



Bayerisches Staatsministerium des Innern • 80524 München

vorab per E-Mail
Präsidentin
des Bayer. Landtags
Frau Barbara Stamm, MdL
Maximilianeum
81627 München

Ihr Zeichen, Ihre Nachricht vom PI/G-4253-3/924 19.10.2011	Unser Zeichen IC5-1119.1-109 Hai Telefon / - Fax 089 2192-2650 / -12762	Bearbeiter Herr Haimerl Zimmer 261	München 21.11.2011 E-Mail stmi.polizeieinsatz@polizei.bayern.de
--	--	---	--

**Schriftliche Anfrage der Frau Abgeordneten Susanna Tausendfreund vom
13.10.2011 betreffend „Verfassungswidriger Einsatz von Trojaner-Software in
Bayern – weitere Aufklärung I“**

Anlagen

5 Kopien dieses Schreibens
Tabellarische Aufstellung (5fach)

Sehr geehrte Frau Landtagspräsidentin,

die Schriftliche Anfrage beantworte ich im Einvernehmen mit dem Bayerischen
Staatsministerium der Justiz und für Verbraucherschutz wie folgt:

Vorbemerkung

Aufgrund der aktuellen Diskussion zur infrage stehenden Thematik der Quellen-
Telekommunikationsüberwachung (Quellen-TKÜ) wird die Schriftliche Anfrage in
der Form ausgelegt, dass hier Maßnahmen der dem Bayerischen Staatsministeri-
um des Innern nachgeordneten Behörden (Polizei und Bayerisches Landesamt für
Verfassungsschutz) sowie Anordnungen und Beschlüsse von Stellen der Bayeri-
schen Justiz betroffen sind. Der Geschäftsbereich des Bayerischen Staatsministe-
riums der Finanzen ist nach dortiger Mitteilung von der Fragestellung nicht betref-
fen.

Im Aufgabenbereich des Landesamtes für Verfassungsschutz wurden in drei Fällen des islamistischen Terrorismus Maßnahmen der Quellen-TKÜ beantragt und von der G 10-Kommission des Bayerischen Landtags gebilligt. Die Maßnahmen betrafen ausschließlich die Kommunikation über Skype. Rechtsgrundlage war das Artikel 10-Gesetz. Darüber hinausgehend wird über Maßnahmen im Bereich des Verfassungsschutzes und die näheren Umstände hierzu nur im Parlamentarischen Kontrollgremium berichtet.

Zu den Fragen im Einzelnen:

Frage 1.1:

Wie ist die genaue Funktionalität der durch Bayerische Behörden eingesetzten Trojaner-Software ausgestaltet?

Die Quellen-TKÜ grenzt sich von der „konventionellen“ TKÜ technisch dadurch ab, dass die Daten nach verdeckter Einbringung einer Überwachungssoftware im Zielsystem (der „Quelle“) noch vor der Verschlüsselung bzw. nach ihrer Entschlüsselung erhoben werden. Eine andere technische Möglichkeit steht den Strafverfolgungsbehörden nicht zur Verfügung. Eine Entschlüsselung der Telekommunikationsdaten ist auch über den Anbieter (z. B. Skype) nicht möglich. Bei einer Quellen-TKÜ werden nur Daten im Rahmen eines laufenden Telekommunikationsvorgangs überwacht. Die technische Konfiguration der Software für eine Maßnahme der Quellen-TKÜ richtet sich an den technischen Parametern des Zielsystems aus, die im Vorfeld einer Quellen-TKÜ durch eine TKÜ-Maßnahme auf Grundlage eines richterlichen Beschlusses erhoben werden (vgl. auch Antwort zur Frage 3.3). Nach Auskunft des BLKA beinhaltet die Quellen-TKÜ-Software ausschließlich Funktionalitäten, die vom richterlichen Beschluss umfasst sind. Der Leistungsumfang der jeweiligen Software ist auf nachstehende Funktionalitäten beschränkt:

- Überwachung verschlüsselter Telekommunikation verschiedener Messenger (z. B. Skype).
- Fertigung sog. Application-Shots, sofern vom richterlichen Beschluss umfasst. Application-Shots sind Abbildungen der bei einem Telekommunikationsvorgang aktiven Kommunikationsanwendung (z. B. Internetbrowser). Weitere auf dem Bildschirm des Zielrechners geöffnete und sichtbare Programme/Fenster/Applikationen (z. B. geöffnetes Word-Dokument), die nicht

mit dem Telekommunikationsvorgang und der Telekommunikationsanwendung in Zusammenhang stehen, werden nicht ausgeleitet. Somit ist im Gesamtkontext der Begriff „Screenshot“ irreführend.

- Verifizierung technischer Systemparameter auf dem Zielsystem, die bereits im Rahmen der „konventionellen TKÜ“ zur Identifizierung des Zielsystems erhoben wurden.
- Update der Quellen-TKÜ-Software auf dem Zielsystem. Diese Funktionalität ist insbesondere deshalb erforderlich, um auf Veränderungen des Zielsystems, z. B. durch Aktualisierungen des Virenschanners oder Skype, reagieren zu können.
- Neustart des Zielsystems, da Updates erst nach einem Neustart des Zielsystems wirksam werden.
- Löschung der Quellen-TKÜ-Software auf dem Zielsystem nach Fristablauf oder Beendigung der angeordneten Überwachungsmaßnahme.

Entgegen der Veröffentlichungen des Chaos Computer Club sind nachstehende, beispielhaft aufgezählte Funktionalitäten nicht Bestandteil der durch das BLKA eingesetzten Quellen-TKÜ-Software:

- Suche nach und Auslesen von benutzerbezogenen Dateien („Online-Durchsuchung“);
- Datenzugriff auf Festplatte;
- Registrierung bzw. Ausleitung von Tastaturanschlägen („Keylogger-Funktionalitäten“);
- Aktivieren von Kameras und Mikrofonen.

Frage 1.2:

In wie vielen Fällen wurden solche oder ähnliche Programme, mit je welchen Funktionen, auf je welcher Rechtsgrundlage (präventiv und repressiv) durch welche Bayerischen Behörden wann eingesetzt und welche Anlassstrafat bzw. welche Anlass-Gefahr und welche Sachverhalte lagen der Anordnung/dem Einsatz zugrunde (bitte Antworten tabellarisch auflisten, wo vorhanden bitte mit gerichtlichen Aktenzeichen)?

Insoweit wird auf die in der Anlage beigefügte tabellarische Auflistung sowie die Anfragen zum Plenum vom 24.10.2011 (LT-Drs. 16/10082 vom 27.10.2011) Bezug genommen.

Frage 1.3:

Ist es zutreffend, dass die Software auch über solche Funktionen verfügt, die vom CCC als rechtswidrig identifiziert wurden, insbesondere die Möglichkeit bereitstellt vom Inhaber unbemerkt Programme auf den Zielrechner nachzuladen und somit ferngesteuert auf Mikrophon, Kamera und Tastatur des überwachten Computers zuzugreifen?

Nein. Vgl. hierzu auch Ausführungen zur Frage 1.1 (bzgl. Funktionalitäten) und Frage 2.1 (bzgl. Update-Funktion). Wie das BLKA darstellt, waren darüber hinausgehende Funktionalitäten nicht vorhanden.

Frage 2.1:

Wie oft und in welchen Fällen wurde beim Einsatz dieser Software die technische Möglichkeit des Nachladens unbemerkter Updates genutzt und welche Programme wurden dabei nachgeladen?

Bei der vom BLKA genutzten Software ist ein „Nachladen“ weiterer Funktionalitäten technisch nicht möglich. Es besteht nur die technische Möglichkeit, ein Update der Quellen-TKÜ-Software in das Zielsystem einzubringen. Ein solches Update wurde durch das BLKA dreimal genutzt, um die Quellen-TKÜ-Software an die zu überwachenden Telekommunikationsclients anzupassen (z. B. aufgrund eines Skype-Updates) und damit die unterbrechungsfreie Aufzeichnung der Telekommunikation realisieren und eine Umsetzung der den Maßnahmen zu Grunde liegenden richterlichen Beschlüsse gewährleisten zu können. Das BLKA hat die Updatefunktion ausschließlich zur Aktualisierung genutzt, d. h. dass ebenso wie die Quellen-TKÜ-Software selbst auch deren Updates nur Funktionen umfassten, die den richterlichen Beschlüssen entsprachen. Jede Nutzung der Updatefunktion wurde umfassend protokolliert.

Frage 2.2:

Wie oft und in welchen Fällen wurde beim Einsatz der Software ferngesteuert auf Mikrofon, Kamera und Tastatur des Zielrechners zugegriffen?

Wie in den Antworten zu den Fragen 1.1 und 1.3 dargestellt, verfügt die vom BLKA eingesetzte Quellen-TKÜ-Software nicht über die in Frage 2.2 bezeichneten Funktionalitäten.

Frage 2.3:

Wie wurde diese Software auf den Zielrechnern jeweils aufgebracht?

Die Einbringungsmethode für die Installation der Quellen-TKÜ-Software ist nicht standardisiert; sie ist vom jeweiligen Sachverhalt im Einzelfall abhängig. Technisch gibt es zwei Möglichkeiten, entweder im Wege der Remote-Installation (Einbringung durch polizeitaktische Maßnahme, z. B. E-Mail) oder durch manuelle Installation (physikalischer Zugriff auf das Zielsystem durch polizeiliche Maßnahme). Eine Aufschlüsselung ergibt sich aus der Anlage.

Frage 3.1:

Ist es zutreffend, dass es insgesamt in Bayern 22 Fälle des Einsatzes dieser oder ähnlicher Software gab, während die Staatsregierung zuvor in ihren Antworten auf die Anfragen vom 17.02.2011 und 14.04.2011 (LT. DS. 16/8125 und LT.DS. 8747) bisher lediglich fünf Fälle eingeräumt hat?

Seit der Übernahme der zentralen Erfassungs- und Berichtspflichten gem. § 100b Abs. 5 und 6 StPO zum 01.01.2009 durch das BLKA wurden in 14 Fällen/Ermittlungsverfahren insgesamt 22 technische Maßnahmen mit einer Quellen-TKÜ-Software zur Überwachung der verschlüsselten Telekommunikation im Internet vom BLKA im Rahmen von Ermittlungsverfahren ausgeführt und statistisch erfasst.

In fünf dieser Fälle/Ermittlungsverfahren wurden Application-Shots (zum Begriff siehe Antwort zu Frage 1.1) der jeweils laufenden Internetverbindung ausgeleitet, da neben der verschlüsselten Sprachübertragung auch die verschlüsselte Datenkommunikation vom richterlichen Beschluss umfasst war. Da in einem der fünf Fälle/Ermittlungsverfahren zwei technische Maßnahmen geschaltet waren, in de-

nen Application-Shots ausgeleitet wurden, ergibt sich eine Gesamtzahl von sechs technischen Maßnahmen mit Application-Shots.

Die schriftlichen Anfragen der Frau Abgeordneten Tausendfreund vom 17.02.2011 und 14.04.2011 bezogen sich ausdrücklich auf „Fälle, in denen grafische Bildschirmhalte (Screenshots) kopiert und gespeichert wurden“; hierzu wurde umfassend berichtet (siehe LT-Drs. 16/8125 vom 29.04.2011 und LT-Drs. 16/8747 vom 05.07.2011).

Frage 3.2:

Wenn ja, welche Umstände lagen diesem Einsatz zugrunde und welche Funktionalitäten bot die Software?

Quellen-TKÜ-Maßnahmen wurden im Auftrag der jeweils zuständigen Staatsanwaltschaft nach richterlichem Beschluss vom BLKA technisch umgesetzt. Die Softwarelösungen umfassten dabei ausschließlich Funktionen, die der Umsetzung des jeweiligen richterlichen Beschlusses dienten. Siehe hierzu auch die Antwort zu Frage 1.2 und die beiliegende tabellarische Übersicht.

Frage 3.3:

Wurde die Überwachung von verschlüsselter Telekommunikation oder deren Vorstufen auch mithilfe anderer technischer Mittel, als der oben beschriebenen Software durchgeführt und wenn ja mit welchen Mitteln und mit welchen Funktionalitäten?

Nein. Grundsätzlich ist zwischen der Quellen-TKÜ und einer der eigentlichen Maßnahme vorgeschalteten „konventionellen“ TKÜ zu unterscheiden. Im Rahmen einer „konventionellen“ TKÜ-Maßnahme werden standardisiert alle Telekommunikationsinhaltsdaten (hierunter fallen auch technische Systemparameter) aufgezeichnet, die über den überwachten Telekommunikationsanschluss übertragen werden. Während die Quellen-TKÜ den Einsatz einer auf das Zielsystem spezifizierten Softwarelösung bedingt, bedarf die Erhebung und Auswertung der technischen Systemparameter („Vorstufe zur Quellen-TKÜ“) lediglich einer „konventionellen“ TKÜ-Maßnahme (vgl. hierzu Ausführungen zur Frage 1.1). Die zur Vorbereitung einer Quellen-TKÜ-Maßnahme erforderlichen technischen Systemparameter werden so im Rahmen einer „konventionellen“ TKÜ-Maßnahme standardisiert

als Teilmenge der Telekommunikationsinhaltsdaten gewonnen; der Einsatz „anderer technischer Mittel“ ist darüber hinaus nicht erforderlich.

Frage 4.1:

In welchen Einsatzfällen legten Betroffene Rechtsmittel gegen Maßnahmen ein, die mittels Trojaner-Software durchgeführt wurden und mit je welchem Ergebnis?

Im Verfahren 45 Js 115652/08 wurde gegen die Entscheidung des Ermittlungsrichters des Amtsgerichts Landshut vom 02.04.2009 (Az. II Gs 1200/09) mit Schriftsatz des Verteidigers des Betroffenen vom 02.03.2010 Antrag auf gerichtliche Entscheidung nach § 101 Abs. 7 Satz 2 StPO gestellt. Mit Beschluss vom 20.01.2011 (Az. 4 Qs 346/10) hat das Landgericht Landshut den Ausgangsbeschluss teilweise abgeändert und gleichzeitig festgestellt, dass der Vollzug des Beschlusses des Amtsgerichts Landshut vom 02.04.2009 rechtswidrig war, soweit grafische Bildschirminhalte kopiert und gespeichert wurden. Im Übrigen wurde das Rechtsmittel als unbegründet verworfen.

Weitere Rechtsmittel gegen gerichtliche Anordnungen von Quellen-TKÜ-Maßnahmen wurden nicht eingelegt.

Frage 4.2:

Wie wurde beim Einsatz der Software sichergestellt, dass das vom Bundesverfassungsgericht aus dem allgemeinen Persönlichkeitsrecht, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz entwickelte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme beim Einsatz der Schadsoftware gewährleistet wird und der als unantastbar definierte Kernbereich privater Lebensgestaltung tatsächlich nicht angetastet wurde?

Das BVerfG hat in seiner Entscheidung zur Onlinedurchsuchung (Urteil vom 27. Februar 2008 - 1 BvR 370/07 -, BVerfGE 120, 274/309 = MMR 2008, 315) ausdrücklich klargestellt, dass bei der Quellen-TKÜ Art. 10 GG der alleinige grundrechtliche Maßstab für die Beurteilung dieses Eingriffs ist (vgl. auch BT-Drs. 16/6885, S. 3 und BT-Drs. 16/7279, S. 3), wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein. Die Quellen-TKÜ ist damit klar von einer Onlinedurchsuchung

abgegrenzt, bei der es erst zu einem Eingriff in das durch Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG geschützte und vom BVerfG aus dem allgemeinen Persönlichkeitsrecht entwickelte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme kommt. Diese verfassungsrechtlichen Vorgaben werden auch durch die den jeweiligen Maßnahmen zugrunde liegenden richterlichen Beschlüsse berücksichtigt.

Zudem wird durch die bereits zu Frage 1.1 dargestellten technischen Vorkehrungen sichergestellt, dass die verfassungsrechtlichen Vorgaben und die den richterlichen Anordnungsbeschlüssen zu Grunde liegenden Beschränkungen der Funktionalitäten der Quellen-TKÜ-Software bei der Umsetzung durch das BLKA beachtet werden. Die Softwarelösung wird im BLKA auch einem Qualitätssicherungsprozess unterzogen, durch den gewährleistet wird, dass die Quellen-TKÜ-Software ausschließlich vom Anordnungsbeschluss umfasste Funktionen beinhaltet. Unabhängig davon, ob es sich um eine „konventionelle“ TKÜ oder eine Maßnahme der Quellen-TKÜ handelt, die beide hinsichtlich ihrer Rechtsgrundlage §§ 100a, 100b StPO unterfallen, ist für den Kernbereichsschutz der privaten Lebensgestaltung die Vorschrift des § 100a Abs. 4 StPO einschlägig.

Mit freundlichen Grüßen

Joachim Herrmann
Staatsminister