Landtag von Baden-Württemberg **Drucksache 15 / 669**

15. Wahlperiode **11. 10. 2011**

Antrag

der Fraktion der FDP/DVP

und

Stellungnahme

des Innenministeriums

Einsatz von sogenannten „Trojanern“ durch die baden-württembergischen Ermittlungsbehörden

Antrag

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. ob und wenn ja in wie vielen Fällen die baden-württembergischen Ermittlungsbehörden und das Landesamt für Verfassungsschutz in den letzten fünf Jahren technische Überwachungssoftware im Rahmen von Gefahrenabwehr und Strafverfolgung sowie im Rahmen der Tätigkeit der Verfassungsschutzämter auf Computern von Dritten ohne deren Wissen eingesetzt haben;

2. wenn ja, auf welcher Rechtsgrundlage sie das jeweils getan haben bzw. welche Rechtsgrundlagen für ein solches Vorgehen überhaupt bestehen;

3. wenn ja, wie die Software jeweils auf den Rechner der Verdachtsperson gekommen ist;

4. wie sie das diesbezügliche Vorgehen der bayerischen Sicherheitsbehörden, welches dem Urteil des Landgerichts Landshut vom 20. Januar 2011 zugrunde lag (Az: 4 Qs 346/10), nämlich das Aufspielen der Software im Zuge einer Sicherheitskontrolle am Flughafen durch die Zollbehörden unter vorgeschobenen Gründen, aus ihrer Sicht rechtlich bewertet;

5. welche Daten die Behörden im Zusammenhang mit dem Einsatz der Software jeweils erhoben haben und welche sie mit der vorhandenen Software zusätzlich hätten technisch erheben können;

Eingegangen: 11. 10. 2011 / Ausgegeben: 04. 11. 2011

6. ob sie generell eine sogenannte „Quellen-Telekommunikationsüberwachung“ für von § 100 a Strafprozessordnung gedeckt ansieht und wie bei einer solchen technisch sichergestellt wird, dass lediglich „Telekommunikation“ überwacht wird, nicht aber weitere Daten auf dem Computer des Betroffenen ausgespäht werden (z. B. durch getaktetes Erstellen von „Screenshots“, Fernsteuerung einer „Webcam“ etc.);

7. ob die baden-württembergischen Ermittlungs- und/oder Verfassungsschutzbehörden eine solche Überwachungssoftware in ihrem Besitz haben, die zur Durchführung einer „Quellen-TKÜ“ und/oder einer Online-Durchsuchung geeignet ist (und falls ja, mit Angabe der Anzahl der Varianten, der Kooperationen mit anderen Bundesländern zur Verwendung der Software und der Ersteller der Software);

8. falls eine eigene Überwachungssoftware nicht vorgehalten wird: ob es Kooperationsvereinbarungen oder andere Abreden mit anderen Bundesländern oder dem Bund gibt, nach denen entsprechende technische Maßnahmen dort angefordert oder angeregt und deren Ergebnisse an das Land mitgeteilt werden können und ob solche Daten bereits für Verfahren in Baden-Württemberg Verwendung gefunden haben;

9. wie sie rechtlich die möglichen Sicherheitslücken einschätzt, die durch eine private Erstellung eines solchen Trojaners im Auftrag von Ermittlungsbehörden bestehen und ob technisch für die Ermittlungsbehörden auszuschließen ist, dass durch entsprechende Gestaltung der Software gesammelte Daten auch an Dritte gelangen können.

11. 10. 2011

Dr. Rülke, Dr. Goll

und Fraktion

Begründung

Nach aktuellen Diskussionen über den Einsatz von „Bundestrojanern“ stellt sich die Frage, wie die Landesregierung die Situation in Baden-Württemberg bezüglich des Einsatzes solcher Software bewertet. Die Behörden des Landes dürfen sich nicht über rechtliche Rahmenbedingungen hinwegsetzen – nicht im präventiven Bereich und erst recht nicht im repressiven Bereich.

In Bayern liegt durch das Landgericht Landshut bereits eine gerichtliche Entscheidung darüber vor, dass das Erstellen eines „Screenshots“, also eines Bildschirmfotos in kleinen Abständen und eine Übertragung an die Ermittlungsbehörden nicht von der Regelung des § 100 a StPO gedeckt ist.

Es wird erwartet, dass die Landesregierung diese Rechtsauffassung teilt und alles dafür tut, dass sich Ermittlungsbehörden und das Landesamt für Verfassungsschutz an die bestehenden rechtlichen Rahmenbedingungen halten!

Stellungnahme

Mit Schreiben vom 2. November 2011 Nr. 3–0531.4/201.5 nimmt das Innenministerium in Abstimmung mit dem Justizministerium zu dem Antrag wie folgt Stellung:

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. ob und wenn ja in wie vielen Fällen die baden-württembergischen Ermittlungsbehörden und das Landesamt für Verfassungsschutz in den letzten fünf Jahren technische Überwachungssoftware im Rahmen von Gefahrenabwehr und Strafverfolgung sowie im Rahmen der Tätigkeit der Verfassungsschutzämter auf Computern von Dritten ohne deren Wissen eingesetzt haben;

Zu 1.:

Baden-württembergische Polizeidienststellen haben bislang in vier Ermittlungsverfahren vier Maßnahmen zur Gewährleistung einer sogenannten Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) umgesetzt. In einem weiteren Ermittlungsverfahren erfolgte die Umsetzung für eine baden-württembergische Staatsanwaltschaft durch eine Bundesbehörde.

Zu Maßnahmen des Landesamts für Verfassungsschutz kann aus operativen Geheimhaltungsgründen keine öffentliche Stellungnahme abgegeben werden.

2. wenn ja, auf welcher Rechtsgrundlage sie das jeweils getan haben bzw. welche Rechtsgrundlagen für ein solches Vorgehen überhaupt bestehen;

Zu 2.:

Die polizeilichen Maßnahmen erfolgten im Rahmen von strafprozessualen Ermittlungsverfahren auf Grundlage richterlicher Anordnungen nach §§ 100 a, 100 b der Strafprozessordnung (StPO).

Für das Landesamt für Verfassungsschutz besteht eine Rechtsgrundlage für die Telekommunikationsüberwachung im Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10). § 1 G 10 erlaubt den Nachrichtendiensten „die Telekommunikation zu überwachen und aufzuzeichnen“. Die Maßnahmen setzen voraus, dass tatsächliche Anhaltspunkte für bestimmte Straftaten vorliegen. Das Verfahren ist im Artikel 10-Gesetz detailliert geregelt und unterliegt der Kontrolle der vom Landtag eingesetzten G 10-Kommission.

Weitere Rechtsgrundlagen, insbesondere im baden-württembergischen Polizeigesetz, bestehen nicht.

3. wenn ja, wie die Software jeweils auf den Rechner der Verdachtsperson gekommen ist;

Zu 3.:

Zu Einzelheiten des polizeitaktischen sowie des operativen Vorgehens kann aus Geheimhaltungsgründen öffentlich keine Stellungnahme abgegeben werden.

4. wie sie das diesbezügliche Vorgehen der bayerischen Sicherheitsbehörden, welches dem Urteil des Landgerichts Landshut vom 20. Januar 2011 zugrunde lag (Az.: 4 Qs 346/10), nämlich das Aufspielen der Software im Zuge einer Sicherheitskontrolle am Flughafen durch die Zollbehörden unter vorgeschobenen Gründen, aus ihrer Sicht rechtlich bewertet;

Zu 4.:

Der Landesregierung sind die konkreten Einzelheiten des dem genannten Urteil zugrunde liegenden Sachverhalts nicht bekannt. Unabhängig davon besteht aus Sicht der Landesregierung keine Veranlassung, das Vorgehen der bayerischen Sicherheitsbehörden in einem konkreten Einzelfall rechtlich zu bewerten. Dies fällt in den Zuständigkeitsbereich der bayerischen Justiz.

5. welche Daten die Behörden im Zusammenhang mit dem Einsatz der Software jeweils erhoben haben und welche sie mit der vorhandenen Software zusätzlich hätten technisch erheben können;

Zu 5.:

Die eingesetzte Software gewährleistete die Überwachung der verschlüsselt geführten Kommunikation im Rahmen der jeweils richterlich angeordneten Telekommunikationsüberwachung. Hierbei kam es zur Übertragung von Internet-Telefonie. Darüber hinaus hätte die Software auch den über die überwachten Kommunikationsprogramme geführten Chat-, SMS- und Datenverkehr erheben können. Zudem wurden von der Software Statusmeldungen zur Einsatzbereitschaft des Systems und technische Daten zum Kommunikationsvorgang (IP-Adresse des Zielsystems, Zeitpunkt von Beginn und Ende des Kommunikationsvorgangs, Kennung des Gesprächspartners) übermittelt.

Weitere Daten hätten durch die Strafverfolgungsbehörden technisch nicht erhoben werden können.

6. ob sie generell eine sogenannte „Quellen-Telekommunikationsüberwachung“ für von § 100 a Strafprozessordnung gedeckt ansieht und wie bei einer solchen technisch sichergestellt wird, dass lediglich „Telekommunikation“ überwacht wird, nicht aber weitere Daten auf dem Computer des Betroffenen ausgespäht werden (z. B. durch getaktetes Erstellen von „Screenshots“, Fernsteuerung einer „Webcam“ etc.);

Zu 6.:

Die Landesregierung geht in Übereinstimmung mit der herrschenden Meinung in Rechtsprechung und Literatur von der Zulässigkeit der Quellen-TKÜ aus. Es handelt sich dabei um eine Telekommunikationsüberwachung, sodass auf §§ 100 a, 100 b StPO sowie §§ 1, 3, 9 und 10 G 10 als Rechtsgrundlage zurückgegriffen werden kann. Auch das Bundesverfassungsgericht geht in seiner Entscheidung vom 27. Februar 2008 – 1 BvR 370/07, 1 BvR 595/07 – von der grundsätzlichen Zulässigkeit der Quellen-TKÜ aus, sofern durch technische Vorkehrungen sowie durch rechtliche Vorgaben sichergestellt ist, dass sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt.

Vom Landeskriminalamt werden die Funktionalitäten der beauftragten Software in jedem Einzelfall vor dem tatsächlichen Einsatz in einer Testumgebung auf die Konformität zur richterlich angeordneten Überwachung überprüft und gegebenenfalls eine Anpassung veranlasst.

7. ob die baden-württembergischen Ermittlungs- und/oder Verfassungsschutzbehörden eine solche Überwachungssoftware in ihrem Besitz haben, die zur Durchführung einer „Quellen-TKÜ“ und/oder einer Online-Durchsuchung geeignet ist (und falls ja, mit Angabe der Anzahl der Varianten, der Kooperationen mit anderen Bundesländern zur Verwendung der Software und der Ersteller der Software);

8. falls eine eigene Überwachungssoftware nicht vorgehalten wird: ob es Kooperationsvereinbarungen oder andere Abreden mit anderen Bundesländern oder dem Bund gibt, nach denen entsprechende technische Maßnahmen dort angefordert oder angeregt und deren Ergebnisse an das Land mitgeteilt werden können und ob solche Daten bereits für Verfahren in Baden-Württemberg Verwendung gefunden haben;

Zu 7. und 8.:

Das Landeskriminalamt hat in allen Fällen bei einem externen Anbieter (Firma DigiTask GmbH) spezifisch programmierte Software für die Durchführung von Maßnahmen der Quellen-TKÜ angemietet. Insgesamt wurden neun Software-Varianten erstellt.

Im Bereich der Telekommunikationsüberwachung besteht eine Kooperationsvereinbarung mit Bayern, in deren Rahmen in zwei Fällen auf von Bayern angemietete Hardware (Proxy-Server) zurückgegriffen wurde. Die Kooperation hat sich nicht auf die gemeinsame Nutzung von Software erstreckt.

Das Landesamt für Verfassungsschutz hat eine solche Überwachungssoftware nicht in seinem Besitz und ist im Einsatzfall auf einen externen Anbieter angewiesen.

Für Maßnahmen der sogenannten Online-Durchsuchung besteht für baden-württembergische Ermittlungsbehörden und den Verfassungsschutz keine Rechtsgrundlage. Entsprechende Software wurde daher auch nicht beauftragt.

9. wie sie rechtlich die möglichen Sicherheitslücken einschätzt, die durch eine private Erstellung eines solchen Trojaners im Auftrag von Ermittlungsbehörden bestehen und ob technisch für die Ermittlungsbehörden auszuschließen ist, dass durch entsprechende Gestaltung der Software gesammelte Daten auch an Dritte gelangen können.

Zu 9.:

Die Zusammenarbeit zwischen dem Landeskriminalamt und der Firma DigiTask GmbH wurde in einer Vereinbarung zur Auftragsdatenverarbeitung nach § 7 des Landesdatenschutzgesetzes geregelt. Bei der Firma handelt es sich um einen spezialisierten Anbieter, der in die Geheimschutzbetreuung des Bundesministeriums für Wirtschaft und Technologie aufgenommen wurde. Die Mitarbeiter der Firma sind sicherheitsüberprüft.

Zur technischen Komponente wird auf die Ausführungen zu 5. und 6. verwiesen. Die Überwachungssoftware leitet die Daten aus dem Zielsystem per Advanced Encyption Standard (AES)-Verschlüsselung an das Aufnahmesystem des Landeskriminalamts weiter. Damit ist eine Kenntnisnahme durch Dritte mit legalen Mitteln ausgeschlossen.

In Vertretung

Dr. Zinell

Ministerialdirektor