Bayerischer Landtag
16. Wahlperiode

Drucksache 16/**10607**

17.01.2012

Schriftliche Anfrage

des Abgeordneten **Florian Streibl FREIE WÄHLER**
vom 19.10.2011

Einsatz von Spionagesoftware in Bayern

Dem Chaos Computer Club (CCC) wurde nach eigenen Angaben eine staatliche Software für das heimliche Ausspähen von Computern zugespielt. Nach einer Analyse dieses Programms erhebt der CCC schwere Vorwürfe gegen staatliche Stellen, da mit dem Einsatz des Trojaners Ermittlungsbehörden massiv gegen ein Urteil des Bundesverfassungsgerichts verstoßen würden. Das Bundesinnenministerium hat auf die Vorwürfe hin erklärt, das Bundeskriminalamt habe den kritisierten Trojaner nicht eingesetzt. Bayerns Innenminister Joachim Herrmann bestätigte nun, dass die Software einem Ermittlungsverfahren der Bayerischen Polizei von 2009 zugeordnet werden kann.

Ich frage die Staatsregierung:

1. Weshalb wurde diese Schadsoftware mit welchen Funktionen beschafft bzw. beauftragt und wie bewertet die Staatsregierung die Aussage des Chaos Computer Clubs, die Schadsoftware weise handwerkliche Mängel auf (sie verursache z. B. Sicherheitslücken, die von Dritten ausgenützt werden können)?

2. a) Wie oft wurde auf wie vielen Rechnern und in welchen Fällen die vom Chaos Computer Club entdeckte Schadsoftware zur Überwachung verwendet?
   b) Aufgrund welcher Rechtsgrundlage und mit welchem Umfang erfolgte die richterliche Anordnung?
   c) Mit welchen Funktionen war die Schadsoftware dabei jeweils ausgestattet und wusste der jeweilige Richter hierüber Bescheid?
   d) Wurde die Möglichkeit genutzt, Schadmodule nachzuladen und auszuführen?

3. a) Besteht für überwachte Personen nun die Möglichkeit festzustellen, dass eine Telekommunikationsüberwachung stattfindet?
   b) Inwiefern ist die Software gegen eine Zweckentfremdung geschützt?
   c) Ist es den „Überwachten“ möglich, diese Software nun zu „extrahieren“ und für eigene Zwecke zu verwenden, und wie gedenkt die Staatsregierung dies gegebenenfalls zu verhindern?

4. Welche Zusammenarbeit gibt bzw. gab es gegebenenfalls bei der Entwicklung bzw. Anwendung der Software mit anderen Bundesländern oder der Bundesebene?

5. a) Wem wurde die Software noch zur Verfügung gestellt?
   b) Wurde sie insbesondere an das Landesamt für Verfassungsschutz oder andere Landesämter für Verfassungsschutz weitergegeben?
   c) Falls ja, wie oft und in welchen Fällen hat das Landesamt für Verfassungsschutz die Schadsoftware mit welchen Funktionen benutzt?

6. a) Welche Vorgaben gibt es für die Zertifizierung derartiger Programme?
   b) Wie wird gewährleistet, dass derartige Programme den verfassungsrechtlichen Vorgaben genügen?
   c) Weshalb wurde der Landesbeauftragte für den Datenschutz nicht früher eingebunden und wird er zukünftig bei der Zertifizierung eingebunden sein?

Antwort

des Staatsministeriums des Innern
vom 02.12.2011

Die Schriftliche Anfrage wird im Einvernehmen mit dem Staatsministerium der Justiz und für Verbraucherschutz wie folgt beantwortet:

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 Staatsministerium des Innern nachgeordneten Behörden (Polizei und Bayerisches Landesamt für Verfassungsschutz) sowie Anordnungen und Beschlüsse von Stellen der Bayerischen Justiz betroffen sind. Der Geschäftsbereich des Bayerischen Staatsministeriums der Finanzen ist nach dortiger Mitteilung von der Fragestellung nicht betroffen.

Zu den Fragen im Einzelnen:

Zu 1.:
Auf Antrag der Staatsanwaltschaft Landshut erließ das Amtsgericht Landshut am 02.04.2009 einen Beschluss nach §§ 100 a, 100 b StPO, in dem ausdrücklich die Überwachung des verschlüsselten Telekommunikationsverkehrs über

HTTPS und über Messenger wie z. B. „Skype“ angeordnet wurde. Mit dem Vollzug dieses Beschlusses beauftragte die Staatsanwaltschaft Landshut das BLKA.

Zum Zwecke der Ausleitung der verschlüsselten Telekommunikation wurde im gegenständlichen Ermittlungsverfahren durch das BLKA bei der Fa. DigiTask eine Software beauftragt, welche über die zwei nachstehend angeführten Funktionen verfügte:

- Überwachung und Ausleitung der verschlüsselten Skype-Kommunikation (SpracheNolP) vor der Verschlüsselung bzw. nach der Entschlüsselung.
- Automatisierte Erstellung sog. Application-Shots der aktiven Skype- und Internetbrowser-Applikation zur Überwachung der verschlüsselten, auch über HTTPS geführten Telekommunikation.

Vgl. hierzu auch die Ausführungen zu Ziffer 1 der LT-Drucksache 16/8125 vom 29.04.2011.

Die durch die Fa. DigiTask programmierte Softwarelösung wurde im BLKA einem aufwendigen Qualitätssicherungsprozess unterzogen. Dadurch wurde gewährleistet, dass die Quellen-TKÜ-Software ausschließlich Funktionen beinhaltete, die vom richterlichen Beschluss umfasst waren. Die Einschätzung des Chaos Computer Clubs (CCC), die „Schadsoftware weise handwerkliche Mängel auf“, wird nicht geteilt. Zum Aspekt „mögliche Sicherheitslücken“ wird auf die Antwort zu Frage 3 b und c verwiesen.

Zu 2. a):
Die im gegenständlichen Ermittlungsverfahren der Staatsanwaltschaft Landshut vom BLKA eingesetzte Quellen-TKÜ-Software wurde nur in diesem einen Fall auf einem Rechner aufgebracht.
Grundsätzlich ist hierzu anzumerken, dass für jede einzelne Maßnahme der Quellen-TKÜ in einem Ermittlungsverfahren zur Umsetzung des zugrunde liegenden richterlichen Beschlusses mit jeweils gesondertem Vertrag eine speziell auf das Zielsystem abgestimmte Quellen-TKÜ-Softwarelösung durch das zuständige Kompetenzzentrum Telekommunikationsüberwachung Bayern des BLKA bei der Fa. DigiTask in Auftrag gegeben wurde. Jede Quellen-TKÜ-Softwarelösung ist durch einen digitalen Fingerabdruck (Hashwert) gekennzeichnet und damit individualisiert.

Zu 2. b):
Die richterliche Anordnung in allen Verfahren, bei denen eine Quellen-TKÜ durchgeführt wurde, stützt sich auf die Eingriffsermächtigung zur Überwachung der Telekommunikation in §§ 100 a, 100 b StPO.

Im Rahmen dieser Anordnung hat der Ermittlungsrichter auch jeweils im konkreten Einzelfall den Umfang der Maßnahme festzulegen.

Zu 2. c):
Hinsichtlich der Funktionen der in Rede stehenden Software wird auf die Ausführungen zu Frage 1 verwiesen.

Die Ermittlungsrichter wurden von den jeweils zuständigen Ermittlungsbehörden über die mit der Anordnung und Umsetzung der Quellen-TKÜ verbundenen Fragestellungen durch die Antragstellung informiert.

Zu 2. d):
Nein. Das BLKA verwendet bei der Umsetzung von richterlichen Quellen-TKÜ-Beschlüssen keine „Schadmodule“. In keinem Fall, also auch nicht im gegenständlichen Ermittlungsverfahren, enthielt die Quellen-TKÜ-Software andere/weitere als die der Umsetzung des richterlichen Beschlusses dienende Funktionalitäten.

Zu 3. a):
Der Wesensgehalt einer Quellen-TKÜ-Maßnahme besteht in besonderem Maße in ihrer Nichtdetektierbarkeit. Darauf wird bei dem eine Quellen-TKÜ-Maßnahme begleitenden Qualitätssicherungsprozess besonderer Wert gelegt. Auch im gegenständlichen Fall wurde die durchgeführte Telekommunikationsüberwachung nicht während der Überwachungsmaßnahme selbst festgestellt, sondern wurde dem Betroffenen erst im Nachhinein im Rahmen der Akteneinsicht bekannt.

Zu 3. b):
Wenn das Zielsystem im Internet eingeloggt ist, erfolgt in festgelegten Intervallen der Versuch eines Kommunikationsaufbaus immer ausgehend von der Quellen-TKÜ-Software über den eingesetzten Proxyserver zum Kompetenzzentrum TKÜ-Bayern des BLKA. Eine Kontaktaufnahme zur Quellen-TKÜ-Maßnahme ist erst durch Annahme dieses Kommunikationsaufbaus und nur von der in der Quellen-TKÜ-Software als Kommunikationspartner hinterlegten IP-Adresse aus möglich (sog. lnside-Out-Kommunikation). Eine Kommunikation mit der Quellen-TKÜ-Software von einer anderen als der in der Quellen-TKÜ-Software festgelegten IP-Adresse ist nicht möglich. Die Ausleitung/Weiterleitung der Datenströme erfolgt dabei ausschließlich verschlüsselt. Darüber hinaus ist die Quellen-TKÜ-Software mit einem elektronischen Fingerabdruck und mit Authentifizierungsprotokollen gegen unberechtigte Nutzung gesichert.

Zu 3. c):
Eine Softwareextraktion würde voraussetzen, dass eine Person vollumfängliche Kenntnisse über die Quellen-TKÜ-Software, ihren Funktionsumfang, ihre exakte Funktionsweise sowie ihre kryptografischen Schlüssel hat. Kumulierend dazu müsste diese Person eine exponierte Stellung innerhalb der Kommunikationsnetze innehaben und der Rechner identifiziert sein, auf dem die Quellen-TKÜ-Software installiert ist.

Aus vorstehenden Ausführungen wird nachvollziehbar, dass durch das BLKA in Form umfangreicher technischer Sicherungsmaßnahmen und Kontrollmechanismen dafür Sorge getragen wurde, die Wahrscheinlichkeit einer „Zweckentfremdung“ bzw. „Extraktion“ der Quellen-TKÜ-Software auf ein Mindestmaß zu begrenzen. Darüber hinaus unterliegen diese Sicherungsmaßnahmen einem ständigen Qualitätssicherungs- und Optimierungsprozess.

Zu 4.:
Das BLKA hat weder im gegenständlichen noch in anderen Ermittlungsverfahren Software zur Quellen-TKÜ entwickelt. Mit anderen Bundesländern und dem Bund erfolgte ein fachlicher Informationsaustausch zur Quellen-TKÜ. Anlassbezogen erfolgte beim Einsatz einer Quellen-TKÜ-Software eine Zusammenarbeit mit der auftraggebenden Dienststelle in Fällen der Amtshilfe.

Zu 5. a):
Die im gegenständlichen Fall bzw. Ermittlungsverfahren eingesetzte Software wurde nicht weiter zur Verfügung gestellt (vgl. Ausführungen zu den Fragen 1 und 2).

Zu 5. b):
Das BLKA hat die in Rede stehende Software weder an das Bayerische Landesamt für Verfassungsschutz noch an andere Landesämter für Verfassungsschutz weitergegeben.

Zu 5. c):
Nachdem die in der Schriftlichen Anfrage angesprochene konkrete Software vom BLKA nicht an das Landesamt für Verfassungsschutz weitergegeben wurde, hat das Landesamt für Verfassungsschutz diese auch nicht benutzt. Unabhängig hiervon wird darauf hingewiesen, dass im Aufgabenbereich des Landesamtes für Verfassungsschutz insgesamt in drei Fällen des islamistischen Terrorismus Maßnahmen der Quellen-TKÜ beantragt und von der G10-Kommission des Bayerischen Landtags gebilligt wurden. 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 6. a):
Die Zertifizierung bezeichnet ein Verfahren, mit dessen Hilfe die Einhaltung bestimmter Anforderungen nachgewiesen wird. Für die Quellen-TKÜ-Software bestehen keine spezifischen Zertifizierungs-Vorgaben. Seitens des BLKA wird durch umfangreiche technische, der Einbringung auf das Zielsystem vorgeschaltete Funktionsprüfungen im Rahmen eines Qualitätssicherungsprozesses (Sicherheitsaudit) in jedem Einzelfall geprüft, sichergestellt und protokolliert, dass der Funktionsumfang der Quellen-TKÜ-Software den rechtlichen Vorgaben und insbesondere dem der Maßnahme zugrunde liegenden richterlichen Beschluss entspricht.

Durch den digitalen Fingerabdruck erfährt jede einzelne Softwarelösung eine „Zertifizierung“. Die Auditierung erfolgte durch Diplom-Ingenieure (Fachrichtung Kommunikationstechnik, Informatik, Nachrichtentechnik) des Kompetenzzentrums Telekommunikationsüberwachung Bayern des BLKA.

Zu 6. b):
Das BVerfG hat in seiner Entscheidung zur Onlinedurchsuchung (Urteil vom 27.02.2008 - 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 die 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 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.

Onlinedurchsuchung und Quellen-TKÜ verfolgen damit völlig unterschiedliche Ziele: Geht es mit der Quellen-TKÜ allein darum, zielgerichtet eine bei Nutzung herkömmlicher Übermittlungsformen überwachbare Kommunikation des Beschuldigten aufzuzeichnen, soll mit der Onlinedurchsuchung auf das komplette Speichermedium des Zielsystems zugegriffen werden und dieses nach beweisrelevanten Dateien durchsucht werden.

Die Einhaltung dieser verfassungsrechtlichen Vorgaben wird durch die Anordnung des zuständigen Ermittlungsrichters am Amtsgericht gewährleistet, der auf Antrag der Staatsanwaltschaft mit seinem Beschluss im konkreten Verfahren den rechtlichen Rahmen für die Umsetzung der Überwachungsmaßnahme in Form der Quellen-TKÜ vorgibt.

Zudem wird bei der Umsetzung der Anordnungen durch das BLKA sowohl durch technische Vorkehrungen als auch durch weitere Kontrollmechanismen sichergestellt, dass die verfassungsrechtlichen Vorgaben und die den richterlichen Anordnungsbeschlüssen zugrunde liegenden Beschränkungen der Funktionalitäten der Quellen-TKÜ-Software beachtet werden.

Zu 6. c):
Unmittelbar nach Bekanntwerden der durch den CCC erhobenen Vorwürfe hinsichtlich durchgeführter Quellen-TKÜ-Maßnahmen habe ich den Bayerischen Landesbeauftragten für den Datenschutz (BayLfD) am 10.10.2011 telefonisch um Prüfung aller einschlägigen Verfahren gebeten.

Seitens des BLKA werden dem BayLfD alle für die datenschutzrechtliche Überprüfung notwendigen Informationen und Daten, bezogen auf alle konkreten Maßnahmen der Quellen-TKÜ, für den von dort gewünschten Prüfzeitraum 2008 bis 2011 zur Verfügung gestellt.

Der BayLfD ist in Ausübung seines Amtes unabhängig, nur dem Gesetz unterworfen und in seinem Prüfungsumfang nicht beschränkt.