Arbeitskreis Vorratsdatenspeicherung
- Ortsgruppe Hannover

% Michael Ebeling
Kochstraße 6
30451 Hannover

og-hannover@vorratsdatenspeicherung.de
http://wiki.vorratsdatenspeicherung.de/Hannover

Arbeitskreis Vorratsdatenspeicherung OG Hannover

An den Präsidenten des Landeskriminalamts Niedersachsen
Herrn Uwe Kolmey
Am Waterlooplatz 11
30169 Hannover

Hannover, den 17. Oktober 2011

Offener Brief zum Einsatz von Trojaner-Spionagesoftware in Niedersachsen

Sehr geehrter Herr Kolmey,

im Zuge der aktuellen öffentlichen Diskussion um den behördlichen Einsatz von Spionagesoftware haben Sie am 11. Oktober 2011 mitgeteilt, dass auch das niedersächsische Landeskriminalamt seit derartige Ermittlungsmethoden einsetzen würde:

> *"Überwacht werden aber nur sogenannte Telekommunikationsdaten, es werden keine Bildschirmbilder gemacht, Tastatureingaben gespeichert oder Festplatten ausspioniert."*

Sie betonen auch:

> *"Bei uns werden die Vorgaben des Bundesverfassungsgerichts jedenfalls befolgt."*

Aussagen von Herrn Uwe Schünemann ist weiterhin zu entnehmen, dass es zwei Fälle des Einsatzes von Spionagesoftware zur Belauschung von Internet-Telefonie nach jeweiligem richterlichen Beschluss gegeben habe.

Weiterhin wurde mitgeteilt, dass eine ehemalig eingesetzte Software von der Firma Digitask stammte und dass es im Zuge von "Modernisierungsmaßnahmen" einen Systemwechsel gegeben habe.

Weiterhin teilen Sie in einer Pressemitteilung vom 12. Oktober 2011 mit:

> *„Aufgrund bereits im Juni dieses Jahres durchgeführter technischer Modernisierungsmaßnahmen ist bei der niedersächsischen Landespolizei auch zukünftig rechtlich und technisch sichergestellt, dass eine Quellen-TKÜ verfassungskonform durchgeführt werden kann."*

Um ehrlich zu sein:

Uns hat weniger überrascht, dass auch Ihre Behörde diese Softwaretools zum Ausspionieren fremder Rechner einsetzt - Methoden, die wir aus prinzipiellen Gründen mit unserer Vorstellung einer demokratischen Gesellschaft und der von den in dieser Gemeinschaft lebenden Menschen ausgehenden Souveränität für völlig unvereinbar halten.

Umso mehr weckt die Debatte unser spezielles Interesse und wir möchten uns mit den folgenden Fragen an Sie wenden. Dass es 23 Fragen an der Zahl sind, ist tatsächlich reiner Zufall.

Unsere Fragen:

1.)
Stimmt unsere oben aufgeführte Zusammenfassung der Fakten und Tatsachen? Falls nicht: Welche Details stimmen nicht?

2.)
Wie viele Fälle von Überwachung bzw. Abgriff von Daten aus fremden Rechnern gab es beim LKA Niedersachsen bisher? Bitte berücksichtigen Sie, dass wir damit nicht nur den Abgriff von Internet-Telefonie berücksichtigt sehen möchten, sondern den Einsatz von Spionagesoftware zur Erlangung von Zugriffsrechten irgendeiner Art im allgemeinen.

3.)
Werden die von einer derartigen Ausspionierung ihres Computers betroffenen Menschen über diese „Maßnahme“ informiert? Ist dieses in den bisher durchgeführten Fällen geschehen?

4.)
Wie lautet der Name des Dienstleisters, der die Spionagesoftware seit Juni 2011 dem LKA Niedersachsen zur Verfügung stellt bzw. diese programmiert und/oder betreut?
Genauer gefragt: Stimmt es, dass die Firma Syborg oder ein anderes der Verint-Gruppe zugehöriges Unternehmen für Programmierung und/oder Betreuung der aktuellen niedersächsischen Spionagesoftware zuständig ist?

5.)
Welches waren die Gründe für den Wechsel der Software zum Juni 2011?

6.)
Wie hoch waren die laufenden und wie hoch die Anschaffungskosten für die ehemalige Spionagesoftware? (Anschaffungskosten und laufende Kosten z.B. für die Geschäftsjahre 2009 und 2010.)

7.)
Wie hoch waren die Investitionskosten für die seit Juni 2011 vorhandene Spionagesoftware?

8.)
Gab es eine Ausschreibung für diese Software und/oder ihren Einsatz? Falls ja: Handelte es sich um eine öffentliche oder um eine beschränkte Ausschreibung und können Sie uns den Ausschreibungstext zukommen lassen?

9.)
Wie hoch sind die laufenden Kosten (z.B. Leasing-/Leihkosten) für die aktuell vorhandene Spionagesoftware?

10.)
Was kostet eine Maßnahme mit der aktuellen Software auf einen konkreten Einsatz bezogen bzw. umgerechnet?

11.)
Halten Sie die in § 100a StPO Absatz 1 und die in Absatz 2 aufgeführte Straftatbestände hinsichtlich Anforderung und Umfang als rechtskonform mit dem Urteil des BVerfG zum "Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme" vom 27.2.2008?

12.)
Bewerten Sie die bis Juni 2011 eingesetzten Computerspionageprogramme und Softwaretools zur Ausspionierung fremder Rechner im Verhältnis zum derzeitigen Stand von Recht und Rechtsprechung für rechts- und verfassungskonform?

13.)
Wie gewährleisten Sie die Integrität der digital erhobenen Daten, Telefongespräche usw.? Welche Maßnahmen haben Sie getroffen, um einen besonderen Schutz dieser Daten zu sichern?

14.)
Gab es im Zusammenhang mit Ausschreibung, Beschaffung und/oder Wartung und Bedienung der Spionagesoftware eine Zusammenarbeit mit anderen Behörden? Falls ja: Um welche Behörden hat es sich dabei gehandelt?

15.)
Über welchen Umfang erstreckt sich eine derartige aktuelle Zusammenarbeit mit dem Bundeskriminalamt?

16.)
Können Sie die von Herrn Schünemann in der Phoenix-Diskussionrunde vom 13.10.2011 getroffene Behauptung, dass für jeden Anwendungsfall des Einsatzes von Spionagesoftware zur TKÜ-Überwachung eine fallbezogene Programmierung erfolgt? Wird der Landesdatenschutzbeauftragte hierbei hinzugezogen?

17.)
Gibt es Statistiken und/oder Untersuchungen zu Umfang, Art und Weise sowie Erfolgen des Einsatzes dieser Software?

18.)
Werden Untersuchungen und Bewertungen des Eingriffes in die Grundrechte der betroffenen Menschen im Verhältnis zum Strafverfolgungserfolg der Maßnahme durchgeführt? Wenn ja: Mit welchem Ergebnis?

19.)
Gab es Anträge zum Einsatz einer solchen Spionagesoftware, der vom zuständigen Richter abgelehnt worden ist? Falls ja: Um wie viele Fälle handelt es sich dabei?

Spätestens seit 2010 ist nicht nur bekannt sondern auch nachweisbar, dass es eine Zusammenarbeit deutscher Polizeibehörden mit Skype Technologies, dem Anbieter des von vielen Menschen gern benutzten Skype-Dienstes zur kostenlosen Internet-Telefonie gibt.

In Ihrer Pressemitteilung vom 12. Oktober betonen Sie, dass Sie Ihre Spionagesoftware ausschließlich zur Überwachung von Kommunikation einsetzen würden. Innenminister Uwe Schünemann betont darüber hinaus, dass es zwei Einsätze der Software zur Überwachung von Internet-Telefonie gegeben habe.

20.)
Warum wurde anstelle der Zusammenarbeit mit Skype Technologies oder eines ihrer Tochterunternehmens der Einsatz der Trojanersoftware bevorzugt, wenn es denn "nur" um die Überwachung der Internettelefonie ging?

Falls es ganz allgemein und unabhängig von diesen beiden Fällen eine solche Zusammenarbeit mit Skype Technologies oder eines ihrer Tochterunternehmens gab oder gibt:

21.)
Wie oft bzw. in wie vielen Fällen wurden Skype-Gespräche durch Ihre Behörde bislang ab- bzw. mitgehört und gab es rechtzeitig vorher richterliche Beschlüsse zur Durchführung dieser Maßnahmen?

Weiterhin:

22.)
Wenn Herr Schünemann betont, dass es konkret zwei Fälle des Einsatzes der Spionagesoftware im Zusammenhang mit der Überwachung von Internet-Telefonie gab, kann man dann davon ausgehen, dass es weitere Fälle des Einsatzes gab, in denen es nicht oder nicht nur die Überwachung der Internet-Telefonie sondern um andere oder weitergehende Überwachungszwecke ging?

Und abschließend:

23.)
Steht ein eingesetzter Trojaner, der aktiv in das ausspionierte Computersystem eingreift und Einstellungen, Daten und Informationen verändern kann (und ohne solches wäre kein Abhören möglich!) nicht im grundsätzlichen Widerspruch zu einer verlässlichen und belastbaren Auswertung und Verwertung der erhobenen Daten?

Wir würden uns freuen, bald von Ihnen etwas dazu zu hören und möchten die Antworten danach gerne veröffentlichen.

Mit freundlichen Grüßen,

Michael Ebeling
für den
AK Vorrat Hannover