Große Anfrage

Fraktion DIE LINKE Hannover, den 19.10.2011

Quellen-Telekommunikationsüberwachung und Onlinedurchsuchungen - Wie steht es mit dem Einsatz von Staats-Trojanern in Niedersachsen?

Der Chaos Computer Club (CCC) hat am 8. Oktober 2011 ein Papier veröffentlicht, in dem er Software analysiert, die sich auf Festplatten von Rechnern aus mehreren Bundesländern befand. In seiner Analyse führt der CCC aus, dass die offensichtlich staatlicherseits aufgespielte und genutzte Software eine sogenannte Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) ermöglicht, aber auch weit darüber hinaus genutzt werden kann und außerdem erhebliche Sicherheitsmängel aufweist. Insbesondere sei es möglich, jederzeit über eine Onlineverbindung Programmcode nachzuladen und damit weitere Funktionen, z. B. zur Raumüberwachung über die Webcam des Computers oder zur Aufzeichnung von Tastaturanschlägen oder Bildschirminhalten, zu aktivieren.

Mit seinem Urteil vom 27. Februar 2008 zu Onlinedurchsuchungen hat das Bundesverfassungsgericht das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme aus dem allgemeinen Persönlichkeitsrecht abgeleitet, das sich aus Artikel 2 Abs. 1 GG in Verbindung mit Artikel 1 Abs.1 GG ergibt.

Das Bundesverfassungsgericht beschreibt in seinem Urteil die weite Verbreitung informationstechnischer Systeme im Alltag und die deutlich gestiegene Bedeutung dieser Systeme für die Persönlichkeitsentfaltung. Es beschreibt auch die Vielzahl der Nutzungsmöglichkeiten durch die Anwender und dass neben neuen Möglichkeiten der Persönlichkeitsentfaltung auch neue Persönlichkeitsgefährdungen bestehen. Es legt dar, dass sich aus diesen Möglichkeiten und Gefahren ein erhebliches grundrechtliches Schutzbedürfnis ergibt, dem die bisherigen grundrechtlichen Bestimmungen wie auch die bis dahin in der Rechtsprechung des Bundesverfassungsgerichts entwickelten Ausprägungen nicht hinreichend Rechnung trugen.

Das Bundesverfassungsgericht erläutert in seinem Urteil, dass mit der Infiltration eines informationstechnischen Systems zum Zweck der Telekommunikationsüberwachung die entscheidende Hürde genommen ist, um das System insgesamt auszuspähen. Es zeigt auch die dadurch bedingte Gefährdung auf, dass Daten zur Kenntnis genommen werden können, die keinen Bezug zur telekommunikativen Nutzung des Systems haben, und erwähnt als Beispiele solcher nicht kommunikationsbezogenen Daten die Inhalte angelegter Dateien, die Aufrufhäufigkeit bestimmter Dienste bis hin zu Daten, die Rückschlüsse auf das Verhalten in der eigenen Wohnung zulassen. Als Schlussfolgerung führt das Bundesverfassungsgericht u. a. in seiner Pressemitteilung zum Urteil aus: „Angesichts der Schwere des Eingriffs ist die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen.“ Das Bundesverfassungsgericht hat also bereits im Februar 2008 einen sehr engen Rahmen für Onlinedurchsuchungen gesteckt und insbesondere auch die Abgrenzung zwischen Quellen-TKÜ und Onlinedurchsuchung vorgenommen. Es hat ausgeführt, dass für die Durchführung von Quellen-TKÜ-Maßnahmen durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt werden müsse, dass sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt, damit in den Kernbereich der privaten Lebensführung nicht unzulässig eingegriffen wird.

Nach Aussagen des niedersächsischen Innenministers wurde in Niedersachsen bisher zweimal Trojaner-Software zur Quellen-TKÜ eingesetzt.

Wir fragen die Landesregierung:

I. Einsatz von Trojaner-Software

1. Von welchen Behörden und Dienststellen des Landes Niedersachsen und von welchen von ihnen beauftragten Unternehmen wurde bisher Trojaner-Software eingesetzt?
2. In wie vielen Fällen und für welche Zeiträume erfolgte jeweils der Einsatz?
3. Welche Art der Kommunikation wurde jeweils überwacht?
4. Wurden bzw. werden bei den bisherigen Einsätzen von Trojaner-Software durch Behörden oder Dienststellen des Landes Niedersachsen oder von ihnen beauftragte Unternehmen jeweils nur Kommunikationsinhalte ermittelt oder auch weitere Daten (z. B. Bildschirminhalte, Tastenanschläge, Web-Cam- oder Mikrofonaufnahmen, gespeicherte Dateien, gegebenenfalls andere Daten)?
5. Auf welcher Rechtsgrundlage erfolgten die jeweiligen Einsätze von Trojaner-Software?
6. Auf welchem Wege wurde die Software jeweils auf die zu überwachenden Computer gespielt?
7. Da bereits mit dem Aufspielen von Trojanersoftware zwangsläufig die Veränderung von Festplatteninhalten und Funktionsweise des betreffenden Systems verbunden ist und diese Maßnahme also über einen nur beobachtenden, lesenden Zugriff hinausgeht: Auf welcher Rechtsgrundlage erfolgten diese Veränderungen von Festplatteninhalten und Funktionsweisen von Computersystemen jeweils?
8. Von welchen Behörden und Dienststellen des Landes Niedersachsen und von welchen von ihnen beauftragten Unternehmen wurde bisher erfolglos der Versuch unternommen, Trojaner-Software einzusetzen?
9. In wie vielen Fällen und wann erfolgten solche nicht erfolgreichen Versuche?
10. Welche Art der Kommunikation sollte bei diesen erfolglosen Versuchen überwacht werden?
11. War bei diesen erfolglosen Versuchen über das Abgreifen von Telekommunikationsinhalten hinaus das Abgreifen weiterer Daten geplant, wenn ja, welcher Art von Daten?
12. Auf welcher Rechtsgrundlage erfolgten die erfolglosen Versuche dieser Trojaner-Einsätze?
13. Auf welchem Wege wurde bei diesen erfolglosen Versuchen versucht, die Software auf die Computer zu spielen?
14. Da bereits mit dem Aufspielen von Trojaner-Software zwangsläufig die Veränderung von Festplatteninhalten und Funktionsweise des betreffenden Systems verbunden ist und diese Maßnahme also über einen nur beobachtenden, lesenden Zugriff hinausgeht: Auf welcher Rechtsgrundlage wurden diese Veränderungen von Festplatteninhalten und Funktionsweisen von Computersystemen jeweils versucht?
15. Welche vermuteten Straftaten bzw. welche Gefahren waren jeweils die konkreten Anlässe für die Durchführung oder den Versuch des Einsatzes von Trojaner-Software?
16. a) Wurden an Behörden oder Dienststellen des Landes Niedersachsen Rechtshilfegesuche anderer Staaten, beispielsweise der Niederlande, gestellt, nach denen Rechner außerhalb Deutschlands mit Trojaner-Software überwacht werden sollten?

    b) Wenn ja, wurde diesen Rechtshilfegesuchen jeweils entsprochen, oder wurden sie abgelehnt?
17. Hat es umgekehrt Rechtshilfegesuche aus Niedersachsen an Behörden oder Dienststellen anderer Staaten gegeben mit dem Ziel, Rechner in Niedersachsen zwecks Quellen-TKÜ oder Onlinedurchsuchungen zu infiltrieren?

18. Wurden an Behörden oder Dienststellen des Landes Niedersachsen Rechtshilfegesuche anderer Bundesländer gestellt, nach denen Rechner außerhalb Niedersachsens mit Trojaner-Software überwacht werden sollten? Wenn ja, wurde diesen Rechtshilfegesuchen jeweils entsprochen, oder wurden sie abgelehnt?

19. Hat es umgekehrt Rechtshilfegesuche aus Niedersachsen an Behörden oder Dienststellen anderer Bundesländer oder an Behörden oder Dienststellen des Bundes gegeben mit dem Ziel, Rechner in Niedersachsen zwecks Quellen-TKÜ oder Onlinedurchsuchungen zu infiltrieren?

II. Erwerb, Anmietung und Eigenentwicklung von Trojaner-Software

20. Wann und von welchen Firmen wurde von Behörden oder Dienststellen des Landes Niedersachsen Trojaner-Software erworben?

21. a) Gab es vor der Entscheidung für Kauf oder Anmietung von Trojaner-Software durch Behörden oder Dienststellen des Landes Niedersachsen eine Ausschreibung?

    b) Wenn ja, mit welchem konkreten Inhalt, und war die Ausschreibung öffentlich?

22. Wie hoch sind bzw. waren jeweils die Beträge für Kauf oder Miete der Software, mit dem Einsatz verbundene Dienstleistungen der Lieferanten und die Bereitstellung der Infrastruktur für die Einsätze?

23. Da Software der Firma DigiTask eingesetzt wurde: Wie bewertet die Landesregierung die Seriosität des Unternehmens DigiTask vor dem Hintergrund der Tatsache, dass laut einem Onlineartikel der *Wirtschaftswoche* vom 23. Juni 2008 das mit DigiTask verbundene Unternehmen Reuter Electronic im Jahr 2002 rechtskräftig wegen Bestechung und Vorteilsgewährung verurteilt wurde, nachdem Reuter erhebliche Summen an das Kölner Zollkriminalamt gezahlt hatte und dieses im Gegenzug bevorzugt DigiTask-Geräte erwarb?

24. Wie bewertet die Landesregierung im Hinblick auf das Vertrauen der Bürgerinnen und Bürger die Tatsache, dass Niedersachsen Trojaner-Software von einem Unternehmen bezieht, das 2009 mit dem Big Brother Award der Kategorie Wirtschaft ausgezeichnet wurde, der von der Bürgerrechtsorganisation Foebud an Unternehmen verliehen wird, „die in auffallender Weise den Datenschutz verletzen oder missachten“?

25. Da der Innenminister im Landtag und gegenüber Medien ausgeführt hat, dass ein Wechsel weg von der Firma DigiTask und hin zu einem anderen Lieferanten erfolgt ist bzw. entsprechende Qualitätssicherungsmaßnahmen gerade laufen:

    a) Welche Gründe haben konkret zur Abkehr vom Lieferanten DigiTask geführt?

    b) Handelt es sich bei dem neuen Lieferanten um die Firma Syborg?

    c) Wenn ja, ist der Landesregierung bekannt, dass Syborg eine Tochterfirma der Firma Verint Systems ist?

    d) Falls ja, sind der Landesregierung Skandale bekannt, in denen die Fima Verint Systems eine Rolle spielte?

    e) Falls der neue Lieferant für Trojaner-Software nicht Syborg ist, welcher ist es dann?

26. a) Hat das Land Niedersachsen Software zur Quellen-TKÜ oder für Onlinedurchsuchungen selbst entwickelt?

    b) Wenn ja, durch welche Behörden oder Dienststellen?

    c) Welche Maßnahmen sind erfolgt, um die Einhaltung rechtlicher Vorgaben und die Verfassungskonformität der entwickelten Software sicherzustellen?

III. Prüfung von Qualität und Rechtmäßigkeit eingesetzter Trojaner-Software

27. Wie wurde und wird jeweils sichergestellt, dass die für Quellen-TKÜ oder Onlinedurchsuchungen von Behörden oder Dienststellen des Landes Niedersachsen oder von ihnen beauftragter Unternehmen eingesetzte Software gesetzes- und verfassungskonform ist und insbesondere den Vorgaben des Bundesverfassungsgerichtsurteils zu Onlinedurchsuchungen vom 27. Februar 2008 genügt?

28. a) Wurde vor Einsatz von Trojaner-Software der Sourcecode von Landesmitarbeiterinnen oder Landesmitarbeitern gesichtet und hinsichtlich Recht- und Verfassungsmäßigkeit bewertet?

    b) Falls nein, warum nicht?

    c) Falls ja, mit welchem Ergebnis, und wie wurde sichergestellt, dass der gesichtete Sourcecode tatsächlich die Quelle für die Kompilierung der dann eingesetzten Software war?

29. a) Durch welche Firmen, Einrichtungen oder Behörden wurde die Software vor Einsatz jeweils überprüft?

    b) Hat es insbesondere wie in Bayern eine Überprüfung ausschließlich durch Landeskriminalämter anderer Länder gegeben?

30. Nachdem in Werbeunterlagen der Firma DigiTask (siehe http://cryptome.org/0005/michael thomas.pdf) ausdrücklich auf die Möglichkeit hingewiesen wird, dass ihre Software jederzeit online aktualisiert, also durch Nachladen von Code geändert oder erweitert werden kann:

    a) War diese Funktion bekannt?

    b) Wenn nicht, warum nicht, nachdem DigiTask damit offenbar sogar wirbt?

    c) Hat es im Rahmen der Überprüfung der Funktionsweise der Software vor ihrem Einsatz eine Bewertung dieser Aktualisierungsmöglichkeit und der damit verbundenen Risiken und möglichen Grundrechtsbeeinträchtigungen gegeben?

    d) Wenn ja, mit welchem Ergebnis?

    e) Wenn nein, warum nicht?

31. Nachdem in Werbeunterlagen der Firma DigiTask (siehe http://cryptome.org/0005/michael thomas.pdf) unter dem Punkt „What is provided by the DigiTask solution?“, Unterpunkt „Data Analysis“ ausdrücklich der Punkt „Core area of private life“, also „Kernbereich der privaten Lebensführung“ erwähnt wird:

    a) Hat die Landesregierung bzw. haben die ihr nachgeordneten, die Trojaner-Software einsetzenden Behörden oder Dienststellen hinterfragt und geprüft, inwieweit hier verfassungswidrige Eingriffe möglich sind oder der Einsatz der Software das Risiko birgt, dass diese geschehen?

    b) Wurde von der Firma DigiTask eine Zusicherung gefordert, dass verfassungswidrige Eingriffe mithilfe der Software nicht erfolgen können?

    c) Hat die Firma DigiTask eine solche Zusicherung abgegeben?

    d) Wenn nicht, warum wurde die Software dennoch eingesetzt?

32. Da der CCC in seiner Analyse der Software der Firma DigiTask ausführt „Das Sicherheitsniveau dieses Trojaners ist nicht besser, als würde er auf allen infizierten Rechnern die Passwörter auf '1234' setzen“:

    a) Sind der Landesregierung bzw. den Behörden und Dienststellen des Landes Niedersachsen, die die Software einsetzten bzw. einsetzen, die vom CCC aufgeführten Sicherheitslücken bekannt?

b) Ist die Software hinreichend gegen Eingriffe von außen geschützt oder besteht ein hohes Risiko der Manipulation der vermeintlich korrekt erhobenen Daten?

c) Macht die Software die infiltrierten Rechner anfällig für weitere Angriffe von außen, die mit der Überwachung nichts zu tun haben?

d) Bringt der Einsatz der Software das Risiko mit sich, den Rechner in seiner Funktionsfähigkeit zu beeinträchtigen, also zu beschädigen?

33. Wie bewertet die Landesregierung die sich zwangsläufig mit der Überwachung eines überwachten Kommunikationspartners ergebende inhaltliche Mitüberwachung des anderen, nicht überwachten Kommunikationspartners bei der Quellen-TKÜ?

34. Da der Geheimdienstkoordinator im Bundeskanzleramt, Günter Heiß, der Presse gegenüber ausführte, dass die Landeskriminalämter zur Telekommunikationsüberwachung „multifunktionale Rohlinge“ kaufen würden, die jedes Mal auf das Ziel und den Überwachungszweck zugeschnitten werden müssten:

a) Wer ist in Niedersachsen für diese Softwarekonfigurationstätigkeit bei Einsatz von Trojaner-Software zuständig?

b) Wer hat diese Aufgabe bei bisherigen erfolgreichen und erfolglosen Einsätzen von Trojaner-Software durchgeführt?

c) Wie wurde bzw. wird diese Tätigkeit daraufhin überwacht, dass die Einhaltung rechtlicher Vorgaben und die Verfassungsmäßigkeit gewährleistet sind?

d) Wurde der Landesdatenschutzbeauftragte jeweils eingebunden und in welcher Form und mit welchem Ergebnis?

35. Welche Funktionen kann bzw. konnte die von niedersächsischen Behörden und Dienststellen und von ihnen beauftragten Unternehmen eingesetzte Trojaner-Software über die reine Quellen-TKÜ hinaus ausführen, unabhängig davon, ob diese Funktionen tatsächlich ausgeführt werden oder wurden?

36. Da die DigiTask-Software durch Befehle (Zahlencodes plus Parameter) von außen steuerbar ist:

a) Wer hatte bzw. hat jeweils in den bisherigen Einsatzfällen die Möglichkeit, solche Steuerungsbefehle abzusetzen?

b) Welche Maßnahmen wurden ergriffen, um zu verhindern, dass Unbefugte solche Befehle an die Trojaner-Software auf dem infiltrierten System senden?

37. Wurde bei den bisherigen Einsatzfällen von DigiTask-Software die Nachladefunktion genutzt, und, wenn ja, was wurde jeweils nachgeladen?

IV. Datenschutz und Datensicherheit

38. a) Wurden bzw. werden beim Einsatz von Software zur Quellen-TKÜ durch Behörden oder Dienststellen des Landes Niedersachsen oder von ihnen beauftragte Unternehmen die ermittelten Daten an Serversysteme in den USA gesendet?

b) Wenn ja, von welchem Unternehmen werden diese Server betrieben?

39. Soweit die ermittelten Daten an Serversysteme in den USA gesendet wurden oder werden:

a) Wie bewertet die Landesregierung die Tatsachen, dass Mitarbeiterinnen und Mitarbeiter der Betreiberfirma der Server auf die Daten zugreifen könnten?

b) Wie bewertet die Landesregierung die Tatsache, dass aufgrund des sogenannten Patriot Act US-amerikanische Behörden berechtigt sind, auf Daten sämtlicher US-amerikanischen Firmen zuzugreifen und daher das laut § 4 b BDSG geforderte angemessene Datenschutzniveau bei einer Weiterleitung der Daten in die USA nicht gewährleistet ist?

40. Vor dem Hintergrund der Tatsache, dass als zu überwachende Telekommunikationsvorgänge vom niedersächsischen Innenminister wiederholt Skype-Telefonate genannt wurden:

    a) Wurde im jeweiligen Einzelfall erwogen, die entsprechenden Kommunikationsinhalte über die Firma Skype zu erhalten, um den Eingriff in das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme für die jeweils Betroffenen zu vermeiden?

    b) Wenn nicht, warum wurde dies nicht erwogen?

    c) Wenn ja, wurde dies versucht und mit welchem Ergebnis?

    d) Wenn nicht, warum nicht?

41. Vor dem Hintergrund, dass als zu überwachender Telekommunikationsvorgang vom niedersächsischen Innenminister wiederholt E-Mail genannt wurde:

    a) Wurde im jeweiligen Einzelfall erwogen, die entsprechenden Kommunikationsinhalte über die jeweiligen Serviceprovider zu erhalten, um den Eingriff in das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme für die jeweils Betroffenen zu vermeiden?

    b) Wenn nicht, warum wurde dies nicht erwogen?

    c) Wenn ja, wurde dies versucht und mit welchem jeweiligen Ergebnis?

    d) Wenn nicht, warum nicht?

42. Da der niedersächsische Innenminister in der Sendung „Phoenix-Runde“ am 13. Oktober 2011 ausführte, dass die Landesdatenschutzbeauftragten „im Vorfeld eingebunden“ würden, diese also „auf das Verfahren im Vorfeld draufschauen“ könnten:

    a) Wurde der niedersächsische Landesdatenschutzbeauftragte im Vorfeld des Einsatzes von Trojaner-Software durch Behörden und Dienststellen des Landes Niedersachsen und von ihnen beauftragte Unternehmen eingebunden?

    b) Wenn ja, in welcher Form, und zu welchem Ergebnis kam der Landesdatenschutzbeauftragte?

    c) Wenn nein, warum nicht?

43. a) Wie bewertet die Landesregierung die Tatsache, dass durch den Einsatz von Trojaner-Software ohne Wissen der jeweils überwachten Person Daten Dritten zur Kenntnis gelangen, zu deren Geheimhaltung sich die überwachte Person verpflichtet hat (z. B. PIN für Onlinebanking oder vertrauliche Geschäftsdaten)?

    b) Wie bewertet die Landesregierung die Tatsache, dass Daten im Verfügungsbereich überwachter Personen ohne ihr Wissen und Zutun weitergegeben werden, hinsichtlich möglicher Haftungs- und Regressfolgen für die überwachte Person?

44. a) Wann und in welchem Umfang werden bzw. wurden Personen, die mittels Trojaner-Software überwacht wurden, über diesen Grundrechtseingriff informiert?

    b) Wann und in welchem Umfang werden bzw. wurden Personen, bei denen Trojaner-Software zur Überwachung eingesetzt werden sollte, der Versuch aber nicht erfolgreich war, über den vorgesehenen Grundrechtseingriff informiert?

    c) Wann und in welchem Umfang wird bzw. wurde der Landesdatenschutzbeauftragte über geplante, erfolgende und erfolgte Einsätze von Trojaner-Software informiert?

V. Gerichtliche Verwertbarkeit der ermittelten Daten

45. Wie bewertet die Landesregierung die gerichtliche Verwertbarkeit der aus Quellen-TKÜ mithilfe der Software der Firma DigiTask erhaltenen Daten vor dem Hintergrund der Tatsache, dass laut Analyse des CCC bei Einsatz dieser Software ohne größere Schwierigkeiten andere Per-

sonen als die zu überwachenden Kommunikationsdaten an den datenempfangenden C+C-Server senden können, die vorgeblich von der überwachten Person stammen und von den tatsächlich von der überwachten Person stammenden Daten dann nicht mehr zu unterscheiden sind?

46. Wie bewertet die Landesregierung die gerichtliche Verwertbarkeit der Ergebnisse einer denkbaren Festplattendurchsuchung eines im Anschluss an eine Quellen-TKÜ beschlagnahmten Rechners hinsichtlich der Tatsachen,

    a) dass laut Analyse des CCC der Einsatz der DigiTask-Software das Risiko mit sich bringt, dass Daten von außen auf die Festplatte der überwachten Person gespielt werden können und der Beweis, dass die Daten vom zu überwachenden Nutzer des Rechners stammen, unmöglich werden könnte,

    b) dass bereits das Aufspielen der Trojaner-Software auf das jeweilige Computersystem ein schreibender, also die Festplatteninhalte und Funktionsweise des Systems verändernder Zugriff ist,

    c) dass Beklagte in einem Verfahren argumentieren könnten, dass offensichtlich auf die Festplatte geschrieben wurde (anders kann die Trojaner-Software ja nicht installiert werden) und daher auf der Festplatte befindliche Daten nicht von ihnen, den Beklagten, stammen müssen, sondern ebenso gut von denjenigen auf die Festplatte geschrieben worden sein könnten, die die Trojaner-Software auf die Festplatte geschrieben haben?

VI. Grundsätzliche Verfassungsmäßigkeit von Trojaner-Software

47. Wie bewertet die Landesregierung die Tatsache, dass nach Ansicht von Experten ein verfassungsgemäßer Einsatz von Trojaner-Software zur Quellen-TKÜ nicht möglich ist, weil die vom Bundesverfassungsgericht geforderte trennscharfe technische Abgrenzung zur deutlich weitergehenden Onlinedurchsuchung nicht zu erreichen ist?

Ursula Weisser-Roelle
Parlamentarische Geschäftsführerin

(Ausgegeben am 27.10.2011)