Deutscher Bundestag **Drucksache 17/11598**

17. Wahlperiode 21. 11. 2012

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Burkhard Lischka, Michael Hartmann (Wackernheim), Brigitte Zypries, weiterer Abgeordneter und der Fraktion der SPD – Drucksache 17/11087 –

Einsatz der Quellen-Telekommunikationsüberwachung

Vorbemerkung der Fragesteller

Am 8. Oktober 2011 veröffentlichte der Chaos Computer Club (CCC) die Analyse einer ihm zugespielten behördlichen Überwachungssoftware, sogenannter Trojaner, welche vom Landeskriminalamt Bayern auf den Laptop eines Verdächtigen aufgespielt worden war. Die Software verfügte über weitaus mehr Funktionen, als es der zugrunde liegende richterliche Beschluss zur Durchführung einer Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) vorsah. In der Folge wurde bekannt, dass entsprechende Software in zahlreichen weiteren Fällen eingesetzt worden war.

Aus den Ermittlungsakten hat sich ergeben, dass die Überwachungssoftware nicht nur die Telekommunikation in Form von Internettelefonaten und E-Mail-Verkehr überwachte, sondern auch alle 30 Sekunden eine Fotografie des Bildschirms, insgesamt 60 000 Screenshots angefertigt hatte. Bildschirminhalte sind jedoch nicht Teil der Telekommunikation. Hinzu kam, dass die Software in der Lage war, weitere Module nachzuladen. Diese sogenannte Nachladefunktion ermöglicht es, die Nutzung des Zielrechners umfassend zu überwachen und den Rechner umfänglich zu manipulieren. So ist es beispielsweise möglich, den Raum, in dem sich der Zielrechner befindet, mit einer eingebauten Kamera oder einem eingebauten Mikrofon zu überwachen, sämtliche auf dem Rechner gespeicherten Daten zu lesen und zu verändern sowie beliebige Programme auf dem Rechner auszuführen. Nach Auskunft des CCC war die Nachladefunktion funktionsfähig, ihr tatsächlicher Einsatz jedoch nicht beweisbar.

Das Programm enthielt nach Einschätzung von Fachleuten massive Sicherheitslücken. Durch eine unprofessionelle Verschlüsselung war das Programm dem Zugriff unautorisierter Dritter ausgesetzt. Der CCC konnte sein Trojanerprogramm in nur wenigen Stunden anpassen mit der Folge, dass er die Software hätte steuern und Funktionen auf den Zielrechner hätte nachladen können. Hinzu kommt, dass die ausgespähten Daten zur Tarnung der Steuerzentrale seitens der Behörde über einen in den USA befindlichen Server umgeleitet wurden. Es ist nicht auszuschließen, dass amerikanische Dienste Zugriff auf die Daten genommen haben.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 19. November 2012 übermittelt.

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

Entwickelt wurde das Überwachungsprogramm von der hessischen Firma DigiTask GmbH, deren Gründer vom Landgericht Köln wegen Bestechung von Beamten des Zollkriminalamtes Köln zu 21 Monaten Freiheitsstrafe auf Bewährung und 1,5 Mio. Euro Geldstrafe verurteilt wurde. Warum ausgerechnet dieses Unternehmen mit der Entwicklung und Lieferung der Software beauftragt wurde, ist bis heute nicht geklärt.

In ihrer Antwort auf die Kleine Anfrage „Staatstrojaner“ (Bundestagsdrucksache 17/7760) verneint die Bundesregierung den Einsatz der vom CCC analysierten Software durch Bundesbehörden. In Ermangelung des Quellcodes habe sie auch keine Kenntnis von den Funktionsmöglichkeiten der von Bundesbehörden eingesetzten Software gehabt. Vor Anwendung der Software seien jedoch in jedem Einzelfall Anwendungstests durchgeführt worden.

Die Bundesministerin der Justiz Sabine Leutheusser-Schnarrenberger und weitere Mitglieder der Bundesregierung haben angesichts der vielfältigen Vorwürfe totale Transparenz und Aufklärung versprochen – bisher jedoch ohne Ergebnis. Noch immer ist nicht abschließend geklärt, welche Behörden Trojaner eingesetzt haben und mit welchem Funktionsumfang.

Auf die Frage, ob die Quellen-TKÜ derzeit von Bundesbehörden angewendet wird, oder ob es bis zur Entwicklung einer eigenen Software ein Moratorium gebe, antwortete der Parlamentarische Staatssekretär bei der Bundesministerin der Justiz in der Fragestunde am 13. Juni 2012, dass er nur die sichere Erkenntnis habe, dass die von der DigiTask GmbH hergestellte Software in Bayern nicht mehr eingesetzt werde. Schriftlich reichte er nach, dass „der zum Geschäftsbereich des Bundesministeriums der Justiz (BMJ) gehörende Generalbundesanwalt die Quellen-TKÜ derzeit weder anwendet noch diese veranlasst“. Gründe für die Nichtanwendung durch den Generalbundesanwalt nannte er nicht. Unbeantwortet blieb auch die Frage, welche Bundesbehörden die Software einsetzen oder Quellen-TKÜ durchführen.

Derzeit findet der Einsatz von Überwachungssoftware zum Zwecke der Strafverfolgung auf Grundlage der §§ 100a ff. der Strafprozessordnung (StPO) statt. Bei der Schaffung der §§ 100a ff. StPO hatte der Gesetzgeber jedoch die netzbasierte Überwachung der herkömmlichen Telekommunikation vor Augen und nicht die wesentlich komplexere Überwachung durch den heimlichen Zugriff auf einen Rechner. § 100a StPO berücksichtigt die durch den Einsatz von Überwachungssoftware bewirkte Beeinträchtigung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht. Insbesondere enthält diese Vorschrift keine Schutzvorkehrungen, um rechtlich und technisch sicherzustellen, dass die Überwachung sich auf die laufende Telekommunikation beschränkt und dass Manipulationen durch Dritte ausgeschlossen sind. Das Bundesverfassungsgericht (BVerfG) hat in seiner Entscheidung zur Onlinedurchsuchung vom 27. Februar 2008 (BVerfGE, 1 BvR 370/07 u. a.) die entsprechenden Anforderungen formuliert. Dazu zählen in erster Linie der möglichst weitgehende Schutz der Integrität des Zielsystems und die Beschränkung auf die laufende Telekommunikation. Das BVerfG hat zudem technische Sicherungen gegen Missbrauch angemahnt und ausgeführt, dass eine Ermächtigung zum heimlichen Zugriff auf informationstechnische Systeme mit geeigneten gesetzlichen Vorkehrungen verbunden werden muss, um die Interessen des Betroffenen verfahrensrechtlich abzusichern (BVerfGE, a. a. O., Rn. 257). Aufgrund der durch heimliche Ermittlungsmaßnahmen bewirkten schwerwiegenden Grundrechtseingriffe ist es geboten, den Betroffenen mittels einer vorbeugenden Kontrolle durch eine unabhängige Instanz zu schützen (BVerfGE, a. a. O., Rn. 259).

Auf die Frage, ob die Bundesregierung beabsichtige, den Entwurf für eine eigene Rechtsgrundlage für die Quellen-TKÜ vorzulegen, antwortete der Parlamentarische Staatssekretär bei der Bundesministerin der Justiz, dass die Gerichte § 100a StPO im Bereich der Strafverfolgung auch für die Quellen-TKÜ anwenden. Hierzu gäbe es mittlerweile eine verfestigte Rechtsprechung. Die Erforderlichkeit einer zusätzlichen Regelung würde derzeit geprüft.

Trotz eindeutiger Formulierungen in der Entscheidung des BVerfG und gewichtiger Gegenstimmen in Rechtsliteratur und Wissenschaft beruft sich die

Bundesregierung allein auf die „einhellige Praxis der Gerichte“, die § 100a StPO als Rechtsgrundlage heranziehen. Während die Bundesministerin der Justiz die Norm noch zu Jahresbeginn als nicht hinreichende Rechtsgrundlage bezeichnet hat, zieht sie sich jetzt auf den Standpunkt zurück, die Erforderlichkeit einer speziellen Rechtsgrundlage sei Gegenstand intensiver Prüfung.

Vorbemerkung der Bundesregierung

Die Fragen 1, 4, 7, 14, 24, 25, 26 und 28 begehren Auskünfte zu Sachverhalten, die aufgrund der Folgen, die bei ihrer Veröffentlichung zu erwarten sind, als „geheimzuhaltende Tatsache“ im Sinne des Sicherheitsüberprüfungsgesetzes (SÜG) in Verbindung mit der Verschlusssachenanweisung (VSA) einzustufen sind. Die Kenntnisnahme von Einzelheiten zu den technischen Fähigkeiten der Bundesbehörden könnte sich nach der Veröffentlichung der Antworten der Bundesregierung auf diese Frage nachteilig für die Interessen der Bundesrepublik Deutschland auswirken. Aus ihrem Bekanntwerden könnten sowohl staatliche als auch nichtstaatliche Akteure Rückschlüsse auf den Modus Operandi und die Fähigkeiten der Behörden des Bundes ziehen. Im Ergebnis würde dadurch die Funktionsfähigkeit der Sicherheitsbehörden und mithin die Sicherheit der Bundesrepublik Deutschland beeinträchtigt bzw. gefährdet.

Diese Informationen werden daher gemäß § 3 Nummer 4 VSA als „Verschlusssache (VS) – Nur für den Dienstgebrauch“ eingestuft und dem Deutschen Bundestag gesondert übermittelt.

1. Wird die Quellen-TKÜ derzeit im Bereich des Bundes durchgeführt, und wenn ja, durch welche Bundesbehörden, und in welchem Umfang?

Auf den dem Deutschen Bundestag gesondert übermittelten als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil wird verwiesen.*

2. Wird nach Kenntnis der Bundesregierung die Quellen-TKÜ derzeit von Landesbehörden durchgeführt, und wenn ja, durch welche Landesbehörden, und in welchem Umfang?

Die Bundesregierung hat keine Kenntnis darüber, ob derzeit Quellen-TKÜ-Maßnahmen von Landesbehörden durchgeführt werden.

3. Welche Überwachungssoftware, in welcher Version und von welchem Hersteller kommt im Bereich des Bundes und nach Kenntnis der Bundesregierung der Länder jeweils zum Einsatz?

Auf die Antworten zu den Fragen 1 und 2 wird verwiesen.

4. In wie vielen Fällen haben welche Bundes- und nach Kenntnis der Bundesregierung Landesbehörden im Zeitraum von 2008 bis 2011 Quellen-TKÜ durchgeführt (bitte gesondert nach Jahr und Behörde)?

Auf den dem Deutschen Bundestag gesondert übermittelten als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil wird verwiesen.*

* Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

5. Haben Behörden rechtliche und/oder technische Bedenken gegen den Einsatz von Softwareprodukten (Trojaner, etc.) zur Quellen-TKÜ und der Onlinedurchsuchung geltend gemacht, und wenn ja, mit welcher Begründung?

Der Generalbundesanwalt beim Bundesgerichtshof hat rechtliche und auch technische Bedenken gegen den Einsatz von Softwareprodukten zur Quellen-TKÜ erhoben. Im Übrigen wird auf die Antwort zu Frage 15b verwiesen.

6. Wurde die eingesetzte Software daraufhin geprüft, ob die Vorgaben des BVerfG für die Quellen-TKÜ technisch eingehalten werden?

   Liegt den jeweiligen Ermittlungsbehörden der Quellcode der eingesetzten Software vor?

Auf die Antwort der Bundesregierung zu den Fragen 6 und 9 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 17/7760 vom 17. November 2011 wird verwiesen.

7. Kann die Bundesregierung ihre nach der Veröffentlichung des CCC im Oktober 2011 vertretene Auffassung bestätigen, dass bis zur Entwicklung einer eigenen Software keine Quellen-TKÜ im Bereich der Bundesbehörden eingesetzt wird?

Die Bundesregierung hat keine Aussage im Sinne der Fragestellung getätigt.

Im Übrigen wird auf den dem Deutschen Bundestag gesondert übermittelten als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil verwiesen.*

8. Gab oder gibt es Überlegungen, das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit der Entwicklung einer Quellen-TKÜ-Software zu betrauen?

Nein.

9. Wurde außer der umstrittenen Software der DigiTask GmbH weitere Software für die Quellen-TKÜ genutzt, und wenn ja, von welchen Anbietern?

   Haben diese Anbieter den Quellcode offengelegt?

Im Jahr 2007 wurde im Zollfahndungsdienst auf Software des schweizerischen Unternehmens ERA-IT Solutions zur Durchführung der Quellen-TKÜ zurückgegriffen. Das Unternehmen hat sich im Jahr 2008 aus diesem Geschäftsfeld zurückgezogen. Eine Offenlegung des Quellcodes erfolgte nicht. Im Übrigen wird auf die Antworten zu den Fragen 6 und 9 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 17/7760 vom 17. November 2011 verwiesen.

Ansonsten wurde zur Quellen-TKÜ ausschließlich Software der Firma DigiTask GmbH von Bundesbehörden eingesetzt.

---

* Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

10. Wird das Zollkriminalamt weiter von der Firma DigiTask GmbH mit Überwachungssoftware beliefert, obwohl die Untersuchung der DigiTask GmbH-Software durch den CCC gravierende Mängel zutage brachte?

Bei der Firma DigiTask GmbH handelt es sich um ein technisch erfahrenes und langjährig bewährtes Unternehmen, bei dem das Zollkriminalamt mit Zuschlagserteilung die dortige TKÜ-Anlage beschafft hat und damit aufgrund der getroffenen technischen Systemauswahl bis heute Hard- und Software bezieht. Eine Neukonzeption der TKÜ-Technik ist jedoch derzeit in Vorbereitung.

11. Wurde auch eine Software der Firma ERA IT Solutions AG genutzt, und wenn ja, von wem, und in welchem Umfang?

Auf die Antwort zu Frage 9 wird verwiesen.

12. Hat die Firma ERA IT Solutions AG den Quellcode offengelegt?

Nein.

13. Wurde die Software der Firma ERA IT Solutions AG überprüft, und wenn ja, mit welchem Ergebnis?

Auf die Antwort zu Frage 9 wird verwiesen.

14. Wurde Quellen-TKÜ-Software auf einem im Ausland befindlichen Rechner genutzt?

Wurde gegebenenfalls die Software bereits im Ausland aufgespielt, oder wurde der infizierte Rechner später ins Ausland verbracht?

Wurden gegebenenfalls die Behörden am ausländischen Standort des Rechners in die Überwachungsmaßnahmen einbezogen?

Auf den dem Deutschen Bundestag gesondert übermittelten als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil wird verwiesen.*

15. a) Auf wessen Veranlassung wendet der Generalbundesanwalt beim Bundesgerichtshof die Quellen-TKÜ derzeit nicht an bzw. veranlasst diese nicht?

Der Generalbundesanwalt beim Bundesgerichtshof ist aufgrund eigener Rechtsprüfung zu dem Ergebnis gelangt, dass derzeit keine ausreichende strafprozessuale Rechtsgrundlage für diese Ermittlungsmaßnahme bestehe.

b) Aus welchem Grund wendet der Generalbundesanwalt beim Bundesgerichtshof die Quellen-TKÜ derzeit nicht an?

Auf die Antwort zu Frage 50 wird verwiesen.

Nach Ansicht des Generalbundesanwalts beim Bundesgerichtshof fehlt es für den strafprozessualen Bereich an der erforderlichen Rechtsgrundlage für einen

* Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

Eingriff in das vom Bundesverfassungsgericht in seiner Entscheidung vom 27. Februar 2008 zur Onlinedurchsuchung (1 BvR 370/07) entwickelte Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes (GG). Die in fachgerichtlichen Entscheidungen als Eingriffsgrundlage für eine Quellen-TKÜ angesehene Vorschrift des § 100a StPO vermöge nach der genannten Entscheidung des Bundesverfassungsgerichts die Maßnahme nur zu rechtfertigen, wenn sichergestellt werden kann, dass ein weitergehender Eingriff in die Vertraulichkeit und die Integrität des geschützten Systems unterbleibt. Eine solche Begrenzung des Eingriffs kann jedoch nach Ansicht des Generalbundesanwalts beim Bundesgerichtshof derzeit technisch nicht hinreichend sicher gewährleistet werden.

c) Hat das BMJ dieses Vorgehen gebilligt?

d) Wie bewertet des BMJ die Entscheidung des Generalbundesanwalts beim Bundesgerichtshof?

Das BMJ ist der Auffassung, dass der Generalbundesanwalt beim Bundesgerichtshof unter Berücksichtigung der Entscheidung des Bundesverfassungsgerichts zur Onlinedurchsuchung gewichtige Gründe für seine Entscheidung habe, derzeit keine Quellen-TKÜ durchzuführen.

16. Zu welchem Ergebnis kommt das dem Generalbundesanwalt beim Bundesgerichtshof vorliegende Gutachten zur Rechtmäßigkeit der Quellen-TKÜ?

Auf die Antworten zu den Fragen 15b und 17 wird verwiesen.

17. Wer hat das Gutachten erstellt, und in wessen Auftrag?

Es handelt sich bei der oben zu Frage 15b dargestellten Bewertung nicht um ein in Auftrag gegebenes Gutachten, sondern um die Rechtsauffassung des Generalbundesanwalts beim Bundesgerichtshof.

18. Wie bewertet die Bundesregierung das Ergebnis des Gutachtens?

19. Wann wird die Bundesregierung den Deutschen Bundestag über die Ergebnisse dieses Gutachtens unterrichten?

Die Fragen 18 und 19 werden wegen ihres Sachzusammenhangs gemeinsam beantwortet.

Auf die Antwort zu Frage 17 wird verwiesen.

20. Was passiert in den Fällen, in denen bereits Ermittlungen laufen und eine Quellen-TKÜ angeordnet ist, wenn die Ermittlungen vom Generalbundesanwalt beim Bundesgerichtshof übernommen werden?

Die regelmäßig zeitlich befristeten richterlichen Anordnungen werden mit Blick auf deren rechtliche Verbindlichkeit bis zu ihrem Ablauf umgesetzt. Nach Auslaufen der Maßnahmen werden keine Verlängerungsanträge gestellt.

21. Kann die Bundesregierung ausschließen, dass Ermittlungsverfahren nicht an den Generalbundesanwalt beim Bundesgerichtshof als ermittlungsführende Staatsanwaltschaft übertragen werden, aus Sorge, die Quellen-TKÜ als Ermittlungsinstrument nicht nutzen zu können?

    a) Wenn ja, wie begründet die Bundesregierung diese Einschätzung?

    b) Wenn nein, was wird die Bundesregierung veranlassen?

Die sich aus § 142a in Verbindung mit § 120 Absatz 1 und 2 des Gerichtsverfassungsgesetzes ergebende Zuständigkeit des Generalbundesanwalts beim Bundesgerichtshof für die Strafverfolgung sieht eine Zuständigkeitsbeschränkung im Sinne der Fragestellung nicht vor. Die Bundesregierung hat keinen Anlass, an der Einhaltung dieser gesetzlichen Vorgaben durch die Strafverfolgungsbehörden der Länder zu zweifeln.

22. Teilt die Bundesregierung die Ansicht des Innnenpolitischen Sprechers der CDU/CSU-Bundestagsfraktion, Dr. Hans-Peter Uhl, der zufolge die Entwicklung einer Software zur Quellen-TKÜ durch das Bundeskriminalamt (BKA) voraussichtlich noch Monate, vielleicht sogar Jahre dauern oder möglicherweise gar nicht realisiert werden kann?

Für die Entwicklung einer Software zur Quellen-TKÜ baut das BKA eine entsprechende Fachgruppe auf. Die hierfür erforderliche Personalgewinnung benötigt ebenso wie die Erstellung der Eigenentwicklung Zeit. Vor diesem Hintergrund wird mit der Fertigstellung der Eigenentwicklung des BKA Ende des Jahres 2014 gerechnet. Im Übrigen liegen der Bundesregierung keine Erkenntnisse vor, die Zweifel an einem erfolgreichen Abschluss der Eigenentwicklung durch das BKA nahelegen würden.

23. Worauf bezogen sich die in Bund und nach Kenntnis der Bundesregierung in den Ländern durchgeführten Maßnahmen zur Quellen-TKÜ (bitte aufschlüsseln):

- Internettelefonie (Voice over IP, z. B. Skype),
- Internetchat,
- E-Mail über HTTP(S)/Webmail,
- Überwachung inhaltsverschlüsselter E-Mail-Kommunikation (S/MIME oder PGP),
- Überwachung transportbasierter E-Mail-Kommunikation (IMAPS, POPS, SMTP mit TSL),
- Onlinebanking,
- andere, und wenn ja, welche?

Die im Verantwortungsbereich des Bundes durchgeführten Maßnahmen bezogen sich überwiegend auf die Internettelefonie, vereinzelt auch auf Internetchat. Zu den in ausschließlicher Zuständigkeit der Länder geführten Verfahren liegen der Bunderegierung keine Kenntnisse vor.

24. Kann die Bundesregierung ausschließen, dass aufgespielte Trojaner zwar „abgeschaltet“, jedoch nicht vom System entfernt wurden?

25. Wenn nein, wie viele Trojaner wurden „abgeschaltet“, ohne vom System entfernt worden zu sein?

26. Erfolgte die Deinstallation der Überwachungssoftware durch die Ermittlungsbehörden, und war sie jeweils erfolgreich?

Die Fragen 24 bis 26 werden wegen ihres Sachzusammenhangs gemeinsam beantwortet.

Auf den dem Deutschen Bundestag gesondert übermittelten als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil wird verwiesen.*

27. Wurden die Betroffenen nach Beendigung der Quellen-TKÜ über den Eingriff informiert?

Soweit keine der gesetzlich geregelten Ausnahmetatbestände für die Benachrichtigung der Betroffenen vorlagen, wurden diese gemäß den jeweiligen rechtlichen Vorgaben benachrichtigt.

28. Warum hat die hessische Firma DigiTask GmbH den Zuschlag für die Entwicklung der Überwachungssoftware bekommen?

Gab es weitere Bewerber, und wenn ja, welche?

Auf den dem Deutschen Bundestag gesondert übermittelten als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil wird verwiesen.*

29. Hat sich die Bundesregierung um die Offenlegung des Quellcodes bemüht, und wenn ja, in welcher Form, und mit welchem Ergebnis?

Wenn nein, warum nicht?

30. Hat die Bundesregierung jemals Verhandlungen zur Änderung des Vertrags geführt?

Wenn nein, warum nicht?

Wenn ja, mit welchem Ergebnis?

Die Fragen 29 und 30 werden wegen ihres Sachzusammenhangs gemeinsam beantwortet.

Auf die Antwort der Bundesregierung zu Frage 9 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 17/7760 vom 17. November 2011 wird verwiesen.

* Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

31. Wie bewertet die Bundesregierung die Tatsache, dass die Firma DigiTask GmbH den Zugang zum Quellcode mit Hinweis auf vertragliche Abreden verweigert, die aus Sicht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) nicht akzeptabel sind?

Der Quellcode einer vermarkteten Software wird als Vermögenswert eines Unternehmens beurteilt und demzufolge als Geschäfts- und Betriebsgeheimnis geschützt. Die Bereitstellung eines Quellcodes ist daher unüblich oder erfolgt unter Nebenabreden, die das Geschäfts- und Betriebsgeheimnis des Herstellers einer Software schützen.

Um dem BfDI Einsichtnahme in den Quellcode zu ermöglichen, hat das BKA als auftraggebende Stelle für die Quellen-TKÜ-Software Kontakt zur Firma DigiTask GmbH aufgenommen. Seitens der Firma DigiTask GmbH bestand Bereitschaft, dem BfDI Einblick in den Quellcode zu gewähren, jedoch unter der Bedingung, dass seine Geschäfts- und Betriebsgeheimnisse nach außen gewahrt bleiben. Nach Verlautbarungen des BfDI konnte dieser die Bedingungen der Firma DigiTask GmbH zur Wahrung der Geschäfts- und Betriebsgeheimnisse nicht akzeptieren, da er seine gesetzliche Kontrollkompetenz beschränkt sah. Die Bundesregierung sieht keine Veranlassung, die Vorgehensweise des BfDI zu bewerten.

32. Wie soll der BfDI seine gesetzliche Aufgabe, also die datenschutzrechtliche Beratung und Kontrolle der Bundesbehörden, ohne Kenntnis des Quellcodes erfüllen?

Die Einsichtnahme in den Quellcode einer Software kann im Einzelfall sinnvoll sein, ohne dass dies allerdings generell bei dem Erwerb von Softwareprodukten geboten erscheint.

Ein Softwarehersteller hat regelmäßig ein wirtschaftliches Interesse, seine Produkte auf diejenigen Funktionen zu beschränken, die der Auftragnehmer seiner Beauftragung zugrunde gelegt hat. Dieser geforderte Funktionsumfang der Software sowie eine Vielzahl von Schlechtleistungen können vom Auftragnehmer in der Regel abschließend anhand von Tests des gelieferten ausführbaren Programms geprüft werden. Demgegenüber lässt sich die Existenz von nicht geforderten Funktionen einer Software anhand des Programms nur näherungsweise testen. Die Einsichtnahme in den Quellcode wäre also dann sinnvoll, wenn Grund für die Annahme besteht, dass die gelieferte Software einen größeren als den geforderten Funktionsumfang aufweist.

Sieht der BfDI im Einzelfall Bedarf, den Quellcode einer Software in seine Prüfung einzubeziehen, bemüht sich die Bundesregierung, ihm diese Einsicht zu ermöglichen.

33. Teilt die Bundesregierung die Auffassung des BfDI, dass § 9 des Bundesdatenschutzgesetzes (BDSG) in verfassungskonformer Auslegung die Dokumentation des Quellcodes bei Maßnahmen der Quellen-TKÜ fordert?

Die Bundesregierung geht davon aus, dass mit „Dokumentation des Quellcodes“ dessen Verfügbarkeit bei der einsetzenden Stelle und die Vorlage des Quellcodes zu Zwecken der datenschutzrechtlichen Prüfung durch den BfDI gemeint ist. Der BfDI hat in seinem Schreiben an den Innenausschuss des Deutschen Bundestages vom 14. August 2012 die in der Frage genannte Rechtsauffassung geäußert und dabei Bezug auf die Analysen des CCC genommen. Diese Analysen geben nach seiner Auffassung Anlass, den Quellcode einzusehen, um insbesondere zu prüfen, dass keine unzulässige Informationserhebung stattfindet.

Der in diesem Einzelfall geäußerten Wunsch, den Quellcode einzusehen, wird seitens der Bundesregierung begrüßt, da eine Reihe der Analyseergebnisse des CCC insbesondere durch eine Quellcodeanalyse hätten näher untersucht werden können. Aus diesem Einzelfall kann jedoch keine generelle Pflicht zur Quellcode-Dokumentation abgeleitet werden. Eine solche einzelfallbezogene Verhältnismäßigkeitsprüfung ist auch in § 9 BDSG angelegt. Dort heißt es sinngemäß, dass technische und organisatorische Maßnahmen nur zu treffen sind, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Ohne Anerkennung einer rechtlichen Verpflichtung haben sich jedoch die Bedarfsträger von Bund und Ländern darauf geeinigt, zukünftig den Quellcode bei Quellen-TKÜ-Maßnahmen zu dokumentieren und den für die datenschutzrechtliche Kontrolle zuständigen Stellen zu Prüfzwecken zur Verfügung zu stellen.

34. Warum haben die Bundesbehörden angesichts der hohen Eingriffsintensität nicht von Anfang an auf die Offenlegung des Quellcodes bestanden?

Auf die Antworten zu den Fragen 32 und 33 wird verwiesen.

35. Teilt die Bundesregierung die Auffassung, dass – um unzulässige Funktionalitäten zuverlässig ausschließen zu können – die Einsichtnahme in den Quellcode unerlässlich ist?

Die Bundesregierung geht davon aus, dass mit „unzulässigen Funktionalitäten“ Funktionsweisen der Software gemeint sind, die bewusst zu der Realisierung eines über den zulässigen Umfang der Überwachungsmaßnahme hinausgehenden Zwecks in der Software integriert sind. Demgegenüber sind „unerwünschte Funktionen“ der Software Funktionsweisen, die beispielsweise aus einer vorher nicht erkennbaren Wechselwirkung zwischen dem zu überwachenden System und der Überwachungssoftware oder Programmierfehlern entstehen könnten.

Die Funktion beschaffter Software hat die einsetzende Stelle durch Tests dahingehend zu prüfen, dass die Software den angeordneten Funktionsumfang erfüllt.

Der Test des Funktionsumfangs anhand des ausführbaren Programms findet jedoch seine Grenzen, wenn die Software Funktionen enthält, von denen auch die einsetzende Stelle keine Kenntnis hat. In diesem Fall kann die Prüfung des Quellcodes zusätzliche Erkenntnisse erbringen. Auf die Antworten zu den Fragen 32 und 33 wird verwiesen.

36. Warum haben das BKA und nach Kenntnis der Bundesregierung die Landeskriminalämter (LKAs) nicht auf der Vereinbarung eines vertraglichen Rechts auf Einsichtnahme in den Quellcode bestanden, das die Kontrolle durch die erhebende und speichernde Stelle und die des BfDI und der jeweiligen Landesbeauftragten für den Datenschutz ermöglicht hätte?

Auf die Antwort zu Frage 29 wird verwiesen.

37. Wer ist an der Erstellung der Leistungsbeschreibung für die Ausgestaltung einer künftigen Überwachungssoftware durch das Kompetenzzentrum Informationstechnische Überwachung (CC ITÜ) beteiligt?

An der Erstellung der Leistungsbeschreibung für die Ausgestaltung einer künftigen Überwachungssoftware (Standardisierende Leistungsbeschreibung) sind das Bundesministerium des Innern (BMI), das Bundesamt für Verfassungs-

schutz (BfV), das BKA, die Bundespolizei (BPOL), der Militärische Abschirmdienst (MAD), das Zollkriminalamt (ZKA) die Innenressorts der Länder sowie die Arbeitskreise II und IV der Ständigen Konferenz der Innenminister und -senatoren der Länder beteiligt.

38. Wer ist an der Entwicklung der Software für die Quellen-TKÜ beteiligt?

Die Eigenentwicklung einer Software zur Durchführung von Maßnahmen der Quellen-TKÜ erfolgt durch das BKA im Kompetenzzentrum Informationstechnische Überwachung. Das BKA wird dabei derzeit durch die Länder Bayern, Hessen und das ZKA unterstützt. Baden-Württemberg hat ebenfalls seine Unterstützung zugesagt. Zur Erfüllung einzelner Aufgaben wie z. B. der Qualitätssicherung sind externe Dienstleister eingebunden.

39. Welche Funktionen soll die zu erstellende Software haben (genaue technische Vorgaben für die zu überwachende Kommunikation, Nachladefunktion, Dokumentation, Löschungsmöglichkeiten für kernbereichsrelevante Inhalte, etc.)?

Die Software soll zum Zeitpunkt der Überwachung laufende Telekommunikation überwachen. Die in der Frage als Nachladefunktion bezeichnete Updatefunktion soll ausschließlich der Aktualisierung der Software dienen, ohne den o. g. Funktionsumfang zu erweitern, und ausschließlich durch die einsetzende Behörde genutzt werden können.

Es wird sichergestellt, dass der Einsatz der Software und jedes Update umfassend protokolliert wird. Darüber hinaus wird ein Hashwert über das Update gebildet, damit im Nachhinein eindeutig festgestellt werden kann, welches Update wann durchgeführt wurde, und ob dieses erfolgreich war.

Die Löschung kernbereichsrelevanter Inhalte wird wie bei der konventionellen Telekommunikationsüberwachung erfolgen.

40. Ist es aus Sicht der Bundesregierung verfassungsrechtlich zulässig, dass der vom CCC analysierte Trojaner nicht nur das Auslesen, sondern auch das Einspielen von Daten auf das Zielsystem ermöglichte?

Für das Einspielen anderer Daten auf das Zielsystem als die der Überwachungssoftware gibt es weder eine Veranlassung noch eine Rechtsgrundlage. Es ist somit unzulässig.

Im Hinblick auf die Bewertung der Updatefunktion wird auf die Antwort zu Frage 45 verwiesen.

41. Durch welche technischen und rechtlichen Vorkehrungen will die Bundesregierung sicherstellen, dass sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt, und inwieweit kann dies angesichts der Nachladefunktion gewährleistet werden?

Gemäß Absatz 190 der Entscheidung des Bundesverfassungsgerichts vom 27. Februar 2008 zur Onlinedurchsuchung ist durch technische Vorkehrungen und rechtliche Vorgaben sicherzustellen, dass sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt.

Im Hinblick auf die rechtlichen Vorgaben wird auf die Antwort zu Frage 50 verwiesen.

Die im Rahmen einer Quellen-TKÜ zu überwachende Kommunikationssoftware weist naturgemäß eine Reihe von Softwareschnittstellen auf, die ausschließlich während eines laufenden Kommunikationsvorgangs aktiv sind. Dabei kann es sich sowohl um einzelne Aktivitäten als auch um einen aktiven Verbund von Schnittstellen handeln, die einen laufenden Kommunikationsvorgang kennzeichnen. Die Festlegung dieser Kriterien, die einen laufenden Kommunikationsvorgang kennzeichnen, muss im Einzelfall abhängig von dem zu überwachenden Kommunikationsprogramm erfolgen und in der Überwachungssoftware verankert sein.

Die Einhaltung der notwendigen Kriterien der zur Quellen-TKÜ genutzten Software wurde bereits in der Vergangenheit durch eine umfassende Protokollierung sichergestellt. Für die zukünftig zur Quellen-TKÜ eingesetzte Software ist das Verfahren für die umfassende Protokollierung zusätzlich auch in der Standardisierenden Leistungsbeschreibung festgelegte. Durch die Dokumentation des Quellcodes, des Prozesses der Programmerzeugung aus diesem Quellcode und des Programms selbst kann im Nachhinein der Funktionsumfang der jeweils eingesetzten Überwachungssoftware abschließend nachvollzogen werden.

42. Wie soll sichergestellt werden, dass nur die von der richterlichen Anordnung umfassten Zielrechner infiltriert werden?

Vor Beginn der Überwachung und Aufzeichnung der Telekommunikation erfolgt anhand von System-Metadaten eine Identifizierung des Zielsystems, auf dem die Überwachungssoftware verankert wurde, die mit den aus der Voraufklärung des Zielsystems bereits bekannten System-Metadaten abgeglichen werden. Nur bei Übereinstimmung der Metadaten erfolgt eine Überwachung und Aufzeichnung der Telekommunikation. Anderenfalls wird die Überwachungssoftware unverzüglich vom Zielsystem gelöscht.

43. Berechtigt die Rechtsgrundlage für die Quellen-TKÜ nach Ansicht der Bundesregierung zum Betreten der Wohnung, in der sich der Zielrechner befindet?

Eine in richterlicher Unabhängigkeit getroffene Auslegung des geltenden Strafprozessrechts, nach der die § 100a und § 100b StPO Grundlage für die Anordnung einer Quellen-TKÜ sein können, berechtigt nach Auffassung der Bundesregierung nicht zugleich zu einem Eingriff in Artikel 13 GG. Dies gilt auch für Präventivbefugnisse nach dem Zollfahndungsdienstgesetz, dem G-10-Gesetz und dem Bundeskriminalamtgesetz.

44. Ist das Auslesen von Softwarelisten im Sinne einer effektiven Strafverfolgung unumgänglich?

Zum Schutz unbeteiligter Dritter muss sichergestellt werden, dass die Überwachungssoftware nur auf dem von der Anordnung umfassten System zur Ausführung kommt. Eine solche Sicherstellung kann nur durch einen Vergleich von im Vorfeld der Maßnahme erhobenen Metadaten mit Metadaten des Systems, auf dem die Überwachungssoftware eingebracht wurde, erfolgen. Diese Metadaten bestehen jedoch nicht notwendigerweise aus Softwarelisten, sondern können jedes Systemdatum umfassen, das für die eindeutige Kennzeichnung des zu überwachenden Systems geeignet ist. Der Erheben und Vergleichen von Metadaten dient somit vornehmlich dem Schutz unbeteiligter Dritter.

45. Wie lässt sich die Quellen-TKÜ von der Onlinedurchsuchung abgrenzen, wenn man die Notwendigkeit der Nachladefunktion unterstellt?

Die Möglichkeit, die zur Quellen-TKÜ verwendete Software während des Anordnungszeitraums an Veränderungen des technischen Systems anzupassen (Updatefunktion), ist fachlich erforderlich. Sie stellt im Übrigen keinen qualitativen Unterschied zu der Einbringung der Überwachungssoftware dar, da anstelle der Durchführung des Updates auch das Löschen der bisher genutzten Software oder das Aufbringen einer an die technischen Gegebenheiten angepassten neuen Version der Quellen-TKÜ-Software erfolgen kann. Auf das Löschen und Wiedereinspielen wird jedoch verzichtet, da die erneute Einbringung einer angepassten Softwareversion den Aufwand und das Entdeckungsrisiko unangemessen erhöht.

Bereits bei der erstmaligen Aufbringung der Quellen-TKÜ-Software wird durch Prüfung sichergestellt, dass der gemäß Anordnung zulässige Umfang der Überwachungsmaßnahme eingehalten wird. Dies ist durch die Dokumentation des eingesetzten Programms auch im Nachhinein belegbar. Ebenso wie bei der erstmaligen Aufbringung der Quellen-TKÜ-Software wird auch das Update vor der Installation auf den gemäß Anordnung zulässigen Umfang der Überwachungsmaßnahme geprüft und ebenfalls für eine Überprüfung im Nachhinein dokumentiert. Die vorsätzliche Umwandlung des Programms zur Quellen-TKÜ in ein Programm zur Onlinedurchsuchung wäre eine rechtlich unzulässige Handlung der einsetzenden Stelle und im Nachhinein anhand der Protokollierung und Dokumentation feststellbar.

Im Übrigen wird auf die Antwort zu Frage 40 verwiesen.

46. Für welche konkreten Fälle ist eine Quellen-TKÜ unerlässlich?

Ob die Durchführung einer Quellen-TKÜ zulässig und im Einzelfall „unerlässlich“ im Sinne der Fragestellung ist, entscheidet im repressiven Bereich das zuständige Gericht, bei Gefahr im Verzug nach § 100b Absatz 1 Satz 2 StPO zunächst die Staatsanwaltschaft. Generell wird die Quellen-TKÜ genutzt, um verschlüsselte Kommunikation überwachen zu können. Die z. B. in der Software Skype implementierte Verschlüsselung führt im Falle von Skype-to-Skype-Telekommunikation dazu, dass diese ausschließlich im Wege eines Eingriffs mit technischen Mitteln in das zur Kommunikation genutzte informationstechnische System in unverschlüsselter Form erschlossen werden kann.

Dies gilt entsprechend für die nach gefahrenabwehrrechtlichen Vorschriften durchgeführte Quellen-TKÜ.

Im Übrigen wird auf die Antworten zu den Fragen 47 und 49 verwiesen.

47. Welche grundrechtsschonenderen Alternativen zum Einsatz von Überwachungssoftware, etwa das Abhören von Internettelefonie über Schnittstellen, hat die Bundesregierung geprüft, und mit welchem Ergebnis?

Die Internettelefonie kann in zwei wesentliche technische Funktionsweisen unterteilt werden. Dabei umfasst der erste Bereich die klassische Telefonie zumeist mit herkömmlichen Endgeräten, die von den Telekommunikationsanbietern auf internetbasierte Verfahren umgestellt worden ist. Der zweite Bereich umfasst Software, die über das Internet Kommunikationsverbindungen unmittelbar zwischen den Kommunikationsteilnehmern (Peer-to-Peer) aufbaut. Die Endgeräte sind in diesem Fall zumeist Computer oder Smartphones. Das verwendete Kommunikationsprotokoll ist in der Regel das Voice over Internet Protocol (VoIP).

Für den zweiten Bereich sind grundsätzlich drei Verfahren denkbar, um an die Inhalte der verschlüsselten Internettelefonie zu gelangen:

- Ausleitung der Telekommunikation über den Anschluss des Betroffenen beim Diensteanbieter und nachfolgende Dechiffrierung der verschlüsselten Kommunikation,
- Umleitung der Kommunikation über zentrale technische Einrichtungen (z. B. Skype-Supernodes), wobei die Kommunikation bei der Übergabe an die zentrale Einrichtungen dechiffriert wird und
- Schaffung einer sogenannten Hintertür (Backdoor) in der Kommunikationssoftware, entweder um an Informationen zu gelangen, mit denen die Verschlüsselung im Nachhinein aufgehoben werden kann, oder um eine parallele Ausleitung der unverschlüsselten Kommunikation zu eröffnen.

Die vorangehend genannten Möglichkeiten begegnen nach vorläufiger, jedoch noch nicht abgeschlossener Prüfung der Bundesregierung in ihrer praktischen Umsetzung erheblichen Schwierigkeiten. So gilt die Dechiffrierung der verschlüsselten Kommunikation außer in Ausnahmefällen (technische Fehler, ungeeignete Schlüssel) nach den Maßstäben der Wissenschaft als praktisch undurchführbar. Ferner fehlen rechtliche Möglichkeiten, ausländische Softwareanbieter zum Betrieb von oder zur Umleitung auf zentrale Einrichtungen oder zur Schaffung von Hintertüren in der Software zu verpflichten.

48. Mit welchen Anbietern, beispielsweise von Internettelefonie oder auch Clouddiensten, hat die Bundesregierung diesbezüglich Gespräche geführt, und mit welchem Ergebnis (bitte aufschlüsseln)?

Derzeit befasst sich das Strategie- und Forschungszentrum Telekommunikation (SFZ TK) im Projekt CLOUD mit Fragestellungen zu Cloud-Computing und dessen Implikationen auf die Telekommunikationsüberwachung. In diesem Zusammenhang erfolgte auch ein erstes Gespräch mit Vertretern der Deutsche Telekom AG sowie der 1&1 Internet AG. Konkrete Ergebnisse im Projekt sind bislang nicht zu verzeichnen. Im Zuge der Standardisierung der Telekommunikationsüberwachung bei ETSI (European Telecommunications Standards Institute) wird derzeit ein „Technischer Report“ zu Clouddiensten unter dem Aspekt der Telekommunikationsüberwachung erarbeitet. Zur Vorbereitung erfolgte ein gemeinsames Gespräch mit der Bundesnetzagentur, der Deutschen Telekom und Telefonica O2. Konkrete Ergebnisse wurden bislang nicht erzielt.

Im Hinblick auf die Überwachung der Internettelefonie wird auf Antwort zu Frage 49 verwiesen.

49. Hat die Bundesregierung geprüft, ob die weit verbreitete Voice-over-IP-Software „Skype“ die technische Möglichkeit bietet, Gespräche auf Anforderung von Sicherheitsbehörden mitzuschneiden (vgl. http://ijure.org/wp/archives/808)?

Verschiedene Stellen der Bundesregierung haben in den vergangenen Jahren mehrfach Kontakt zu der Firma Skype aufgenommen, um Näheres über die Funktionsweise und angebliche Überwachbarkeit der Skype-Kommunikation zu erfahren. Die Firma Skype hat in diesem Zusammenhang auf ihr Informationsblatt „Responding to Law Enforcement Records Requests“ verwiesen, nach dem bestimmte Bestands- und Verkehrsdaten, die bei der Nutzung von Skype entstehen, aufgrund einer Anordnung (subpoena) beauskunftet werden können. Im Weiteren führte sie aus, dass insbesondere Inhaltsdaten aufgrund technischer

Gegebenheiten der Skype-Kommunikation weder für die Skype-to-Skype noch für die Skype-In/Out-Kommunikation zur Verfügung gestellt werden können.

Im Übrigen hat die Bundesregierung auch keine Kenntnis, dass in anderen Staaten eine Überwachung von Skype über den in dem o. g. Informationsblatt genannten Umfang hinaus möglich ist.

50. Ist die Bundesregierung der Auffassung, dass es sich bei § 100a StPO um eine verfassungsgemäße Rechtsgrundlage für die Quellen-TKÜ handelt?

Wie begründet die Bundesregierung ihre Position?

Bei einer Quellen-TKÜ besteht für den Betroffenen – anders als bei der herkömmlichen Telekommunikationsüberwachung – das Risiko, dass über die Inhalte und Umstände der Telekommunikation hinaus weitere, insbesondere auch persönlichkeitsrelevante Informationen erhoben werden. Den Vorgaben des Bundesverfassungsgerichts in seiner Entscheidung zur Onlinedurchsuchung entsprechend, muss daher durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt werden, dass sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt.

Die Frage nach Inhalt und Umfang gesetzlicher Regelungen ist Gegenstand einer intensiven, noch nicht abgeschlossenen Prüfung durch die Bundesregierung, in die die Erkenntnisse aus der noch laufenden Entwicklung der für die Durchführung einer Quellen-TKÜ erforderlichen Software ebenso einfließen werden wie – etwa im Rahmen einer Anhörung im Unterausschuss Neue Medien am 27. November 2011 geäußerte – sachverständige Hinweise.

51. Wenn die Bundesregierung § 100a StPO als verfassungsgemäße Rechtsgrundlage für die Quellen-TKÜ betrachtet, warum duldet die Bundesministerin der Justiz, dass der Generalbundesanwalt beim Bundesgerichtshof die Ermittlungsmaßnahme zur Aufklärung schwerer Straftaten unterlässt?

Auf die Antwort zu Frage 50 wird verwiesen.

52. Falls die Bundesregierung eine neue Rechtsgrundlage in der StPO nicht für erforderlich hält, warum wurde das Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG) um eine spezifische Ermächtigungsgrundlage für die Quellen-TKÜ ergänzt (§ 20l Absatz 2 BKAG), obwohl das Gesetz bereits eine Parallelnorm zu § 100a StPO für klassische Telekommunikationsüberwachung enthielt und auch heute noch enthält (vgl. § 20l Absatz 1 BKAG)?

Auf die Antwort zu Frage 50 wird verwiesen.

53. Teilt die Bundesregierung die Einschätzung des Bayerischen Landesbeauftragten für den Datenschutz, dem zufolge die Maßnahmen zum Abhören der Internettelefonie in einem „tiefdunklen Graubereich“ erfolgt sind sowie dessen Forderung nach entsprechenden „Trojaner-Gesetzen“ für Bund und Länder, um den Einsatz der Überwachungssoftware für die Quellen-TKÜ zu regeln?

Die Einschätzung des bayerischen Datenschutzbeauftragten beschränkt sich auf die Einsätze von Quellen-TKÜ in der Verantwortung des Freistaats Bayern. Ob die Prüfergebnisse des bayerischen Datenschutzbeauftragten auf die zur Quel-

len-TKÜ berechtigten Stellen des Bundes übertragbar sind, lässt sich aus seinem Prüfbericht nicht folgern. Insofern sieht sich die Bundesregierung nicht in der Lage, die Einschätzung des bayerischen Datenschutzbeauftragten zu bewerten.

Im Übrigen wird auf die Antwort zu Frage 50 verwiesen.

54. Teilt die Bundesregierung die Auffassung, dass eine verfassungsgemäße Rechtsgrundlage für die Quellen-TKÜ sowohl deren hohe Eingriffsintensität als auch die technischen Besonderheiten berücksichtigen sowie die Modalitäten des Aufspielens der Software und Benachrichtigungspflichten regeln muss?

Auf die Antwort zu Frage 50 wird verwiesen.

55. Wie will die Bundesregierung die verfassungsgerichtliche Forderung gewährleisten, dass sich die Überwachung im Rahmen einer Quellen-TKÜ ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang erstrecken darf?

Auf die Antwort zu Frage 41 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