Prüfbericht zum „Staatstrojaner“

Der BayLfD hat am 02.08.2012 seinen Prüfbericht Quellen-TKÜ vorgestellt. Anlass für die Prüfung war die Analyse eines „Staatstrojaners“ durch den Chaos Computer Club (CCC) im Herbst 2011, wonach der Trojaner nicht nur höchst intime Daten ausleiten konnte, sondern auch eine Fernsteuerungsfunktion zum Nachladen und Ausführen beliebiger weiterer Software bot. Der untersuchte Staatstrojaner wurde später einem bayerischen Ermittlungsverfahren zugeordnet. Unabhängig von einer möglichen Überprüfung von Amts wegen hatte der bayerische Staatsminister des Innern deshalb den BayLfD gebeten, die Umsetzung der bayerischen Maßnahmen zur Quellen-TKÜ zu überprüfen. Der BayLfD kontrollierte alle 23 Maßnahmen der Quellen-TKÜ, die die bayerischen Ermittlungsbehörden in dem Zeitraum vom 01.01.2008 bis 31.12.2011 durchgeführt hatten und die sämtlich der Strafverfolgung dienten. Gemäß dem jetzt vorgelegten Prüfbericht Quellen-TKÜ lagen zu allen Maßnahmen richterliche Anordnungen vor.

Dem Bericht zufolge hätte die verwendete Software beispielsweise mithilfe ihrer Nachladefunktion unzulässige Datenerhebungen ermöglichen können. Anhaltspunkte dafür, dass bei den Maßnahmen tatsächlich Zugriffe auf Mikrofone bzw. Kameras erfolgten oder Keylogger zum Einsatz gekommen waren, ergaben sich zwar nicht. Der BayLfD teilte aber insoweit die Auffassung des CCC, wonach nur die Einsichtnahme in den Quelltext der Überwachungssoftware zuverlässig verdeckte überschießende Funktionalitäten hätte ausschließen können. Hinsichtlich der technischen Durchführung der Maßnahmen im Übrigen ergab sich eine ganze Reihe von Mängeln im Detail.

In rechtlicher Hinsicht verdeutlicht der Bericht, dass die Abgrenzung der Quellen-TKÜ von der Online-Durchsuchung in der Vollzugspraxis mit großen Schwierigkeiten verbunden ist. Eine Quellen-TKÜ kann nur angenommen werden, wenn die Sicherheitsbehörden aus dem infiltrierten IT-System ausschließlich Daten erheben, die einem laufenden Telekommunikationsvorgang entnommen sind. Dies ist durch technische Vorkehrungen und rechtliche Vorgaben sicherzustellen (vgl. BVerfGE 120, S. 274, 309). Insoweit bewegten sich einige Vorgehensweisen der Ermittlungsbehörden laut Aussage des BayLfD in der Pressekonferenz „im tiefdunklen Graubereich“. Das betraf zunächst die Ausleitung von Applicationshots, wie sie in einigen Fällen durchgeführt wurden. Eine dieser Maßnahmen war von dem LG Landshut für rechtswidrig erklärt worden – diese Entscheidung ist jedoch noch nicht rechtskräftig (vgl. LG Landshut, B.v.20.01.2011 – 4 Qs 346/10). Insoweit konnte der BayLfD aus kompetenzrechtlichen Gründen keine abschließende Bewertung treffen, weil er sowohl gerichtliche Entscheidungen als auch laufende Strafverfahren nicht kontrollieren darf. In Bezug auf neun Maßnahmen stellte der BayLfD fest, dass die Strafverfolgungsbehörden auf den IT-Systemen befindliche Softwarelisten ausgelesen hatten um sicherzugehen, die richtigen Zielrechner infiltriert zu haben. Die Auslesung von Softwarelisten war jedoch rechtswidrig erfolgt, weil diese Daten nicht einer laufenden Telekommunikation entnommen waren. In zwei Fällen hatten die Gerichte eine Durchsuchung angeordnet, um das Aufbringen des Trojaners zu ermöglichen. Auch die Anordnung dieser Begleitmaßnahmen konnte der BayLfD aus Kompetenzgründen nicht rechtlich bewerten, er wies jedoch sinngemäß darauf hin, dass derartige Begleitmaßnahmen im Hinblick auf die Beeinträchtigung des Grundrechts auf Unverletzlichkeit der Wohnung aus Art. 13 GG zumindest in Bezug auf die hier nicht zu bewertende polizeiliche Gefahrenabwehr unzulässig gewesen wären.

Die Feststellungen des Prüfberichts unterstreichen insbesondere folgenden gesetzlichen Regelungsbedarf:

- Sofern Begleitmaßnahmen (z.B. das Auslesen von Softwarelisten zur Vorbereitung der Installation der Software) als notwendig angesehen werden, müssen auch die Art und Weise ihrer Durchführung gesetzlich eindeutig geregelt werden.
- Die Quellen-TKÜ ist durch klare Vorgaben von der Online-Durchsuchung abzugrenzen. Hierbei ist insbesondere die Problematik der Überwachung von Texten außerhalb einer laufenden Telekommunikation zu klären (z.B. Überwachung noch nicht abgesandter E-Mail-Entwürfe).
- Gesetzliche Bestimmungen zur Quellen-TKÜ sind aufgrund ihrer erhöhten Eingriffsintensität in ihren Voraussetzungen enger als die derzeitigen Bestimmungen zur konventionellen Telekommunikationsüberwachung zu fassen.
- Geboten sind weiterhin Regelungen, die technisch und organisatorisch unzulässige Überwachungsfunktionalitäten unterbinden und eine effektive Kontrolle ermöglichen (z.B. Begrenzung von Nachladefunktionen, Möglichkeit einer Einsichtnahme in den Quelltext der Überwachungssoftware).
- Klargestellt werden sollte weiterhin, dass Betroffene nicht nur über die Telekommunikationsüberwachung als solche, sondern auch über den erfolgten Eingriff in ihr IT-System nachträglich zu unterrichten sind.

Dr. Petri kam zu dem Fazit: „Strafverfolgungsbehörden und Gesetzgeber müssen nachbessern! Ich erwarte, dass die bayerischen Strafverfolgungsbehörden die festgestellten Mängel beheben. Vor allem aber müssen die gesetzlichen Voraussetzungen der Quellen-TKÜ präziser geregelt werden. Im Vergleich zur Überwachung beispielsweise eines Festnetz-Telefongesprächs beinhaltet die Quellen-TKÜ zusätzlich einen Eingriff in die Integrität eines PCs, Notebooks oder sonstigen IT-Systems des Betroffenen. Soweit politisch an der Quellen-TKÜ zur Strafverfolgung und zur Gefahrenabwehr festgehalten wird, empfehle ich den Gesetzgebern in Bund und Bayern dringend, Bestimmungen zu schaffen, die der erhöhten Eingriffsintensität und den technischen Besonderheiten der Quellen-TKÜ gerecht werden.“

Diese Forderungen des BayLfD unterstreichen die Forderungen der Konferenz der Daten-schutzbeauftragten des Bundes und der Länder in einer Entschließung vom 16./17. März 2011 „Ohne gesetzliche Grundlage keine Telekommunikationsüberwachung auf Endgeräten“[1].

Bayerischer Landesbeauftragter für den Datenschutz
Dr. Thomas Petri

1 DuD Heft 5, 2011, S. 355