Deutscher Bundestag **Drucksache 17/11087**

17. Wahlperiode 17. 10. 2012

Kleine Anfrage

der Abgeordneten Burkhard Lischka, Michael Hartmann (Wackernheim), Brigitte Zypries, Petra Ernstberger, Iris Gleicke, Lars Klingbeil, Ute Kumpf, Christine Lambrecht, Thomas Oppermann, Gerold Reichenbach, Dr. Frank-Walter Steinmeier und der Fraktion der SPD

Einsatz der Quellen-Telekommunikationsüberwachung

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.

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.

Wir fragen die Bundesregierung:

1. Wird die Quellen-TKÜ derzeit im Bereich des Bundes durchgeführt, und wenn ja, durch welche Bundesbehörden, und in welchem Umfang?
2. Wird nach Kenntnis der Bundesregierung die Quellen-TKÜ derzeit von Landesbehörden durchgeführt, und wenn ja, durch welche Landesbehörden, und in welchem Umfang?
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?
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)?
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?
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?
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?
8. Gab oder gibt es Überlegungen, das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit der Entwicklung einer Quellen-TKÜ-Software zu betrauen?
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?
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?
11. Wurde auch eine Software der Firma ERA IT Solutions AG genutzt, und wenn ja, von wem, und in welchem Umfang?
12. Hat die Firma ERA IT Solutions AG den Quellcode offengelegt?
13. Wurde die Software der Firma ERA IT Solutions AG überprüft, und wenn ja, mit welchem Ergebnis?
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?

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

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

    c) Hat das BMJ dieses Vorgehen gebilligt?

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

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

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

18. Wie bewertet die Bundesregierung das Ergebnis des Gutachtens?

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

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?

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?

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?

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?

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?

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

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

    Gab es weitere Bewerber, und wenn ja, welche?

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?

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?

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

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?

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

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

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?

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

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

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

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?

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?

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

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

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

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

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

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

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

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)?

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?

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?

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)?

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?

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?

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?

Berlin, den 17. Oktober 2012

Dr. Frank-Walter Steinmeier und Fraktion

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