Presseinformation

Landtagsfraktion Schleswig-Holstein

Stellv. Pressesprecher
Dr. Jörg Nickel

Landeshaus
Düsternbrooker Weg 70
24105 Kiel

Telefon: 0431 / 988 - 1503
Fax: 0431 / 988 - 1501
Mobil: 0178/28 49 591

presse@gruene.ltsh.de
www.sh.gruene-fraktion.de

Nr. 565.10 / 12.10.2011

Grüne fordern Moratorium des Einsatzes von Ausspäh-Trojanern in Schleswig-Holstein und legen Fragenkatalog vor

Die Fraktion Bündnis 90/Die Grünen hat heute einen umfangreichen Fragenkatalog für die kommende Sitzung des Innen- und Rechtsausschusses vorgelegt, in der der Innenminister zum Einsatz von Ausspähsoftware in Schleswig-Holstein Stellung nehmen soll. Dazu erklärt der innen- und rechtspolitische Sprecher der Fraktion, **Thorsten Fürter**:

Schleswig-Holstein sollte den Einsatz von Ausspähsoftware zunächst einmal aussetzen. Während des Moratoriums können die offenen Fragen geklärt werden. Wenn die Bedenken gegen den Einsatz nicht ohne Wenn und Aber ausgeräumt werden können, dürfen Trojaner in Schleswig-Holstein nicht verwendet werden. Wir lehnen es ab, das heimliche Ausspähen von Computern und des Telekommunikationsverkehrs immer weiter auszudehnen. Es muss eine verfassungsrechtlich geschützte Privat- und Intimsphäre bleiben. Solange das nicht einwandfrei gesichert werden kann: Hände weg von staatlichen Ausspähprogrammen!

Vorbereitende Fragen an das Innenministerium für die kommende Sitzung des Innen- und Rechtsausschusses:

1. Verfügt auch Schleswig-Holstein über ein Programm, wie das vom Chaos Computer Club untersuchte oder eine modifizierte Version mit gleichen oder ähnlichen Fähigkeiten oder ein vergleichbares Programm mit gleichen oder ähnlichen Fähigkeiten zur Quellen-Telekommunikationsüberwachung und/oder zur Online-Durchsuchung inklusive der Möglichkeit en, die über eine Quellen-TKÜ hinausgehen (z.B. das regelmäßige Anfertigen von Bildschirmfotos, die Aktivierung von Mikrofon oder Webcam)?

2. Wurde oder wird ein Programm wie vorstehend spezifiziert in Schleswig-Holstein eingesetzt? Wenn ja, wie ist die genaue Funktionalität des Programms ausgestaltet, in wie vielen Fällen wurde das Programm eingesetzt, mit je welchen Funktionen, auf je welcher Rechtsgrundlage (präventiv oder repressiv), wer zeichnete für die Beschaffung des Software-Programms, 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? Wenn nein, ist die Anschaffung einer vergleichbaren Software geplant, welche Fähigkeiten sind vorgesehen, für welche Behörden soll die Software bei welchen Lieferanten beschafft werden?

3. Welche Kosten sind durch die Entwicklung der Software bzw. durch deren Ankauf entstanden? Welche Kosten entstanden beim Einsatz der Software? Welche durchschnittlichen Kosten entstehen pro Einsatz? Von wem werden die vorgenannten Kosten je getragen?

4. Wie und von wem wurde und wird solche Software auf Gesetzeskonformität überprüft?

5. Welche ministeriellen bzw. behördlichen Vorgaben existieren zum Einsatz der fraglichen Software, hinsichtlich der Fragen unter welchen Voraussetzungen der Einsatz ggf. auch zwecks Strafverfolgung erfolgen darf, unter welchen Voraussetzungen dies zwecks Gefahrenabwehr erfolgen darf, welche Maßnahmen sowie welche Konfiguration der Software je zur Überwachung und Aufzeichnung des Telekommunikationsverkehrs im repressiven und ggf. im präventiven Bereich von den Ermächtigungsgrundlagen umfasst sind und welche darüber hinausgehen?

6. Wer hat jeweils bei den einzelnen Einsätzen die Überwachungssoftware auf die Computer der Betroffenen aufgespielt und wie geschah dies jeweils?

7. Welche Gerichte haben jeweils aufgrund welcher Rechtsgrundlagen und (sofern repressiv) des Verdachts welcher Straftaten die Maßnahmen angeordnet, welcher Sachverhalt lag den Einsätzen bzw. den geführten Ermittlungsverfahren jeweils zugrunde und wie ist der Stand dieser Ermittlungsverfahren bzw. Gefahren-Annahmen heute?

8. In welchen Einsatzfällen legten Betroffene Rechtsmittel gegen die Maßnahme ein und mit jeweils welchem Ergebnis?

9. Ist der Landesregierung bekannt, ob andere Landes- oder Bundesbehörden in der Bundesrepublik auf vergleichbare Maßnahmen zurückgreifen? Wenn ja, welche und in welchen Fällen?

10. Welche Funktionen, die über eine Quellen-TKÜ hinausgehen (z.B. das regelmäßige Anfertigen von Bildschirmfotos, die Aktivierung von Mikrofon oder Webcam) sind mit welchen richterlichen Beschlüssen zum Einsatz gekommen? Wurde dabei das Urteil des Landgerichts Landshut (Beschl. v. 20.1.2011 - AZ: 4 Qs 346/10) berücksichtigt, mit dem die Erstellung von Bildschirmfotos in einem Fall für rechtswidrig erklärt wurde?

11. Wurde die Software, die die verdeckte Ermittlungsmaßnahme ermöglicht, durch die Behörden von Schleswig-Holstein entwickelt oder erfolgte dies durch eine private Firma? Wenn letzteres, durch welche?

12. Welche Behörde hat Entwicklung, Kauf oder Lizenzierung der Software in Auftrag gegeben?

13. Haben Bundesbehörden bei der Beschaffung der Software (ggf. nur für einzelne Einsätze) Amtshilfe geleistet? Wenn ja, welche Bundesbehörden und wie genau?

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

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

16. Welche externen Anbieter wurden in die Planung oder Konzeptionierung oder Durchführung einbezogen? Sind hierfür Ausschreibungen erfolgt und wenn ja, mit welchen Anforderungen und welchen Serviceverträgen?

17. Welche Klauseln waren in den Verträgen mit externen Anbietern enthalten und wie wurde damit sichergestellt, dass der Rechtsprechung des Bundesverfassungsgerichtes zur Vertraulichkeit und Integrität informationstechnischer Systeme Rechnung getragen wurde und die Software oder Elemente hiervon nicht von externen Anbietern an private Dritte weitergegeben wird?

18. Auf welche Weise wird sichergestellt, dass das bei der externen Herstellung entstandene Wissen der jeweiligen Mitarbeiter und Abteilungen nicht innerhalb des Unternehmens für anderweitige Zwecke verwendet wird?

19. Wurde ein Sicherheitsaudit der Software durchgeführt? Wenn ja, durch wen wurde diese Auditierung durchgeführt?

20. War der Landesdatenschutzbeauftragte an der Auditierung beteiligt? Wenn nein, warum nicht?

21. 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?

22. 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?

23. 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?

24. 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?

25. Ist der Landesregierung bekannt, dass die vom Chaos Computer Club untersuchten Programme massive Sicherheitslücken, v.a. was die Verschlüsselung angeht, aufweisen und welche Maßnahmen hat die Landesregierung unternommen, die Manipulation an den verwendeten Programmen durch Dritte zu erschweren bzw. auszuschließen?

26. Für welche Betriebssysteme wurde die Software entwickelt und ist der Landesregierung bewusst, dass die vom Chaos Computer Club untersuchten Programme lediglich auf Windows-Betriebssysteme ausgerichtet sind, d.h. sich die Nutzer anderer Betriebssysteme durch Verwendung von anderen Betriebssystemen der Überwachung von vornherein entziehen können?

27. Wurde, 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?

28. 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?

29. Ist die Landesregierung der Ansicht, dass die hohen Hürden des Bundesverfassungsgerichts technisch eingehalten werden können und welche Anstrengungen hat sie unternommen, diesen Vorgaben gerecht zu werden?

30. Wie bewertet die Landesregierung die Frage nach einer nicht gegebenen Verwertbarkeit der auf diesem Wege erlangten Daten in Gerichtsverfahren, speziell vor dem Hintergrund, dass die Daten, die mit Hilfe der vom Chaos Computer Club untersuchten Software manipuliert werden können?

***