Rainer Rehak

FIfF-Studienpreis 2012
1. Preis

Angezapft

Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung

– Eine Zusammenfassung –

Vielen herzlichen Dank noch einmal an das FIfF für die Auszeichnung meiner Diplomarbeit über die heimliche Online-Durchsuchung. Ich habe mich insbesondere darüber gefreut, weil das Thema nicht nur die Rolle der Informati(onstechni)k in einer digitalen Gesellschaft allgemein berührt, sondern speziell den Umgang staatlicher Stellen mit derartigen neuen Möglichkeiten. Doch warum ist gerade dieser Aspekt so interessant und wichtig?

Der freiheitliche Staat ist ein Mittel menschlich-gesellschaftlicher Selbstorganisation. Im Gegensatz zu anderen gesellschaftlichen Interaktions-, Aushandlungs- und Regelungsmechanismen sind das Staatskonstrukt und seine Prozesse stark strukturiert und formalisiert, was deren Betrachtung und Diskussion einerseits einfacher und andererseits schwieriger macht. Einfacher, weil dadurch eine gewisse Vorhersagbarkeit staatlicher Aktivität erzeugt wird, wofür die Strukturierung gedacht ist. Schwieriger, weil die Formalisierung viele Tücken (u. a. Mehrdeutigkeit, fehlerhafte Modellierung, usw.) birgt, wie gerade wir als Informatiker wissen.

Die Fragestellung der Arbeit nach der Analyse, Reglementierung und Folgen staatlicher Instrumente aus dem Werkzeugkasten der Informationstechnik berührt im Grunde nichts weniger, als die Frage nach den Bedingungen für die Freiheit des Menschen in einem digitalen Zeitalter. Eine Welt, in der vormals verborgene innere Vorgänge einer Person zunehmend nach außen in informationstechnische Systeme verlagert werden, und somit auch zunehmend zugreifbarer werden, gibt diese Vorgänge potentiell auch staatlichen Zugriffen preis. Um diese komplexen Sachverhalte zu erforschen, zu erklären und zu „modellieren" sind gerade Informatiker aus dem Bereich *Informatik und Gesellschaft* gefragt, von der Analyse technischer Methoden über die Erforschung der gesellschaftlichen Implikationen bis hin zur konstruktiven Teilnahme an der Diskussion über die Regulierung des Einsatzes solcher Methoden. Diese Partizipation der Informatik ist sehr wünschenswert, ja sogar verantwortungsvolle Pflicht, denn wie oben erwähnt handelt der Staat natürlich auch „im Auftrag" aller Informatiker.

Der explizite Verweis auf *Informatik und Gesellschaft* soll hervorheben, dass diese Art Vorhaben weder von reinen Informatikern noch von reinen Geistes- und Rechtswissenschaftlern sinnvoll durchgeführt werden kann, denn nur technische Sachkenntnis, also ein Verständnis der Möglichkeiten und Grenzen informationstechnischer Methoden, gepaart mit dem Verständnis gesellschaftlich-rechtlicher Sachverhalte, lassen tatsächliche gesellschaftlich-rechtliche Analysen technischer Belange gelingen. Auch wegen dieses fächerübergreifenden Ansatzes sind besonders in den informatikfremden Bereichen der Arbeit detaillierte Belege vollzogen worden.

Wenn Menschen in einer Gesellschaft leben wollen, die sich in großem Maße auf Computertechnologie verlässt und ihr einen zentralen Stellenwert im gesellschaftlichen Miteinander einräumt, ist die Erforschung dieser Aspekte unabdingbar. Die im folgenden zusammengefasste Arbeit hat das Ziel, die heimliche Online-Durchsuchung technisch fundiert, aber gut verständlich und mit explizitem gesellschaftlichen Bezug zu bearbeiten und so einen Beitrag zur Klärung diesbezüglicher Missverständnisse und auch -stände zu leisten.

Einleitung

Eine *heimliche Online-Durchsuchung* ist ein verdeckter staatlicher Zugriff auf persönlich genutzte informationstechnische Systeme. Im gesellschaftlichen Diskurs haben sich für diese Maßnahme die Begriffe *Bundestrojaner* und *Staatstrojaner* durchgesetzt, wobei der Einsatz dieser Maßnahme nach wie vor hoch umstritten ist.[1]

Die ersten Online-Durchsuchungen wurden 2005 per geheimer Dienstanweisung durchgeführt, um verschlüsselten Inhalten auf entfernten Computern habhaft zu werden. Ab diesem Zeitpunkt wurde sie schon einige tausend mal von Geheimdiensten und mindestens 100-mal von anderen staatlichen Stellen eingesetzt.[2] Bislang ist sie nur für einige Behörden und Polizeien zur Gefahrenabwehr geregelt.

	Bundesebene	Länderebene
Gefahrenabwehr	Bundeskriminalamt (BKA), Verfassungsschutz, Militärischer Abschirmdienst (MAD), Bundesnachrichtendienst (BND)	Bayerische Polizei, Bayerischer Verfassungsschutz, Rheinland-Pfälzische Polizei
Strafverfolgung	keine Gesetzesgrundlage (laut BGH-Urteil)	keine Gesetzesgrundlage

Abbildung 1: Ermächtigungsmatrix Online-Durchsuchung 2013

Methodik

Die Methodik der Arbeit besteht in der Analyse und Gegenüberstellung dessen, wozu diese Art von Maßnahme technisch in der Lage ist und wozu sie rechtlich gesehen nur in der Lage sein sollte. Aus dem in der Arbeit herausgearbeiteten Unterschied, dass die heimliche Online-Durchsuchung prinzipiell technisch

viel mehr kann, als sie rechtlich darf und der in der Arbeit aufgestellten und belegten These, dass ihre technischen Möglichkeiten auch nicht sinnvoll beschränkt werden können, werden gesellschaftlich-rechtliche Bedeutung und Folgen des trotzdem stattfindenden Einsatzes abgeleitet.

Zunächst werden anhand der Aussagen von verantwortlichen Politikern, Staatsorganen, anderen an der Diskussion beteiligten Personen und insgesamt des rechtlichen, technischen und gesellschaftlichen Kontextes der Situation konzeptionelle Anforderungen an eine heimlichen Online-Durchsuchung formuliert. Diese beschreiben bestimmte Eigenschaften, Funktionen und „Verhaltensweisen", die notwendig oder zumindest sehr wünschenswert für eine sinnvolle Anwendbarkeit der Online-Durchsuchung sind. Dies umfasst auch negative Anforderungen, also Folgen, Umstände und Aktivitäten des technischen Aspekts der Maßnahme, die auf jeden Fall vermieden werden müssen oder deren Auftreten zumindest sehr unwahrscheinlich sein muss.

Aus dieser konzeptionellen Beschreibung können konkrete technische Eigenschaften abgeleitet werden. Dies ist möglich, weil die beschriebenen Konzepte und Fähigkeiten in einer gegebenen Computersystemarchitektur nicht beliebig implementierbar sind. Oder anders ausgedrückt: Die aktuelle Computersystemarchitektur definiert funktionale Abhängigkeiten, in denen bestimmte Funktionen nur auf bestimmte Weise realisiert werden können.[3]

Die so abgeleiteten technischen Eigenschaften einer idealen heimlichen Online-Durchsuchungs-Software werden dann einer Analyse unterzogen, wobei das Augenmerk auf unbeabsichtigte Eigenschaften, technische Grenzen und ungewollte Nebeneffekte gerichtet ist, was insofern keine Unausgewogenheit darstellt, als dass die beabsichtigten Funktionen und Eigenschaften einer heimlichen Online-Durchsuchung den Ausgangspunkt der Betrachtung bilden.

Im Anschluss erfolgt in der Arbeit eine Zusammenfassung des Urteils des Bundesverfassungsgerichtes zu heimlichen Online-Durchsuchungen mit spezieller Analyse und Bewertung der Entscheidung aus technischer Sicht. Das Gericht hatte neben der Aufhebung der damaligen Regelung für den heimlichen Zugriff auf informationstechnische Systeme auch hohe Schranken für eine erneute Schaffung derartiger gesetzlicher Grundlagen formuliert, die den informationsgesellschaftlichen Folgen, Möglichkeiten und Risiken einer solchen Maßnahme Rechnung tragen sollen.[4]

Mit dieser zweifachen Herangehensweise ist es möglich, das vorher entwickelte Bild der beabsichtigten und unbeabsichtigten Konsequenzen und Eigenschaften einer heimlichen Online-Durchsuchung mit der Kritik und den Anforderungen des Bundesverfassungsgerichtes in Deckung zu bringen. Dies macht es möglich, konkrete Aussagen für den Einsatz verfassungsmäßiger heimlicher Online-Durchsuchungen zu erarbeiten, die die technischen Möglichkeiten und Grenzen dieser Maßnahme mit einbeziehen. Technikabhängige Implikationen des Urteils können somit aufgelöst werden.

Resultat sind die Sichtbarmachung des vom Gericht vorgegebenen verfassungsmäßigen Rahmens für derartige rechtlich-technische Regelungen und die dadurch mögliche Kritik der aktuellen Rechts- und Anwendungspraxis sowie eine Kritik des Urteils selbst und konkrete Forderungen für die Neubewertung der Maßnahme.[5]

Gesellschaftliche Einbettung

Eine Analyse der technisch-konzeptionellen und gesellschaftlichen Folgen der Online-Durchsuchung verlangt zunächst die Anerkennung, dass informationstechnische Systeme in vielen Bereichen des menschlichen Lebens Einzug gehalten haben, was Lebenswelt und Alltag immer mehr zu Prozessen informationstechnischer Verarbeitung werden lässt.[6]

Dies gilt auch für die Erledigung von Staatsaufgaben, z. B. die Ausübung von Exekutivbefugnissen. Da die Befugnisse rechtlich geregelt sind, muss sich die Beschränkung staatlicher Macht auch in ihren informationstechnischen Werkzeugen wiederfinden.[7]

Die Konvergenz verschiedener individueller und sozialer Lebensbereiche der Menschen im Computer nimmt ein immer größeres Ausmaß an, ohne dass das Verständnis des Computers und seiner Funktionsweise vergleichbar mitwüchse. Dies ergibt eine Abhängigkeit des Einzelnen von komplexen Systemen, die er nicht mehr überblickt.[8] Fremde Eingriffe können daher vom durchschnittlichen Nutzer weder wahrgenommen noch technisch verhindert werden.[9]

Beispiele dieser Komplexität sind unabsichtlich erzeugte Daten, die im Hintergrund Verhalten und Persönlichkeit des einzelnen Nutzers zeitlich festhalten, oder auch die zentrale Anhäufung von Telekommunikationsdaten vieler Personen in derartigen Systemen. All dies erreicht eine neue Qualität in der Ausweitung des Kernbereichs privater Lebensgestaltung ins Digitale. Ein geheimer Eingriff bedeutet den vollständigen Kontrollverlust über diesen Kernbereich; dort setzt die Online-Durchsuchung an.

Die Analyse der Online-Durchsuchung

Eine Online-Durchsuchung wird mittels einer Online-Durchsuchungs-Software (ODS) durchgeführt. Diese muss jeweils für den Einzelfall zusammengestellt werden[10] und kann daher nicht getestet werden. Die Aufbringung auf das zu durchsuchende System ist zudem mit hohen Fehlerrisiken verbunden[11], insbesondere wenn die Infiltration über das Internet erfolgen soll. Um effektiv und effizient heimlich[12] im zu infiltrierenden System suchen und insgesamt agieren zu können, muss die ODS nicht nur mit Benutzerrechten, sondern mit Betriebssystemrechten bzw. im Kernelmode laufen. Nur so kann sie sich z. B. aus Prozesslisten löschen oder Antivirenprogramme täuschen. Um Passwörter direkt aus dem Arbeitsspeicher auszulesen[13], Tastatureingaben abzufangen oder anderweitig Geräte abzufragen ist der Kernelmode zwingend nötig. Somit erlangt die ODS allumfassende Kontrollmöglichkeiten auf dem System.

Die Informationssuche selbst kann bei klassischen, textbasierten Dokumenten ausschließlich anhand syntaktischer Kriterien realisiert werden und ist somit sehr ungenau. Bei vielen Datenquellen aber müssen alle Daten gespeichert werden, da eine Auswertung (teilweise noch) nicht automatisiert erfolgen kann. Das Durchsuchen selbst hinterlässt Datenspuren im System (Datei-

system, Metadaten), die die ODS nach ihrer Aktivität wieder entfernen/zurücksetzen muss. Die gesammelten Daten werden auf dem System vorgehalten und wenn möglich zur entsprechenden staatlichen Stelle übermittelt oder später vor Ort abgeholt, auch dafür muss die ODS schreibend auf das System zugreifen.[14]

Da die ODS auf einem fremden System operiert, ist es nicht möglich, zuverlässige Kryptographie zu betreiben[15], weil auch die ODS weder ihre Integrität noch ihre Vertraulichkeit sicherstellen kann. Dadurch sind folglich weder die Funktionen noch die Aktivitäten der ODS verlässlich belegbar oder rekonstruierbar, was insbesondere wegen der notwendigen Updatefähigkeit der ODS, aber auch wegen der forensischen Bewertung der Funde höchst kritisch zu sehen ist.

Aktuell konzentriert sich die politische Diskussion auf die vermeintlich weniger eingriffsintensive Quellen-Telekommunikationsüberwachung (Quellen-TKÜ), die ausschließlich Daten aktuell laufender Kommunikation ableiten soll. Die Unterscheidung zwischen Online-Durchsuchung und Quellen-Telekommunikationsüberwachung ist aus zwei Gründen jedoch technisch nicht leistbar:

1. Die Quellen-TKÜ-Software wird für das Abfangen zuvor verschlüsselter Daten (Inhalteverschlüsselung, z. B. via pgp) verwendet. Der Versand von Klardaten durch verschlüsselte Verbindungen (Kanalverschlüsselung, z. B. via https) ist in diesem Kontext nicht relevant. Technisch ist jedoch nicht ermittelbar, ob inhalteverschlüsselte Daten überhaupt verschickt werden sollen oder einfach auf dem System verbleiben.

2. Es sind umfassende Informationen über das System nötig, um festzustellen, ob bestimmte Daten z. B. der Bildschirminhalt oder der Inhalt eines Ordners aktuell übertragen wird und somit Gegenstand eines Kommunikationsvorganges ist oder nicht. Diese Informationen darf eine Quellen-TKÜ nicht sammeln.

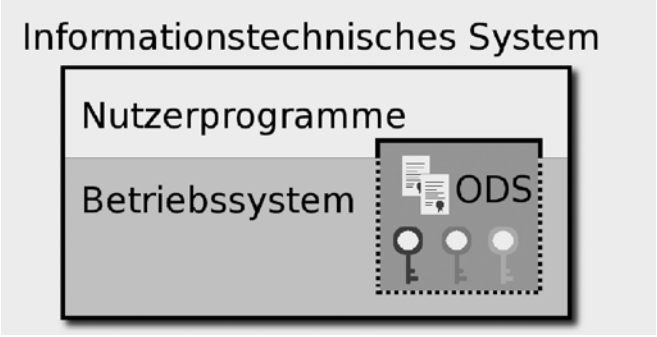


Abbildung 2: Informationstechnisches System

Online-Durchsuchungs-Software und Quellen-Telekommunikationsüberwachungs-Software sind folglich funktionsidentisch. Eine Unterscheidung der Eingriffstiefe der Maßnahmen ist nicht begründbar.

Auch eine Erkennung des Kernbereichs einer Person ist technisch nicht realisierbar[16], weil sie sich den gleichen Problemen gegenübersieht, wie die oben angesprochene Informationssuche. Bei den durchführenden Behörden wird daher eine Anhäufung privater und privatester Daten stattfinden. Daraus ergibt sich, welche Eingriffstiefe eine Maßnahme wie die Online-Durchsuchung für den Betroffenen haben kann und regelmäßig haben wird.

Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und ihre Abwägung

Das Bundesverfassungsgericht erkannte im Jahre 2008 die Abhängigkeit der Bürger von informationstechnischen Systemen und die damit in einem freiheitlichen Rechtsstaat verbundenen berechtigten Erwartungen an Vertraulichkeit und Integrität. Es formulierte nicht nur ein Recht auf diese beiden Eigenschaften, sondern ein Grundrecht auf deren Gewährleistung, auch gegenüber Dritten.[17] Damit beschreibt es einen von der konkreten Sicherheit eines Systems unabhängigen Schutz der Vertraulichkeits- und Integritätserwartung des Einzelnen an das System. Mit dieser Gewährleistung müssen alle Eingriffe in informationstechnische Systeme abgewogen werden.

Zu den oben bereits zusammengetragenen technischen Konsequenzen der Online-Durchsuchung kommen noch andere, weiterreichende Folgen hinzu. Dazu zählt das vergleichsweise hohe Missbrauchspotential[18], u. a. erzeugt durch die einfache Kopierbarkeit digitaler Daten, die geringe Größe heutiger Datenträger und die hohe Komplexität behördeninterner Verarbeitungsabläufe gepaart mit unklaren Handhabungsregeln. Aber auch die Gefährdung Dritter durch die große Streubreite der Maßnahme – auf Computern liegen im Allgemeinen nicht nur Daten des Besitzers – und die hohen gesellschaftlichen Kosten müssen bedacht werden. Ansehen und Glaubwürdigkeit in Sachen IT-Sicherheit, eGovernment usw. sind für einen „hackenden Staat", der durch seine Handlungen auch den Sicherheitslückenschwarzmarkt florieren lässt, selbst optimistisch nur als fragil zu bezeichnen.

Auf den konkreten Nutzen der durch eine Online-Durchsuchung erlangten Informationen bezogen ergibt sich, dass die Funde einer ODS keinesfalls forensischen Standards genügen. Datenmanipulation ist prinzipiell nicht erkennbar und die Echtheit von Funden technisch nicht belegbar.[19] Dennoch sind die Funde laut Bundesverfassungsgericht nicht ohne Informationswert.

Neben diesem nach wie vor laufenden gesellschaftlichen Abwägungsprozess gibt es noch die oben entwickelten, direkt greifbaren Konsequenzen und Erkenntnisse, die aus den technischen Gegebenheiten folgen und nicht Gegenstand, sondern Voraussetzung für eine Diskussion über die Online-Durchsuchung sein sollten.

Zusammenfassung der Ergebnisse

- Eine Funktionsbeschränkung der Software kann **weder sichergestellt noch belegt** werden, daher muss immer die maximale Eingriffshürde zur Anwendung kommen.

- Erlangte Daten haben grundsätzlich **keinen Beweiswert**, sofern sie keinen eigenen intrinsischen Personenbezug aufweisen (z. B. Bilder, die Personen zeigen).

- Die **Trennung** von Telekommunikations- und Nichttelekommunikationsdaten ist insbesondere bei verschlüsselten Daten **technisch nicht lösbar**, daher muss immer – auch für eine Quellen-TKÜ – die maximale Eingriffshürde zur Anwendung kommen.

- Der Kernbereich privater Lebensgestaltung ist praktisch immer betroffen, technischer **Kernbereichsschutz ist prinzipiell nicht möglich**.

Die Beachtung dieser Erkenntnisse ist in der nach wie vor nötigen Diskussion um Einsatz und Verhältnismäßigkeit der Online-Durchsuchung sowie der Interpretation des diesbezüglichen Bundesverfassungsgerichtsurteils dringend notwendig. Darüber hinaus widersprechen die Ergebnisse der aktuellen politischen Praxis und implizieren, dass Exekutive und Legislative ihr Verständnis der Online-Durchsuchung konsequent korrigieren müssen.

Die Folien eines Vortrages zur Online-Durchsuchung an der FAU-Erlangen sind unter folgender URL frei (CC-BY) herunterladbar: *https://od.laryllian.de/downloads/2013.1.7_Online-Durchsuchung.pdf*

Die Arbeit ist unter folgender URL frei (CC-BY) herunterladbar: *https://netzpolitik.org/wp-upload/Rehak-Angezapft.pdf*

Referenzen

Ross Anderson. Security Engineering. Wiley, Indianapolis, 2. Auflage, 2008.

Ulf Buermeyer und Matthias Bäcker. Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des §100a StPO. Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht (HRRS), (10):S eiten 433-441, 2009.

Andreas Bogk (Chaos Computer Club). Antwort zum Fragenkatalog zur Verfassungsbeschwerde 1 BvR 370/07 und 1 BvR 95/07. 23.9.2007.

Frank Braun. 0zapftis – (Un)Zulässigkeit von "Staatstrojanern". Kommunikation & Recht, (11): Seiten 681-686, 2011. Passau.

Bundesministerium des Innern. Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien. Berlin, 22.8.2007.

Bundesregierung der 16. Wahlperiode. Drucksache 16/4997. 10.4.2007.

Bundesregierung der 17. Wahlperiode. Drucksache 17/11598. 21.11.2012 .

Bundesverfassungsgericht. Bundesverfassungsgerichtsurteil zur Online-Durchsuchung. 27.2.2008.

Bundesamt für Sicherheit in der Informationstechnik. „Leitfaden IT-Forensik". Bonn, Version 1.0.1, März 2011.

Alexander Geschonneck. Computer-Forensik. dpunkt.verlag, Heidelberg, 5. Auflage, 2011.

Kristian Köhntopp und Marit Köhntopp. Why Internet Content Rating and Selection does not work, 1999.

Constanze Kurz. Kernbereichsschutz. transcript-verlag, März 2009.

Henry Krasemann und Jörg Ziercke. Interview u. a. zur Online-Durchsuchung. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, MARITIM Hotel Bellevue, Kiel, 2007.

Bodo Pieroth und Bernhard Schlink. Grundrechte. C.F. Müller, Heidelberg, 26. Auflage, 2010.

Bruce Schneier. Secrets and Lies. Wiley, Indianapolis, 2004.

Holger Stark. Digitale Spionage. Der Spiegel, (11): 32-34, 2009.

Andrew S. Tanenbaum. Modern operating systems. Pearson Prentice-Hall, 3. Auflage, 2008.

Anmerkungen

1 *Buermeyer und Bäcker, „Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des §100a StPO", Seite 9, 2009, Braun, „0zapftis – (Un)Zulässigkeit von ‚Staatstrojanern'", Seite 686, 2011 oder der Generalbundesanwalt, siehe Bundesregierung der 17. Wahlperiode. Drucksache 17/11598. Antwort zu Frage 5, 2012.*

2 *Stark, „Digitale Spionage", 2009.*

3 *Z. B. das Rechtekonzept bei Tanenbaum, Modern operating systems, Seite 2 oder das Datei-/Metadatenkonzept, a. a. O., Seite 257, 2008.*

4 *Bundesverfassungsgericht, Bundesverfassungsgerichtsurteil zur Online-Durchsuchung, Absatz 190, 2008.*

5 *Buermeyer und Bäcker, „Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des §100a StPO", 2009.*

6 *Kurz, Kernbereichsschutz, 2009.*

7 *Pieroth und Schlink, Grundrechte, Seite 66 ff, 2010.*

8 *Schneier, Secrets and Lies, Seite 6 ff, 2004.*

9 *Bundesverfassungsgericht, Bundesverfassungsgerichtsurteil zur Online-Durchsuchung, Absatz 180, 2009.*

10 *Krasemann und Ziercke, Interview u. a. zur Online-Durchsuchung, Minute 2:35, 2007.*

11 *Bogk (Chaos Computer Club), Antwort zum Fragenkatalog zur Verfassungsbeschwerde 1 BvR 370/07 und 1 BvR 95/07, Seite 16, 2007.*

12 *Bundesregierung der 16. Wahlperiode, Drucksache 16/4997, Antwort zu Frage 5, 2007.*

13 *a.a.O., Antwort zu Frage 13.*

14 *Bundesministerium des Innern, Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien, Antwort auf Frage 39, 2007.*

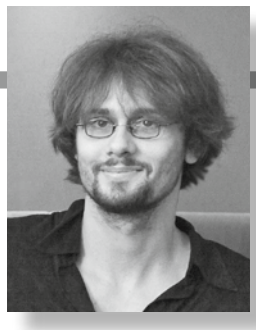
15 *Anderson, Security Engineering, Seite 147 ff., 2008.*

16 *Siehe dazu Köhntopp und Köhntopp, Why Internet Content Rating and Selection does not work, 1999.*

17 *Bundesverfassungsgericht, Bundesverfassungsgerichtsurteil zur Online-Durchsuchung, Absätze 181, 169, 204 und 206, 2007.*

18 *Stark, „Digitale Spionage", 2009.*

19 *Vergleiche Geschonneck, Computer-Forensik, Seite 91 ff, 2011 und Bundesamt für Sicherheit in der Informationstechnik, Leitfaden „IT-Forensik", Seite 89 ff, 2011.*



Rainer Rehak

Rainer Rehak ist Diplom Informatiker (HU-Berlin) und schrieb seine Diplomarbeit zum Thema „Angezapft – Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung". Er studierte von 2002-2012 Informatik und Philosophie in Berlin und Hong Kong und war zwischenzeitlich studentischer Mitarbeiter am Lehrstuhl von Wolfgang Coy. 2012 erhielt er den FIfF-Studienpreis für seine Diplomarbeit. Er ist Mitglied der GI, des CCC und des FIfF.