CyLaw-Report XXXV
ISSN: 1867-1969

TECHNISCHE UNIVERSITÄT DARMSTADT

V. Schmid (Hrsg.): Studienarbeit von cand. Wirtsch. Inf. Hanno Baur: Zur „Beweiskraft informationstechnologischer Expertise“ (Stand 6/2010)

Die ersten CyLaw-Reports I-XIX wurden im Rahmen eines vom Bundesministerium für Bildung und Forschung geförderten Projekts (SICARI (2003 – 2007)) erstellt. Mit CyLaw-Report XX ff. wurde dieses Online-Legal-Casebook vom Fachgebiet Öffentliches Recht an der Technischen Universität Darmstadt (Prof. Dr. Viola Schmid, LL.M. (Harvard)) fortgeführt. Mit CyLaw-Report XXXIV ff. erfolgt auch eine Förderung durch das vom Bundesministerium für Bildung und Forschung initiierte Projekt „Sicherheit im öffentlichen Raum“ (SIRA). Die CyLaw-Reports sind keine „Living Documents“, die ständig aktualisiert werden. Zitierungen können deswegen veraltet sein. Die Rechtfertigung für diese klassische Perspektive ist, dass den in den CyLaw-Reports präsentierten Entscheidungen der Gerichte nur die jeweils geltende Rechtslage zu Grunde gelegt werden konnte. Der Aufgabe der Aktualisierung stellt sich der Lehrstuhl in den integrierten Veranstaltungen Cyberlaw I und Cyberlaw II. Hier wird das Methodenwissen von Studierenden der Technikwissenschaft so gefördert, dass sie in Übungen an der notwendigen Aktualisierung selbst mitwirken können.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Die Forschungen am Fachgebiet Öffentliches Recht widmen sich dem Cyberlaw, dem Recht der Verteilung von Chancen und Risiken, Rechten und Pflichten im Cyberspace. Ein Kernbereich des Cyberlaw sind die Computer Forensics (Cyber Forensics, Forensic Informatics). Erste Vorarbeiten zum Forschungsgebiet Cyber Forensics hat der Studierende der Wirtschaftsinformatik, Herr Hanno Baur, mit seiner Studienarbeit geleistet. Diese Studienarbeit wurde am 11.11.2011 mit dem Absolventenpreis der Deutschen Stiftung für Recht und Informatik ausgezeichnet. Aufbauend auf diese und andere Forschungen machte Frau Prof. Dr. Viola Schmid anlässlich der Teilnahme am Seminar „Forensic Computing“ am 06.10.2011 in Dagstuhl den Vorschlag, ein Casebook on Cyber Forensics (CCF) [1] aufzubauen. Weitere Informationen zu ersten Überlegungen zur „Beweisbaren IT-Sicherheit – und zu sicheren IT-Beweisen“ finden sich auch im Cylaw-Report Nr. XXXIV.

[1] Veröffentlicht unter http://www.dagstuhl.de/drs/index.en.phtml?11401

Abkürzungsverzeichnis

BayVSG	Bayerisches Verfassungsschutzgesetz
BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten
BMI	Bundesministerium des Innern
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
DNA	Desoxyribonukleinsäure, Trägerin der Erbinformation
DoS	Denial of Service
GB	Gigabyte = 1000 MB
GG	Grundgesetz
GPS	Global Positioning System
GUI	Graphical User Interface
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
ISP	Intertnet Service Provider
IP	Internetprotokoll
IT	Informationstechnik
KB	Kilobyte = 1000 Byte
k-NN	k Nearest Neighbor
LG	Landesgericht
LKA	Landeskriminalamt
LSG	Landessozialgericht
MB	Megabyte = 1000 KB
Mio	Millionen
Mrd	Milliarden
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
PAG	Polizeiaufgabengesetz
PC	Personal Computer
SAP	Sichern Analysieren Präsentieren
SPAM	Siced Ham; synonym für unverlangte E-Mail

StGB	Strafgesetzbuch
STINA	Steuerliche Ermittlungen im Internet und Auswertung
StPO	Strafprozessordnung
SVM	Support Vector Machine
TB	Terrabyte = 1000 GB
URL	Uniform Resource Locator
USt-IdNr.	Umsatzsteuer-Identifikationsnummer
VoIP	Voice-over-IP
WLAN	Wireless Local Area Network
WWW	World Wide Web
ZPO	Zivilprozessordnung

Abbildungsverzeichnis

Teil 1: Motivation und Aufbau

Auch wenn das komplette papierlose Büro noch in weiter Ferne liegt, werden immer mehr Informationen nur noch elektronisch erfasst, gespeichert und verarbeitet.[2] Mails erreichen innerhalb weniger Minuten ihren Empfänger, Onlinebanking erspart das Ausfüllen von Überweisungsträgern und die Entgegennahme von Paketen wird elektronisch bestätigt. Ganze Geschäftsprozesse sind digitalisiert, auch die Kommunikation, z.B. mit der Finanzbehörde, läuft elektronisch über das Internet. Da u.a. das Internet kein rechtsfreier Raum ist, besteht die Notwendigkeit auch dort Beweismittel sicherzustellen. Neben der Ausdehnung auf die elektronische Datenverarbeitung und die Nutzung von informationstechnischen Systemen als Tatmittel,[3] ist mit dem Internet auch ein neues Betätigungsfeld für Kriminelle entstanden.[4]

- Erpressung (gedroht wird z.B. mit Denial of Sevice (DoS)-Attacken oder es werden Daten verschlüsselt)[5]
- Vertrieb illegaler Produkte (Internet als Werbeträger, z.B. illegale Server oder SPAM)
- Abfangen von Daten

Nach der Kriminalitätsstatistik ist es 2009, auch wegen der Einführung neuer Straftatbestände, wie beispielsweise dem Abfangen von Daten (§ 202b Strafgesetzbuch (StGB)), zu deutlichem Anstieg der polizeilichen Verdachtsfälle in der Computerkriminalität gekommen.[6] Neben der Steigerung kann auch eine Verlagerung beobachtet werden, so hat sich der durch organisierte Kriminalität verursachte Schaden 2009 gegenüber 2008 von 691 Millionen (Mio) Euro auf 1,3 Milliarden (Mrd) Euro annähernd verdoppelt[7] und gleichzeitig wurde erstmals mit Kreditkartenbetrug mehr Geld umgesetzt als im Rauschgifthandel.[8]

§ 202b StGB Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

[2] York, Ecological Paradoxes: William Stanley Jevons and the Paperless Office, HER 2006, 143, 143.
[3] Hilgendorf, Frank und Valerius, Computer- und Internetstrafrecht, 2005, S. 35.
[4] Freiling, Schriftliche Stellungnahme zum Fragenkatalog Verfassungsbeschwerden, 27.09.2007, https://pi1.informatik.uni-mannheim.de/filepool/publications/stellungnahme-online-durchsuchung.pdf, S. 3, (20.01.2010).
[5] Bachfeld, Trojaner verschlüsselt Daten und Dokumente [Update], heise news, 14.05.2005 http://www.heise.de/newsticker/meldung/Trojaner-verschlüsselt-Daten-und-Dokumente-Update-162911.html (20.01.2010).
[6] Stadler, Anstieg der Computerkriminalität, Internet-Law, 18.05.2010, http://www.internet-law.de/2010/05/anstieg-der-computerkriminalitat.html, (28.05.2010).
[7] o.A., Bundeslagebild Organisierte Kriminalität, Pressereferat im Bundesministerium des Inneren, 04.06.2010, http://www.bka.de/pressemitteilungen/2010/pm100701_bmi.pdf, (04.06.2010).
[8] Faber, Was war. Was wird., heise news, 04.06.2010, http://www.heise.de/newsticker/meldung/Was-war-Was-wird-1032813.html, (04.06.2010).

Der Anstieg von Gerichtverfahren, die (auch) virtuelle Beweismittel bewerten müssen, macht es nötig, die Besonderheiten virtueller Beweise zu untersuchen und zu bewerten. In dieser Arbeit soll der Beweismittelgewinnungsprozess und dessen Implikationen auf den Beweiswert betrachtet werden. Dazu werden allgemeine Ausführungen über den Beweis in Gerichtsverfahren und eine Einführung in das Thema der Indizienbewertung vorangestellt und auf die Eigenschaften digitaler Daten entsprechend eingegangen. Hierbei wird besonders auf die Möglichkeit der vollständigen und rückstandslosen Vernichtung der gespeicherten Informationen hingewiesen, die ein perfektes virtuelles Verbrechen, also ein Verbrechen ohne Spuren, zumindest theoretisch ermöglichen. In den folgenden Kapiteln werden drei Ermittlungsmethoden vorgestellt und soweit allgemein möglich, in Bezug auf den Beweiswert bewertet. Unberücksichtigt bleibt hierbei, ob die Ermittlungsmethoden mit dem Grundgesetz (GG) vereinbar sind oder ob eine nötige Ermächtigungsgrundlage existiert.[9]

Teil 2: Beweis und Beweismittel

Allgemein wird durch einen Beweis eine Tatsache festgestellt. In einem Prozess ist ein Beweis das Mittel, das Gericht von einer Tatsache zu überzeugen. Unbewiesene Tatsachen werden als Sachverhalte bezeichnet, erst durch die Verifizierung mit einem Beweis wird dieser zur Tatsache. Offenkundige Tatsachen müssen nicht bewiesen werden.[10]

A. Beweismaß

Als nötiges Beweismaß muss der Richter dabei persönlich von der Wahrheit der Tatsachenbehauptung überzeugt sein und es muss eine objektive, eine hohe Wahrscheinlichkeit für die Richtigkeit der Tatsachenbehauptung sprechen. Dazu darf keine absolute Gewissheit verlangt werden, die alle theoretisch möglichen Zweifel ausschließt. Zu § 261 Strafprozessordnung (StPO) führt das Bundesverwaltungsgericht (BVerwG) aus:[11]

BVerwG:
<16>[...] § 261 StPO setzt die freie, aus dem Inbegriff der Verhandlung geschöpfte Überzeugung des Tatrichters in subjektiver Hinsicht die für die Überführung des Angeschuldigten erforderliche volle persönliche Gewissheit des Tatrichters voraus. Dies schließt die Möglichkeit eines anderen, auch gegenteiligen Geschehensablaufes nicht aus; denn im Bereich der vom Tatrichter zu würdigenden tatsächlichen Umstände ist der menschlichen Erkenntnis ein absolut sicheres Wissen über den Tathergang, demgegenüber andere Möglichkeiten seines Ablaufs unter allen Umständen ausscheiden müssten, verschlossen. Nach der gesetzlichen Regelung ist es allein Aufgabe des Tatrichters, ohne Bindung an feste gesetzliche Beweisregeln und nur nach seinem Gewissen verantwortlich zu prüfen

[9] Neben der im Teil 6 erwähnten Klage vor dem Bundesverfassungsgericht (BverfG) betrifft dies das Programm Steuerliche Ermittlungen im Internet und Auswertung (STINA) für das nach Ansicht des Bundesdatenschutzbeauftragten die Ermächtigung für eine automatisierte Auswertung fehlt. Schaar, Unterrichtung durch den Bundesbeauftragten für den Datenschutz, Drucksache 15/5252, 19.03.2005, http://www.bfdi.bund.de/cae/servlet/contentblob/409318/publicationFile/25223/20TB_2003_04.pdf, (01.06.2010).

[10] o.A., Rechtslexikon, LexisNexis Deutschland GmbH, 22.08.2007, http://www.juraforum.de/lexikon/, (20.01.2010).

[11] BVerwG Beschl. v. 13.01.2009, Az.2 WD 5.08 Rz. 16 Homepage: http://www.bundesverwaltungsgericht.de (01.02.2010).

und zu entscheiden, ob er die an sich möglichen Zweifel überwinden und sich von einem bestimmten Sachverhalt überzeugen kann oder nicht. Die für die Überführung eines Angeschuldigten erforderliche (volle) persönliche Gewissheit des Tatrichters erfordert ein nach der Lebenserfahrung ausreichendes Maß an Sicherheit, das vernünftige und nicht bloß auf denktheoretische Möglichkeiten gestützte Zweifel nicht mehr aufkommen lässt [...].

<17> Zur Überführung eines Angeschuldigten ist dabei keine "mathematische" Gewissheit erforderlich. Die subjektive Überzeugung des Tatsachengerichts/Tatrichters muss aber auf einer objektiv tragfähigen Tatsachenbasis beruhen. Der Beweis muss mit lückenlosen, nachvollziehbaren logischen Argumenten geführt sein. Allein damit wird die Unschuldsvermutung (Art. 6 Abs. 2 EMRK) widerlegt (vgl. Urteile vom 12. Februar 2003 a.a.O. und vom 3. Juli 2003 a.a.O.).

§ 261 StPO

Über das Ergebnis der Beweisaufnahme entscheidet das Gericht nach seiner freien, aus dem Inbegriff der Verhandlung geschöpften Überzeugung.

Der Bundesgerichtshof (BGH) führt zu rechtsfehlerhaften Urteilen aus:[12]

BGH:
Eine Beweiswürdigung ist demgegenüber etwa dann rechtsfehlerhaft, wenn sie lückenhaft ist, namentlich wesentliche Feststellungen nicht erörtert, widersprüchlich oder unklar ist, gegen Gesetze der Logik oder gesicherte Erfahrungssätze verstößt oder wenn an die zur Verurteilung erforderliche Gewißheit überspannte Anforderungen gestellt sind (st. Rspr., vgl. BGH NJW 2002, 2188, 2189; wistra 1999, 338, 339 jew. m.N.). Dies ist auch dann der Fall, wenn eine nach den Feststellungen naheliegende Schlußfolgerung nicht gezogen ist, ohne daß konkrete Gründe angeführt sind, die dieses Ergebnis stützen können (vgl. Gollwitzer in LR StPO 25. Aufl. § 261 Rdn. 47). Es ist weder im Hinblick auf den Zweifelssatz noch sonst geboten, zu Gunsten des Angeklagten von Annahmen auszugehen, für deren Vorliegen das Beweisergebnis keine konkreten tatsächlichen Anhaltspunkte erbracht hat (BGH NJW 2002, 2188, 2189 m.N.; BGH StraFo 2003, 381). Für die Feststellung von (hier: inneren) Tatsachen genügt demnach, daß ein nach der Lebenserfahrung ausreichendes Maß an Sicherheit besteht, an dem vernünftige Zweifel nicht aufkommen können. Außer Betracht zu bleiben haben solche Zweifel, die keinen realen Anknüpfungspunkt haben (vgl. BGH Beschluß vom 21.06.2001 - 4 StR 85/01 -, BGH NStZ-RR 1999, 332, 333 m.w.N., zu den Anforderungen an die Beweiswürdigung vgl. BGH NStZ-RR, 2003, 271).

Ist im Gesetz ein geringes Beweismaß vorausgesetzt, spricht man von Glaubhaftmachung. Im Gegensatz zum Vollbeweis ist, für eine erfolgreiche Glaubhaftmachung, der Richter nur von der überwiegenden Wahrscheinlichkeit der Tatsachenbehauptung zu überzeugen.[13]

Damit Ermittlungen aufgenommen oder bestimmte Ermittlungsmaßnahmen zulässig sind, müssen im Laufe einer Ermittlung Tatsachen unterschiedlich überzeugend bewiesen werden. Die StPO unterscheidet dafür mehrere Verdachtsstufen.[14] Dabei steht der beurteilenden

[12] BGH, Urt. v. 14.09.2004, Az. 1 StR 180/04, S. 8 f Homepage: http://www.bundesgerichtshof.de (01.06.2010).
[13] o.A., Rechtslexikon, LexisNexis Deutschland GmbH, 22.08.2007, http://www.juraforum.de/lexikon/, (20.01.2010).
[14] o.A., Rechtslexikon, LexisNexis Deutschland GmbH, 22.08.2007, http://www.juraforum.de/lexikon/, (20.01.2010).

Stelle ein gewisser Beurteilungsspielraum zu, der sich allerdings im Laufe des Ermittlungsverfahrens mit Vorliegen von gesicherten Erkenntnissen immer mehr einengt.[15]

- **Anfangsverdacht** liegt vor, wenn es möglich erscheint, dass eine verfolgbare Straftat vorliegt. Der Anfangsverdacht ist z.B. die Voraussetzung für die Aufnahme von Ermittlungen (§ 160 Abs. 1 StPO)

- **Begründeter Tatverdacht** liegt vor, wenn schlüssiges Tatsachenmaterial in erheblichem Maße auf eine Tat hindeutet.[16] Ein begründeter Verdacht ist z.B. für die Anordnung einer Telekommunikationsüberwachungsmaßnahme nötig. (§ 100 a Abs. 1 Nr. 1 StPO)

- **Hinreichender Tatverdacht** liegt vor, wenn eine Verurteilung wahrscheinlicher als eine Freispruch ist.[17] Ein hinreichender Tatverdacht ist z.B. die Voraussetzung für einen Eröffnungsbeschluss, also die Eröffnung des Hauptverfahrens. (§ 203 StPO)

- **Dringender Tatverdacht** liegt vor, wenn ein Beschuldigter mit hoher Wahrscheinlichkeit eine Tat begangen hat.[18] Der dringende Tatverdacht ist z.B. die Voraussetzung für einen Haftbefehl. (§ 112 Abs. 1 S. 1 StPO)

§ 100a StPO

(1) Auch ohne Wissen der Betroffenen darf die Telekommunikation überwacht und aufgezeichnet werden, wenn

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

[...]

§ 112 StPO

(1) Die Untersuchungshaft darf gegen den Beschuldigten angeordnet werden, wenn er der Tat dringend verdächtig ist und ein Haftgrund besteht. Sie darf nicht angeordnet werden, wenn sie zu der Bedeutung der Sache und der zu erwartenden Strafe oder Maßregel der Besserung und Sicherung außer Verhältnis steht.

[...]

[15] BGH, Beschl. v. 11.03.2010, Az. StB 16/09, Rz. 10 Homepage: http://www.bundesgerichtshof.de (01.06.2010).
[16] BVerfG, Urt. vom 03.03.2004, Az. 1 BvR 2378/98, 1 BvR 1084/99, Rz. 247 Homepage: http://www.bundesverfassungsgericht.de (01.06.2010).
[17] BGH, Beschl. v. 22.04.2003, Az. StB 3/03, S. 6 Homepage: http://www.bundesgerichtshof.de (01.06.2010).
[18] BGH, Beschl. v. 22.04.2003, Az. StB 3/03, S. 6 Homepage: http://www.bundesgerichtshof.de (01.06.2010).

§ 160 StPO

(1) Sobald die Staatsanwaltschaft durch eine Anzeige oder auf anderem Wege von dem Verdacht einer Straftat Kenntnis erhält, hat sie zu ihrer Entschließung darüber, ob die öffentliche Klage zu erheben ist, den Sachverhalt zu erforschen.

[...]

§ 203 StPO

Das Gericht beschließt die Eröffnung des Hauptverfahrens, wenn nach den Ergebnissen des vorbereitenden Verfahrens der Angeschuldigte einer Straftat hinreichend verdächtig erscheint.

B. Beweismittel

An die Beweisführung können unterschiedliche Anforderungen gestellt werden. Beim Strengbeweis sind nur die, in entsprechenden Gesetzen zugelassenen Beweismittel, erlaubt, wogegen der Freibeweis nach Ermessen des Gerichts geführt werden kann.

Die Beweismittel können nach der Erbringung in Sachbeweise und Personenbeweise oder nach der zu schließenden Sache in Hauptbeweise und Indizenbeweise (Hilfsbeweise) unterteilt werden. Hauptbeweise dienen dazu, Haupttatsachen zu beweisen. Haupttatsachen sind alle rechtserheblichen Tatsachen.[19] Indizienbeweise dienen dazu, mittelbar positiv oder negativ auf die Haupttatsache zu schließen. Hilfstatsachen bilden eine Untergruppe der Indizientatsachen und dienen zur Beurteilung des Beweiswertes eines Beweismittels.[20]

BGH:
<5>[...] Bei der Würdigung indizieller Beweisergebnisse ist es in der Regel erforderlich, in den Urteilsgründen die tatsächlichen Anknüpfungspunkte der Würdigung so mitzuteilen, dass dem Revisionsgericht eine Überprüfung möglich ist. Den Angeklagten belastende Schlussfolgerungen dürfen nicht auf Vermutungen oder bloße Möglichkeiten gestützt werden..

Für den **Strengbeweis** sind in Zivil-,[21] Straf-,[22] Verwaltungs-,[23] Sozial- und Finanzprozessen folgende Beweismittel zugelassen:

- **Augenscheinbeweis**[24] (sachliches Beweismittel)
- **Parteivernehmung, Beteiligtenanhörung oder Aussagen des Beschuldigten** (personales Beweismittel)

[19] Im Strafprozess wären dies beispielsweise die Täterschaft, der Vorsatz oder die Bereicherungsabsicht. Bender, Nack und Treuer, Tatsachenfeststellung vor Gericht, 2007, Rn. 586.
[20] Eisenberg, Beweisrecht der StPO, 2008, Rn. 8 f.
[21] Zeiss und Schreiber, Zivilprozessrecht, 2003, S. 181.
[22] Krey, Deutsches Strafverfahrensrecht, 2007, S. 44.
[23] Lorenz, Verwaltungsprozessrecht, 2000, S. 575.
[24] Der Augenscheinbeweis ist im Normalfall der einzige unmittelbare Beweis, bei dem gegebenenfalls keine Hilfstatsachen gewürdigt werden müssen. Bender, Nack und Treuer, Tatsachenfeststellung vor Gericht, 2007, Rn. 579.

- **Sachverständigenbeweis** (personales Beweismittel)
- **Urkundenbeweis** (sachliches Beweismittel)[25]
- **Zeugenbeweis**[26] (personales Beweismittel)

Beim Anscheinbeweis wird die auf der Grundlage der allgemeinen Lebenserfahrung beruhende Vermutung erbracht und so typische Geschehensabläufe bewiesen ohne diese genau zu kennen. Hierbei wird keine Gewissheit, sondern nur überwiegende Wahrscheinlichkeit verlangt. Der Anscheinbeweis kann durch den Beweis einer ernsthaften Möglichkeit eines untypischen Verlaufs eines Geschehens entkräftet werden.[27] Hauptanwendungsbereich des Anscheinbeweises ist das Verkehrsrecht, wo z.B. bei einem Unfall unter Alkoholeinfluss der Unfall dem Anschein nach auf die alkoholbedingte Fahruntüchtigkeit zurückgeführt wird. Eine individuelle Entscheidungen kann nie mittels Anscheinbeweises nachgewiesen werden.[28] Ein weiteres Beispiel für einen Anscheinsbeweis ist der Urheberrechtsnachweis eines Fotos, wenn der Fotograf eine zusammenhängende Serie um das strittige Foto vorlegen kann. Dagegen sind die Metadaten einer Fotodatei wegen ihrer Manipulierbarkeit für den Anscheinsbeweis ungeeignet.[29]

C. Indizientatsache

Tatsachen sind dann Indizien, wenn von der Tatsache auf eine Haupttatsache geschlossen werden kann, also wenn im konkreten Einzelfall das Auftreten der Haupttatsache durch die Indizientatsache beeinflusst wird.[30] Eine Tatsache kann dann als Indiz dienen, wenn bezogen auf die zu beweisende Haupttatsache, eine asymmetrische Häufigkeit vorliegt. Eine Indizientatsache muss also häufiger oder seltener in Kombination mit der Haupttatsache auftreten als bei nicht Vorliegen der Haupttatsache. Dabei ist die Häufigkeit des Indizes unerheblich, solange sie entweder häufiger oder seltener im Zusammenhang mit der Haupttatsache auftritt.[31]

[25] Wenn der Richter eine evtl. vorliegende Fälschung eigenständig erkennen kann, ist der Urkundenbeweis ein rein unmittelbarer Beweis, ist dies nicht der Fall, muss gegebenenfalls die Echtheit mittelbar bestimmt werden. Bender, Nack und Treuer, Tatsachenfeststellung vor Gericht, 2007, Rn. 579.
[26] Da neben der Zeugenaussage auch Indizien über die Glaubhaftigkeit des Zeugen ausschlaggebend sind, kann auch der Augenzeuge als mittelbarer Beweis angesehen werden. Bender, Nack und Treuer, Tatsachenfeststellung vor Gericht, 2007, Rn. 582.
[27] Schmid, Sicherheit von ec-Karten, CyLaw-Report V, 17.10.2008, http://tuprints.ulb.tu-darmstadt.de/1103/1Cylaw_Report_V_060117.pdf, (20.01.2010).
[28] o.A., Rechtslexikon, LexisNexis Deutschland GmbH, 22.08.2007, http://www.juraforum.de/lexikon/, (20.01.2010).
[29] LG München, Urt. v. 21.05.2008, Az. 21 O 10753/07, S. 7 f, Homepage: http://medien-internet-und-recht.de, (02.03.2010).
[30] Bender, Nack und Treuer, Tatsachenfeststellung vor Gericht, 2007, Rn. 586 f.
[31] Bender, Nack und Treuer, Tatsachenfeststellung vor Gericht, 2007, Rn. 595.

Die Würdigung der Indizienbeweise muss in der Urteilsbegründung angegeben sein, damit diese im Falle einer Revision geprüft werden können.[32]

I. Beweiskraft von Indizien

Auf Grundlage des Theorems von Bayes, kann die Bewertung des Beweiswertes eines Indizes anhand folgender Fragentrias durchgeführt werden.[33]

1. Wie häufig kommt das Indiz bei gleichzeitigem Vorliegen der Haupttatsache vor?
2. Wie häufig kommt das Indiz bei nicht Vorliegen der Haupttatsache vor?
3. Liegt das Indiz häufiger bei Vorliegen der Haupttatsache oder bei nicht Vorliegen der Haupttatsache vor?

Können beide Fragen über die Verteilung eines Indizes verlässlich beantwortet werden, könnte der Beweiswert eines Indizes mathematisch bestimmt werden. Das Errechnen von Urteilen wird von der überwiegenden Literaturmeinung abgelehnt.[34] Da bei der Beweiswürdigung die Gesetze der Logik und Mathematik eingehalten werden müssen,[35] kann das Theorem von Bayes aber als eine Richtschnur bei der Beweiswürdigung dienen.[36]

Können die Fragen nicht beantwortet werden, ist das Indiz aus rein wissenschaftlicher Sicht wertlos.[37] Nur in seltenen Fällen, wie beispielsweise bei DNA-Tests, liegen empirisch abgesicherte Erkenntnisse über die konkrete Häufigkeitsverteilung vor.[38] Gerichte sind also in der Regel gezwungen Überlegungen zur Häufigkeitsverteilung aufzustellen und diese unter Einbeziehung der jeweils gültigen Randbedingungen auf Plausibilität zu prüfen. Dabei ist davon auszugehen, dass in der Regel Dissens über die zugrundeliegende Wahrscheinlichkeit zwischen den einzelnen Parteien besteht.[39] Durch Angabe der angenommenen Verteilung kann eine höhere Transparenz[40] erreicht werden und so die Anforderung des BGH bezüglich der Revisionsfähigkeit der Indizienwürdigung erfüllt werden.[41]

Zur Lösung des Problems der unbekannten Anfangswahrscheinlichkeit, schlägt Dieter Kochheim die Nutzung von Erfahrungswerten als Anhaltspunkte für die Bewertung der Indizien vor. Hierzu soll über Erfahrungswerte ein fünfstufiger Geltungsgrad zugeordnet werden,

---

[32] BGH, Beschl. v. 31.10.2006, Az. 2 StR 417/06, S.4 Homepage: http://www.bundesgerichtshof.de (01.02.2010).
[33] Bender, Nack und Treuer, Tatsachenfeststellung vor Gericht, 2007, Rn. 592.
[34] Schweizer, Intuition, Statistik und Beweiswürdigung, 01.04.2006, http://www.decisions.ch/publikationen/intuition_statistik.html, (20.01.2010), Rn. 32.
[35] Eisenberg, Beweisrecht der StPO, 2008, Rn. 102.
[36] Rüßmann, Das Theorem von Bayes und die Theorie des Indizienbeweises, ZfZ 1990, 62, 63.
[37] Schweizer, Kognitive Täuschung vor Gericht, 2005, Rn. 400.
[38] Bender, Nack und Treuer, Tatsachenfeststellung vor Gericht, 2007, Rn. 603.
[39] Bender, Nack und Treuer, Tatsachenfeststellung vor Gericht, 2007, Rn. 604.
[40] Gleichzeitig eine höhere Angreifbarkeit
[41] Bender, Nack und Treuer, Tatsachenfeststellung vor Gericht, 2007, Rn. 606.

über den dann bestimmt wird, ob und wie viele zusätzliche Hilfstatsachen zu untersuchen sind.[42]

1. Erfahrung aus einem Einzelfall
2. Erfahrung, die aus verschiedenen Einzelfällen gewonnen wurde
3. Erfahrung mit überwiegender Wahrscheinlichkeit
4. sichere Erkenntnis, für die Ausnahmen bekannt oder denkbar sind
5. sichere Erkenntnis, für die keine Ausnahmen bekannt oder denkbar sind

Die Heranziehung von Erfahrungswerten ist kritisch zu sehen, da wie im nächsten Kapitel gezeigt wird, die Anfangswahrscheinlichkeit einen hohen Einfluss auf den Beweiswert hat. Erfahrungen von Ermittlern beziehen sich unter Umständen nur auf Sachverhalte bei denen bereits ein Anfangsverdacht vorliegt. Es stehen also nur geringe oder überhaupt keine Erfahrungswerte mit anderen, „unverdächtigen" Sachverhalten zur Verfügung. Deswegen kann es leicht zu den im Teil 2, C, III beschriebenen Fehlern einer zu hoch angesetzten Anfangswahrscheinlichkeit kommen.[43]

II. Berechnung des Beweiswertes

Da sich Beweise auf Tatsachen in der Vergangenheit beziehen, liegt die Wahrscheinlichkeit, ob ein Indiz (belastend oder entlastend) vorliegt, streng genommen bei 1 oder 0, es steht also im Zusammenhang mit der betrachteten Haupttatsache oder nicht.[44] Da gerade dieses Wissen aber fehlt, kann über Wahrscheinlichkeiten ein Grad der Überzeugung über die Aussagekraft eines Indizes ausgedrückt und so als ein Maß für die Beweiskraft eines Indizes herangezogen werden.

- $P(T)$ sei die Anfangswahrscheinlichkeit, dass die Haupttatsache vorliegt
- $P(\overline{T})$ sei die Anfangswahrscheinlichkeit, dass die Haupttatsache nicht vorliegt
- $P(I)$ sei die Wahrscheinlichkeit, dass das Indiz vorliegt
- $P(\overline{I})$ sei die Wahrscheinlichkeit, dass das Indiz nicht vorliegt

Damit lässt sich die Fragentrias mathematisch wie folgt darstellen:[45]

1. $P(I|T)$ sei die Wahrscheinlichkeit, dass das Indiz I unter der Bedingung: Vorliegen der Haupttatsache T, auftritt
2. $P(I|\overline{T})$ sei die Wahrscheinlichkeit, dass das Indiz I unter der Bedingung: nicht Vorliegen der Haupttatsache T, auftritt

[42] Kochheim, Geltung von Beweisen und Erfahrungen, Cyberfahnder, 29.11.2009, http://www.cyberfahnder.de/nav/them/pish/skimkrimerf.html (10.07.2010).
[43] Schweizer, Kognitive Täuschung vor Gericht, 2005, Rn. 397.
[44] Lehn, Wegmann und Rettig, Einführung in die Statistik, 2001, S. 34.
[45] Lehn, Wegmann und Rettig, Einführung in die Statistik, 2001, S. 33.

3. $\frac{P(I \mid T)}{P(I \mid \overline{T})}$ wird als Likelihood-Quotient bezeichnet und beschreibt die abstrakte Beweiskraft eines Indizes.[46]

Ein Indiz ist immer dann belastend, wenn der Likelihood-Quotient größer als 1 ist und entlastend, wenn er kleiner als 1 ist. Ist der Likelihood-Quotient gleich 1, verhält sich die Tatsache neutral und erfüllt somit nicht die Voraussetzung eines Indizes.[47]

In Abbildung 1 werden die beiden ersten Fragen visualisiert. Dabei wird durch das Quadrat der Raum mit allen möglichen Ereignissen dargestellt. Die beiden Kreise stellen die zu beweisende Haupttatsache T und das betrachtete Indiz I dar. Die karierte Fläche zeigt die Kombination beider Ereignisse T und I. Die vertikal gestreifte Fläche symbolisiert die Ereignisse I ohne Vorliegen der Ereignisse T.

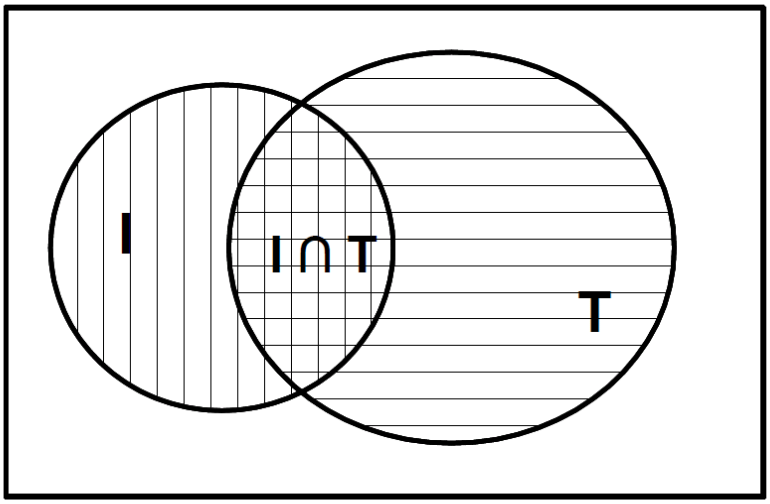

Abbildung 1: Kombination zweier Ereignisse

Wenn die Wahrscheinlichkeit des Auftretens der Haupttatsache P(T) > 0 ist, kann die bedingte Wahrscheinlichkeit $P(I \mid T) = \frac{P(I \cap T)}{P(T)}$ bestimmt werden.[48] Ist die Wahrscheinlichkeit des Auftretens der Haupttatsache T bekannt, kann durch die Anwendung des Theorems von Bayes die Belastungswahrscheinlichkeit eines Indizes, also die bedingte Wahrscheinlichkeit P(T|I), berechnet werden.[49]

[46] Bender, Nack und Treuer, Tatsachenfeststellung vor Gericht, 2007, Rn. 682.
[47] Schweizer, Kognitive Täuschung vor Gericht, 2005, Rn. 685.
[48] Lehn, Wegmann und Rettig, Einführung in die Statistik, 2001, S. 33.
[49] Schweizer, Kognitive Täuschung vor Gericht, 2005, Rn. 369.

$$P(T|I) = \frac{P(I|T)*P(T)}{P(I)} = \frac{P(I|T)*P(T)}{P(T)*P(I|T)+P(\bar{T})*P(I|\bar{T})}$$ [50]

Setzt man die Belastungswahrscheinlichkeit P(T|I) ins Verhältnis mit der bedingten Wahrscheinlichkeit P(\bar T|I), also der Wahrscheinlichkeit, dass die Haupttatsache bei vorliegendem Indiz nicht vorliegt, bekommt das Bayes-Theorem folgende Form:[51]

$$\frac{P(T|I)}{P(\bar{T}|I)} = \frac{P(T)}{P(\bar{T})} * \frac{P(I|T)}{P(I|\bar{T})}$$

Die bedingte Chance ist also gleich der Anfangschance multipliziert mit dem Likelihood-Quotienten.[52] Je niedriger die Ausgangswahrscheinlichket, desto höher muss also die abstrakte Beweiskraft liegen, um eine hohe Endwahrscheinlichkeit zu erreichen. Bei einer Anfangswahrscheinlichkeit von 1% ist eine abstrakte Beweiskraft von 1.000 nötig, um eine Endwahrscheinlichket von über 90% zu erreichen. Liegt die Anfangswahrscheinlichkeit bei 50%, wird dagegen schon bei einer abstrakten Beweiskraft von 10, 91% Endwahrscheinlichkeit erreicht.[53]

Für die Überzeugungsbildung reicht nach dem BGH z.B. ein moderner DNA-Test, mit einer Wahrscheinlichkeit von 1:256 Billiarden, dass die DNA-Spur einem Verursacher zuzuordnen ist, aus.[54] Bei dieser Merkmalswahrscheinlichkeit wirkt sich eine geringe Anfangswahrscheinlichkeit kaum noch aus.[55]

III. Fehler bei der Beweiswürdigung

Bei der Bewertung kann es zu zwei typischen Fehlern kommen, die auch als Trugschluss des Anklägers[56] bzw. Trugschluss des Verteidigers[57] bezeichnet werden. Mathematisch formuliert werden dabei fälschlicherweise P(T|I) und P(I|T) vertauscht.[58]

Wenn zu Unrecht von einer überhöhten Anfangswahrscheinlichkeit von 50% ausgegangen wird, liegt der Trugschluss des Anklägers vor. Bei einer 50%igen Anfangswahrscheinlichkeit, kann von der Information, wie häufig ein Indiz bei Vorliegen der Haupttatsache auftritt, direkt auf die Wahrscheinlichkeit der Haupttatsache beim Vorliegen des Indizes geschlossen wer-

[50] Im Umformungsschritt, wird die Anfangswahrscheinlichkeit für das Vorliegen des Indizes I P(I) mit Hilfe der bedingten Wahrscheinlichkeiten im Zusammenhang mit der Haupttatsache T dargestellt.
[51] Schweizer, Kognitive Täuschung vor Gericht, 2005, Rn. 366.
[52] Schweizer, Kognitive Täuschung vor Gericht, 2005, Rn. 372.
[53] Bender, Nack und Treuer, Tatsachenfeststellung vor Gericht, 2007, Rn. 704.
[54] BGH, Beschl. v. 21.01.2009, Az. 1 StR 722/08, Rz.: 1 Homepage: http://www.bundesgerichtshof.de (29.06.2010).
[55] Bender, Nack und Treuer, Tatsachenfeststellung vor Gericht, 2007, Rn. 652.
[56] Schweizer, Kognitive Täuschung vor Gericht, 2005, Rn. 135.
[57] Bender, Nack und Treuer, Tatsachenfeststellung vor Gericht, 2007, Rn. 613.
[58] Schweizer, Kognitive Täuschung vor Gericht, 2005, Rn. 403.

den.[59] Kann beispielsweise durch einen Test zu 95% beim Vorliegen der Haupttatsache dies richtig angezeigt werden und werden gleichzeitig bei einem Prozent der Tests, bei denen die Haupttatsache nicht vorliegt, diese angezeigt, so liegt die abstrakte Beweiskraft bei 95 zu 1. Bei unterschiedlicher Anfangswahrscheinlichkeit von 0,1% bzw. 10% ergeben sich daraus dann die Belastungswahrscheinlichkeiten von 9% und 91%.[60] Kann begründet von einer Anfangswahrscheinlichkeit von 50% ausgegangen werden, liegt kein Trugschluss vor, es kann allerdings zum Trugschluss kommen, wenn sich die angenommene Anfangswahrscheinlichkeit nicht bestätigt.[61]

Beim Trugschluss des Verteidigers wird etwas sehr Untypisches fälschlich als nicht belastend angesehen, weil das Indiz nur in sehr geringer Anzahl in Kombination mit der Haupttatsache auftritt. Auch hierbei werden die Fragen umgedreht und nach der Wahrscheinlichkeit gefragt, dass die Haupttatsache bei Vorliegen des Indizes eintritt.[62]

Durch Kenntnis des Theorems von Bayes und der daraus ergebenen Fragentrias lässt sich die Häufigkeit der beschriebenen Trugschlüsse reduzieren, auch wenn die Anwendungsvoraussetzungen, also z.B. die Bekanntheit der Anfangswahrscheinlichkeiten, nicht gegeben sind.[63]

D. Kombination von Indizien

Kann durch ein einzelnes Indiz keine ausreichende Beweiskraft aufgebracht werden oder lässt es keinen mittelbaren Schluss zu, müssen gegebenenfalls mehrere Indizien kombiniert werden, um die nötige Gewissheit zu erreichen. Dabei kann die Kombination von unabhängigen Indizien als Beweisring oder als Beweiskette erfolgen.[64] Unabhängig sind Indizien immer dann, wenn sie sich in ihrem jeweiligen Auftreten gegenseitig nicht beeinflussen.[65] Abhängige Indizien können in Indizienfamilien gebündelt und ausgewertet werden.

I. Indizienring

Bei einem Beweisring werden, wie in Abbildung 2 dargestellt, mehrere schwache Indizien kombiniert und somit eine höhere Beweiskraft erreicht. Dabei wird von allen Indizien auf die

[59] Bender, Nack und Treuer, Tatsachenfeststellung vor Gericht, 2007, Rn. 611.
[60] Bender, Nack und Treuer, Tatsachenfeststellung vor Gericht, 2007, Rn. 600.
[61] Schweizer, Kognitive Täuschung vor Gericht, 2005, Rn. 410.
[62] Als Beispiel führt u.a. Schweizer hier den Prozess gegen O.J.Simpson aus der USA an. O.J.Simpson war angeklagt, seine Frau umgebracht zu haben und als ein Beweis wurde vorgebracht, O.j. Simpson habe erwiesenermaßen seine Frau geschlagen. Die Verteidigung legte dar, dass nur 0,001% der schlagenden Ehemänner ihre Frauen auch umbringen. Das Indiz "`Schläger"' sei somit nicht belastend für die untersuchte Haupttatsache. Irving j Good widerlegte diese Argumentation, indem er die Anfangswahrscheinlichkeit mit einbezog und nicht vom Indiz, als dem Schlagen, sondern von der Tatsache, dass die Frau ermordet wurde ausging. Bei einer in der USA ermordeten Frau, lag die Wahrscheinlichkeit, dass ihr schlagender Ehemann der Mörder ist, ohne die Betrachtung weiterer Beweise bei 50%. Schweizer, Kognitive Täuschung vor Gericht, 2005, Rn. 412 ff.
[63] Schum und Martin, Formal and Empirical Research on Cascaded Inference in Jurisprudence, LSR 1982, 105, 152.
[64] Bender, Nack und Treuer, Tatsachenfeststellung vor Gericht, 2007, Rn. 622.
[65] Lehn, Wegmann und Rettig, Einführung in die Statistik, 2001, S. 36.

Haupttatsache geschlossen. Der Beweiswert kann über das Theorem von Bayes errechnet werden. Dabei können entweder die errechneten Belastungswahrscheinlichkeiten eines Indizes jeweils als Anfangswahrscheinlichkeit für das nächste Indiz herangezogen werden oder das Produkt über die Beweiskraft der Einzelindizien gebildet oder es wird eine erweiterte Formel von Bayes verwendet, die hier beispielhaft für zwei Indizien A und B dargestellt wird:[66]

$$P(T|A\&B) = \frac{P(T)*P(A|T)*P(B|T)}{P(T)*P(A|T)*P(B|T)+P(\bar{T})*P(A|\bar{T})*P(B|\bar{T})}$$

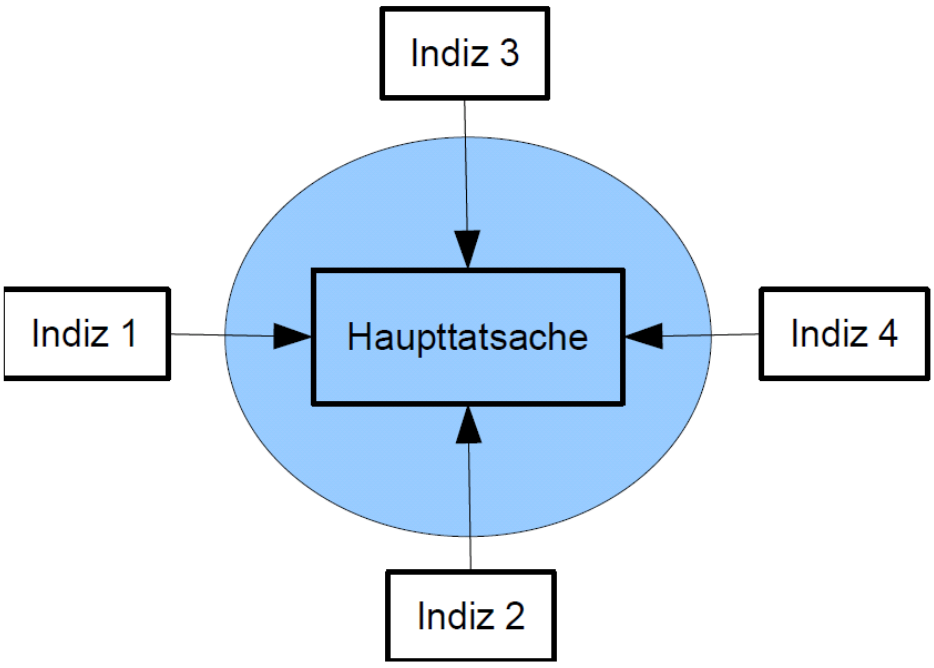

Abbildung 2: Indizien in einem Beweisring[67]

II. Indizienkette

Bei einer Indizienkette werden die Indizien, wie in Abbildung 3 dargestellt, einzeln hintereinander gereiht. Dabei nimmt die Beweiskraft mit steigender Anzahl an verketteten Indizien ab. Für die Berechnung der Gesamtbeweiskraft der Kette, muss die Belastungswahrscheinlichkeit aller notwendigerweise gleichzeitig vorliegenden Indizien multipliziert werden.[68] Bei einer dreistufigen Indizienkette mit der jeweiligen Einzelbelastungswahrscheinlichkeit von 90%, 80% und 70% ergibt sich nach Anwendung der Produktregel nur noch eine Gesamtbelastungswahrscheinlichkeit von 0,9*0,8*0,7=0,504=50,4%.

[66] Bender, Nack und Treuer, Tatsachenfeststellung vor Gericht, 2007, Rn. 674.
[67] Nach Bender, Nack und Treuer, Tatsachenfeststellung vor Gericht, 2007, S. 160. .
[68] Bender, Nack und Treuer, Tatsachenfeststellung vor Gericht, 2007, Rn. 637 ff.

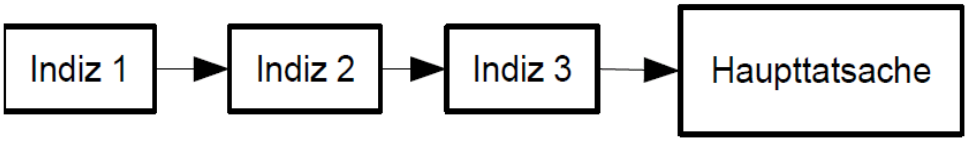

Abbildung 3: Indizien in einer Beweiskette[69]

III. Indizienfamilie

Sind die Indizien abhängig, beeinflussen sie ihr Eintreten untereinander. Durch Zusammenfassung der abhängigen Indizien in Indizienfamilien, kann die Fragentiras auf die komplette Indizienfamilie angewendet werden. Bei der Kombination der Indizien muss die Art der Abhängigkeit berücksichtigt werden. Besteht zwischen den einzelnen Indizien eine positive Abhängigkeit, erhöht sich die Beweiskraft durch die Kombination der Indizien weniger, als bei einer entsprechenden Anzahl unabhängiger Indizien. Besteht hingegen eine negative Abhängigkeit, kann sich die Beweiskraft gegenüber den unabhängigen Indizien stärker erhöhen.[70]

E. Beweismittelgewinnung

Einige Beweismittel stehen nicht, wie z.B. die Beteiligtenanhörung, automatisch zur Verfügung, sondern sie müssen erst ermittelt werden. Dazu kann es nötig sein, die Beweise, die nicht direkt als Beweise verwertbar sind, wie z.B. Zeugen-, Anschein- oder Urkundenbeweis, aus Spuren zu ermitteln. Allgemein kann ein Ermittlungsprozess in drei Phasen: **S**ichern, **A**nalysieren und **P**räsentieren (SAP-Modell)[71], unterteilt werden. In der Sicherungsphase sind dabei folgende Tätigkeiten durchzuführen:

- Untersuchungsbereich gegen Manipulation absichern
- Beweisspuren sichern
- Protokollieren der durchgeführten Tätigkeiten

Während der Analysephase werden die vorher festgestellten Spuren ausgewertet. Ziel ist es, möglichst alle W-Fragen (wer, was, wo, wann, womit, wie und weshalb) zu beantworten, alle Schlüsse werden dabei kritisch hinterfragt. Die Ergebnisse sind möglichst vollständig und allgemein verständlich zu dokumentieren.[72]

---

[69] Nach Bender, Nack und Treuer, Tatsachenfeststellung vor Gericht, 2007, S. 162.
[70] Bender, Nack und Treuer, Tatsachenfeststellung vor Gericht, 2007, Rn. 636 f.
[71] Auch als Secure-Analyse-Present-Modell bezeichnet, Geschonneck, Computer Forensik, 2008, S. 64.
[72] Greifeneder, Disk Forensik, 22.05.2008, http://de.wikibooks.org/wiki/Disk_Forensik/_Richtlinien/_Das_SAP-Modell, (20.01.2010).

F. Der Sachverständigenbeweis

Ein Sachverständiger stellt dem Richter Fachwissen zu Verfügung, wenn ihm dieses fehlt und wird vom Gericht beauftragt. Dabei kann der Sachverständige herangezogen werden, um allgemeine Erfahrungssätze weiterzugeben. Er selbst hat keine Schlussfolgerungen durchzuführen, sondern nur Informationen zur Abschätzung der Anfangswahrscheinlichkeit bereitzustellen. Eine zweite Aufgabe liegt in der Begutachtung einer bestimmten einzelnen Tatsache, zu dessen Wahrnehmung bestimmte Sachkenntnis nötig ist. Die dritte und weitreichendste Aufgabe eines Sachverständigen ist die Begutachtung kompletter Sachverhalte. Dabei ist zu beachten, dass es nicht zu einer Verlagerung der rechtsprechenden Gewalt, wie sie in Art. 92 1. HS GG festgelegt ist, vom Richter zum Gutachter kommt.[73] Die Ausführungen des Sachverständigen dürfen vom Gericht nicht kritiklos übernommen werden, sondern müssen von diesem auf Plausibilität geprüft werden.[74] Da der Sachverständige dem Gericht fehlenden Sachverstand zu Verfügung stellt, wird der Richter allerdings im Normalfall die Ausführungen fachlich nicht im Einzelfall prüfen können und muss so Indizien auswerten, die auf die Glaubwürdigkeit des Sachverständigen hinweisen.

BGH:
[...] Folgt der Richter dem Gutachten eines Sachverständigen, hat er die wesentlichen Anknüpfungstatsachen und Ausführungen des Gutachters so darzulegen, daß das Rechtsmittelgericht prüfen kann, ob die Beweiswürdigung auf einer tragfähigen Tatsachengrundlage beruht und ob die Schlußfolgerungen nach den Gesetzen der Logik, den Erfahrungssätzen des täglichen Lebens und den Erkenntnissen der Wissenschaft möglich sind. Der Sachverständige hat als Gehilfe des Richters die zur Beurteilung der Rechtsfragen notwendigen Tatsachen und wissenschaftlichen Erkenntnisse beizusteuern. (BGHSt 7, 238; 8, 113, 118; 12, 311, 314; 34, 29, 31 m.w.N.). Deshalb bedarf es der Kontrolle des Rechtsmittelgerichts, ob der Tatrichter gegenüber dem Sachverständigen die Selbständigkeit des Urteils gewahrt hat (vgl. BGHSt 7, 238, 239; 8, 113, 118; BGH GA 1962, 116; BGHR StPO § 261 Sachverständiger 1, Überzeugungsbildung 17).

Art. 92 GG

Die rechtsprechende Gewalt ist den Richtern anvertraut; sie wird durch das Bundesverfassungsgericht, durch die in diesem Grundgesetze vorgesehenen Bundesgerichte und durch die Gerichte der Länder ausgeübt.

Das Gericht muss, um einem möglichen Revisionsgericht die gebotene Nachprüfung zu ermöglichen, die Ausführungen des Sachverständigen, die dazugehörenden Anknüpfungspunkte und die aus dem Gutachten gezogenen Schlussfolgerungen im Urteil wiedergeben.[75] Der Umfang der Darstellung hängt dabei, neben der jeweiligen Beweislage und der Bedeu-

[73] Krey, Deutsches Strafverfahrensrecht, 2007, Rn. 941 f.
[74] BGH, Beschl. v. 19.03.1993, Az. 4 StR 627/92 Homepage: http://www.bundesgerichtshof.de (01.02.2010).
[75] BGH, Urteil. v. 27.11.1999, Az. 3 StR 241/99, Rn.: 8 Homepage: http://www.bundesgerichtshof.de (01.02.2010).

tung der Beweisfrage, davon ab, ob es sich um eine standardisierte Untersuchungsmethode handelt.[76]

I. Allgemeine Anforderungen

Der Sachverständige sollte aktuelle, dem wissenschaftlichen Kenntnisstand entsprechenden und anerkannte Methoden anwenden. Stehen mehrere anerkannte Methoden zur Verfügung, ist es die freie Wahl des Sachverständigen welche Methode dieser anwendet. Werden andere Testverfahren eingesetzt, muss dies im Sinne der Revisionsfähigkeit begründet werden.[77] Die Methoden und eingesetzten Hilfsmittel müssen bei der Anwendung durch, z.B. einen weiteren Sachverständigen, die gleichen Ergebnisse liefern. Insgesamt muss sichergestellt sein, dass ermittelte Ergebnisse nicht nachträglich manipuliert und die Methoden zusammen mit den Ergebnissen angemessen dokumentiert werden.[78]

Neben den inhaltlichen Gesichtspunkten muss auch die Darstellung des Gutachtens mängelfrei erfolgen, damit das Gericht den entsprechenden Ausführungen folgen kann und nicht einem Trugschluss unterliegt.

Ein Sachverständiger kann Hilfskräfte bei der Gutachtenerstellung heranziehen, wenn die Gesamtverantwortung durch den Sachverständigen gesichert bleibt und dieser nicht lediglich das Gutachten unterschreibt.[79]

II. Erweiterte Anforderungen

Über die Wahl der Informationsdarstellung im Gutachten hat der Sachverständige direkt Einfluss auf die Häufigkeit der oben beschriebenen Trugschlüsse. Deshalb wird u.a. gefordert, dass ein Gutachter nicht die Belastungswahrscheinlichkeit, ausgehend von der "neutralen" Anfangswahrscheinlichkeit von 50%, sondern den Likelihood-Quotienten angeben soll. Diese Forderung ist kritisch zu sehen, da sich dadurch ein Großteil der Beweiswürdigung, wie z.B. die Annahme der Anfangswahrscheinlichkeit, vom Richter zum Sachverständigen verlagert und der Sachverständige alle Umstände des konkreten Einzelfalls berücksichtigen müsste.[80] Anstelle der Belastungswahrscheinlichkeit, bei der dem Gericht leicht der Trugschluss des Anklägers unterlaufen kann,[81] kann die Merkmalswahrscheinlichkeit, z.B. bezogen auf die Gesamtbevölkerung, angegeben werden. Dadurch wird offensichtlicher, welche zusätzlichen Fragen durch das Gericht beantwortet und begründet werden müssen.[82]

---

[76] OLG Bamberg, Beschl. v. 06.04.2010, Az. 3 Ss OWi 378/10 Homepage: http://www.beck.de (01.07.2010).

[77] BGH, Urteil. v. 30.07.1999, Az. 1 StR 618/98, Rn.: 17 Homepage: http://www.bundesgerichtshof.de (01.02.2010).

[78] Geschonneck, Computer Forensik, 2008, S. 63.

[79] Rüping, Zur Rolle des Sachverständigen im Strafverfahren, 10.12.2009, http://www.pknds.de/fileadmin/user_upload/Dokumente/Sonstiges/Berichte/Herr_Prof._Dr._Hinrich_Rueping_2.pdf, (20.01.2010).

[80] Schweizer, Kognitive Täuschung vor Gericht, 2005, Rn. 500 ff.

[81] Dieser Fehler unterlief z.B. dem Landesgericht (LG) Hannover bei der Bewertung eines DNA-Test im Jahr 1987. BGH, Urt. v. 12.08.1992, Az. 5 StR 239/92, Rn.: 15 Homepage: http://www.hrr-strafrecht.de (01.02.2010).

[82] Schweizer, Kognitive Täuschung vor Gericht, 2005, Rn. 500 ff.

Die zweite Forderung betrifft die Präsentation der bedingten Wahrscheinlichkeit. In Gutachten wird oft dargelegt, wie häufig ein Indiz auftritt, wenn die Haupttatsache nicht vorliegt. Im Sinne der oben vorgestellten Fragentrias interessiert das Gericht allerdings, wie häufig die Haupttatsache nicht vorliegt (ein Angeklagter beispielsweise unschuldig ist), obwohl das Indiz vorliegt. Das intuitive Verständnis wird dabei erleichtert, wenn anstelle von Prozentwerten die natürliche Häufigkeit angegeben wird. Anstelle von 15% Wahrscheinlichkeit beispielsweise 15 von 100.[83]

Teil 3: Digitale Beweismittel

Ausschlagsgebend für ein Beweismittel ist der auf oder mit ihm verkörperte Informationswert. Datenträger, als Träger von Informationen, gehören damit zu möglichen Beweismitteln und sind z.B. nach § 94 Abs. 1 StPO sicherstellbar.[84] Neben der Beschlagnahme des Datenträgers, wird auch das Kopieren der Daten abgedeckt.[85] Andere gesetzliche Beweisregelungen wie z.B. in § 371 Abs. 1 S. 2 ZPO sprechen explizit von Dateien als Beweismittel. Grundsätzlich können Daten damit in vielfältiger Form als Beweismittel Verwendung finden und sind in der Regel als Augenscheinobjekte einzustufen.[86]

§ 94 StPO

(1) Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können, sind in Verwahrung zu nehmen oder in anderer Weise sicherzustellen.

(2) Befinden sich die Gegenstände in dem Gewahrsam einer Person und werden sie nicht freiwillig herausgegeben, so bedarf es der Beschlagnahme.

[...]

§ 371 ZPO Beweis durch Augenschein

(1) Der Beweis durch Augenschein wird durch Bezeichnung des Gegenstandes des Augenscheins und durch die Angabe der zu beweisenden Tatsachen angetreten. Ist ein elektronisches Dokument Gegenstand des Beweises, wird der Beweis durch Vorlegung oder Übermittlung der Datei angetreten.

[...]

A. Eigenschaften digitaler Daten

Technisch sind Daten definiert als Zeichen, die eine bekannte oder vermutete Zuordnung, Information darstellen.[87] Bei digitalen Daten werden die Informationen im Binarcode, also

[83] Schweizer, Kognitive Täuschung vor Gericht, 2005, Rn. 446 ff.

[84] BVerfG, Beschl. v. 18.02.2003, Az. 2 BvR 372/0,1 Rz. 9, Homepage: http://www.bundesverfassungsgericht.de (05.04.2010).

[85] BVerfG, Beschl. v. 12.04.2005, Az. 2 BvR 1027/02, Rz. 100, Homepage: http://www.bundesverfassungsgericht.de (05.04.2010).

[86] Eisenberg, Beweisrecht der StPO, 2008, Rn. 2023.

[87] Bach u.a., Tabellenbuch Kommunikationselektronik, 1995, S. 287.

durch ausschließliche Verwendung von zwei Symbolen (z.B. 0 und 1) dargestellt. Zur physikalischen Speicherung werden die beiden Symbole beispielsweise in magnetische Polarität (Nord/Süd), optische Höhenunterschiede (Pits/Lands) oder elektronische Ladungen (geladen/ungeladen) umgesetzt. Beiden Zuständen zur Datenspeicherung ist eine Bedeutung zugeordnet, damit wird ersichtlich, dass Daten nicht gelöscht, im Sinne von entfernt, sondern nur überschrieben werden können, da beide Zustände Informationen tragen. Wird z.B. die Speicherstelle im Hauptspeicher, welche die Zeitinformation enthält, auf 0 gesetzt, würde dies nur zu einem Rücksetzen der Zeit auf das Ausgangsdatum bedeuten und die ebenfalls kodierten Informationen über die Dauer einer Zeiteinheit gelöscht. Überschreibt man die Zieladresse eines Sprungbefehls mit 0, würde der Sprung nicht abgebrochen, sondern nur das Sprungziel auf dem ersten Speicherblock verändert. Bei anwendernahen Anwendungen werden Daten meistens nicht gelöscht, sondern deren Speicherplatz wird nur zum Überschreiben freigegeben. Dazu wird lediglich die Information über den Speicherort der Datei überschrieben.[88] Um die Daten unbrauchbar zu machen, überschreibt man sie komplett mit einem Bitmuster. Danach lassen sich die Informationen nicht mehr rekonstruieren, aber möglicherweise der Löschvorgang erkennen.[89] Bei flüchtigen Speichern geschieht die Überschreibung, wenn über einen ausreichenden Zeitraum keine Betriebsspannung mehr zur Verfügung steht, automatisch.[90] Danach können nur noch die neu abgelegten Informationen gelesen werden. Wurden nur einzelne Bereiche überschrieben, kann zusätzlich noch die Anzahl der überschriebenen Daten festgestellt werden. Es besteht also nicht die Möglichkeit, die Veränderungen der Daten nachzuvollziehen, wenn nicht zusätzlich Daten über die Entwicklung der betrachteten Daten gespeichert werden. Ist ein Überschreiben nicht möglich, können Daten durch Zerstörung des Trägermediums unlesbar gemacht werden.[91] In der Regel wird, zum Auslesen und Darstellen der auf dem Trägermedium gespeicherten Information, Hardware benötigt. Beim Zugriff auf Speichermedien wie in § 110 Abs. 3 StPO vorgesehen, ist davon auszugehen, dass damit immer auch die Nutzung entsprechender technischer Mittel zum Auslesen und Anzeigen der Informationen gemeint ist.[92]

§ 110 StPO

[...]

(3) Die Durchsicht eines elektronischen Speichermediums bei dem von der Durchsuchung Betroffenen darf auch auf hiervon räumlich getrennte Speichermedien, soweit auf sie von dem Speichermedium aus zugegriffen werden kann, erstreckt werden, wenn andernfalls der Verlust der gesuchten Daten zu besorgen ist. Daten, die für die Untersuchung von Bedeutung sein können, dürfen gesichert werden; § 98 Abs. 2 gilt entsprechend.

[88] Tanenbaum, Moderne Betriebssysteme, 2003, S. 407 ff.

[89] Wright, Kleiman und Sundhar, Overwriting Hard Drive Data: The Great Wiping Controversy, ICISS 2008, 243, 243.

[90] Der Zeitraum bis zum Verlust der Daten kann dabei durch Temperaturreduktion verlängert werden. Haderman u.a., Lest We Remember: Cold Boot Attacks on Encryption Keys, USENIX SS 2008, 45, 45.

[91] Beim Zerstören eines Mediums könnten physikalische Spuren entstehen.

[92] Schlegel, Online-Durchsuchung light, HRRS 2008, 23, 28.

B. Digitale Daten als Beweismittel

Auf einem Speichermedium steht nur eine kontrollierbare, feste Anzahl an Speicherstellen zur Verfügung.[93] Dabei wächst die Anzahl der möglichen Zustände exponentiell mit der Fortentwicklung der Technik. Auf einer heute handelsüblichen 1 TB Festplatte lassen sich z.B. 2^{10}^^{12} verschiedene Zustände abspeichern. Oft sind dabei nicht einzelne Zustände, sondern eine Gruppierung von Zuständen von Interesse. Wenn das System eingegrenzt und kontrolliert werden kann, besteht die Möglichkeit, alle eventuell verursachten Spuren im Datenbestand zu erfassen und zu vernichten oder zu vermeiden.[94] Neben der Vermeidung und Zerstörung der Daten, könnten diese auch bewusst manipuliert werden, um einen, für den Anwender, günstigen Anschein zu erwecken. Das gilt ebenso für herkömmliche Beweismittel, beispielsweise können DNA Spuren, das Wissen über die Ausprägung der speziellen DNA vorausgesetzt, vollständig erzeugt werden.[95] Digitale Daten lassen sich dabei ohne zusätzliche Ausrüstung direkt am entsprechenden System erzeugen. Mit steigender Komplexität und Ausdehnung des Systems sind allerdings sehr detaillierte Fachkenntnisse oder technische Hilfsmittel notwendig.[96] Daneben können Daten fast beliebig verlustfrei kopiert werden, ohne dass die Ursprungsdaten verändert werden.

Für die Beweiskraft der Daten stellen sich allgemein zwei Aufgaben, die beantwortet werden müssen:[97]

1. **Zurechenbarkeit** der Daten: Quellendetektion (Wer hat die Daten erstellt oder Warum wurden sie erstellt)
2. **Integrität** der Daten: Manipulationsdetektion

I. Datenkategorien

Nach der Zurechenbarkeit, lassen sich sie Daten in drei Kategorien gliedern:

- **manuell erstellte Daten,** das sind alle Daten-Fallen, die "`direkt"' über eine Eingabe eines Anwenders erzeugt werden. Dazu gehören auch Daten, die auf explizite Anforderung eines Anwenders durch ein Programm erstellt werden. Dies können u.a. Übersetzungen, die ein Programm durchführt oder Ergebnisse von Berechnungen sein.
- von Programmen **automatisch erstellte Daten**, wie beispielsweise Protokolldateien, die z.B. den Zugriffe oder Fehler protokollieren, Grafiken, die für Effekte auf dem Display erzeugt werden oder Indexlisten für eine schnelle Suche.
- von **Sensoren** wie z.B. Kameras, Scanner, Temperaturfühler, Mikrofon, usw. **eingelesen Daten**.

[93] Carrier, A hypothesis-based approach to digital forensic investigations, 2006, S. 4.
[94] Böhme u.a., Multimedia-forensik als Teildisziplin der digitalen Forensik, 2009, http://www1.inf.tu-dresden.de/~rb21/publications/BFGK2009_MultimediaForensik_GI.pdf, (20.01.2010).
[95] Fumkin u.a., Authentication of forensic DNA samples, FSI 2009, 95, 95.
[96] Geschonneck, Onlinedurchsuchung: ich jetzt auch mal [update], 07.10.2007, http://computer-forensik.org/2007/10/07/onlinedurchsuchung-ich-jetzt-auch-mal, (20.01.2010).
[97] Böhme u.a., Multimedia-forensik als Teildisziplin der digitalen Forensik, 2009, http://www1.inf.tu-dresden.de/~rb21/publications/BFGK2009_MultimediaForensik_GI.pdf, (20.01.2010).

Außer den beständigen Daten können auch "`empfindliche"' Datentypen bei der Beweismittelgewinnung von Interesse sein. Neben der Auswertung dieser Daten, stellt sich hier die Aufgabe der Datensicherung und der Integritätsschutz. Grundsätzlich lassen sich diese Daten wie folgt einteilen:[98]

- **Flüchtige Daten,** gehen beim Herunterfahren oder einem Spannungsabfall verloren.
- **Fragile Daten** sind zwar dauerhaft gespeichert, verändern sich aber beim Zugriff.
- **Temporär zugreifbare Daten**, diese Daten stehen z.B. nur, während eine Anwendung aktiv ist, zur Verfügung.

Während fragile Daten über den Datenträger gesichert werden können, lassen sich flüchtige Daten nicht oder nur beschränkt[99] durch Beschlagnahme des Datenträgers sicherstellen und müssen zur Beweissicherung kopiert werden. Bei temporär zugreifbaren Daten kann es sein, dass die Daten an einem anderen Ort auf einem Datenträger abgelegt sind oder dass sie durch Ausführen einer Anwendung erneut erzeugt werden können, also rekonstruierbar sind.

II. Bewertung von Daten als Indizien

Zur Bewertung erfasster Daten, müssen die Daten auf ihre Beweiskraft hin untersucht werden. Die Tatsachenvermutungen werden dabei als Hypothesen formuliert und die einzelnen Daten in drei Gruppen eingeteilt.[100]

- Daten, die für eine Hypothese sprechen (abstrakte Beweiskraft > 1)
- Daten, die gegen eine Hypothese sprechen (abstrakte Beweiskraft < 1)
- Daten, die sich auf die Hypothese nicht auswirken (abstrakte Beweiskraft = 1)

Abhängige Daten können dabei als Indizienfamilie betrachtet und entsprechend gemeinsam bewertet werden. Hierbei kann durch die Abhängigkeit der Daten untereinander eine erhöhte Beweiskraft entstehen. Wurde beispielsweise eine Logdatei eines Kommunikationsprogramms manuell als einzige Logdatei entfernt, liegt die Belastungswahrscheinlichkeit in dem Nichtvorhandensein der Datei ungleich höher, als wenn der Anwender regelmäßig alle Logdateien löscht.[101]

Aus den vorangegangenen Überlegungen zur Beweiskraft von Indizien ergibt sich, dass bei Vorliegen neuer Erkenntnisse über die Ausgangswahrscheinlichkeit eine Neuzuordnung der Daten nötig werden kann. Auch hier finden sich Beispiele, bei denen der Trugschluss des Anklägers vorliegt. So bewertet die Generalbundesanwaltschaft die Verschlüsselung der Kommunikation mit ausreichend hohem Beweiswert, um damit einen hinreichenden Verdacht

[98] Geschonneck, Computer Forensik, 2008, S. 78.
[99] Beispielsweise durch starke Kühlung von normalerweise flüchtigen Speicherbausteinen. Haderman u.a., Lest We Remember: Cold Boot Attacks on Encryption Keys, USENIX SS 2008, 45, 45.
[100] Geschonneck, Computer Forensik, 2008, S. 79.
[101] Akte

zu begründen. Der BGH korrigierte diese Einschätzung in seinem Urteil vom 18. Oktober 2007.[102]

Teil 4: Datenträgeruntersuchung

Bei der Auswertung von Datenträgern kommen zu den allgemeinen Anforderungen an ein Sachverständigengutachten die beiden für die Beweiskraft der Daten zu beantwortenden Fragestellungen. Daraus ergeben sich folgende Anforderungen an die informationstechnologische Expertise:[103]

- Die angewandten Methoden müssen in der Fachwelt allgemein akzeptiert sein.
- Die Funktion der eingesetzten Werkzeuge und Methoden muss nachweisbar sein.
- Alle Methoden und Schritte müssen bei wiederholten Anwendungen zum gleichen Ergebnis kommen.
- Ermittlungsergebnisse dürfen nicht unbemerkt verändert werden.
- Es müssen logisch nachvollziehbare Verbindungen zwischen Personen, Ereignissen und Beweisspuren hergestellt werden.
- Es muss eine angemessene Dokumentation erstellt werden.

Das konkrete Vorgehen ist dabei vom Einzelfall abhängig und unterscheidet sich nach dem zu untersuchenden Sachverhalt. Dabei ist es unerheblich, ob ein "`Werkzeug'", also beispielsweise ein Computer, mit dem eine Straftat begangen wurde oder ein "`Tatort'", z.B. ein Computer auf dem Daten manipuliert wurden, untersucht wird. In beiden Fällen kann jeweils auch der andere Fall vorliegen oder es kann versucht werden den jeweiligen anderen Anschein zu erwecken.[104]

A. Analyse von Informationssystemen

Die ersten Schritte bei der Datenträgeruntersuchung sind abhängig, ob das System im eingeschalteten Zustand vorgefunden oder ob es ausgeschaltet ist. Ist das System eingeschaltet, können und sollten flüchtige Daten gesichert werden.[105] Dabei können durch Sicherung der Daten im Hauptspeicher gegebenenfalls vorhandene Schlüssel zum Entschlüsseln von verschlüsselten Daten gewonnen werden. Stehen diese Schlüssel nicht zur Verfügung und

[102] BGH, Urt. v. 18.10.2007, Az. 5 StB 34/07, Rn.: 7 Homepage: http://www.bundesgerichtshof.de (01.02.2010).
[103] Geschonneck, Computer Forensik, 2008, S. 62 f.
[104] Gegen einen US-Angestellten wurde Anklage wegen Abruf von Kinderpornografieseiten über seinen Arbeitslaptop erhoben. Ein Gutachter fand Viren auf dem Laptop, die darauf programmiert waren 40 entsprechende Webseiten pro Minute aufzurufen. Die Anklage wurde nach 11 Monaten und Ausgaben für die Verteidigung in Höhe von 250.000 Dollar, fallen gelassen. cis, Virenattacke mit Kinderpornos, SPON, 10.11.2009, http://www.spiegel.de/netzwelt/web/0,1518,660199,00.html, (01.06.2010).
[105] Geschonneck, Computer Forensik, 2008, S. 85.

können auch nicht, z.B. durch Kooperation des Eigentümers, beschafft werden, ist es in der Regel nicht möglich auf verschlüsselte Daten zuzugreifen.[106]

I. Analysen an aktiven Systemen

In Abhängigkeit des Untersuchungsziels, sind neben dem Hauptspeicher weitere flüchtige Daten für die spätere Auswertung zu sichern. Bei den zu sichernden Daten kann es sich z.B. um folgende Daten handeln:[107]

- Systemdatum
- Abweichung der Systemuhrzeit zu einer Referenzzeit
- Liste aktiver Prozesse[108]
- Liste geöffneter Sockets[109]
- Liste aller Anwendungen, die an Sockets lauschen
- Liste aller gerade angemeldeter Anwender
- Liste von Netzwerkverbindungen
- [...]

Erfolgt die Sicherung nicht auf Hardwareebene[110] kommt es bei der Sicherung der flüchtigen Daten in der Regel zu Veränderungen am System.[111] Auch wenn es nur zu minimalen[112] Veränderungen kommt, kann danach der Ursprungszustand nicht mehr sicher hergestellt werden. Somit entsteht eine zusätzliche Datenmanipulationsmöglichkeit, die bei weiteren Ermittlungen zu berücksichtigen ist. Um die Datenveränderungen zuordnen zu können, ist es besonders wichtig, die aktuelle Systemzeit und alle am System durchgeführten Handlungen zu dokumentieren. Nur so kann später festgestellt werden, welche der Änderungen an fragilen Daten der Ermittlungstätigkeit zugeordnet werden müssen.[113] Fehlt diese Dokumentation, kann später kein Dritter mehr die einzelnen Erhebungsschritte nachvollziehen und bewerten.[114] Neben den flüchtigen Daten werden auch noch nur temporär zugreifbare Daten ge-

[106] o.A., FBI beißt sich an verschlüsselten Festplatten die Zähne aus, derStandard.at, 27.06.2010, http://derstandard.at/1277336831638/FBI-beisst-sich-an-verschluesselten-Festplatten-die-Zaehne-aus, (27.06.2010).
[107] Geschonneck, Computer Forensik, 2008, S. 85.
[108] Prozesse sind aktiv ablaufende Programme, ein Prozess kann exklusiv die Hardware eines Systems nutzen.
[109] Socket sind Softwareteile über die Computerprogramme sich mit einem Netzwerk verbinden. Über das Netzwerk können mittels Sockets Daten mit anderen Programmen ausgetauscht werden. Dabei können normalerweise Daten gesendet und empfangen werden.
[110] Carrier, A hypothesis-based approach to digital forensic investigations, 2006, S. 51.
[111] Murr, Forensically Sound Duplicate, 02.08.2006, http://www.forensicblog.org/2006/08/02/forensically-sound-duplicate, (01.07.2010).
[112] Libster und Kornblum, A proposal for an integrated memory acquisition mechanism, SIGOPS 2008, 14, 14.
[113] Geschonneck, Computer Forensik, 2008, S. 86.
[114] Akte

sucht, die beispielsweise auf einem anderen physikalischen Computer über eine Netzwerkverbindung gespeichert wurden.[115]

Die Problematik des sich verändernden System bei der Sicherung flüchtiger Daten und die Implikationen auf den Wert der danach angefertigten forensische Kopie, hat zu einer Diskussion geführt, wie eine forensische Kopie zu definieren ist.[116]

Die erzielten Ergebnisse bei dieser Untersuchung können nicht reproduziert werden, somit entfällt die für den Sachverständigen nötige Austauschbarkeit.[117] Formell reicht allerdings die Beauftragung des Sachverständigen durch ein Gericht, einer Staatsanwaltschaft oder der Polizei aus, um den sachverständigen Zeugen von einem Sachverständigen abzugrenzen.[118] Eine vollständige Abgrenzung ist in diesem Falle nicht eindeutig möglich.

Bei einem solchen Fall werden höhere Anforderungen an die Dokumentation der Ermittlungsschritte und des vorgefundenen Umfelds gestellt, weil nur über die Dokumentation und die Erinnerung des Sachverständigen die Ergebnisse geprüft werden können. Da sich kaum ein Sachverständiger über einen längeren Zeitraum an die einzelnen eingegebenen Steuerbefehle und Zustände des vorgefundenen Computersystems erinnern wird, wird in der Regel die Dokumentation als Einziges zuverlässig über die Ermittlungsschritte Auskunft geben können und so dazu beitragen, Erinnerungsfehler zu vermeiden. Aus der Dokumentation sollte ein sachverständiger Dritter jederzeit die Schritte nachvollziehen und diese bewerten können.[119]

II. Analysen an ausgeschalteten Systemen

Nach dem Sichern der flüchtigen und temporär zugreifbaren Daten ist es für weitere Untersuchungen notwendig, eine Kopie des zu untersuchenden Datenträgers anzufertigen. Dabei wird der Datenträger an ein Analysesystem angeschlossen und bitweise auf einen sauberen Datenträger kopiert. Hierbei ist der untersuchte Datenträger durch sogenannte Writeblocker physikalisch vor Schreibzugriffen zu sichern.[120] Ab diesem Zeitpunkt erfolgen alle Untersuchungen an der Kopie des Datenträgers. Die Identität der Kopie mit dem Original wird durch die Verwendung einer Prüfsumme[121] über den kompletten Datenträger sichergestellt.[122] Der

[115] Geschonneck, Computer Forensik, 2008, S. 86.
[116] o.A.,Forensically Sound, Yahoo Groups, 09.08.2006, http://tech.groups.yahoo.com/group/forensically_sound/, (01.07.2010).
[117] Da eine Wiederholung der einzelnen Schritte nicht mehr automatisch zum gleichen Ergebnis führt.
[118] OVG NRW, Beschluss. v. 18.07.2007, Az. 8 A 1075/06.A, Rn.: 23 Homepage: http://www.justiz.nrw.de (05.06.2010).
[119] Geschonneck, Computer Forensik, 2008, S. 80 ff.
[120] Eisenberg fordert mindestens zwei Kopien des Datenträgers, Beweisrecht der StPO, 2008, Rn. 1939a.
[121] Dazu werden kryptologischen Hashfunktionen verwendet, die eine Datenbestand beliebiger Größe auf eine Zeichenfolge mit fester Länge, dem sogenannten Hashwert abbildet. Eine solche Hashfunktion ist kollisionsresistenz wenn es praktisch unmöglich ist, zwei Datensätze mit gleichem Hashwert zu finden. Zur Beweissicherung sollte eine kollisionsresistente Hashfunktion eingesetzte werden. Buchmann, Einführung in die Kryptographie, 2008, S. 189 ff.
[122] Geschonneck, Computer Forensik, 2008, S. 87 ff.

Originaldatenträger ist nach der Kopie gegen Nutzung zu sichern und sicher zu verwahren.[123]

Auf Datenträgerkopien können nun Beweisspuren gesucht werden, die dann in einen kausalen und zeitlichen Zusammenhang zu bringen sind. Um die Daten gegen Manipulation zu schützen, sollten die gefundenen Daten mit entsprechenden Prüfsummen gespeichert werden, um gegebenenfalls Manipulationen zu erkennen oder die Unverfälschtheit nachzuweisen. In Abbildung 4 wird eine ermittelte Indizienfamilie dargestellt. Es handelt sich dabei nicht um eine Beweiskette oder einen Beweisring, weil die Einzelindizien nicht unabhängig voneinander sind. Die komplette Indizienfamilie muss also als Ganzes bewertet werden und es kann nicht die Produktregel oder das Produkt der Beweiskraft herangezogen werden.[124]

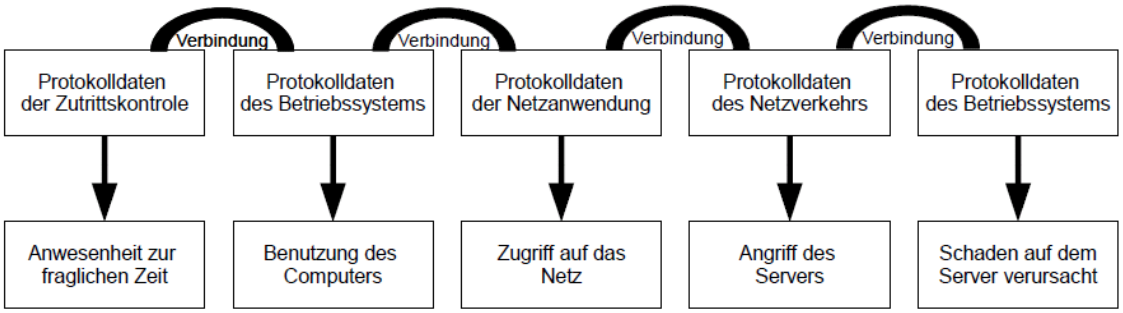

Abbildung 4: Abhängigkeiten zwischen den einzelnen Indizien[125]

Innerhalb der Indizienfamilie bilden die abhängigen Indizien eine Kette. Fehlt eines der Indizien innerhalb der Kette, kann sich dies auf die Tatsache auswirken, auf die die Indizien hinweisen. Entfällt das Indiz am Beginn der Kette, ändert sich in diesem Fall nur die Anfangswahrscheinlichkeit und damit nicht der Sachverhalt sondern der Beweiswert. Anstelle der anwesenden Anwender, erhöht sich der Kreis der potentiellen Nutzer auf alle die theoretisch die Möglichkeit hatten, zum entsprechenden Zeitpunkt physischen Zugriff auf das System zu haben. In Abhängigkeit der Anzahl, der nun in Betracht kommenden Personen, reduziert sich der Beweiswert dadurch, wie im Teil 2, C, I dargestellt, deutlich.

Für die einzelnen Indizien der Indizienfamilie müssen jeweils Hilfstatsachen untersucht werden, um deren Authentizität zu untersuchen.

[123] Dass sowohl Original als auch Kopie verloren gehen können, zeigt die Staatsanwaltschaft in Augsburg. Dort gingen nach Informationen des Spiegels neben der Festplatte auch ein Datensicherungsband des Computers von Max Strauß verloren. o.A., Auch Datenkopie von Strauß-Computer weg, sueddeutsche.de, 20.05.2001, http://www.sueddeutsche.de/politik/justizaffaere-auch-datenkopie-von-strauss-computer-weg-1.315208, (27.10.2010).
[124] Geschonneck, Computer Forensik, 2008, S. 93 ff.
[125] Geschonneck, Computer Forensik, 2008, S. 94.

B. Angewandte Methoden

Das Vorgehen bei der Untersuchung der Datenträger kann sich direkt auf die Belastungswahrscheinlichkeit auswirken. Die Güte einer Methode kann anhand folgender Fragen abgeschätzt werden:[126]

- Wurde das Vorgehensmodell publiziert oder ist es bekannt?
- Wird das Vorgehensmodell unter Experten anerkannt?
- Kann das Vorgehensmodell getestet werden?
- Wie hoch ist die Fehlerrate des Vorgehensmodells?

Auch hier ist für die Bestimmung der Belastungswahrscheinlichkeit neben der Fehlerrate die Kenntnis über die Anfangswahrscheinlichkeit Voraussetzung.

Die Anforderungen, nur allgemein akzeptierte Methoden einzusetzen, schließt die verwendeten Werkzeuge ein, die bei Untersuchungen von Datenträgern oft eingesetzt werden müssen, um z.B. identische Kopien mit vertretbarem Aufwand anzufertigen oder größere Datenmengen in annehmbarer Zeit auszuwerten.[127] Dabei darf es bei keinem der eingesetzten Werkzeuge Zweifel bezüglich der Zuverlässigkeit und der Integrität geben. Dazu kann es nötig sein, Erkenntnisse mit alternativen Werkzeugen zu prüfen.[128] Open-Source Werkzeuge bieten zusätzlich die Möglichkeit, im Bedarfsfall die Funktionsweise des eingesetzten Werkzeugs am Quellcode nachzuvollziehen und so durch Dritte überprüfen zu lassen.[129]

Bei den verwendeten Werkzeugen bedeutet eine weitere Verbreitung und damit größere Erfahrung, keine Verbesserung der Beweisaussage. Im Falle eines gezielten Einbruchs in ein System, können Angreifer gezielt Spuren kontrollieren und vermeiden, so dass die bekannten Werkzeuge keine Auffälligkeiten entdecken können. Dazu genügt es, anhand der Funktionsweise eines Werkzeugs, ein entsprechendes Gegenwerkzeug zu programmieren.[130] Hierbei muss eine Abwägung zwischen der Erfahrung beim Werkzeugeinsatz und damit der Genauigkeit in der Bewertung der gefundenen Spuren und einer kreativen Ermittlung erfolgen.

---

[126] Carrier, A hypothesis-based approach to digital forensic investigations, 2006, S. 2.

[127] Bei der bundesweiten Operation Himmel wurden 2007 Datenträger in solchem Umfang beschlagnahmt, dass die Auswertungskapazität der Polizei überschritten und externe Stellen mit der Auswertung beauftragt werden mussten. Lill, Digitale Autopsie, SPON, 08.02.2008, http://www.spiegel.de/netzwelt/web/0,1518,533078,00.html, (04.06.2010).

[128] Geschonneck, Computer Forensik, 2008, S. 136 f.

[129] Morgenstern, Digitale Autopsie, heise security, 05.04.2004, http://www.heise.de/security/artikel/Computer-Forensik-mit-Open-Source-Tools-270468.html, (04.06.2010).

[130] Geschonneck, Computer Forensik, 2008, S. 97 ff.

C. Kritische Würdigung und Ausblick

Bei der informationstechnologischen Expertise wird deutlich, dass hier kein klassischer Sachverständigenbeweis vorliegt. Der Sachverständige verlässt hier gegebenenfalls die Rolle als Gehilfe des Gerichts, der dem Gericht fehlendes Fachwissen, z.B. über die Merkmalswahrscheinlichkeit, zur Verfügung stellte und nimmt (zusätzlich)[131] die vollständigen Aufgaben eines Ermittlers war. Es kommt also nicht nur zu einer teilweisen Abtretung der Beweiswürdigung, wie es beim klassischen Sachverständigenbeweis bereits kritisiert wurde,[132] sondern die Beweiswürdigung wird in noch stärkerem Maße dem Ermittler überlassen. Im Gegensatz zur Begutachtung einzelner Fragestellungen, wie z.B. bei einer aussagepsychologischen Begutachtung, in der nur Angaben zu einem bestimmten Geschehen beurteilt werden[133] oder bei der DNA-Analyse, bei der nur der Verursacher der DNA-Probe identifiziert wird,[134] werden in der Computer Forensik, wie beispielhaft in Abbildung 4 dargestellt, mitunter keine einzelnen Hilfstatsachen, sondern direkte, rechtserhebliche Tatsachen untersucht. Steht zu dem entsprechenden Sachverhalt keine repräsentative Datenbasis zur Verfügung und lassen sich so keine wissenschaftlich verlässliche Informationen über Anfangswahrscheinlichkeiten treffen, müssen zur Würdigung, zumindest intuitiv, Wahrscheinlichkeiten angenommen werden. Wie mit dem Theorem von Bayes gezeigt, kann die Anfangswahrscheinlichkeitsannahme sich signifikant auf den Beweiswert auswirken und so erheblich zur persönlichen Überzeugung beitragen. Daraus ergibt sich die Notwendigkeit, dass die Abschätzung, wie im Teil II. F. II angeregt, vom Gericht durchgeführt wird oder zumindest die Annahmen des Sachverständigen vollständig nachvollzogen und geteilt werden. Dem entgegen steht, dass die Auswertung virtueller Vorgänge oft als intransparent und besonders komplex angesehen wird,[135] und es sehr unterschiedliche Anwendungserfahrungen mit modernen Kommunikationstechnologien gibt.[136] Daraus könnten sich stark schwankende Einschätzungen ergeben.

Wurden vom Sachverständigen fragile Daten ausgewertet und entfällt damit die Möglichkeit die Ermittlungen von einem dritten Sachverständigen in Erwartung des gleichen Ergebnisses wiederholen zu lassen, kommt es zu einer Art Doppelrolle des Sachverständigen. Diese

---

[131] Akte

[132] Erb, Die Abhängigkeit des Richters vom Sachverständigen, ZStW 2009, 882, 882.

[133] BGH, Urt. v. 30.06.1999, Az. StB 618/98, Rz. 11 Homepage: http://www.hrr-strafrecht.de (01.06.2010).

[134] BGH, Beschl. v. 21.01.2009, Az. 1 StR 722/08, Rz.: 2 Homepage: http://www.bundesgerichtshof.de (29.06.2010).

[135] So schreibt Eichberg beispielsweise von "besonderen Softwareprogrammen" die zum Herstellen einer Kopie des Datenträgers Verwendung finden. Eine solche Kopie lässt sich dabei unter anderem mit dem Unix-Befehl "dd" direkt durchführen. Auch kommerzielle Softwareprogramme, die diese Aufgabe leisten, sind im Handel frei erhältlich und damit ist keine Besonderheit an diesen Programmen feststellbar, auch weil der Nachweis der Identität über einen Hashwert nach dem Kopiervorgang erbracht wird. Eisenberg, Beweisrecht der StPO, 2008, Rn. 1939c.

[136] Ein Bochumer Richter sieht im Ausdrucken eines Handelsregistereintrags eine unzumutbare Hilfstätigkeit, die ihn in seiner Unabhängigkeit beeinträchtigt, auch wegen des Haftungsrisikos, das nicht von ihm selbst durchzuführen ist. OLG Hamm, Beschl. v. 20.10.2009, Az. 1 DGH 2/08, kommentiert von Reinelt, Elektronischer Rechtsverkehr – Die Justiz im Elfenbeinturm, LTO 2006, http://www.lto.de/de/html/nachrichten/508/Die-Justiz-im-Elfenbeinturm-neu/, (10.07.2010).

Vermischung scheint den Anforderungen an einen Strengbeweis, der zwischen Sachverständigen und Zeugen unterscheidet, nicht gerecht zu werden. Eine Trennung von Ermittlungstätigkeiten und Hilfsfunktionen sind für das Gericht erstrebenswert. Es ist auch nicht ersichtlich, warum ein Sachverständiger, der als "`privater'" Ermittler fungiert, bei der Beweiserbringung anders behandelt werden sollte als "`staatliche'" Ermittler, die in einem Strafverfahren als Zeugen auftreten.[137] Im deutschsprachigen Standardwerk zur Computerforensik wird die Problematik der Beweisart ausgeklammert, indem übergeordnet vom Personalbeweis gesprochen wird.[138]

Durch die wachsende Bedeutung des Internets, hat sich die Computernutzung zu einer entschädigungsfähigen Vermögensposition entwickelt.[139] Da die Möglichkeit besteht, Daten verlustfrei zu kopieren und deren Identität zu verifizieren, ist eine Beschlagnahme eines Datenträgers für längere Zeit nicht notwendig. Dazu sind robuste Prozesse zu verankern, die die Verwendung einer Datenträgerkopie, anstelle eines Originals, ohne Beweiswertverlust sicher stellt.

Teil 5: Offener Zugriff auf Informationssysteme

Offene Quellen wie Zeitschriften, Webportale und Informationsdienste für jedermann können schrankenlos für die Strafverfolgung genutzt werden.[140]

BVerfG:
<308> aa) Eine Kenntnisnahme öffentlich zugänglicher Informationen ist dem Staat grundsätzlich nicht verwehrt. Dies gilt auch dann, wenn auf diese Weise im Einzelfall personenbezogene Informationen erhoben werden können [...]. Daher liegt kein Eingriff in das allgemeine Persönlichkeitsrecht vor, wenn eine staatliche Stelle im Internet verfügbare Kommunikationsinhalte erhebt, die sich an jedermann oder zumindest an einen nicht weiter abgegrenzten Personenkreis richten. So liegt es etwa, wenn die Behörde eine allgemein zugängliche Webseite im World Wide Web aufruft, eine jedem Interessierten offen stehende Mailingliste abonniert oder einen offenen Chat beobachtet.

International Beachtung[141] fanden 2007 Ermittlungen der Bundesanwaltschaft gegen eine vermeidlich terroristische Vereinigung.[142] Dabei entstand nach Berichten der Tageszeitungen

[137] Bender, Nack und Treuer, Tatsachenfeststellung vor Gericht, 2007, Rn. 1278.
[138] Geschonneck, Computer Forensik, 2008, S. 306.
[139] LG Stuttgart, Urt. v. 15.05.2009, Az. 15 O 306/08, Rz. 18 Homepage: http://www.justizportal-bw.de (05.06.2010) und OLG München, Beschl. v. 23.03.2010, Az. 1 W 2689/09, Rz. 8 Homepage: http://www.juris.de (10.07.2010) dagegen hält unter anderem das Landessozialgericht (LSG) NRW einen PC nicht für die Grundversorgung mit Informationen erforderlich, wenn Informationen über ein Radioempfangsgerät oder einen Fernseher abgerufen werden können. LSG NRW, Besch. v. 23.04.2010, Az. L 6 AS 297/10 B, Rz. 7 Homepage: http://www.justiz.nrw.de (01.07.2010).
[140] BVerfG, Urt. v. 27.02.2008, Az. 1 BvR 370/07, 1 BvR 595/07, Rz. 308 Homepage: http://www.bundesverfassungsgericht.de (01.06.2010).
[141] Sennett und Sassen, Guantánamo in Germany, the Guardian, 21.08.2008, http://www.guardian.co.uk/education/2007/aug/21/highereducation.ukl, (15.06.2010).
[142] Kuri, Durch google-Suche in die Einzelhaft [Update], heise news, 22.08.2007, http://www.heise.de/newsticker/meldung/Durch-Google-Suche-in-die-Einzelhaft-Update-165722.html, (20.01.2010).

ein Anfangsverdacht durch die Suche mit der Suchmaschine Google nach Schlüsselwörtern aus den Bekennerschreiben. Anhand stilistischer und textgestalterischer Vergleiche der gefundenen Texte mit bekannten Texten der Vereinigung wurde vom Generalbundesanwalt ein begründeter Tatverdacht angenommen.[143] Der BGH konnte dieser Einschätzung nicht folgen und bewertete die Indizien der Übereinstimmung in thematischer, stilistischer und textgestalterischer Hinsicht mit einem allenfalls äußerst geringen Beweiswert.[144]

BGH:
<33> Der Ansicht des Generalbundesanwalts, der Verdacht für das Bestehen einer Vereinigung ergebe sich aus den bei den Analysen der Bekennerschreiben vorgefundenen Übereinstimmungen in thematischer (Themen wie Globalisierung, Gentechnik, Imperialismus u.a.), stilistischer (Begriffe wie Intervention, "rund um den Globus", Prekariat, Euromayday u.a.) und textgestalterischer (Textgliederung durch Leerzeichen, willkürliche Ein- und Ausrückungen, uneinheitliche Verwendung von Abkürzungen, Ausschreibung von Zahlwörtern, Rechtschreibunsicherheiten in Bezug auf "ß" und "ss" u.a.) Hinsicht, der schlüssigen Auswahl der Anschlagsziele sowie der zeitlichen Abfolge der Taten, vermag der Senat nicht zu folgen. Es handelt sich insoweit um Indizien mit einem allenfalls äußerst geringen Beweiswert.

A. XPider

Seit 2003[145] werden, in einem 2002 gestarteten Projekt, durch das Programm XPider vom Finanzamt automatisiert Webseiten nach Steuervergehen durchsucht. Dafür wurden 2007 bis 2008 täglich 100.000 Seiten auf steuerlich relevante unternehmerische Aktivitäten geprüft.[146] Die maximale Kapazität soll dabei 2008 bei 2,5 Millionen Internetseiten pro Tag gelegen haben. Die identifizierten Daten werden regelmäßig über das Programm STINA an die zuständigen Landesfinanzbehörden weitergeleitet.[147]

Der XPider setzt sich aus mehreren Komponenten zusammen und verfügt zur Steuerung und Administration über ein Graphical Unser Interface (GUI). Daneben existieren zwei getrennte Programmeinheiten für die Suche nach Seiten im World Wide Web (WWW) und für die Auswertungen der gefundenen Seiten.[148]

[143] Rada, Kommissar Google jagt Terroristen, taz.de, 22.08.2007, http://www.taz.de/?id=start&art=3471&id=detuschland-artikel&cHash=5218eee73a, (16.06.2010).
[144] BGH, Beschl. v. 20.12.2007, Az. StB 12, 13 und 47/07, Rz. 33 Homepage: http://www.bundesgerichtshof.de (01.06.2010).
[145] In den Niederlanden wurde ein ähnliches Projekt bereits Ende der 90er Jahre begonnen und später zusammen mit Großbritannien weiterentwickelt. o.A., Compliance Risk Management: Progress with the Development of Internet Search Tools for Tax Administration, OECD, 01.10.2004, http://www.oecd.org/dataoecd/44/15/33818593.pdf, S. 1, (15.06.2010).
[146] o.A., Auf den Spuren von Internet-Verkäufern, Drucksache 16/7782, 06.02.2008, http://dipbt.bundestag.de/dip21/btd/16/079/1607978.pdf (01.06.2010),
[147] Lübke in Lübke/Müller/Bonenberger, Ermittlungsmöglichkeiten der Steuerfahndung, 2008, S. 132.
[148] Nowitzky, Xpider (eXtended sPIDER) Internet Steuersündern auf der Spur, 07.2003, http://www.minet.uni-jena.de/dbis/veranstaltungen/datenbanktage-2003/DBTage2003-Nowitzky.pdf, S. 3, (01.06.2010).

B. Seitensuche

Der Webcrawler XPider durchsucht das (WWW) und bereitet die gefundenen Seiten für die Auswertung auf. Prinzipiell werden dabei, ausgehend von einer Startseite, immer folgende Schritte wiederholt:[149]

1. Laden einer Uniform Resource Locater (URL), entweder der über die Benutzeroberfläche übergebenen Startseite oder eine der bereits ermittelten und gespeicherten Adressen.
2. Herunterladen der Webseite, die über die URL adressiert wird.
3. Extrahieren aller Links aus der gefundenen Seite und speichern die noch unbekannten Links.
4. Entfernen aller Tags[150] von der Webseite und speichern die Seite für die Analyse.
5. Initialisieren der Auswertung der soeben gespeicherten Seite.

C. Seitenauswertung

Die Auswertung erfolgt ebenfalls in mehreren Schritten und kann synchron an mehreren gefundenen Seiten durchgeführt werden.[151]

1. Laden der gespeicherten Seite
2. Überprüfung der Suchbegriffe
3. Kategorisierung der Seite
4. Extrahierung weiterer Informationen (z.B. Sprache, Adressen, Steuer-Nummer, Telefonnummern, usw.)
5. Übermittlung der Ergebnisse

Die übermittelten Daten werden über das GUI aufbereitet und gleichzeitig für spätere Abrufe archiviert.

Für die Dokumentenkategorisierung werden dabei in einem hybriden Ansatz Techniken aus dem maschinellen Lernen und ein regelbasierter Ansatz kombiniert.[152]

---

[149] Nowitzky, Xpider (eXtended sPIDER) Internet Steuersündern auf der Spur, 07.2003, http://www.minet.uni-jena.de/dbis/veranstaltungen/datenbanktage-2003/DBTage2003-Nowitzky.pdf, S. 11, (01.06.2010).

[150] Über Tags werden Daten mit zusätzlichen Informationen versehen. Bei Webseiten werden über Tags u.a. Textformatierungen durchgeführt.

[151] Nowitzky, Xpider (eXtended sPIDER) Internet Steuersündern auf der Spur, 07.2003, http://www.minet.uni-jena.de/dbis/veranstaltungen/datenbanktage-2003/DBTage2003-Nowitzky.pdf, S. 11, (01.06.2010).

[152] Nowitzky, Xpider (eXtended sPIDER) Internet Steuersündern auf der Spur, 07.2003, http://www.minet.uni-jena.de/dbis/veranstaltungen/datenbanktage-2003/DBTage2003-Nowitzky.pdf, S. 13, (01.06.2010).

Allgemein versucht hierbei die Software, anhand von einigen manuell klassifizierten Datensätzen, Klassifikationskriterien für die automatische Klassifikation zu ermitteln.[153]

Als Attribute der Webseiten werden dabei im Allgemeinen deren Worte verwendet. Um die Anzahl an Merkmalen in Grenzen zu halten, werden häufig vorkommende und zur Klassifikation ungeeignete Worte (z.B. Artikel und Präposition) nicht verwendet.[154] Bei allen eingesetzten Methoden zur Klassifikation handelt es sich um Textvergleiche. Der Beweiswert ist also äußerst gering.[155]

I. Regelbasierte Auswertung

Ein Regellerner versucht in den Beispieldaten Regeln für die Klassifikation zu ermitteln. Dazu werden beispielsweise alle möglichen Regeln miteinander verglichen und immer die besten Regeln übernommen, um dann, unter Voraussetzung der bereits bekannten Regeln, neue Regeln zu ermitteln. Die Stärken und Schwächen der gelernten Regeln können dabei über die Bewertung der Regeln beeinflusst werden.[156] Die gefundenen Regeln können von einem Experten begutachtet, bewertet und gegebenenfalls verändert werden. So ist es möglich, Ungenauigkeiten in den Trainingsdaten zu erkennen und auszubessern.

Eine denkbare zweiteilige Regel wäre z.B.: "Richtige Umsatzsteuer-Identifikationsnummer (USt-IdNr.)“ auf der untersuchten Seite vorhanden?".

Die Regeln lassen sich sehr effektiv auf gefundene Seiten anwenden, da nur die, für die Regeln notwendigen Informationen, ausgewertet werden. Gleichzeitig sind die Regeln meistens unflexibel und lassen sich nicht beliebig auf alle Webseiten anwenden. Sie lassen sich nicht uneingeschränkt, beispielsweise von einer Handelsplattform auf eine andere, übertragen.[157]

II. Naive Bayes Klassifikation

Bei der Naive Bayes Klassifikation wird das bereits im Teil I, C, I vorgestellte Theorem von Bayes zur Klassifikation herangezogen. Es wird jeder Datensatz der Klasse zugeordnet, der er am wahrscheinlichsten angehört. Dabei wird "`naiv"' angenommen, dass die einzelnen Merkmale (also die Wörter im analysierten Text) voneinander unabhängig wären. Aus den einzelnen Merkmalen w_i und jeder Klasse k_j der Trainingsdaten werden die bedingten Wahrscheinlichkeiten $P(w_i|k_j)$, also die Wahrscheinlichkeit, dass das Wort w_i in einem Datensatz aus der Klasse k_j vorkommt, bestimmt. Aus diesen Daten kann dann für die zu klassifizierenden Datensätze D mit n Merkmalen die Wahrscheinlichkeit für die einzelnen Klassen berechnet werden. Ausgewählt wird dabei die Klasse mit der höchsten Wahrscheinlichkeit. Für Merkmale die nur in zu klassifizierenden Datensätzen vorkommen, kann keine Wahrscheinlichkeitsberechnung vorgenommen werden. Damit die Berechnung der Klassenwahrschein-

[153] Chakrabarti, Mining the Web: Discovering Knowledge form Hypertext Data, 2003, S. 81 ff.
[154] Chakrabarti, Mining the Web: Discovering Knowledge form Hypertext Data, 2003, S. 48 f.
[155] BGH, Beschl. v. 20.12.2007, Az. StB 12, 13 und 47/07, Rz. 33 Homepage: http://www.bundesgerichtshof.de, (01.06.2010).
[156] Chakrabarti, Mining the Web: Discovering Knowledge form Hypertext Data, 2003, S. 71 ff.
[157] Nowitzky, Xpider (eXtended sPIDER) Internet Steuersündern auf der Spur, 07.2003, http://www.minet.uni-jena.de/dbis/veranstaltungen/datenbanktage-2003/DBTage2003-Nowitzky.pdf, S. 13, (01.06.2010).

lichkeit dennoch möglich ist, kann für jedes Wort eine "`Grundwahrscheinlichkeit"' angenommen werden.[158]

$$P(D|k_j) = P(k_j) \prod_{i=1}^{n} P(w_i|k_j)$$

Werden nur zwei Klassen unterschieden, kann die Einteilung über die Bildung des Quotienten erfolgen. Die Klasseneinteilung erfolgt dann analog zur Entscheidung, ob es sich um ein belastendes oder entlastendes Indiz handelt, wie im Teil 2, C, II ausgeführt.

$$\frac{P(D|k_1)}{P(D|k_2} = \frac{P(D|k_1)}{P(D|\overline{k_2})}$$

Die abstrakte Beweiskraft unterscheidet sich in zwei Punkten mit dem hier gebildeten Quotienten:

1. Die verwendeten Merkmale verfügen nicht über die geforderte Unabhängigkeit.
2. Die Anfangswahrscheinlichkeit bezieht sich nur auf das Auftreten eines Merkmals innerhalb der Trainingsdaten.

III. k-NN

Beim k-NN Algorithmus erfolgt die Klassifikation über eine Distanzfunktion. Für den unklassifizierenden Datensatz wird die Distanz zu allen Trainingsdaten berechnet. Die k naheliegendsten Trainingsdaten bestimmen dann über eine Abstimmungsfunktion der Klasse des zu klassifizierenden Datensatzes.[159]

IV. SVM

Bei der SVM werden die Trainingsdokumente anhand ihrer Merkmale in einem ein- oder mehrdimensionalen Raum platziert und anschließend eine Hyperebene zwischen die einzeln Klassen gelegt. Dazu wird versucht eine Ebene zu finden, welche die Klassen trennt und gleichzeitig einen größtmöglichen Abstand zu den Trainingsdokumenten aufweist, also möglichst im „Niemandsland“ zwischen den Klassen verläuft. Die Klassifizierung erfolgt dann durch Bestimmung der Position im Raum bezogen auf die Trennebene. Wenn es nicht möglich ist, die Klassen mit Hilfe einer Hyperebene fehlerfrei zu trennen, werden die Positionen der Trainingsdokumente im Raum verfälscht, bis eine Trennung möglich ist.[160]

[158] Chakrabarti, Mining the Web: Discovering Knowledge form Hypertext Data, 2003, S. 147 ff.
[159] Chakrabarti, Mining the Web: Discovering Knowledge form Hypertext Data, 2003, S. 133 ff.
[160] Chakrabarti, Mining the Web: Discovering Knowledge form Hypertext Data, 2003, S. 164 ff.

V. Qualität der Auswertung

Werden nicht alle vorklassifizierten Datensätze zum Trainieren verwendet, kann die Güte der Klassifizierung getestet werden. Hierbei ist allerdings zu beachten, dass sich die Güte der Trainingsdaten direkt auf die Klassifizierung auswirkt. Werden die Klassifizierer mit stark korrelierenden Datensätzen trainiert und getestet, haben die Tests nur sehr eingeschränkte Aussagekraft.

Bei der Klassifizierung mit zwei Klassen, kann es, wie bei der Betrachtung von Indizien, zu zwei in Tabelle 1 aufgezeigten grundsätzlichen Fehlern kommen. Werden mehrere Klassen betrachtet, erhöht sich die mögliche Fehlerzahl entsprechend.

	Klassifiziert als Klasse 1	Klassifiziert als Klasse 2	
Gehört zu Klasse 1	a	b	a+b
Gehört zu Klasse 2	c	d	c+d
	a+c	b+d	n = a+b+c+d

Tabelle 1: Auswertung bei zwei Klassen[161]

Daraus lassen sich mehrere Gütewerte für den Klassifizierer bestimmen:[162]

- Die **Accuracy** gibt die prozentual richtig klassifizierten Datensätze an. Im Zweiklassenfall wird die Accuracy wie folgt berechnet: Accuracy $= \frac{a+d}{n} = P$ (erfolgreich klassifiziert)
- Die **Precision** gibt für eine Klasse an, wie viel Prozent der in der Klasse klassifizierten Datensätze auch zur Klasse gehören. Precision für Klasse 1 $= \frac{a}{a+c} = P$ (erfolgreich klassifiziert | gehört zu Klasse 1)
- Der **Recall** gibt für eine Klasse an, wie viel Prozent der Klassenzugehörigen richtig erkannt wurden. Recall für die Klasse 1 $= \frac{a}{a+c} = P$ (erfolgreich klassifiziert | klassifiziert in Klasse 1)

Werden das Vorliegen einer Haupttatsache und das nicht Vorliegen dieser als Klassen verwendet und sieht man die durchgeführte Klassifizierung als Indiz an, entspricht der Precision-Wert für die Trainings- und Testdaten der bedingten Wahrscheinlichkeit P(I|T). Über die Berechnung des Recalls der anderen Klasse 1 $= \frac{a}{a+b} = P$ wird die Wahrscheinlichkeit angegeben, dass das Indiz, bei nicht Vorliegen der Haupttatsache, vorliegt.

[161] Nach Chakrabarti, Mining the Web: Discovering Knowledge form Hypertext Data, 2003, S. 132.
[162] Chakrabarti, Mining the Web: Discovering Knowledge form Hypertext Data, 2003, S. 131 f.

Yang und Liu haben die verschiedenen Ansätze an einem von Reuters bereitgestellten Datensatz verglichen und sind dabei auf das in der Tabelle 2 dargestellte Ergebnis gekommen.[163]

Methode	Recall	Precision
Linear SVM	0.812	0.914
k-NN	0.834	0.881
Naive Bayes	0.778	0.825

Tabelle 2: Gegenüberstellung der Klassifikationsarten[164]

Für die Interpretation der Wahrscheinlichkeiten muss jedoch wieder die im Teil 2, C, II angegebene Interpretation herangezogen werden. Bei einer Genauigkeit von 95% wird ein Datensatz also nicht zu 0.95 richtig klassifiziert, sondern von 1000 werden 950 Datensätze richtig zugeordnet. Für den einzelnen Datensatz ist aber keine Aussage möglich.[165]

D. Beweiskraft der durch die XPider gewonnenen Daten

Alle als verdächtig klassifizierten Daten der XPider werden durch die zuständigen Finanzämter geprüft, den Finanzbehörden stehen somit umfangreiche Datensätze über die Zuverlässigkeit der Kategorisierung zur Verfügung.[166] Ein Underreporting durch die XPider soll dabei ebenfalls erkannt, nicht aber gemessen werden.[167] Der Bundesrechnungshof rügte 2006 den Einsatz der XPider, weil diese nicht wesentlich zur Identifizierung von unversteuerten Umsätzen beigetragen haben. Die von der Software gelieferte Datenqualität wird als zu gering eingestuft und den Landesfinanzbehörden fehlt die notwendige personelle und organisatorische Ausstattung.[168] In den darauffolgenden Berichten des Bundesrechnungshofs fehlt diese Kritik und nach Presseberichten kann vermutet werden, dass die Qualität der Sucherergebnisse verbessert wurde.[169]

Kommt es zu einer vollständigen Auslastung der XPider, also das Identifizieren und Klassifizieren von 2,5 Millionen Webseiten pro Tag, werden selbst bei einer angenommenen Accuracy von 99,99% noch täglich 250 Seiten falsch klassifiziert. Für eine Auswertung der Recall- und Precision-Werte müsste die Anfangswahrscheinlichkeit bekannt sein. Hierbei ist

[163] Yang und Liu, A re-examination of text categorization methods, SIGIR 1999, 42, 48.
[164] Nach Yang und Liu, A re-examination of text categorization methods, SIGIR 1999, 42, 48.
[165] Lehn, Wegmann und Rettig, Einführung in die Statistik, 2001, S. 34.
[166] Oliver Heyer-Rentsch, Sprecher des Bundesamtes für Finanzen in Böhme, Unschuldig im Visier der Steuerfahnder, der Westen, 09.03.2008, http://www.derwesten.de/wr/westfalen/Unschuldige-im-Visier-der -Steuerfahnder-id1436361.html, (19.06.2010).
[167] o.A., Compliance Risk Management: Progress with the Development of Internet Search Tools for Tax Administration, OECD, 01.10.2004, http://www.oecd.org/dataoecd/44/15/33818593.pdf, S. 12, (15.06.2010).
[168] o.A., Unterrichtung durch den Bundesrechnungshof, Drucksache 16/3200, 13.11.2006, http://dipbt.bundestag.de/dip21/btd/16/032/1603200.pdf, S. 202 f., (01.06.2010)
[169] Böhme, Unschuldig im Visier der Steuerfahnder, der Westen, 09.03.2008, http://www.derwesten.de/wr/westfalen/Unschuldige-im-Visier-der -Steuerfahnder-id1436361.html, (19.06.2010).

auch zu beachten, dass die ermittelten Werte, nur auf die vorklassifizierten Trainingsdaten zutreffen und deswegen von diesen abhängig sind.

E. Zusammenfassung und kritische Würdigung

Die ständig wachsenden Datenmengen werden auf Dauer nicht manuell bewertbar bleiben und es wird nötig sein, auf eine automatisierte Vorauswahl zurückzugreifen. Hier ist es eine Verbesserung, wenn Ermittlungsbehörden unabhängig eigene Daten erheben und nicht auf die Datenerhebung von Unternehmen zurückgreifen, die ihre Datensätze vorsortieren[170] und nach wirtschaftlichen Kriterien präsentieren.[171] Die so ermittelten Seiten können dabei nur einen Anfangsverdacht rechtfertigen, der entsprechende Sachverhalt muss weiter untersucht werden. Ob mit technologischer Weiterentwicklung auch ein ausreichendes Indiz für einen begründeten Tatverdacht vorliegen wird, ist fraglich, da immer Datensätze mit Trainingsdaten verglichen werden und zumindest bei Textdokumenten ein Textvergleich vorliegt. Beim Einsatz von Regellernern, werden Indizienregeln aufgestellt, es kommt also zur Festschreibung, was als Indiz anzusehen ist und die übrigen Randbedingungen werden nicht betrachtet. Es wird ein mit der Rasterfahndung vergleichbarer Ansatz gewählt und ist somit eher ein Mittel zum Erkenntnisgewinn, der sich nur in Ausnahmefällen als Beweismittel eignet.[172]

Im Bezug auf die Zurechenbarkeit und eine Manipulationsdetektion, liegen über die durchgeführten Auswertungen keine Aussagen vor. Die von dem XPider extrahierten Kontaktinformationen können nicht direkt als Annahme für die Zurechenbarkeit Verwendung finden, da diese Angaben in der Regel unverifiziert ins Netz gestellt werden können.[173]

Problematisch beim Einsatz der hier beschriebenen Klassifizieren ist, dass mit diesen ebenfalls versucht wird, zukünftige Sachverhalte vorherzusagen[174] und es so zum "Pygmalioneffekt" kommen kann, da wegen der Ungewissheit hierfür noch keine belastenden oder entlastenden Indizien gesammelt werden können.[175] Hierbei wird nur eine einseitige Hypothese untersucht und nicht in alle Richtungen ermittelt. Bei Ermittlungen über die Gewaltbereitschaft einer Gruppe, erstellten Ermittler nach Presseinformationen Dokumente, um eine Reaktion

[170] Um beispielsweise mit den eigenen Suchergebnissen keine Beihilfe zu leisten. Bager, Google zensiert Scientology-Kritiker, heise news, 21.03.2002, http://www.heise.de/newsticker/meldung/Google-zensiert-Scientology-Kritiker-63741.html, (20.01.2010).

[171] Kuri, Durch Google-Suche in die Einzelhaft [Update], heise news, 22.08.2007, http://www.heise.de/newsticker/meldung/Durch-Google-Suche-in-die-Einzelhaft-Update-165722.html, (20.01.2010).

[172] Phel, Die Implementation der Rasterfahndung, Max-Planck-Institus für ausländisches und internationales Strafrecht, 30.01.2008, http://www.iuscrim.mpg.de/ww/de/pub/forschung/forschungsarbeit/kriminologie/rasterfahndung.htm, (01.06.2010).

[173] Nowitzky, Xpider (eXtended sPIDER) Internet Steuersündern auf der Spur, 07.2003, http://www.minet.uni-jena.de/dbis/veranstaltungen/datenbanktage-2003/DBTage2003-Nowitzky.pdf, S. 5, (01.06.2010).

[174] Für die Privatkreditvermittlungsplattform Smarva wird beispielsweise ein Credit Scoring über eine SVM durchgeführt. Typke, Social Lending: Credit Scoring für Normalbürger (mit Open Source-Software), 27.06.2009, http://www.beobach.de/uploads/media/LinustagSocialLending.pdf, S. 1 ff., (01.06.2010).

[175] Bender, Nack und Treuer, Tatsachenfeststellung vor Gericht, 2007, Rn. 103 ff.

zu provozieren, um deren Gewaltbereitschaft zu beweisen.[176] Gleichzeitig sollte durch einen Verweis auf die Webseite des Bundeskriminalamt über die IP-Adresse die Identität der Diskussionsteilnehmer ermittelt werden. [177]

Teil 6: Verdeckter Eingriff in Informationssysteme

Beim verdeckten Eingriff wird heimlich auf ein Informationssystem zugegriffen.

Dabei kann, muss aber keine Auswirkung auf ein Schutzgut eines Grundrechts vorliegen. Im Weiteren wird mit verdecktem Eingriff nur der heimliche physikalische oder logische Zugriff auf ein Informationssystem bezeichnet. Methoden, die nur Informationen abgreifen, wie eine optische Überwachung eines Eingabegerätes oder die verdeckte Analyse der physischen Abstrahlung eines Endgerätes,[178] sollen nicht zu den verdeckten Eingriffen gezählt werden, weil hier nicht in das Informationssystem eingegriffen, sondern nur die Bedienung bzw. die Abstrahlung dieses Systems ausgewertet wird. Dabei werden nur aktiv von einem Anwender genutzte Daten erfasst. Wird nur eine Abstrahlung, etwa das Geräusch der Tastaturanschläge oder die magnetische Abstrahlung des Monitors verwendet, können nur die auf der Tastatur eingebenden bzw. am Monitor angezeigten Daten abgegriffen werden.

A. Motivation

Ein verdeckter Eingriff bietet den Ermittlungsbehörden den Vorteil des heimlichen Vorgehens, dabei werden Verdächtige möglichst nicht gewarnt und es ist kein Beweismittelverlust zu befürchten.[179] Gleichzeitig können Betroffene, wegen der Unkenntnis der Maßnahme, ihre rechtlichen Interessen nicht selbst wahrnehmen.[180] Durch einen verdeckten Zugriff können auch Hinweise auf die physikalischen Speicherorte der Daten gewonnen werden und so erst einen physikalischen Zugriff ermöglichen. Werden Kommunikationsdaten verschlüsselt, kann eine herkömmliche Telekommunikationsüberwachungsmaßnahme möglicherweise nicht zum Einsatz kommen und so einen verdeckten Eingriff in das System nötig machen.[181] Dazu wird auf die Daten vor der Verschlüsselung bzw. nach der Entschlüsselung zugegriffen oder die

[176] Neuber, Militante Ermittler, Telepolis, 01.04.2009, http://www.heise.de/tp/r4/artikel/30/30054/1.html, (20.04.2010).

[177] Ehrmann, Spiegel: Innenministerium stoppt Überwachung der BKA-Seite, heise news, 21.03.2009, http://www.heise.de/newsticker/meldung/Spiegel-Innenministerium-stoppt-ueberwachung-der-BKA-Seite-208339.html, (04.06.2010).

[178] Pfitzmann, Möglichkeiten und Grenzen der Nutzungsüberwachung von Informations- und Kommunikationssystemen in einer freiheitlichen demokratischen Gesellschaft. 26.09.2007, http://dud.inf.tu-dresden.de/literatur/MoegGrenzderNutzuebIuK-Sys-V1-0.pdf, S. 3, (20.01.2010).

[179] Siebert, Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts, 09.10.2007, http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf, S. 2, (20.01.2010).

[180] In Dänemark wird durch eine gerichtliche Anordnung ohne Wissen des Verdächtigen ein Anwalt zur Wahrnehmung dessen Interessen bestellt. Siebert, Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts, 09.10.2007, http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf, S. 23, (20.01.2010).

[181] Fox, Stellungnahme zur Online-Durchsuchung, 07.09.2007, http://www.secorvo.de/publikationen/stellungnahme-secorvo-bverfg-online-durchsuchung.pdf, S. 3, (20.01.2010).

zur Entschlüsselung nötigen geheimen Schlüssel abgegriffen[182] So können die logischen Schutzmechanismen, die eine vertrauliche Kommunikation ermöglichen, umgangen werden. Darüber hinaus besteht die Möglichkeit auf im System vorhandene Sensoren wie Kameras, Mikrofon, GPS-Empfänger oder Temperaturabnehmer zuzugreifen, um so digitale Beweise mit physikalischen Beweisen zu kombinieren.[183] Durch die Überwachung eines Systems können flüchtige Inhalte, wie z.B. gelöschte Dateien, Chat-Protokolle, anonyme Foreneinträge, gesichert werden.[184]

Im Weiteren wird davon ausgegangen, dass durch den verdeckten Zugriff Daten gewonnen wurden, der Zugriff also erfolgreich oder scheinbar erfolgreich durchgeführt werden konnte und entsprechende Schutzmechanismen entweder nicht eingesetzt[185] wurden oder nicht wirksam waren. Aus einer erfolgreichen Abwehr eines verdeckten Eingriffes folgen keine elektronischen Beweismittel und damit erübrigt sich die Frage bezüglich deren Beweiskraft. Der Einsatz von wirkungsvollen Maßnahmen zur Absicherung eines Informationssystems oder der Kommunikation allein reichen nicht aus, um einen hinreichenden Verdacht zu begründen.[186]

Das Bundesministerium des Inneren unterscheidet beim Online-Zugriff zwischen Quellen-Telekommunikationsüberwachung, Online-Durchsuchung und Online-Überwachung. Während bei der Quellen-Telekommunikationsüberwachung Kommunikationsverbindungen abgegriffen werden, sollen bei der Online-Durchsicht Daten ermittelt werden, die in der Vergangenheit angefallen sind. Bei der Online-Überwachung sollen über einen Zeitraum Aktivitäten des Nutzers protokolliert werden. Die Online-Überwachung ergänzt also die Online-Durchsicht durch flüchtige Daten und Klartextdaten vor einer Verschlüsselung oder nach einer Entschlüsselung.[187] Die Abgrenzung zwischen Online-Überwachung und Quellen-Telekommunikationsüberwachung scheint willkürlich, da der Aufbau einer Kommunikationsverbindung und die Durchführung der darauf folgenden Kommunikation ebenfalls eine Aktivität eines Nutzers darstellt und für die Überwachung einer möglichen Sprachsteuerung die Daten auch erhoben werden müssen. Nur durch technische Beschränkungen kann diese Doppelfunktionalität eingeschränkt werden, durch minimale Änderungen können allerdings alle Audio-Ein/Ausgaben erfasst bzw. die Überwachung auf weitere Ein/Ausgabenkanäle ausgedehnt werden.

---

[182] Ziercke, Pro Online-Durchsuchung, Informatik-Spektrum 2008, 62, 63.

[183] Siebert, Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts, 09.10.2007, http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf, S. 4, (20.01.2010).

[184] Fox, Stellungnahme zur Online-Durchsuchung, 07.09.2007, http://www.secorvo.de/publikationen/stellungnahme-secorvo-bverfg-online-durchsuchung.pdf, S. 4, (20.01.2010).

[185] Bei rechtsradikalen Tätergruppen wurden sehr gute Anleitungen zum Einsatz von Kryptografie gefunden, die allerdings nicht umgesetzt wurden. Siebert, Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts, 09.10.2007, http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf, S. 13, (20.01.2010).

[186] BGH, Beschl. v. 18.10.2007, Az. StB 34/07, S. 4, Homepage: http://www.bundesgerichtshof.de (01.02.2009).

[187] Stawowy, Fragenkatalog des Bundesministeriums der Justiz, netzpolitik.org, 22.09.2007, http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf, S. 6, (20.01.2010).

Daneben können über verdeckte Eingriffe in ein informationstechnisches System durch die darin vorhandenen Sensoren eine Vielzahl weiterer Informationen gewonnen werden, z.B. erlauben Mikrofone und Kameras die Durchführung von akustischer und visueller Überwachung, und GPS-Empfänger Positionsverfolgungen.

B. Ermächtigungsgrundlage

Nach dem "Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG)"[188] können informationstechnische Systeme Ziel eines verdeckten Zugriffs werden, um die Telekommunikation nach § 20l Abs. 2 BKAG zu überwachen oder um nach § 20k Abs. 1 S. 1 BKAG Daten zu erheben.

§ 20l BKAG Überwachung der Telekommunikation

[...]

(2) Die Überwachung und Aufzeichnung der Telekommunikation darf ohne Wissen des Betroffenen in der Weise erfolgen, dass mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn

1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, und

2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.

§ 20k Abs. 2 und 3 gilt entsprechend. § 20k bleibt im Übrigen unberührt.

[...]

§ 20k BKAG Verdeckter Eingriff in informationstechnische Systeme

(1) Das Bundeskriminalamt darf ohne Wissen des Betroffenen mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme eingreifen und aus ihnen Daten erheben, wenn bestimmte Tatsachen die Annahme rechtfertigen, dass eine Gefahr vorliegt für

1. Leib, Leben oder Freiheit einer Person oder

2. solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.

Eine Maßnahme nach Satz 1 ist auch zulässig, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass ohne Durchführung der Maßnahme in näherer Zukunft ein Schaden eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für eines der in Satz 1 genannten Rechtsgüter hinweisen. Die Maßnahme darf nur durchgeführt werden, wenn sie für die Aufgabenerfüllung

[188] Gegen die gesetzliche Grundlage sind Verfassungsbeschwerden anhängig. Vgl z.B. Verfassungsbeschwerde gegen das BKAG: Winsemann, Verfassungsbeschwerde gegen das BKA-Gesetz, Telepolis, 27.01.2009, http://www.heise.de/tp/r4/artikel/29/29614/1.html, (20.01.2010).

nach § 4a erforderlich ist und diese ansonsten aussichtslos oder wesentlich erschwert wäre.

[...]

Vergleichbare Regelungen finden sich teilweise in den Polizeigesetzen der Länder, u.a. Quellen-Telekommunikaitonsüberwachung im „Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG)“ in § 15b Abs. 1 HSOG oder der verdeckte Zugriff auf informationstechnische Systeme im bayerischen[189] „Polizeiaufgabengesetz (PAG)“ in Art 34d Abs. 1 PAG. In der Strafprozessordnung gibt es noch keine Regelung für einen verdeckten Zugriff.[190] Momentan kann ein verdeckter Zugriff für eine Online-Durchsuchung oder Online-Überwachung nur zur Gefahrenabwehr oder bei mehrdeutigen Maßnahmen, mit Schwerpunkt auf die Gefahrenabwehr, gehandelt werden.[191] Die auf der Grundlage von § 110 Abs. 3 StPO durchgeführte Online-Durchsicht wird, wegen der fehlenden Heimlichkeit, nicht als verdeckter Zugriff gewertet. In § 110 Abs. 3 S. 2 2. HS. StPO wird auf § 98 Abs. 2 StPO verwiesen und damit wird nach § 33 Abs. 2 und Abs. 3 StPO der Betroffene durch das bestätigende Gericht gehört und kann so seine rechtlichen Interessen wahrnehmen.[192]

Auf der Grundlage einer Dienstvorschrift wurden bis 2007 durch die Geheimdienste[193] knapp ein Dutzend verdeckte Zugriffe durchgeführt. Das BKA hat in dem Zeitraum Januar 2009 bis Mai 2010 keine Maßnahmen der Online-Durchsuchung beantragt.[194] Für das Landesamt für Verfassungsschutz in Bayern beinhaltet das Bayrische Verfassungsschutzgesetz (BayVSG) eine direkte Ermächtigung für den verdeckten Zugriff in Art. 6e BayVSG.

§ 15b HSOG Telekommunikationsüberwachung an informationstechnischen Systemen

(1) Wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich ist, kann die Überwachung und Aufzeichnung der Telekommunikation ohne Wissen der betroffenen Person in der Weise erfolgen, dass mit technischen Mitteln in von der betroffenen Person genutzte informationstechnische Systeme eingegriffen wird, wenn

1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, und

[189] Bayern ist momentan das einzige Bundesland mit einer Befugnisnorm für Eingriffe in informationstechnische Systeme für die Polizei. o.A., Bilanz der Online-Durchsuchung, Drucksache 17/1814, 21.05.2010, http://dip21.bundestag.de/dip21/btd/17/018/1701814.pdf, S. 2, (10.07.2010).

[190] BGH, Beschl. v. 31.01.2007, Az. StB 18/06, S. 1 Homepage: http://www.bundesgerichtshof.de (01.02.2009).

[191] Schmid, Verdeckte Online-Durchsuchungen (11/2007), CyLaw-Report XX, 07.01.2008, http://www.cylaw.tu-darmstadt.de/media/jus4/cylawreports/cylaw_report_xx.pdf, S. 25, (20.01.2010).

[192] BVerfG, Beschl. v. 15.10.2008, Az. 2 BvR 236/ 08 , Rn. 121 Homepage: http://www.bundesverfassungsgericht.de (01.02.2009).

[193] o.A., Ein Dutzend Online-Durchsuchungen seit 2005, Tagesschau.de, 27.04.2007, http://www.tagesschau.de/inland/meldung36524.html, (20.01.2010).

[194] o.A., Bilanz der Online-Durchsuchung, Drucksache 17/1814, 21.05.2010, http://dip21.bundestag.de/dip21/btd/17/018/1701814.pdf, S. 2, (10.07.2010).

2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.

[...]

Art. 34d PAG Verdeckter Zugriff auf informationstechnische Systeme

(1)[1] Die Polizei kann mit technischen Mitteln verdeckt auf informationstechnische Systeme zugreifen, um Zugangsdaten und gespeicherte Daten zu erheben von Personen,

1. die für eine Gefahr verantwortlich sind, soweit dies zur Abwehr einer dringenden Gefahr für

1. den Bestand oder die Sicherheit des Bundes oder eines Landes,

2. Rechtsgüter der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, oder

3. Leib, Leben oder Freiheit einer Person

erforderlich ist, oder

2. soweit bestimmte Tatsachen die begründete Annahme rechtfertigen, dass

1. sie für Personen nach Nr. 1 bestimmte oder von diesen herrührende Mitteilungen entgegennehmen oder entgegengenommen haben, ohne insoweit das Recht zur Verweigerung des Zeugnisses nach §§ 53 , 53a StPO zu haben, oder solche Mitteilungen weitergeben oder weitergegeben haben oder

2. die unter Nr. 1 genannten Personen ihre informationstechnischen Systeme benutzen oder benutzt haben.

[2] Eine Maßnahme nach Satz 1 darf nur durchgeführt werden, wenn die Erfüllung einer polizeilichen Aufgabe auf andere Weise aussichtslos oder wesentlich erschwert wäre. [3] Daten dürfen unter den Voraussetzungen des Satzes 1 gelöscht werden, wenn eine gegenwärtige Gefahr für Leib oder Leben nicht anders abgewehrt werden kann. [4] Wird erkennbar, dass in ein durch ein Berufsgeheimnis geschütztes Vertrauensverhältnis im Sinn der §§ 53 , 53a StPO eingegriffen wird, ist die Maßnahme insoweit unzulässig, es sei denn, sie richtet sich gegen den Berufsgeheimnisträger selbst. [5] Soweit dies informationstechnisch und ermittlungstechnisch möglich ist, hat die Polizei durch geeignete Vorkehrungen sicherzustellen, dass die Erhebung von Daten unterbleibt, die dem Kernbereich der privaten Lebensgestaltung zuzurechnen sind. [6] Wird erkennbar, dass solche Daten betroffen sind und bestehen keine Anhaltspunkte dafür, dass diese Daten dem Zweck der Herbeiführung eines Erhebungsverbots dienen sollen, ist die Maßnahme insoweit unzulässig. [7] Maßnahmen nach den Sätzen 1 und 3 sind zu dokumentieren.

[...]

§ 33 StPO

[...]

(2) Eine Entscheidung des Gerichts, die außerhalb einer Hauptverhandlung ergeht, wird nach schriftlicher oder mündlicher Erklärung der Staatsanwaltschaft erlassen.

(3) Bei einer in Absatz 2 bezeichneten Entscheidung ist ein anderer Beteiligter zu hören, bevor zu seinem Nachteil Tatsachen oder Beweisergebnisse, zu denen er noch nicht gehört worden ist, verwertet werden.

[...]

Art. 6e BayVSG Verdeckte Online-Datenerhebung

(1) [1] Das Landesamt für Verfassungsschutz kann bei Vorliegen tatsächlicher Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut unter den Voraussetzungen des Art. 6a Abs. 2 im Einzelfall mit technischen Mitteln verdeckt auf informationstechnische Systeme zugreifen, um Zugangsdaten und gespeicherte Daten zu erheben; die Maßnahmen sind zu dokumentieren. [2] Die Anordnung ist nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre. [3] Sie darf sich nur gegen Verdächtige und ihre Nachrichtenmittler richten. [4] Gegen Nachrichtenmittler darf sich die Maßnahme nur insoweit richten, als sie kein Recht zur Verweigerung des Zeugnisses nach den §§ 53 , 53a StPO haben. [5] Wird erkennbar, dass in ein durch ein Berufsgeheimnis geschütztes Vertrauensverhältnis im Sinn der §§ 53 , 53a StPO eingegriffen wird, ist die Maßnahme insoweit unzulässig, es sei denn, sie richtet sich gegen den Berufsgeheimnisträger selbst. [6] Soweit informationstechnisch und ermittlungstechnisch möglich, sind alle Maßnahmen zu ergreifen, mit denen die Erhebung von Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, vermieden werden kann. [7] Wird erkennbar, dass solche Daten betroffen sind und bestehen keine Anhaltpunkte dafür, dass diese Daten dem Zweck der Herbeiführung eines Erhebungsverbots dienen sollen, ist die weitere Datenerhebung insoweit unzulässig.

(2) [1] Zur Vorbereitung einer Maßnahme nach Abs. 1 dürfen auch technische Mittel eingesetzt werden, um spezifische Kennungen sowie den Standort eines informationstechnischen Systems zu ermitteln. [2] Personenbezogene Daten Dritter dürfen dabei nur erhoben werden, soweit dies aus technischen Gründen unvermeidbar ist. [3] Nach Beendigung der Maßnahme sind diese unverzüglich zu löschen.

Ein "informationstechnisches System" besteht dabei aus Hard- und Software sowie Daten zur Erfassung, Speicherung, Verarbeitung, Übertragung und Anzeige von Informationen. Damit können einzelne PCs und ganze Netzwerke, z.B. das Internet, als informationstechnisches System verstanden werden.[195] Als kleinere Einheiten könnten Mobiltelefone, Armbanduhren, Waschmaschinen, Chipkarten, medizinische Stimmulationsgeräte[196] oder PKWs

[195] Stawowy, Fragenkatalog des Bundesministeriums der Justiz, netzpolitik.org, 22.09.2007, http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf, S. 1 f., (20.01.2010).

[196] Beispielsweise ein Hirnschrittmacher, vgl. Kupsch, Ulm und Funk, „Hirnschrittmacher“ gegen die Parkinson-Erkrankung. Eine Patientenaufklärung, Charité – Universitätsmedizin Berlin, 06.09.2005, http://www.charite.de/ch/neuro/klinik/patienten/ag_bewegungsstoerungen/pdf/DBS_Aufklaerungsmaterial.pdf,S. 8, (20.01.2010).

aufgefasst werden, also alle Systeme die selbständig ein Programm ausführen und Daten lokal abspeichern können.[197]

Die sog. technischen Mittel werden sehr unterschiedlich bezeichnet. Das Bundesministerium des Inneren nennt die Software für die Online-Durchsuchung und Online-Überwachung „Remote Forensic Software“ und suggeriert damit einen Beweiswert wie den einer forensischen Analyse.[198] In der Presse wird mit der Benennung als "`Bundestrojaner"' eine bestimmte Methode des Eindringens in das System unterstellt oder mittels "Bundeswanze" von einer Abhörsoftware ausgegangen[199] Allgemein wird von "Durchsuchungssoftware" gesprochen, womit allerdings eine Beschränkung auf eine Softwarelösung angenommen wird.[200] Technisch ist eine solche Abgrenzung nicht sinnvoll, da unter anderem bei der Sicherung des flüchtigen Hauptspeichers keine Unterscheidung nach der Datenart gemacht wird. Ein solches Abbild kann sowohl Passwörter, als auch Kamerabilder einer angeschlossenen Kamera enthalten.[201] Im Weiteren sollen die Hilfsmittel (Software + Hardware) für einen verdeckten Zugriff allgemein als Werkzeug bezeichnet werden. Die Begriffe Online-Durchsuchung und Online-Überwachung sollen beibehalten werden, auch wenn weder die Durchsuchung noch die Überwachung eine im eigentlichen Sinne "Online", also mit bestehender Kommunikationsverbindung zu einem anderen Informationssystem, erfolgt. Die Überwachung/Durchsuchung wird nicht mit z.B. der Trennung der DSL-Leitung oder Abschalten des Wireless Local Area Network (WLAN) Adapters unterbrochen bzw. aufgehalten.

Da die Art der Einbringung und die Arbeitsweise der eingesetzten Werkzeuge beim verdeckten Zugriff durch die Strafverfolgungsbehörden, in Abhängigkeit vom Aufbau und der Nutzung des Zielsystems, im Einzelfall angepasst werden sollen,[202] müssen im Bezug auf den Beweiswert verschiedene Szenarien betrachtet werden.

C. Allgemeines Vorgehen

Der Gesetzgeber macht keine Vorgaben, die den Ablauf eines verdeckten Eingriffs regeln. Allgemein kann ein verdeckter Eingriff in folgenden Schritten ablaufen:[203]

1. Informationssammlung (Zielperson und Zielsystem)
2. Einbringung der Werkzeuge - Infiltration

---

[197] Freiling, Schriftliche Stellungnahme zum Fragenkatalog Verfassungsbeschwerden, 27.09.2007, https://pi1.informatik.uni-mannheim.de/filepool/publications/stellungnahme-online-durchsuchung.pdf, S. 2, (20.01.2010).

[198] Stawowy, Fragenkatalog des Bundesministeriums der Justiz, netzpolitik.org, 22.09.2007, http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf, S. 1 ff., (20.01.2010).

[199] Winkler, Bundeswanze statt Trojaner, IT-News World, 03.08.2007, http://www.it-news-world.de/news_1017/Bundeswanze+statt+Trojaner, (20.01.2010)

[200] Fox, Stellungnahme zur Online-Durchsuchung, 07.09.2007, http://www.secorvo.de/publikationen/stellungnahme-secorvo-bverfg-online-durchsuchung.pdf, S. 3, (20.01.2010).

[201] Stawowy, Fragenkatalog des Bundesministeriums der Justiz, netzpolitik.org, 22.09.2007, http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf, S. 7, (20.01.2010).

[202] Ziercke, Pro Online-Durchsuchung, Informatik-Spektrum 2008, 62, 64.

[203] Ziercke, Pro Online-Durchsuchung, Informatik-Spektrum 2008, 62, 64.

3. Steuerung der Suchroutinen oder Aufzeichnung - Manipulation und Durchsuchung
4. Ausleitung der gefundenen Daten - Übertragung
5. Löschung vom Zielsystem - Deinfiltration

I. Informationssammlung

Aufgabe der Informationssammlung ist es, eine Möglichkeit zum verdeckten Eindringen in das gewünschte Informationssystem zu finden.

Um die dazu nötigen Werkzeuge zu ermitteln, sind möglichst detaillierte Informationen über das Zielsystem und die Anwender erforderlich. Neben der Art des zu infiltrierenden Gerätes (Laptop, Handy, PC), Netzwerk, usw.) müssen die eingesetzten Prozessoren ermittelt werden, weil sonst die Werkzeuge für den verdeckten Eingriff evtl. nicht auf dem Prozessor ausgeführt werden können. Bei der Software muss aus gleichen Gründen zumindest das Betriebssystem bekannt sein. Sind diese Informationen notwendig, um in das System einzudringen, erhöhen alle weiteren Informationen die Erfolgsaussichten. Informationen, z.B. über Anwendungen oder eingesetzte Netzwerkverbindungen, können mögliche Schwachstellen offenbaren und so die Auswahl an möglichen Angriffsvektoren (Angriffswege) vergrößern.

Die Informationen können durch klassische Beobachtung des Anwenders oder durch klassische Telekommunikationsüberwachung und der Analyse einer möglichen Kommunikationsverbindung erfolgen.[204] Darüber hinaus besteht noch die Möglichkeit durch eine Art Reaktionstest, möglicherweise automatisiert, Informationen über das System zu bekommen. Dabei wird beobachtet, wie das System auf Daten von außerhalb reagiert oder nicht reagiert. Aus der Art der Reaktion, der zurückgesendeten Daten oder eben der Blockierung dieser, können Schlüsse über die verwendete Software/Hardware gezogen werden.[205] Dieses Abklopfen des Systems kann bereits zu Veränderungen am System, wenn dieses z.B. den Abklopfvorgang mitprotokolliert, führen. Neben diesen Veränderungen am System, kann sich dann die Informationssammlung auf die Beweiskraft der Daten auswirken, wenn der Anwender oder das Zielsystem diese Voraufklärung bemerkt und darauf reagiert. Bei geschicktem und individualisiertem Vorgehen ist die Wahrscheinlichkeit einer Entdeckung geringer, als bei einer herkömmlichen Observation, einzuschätzen. Kann zur Informationsbeschaffung physikalisch auf das Informationssystem zugegriffen werden, können die Werkzeuge so an das Informationssystem angepasst werden und es kann, wenn der physikalische Zugriff unbemerkt bleibt, eine Entdeckung nahezu ausgeschlossen werden.[206] Wird der verdeckte Zugriff bemerkt und als solcher erkannt, ist anzunehmen, dass entlastende Daten bereitgehalten werden.

[204] Stawowy, Fragenkatalog des Bundesministeriums der Justiz, netzpolitik.org, 22.09.2007, http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf, S. 10, (20.01.2010).
[205] Lyon, Nmap Reference Guide, http://nmap.org/book/man.html, (20.01.2010).
[206] Roggan, Präventive Online-Durchsuchungen. Überlegungen zu den Möglichkeiten einer Legalisierung im Polizei- und Geheimdienstrecht, 2008, 97, 99.

II. Einbringen der Software

Nach übereinstimmender Expertenmeinung sind allgemein drei Einbringungsarten möglich, die einzeln oder kombiniert angewandt werden können.[207] [208] [209] Hierbei ist es möglich, dass durch das Einspielen der Werkzeuge bereits Daten überschrieben und somit Beweismittel verloren gehen.

- Ausnutzung von Software-Schwachstellen oder soziale Manipulation
- Unterstützung Dritter
- physischer Zugang zum Zielsystem

1. Ausnutzung von Schwachstellen

Wirtschaftliche Interessen der Hersteller führen zu einem immer besseren logischen Eigenschutz einzelner Geräte[210] oder ganzer Netzwerke.[211] Durch die steigende Funktionalität und damit verbundenen Komplexität, wird diese marktgetriebene Sicherung nur langfristig greifen. Für das Jahr 2008 hat Symantic einen Anstieg der neu entdeckten Sicherheitslücken um 19% auf 5.491 erfasst.[212] Werden alle als Informationssystem klassifizierbaren Geräte betrachtet und damit z.B. auch Autos oder medizinische Geräte wie intelligente Herzschrittmacher, ist der Druck auf den Hersteller, sichere Systeme anzubieten, ungleich höher.

Bei der Ausnutzung von Schwachstellen, kann zwischen bekannten und unbekannten Schwachstellen unterschieden werden. Für bekannte Schwachstellen stellt der Hersteller meist schnell ein Update zur Verfügung, welches die Schwachstelle behebt.[213] Für noch nicht bekannte Schwachstellen existiert ein Schwarzmarkt, wo Informationen über Schwachstellen gehandelt werden. Eine noch unbekannte Schwachstelle wird durchschnittlich nach einem Jahr entdeckt und durch ein Softwareupdate des Herstellers geschlossen.[214] Neben den Schwachstellen in der Software, können auch Administrationsfehler zu Infiltrationsmöglich-

[207] Freiling, Schriftliche Stellungnahme zum Fragenkatalog Verfassungsbeschwerden, 27.09.2007, https://pi1.informatik.uni-mannheim.de/filepool/publications/stellungnahme-online-durchsuchung.pdf, S. 4, (20.01.2010).

[208] Pfitzmann, Möglichkeiten und Grenzen der Nutzungsüberwachung von Informations- und Kommunikationssystemen in einer freiheitlichen demokratischen Gesellschaft. 26.09.2007, http://dud.inf.tu-dresden.de/literatur/MoegGrenzderNutzuebIuK-Sys-V1-0.pdf, S. 5, (20.01.2010).

[209] Siebert, Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts, 09.10.2007, http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf, S. 12, (20.01.2010).

[210] Pfitzmann, Möglichkeiten und Grenzen der Nutzungsüberwachung von Informations- und Kommunikationssystemen in einer freiheitlichen demokratischen Gesellschaft. 26.09.2007, http://dud.inf.tu-dresden.de/literatur/MoegGrenzderNutzuebIuK-Sys-V1-0.pdf, S. 2, (20.01.2010).

[211] Bachfeld, 1&1 will gegen Bot-Netze vorgehen, heise security, 10.02.2009, http://www.heise.de/security/meldung/1-1-will-gegen-Bot-Netze-vorgehen-193968.html, (20.01.2010).

[212] Fossi, Symatec Sicherheitsbericht, 2009, S. 3.

[213] Pfitzmann, Möglichkeiten und Grenzen der Nutzungsüberwachung von Informations- und Kommunikationssystemen in einer freiheitlichen demokratischen Gesellschaft. 26.09.2007, http://dud.inf.tu-dresden.de/literatur/MoegGrenzderNutzuebIuK-Sys-V1-0.pdf, S. 2, (20.01.2010).

[214] o.A., Durchschnittliche Haltbarkeit von Zero-Day-Lücken liegt bei einem Jahr, heise news, 10.07.2007, http://www.heise.de/security/meldung/Durchschnittliche-Haltbarkeit-von-Zero-Day-Luecken-liegt-bei-einem-Jahr-149435.html, (20.01.2010).

keiten führen. Beispiele für Administrationsfehler wären: die Verwendung unsicherer Zugangspasswörter, unsichere Verschlüsselungstechnologie, Konfigurationsfehler z.B. bei Filtern oder das nicht Einspielen von sicherheitsrelevanten Softwareupdates.

Bekannte und unbekannte Schwachstellen können auch von Dritten ausgenutzt werden. Diese können das System manipulieren oder komplett kontrollieren. Stehen Exploits, das sind Befehlsfolgen oder kurze Programme, die die Schwachstellen ausnützen, zur Verfügung und ist das Informationssystem mit einem öffentlichen Kommunikationsnetz verbunden, erfolgt meist ein verdeckter Zugriff innerhalb von wenigen Minuten.[215] Dabei kommen permanent neue Exploits zum Einsatz, bzw. mutieren bereits bekannte Exploits. Allein im Jahr 2008 wurden von Symantec pro Monat 28,7 Millionen neue Schadcode-Varianten erfasst.[216]

Bei sozialer Manipulation[217] wird versucht, den Anwender dazu zu bringen, die für den Zugang nötigen Werkzeuge selbst auszuführen oder eine, für das Ausnutzen einer Schwachstelle, nötige Hilfshandlung durchzuführen, wie das Nutzen einer Software mit einer gewünschten Schwachstelle oder das Beziehen einer Software, die mit einem Werkzeug (Trojanisches Pferd) kombiniert ist. Weitere Beispiele sind das Verteilen von Speichermedien[218] oder Versenden von manipulierten Nachrichten, z.B. Mails von anderen Behörden, mit der Absicht, eine Handlung durch den Anwender hervorzurufen.[219] In diesen Beispielen wären gewünschte Aktionen durch den angegriffenen Nutzer, das Verbinden der Speichermedien mit dem zu infiltrierenden Informationssystem oder der Besuch einer präparierten Webseite, bei deren Aufruf Sicherheitslücken im Browser ausgenutzt werden, um ein Werkzeug einzubringen (Drive-by-Download) oder Zugangsdaten abzufragen (Phishing). Es kann auch versucht werden, Zugangsdaten mittels inszenierter Kontaktaufnahme, z.B. über ein Telefon, zu bekommen. Kevin Mitnick spricht diesbezüglich vom Mensch als schwächstes Glied in der Kette und einer Erfolgswahrscheinlichkeit von 99,5%.[220]

2. Unterstützung durch Dritte

Mögliche Dritte, die eine Online-Durchsuchung unterstützen könnten, wären beispielsweise Administratoren und deren Vorgesetzte[221] oder die Manipulation eines vom Anwender ausgeführten Downloads. Dazu kann man Online-Aktualisierung von bereits installierter Soft-

[215] o.A., Survival Time, SANS Internet Storm Center, 02.2010, http://isc.sans.org/survivaltime.html, (20.01.2010).

[216] Fossi, Symatec Sicherheitsbericht, 2009, S. 2.

[217] ob dies als List oder unzulässige Täuschung anzusehen ist, hat keine direkte Auswirkung auf den Beweiswert bezogen auf die Integrität und Zurechenbarkeit.

[218] Kuhn, Sicherheitsbetrachtungen von Wechselmedien, insbesondere USB-Sticks unter Windwos, ERNW, 22.03.2008, http://www.ernw.de/content/e15/e28/e1180/download1182/ERNW_Newsletter_22_v1.0_ger.pdf, S. 5, (20.01.2010).

[219] Stawowy, Fragenkatalog des Bundesministeriums der Justiz, netzpolitik.org, 22.09.2007, http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf, S. 14, (20.01.2010).

[220] Sperlich, Es hat sich viel verändert, Technology Review, 20.06.2008, http://www.heise.de/tr/artikel/Es-hat-sich-viel-veraendert-275332.html, (20.01.2010).

[221] Beide können in der Regel physikalisch auf das Informationssystem zugreifen. Stawowy, Fragenkatalog des Bundesministeriums der Justiz, netzpolitik.org, 22.09.2007, http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf, S. 20, (20.01.2010).

ware durch den Hersteller dieser Software verändern oder über einen Internet-Service-Provider den Datenstrom manipulieren.[222] Software könnte vom Hersteller auch mit Hintertüren,[223] also eingeplanten Schwachstellen, ausgestattet werden und darüber einen Zugriff auf ein Informationssystem ermöglichen. Neben dem Hersteller können auch alle anderen Parteien, die entlang des Vertriebsweges Zugriff auf das Informationssystem haben, eine Schwachstelle zur Infiltration des Systems einbauen[224]. Internet Service Provider (ISP) könnten die Schutzmechanismen, die sie aus eigenen Interessen betreiben, für den Zugriff deaktivieren.[225] Auch bei einer exklusiven Kooperation mit einer dritten Instanz besteht für weitere Angreifer die Möglichkeit, dass sie sich einer ähnlichen Methode bedienen. Durch Ausnutzung von Schwachstellen können unter anderem Angreifer erfolgreich die Infrastruktur des Softwareanbieters[226] angreifen, sich in den Datenstrom über die Bereitstellung eines Proxys, z.B. bei einem Anonymisierungsdienst, einklinken oder sich mittels sogenannter Man in the Middle Attacken[227] in den Datenstrom einschalten und über manipulierte Cacheeinträge[228] die Zugriffe auf manipulierte Server umleiten (Pharming).

Es besteht theoretisch auch die Möglichkeit die Kontrolle eines bereits infizierten Informationssystems auf dem Schwarzmarkt zu erwerben.[229]

3. Physikalischer Zugriff

Bei physikalischem Zugriff müssen physikalische Schutzmaßnahmen überwunden werden. Da physikalische Schutzmechanismen die Kontroll- und Nutzermöglichkeiten einschränken und sich die Geräte gegebenenfalls in einem physikalischen Schutzbereich, wie z.B. der Wohnung, befinden, besteht ein geringerer wirtschaftlicher Druck, die Schutzmechanismen bei Standardgeräten besonders ausgeprägt zu gestalten. Die Schutzmaßnahmen sind damit oft vom Informationssystem abgekoppelt und werden vom Nutzer zusätzlich eingerichtet.[230]

---

[222] Freiling, Schriftliche Stellungnahme zum Fragenkatalog Verfassungsbeschwerden, 27.09.2007, https://pi1.informatik.uni-mannheim.de/filepool/publications/stellungnahme-online-durchsuchung.pdf, S. 4, (20.01.2010).

[223] dmkl, Sony BMGs Kopierschutz mit Rootkit-Funktionen, heise news, 01.11.2005, http://www.heise.de/newsticker/meldung/Sony-BMGs-Kopierschutz-mit-Rootkit-Funktionen-143366.html, (20.01.2010).

[224] o.A., Small Number of Video iPads Shipped With Windwos Virus, Apple Inc., 27.04.2007, http://www.apple.com/support/windowsvirus/, (20.01.2010).

[225] Brors, EU-Strafermittler nehmen Vorwürfe gegen Skype zurück, heise news, 28.02.2009, http://www.heise.de/newsticker/meldung/EU-Strafermittler-nehmen-Vorwuerfe-gegen-Skype-zurueck-202086.html, (20.01.2010).

[226] Schulze, Debian Investigation Report after Server Compromises, 02.12.2003, http://lists.debian.org/debian-announce/2003/msg00003.html, (20.01.2010).

[227] o.A., Microsoft Security Advisory (977377): Vulnerability in TLS/SSL Cloud Allow Spoofing, 09.02.2010, http://www.microsoft.com/technet/security/advisory/977377.mspx, (01.06.2010).

[228] o.A., Massives DNS-Sicherheitsproblem gefährdet das Internet, heise security, 09.07.2008, http://www.heise.de/security/meldung/Massives-DNS-Sicherheitsproblem-gefaehrdet-das-Internet-184975.html, (20.01.2010).

[229] Fossi, Symantec Report on the Underground Economy, symantec 2008, S. 73.

[230] Pfitzmann, Möglichkeiten und Grenzen der Nutzungsüberwachung von Informations- und Kommunikationssystemen in einer freiheitlichen demokratischen Gesellschaft. 26.09.2007, http://dud.inf.tu-dresden.de/literatur/MoegGrenzderNutzuebIuK-Sys-V1-0.pdf, S. 2, (20.01.2010).

Die einfachsten Schutzmechanismen gegen einen physikalischen Zugriff sind, unter der Voraussetzung der Unnachahmbarkeit, die Verwendung von Sigeln, damit wird der Zugriff angezeigt und kann dann durch Entfernen der Werkzeuge verhindert werden.

Neben der Einbringung von Softwarewerkzeugen können beim physikalischen Zugriff Hardwarewerkzeuge, beispielsweise in die Datenleitungen von Eingabegeräten, eingebracht werden.[231] Ein solches Werkzeug kommt ohne die Möglichkeit aus, selbst Signale an das Informationssystem zu senden und führt so nicht zwangsweise zu Änderungen an den Daten. Softwarewerkzeuge können direkt oder über ein angeschlossenes Speichermedium beim nächsten Systemstart automatisch installiert werden. Auch hier wird mit einem erfolgreichen Zugriff die Manipulationsmöglichkeit durch Dritte gezeigt. Die gegenteilige Meinung, dass das physikalische Einspielen die exklusive Kontrolle erlaubt,[232] geht davon aus, dass die Informationssysteme in einem geschützten Wohnraum aufgestellt sind, keine Verbindungen zu anderen Informationssystemen bestehen und dass kein Dritter in diese eindringen möchte oder kann. Die letzteren Punkte sind zu bezweifeln, da, z.B. bei organisierter Kriminalität, davon auszugehen ist, dass sie über dieselben Möglichkeiten wie die Strafverfolger verfügen und dabei nicht an gesetzliche Beschränkungen gebunden sind. Durch einen physikalischen Zugriff lässt sich sicherstellen, dass das Informationssystem zweifelsfrei identifiziert wird und nicht versehentlich in ein Fremdsystem eingedrungen wird. Ein Eindringen in den Wohnraum zum Zweck eines verdeckten Eingriffes sieht das BKAG nicht vor.[233] [234] Der Vertreter des Bayrischen Landeskriminalamts (LKA) hielt, bei der Anhörung zum BKAG Entwurf im Bundestag, die verdeckte Wohnraumdurchsuchung für eine erfolgreiche Installation und den Zugriff für notwendig.[235] Ein unverifiziertes Dokument eines unbekannten Hinweisgebers vom Bayerischen Staatsministerium der Justiz, über die Kostenteilung zwischen Polizei und Staatsanwaltschaften für die Telekommunikationsüberwachung der Voice-over-IP (VoIP) Software Skype,[236] lässt die Schlussfolgerung zu, dass die Installation physikalisch erfolgen sollte, da die Kosten aus der Leistungsbeschreibung[237] für den Fall, dass das Überwachungswerkzeug nicht manuell installiert oder per E-Mail verschickt werden kann, nicht als

[231] o.A., Hardware Keylogger, KeeyLog, 20.01.2010, http://www.keelog.com/de/, (20.01.2010).

[232] Roggan, Präventive Online-Durchsuchungen. Überlegungen zu den Möglichkeiten einer Legalisierung im Polizei- und Geheimdienstrecht, 2008, 97, 100.

[233] Poscher, Schriftliche Stellungnahme zum BKAG Entwurf, 01.09.2008, http://www.bundestag.de/bundestag/ausschuesse/a04/anhoerungen/Anhoerung15/Stellungnahmen_SV/Stellungnahme_10.pdf, S. 21, (20.01.2010).

[234] Möstl, Schriftliche Stellungnahme zum BKAG Entwurf, 03.09.2008, http://www.bundestag.de/bundestag/ausschuesse/a04/anhoerungen/Anhoerung15/Stellungnahmen_SV/Stellungnahme_09.pdf, S.7, (20.01.2010)

[235] Dathe, Schriftliche Stellungnahme zum BKAG Entwurf, 01.09.2008, http://www.bundestag.de/bundestag/ausschuesse/a04/anhoerungen/Anhoerung15/Stellungnahmen_SV/Stellungnahme_06.pdf, S.6, (20.01.2010)

[236] Dessen Betreiber mittlerweile mit Strafermittlern zusammenarbeitet und ein Abhören ermöglicht. Brors, EU-Strafermittler nehmen Vorwürfe gegen Skype zurück, heise news, 28.02.2009, http://www.heise.de/newsticker/meldung/EU-Strafermittler-nehmen-Vorwuerfe-gegen-Skype-zurueck-202086.html, (20.01.2010).

[237] o.A., Telekommunikationsüberwachung bei Einsatz von Voice-over IP, Bayerisches Staatsministerium der Justiz, 18.05.2003, http://wiki.piratenpartei.de/wiki/images/5/54/Bayern-skype-tkue.pdf, S. 6, (20.01.2010).

mögliche Kosten in der Kostenaufstellung[238] des Justizministeriums aufgeführt werden können. Die entsprechende Ermächtigung im PAG wurde zum 01.08.2009 aufgehoben. Damit entfällt für BKA und Landeskriminalamt (LKA) momentan die Möglichkeit eines physikalischen Vorgehens, wenn sich das Informationssystem in einer geschützten Umgebung befindet.

Neben der Einbringung der Werkzeuge können bei physikalischem Zugang Kopien von den integrierten Datenträgern erstellt werden, auch wenn diese logisch, z.B. durch Verschlüsselung, geschützt wurden. Dazu müsste allerdings ausreichend Zeit zur Verfügung stehen, für eine 1 TB große SATA Festplatte wären für die Datenübertragung knapp zwei Stunden nötig. Nachträglich kann eine solche Kopie auch nicht mehr auf Manipulation überprüft werden. Hierbei könnte über Berechnung und entsprechende sichere Verwahrung eines kollisionsresistenten Hashwertes die Authentizität gesichert werden. Liegen die Daten verschlüsselt auf der Platte, kann mittels Online-Überwachung zu einem späteren Zeitpunkt der Schlüssel abgefangen und danach könnten die Daten entschlüsselt werden.[239] Ein Hardwarewerkzeug hat darüber hinaus den Vorteil, dass es mit eigenem Speicher ausgestattet werden kann und so keinen Speicherplatz belegt. Bei Personal Computern steht dieser zwar ausreichend zu Verfügung, dies ist jedoch bei modernen Informationssystemen wie Autos, tragbaren medizinischen Geräten oder Kleinstgeräten nicht unbedingt der Fall. Hier müsste entweder durch Optimierung der installierten Programme Speicherplatz gewonnen oder Daten gelöscht werden.[240]

4. Beurteilung der Einbringungsmöglichkeiten

Für die Beweiskraft lässt sich für die Einbringung zusammenfassen:

- Alle Methoden erbringen nebenbei den Beweis der Manipulierbarkeit des Informationssystems. Wird für den Zugriff die Kontrolle über oder der Zugang in das Informationssystem gekauft, wird sogar die Manipulation durch Dritte vorausgesetzt. Das Informationssystem könnte also zur Verschleierung oder mit dem Ziel, dem Besitzer zu Schaden, manipuliert worden sein. Wenn es sich nicht um eine nationale Bedrohung handelt, könnten fremde Ermittler oder Nachrichtendienste ebenfalls versucht haben, das System zu infiltrieren.
- Bei einem physischen Zugang können die Daten vor der Manipulation durch Einbringung der Werkzeuge gesichert werden.
- Bei einem physischem Zugang kann das Informationssystem zweifelsfrei identifiziert werden.[241]

---

[238] o.A., Telekommunikationsüberwachung bei Einsatz von Voice-over IP, Bayerisches Staatsministerium der Justiz, 18.05.2003, http://wiki.piratenpartei.de/wiki/images/5/54/Bayern-skype-tkue.pdf, S. 2, (20.01.2010).

[239] Siebert, Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts, 09.10.2007, http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf, S. 12, (20.01.2010).

[240] o.A., Hack a bike, CCC, 2004, http://www.ccc.de/hackabike, (20.01.2010).

[241] Ein Techniker des BKA führte zur Frage, woran man das richtige Informationsystem erkennt, aus, man erkenne dies, wenn man die Daten findet, die man suche. Hansen und Pfitzmann in Roggan, Techniken der Online-Durchsuchung: Gebrauch, Missbrauch, Empfehlungen, 2008, 137, 139.

- Bei allen Softwarewerkzeugen, die in das Informationssystem eingebracht wurden, werden Veränderungen am Informationssystem vorgenommen und damit der Datenbestand manipuliert.

III. Steuerung der Suchroutinen oder Aufzeichnungen

Unter der Steuerung des eingebrachten Werkzeugs versteht man eine gerichtete Beeinflussung des Verhaltens durch Signale von außerhalb des Werkzeugs. Hierbei können die Steuerungsimpulse auch vom infiltrierten Informationsionssystem selbst ausgelöst werden. Das Verhalten des Werkzeugs würde dann nach vorher festgelegten Regeln auf Ereignisse und Zustände reagieren. Unbekannte Zustände und Ereignisse könnten ignoriert werden oder das Werkzeug kann versuchen diese zu deuten, z.B. über die Anwendung einer Heuristik. Eine solche interne Steuerung eignet sich beispielsweise für Telekommunikationsüberwachung, weil dazu einfach die Audiodaten abgegriffen werden müssen, wenn eine entsprechende Telekommunikationssoftware aktiv ist und erkannt wird. Die Audiodaten werden innerhalb des Betriebssystems abgegriffen, noch bevor diese durch die Telekommunikationssoftware verschlüsselt bzw. nachdem sie von dieser entschlüsselt wurde.[242] Andere Ereignisse, die ein Werkzeug steuern, wären z.B. die Inbetriebnahme des Informationssystems als Startpunkt der Online-Überwachung oder der Aufbau einer Internetverbindung als Auslöser einer Datenübertragung. Steht zu keiner Zeit ein Kommunikationskanal zu einem anderen Informationssystem zur Verfügung, ist die voll automatisierte Durchführung die einzige mögliche Steuerung.

Die Steuerung von außerhalb des Informationssystems kann direkt über eine Verbindung ins Informationssystem erfolgen oder es werden Steuerungsbefehle durch Abrufen von Informationen angefordert. Hierbei können Informationen direkt, z.B. von Webservern, abgerufen, über Chatkanäle oder indirekt, z.B. durch die Überwachung von Schnittstellen, übertragen werden.[243] Dazu werden Kommunikationsschnittstellen überwacht und Versuche, eine Verbindung aufzubauen, registriert und ausgewertet. Steuerungsbefehle können beispielsweise in einer bestimmten Reihenfolge von Zugriffsversuchen auf unterschiedliche Schnittstellen codiert werden.[244] Die einzelnen Verbindungsversuche sind dabei unauffällig, weil jedes Informationssystem im Internet ständig solchen Versuchen ausgesetzt ist.

Für all diese Steuerungen von außerhalb muss dem Werkzeug allerdings ein Kommunikationskanal zur Verfügung stehen. Um eine Übernahme der eingesetzten Werkzeuge durch Dritte zu verhindern,[245] sollten Daten für die Steuerung ausreichend, z.B. über Verwendung einer sicheren Signatur und der Überprüfung dieser durch das angesprochene Werkzeug,

---

[242] Jäger, Blog Archive: Updated SkypeTrojan version available now, Megapanzer, 06.10.2009, http://www.megapanzer.com/2009/10/06/updated-skypetrojan-version-available-now/, (20.01.2010).

[243] Jäger, Confliker – das größte Botnet aller Zeiten, TecChannel, 05.01.2010, http://www.tecchannel.de/sicherheit/spam/1986704/conficker_das_groesste_botnetz_aller_zeiten/, (20.01.2010).

[244] Kunz, Horch, wer kommt von draußen rein..., C't magazin für computertechnik 2001, 206, 206 ff.

[245] Dies soll über die Designkriterien sichergestellt werden. Stawowy, Fragenkatalog des Bundesministeriums der Justiz, netzpolitik.org, 22.09.2007, http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf, S. 21, (20.01.2010).

eingesetzt werden.[246] Damit könnten die Anforderungen nach § 20k Abs. 2 S. 2 1. BKAG oder § 15b Abs. 2 S. 2 HSOG zur Sicherung gegen unbefugtes Nutzen umgesetzt werden. Sollen die Werkzeuge gezielt gesteuert werden, ist der Steuerungsprozess mit der Ausleitung der Daten zu verbinden und entsprechend zu schachteln.

Alle Vorgänge führen zu einem Ressourcenverzehr des Informationssystems, die dem Anwender dann nicht mehr zur Verfügung stehen. Die Belastung kann theoretisch vom Anwender bemerkt werden, ist aber im Vergleich zum Ressourcenverbrauch bei der Ausleitung unwahrscheinlich. Wird dagegen die Suche und Überwachung automatisiert, kann dies zu einer Art Blindheit führen. Da nur im Vorfeld nach erwarteten Daten gesucht werden kann. Dies kann durch flexible Ansätze, wie sie z.B. im maschinellen Lernen eingesetzt, ausgeglichen werden, um so auf unbekannte Ereignisse und Konstellationen reagieren zu können. Der für die Bewertung der unbekannten Ereignisse nötige BIAS kann sich auch verzerrend auf die bekannten Ereignisse auswirken.

Nach § 20k Abs. 2 S. 1 Nr. 1 BKAG, § 20l Abs. 2 S. 1 Nr. 1 BKAG und § 15b Abs. 2 S. 1 Nr. 1 HSOG werden technische Beschränkungen gefordert, die nur unerlässliche Manipulationen am Informationssystem zulassen. Dies spricht für einen hohen Automatisierungsgrad, der vor dem Einsatz entsprechend getestet wurde. Werden Informationen an den Schnittstellen des Informationssystems durch Hardwarewerkzeuge abgegriffen, ist eine vollständige technische Beschränkung möglich, wenn diese Werkzeuge über keine Möglichkeit verfügen, Informationen an das Informationssystem zu senden.

§ 20k BKAG Verdeckter Eingriff in informationstechnische Systeme

[...]

(2) Es ist technisch sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und

2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

[...]

[246] Jäger, Confliker – das größte Botnet aller Zeiten, TecChannel, 05.01.2010, http://www.tecchannel.de/sicherheit/spam/1986704/conficker_das_groesste_botnetz_aller_zeiten/, (20.01.2010).

§ 15bHSOG Telekommunikationsüberwachung an informationstechnischen Systemen

[...]

(2) Es ist technisch sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und

2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen.

[...]

Das PAG sieht dagegen in § 34d Abs. 1 S. 3 PAG auch die Löschung[247] von Daten vor, wenn eine gegenwärtige Gefahr für Leib oder Leben nicht anders abgewehrt werden kann. Technisch können, durch Löschen von Daten, neben der Möglichkeit Informationen zu löschen, auch Maschinen gesteuert werden, indem z.B. das Programm für die Steuerung komplett gelöscht oder durch Löschen einzelner Befehle das Programm damit in einen Fehlerzustand gesetzt wird. Erfolgt diese Abwägung erst nach dem Einbringen des Werkzeugs, muss dazu die Ausleitung der Daten nach außen und die Steuerung von außen erfolgen.

IV. Ausleitung gefundener Daten

Wurden Daten erhoben, müssen diese zur Klassifikation und Bewertung ausgeleitet werden. In Abhängigkeit von der Einbringung und der Vernetzung des Informationssystems kann die Ausleitung unterschiedlich organisiert werden. Besteht zumindest zeitweise ein Kommunikationskanal, können die Daten selbstständig auf einen vorher festgelegten Ort (Drop-Zone), z.B. ein Server im Internet, transferiert oder vom Informationssystem heruntergeladen werden.[248] Dies ist bei einer Telekommunikationsüberwachung gegeben, bei der auch gleichzeitig immer Datenverkehr besteht, der zur Tarnung der Datenausleitung beiträgt. Damit die Daten bei der Übertragung nicht abgegriffen oder manipuliert werden können, sollten sie vor der Ausleitung verschlüsselt[249] und signiert werden. Damit die Verschlüsselung und Signierung nicht kompromittiert werden kann, ist die exklusive Kontrolle über das zu verschlüsselnde System notwendig. Dies lässt sich nur mit sehr gut manipulationsgeschützten Hardwarewerkzeugen, die mit eigenem Speicher ausgerüstet sind, erreichen. [250]

Besteht keine dauerhafte Kommunikationsverbindung nach außerhalb, müssen die gefundenen oder aufgezeichneten Daten zwischengespeichert werden. Da sich verschlüsselte Daten wegen ihrer internen Struktur leicht auf Datenträgern auffinden lassen, sollten die Daten zu-

[247] Inwieweit Daten überhaupt gelöscht werden können vgl. Teil 3, A.

[248] Stawowy, Fragenkatalog des Bundesministeriums der Justiz, netzpolitik.org, 22.09.2007, http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf, S. 21, (20.01.2010).

[249] o.A., Telekommunikationsüberwachung bei Einsatz von Voice-over IP, Bayerisches Staatsministerium der Justiz, 18.05.2003, http://wiki.piratenpartei.de/wiki/images/5/54/Bayern-skype-tkue.pdf, S. 62, (20.01.2010).

[250] Hansen und Pfitzmann in Roggan, Techniken der Online-Durchsuchung: Gebrauch, Missbrauch, Empfehlungen, 2008, 137, 138.

sätzlich mittels Steganographie versteckt werden. Dazu werden z.B. die Daten als Rauschen in Mediendaten eingebunden.[251] Die Übertragungsdauer ist, neben der Größe der zu übertragenden Daten, von der zur Verfügung stehenden Bandbreite abhängig und kann sich über mehrere Tage erstrecken.[252] Besteht kein eigener Kommunikationskanal zu einem anderen Informationssystem, können die Daten auch über die physische Abstrahlung ausgeleitet werden, dazu würde es ausreichen, die Daten mehrfach über den systeminternen Rechnerbus zu leiten.[253] Sie können auch lokal gespeichert und über einen physikalischen Zugriff abgeholt werden.

Mit steigendem Datenvolumen wird eine Entdeckung der Maßnahme wahrscheinlicher.[254] Wird die Ausleitung entdeckt, ist davon auszugehen, dass der Anwender versuchen wird, die Übertragung abzubrechen und so geht ein Teil der ermittelten Informationen verloren.

Werden die Daten zu Sammelstellen im Internet transferiert, könnten diese angegriffen werden. Bei Erfolg eines solchen Angriffs, könnten die dort gelagerten Daten zerstört, manipuliert oder ergänzt werden. Sind die Daten signiert und verschlüsselt worden, sind dazu Kenntnisse über die verwendeten Schlüssel nötig. Diese könnten bei Entdeckung aus den eingesetzten Werkzeugen extrahiert werden. § 20k Abs. 2 S. 3 BKAG, sieht Schutzmechanismen gegen Veränderung, Löschung und unbefugter Kenntnisnahme vor. Neben dem Schutz vor externen Gefahren, gehört dazu auch der Schutz vor internen Zugriffen durch eine entsprechende Organisation.

V. Löschung vom Zielsystem

Nach der Übertragung der gefundenen Daten sollen alle eingesetzten Werkzeuge restlos gelöscht und somit die Spuren des Eingriffs verwischt werden.[255] § 20k Abs. 2 S. 1 Nr. 2 BKAG, § 20l Abs. 2 S. 2 i.V.m. § 20k Abs. 2 S. 1 Nr. 2 BKAG und § 15b Abs. 2 S. 1 Nr. 2 HSOG sehen ein automatisiertes Löschen der Werkzeuge vor, soweit dies möglich ist. Das Löschen aller Spuren ist mit dem perfekt digitalen „Verbrechen“ vergleichbar und wird mit steigender Komplexität der Werkzeuge und Dauer des verdeckten Eingriffs schwerer bis unmöglich. Wurde eines oder mehrere der eingesetzten Werkzeuge bei einer Datensicherung, z.B. auf einer DVD,[256] gesichert, ist ein Löschen nur noch über ein physikalisches Zerstören des Datenträgers möglich.[257] Wird der verdeckte Zugriff über das Einbringen von Hardware an den Schnittstellen des Informationssystems durchgeführt und speichern diese die gefundenen In-

[251] Hansen und Pfitzmann in Roggan, Techniken der Online-Durchsuchung: Gebrauch, Missbrauch, Empfehlungen, 2008, 137, 139.

[252] Stawowy, Fragenkatalog des Bundesministeriums der Justiz, netzpolitik.org, 22.09.2007, http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf, S. 5, (20.01.2010).

[253] Hansen und Pfitzmann in Roggan, Techniken der Online-Durchsuchung: Gebrauch, Missbrauch, Empfehlungen, 2008, 137, 136.

[254] Der US-Angestellte, auf dessen PC Viren belastendes Material hinterlegt wurde, fiel der IT-Abteilung durch einen vierfach höheren Datentransfer auf. cis, Virenattacke mit Kinderpornos, SPON, 10.11.2009, http://www.spiegel.de/netzwelt/web/0,1518,660199,00.html, (01.06.2010).

[255] Ziercke, Pro Online-Durchsuchung, Informatik-Spektrum 2008, 62, 64.

[256] So könnten die Werkzeuge komplett oder teilweise auf anderer Informationssysteme übertragen werden.

[257] Siebert, Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts, 09.10.2007, http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf, S. 2, (20.01.2010).

formationen auf eigenen Speichermedien oder leiten die Daten sofort aus, erfolgt eine vollständige Löschung der Werkzeuge durch Entfernen der Werkzeuge.

Durch das Löschen der Werkzeuge wird die Revisionsfähigkeit erheblich eingeschränkt. Sind die Werkzeuge überschrieben, können im Einzelfall oder in besonderer Konstellation auftretende Wechselwirkungen[258] mit anderen Programmen nicht mehr nachvollzogen werden. Ebenso entfällt die Möglichkeit, die eingesetzten Werkzeuge zu identifizieren und deren Funktionstüchtigkeit zu prüfen. Gelingt eine vollständige Entfernung aller Spuren, ist auf dem betroffenen System der verdeckte Zugriff nicht mehr nachzuweisen, dies ist ein Beleg, dass das System, ohne Datenspuren zu hinterlassen, kontrolliert werden kann.

Neben den Veränderungen am Datenbestand, werden aber noch weitere Veränderungen vorgenommen. Dazu gehört z.B. das Abgreifen und Ausleiten von Passwörtern, dabei werden keine Daten verändert, aber die Passwörter verlieren ihre Schutzfunktion. Um dies rückgängig zu machen, sind neue Passwörter zu vergeben, dies ist nur unter Hinzunahme des Anwenders möglich.[259]

D. Dokumentation

Wie bereits in 1 ausgeführt, kommt der Dokumentation eine Schlüsselrolle in Bezug auf den Beweiswert der ermittelten Daten zu. Nur bei ausreichender Dokumentation können die durchgeführten Schritte lückenlos nachvollzogen und damit von Sachverständigen bewertet werden. Da die ermittelten Daten erst nach der Ausleitung gesichtet werden können, muss die Dokumentation so ausgelegt sein, dass alle durch die Werkzeuge ausgeführten Aktionen, den ausgeleiteten Daten zugeordnet werden können. Bei automatisierten Softwarewerkzeugen entfällt zusätzlich die Möglichkeit, Zeugen hinzuzuziehen, da die Arbeitsweise des Werkzeugs nicht beobachtet werden kann.

Nach § 34d Abs. 1 S. 7 PAG sind verdeckte Zugriffe und das Löschen von Daten zu dokumentieren. § 20k Abs. 3 S. 1 und § 20l Abs. 3 BKAG sowie § 15 b Abs. 3 S. 1 HSOG schreiben die einzeln zu protokollierenden Punkte vor. Wird diese Aufzählung als abschließend angesehen, enthält die Dokumentation nicht den nötigen Informationswert.

§ 20k BKAG Verdeckter Eingriff in informationstechnische Systeme

[...]

(3) Bei jedem Einsatz des technischen Mittels sind zu protokollieren

1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,

2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,

3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und

[258] Freiling, Schriftliche Stellungnahme zum Fragenkatalog Verfassungsbeschwerden, 27.09.2007, https://pi1.informatik.uni-mannheim.de/filepool/publications/stellungnahme-online-durchsuchung.pdf, S. 1, (20.01.2010).

[259] Hansen und Pfitzmann in Roggan, Techniken der Online-Durchsuchung: Gebrauch, Missbrauch, Empfehlungen, 2008, 137, 169.

4. die Organisationseinheit, die die Maßnahme durchführt,

Die Protokolldaten dürfen nur verwendet werden, um dem Betroffenen oder einer dazu befugten öffentlichen Stelle die Prüfung zu ermöglichen, ob die Maßnahme nach Absatz 1 rechtmäßig durchgeführt worden ist. Sie sind bis zum Ablauf des auf die Speicherung folgenden Kalenderjahres aufzubewahren und sodann automatisiert zu löschen, es sei denn, dass sie für den in Satz 2 genannten Zweck noch erforderlich sind.

[...]

§ 20l BKAG Überwachung der Telekommunikation

[...]

(3) Bei jedem Einsatz des technischen Mittels sind zu protokollieren

1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,

2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,

3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und

4. die Organisationseinheit, die die Maßnahme durchführt.

Die Protokolldaten dürfen nur verwendet werden, um der betroffenen Person oder einer hierzu befugten öffentlichen Stelle die Prüfung zu ermöglichen, ob die Maßnahme nach Absatz 1 rechtmäßig durchgeführt worden ist. Sie sind bis zum Ablauf des auf die Speicherung folgenden Kalenderjahres aufzubewahren und sodann automatisiert zu löschen, es sei denn, dass sie für den in Satz 2 genannten Zweck noch erforderlich sind.

[...]

§ 15b HSOG Telekommunikationsüberwachung an informationstechnischen Systemen

[...]

(3) Bei jedem Einsatz des technischen Mittels sind zum Zwecke der Datenschutzkontrolle und der Beweissicherung zu protokollieren:

1. die Bezeichnung des technischen Mittels und der Zeitraum seines Einsatzes,

2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,

3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und

4. die Organisationseinheit, die die Maßnahme durchführt.

Die Protokolldaten dürfen nur verwendet werden, um der betroffenen Person oder einer hierzu befugten öffentlichen Stelle oder einem Gericht die Prüfung zu ermöglichen, ob die Maßnahme nach Abs. 1 rechtmäßig durchgeführt worden ist. Sie sind bis zum Ablauf des auf die Speicherung folgenden Kalenderjahres aufzubewahren und sodann automatisiert zu löschen, wenn sie für den in Satz 2 genannten Zweck nicht mehr erforderlich sind.

[...]

I. Online-Durchsuchung

Ziel der Online-Durchsuchung ist es, den aktuellen Zustand eines Informationssystems festzustellen. Dazu kann man auf dem Informationssystem gezieltes Suchen durchführen. Hier werden auf dem Informationssystem gespeicherte Daten sowie Daten über das Informationssystem ermittelt.[260] Um diesen Zeitpunktbezug zu ermöglichen, müsste das Informationssystem in einem definierten Zustand eingefroren werden, so dass der Anwender keine Veränderungen mehr am System durchführen kann. Dies würde aber die Heimlichkeit des Zugriffs aufheben und so ist anzunehmen, dass alle möglichen Veränderungen ignoriert werden. Die gefundenen Daten können damit ständigen Veränderungen unterworfen sein und können sich so auch während oder wegen der Datenerhebung ändern.[261] Eine Revision der Erkenntnisse oder die direkte Zuordnung der gefundenen Daten zu einem Anwender ist nicht möglich.[262] Zusätzlich zu den bestehenden Daten, lassen sich auch flüchtige Inhalte, z.B. aus dem Hauptspeicher, gewinnen. Die Datenzugriffe bei der Online-Durchsuchung können Einträge in die Protokolldatei zur Folge haben und so die Informationen überschreiben, ob ein Anwender die fraglichen Daten überhaupt kennt oder genutzt hat. Für die Identifikation der Datenquellen muss es möglich sein, zusätzliche Ermittlungen durchführen zu können. Stammen die Daten beispielsweise von einem Sensor, z.B. Scanner oder Kamera, können diese zu einem späteren Zeitpunkt durch Multimedia-Forensik einer Quelle zugeordnet und so evtl. durch zusätzliche Spuren auf den Eingabesensoren einem Anwender zugeordnet werden. Über solche Untersuchungen lassen sich gegebenenfalls auch Manipulationen erkennen.[263]

Unabhängig von dem, wegen der fehlenden, exklusiven Kontrolle über das System bestehenden Einschränkungen bezüglich des Beweiswerts, erlöscht der Informationswert der erhobenen Daten nicht.[264]

II. Online-Überwachung

Bei der Online-Überwachung sollen Nutzeraktivitäten über einen festen Zeitraum erfasst werden. Zusätzlich zu den Funktionen der Online-Durchsicht werden dazu Änderungen an den Daten erfasst.[265] Fragile, temporäre Daten sowie Änderungen durch den Anwender sollten mit Zeitbezug erfasst werden, so kann man auch die Entwicklung der Daten erfassen. Die Manipulation wird aufgezeichnet. Dadurch verliert der Anwender die Möglichkeit, Datenspuren zu manipulieren. Da ebenfalls keine exklusive Kontrolle über das Informationssystem

---

[260] Stawowy, Fragenkatalog des Bundesministeriums der Justiz, netzpolitik.org, 22.09.2007, http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf, S. 6, (20.01.2010).

[261] Siebert, Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts, 09.10.2007, http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf, S. 12, (20.01.2010).

[262] Freiling, Schriftliche Stellungnahme zum Fragenkatalog Verfassungsbeschwerden, 27.09.2007, https://pi1.informatik.uni-mannheim.de/filepool/publications/stellungnahme-online-durchsuchung.pdf, S. 6, (20.01.2010).

[263] Böhme u.a., Multimedia-forensik als Teildisziplin der digitalen Forensik, 2009, http://www1.inf.tu-dresden.de/~rb21/publications/BFGK2009_MultimediaForensik_GI.pdf, S. 6, (20.01.2010).

[264] BVerfG, Urt. v. 27.02.2008, Az.1 BvR 370/07 Rz. 223, Homepage: http://www.bundesverfassungsgericht.de/ (01.02.2010).

[265] Stawowy, Fragenkatalog des Bundesministeriums der Justiz, netzpolitik.org, 22.09.2007, http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf, S. 6, (20.01.2010).

besteht, sind auch hier die Daten nur durch zusätzliche Untersuchungen zurechenbar. Durch die Aufzeichnung der Eingabe und der Möglichkeit diese mit Zeitinformationen zu kombinieren, bestehen zusätzliche Möglichkeiten, den Anwender über dessen Gewohnheiten zu identifizieren. Dazu wird beispielsweise die Latenz zwischen den einzelne Tastaturanschlägen ausgewertet.[266] Besitzt das Informationssystem optische oder akustische Sensoren, kann auch versucht werden, den Anwender darüber zu identifizieren.[267]

Die durch die Online-Überwachung gewonnenen Erkenntnisse, können bei einer späteren Auswertung von Datenträgern[268] zur Hypothesenerstellung verwendet werden und so die Ermittlungen erheblich vereinfachen.

E. Telekommunikationsüberwachung

Verdeckte Zugriffe zur Telekommunikationsüberwachung (vom Bundesministerium des Innern (BMI) auch als Quellen-Telekommunikationsüberwachung bezeichnet) sind nach § 20l Abs 2 S. 1 Nr. 1 BKAG sowie nach § 15b Abs. 1 S. 1 Nr. 1 HSOG nur erlaubt, wenn technisch sichergestellt ist, dass nur die laufende Telekommunikation erfasst wird. Die Kommunikationsteilnehmer können, ausreichende Qualität vorausgesetzt, durch analoge Forensik anhand ihrer Stimme identifiziert oder verifiziert werden.[269] Erfolgt die Kommunikation mittels Textnachrichten, können die Teilnehmer, wie bei der Online-Überwachung, ermittelt werden, soweit die zusätzlichen Zeitinformationen zur Verfügung stehen. Erfolgt die Eingabe der Textnachrichten nicht direkt in den Kommunikationskanal, ist die Eingabe allerdings nicht Teil der Telekommunikation.[270]

F. Verwertungsverbote

Verwertungsverbote führen zu einem Erlöschen der Beweiskraft des gefundenen Beweismittels, da es nicht mehr im Rahmen eines Beweises verwendet werden darf. Bei verdeckten Eingriffen in informationstechnische Systeme geht der Verwertung ein Erhebungsverbot voraus. Damit das Erhebungsverbot greift, müssen beispielsweise tatsächliche Anhaltspunkte vorliegen, dass durch die Maßnahme allein Erkenntnisse aus dem Intimbereich erlangt werden (§ 20k Abs. 7 S. 1 BKAG, § 20l Abs. 6 S. 1 BKAG, § 15b Abs. 5 1. HS i.V.m. § 15 Abs. 4 S.4 HSOG). Zusätzlich ist, soweit technisch möglich, die Datenerhebung auf Daten aus dem Kernbereich privater Lebensgestaltung zu verhindern, § 20k Abs. 7 S. 2 BKAG. Da sich Daten nicht ohne eine Durchsicht verlässlich den verschiedenen Sphären[271] zuordnen lassen, ist davon auszugehen, dass eine Bewertung erst nach dem Erfassen und Ausleiten der Daten durchgeführt werden kann. Die Vielzahl von möglichen verwendeten Sprachen, Kodie-

[266] Joyce und Gupta, Identity authentication based on keystroke latencies, Commun. ACM 1990, 168, 168.
[267] Siebert, Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts, 09.10.2007, http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf, S. 16, (20.01.2010).
[268] Die nach Möglichkeit vor der Einbringung zur Beweissicherung kopiert wurden.
[269] Widmaier, Münchener Anwaltshandbuch Strafverteidigung, 2006, § 77 Rn. 3.
[270] BVerfG, Urt. v. 16.06.2009, Az.2 BvR 902/06 Rz. 45, Homepage: http://www.bundesverfassungsgericht.de (01.02.2010).
[271] Geschäftssphäre, Individualsphäre und Intimsphäre.

rungen und Dateiformaten machen eine verlässliche, automatisierte Klassifizierung in verwertbare und unverwertbare Daten nahezu unmöglich. Daneben könnten Daten, z.B. über einen tagebuchartigen Prolog, als Daten aus der Intimsphäre getarnt werden.[272] Zusätzlich ist die Klassifizierung erschwert, da Art. 34d Abs. 5 S. 3 Nr. 3 PAG die Verwendung von Daten, den Kernbereich privater Lebensgestaltung betreffend und Daten, die Berufgeheimnisträgern zuzuordnen sind, nur erlaubt, wenn diese Bezug zu den abzuwehrenden Gefahren haben und bei der Durchsicht der Daten entweder keine Anhaltspunkte vorliegen (Art. 34d Abs. 4 S. 1 1. HS PAG) oder ein zuständiger Richter die Entscheidung für eine weitere Verwendung getroffen hat (Art. 34d Abs. 4 S. 3 2. Alt. PAG). Besteht jedoch kein unmittelbarer Bezug oder haben nach Art. 34d Abs. 5 S. 3 Nr. 2 PAG die Voraussetzungen für die Erhebung nicht vorgelegen oder betreffen diese Inhalte, für die ein Zeugnisverweigerungsrecht nach Art. 34d Abs. 5 S. 3 Nr. 3 PAG besteht, dürfen die Daten nicht verwendet werden.

Nach § 20k Abs. 7 S. 5 BKAG und § 20l Abs. 6 S. 6 BKAG besteht ein Verwertungsverbot für Daten, die den Kernbereich privater Lebensgestaltung betreffen. Nach § 15b Abs. 5 1. HS i.V.m. § 15 Abs. 5 S.8 HSOG entscheidet das zuständige Gericht über die Verwertbarkeit der ermittelten Daten.

§ 20k BKAG Verdeckter Eingriff in informationstechnische Systeme

[...]

(7) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Soweit möglich, ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Erhobene Daten sind unter der Sachleitung des anordnenden Gerichts nach Absatz 5 unverzüglich vom Datenschutzbeauftragten des Bundeskriminalamtes und zwei weiteren Bediensteten des Bundeskriminalamtes, von denen einer die Befähigung zum Richteramt hat, auf kernbereichsrelevante Inhalte durchzusehen. Der Datenschutzbeauftragte ist bei Ausübung dieser Tätigkeit weisungsfrei und darf deswegen nicht benachteiligt werden (§ 4f Abs. 3 des Bundesdatenschutzgesetzes). Daten, die den Kernbereich privater Lebensgestaltung betreffen, dürfen nicht verwertet werden und sind unverzüglich zu löschen. Die Tatsachen der Erfassung der Daten und der Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.

§ 20l BKAG Überwachung der Telekommunikation

[...]

(6) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach den Absätzen 1 und 2 allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Soweit im Rahmen von Maßnahmen nach den Absätzen 1 und 2 neben einer automatischen Aufzeichnung eine unmittelbare Kenntnisnahme erfolgt, ist die Maßnahme unverzüglich zu unterbrechen, soweit sich während der Überwachung tatsächliche Anhaltspunkte dafür ergeben, dass Inhalte, die

[272] Siebert, Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts, 09.10.2007, http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf, S. 16, (20.01.2010).

dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Bestehen insoweit Zweifel, darf nur eine automatische Aufzeichnung fortgesetzt werden. Automatische Aufzeichnungen nach Satz 3 sind unverzüglich dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit oder Löschung der Daten vorzulegen. Ist die Maßnahme nach Satz 2 unterbrochen worden, so darf sie für den Fall, dass sie nicht nach Satz 1 unzulässig ist, fortgeführt werden. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach den Absätzen 1 und 2 erlangt worden sind, dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsachen der Erfassung der Daten und der Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.

Art. 34d PAG Verdeckter Zugriff auf informationstechnische Systeme

[...]

(4) [1] Bestehen bei der Durchsicht der Daten Anhaltspunkte dafür, dass Daten

1. dem Kernbereich privater Lebensgestaltung zuzuordnen sind oder

2. Inhalte betreffen, über die das Zeugnis als Geistlicher, Verteidiger, Rechtsanwalt, Arzt, Berater für Fragen der Betäubungsmittelabhängigkeit, Psychologischer Psychotherapeut oder Kinder- und Jugendlichenpsychotherapeut nach §§ 53 , 53a StPO verweigert werden könnte, oder

3. einem Vertrauensverhältnis mit anderen Berufsgeheimnisträgern zuzuordnen sind,

sind diese unverzüglich zu löschen oder dem für die Anordnung nach Abs. 1 zuständigen Richter zur Entscheidung über ihre weitere Verwendung vorzulegen. [2] Bei Gefahr im Verzug kann die Entscheidung auch eine in Art. 33 Abs. 5 Satz 1 genannte Stelle treffen; in diesem Fall ist eine richterliche Entscheidung unverzüglich nachzuholen. [3] Die Löschung ist zu dokumentieren.

[...]

Art. 34d PAG Verdeckter Zugriff auf informationstechnische Systeme

[...]

(5) [1] Die durch eine Maßnahme nach den Abs. 1 und 2 erlangten personenbezogenen Daten sind besonders zu kennzeichnen. [2] Sie dürfen nur zu den Zwecken verwendet werden, zu denen sie erhoben wurden. [3] Daten, bei denen sich nach der Auswertung herausstellt, dass

1. die Voraussetzungen für ihre Erhebung nicht vorgelegen haben oder

2. sie Inhalte betreffen, über die das Zeugnis als Geistlicher, Verteidiger, Rechtsanwalt, Arzt, Berater für Fragen der Betäubungsmittelabhängigkeit, Psychologischer Psychotherapeut oder Kinder- und Jugendlichenpsychotherapeut nach §§ 53 , 53a StPO verweigert werden könnte, oder

3. sie dem Kernbereich privater Lebensgestaltung oder einem Vertrauensverhältnis mit anderen Berufsgeheimnisträgern zuzuordnen sind und keinen unmittelbaren Bezug zu den in Abs. 1 Satz 1 Nr. 1 genannten Gefahren haben,

dürfen nicht verwendet werden. [4] Dies gilt nicht, wenn ihre Verwendung zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist und Daten im Sinn der Nr. 2 oder 3 nicht betroffen sind. [5] In diesen Fällen ist eine richterliche Entscheidung über die Zulässigkeit der Verwendung unverzüglich nachzuholen; Abs. 3 Satz 2 findet entsprechende Anwendung.

[...]

§ 15b HSOG Telekommunikationsüberwachung an informationstechnischen Systemen

[...]

(5) § 15 Abs. 4 Satz 2 bis 5 und Abs. 5 gilt entsprechend mit der Maßgabe, dass das informationstechnische System, in das zur Datenerhebung eingegriffen werden soll, in der Anordnung möglichst genau zu bezeichnen ist.

§ 15 HSOG Datenerhebung durch Observation und Einsatz technischer Mittel

[...]

(4) In oder aus Wohnungen können die Polizeibehörden ohne Kenntnis der betroffenen Person Daten nur erheben, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich ist. Ein Eingriff mit technischen Mitteln ist nicht zulässig, soweit keine Auskunftspflicht der betroffenen Person nach § 12 Abs. 2 besteht. Das Verbot nach Satz 2 gilt auch, wenn durch eine gegen einen Dritten gerichtete Maßnahme Erkenntnisse erlangt würden, die nicht der Auskunftspflicht nach § 12 Abs. 2 unterliegen. Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Bestehen insoweit Zweifel, darf die Datenerhebung ausschließlich durch eine automatische Aufzeichnung erfolgen und fortgesetzt werden. § 38 Abs. 7 gilt entsprechend, soweit die Datenerhebung nicht mit technischen Mitteln erfolgt.

[...]

G. Kritische Würdigung

Die Online-Durchsuchung/Überwachung werden als Ultima-Ratio-Maßnahmen[273] bezeichnet. Sie sollen nur dann zum Einsatz kommen, wenn andere Ermittlungsmaßnahmen keinen Erfolg versprechen.[274] Liegt das Versagen der sonstigen Ermittlungsmaßnahmen an einem hö-

[273] o.A., Bilanz der Online-Durchsuchung, Drucksache 17/1814, 21.05.2010, http://dip21.bundestag.de/dip21/btd/17/018/1701814.pdf, S. 2, (10.07.2010).

[274] Bei den Gefahren, die zur Abwehr eine der heimlichen Maßnahmen rechtfertigen, wird es sich meist, solang es nicht um einen Angriff auf die IT-Infrastruktur geht, nicht um ein rein virtuelles Vorgehen handeln. § 20k Abs. 1 S. 1 Nr. 1 BKAG setzt beispielsweise eine Gefährdung von Leib, Leben, Freiheit einer Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt, voraus. Diese Voraussetzungen werden beispielsweise die Vorbereitung des rein virtuellen Abgreifens von Bankdaten in der Regel nicht erfüllen und so nicht zu einem heimlichen Eindringen in eine sogenannten "`Drop Zo-

heren konspirativen Verhalten des von der Maßnahme Betroffenen, sind Schutzmaßnahmen oder gar die Bereitstellung eines Honypots[275] zumindest nicht auszuschließen. Daraus ergibt sich die Notwendigkeit, immer Hilfstatsachen auszuwerten. In Abhängigkeit des gewählten Vorgehens bei der Maßnahme, kommt es zu den beschriebenen unterschiedlichen Manipulationsmöglichkeiten bei den einzelnen Schritten. Dabei steigt die Wahrscheinlichkeit einer Manipulation in gleicher Größenordnung wie die Beweiskraftreduktion bei der Indizienkette. Die Wahrscheinlichkeit einer Fremdkontrolle des Informationssystems ist dabei indirekt abhängig von den ergriffenen Sicherheitsmaßnahmen am Informationssystem. Der potentielle Beweiswert steigt also mit wachsender Sicherheit und damit höherem Aufwand bei der Infiltration.[276]

Die Zurechenbarkeit der Daten ist nur mittels zusätzlichen Erkenntnissen möglich, die, wenn sie einer Unsicherheit unterliegen, gegebenenfalls den Beweiswert reduzieren.

Da noch keine Maßnahme durch das BKA durchgeführt wurde, liegen auch noch keine Erkenntnisse über die gewonnenen Beweise vor. Für eine bessere Beurteilung ist deswegen die Verwendung von Ergebnissen von durchgeführten Maßnahmen in einem Gerichtsverfahren abzuwarten.

Teil 7: Ausblick

Nach der Betrachtung der Erhebungsmethode muss sich bei der Beweisbewertung die Untersuchung des einzelnen Indizes anschließen. Folgt man dem Theorem von Bayes sind dafür repräsentative Erhebungen nötig, die das allgemeine Auftreten des Indizes und das Auftreten in Kombination mit einem Sachverhalt betrachten. Hierbei kann, wie am Beispiel des Fingerabdrucks[277] deutlich wird, eine ständige Verschiebung des Beweiswertes eintreten und so müssen immer wieder aktuelle Erkenntnisse berücksichtigt werden. Wurde beispielsweise

ne'" (so werden Abwurfstellen im Internet bezeichnet, auf denen z.B. von Schadsoftware geklaute Kreditkartendaten zur Abholung zwischengespeichert werden) ermächtigen.

[275] Auf die "`normalen'" Testmethoden von Schadsoftware auf Honypots, kann dabei nicht zurückgegriffen werden, da ein solcher Honypot auf den Zugriff von einzelnen Ermittlern und nicht auf das Abfischen von allgemeiner Schadsoftware ausgelegt ist. Krawetz, Anti-Honeypot Technology, IEEE Security and Privacy 2004, 76, 77.

[276] Geschonneck befürchtet eine Beeinflussung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) durch das (BKA), damit diese Sicherheitslücken, die das (BKA) ausnützen möchte, zurückhält und es so zu einer Reduktion der technischen Sicherheit in Deutschland kommt. Geschonneck, Onlinedurchsuchung: ich jetzt auch mal [update], 07.10.2007, http://computer-forensik.org/2007/10/07/onlinedurchsuchung-ich-jetzt-auch-mal, (20.01.2010).

[277] Durch die Verwendung von Fingerabdrücken in der Zugangskontrolle, Bezahlsystemen und als Identifikationsmerkmal in Ausweisen, hat sich das Wissen über die Reproduktion einer Fingerabdruckfälschungen verbreitet. Im Rahmen der politischen Auseinandersetzung mit dem Thema wurde eine Attrappe eines Fingerabdrucks von dem zu dieser Zeit amtierenden Innenministers bundesweit verbreitet. Damit wurde die Beweiskraft dieses Fingerabdrucks deutlich reduziert. Starbug, Wie können Fingerabdrücke nachgebildet werden?, CCC, 09.10.2004, http://dasalte.ccc.de/biometrie/fingerabdruck_kopieren, (20.01.2010)

als Indiz eine IP-Adressen erhoben, muss neben dem Erhebungsprozess[278] die allgemeine Aussagekraft beurteilt werden. Die IP-Adresse allein kann dynamischer zugeteilt werden. In diesem Fall wären zusätzlich zur IP-Adresse noch die Einbeziehung eines Zeitstempels nötig.[279] Daneben besteht noch die Möglichkeit, die Adresse zu „entführen“ oder durch einen Fehler in der Protokollierung falsch zuzuordnen.[280] Die gezielte Entführung ist zwar nur mit erheblichem Aufwand und ausreichendem Fachwissen möglich, macht aber deutlich, dass es zumindest möglich ist und zur Bewertung zusätzliche Kenntnisse[281] über das Auftreten der IP-Adressenfälschung nötig sind. Auch hier kann es über die Zeit zu erheblichen Verschiebungen kommen. Stehen Dienstleistungen oder fertige Programme mit dieser Funktion zur Verfügung und kommt es so zu einer häufigen Verschleierung, verliert die IP-Adresse auch in Kombination mit einem Zeitstempel an Beweiskraft.

[278] Der Staatsanwaltschaft Duisburg unterlief bei einer Anschriftenabfrage bei einem Provider ein Fehler bei der Nutzerkennung und bekam so eine „falsche“ Anschrift übermittelt. LG Stuttgart, Urt. v. 16.07.2007, Az. 17 O 243/07, S. 2, Homepage: http//medien-internet-und-recht.de (14.07.2010).

[279] Schmitt, IP-Adressen nur mit sicherem Routing eindeutig, heise news, 13.05.2010, http://www.heise.de/newsticker/meldung/IP-Adressen-nur-mit-sicherem-Routing-eindeutig-999457.html, (13.05.2010).

[280] Endres, Beweismittel IP-Adresse fragwürdig, heise Netze, 19.04.2010, http://www.heise.de/netze/meldung/Beweismittel-IP-Adresse-fragwuerdig-980685.html, (13.05.2010).

[281] In diesem Fall ob es sich nur um eine bloße Möglichkeit handelt oder ob es ein realistisch anzunehmendes Szenario ist.

Literatur

Bach, Klaus Dieter u.a., Tabellenbuch Kommunikationselektronik, 4, 1995.

Bachfeld, Daniel, 1&1 will gegen Bot-Netze vorgehen, heise security, 10.02.2009, http://www.heise.de/security/meldung/1-1-will-gegen-Bot-Netze-vorgehen-193968.html, (20.01.2010).

Bachfeld, Daniel, Trojaner verschlüsselt Daten und Dokumente [Update], heise news, 14.05.2005 (20.01.2010).

Bager, Jo, Google zensiert Scientology-Kritiker, heise news, 21.03.2002, http://www.heise.de/newsticker/meldung/Google-zensiert-Scientology-Kritiker-63741.html, (20.01.2010).

Bender, Rolf; Nack, Armn und Treuer, Wolf-Dieter, Tatsachenfeststellung vor Gericht, 2007.

Böhme, Andreas, Multimedia-forensik als Teildisziplin der digitalen Forensik, 2009, http://www1.inf.tu-dresden.de/~rb21/publications/BFGK2009_MultimediaForensik_GI.pdf, (20.01.2010).

Böhme, Andreas, Unschuldig im Visier der Steuerfahnder, der Westen, 09.03.2008, http://www.derwesten.de/wr/westfalen/Unschuldige-im-Visier-der -Steuerfahnder-id1436361.html, (19.06.2010).

Brors, Dieter, EU-Strafermittler nehmen Vorwürfe gegen Skype zurück, hese news, 28.02.2009, http://www.heise.de/newsticker/meldung/EU-Strafermittler-nehmen-Vorwuerfe-gegen-Skype-zurueck-202086.html, (20.01.2010).

Buchmann, Johannes, Einführung in die Kryptographie, 4, 2008.

Carrier, Brian D.; Grand, Joe, A hypothesis-based approach to digital forensic investigations, 2006.

Chakrabarti, Soumen, Mining the Web: Discovering Knowledge form Hypertext Data, 1, 2003.

cis, Virenattacke mit Kinderpornos, SPON, 10.11.2009, http://www.spiegel.de/netzwelt/web/0,1518,660199,00.html, (01.06.2010).

Dathe, Peter, Schriftliche Stellungnahme zum BKAG Entwurf, 01.09.2008, http://www.bundestag.de/bundestag/ausschuesse/a04/anhoerungen/Anhoerung15/Stellungnahmen_SV/Stellungnahme_06.pdf, (20.01.2010).

dmkl, Sony BMGs Kopierschutz mit Rootkit-Funktionen, heise news, 01.11.2005, http://www.heise.de/newsticker/meldung/Sony-BMGs-Kopierschutz-mit-Rootkit-Funktionen-143366.html, (20.01.2010).

Ehrmann, Stephan, Spiegel: Innenministerium stoppt Überwachung der BKA-Seite, heise news, 21.03.2009, http://www.heise.de/newsticker/meldung/Spiegel-Innenministerium-stoppt-ueberwachung-der-BKA-Seite-208339.html, (04.06.2010).

Eisenberg, Ulrich, Beweisrecht der StPO, 6, 2008.

Endres, Johannes Manuel, Beweismittel IP-Adresse fragwürdig, heise Netze, 19.04.2010, http://www.heise.de/netze/meldung/Beweismittel-IP-Adresse-fragwuerdig-980685.html, (13.05.2010).

Erb, Volker, Die Abhängigkeit des Richters vom Sachverständigen, Zeitschrift für die gesamte Strafrechtswissenschaft, 2009, 882.

Faber, Hai, Was war. Was wird., heise news, 04.06.2010, http://www.heise.de/newsticker/meldung/Was-war-Was-wird-1032813.html, (04.06.2010).
Fossi, Marc, Symantec Report on the Underground Economy, 2008.
Fossi, Marc, Symatec Sicherheitsbericht. Kernaussagen des 14 Symantec Internet Security Threat Reports, 2009.
Fox, Dirk, Stellungnahme zur Online-Durchsuchung, 07.09.2007, http://www.secorvo.de/publikationen/stellungnahme-secorvo-bverfg-online-durchsuchung.pdf, (20.01.2010).
Freiling, Felix C., Schriftliche Stellungnahme zum Fragenkatalog Verfassungsbeschwerden, 27.09.2007, https://pi1.informatik.uni-mannheim.de/filepool/publications/stellungnahme-online-durchsuchung.pdf, S. 3, (20.01.2010).
Fumkin, Dan u.a., Authentication of forensic DNA samples, Forensic Science International: Genetics 4, 2009, 95.

Geschonneck, Alexander, Computer Forensik. Computerstraftaten erkennen, ermitteln, aufklären, 3, 2008.
Geschonneck, Alexander, Onlinedurchsuchung: ich jetzt auch mal [update], 07.10.2007, http://computer-forensik.org/2007/10/07/onlinedurchsuchung-ich-jetzt-auch-mal, (20.01.2010).
Greifeneder, Horst Disk Forensik, 22.05.2008, http://de.wikibooks.org/wiki/Disk_Forensik/_Richtlinien/_Das_SAP-Modell, (20.01.2010).

Haderman, J. Alex, u.a., Lest We Remember: Cold Boot Attacks on Encryption Keys, USENIX Security Symposium, 2008, 45, 45.
Hansen, Markus und Pfitzmann, Andreas, Techniken der Online-Durchsuchung: Gebrauch, Missbrauch, Empfehlungen, Online-Durchsuchungen. Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008 2008, 137.
Hilgendorf, Eric, Frank, Thomas und Valerius, Brian, Computer- und Internetstrafrecht. Ein Grundriss, 1, 2005.

Jäger, Moritz, Blog Archive: Updated SkypeTrojan version available now, Megapanzer, 06.10.2009, http://www.megapanzer.com/2009/10/06/updated-skypetrojan-version-available-now /, (20.01.2010).
Jäger, Moritz, Confliker – das größte Botnet aller Zeiten, TecChannel, 05.01.2010, http://www.tecchannel.de/sicherheit/spam/1986704/conficker_das_groesste_botnetz_aller_zeiten/, (20.01.2010).
Joyce, Rick und Gupta,Gopal, Identity authentication based on keystroke latencies, Commun. ACM 1990, 168.

Kochheim, Dieter, Geltung von Beweisen und Erfahrungen, Cyberfahnder, 29.11.2009, http://www.cyberfahnder.de/nav/them/phish/skimkrimerf.htm, (10.07.2010).
Krawetz, Neal,, Anti-Honeypot Technology, IEEE Security and Privacy 2004, 76.
Krey, Volker Deutsches Strafverfahrensrecht. Hauptverhandlung, Beweisrecht, Gerichtliche Entscheidungen, Tatbegriff und Rechtskraft, Rechtsmittel und Rechtsbehelfe, 1, 2007.
Kuhn, Friedwart, Sicherheitsbetrachtungen von Wechselmedien, insbesondere USB-Sticks unter Windwos, ERNW Newsletter 22, 22.03.2008, http://www.ernw.de/content/e15/e28/e1180/download1182/ERNW_Newsletter_22_v1.0_ger.pdf, (20.01.2010).

Kunz, Christopher, Horch, wer kommt von draußen rein... Portknocking als Sicherheitskonzept unter Linux, C't Magazin für Computertechnik 2001, 206.

Kupsch, Andreas, Ulm, Gudrun und Funk, Thomas, „Hirnschrittmacher" gegen die Parkinson-Erkrankung. Eine Patientenaufklärung, Charité – Universitätsmedizin Berlin, 06.09.2005, http://www.charit.de/ch/nero/klinik/patienten/ag_bewegungsstoerungen/pdf/DBS_Aufklaerungsmatierial.pdf, (20.01.2010).

Kuri, Jürgen, Durch Google-Suche in die Einzelhaft [Update], heise news, 22.08.2007, http://www.heise.de/newsticker/meldung/Durch-Google-Suche-in-die-Einzelhaft-Update-165722.html, (20.01.2010).

Lehn, Jürgen, Wegmann, Helmut und Rettig, Stefan, Einführung in die Statistik, 3, 2001.

Libster, Eugen und Kornblum, Jesse D., A proposal for an integrated memory acquisition mechanism, SIGOPS 2008, 14.

Lill, Tobias, Digitale Autopsie, SPON, 08.02.2008, http://www.spiegel.de/netzwelt/web/0,1518,533078,00.html, (04.06.2010).

Lorenz, Dieter, Verwaltungsprozessrecht, 1, 2000.

Lübke, Wolfgang, Müller, Ulrike und Bonenberger, Saskia, Ermittlungsmöglichkeiten der Steuerfahndung, 1, 2008.

Lyon, Gordon, Nmap Reference Guide, http://nmap.org/book/man.html, (20.01.2010).

Morgenstern, Holger, Digitale Autopsie, heise security, 05.04.2004, http://www.heise.de/security/artikel/Computer-Forensik-mit-Open-Source-Tools-270468.html, (04.06.2010).

Möstl, Markus, Schriftliche Stellungnahme zum BKAG Entwurf, 03.09.2008, http://www.bundestag.de/bundestag/ausschuesse/a04/anhoerungen/Anhoerung15/Stellungnahmen_SV/Stellungnahme_09.pdf, (20.01.2010)

Murr, Mike, Forensically Sound Duplicate, 02.08.2006, http://www.forensicblog.org/2006/08/02/forensically-sound-duplicate, (01.07.2010).

Neuber, Harald, Militante Ermittler, Telepolis, 01.04.2009, http://www.heise.de/tp/r4/artikel/30/30054/1.html, (20.04.2010).

Nowitzky, Jan, Xpider (eXtended sPIDER) Internet Steuersündern auf der Spur, 07.2003, http://www.minet.uni-jena.de/dbis/veranstaltungen/datenbanktage-2003/DBTage2003-Nowitzky.pdf, (01.06.2010).

o.A., Bundeslagebild Organisierte Kriminalität, Pressereferat im Bundesministerium des Inneren, 04.06.2010, http://www.bka.de/pressemitteilungen/2010/pm100701_bmi.pdf, (04.06.2010).

o.A., Compliance Risk Management: Progress with the Development of Internet Search Tools for Tax Administration, OECD, 01.10.2004, http://www.oecd.org/dataoecd/44/15/33818593.pdf, (15.06.2010).

o.A., Survival Time, SANS Internet Storm Center, 02.2010, http://isc.sans.org/survivaltime.html, (20.01.2010).

o.A., Auch Datenkopie von Strauß-Computer weg, sueddeutsche.de, 20.05.2001, http://www.sueddeutsche.de/politik/justizaffaere-auch-datenkopie-von-strauss-computer-weg-1.315208, (27.10.2010).

o.A., Auf den Spuren von Internet-Verkäufern, Drucksache 16/7782, 06.02.2008, http://dipbt.bundestag.de/dip21/btd/16/079/1607978.pdf, (01.06.2010),

o.A., Bilanz der Online-Durchsuchung, Drucksache 17/1814, 21.05.2010, http://dip21.bundestag.de/dip21/btd/17/018/1701814.pdf, (10.07.2010).
o.A., Durchschnittliche Haltbarkeit von Zero-Day-Lücken liegt bei einem Jahr, heise news, 10.07.2007, http://www.heise.de/security/meldung/Durchschnittliche-Haltbarkeit-von-Zero-Day-Luecken-liegt-bei-einem-Jahr-149435.html, (20.01.2010).
o.A., Ein Dutzend Online-Durchsuchungen seit 2005, Tagesschau.de, 27.04.2007, http://www.tagesschau.de/inland/meldung36524.html, (20.01.2010).
o.A., FBI beißt sich an verschlüsselten Festplatten die Zähne aus, derStandard.at, 27.06.2010, http://derstandard.at/1277336831638/FBI-beisst-sich-an-verschluesselten-Festplatten-die-Zaehne-aus, (27.06.2010).
o.A., Forensically Sound, Yahoo Groups, 09.08.2006, http://www.forensicblog.org/2006/08/02/forensically-sound-duplicate, (01.07.2010).
o.A., Hack a bike, CCC, 2004, http://www.ccc.de/hackabike, (20.01.2010).
o.A., Hardware Keylogger, KeeyLog, 20.01.2010, http://www.keelog.com/de/, (20.01.2010).
o.A., Massives DNS-Sicherheitsproblem gefährdet das Internet, heise security, 09.07.2008, http://www.heise.de/security/meldung/Massives-DNS-Sicherheitsproblem-gefaehrdet-das-Internet-184975.html, (20.01.2010).
o.A., Microsoft Security Advisory (977377): Vulnerability in TLS/SSL Cloud Allow Spoofing, 09.02.2010, http://www.microsoft.com/technet/security/advisory/977377.mspx, (01.06.2010).
o.A., Rechtslexikon, LexisNexis Deutschland GmbH, 22.08.2007, http://www.juraforum.de/lexikon/, (20.01.2010).
o.A., Small Number of Video iPads Shipped With Windwos Virus, Apple Inc., 27.04.2007, http://www.apple.com/support/windowsvirus/, (20.01.2010).
o.A., Telekommunikationsüberwachung bei Einsatz von Voice-over IP, Bayerisches Staatsministerium der Justiz, 18.05.2003, http://wiki.piratenpartei.de/wiki/images/5/54/Bayern-skype-tkue.pdf,, (20.01.2010).
o.A., Unterrichtung durch den Bundesrechnungshof, Drucksache 16/3200, 13.11.2006, http://dipbt.bundestag.de/dip21/btd/16/032/1603200.pdf, (01.06.2010)

Pfitzmann, Andreas, Möglichkeiten und Grenzen der Nutzungsüberwachung von Informations- und Kommunikationssystemen in einer freiheitlichen demokratischen Gesellschaft. 26.09.2007, http://dud.inf.tu-dresden.de/literatur/MoegGrenzderNutzuebIuK-Sys-V1-0.pdf, (20.01.2010).
Phel, Dirk, Die Implementation der Rasterfahndung, Max-Planck-Institus für ausländisches und internationales Strafrecht, 30.01.2008, http://www.iuscrim.mpg.de/ww/de/pub/forschung/forschungsarbeit/kriminologie/rasterfahndung.htm, (01.06.2010).
Poscher, Ralf, Schriftliche Stellungnahme zum BKAG Entwurf, 01.09.2008, http://www.bundestag.de/bundestag/ausschuesse/a04/anhoerungen/Anhoerung15/Stellungnahmen_SV/Stellungnahme_10.pdf, (20.01.2010).

Rada, Uwe, Kommissar Google jagt Terroristen, taz.de, 22.08.2007, http://www.taz.de/?id=start&art=3471&id=detuschland-artikel&cHash=5218eee73a,, (16.06.2010).
Reinelt, Ekkehart, Elektronischer Rechtsverkehr – Die Justiz im Elfenbeinturm, LTO 2006, http://www.lto.de/de/html/nachrichten/508/Die-Justiz-im-Elfenbeinturm-neu/, (10.07.2010).

Roggan, Frederik, Präventive Online-Durchsuchungen. Überlegungen zu den Möglichkeiten einer Legalisierung im Polizei- und Geheimdienstrecht, 2008, 97.

Rüping, Hinrich, Zur Rolle des Sachverständigen im Strafverfahren, 10.12.2009, http://www.pknds.de/fileadmin/user_upload/Dokumente/Sonstiges/Berichte/Herr_Prof._Dr._Hinrich_Rueping_2.pdf, (20.01.2010).

Rüßmann, Helmut, Das Theorem von Bayes und die Theorie des Indizienbeweises. Anmerkung zum BGH, Urteil vom 8. März 1989 – VU ZR 232/88, Zeitschrift für Zivilprozess 1990, 62.

Schaar, Peter, Unterrichtung durch den Bundesbeauftragten für den Datenschutz, Drucksache 15/5252, 19.03.2005, http://www.bfdi.bund.de/cae/servlet/contentblob/409318/publicationFile/25223/20TB_2003_04.pdf, (01.06.2010).

Schlegel, Stephan, Online-Durchsuchung light. Die Änderung des § 110 stopp durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung, Online Zeitschrift für Höchstrichterliche Rechtsprechung im Strafrecht 2008, 23.

Schmid, Viola, Sicherheit von ec-Karten, CyLaw-Report V, 17.10.2008, http://tuprints.ulb.tu-darmstadt.de/1103/1Cylaw_Report_V_060117.pdf, (20.01.2010).

Schmid, Viola, Verdeckte Online-Durchsuchungen (11/2007), CyLaw-Report XX, 07.01.2008, http://www.cylaw.tu-darmstadt.de/media/jus4/cylawreports/cylaw_report_xx.pdf, (20.01.2010).

Schmitt, Manuel, IP-Adressen nur mit sicherem Routing eindeutig, heise news, 13.05.2010, http://www.heise.de/newsticker/meldung/IP-Adressen-nur-mit-sicherem-Routing-eindeutig-999457.html, (13.05.2010).

Schulze, Martin, Debian Investigation Report after Server Compromises, 02.12.2003, http://www.heise.de/newsticker/meldung/IP-Adressen-nur-mit-sicherem-Routing-eindeutig-999457.html, (20.01.2010).

Schum, David A. und Martin, Anne W., Formal and Empirical Research on Cascaded Inference in Jurisprudence, Law & Society Review 1982, 105.

Schweizer, Mark, Intuition, Statistik und Beweiswürdigung, 01.04.2006, http://www.decisions.ch/publikationen/intuition_statistik.html, (20.01.2010).

Schweizer, Mark, Kognitive Täuschung vor Gericht, 1, 2005.

Sennett, Richard und Sassen, Saskia, Guantánamo in Germany, the Guardian, 21.08.2008, http://www.guardian.co.uk/education/2007/aug/21/highereducation.ukl, (15.06.2010).

Siebert, Ulrich, Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts, 09.10.2007, http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf, (20.01.2010).

Sperlich, Tom, Es hat sich viel verändert, Technology Review, 20.06.2008, http://www.heise.de/tr/artikel/Es-hat-sich-viel-veraendert-275332.html, (20.01.2010).

Stadler, Thomas, Anstieg der Computerkriminalität, Internet-Law, 18.05.2010, http://www.internet-law.de/2010/05/anstieg-der-computerkriminalitat.html, (28.05.2010).

Starbug, Wie können Fingerabdrücke nachgebildet werden?, CCC, 09.10.2004, , (20.01.2010)

Stawowy, Fragenkatalog des Bundesministeriums der Justiz, netzpolitik.org, 22.09.2007, http://dasalte.ccc.de/biometrie/fingerabdruck_kopieren, (20.01.2010).

Tanenbaum, Andrew S., Moderne Betriebssysteme, 2, 2003.

Typke, Rainer, Social Lending: Credit Scoring für Normalbürger (mit Open Source-Software), 27.06.2009, http://www.beobach.de/uploads/media/LinustagSocialLending.pdf, (01.06.2010).

Widmaier, Gunter, Münchener Anwaltshandbuch Strafverteidigung, 1, 2006.

Winkler, Jan, Bundeswanze statt Trojaner, IT-News World, 03.08.2007, http://www.it-news-world.de/news_1017/Bundeswanze+statt+Trojaner, (20.01.2010)

Winsemann, Bettina, Verfassungsbeschwerde gegen das BKA-Gesetz, Telepolis, 27.01.2009, http://www.heise.de/tp/r4/artikel/29/29614/1.html,, (20.01.2010).

Wright, Craig, Kleiman, Dave und Sundhar, Shyaam R.S., Overwriting Hard Drive Data: The Great Wiping Controversy, ICISS'08: Proceedings of the 4th International Conference on Information Systems Security 2008, 243.

Yang, Yiming und Liu, Xin, A re-examination of text categorization methods, SIGIR conference on Research and development in information retrieval 1999, 42.

York, Richard, Ecological Paradoxes: William Stanley Jevons and the Paperless Office, Human Ecology Review 2006, 143.

Zeiss, Walter und Schreiber, Klaus, Zivilprozessrecht, 10, 2003.

Ziercke, Jörg, Pro Online-Durchsuchung, Informatik-Spektrum 2008, 62.