Der Bayerische Landesbeauftragte für den Datenschutz

Prüfbericht Quellen-TKÜ

30.07.2012

Hausanschrift
Wagmüllerstr. 18
80538 München

Postanschrift
Postfach 221219
80502 München

Tel. 089 . 21 26 72 - 0
Fax 089 . 21 26 72 - 50

www.datenschutz-bayern.de
E-Mail: poststelle@
datenschutz-bayern.de

Inhaltsverzeichnis

1 Zusammenfassende Feststellungen und Bewertungen

1. In dem Zeitraum vom 01.01.2008 bis zum 31.12.2011 führten bayerische Strafverfolgungsbehörden 23 Maßnahmen der sogenannten Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) durch. Zu allen Maßnahmen lagen richterliche Anordnungen vor. Zu Zwecken der Gefahrenabwehr wurden für den überprüften Zeitraum keine Maßnahmen festgestellt.

2. In tatsächlicher Hinsicht hat die Prüfung bestätigt, dass die gegenwärtigen strafprozessualen Befugnisnormen auf die konventionelle TKÜ ausgerichtet sind. Sofern an der Notwendigkeit der Quellen-TKÜ festgehalten wird, ist die Verabschiedung von weiteren Vorschriften zu empfehlen, die den Besonderheiten der Quellen-TKÜ besser gerecht werden (Abschnitte 5.2.1 und 5.2.2). Vergleichbares gilt für die Quellen-TKÜ im Rahmen der Gefahrenabwehr.

3. Zur Durchführung der Maßnahmen verwendete das Bayerische Landeskriminalamt (BLKA) durchweg Software des Unternehmens DigiTask. Dabei unterstützte das Unternehmen die Einrichtung einer Überwachungskonsole beim BLKA und lieferte je Einzelmaßnahme die Überwachungssoftware („Trojaner“), die vom BLKA anschließend auf den jeweiligen Zielrechnern eingebracht wurde. Im Zusammenhang mit der jeweiligen Auftragserteilung konnten die Geschehensabläufe dabei mangels hinreichender Dokumentation beim BLKA nicht vollständig nachvollzogen werden. Im Hinblick auf die Eingriffsintensität der Maßnahmen sind derartige Dokumentationsdefizite als Datenschutzverstöße anzusehen (Abschnitt 4.2.1).

4. Die Aufträge an DigiTask waren in mehrfacher Hinsicht mängelbehaftet. So wäre es etwa angezeigt gewesen, DigiTask vertraglich ausdrücklich zu verpflichten, keine überschießenden Überwachungsfunktionalitäten zu liefern und die Möglichkeit einer Einsichtnahme in den Quellcode vorzusehen (Abschnitte 4.2.1 und 4.2.2). Überdies fehlte die gebotene Regelung zur Verpflichtung des privaten Wartungspersonals auf das Datengeheimnis und nach dem Verpflichtungsgesetz (Abschnitt 4.6.9).

5. Nach der Lieferung von Überwachungssoftware führte das BLKA jeweils Funktions- und Abnahmetests durch. Dabei ist es datenschutzrechtlich nicht zu beanstanden, dass das BLKA nicht in jedem Fall hierzu Einsicht in den jeweiligen

Quellcode der Software genommen hat. Eine Einsichtnahme in den Quellcode sollte allerdings stichprobenartig erfolgen, um zuverlässig verdeckte Funktionalitäten auszuschließen (Abschnitt 4.2.2).

6. Was die Einbringung der Überwachungssoftware auf den Zielrechnern anbelangt, hat das BLKA - soweit nachvollziehbar - die datenschutzrechtlich gebotenen Sorgfaltspflichten beachtet, um sicherzustellen, dass nur die von einer richterlichen Anordnung umfassten Zielrechner infiltriert wurden (Abschnitt 4.3.1).

7. Hinsichtlich der Funktionsweise der Überwachungssoftware konnte ich feststellen, dass das BLKA bemüht war, die Beeinträchtigung der Stabilität des jeweils überwachten IT-Systems so gering wie möglich zu gestalten (Abschnitt 4.4.1).

8. Bei den zwanzig insoweit überprüften Maßnahmen konnten in vier Maßnahmen Aufzeichnungen von Anwendungsfensterinhalten (Applicationshots) von Browsern durchgeführt werden, in zwei weiteren Maßnahmen konnten nur Applicationshots von Instant Messengern gefertigt werden. In zwei weiteren, noch nicht abgeschlossenen, Maßnahmen habe ich anhand meiner in meinem Haus aufgebauten Testumgebung festgestellt, dass die Software nicht nur die Übertragung eines Browserfensters, sondern auch eines gesamten Bildschirms ermöglicht. Da es mir lediglich möglich war, die einzelnen Binärdateien zu testen, kann ich insoweit keine Aussage treffen, ob das BLKA von der Funktion tatsächlich Gebrauch gemacht hat, komplette Screenshots aufzuzeichnen (Abschnitt 4.4.2.1).

9. Unabhängig von der rechtlichen Frage, ob Applicationshots einer laufenden Telekommunikation entnommen sind und damit nach gegenwärtiger Gesetzeslage im Grundsatz zulässig sein können, sollte die Frage durch den jeweiligen Gesetzgeber geklärt werden. Denn die Fertigung von Applicationshots ist sowohl aus sicherheitsbehördlicher Perspektive als auch aus grundrechtlicher Sicht von hoher Relevanz (Abschnitt 5.2).

10. Soweit überprüfbar enthielt die Überwachungssoftware keine zuverlässige technische Begrenzung auf bestimmte Überwachungsfunktionen. Eine solche Funktionsbeschränkung wäre aus datenschutzrechtlicher Sicht nicht nur über die Beschränkung der Benutzeroberfläche der Überwachungskonsole geboten gewesen. Unabhängig hiervon habe ich im Rahmen meiner Prüfung keine Anhaltspunkte dafür gefunden, dass das BLKA (mit Ausnahme der Deinstallation

in einem Fall) von derartigen Funktionen Gebrauch gemacht hätte (Abschnitt 4.4.2.5).

11. Das BLKA hat die Überwachungssoftware nicht nach einem bestimmten Zeitpunkt automatisch deinstalliert. Dementsprechend war eine erfolgreiche Deinstallation davon abhängig, dass der bei der Überwachung verwendete Proxy-Server in Betrieb blieb. Insbesondere bei Proxy-Servern im Ausland hätte das BLKA eine dauerhafte Verfügbarkeit sicherstellen müssen (Abschnitte 4.4.2.7 und 4.5).

12. In Bezug auf die abgeschlossenen Maßnahmen konnte die Verschlüsselung der Übertragungswege zum damaligen Zeitpunkt zu den damaligen Rahmenbedingungen noch als ausreichend angesehen werden. Zum gegenwärtigen Zeitpunkt wäre die Verschlüsselung allerdings als unzureichend anzusehen (Abschnitt 4.4.3.2).

13. Das technische Gesamtsystem der Überwachung setzt eine zuverlässige Authentisierung zwischen der Überwachungssoftware auf dem infiltrierten IT-System und der Überwachungskonsole voraus. Eine solche Zuverlässigkeit war nicht hinreichend gegeben (Abschnitt 4.4.3.3).

14. Die Überwachungskonsole wurde ohne Sicherheitsupdates betrieben, was ich zumindest als bedenklich bewerte (Abschnitt 4.6.3).

15. Die Vergabe und Verwaltung der Nutzerkennungen sowie die Sicherungsmaßnahmen der einzelnen Kennungen entsprachen nicht den üblichen und gebotenen datenschutzrechtlichen Anforderungen (Abschnitt 4.6.5).

16. Es erfolgte keine ausreichende Protokollierung auf der Überwachungskonsole (Abschnitt 4.6.6). Demgegenüber habe ich bei der Protokollierung auf der Firewall keine wesentlichen Mängel feststellen können (Abschnitt 4.6.7).

17. Konkrete Hinweise auf Maßnahmen, die den Kernbereich privater Lebensgestaltung beeinträchtigt hätten, habe ich nicht vorgefunden (Abschnitt 4.6.8).

18. Zur Vorbereitung der Quellen-TKÜ wurden diverse Begleitmaßnahmen eingesetzt: a) In neun von zwanzig geprüften Maßnahmen wurden auf dem IT-System befindliche Softwarelisten ausgelesen; insoweit ist es zumindest fraglich, ob dieser Ausleseprozess von den richterlichen Anordnungen erfasst war (Abschnitte 4.4.2.4 und 5.2.2); b) in zwei Fällen wurde durch das anordnende

Gericht eine Durchsuchung gestattet, um die Überwachungssoftware aufzubringen; eine rechtliche Bewertung ist mir insoweit verwehrt. Ich weise allerdings darauf hin, dass für den Bereich der Gefahrenabwehr eine Wohnungsbetretung als Begleitmaßnahme in vergleichbaren Fällen unzulässig wäre (Abschnitt 5.2.2).

19. Nach Abschluss einer Quellen-TKÜ ist der Betroffene des infiltrierten Gerätes regelmäßig nicht nur über Beeinträchtigungen der Vertraulichkeit eines Gesprächs, sondern auch über eine etwaige Beeinträchtigung der Integrität eines infiltrierten IT-Systems zu unterrichten. Aus den mir vorgelegten Unterlagen ergibt sich, dass die Betroffenen nicht über die Integritätsbeeinträchtigung informiert wurden (Abschnitte 5.2.1 und 6).

2 Vorbemerkungen

2.1 Prüfungsanlass

Am 08.10.2011 veröffentlichte der Chaos Computer Club (CCC) eine Pressemitteilung, wonach er die extrahierte Binärdatei einer Schadsoftware zur Durchführung einer Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) untersucht habe. Der CCC erhob den Vorwurf, die untersuchten Trojaner könnten nicht nur höchst intime Daten ausleiten, sondern böten auch eine Fernsteuerungsfunktion zum Nachladen und Ausführen beliebiger weiterer Schadsoftware. Nach seiner Einschätzung entstünden aufgrund von groben Design- und Implementierungsfehlern außerdem eklatante Sicherheitslücken in den infiltrierten Rechnern, die auch Dritte ausnutzen könnten. Im Ergebnis habe der CCC also mehrere technische Funktionalitäten festgestellt, die eine solche Software nicht haben dürfe.

Das Bayerische Staatsministerium des Innern erklärte anlässlich einer Pressekonferenz am 11.10.2011 sinngemäß, nach Erstbewertung des Bayerischen Landeskriminalamtes (BLKA) könne die dem CCC zugespielte Schadsoftware einem Ermittlungsverfahren der Bayerischen Polizei aus dem Jahr 2009 zugeordnet werden.

Unabhängig von einer mir möglichen Überprüfung von Amts wegen hat mich der Bayerische Staatsminister des Innern Joachim Herrmann gebeten, die technische Umsetzung der Maßnahmen zur Quellen-TKÜ sowie die Einhaltung der rechtlichen Vorgaben zu überprüfen. Ich werte diese Bitte als Ersuchen der Staatsregierung im Sinne des Art. 30 Abs. 6 Bayerisches Datenschutz (BayDSG).

2.2 Prüfungsumfang

Grundsätzlich ist mir gem. Art. 2 Abs. 6 BayDSG die datenschutzrechtliche Kontrolle gerichtlicher Entscheidungen - soweit es sich nicht lediglich um Verwaltungsangelegenheiten handelt - entzogen. Aufgrund dieser Vorgabe des Gesetzgebers ist mir vorliegend eine Kontrolle und Bewertung der richterlichen Anordnungen von Quellen-TKÜ-Maßnahmen nicht möglich. Sofern ich nachfolgend eine andere rechtliche Auffassung als die anordnenden Gerichte zur Rechtsgrundlage der Quellen-TKÜ vertrete, stelle ich diese in Abschnitt 5.2 allgemein dar, um das Finden datenschutzpolitischer Entschei-

dungen zu unterstützen. Abgesehen von diesen datenschutzpolitischen Empfehlungen lege ich bei meiner rechtlichen Beurteilung die richterlichen Entscheidungen zu den durchgeführten Maßnahmen zugrunde.

Weiterhin kann ich die Datenerhebungen durch Strafverfolgungsbehörden in einem laufenden Ermittlungs- bzw. Strafverfahren aufgrund von Art. 30 Abs. 4 Satz 1 BayDSG erst nach Abschluss des Verfahrens kontrollieren. Sofern diese Datenerhebungen jedoch gerichtlich überprüft wurden, ist mir eine datenschutzrechtliche Kontrolle aufgrund von Art. 30 Abs. 4 Satz 2 BayDSG verwehrt.

Etwaige Quellen-TKÜ-Maßnahmen des Bayerischen Landesamtes für Verfassungsschutz wurden von mir aufgrund Art. 30 Abs. 3 BayDSG nicht geprüft. Diese Vorschrift erlaubt mir keine datenschutzrechtliche Kontrolle in Bezug auf personenbezogene Daten, die der Kontrolle nach Art. 2 des Gesetzes zur Ausführung des Gesetzes zu Artikel 10 Grundgesetz unterliegen.

2.3 Geprüfte Fälle

Aufgrund der oben dargestellten Einschränkungen habe ich konkrete datenschutzrechtliche Prüfungen nur in den bereits abgeschlossenen Ermittlungs- und Strafverfahren durchgeführt. Von den 23 Maßnahmen, die im Zeitraum 01.01.2008 bis 31.12.2011 durch das Bayerische Landeskriminalamt (BLKA) durchgeführt wurden, sind bisher in Bezug auf 14 Maßnahmen die zugrundeliegenden Ermittlungs- bzw. Strafverfahren („Fälle“) abgeschlossen. Dabei handelt es sich um die unter 6.2 aufgeführten Verfahren bzw. Verfahrenskomplexe der Staatsanwaltschaften München I, Bayreuth, Nürnberg-Fürth, Landshut, Traunstein, Hof und Ansbach.

Ich habe dabei die Verfahren als abgeschlossen gewertet, die zum Stichtag 01.04.2012 (rechtskräftig) abgeschlossen waren. Ältere Maßnahmen als 2008 habe ich in meine Überprüfung nicht mit einbezogen, da das Bundesverfassungsgericht Anfang 2008 in seiner Entscheidung zur sog. Online-Durchsuchung, auf die ich in Abschnitt 5.1 näher eingehe, grundlegende Feststellungen u. a. zur Quellen-TKÜ gemacht hat und insofern hier aus datenschutzrechtlicher Sicht von einer gewissen Zäsur auszugehen ist.

Mit den übrigen, zum Stichtag noch nicht rechtskräftig abgeschlossenen Maßnahmen habe ich mich abstrakt auseinandergesetzt, insbesondere um Anhaltspunkte für grundsätzliche Probleme der Quellen-TKÜ zu ermitteln und aufzeigen zu können.

Präventive Quellen-TKÜ-Maßnahmen wurden im Prüfungszeitraum nicht festgestellt. Die in diesem Bericht vorgenommen Wertungen wären aber auf Maßnahmen nach dem Polizeiaufgabengesetz (PAG) inhaltlich weitgehend übertragbar.

2.4 Vorgehensweise bei der Prüfung

Im Rahmen meiner Prüfung fanden mehrere Besprechungen mit dem BLKA und dem Staatsministerium der Justiz und für Verbraucherschutz statt. In diesem Zusammenhang habe ich mir die Durchführung der Maßnahmen, sowohl in grundsätzlicher Hinsicht, wie auch bezogen auf die konkreten Einzelfälle erläutern lassen. Ich habe mir dabei auch die aktuelle Software zur Durchführung der Quellen-TKÜ und sämtliche noch beim BLKA vorhandenen Unterlagen zeigen lassen.

Die genaue Umsetzung der Maßnahmen habe ich mir zusätzlich auch schriftlich erläutern lassen. Dazu habe ich mir bezüglich sämtlicher durchgeführter Maßnahmen u.a. folgende Unterlagen vorlegen lassen:

- Software, die auf den überwachten Rechnern installiert wurde
- Software, die zur Weiterleitung der Daten (als „Proxy“) verwendet wurde
- Funktionstests der Software
- Protokolldaten
- Auftragsunterlagen
- Richterliche Anordnungen (Beschlüsse)

In den Fällen der bereits abgeschlossenen Ermittlungs- und Strafverfahren habe ich die Ermittlungs- und Strafakten eingesehen.

In diesen Fällen hat mir das BLKA auch die Binärcodes übergeben.

Des Weiteren habe ich versucht, auch den Quellcode einzusehen. Diese Einsichtnahme war mir im Ergebnis jedoch nicht möglich. Grundsätzlich war zwar seitens des Herstel-

lerunternehmens der Überwachungssoftware (Digi Task GmbH Gesellschaft für besondere Telekommunikationssysteme – nachfolgend: DigiTask) eine Einsichtnahme in den Raum gestellt worden. Jedoch hat DigiTask eine Einsichtnahme vom Abschluss einer Vertraulichkeitsvereinbarung durch meine Mitarbeiter abhängig gemacht. Ich habe gegenüber dem BLKA verdeutlicht, dass ich keine Möglichkeit sehe, eine entsprechende Vereinbarung abzuschließen. Gemäß Art. 33a Abs. 4 der Bayerischen Verfassung und Art. 30 Abs. 1 BayDSG kontrolliere ich bei den öffentlichen (bayerischen) Stellen die Einhaltung datenschutzrechtlicher Bestimmungen. Etwaige Ein- oder Beschränkungen meiner Prüfungskompetenz kommen nur auf Grund gesetzlicher Vorschriften - insbesondere solcher des BayDSG - in Betracht. Eine vertragliche Einschränkung meiner gesetzlichen Prüfkompetenz ist daher mit den Vorgaben des BayDSG nicht zu vereinbaren.

Ich habe gegenüber dem BLKA weiterhin zum Ausdruck gebracht, dass ich auch keine Erforderlichkeit für den Abschluss solcher Vereinbarungen sehe, da meine Mitarbeiter kraft Gesetzes zur Verschwiegenheit verpflichtet sind.

Trotz nachhaltiger Bemühungen des BLKA, mir eine Einsicht in den Quellcode zu ermöglichen, wurde diese mir aufgrund der dargelegten Umstände letztlich nicht ermöglicht.

3 Einleitung

3.1 Zur Notwendigkeit einer Quellen-TKÜ aus Sicht der Ermittlungsbehörden

Die Überwachung des Telekommunikationsverkehrs gehört zu den Standardermittlungsmaßnahmen bei der Aufklärung von Straftaten. Gesetzlich verankert ist sie seit 1968 in den §§ 100a, 100b der Strafprozessordnung (StPO). Aus datenschutzrechtlicher Sicht ermöglichen diese Vorschriften Grundrechtseingriffe von erheblichem Gewicht. Dies muss im Rahmen der Entscheidung über ihren Einsatz und während der Durchführung des Einsatzes berücksichtigt werden.

Bei der konventionellen Telekommunikationsüberwachung (TKÜ) wird der Telekommunikationsanbieter aufgrund einer richterlichen Anordnung aufgefordert, die im Rahmen eines laufenden Telekommunikationsvorgangs anfallenden Daten direkt an die Strafverfolgungsbehörden auszuleiten.

Bei einer internetbasierten Telekommunikation ist diese Vorgehensweise in der Regel technisch nicht zielführend. Typischerweise stehen die Ermittlungsbehörden vor dem Problem, dass keiner der beteiligten Telekommunikationsanbieter in der Lage ist, die Telekommunikationsinhalte unverschlüsselt auszuleiten. Ausgeleitete verschlüsselte Kommunikation ist indes regelmäßig nicht oder allenfalls mit nur unverhältnismäßig hohem Aufwand zu entschlüsseln. Deshalb ist eine Überwachung des Inhaltes der Telekommunikation in der Regel nur möglich, wenn die Daten vor der Verschlüsselung oder nach der Entschlüsselung erhoben und ausgeleitet werden. Hierzu ist es jedoch erforderlich, die Daten noch auf dem Telekommunikationsgerät – etwa dem PC – des Nutzers, also „an der Quelle“, abzugreifen. Zu diesem Zweck wird eine Software installiert, die diese Daten vor der Verschlüsselung bzw. nach der Entschlüsselung erfasst und an die Strafverfolgungsbehörden ausleitet.

3.2 Beteiligte

Bei einer Quellen-TKÜ Maßnahme im Rahmen eines strafrechtlichen Ermittlungsverfahrens gibt es grundsätzlich folgende Beteiligte:

3.2.1 Sachleitende Staatsanwaltschaft

Die Staatsanwaltschaft leitet das Ermittlungsverfahren grundsätzlich selbst. Sie trägt die Letztverantwortung für die Rechtmäßigkeit des Ermittlungsverfahrens. Gem. § 152 Abs. 1 Gerichtsverfassungsgesetz (GVG) ist die Staatsanwaltschaft gegenüber den sog. Ermittlungspersonen der Staatsanwaltschaft – in erster Linie den Polizeibeamten – weisungsbefugt. Insofern wird die Staatsanwaltschaft häufig auch als „Herrin des Ermittlungsverfahrens“ bezeichnet.

Die Staatsanwaltschaft hat im Zusammenhang mit einer TKÜ die Erforderlichkeit einer solchen Maßnahme und das Vorliegen der gesetzlichen Voraussetzungen zu überprüfen. Sie ist zuständig für die Beantragung einer richterlichen Anordnung beim Ermittlungsrichter (vgl. § 162 StPO). Bei besonderer Eilbedürftigkeit (Gefahr im Verzug) kann die TKÜ gem. § 100b Abs. 1 Satz 2, 3 StPO auch von der Staatsanwaltschaft angeordnet werden. Diese Anordnung tritt jedoch außer Kraft, wenn sie nicht binnen drei Tagen von einem Richter bestätigt wird.

3.2.2 Sachbearbeitende Polizeidienststelle

Gem. § 161 Abs. 1 StPO kann die Staatsanwaltschaft die Ermittlungen selbst vornehmen oder diese durch die Polizei vornehmen lassen. In der Praxis werden Ermittlungen regelmäßig von der Polizei durchgeführt, da die Polizeivollzugsbeamten aufgrund ihrer Sachkenntnisse die zur Tataufklärung erforderlichen Maßnahmen in den meisten Fällen selbständig treffen können. In schwierigen oder umfangreichen Verfahren erfolgt meistens eine besonders enge Abstimmung zwischen Staatsanwaltschaft und Polizei.

3.2.3 Ermittlungsrichter

Bestimmte grundrechtsintensive Ermittlungsmaßnahmen unterliegen einem Richtervorbehalt, d.h. sie können grundsätzlich nur von einem Richter angeordnet werden. Aufgrund des damit einhergehenden Eingriffs in den Schutzbereich des Grundrechts auf Vertraulichkeit der Telekommunikation gem. Art. 10 GG bedarf die TKÜ einer richterlichen Anordnung (bzw. Bestätigung im Eilfall).

Bei den zuständigen Amtsgerichten sind bestimmte Richter mit der Wahrnehmung von Entscheidungen im Ermittlungsverfahren betraut. Diese Ermittlungsrichter entscheiden über die Anträge der Staatsanwaltschaft durch Beschluss.

3.2.4 BLKA

Da die sachbearbeitende Polizeidienststelle in der Regel nicht über die nötige Ausstattung verfügt, um eine TKÜ oder eine Quellen-TKÜ vornehmen zu können, wird von der Staatsanwaltschaft das BLKA beauftragt, den Beschluss des Ermittlungsrichters zur Durchführung umzusetzen. Beim BLKA wurde zu diesem Zweck ein eigenes Sachgebiet eingerichtet, das über die entsprechenden personellen und sachlichen Voraussetzungen verfügt.

3.2.5 Überwachte Personen

Im Beschluss zur Durchführung einer Quellen-TKÜ legt das anordnende Gericht fest, dass für einen zu überwachenden Anschluss die über das Internet geführte Kommunikation direkt „an der Quelle“ aufgezeichnet werden soll. Aus datenschutzrechtlicher Sicht sind damit nicht nur der Inhaber des Anschlusses, sondern auch etwaige Mitbenutzer und die Gesprächspartner des zu überwachenden Anschlusses von der Maßnahme betroffen. Der Vereinfachung halber wird im Folgenden sprachlich nur auf die zu überwachenden Personen abgestellt.

3.3 Operative Vorbereitung

Der technischen Umsetzung einer Maßnahme der Quellen-TKÜ durch das BLKA ist in der Regel eine konventionelle TKÜ vorausgegangen.

Stellt eine sachbearbeitende Polizeidienstelle im Rahmen dieser Überwachung fest, dass wesentliche Inhalte der tatrelevanten Kommunikation über verschlüsselte Internetkommunikation (z. B. Chat oder Voice over IP) abgewickelt werden, so tritt diese Dienststelle mit dem BLKA in Kontakt, um gemeinsam weitere ermittlungstaktisch gebotene und technisch mögliche Folgemaßnahmen (z.B. Quellen-TKÜ) zu erörtern.

Die hierbei gewonnenen Erkenntnisse teilen die kriminalpolizeilichen Fallsachbearbeiter der jeweiligen sachleitenden Staatsanwaltschaft mit. Anschließend werden ggf. noch offene Fragestellungen zu technischen Details über die nötigen Funktionalitäten der Überwachungssoftware geklärt. Hierzu werden anlassbezogen auch gemeinsame Besprechungen initiiert.

Die sachleitende Staatsanwaltschaft beantragt daraufhin beim zuständigen Ermittlungsrichter einen entsprechenden richterlichen Beschluss. Der durch das Gericht erlassene Beschluss wird über die sachbearbeitende Polizeidienststelle anschließend dem BLKA zur technischen Umsetzung zugeleitet.

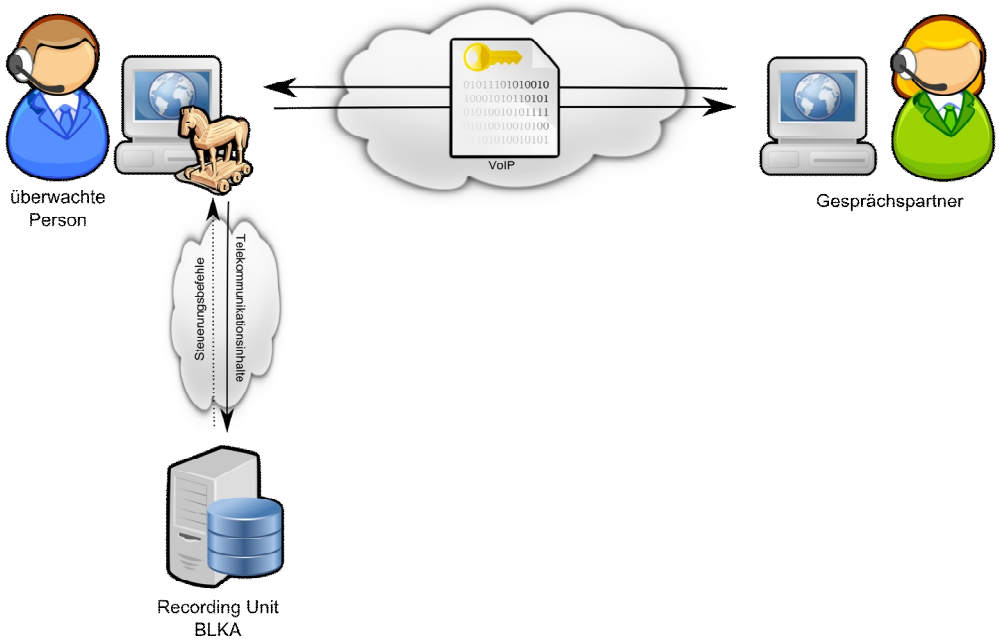
4 Technische Umsetzung der Maßnahmen

4.1 Übersicht

Wie bereits unter Abschnitt 3 beschrieben, ist es zur Überwachung einer sicher verschlüsselten Internetkommunikation notwendig, diese bereits vor der Verschlüsselung oder nach der Entschlüsselung aufzuzeichnen.

Während die überwachte Person direkt mit ihrem Gesprächspartner kommuniziert, wird versucht, möglichst verdeckt die Telekommunikationsdaten vor der Verschlüsselung an den Überwacher (das BLKA) auszuleiten. Dies geschieht mit Hilfe einer verdeckt arbeitenden Software, der „Remote Capture Unit“ („Trojaner“), auf dem Gerät der überwachten Person.

Im BLKA werden diese Daten dann in der sogenannten „Recording Unit“ aufgezeichnet.



4.1.1 Überwachungssoftware (RCU)

Die „Remote Capture Unit“ (RCU) besteht aus einem oder mehreren Programmen, die auf dem Rechner der zu überwachenden Person ohne deren Wissen installiert werden und die unbemerkt die noch unverschlüsselten Telekommunikationsdaten der über-

wachten Person und die bereits wieder entschlüsselten Telekommunikationsdaten des Gesprächspartners kopieren und möglichst unbemerkt an das BLKA senden.

Der Begriff RCU entspricht dem häufig verwendeten, aber hier nicht vollständig passenden Begriff „Trojaner“. Wenn man bei einer Quellen-TKÜ von einem „Trojaner“ sprechen möchte, dann würde die RCU die „Schadfunktion“ des Trojaners darstellen.

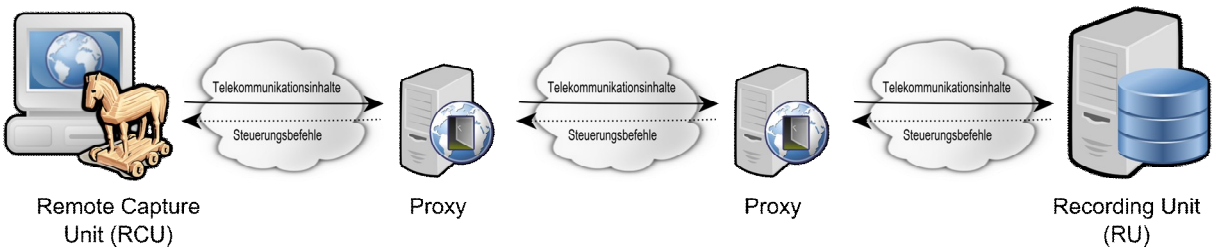
Die RCU sendet Daten an und erhält Befehle von der Überwachungskonsole (RU).

4.1.2 Überwachungskonsole (RU)

Die „Recording Unit“ (RU) ist das Gegenstück zur RCU. Sie besteht aus einem Rechner beim BLKA, der Software zum Aufzeichnen und Abrufen der ausgeleiteten Daten und zum Steuern der RCUs enthält. Eine RU kann für mehrere RCUs verwendet werden.

4.1.3 Proxy-Server

Der Datenaustausch zwischen RU und RCU erfolgt nicht direkt, sondern über eine oder mehrere vermittelnde Zwischenstationen, sogenannte *Proxy-Server*. Ein Quellen-TKÜ-Proxy ist ein Server im Internet, der Daten entgegennimmt und unverändert weiterleitet (siehe Abschnitt 4.5).



4.2 Softwarebereitstellung

Das BLKA bereitet die Quellen-TKÜ vor, in dem es die bereits aus der bestehenden konventionellen TKÜ gewonnenen Daten nutzt, um die installierten Softwarekomponenten der Rechner der überwachten Person herauszufinden. Anhand dieser Ergebnisse und der Vorgaben des jeweiligen Anordnungsbeschlusses beauftragt das BLKA die Erstellung einer maßgefertigten Software (RCU) bei einem externen Unternehmen.

4.2.1 Auftragserteilung zur Softwareerstellung

Bei allen geprüften Maßnahmen kam Software von DigiTask zum Einsatz.

Die bei der konventionellen TKÜ gewonnenen Systemparameter und die für die Quellen-TKÜ benötigten Überwachungsfunktionen werden in der Regel per verschlüsselter E-Mail an DigiTask übermittelt. In Abstimmung mit dem BLKA wird von DigiTask daraufhin eine speziell angepasste Software (RCU) angefertigt.

Dabei ist zwischen der individuell zusammengestellten Software (RCU) für den Rechner der zu überwachenden Person und der für alle Maßnahmen identischen Überwachungskonsole (RU) zur Aufzeichnung der gewonnenen Daten zu unterscheiden. Bei der RCU handelt es sich um Individualsoftware, bei der RU um Standardsoftware.

Die Dokumentation der an den Hersteller übersandten Systemparameter und der bestellten Funktionalität erfolgt elektronisch ohne weitere Vorkehrungen zur Sicherung der Authentizität (etwa elektronische Signatur). Es ist nicht erkennbar, welcher Ermittler die Übermittlung veranlasst hat und dafür gegebenenfalls auch inhaltlich die Verantwortung trägt.

Zur Prüfung wurden die als E-Mail-Anhang vom BLKA an DigiTask übersendeten Dokumente vorgelegt. Da die zugehörigen E-Mails nicht gespeichert wurden, konnte nicht mehr festgestellt werden, wie genau, ob und wann diese versandt wurden – selbst wenn sich im Rahmen der Prüfung keine Hinweise fanden, die die Authentizität der vorgelegten E-Mail-Anhänge in Frage gestellt hätten.

Die vorgelegten Verträge für die Standardsoftware zwischen DigiTask und dem BLKA enthielten keine detaillierten Funktionsbeschreibungen zu den einzelnen Softwarebestellungen, sondern legten im Wesentlichen nur die monatlichen Kosten für die Überlassung der (allgemein beschriebenen) Software fest.

Die für jede Maßnahme individuell bestellte Funktionalität stellt soweit für mich erkennbar lediglich eine Mindestfunktionalität dar, schließt aber nicht ausdrücklich und nachvollziehbar alle weiteren Überwachungsfunktionen aus. So könnte das Softwarepaket des Herstellers unter anderem durchaus auch Tastaturanschläge oder Kamerabilder

überwachen. Es ist aus den Dokumenten nicht ersichtlich, welche Funktionalitäten immer automatisch in der RCU eingebaut sind und somit implizit bestellt werden.

Zusammengefasst konnten die Geschehensabläufe mangels hinreichender Dokumentation nicht umfassend nachvollzogen werden. Im Hinblick auf die Eingriffsintensität sind derartige Dokumentationsdefizite aus datenschutzrechtlicher Sicht als Verstöße gegen § 9 BDSG bzw. Art. 7 BayDSG anzusehen.

Auch wäre es angezeigt gewesen, den Hersteller vertraglich ausdrücklich dazu zu verpflichten, dass keine überschießenden, nicht in Auftrag gegebenen, Überwachungsmöglichkeiten geliefert werden (siehe hierzu auch 4.4.2.8).

4.2.2 Funktions- und Abnahmetest

Nach der Lieferung der RCU wurde diese vom BLKA auf einem, dem zu überwachendem Rechner möglichst nahekommenden, Testsystem installiert und auf die gewünschte Funktionalität hin getestet. Zu allen Maßnahmen wurden mir die Testprotokolle übergeben.

Die Testprotokolle enthielten in allen Fällen das Datum des Tests, die getestete Dateiversion, die Art der Installation und die benötigte Funktionalität. Allerdings fehlte in allen Protokollen die Angabe, wer den Test durchgeführt hat und für die Vollständigkeit, Richtigkeit und Echtheit des Tests verantwortlich ist.

Während in den zeitlich ersten Maßnahmen lediglich positiv getestet wurde, dass die von den Ermittlern gewünschte Funktionalität auch vorhanden ist, wurde in den späteren Verfahren auch getestet, ob keine, von der jeweiligen richterlichen Anordnung nicht abgedeckte, Funktionalität vorhanden ist. Auch der Detailgrad der einzelnen Testprotokolle hat sich im Laufe der Zeit gesteigert. Zu keinem Zeitpunkt ist allerdings getestet worden, ob die RCU von dem Hersteller verdeckt eingebaute Funktionalitäten aufweist.

Zur Kontrolle der rechtmäßigen Ausgestaltung der Überwachungssoftware war das BLKA nach meinem Dafürhalten zumindest nicht generell zur Einsichtnahme in den Quellcode der jeweils eingesetzten Version der Überwachungssoftware verpflichtet. Es wäre jedoch geboten, den jeweiligen Quellcode einzusehen, wenn

hierzu ein konkreter Anlass besteht. Um verdeckte Funktionalitäten zuverlässig auszuschließen, ist auch die stichprobenartige Einsichtnahme in den Quellcode zu empfehlen (das gilt insbesondere für wesentliche Weiterentwicklungen). Beides wiederum setzt voraus, dass für das BLKA die rechtliche Möglichkeit einer Einsichtnahme in den Quellcode besteht.

Aufgrund der datenschutzrechtlichen Verantwortlichkeit hätte das BLKA den Hersteller vertraglich verpflichten müssen, eine zu Kontrollzwecken erfolgende Einsichtnahme zu gestatten. Eine solche Verpflichtung hat dabei nicht nur die Kontrolle durch die erhebende und speichernde Stelle, sondern auch durch den Landesbeauftragten für den Datenschutz zu umfassen.

4.3 Durchführung der Maßnahme

4.3.1 Einbringung der Überwachungssoftware auf dem Zielsystem

Grundsätzlich gibt es für die verdeckte Installation der Überwachungssoftware auf einem Rechnersystem die Möglichkeiten, diese in einem vom Besitzer unbemerkten Moment durchzuführen oder den Besitzer selbst unbewusst installieren zu lassen. Von beiden Möglichkeiten machte das BLKA Gebrauch.

Zur Installation wurden vom BLKA keine eventuell auf dem Rechnersystem vorhandenen Sicherheitslücken aktiv ausgenutzt („Exploits“).

Vor allem bei einer vom BLKA nicht direkt manuell durchgeführten Installation könnte es passieren, dass die Überwachungssoftware auf einem falschen Rechner installiert und damit eine andere als die verdächtige Person überwacht wird. Aus Sicht des BLKA ist es sicherzustellen, bei der Installation auch den gewollten Rechner der zu überwachenden Person zu „treffen“. Deshalb hat das BLKA im Vorfeld die in der Regel bereits bestehende Telekommunikations- und Internetüberwachung genutzt, um einen möglichst genauen Überblick über die auf dem Zielrechner vorhandenen Softwarepakete und deren Versionen zu erhalten. Bei der Installation der RCU kann diese soweit nötig mit der aktuell ausgelesenen Softwareliste (siehe Abschnitt 4.4.2.4) verglichen werden. Außerdem kann festgestellt werden, ob der Datenverkehr, den die RCU an die RU sendet, mit

der bestehenden Internetüberwachung aufgezeichnet wird, wenn der überwachte Rechner diesen Anschluss benutzt.

Das BLKA hat mir dazu mitgeteilt, dass ihm kein Fall bekannt sei, in dem die Überwachungssoftware auf einem falschen Rechner aufgespielt worden wäre.

Die Ermittlungsbehörden haben mit Hilfe von verfahrens- und organisationsrechlichen Maßnahmen dafür Sorge zu tragen, dass ein versehentliches Installieren auf falschen Zielrechnern nicht erfolgt.

Soweit nachvollziehbar hat das BLKA insoweit alle gebotenen Sorgfaltsanforderungen erfüllt, um sicherzustellen, dass nur die von der richterlichen Anordnung umfassten Zielrechner infiltriert wurden.

4.3.2 Auslandsbezug

Ich habe keine Anhaltspunkte dafür, dass eine Quellen-TKÜ-Software auf einem im Ausland befindlichen Rechner genutzt wurde.

4.4 Überwachungssoftware

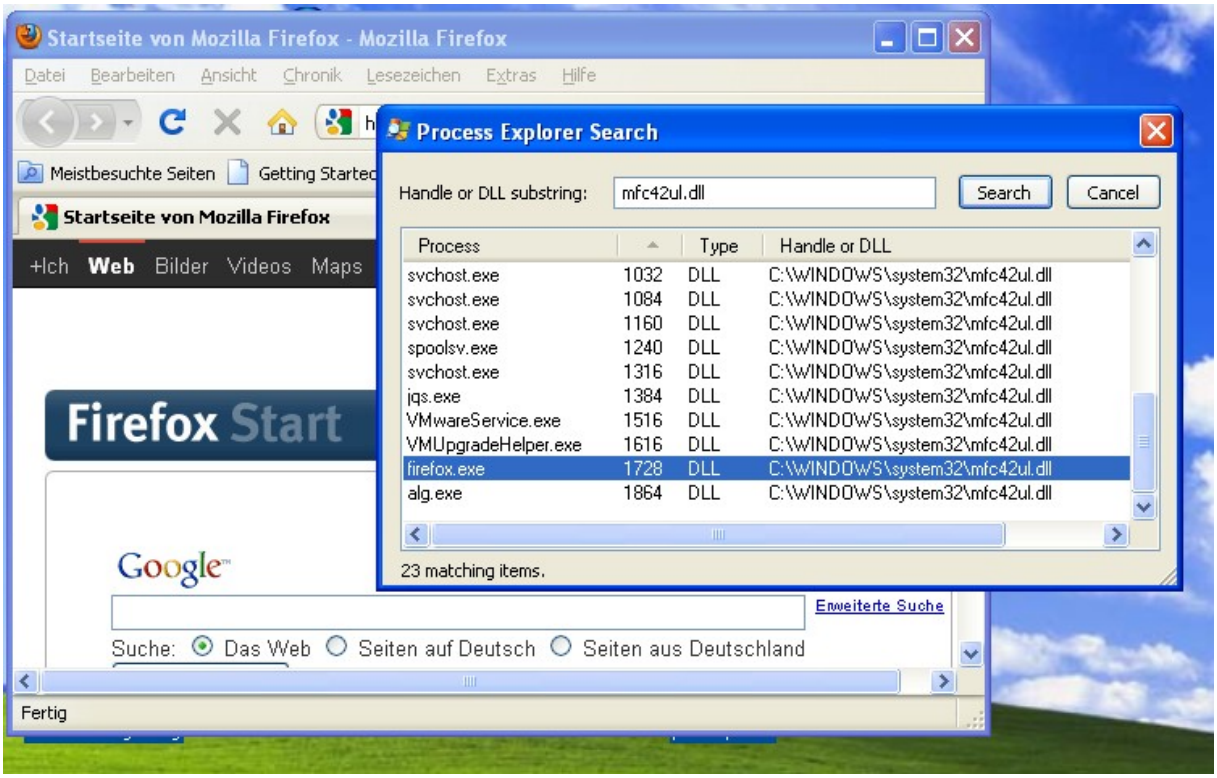
Für meine Prüfung wurde mir für 20 Maßnahmen die verwendete Software übergeben, die auf den jeweils überwachten Rechnern installiert worden war. Für drei Maßnahmen hatte das BLKA alle Daten auf Grund der geltenden datenschutzrechtlichen Regelungen bereits gelöscht. Da im Rahmen einiger Maßnahmen die Aktualisierung der Software nötig wurde, erhielt ich insgesamt 30 verschiedene Softwarepakete.

4.4.1 Funktionsweise

Die geprüften Versionen der Überwachungssoftware bestehen im Wesentlichen aus je einer Windows-Bibliothek (DLL), die im System32-Verzeichnis installiert wurden. Um die DLL zu „laden“, wird der „AppInit_DLLs“ Windows Registry Schlüssel verwendet. Alle im

Wert dieses Schlüssels angegebenen Bibliotheken werden von jeder Anwendung geladen, die in der aktuellen Anmeldesitzung ausgeführt wird[1].

Damit kann die Bibliothek potentiell jede Anwendung infiltrieren. Startet man etwa den Firefox Browser, so kann sich die DLL sofort nach dessen Start einklinken:



Die DLL wird geladen, sobald sich ein beliebiger Nutzer am System anmeldet. Sobald die DLL geladen und damit die RCU aktiv ist, versucht sie sich, solange ein Nutzer am System angemeldet ist, in regelmäßigen Intervallen mit der RU zu verbinden.

Die Verbindung zwischen RCU und RU erfolgt nicht direkt, sondern über mehrere Proxy-Server (siehe Abschnitt 4.5). Die IP Adresse des aus Sicht der RCU ersten Proxy-Servers ist dabei fest in die RCU codiert. Die RCU verbindet sich, sobald sie aktiv wird, auf den, üblicherweise für HTTPS Übertragungen genutzten, Port 443 dieser IP Adresse.

[1] http://support.microsoft.com/kb/197571

Somit baut nicht die beim BLKA installierte RU eine Verbindung zum überwachten Rechner auf, sondern der Verbindungsaufbau erfolgt immer vom überwachten Rechner durch die RCU. Die Funktionen der RCU werden in der Regel nicht von sich aus aktiv (indem etwa die nächsten zwei Wochen Applicationshots gesendet werden), sondern jede einzelne Überwachungsaktivität der RCU muss vom BLKA durch entsprechende Kommandos der RU „angeordnet“ werden.

Der überwachte Rechner verhält sich aus Sicht des angemeldeten Benutzers nicht auffällig anders als ohne installierte RCU.

Da die Systemmanipulation vergleichsweise gering ist, erscheint eine Beeinträchtigung der Stabilität des überwachten Rechners, abgesehen von den durch die RCU gewollten Eigenschaften, als nicht sehr wahrscheinlich. In diesem Sinne erfolgt lediglich die erforderliche Beeinträchtigung der Integrität des infiltrierten informationstechnischen Systems.

4.4.2 Funktionalität der Überwachungssoftware

4.4.2.1 Applicationshots

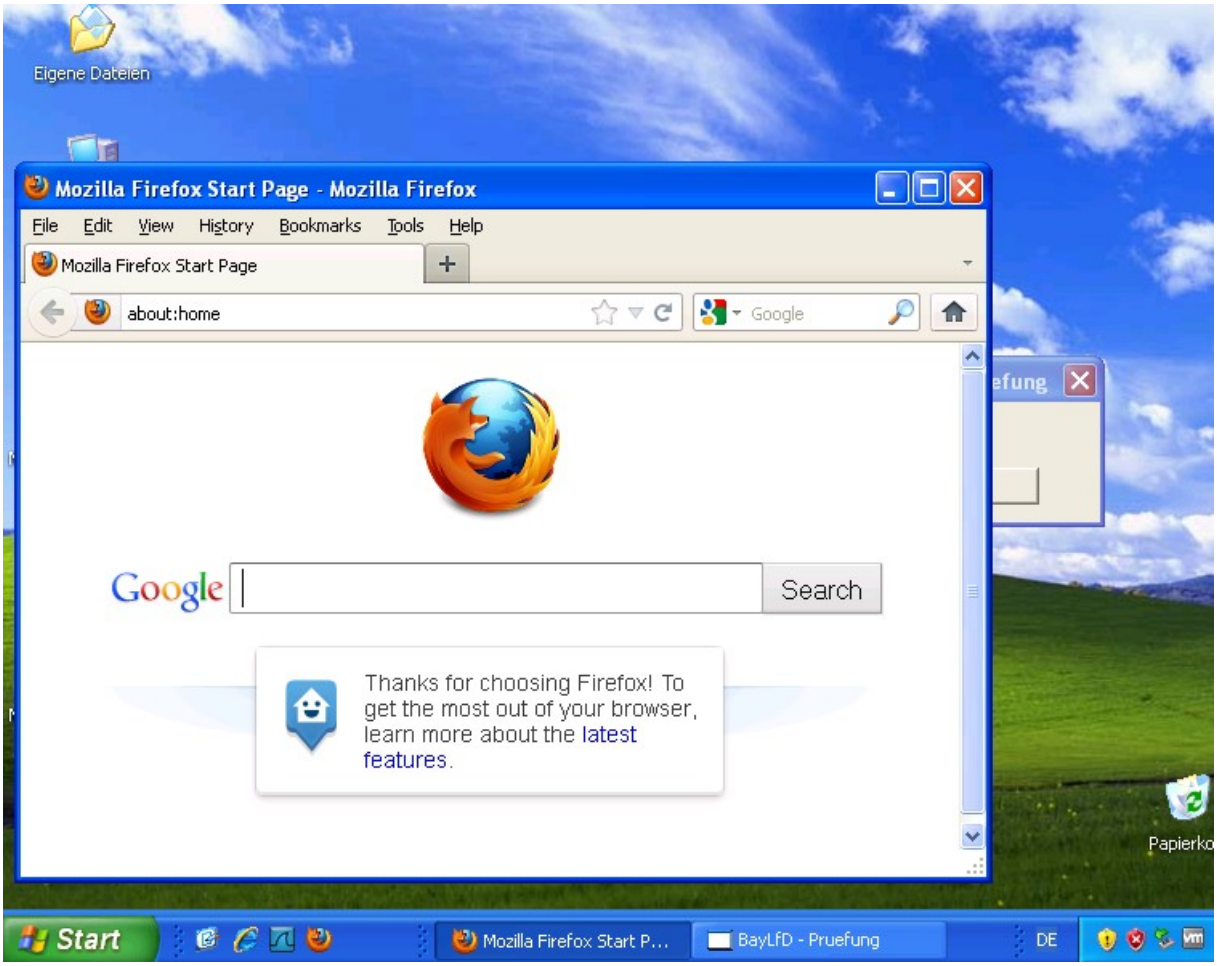
Laut Aussage des BLKA werden für die Fälle, in denen kein direkter Zugriff auf die Daten vor einer Verschlüsselung möglich ist, die Inhalte des Bildschirms an die RU übertragen, so dass anhand derer die Telekommunikationsinhalte rekonstruiert werden können.

Daraus folgt, dass im engeren Sinne nicht die Telekommunikation an sich, sondern vielmehr die „Vorbereitung“, also etwa ein Applicationshot, der das Eintippen einer Nachricht zeigt, aufgezeichnet werden kann. Ebenso werden empfangene Nachrichten nicht während der Übertragung überwacht, sondern es wird versucht, das Anzeigen der empfangenen Nachricht zu erfassen.

Die RCU fertigt dazu laut BLKA keine vollständigen Screenshots an. Es werden nur die Inhalte bestimmter Fenster von Anwendungen (Prozesse), sog. Applicationshots, übertragen. Die Liste der erlaubten Prozesse, deren Fensterinhalte überwacht werden dürfen, ist fest in die RCU kodiert. In der Regel waren dies gängige Browser oder Chat

Programme. Von welchen Anwendungen Applicationshots gefertigt werden können, legt das BLKA bei der Beauftragung der Überwachungssoftware individuell anhand der jeweiligen Beschlüsse und den aus der regulären TKÜ gewonnenen Erkenntnisse fest.

Versucht man mit der Überwachungssoftware einen Applicationshot eines Fensters einer nicht in dieser Liste beinhalteten Anwendung anzufertigen, blockt die RCU bereits auf dem überwachten System diesen Versuch. Ist jedoch ein erlaubtes Fenster aktiv, kann dessen Inhalt manuell oder in regelmäßigen Zeitabständen übertragen werden. Ein Applicationshot dieses Bildschirms



liefert beispielsweise folgendes Bild des Mozilla Firefox Browsers als Ergebnis:

Die Auflösung der gefertigten Applicationshots ist in den einzelnen Maßnahmen unterschiedlich und wurde der zur Verfügung stehenden Bandbreite des Internetanschlusses angepasst.

Da mittels Applicationshots unter anderem die Inhalte von Browser-Fenstern überwacht wurden, wurde damit zwangsläufig nicht nur etwa mittels HTTPS verschlüsselte Kommunikation, sondern auch beispielsweise der unverschlüsselte Abruf von Internetseiten mittels HTTP überwacht. In den mir zur Verfügung gestellten Prozessunterlagen fanden sich daher auch Applicationshots etwa von Google Diensten oder Internetverkaufsbörsen, die keine Verschlüsselung nutzten. Diese Applicationshots waren von richterlichen Anordnungen erfasst, die sich auf parallel zur Quellen-TKÜ laufende konventionelle TKÜ bezogen.

Da Browser in der Regel auch das Anzeigen von lokal auf dem PC gespeicherten Daten ermöglichen, ist des Weiteren auch nicht gänzlich auszuschließen, dass während einer Maßnahme auch solche Daten an die RU übermittelt werden. In den von mir geprüften Maßnahmen, in denen Applicationshots gefertigt wurden, fand ich jedoch keine Hinweise, dass dies geschehen ist.

Von den 20 Maßnahmen, von denen ich die Binärdateien erhalten habe, konnten vier Maßnahmen Applicationshots von Browsern durchführen. Zwei weitere Maßnahmen konnten nur Applicationshots von Instant Messengern aufzeichnen.

In zwei anderen, noch nicht abgeschlossenen Maßnahmen, die daher noch nicht konkret prüfbar und zu denen mir auch die dazugehörenden Beschlüsse nicht vollständig bekannt sind, konnte in der in meinem Haus aufgebauten Testumgebung mit den exakt gleichen Aufrufparametern nicht nur der Inhalt eines Browserfensters, sondern der des gesamten Bildschirms übertragen werden. Dies war unabhängig von dem gerade aktiven Fenster möglich. Auch wenn etwa als einziges Fenster ein Office-Dokument geöffnet war, konnte mit den beiden Binärdateien dieser Maßnahmen ein vollständiger Screenshot gefertigt werden.

Unabhängig von dem unter 5.2 dargestellten Streit über die Zulässigkeit von Applicationshots ist jedenfalls die Anfertigung von Screenshots im Rahmen einer Quellen-TKÜ unzulässig, weil und soweit sie auch auf dem Bildschirm befindliche Daten erfasst, die offenkundig nicht einer laufenden Telekommunikation zuzuordnen sind.

Da ich lediglich die einzelnen Binärdateien getestet und nicht das ganze, real im Einsatz befindliche System geprüft habe, kann ich jedoch keine Aussage treffen, ob von der Funktion, komplette Screenshots aufzuzeichnen, Gebrauch gemacht wurde oder ob diese überhaupt über die RU aktivierbar war.

4.4.2.2 Voice over IP (VoIP)

Der konventionellen TKÜ am nahsten ist das Ausleiten der Gespräche, die per Internet-Telefonie (VoIP) geführt werden. Im Gegensatz zu „normaler“ Telefonie, bei der Gespräche in aller Regel unverschlüsselt über mindestens einen (deutschen) Anbieter geführt werden, benötigt VoIP nicht zwingend einen Vermittler für die Gesprächsdaten und auf Grund der Struktur des Internets können auch problemlos Anbieter im Ausland verwendet werden. Da die Gesprächsdaten über öffentliche Netze gesendet werden, werden sie grundsätzlich verschlüsselt übertragen. Bei einer Ende-zu-Ende Verschlüsselung zwischen zwei Gesprächsteilnehmern ist dann eine Überwachung des Gesprächs nicht mehr auf dem üblichen Weg einer TKÜ realisierbar.

Der Grundgedanke bei der Quellen-TKÜ ist daher, diese Gespräche bereits vor der Verschlüsselung und Übertragung „an der Quelle“, also dem PC des überwachten Ge-

sprächsteilnehmers, in Kopie zur Aufzeichnung an die überwachende Behörde weiterzusenden.

Laut BLKA verbindet sich die RCU in der Regel über eine vorhandene Plugin-Schnittstelle mit der VoIP-Software und sendet von sich aus immer dann, wenn ein Gespräch stattfindet, eine Kopie des noch unverschlüsselten bzw. schon wieder entschlüsselten Gesprächsinhalts an den Überwachungsrechner. Ein manuelles Aktivieren dieser Funktion während eines Gesprächs ist prinzipbedingt nicht sinnvoll, da dem BLKA der Zeitpunkt eines Telefongesprächs regelmäßig nicht bekannt ist. Da die Durchführung des Gesprächs über eine Internetverbindung abgewickelt wird, besteht immer die Möglichkeit, diese Verbindung zeitgleich auch zum Übertragen der Gesprächskopien an das BLKA zu verwenden.

Die VoIP Kommunikation kann „live“ durch einen Sachbearbeiter mitgehört oder auch im Nachhinein abgespielt werden.

4.4.2.3 Instant Messenger

Mit Hilfe eines Instant Messengers (Chat-Programm) können sich zwei oder mehrere Personen gegenseitig beispielsweise Textnachrichten senden. Dies kann etwa mit den Produkten Skype, ICQ, Yahoo Messenger oder mittels des IRC Protokolls geschehen.

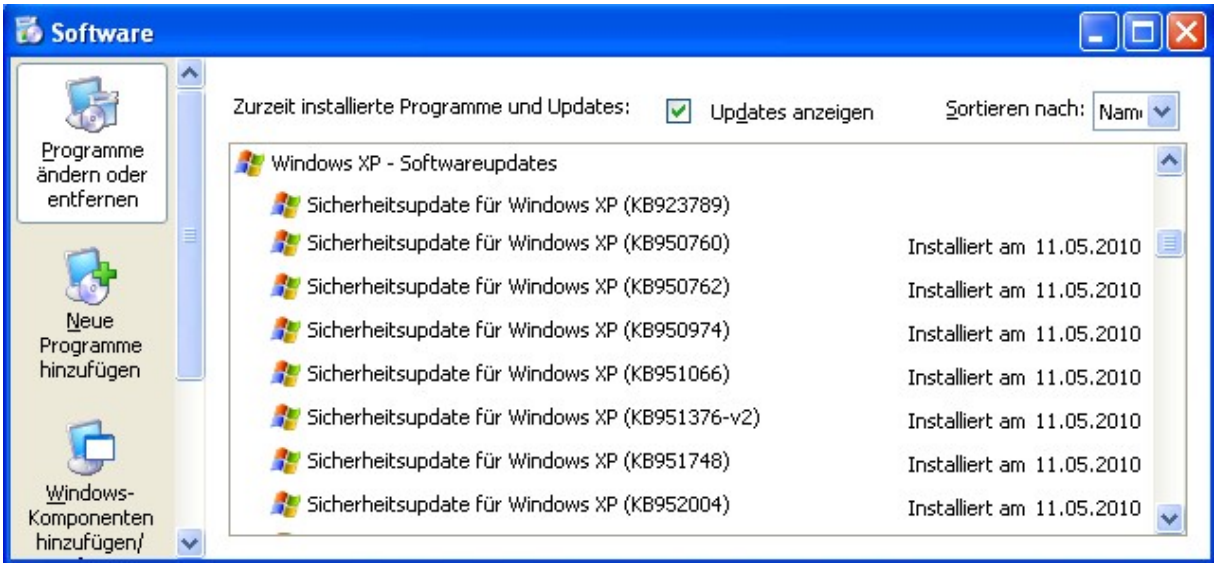
Für einzelne dieser Dienste bietet die Quellen-TKÜ-Software spezielle Funktionen an, mit denen übertragene Nachrichten als Kopie an die RU gesendet werden können. Da es aber eine hohe Anzahl sehr verschiedener Instant Messenger Software gibt, wird es immer Fälle geben, bei denen ein direktes Überwachen nicht möglich ist. Auch ist unter Umständen nicht bereits vor Beginn der Quellen-TKÜ-Maßnahme absehbar, welche Dienste genau benutzt werden. Deshalb ist es in diesen Fällen laut BLKA ebenfalls notwendig, die Überwachung des Instant Messengers mit Hilfe von Applicationshots (siehe Abschnitt 4.4.2.1) vorzunehmen.

Dies führt aber ebenfalls zu der bereits in Abschnitt 4.4.2.1 geschilderten Problematik, dass in solchen Fällen nicht nur die laufende Kommunikation überwacht und aufgezeichnet wird. Die Kommunikationsinhalte werden nämlich erst nach dem Drücken etwa des Sende-Buttons echt übertragen und nicht schon während der Eingabe der einzel-

nen Zeichen. Im Vergleich zum Schreiben einer E-Mail mag zwar die Wahrscheinlichkeit, dass einzelne Sätze oder Wörter vor dem Senden nochmals gelöscht oder geändert werden geringer sein, sie ist aber gleichwohl gegeben.

4.4.2.4 Softwareliste

Die Quellen-TKÜ Software verfügt über eine Funktion, alle auf dem überwachten Rechner installierten Programme auszulesen. Die ausgelesene Liste entspricht der Softwareliste, die über die Systemsteuerung des Rechners angezeigt werden kann. Es werden nur die Paketnamen und Versionsnummern übertragen, jedoch keine weiteren Details wie Installationszeitpunkt, Nutzungshäufigkeit, Größe oder Seriennummer.



Davon wird an die RU gesendet:

```
...
Sicherheitsupdate für Windows XP (KB923789)
Sicherheitsupdate für Windows XP (KB950760)
Sicherheitsupdate für Windows XP (KB950762)
Sicherheitsupdate für Windows XP (KB950974)
Sicherheitsupdate für Windows XP (KB951066)
Sicherheitsupdate für Windows XP (KB951376-v2)
Sicherheitsupdate für Windows XP (KB951748)
Sicherheitsupdate für Windows XP (KB952004)
...
```

Laut BLKA wird das Auslesen der Softwareliste verwendet um festzustellen, ob die Überwachungssoftware auf dem richtigen Rechner installiert wurde, da zumindest Teile der Softwarekonfiguration in der Regel bereits durch die reguläre TKÜ bekannt sind.

Durch Auslesen der Liste lässt sich auch abschätzen, ob etwa durch neu installierte Software eine Aktualisierung der RCU nötig wird.

In den zwanzig Maßnahmen, für die mir die Binärdateien zur Verfügung gestellt wurden, konnte in neun Maßnahmen die Softwareliste während des gesamten Überwachungszeitraums ausgelesen werden. Ob und wie häufig von dieser Funktion in den einzelnen Maßnahmen Gebrauch gemacht wurde, lässt sich nicht mehr klären. Weder in den Strafprozessakten noch in den Protokollen des BLKA finden sich dazu Aufzeichnungen.

Die Beschlüsse zur Quellen-TKÜ enthalten regelmäßig den Zusatz, dass zur Überwachung und Aufzeichnung der verschlüsselten Telekommunikation auch die „*Vornahme hierfür erforderlicher Maßnahmen im Rahmen der Fernsteuerung angeordnet*“ wird. Insofern könnte das Auslesen der Softwareliste grundsätzlich hiervon umfasst sein. Allerdings konnten – wie oben dargestellt – nur in neun von zwanzig Maßnahmen die Softwarelisten ausgelesen werden.

Insofern stellt sich schon in tatsächlicher Hinsicht die Frage, ob das Auslesen einer Softwareliste erforderlich im Sinne der Anordnungen ist. Entscheidend hierfür sind letztlich die Umstände des Einzelfalls und hierbei insbesondere die Aufbringungswege (Installation der Überwachungssoftware). Zur rechtlichen Bewertung siehe Abschnitt 5.2.

4.4.2.5 Ausführen von Programmen

Alle getesteten RCUs erlaubten das Starten von selbst eingebrachten Programmen (Software) auf dem überwachten Rechner. Die zu startenden Programme werden bei bestehender Verbindung auf den Zielrechner übertragen und dort umgehend ausgeführt. Es erfolgt keine Speicherung dieser Programme auf den Datenträgern des überwachten PCs. Es ist - soweit erkennbar - nicht möglich, bereits auf dem PC installierte Programme direkt zu starten.

Da diese Funktion das Ausführen von beliebigen Programmen auf dem überwachten Rechner mit Systemadministrator-Rechten erlaubt, gibt es somit keine zuverlässige, technische Funktionseinschränkung der RCU, da jederzeit weitere Funktionen nachinstalliert werden könnten. So ließe sich mit dieser Funktion beispielsweise weitere

(Schad-) Software installieren, um z.B. den Festplatteninhalt zu durchsuchen, Daten vom überwachten Rechner zum BLKA und vom BLKA auf den überwachten Rechner zu laden sowie Daten auf dem überwachten Rechner zu manipulieren.

Von drei der 23 Maßnahmen wurden mir die Protokolldaten der RU (siehe hierzu auch 4.6.6) zur Verfügung gestellt. Darin fanden sich keine Hinweise, dass auf den überwachten Rechnern weitere Programme ausgeführt wurden.

Die Prüfung der RU ergab, dass sich die Funktion, Programme auf dem überwachten Rechner auszuführen, nicht über die vorhandene Oberfläche aktivieren lässt. Es fand sich kein entsprechender „Knopf“ zum Auslösen der im Hintergrund vorhandenen Funktion. Mir wurde vom BLKA auch glaubhaft versichert, dass dort nicht bekannt gewesen sei, dass die Funktion in allen Binärdateien vorhanden war.

In einer Maßnahme konnte technisch bedingt keine Deinstallation der Überwachungssoftware über die reguläre Deinstallationsfunktion (siehe 4.4.2.7) durchgeführt werden. Deshalb wurde von dem Hersteller ein eigenständiges Programm für die Deinstallation mitgeliefert. Um dies auf dem überwachten Rechner starten zu können, wurde zusätzlich ein spezieller Lizenzschlüssel geliefert, der die Funktion „Ausführen von Programmen“ in der Oberfläche der RU für diese Deinstallation aktiviert hat.

Es ließ sich bei der Prüfung des Gesamtsystems feststellen, dass ein Starten von beliebigen Programmen nicht möglich war. Allerdings könnte diese Funktion wohl einfach durch das Einspielen eines Lizenzschlüssels für jede einzelne Maßnahme freigeschaltet werden.

Eine rechtlich gebotene Begrenzung auf bestimmte Überwachungsfunktionen wird durch diese Möglichkeit, beliebige Programme zu starten, praktisch unmöglich gemacht.

Es ist durch technische Vorkehrungen sicherzustellen, dass sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dass alle RCUs eine nicht benötigte Funktionalität beinhalteten, stellt daher einen technischen Datenschutzverstoß dar.

Unabhängig davon ist zudem festzuhalten, dass ich im Rahmen meiner Prüfung keinerlei Hinweise darauf gefunden habe, dass das BLKA (mit Ausnahme der bereits genannten Deinstallation) von derartigen Funktionen Gebrauch gemacht hätte.

4.4.2.6 Updates der RCU

Für Updates der RCU werden vom Hersteller die entsprechenden neuen Binärdateien geliefert und von Mitarbeitern des BLKA auf die RU übertragen. Über die Oberfläche der RU können diese dann für ein Update ausgewählt werden.

Updates der RCU wurden auf der RU mit zugehörigem Hashwert im datenschutzrechtlichen Sinne ordnungsgemäß protokolliert, z.B. [2]:

```
30.12.2010 13:02:31 Update
Version 3.x.x,
Signatur DLL SHA-1: 3072daf44b4d64d5039c7906f5b118cbb87ab018,
SYS SHA-1: 9cc54049e96912c42f1f0450ba16ef25ce7b2f37
```

4.4.2.7 Deinstallation

Spätestens nach dem Ende des im zugrundeliegenden Anordnungsbeschluss bestimmten Überwachungszeitraums muss die Quellen-TKÜ-Software vom überwachten Rechner entfernt werden. Dies geschah entweder manuell, also etwa nach der Beschlagnahme des Rechners im Rahmen weiterer Ermittlungen oder mittels der RU remote über das Internet.

Bei den vom BLKA eingesetzten Versionen der Quellen-TKÜ-Software war eine Deinstallation über das Internet nur dann möglich, wenn eine Online-Verbindung zwischen RCU und RU bestand. Daraus resultiert, dass eine Deinstallation nicht zu einem speziellen Zeitpunkt möglich ist, sondern erst dann, wenn sich der überwachte Rechner nach dem vorgeschriebenen Endzeitpunkt mit dem Internet und damit der RCU verbindet. Kann die RCU keine Verbindung mit der RU mehr herstellen, so bleibt die Quellen-TKÜ-Software auf dem Rechner.

[2] Dies sind fiktive Hashwerte.

Für eine Möglichkeit zur Deinstallation muss aber auch erfüllt sein, dass der in der RCU konfigurierte Proxy-Server erreichbar ist. Sollte die RCU erst sehr spät, nachdem etwa der Proxy-Server nicht mehr betrieben wird, versuchen, die RU zu erreichen, so wäre eine Deinstallation durch das BLKA unmöglich und die Quellen-TKÜ-Software würde auf dem Rechner verbleiben.

Gleiches gilt auch dann, wenn der Proxy-Server unter der konfigurierten IP-Adresse, etwa wegen des Bekanntwerdens der IP-Adresse durch eine Veröffentlichung im Internet, nicht mehr weiter betrieben werden kann.

Aber auch nach einer erfolgreichen Deinstallation besteht noch die Gefahr, dass die Überwachungssoftware etwa nach dem Wiedereinspielen eines Backups oder dem versehentlichen Neuinstallieren des „Trojaners“ durch den Benutzer wieder aktiv wird. Da sich dieser Zeitpunkt jedoch nicht eingrenzen lässt, besteht bei jeder Maßnahme, vor allem bei denen, die über das Internet installiert wurden und wieder über das Internet deinstalliert werden sollen, potentiell die Gefahr, dass dies nicht erfolgreich durchgeführt werden kann.

Derartige „verwaiste“ RCUs stellen potentiell eine Gefahr für die Daten auf diesem Rechner dar, so dass die Möglichkeiten zur Deinstallation in der durchgeführten Art und Weise, insbesondere auch im Hinblick auf das Grundrecht auf Integrität informationstechnischer Systeme, als aus datenschutzrechtlicher Sicht nicht ausreichend zu bewerten sind.

Hierfür hätte von der - laut Herstellerangaben vorhandenen - Funktionalität der automatischen Deinstallation nach einem bestimmten Zeitpunkt (hier: dem Ende des angeordneten Überwachungszeitraums) zwingend Gebrauch gemacht werden müssen. Das BLKA hat sich jedoch gegen diese Option entschieden, um bei einer eventuellen Verlängerung der Überwachung auch noch über eine Zugriffsmöglichkeit zu verfügen, wenn sich der Rechner nach einer längeren „Offline-Zeit“ erst wieder nach Ablauf des ursprünglichen Überwachungszeitraums an der RCU anmeldet.

Die Art und Weise der Deinstallation ist in der bisherigen Form nicht akzeptabel. Es muss uneingeschränkt sichergestellt sein, dass nach dem Ende des in dem zugrunde-

liegenden Beschluss bestimmten Überwachungszeitraums die Quellen-TKÜ-Software so schnell wie möglich deaktiviert und deinstalliert wird, auch wenn laut Aussage des BLKA Daten auf der RU nur während dieses Überwachungszeitraums aufgezeichnet werden. Genau genommen darf nach Ablauf des Zeitraums keine Verbindung von der RCU zur RU mehr aufgebaut werden, auch nicht, um nur kurz einen Deinstallationsbefehl zu empfangen.

Sobald die RCU ausreichend sicher festgestellt hat, dass der Überwachungszeitraum beendet ist, muss sie sich selbst deaktivieren und deinstallieren. Der Endzeitpunkt muss dafür fest in die Quellen-TKÜ-Software codiert werden. Sollte eine Verlängerung des Beschlusses erfolgen, so muss ein Update mit dem neuen Ablaufzeitpunkt fest codiert aufgespielt werden.

4.4.2.8 Weitere Funktionen

Neben den bereits genannten Funktionen gibt es gegebenenfalls noch weitere Funktionen, die etwa den überwachten Rechner zu einem gewollten Systemabsturz („Blue Screen“) oder zu einem Neustart veranlassen, um beispielsweise vom BLKA eingespielte Updates zu aktivieren.

Zusätzliche Funktionen, die datenschutzrelevante Daten ausleiten, konnten im Rahmen der Prüfung jedoch nicht festgestellt werden. Insbesondere liegen keine Anhaltspunkte für den Einsatz von Keyloggern, den Zugriff auf Mikrofone bzw. Kameras, die Manipulation von Dateien oder „beabsichtigte“ Online-Durchsuchungen vor.

4.4.3 Datenübertragung

4.4.3.1 Übertragungsprotokoll

Nachdem die Überwachungssoftware (RCU) eine Verbindung zur RU aufgebaut hat, kann die RU Kommandos (etwa „Lese die Softwareliste aus“) an die RCU senden. Die verschiedenen RCUs kann man aufgrund des verwendeten Kommunikationsprotokolls in zwei Gruppen einteilen.

Drei zeitlich alte RCUs nutzten noch ein einfacheres Protokoll, das eine schwächere Verschlüsselung und Authentisierung verwendete. Im Folgenden werden daher die

Begriffe „altes Protokoll“ und „alte Version“ immer im Zusammenhang mit den zeitlich zuerst eingesetzten RCUs verwendet. 17 Binärdateien sind „neue Versionen“ und verwenden das „neue Protokoll“. Für drei Maßnahmen waren die RCUs bereits beim BLKA gelöscht und somit keine Binärdateien mehr für eine Prüfung vorhanden.

Maßnahmen in zeitlicher Abfolge:

Maßnahme	Protokollversion
1	keine Binärdateien mehr vorhanden
2 - 4	altes Protokoll
5 - 6	neues Protokoll
7	keine Binärdateien mehr vorhanden
8	neues Protokoll
9	keine Binärdateien mehr vorhanden
10 - 23	neues Protokoll

Auch das neue Protokoll wurde im Laufe der Zeit etwas angepasst, so dass es auch hier nochmals drei unterschiedliche Ausprägungen gibt. Diese kleineren Abweichungen ergeben aber im Bezug auf das Prüfungsergebnis keinen relevanten Unterschied.

Zur Anwahl der einzelnen Funktionen (siehe Abschnitt 4.4.2) wie etwa „Fertige einen Applicationshot“ sendet die RU je einen speziellen Wert (etwa „7“) an die RCU. Diese Werte scheinen in allen Versionen gleich. Für die Kodierung und deren Bedeutung stand im Rahmen der Prüfung jedoch keine ausreichende Dokumentation zur Verfügung. Sie konnte somit nur anhand bereits im Internet vorhandener Dokumente, Disassemblierung und mittels Versuchen ermittelt werden. Der Aufwand, diese Kodierung zu ermitteln, wäre aber auch mit einer Dokumentation zumindest teilweise nötig gewesen, um diese zu verifizieren.

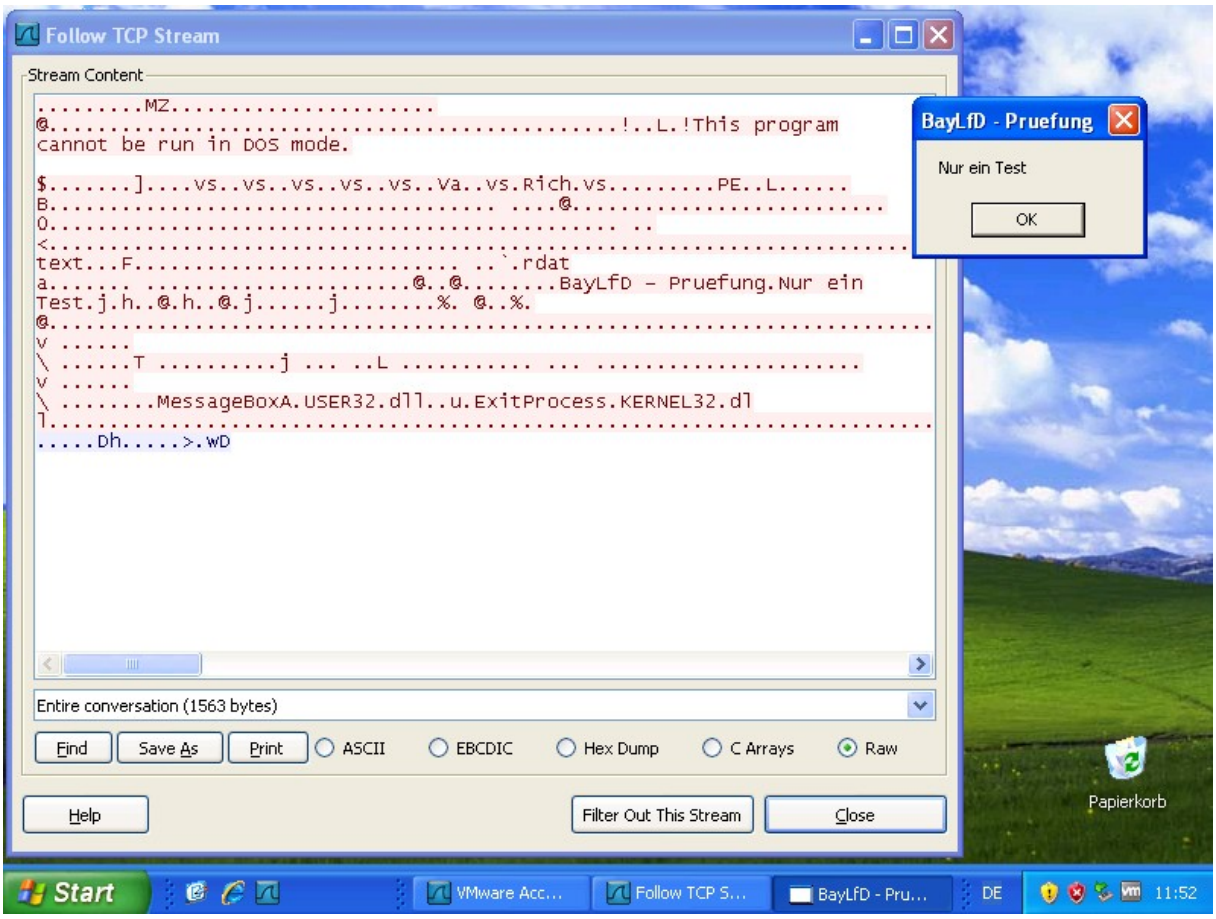
Je nach Art der Funktion folgen noch weitere Parameter oder Daten.

Für die Prüfung wurde eine in Perl selbstentwickelte „Testkonsole“ verwendet, um die Funktionalitäten der RU nachzubilden. Diese kann somit die wesentlichen Funktionalitä-

ten der einzelnen RCUs steuern. Alle Tests und Screenshots in diesem Prüfungsbericht wurden mit Hilfe dieser Testkonsole erzeugt.

4.4.3.2 Verschlüsselung der Datenströme

In der alten Protokollversion wurden die Steuerbefehle von der RU an die RCU nicht verschlüsselt, sondern im Klartext übertragen. In der in meinem Haus aufgebauten Testumgebung ließ sich dies bei bestimmten Kommandos leicht erkennen:



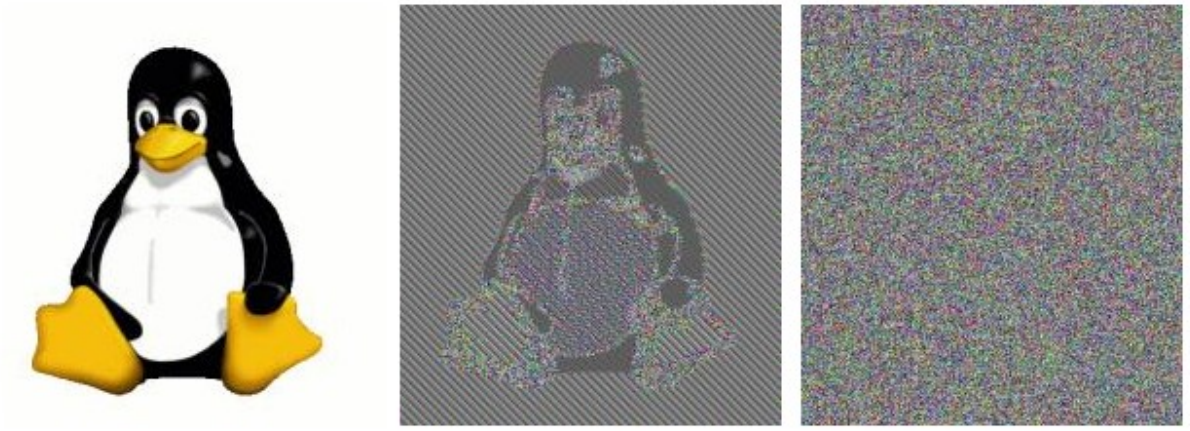
Hier sieht man die auf Netzwerkebene übertragenen Daten („Follow TCP Stream“) des Kommandos „Lade ein Programm auf den überwachten PC und führe es aus“. Auch wenn ein unbefugter Beobachter das Kommando an sich nicht kennt, so kann er sehr wohl erkennen, dass hier ein kleines Testprogramm übertragen wird.

Antworten (also die Überwachungsergebnisse) des überwachten PCs werden in allen Protokollversionen verschlüsselt übertragen. Als Verschlüsselungsalgorithmus wird hier Advanced Encryption Standard (AES) im Electronic Code Book Mode (ECB) mit einem

in allen Protokollversionen identischen 256-Bit Schlüssel verwendet, was sich im Testsystem ebenfalls verifizieren ließ.

„*Der Electronic Code Book Mode (ECB Mode) ist eine Betriebsart (Modus, Mode) für Blockverschlüsselungen. Ein Betriebsmodus wie ECB ist unabhängig vom verwendeten Blockverschlüsselungsalgorithmus*“ [3].

ECB wird als eine unsichere Betriebsart angesehen, weil gleiche Klartextdaten zu gleichen verschlüsselten Daten führen. Wie problematisch dieser Modus etwa bei einfachen Bildern sein kann zeigt ein Beispiel auf Wikipedia:



Original | *Verschlüsselt im ECB-Modus* | *Verschlüsselt in einem verketteten Modus*

Auch wenn das mittlere Bild mittels AES verschlüsselt ist, so ist das Bild dennoch dadurch erkennbar, dass gleichfarbige Bereiche (also etwa weiße Bildelemente) immer gleiche verschlüsselte Daten (also etwa graue Bildelemente) ergeben. Verwendet man jedoch statt ECB einen verketteten Modus, ist wie auf dem rechten Bild lediglich ein „zufälliges“ Rauschen erkennbar.

Im Falle von komprimierten Bildern, wie bei der vom BLKA eingesetzten Software, ist dieser Effekt jedoch bei Weitem nicht so einfach ersichtlich. Der linke Pinguin würde bei einer Übertragung durch einen der verwendeten RCUs zuerst mittels einer Umwandlung in ein JPEG Bild komprimiert, so dass das mittlere Bild deutlich kleiner sein würde und nur noch Rauschen erkennbar wäre. Die JPEG Komprimierung behebt aber kei-

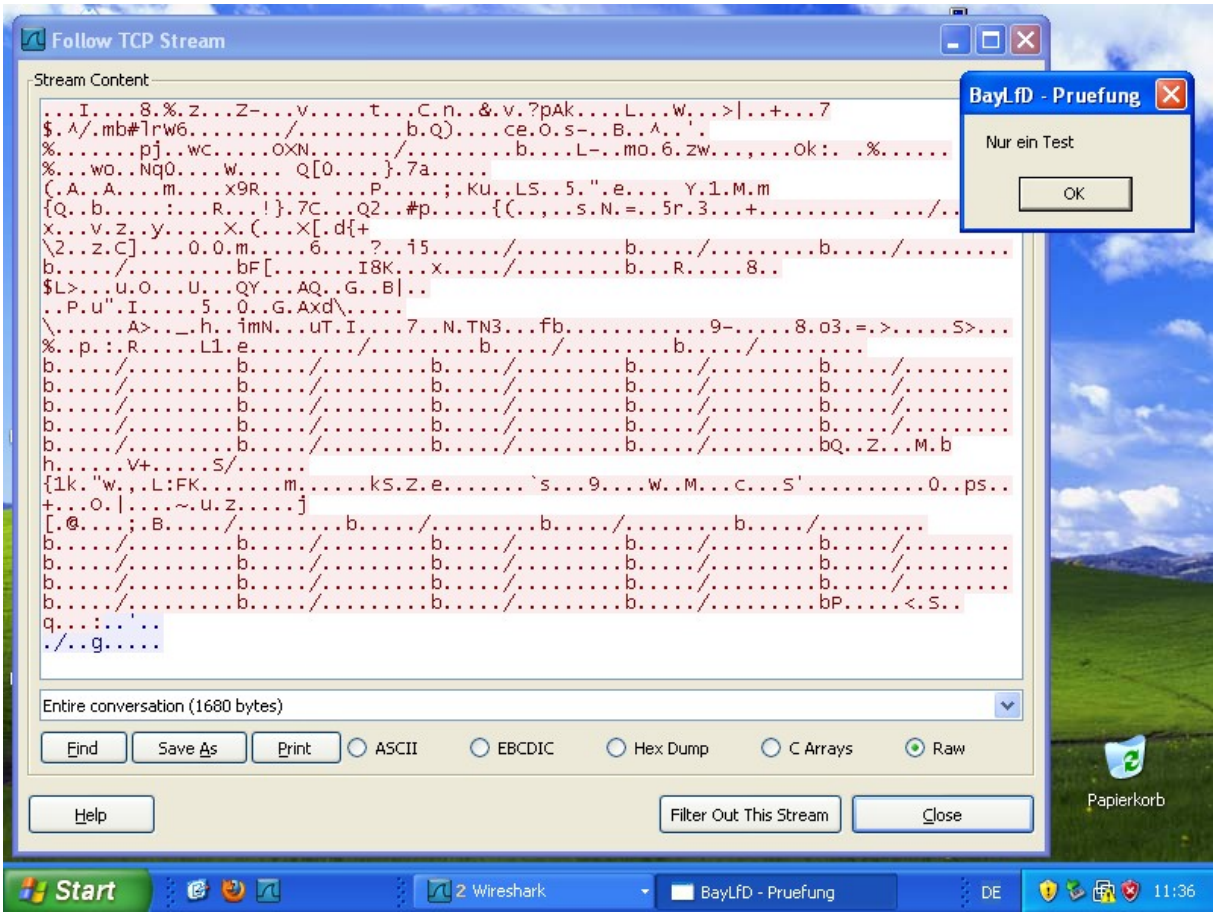
[3] http://de.wikipedia.org/wiki/Electronic_Code_Book_Mode

neswegs die Defizite, die der ECB Mode im Hinblick auf eine potentielle Angreifbarkeit bietet.

Geht man davon aus, dass der Angreifer den verwendeten Verschlüsselungsalgorithmus und den AES Schlüssel nicht kennt, er keine zusammengehörenden Klartext - Ciphertext Blöcke zur Verfügung hat und auch die binären Befehlssequenzen der RU an die RCU nicht kennt, so ist es grundsätzlich nicht trivial möglich, die mittels AES-ECB verschlüsselt übertragenen Daten zu entschlüsseln.

In der neuen Protokollversion werden auch die Befehle an die RCU verschlüsselt übertragen. Da aber gleiche Klartextdaten immer gleiche Verschlüsselungsdaten erzeugen, ist dies lediglich für die Übertragung von Updates und ausführbaren Dateien von Bedeutung. Ob ein Kommando, das nur aus wenigen Bytes besteht (etwa 0x42) im Klartext oder verschlüsselt (dann beispielsweise immer 0x2A) übertragen wird, ergibt für einen Beobachter, dem die Kommandos unbekannt sind, keinen Unterschied. Insofern ist dies für die Beurteilung der Sicherheit der Verschlüsselung nur bedingt von Bedeutung.

Im Unterschied zur unverschlüsselten Übertragung mit Hilfe des alten Protokolls, kann man im neuen Protokoll das ausführbare Programm nicht mehr direkt erkennen:



Sicherheit kann dahingehend definiert werden, dass ein Angreifer mit genau definierten Fähigkeiten ein Ziel nicht erreichen kann.

Da zum aktuellen Zeitpunkt jeder Angreifer alle nötigen Informationen (Schlüssel und Protokollbeschreibung) im Internet finden kann, hat er damit mehr als ausreichende Fähigkeiten, so dass die Verschlüsselung als ungenügend sicher einzustufen ist.

Betrachtet man die realistische Möglichkeit eines Angreifers, der über keine weitergehenden Informationen zum Verschlüsselungsverfahren oder über einen Zugriff auf RCU-Binaries verfügt, ist es für ihn nahezu unmöglich, die übermittelten Daten zu entschlüsseln. Somit kann die Verschlüsselung zum damaligen Überwachungszeitpunkt gerade noch als ausreichend angesehen werden, auch wenn durch die Vermeidung des ECB-Modus ein höheres Sicherheitsniveau einfach zu erreichen gewesen wäre.

Nach dem Bekanntwerden der für einen (einfachen) Angriff nötigen Informationen wurde der Einsatz der Überwachungssoftware umgehend gestoppt.

4.4.3.3 Gegenseitige Authentisierung

Unter gegenseitiger Authentisierung versteht man, dass sich zwei Kommunikationspartner erst gegenseitig ihre Identität nachweisen müssen, bevor sie sich vertrauen. Dies bedeutet, dass hier die RCU sicher sein will, mit „ihrer“ RU zu kommunizieren und umgekehrt. Für Maßnahmen der Quellen-TKÜ ist eine zuverlässige gegenseitige Authentisierung aus Datenschutzsicht von großer Bedeutung.

Damit die Aufzeichnungsstation (RU) im Quellen-TKÜ-System den empfangenen Daten vertrauen kann, müssen mindestens folgende Bedingungen erfüllt sein:

- Die Daten müssen vom konfigurierten Proxy-Server (siehe Abschnitt 4.1.3 und 4.5) empfangen werden.
- Zur Verschlüsselung muss der korrekte symmetrische Schlüssel verwendet werden.
- Die Klartext-Nachricht muss mit einer bestimmten Zeichenfolge beginnen.
- Die Struktur der Nachricht muss syntaktisch richtig sein.
- Die übermittelte Maßnahmen-Kennnummer muss korrekt sein.
- Die übermittelte Version der RCU muss korrekt sein.

Sofern sich der überwachte Rechner mittels eines Anschlusses, für den eine reguläre TKÜ besteht, mit dem Internet verbindet, kann darüber auch festgestellt werden, ob die von der RCU empfangenen Daten über diesen Internetanschluss gesendet wurden.

Zu kritisieren ist hier, dass bei allen Maßnahmen der gleiche, symmetrische Schlüssel und die gleiche Identifizierungszeichenfolge verwendet wurden.

In der Summe aller oben genannten Bedingungen bewerte ich die Authentisierung der RCU trotz einiger Bedenken noch als ausreichend.

Damit eine RCU Kommandos annimmt und Daten übermittelt, müssen folgende Bedingungen erfüllt sein:

- Die Verbindung erfolgt über die eine, fest konfigurierte Proxy-Server IP Adresse.
- Die Kommandos müssen syntaktisch korrekt sein.

Die Authentisierung in dieser Richtung ist daher deutlich schwächer, als die Authentisierung der RCU gegenüber der RU.

In den neuen Software-Versionen gelten zusätzlich noch folgende Bedingungen:

- Die empfangenen Kommandos müssen mit dem korrekten symmetrischen Schlüssel verschlüsselt sein.
- Die Klartext-Nachricht muss mit einer bestimmten Zeichenfolge beginnen.

Auch unter diesen erweiterten Bedingungen ist die Authentisierung schwächer, als in der Gegenrichtung und im Zusammenspiel anderer Bedingungen damit nicht mehr ausreichend.

Eine ausreichende Sicherheit des Gesamtsystems setzt aus meiner Sicht mindestens eine zuverlässige Authentisierung zwischen RU und RCU etwa mit individuellen, asymmetrischen Schlüsselpaaren für die RCUs und die RU voraus.

4.4.4 Verdeckte Funktionen

Auch wenn bei der Prüfung großer Aufwand bzgl. der Untersuchung der RCU Binärdateien mittels Disassembler und Debugging-Werkzeugen und bzgl. der Untersuchung der Kommunikation zwischen den einzelnen Komponenten betrieben wurde, so kann letztendlich nicht sicher die Aussage getroffen werden, dass keine weiteren Funktionen in einer oder mehreren der RCUs vorhanden sind.

Es kann auch nicht ausgeschlossen werden, dass die im Rahmen der Prüfung gefundenen und analysierten Funktionen durch andere oder zusätzliche Parameter oder geänderte Umgebungen andere Eigenschaften erhalten. Um hier sicherere Aussagen tref-

fen zu können, wäre eine Einsicht in den Quellcode der einzelnen RCUs nötig gewesen (siehe Abschnitt 2.4).

4.4.5 Ergebnis

Die RCU ist im Quellen-TKÜ-Verfahren die kritischste Komponente, da sie das überwachte System beeinträchtigen kann und sensible Daten an die RU überträgt.

Funktional wird das überwachte System bis auf einen allenfalls kaum bemerkbaren Performanzverlust nicht beeinträchtigt.

Auch wenn dem BLKA die Nutzung der Funktion, beliebige Programme nachladen zu können, nicht ohne weiteres möglich war, lässt sich der Einsatz einer solchen Software mit den Vorgaben des Bundesverfassungsgerichts, wonach durch technische Vorkehrungen sicherzustellen ist, dass sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt, nicht in Einklang bringen. Deshalb muss vor Einsatz einer Quellen-TKÜ-Software sichergestellt sein, dass diese keine verborgenen Funktionalitäten beinhaltet. Aus Sicht des BLKA wäre es etwa angezeigt gewesen, sich vom Hersteller im Vertrag zusichern zu lassen, dass keine überschießende Funktionalität vorhanden ist und dass dies im Einzelfall, etwa auch durch die Möglichkeit der Einsicht in den Quellcode, für jede einzelne Maßnahme nachgeprüft werden kann.

Besonders bei der Überwachung nichtsprachlicher Telekommunikation (z.B. E-Mail und Chat) ist - wie oben dargelegt - darauf zu achten, dass ausschließlich laufende Telekommunikationsvorgänge erfasst werden. Technisch kann dies aber beim Anfertigen von Applicationshots nicht vollständig sichergestellt werden.

Die Übermittlung der aufgezeichneten Daten hat sich in Bezug auf die Vertraulichkeit zwar mit neueren Versionen der RCU-Software verbessert, ist aber spätestens nach dem Bekanntwerden der Details des Übertragungsprotokolls mangelhaft.

Das Problem der nur sehr bedingt vorhandenen gegenseitigen Authentisierung und unter den aktuellen Umständen in einigen Maßnahmen nicht mehr möglichen Deinstallati-

on führte zu einer Gefahr für die überwachten Systeme. Die eingesetzten Verfahren sind hier offensichtlich nicht ausreichend gewesen.

4.5 Proxy-Server

Um eine direkte Kommunikation zwischen einem überwachten Rechner und der Überwachungskonsole zu verschleiern, setzte das BLKA zwei Proxy-Server als Kaskade ein. Wie bereits aus dem Bericht des CCC „Analyse eines Staatstrojaners“ bekannt, wurde die IP Adresse 207.158.22.134 als Ziel für die Ausleitung der Daten verwendet.

Bei der vom BLKA eingesetzten Software übernimmt ein Proxy-Server die Aufgabe, eingehende Befehle zur Steuerung der Überwachungssoftware (RCU) entweder an einen anderen Proxy-Server oder den Zielrechner selbst weiterzuleiten. Ebenso leitet er vom Zielrechner gewonnene Daten entweder an einen weiteren Proxy-Server oder an die Überwachungskonsole (RU) beim BLKA weiter.

Für alle Maßnahmen, die das BLKA durchführte, wurde als erste Zieladresse für die aus der RCU ausgeleitete Kommunikation immer der gleiche Proxy-Server verwendet, so dass er die einzige „Kontaktadresse“ für die überwachten Rechner darstellte.

Für den Betrieb des Proxy-Servers 207.158.22.134, der die Kommunikation mit den überwachten Rechnern sicherstellte, wurde vom BLKA ein sog. Root-Server bei einem amerikanischen Anbieter angemietet. Auf diesem Server lief ein Linux Betriebssystem und die von DigiTask gelieferte Proxy-Server Software („proxysrv“).

Die Anmietung erfolgte soweit wie möglich „verdeckt“, so dass deswegen die üblichen Allgemeinen Geschäftsbedingungen (AGB) des Anbieters akzeptiert wurden. Zur Prüfung wurden mir die zum Prüfungszeitpunkt gültigen AGB vorgelegt, die zum Zeitpunkt der Anmietung und des Betriebs des Servers gültigen AGB konnten jedoch nicht vorgelegt werden.

Die mir vorgelegten AGB enthielten unter anderem ein jederzeitiges, anlassloses, einseitiges Kündigungsrecht durch den Anbieter. Über die AGB hinausgehende, spezielle Regelungen, die eine garantierte Verfügbarkeit des Servers und dessen IP Adresse auch über einen längeren Zeitraum gewährleistet hätten, wurden nicht getroffen.

Zum Prüfungszeitpunkt war der Vertrag über die Anmietung des Servers mit der IP-Adresse 207.158.22.134 bereits durch das BLKA gekündigt, so dass keine Prüfung des originalen Systems mehr möglich war.

Bei der Kündigung wurden seitens des BLKA nicht die gebotenen Vorkehrungen getroffen, dass die IP-Adresse nicht erneut an einen anderen Kunden des Anbieters vergeben werden konnte. Für den Fall, dass ein neuer Kunde diese IP-Adresse zugeteilt bekommen hätte, hätte er - bei entsprechenden Kenntnissen - alle noch aktiven RCUs steuern und die gewonnenen Daten empfangen können. Dieses Szenario ist nicht unwahrscheinlich, zum einen da ein neuer Kunde beim „googlen“ dieser (seiner neuen) IP-Adresse auf eine Vielzahl von Berichten zum Thema „Staatstrojaner“ gestoßen wäre. Zum andere wären die Anfragen von noch aktiven RCUs auf den sonst üblicherweise für das HTTPS Protokoll verwendeten Port 443 unter Umständen auffällig gewesen, da diese in keiner Weise dem HTTPS Protokoll ähnlich waren und dies eine ggf. stattfindende Auswertung von Firewall Protokollen gemeldet hätte. Mit den im Internet leicht auffindbaren Informationen wäre man auch grundsätzlich in der Lage gewesen, die Kommunikation mit den RCUs ausreichend nachzubilden und somit Zugriff auf die entsprechenden Rechner zu erhalten.

Meine Nachfrage beim Anbieter ergab, dass der IP Bereich, in dem der Proxy-Server betrieben wurde, zufälligerweise aktuell nicht mehr neu vergeben wird, so dass zumindest zum jetzigen Zeitpunkt diesbezüglich keine Gefahr bestehen dürfte.

Die Funktionalität der Proxy-Server gewährleistet ein Linux-Programm, das die auf einem TCP Port eingehenden Daten an einen weiteren Proxy-Server oder die Überwachungskonsole (RU) weiterleiten kann. Sowohl nach Aussage des BLKA als auch des Herstellers leitet der Proxy-Server die Daten lediglich durch und nimmt keine Ver- oder Entschlüsselung vor.

Die Proxy-Server Software kann sowohl die IP Adressen der überwachten Rechner und die Verbindungszeitpunkte als auch die empfangenen, ggf. verschlüsselten, Daten protokollieren. Standardmäßig werden Verbindungszeitpunkte und IP Adressen protokol-

liert. Laut Auskunft des BLKA wurden auf dem System jedoch keine Protokolldaten erzeugt. Eine Überprüfung meinerseits war aus den vorgenannten Gründen nicht möglich.

Die Proxy-Software wurde mir in einem RPM-Paket zur Prüfung übergeben. Ein Nachweis, dass diese Software genau der bei den Überwachungsmaßnahmen verwendeten entspricht, konnte nicht erbracht werden.

Das ca. ein MB große Programm enthält nicht den in den RCUs verwendeten Schlüssel, was ein Indiz dafür ist, dass die Daten bei deren Durchleitung durch den Proxy-Server nicht entschlüsselt werden.

Beobachtet man den Proxy-Server Prozess mittels des Programms „strace“, so lässt sich nachweisen, dass die Daten tatsächlich unverändert weitergesendet werden:

```
[pid  1876] read (4, "\304:$B$\372\1\271\220\201w\273\32\37\366MP\265"..., 8192) = 64
[pid  1876] write(3, "\304:$B$\372\1\271\220\201w\273\32\37\366MP\265"..., 64) = 64
```

Trotzdem könnte das Proxy-Server Programm prinzipiell zwischen den Lese- und Sende-Operationen eine Entschlüsselung vornehmen.

Auffällig ist, dass das Proxy-Server Programm alle zur Ver- und Entschlüsselung notwendigen Funktionen in Form der statisch gelinkten Crypto++ Bibliothek[4] enthält. Laut Dokumentation des Herstellers können Proxy-Server so konfiguriert werden, dass sie verschlüsselte Befehle zur Änderung der Konfiguration entgegen nehmen können. Dies könnte das Vorhandensein der Bibliothek erklären.

Um sicherzugehen, dass die Crypto++ Bibliothek nicht zusätzlich noch zur Entschlüsselung der durchgeleiteten Daten Verwendung findet, wurde der Teil der Proxy-Software, der für das Empfangen und Weiterleiten der Daten verantwortlich ist, mittels dem Programm „objdump“ disassembliert und mit den aus der „strace“ Ausgabe gewonnenen Details verglichen. Zwischen dem Empfangen und dem Weiterleiten werden jedoch keine Funktionen zur Entschlüsselung aufgerufen.

[4] http://www.cryptopp.com/

Verschlüsselte Daten werden somit ohne Veränderung des Inhalts und ohne Entschlüsselung von den Proxy-Servern weitergeleitet. Im Fall von unverschlüsselten Daten werden diese unverschlüsselt weitergeleitet.

Wenn eine ausreichend wirkungsvolle Verschlüsselung, die ich im Blick auf die Gesamtsituation gerade noch zugestehen kann, eingesetzt wird und auf dem Proxy-Server selbst keine personenbezogenen Daten gespeichert oder verarbeitet werden, spricht grundsätzlich nichts gegen eine Platzierung von Proxy-Servern im Ausland. Die Ermittlungsbehörden trifft dann allerdings eine besondere Sorgfaltspflicht bezüglich der Sicherstellung der Verfügbarkeit des in Anspruch genommenen Proxy-Servers. Diese gesteigerte Sorgfaltspflicht wurde vorliegend nicht beachtet.

4.6 Überwachungskonsole (RU)

Für die Kommunikation mit den RCUs ist beim BLKA eine Überwachungskonsole - Recording Unit (RU) – von DigiTask im Einsatz. Diese bietet über eine per Secure Sockets Layer (SSL) gesicherte Web-Benutzeroberfläche die Möglichkeit, die in Abschnitt 4.4.2 beschriebenen Funktionalitäten aufzurufen, die Proxy-Kaskade zu steuern und Daten der RCUs entgegenzunehmen.

Die bei der Quellen-TKÜ verwendete Konsole wurde im Rechenzentrum des BLKA geprüft. Zum Zeitpunkt der Prüfung waren noch die vollständigen Daten von 17 Maßnahmen gespeichert. Von drei Maßnahmen sind alle Daten gemäß den von den Staatsanwaltschaften erfolgten Löschanordnungen datenschutzgerecht gelöscht worden. Für drei weitere Maßnahmen lagen bereits Löschanordnungen vor, die aber aufgrund der Prüfung des Quellen-TKÜ-Einsatzes vor der Löschung exportiert wurden.

4.6.1 Betrieb

Betrieben wird die RU in einem eigenen Netzwerksegment, das über eine Firewall mit dem Internet und dem internen Netz der Polizei verbunden ist. Die Firewall-Regeln sind gegenüber beiden Netzen restriktiv, aus dem Internet ist die RU lediglich von der IP-Adresse des aus der Sicht des BLKA nächsten Proxy-Servers erreichbar.

Für Testzwecke gibt es eine zweite Konsole.

4.6.2 Hardware

Die RU wird auf BLKA-eigener Hardware betrieben. Der Rechner ist in einem klimatisierten, zugangsgesicherten Raum in einem 19-Zoll Schrank installiert. Er hat außer einer Netzwerkverbindung zur Firewall und einer Verbindung zu einer Bildschirmkonsole keine weiteren Verbindungen etwa zu Backup- oder Storage-Systemen.

4.6.3 Betriebssystem

Die RU wird auf einem SuSE Linux Server betrieben. Das System wird nicht aktuell mit Sicherheitsupdates versorgt. Laut Aussage des BLKAs ist nicht vorgesehen, das Betriebssystem regelmäßig zu aktualisieren. Der Softwarestand entsprach zum überwiegenden Teil dem der Jahre 2008 bzw. 2009.

Auch wenn der Zugriff über die Firewall aus dem Internet nahezu vollständig unmöglich ist, so ist ein nicht mit Sicherheitsupdates versorgtes System eine potentielle Gefahr für die darauf gespeicherten Daten. Beispielsweise im Falle eines etwaigen Konfigurationsfehlers bei der verwendeten Firewall wäre das System ungeschützt im Internet.

Einen Betrieb ohne Sicherheitsupdates beurteile ich unter den gegebenen Umständen zumindest als bedenklich.

4.6.4 Software

Aus Sicht des Anwenders besteht die RU aus einer über HTTPS erreichbaren Weboberfläche, die einen Überblick über alle aktuellen Maßnahmen darstellt. Hat der Nutzer ausreichende Rechte, kann er einzelne Maßnahmen aufrufen und die dort aufgezeichneten Daten abrufen.

Aktive Aktionen, wie etwa das Aktivieren einzelner Funktionen, können nur von den Administratoren vorgenommen werden.

4.6.5 Zugangsberechtigungen

Die RU bietet die Möglichkeit, Nutzern verschiedene Rollen zuzuordnen. Das BLKA nutzt die Rollen „Administrator“ und „Sachbearbeiter“. Während die Administratoren vollständigen Zugriff auf alle Funktionalitäten der RU haben, haben Sachbearbeiter außer Leserechten nur die Möglichkeit, Daten zu „beschlagworten“ oder auszublenden.

Ein Administrator richtet einen neuen Sachbearbeiter nach Anforderung der sachbearbeitenden Dienststelle, die entweder per (interner) E-Mail oder telefonisch übermittelt wurde, ein. Dem Sachbearbeiter werden dann die jeweiligen Überwachungsmaßnahmen in seinem Aufgabengebiet zugewiesen. Die Kennung und das Zugangspasswort werden per E-Mail über das gesicherte Polizeinetz an die Dienststelle gesendet.

Das Einrichten, Ändern und Löschen von Zugangskennungen wird nicht revisionssicher protokolliert. Es ist nicht möglich, rückwirkend festzustellen, wer wann welche Rechte auf der RU hatte. Es kann lediglich für den aktuellen Zeitpunkt festgestellt werden, wer momentan welche Rechte im System hat. Sobald eine Kennung gelöscht wird, gibt es keine Aufzeichnungen mehr darüber.

Für die Komplexität der verwendeten Passwörter gibt es keine technisch erzwungenen Vorgaben (maximale Gültigkeitsdauer, Komplexität etc.), auch die Verwendung eines leeren Passworts ist möglich. Es gelten lediglich die allgemeinen, organisatorischen Anweisungen für die Verwendung ausreichend sicherer Passwörter. Neue Nutzer können ihr Initialpasswort wechseln.

Auf der RU waren ca. 90 Nutzerkennungen vorhanden. Diese waren neben administrativen Kennungen polizeiliche Sachbearbeiter in den sachbearbeitenden Dienstellen vor Ort. Den einzelnen Nutzerkennungen waren jeweils nur wenige Maßnahmen zugeordnet.

Die Nutzerkennungen sind auf Anwendungsebene eingerichtet, spezielle Kennungen auf Ebene des Betriebssystems sind nicht eingerichtet.

Die Vergabe und Verwaltung der Nutzerkennungen, sowie die Sicherungsmaßnahmen der einzelnen Kennungen entsprechen nicht den üblichen und auch hier gebotenen datenschutzrechtlichen Anforderungen an einen sicheren Betrieb.

4.6.6 Protokollierung auf der RU

Die RU erzeugt für jede Maßnahme eine Protokolldatei, die über die durchgeführten Aktionen und Konfigurationsänderungen Auskunft geben soll. Allerdings geben diese Protokolle nicht wieder, was genau auf der RCU konfiguriert wird. So lassen sich beispielsweise laut BLKA in der RU einige vom Produkt angebotene Funktionen aktivieren, auch wenn in der verwendeten RCU diese Funktionen nicht eingebaut sind. In der Protokolldatei wird dann aber das erfolgreiche Einschalten der Funktion protokolliert. So ließen sich auf dem Testsystem selbst für nicht erreichbare RCUs Funktionen scheinbar aktivieren und im Protokoll wurde dies als erfolgreich vermerkt. Protokolliert wird somit in einigen Fällen „das Drücken des Knopfes“ und nicht, ob dies auch eine konkrete Auswirkung hatte.

Die Protokolle enthalten neben dem Zeitpunkt nur eine kurze Beschreibung der Aktion (z.B. „First registration“ oder „Screenshots activated“), geben aber keine Auskunft darüber, wer diese Aktion veranlasst hat. In den drei von mir umfangreich geprüften Protokollen fanden sich im Schnitt je drei Einträge über den gesamten Zeitraum der Maßnahmen. Mehr als fünf Einträge fanden sich in keinem Protokoll.

Aus datenschutzrechtlicher Sicht waren die Einträge in den Protokolldateien sowohl wegen der mangelnden Quantität als auch der ungenügenden Qualität sowie der nicht nachprüfbaren Authentizität nicht ausreichend.

In den Protokolldateien müsste mindestes erkennbar sein, welche individuelle Person Aktionen veranlasst hat. Gruppenkennungen reichen hier nicht aus. Auch müssten alle relevanten Aktionen, wie etwa „Funktionalität ein- oder ausgeschaltet“ und ob diese Aktion wirksam war, protokolliert werden.

Auch Datenaufzeichnungen sind zuverlässig und nachvollziehbar zu protokollieren. Auch für lesende Zugriffe auf die aufgezeichneten Daten wäre es, ähnlich wie bei anderen Systemen der Polizei, empfehlenswert, diese aufzuzeichnen.

4.6.7 Protokollierung auf der Firewall

Auf der der RU vorgeschalteten Firewall werden alle erfolgreichen sowie abgewiesenen Verbindungsversuche protokolliert. Verbindungsinhalte werden nicht protokolliert.

Die Protokolle werden laut Aussage des BLKA für maximal 50 Kalenderwochen aufbewahrt. Im Rahmen der Prüfung fanden sich Protokolldaten für die letzten neun Monate.

Die Protokollierung dient ausschließlich der Sicherheit sowie der Fehlersuche und stellt einen absolut notwendigen Baustein zur Sicherheit des Gesamtsystems dar, vor allem da Sicherheitsupdates auf der RU nicht installiert wurden (siehe 4.6.3).

Da die Protokolldaten keine IP-Adressen von überwachten Personen, sondern nur die IP-Adressen der Proxy-Server und der Fernwartungsrechner, sowie IP-Adressen von nicht erlaubten Zugriffen enthalten, ist die Aufzeichnung für Sicherheitszwecke zulässig.

Aus Datenschutzsicht empfehle ich, den Protokollierungszeitraum auf maximal sechs Monate zu beschränken.

4.6.8 Kernbereich privater Lebensgestaltung

Bei Überwachungsmaßnahmen, die den Kernbereich privater Lebensgestaltung berühren können, ist so weitgehend wie möglich sicherzustellen, dass Daten mit Kernbereichsbezug nicht erhoben werden (ständige Rechtsprechung des Bundesverfassungsgericht; zuletzt BVerfG, Beschluss v. 12.10.2011, 2 BvR 236/08, m.w.N). Bei einer normalen TKÜ müssen und können daher Gesprächsinhalte, die den Kernbereich betreffen, aus den aufgezeichneten Gesprächen gelöscht werden. Dieser sogenannte Kernbereichsschutz muss selbstverständlich auch bei einer Quellen-TKÜ gewährleistet sein.

Die vom BLKA verwendete Software für die Quellen-TKÜ bietet selbst kein selektives, teilweises Löschen an. Der Sachbearbeiter kann Gespräche nur komplett löschen oder über einen Export und Reimport entsprechende Abschnitte entfernen. Bei aufgezeichneten Bildschirminhalten hat er die Möglichkeit, diese zu „verstecken“, also datenschutzrechtlich zu „sperren“, so dass diese für ihn nicht mehr sichtbar sind. Der Administrator hat dann die Möglichkeit bzw. die Aufgabe, diese zu löschen oder auch wieder

zu reaktivieren. Der Sachbearbeiter selbst hat keine Möglichkeit, Bildschirminhalte zu löschen.

Laut Aussage des BLKA wurde in den bisher durchgeführten Maßnahmen der Kernbereich nie tangiert. Auch in den von mir gesichteten Unterlagen fanden sich keine Hinweise darauf.

Die Möglichkeiten, die in der konventionellen TKÜ genutzt werden, sollten auch für die Quellen-TKÜ zur Verfügung stehen. Insbesondere sollten die Funktionalitäten der RU auch die Löschung von Gesprächsteilen technisch unterstützen.

4.6.9 Fernwartung

Das BLKA hat mit der DigiTask zu Wartungszwecken einen Vor-Ort-Service vereinbart, so dass in der Regel ein Fernwartungszugriff nicht notwendig ist.

Gleichwohl räumt das BLKA die Möglichkeit eines anlassbezogenen Fernzugriffs in Einzelfällen ein. Dieser verschlüsselte Zugang wird nur im Bedarfsfall durch das BLKA für eine individuelle IP Adresse frei geschaltet.

Im Zeitraum der Protokollierung auf der Firewall (siehe 4.6.7) erfolgten sieben Fernzugriffe auf die RU. Drei bzw. zwei Zugriffe erfolgten an jeweils hintereinander liegenden Tagen, so dass im Ergebnis wohl vier Wartungsfälle mit Fernzugriff stattfanden. Laut Aussagen des BLKA wurden dadurch Software-Updates installiert. Eine aktive Mitarbeit an einzelnen Quellen-TKÜ Maßnahmen durch Mitarbeiter der DigiTask fand nicht statt.

Welche Tätigkeiten genau im Rahmen der Fernwartung durchgeführt werden, wird nicht protokolliert, kann aber laut Aussage des BLKA im Regelfall live via Bildschirm mitverfolgt werden.

Der Wartungsvertrag wurde zur Prüfung vorgelegt. Darin wurde unter anderem auch festgelegt, dass vom Auftragnehmer keine Personen eingesetzt werden dürfen, die der Auftraggeber nach polizeilicher Überprüfung aus Sicherheitsgründen ablehnt und dass

eventuell aus dem Bereich des Auftraggebers erlangte Informationen nicht verwertet oder an Dritte weitergegeben werden dürfen.

Es fehlte eine aus datenschutzrechtlicher Sicht gebotene Regelung zur Verpflichtung des privaten Wartungspersonals auf das Datengeheimnis und nach dem Verpflichtungsgesetz.

5 Erfüllung rechtlicher Anforderungen

Das Ermittlungsinteresse der Strafverfolgungsbehörden ist bei der Quellen-TKÜ wie bei der herkömmlichen TKÜ auf den Inhalt und die Umstände der Telekommunikation gerichtet. Wie unter Abschnitt 3 ausgeführt, werden die (Telekommunikations-)Daten im Rahmen der Quellen-TKÜ allerdings direkt durch die Strafverfolgungsbehörden auf dem Telekommunikationsgerät des Betroffenen erhoben und an diese ausgeleitet. Aus technischer Sicht gleicht die Quellen-TKÜ daher in wesentlichen Bestandteilen der Online-Durchsuchung. Aus dieser technischen Vergleichbarkeit der beiden Überwachungsmaßnahmen wiederum ergeben sich auch rechtliche Anforderungen, die das Bundesverfassungsgericht in seiner Entscheidung zur Online-Durchsuchung festgestellt hat.

Entscheidend für die datenschutzrechtliche Beurteilung der überprüften Maßnahmen ist die Beantwortung der Frage, ob sie noch als (Quellen-)TKÜ am Maßstab des Art. 10 Abs. 1 Grundgesetz (GG) zu messen oder bereits als Online-Durchsuchung anzusehen sind. Für letztere sieht die Strafprozessordnung unstreitig keine Rechtsgrundlage vor.

5.1 Verfassungsrechtliche Anforderungen

Die verfassungsrechtlichen Maßstäbe zur Beurteilung der aufgeworfenen Frage nach der Abgrenzung der Quellen-TKÜ von der Online-Durchsuchung ergeben sich im Wesentlichen aus der Entscheidung des Bundesverfassungsgerichts zur sogenannten Online-Durchsuchung vom 27.02.2008 (BVerfGE 120, S. 274 ff. Die Entscheidung ist im Internet unter www.bundesverfassungsgericht.de abrufbar, die zitierten Absätze sind nach der dortigen Veröffentlichung zitiert). Beschwerdegegenstand der zugrundeliegenden Verfassungsbeschwerden waren Normen aus dem Verfassungsschutzgesetz des Landes Nordrhein-Westfalen, das u. a. eine Online-Durchsuchung, also die Durchsuchung von informationstechnischen Systemen durch einen Fernzugriff und die Ausleitung der dort vorhandenen Daten, vorsah.

Behördliche Zugriffe auf fremde informationstechnische Systeme können nach dieser Entscheidung des Bundesverfassungsgerichts das Fernmeldegeheimnis oder aber das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme beeinträchtigen. Der Schutzbereich des Art. 10 Abs. 1 GG (Telekommunikationsgeheimnis) ist danach allein eröffnet, *soweit eine Ermächtigung sich auf eine staatliche Maßnahme beschränkt, durch welche die Inhalte und Umstände der laufen-*

den Telekommunikation im Rechnernetz erhoben oder darauf bezogene Daten ausgewertet werden (…). Der Schutzbereich dieses Grundrechts ist dabei unabhängig davon betroffen, ob die Maßnahme technisch auf der Übertragungsstrecke oder am Endgerät der Telekommunikation ansetzt (vgl. BVerfGE 106, 28 <37 f.>; 115, 166 <186 f.>). Dies gilt grundsätzlich auch dann, wenn das Endgerät ein vernetztes komplexes informationstechnisches System ist, dessen Einsatz zur Telekommunikation nur eine unter mehreren Nutzungsarten darstellt (BVerfGE 120, 274, 307, Absatz 184).

Allerdings stellt das Bundesverfassungsgericht weiterhin fest, dass sich *der Grundrechtsschutz des Art. 10 Abs. 1 GG (…) nicht auf die nach Abschluss eines Kommunikationsvorgangs im Herrschaftsbereich eines Kommunikationsteilnehmers gespeicherten Inhalte und Umstände der Telekommunikation* erstreckt*, soweit dieser eigene Schutzvorkehrungen gegen den heimlichen Datenzugriff treffen kann. Dann bestehen hinsichtlich solcher Daten die spezifischen Gefahren der räumlich distanzierten Kommunikation, die durch das Telekommunikationsgeheimnis abgewehrt werden sollen, nicht fort (vgl. BVerfGE 115, 166 <183 ff.>). Der durch das Telekommunikationsgeheimnis bewirkte Schutz besteht ebenfalls nicht, wenn eine staatliche Stelle die Nutzung eines informationstechnischen Systems als solche überwacht oder die Speichermedien des Systems durchsucht. Hinsichtlich der Erfassung der Inhalte oder Umstände außerhalb der laufenden Telekommunikation liegt ein Eingriff in Art. 10 Abs. 1 GG selbst dann nicht vor, wenn zur Übermittlung der erhobenen Daten an die auswertende Behörde eine Telekommunikationsverbindung genutzt wird, wie dies etwa bei einem Online-Zugriff auf gespeicherte Daten der Fall ist (vgl. Germann, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 497; Rux, JZ 2007, S. 285 <292>). Soweit der heimliche Zugriff auf ein informationstechnisches System dazu dient, Daten auch insoweit zu erheben, als Art. 10 Abs. 1 GG nicht vor einem Zugriff schützt, bleibt eine Schutzlücke, die durch das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Schutz der Vertraulichkeit und Integrität von informationstechnischen Systemen zu schließen ist (BVerfGE 120, 274, 307 f., Absätze 185 – 187).*

Zusammengefasst darf sich das Ermittlungsinteresse der Strafverfolgungsbehörden auch im Rahmen einer Quellen-TKÜ also allein auf die Inhalte und die Umstände der Telekommunikation beziehen.

Soweit die Quellen-TKÜ in technischer Hinsicht dadurch geprägt ist, dass die Daten auf dem Endgerät noch vor der Verschlüsselung erhoben und ausgeleitet werden, hat das Bundesverfassungsgericht folgende Hinweise zur verfassungsrechtlichen Rechtslage gegeben:

Wird ein komplexes informationstechnisches System zum Zweck der Telekommunikationsüberwachung technisch infiltriert („Quellen-Telekommunikationsüberwachung"), so ist mit der Infiltration die entscheidende Hürde genommen, um das System insgesamt auszuspähen. Die dadurch bedingte Gefährdung geht weit über die hinaus, die mit einer bloßen Überwachung der laufenden Telekommunikation verbunden ist. Insbesondere können auch die auf dem Personalcomputer abgelegten Daten zur Kenntnis genommen werden, die keinen Bezug zu einer telekommunikativen Nutzung des Systems aufweisen. Erfasst werden können beispielsweise das Verhalten bei der Bedienung eines Personalcomputers für eigene Zwecke, die Abrufhäufigkeit bestimmter Dienste, insbesondere auch der Inhalt angelegter Dateien oder - soweit das infiltrierte informationstechnische System auch Geräte im Haushalt steuert - das Verhalten in der eigenen Wohnung (BVerfGE 120, 274, 308 f., Absatz 188).

In Abgrenzung zu einer (auch unbeabsichtigten) Online-Durchsuchung ist Folgendes zu beachten:

Nach Auskunft der in der mündlichen Verhandlung angehörten sachkundigen Auskunftspersonen kann es im Übrigen dazu kommen, dass im Anschluss an die Infiltration Daten ohne Bezug zur laufenden Telekommunikation erhoben werden, auch wenn dies nicht beabsichtigt ist. In der Folge besteht für den Betroffenen - anders als in der Regel bei der herkömmlichen netzbasierten Telekommunikationsüberwachung - stets das Risiko, dass über die Inhalte und Umstände der Telekommunikation hinaus weitere persönlichkeitsrelevante Informationen erhoben werden. Den dadurch bewirkten spezifischen Gefährdungen der Persönlichkeit kann durch Art. 10 Abs. 1 GG nicht oder nicht hinreichend begegnet werden (BVerfGE 120, 274, 309, Absatz 189).

Aufgrund dieser spezifischen Gefährdung ist Art. 10 Abs. 1 GG nur dann der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung *zu einer „Quellen-Telekommunikationsüberwachung", wenn sich die Überwachung ausschließlich auf Da-*

ten aus einem laufenden Telekommunikationsvorgang beschränkt. Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein (BVerfGE 120, 274, 309, Absatz 190, Hervorhebung nicht im Entscheidungstext).

Demgegenüber kommt das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität aus Art. 2 Abs. 1, Art. 1 Abs. 1 GG zum Tragen, soweit es *den persönlichen und privaten Lebensbereich der Grundrechtsträger vor staatlichem Zugriff im Bereich der Informationstechnik auch insoweit (bewahrt), als auf das informationstechnische System insgesamt zugegriffen wird und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten. (BVerfGE 120, 274, 313, Absatz 201).*

Geschützt von diesem Grundrecht ist nach Auffassung des Bundesverfassungsgerichts *zunächst das Interesse des Nutzers, dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Ein Eingriff in dieses Grundrecht ist zudem dann anzunehmen, wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen (BVerfGE 120, 274, 314, Absatz 204.)*

Das allgemeine Persönlichkeitsrecht in der hier behandelten Ausprägung schützt insbesondere vor einem heimlichen Zugriff, durch den die auf dem System vorhandenen Daten ganz oder zu wesentlichen Teilen ausgespäht werden können. Der Grundrechtsschutz umfasst sowohl die im Arbeitsspeicher gehaltenen als auch die temporär oder dauerhaft auf den Speichermedien des Systems abgelegten Daten. Das Grundrecht schützt auch vor Datenerhebungen mit Mitteln, die zwar technisch von den Datenverarbeitungsvorgängen des betroffenen informationstechnischen Systems unabhängig sind, aber diese Datenverarbeitungsvorgänge zum Gegenstand haben. So liegt es etwa bei einem Einsatz von sogenannten Hardware-Keyloggern oder bei einer Messung der elektromagnetischen Abstrahlung von Bildschirm oder Tastatur (BVerfGE 120, 274, 314 f., Absatz 205).

5.2 Einfachgesetzliche Rechtsgrundlage für die Quellen-TKÜ?

Die verfassungsrechtlichen Vorgaben sind dahingehend zusammenzufassen, dass Maßnahmen im Rahmen einer Quellen-TKÜ sich nur dann als alleiniger Eingriff in Art. 10 Abs. 1 GG darstellen und damit als Telekommunikationsüberwachungsmaßnahmen einzuordnen sind, wenn durch rechtliche Vorgaben und technische Vorkehrungen sichergestellt ist, dass sich die Maßnahmen auf die laufende Kommunikation beschränken.

In Bezug auf diese verfassungsgerichtlich getroffene Abgrenzung sind im Rahmen der Prüfung insbesondere die folgenden Fragestellungen relevant geworden.

5.2.1 §§ 100a, 100b StPO als hinreichende rechtliche Vorgaben?

Zunächst zu beantworten ist die Frage, was unter „rechtlichen Vorgaben und technischen Vorkehrungen“ zu verstehen ist, die sicherstellen sollen, dass die Datenerhebungen im Rahmen einer Quellen-TKÜ nur auf die laufende Kommunikation beschränkt bleiben.

Die zitierte Feststellung des Bundesverfassungsgerichts kann als Hinweis auf den grundrechtlichen Gesetzesvorbehalt verstanden werden. Hierfür spricht der erwähnte sinngemäße Hinweis des Bundesverfassungsgerichts, dass mit der Infiltration eines IT-Systems die „entscheidende“ Hürde für eine Ausspähung des gesamten IT-Systems genommen sei und hieraus eine Gefährdung des allgemeinen Persönlichkeitsrechts resultiere, die in ihren Auswirkungen typischerweise weit über die einer Telekommunikationsüberwachung hinausgehe. Anders ausgedrückt: Grundrechtlich betrachtet ist eine Quellen-TKÜ nicht nur eine herkömmliche TKÜ, sondern eine TKÜ, die zusätzlich die Integrität eines IT-Systems beeinträchtigt. Vor diesem Hintergrund vertritt unter anderem die 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Auffassung, dass die Quellen-TKÜ ebenso wie die Online-Durchsuchung nicht in der Strafprozessordnung geregelt ist. Schutzvorkehrungen nur im Rahmen von Gerichtsbeschlüssen auf der Grundlage der §§ 100a, 100b StPO reichten nicht aus. Gefordert sei eine ausdrückliche gesetzliche Grundlage (vgl. Entschließung vom 16./17.Mai 2011 in Würzburg: Ohne gesetzliche Grundlage keine Telekommunikationsüberwachung auf Endgeräten). Persönlich teile ich diese Auffassung. Das Bundesverfassungsgericht hat insoweit durch die Forderung von rechtlichen Vorgaben im Zusammenhang mit der Be-

urteilung einer Ermächtigung zur Quellen-TKÜ sinngemäß eine bereichsspezifische Ermächtigungsgrundlage gefordert, die nach meiner Auffassung insbesondere in §§ 100a, 100b StPO nicht gesehen werden kann.

Im Rahmen der rechtlichen Würdigung der Maßnahmen habe ich allerdings zu respektieren, dass die bayerischen Fachgerichte bislang hierzu sinngemäß eine andere Auffassung vertreten. Danach sind die Maßnahmen zur Quellen-TKÜ rechtlich als Maßnahmen zur TKÜ anzusehen.

Das Staatsministerium des Innern und das Staatsministerium der Justiz und für Verbraucherschutz haben mir übereinstimmend sinngemäß mitgeteilt, dass man dort die in den fachgerichtlichen Anordnungen zum Ausdruck kommende Auffassung insoweit teilt. Denn durch entsprechende Vorgaben in der (richterlichen) Anordnung könne rechtlich sichergestellt werden, dass die Überwachung auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt ist. Weiterhin seien Zugriffe auf Festplatten oder andere Speichermedien technisch ausgeschlossen, da die eingesetzte Software im Rahmen von TKÜ-Maßnahmen nicht die Durchsuchung von IT-Systemen ermögliche.

Die TKÜ ist in §§ 100a, 100b StPO geregelt. Nach § 100a Abs. 1 StPO darf auch ohne Wissen der Betroffenen die Telekommunikation überwacht und aufgezeichnet werden, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht, oder durch eine Straftat vorbereitet hat,

2. die Tat auch im Einzelfall schwer wiegt und

3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

In § 100a Abs. 2 StPO wird gesetzlich definiert, welche Straftaten als schwere Straftaten im Sinne von Abs. 1 Nr. 1 anzusehen sind. In § 100b StPO ist geregelt, dass die Maßnahmen grundsätzlich durch das Gericht (Ausnahme: Anordnung der Staatsanwaltschaft bei Gefahr im Verzug und richterliche Bestätigung binnen drei Werktagen) anzuordnen sind.

Auf Grund der Grenzen meiner Kontrollkompetenzen lege ich bei der rechtlichen Beurteilung im Folgenden die Auffassung der fachgerichtlichen Entscheidungen zugrunde.

Bei meiner Prüfung hat sich allerdings bestätigt, dass die derzeitige Regelungslage in tatsächlicher Hinsicht problematisch ist, da die §§ 100a, 100b StPO den Besonderheiten der Quellen-TKÜ nicht hinreichend gerecht werden. Wie bereits oben ausgeführt, beinhaltet eine richterliche Anordnung zur Telekommunikationsüberwachung nach § 100a StPO die Verpflichtung des Telekommunikationsdiensteanbieters, den Telekommunikationsinhalt an die Ermittlungsbehörden auszuleiten. Diese Ausleitung findet im Herrschaftsbereich des Telekommunikationsdiensteanbieters statt. Ein über die Mitteilung von Gesprächsinhalten hinausgehender Grundrechtseingriff hinsichtlich der Betroffenen geschieht hierbei nicht. Zu der Frage, welche technischen und verfahrensrechtlichen Voraussetzungen im Rahmen einer Quellen-TKÜ zu beachten sind, geben die §§ 100a, 100b StPO den Gerichten und den Ermittlungsbehörden keine werthaltigen Hilfestellungen.

Darüber hinaus geht auch die Mitteilungspflicht nach § 101 Absätze 3 bis 7 StPO nicht auf die Besonderheiten der Quellen-TKÜ ein. In den überprüften Fällen wurden die Betroffenen bei der Benachrichtigung über eine Quellen-TKÜ lediglich im Hinblick auf Art. 10 GG über die Aufhebung der Vertraulichkeit ihrer Telekommunikation informiert. Aus dem Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme müsste sich jedoch auch eine Pflicht ergeben, den Betroffenen einer „Infiltration“ zu gegebener Zeit über die etwaig vorgenommenen Änderungen in seinem informationstechnischen System zu informieren.

5.2.2 Fehlende Rechtsgrundlage für Begleitmaßnahmen

Weiterhin habe ich festgestellt, dass die Überwachungssoftware in mehreren Fällen im Rahmen einer Durchsuchung eingebracht worden ist. In zwei Fällen wurde die Durch-

suchung ausdrücklich zur Aufbringung der Überwachungssoftware angeordnet. Ob eine Durchsuchung zum Zwecke der Aufbringung von Überwachungssoftware mit dem Willen des Gesetzgebers in Einklang zu bringen ist, kann ich ebenfalls vorliegend nicht bewerten, da es sich um richterliche Anordnungen handelt.

Vorsorglich weise ich jedoch darauf hin, dass eine Durchsuchung zum Zweck der Aufbringung einer Überwachungssoftware nach dem Polizeiaufgabengesetz im Hinblick auf die Unverletzlichkeit der Wohnung unzulässig wäre. Die Rechtslage ist insoweit vor dem Hintergrund der Streichung des früheren Art. 34e PAG meines Erachtens eindeutig: Wenn das Betretungsrecht schon bei der Online-Durchsuchung unzulässig ist, gilt dies erst Recht für die präventive Quellen-TKÜ.

Sofern politisch an der Notwendigkeit der Quellen-TKÜ festgehalten wird, empfehle ich allerdings aus datenschutzpolitischer Sicht, in der Strafprozessordnung und im Bayerischen Polizeiaufgabengesetz Vorschriften zu verankern, die den verfassungsrechtlichen Besonderheiten besser gerecht werden als die erwähnten §§ 100a, 100b StPO (sowie entsprechend in Art. 34a – 34c Polizeiaufgabengesetz). Insbesondere sollten dabei die erhöhte Eingriffsintensität der Maßnahme und die technischen Besonderheiten der Quellen-TKÜ angemessen berücksichtigt werden. Überdies sind die rechtlichen Rahmenbedingungen für das Aufbringen der Software klärungsbedürftig. Hilfreich wären Vorgaben zu den etwaigen Besonderheiten bei den Benachrichtigungspflichten.

Auch soweit die Quellen-TKÜ Software über die Funktion verfügt, über eine Softwareliste alle Namen der auf dem überwachten Rechner installierten Programme auszulesen (vgl. dazu Abschnitt 4.4.2.4), halte ich dies für datenschutzrechtlich unzulässig. Denn hierbei erheben die Ermittlungsbehörden per Zugriff auf das infiltrierte IT-System personenbezogene Daten, die eindeutig nicht einer laufenden Telekommunikation entnommen sind.

Insbesondere im Hinblick auf die Feststellungen des Bundesverfassungsgerichts, dass sich die Überwachung im Rahmen einer Quellen-TKÜ *ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang* erstrecken darf, ist es aus datenschutzrechtlicher und aus verfassungsrechtlicher Sicht jedenfalls äußerst

problematisch, weitergehende Datenerhebungen als unselbständige Begleitmaßnahme zu rechtfertigen. Auch insoweit zeigt es sich, dass die Vorschriften der §§ 100a, 100b StPO die Besonderheiten der Quellen-TKÜ nicht hinreichend abbilden. Falls das Auslesen von Softwarelisten im Sinne einer effektiven Strafverfolgung als geboten angesehen wird, müsste dies de lege ferenda klargestellt werden. Zugleich ist die Frage aufzuwerfen, inwieweit dann eine Quellen-TKÜ überhaupt noch von einer Online-Durchsuchung abgegrenzt werden kann.

5.2.3 Applicationshots

Auch in Bezug auf die Beurteilung von Applicationshots ist die Frage zu beantworten, was im Sinne der zitierten Entscheidung des Bundesverfassungsgerichts konkret unter einer „laufenden Telekommunikation“ zu verstehen ist, auf die sich die Maßnahme zu beschränken hat.

Die mir vorliegenden Beschlüsse ordnen insofern ausdrücklich die „Überwachung und Aufzeichnung des Telekommunikationsverkehrs“ an und verweisen insoweit inhaltlich auf die Voraussetzungen der §§ 100a, 100b StPO. Diese Voraussetzungen liegen bei der Anfertigung und Ausleitung von Applicationshots meines Erachtens nicht vor.

In einem der Fälle, in denen durch das BLKA Maßnahmen zur Quellen-TKÜ durchgeführt worden sind, hat das Landgericht Landshut (Beschluss vom 20.01.2011, 4 Qs 346/10) insofern auch die Anfertigung von Applicationshots für rechtswidrig erklärt. Eine konkrete Überprüfung des zugrundeliegenden Verfahrens ist mir hier allerdings nicht möglich, da das Verfahren jedenfalls noch nicht (rechtskräftig) abgeschlossen ist.

6 Geprüfte Einzelfälle

6.1 Allgemeine Feststellungen

Im Rahmen meiner datenschutzrechtlichen Prüfung habe ich festgestellt, dass in allen Fällen, in denen im Prüfungszeitraum durch das BLKA Maßnahmen im Rahmen einer Quellen-TKÜ durchgeführt worden sind, richterliche Anordnungen vorlagen. Sämtliche Ermittlungsrichter haben als Rechtsgrundlage der Anordnung die §§ 100a, 100b StPO angesehen. In dem Fall, der auch den Feststellungen des CCC zugrunde lag, hat das zuständige Landgericht Landshut (Beschluss vom 20.01.2011, 4 Qs 346/10) in der Beschwerdeentscheidung diese rechtliche Bewertung - mit Ausnahme der Fertigung von Applicationshots - bestätigt.

Wie bereits dargestellt, ist mir eine datenschutzrechtliche Bewertung von richterlichen Entscheidungen im konkreten Einzelfall nicht möglich. Neben den o.g. Feststellungen bleibt mir jedoch, auf Folgendes hinzuweisen:

Es zeigt sich, dass die Quellen-TKÜ (noch) nicht zum „Standard-Programm“ der Strafverfolgungsbehörden gehört. Dies wird im Hinblick auf die richterlichen Anordnungen u.a. dadurch deutlich, dass die Beschlüsse in ihren Formulierungen im Prüfungszeitraum einem relativ starken Wandel unterliegen. Die Formulierungen unterscheiden sich zum Teil relativ stark, so dass sich für den „Anwender“ Probleme bei der Umsetzung des Beschlusses ergeben. Es ist nicht klar, ob unterschiedliche Formulierungen unterschiedliche Bedeutungen haben. Dies führt insbesondere zu Problemen bei der Ermittlung des Anordnungsumfanges, etwa bei der Frage, ob Applicationshots mit vom Beschluss umfasst sind. Ich habe diese Problematik im Rahmen meiner Prüfung ausführlich mit Vertretern des BLKA und des Bayerischen Staatsministeriums der Justiz und für Verbraucherschutz erörtert. Deren Auffassung, dass es sich auch bei der Anfertigung und Ausleitung von Applicationshots um TKÜ handelt, teile ich – wie bereits ausgeführt – vor dem Hintergrund der Rechtsprechung des Bundesverfassungsgerichts nicht.

Im Hinblick darauf, dass das Bundesverfassungsgericht in der genannten Entscheidung zur sog. Online-Durchsuchung festgelegt hat, dass durch rechtliche Vorgaben und technische Vorkehrungen sicherzustellen ist, dass sich Maßnahmen im Rahmen einer Quellen-TKÜ auf Telekommunikationsinhalte beschränken, begegnen etwaige Unsi-

cherheiten in den Festlegungen der Beschlüsse besonderen Bedenken. Wie bereits dargestellt, vertritt die Konferenz des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz die Ansicht, dass beide Aspekte nur durch eine eigene, bereichsspezifische Rechtsgrundlage sichergestellt werden können. Zumindest hinsichtlich der Frage der rechtlichen Vorgaben wurde seitens des Bayerischen Staatsministeriums der Justiz und für Verbraucherschutz der Standpunkt vertreten, dass diese auch durch die richterliche Anordnung vorgegeben werden können.

Angaben zu technischen Vorkehrungen, insbesondere zum Einsatz bestimmter technischer Mittel (etwa der Überwachungssoftware), enthalten die Beschlüsse nicht. Zwar enthalten richterliche Anordnungen bei klassischen TKÜ-Maßnahmen solche Angaben ebenfalls nicht. Allerdings ist hier im Vergleich zu berücksichtigen, dass es sich bei der Quellen-TKÜ um eine vergleichsweise neue Ermittlungsmaßnahme handelt, die insbesondere auch in technischer Hinsicht noch einem stärkeren Wandel unterliegt. Weiterhin werden – wie oben ausgeführt – im Rahmen der Quellen-TKÜ Begleitmaßnahmen erforderlich, die nicht direkt die Überwachung und Aufzeichnung der Telekommunikation betreffen.

6.2 Konkret überprüfte Fälle

Die in diesem Abschnitt aufgeführten Verfahren wurden von mir konkret überprüft. Im Folgenden stelle ich lediglich Vorgänge dar, die in direktem Zusammenhang mit der Quellen-TKÜ stehen. Da ich oben bereits meine allgemeinen Feststellungen im Zusammenhang mit der Durchführung der Quellen-TKÜ-Maßnahmen ausgeführt habe, beschränke ich mich in meinen nachstehenden Ausführungen beim Prüfungsergebnis auf die jeweiligen Besonderheiten des Einzelfalls.

Ergänzend ist anzumerken, dass mir das BLKA in allen diesen Fällen mitgeteilt hat, dass die Deinstallation der Überwachungssoftware von den jeweiligen Rechnern veranlasst wurde. Ob diese Deinstallationen erfolgreich waren, kann ich jedoch nicht überprüfen, da weder die Strafverfolgungsbehörden noch ich Zugriff auf die betroffenen Rechner haben.

6.2.1 Fall 1 (Staatsanwaltschaft München I)

Gegen die beiden Beschuldigten bestand der Verdacht des banden- und gewerbsmäßigen Einschleusens von Ausländern. Die Erkenntnisse, die zu dem Verdacht führten, stammten aus einer bereits bestehenden TKÜ in einem anderen Verfahren. Nach Mitteilung des BLKA wurde eine Maßnahme im Rahmen der Quellen-TKÜ durchgeführt.

Mit Beschlüsse des Amtsgerichts München vom 27.02. und 13.03.2008 wurde die Überwachung des Telekommunikationsverkehrs angeordnet. Aus der durchgeführten Überwachung ergaben sich Hinweise auf die Nutzung von verschlüsselter VoIP-Kommunikation. Aus diesem Grund wurden die Möglichkeiten einer Quellen-TKÜ mit dem BLKA besprochen. Mit Beschluss vom 03.04.2008 ordnete das Amtsgericht München die Quellen-TKÜ an.

Mit Urteil des Amtsgerichts München vom 04.02.2009 wurde einer der Beschuldigten u.a. wegen neun tatmehrheitlicher Fälle des Einschleusens von Ausländern zu einer Freiheitsstrafe von 1 Jahr und 8 Monaten verurteilt. Die Verfahren gegen die übrigen Beschuldigten wurden abgetrennt.

Am 29.06.2009 ordnete die Staatsanwaltschaft München die Löschung der aufgezeichneten Telekommunikation an.

Die Unterlagen, die Mitschriften der TKÜ enthielten, wurden aus der Akte entnommen und durch Fehlblätter ersetzt. Dem Inhalt des Sonderbandes TKÜ ist nicht zu entnehmen, ob es sich um Erkenntnisse aus der TKÜ oder der Quellen-TKÜ handelte.

Eine umfassende Prüfung war mir in diesem Fall nicht möglich, da aufgrund der Löschanordnung kaum mehr Unterlagen vorhanden waren. Den zu meiner Prüfung herangezogenen Restunterlagen sowie der Strafverfahrensakte ist zu entnehmen, dass in diesem Fall wohl nur die Ausleitung von VoIP-Gesprächen stattgefunden hat und diese Maßnahme vom Beschluss des Amtsgericht München vom 03.04.2008 umfasst war.

Nachweise über die Mitteilung an die von der TKÜ-Maßnahme Betroffenen nach § 101 Absätze 3 bis 7 StPO konnte ich der Strafverfahrensakte nicht entnehmen. Ich werde

diesbezüglich die Staatsanwaltschaft München I gesondert zur Stellungnahme auffordern.

6.2.2 Fall 2 (Staatsanwaltschaft München I)

In diesem Verfahren wurde gegen verschiedene Beschuldigte aus dem islamistischen Milieu wegen des Verdachts des Herbeiführens einer Sprengstoffexplosion ermittelt. Nach Mitteilung des BLKA wurden zwei Maßnahmen im Rahmen der Quellen-TKÜ durchgeführt.

Mit Beschlüssen des Amtsgerichts München vom 06.03. und 11.03.2009 wurde die Überwachung verschiedener Telekommunikationsanschlüsse angeordnet. Mit Beschluss des Amtsgerichts München vom 19.03.2009 wurde die Durchführung einer Quellen-TKÜ angeordnet.

Mit Verfügung der Staatsanwaltschaft München I vom 07.07.2010 wurde das Ermittlungsverfahren gem. § 170 Abs. 2 StPO eingestellt, da die umfangreichen Ermittlungen den Tatverdacht nicht erhärten konnten.

Die Betroffenen wurden mit Schreiben vom 29.07.2010 über die durchgeführten TKÜ-Maßnahmen unterrichtet. Die Staatsanwaltschaft München I forderte mit Schreiben vom 30.01.2012 zur Löschung der TKÜ-Inhalte auf. Mit Schreiben vom 10.02.2012 teilte das BLKA die Durchführung der Löschung mit.

Den zu meiner Prüfung herangezogenen Unterlagen ist zu entnehmen, dass in diesem Fall eine Ausleitung von VoIP-Gesprächen sowie der Softwareliste stattgefunden hat. Die Ausleitung der VoIP-Gespräche war vom Beschluss des Amtsgerichts München vom 19.03.2009 umfasst.

Des Weiteren habe ich bei meiner Prüfung festgestellt, dass in diesem Verfahren auch Applicationshots von einem Instant Messenger (Chat-Programm) gefertigt wurden. Aufgrund der Gesamtumstände des Verfahrens gibt es Anhaltspunkte dafür, dass es im Zusammenhang mit der Beantragung einer Quellen-TKÜ insbesondere auch auf die Überwachung des Chatverkehrs ankam. Eine ausdrückliche Ermächtigung zur Anfertigung von solchen Applicationshots kann ich dem Wortlaut des Beschlusses des Amts-

gerichts München vom 19.03.2009 jedoch nicht entnehmen. Danach „*wird insbesondere auch die Überwachung und Aufzeichnung der (…) geführten verschlüsselten Telekommunikation sowie die Vornahme der hierzu erforderlichen Maßnahmen im Rahmen einer Fernsteuerung*“ angeordnet. Auch insoweit sind jedoch „*nur solche Maßnahmen zulässig, die der Überwachung der Telekommunikation dienen und die für die technische Umsetzung der Überwachung zwingend erforderlich sind. Unzulässig sind insbesondere die Durchsuchung eines Computers nach bestimmten, auf diesen gespeicherten Daten sowie das Kopieren und Übertragen von Daten von einem Computer, die nicht Telekommunikation des Beschuldigten über das Internet mittels Voice-over-IP betreffen. Auch das Abhören von Gesprächen, die außerhalb eines Telekommunikationsvorgangs im Sinne des § 100a StPO erfolgen, ist unzulässig. Durch technische Vorkehrungen ist sicherzustellen, dass sich die Überwachung allein auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt bzw. weitergehende Überwachungsmaßnahmen nicht möglich sind.“* Soweit seitens der Strafverfolgungsbehörden der Beschluss des Amtsgerichts München dahingehend ausgelegt worden ist, dass hiervon auch die Anfertigung von Applicationshots von Chat-Programmen gedeckt sei, halte ich dies für nicht überzeugend. Wie oben (siehe Abschnitt 4.4.2.3) dargelegt, besteht auch bei der Überwachung verschlüsselter Chat-Programme die bereits im Zusammenhang mit der Fertigung von Browser-Applicastionshots (siehe Abschnitt 4.4.2.1) geschilderte Problematik, dass hier nicht nur die laufende Kommunikation überwacht und aufgezeichnet wird. Die Kommunikationsinhalte werden nämlich erst nach dem Drücken etwa des Sende-Buttons echt übertragen und nicht schon während der Eingabe der einzelnen Zeichen. Im Vergleich zum Schreiben einer E-Mail mag zwar die Wahrscheinlichkeit, dass einzelne Sätze oder Wörter vor dem Senden nochmals gelöscht oder geändert werden geringer sein, sie ist aber gleichwohl gegeben. Im konkreten Fall ist allenfalls zu berücksichtigen, dass zum Zeitpunkt der Durchführung dieser Maßnahme noch keine strafgerichtliche Entscheidung zur Frage der Zulässigkeit der Anfertigung von Applicationshots ergangen war. Die bereits angesprochene Entscheidung des Landgerichts Landshut (siehe Abschnitt 4.4.2.1) erging erst zu einem späteren Zeitpunkt.

6.2.3 Fall 3 (Staatsanwaltschaft München I)

Fall 3 betrifft einen Verfahrenskomplex der Staatsanwaltschaft München I, der mehrere Einzelverfahren umfasst. Zur Prüfung lagen mir aus diesem Komplex die Akten von vier

bereits abgeschlossenen Verfahren zur Prüfung vor, die teilweise mehrere tausend Seiten umfassten. Vom BLKA wurden mir hierzu zwei durchgeführte Maßnahmen im Rahmen der Quellen-TKÜ mitgeteilt.

Gegen eine Gruppe Beschuldigter bestand der Verdacht, dass sich diese zu einer Bande zur Begehung von Diebstählen (hauptsächlich im Einzelhandel) zusammengeschlossen haben. Darüber hinaus bestand gegen mehrere Beschuldigte der Verdacht, dass diese das Stehlgut ins Ausland verbringen.

In einem Verfahren wurden die dortigen drei Beschuldigten mit Urteil des Landgerichts München I vom 10.09.2010 u.a. wegen schweren bandenmäßigen Diebstahls in mehreren Fällen zu einer Gesamtfreiheitsstrafe von 4 Jahren und 6 Monaten, zu einer Jugendstrafe von 2 Jahren und (unter Einbeziehung eines älteren Urteils des Amtsgerichts München) zu einer Gesamtfreiheitsstrafe von 2 Jahren und einer weiteren Gesamtfreiheitsstrafe von 2 Jahren und 6 Monaten verurteilt. Eine weitere Beschuldigte wurde in einem hiervon abgetrennten Verfahren mit Urteil des Landgerichts München I vom 14.04.2011 u.a. wegen schweren Bandendiebstahls in mehreren Fällen zu einer Gesamtfreiheitsstrafe von 4 Jahren und 4 Monaten verurteilt. Weiterhin wurde ein Beschuldigter mit Urteil des Amtsgerichts München vom 23.07.2010 u.a. wegen mehrerer Fälle des Diebstahls zu einer Gesamtfreiheitsstrafe von 2 Jahren verurteilt. Die Vollstreckung dieser Freiheitsstrafe wurde zur Bewährung ausgesetzt. Schließlich wurden gegen zwei Beschuldigte Strafbefehle wegen Diebstahls oder Hehlerei in Tateinheit mit Hehlerei erwirkt.

Aus den eingesehenen Unterlagen ergibt sich, dass an alle Betroffenen Schreiben versandt wurden, mit denen diese über die TKÜ-Maßnahmen unterrichtet wurden.

Hinweise auf eine Löschung von TKÜ-Unterlagen finden sich in den Akten nicht. Ich werde diesbezüglich die Staatsanwaltschaft München I gesondert zur Stellungnahme auffordern.

Eine konkrete Prüfung auch der Datenerhebung im Rahmen der Quellen-TKÜ ist mir in diesem Fall nicht möglich, da ich davon ausgehe, dass das Landgericht München die Datenerhebung mittels einer Quellen-TKÜ-Maßnahme inzident überprüft hat (vgl. 2.2).

6.2.4 Fall 4 (Staatsanwaltschaft Bayreuth)

In dem Verfahren wurde gegen drei Beschuldigte wegen des Verdachts auf Handel mit Betäubungsmitteln (Cannabis in nicht geringer Menge, Untergrenze 1 Kilo) ermittelt. Nach Mitteilung des BLKA wurde eine Maßnahme im Rahmen der Quellen-TKÜ durchgeführt.

Mit Beschluss des Amtsgerichts Bayreuth vom 28.05.2009 wurde die Überwachung und Aufzeichnung der über einen Anschluss des Hauptbeschuldigten geführten Telekommunikation angeordnet. Mit Beschluss vom 17.09.2009 wurde hinsichtlich des gleichen Anschlusses der zuvor genannte Beschluss um die Anordnung zur Durchführung einer Quellen-TKÜ ergänzt.

Der Hauptbeschuldigte wurde mit Urteil des Landgerichts Bayreuth vom 07.12.2010 wegen unerlaubten Handeltreibens mit Betäubungsmitteln in nicht geringer Menge in drei Fällen (ca. 100g, ca. 1 kg, ca. 10 kg) zu einer Gesamtfreiheitsstrafe von 3 Jahren und 3 Monaten verurteilt. Mit Beschluss vom 26.07.2011 hat der Bundesgerichtshof die dagegen eingelegte Revision der Verteidigung verworfen. Das Verfahren gegen eine Mitbeschuldigte wurde zwischenzeitlich mit Verfügung vom 22.07.2010 gem. § 170 Abs. 2 StPO eingestellt.

Unterlagen über die durchgeführte TKÜ sind in der Strafverfahrensakte nicht enthalten.

Seitens der Staatsanwaltschaft Bayreuth wurde am 05.09.2011 verfügt, dass die Unterrichtung an die Betroffenen nach § 101 Abs. 4 StPO unterbleibt, da alle betroffenen Personen im Rahmen des Strafverfahrens von der TKÜ Kenntnis erhalten haben. Gleichzeitig wurde gegenüber der sachbearbeitenden Polizeidienstelle angeordnet, die dort vorhandenen TKÜ-Unterlagen zu löschen bzw. zu vernichten. Die Löschung wurde durch das BLKA am 09.09.2011 und von der sachbearbeitenden Polizeidienststelle am 08.09.2011 intern vermerkt und der Staatsanwaltschaft Bayreuth am 19.09.2011 mitgeteilt. Zwischenzeitlich wurde am 06.09.2011 intern die Vernichtung der CD mit dem Inhalt der TKÜ bei der Staatsanwaltschaft vermerkt.

Welche Maßnahmen im Einzelnen durchgeführt wurden, insbesondere ob etwa Applicationsshots gefertigt worden sind, konnte mir nicht mehr mitgeteilt werden. Seitens des

BLKA wurde darauf verwiesen, dass sämtliche Unterlagen bereits gelöscht worden seien. Die Akte der Staatsanwaltschaft war insofern – wie oben bereits dargestellt – ebenfalls nicht ergiebig. Eine datenschutzrechtliche Bewertung der durchgeführten Maßnahmen ist mir insofern nicht möglich.

6.2.5 Fall 5 (Staatsanwaltschaft Nürnberg-Fürth)

In diesem Verfahren bestand der Verdacht, dass der Beschuldigte illegalen Handel mit Dopingmitteln betreibt. Nach Mitteilung des BLKA wurde eine Maßnahme im Rahmen der Quellen-TKÜ durchgeführt.

Mit Beschlüssen vom 18.12.2009 wurde vom Amtsgericht Nürnberg u.a. die Überwachung verschiedener Telefonanschlüsse des Beschuldigten angeordnet. Da sich aus der TKÜ Hinweise auf eine verschlüsselte Kommunikation ergaben, wurde mit Beschluss des Amtsgerichts Nürnberg vom 21.01.2010 daraufhin auch die Überwachung und Aufzeichnung der verschlüsselten Telekommunikation angeordnet.

Mit Urteil des Landgerichts Nürnberg wurde der Beschuldigte nach einem umfassenden Geständnis und einer verfahrensfördernden Absprache nach § 257c StPO zu einer Gesamtfreiheitsstrafe von 4 Jahren und 6 Monaten verurteilt.

In diesem Fall fand eine Ausleitung von VoIP-Gesprächen statt. Die Ausleitung der VoIP-Gespräche war vom Beschluss des Amtsgerichts Nürnberg vom 21.01.2010 umfasst.

Nach Mitteilung des BLKA wurden in diesem Verfahren auch Applicationshots von WWW-Browsern bei der Nutzung von Webmaildiensten gefertigt. Auch hier finden sich aufgrund der Gesamtumstände des Verfahrens Anhaltspunkte dafür, dass es im Zusammenhang mit der Beantragung einer Quellen-TKÜ insbesondere auch auf die Überwachung des E-Mail-Verkehrs ankam. Eine ausdrückliche Ermächtigung zur Anfertigung von solchen Applicationshots kann ich jedoch auch hier dem Wortlaut des Beschlusses des Amtsgerichts Nürnberg vom 21.01.2010 nicht entnehmen. Danach wird „*zur Überwachung und Aufzeichnung der über den Anschluss (Internet-Surfstick) geführten verschlüsselten Telekommunikation (…) die Vornahme hierfür erforderlicher Maßnahmen im Rahmen der Fernsteuerung angeordnet*“. Ebenfalls im Tenor des Be-

schlusses wird jedoch festgestellt, dass „*nur solche Maßnahmen* (zulässig sind)*, die der Überwachung der Telekommunikation dienen und für deren Umsetzung zwingend erforderlich sind. Unzulässig sind insbesondere die Durchsuchung des Computers des Beschuldigten nach bestimmten gespeicherten Daten sowie das Übertragen und Kopieren entsprechender Daten außerhalb eines Telekommunikationsvorgangs (Datenspiegelung und Datenmonitoring).“* Soweit seitens der Strafverfolgungsbehörden der Beschluss des Amtsgerichts Nürnberg dahingehend ausgelegt worden ist, dass hiervon auch die Anfertigung von Applicationshots gedeckt sei, halte ich dies für nicht überzeugend. Wie bereits oben (siehe Abschnitt 4.4.2.1) ausgeführt, kann sich m. E. eine TKÜ nur auf laufende Telekommunikation beziehen. Auch hier ist allenfalls zu berücksichtigen, dass zum Zeitpunkt der Durchführung dieser Maßnahme noch keine strafgerichtliche Entscheidung zur Frage der Zulässigkeit der Anfertigung von Applicationshots ergangen war. Die bereits angesprochene Entscheidung des Landgerichts Landshut (siehe Abschnitt 4.4.2.1) erging - wie bereits erwähnt - erst zu einem späteren Zeitpunkt.

6.2.6 Fall 6 (Staatsanwaltschaft Landshut)

In diesem Verfahren wurde dem Beschuldigten gewerbsmäßige Hehlerei gem. § 260 Abs. 2 StGB vorgeworfen. Hintergrund waren Erkenntnisse aus einem anderen Verfahren dahingehend, dass der hier Beschuldigte Hehlerware in Form diverser Elektroartikel (insbesondere Mobiltelefone und Laptops) verkaufe. Nach Mitteilung des BLKA wurde eine Maßnahme im Rahmen der Quellen-TKÜ durchgeführt.

Mit Beschlüssen des Amtsgerichts Landshut vom 11.03.2010 bzw. 29.03.2010 und 23.04.2010 wurde für mehrere Anschlüsse des Beschuldigten die Überwachung und Aufzeichnung des Telekommunikationsverkehrs angeordnet. Da die TKÜ ergab, dass der Beschuldigte auch Gespräche über „Skype“ führte, wurde mit Beschluss des Amtsgerichts Landshut vom 20.05.2010 auch die Durchführung einer Quellen-TKÜ angeordnet.

Unterlagen, die auf die tatsächliche Durchführung der Quellen-TKÜ hinweisen, sind der Ermittlungsakte nicht zu entnehmen.

Das Verfahren wurde mit Verfügung der Staatsanwaltschaft Landshut vom 09.02.2011 gem. § 170 Abs. 2 StPO eingestellt. Die von der TKÜ Betroffenen sind unterrichtet wor-

den. Die zuständige Polizeidienststelle wurde am 06.04.2011 aufgefordert, die Daten aus der Telekommunikationsüberwachung zu löschen. Die Löschung wurde mit Schreiben vom 27.10. bzw. 10.10.2011 durch die zuständige Polizeidienststelle und das BLKA bestätigt.

Auch in diesem Fall war eine umfassende Prüfung nicht mehr möglich, da aufgrund der Löschanordnung kaum mehr Unterlagen vorhanden waren. Den zu meiner Prüfung herangezogenen Restunterlagen sowie der Ermittlungsakte ist zu entnehmen, dass in diesem Fall wohl nur die Ausleitung von VoIP-Gesprächen stattgefunden hat und diese Maßnahme vom Beschluss des Amtsgericht Landshut vom 20.05.2010 umfasst war.

6.2.7 Fall 7 (Staatsanwaltschaft Traunstein)

Gegen den Beschuldigten bestand der Verdacht der Einfuhr und des Handels mit Betäubungsmitteln (Kokain und Haschisch) in nicht geringer Menge in mehreren Fällen. Nach Mitteilung des BLKA wurde eine Maßnahme im Rahmen der Quellen-TKÜ durchgeführt.

Mit Beschlüssen des Amtsgerichts Traunstein vom 08.06.2010 bzw. 11.06.2010 (Erweiterungsbeschluss) wurde die Überwachung und Aufzeichnung des Telekommunikationsverkehrs bezüglich zweier Anschlüsse angeordnet. Im Rahmen der TKÜ ergaben sich Hinweise darauf, dass der Beschuldigte für Absprachen „Skype“ nutzt. Mit Beschluss des Amtsgerichts Traunstein vom 30.07.2010 wurde hinsichtlich der beiden Anschlüsse auch die Durchführung einer Quellen-TKÜ angeordnet.

Mit Urteil des Landgerichts Traunstein vom 06.02.2012 wurde der Beschuldigte nach einem umfassenden Geständnis und einer verfahrensfördernden Absprache nach § 257c StPO zu einer Gesamtfreiheitsstrafe von 5 Jahren (unter Einbeziehung einer bereits verhängten Freiheitsstrafe) und einer weiteren Gesamtfreiheitsstrafe von 3 Jahren verurteilt. Weiterhin wurde die Unterbringung in einer Entziehungsanstalt angeordnet.

Aus der Strafverfahrensakte ergibt sich weder eine Anordnung zur Löschung der TKÜ-Unterlagen, noch eine Entscheidung über die Mitteilung der Maßnahmen an die von der

TKÜ Betroffenen. Ich werde diesbezüglich die Staatsanwaltschaft Traunstein gesondert zur Stellungnahme auffordern.

Den mir vorgelegten Unterlagen ist zu entnehmen, dass in diesem Fall wohl lediglich eine Ausleitung von VoIP-Gesprächen stattgefunden hat. Die Ausleitung der VoIP-Gespräche war vom Beschluss des Amtsgerichts Traunstein vom 30.07.2010 umfasst.

6.2.8 Fall 8 (Staatsanwaltschaft Bayreuth bzw. Hof)

Aufgrund einer Geldwäscheverdachtsanzeige wurde ein Verfahren wegen des Verdachts der Geldwäsche gegen drei Beschuldigte (ein Ehepaar und den Vater des Ehemannes) eingeleitet. Hintergrund waren nicht nachvollziehbare Finanztransaktionen u.a. über das Privatkonto der beschuldigten Ehefrau. Nach Mitteilung des BLKA wurde vom 03.02.2011 bis 28.02.2011 eine Maßnahme im Rahmen der Quellen-TKÜ durchgeführt.

Das Amtsgericht Bayreuth ordnete zuvor im Rahmen des laufenden Ermittlungsverfahrens mit verschiedenen Beschlüssen die Überwachung und Aufzeichnung der Telekommunikation über verschiedene Anschlüsse an (auf die Angabe der jeweiligen Daten der Beschlüsse verzichte ich in diesem Fall aus Gründen der besseren Übersichtlichkeit). Im Rahmen der Überwachung ergaben sich Hinweise auf verschlüsselte Telekommunikation mittels „Skype“. Die bestehenden und auch ein neuer Beschluss des Amtsgerichts Bayreuth zur Telekommunikationsüberwachung wurden daraufhin teilweise um die Anordnung zur Durchführung einer Quellen-TKÜ ergänzt. Nachträglich wurden diese Beschlüsse dahingehend ergänzt bzw. wurde klargestellt, dass hiervon auch die „*notwendigen Maßnahmen zur Errichtung der Überwachung, insb. auch das Betreten der betroffenen Räume*“ umfasst ist. Einer dieser Beschlüsse wurde laut Vermerk dadurch vollzogen, dass die erforderliche Software auf einem Computer des Hauptbeschuldigten im Rahmen einer Durchsuchung aufgespielt wurde.

Mit Verfügung vom 21.04.2011 wurde das Verfahren von der Staatsanwaltschaft Bayreuth an die Staatsanwaltschaft Hof abgegeben. Von dort wurde am 11.07.2011 gegen den Hauptbeschuldigten ein Steuerstrafverfahren eingeleitet. Das Verfahren wurde insoweit mit Verfügung vom 07.11.2011 abgetrennt. Das Verfahren wegen des Verdachts der Geldwäsche wurde mit Verfügung vom 15.11.2011 gem. § 170 Abs. 2 StPO eingestellt, da ein Tatnachweis nicht zu führen war. Die Löschung bzw. Vernichtung der in

der Ermittlungsakte vorhandenen Inhalte der TKÜ wurde am 15.03.2012 verfügt. Weiterhin wurde am gleichen Tag die Löschung der entsprechenden Inhalte bei der Polizei verfügt.

Der Hauptbeschuldigte wurde mit Schreiben vom 12.01.2012 über die durchgeführte TKÜ informiert. Von der Benachrichtigung eines Beschuldigten wurde abgesehen, da dieser nicht in Deutschland sei.

Meine Prüfung ergab, dass in diesem Fall wohl lediglich eine Ausleitung von VoIP-Gesprächen stattgefunden hat. Die Ausleitung der VoIP-Gespräche war von den Beschlüssen des Amtsgerichts Bayreuth umfasst. Insoweit war auch gerade die Aufbringung der Software im Rahmen einer Durchsuchung richterlich angeordnet. Eine konkrete datenschutzrechtliche Überprüfung ist mir deshalb verwehrt. Bezüglich meiner grundsätzlichen Bedenken, inwieweit „Begleitmaßnahmen“ zur Quellen-TKÜ auf die §§ 100a, 100b StPO gestützt werden können, verweise ich auf meine obigen Ausführungen (siehe Abschnitt 5.2.2).

6.2.9 Fall 9 (Staatsanwaltschaft Ansbach)

Aufgrund einer Geldwäschemitteilung durch eine Bank bei der Generalstaatsanwaltschaft München wurde gegen mehrere Beschuldigte wegen des Verdachts der Geldwäsche ermittelt. Hintergrund waren Barabhebungen eines Beschuldigten, die zur Bezahlung von Autos dienten, die für Kunden im Ausland bestimmt waren. Zusätzlich bestand der Verdacht der Einreichung gefälschter Schecks. Nach Mitteilung des BLKA wurden vier Maßnahmen im Rahmen der Quellen-TKÜ durchgeführt.

Mit verschiedenen Beschlüssen des Amtsgerichts Ansbach wurde die Überwachung von mehreren Telefonanschlüssen angeordnet. Aus der Überwachung ergaben sich Hinweise auf Telekommunikation mittels „Skype“. Durch Beschluss vom 17.02.2011 wurde schließlich auch die Durchführung einer Quellen-TKÜ angeordnet.

Der – zumindest auf deutscher Seite – Hauptbeschuldigte wurde vom Amtsgericht Ansbach wegen vorsätzlicher Geldwäsche in 58 Fällen zur Gesamtfreiheitsstrafe von 2 Jahren und ein weiterer Täter wegen Beihilfe zu o.g. Taten zu einer Gesamtfreiheitsstrafe von 6 Monaten verurteilt. Beide Freiheitsstrafen wurden zur Bewährung ausgesetzt.

Das Verfahren wurde betreffend dreier weiterer Mitbeschuldigter mit Verfügungen vom 16. bzw. 17.11.2011 gem. § 170 Abs. 2 StPO eingestellt.

Mit Schreiben vom 23.11.2011 wurden die durchgeführten TKÜ-Maßnahmen einzelnen Betroffenen mitgeteilt. Bei den übrigen Betroffenen wurde auf die Mitteilung verzichtet, da diese „nur unerheblich betroffen“ seien und deshalb kein Interesse an der Mitteilung bestehe und der Rest Akteneinsicht hatte.

Aus der Strafverfahrensakte ergibt sich keine Anordnung zur Löschung der TKÜ-Unterlagen. Ich werde diesbezüglich die Staatsanwaltschaft Ansbach gesondert zur Stellungnahme auffordern.

Den mir vorgelegten Unterlagen ist zu entnehmen, dass in diesem Fall wohl lediglich eine Ausleitung von VoIP-Gesprächen stattgefunden hat. Die Ausleitung der VoIP-Gespräche war vom Beschluss des Amtsgerichts Ansbach vom 17.02.2011 umfasst.

München, den 30.07.2012

Dr. Thomas Petri