Staatliche Malware in Deutschland

Colin Benner

23. Januar 2012

1 Einleitung

Es gibt viele Begriffe für Staatliche Malware: „Online-Durchsuchung", „remote forensic software" (RFS), „Bundestrojaner", „Staatstrojaner", „Behördentrojaner", „Computerwanze", ...

Hinter all diesen Begriffen verbirgt sich eine Software, mit der heimlich Daten auf einem Rechner ausgespäht und diese Daten an die durchführende Behörde übermittelt werden können. Bei jedem dieser Begriffe geht es um die gleiche Art von Software, sie unterscheiden sich nur dadurch, dass sie verschiedene Eigenschaften suggerieren.

„Online-Durchsuchung" deutet eine Ähnlichkeit zur Hausdurchsuchung mit entsprechendem Anspruch auf Rechtsstaatlichkeit an. Dabei hat aber eine Online-Durchsuchung wenig mit einer Hausdurchsuchung zu tun. Bei einer Hausdurchsuchung handelt es sich um eine offene Maßnahme, von der die Betroffenen meist bei Beginn der Durchsuchung erfahren (wenn sie zu Hause sind) und bei der sie das Recht haben, dass die Durchsuchung von einem unbeteiligten Zeugen beobachtet wird. Im Gegensatz dazu erfahren Betroffene bei der Online-Durchsuchung (im Idealfall, dass heißt wenn sie die Software nicht vorher entdecken) erst nach Ende der Maßnahme davon, dass diese durchgeführt wurde. Es gibt weder eine Möglichkeit einen Zeugen dabeizuhaben, noch die Möglichkeit frühzeitig einen Anwalt einzuschalten.

„Remote forensic software" impliziert, es handele sich um eine Software, mit der aus der Ferne forensische Beweise gesichert würden, die also gerichtsverwertbare Beweise liefert. Wenn Beweismittel von einer Festplatte sichergestellt werden, muss aber sichergestellt sein, dass die Originaldaten nicht verändert werden, allein schon damit sie nochmals von einem unabhängigen Experten analysiert werden können. Beim Einsatz einer RFS wird jedoch auf dem zu durchsuchenden Rechner zunächst einmal die RFS installiert, der Zustand des Rechners also verändert.

Diese eher positiv besetzten Begriffe werden von den Behörden verwendet, um die Software in ein gutes Licht zu rücken, die Firmen, die solche Software anbieten bezeichnen sie meist als RFS.

Im Gegensatz dazu werden die Begriffe „Bundestrojaner", „Staatstrojaner", „Behördentrojaner" und „Computerwanze" vor allem von Gegnern der Online-Durchsuchung verwendet. Dabei wird bei den ersten drei Begriffen die verwendete Software als eine

Art staatliche Malware beschrieben. „Computerwanze" stellt den Spionageaspekt in den Vordergrund und schafft damit den Eindruck eines geheimdienstlichen Instruments. Der Begriff ist aber weit genug gefasst, um sowohl jegliche Form von Spyware, als auch Hardware zur Rechnerüberwachung, wie etwa einen Hardware-Keylogger, zu beschreiben. Im Gegensatz zu den von Befürwortern verwendeten Begriffen haben diese vier Bezeichnungen stark negative Konnotationen, sei es nun aus dem Bereich der Malware oder aus dem Bereich der Spionage.

2 Geschichte

Bereits im März 2005 erlaubte der damalige Bundesinnenminister Otto Schily den Geheimdiensten sowie dem BKA die heimliche Online-Durchsuchung auf Bitte des Präsidenten des Bundesamtes für Verfassungsschutz durch einen geheimen Diensterlass.[1] Öffentlich diskutiert wurde die Online-Durchsuchung erst nachdem Bundesinnenminister Wolfgang Schäuble im Oktober 2006 forderte, zur Terrorismus-Bekämpfung müsse das BKA in der Lage sein PCs aus der Ferne zu durchsuchen.[2]

Eingesetzt wurde die Online-Durchsuchung schon im Frühjahr 2006. Der überwachte gab an, den Trojaner dank eines Virenscanners erkannt zu haben. Zum Chatten habe er deshalb ein Internet-Café benutzt.[3]

Zur Herstellung der bisher als fehlend kritisierten gesetzlichen Grundlage für die Online-Durchsuchung wurde eine entsprechende Regelung am 20. 12. 2006 bei der Änderung des nordrhein-westfälischen Verfassungsschutzgesetzes diesem hinzugefügt.[4]

Am 26. 12. 2006 wurde eine Petition gegen die Online-Durchsuchung eingereicht.

Nach einem Beschluss des Bundesgerichtshofs vom 5. 2. 2007 lässt die Strafprozessordnung zwar offene, nicht aber heimliche Durchsuchungen zu, stellt also keine Rechtsgrundlage für eine Online-Durchsuchung auf Bundesebene dar.[5] Gegen das nordrhein-westfälische Verfassungsschutzgesetz wird bereits eine Klage vor dem Bundesverfassungsgericht vorbereitet.[6]

Am 27. 2. 2008 entschied das Bundesverfassungsgericht, dass das nordrhein-westfälische Verfassungsschutzgesetz verfassungswidrig ist und Online-Durchsuchungen grundsätzlich nur unter strengen Auflagen zulässig sind. Insbesondere wurde hier festgelegt, dass sonst ausschließlich eine Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) zulässig ist, bei der an der Quelle (im Rechner) eine Telekommunikation abgehört werden darf.[7]

Durch das sogenannte BKA-Gesetz wurde die Online-Durchsuchung auch auf Bundesebene gesetzlich geregelt.[8, 9]

3 Installation

Es wurde viel spekuliert, wie eine solche Installation durchgeführt werden könnte. Eine Vermutung war, es könne sich um einen gewöhnlichen Trojaner handeln, der sich für etwas anderes ausgebend die Zielperson dazu veranlassen könnte, ihn zu installieren. Weitere Vermutungen waren, dass die Installation bei einer Kontrolle am Flughafen oder durch physikalisches Eindringen in die Wohnung und manuelles Installieren der Software

durch die ermittelnde Behörde erfolgen könnte. Zudem gab es die Überlegung, ob die Installation wie bei Würmern üblich aus der Ferne durch Schwachstellen in der von der Zielperson eingesetzten Software erfolgen könnte.

In einem Fall wurde einem „Verdächtigen eine CD in den Briefkasten geworfen, ‚die aussah wie die Zugangssoftware eines großen Internet-Providers'. Installiert habe der ins Visier Genommene die Software aber nicht."[?] Der Versuch die Software als Trojaner auf den Zielrechner zu bringen wurde also (recht dilettantisch) unternommen. Ebenso wurde in einem Fall (durch den später die Binärdateien einer Version des Trojaners an den Chaos Computer Club (CCC) gelangten) die Software während einer Kontrolle am Flughafen durch den Zoll installiert. Das heimliche Eindringen in Wohnungen wurde etwa von der saarländischen CDU Mitte 2008 gefordert[10] und 2009 in Bayern gegen drei Diebe auch eingesetzt.[11]

4 Einige bekannt gewordene Fälle

Eingesetzt wurde der Staatstrojaner unter anderem gegen einen kaufmännischen Angestellten aus Landshut, der weder unter Terrorverdacht stand, noch eines Kapitalverbrechens, sondern nur des „banden- und gewerbsmäßigen Handels und Ausfuhr von Betäubungsmitteln" beschuldigt wurde[12], gegen „drei Personen, die Kleidung und Drogerieartikel gestohlen und im Ausland weiterverkauft haben sollen", gegen einen Verdächtigen, der Arzneimittel illegal ins Ausland verkauft haben soll und in einem Fall, in dem der Verdächtige „Drogen und Dopingmittel aus dem Ausland" eingekauft und an Türsteher und Personen aus dem Rotlichtmilieu verkauft haben soll.[11]

Von den ursprünglichen Behauptungen, die Online-Durchsuchung werde nur gegen einzelne Schwerstkriminelle eingesetzt ist nicht viel übrig geblieben. Auch die Entscheidung des Bundesverwaltungsgerichts, dass eine Online-Durchsuchung nur erlaubt ist, wenn es tatsächlich Anhaltspunkte für eine konkrete Gefahr, dass heißt eine Gefahr, durch die unmittelbar ein Schaden bevorsteht, für ein überragend wichtiges Rechtsgut gibt. Das Bundesverfassungsgericht hat auch festgelegt, was in diesem Zusammenhang unter überragend wichtigen Rechtsgütern zu verstehen ist, und zwar „Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschenberührt."[7]

Zu beachten ist hier, dass hier zwar offensichtlich offensichtlich eine Online-Durchsuchung nicht erlaubt ist, eine reine Quellen-TKÜ aber schon. Die vom CCC analysierte Trojanerversion verfügt aber nicht über die technischen Schranken, die bei einer Quellen-TKÜ erforderlich sind. Im Landshuter Fall wurden genau diese vom Bundesverwaltungsgericht vorgeschrieben Grenzen überschritten, indem ca. 4000 Screenshots vom Rechner des Überwachten gemacht und an die Polizei übermittelt wurden.

5 Analyse des Trojaners durch den CCC

Am 8. 10. 2011 veröffentlichte der CCC eine umfangreiche Analyse[13] einer 2008 eingesetzten Variante des Bundestrojaners, die dem CCC vom Anwalt des damit Überwach-

ten zugeschickt wurde. Nach dieser Veröffentlichung wurden die Medien am Sonntag klar vom Thema Bundestrojaner dominiert. In der Frankfurter Allgemeinen Sonntagszeitung wurde sogar auf fünf Seiten das Disassemblat der Funktion zum Nachladen beliebigen Codes abgedruckt komplett und mit einer allgemeinverständlichen Erklärung abgedruckt.[14, 15]

Aus der Analyse geht hervor, dass der Trojaner – anders als immer wieder beteuert – keineswegs sicher ist und über die vom Bundesverfassungsgericht für die Quellen-TKÜ gemachten Vorgaben weit hinausgeht.

So wurden ausschließlich die Daten, die der Trojaner an den Server schickt verschlüsselt. Das verwendete Verfahren ist der Advanced Encryption Standard (AES) im Electronic Code Book Modus (ECB) mit fest einprogrammiertem Schlüssel, der auch noch in verschiedenen Fällen verwendet wurde. Eine sichere Authentifizierung findet nicht statt (weder eine Authentifizierung des Servers noch des Clients). Es wird noch nicht einmal eine Integritätsprüfung durchgeführt.

Weiterhin bietet der Trojaner die Möglichkeit, beliebige Daten an den verwanzten Rechner zu schicken und auszuführen, womit es natürlich ohne Probleme möglich ist andere Module nachzuladen, die in der Lage sind zum Beispiel mit einem angeschlossenen Mikrofon oder einer Webcam die Umgebung des Rechners zu überwachen, was gemäß dem Urteil des Bundesverfassungsgerichts nicht zulässig ist (nur Quellen-TKÜ). Im Urteil hieß es, es seien technische und rechtliche Hürden erforderlich, um sicherzustellen, dass nur eine Quellen-TKÜ, nicht aber eine Online-Durchsuchung durchgeführt werden kann; für den Einsatz einer richtigen Online-Durchsuchung legte das Bundesverfassungsgericht sehr viel höhere Hürden fest.[7]

Zudem erstellt der Staatstrojaner Screenshots unter anderem von Browserfenstern, die bei weitem nicht nur Kommunikation enthalten müssen. Würde etwa ein Text im Browser eingegeben, aber nicht abgeschickt, würde dieser zwar auf dem Screenshot auftauchen, wäre aber keine Kommunikation. Insbesondere widerspricht dies der Vorgabe des Bundesverfassungsgerichts, dass ausschließlich eine Quellen-TKÜ erlaubt ist.

In den Binärdateien befand sich weiterhin Code zur Audio-Aufzeichnung. Dabei kommt der freie Speex-Codec zum Einsatz, dessen Lizenz vorschreibt, dass der Benutzer auf die Verwendung des Codecs an geeigneter Stelle aufmerksam gemacht werden muss. Dies ist aus offensichtlichen Gründen unterblieben.

Immer wieder wurde von den Behörden beteuert, die Software für die Quellen-TKÜ würde für jeden Fall neu zusammengestellt. In Anbetracht der Tatsache, dass alle dem CCC vorliegenden Versionen den gleichen AES-Schlüssel enthielten, kann davon wohl kaum die Rede sein.

Der C&C-Server des Trojaners befand sich bei der vom CCC zuerst analysierten Variante in den USA. Interessant ist dies aus Sicht des Datenschutzes, der in den USA einen bedeutend kleineren Stellenwert hat, als in Deutschland. Bei überwachten Rechnern, die (auch) für berufliche Zwecke eingesetzt werden besteht nicht zuletzt wegen der mangelhaften Verschlüsselung so auch unnötigerweise die Gefahr, dass so Geschäftsgeheimnisse an ausländische Konkurrenten gelangen.

Interessanterweise erkannte zum Zeitpunkt der Veröffentlichung der Analyse des CCC noch keiner der üblichen Virenscanner die vom CCC analysierte Variante des Staatstro-

janers. War der in [3] genannte Fall möglicherweise der Grund für die Verschleierung der Funktion zum Ausführen eines nachgeladenen Prozesses?

5.1 Zweite Version

Am 26. 10. 2010 veröffentlichte der CCC dann eine Analyse [16] einer aktuelleren Version des Staatstrojaners.

Bei dieser Version kam eine rudimentäre Authentifizierung zum Einsatz und der Datenverkehr wurde in beiden Richtungen verschlüsselt. Dazu wurde aber wieder derselbe AES-Schlüssel unter Verwendung des ECB-Modus wie bei der Version von 2008 benutzt.

5.2 Reaktionen auf die Analyse

Mit der Veröffentlichung der Analyse war das Thema „Staatstrojaner“ wieder eines der Hauptthemen der Mainstream-Medien. Es wurde scharf kritisiert, dass die Vorgaben des Bundesverfassungsgerichts, dass rechtliche und technische Schranken nötig seien, um eine andere Verwendung als für die Quellen-TKÜ, zu verhindern, nicht einmal im Ansatz umgesetzt wurden.

Oppermann: „Verdanken Debatte dem CCC. CCC ist Repräsentant einer wachsamen Zivilgesellschaft.“[17]

6 Begründungen für die Notwendigkeit der Online-Durchsuchung

Immer wieder behaupteten die Bedarfsträger, man könne sonst beispielsweise Kommunikation per Skype anders als gewöhnliche Telefongespräche nicht abhören. Interessanterweise ist das in anderen Ländern sehr wohl möglich, denn Skype stellt eine Abhörschnittstelle für Ermittlungsbehörden bereit, worauf Skype auch mehrfach öffentlich hingewiesen hat.

So heißt es etwa in den Skype-Datenschutzrichtlinien: „Skype, der örtliche Skype-Partner oder der Betreiber bzw. Anbieter, der die Kommunikation ermöglicht, stellt personenbezogene Daten, Kommunikationsinhalte oder Verkehrsdaten Justiz-, Strafvollzugs- oder Regierungsbehörden zur Verfügung, die derartige Informationen rechtmäßig anfordern.“[18] Weiterhin stellten sie klar, dass es seitens der eurpäischen Behörden schlicht noch keine Anfrage gegeben habe. Skype habe sogar von sich aus Eurojust die Mitarbeit angeboten.[19]

Generalbundesanwältin Harms: „Wir wollen doch gar nicht in den Computer des Privatbürgers schauen, sondern bei einem verdichteten Verdacht die Gefahr schwerster Anschläge abwehren.”[20] Wer ist denn nicht Privatbürger? Soll die Online-Durchsuchung gegen Behörden oder Firmen eingesetzt werden?

Rechtsprofessor Dirk Heckmann, Vertreter der Regierung vor dem BVerfG bei der Verhandlung über die Online-Durchsuchung, Mitarbeiter des Bayerischen Verfassungsgerichtshofs: „Die Vorratsdatenspeicherung und die Online-Durchsuchung dienen auch dem

Schutz des Menschen, der Privatsphäre."[21] Es stellt sich die Frage, wie die Einführung einer weiteren Überwachungsmaßnahme die Privatsphäre schützen kann.

Beim europäischen Polizeikongress sagte der Datenschützer Wolfgang von Pommer Esche, der den Bundesdatenschützer Peter Schaar vertrat „Jeder Kriminelle macht mal Fehler. Da muss man Geduld haben." Er scheint also der Online-Durchsuchung nicht besonders kritisch gegenüberzustehen. „Außerdem sei die Methode, einen Trojaner zu programmieren so aufwendig, dass die Behörden den Zielrechner genau auskundschaften müssten, sodass keine Gefahr bestehe, dabei irrtümlich einen Normalverbraucher ins Visier zu nehmen."[22]

Wie der Fall des Berliner Soziologen Andrej Holm, der verhaftet wurde und seit Jahren überwacht wird, weil er in einem wissenschaftlichen Artikel Fachbegriffe verwendete, die auch in einem Bekennerschreiben von „Terroristen", die in Berlin Autos angezündet hatten, auftauchten, zeigt, dass die Polizei auch gegenüber Normalbürgern nicht unbedingt zurückhaltend mit Überwachungsmaßnahmen umgeht.[23]

6.1 Wogegen soll die Online-Durchsuchung eingesetzt werden

Ursprünglich wurde die Online-Durchsuchung in erster Linie für die Gefahrenabwehr gefordert, also um konkret vorliegende Gefahren angemessen zu begegnen, und um im Laufe polizeilichere Ermittlungen Erkenntnisse für weitere Ermittlungen zu erhalten, das heißt, in welche Richtung diese weitergehen sollen.

Für diese Einsatzzwecke ist es im Gegensatz zu der Forderung, die Bundesinnenminister De Maizière 2010 stellte, die heimliche Online-Durchsuchung auch für die Strafverfolgung einzusetzen[24], nicht nötig gerichtsverwertbare Beweise zu erhalten. Für den Einsatz bei der Strafverfolgung gelten für das Sammeln von Beweisen deutlich höhere Anforderungen, die ursprünglich für den Staatstrojaner gar nicht eingeplant waren.

Liste von Einsatzzwecken[25]:

- Terrorismus: Immer wieder wurde die Notwendigkeit der Online-Durchsuchung mit der Gefahr durch den islamistischen Terrorismus begründet. So sagte etwa BKA-Präsident Ziercke 2007, das BKA habe Probleme Ermittler bei islamistischen Terroristen einzuschleusen und verfüge über keine arabisch sprechenden Mitarbeiter.[53] Es stellt sich die Frage, ob das BKA durch den Einsatz der Online-Durchsuchung plötzlich über arabisch sprechende Mitarbeiter verfügt, die dann die per Online-Durchsuchung erlangten Daten auswerten
- Wirtschaftskriminalität
- Kinderpornographie
- Mafia / organisierte Kriminalität: Ziercke wollte Bundestrojaner gegen organisierte Kriminalität in Osteuropa einsetzen.[26] Es stellt sich die Frage, seit wann das BKA für Ermittlungen im Ausland zuständig ist. Mit organisierter Kriminalität sind unter anderem Phishing, Spamming und Botnetze gemeint. Trojaner gegen Trojaner?!

- Phishing, Denial of Service-Attacken, Finanzagenten und der ganze Rest der Internetkriminalität
- Hooligans: Einsatz bei gewaltbereiten Fußballfans wurde vom rheinland-pfälzischen CDU-Chef Christian Baldauf vorgeschlagen.[27]
- Steuerhinterziehung, Geldwäsche, Erpressung, EC-/Kreditkartenbetrug
- Straftaten allgemein

7 Kritik

Gegen die Online-Durchsuchung wurden vielfältige Argumente genannt.

7.1 Grundrechtseingriffe

Ein zentraler Aspekt der Kritik an der Online-Durchsuchung ist der Eingriff in die Grundrechte der betroffenen Personen. Den Ermittlungsbehörden steht mit der geheimen Online-Durchsuchung ein Mittel, das sonst in den Bereich der Geheimdienste gehört, zur Verfügung. Auch die strikte Trennung von Polizei und Geheimdiensten wird durch den Einsatz der Online-Durchsuchung durch die Polizei aufgeweicht. Diese Trennung wurde, als Lehre aus der Zeit des Nationalsozialismus, in Deutschland gesetzlich verankert, um einen geheimdienstlich agierenden Polizeiapparat wie die Gestapo nicht noch einmal zu ermöglichen.

Auch aufgrund des massiven Eingriffs in die Privatsphäre wurde die Online-Durchsuchung kritisiert. So bezeichnete der Bürgerrechtler Burkhard Hirsch (FDP) das Ausspähen von Privatcomputern als brutalen Eingriff in die Privatsphäre, denn „der PC ist ja wie ein ausgelagertes Gehirn.“[28]

Das Bundesfinanzministerium bestätigte den Einsatz von Quellen-TKÜ zum Abhören von Skype-Telefonaten durch den Zoll: „Die Überwachung beziehe sich ‚ausschließlich auf Daten aus laufenden Kommunikationsvorgängen’ und stehe damit im Einklang mit dem Urteil des Bundesverfassungsgerichts zur sogenannten Online-Durchsuchung.“[29]

7.2 Missbrauchspotential

Es stellt sich die Frage, wie viel Beweiskraft Daten haben, die unter Veränderungen des Systems von einem Computer erhoben wurden. Während bei einer normalen forensischen Untersuchung einer Festplatte sicherzustellen ist, dass die darauf befindlichen Daten in keiner Weise verändert werden, dass also nicht etwa gefälschte „Beweise” hinterlegt werden können, ist der Eingriff ins laufende System und damit die Veränderung der gespeicherten Daten beim Einsatz eines Trojaners unumgänglich. Damit bereitet der Einsatz der Online-Durchsuchung auch Probleme hinsichtlich der Beweiskraft von Daten, die bei einer späteren Hausdurchsuchung gefunden werden.

In diesem Zusammenhang ist eine Reihe von Fällen bei der Deutschen Bahn zu nennen, bei denen Mitarbeitern „falsche ‚Beweise’ wie Hitlers ‚Mein Kampf’ oder Porno-Dateien„

untergeschoben wurden, “um diese besser kündigen zu können.„ Man fragt sich, warum man den Polizeibehörden mehr Vertrauen entgegenbringen soll als dem Staatsbetrieb “Bahn„.[30]

Beim Bundesnachrichtendienst (BND) wurden die Computer von Mitarbeitern durchsucht. Das Bundesverwaltungsgericht stellte später fest, dass dies illegal war.

In einem anderen Fall benutzte ein Beamter des BND, der für die Überwachung einiger Botschaften zuständig war die ihm zur Verfügung stehenden technischen Möglichkeiten, um einer Affäre seiner Frau hinterherzuschnüffeln.[31]

Während des Prozesses zur „Militanten Gruppe“ („mg“), in der der Berliner Soziologe Andrej Holm Mitglied zu sein beschuldigt wurde, log ein als Zeuge auftretender BKA-Mitarbeiter und das BKA legte dem Gericht manipulierte Akten vor.[32]

Dies Fälle zeigen, dass der Missbrauch polizeilicher Befugnisse häufig genug dokumentiert ist, um ihn als wichtiges Argument gegen weitere Befugnisse ins Feld zu führen, auch wenn er sicherlich nicht der Normalfall ist.

7.3 Verhandlung vor dem Bundesverfassungsgericht

Bei der Verhandlung zum nordrhein-westfälischen Verfassungsschutzgesetz vor dem Bundesverfassungsgericht wurde unter anderem kritisiert, dass kein Richtervorbehalt vorgesehen ist.

„Mensch und Computer würden in naher Zukunft immer engere symbiotische Verbindungen eingehen, wie es bei Menschen mit intelligenten Hörgeräten heute bereits ersichtlich werde: ‚Wir werden in diese Rechner zunehmend verloren gegangene Fähigkeiten auslagern, um sie so wiederzugewinnen. Wir werden an sie persönlichste Denk- und Merkfunktionen delegieren, um uns zu entlasten,‘ so Pfitzmann in seiner Argumentation.„[33]

Als Beispiel nannte Pfitzmann implantierbare Rechner, etwa intelligente Hörgeräte. Es gehe daher in Zukunft beim Thema Online-Durchsuchung um den „Schutz des autonomen und unbeobachteten Denkens.“[33]

Vertreter der Landesregierung NRW Heckmann: „Es geht hier nicht um das Auslesen des gesamten Festplatteninhalts!“ Daraufhin der Präsident des Bundesverfassungsgerichts Papier: „Ich gestatte mir die Frage, ob wir vom gleichen Gesetz ausgehen!“[34]

Als Alternative schlug Pfitzmann vor, man könne die physische Abstrahlung des Endgeräts zur Erhebung der Daten verwenden. Dies biete kein Missbrauchspotential in Richtung Massenüberwachung, sei aber dennoch wirksam. Zur Machbarkeit verwies er auf einen Bericht, den Experten unter anderem vom CCC dem Verfassungsgericht zum Abhören von Wahlcomputern vorgelegt hatten.[35]

7.4 Urteil des Bundesverfassungsgerichts

Das Bundesverfassungsgericht stellte fest, dass die präventive Online:Durchsuchung durchaus verfassungskonform geregelt werden kann, das vorliegende Gesetz aber eindeutig verfassungswidrig sei.[7]

Mit dem Urteil wurde auch das neue „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ (auch „IT-Grundrecht“ oder „di-

gitale Intimsphäre“) geschaffen. Ein neues Grundrecht hatte das Verfassungsgericht zuletzt 1983 im Rahmen des Volkszählungsurteils mit den „Grundrecht auf informationelle Selbstbestimmung“ geschaffen.[63]

Die Online-Durchsuchung zur Gefahrenabwehr ist nur zulässig, wenn eine entsprechende gesetzliche Regelung für diese geschaffen wird, wobei der Einsatz auch dann nur zur Abwehr einer konkreten Gefahr für ein überragend wichtiges Rechtsgut vorgenommen werden darf, wenn klare Anhaltspunkte für diese Gefahr vorhanden sind und ein Richter den Einsatz anordnet.[7, 63]

Von diesen hohen Hürden gibt es jedoch eine Ausnahme für die Durchführung einer reinen Quellen-TKÜ, wobei dann rechtliche und technische Regelungen getroffen werden müssen, um zu verhindern, dass aus der Quellen-TKÜ eine volle Online-Durchsuchung wird.[63]

Um eine solche technische Schranke in einer sicheren Form zu Schaffen, muss eigentlich sichergestellt werden, dass das verwendete Programm genau die definierten Fähigkeiten hat und nicht mehr. Dazu ist eine unabhängige Kontrolle der Software notwendig, bei der der Quelltext vorliegt und genau genommen müsste man dann einen formalen Korrektheitsbeweis für diese Software führen und ebenfalls sicherstellen, dass das erstellte Binärprogramm exakt dem Quelltext entspricht.

Andernfalls könnte das Programm wie man etwa an den Einreichungen beim „Underhanded C Contest“ oder in „Reflections on Trusting Trust“ von Ken Thompson[36] sehen kann licht Funktionen haben könnte, die es nicht haben darf, ohne dass man es auch bei genauem Hinschauen sähe.

7.5 Nutzen

Nach Aussage eines Bundesanwalts ist die Aufdeckung oder Vereitlung von Straftaten mit Hilfe der Online-Durchsuchung eher die Ausnahme.[37] Es fragt sich, ob diese Ausnahmen der Grund für die vehemente Verteidigung der Online-Durchsuchung durch Politiker und Sicherheitsbehörden ist, oder ob etwas anderes dahinter steckt.

Auf dem europäischen Polizeikongress äußerte sich ein IT-Experte der Berliner Polizei wie folgt: „Ich frage mich, gegen wen sich das vorgeschlagene Gesetz eigentlich richtet. Wenn wir wissen, dass wir mit unseren Tools nicht gegen die OK [organisierte Kriminalität] und Geldwäsche ankommen, weil die strikt Klartextdateien nur auf separaten Rechnern führen, dann müssen wir uns fragen, was unter dem Deckmantel der terroristischen Bedrohung passiert. Wir produzieren dann nur gemeinte Sicherheit und fangen Otto Normalverbraucher, der mal ein paar Dateien aus dem Netz geladen hat, ob das Nazireden oder Pornografie ist. Da habe ich als Beamter ein großes Problem.”[22]

Wie die Vorratsdatenspeicherung würde die Online-Durchsuchung gegen file sharing vielleicht mehr helfen, als gegen Terrorismus.

7.6 Nach der Analyse

Bei der Veröffentlichung seiner Analyse gab der CCC keine Hinweise darauf, von welcher Behörde der Trojaner angewandt worden sein könnte. Er wurde auch deshalb recht

neutral als „Staats"- oder „Behördentrojaner" bezeichnet, statt den alten Kampfbegriff „Bundestrojaner" zu verwenden. Dies hatte zur Folge, dass sich zunächst die Landeskriminalämter, das Bundeskriminalamt und das Zollkriminalamt beziehungsweise die für diese zuständigen Ministerien sich gegenseitig den Scharzen Peter zuschoben und jeweils beteuerten den Trojaner selbst nicht eingesetzt zu haben. Nur zwei Tage nach der Veröffentlichung begannen die ersten Landesregierungen zuzugeben, dass sie den Trojaner einsetzten. Zuerst Niedersachsen, Brandenburg, Baden-Württemberg und Bayern, später auch Rheinland-Pfalz, Nordrhein-Westfalen, Schleswig-Holstein, Bremen und Hamburg.[38, 39, 40, 41, 42, 43, 44, 45, 46] Die hessische Landesregierung gab bekannt, man habe nur Software für die Quellen-TKÜ eingesetzt, und sich dabei strikt an den rechtlichen Rahmen gehalten[47] (der aber laut eines Aufsatzes in „Kommunikation & Recht" eigentlich nicht vorhanden ist[48]), so wie auch andere Behörden beteuert haben, sich stets an geltendes Recht gehalten zu haben. Auch das Zollkriminalamt gab zu den Staatstrojaner von DigiTask eingesetzt zu haben.[49]

Kurz nach Veröffentlichung der Analyse des CCC beteuerte Bundesinnenminister Friedrich (CSU), „Unsere Beamten halten sich strikt an das, was sie dürfen." „Die Behauptung, sie hätten mehr gemacht, ist falsch." Diese Behauptung stand zu diesem Zeitpunkt eigentlich gar nicht zur Debatte. Der wesentliche Kritikpunkt war nicht, dass die Polizei mit Hilfe des Staatstrojaners mehr als eine Quellen-TKÜ gemacht hat, sondern dass der Staatstrojaner dadurch, dass er mehr als eine Quellen-TKÜ ohne Probleme erlaubt, grundsätzlich nicht hätte eingesetzt werden dürfen.[50]

Seitens der Innenminister der Länder, etwa des Bayerischen Innenministers Joachim Herrmann hieß es, der CCC setze falsche Behauptungen in die Welt, ohne Details zu nennen, was denn genau falsch sei. Vom Unions-Bundestagsfraktionsvize Günter Krings kam der Vorwurf, der CCC „habe die Sicherheitsbehörden des Bundes leichtfertig unter Generalverdacht gestellt", obwohl der CCC nicht behauptet hatte, dass die Malware von einer Bundesbehörde eingesetzt worden wäre.[51]

Trotz des Urteils des Landgerichts Landshut, das feststellte, dass in einem Fall das Erstellen von ca. 4000 Screenshots illegal war, behauptete Krings weiter, es gäbe „keinerlei Belege dafür, dass die analysierte Software tatsächlich illegal eingesetzt worden sei".[51]

Da Bayerische Landesinnenministerium argumentierte, das Erstellen dieser Bildschirmfotos sei rechtens gewesen und verwieß „darauf, dass es dazu noch keine höchstrichterliche Entscheidung" gäbe, so als sei die Entscheidung des Landgerichts für das Ministerium nicht bindend. Tatsächlich ist aber bei solchen Beschlüssen das Landgericht die höchste Instanz.[51, 52]

8 Vorstellungen der Behörden und Politiker

BKA-Präsident Ziercke: „Kriminelle laden [sic] diese Daten, die man auf der Festplatte normalerweise hat, ins World Wide Web aus. Das heißt, der Speicherplatz ist das Internet irgendwo weltweit."[53]

Ziercke: Es würden keine Applikationen eingesetzt, durch die sich Daten löschen oder verändern lassen würden. „Wir müssen keine Schwachstellen ausnutzen." Weiter hieß es

„der Quellcode ‚einer solchen Untersuchung' könne beim Gericht hinterlegt werden."[54]

Schäuble am 15. 5. 2007: „wenn Sie wollen, kann der Herr Fromm das auch genauer erläutern, der versteht's ein wenig – richtig verstehen tut er es wahrscheinlich auch nicht, denn das wäre auch nicht gut, wenn der Präsident des Bundesamtes für Verfassungsschutz ein Online-Experte wäre."[55, 56]

Angesprochen darauf, dass die Bundesanwaltschaft trotz mangelnder Rechtsgrundlage die Online-Durchsuchung angewendet habe, antwortete die Generalbundesanwältin Harms: „Von uns nicht!", woraufhin der SPIEGEL entgegnete, die Online-Durchsuchung sei von der Bundesanwaltschaft „zumindest zweimal beantragt" worden.[57]

netzpolitik.org veröffentlicht Fragenkatalog der SPD an das Bundesinnenministerium zur Online-Durchsuchung mit den dazugehörigen Antworten.[58]

- „Die Analyse der RFS (Disassembling) wird jedoch durch die Verwendung kryptographischer Methoden nahezu unmöglich gemacht."

  Aus technischer Sicht ist dies natürlich Unsinn. Um vom Prozessor ausgeführt werden zu können müssen die Instruktionen des Programms spätestens zum Zeitpunkt der Ausführung unverschlüsselt vorliegen. Die Instruktionen können dann mit Hilfe eines Emulators ohne Probleme extrahiert werden. Kryptographische Methoden können die Analyse vielleicht ein bisschen arbeitsaufwendiger machen, ein echtes Hindernis kann dies aber grundsätzlich nicht sein. Interessanterweise wurde auch kaum Obfuscation betrieben, von kryptographischen Methoden ganz zu schweigen.

- „Die Sicherheitsbehörden und das Bundesministerium des Innern verfügen grundsätzlich über genügenden Sachverstand."

  Interessanterweise sind diese aber nicht in der Lage, sich wirksam gegen chinesische Spionageprogramme zu schützen, wie sollen das dann einfache Bürger schaffen, bei denen der Bundestrojaner möglicherweise „Beweise" findet? [59]

- „Es ist nicht zu erwarten, dass die RFS entdeckt wird."

  Wie sich später zeigte war das offensichtlich nicht richtig. Im Vergleich mit sonstiger Malware fällt auf, dass fast keine Tarnung der Funktionen vorhanden ist. Insbesondere ist der komplette Maschinencode weder verschlüsselt und noch gepackt. Warum man davon ausging, dass mit einer Entdeckung nicht zu rechnen sei bleibt unklar.

- „Die RFS wird so entwickelt, dass von ihr nach dem aktuellen Stand der Technik keine Schadfunktionen ausgehen."

- „Mit der Online-Durchsuchung werden keine Personen ausgespäht, sondern relevante Erkenntnisse auf informationstechnischen Systemen erhoben."

  Gehören die Daten aus denen die „relevanten Erkenntnisse" gewonnen werden nicht irgendwelchen Personen? Hier geht es offensichtlich nicht um den Inhalt, sondern darum, den Sachverhalt euphemistisch zu beschreiben.

- „Bei der hier in Rede stehenden RFS handelt es sich nicht um eine „Spionagesoftware", sondern um ein technisches Mittel zur Datenerhebung."

  Was da der Unterschied ist, abgesehen davon, dass es auf den ersten Blick weniger negativ klingt ist ebenfalls fraglich.

- „Das Bundeskriminalamt hat beim (verdeckten) Zugriff auf das informationstechnische System kein Interesse an der Kenntnisnahme etwa von Krankheitsberichten, Tagebüchern oder Liebesbriefen."

  Soll diese Behauptung die technischen und rechtlichen Hürden, die solche Zugriffe verhindern sollen, darstellen? Und was ist mit einzelnen Mitarbeiter? Da könnte es schließlich auch Begehrlichkeiten geben.

- „Speziell wird sichergestellt, dass die Software nicht ohne erheblichen Aufwand dazu veranlasst werden kann, an einen anderen Server, als den vom Bundeskriminalamt verwendeten zurückmelden, und dass die Software weder von außen erkannt noch angesprochen werden kann. Das Entdeckungsrisiko kann durch technische Maßnahmen reduziert werden."

  Die Verwendung eines anderen Servers zu erreichen ist gemäß der Analyse des CCC einfach möglich, indem man, sich als Server des BKA ausgebend, den Trojaner neue Binärdateien laden und ausführen lässt. Weiterhin kann man von einem anderen Rechner dem Server ohne weiteres Nachrichten die scheinbar vom überwachten Rechner kommen, unterschieben.

- „. . . oder sogar die Beendigung der Maßnahme wegen eines zu hohen Entdeckungsrisikos angezeigt erscheinen lassen, erfolgt die Anweisung an das Programm sich selbst zu deinstallieren."

  Das ist ein interessanter Aspekt, wenn man bedenkt, dass die Software ja angeblich von außen weder erkannt noch angesprochen werden kann.

Kriminalhauptkommissar Mirko Manska sagte: „Der PC wird mit kleinen Programmen infiziert, die sich erst hinter dem Firewall zum schädlichen Trojaner zusammensetzen."[60]

9 Kosten

2006 hieß es noch, die Kosten für das Tool zur Online-Durchsuchung sollen sich auf nicht mehr als 200.000 € belaufen[6], tatsächlich sie die Realität wie 2011 öffentlich bekannt wurde anders aus.

Hier ein kleiner Teil davon, was verschiedene Behörden bei DigiTask zu welchem Preis erworben haben. Die Daten stammen allesamt aus dem „Supplement zum Amtsblatt der Europäischen Union."

Behörde	Betrag	Beschreibung
LKA Baden-Württemberg	1 218 225,35 €	Lieferung einer TKÜ-Anwendung und Dienstleistung zur Erstellung eines kompletten TKÜ-Systems für die Polizei des Landes Baden-Württemberg sowie die Wartung des kompletten Systems.[1]
LKA Bayern	247 773,47 €	Erweiterung des TKÜ-Systems um ein Archivsystem, Teilbereich 1.[2]
Zollkriminalamt	2 075 256,07 €	Lieferung von Hard- und Software zur Telekommunikationsüberwachung (TKÜ).[3]
Zollkriminalamt	551 112,00 €	TKÜ Auswerte - SW.[4]
Zollkriminalamt	208 750,38 €	TKÜ Auswerte Hardware u. Softwarelizenzen.[5]

Als Reaktion auf die eklatanten Mängel an dem von DigiTask gelieferten Trojaner wurden auch die Pläne, das BKA könne die benötigte Software selbst programmieren, wieder aus der Schublade geholt. Es hieß sogar, das BKA habe bereits für 680 000 € an Personal- und Sachkosten die „entsprechende Software ... für Online-Durchsuchungen codiert."[61]

10 Reaktionen

Anfang 2012 stellte das Bundesamt für Sicherheit in der Informationstechnik (BSI) unter der Adresse `http://dns-ok.de` eine Seite zur Verfügung, von der Nutzer testen lassen konnten, ob ihr Rechner mit dem DNS-Changer-Trojaner infiziert war. Viele Nutzer taten dies jedoch nicht, da sie fürchteten, dies könne ein Trick sein, mit dem das BSI versuchen könnte ihnen den Staatstrojaner unterzuschieben.[62] Dies zeigt deutlich, wie sehr das Vertrauen der Bevölkerung in die Behörden durch die Online-Durchsuchungen geschädigt wurde. In diesem Fall nehmen Nutzer sogar in Kauf, dass sie nicht erfahren, ob ihr Rechner tatsächlich mit dem DNS-Changer infiziert ist aus Angst vor dem Bundestrojaner.

Literatur

[1] „Schily erlaubte Online-Durchsuchungen" *tagesschau*, 25. 04. 2007, `http://www.tagesschau.de/inland/meldung21410.html` (01. 01. 2012).

[1] `http://ted.europa.eu/udl?uri=TED:NOTICE:23600-2008:TEXT:DE:HTML`
[2] `http://ted.europa.eu/udl?uri=TED:NOTICE:307886-2008:TEXT:DE:HTML`
[3] `http://ted.europa.eu/udl?uri=TED:NOTICE:26158-2009:TEXT:DE:HTML`
[4] `http://ted.europa.eu/udl?uri=TED:NOTICE:70229-2008:TEXT:DE:HTML&src=0`
[5] `http://ted.europa.eu/udl?uri=TED:NOTICE:70231-2008:TEXT:DE:HTML&src=0`

[2] „132 Millionen Euro für Terrorabwehr", *SPIEGEL ONLINE*, Stand 25.10.2006, http://www.spiegel.de/politik/deutschland/0,1518,444687,00.html (01. 01. 2012).

[3] „Medienbericht: BND hat bereits Online-Razzien durchgeführt", *Heise Newsticker*, 5. 1. 2008, http://heise.de/-175499 (9. 1. 2012).

[4] „Verfassungsbeschwerde gegen NRW-Verfassungsschutzgesetz angekündigt", *Heise Newsticker*, 20. 12. 2006, http://www.heise.de/-128613.html (01. 01. 2012).

[5] Bundesgerichtshof, „Verdeckte Online-Durchsuchung unzulässig", Stand 05. 02. 2007, http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2007&Sort=3&nr=38775&pos=0&anz=16 (01. 01. 2012).

[6] „Heimliche Online-Durchsuchungen sind unzulässig", *Heise Newsticker*, Stand 05. 02. 2007, http://heise.de/-142370 (01. 01 2012).

[7] Urteil des Bundesverfassungsgericht vom 27. 2. 2008, http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html (14. 1, 2012).

[8] „Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt", *Bundesgesetzblatt*, Teil 1, Nr. 66, http://www.bgbl.de/Xaver/start.xav?startbk=Bundesanzeiger_BGBl&bk=Bundesanzeiger_BGBl&start=//*%5B@attr_id=%27bgbl108s3083.pdf%27%5D (15. 1. 2012).

[9] „Schäuble plant vorbeugenden Lauschangriff", *netzzeitung.de*, 12. 7. 2007, http://www.netzeitung.de/deutschland/692770.html (30. 12. 2011).

[10] „Saarland: Eindringen in Wohnungen für heimliche Online-Durchsuchungen", *Heise Newsticker*, 29. 7. 2008, http://heise.de/-190948 (30. 12. 2011).

[11] „Staatstrojaner gegen Drogendealer: Heimlicher Einbruch bei Dieben", *taz.de*, 11. 10. 2011, http://taz.de/!79701/ (14. 1. 2012).

[12] „Fahnder: Massiver Eingriff", *SPIEGEL Online*, 28. 2. 2011, http://www.spiegel.de/spiegel/0,1518,748110,00.html (14. 1. 2012).

[13] „Chaos Computer Club analysiert Staatstrojaner", *Pressemitteilung des Chaos Computer Clubs*, 8. 10. 2011, http://ccc.de/de/updates/2011/staatstrojaner (29. 12. 2011).

[14] „Die Software von Innen: Der Text des Staatstrojaners", *FAZ*, 8. 10. 2011, http://www.faz.net/aktuell/feuilleton/-11487209.html (15. 1. 2012).

[15] Ausschnitt aus der FAS vom 9. 10. 2011, http://www.faz.net/dynamic/download/fas/FAS_09_2011_S41_S47_Staatstrojaner.pdf (15. 1. 2012).

[16] „Chaos Computer Club analysiert aktuelle Version des Staatstrojaners", *Pressemitteilung des Chaos Computer Clubs*, 26. 10. 2011, http://ccc.de/de/updates/2011/analysiert-aktueller-staatstrojaner (14. 1. 2012).

[17] Thomas Oppermann (SPD), gepostet bei Twitter, https://twitter.com/#!/ThomasOppermann/status/126584988882829312 (15. 1. 2012).

[18] „Skype-Datenschutzrichtlinien", http://www.skype.com/intl/de/legal/privacy/general/ (15. 1. 2012).

[19] „EU-Strafermittler nehmen Vorwürfe gegen Skype zurück", *heise online*, http://heise.de/-202086 (15. 1. 2012).

[20] „Generalbundesanwältin fordert Vertrauen in Ermittlungsmaßnahmen", *Heise Newsticker*, 30. 10. 2008, http://heise.de/-214473 (30. 12. 2011).

[21] „Internetrechtler: Vorratsdatenspeicherung dient dem Schutz der Menschenwürde", *Heise Newsticker*, 9. 12. 2008, http://heise.de/-187860 (30. 12. 2011).

[22] „Europäischer Polizeikongress: Polizei vor dem Umbruch", *Heise Newsticker*, 31. 1. 2008, http://heise.de/-185597 (30. 12. 2011).

[23] „Durch Google-Suche in die Einzelhaft", *Heise Newsticker*, 22. 8. 2007, http://heise.de/-165722 (14. 1. 2012).

[24] „De Maizière will heimliche Online-Durchsuchungen auch zur Strafverfolgung", *Heise Newsticker*, 24. 09. 2010, http://heise.de/-1095801 (14. 1. 2012).

[25] „10 bis 20 Fälle", *Hanno's Blog*, 31. 10. 2007, http://www.hanno.de/blog/2007/10-bis-20-faelle/ (15. 1. 2012).

[26] „BKA-Chef will Bundestrojaner auch gegen organisierte Kriminalität einsetzen", *Heise Newsticker*, 20. 1. 2009, http://heise.de/-199929 (30. 12. 2011).

[27] „ ‚Trojaner' für Hooligans?", *Wormser Zeitung*, 20. 9. 2007, http://web.archive.org/web/20080616101913/http://www.wormser-zeitung.de/rhein-main/objekt.php3?artikel_id=2976294 (15. 1. 2012).

[28] „Harsche Kritik an Online-Durchsuchungen", *Heise Newsticker*, 3. 2. 2007, http://heise.de/-142144 (01. 01. 2012).

[29] „Zollfahnder belauschen Web-Telefonate", *SPIEGEL Online*, 9. 10. 2010, http://www.spiegel.de/netzwelt/netzpolitik/0,1518,722221,00.html (30. 12. 2011).

[30] „Computer-Manipulation bei der Bahn: Allumfassende Überwachung", *Frankfurter Rundschau*, 23. 4. 2009, http://www.fr-online.de/datenschutz/computer-manipulation-bei-der-bahn-allumfassende-ueberwachung,1472644,2772996.html (14. 1. 2012).

[31] Felix von Leitner, *Fefes Blog*, 31. 8. 2007, http://blog.fefe.de/?ts=b82928f2 (15. 1. 2012).

[32] „BKA Zeuge lügt – Bundeskriminalamt manipuliert Akten: Pressemitteilung der Verteidigung im ‚mg'-Verfahren", 26. 3. 2009, http://einstellung.so36.net/de/pm/1352 (15. 1. 2012).

[33] „Informatiker plädiert bei der Verhandlung vorm Bundesverfassungsgericht für ‚Schutz des Denkens'", *heise online*, 10. 10. 2007, http://heise.de/-183531 (15. 1. 2012).

[34] „NRW-Regierung: ‚Hier gibt es keine Online-Durchsuchung'", *heise online*, 10. 10. 2007, http://heise.de/-183591 (15. 1. 2012).

[35] Sprechzettel des Experten bei der Verhandlung vorm Bundesverfassungsgericht Andreas Pfitzmann, http://dud.inf.tu-dresden.de/literatur/BVG2007-10-10.pdf (15. 1. 2012).

[36] Ken Thompson: „Reflections on Trusting Trust", *Communication of the ACM*, Vol. 27, No. 8, August 1984, S. 761-763, http://cm.bell-labs.com/who/ken/trust.html

[37] „Bundesanwalt bezweifelt Sinn von Online-Razzien", *SPIEGEL Online*, 7. 12. 2007, http://www.spiegel.de/politik/debatte/0,1518,521984,00.html (9. 1. 2012).

[38] „Niedersachsen wechselte Trojaner-Lieferanten ", *NDR.de*, 12. 10. 2011, http://www.ndr.de/regional/niedersachsen/bundestrojaner101.html (14. 1. 2012).

[39] „Brandenburg setzt Trojaner-Software ein", *Berliner Morgenpost*, 10. 10. 2011, http://www.morgenpost.de/newsticker/dpa_nt/regioline_nt/berlinbrandenburg_nt/article1789549/Brandenburg-setzt-Trojaner-Software-ein.html (14. 1. 2012).

[40] „Baden-Württemberg stoppt den Trojaner-Einsatz", *Badische Zeitung*, 10. 10. 2011, http://www.badische-zeitung.de/nachrichten/deutschland/baden-wuerttemberg-stoppt-den-trojaner-einsatz--50456952.html (14. 1. 2012).

[41] „Pressemitteilung Nr. 385/11", *Bayrisches Staatsministerium des Innern*, 10. 10. 2011, http://www.stmi.bayern.de/presse/archiv/2011/385.php (14. 1. 2012).

[42] „#0zapftis: Auch Polizei Rheinland-Pfalz arbeitet mit Staatstrojaner", *Netzpolitik.org*, 11. 10. 2011, https://netzpolitik.org/2011/0zapftis-auch-polizei-rheinland-pfalz-arbeitet-mit-staatstrojaner/ (14. 1. 2012).

[43] „Auch NRW-Polizei setzte Trojaner ein", *DerWesten*, 11. 10. 2011, http://www.derwesten.de/unresolved/auch-nrw-polizei-setzte-trojaner-ein-id5150937.html (14. 1. 2012).

[44] „Staatliche Überwachung auch in SH außer Kontrolle? ", *Pressemitteilung der Piratenpartei Schleswig-Holstein*, 11. 10. 2011, http://piratenpartei-sh.de/index.php/presse/pressemitteilungen/458-staatsueberwachung-auch-in-sh-ausser-kontrolle (14. 1. 2012).

[45] „POL-HB: Nr.:–0418– Informationen zum Einsatz einer ‚Bundestrojaner'-Software", *Pressemitteilung der Polizei Bremen*, 12. 10. 2011, http://www.presseportal.de/polizeipresse/pm/35235/2128673/pol-hb-nr-0418-informationen-zum-einsatz-einer-bundestrojaner-software/ (14. 1. 2012).

[46] „Auch Hamburg setzte Überwachungssoftware ein", *WELT ONLINE*, 12. 10. 2011, http://www.welt.de/print/die_welt/hamburg/article13655724/Auch-Hamburg-setzte-Ueberwachungssoftware-ein.html (14. 1. 2012).

[47] „Landeskriminalamt: ‚Staatstrojaner' nicht eingesetzt", *hr-online.de*, 10. 10. 2011, http://www.hr-online.de/website/rubriken/nachrichten/indexhessen34938.jsp?rubrik=34954&key=standard_document_42836926 (14. 1. 2012).

[48] Dr. Frank Braun: „0zapftis – (Un)Zulässigkeit von ‚Staatstrojanern' ", *Kommunikation & Recht*, 10/2011, http://www.kommunikationundrecht.de/delegate/resources/dok751.pdf?fileid=dok751.pdf_kur&type=asset (14. 1. 2012).

[49] „DigiTask-Software: Zollkriminalamt ermittelte 19-mal per Staatstrojaner", *SPIEGEL Online*, 12. 10. 2011, http://www.spiegel.de/netzwelt/netzpolitik/0,1518,791434,00.html (14. 1. 2012).

[50] „Online-Durchsuchung: Friedrich verteidigt Überwachung durch Trojaner", *FAZ*, 15. 10. 2011, http://www.faz.net/aktuell/politik/online-durchsuchung-friedrich-verteidigt-ueberwachung-durch-trojaner-11494164.html (14. 1. 2012).

[51] „Trojaner zur Telefonüberwachung: Freistaat Bayern verteidigt Spähangriff", *Süddeutsche.de*, 11. 10. 2011, http://www.sueddeutsche.de/digital/trojaner-vorwurf-gegen-bayern-herrmann-verteidigt-erfolgte-spaehangriffe-als-zulaessi
1158830 (14. 1. 2012).

[52] Felix von Leitner, *Fefes Blog*, 11. 10. 2011, http://blog.fefe.de/?ts=b06ae3d7 (14. 1. 2012).

[53] Bernd Kling, „Die Vaporware des BKA", *Telepolis* Stand 19. 2. 2007, http://www.heise.de/tp/artikel/24/24678/1.html (01. 01. 2012).

[54] „BKA-Präsident: Online-Durchsuchung klappt ohne Schadsoftware", *Heise Newsticker*, 27. 03. 2007, http://heise.de/-161841.

[55] „Schäuble stoibert über die Online-Durchsuchung", Netzpolitik.org, 07.06.2007, http://netzpolitik.org/2007/schaeuble-stoibert-ueber-die-online-durchsuchung/ (01. 01. 2012).

[56] Teilmitschnitt der Bundespressekonferenz vom 15. 05. 2007, http://www.netzpolitik.org/wp-upload/schaueble_onlinedurchsuchung.mp3 (01. 01. 2012).

[57] Der Spiegel 22/2007, 26. 5. 2007 http://www.spiegel.de/spiegel/print/d-51714176.html (30. 12. 2011).

[58] „Bundesinnenministerium beantwortet Fragen zur Online-Durchsuchung", *netzpolitik.org*, 27. 8. 2007, http://netzpolitik.org/2007/bundesinnenministerium-beantwortet-fragen-zur-online-durchsuchung/, http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (30. 12. 2011).

[59] „Chinesische Trojaner auf PCs im Kanzleramt", *SPIEGEL Online*, 25. 8. 2009, http://www.spiegel.de/netzwelt/tech/0,1518,501954,00.html (9. 1. 2012).

[60] „Das BKA berichtet aus der unsicheren digitalen Welt", *heise online*, 10. 11. 2006, http://heise.de/-198300 (15. 1. 2012).

[61] „Staatstrojaner-Enthüllung: Minister mokiert sich über Chaos Computer Club", *SPIEGEL Online*, 16. 10. 2011, http://www.spiegel.de/netzwelt/netzpolitik/0,1518,792072,00.html (14. 1. 2012).

[62] „Angst vor einem Staatstrojaner: Internetnutzer trauen dns-ok.de nicht", *FOCUS Online*, 12. 1. 2012, http://www.focus.de/digital/internet/angst-vor-dem-staatstrojaner-internetnutzer-trauen-dns-ok-de-nicht_aid_701936.html (13. 1. 2012).

[63] Ulf Buermeyer, Constanze Kurz, Frank Rieger und Thorsten Schröder, „Der Staatstrojaner: Vom braunen Briefumschlag bis zur Publikation", http://media.ccc.de/browse/congress/2011/28c3-4901-de-der_staatstrojaner_aus_sicht_der_technik.html (14. 1. 2012).