Landtag Brandenburg **Drucksache 5/4298**
5. Wahlperiode

Antwort
der Landesregierung

auf die Kleine Anfrage 1637
der Abgeordneten Ursula Nonnemacher, Sabine Niels, Marie-Luise von Halem, Michael Jungclaus und Axel Vogel
Fraktion BÜNDNIS 90/DIE GRÜNEN
Drucksache 5/4154

Einsatz von Überwachungssoftware (Trojanern) im Land Brandenburg

Wortlaut der Kleinen Anfrage 1637 vom 19.10.2011:
Der Chaos Computer Clubs (CCC) hat am 8. Oktober 2011 die Analyse einer staatlich eingesetzten Überwachungssoftware veröffentlicht. Gerade angesichts der Bedrohung der Grundrechte der Bürgerinnen und Bürger durch eine unverhältnismäßige staatliche Überwachung von Computern hat das Bundesverfassungsgericht 2008 ein Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme geschaffen. Die heimliche Infiltration informationstechnischer Systeme, z. B. durch eine Online-Durchsuchung mittels Trojaner, ist demnach nur dann zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Der nun analysierte Staatstrojaner verfügt über sehr umfangreiche, grundrechtsgefährdende Funktionen, die mit den Vorgaben, die das Bundesverfassungsgericht in seinem Urteil zur Online-Durchsuchung vorgegeben hat, kaum zu vereinbaren sind. So kann die Spionagesoftware über das Internet weitere Programme nachladen und ferngesteuert zur Ausführung bringen. Eine Erweiterbarkeit auf das Durchsuchen, Schreiben, Lesen sowie Manipulieren von Dateien scheint somit von Anfang vorgesehen worden zu sein. Selbst ein digitaler großer Lausch- und Spähangriff ist möglich, indem ferngesteuert auf das Mikrofon, die Kamera und die Tastatur des Computers zugegriffen wird, so dass z. B. regelmäßig Fotos des Bildschirms während der Nutzung erstellt werden können. Zudem gibt es Hinweise, dass sich der Kontrollserver in einem US-amerikanischen Rechenzentrum befindet; auch dies wäre unter datenschutzrechtlichen Gesichtspunkten hochproblematisch. Darüber hinaus entspricht die Software nicht den modernen datensicherheitstechnischen Anforderungen. So findet die Fremdsteuerung des infiltrierten Rechners unverschlüsselt statt. Beim Ausspionieren eines privaten Computers handelt es sich um einen massiven Eingriff in die verfassungsrechtlich geschützte Privat- und Intimsphäre der Bürgerinnen und Bürger, der nicht mit den Vorgaben des BverfG im Einklang zu bringen ist. Medienberichten zufolge bestätigten das Brandenburger Innen- und das Justizministerium, dass bereits Überwachungsprogramme im Land Brandenburg eingesetzt werden, dafür sei allerdings die Amtshilfe von Bundesbehörden nötig gewesen.

Datum des Eingangs: 18.11.2011 / Ausgegeben: 23.11.2011

Wir fragen die Landesregierung:

1. Benutzte das Land Brandenburg ein Programm, wie das vom CCC untersuchte oder ein vergleichbares Programm mit gleichen oder ähnlichen Fähigkeiten zur Quellen-Telekommunikationsüberwachung und/oder zur Online-Durchsuchung?
2. Wie ist die genaue Funktionalität des benutzten Programms ausgestaltet? In wie vielen Fällen wurde das Programm eingesetzt, mit je welchen Funktionalitäten, auf je welcher Rechtsgrundlage (präventiv oder repressiv), wer zeichnete für die Beschaffung der Software, für dessen Konfiguration zu Einsatzzwecken, für die Anordnung des jeweiligen Einsatzes bzw. den dahingehenden Antrag, für etwaige Amtshilfe-Ersuchen an andere Behörden (zwecks Beschaffung und/oder Installation des fraglichen Programms auf verdächtigen Rechnern) und für die Art und Weise der jeweiligen Einsatz-Durchführung verantwortlich? (bitte Antworten tabellarisch auflisten)
3. Auf welchen Rechtsgrundlagen beruhte und beruht der Einsatz derartiger Software im Land Brandenburg?
a) Wie und von wem wurde und wird solche Software auf Grundrechtskonformität überprüft?
b) Welche Vorgaben existieren zum Einsatz der fraglichen Software? Unter welchen Voraussetzungen darf der Einsatz ggf. auch zur Strafverfolgung erfolgen? Unter welchen Voraussetzungen darf der Einsatz zur Gefahrenabwehr erfolgen? Welche Maßnahmen sowie welche Konfiguration der Software je zu Überwachung und Aufzeichnung des Telekommunikationsverkehrs im repressiven und ggf. im präventiven Bereich sind von den Ermächtigungsgrundlagen umfasst und welche gehen darüber hinaus?
4. Wer hat jeweils bei den einzelnen Einsätzen die Überwachungssoftware auf die Computer der Betroffenen aufgespielt und wie geschah dies jeweils? (bitte mit genauer Beschreibung der je vorgenommenen Eingriffe)
5. Welche Behörde hat Entwicklung, Kauf oder Lizenzierung der Software in Auftrag gegeben?
a) Welche Kosten sind durch die Entwicklung der Software bzw. durch deren Ankauf entstanden? Welche Kosten entstanden beim Einsatz der Software? Von wem werden die vorgenannten Kosten getragen?
b) Ist die Anschaffung einer vergleichbaren Software geplant, welche Fähigkeiten sind vorgesehen, für welche Behörden soll die Software bei welchen Lieferanten beschafft werden?
6. Haben Bundesbehörden bei der Beschaffung der Software (ggf. nur für einzelne Einsätze) Amtshilfe geleistet? Wenn ja, welche Bundesbehörden und im welchen Umfang?
7. Haben Behörden anderer Bundesländer bei der Beschaffung der Software (ggf. nur für einzelne Einsätze) Amtshilfe geleistet? Wenn ja, wie sah diese konkret aus?
8. Waren bei der Erhebung, Verarbeitung oder Nutzung der erhobenen Daten private Firmen beteiligt? Wenn ja, welche und in welcher Form?
9. Auf welchem Weg gelangen die Daten ausgespähter Personen an die Behörden? Wo stehen die Server, die zur Kontrolle des Trojaners verwendet werden? Wo stehen die Server, auf die die Daten übertragen werden? Wer hat alles Zugriff auf die Server? Kann der Zugriff Dritter ausgeschlossen werden und in welcher Form erfolgt die Archivierung der Daten? Wie ist sichergestellt, dass keine unbefugten Dritten Zugriff auf diese Daten bekommen können?
10. In welcher Form und wie lange werden die ermittelten Daten sowie deren Auswertung gespeichert? Findet ein Austausch der erlangten Daten auch mit anderen Landes- oder Bundesbehörden statt?
11. Wie wird im Rahmen der Maßnahme der Schutz Dritter gewährleistet und verhindert, dass Daten von Personen, die in Kontakt mit der Zielperson stehen, eventuell mit erfasst werden?

12. Wie wird sichergestellt, dass es sich bei dem überwachten Rechner um den Rechner der Zielperson handelt, beziehungsweise er allein von dieser Person benutzt wurde und die gewonnen Erkenntnisse zweifelsfrei und eindeutig diesem Benutzer zugeordnet werden können?
13. Ist der Landesregierung bekannt, dass die vom CCC untersuchten Programme massive Sicherheitslücken, v. a. was die Verschlüsselung angeht, aufweisen und welche Maßnahmen hat die Landesregierung unternommen, die Manipulation durch Dritte zu erschweren bzw. auszuschließen?
14. Wurden, sofern ein vergleichbares Programm bisher zum Einsatz kam, die von der Überwachung betroffenen Personen nach der Maßnahme über den Vorgang informiert? Wenn ja, wie sah diese Information aus? Wenn nein, warum nicht?
15. Kann nach Ansicht der Landesregierung ausgeschlossen werden, dass Daten des nach der Rechtsprechung absolut geschützten Kernbereiches privater Lebensgestaltung (BVerfG, Urteil vom 3. März 2004, AZ 1 BvR 2378/98 und 1084/99) durch die Maßnahmen erfasst wurden?
16. Wie bewertet die Landesregierung, dass die auf diesem Wege erlangten Daten in Gerichtsverfahren nicht verwertet werden können sowie dass die Daten, die mit Hilfe der vom CCC untersuchten Software, manipuliert werden können?

Namens der Landesregierung beantwortet der Minister des Innern die Kleine Anfrage wie folgt:

Frage 1: Benutzte das Land Brandenburg ein Programm, wie das vom CCC untersuchte oder ein vergleichbares Programm mit gleichen oder ähnlichen Fähigkeiten zur Quellen-Telekommunikationsüberwachung und/oder zur Online-Durchsuchung?

zu Frage 1: Im Land Brandenburg wurde in bisher einem Fall zur Durchführung einer Quellen-TKÜ durch eine Bundessicherheitsbehörde (ZKA) ein vergleichbares Programm genutzt. Aus technischen Gründen hat jedoch eine Überwachung nicht stattgefunden. Zudem wurde in einem weiteren Verfahren, in dem das Zollfahndungsamt die Ermittlungen durchgeführt hat, aufgrund eines richterlichen Beschlusses eine Quellen-TKÜ-Maßnahme angeordnet und auch durchgeführt.

Frage 2: Wie ist die genaue Funktionalität des benutzten Programms ausgestaltet? In wie vielen Fällen wurde das Programm eingesetzt, mit je welchen Funktionalitäten, auf je welcher Rechtsgrundlage (präventiv oder repressiv), wer zeichnete für die Beschaffung der Software, für dessen Konfiguration zu Einsatzzwecken, für die Anordnung des jeweiligen Einsatzes bzw. den dahingehenden Antrag, für etwaige Amtshilfe-Ersuchen an andere Behörden (zwecks Beschaffung und/oder Installation des fraglichen Programms auf verdächtigen Rechnern) und für die Art und Weise der jeweiligen Einsatz-Durchführung verantwortlich? (bitte Antworten tabellarisch auflisten)

zu Frage 2: In Brandenburg beschränkte sich der Einsatz des benannten Programms ausschließlich auf die Überwachung der via „Skype“ geführten Telekommunikation. Die dazu erforderliche Überwachungssoftware wurde nach hier vorliegenden Erkenntnissen im Auftrag des ZKA entwickelt. Einzelheiten zur dortigen Beschaffung der Software, der Funktionalität, Konfiguration und dortigen Anordnung des jeweiligen Einsatzes sind der Landesregierung nicht bekannt. In Brandenburg erfolgte der Einsatz auf Grundlage der StPO und im Zuge der Amtshilfe durch das ZKA.

Frage 3: Auf welchen Rechtsgrundlagen beruhte und beruht der Einsatz derartiger Software im Land Brandenburg?

a) Wie und von wem wurde und wird solche Software auf Grundrechtskonformität überprüft?
b) Welche Vorgaben existieren zum Einsatz der fraglichen Software? Unter welchen Voraussetzungen darf der Einsatz ggf. auch zur Strafverfolgung erfolgen? Unter welchen Voraussetzungen darf der Einsatz zur Gefahrenabwehr erfolgen? Welche Maßnahmen sowie welche Konfiguration der Software je zu Überwachung und Aufzeichnung des Telekommunikationsverkehrs im repressiven und ggf. im präventiven Bereich sind von den Ermächtigungsgrundlagen umfasst und welche gehen darüber hinaus?

zu Frage 3: In Brandenburg beruht der Einsatz auf der Grundlage eines richterlichen Beschlusses gemäß § 100a ff StPO. Im strafrechtlichen Ermittlungsverfahren sind Quellen-TKÜ auf der Rechtsgrundlage des § 100a StPO zulässig (vgl. LG Hamburg, Beschluss vom 13. Sept. 2010, 608 Qs 17/10; LG Landshut, Beschluss vom 20. Jan. 2011, 4 Qs 346/10). Leistet eine Polizeibehörde einer anderen Behörde Amtshilfe, trägt nach den Grundsätzen der Amtshilfe die ersuchende Behörde gegenüber der ersuchten Behörde die Verantwortung für die Rechtmäßigkeit der zu treffenden Maßnahme. Die ersuchte Behörde ist allerdings für die Durchführung der Amtshilfe selbst verantwortlich. Beiden Behörden, sowohl der ersuchenden als auch der ersuchten, wäre im Falle einer Quellen-TKÜ ein Einsatz von Software untersagt, der sich nicht nur auf Inhalte und Umstände der laufenden Telekommunikation beschränkt, sondern auf weitere Bereiche des informationstechnischen Systems Zugriff nimmt.

Frage 4: Wer hat jeweils bei den einzelnen Einsätzen die Überwachungssoftware auf die Computer der Betroffenen aufgespielt und wie geschah dies jeweils? (bitte mit genauer Beschreibung der je vorgenommenen Eingriffe)

zu Frage 4: Die Überwachungssoftware wurde im Rahmen der Amtshilfe durch das ZKA eingebracht. Eine Beschreibung des Vorgehens kann daher nur von dort erfolgen.

Frage 5: Welche Behörde hat Entwicklung, Kauf oder Lizenzierung der Software in Auftrag gegeben?
a) Welche Kosten sind durch die Entwicklung der Software bzw. durch deren Ankauf entstanden? Welche Kosten entstanden beim Einsatz der Software? Von wem werden die vorgenannten Kosten getragen?
b) Ist die Anschaffung einer vergleichbaren Software geplant, welche Fähigkeiten sind vorgesehen, für welche Behörden soll die Software bei welchen Lieferanten beschafft werden?

zu Frage 5: Diese Fragen können von hier nicht beantwortet werden, da Entwicklung, Kauf oder Lizenzierung nach den hier vorliegenden Erkenntnissen in Bundeszuständigkeit erfolgten (siehe auch zu Frage 2). In Brandenburg ist gegenwärtig keine Beschaffung einer vergleichbaren Software geplant. Die Kosten für derartige Überwachungsmaßnahmen im Ermittlungsverfahren trägt die sachleitende Staatanwaltschaft. Eine genaue Bezifferung der Kosten kann erst nach Abschluss des staatsanwaltschaftlichen Ermittlungsverfahrens erfolgen.

Frage 6: Haben Bundesbehörden bei der Beschaffung der Software (ggf. nur für einzelne Einsätze) Amtshilfe geleistet? Wenn ja, welche Bundesbehörden und im welchen Umfang?

Frage 7: Haben Behörden anderer Bundesländer bei der Beschaffung der Software (ggf. nur für einzelne Einsätze) Amtshilfe geleistet? Wenn ja, wie sah diese konkret aus?

zu Fragen 6 und 7: Nein. Es erfolgte keine Amtshilfe zur Beschaffung bzw. zum Erwerb einer Software.

Frage 8: Waren bei der Erhebung, Verarbeitung oder Nutzung der erhobenen Daten private Firmen beteiligt? Wenn ja, welche und in welcher Form?

zu Frage 8: Dazu liegen der Landesregierung keine Erkenntnisse vor.

Frage 9: Auf welchem Weg gelangen die Daten ausgespähter Personen an die Behörden? Wo stehen die Server, die zur Kontrolle des Trojaners verwendet werden? Wo stehen die Server, auf die die Daten übertragen werden? Wer hat alles Zugriff auf die Server? Kann der Zugriff Dritter ausgeschlossen werden und in welcher Form erfolgt die Archivierung der Daten? Wie ist sichergestellt, dass keine unbefugten Dritten Zugriff auf diese Daten bekommen können?

Frage 10: In welcher Form und wie lange werden die ermittelten Daten sowie deren Auswertung gespeichert? Findet ein Austausch der erlangten Daten auch mit anderen Landes- oder Bundesbehörden statt?

Frage 11: Wie wird im Rahmen der Maßnahme der Schutz Dritter gewährleistet und verhindert, dass Daten von Personen, die in Kontakt mit der Zielperson stehen, eventuell mit erfasst werden?

zu Fragen 9 bis 11: Da die im Brandenburg durchgeführte Maßnahme im Zuge der Amtshilfe durchgeführt wurde, liegen der Landesregierung keine Informationen zur Beantwortung der im Sinne der Fragestellungen formulierten Aspekte der Erhebung, Verarbeitung und Nutzung der Daten vor.

Frage 12: Wie wird sichergestellt, dass es sich bei dem überwachten Rechner um den Rechner der Zielperson handelt, beziehungsweise er allein von dieser Person benutzt wurde und die gewonnen Erkenntnisse zweifelsfrei und eindeutig diesem Benutzer zugeordnet werden können?

zu Frage 12: In den beiden beschriebenen Fällen wurden auf Grundlage der richterlichen Beschlüsse lediglich die Rechner der Betroffenen überwacht. Die Auswertung, d.h. das Auslesen der Daten einschließlich des Hörbarmachens der ausgeleiteten Audiodateien erfolgte durch Ermittlungsbeamte des Zollfahndungsamtes. Probleme bei der Zuordnung wurden nicht berichtet.

Frage 13: Ist der Landesregierung bekannt, dass die vom CCC untersuchten Programme massive Sicherheitslücken, v. a. was die Verschlüsselung angeht, aufweisen und welche Maßnahmen hat die Landesregierung unternommen, die Manipulation durch Dritte zu erschweren bzw. auszuschließen?

zu Frage 13: Der Landesregierung sind diesbezügliche Presseberichte bekannt. Abschließende Bewertungen können dazu hier jedoch nicht getroffen werden. Das Innenressort beteiligt sich aber an der beabsichtigten Prüfung des zukünftigen Umgangs mit Quellen - TKÜ im Rahmen der Konferenz der Innenminister und -senatoren der Länder.

Frage 14: Wurden, sofern ein vergleichbares Programm bisher zum Einsatz kam, die von der Überwachung betroffenen Personen nach der Maßnahme über den Vorgang informiert? Wenn ja, wie sah diese Information aus? Wenn nein, warum nicht?

zu Frage 14: Nein. Das Gesetz sieht vor, dass die Telekommunikation auch ohne Wissen der Betroffenen überwacht und aufgezeichnet werden darf. Es ist des Weiteren vorgesehen, dass eine Benachrichtigung erfolgt, sobald dies ohne Gefährdung des Untersuchungszwecks, des Lebens, der körperlichen Unversehrtheit und der persönlichen Freiheit einer Person oder von bedeutenden Vermögenswerten möglich ist. Vorliegend ist das unter Sachleitung der Staatsanwaltschaft Frankfurt (Oder) durchzuführende strafrechtliche Ermittlungsverfahren noch nicht abgeschlossen.

Frage 15: Kann nach Ansicht der Landesregierung ausgeschlossen werden, dass Daten des nach der Rechtsprechung absolut geschützten Kernbereiches privater Lebensgestaltung (BVerfG, Urteil vom 3. März 2004, AZ 1 BvR 2378/98 und 1084/99) durch die Maßnahmen erfasst wurden?

zu Frage 15: Dazu liegen der Landesregierung keine Erkenntnisse vor.

Frage 16: Wie bewertet die Landesregierung, dass die auf diesem Wege erlangten Daten in Gerichtsverfahren nicht verwertet werden können sowie dass die Daten, die mit Hilfe der vom CCC untersuchten Software, manipuliert werden können?

zu Frage 16: Die Landesregierung hat keine Erkenntnisse, dass auf diesem Wege erlangte Daten in gerichtlichen Verfahren eingeführt werden sollen.