Erschien in: Alcatel-Lucent Stiftung (Hrsg.): Mensch, Technik, Kommunikation; Beiträge zur Informatisierung in Gesellschaft, Recht, Ökonomie und Technik; ISBN 978-3-00-028947-7; Oktober 2009, Seite 143-159

Möglichkeiten und Grenzen der Nutzungsüberwachung von Informations- und Kommunikationssystemen in einer freiheitlichen demokratischen Gesellschaft an den Beispielen Vorratsdatenspeicherung und Online-Durchsuchung[1]

Andreas Pfitzmann, Stefan Köpsell
Lehrstuhl Datenschutz und Datensicherheit, Fak. Informatik, TU Dresden

V0.13, 16.10.2009

Zusammenfassung

Eine systematische Darstellung und Analyse der Möglichkeiten und Grenzen, wie der Gebrauch von Informations- und Kommunikationstechnik in einer freiheitlichen demokratischen Gesellschaft überwacht werden kann, ergibt:

Eine *Vorratsdatenspeicherung von Kommunikationsdaten* sollte unterlassen werden, da sie eine bedeutende zusätzliche Sicherheitslücke schafft, zu Überwachende ihr vergleichsweise leicht ausweichen können und ihr Übermaß eine gesellschaftliche Akzeptanz für andere, sehr viel zielgerichtetere und zweckgeeignetere Überwachungsmaßnahmen vermutlich verhindert.

Hält man es für notwendig, zusätzliche Sicherheitslücken zu schaffen, dann ist eine *Vorratsdatenspeicherung von digitalen Zahlungsvorgängen* zielgerichteter als eine Vorratsdatenspeicherung von Kommunikationsdaten. Ihr kann weit weniger gut ausgewichen werden und sie ist zur Aufdeckung krimineller und terroristischer Strukturen vermutlich genauso gut, wenn nicht besser geeignet.

Deutlich weniger kritisch als die Schaffung zusätzlicher Sicherheitslücken ist die Nutzung ohnehin bestehender. Prominentestes Beispiel für die Nutzung ohnehin bestehender Sicherheitslücken ist die so genannte Online-Durchsuchung.

Falls eine *Online-Durchsuchung* in begründeten Fällen erlaubt werden soll, ist als Eindringmethode ausschließlich der „physische Zugriff auf das Endgerät“ zu erlauben. Wo immer möglich, sollte statt einer Online-Durchsuchung eine *verdeckte Analyse der physischen Abstrahlung des Endgeräts* durchgeführt werden. Sie ergibt nur Erkenntnisse über die gegenwärtige Datenverarbeitung. Sollten Erkenntnisse über vergangene Datenverarbeitung benötigt werden, kann die verdeckte Analyse der physischen Abstrahlung des Endgeräts mit einer späteren offenen Beschlagnahme des Endgeräts kombiniert werden.

[1] Dieser Aufsatz erweitert die dem BVerfG am 26. Sept. 2007 anlässlich der Verhandlung zur so genannten Online-Durchsuchung vorgelegte Papier „Andreas Pfitzmann: Möglichkeiten und Grenzen der Nutzungsüberwachung von Informations- und Kommunikationssystemen in einer freiheitlichen demokratischen Gesellschaft“ um eine vertiefte Diskussion des Beispiels Vorratsdatenspeicherung.

1 Einführung

Abhörschnittstellen, Zahlungsstromüberwachung, Vorratsdatenspeicherung, Online-Durchsuchung, Video-Überwachung, Fingerabdruck-Biometrie in Reisepässe – der Staat rüstet auf mit dem Ziel, sich und seine Bürger zu schützen. Aber welche dieser Maßnahmen schützen die Bürger mehr, als dass sie sie gefährden? Welche dieser Maßnahmen stärken das Vertrauen und den Zusammenhalt innerhalb der Gesellschaft und zwischen Bürgern und Staat? Welche stellen dagegen wichtige Vertrauensverhältnisse in Frage und schwächen so die freiheitliche demokratische Gesellschaft?

Leider können auch wir Wissenschaftler nicht alle Fragen beantworten. Aber wir wollen einerseits dazu beitragen, dass keine wichtigen Fragen vergessen oder gar unterschlagen werden. Andererseits sind manche Antworten durchaus möglich – auch wenn sie manchen Akteuren unbequem erscheinen mögen.

Nachfolgend erläutern wir zuerst wichtige Fakten über die Informations- und Kommunikationstechnik, ihre Unsicherheit sowie die mögliche Entwicklung. Hieraus ergeben sich wichtige Grundsätze für den Umgang einer hoch entwickelten Gesellschaft mit dieser Technik. Vor diesem Hintergrund ziehen wir dann Schlussfolgerungen bezüglich Vorratsdatenspeicherung und Online-Durchsuchung. Wir schließen mit der sich ergebenden Empfehlung, eine Vorratsdatenspeicherung von Kommunikationsdaten zu unterlassen.

2 Technische Fakten

Informationstechnik (IT) hat in den letzten zwei Jahrzehnten eine Komplexität erreicht, mit der weder die Wissenschaft Informatik einschließlich der durch sie bereitgestellten Werkzeuge zum Entwurf und zur Analyse von IT noch unsere Fähigkeit, IT-Systeme zu betreiben, Schritt gehalten haben. Im Ergebnis sind heute viele IT-Systeme abenteuerlich unsicher – auch angeblich gut gesicherte IT-Systeme sind durch Fachleute erfolgreich angreifbar.

Kommunikationstechnik (KT) basiert zunehmend auf IT, so dass die Knoten der KT zur Übertragung von Daten durch Fachleute erfolgreich angreifbar sind. Werden Daten vor der Übertragung nicht verschlüsselt, sind sie also weitestgehend ungeschützt – gegenüber einem Zugriff auf einen der Knoten, die sie durchlaufen, wie auch auf den Kommunikationskanälen.

IT und KT wachsen zunehmend zur Informations- und Kommunikationstechnik (IKT) zusammen (d.h. multifunktionale Endgeräte verbunden durch Kommunikationstechnik), was die Unsicherheit steigert und immer mehr Akteuren erfolgreiche Angriffe ermöglicht.

Selbst bei größten Anstrengungen aller Beteiligten (insbesondere der IKT-Hersteller, Betreiber und Nutzer) wird eine rein marktgetriebene deutliche Verringerung der Unsicherheit von IKT etliche Jahrzehnte dauern. Um eine deutliche Steigerung der Sicherheit von IKT in überschaubaren Zeiträumen zu erreichen, wäre eine nur regulatorisch herbeiführbare, drastische Komplexitätsreduktion nötig, die unweigerlich mit einer Funktionsreduktion einherginge. Dies erscheint so wenig durchsetzbar, dass darüber nicht einmal nachgedacht wird.

Es ist zu erwarten, dass für weit verbreitete persönlich genutzte Endgeräte (u.a. alle Arten von Telefonen, PDAs, Laptops, Desktop-PCs) Eigentümer und Benutzer identisch sind

(*Eigennutzer*) und diese Endgeräte u.a. aus marktwirtschaftlichen Gründen vorwiegend für die (Sicherheits-)Interessen ihrer Eigennutzer gebaut werden. Andernfalls wären sie schlicht unverkäuflich. Würde in Märkte regulatorisch eingegriffen, um Endgeräte anders zu gestalten, als dies die (Sicherheits-)Interessen ihrer Eigennutzer nahelegen, dann würden insbesondere Kriminelle und Terroristen sich solcher Endgeräte keinesfalls bedienen.

Da (Mobil-)Telefone, PDAs, Laptops und Desktop-PCs sich normalerweise in einem durch den Eigennutzer weitgehend kontrollierten physischen Schutzbereich befinden (je nach Lebensstil in Hemden- oder Jackettasche, Rucksack oder Aktenkoffer, Wohnung oder Büro), ist nicht zu erwarten, dass ihre Eigennutzer Wert auf Schutz gegen physische Eingriffe (tamper resistance) legen werden. Eher im Gegenteil, da physischer Schutz gegen sie selbst ihre Kontroll- und Nutzungsmöglichkeiten reduziert. „Digital Rights Management“, treffender „Digital Restrictions Management“ ist bei Eigennutzern nicht gerade beliebt – dies reicht vom Wunsch, Inhalte, z.B. Musik- und Videodateien, frei benutzen zu können bis hin zum „Befreien“ von im Verkaufszustand nur eingeschränkt nutzbarer Hardware, z.B. des iPhones. Zu erwarten ist also, dass persönliche Endgeräte „von der Stange“ zunehmend gesichert werden gegen „logische“ Angriffe über Kommunikationsnetze, nicht aber gegen physische Angriffe. Dies liegt nicht nur an den gerade geschilderten Interessen an Autonomie der Eigennutzer und wirtschaftlichen Interessen der international tätigen Hersteller der Endgeräte, sondern auch an physischen Gründen: Schutz gegen physische Eingriffe macht Geräte schwerer und unhandlicher. Dieser allgemeine Trend schließt natürlich nicht aus, dass einzelne Eigennutzer ihr Endgerät mit Erkennungsmechanismen für physische Eingriffe (tamper detection) ausstatten, beispielsweise schwer nachmachbare und kaum lösbare Klebestreifen zur Sicherung der Öffnungsmöglichkeiten des Gehäuses anbringen.

Physische Gründe begrenzen auch den Schutz gegen physische Abstrahlung (TEMPEST). TEMPEST-Angriffe bezeichnen Methoden, mit denen von einem Gerät abgestrahlte elektromagnetische Wellen (z.B. von Tastatur oder Grafikkarte) aufgefangen und genutzt werden, um daraus die im Gerät momentan verarbeiteten Informationen (z.B. Tastatureingaben oder Bildschirminhalte) abzuleiten. TEMPEST-Angriffe verändern die im Gerät verarbeiteten Daten und Programme nicht. Selbst durch Inkaufnahme deutlichen Mehrgewichts ist Schutz gegen TEMPEST-Angriffe keinesfalls auch nur annähernd perfekt zu realisieren. Wegen der durch das Mehrgewicht deutlich geringeren Marktgängigkeit und zusätzlichem technischem Aufwand sind TEMPEST-geschützte Geräte deutlich teurer als entsprechende Geräte ohne TEMPEST-Schutz. Wer TEMPEST-geschützte Geräte kauft oder benutzt fällt also auch in der vorhersehbaren Zukunft auf.

Dienste wie z.B. E-Mail, die heutzutage noch über Server abgewickelt werden, so dass sie nicht nur in Endgeräten oder via physischer Abstrahlung in deren Nähe überwacht werden können, sondern auch in Servern, werden zunehmend Verschlüsselung der Nutzdaten verwenden, so dass diese Nutzdaten, z.B. die Inhalte der E-Mails, auch vor den Servern (und damit auch vor Überwachung der Server oder in den Servern) geschützt sind. Zusätzlich ist es mittels so genannter Peer-to-Peer-Netzwerke (P2P) zunehmend möglich, Dienste ohne professionell betriebene Server anzubieten. Zusammen bedeutet dies, dass zukünftig Überwachung sinnvollerweise nicht an Servern ansetzt, sondern bezogen auf Nutzdaten ausschließlich am Endgerät und bezogen auf Verbindungsdaten („wer kommuniziert wann von wo mit wem wohin?“) hauptsächlich am Endgerät. Kommt es auf die Beweiseignung von Nutzdaten oder Verbindungsdaten an, ist darauf zu achten, dass Daten und Programme im Endgerät nicht zu Überwachungszwecken verändert werden [Hansen, Pfitzmann 2007].

3 Wichtige Grundsätze

Für die Nutzungsüberwachung von Informations- und Kommunikationssystemen in einer freiheitlichen demokratischen Gesellschaft sind die folgenden Grundsätze essentiell:

1. Da die hoch entwickelte Gesellschaft auf IKT und damit um der Sicherheit der Gesellschaft willen auf sichere IKT sehr viel mehr angewiesen ist als die organisierte Kriminalität oder terroristische Netzwerke, sollte der Staat alles unterlassen, was die Entwicklung der IKT hin zu mehr Sicherheit erschwert und damit zumindest verzögert.

2. Bei aller IKT für staatliche Sicherheitszwecke (Abhörschnittstellen, Datenbanken der Sicherheitsbehörden, Vorratsdatenspeicherung von Kommunikationsdaten bei KT-Betreibern oder von Zahlungsvorgängen bei Banken) muss man sich bewusst sein, dass auch diese IKT nicht wirklich sicher betrieben werden kann, solange die IT-Basissysteme derart unsicher sind, wie dies für wenigstens die nächsten zwei Jahrzehnte, vermutlich deutlich länger, zu erwarten ist. Im Klartext bedeutet dies, dass keineswegs nur Partner-Geheimdienste, sondern auch solche von so genannten Schurkenstaaten sowie die organisierte Kriminalität und auch terroristische Netzwerke sehr gute Chancen haben, sich „unserer“ – für staatliche Sicherheitszwecke vorgesehenen – IKT zu bedienen. Dies gilt insbesondere selbst dann, wenn unsere Sicherheitsbehörden organisatorisch perfekt geführt würden und es bei ihnen, was eine historische Weltneuheit wäre, weder Doppelagenten noch irgendwelche Korruption oder Erpressbarkeit gäbe. Also muss IKT für staatliche Sicherheitszwecke zumindest für die nächsten Jahrzehnte sehr vorsichtig geplant und eingesetzt werden.

3. Der Staat sollte also die Entwicklung hin zu wirklich sicherer IKT fördern. Und dies bedeutet auch, dass diese IKT tendenziell auch gegenüber dem Staat sicher sein muss, zumindest solange Grundsatz 2 aus technischen Gründen gilt. Da auch staatliche Sicherheitsorgane aus fehlbaren Menschen bestehen, gilt diese Aussage vermutlich zeitlich uneingeschränkt.

4. Da Kriminelle, Terroristen wie auch fremde Geheimdienste Sicherheitslücken bestehender IKT nutzen, sollte dies durch einen geeigneten (grund-)gesetzlichen Rahmen auch unseren Bedarfsträgern eher erlaubt werden, als dass für sie zusätzliche Sicherheitslücken geschaffen werden. Dabei muss sehr darauf geachtet werden, dass unsere Bedarfsträger kein Interesse an der Konservierung der von ihnen mitgenutzten Sicherheitslücken entwickeln oder diesem Interesse zumindest keine Geltung verschaffen können.

5. Schon heute werden auf eigengenutzten Endgeräten persönlichste Informationen gespeichert (Tagebücher, privateste Gedanken, Notizen, ...). Diese müssten bei einer Durchsuchung konsequenterweise auch ausgewertet werden, da bei jeder Beschränkung der Durchsuchung auf einen wie auch immer gearteten Teilbereich zum Schutz des Kernbereichs privater Lebensgestaltung dies zum Verbergen ermittlungsrelevanter Information genutzt werden kann. Also muss die Hürde für die Zulässigkeit einer Online-Durchsuchung mindestens so hoch gelegt werden wie für eine akustische Wohnraumüberwachung.

6. IKT für staatliche Sicherheitszwecke sollte so gestaltet werden, dass Kriminelle und Terroristen ihr nur sehr aufwändig ausweichen können – insbesondere sollte

organisierten Kriminellen und allen Terroristen hierbei Intelligenz und Sachkunde unterstellt werden.

4 Risiken der Vorratsdatenspeicherung und Schutzmöglichkeiten

Bezüglich der Vorratsdatenspeicherung sollen nachfolgend verschiedene Punkte näher betrachtet werden. Diese betreffen zum einen das Gefahrenpotential der auf Vorrat gespeicherten Daten und Schutzmöglichkeiten für sie (vgl. Grundsätze 1 und 2). Zum anderen geht es darum zu erläutern, warum die gemäß den momentan gültigen gesetzlichen Bestimmungen auf Vorrat gespeicherten Daten für die Strafverfolgung nur eingeschränkten Nutzen haben – insbesondere wenn man intelligente Täter unterstellt (vgl. Grundsatz 6).

Zunächst betrachten wir dabei die Vorratsdatenspeicherung von Kommunikationsdaten, danach die Vorratsdatenspeicherung von digitalen Zahlungsvorgängen, wobei sich viele Parallelen ziehen lassen.

4.1 Informationsgehalt von Verkehrsdaten

Betrachtet man das Gefährdungspotential der auf Vorrat gespeicherten Daten, so kann im ersten Moment der Eindruck entstehen, als sei es nicht sehr groß, da ja gemäß den aktuell gültigen Regelungen zumindest keine Kommunikationsinhalte gespeichert werden dürfen.

Hier ist allerdings anzumerken, dass sich Schwierigkeiten in der Umsetzung ergeben. Dies trifft insbesondere auf Internet-basierte Kommunikation zu. Konkret ergeben sich Probleme aus der Schichtenarchitektur des Internets. Dabei ist es so, dass höhere Schichten niedrigere Schichten für den Datentransport benutzen. Bei diesen von der niedrigeren Schicht zu transportierenden Daten handelt es sich sowohl um Protokolldaten (also beispielsweise Adressinformationen) als auch Inhaltsdaten der höheren Schicht. Da die niedrigere Schicht die „Bedeutung“ der zu transportierenden Daten aber nicht kennt, stellen sich für diese Schicht die zu transportierenden Daten insgesamt schlicht als Inhaltsdaten dar, die dann nicht zu speichern wären. Letztlich bedarf es für jede (neue) Internet-basierte Anwendung einer Einzelfallentscheidung, welche Daten als Verkehrsdaten zu speichern sind und welche als Inhaltsdaten anzusehen und folglich nicht zu speichern sind. Diese Entscheidung wird insbesondere dann schwierig, wenn Verkehrs- und Inhaltsdaten kaum zu trennen sind. Als Beispiel sei folgende URL betrachtet: `http://www.google.de/search?q=aids`. Einerseits handelt es sich klar um Adressinformationen bezüglich des Ziels einer Web-Anfrage. Andererseits enthält die URL aber auch Inhaltsdaten, da aus ihr hervorgeht, dass jemand nach dem Begriff „aids“ gesucht hat.

Weiteres Gefährdungspotential ergibt sich aus der Tatsache, dass sich aus den auf Vorrat gespeicherten Daten oftmals mehr Informationen gewinnen lassen, als dies zunächst den Anschein hat. Als ein Beispiel sei hier das Erstellen von Bewegungsprofilen von mobilen Internetnutzern genannt – und dies obwohl (anders als beim Mobilfunk) keinerlei geographische Angaben unmittelbar auf Vorrat gespeichert werden müssen. An diese Informationen gelangt man jedoch mittelbar anhand der durch das Endgerät eines Nutzers verwendeten IP-Adresse, beispielsweise wenn der Nutzer über sogenannte Hot Spots auf das Internet zugreift. In der Regel erhält das Endgerät des Nutzers dabei eine IP-Adresse zugewiesen, die aus einem Adresspool kommt, den nur dieser Hot Spot verwendet (gleiches gilt für alle Zugangspunkte zum Internet, beispielsweise auch für Internet via Kabel in einem Hotelzimmer). Insofern lässt sich aus der zu speichernden IP-Adresse auf den verwendeten

Hot Spot und somit letztlich auf den ungefähren Standort des Endgerätes schließen. Darüber hinaus lässt sich anhand der verwendeten IP-Adresse feststellen, welcher „Zugangsanbieter" verwendet wird. Dies dürfte in der Regel für die private Nutzung zu Hause ein anderer als am Arbeitsplatz sein, so dass sich Bewegungen zwischen Arbeitsplatz und Wohnung nachvollziehen lassen. Es existieren darüber hinaus Internetdienste, die kostenfrei oder gegen geringes Entgelt eine Zuordnung einer IP-Adresse zu einem ungefähren geographischen Standort vornehmen (beispielsweise: `http://www.maxmind.com`).

Eine Analyse, wie gut sich das Bewegungsverhalten aus IP-Adressen analysieren lässt, kann [Guhal, Francis 2007] entnommen werden.

4.2 Rechtlich induzierte Sicherheitsprobleme

Darüber hinaus besitzen die insbesondere im Bereich der klassischen Telekommunikationsdienste (Festnetz- und Mobiltelefonie) vielfältigen zu speichernden Angaben ein hohes Gefährdungspotential. Es stellt sich also die Frage, ob sich die auf Vorrat gespeicherten Daten wenigstens ausreichend gegen Missbrauch, also beispielsweise unberechtigte Kenntnisnahme schützen lassen.

Nachfolgend soll darauf eingegangen werden, welcher Schutz der Vorratsdaten aus wissenschaftlicher Sicht theoretisch möglich ist und wo die jeweiligen Schwierigkeiten bei einer praktischen Umsetzung liegen. Letztere ergeben sich dabei zum einen auf Grund der vorliegen gesetzlichen Regelungen und sind zum anderen inhärent technischer Natur.

Zu ersterem lässt sich anmerken, dass ein genereller Konflikt besteht zwischen einerseits der Forderung gemäß TKG „durch technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den gespeicherten Daten ausschließlich hierzu von ihm besonders ermächtigten Personen möglich ist."[2] und andererseits zu verlangen, dass „[d]ie Speicherung der Daten … so zu erfolgen [hat], dass Auskunftsersuchen der berechtigten Stellen unverzüglich beantwortet werden können."[3] Wird beispielsweise zum Zugriff auf die Vorratsdaten technisch ein Mehr-Personen-Prinzip erzwungen, so ist dies natürlich positiv für den Schutz der Vorratsdaten vor unberechtigtem Zugriff. Auf der anderen Seite erfordert es im Falle eines Auskunftsersuchens aber auch, dass die notwendigen Personen verfügbar sind, um die Anfrage zu beantworten. Es ergibt sich also im Allgemeinen ein negativer Einfluss auf die unverzügliche Beantwortbarkeit von Anfragen.

Ein anderer negativer Einfluss auf den Schutz der Vorratsdaten ergibt sich aus den Regelungen zur Aufwandsentschädigung. Da Vorratsdatenspeicherung nicht zum Kerngeschäft eines Telekommunikationsanbieters gehört, ist klar, dass er diesbezüglich nur ein Mindestmaß an Investitionen tätigen wird bzw. nur soviel investiert, wie ihm gemäß Entschädigungsregelung an Entschädigung[4] zusteht. Betrachtet man beispielsweise die aktuellen anfragebezogenen Entschädigungen, so ist klar, dass sich nicht mehrere Mitarbeiter eines Telekommunikationsunternehmens mit der Bearbeitung einer einzelnen Anfrage beschäftigen können. Insofern scheidet eine konsequente Umsetzung eines Mehr-Personen-Prinzips von vornherein aus.

---

[2] § 113a TKG Absatz 10

[3] § 113a TKG Absatz 9

[4] Gemäß Anlage 3 Nr. 300 JVEG sind dies 30 € für eine Auskunft über gespeicherte Verkehrsdaten. Erfolgt die Anfrage über eine zentrale Kontaktstelle der Strafverfolgungsbehörden, so ermäßigt sich der Entschädigungsbeitrag um 20 Prozent.

4.3 Technikinhärente Sicherheitsprobleme

Zu den technikinhärenten Problemen ist anzumerken, dass zwar in der Theorie viele Verfahren bekannt sind, die eine sichere Speicherung der Vorratsdaten ermöglichen – jedoch handelt es sich bei dem IT-System zur Speicherung und Beauskunftung um ein komplexes System und die Erfahrungen haben gezeigt, dass es nicht möglich ist, ein solches System fehlerfrei zu realisieren (vgl. Grundsatz 2). Als Beispiel seien die vielen regelmäßig veröffentlichten Sicherheitsupdates aus dem Betriebssystembereich genannt. Diese Sicherheitsupdates reagieren keineswegs auf bis dahin nicht bekannte neue Bedrohungen – sie reparieren vielmehr Fehler, die sich bei der Implementierung ergeben haben. Dabei ist zusätzlich zu berücksichtigen, dass die prinzipiellen Fehlerursachen seit Jahren bekannt und wohl untersucht sind. Obwohl also bekannt ist, worauf bei einer sicheren Umsetzung im Betriebssystembereich besonders zu achten ist und obwohl große IT-Unternehmen sehr große Anstrengungen zur Verbesserung der Sicherheit ihrer Produkte unternehmen, ist es ihnen trotzdem nicht gelungen, die erwähnten Fehler zu vermeiden. Geht man nun im Falle der Vorratsdatenspeicherung von einer eher geringen Investitionsbereitschaft aus, so ist klar, dass eine auch nur annähernd fehlerfreie Umsetzung der theoretischen Konzepte nicht erfolgen wird. Selbst wenn man eine hohe Investitionsbereitschaft annimmt, werden immer noch genügend Fehler verbleiben, um erfolgreiche Angriffe zu ermöglichen. Dabei kommt erschwerend hinzu, dass – ebenfalls aus Kostengründen – die Telekommunikationsanbieter keine jeweils unabhängig entwickelten Lösungen verwenden werden, sondern eine Entwicklung eines Drittanbieters einkaufen werden. Es ist dabei nicht zu erwarten, dass es sehr viele unterschiedliche derartige Anbieter geben wird. Insofern werden auch hier die bekannten IT-Sicherheitsprobleme eintreten, die sich aus Monokulturen ergeben [Geer et al. 2003]. Diese liegen unter anderem darin, dass es für einen Angreifer lohnend ist, Schwachstellen in dem angebotenen System zur Vorratsdatenspeicherung zu suchen, da er dann die Systeme vieler Telekommunikationsanbieter kompromittieren kann.

4.4 Notwendige Schutzmaßnahmen

Nach der Schilderung der generellen Probleme, die eine wirklich sichere Speicherung der Vorratsdaten verhindern, sollen einige der möglichen Verfahren zum Schutz der Vorratsdaten diskutiert werden. Notwendig ist dabei zunächst in jedem Falle eine Verschlüsselung der auf Vorrat zu speichernden Daten mit einem oder mehreren öffentlichen Schlüsseln – und zwar spätestens unmittelbar vor der ersten Aufzeichnung auf Datenträgern. Darüber hinaus ist mit geeigneten Verfahren wie beispielsweise Hashwerten bzw. digitalen Signaturen sicher zu stellen, dass Manipulationen an den auf Vorrat gespeicherten Daten erkannt werden. Die verwendeten kryptographischen Schlüssel sind sicher zu speichern. Dies bedeutet, dass geheime Schlüssel nur zum Zeitpunkt einer Auskunftserteilung durch ein IT-System zugreifbar sein dürfen und andernfalls an einem auch physisch gesicherten Ort aufzubewahren sind. Der Zugriff auf die geheimen Schlüssel ist durch geeignete Authentisierungsverfahren zu schützen – hierzu sollte mindestens die Eingabe eines Geheimnisses (PIN) notwendig sein. Empfehlenswert wäre natürlich die Umsetzung eines Mehr-Personen-Prinzips, das heißt, dass der Zugriff auf die geheimen Schlüssel durch mehrere Personen autorisiert werden muss bzw. dass ein Entschlüsseln der Vorratsdaten nur durch die Verwendung mehrerer unterschiedlicher geheimer Schlüssel möglich ist. Zusätzlich sollten als Medien für den Schlüsselspeicher Geräte verwendet werden, die auch im Falle eines Diebstahls einen gewissen Schutz der Schlüssel bieten (so genannte „tamper resistant“ Geräte). Smartcards bieten beispielsweise diesen minimalen Schutz halbwegs – wohingegen eine gewöhnliche Festplatte oder ein gewöhnlicher USB-Stick als nicht ausreichend angesehen werden muss. Darüber hinaus sollte dieses Gerät die Möglichkeit haben, Kenntnis über die aktuelle Zeit zu

erlangen. Somit kann das Gerät den Zugriff auf die Schlüssel (und in der Konsequenz letztlich die Entschlüsselung von auf Vorrat gespeicherten Daten) verweigern, wenn diese Daten beispielsweise älter als sechs Monate sind. Insofern handelt es sich um eine technische Unterstützung der Forderung aus §113a TKG Absatz 11.

In jedem Fall hat der Zugriff auf die Schlüssel und somit letztlich die Beauskunftung unter Benutzung eines besonders geschützten IT-Systems zu erfolgen. Dies bedeutet, dass keinerlei Verbindung zu irgendeinem Rechnernetz bestehen darf. Generell sind alle Zugriffe auf die Vorratsdaten und die benutzten kryptographischen Schlüssel revisionssicher zu protokollieren. Dabei ist sicherzustellen, dass diejenigen, die Zugriff auf die Vorratsdaten und die zugehörigen Schlüssel haben, keinen Zugriff auf die protokollierten Audit-Daten erlangen können.

4.5 Notwendige Kontrollen

Abschließend ist festzustellen, dass jegliche IT-Systeme, die zur Umsetzung der Vorratsdatenspeicherung und zum Schutz der gespeicherten Daten eingesetzt werden ebenso wie die damit verbundenen organisatorischen Prozesse auf eine ständige Überprüfung angewiesen sind. Der Sicherheitsexperte Bruce Schneier formulierte dazu treffend: „Security is a process, not a product.“ (Sicherheit ist ein Prozess, kein Produkt) [Schneier 2000]. Inwieweit Telekommunikationsanbieter tatsächlich gesetzlich zu einer fortlaufenden Überprüfung und Aktualisierung verpflichtet sind und inwieweit tatsächlich eine Überprüfung einer derartigen Verpflichtung erfolgt, ist unklar. Im TKG ist (beispielsweise in § 109) im Wesentlichen eine einmalige Abnahme durch die Bundesnetzagentur geregelt. Zwar finden sich Formulierungen wie: „Sofern sich die dem Sicherheitskonzept zu Grunde liegenden Gegebenheiten ändern, hat der Betreiber das Konzept anzupassen und der Bundesnetzagentur unter Hinweis auf die Änderungen erneut vorzulegen.“ Daraus lässt sich aber vermutlich nicht die Verpflichtung zu einer regelmäßigen Überprüfung ableiten. Zwar kann die Bundesnetzagentur gemäß §115 TKG prinzipiell zu jeder Zeit eine Überprüfung der Einhaltung der Vorschriften vornehmen, jedoch ist sie dazu nicht verpflichtet und insofern ist unklar, inwieweit eine Überprüfung durch die Bundesnetzagentur in Praxis tatsächlich erfolgt.

Zusammenfassend kann man sagen, dass die Sicherheit auf Vorrat gespeicherter Daten kaum durch deren Umfang und Speicherdauer bestimmt wird, sondern durch die in Kauf genommene Zeit für den Zugriff auf sie. Verschlüsselung mit mehreren öffentlichen Schlüsseln bereits bei der Erfassung der Daten sichert sie sehr gut – kritisch ist, wie der Zugriff auf die Entschlüsselungsschlüssel und deren Verwendung beschränkt wird.

4.6 Nutzen der Vorratsdatenspeicherung von Verkehrsdaten

Nachdem auf das prinzipielle Gefährdungspotential von auf Vorrat gespeicherten Daten hingewiesen wurde und gleichzeitig die Schwierigkeiten bezüglich einer wirklich sicheren Speicherung aufgezeigt wurden, ist für die Frage der Verhältnismäßigkeit der Umsetzungsregelungen zur Vorratsspeicherung die Frage von Bedeutung, welcher Nutzen sich aus der Vorratsdatenspeicherung ergibt. Hier ist natürlich insbesondere der Fall interessant, der einen intelligenten Straftäter unterstellt.

Intelligente Kriminelle und Terroristen werden u.a. Anonymisierungsdienste im Ausland außerhalb der Vorratsdatenspeicherungsbereiche nutzen, um sich selbst zu schützen. Selbst wenn diese Anonymisierungsdienste über unveröffentlichte Sicherheitslücken [Pohl 2007] der zugrunde liegenden IT angreifbar wären, so kann deren Angreifbarkeit über minimale Installation von Funktionalität (Anonymisierungsknoten brauchen bei weitem nicht alle

Dienste, die „normale“ Endgeräte heutzutage so leicht angreifbar machen) sowie physische Verteilung und Diversität (unterschiedliche Betriebssysteme, etc.) bereits heute so deutlich reduziert werden, dass sie für praktische Ermittlungen kaum eine Rolle spielen dürften.

Eine andere einfache Möglichkeit, sich den Auswirkungen der Vorratsdatenspeicherung zu entziehen, besteht in der Benutzung von sogenannten Bot-Netzen. Dabei handelt es sich um Rechner unbeteiligter Dritter, die mit Hilfe von Trojanischen Pferden oder ähnlicher Schadsoftware durch Kriminelle für ihre Zwecke missbraucht werden können – beispielsweise dafür, ihre Kommunikationsbeziehungen zu verschleiern. Hier ergibt sich insbesondere ein Konflikt mit der Online-Durchsuchung, da diese – wie im BKA-Gesetz erlaubt – gerade auf die Schwachstellen aufbaut, die Kriminelle nutzen können, um ein Bot-Netz zu erstellen und somit letztlich die Vorratsdatenspeicherung zu umgehen.

Allerdings ist es momentan gar nicht notwendig, Anonymisierungsdienste im Ausland oder Bot-Netze zum Schutz illegaler Aktivität vor der Vorratsdatenspeicherung zu benutzen. Da in den aktuellen gesetzlichen Vorschriften bezüglich Internet-basierter Kommunikation vorgeschrieben ist, dass Informationen über das Ziel der Kommunikation nicht zu speichern sind, kann ebenso gut ein deutscher Anonymisierungsdienst benutzt werden. Selbst ein einfacher Proxy oder ein NAT-Gateway („Network Address Translation“) reichen aus, solange diese von einer genügend großen Zahl an Nutzern benutzt werden. Der Grund dafür ist, dass sich bei den erwähnten Netzkomponenten alle Nutzer ausgangsseitig eine IP-Adresse „teilen“. Diese IP-Adresse wiederum taucht dann in den auf Vorrat gespeicherten Daten als Absender auf. Ein Auskunftsersuchen beim Anbieter des Anonymisierungsdienstes, Proxies bzw. NAT-Gateways führt somit lediglich zu einer Liste mit IP-Adressen derjenigen Nutzer, die zu dem betreffenden Zeitpunkt den Dienst benutzt haben. Eine weitere Eingrenzung ist schlicht nicht möglich, da dafür notwendige Daten (etwa Zieladressen oder Portnummern im Falle des NAT-Gateways) nicht zu speichern und somit nicht vorhanden sind (siehe auch: [Berthold, Böhme, Köpsell 2008]).

Konsequenterweise müsste man für eine wirkungsvolle Strafverfolgung fordern, dass die zu speichernden Daten im Falle einer Internet-basierten Kommunikation deutlich ausgeweitet werden. Allerdings ist dies nicht – wie im Falle der klassischen Telekommunikation – durch eine Aufzählung einzelner Datentypen möglich: Die grundlegenden Protokolle des Internet (IP, UDP, TCP) sind auf eine flexible Erweiterbarkeit ausgelegt, d. h. dass sich zwei Kommunikationspartner stets auf eigene, neue Protokollerweiterungen einigen können. Letztlich können sie sich – dank der Offenheit und Flexibilität des Internets – auf vollkommen eigene und neue Protokolle einigen, bei denen dann auch neue Arten von Verkehrsdaten anfallen. Somit bleibt nur die Möglichkeit, in gesetzlichen Regelungen allgemeine Formulierungen wie etwa: „zu speichern sind alle Angaben, die zur Rückverfolgung einer Kommunikationsbeziehung notwendig sind“ vorzunehmen. Dies würde natürlich die Normenklarheit untergraben und das Missbrauchspotential der auf Vorrat gespeicherten Daten deutlich erhöhen.

Zusammenfassend lässt sich also feststellen, dass von den auf Vorrat gespeicherten Daten ein nicht zu unterschätzendes Gefährdungspotential ausgeht und sie sich nicht wirklich schützen lassen (vgl. Grundsätze 1 und 2) – während sie auf der anderen Seite für eine Verfolgung von intelligenten Straftätern nur von geringem Nutzen sind (vgl. Grundsatz 6).

4.7 Vorratsdatenspeicherung von digitalen Zahlungsvorgängen

Die Aussagen zum Missbrauchspotential und zu den Schwierigkeiten bezüglich einer sicheren Speicherung lassen sich direkt auf die Vorratsdatenspeicherung von digitalen Zahlungsvorgängen (wie sie bei SWIFT wohl international realisiert wird) übertragen (vgl. Grundsätze 1 und 2). Allerdings gibt es Vorteile bezüglich des Nutzens für Strafverfolgung bei der Vorratsdatenspeicherung von Zahlungsvorgängen verglichen mit der Vorratsdatenspeicherung von Kommunikationsdaten (vgl. Grundsatz 6): Organisiert Kriminelle wie auch Terroristen können die überwachten digitalen Zahlungssysteme sehr viel schwieriger vermeiden als die überwachten Kommunikationssysteme. Denn Kommunikation kann jede Gruppe selbst definieren und betreiben, während Geld nicht nur für ihre Binnen-, sondern insbesondere für ihre Außenbeziehungen wichtig ist, und von daher nicht von ihr selbst definiert werden kann. Sie muss nehmen, was „üblich“ ist.[5]
Zusätzlich schlagen sich auch künftig nicht nahezu alle Aktivitäten des täglichen Lebens in digitalen Zahlungsvorgängen nieder, während sie dies bereits heute bzgl. Kommunikationsdaten weitgehend tun. Wenn überhaupt Vorratsdatenspeicherung, dann ist die von digitalen Zahlungsvorgängen also die zweckgeeignetere wie auch angemessenere Maßnahme.

5 Zur Online-Durchsuchung

Unter Beachtung von Grundsatz 4 kann eine verdeckte Online-Durchsuchung angemessen sein, wenn sich alle Beteiligten der Schwierigkeiten und Risiken bewusst sind und insbesondere Konsens darüber besteht, dass sie nur zur Indiziengewinnung, zur Steuerung von Ermittlungen, wegen mangelnder forensischer Beweiskraft ihrer Ergebnisse aber nicht zur Beweiserhebung geeignet ist [Hansen, Pfitzmann 2007]. Wegen Grundsatz 5 muss die Zulässigkeit der verdeckten Online-Durchsuchung auf die Prävention schwerwiegendster Verbrechen beschränkt werden.

Für Erfolg und Angemessenheit einer verdeckten Online-Durchsuchung wie auch für ihr Missbrauchspotential ist die *Eindringmethode* wesentlich. Zunächst sind folgende Optionen denkbar [Hansen, Pfitzmann 2007]:

a) Methoden, die *unbewusste konstruktive Mitarbeit* desjenigen erfordern, dessen Endgerät durchsucht werden soll. Beispiele sind das Zusenden von E-Mails, die als Attachment ein Trojanisches Pferd enthalten, zu dessen Start der Eigennutzer verführt werden soll, oder das Zuspielen präparierter Datenträger.
b) Verpflichtung von Internet-Service-Providern, einen Programm-Download desjenigen, dessen Endgerät durchsucht werden soll, so zu modifizieren, dass das heruntergeladene Programm ein Trojanisches Pferd enthält.
c) Hacken des Endgeräts durch Ausnutzen von Sicherheitslücken, die noch nicht allgemein bekannt sind [Pohl 2007].
d) Erreichen des *physischen Zugriffs auf das Endgerät* (sei es durch „Ausleihen“ eines Mobiltelefons, Einstieg in eine Wohnung zum Zugriff auf Desktop-PCs oder auf dort befindliche PDAs und Laptops), Kopieren seines Speichers, ggf. Maßschneidern einer Online-Durchsuchungs-Software für genau die vorgefundene Softwarekonfiguration, Einbringen der Online-Durchsuchungs-Software, ggf. bei einem zweiten „Ausleihen“ oder Wohnungseinstieg [Leipold 2007].

[5] Als Geldtransportmittel innerhalb der Gruppe kann jede Gruppe nehmen, was immer sie mag, beispielsweise Edelmetalle, Diamanten, etc. Aber vor der Zahlung nach außen muss in eine übliche Währung konvertiert werden.

Die Anwendung von Eindringmethode b) lässt sich durch eine leichte Erweiterung der heute üblichen Sicherheitsmechanismen beim Download von Software entdecken – und damit wirkungslos machen. Hierzu müssen nur viele Endgeräte miteinander Hashwerte ihrer Downloads austauschen, um Inkonsistenzen zu entdecken und bei entdeckten Inkonsistenzen auch die Downloads selbst auszutauschen[6]. Diese Entdeckung und Vereitelung funktioniert selbst dann, wenn der Hersteller des Programms rechtlich zur Kooperation verpflichtet wäre, indem er eine digitale Signatur für sein um das Trojanische Pferd erweiterte Programm liefert. Damit solch eine Konsistenzprüfung leer läuft, müssten sich Programm-Downloads generell unterscheiden oder alle Nutzer (und damit in konsistenter Weise weltweit) ein Trojanisches Pferd erhalten. Ersteres ist technisch nicht plausibel[7]. Letzteres verstößt so eklatant gegen Grundsatz 3 und vermutlich auch gegen internationales Recht, dass sich eine weitere Diskussion erübrigt.

Da die Eindringmethoden a), b) und c) zwar einen Grundaufwand zum Bereitstellen des Trojanischen Pferdes bzw. Know-hows erfordern, danach aber weitgehend ohne große Kosten im jeweiligen Anwendungsfall eingesetzt werden können, haben sie ein sehr großes Missbrauchspotential: Bei der Programmierung Trojanischer Pferde ist dies evident – sie können, wenn vorhanden, massenhaft eingesetzt werden, zumindest solange Endgeräte mit Softwarekonfigurationen „von der Stange“ (d.h. wie als Komplettsystem gekauft) durchsucht werden sollen. Gleiches gilt für eine Infrastruktur zum Einfügen von Trojanischen Pferden in Downloads. Zum Finden von neuen Sicherheitslücken wird eine bereits jetzt vorhandene „Szene“ noch weiter ermuntert und monetär unterstützt – und sie wird nicht nur an deutsche Bedarfsträger verkaufen.

Eindringmethode d) gibt der Online-Durchsuchung ein deutlich geringeres Missbrauchspotential, da sie wirklich einen deutlich spürbaren Aufwand in jedem einzelnen Anwendungsfall verursacht. Hierbei kommt es nicht auf das Maßschneidern der Online-Durchsuchungs-Software für die vorgefundene Softwarekonfiguration an – das ließe sich aus Sicht der Informatik gut automatisieren und damit bei Masseneinsatz nahezu beliebig billig pro Einsatz gestalten –, sondern auf den aufwändigen physischen Zugriff auf jedes einzelne Endgerät.

Wegen Grundsatz 3 ist die Möglichkeit der verdeckten Online-Durchsuchung mit den Eindringmethoden a), b) und c) ein Auslaufmodell: Je sicherer die Endgeräte werden, desto aufwändiger werden diese drei Eindringmethoden, bis sie bei wirklich sicherer IKT schließlich unwirksam werden. Auch dies spricht dafür, sich auf Eindringmethode d) zu beschränken und auch zu konzentrieren.

Wegen Grundsatz 6 ist gegenüber einer verdeckten Online-Durchsuchung eine *verdeckte Analyse der physischen Abstrahlung des Endgeräts* vorzuziehen.

---

[6] Sollten Hersteller den Austausch der Downloads selbst verbieten (wie dies bei Microsoft wohl momentan der Fall ist), dann ist dies, zusammen mit der in diesem Papier diskutierten Bedrohung, ein sehr gutes Argument für die Verwendung von Open Source-Software. Außerdem werden organisiert Kriminelle und Terroristen solch ein Verbot vermutlich nicht befolgen.

[7] Selbst wenn Programm-Downloads etwa bei Update-Funktionen jeweils für die installierte Version maßgeschneidert werden, gibt es immer noch im Vergleich zur Zahl der Downloads wenige Varianten, so dass der beschriebene Mechanismus zur Konsistenzprüfung funktioniert.

- Ihr können sich Kriminelle und Terroristen auch langfristig kaum entziehen (s.o.), insbesondere auch nicht dadurch, dass sie ihr Endgerät nur offline betreiben (also beispielsweise ihren PDA, Laptop oder Desktop-PC nie ans Internet anschließen) oder mit Erkennungsmechanismen für physische Eingriffe versehen.
- Ihr deutlich spürbarer Aufwand in jedem einzelnen Anwendungsfall schließt einen Missbrauch durch massenhaften Einsatz aus.
- So gewonnene Erkenntnisse sind forensisch als Beweismittel verwertbar – im Gegensatz zu Erkenntnissen, die durch eine Online-Durchsuchung, egal mit welcher Eindringmethode, gewonnen wurden, da bei der Online-Durchsuchung das Endgerät immer manipuliert wird [Hansen, Pfitzmann 2007].
- Sie kann ggf. ergänzt werden durch eine später durchgeführte Beschlagnahme des Endgerätes und der auf ihm gespeicherten Daten, die etwa mittels der per Tastatureingabenaufzeichnung in Erfahrung gebrachten kryptographischen Schlüssel entschlüsselt werden können. Da bei diesem Vorgehen keine Manipulationen an den Daten oder Programmen auf dem Endgerät durchgeführt werden, sind die Ergebnisse forensisch als Beweismittel verwertbar.

Sowohl die Online-Durchsuchung mit Eindringmethode d) „physischer Zugriff auf das Endgerät“ wie auch die verdeckte Analyse der physischen Abstrahlung des Endgeräts stellen Maßnahmen mit lokal begrenzter Wirkungsentfaltung dar und passen so deutlich besser zu unserem Rechtssystem: Internationale Verwicklungen etwa durch Verstöße gegen das Völkerrecht bei unbeabsichtigtem „Auslandseinsatz“ werden vermieden; die Maßnahmen werden zielgerichteter und sind deutlich weniger missbrauchsgeeignet.

6 Empfehlungen

Eine *Vorratsdatenspeicherung von Kommunikationsdaten* sollte unterlassen werden, da sie eine bedeutende zusätzliche Sicherheitslücke schafft, zu Überwachende ihr vergleichsweise leicht ausweichen können und ihr Übermaß eine gesellschaftliche Akzeptanz für andere, sehr viel zielgerichtetere und zweckgeeignetere Überwachungsmaßnahmen vermutlich verhindert.

Hält man es für notwendig, zusätzliche Sicherheitslücken zu schaffen, dann ist eine *Vorratsdatenspeicherung von digitalen Zahlungsvorgängen* zielgerichteter als eine Vorratsdatenspeicherung von Kommunikationsdaten. Ihr kann weit weniger gut ausgewichen werden und sie ist zur Aufdeckung krimineller und terroristischer Strukturen vermutlich genauso gut, wenn nicht besser geeignet.

Deutlich weniger kritisch als die Schaffung zusätzlicher Sicherheitslücken ist die Nutzung ohnehin bestehender. Prominentestes Beispiel für die Nutzung ohnehin bestehender Sicherheitslücken ist die so genannte Online-Durchsuchung.

Falls eine *Online-Durchsuchung* in begründeten Fällen erlaubt werden soll, ist als Eindringmethode ausschließlich der „physische Zugriff auf das Endgerät“ zu erlauben. Wo immer möglich, sollte statt einer Online-Durchsuchung eine *verdeckte Analyse der physischen Abstrahlung des Endgeräts* durchgeführt werden. Sie ergibt nur Erkenntnisse über die gegenwärtige Datenverarbeitung, was für ihren kontrollierbaren Einsatz verglichen mit der Online-Durchsuchung ein großer Vorteil ist. Sollten Erkenntnisse über vergangene Datenverarbeitung benötigt werden, kann die verdeckte Analyse der physischen Abstrahlung des Endgeräts mit einer späteren offenen Beschlagnahme des Endgeräts kombiniert werden.

Dies hat den Vorteil, dass die Beweiseignung der gewinnbaren Erkenntnisse so nicht zerstört wird.

7 Ausblick

Gelingt es nicht, einen breiten gesellschaftlichen Konsens für zielgerichtete, zweckgeeignete und keinesfalls massenüberwachungstaugliche Überwachungsmaßnahmen herbeizuführen, dann werden Maßnahmen wie Vorratsdatenspeicherung von Kommunikationsdaten und Online-Durchsuchung organisiert Kriminelle, Terroristen und Computer-Geeks in dieselbe Anonymitätsmenge drängen. Dies wäre für eine effiziente Arbeit der Bedarfsträger sehr sehr ungeschickt.

Danksagung

Für hilfreiche Diskussionen zum Text vom 26.09.2007 danken wir Stefan Berthold, Dr. Rainer Böhme, Dr. Sebastian Clauß, Rüdiger Dierstein, Marit Hansen, Markus Hansen, Prof. Dr. Hartmut Pohl, Dr. Manfred Reitenspieß und Dr. Dagmar Schönfeld herzlich. Dr. Rainer Böhme, Dr. Sebastian Clauß, Prof. Dr. Alexander Roßnagel und Dr. Dagmar Schönfeld haben wir auch für hilfreiche Kommentare zu diesem Text zu danken.

Literatur

[Berthold, Böhme, Köpsell 2008] Stefan Berthold, Rainer Böhme, Stefan Köpsell: Data Retention and Anonymity Services; Proc. The Future of Identity in the Information Society - Challenges for Privacy and Security, FIDIS/IFIP Internet Security & Privacy Fourth International Summer School, Springer Boston, IFIP Advances in Information and Communication Technology, Volume 209, 2009, Seite 92-106, http://www1.inf.tu-dresden.de/~rb21/publications/BBK2009_DataRetention_Anonymity.pdf.

[Geer et al. 2003] Dan Geer et al.: CyberInsecurity: The Cost of Monopoly; Diskussionspapier, 2003, http://cryptome.org/cyberinsecurity.htm (29. Juli 2009).

[Guhal, Francis 2007] Saikat Guhal, Paul Francis: Identity Trail: Covert Surveillance Using DNS; Proc. Privacy Enhancing Technologies Symposium (PET 2007), Springer Berlin / Heidelberg, LNCS 4776, Seite 153-166.

[Hansen, Pfitzmann 2007] Markus Hansen, Andreas Pfitzmann: Technische Grundlagen von Online-Durchsuchung und -Beschlagnahme; Deutsche Richterzeitung, August 2007, Seite 225-228.

[Leipold 2007] Roman Leipold: Der Bundestrojaner ist eine Wanze; Chip 09/2007 http://www.focus.de/digital/computer/chip-exklusiv/chip-exklusiv_aid_68603.html (20. Sept. 2007). (Authentizität der Aussagen wurde vom BKA dementiert http://www.ftd.de/forschung_bildung/forschung/238034.html?mode=print (20. Sept. 2007)).

[Pohl 2007] Hartmut Pohl: Zur Technik der heimlichen Online-Durchsuchung; DuD Datenschutz und Datensicherheit 31 (September 2007) Seite 684-688.

[Schneier 2000] Bruce Schneier: Crypto-Gram Newsletter; May 15, 2000 http://www.schneier.com/crypto-gram-0005.html (30. Juli 2009).