran teil?

Es fanden drei Treffen der Projektbeteiligten sowie von Behörden- und Industrievertretern statt.

f) Welche weiteren Institutionen, Firmen oder wissenschaftlichen Einrichtungen wurden für das Projekt mit welchem Ziel angesprochen?

Die für das Projekt notwendigen Dienstleistungen wurden im Rahmen einer Ausschreibung vergeben. Hierfür wurden in Frage kommende Dienstleister angesprochen.

g) Wie haben die Angesprochenen darauf reagiert?

Die angesprochenen Marktteilnehmer haben jeweils ein Angebot abgegeben.

h) Welche weiteren Institutionen, Firmen oder wissenschaftlichen Einrichtungen sollen zukünftig für das Projekt angesprochen werden?

Es ist derzeit nicht geplant, weitere Projektbeteiligte zu gewinnen.

i) Wann, wo und wem werden etwaige Ergebnisse des Projekts „CLOUD“ vorgestellt und beraten?

Nach Vorliegen und Auswertung der Projektergebnisse werden diese den Sicherheitsbehörden dargestellt.

j) Inwieweit sind diese öffentlich zugänglich?

Eine Veröffentlichung ist nicht vorgesehen.

11. Auf welche Art und Weise bzw. mit welchem Inhalt wurden innerhalb von „CLOUD“ folgende Themen erörtert oder bearbeitet:

a) Software und Betriebssysteme,

Es erfolgte keine diesbezügliche Erörterung.

b) auf verschlüsselten Kommunikationsprotokollen basierender Zugang zu Cloud-Diensten,

Es wurden keine konkreten Kommunikationsprotokolle betrachtet. Vielmehr wurde die Verschlüsselung im Bereich des Cloud-Computing im Allgemeinen behandelt.

c) Zugriff der Sicherheitsbehörden,

Gegenstand des Projekts waren die rechtlichen Rahmenbedingungen und die Erörterung potentieller technischer Möglichkeiten für einen Zugriff der Sicherheitsbehörden.

d) Forensik?

Die Auswirkungen auf die Forensik wurden aufgegriffen, jedoch nicht abschließend betrachtet.

12. Welche weiteren Details kann die Bundesregierung zu Inhalten, Zielsetzung und Beteiligten der Studien „Entwicklung der Netze“, „Next Generation Network“ und „Rufnummernmanipulation“ mitteilen (Plenarprotokoll 17/210)?

Die Inhalte und Zielsetzung der SFZ TK-Studien zur Entwicklung der Netze/ Next Generation Networks und der Studie zur Untersuchung des Phänomens Caller-ID-Spoofing wurden in dem referenzierten Plenarprotokoll dargestellt. Die Studien werden unter Beteiligung der Sicherheitsbehörden im Geschäftsbereich des BMI und ausgewählten Unternehmen der TK-Industrie durchgeführt.

13. Auf welche Weise befasst sich die Kommission Grundlagen der Überwachungstechnik mit der (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten?

Auf die Antworten zu den Fragen 20 ff. auf Bundestagsdrucksache 17/11239 wird verwiesen.

Technische Innovationen im Themenfeld der Überwachungstechnik haben regelmäßig Auswirkungen auf polizeitaktische Möglichkeiten und Anforderungen. Die sich dabei regelmäßig ergebenden Verflechtungen der Felder Technik, Taktik und Recht erfordern im föderalen Verbund die Zusammenarbeit mit anderen Gremien und in Teilen mit Industrie und Verbänden. In diesem Kontext kommt der Kommission Grundlagen der Überwachungstechnik (KomGÜT) die Funktion einer bund-/länderübergreifenden Beratungsinstanz zu, die die notwendigen Anpassungsprozesse für die polizeiliche Telekommunikationsüberwachung (TKÜ) insbesondere aus technischer Sicht erkennt, bewertet und schließlich entsprechende Handlungs-/Umsetzungserfordernisse für die Polizeien des Bundes und der Länder anregt.

Mit der (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten hat sich die KomGÜT bislang nur als einem von vielen Aspekten der notwendigen Fortentwicklung der polizeilichen Telekommunikationsüberwachung befasst.

a) Welche „Synergien durch Abstimmungen und Kooperationen auf Bund-/Länderebene“ wurden hinsichtlich der (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten bereits erzeugt bzw. welche sind angestrebt?

Auf Basis der gebündelten Expertise der für die polizeiliche TKÜ Verantwortlichen der Polizeien des Bundes und der Länder bewertet die KomGÜT den Prozess der polizeilichen TKÜ insbesondere unter technischen, betrieblichen und organisatorischen Aspekten. Synergetische Effekte bei der Umsetzung der so erarbeiteten und konsentierten Empfehlungen sind zunächst für fiskalische/ haushalterische Belange in Bund und Ländern zu verzeichnen (z. B. bei länder-

übergreifenden Kooperation für die kostenintensive Beschaffung und den Betrieb von TKÜ-Anlagen). Daneben steht die Initiierung und/oder Harmonisierung polizeitaktischer Vorgehensweisen und kriminalpolitischer Forderungen.

b) Auf wessen Initiative kamen die Vorhaben zustande, und wie werden diese finanziert?

Als Beratungs- bzw. Harmonisierungsinstanz innerhalb der föderalen Strukturen der IMK betreibt die KomGÜT keine Vorhaben im Sinne konkreter/definierter Realisierungs- oder Umsetzungsprojekte.

c) Unter wessen Leitung stehen die Vorhaben?

d) Mit welchen weiteren Behörden, Firmen oder anderen Institutionen arbeitet die KomGÜT hierfür zusammen?

e) Wann und wo werden etwaige Ergebnisse der Vorhaben vorgestellt und beraten?

f) Inwieweit sind diese öffentlich zugänglich?

Auf die Antwort zu Frage 13b wird verwiesen.

g) Inwiefern wurde innerhalb der KomGÜT erörtert, ob durch die Mitarbeit des Bundesamtes für Verfassungsschutz (auch als „Gast“) das Trennungsgebot von Geheimdiensten und Polizei aufgeweicht werden könnte?

Das BfV ist nicht Mitglied der KomGÜT. Bei der Teilnahme des BfV zu ausgewählten Tagesordnungspunkten an bestimmten Sitzungen der KomGÜT steht der fachliche Austausch zu ausgewählten Fachfragen zur TKÜ im Sinne eines „Best-Practice-Austauschs“ im Vordergrund. Operative und/oder personenbezogene Angelegenheiten sind hiervon nicht umfasst. Das „Trennungsgebot“ ist somit nicht tangiert.

14. Auf welche Weise befasst sich der Unterausschuss Information und Kommunikation nach Kenntnis der Bundesregierung mit der (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten?

a) Auf wessen Initiative kamen die Vorhaben zustande, und wie werden diese finanziert?

b) Unter wessen Leitung stehen die Vorhaben?

c) Mit welchen weiteren Behörden, Firmen oder anderen Institutionen arbeitet die KomGÜT hierfür zusammen?

d) Wann und wo werden etwaige Ergebnisse der Vorhaben vorgestellt und beraten?

e) Inwieweit sind diese öffentlich zugänglich?

Die KomGÜT ist dem Unterausschuss Information und Kommunikation (UA IuK), der als Beschlussgremium fungiert, nachgeordnet. Sie berichtet ihm regelmäßig. Mit der (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten hat sich der UA IuK bislang in dem dargelegten Umfang (siehe Antwort zu Frage 13) befasst.

Im Übrigen wird auf die Antwort zu den Fragen 20 ff. auf Bundestagsdrucksache 17/11239 verwiesen.

15. Auf welche Weise befassen sich Agenturen oder Ratsarbeitsgruppen der Europäischen Union mit konkreten Vorhaben der (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten bzw. deren gesetzlichen und organisatorischen Rahmenbedingungen?

Auf die Antworten zu Frage 16 wird verwiesen. Die Europäische Polizeiagentur (Collège Européen de Police – CEPOL) bietet Trainingsangebote für Polizeiangehörige zum Thema Cybercrime an, die auch das Thema Cloud Computing umfassen. Der Bundesregierung ist nicht bekannt, dass sich europäische Agenturen oder Ratsarbeitsgruppen darüber hinaus mit konkreten Vorhaben der (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten bzw. deren gesetzlichen und organisatorischen Rahmenbedingungen befassen.

16. Welche weiteren Details kann die Bundesregierung zum „Technische[n] Report“ zu Cloud-Diensten des European Telecommunications Standards Institute mitteilen (Bundestagsdrucksache 17/11598)?

a) Unter wessen Leitung steht der „Technische Report“?

Zu den Fragen 16 und 16a wird auf die Antwort zu Frage 15 auf Bundestagsdrucksache 17/11239 verwiesen.

b) Wer hat die Einrichtung des Projekts angeregt und verfügt?

Die Einrichtung des Projekts erfolgte auf Initiative der Arbeitsgruppe ETSI TC LI.

c) Welche konkreten Aufgaben übernehmen das BKA, die Bundespolizei und das Bundesamt für Verfassungsschutz im Rahmen des Projekts?

BfV und BKA nehmen an den Arbeitsgruppensitzungen des ETSI TC LI teil, übernehmen dabei jedoch keine konkreten Aufgaben.

d) Welche Treffen haben hierzu stattgefunden, und wer nahm daran teil?

Der in der Frage genannte „Technische Report“ wurde im September 2011 erstellt und wird seitdem in allen regulär stattfindenden Treffen der Arbeitsgruppe ETSI TC LI weiterentwickelt. Die Teilnahme beschränkt sich auf die Mitglieder der Arbeitsgruppe ETSI TC LI. Im Übrigen wird auf die Antwort zu Frage 10 auf Bundestagsdrucksache 17/11239 verwiesen.

e) Welche weiteren Institutionen, Firmen oder wissenschaftlichen Einrichtungen wurden für das Projekt mit welchem Ziel angesprochen?

Der Bundesregierung liegen hierzu keine Erkenntnisse vor.

f) Wie haben die Angesprochenen darauf reagiert?

g) Welche weiteren Institutionen, Firmen oder wissenschaftlichen Einrichtungen sollen zukünftig für das Projekt angesprochen werden?

Auf die Antwort zu Frage 16e wird verwiesen.

h) Wann und wo wird der „Technische Report“ vorgestellt und beraten?

Auf die Antwort zu Frage 16d wird verwiesen.

i) Inwieweit ist dieser öffentlich zugänglich?

Der Technische Report befindet sich in einer Entwurfsfassung und wird von ETSI nicht öffentlich zur Verfügung gestellt.

17. Welche Treffen der Arbeitsgruppen TC LI und SA 3 LI des ETSI haben nach Kenntnis der Bundesregierung bzw. ihrer teilnehmenden Behörden in den letzten fünf Jahren an welchen Orten in Deutschland stattgefunden?

Es existiert keine Unterarbeitsgruppe „SA3 LI“ des ETSI. Die Antworten beziehen sich daher auf die ETSI-Arbeitsgruppe TC LI. Auf Bundestagsdrucksache 17/11239 wird verwiesen.

Die folgenden Treffen haben in den letzten fünf Jahren in Deutschland stattgefunden:

- ETSI TC LI Rapporteur’s Meeting #19 (26. März bis 28. März 2008) in Mainz
- ETSI TC LI Meeting #24 (15. Juni bis 17. Juni 2010) in Aachen
- ETSI TC LI Rapporteur’s Meeting #25 (1. Dezember bis 3. Dezember 2010) in Duisburg
- ETSI TC LI Rapporteur’s Meeting #26 (4. April bis 5. April 2012) in Mainz
- ETSI TC LI Rapporteur’s Meeting #27 (26. November bis 30. November 2012) in Duisburg

a) Welche deutschen Firmen oder Behörden waren für die Einladung oder Tagesordnung jeweils verantwortlich?

Die Treffen in Mainz wurden von der Bundesnetzagentur, die Treffen in Duisburg vom Landesamt für Zentrale Polizeiliche Dienste (LZPD) bzw. dem Landeskriminalamt Nordrhein-Westfalen und das Treffen in Aachen von einem teilnehmenden Unternehmen jeweils in Zusammenarbeit mit ETSI organisiert. Die Tagesordnungen werden durch die Beiträge der Mitglieder von ETSI TC LI bestimmt und durch den Vorsitzenden erstellt.

b) Welche deutschen Firmen oder Behörden haben an den Treffen teilgenommen?

Auf Bundestagsdrucksache 17/11239 wird verwiesen.

c) Welche Teilnehmer/-innen sind ihren Behörden noch erinnerlich, sofern die Bundesregierung über keine Teilnahmelisten verfügt?

Es liegen keine Teilnehmerlisten vor; auf die Antwort zu Frage 17b wird verwiesen.

d) Mit welchen Zielen und mit welchen Initiativen haben sich das Landesamt für Zentrale Polizeiliche Dienste der Polizei Nordrhein-Westfalen und (soweit den Beteiligten der Bundesregierung bekannt oder erinnerlich) der Aachener Hersteller von Überwachungstechnologien Utimaco in den letzten fünf Jahren in den Arbeitsgruppen TC LI und SA 3 LI eingebracht?

Dazu liegen der Bundesregierung keine Informationen vor.

18. Auf welche Weise befasst sich die Internationale Fernmeldeunion (ITU) nach Kenntnis der Bundesregierung mit der (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten?

Die Internationale Fernmeldeunion (ITU) hat als technikorientierte VN-Sonderorganisation breite Erfahrungen im Bereich der Telekommunikationsinfrastruktur. Sie legt Standards fest und sorgt für die weltweite Koordinierung und Zuweisung von Funkfrequenzen. Zudem bietet sie Entwicklungsländern umfassende Beratung für den Ausbau der Telekommunikationsdienste und -netze an. Die Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten fällt nicht in das Mandat der ITU.

a) Inwiefern wurde die Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten auch auf der World Conference on International Telecommunications (WCIT) in Dubai thematisiert?

Auf Cloud-Dienste fokussierte Fragen sind nicht Gegenstand der im Rahmen der WCIT neu verhandelten International Telecommunication Regulations (ITRs).

b) Wie hat sich die Bundesregierung zu entsprechenden Dokumenten oder Abstimmungen verhalten?

Deutschland hat die Schlussakte der WCIT nicht gezeichnet.

19. Wie beurteilt die Bundesregierung das Ergebnis der im Auftrag des Ausschusses für Bürgerrecht, Justiz und Inneres des EU-Parlaments in Auftrag gegebenen Studie des Centre D'Etudes sur les Conflits und des Centre for European Policy Studies, wonach die größte Gefahr beim Cloud-Computing nicht in der Cyberkriminalität, sondern durch Zugriffe von Behörden bestünde („Fighting cyber crime and protecting privacy in the cloud", European Parliament 2012)?

Auf Anlage 30 des Plenarprotokolls 17/216 wird verwiesen.

20. Welche Rechtsakte der US-Regierung sind der Bundesregierung bekannt, die einen Zugriff durch US-Behörden auf in den USA befindlichen Cloud-Servern gespeicherte Daten von Nutzerinnen und Nutzern aus der Europäischen Union ermöglichen?

Zu Rechtsakten der Regierung der Vereinigten Staaten von Amerika, die einen Zugriff von US-Behörden auf Daten von Nutzern aus der Europäischen Union erlauben, die auf in den USA befindlichen „Cloud-Server" gespeichert sind, liegen der Bundesregierung nur Hinweise aus öffentlich zugänglichen Quellen vor. Zu Inhalt und Auslegung ausländischen Rechts nimmt die Bundesregierung grundsätzlich nicht Stellung.

a) Inwieweit wurde die Bundesregierung von welchen Stellen der US-Regierung hierüber in Kenntnis gesetzt, etwa im Rahmen der kürzlichen Verlängerung des sogenannten Foreign Intelligence Surveillance Act (FISA) durch den US-Präsidenten Barack Obama oder des sogenannten Patriot Act?

Die Bundesregierung wurde hierzu nicht in Kenntnis gesetzt.

b) Inwiefern hat die Bundesregierung sichergestellt, dass betroffene deutsche Staatsangehörige von etwaigen Abhörmaßnahmen im Vorfeld oder nachträglich unterrichtet werden?

Die Unterrichtung betroffener Personen richtet sich nach dem jeweils einschlägigen Recht des Drittstaates.

c) Inwiefern ist für die Durchsuchung der Cloud-Daten nach den jeweiligen Rechtsakten eine richterliche Genehmigung erforderlich?

Auf die Antwort zu Frage 20 wird verwiesen.

21. Inwiefern ist der Bundesregierung bekannt, ob der Patriot Act oder der FISA auch Zugriffe von US-Behörden außerhalb der USA erlaubt, wie es niederländische Wissenschaftler kürzlich in einer Studie beschrieben hatten („Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act“, November 2012)?

Zur extraterritorialen Wirkung des genannten ausländischen Rechts liegen der Bundesregierung keine Erkenntnisse vor. Im Übrigen wird auf die Antwort zu Frage 20 verwiesen.

a) Wenn ja, wie bewertet die Bundesregierung die Rechtmäßigkeit eines Zugriffs von US-Behörden auf in Deutschland gespeicherte oder prozessierte Daten bei Unternehmen, Behörden oder sonstigen Stellen?

Auf die Antwort zu Frage 21 wird verwiesen.

b) Inwieweit ist diese Praxis durch Rechtshilfeabkommen der Bundesregierung mit den USA gedeckt, bzw. inwieweit widerspricht sie diesen?

Rechtsgrundlagen für Ersuchen im Bereich der justiziellen Rechtshilfe in Strafsachen mit dem Ziel des Zugriffs und der Übermittlung von Daten, die in einer Cloud gespeichert sind, sind im Wesentlichen der Vertrag vom 14. Oktober 2003 zwischen der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika über die Rechtshilfe in Strafsachen (RhV D-USA) in Verbindung mit dem Zusatzvertrag vom 18. April 2006 zu dem vorbezeichneten Vertrag sowie das Übereinkommen des Europarats über Computerkriminalität vom 23. November 2001 (EuCybercrimeÜbk).

Im Hinblick auf den Zugriff auf diese Daten ist zu differenzieren:

Sollen Daten aus der Cloud gesichert werden, ist die Geschwindigkeit der Maßnahme von zentraler Bedeutung. Der Anwendungsbereich der Artikel 32 und 29 des EuCybercrimeÜbk ist zu prüfen. Anschließend muss die Verwertung der Daten ermöglicht werden. Hier ist eine sorgfältige Prüfung rechtshilferechtlicher Standards zu gewährleisten. Der Anwendungsbereich des RhV D-USA ist eröffnet.

Die Voraussetzungen der grenzüberschreitenden justiziellen Zusammenarbeit in Strafsachen sind zudem unterschiedlich, wenn der berechtigte Nutzer die Daten selbst und freiwillig auf seinen Rechner zurückholt, wenn er das Passwort bekanntgibt oder die Daten nicht gesichert sind, aber ein deutscher Ermittler am ausländischen Standort hoheitlich tätig wird, oder wenn der berechtigte Nutzer nicht mit der Rückholung der Daten einverstanden ist.

Auf die Antwort zu Frage 21 wird verwiesen.

c) Inwieweit treffen Medienberichte zu, wonach weder der EU-Kommission noch dem EU-Parlament oder nationalen Datenschützern die Möglichkeit des US-Zugriffs auf Daten im Ausland bekannt war (Die Presse, 11. Januar 2013)?

Die Bundesregierung hat keine Kenntnis davon, ob der Europäischen Kommission, dem Europäischen Parlament oder nationalen Datenschützern die Möglichkeit des US-Zugriffs auf Daten im Ausland bekannt war.

d) Inwiefern sieht sich die Bundesregierung auch durch Medienberichte veranlasst, die Auslegung des Patriot Act oder des FISA für Spionagemaßnahmen auf ihrem Hoheitsgebiet zu unterbinden, und welche Schritte hat sie gegenüber welchen US-Stellen bereits unternommen?

Die Bundesregierung sieht derzeit keine Veranlassung zu etwaigen Schritten im Sinne der Fragestellung.

e) Wie werden die Bundesregierung und die EU zukünftig dafür sorgen, dass Cloud-Daten in Deutschland bzw. in der EU vor Abfragen aus den USA geschützt werden (bitte die konkreten Maßnahmen, Rechtsakte oder sonstigen Schritte erläutern)?

Im Bereich der justiziellen Rechtshilfe in Strafsachen werden Probleme in bilateralen Gesprächen mit den zuständigen US-Behörden erörtert.

22. Wie viele Rechtshilfeersuchen zur Sicherung oder Herausgabe von Cloud-Daten haben welche Bundesbehörden in den letzten zwei Jahren bei welchen Einrichtungen welcher Länder gestellt?

a) Wie viele Rechtshilfeersuchen zur Sicherung oder Herausgabe von Cloud-Daten haben welche Behörden welcher Länder in den letzten zwei Jahren bei welchen Bundesbehörden gestellt?

b) Wie wurden die Rechtshilfeersuchen jeweils beantwortet?

Weder die Anzahl eingehender, noch ausgehender Rechtshilfeersuchen, bzw. die Art der Beantwortung werden statistisch erfasst.

c) Welche sonstigen Angaben kann die Bundesregierung zu deren Umfang und Beantwortung machen, sofern sie die Rechtshilfeersuchen und ihren Ausgang nicht protokolliert?

Im BKA aus dem Ausland eingehende Ersuchen um Sicherung oder Herausgabe von Cloud-Daten sowie deren Beantwortung werden in der Praxis regelmäßig über das G8 24/7-Netzwerk abgewickelt. Ein von den deutschen Polizeidienststellen bzw. Justizbehörden ausgehenden Rechtshilfeersuchen ist immer dann erforderlich, wenn die Daten auf einem Server/Speicherplatz von einer ausländischen Firma im Ausland gespeichert sind oder die Daten auf einem Server/Speicherplatz einer deutsche Firma im Ausland ausgelagert sind.

In einem Ermittlungsverfahren hat der Generalbundesanwalt im Jahr 2012 ein Rechtshilfeersuchen an das Justizministerium der Vereinigten Staaten von Amerika mit der Bitte gerichtet, bei einem Dienstleister die vollständigen Inhalte eines dort von einem der Beschuldigten eingerichteten Speicherplatzes zu erheben und zur Verfügung zu stellen. Grundlage war ein entsprechender ermittlungsrichterlicher Durchsuchungsbeschluss. Das Rechtshilfeersuchen ist im Juli 2012 seitens der USA erledigt worden. Weiterhin ist zu bemerken, dass es bei der Stellung eines Rechtshilfeersuchens häufig nicht bekannt ist, ob der Provider die erbetenen Daten auf einem lokalen Server oder „in der Cloud“ gespeichert hat.

23. Trifft es zu, dass die Bundesregierung die Abfrage von Cloud-Passwörtern im Rahmen des neuen Telekommunikationsgesetzes erleichtern möchte?

a) Wie würde dieser Grundrechtseingriff begründet?

b) Inwiefern wäre hierfür ein Richtervorbehalt notwendig?

Nein. Vielmehr soll in Umsetzung der Vorgaben der Entscheidung des Bundesverfassungsgerichts vom 24. Januar 2012 eine Auskunft über Passwörter (PIN und PUK) nur gestattet werden, wenn auch die gesetzlichen Voraussetzungen für die Nutzung der dadurch geschützten Daten vorliegen.

24. Wie steht die Bundesregierung zu den Ausführungen des Strafrechtlers und Juniorprofessors Dr. Tobias Singelnstein, wonach sich technische Möglichkeiten zum Knacken der Passwörter von Cloud-Diensten für die Strafverfolgung verbieten, da diese nicht von der Strafprozessordnung gedeckt sind (NStZ – Neue Zeitschrift für Strafrecht, Heft 11/2012, S. 593 bis 606)?

Die Bundesregierung sieht davon ab, Veröffentlichungen einzelner Rechtswissenschaftler zu bewerten.

a) Auf welcher rechtlichen Grundlage hält die Bundesregierung das heimliche Auslesen von Mobiltelefonen, etwa im Polizeigewahrsam oder bei Grenzkontrollen, für zulässig?

Die Bundesregierung sieht im repressiven Bereich keine rechtliche Grundlage für ein heimliches „Auslesen von Mobiltelefonen“. Eine Ermittlung und Auswertung von in Mobiltelefonen gespeicherten Daten kann aber im Anschluss an eine Sicherstellung oder Beschlagnahme nach §§ 94 ff. der Strafprozessordnung (StPO) bzw. entsprechenden gefahrenabwehrrechtlichen Vorschriften zulässig sein. Dabei handelt es sich indes um eine offene Maßnahme, die auf Grund richterlicher Anordnung nach § 98 StPO erfolgt.

b) Inwiefern ist hierfür ein richterlicher Beschluss vonnöten?

Auf die Antwort zu Frage 24a wird verwiesen.

c) In welchem Umfang wird dies von welchen Bundesbehörden praktiziert?

Es erfolgt keine statistische Erfassung entsprechender Maßnahmen.

d) Auf welcher rechtlichen Grundlage hält die Bundesregierung die Einrichtung von Schnittstellen zum unbemerkten Ausleiten des Datenverkehrs bei Telekommunikationsanbietern für unbedenklich?

Die Einrichtung von Schnittstellen zum Ausleiten des Datenverkehrs bei Telekommunikationsanbietern ohne Kenntnis des Anschlussinhabers oder -nutzers ist zur repressiven Überwachung der Telekommunikation und Erhebung von Verkehrsdaten nach Maßgabe der §§ 100a, 100b Absatz 3 Satz 1 und 2, § 100g Absatz 3 Satz 1 StPO in Verbindung mit § 110 des Telekommunikationsgesetzes und der Telekommunikationsüberwachungs-Verordnung zulässig.

25. Über welche technischen Werkzeuge (Hardware, Software) verfügen welche Bundesbehörden zum Auslesen, Erraten oder Knacken von Passwörtern von Internetdiensten oder Kommunikationsgeräten?

Zur Überwindung von Gerätesperrcodes bei Kommunikationsgeräten (Mobilfunkgeräten) werden im BKA kommerziell verfügbare Softwarewerkzeuge eingesetzt. Diese Maßnahmen werden jedoch ausschließlich bei Mobilfunkgeräten durchgeführt, die zuvor im Rahmen von Ermittlungsverfahren bei strafprozessualen Maßnahmen unter Beachtung der damit verbundenen einschlägigen Rechtsvorschriften sichergestellt wurden.

Der BND und das BfV setzen zur Entzifferung handelsübliche wie auch eigenentwickelte Hard- und Software ein.

Das BSI führt gemäß § 3 Absatz 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) im Auftrag von behördlichen Kunden technische Sicherheitsprüfungen auf deren zu prüfenden IT-Systemen, Anwendungen und Netzen durch. Im Rahmen dieser technischen Sicherheitsprüfungen, insbesondere im Rahmen von Penetrationstests, werden IT-Systeme – im Auftrag des Kunden – auch auf leicht erratbare Passworte geprüft. Die Behebung hierbei identifizierter Schwachstellen erhöht die Robustheit der geprüften IT-Systeme und fördert die IT-Sicherheit insgesamt.

26. Inwiefern wurden nach Kenntnis der Bundesregierung in die genannten Vorhaben und Initiativen zur (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten auch Vertreter/-innen aus den Bereichen Datenschutz, Bürgerrechte oder Netzpolitik eingebunden (insbesondere im SFZ TK, in der KomGÜT, dem UA IuK und dem ETSI)?

In den vorgenannten Forschungsprojekten des SFZ TK erfolgte keine Einbindung von Vertretern aus den genannten Bereichen.

In der Arbeitsgruppe ETSI TC LI werden keine gesellschaftspolitischen Diskussionen geführt, sondern ausschließlich Fragen erörtert, die einer telekommunikationstechnischen Umsetzung bestehender gesetzlicher Anforderungen bedürfen. Vertreter oder Vertreterinnen der in der Frage genannten Gruppen sind daher nicht in die Arbeitsgruppe ETSI TC LI eingebunden. Auf die Antworten zu den Fragen 16d und 16i wird verwiesen.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, 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