

Sehr geehrte Damen und Herren,

wie in zahlreichen Medien berichtet, hat der Chaos Computer Club (CCC) eine Software analysiert, bei der die Experten davon ausgehen, dass es sich um einen „Staatstrojaner“ handelt. Der Vorstoß des CCC und der Verweis auf bisher nicht veröffentlichte Quellen bekräftigen diese Aussage. Dabei wurde festgestellt, dass diese Software weder elementaren Sicherheitsanforderungen genügt, noch die gesetzlichen Rahmenbedingungen einhält. Beispielsweise können Beweisdaten sowohl durch Ermittler als auch durch Außenstehende manipuliert werden. Die erhaltenen Informationen sind somit weder aussagekräftig noch rechtlich verwertbar.

Das Bundesverfassungsgericht hat festgehalten, dass die Quellen-TKÜ ausschließlich der Überwachung der Telekommunikation dienen darf. Im Gegensatz dazu fertigt die analysierte Software auch Bildschirmfotos an, die zum Ausspähen von nicht versendeten E-Mails, Tagebucheinträgen oder anderen privaten Daten missbraucht werden können. Sie erlaubt die Installation zusätzlicher externer Software und von Softwaremodulen, das Unterschieben von Beweisen, sowie die Ausführung beliebiger Programme. Damit beinhaltet sie Funktionen, die vom Bundesverfassungsgericht explizit verboten wurden. Der Einsatz einer Software in der vorliegenden Ausführung ist somit nach unserer Ansicht grundgesetzwidrig. Zur Aufklärung des Sachverhaltes stellen wir Ihnen folgende Fragen und bitten um zeitnahe Beantwortung:

1. Wurde oder wird die durch den CCC analysierte Software – oder Software mit vergleichbarer Funktionalität – auch durch das Landeskriminalamt NRW oder andere Behörden des Landes NRW genutzt?
2. In wie vielen und welchen Fällen wurde oder wird dieser „Staatstrojaner“ oder Software mit vergleichbarer Funktionalität im Land NRW bereits eingesetzt?
3. In welchen Fällen ist der Einsatz der vom CCC analysierten Software Ihrer Ansicht nach angemessen und gerechtfertigt und in welchen nicht?
4. Auf welchen Rechtsgrundlagen beruhte und beruht der Einsatz im Land NRW?
5. Wie wurde und wird solche Software auf Gesetzeskonformität überprüft?
6. Welchen Umfang an Überwachungsmaßnahmen und welche weiteren Möglichkeiten bietet die Software?
7. Welche Behörde hat Entwicklung, Kauf oder Lizenzierung der Software in Auftrag gegeben? Welche Personen in der Landesregierung waren darüber informiert? Erfolgte die Softwareentwicklung intern oder wurde damit eine externe Firma beauftragt? Wenn letzteres zutrifft, um welche Firma handelt es sich? Wurde die Verwaltung, Betreuung oder Datensammlung einer privaten Firma übertragen?
8. Für wen arbeitete die beauftragte Firma zusätzlich? Waren anderen Behörden des Landes NRW oder Behörden anderer Länder die grundsätzlichen Defizite der Software bekannt?
9. Wie wurde, im Falle einer externen Beauftragung zur Programmierung der Software, sichergestellt, dass die beauftragte Firma entsprechend zertifiziert ist, solche Aufträge zu bearbeiten? Führt die externe Firma ein Sicherheitsaudit der Software durch,

beziehungsweise wurde dieses Audit von einem unabhängigen Unternehmen oder einer anderen Institution, wie zum Beispiel dem BSI, durchgeführt? Wenn nein, wieso nicht?

10. Sind weitere Versionen der Software in Entwicklung und wenn ja, welche neuen Eigenschaften sollen diese Versionen bekommen?

11. Sind weitere Softwaremodule zur dynamischen Erweiterung des Bundestrojaners mit dem eigentlichen Bundestrojaners mitgeliefert worden, die dem Urteil des Bundesverfassungsgerichts vom 27.2.2008 widersprechen (BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. 3-4)?

12. War den beauftragenden Behörden vor dem ersten Einsatz der Software bekannt, dass der Zugriff auf die Software ohne Authentifizierung stattfinden und auch von nicht dazu autorisierten Personen beliebige, weitere Software zur Ausführung gebracht werden kann? Wurden diese Funktionen konkret beauftragt oder hat die beauftragte Firma die Software ohne expliziten Auftrag mit diesen Sicherheitslücken ausgestattet?

13. Gibt es besondere Handlungsanweisungen zur Wahrung der Rechte der ausgespähten Personen und anderer Unbeteiligter? Wenn ja, wie lauten diese?

14. Von wem wird beziehungsweise wurde die Software installiert und ausgeführt? Auf welchen Wegen gelangt sie auf das Endgerät des zu Überwachenden und in welcher Weise wird das Endgerät des zu Überwachenden manipuliert? Sind Hardwareeingriffe notwendig, um die Überwachung durchzuführen?

15. Hat es Absprachen mit Internet-Diensteanbietern gegeben, um deren Infrastruktur und/oder Hard- und Software zur mittelbaren oder unmittelbaren Infektion des Zielrechners einzusetzen? Wenn ja, welche Firmen waren hier involviert?

16. Auf welche Weise setzt sich die Software im System fest und welche Dateien sind davon betroffen?

17. Sind Hersteller von Geräten und Programmen zur Sicherheit von Computern und Netzwerken (zum Beispiel Firewalls und Antivirenprogramme) mit eingebunden, so dass die Software und die verwendeten Methoden bewusst nicht von diesen Schutzprogrammen erkannt wird? Wurde anderweitig dafür gesorgt, dass Programme zum Aufspüren von Trojanern die Software nicht erkennen konnten?

18. Inwieweit kann die eingesetzte Software gängige Anonymisierungs- und Verschlüsselungsmechanismen wie zum Beispiel TLS, AES, Onion Routing umgehen beziehungsweise manipulieren?

19. Welchem Stand der Technik entspricht die Software? Wie viel Zeit ist zwischen der Planung und Auftragsvergabe bis hin zur Auslieferung und dem ersten Einsatz der Software vergangen? Wurden die Software-Lizenzen (zum Beispiel für den Speex-Codec) konsequent eingehalten?

20. Über welchen Weg gelangen die Daten vom überwachten Endgerät zu den Ermittlungsbehörden?

21. Durch welche Netzwerke werden die Daten ausgespähter Personen geleitet? Welche Firmen, Behörden und/oder andere, dritte Personen und Institutionen haben Zugriff auf die benötigten Server, zum Beispiel auf einen Command-and-Control-Server?
22. In welchem Maße wurden beziehungsweise werden die so gewonnenen Erkenntnisse verwertet?
23. Durch welche Maßnahmen wurde und wird eine Manipulation der Ermittlungen durch Dritte erschwert? Wie wurde und wird eine Manipulation der Daten auf diesem Weg ausgeschlossen?
24. Wie wurde und wird sichergestellt, dass der Überwachte nach der Entdeckung der Software diese oder deren gesammelten Ergebnisse vor der Übersendung an die einschlägigen Server nicht manipulieren oder entfernen kann?
25. Inwieweit ist die Software selbstständig in der Lage, sich innerhalb eines Computernetzwerkes zu verbreiten, um so Zweit- oder Drittgeräte des Überwachten oder anderer auch unbeteiligter Dritter zu infiltrieren?
26. Steht die Software für unterschiedliche Betriebssystem-Plattformen zur Verfügung oder könnten sich Zielpersonen durch Verwendung von alternativen Betriebssystemen der Überwachung entziehen? Falls ja, um welche Betriebssysteme handelt es sich?
27. Wie wird sichergestellt, dass der Überwachte nach der Überwachungsaktion über den Vorgang informiert wird? Ist dies in allen bisherigen Maßnahmen erfolgt? Wenn nein, aus welchen Gründen ist dies nicht erfolgt?
28. Ist es möglich sicherzustellen, dass keine Programme oder Dateien auf das System des Überwachten übertragen und/oder ausgeführt wurden? Wenn ja, wie wird dies beweissicher festgestellt?
29. Welche konkreten Maßnahmen werden getroffen um zu verhindern dass einzelne Beamte missbräuchlich an persönliche Daten gelangen, die gesondert durch das Grundgesetz und besonders durch das Urteil des BVerfG im Jahr 2008 geschützt sind? ("Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme")
30. Inwieweit kann ausgeschlossen werden, dass Informationen und Daten des unantastbaren Kernbereiches privater Lebensgestaltung nicht erfasst werden?
31. Kann es ausgeschlossen werden, dass derartige Daten den Hoheitsbereich der deutschen Strafverfolgung verlassen? Befindet sich ein Teil der eingesetzten Netzwerk-Infrastruktur im Ausland? Wenn ja, wieso und auf welcher rechtlichen Grundlage?
32. In welcher Form und wie lange werden die ermittelten Daten sowie deren Auswertung gespeichert? Stehen diese Daten auch anderen Behörden zur Verfügung?
33. Wie wurde und wird der Schutz Dritter gewährleistet, die zufällig in Kontakt mit einer Zielperson stehen, aber im ermittelten Fall nicht betroffen sind?
34. 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?

35. Ist es beabsichtigt – in Anbetracht der Manipulationsmöglichkeit und Anfälligkeit der Beweismittelsicherung durch die Software – betroffene Ermittlungsverfahren erneut aufzunehmen, da die Beweissicherheit nicht gewährleistet werden kann?

36. Welche Kosten sind durch die Entwicklung, welche beim Einsatz der Software entstanden und werden voraussichtlich noch entstehen? Von wem werden diese Kosten getragen?

37. Wie ist die Gewährleistung für die Software vertraglich geregelt? Welche Fristen haben etwaige Wartungsverträge?

38. Wer im Land NRW ist bei Einsätzen der Software im Einzelfall in der Verantwortung gewesen und hat deren Einsatz autorisiert?

39. Welche Landes- sowie Bundesbehörden sind zwecks Amtshilfe an dem jeweiligen Einsatz der Software beteiligt gewesen?

40. In welcher Form erfolgt die Archivierung der gesammelten Daten? Wie ist sichergestellt, dass keine Unbefugten Zugriff auf diese Daten bekommen?

Wir weisen Sie darauf hin, dass wir diesen Brief auf der Webseite unseres Landesverbandes veröffentlichen werden, ebenso Ihre Antwort. Wir gehen davon aus, dass Sie uns alle Fragen vollständig und umfassend beantworten werden und bedanken uns bereits im Voraus für Ihr Bemühen.

Mit freundlichen Grüßen,
Kai Schmalenbach
2. Vorsitzender Piratenpartei Landesverband NRW
i.V. des Landesverbandes NRW
der Piratenpartei Deutschland