Offener Brief zum Staatstrojaner

12.10.2011, 17:42 | Politik, Recht & Gesellschaft

Pressemitteilung von: *Piratenpartei Deutschland Landesverband Baden-Württemberg*

Logo der Piratenpartei Baden-Württemberg

Der folgende offene Brief ging heute an die Fraktionen des Landtages, das Landeskriminalamt, das Landesamt für Verfassungsschutz, die Landespolizei, den Innenminister und den Ministerpräsidenten von Baden-Württemberg.

Sehr geehrte Damen und Herren,

wie im Laufe der letzten Tage bekannt wurde, hat auch Baden-Württemberg den sogenannten „Staatstrojaner“ eingesetzt.

Innenminister Gall betonte dabei, dass es sich nur um eine „Basisversion“ handeln würde. Zudem hat das LKA erklärt, dass die Anwendung rechtlich korrekt gewesen sei. Allerdings hat der CCC festgestellt, dass die gefundene Software deutlich weitergehende Fähigkeiten, als nach dem Urteil des Bundesverfassungsgerichts (BVerfG) erlaubt, besitzt. Dies schließt die beliebige Manipulation lokaler Dateien, Bildschirmfotos von nicht zur Kommunikationsübertragung gedachten Daten sowie das Ausspähen von Mikrofon und Webcam ein.

Das Land Baden-Württemberg hat sich damit klar grundgesetzwidrig verhalten und das Urteil des BVerfG in eklatanter Art und Weise missachtet. Wir fordern eine sofortige Aufklärung dieser Umstände und stellen Ihnen deshalb folgende Fragen:

Zum rechtlichen Rahmen

1. In welchen Fällen ist der Einsatz der vom CCC analysierten Software Ihrer Ansicht nach angemessen und gerechtfertigt und in welchen nicht?
2. Auf welchen Rechtsgrundlagen beruhte und beruht der Einsatz im Land Baden-Württemberg?
3. Wie wurde und wird solche Software auf Gesetzeskonformität überprüft?
4. In welchem Maße wurden beziehungsweise werden die durch den Trojanereinsatz gewonnenen Erkenntnisse verwertet?
5. Wie wird sichergestellt, dass der Überwachte nach der Überwachungsaktion über den Vorgang informiert wird? Ist dies bei allen bisherigen Maßnahmen erfolgt? Wenn nein, warum nicht?
6. Wer im Land Baden-Württemberg ist bei Einsätzen der Software im Einzelfall in der Verantwortung gewesen und hat deren Einsatz autorisiert?
7. Welche Landes- sowie Bundesbehörden sind zwecks Amtshilfe an dem jeweiligen Einsatz der Software beteiligt gewesen?

Zur Finanzierung

8. Welche Kosten sind durch die Entwicklung, welche bei Anpassung, welche beim Einsatz der Software entstanden und werden voraussichtlich noch entstehen? Von wem werden diese Kosten getragen?
9. Wie ist die Gewährleistung für die Software vertraglich geregelt? Welche Fristen haben etwaige Wartungsverträge?

Zur technischen Umsetzung

10. Welche Funktionalität besitzt die „Basisversion“ des Trojaners? Welche zusätzlichen Funktionen können ihr noch hinzugefügt werden? Wir erwarten eine lückenlose Liste der vorhandenen, geplanten und in Entwicklung befindlichen Erweiterungen.
11. Sind weitere Versionen der Software in Entwicklung und wenn ja, welche neuen Eigenschaften sollen diese Versionen enthalten?
12. Auf welche Weise setzt sich die Software im Zielsystem fest und welche Dateien sind davon betroffen?
13. Inwieweit kann die eingesetzte Software gängige Anonymisierungs- und Verschlüsselungsmechanismen wie zum Beispiel TLS, AES oder Onion Routing umgehen beziehungsweise manipulieren?
14. 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?
15. Über welchen Weg gelangen die Daten vom überwachten Endgerät zu den Ermittlungsbehörden?
16. 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?
17. 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?

Zur konkreten Nutzung

18. In angeblich fünf Fällen wurde oder wird dieser „Staatstrojaner“ oder Software mit vergleichbarer Funktionalität im Land Baden-Württemberg bereits eingesetzt. Ist diese Zahl korrekt? Wie wurde der Einsatz jeweils begründet? Welche Version des Trojaners kam mit jeweils welchen Fähigkeiten zum Einsatz?
19. 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?
20. Gibt es besondere Handlungsanweisungen zur Wahrung der Rechte der ausgespähten Personen und anderer Unbeteiligter? Wenn ja, wie lauten diese?
21. 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?
22. 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?
23. 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?
24. 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?
25. 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“)?
26. Inwieweit kann ausgeschlossen werden, dass Informationen und Daten des unantastbaren Kernbereiches privater Lebensgestaltung nicht erfasst werden?
27. In welcher Form und wie lange werden die ermittelten Daten sowie deren Auswertung gespeichert? Stehen diese Daten auch anderen Behörden zur Verfügung?

28. Wie wurde und wird der Schutz Dritter gewährleistet, die zufällig in Kontakt mit einer Zielperson stehen, aber im ermittelten Fall nicht betroffen sind?
29. Wie wird sichergestellt, dass es sich bei dem überwachten Rechner um den Rechner der Zielperson handelt, beziehungsweise dass er allein von dieser Person benutzt wurde und die gewonnen Erkenntnisse zweifelsfrei und eindeutig diesem Benutzer zugeordnet werden können? Wie wird der Schutz von weiteren Nutzern eines Zielcomputers sicher gestellt?
30. 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?
31.In welcher Form erfolgt die Archivierung der gesammelten Daten? Wie ist sichergestellt, dass keine Unbefugten Zugriff auf diese Daten bekommen?

Zu externen Dienstleistern

32. Für wen arbeitete die beauftragte Firma zusätzlich? Waren anderen Behörden des Landes Baden-Württemberg oder Behörden anderer Länder die grundsätzlichen Defizite der Software bekannt?
33. Wie wurde sichergestellt, dass die beauftragte Firma entsprechend zertifiziert ist, solche Aufträge zu bearbeiten? Führte 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, warum nicht?
34. Hat es Absprachen mit Internetdienstanbietern gegeben, um deren Infrastruktur und/oder Hard- und Software zur mittelbaren oder unmittelbaren Infektion des Zielrechners einzusetzen? Wenn ja, welche Firmen waren hier involviert?
35. 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?
36. 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?
37. Kann es ausgeschlossen werden, dass Informationen und Daten des unantastbaren Kernbereiches privater Lebensgestaltung den Hoheitsbereich der deutschen Strafverfolgung verlassen? Befindet sich ein Teil der eingesetzten Netzwerk-Infrastruktur im Ausland? Wenn ja, warum und auf welcher rechtlichen Grundlage?

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,
André Martens,
i.V. des Landesverbandes Baden-Württemberg der Piratenpartei Deutschland

Portrait

Über die Piratenpartei Deutschland:

Die Piratenpartei ist mit bundesweit 15.000 Mitgliedern die größte der nicht im Bundestag vertretenen Parteien. Bei der

Europawahl (0,9%) und der Bundestagswahl (2,0%) hatten die PIRATEN in 2009 erste Achtungserfolge erzielt und sind im Europaparlament durch die schwedische Piratenpartei schon mit zwei Abgeordneten vertreten. Bei der Landtagswahl 2011 in Baden-Württemberg erreichten die PIRATEN ein Ergebnis von 2,1%, in Berlin zogen sie im gleichen Jahr mit 8,9% und 15 Sitzen in das Abgeordnetenhaus ein.