Die Online-Durchsuchung in Deutschland

Nothing to hide?

Martin Amberg, Kai Dietrich, Felix Friedrich,
Mai Huong Nguyen, Milan Mehner, Max Ulbricht

26. Oktober 2008

Inhaltsverzeichnis

1 Einleitung

Nach den Vorfällen des 11. Septembers des Jahres 2001 in den USA sind aus Sicherheitsinteressen heraus international Bestrebungen entstanden Kommunikation zu überwachen. Auch in der Bundesrepublik Deutschland sind inzwischen Gesetze entstanden oder in der Entstehung, die den Sicherheitsorganen des Staates oder der Länder Zugriff auf informationstechnische Systeme gewähren. In dieser Arbeit sollen die Realitäten und Möglichkeiten rund um die Online-Durchsuchung auf technischer, rechtlicher und politischer Ebene zusammengefasst werden.

Wir beginnen mit einer technischen Analyse der Voraussetzungen und Möglichkeiten ein informationstechnisches System durchsuchen zu können. Mit diesem Wissen ausgestattet wird der Leser dann durch die aktuelle rechtliche Lage geleitet. Anschließend werden wir auf die Positionen und Argumente der politischen Akteure in Deutschland eingehen.

Vorab sei kurz angemerkt, dass sich, wenn auch technisch ähnlich, die Online-Durchsuchung im Sprachgebrauch des Bundesministerium des Innern von der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) unterscheidet. Die Quellen-TKÜ stellt eine Form der Telekommunikationsüberwachung dar, die, anders als die herkömmlichen Telekommunikationsüberwachung, auch verschlüsselte Kommunikation überwachen kann und nur diese Kommunikationsinhalte umfasst. Die Online-Durchsuchung umfasst dagegen die Inhalte, die in einem informationstechnischen System gespeichert sind. Eine genauere Differenzierung und die Implikationen werden wir auf technischer Ebene in Kapitel 2 vornehmen. Generell beziehen wir uns in dieser Arbeit aber nur auf die Online-Durchsuchung, nicht die Quellen-TKÜ.

2 Technik

Die Online-Durchsuchung ist ein in besonderer Weise durch technische Artefakte dominiertes Diskussionsthema. Wer die notwendige Technik hinter den Überwachungswünschen der Sicherheitsbehörden und deren Grenzen nicht versteht läuft Gefahr Fehlentscheidungen zu treffen. Deshalb werden im Folgenden die Möglichkeiten und Grenzen der Online-Durchsuchung möglichst systematisch ausgelotet. Wir werden dabei noch auf einer sehr generalisierenden Beschreibungsebene bleiben um den Leser nicht von den wichtigen Fakten abzulenken und auf weiterführende Literatur verweisen.

DIFFERENZIERUNG

Unter einer Online-Durchsuchung versteht man das Eindringen in ein informationstechnisches System über dessen Kommunikationsschnittstellen und das anschließende Durchsuchen der Inhalte. Dies geschieht meist mit Hilfe einer sog. RFS – einer „Remote Forensic Software“. Die Kommunikationsschnittstellen sind in erster Linie Verbindungen zum Internet. In Frage könnten aber auch andere Verbindungen wie z.B. Bluetooth oder WLAN kommen.

Das Bundesministerium des Innern unterscheidet zwischen einer Online-Durchsicht und einer Online-Überwachung. Die Online-Durchsuchung ist dementsprechend der Oberbegriff über beides. Eine Online-Durchsicht ist eine einmalige Durchsicht der Inhalte eines informationstechnischen Systems, eine Online-Überwachung ist dagegen zeitlich länger ausgedehnt[1]. Damit stellt die Online-Überwachung einen signifikant höheren Eingriff in die Persönlichkeitsrechte des Betroffenen dar. Auch technisch ergeben sich Unterschiede durch neue Anforderungen an die RFS.

Eine weitere Abgrenzung muss zur Quellen-Telekommunikationsüberwachung oder auch kurz Quellen-TKÜ gemacht werden. Ziel der Quellen-TKÜ ist die

[1] Vgl. Bundesministerium des Innern (2007b, S.1)

Überwachung von verschlüsselten Kommunikationsverbindungen. Dies ist bei Verbindungen, die nach aktuellem Stand der Technik abgesichert sind, nur an den Endpunkten vor der Verschlüsselung oder nach der Entschlüsselung möglich. Zu diesem Zweck muss wie bei der Online-Durchsuchung eine Software auf mindestens einem der Endpunkte eingebracht werden. Bei der Quellen-TKÜ dürfen nur die aktuellen Kommunikationsinhalte überwacht werden und nicht auf die gespeicherten Inhalte des informationstechnischen Systems zugegriffen werden. Die Methoden der Einbringung und Entfernung der Überwachungssoftware sind denen der Online-Durchsuchung auf jeden Fall äquivalent. In dieser Arbeit soll es jedoch nur um die Online-Durchsuchung an sich gehen.

Eine Online-Durchsuchung lässt sich nun in mehrere Phasen einteilen:

1. Analyse des Zielsystems
2. Einbringung der RFS
3. Selektion relevanter Daten
4. Rückübertragung relevanter Daten
5. Entfernung der RFS

Die technische Realisierung dieser Phasen trifft auf verschiedene Probleme. Im Folgenden werden wir auf jede dieser Phasen genauer eingehen.

2.1 Analyse des Zielsystems

2.1.1 Zielstellung und Methoden

Bevor überhaupt eine Software auf dem Zielsystem installiert werden kann, muss das Zielsystem genau analysiert werden. Ziel ist es genug Informationen zu erlangen um eine Einbringungsweg für die RFS zu ermitteln. Ergebnis dieser Analyse kann auch sein, dass eine Einbringung mit den zur Verfügung stehenden Mitteln nicht möglich ist.

Zur Analyse können sowohl technische als auch herkömmliche Ermittlungsverfahren eingesetzt werden. Zu den herkömmlichen Ermittlungsverfahren können z. B. verdeckte Ermittler oder eine Telekommunikationsüberwachung zählen.

Die technische Analyse über die Kommunikationsverbindungen setzt u. U. eine Mitwirkung von Diensteanbietern vorraus. Es ist hier zwischen lokalen Funkverbindungen (Bluetooth, WLAN) und Internetverbindungen zu unterscheiden. Vorwiegende Schwierigkeit ist die Identifikation des Zielsystems. Bei lokalen Funkverbindungen gestaltet sich diese als rel. einfach, da die Anzahl der in Frage kommenden Systeme meist sehr klein ist. Bei Internetverbindungen ist ein Mitwirkung eines Diensteanbieters erforderlich. Dieser kennt die Zuordnung von technischer Adresse und Zielperson, womit eine Identifizierung des Zielsystems gegeben wäre. Ebenso könnten andere Diensteanbieter die der Benutzer verwendet, wie z. B.Email-Provider oder Internetportale, bei einer Identifizierung helfen. Ist die Identifizierung gegeben, so kann über sog. Portscanner nach Einbringungswegen gesucht werden.

2.1.2 Behinderungsmöglichkeiten

Die technische Analyse kann leicht verhindert bis unmöglich gemacht werden. Dazu kann als erstes die Identifikation des Zielsystems erschwert werden. Wenn der Nutzer nur über Fremde Netze, also z. B.in Internet-Cafés, über offene, halboffene oder fremde (illegal genutzte) WLANs in das Internet geht, so ist die Identifizierung schon deutlich erschwert. Weiter könnten anonyme, ausländische Prepaid UMTS oder GSM Karten verwendet werden.

Damit ist es nahezu unmöglich das Zielsystem im Netzwerk zu finden. Einzig wenn das Zielsystem eine Verbindung zu einem Diensteanbieter (Email, Instant Messaging, ...) aufnimmt, kann es noch gefunden werden. Aber auch dies kann umgangen werden, indem Anonymisierungsdienste (wie z. B.TOR[2]) genutzt werden. Weiterhin ist nicht gegeben, dass das Zielsystem direkte Verbindungen zum Internet aufbaut, sondern es kann sich in einem lokalen Netz hinter einem Router befinden und kann damit gar nicht direkt untersucht werden.

Eine vorbereitete Zielperson könnte sogar bewusst Fehlinformationen streuen,

[2] `www.torproject.org`

z. B.bilden sog. Honey-Pots scheinbar verwundbare Systeme ab, lassen einen Angreifer dann aber ins Leere laufen. Firewalls und Intrusion Detection Systeme sind außerdem darauf vorbereitet laufende Analysen zu erkennen und zu unterbinden. Auf technischer Ebene sind der Behinderung also kaum Grenzen gesetzt.

2.2 Einbringung der RFS

2.2.1 Zielstellung und Methoden

Die Einbringung der RFS in das Zielsystem kann auf verschiedenen Wegen stattfinden. Dies können zum einen (Fern-)Kommunikationsverbindungen sein, zum anderen auch der lokale Zugriff auf das Zielsystem. Eine zweite Unterscheidung kann nach der nötigen Mitwirkung des Benutzers des Zielsystems vorgenommen werden: Die Einbringung kann entweder mit oder ohne (unwissentliche) Mitwirkung des Benutzers stattfinden. Es entstehen folgende vier Kombinationen:

1. Lokaler Zugriff, mit Hilfe Benutzers
2. Lokaler Zugriff, ohne Hilfe des Benutzers
3. Zugriff über Kommunikationsverbindungen, mit Hilfe des Benutzers
4. Zugriff über Kommunikationsverbindungen, ohne Hilfe des Benutzers

In jedem Fall gleich ist das Prinzip eine Software vermutlich gegen den Willen und ohne das Wissen des Benutzers auf dessen System zu installieren. Die technische Schwierigkeit wird, nach heutigem Stand der Technik, vorwiegend davon bestimmt ob ein menschlicher Bediener an der Installation mitwirkt oder nicht. Ein solcher Benutzer ist in der Lage kritische Operationen gegenüber dem Betriebsystem oder anderer Software zu autorisieren. Dies kann z.B. das manuelle Öffnen eines Anhangs in einer Email (womit die Installation implizit autorisiert wird) oder auch das Einstecken eines USB Sticks sein (womit ebenfalls eine Installation impliziert autorisiert werden kann). Existiert kein solcher lokaler Benutzer der an der Installation mitwirkt, z.B. bei der Installation über Kommunikationsverbindungen, so steigt die Schwierigkeit enorm an, denn die

vorgesehen Sicherheitsmechanismen des Betriebsystems müssen nun mit hohem Aufwand umgangen werden.

Dem technisch mehr versierten Leser wird auffallen, dass die Methoden zur Installation von ungewollter Software den Methoden von Viren, Spyware und anderer, als Malware bekannter Schadsoftware, weitgehend entsprechen[3]. Die genutzten Einbringungswege werden generell als Sicherheitslücken betrachtet. Ein Anreißen der technischen Details würde hier eine irreführende Vereinfachung der Vielfalt und Komplexität dieser Angriffswege darstellen[4]. Um der Bedrohung durch nicht-staatliche Schadsoftware zu begegnen arbeiten Softwareentwickler weltweit an der Verringerung sowohl der Zahl als auch der Gefährlichkeit dieser Sicherheitslücken. Die Kontinuität in dieser Arbeit führt dazu, dass Sicherheitslücken die öffentlich bekannt geworden sind schon nach kurzer Zeit geschlossen werden. Neue Sicherheitslücken „müssen sehr aufwändig recherchiert, teuer erworben oder ersteigert werden“[5]. Alternativ könnten Sicherheitslücken (Hintertüren, sog. Backdoors) in verbreitete Software zum Gebrauch für Sicherheitsbehörden injiziert werden. Gegen diese zweifelhafte Praxis spricht, dass solche künstlichen Sicherheitslücken schnell bekannt werden würden und damit vermutlich außerhalb der betroffenen Software geschlossen würden. Es bleibt auch ein Missbrauchspotential durch andere Angreifer bestehen. Da dieses Vorgehen moralisch, rechtlich und technisch äußerst fragwürdig ist, kann es als möglicher Realisierungsweg ausgeschlossen werden und auch das BMI hält dies für „politisch nicht gewollt“[6]. Aus diesen Gründen ist das Einbringen einer wie auch immer gearteten Software ohne die Hilfe eines Benutzers deutlich schwieriger.

[3] Dieser Vergleich findet sich auch bei Fox (2007a, S.829).

[4] Für weiterführende Informationen über die Techniken hinter den Angriffen auf Computersysteme sei hier auf Aleph One (1996) und Hoglund u. McGraw (2004) verwiesen.

[5] Siehe Fox (2007a, S.829)

[6] Siehe Bundesministerium des Innern (2007b, S.19).

Soll ein lokaler Benutzer bei der Installation mitwirken, so wird die Einbringung deutlich erleichtert. Ein lokaler Zugriff auf das Zielsystem durch eine Sicherheitsbehörde erlaubt sofort die Installation entsprechender Software. Ist ein lokaler Zugriff nicht möglich oder gewünscht muss die Zielperson oder ein anderer Benutzer unwissentlich an der Installation mitwirken. Ein Nutzer kann z.B. durch Irreführung dazu gebracht werden der Installation einer Software zuzustimmen oder die Software kann als sog. Trojaner in einer durch den Nutzer erwünschten Software verborgen sein[7][8].

IDENTIFIZIERUNG DES ZIELSYSTEMS

Wie auch bei der Analyse des Zielsystem ist die eindeutige Identifizierung des Zielsystems eine weitere Hürde und notwendige Voraussetzung zur Einbringung der RFS.

Soll ein lokaler Zugriff auf das System erfolgen, so ist die Identifizierung i.d.R. sofort gegeben. Ist ein Zugriff über Kommunikationsleitungen geplant, so sind die technischen Details entscheidend ob eine wirklich sichere Identifizierung möglich ist. In den gängigen Internetprotokollen sind keine eindeutig rechneridentifizierenden Merkmale enthalten. Die Internet-Adresse (IP) wird üblicherweise dynamisch vergeben, so dass jeder Rechner bei jeder neuen Verbindung eine neue Adresse zugewiesen bekommen. Vom Benutzer eingegebene Identifikationsmerkmale (Benutzernamen, Passwörter, Cookies, Session IDs) identifizieren nur den Benutzer, nicht das Gerät. Eine Verbindung von Rechner- und Benutzeridentifikation ist erst durch zukünftige (Trusted Computing) Technologien in weiter Ferne gegeben[9].

[7] So hat z.B. der Chaos Computer Club am 1. April 2007 orakelt, dass der „Bundestrojaner" in der Elster Software zur elektronischen Steuererklärung verborgen sei (Chaos Computer Club e.V. 2007). Obwohl dies vordergründig abwegig erscheint und ein Aprilscherz geblieben ist, ist es doch als eine Alternative aufzuführen.

[8] Denkbar und sehr attraktiv ist auch die Manipulation von eigentlich gewollten System-Updates in denen sich dann die RFS verbirgt.

[9] Gemeint sind Trusted Computing Technologien und TPM Chips. Diese Technologien erlauben einen kryptographisch sicheren Nachweis der Identität eines Nutzers und vor allem auch Rechners. Einen Einstieg kann Wikipedia (2008) bieten.

2.2.2 Behinderungsmöglichkeiten

Wer sich gegen die Einbringung von unerwünschter Software absichern will, der kann zum einen die Identifizierung seines Systems verhindern, sollte also seine Anonymität wahren und zum anderen die Installation verhindern, also die Integrität seines Systems sicher stellen.

Wie in Abschnitt 2.1 kann auch hier kein vollständiger Leitfaden zur Wahrung der Anonymität gegeben werden. Ein häufiger Wechsel der verwendeten Kommunikationsleitungen und Internet Service Provider kann aber zu erheblichen Schwierigkeiten bei der Identifizierung führen. Der Festnetzanschluß in der Wohnung des Betroffenen kann noch leicht durch den Telekommunikationsanbieter (unter Beachtung entsprechender Rechtsvorschriften) so verändert werden, dass immer die gleiche IP vergeben wird und damit eine Identifizierung beinahe gegeben ist. Ist das Zielsystem ein üblicher mobiler Rechner mit wechselnden kabellosen Kommunikationsverbindungen in öffentlichen oder halböffentlichen Umgebungen, dürfte dies deutlich schwerer sein.

Zur Wahrung der Integrität von IT-Systemen existieren eine Vielzahl von technischen Möglichkeiten. Während das System im Betrieb ist sollen die Sicherheitsmechanismen des Betriebsystem die Integrität wahren und können durch zusätzliche Maßnahmen ergänzt werden. Diese reichen vom einfachen Verwenden eines Virenscanners und regelmäßigen Updates des Systems bis zu einigen Lösungen die sogar teilweise die Wirksamkeit von noch nicht bekannten Sicherheitslücken verhindern[10]. Weiterhin kann ein Integritätschecker installiert werden. Ein solches Programm kann alle Dateien eines Systems auf Veränderungen überwachen und somit auch neu hinzugekommene Dateien erkennen. Ist das System ausgeschaltet, können Manipulationen bei einen lokalen Zugriff durch eine Verschlüsselung der Datenträger ausgeschlossen werden. Es bleiben Eingriffe in die Hardware als leicht zu realisierende Möglichkeiten.

[10] Beispiele sind die sog. Address Space Layout Randomization, Stack-Smashing Protection, Data Execution Prevention. Implementierungen finden sich z.B. in PaX und ProPolice für Linux oder Microsoft Windows XP mit Service Pack 2.

2.3 Selektion relevanter Daten

2.3.1 Zielstellung und Methoden

Ist die RFS einmal auf dem Zielsystem installiert so kann sie verwendet werden um die lokalen Datenbestände zu durchsuchen und die Ein- und Ausgaben in das und vom informationstechnischen System zu protokollieren. Sie kann bei bestehender Online-Verbindung interaktiv gesteuert werden oder auch selbstständig programmiert ohne menschliche Aufsicht arbeiten. Es wird aber davon ausgegangen, dass die Online-Verbindung jeweils nur für rel. kurze Zeit besteht und die RFS unbeaufsichtigt programmiert arbeiten soll. Die Arbeit der RFS sollte vom Benutzer des Systems nicht bemerkt werden und darf deshalb nur wenige Ressourcen des Systems beanspruchen.

Zentrale technische und rechtliche Schwierigkeit ist die Trennung von straftatsrelevanten Daten von Daten aus dem Kernbereich der persönlichen Lebensführung des betroffenen Benutzers. Um diese Trennung überhaupt vornehmen zu können muss bereits ein lesender Zugriff auf die Daten durchgeführt werden. Nachdem die Daten gelesen sind, muss dann je nach Arbeitsmodus nach einem Regelsatz oder von einem menschlichen Operator entschieden werden, ob die Daten straftatsrelevant oder Kernbereichsdaten sind.

An dieser Stelle ist auch der Hauptunterschied zwischen einer Online-Durchsicht und einer Online-Überwachung. Bei einer Online-Durchsicht werden nur die Bestandsdaten auf dem System betrachtet während bei einer Online-Überwachung auch die Ein- und Ausgaben protokolliert werden sollen[11]. Dies betrifft insbesondere Schlüssel für verschlüsselt vorliegende Datenbestände oder Daten vor einer Verschlüsselung oder nach einer Entschlüsselung.

Bei den zu begutachtenden Daten kann es sich z.B. um natürlichsprachlichen Text (Emails, Briefe, Textdokumente, Blog-Einträge), Bilder, Audio-Aufnahmen, Video-Aufnahmen oder maschinenlesbaren Text (Konfigurationsdateien, Datenbanken, Tabellen) handeln. Für jede einzelne dieser Datenarten (bis auf maschinenlesbaren Text) bestehen spezifische Probleme bei der Verarbeitung die von der Berechenbarkeitstheorie beschrieben werden und nicht vollständig sondern nur näherungsweise gelöst werden können. Ein wie auch immer gearteter Algorithmus kann z.B. nie den Inhalt eines natürlichsprachigen Textes verste-

[11] Vgl. Bundesministerium des Innern (2007b, S.6)

hen und zuverlässig über die Relevanz entscheiden. Statistische und heuristische Verfahren zur Entscheidung über die Relevanz behalten so immer eine Ungenauigkeit bei der Relevanzentscheidung, es können falsche Positiv- und Negativentscheidungen entstehen. Daraus resultiert eine unvermeidbare Gefahr für die Verletzung des Kernbereichs der persönlichen Lebensführung.

Die RFS ist ausdrücklich auch dazu gedacht angeschlossene Speichermedien und Netzlaufwerke zu durchsuchen. Es ist nicht unwahrscheinlich, dass auf Netzwerklaufwerken auch die Daten anderer Personen liegen so dass nicht nur eine Gefahr für die Verletzung des Kernbereichs der persönlichen Lebensführung der Zielperson besteht, sondern auch für den anderer unbetroffener Personen. Ebenso kann nicht ausgeschlossen werden, dass mehrere Personen mit ein und dem selben IT-System arbeiten.

2.3.2 Behinderungsmöglichkeiten

Mathematik und Informatik haben wirksame Methoden entwickelt um sensible Informationen vor der Entdeckung zu schützen. Dies sind die Verfahren der Kryptographie und der Steganographie. Kryptographisch verschlüsselte Daten lassen sich mit der Erlangung des Schlüssels wieder entschlüsseln und somit auch sichten. Das Prinzip der Steganographie ist subtiler.

Während das Ergebnis einer Verschlüsselung häufig als ein solches erkennbar ist, ist es das Ziel der Steganographie Inhalte in anderen Inhalten, quasi hinter einer Fassade, zu verbergen. Es existieren verschiedene Verfahren die einen kurzen Text in einer größeren Datei (z.B. einem Video, einem Foto oder einer Audio-Datei) verbergen. An der veränderten Datei aus Zieltext und Trägerdaten fällt nicht auf, dass zusätzliche Daten enthalten sind. Sie würden so jeder Suche nach relevanten Daten entgehen, es werden also falsch-negativ Entscheidungen provoziert. Entsprechende Software ist frei verfügbar[12].

Eine viel einfachere Möglichkeit die Funktion der RFS zu behindern ist es sehr viel sinnloses Datenmaterial auf dem System zu platzieren, das mit scheinbar kompromitierenden Suchstichworten gefüllt ist. Auf diese Weise würden palsch-positiv Erkennungen provoziert. Die RFS würde dieses Material als relevant erkennen und zur Rückübertragung vorsehen. Erst eine spätere Analyse würde zeigen, dass nur sinnloses Material gewonnen wurde.

[12] z.B. „Steghide“ – `http://steghide.sourceforge.net/`

2.4 Rückübertragung relevanter Daten

2.4.1 Zielstellung und Methoden

Nach der hoffentlich erfolgreichen Selektion relevanter Daten müssen diese wieder an die Sicherheitsbehörden übertragen werden. Dies erfolgt vermutlich über die gleiche Kommunikationsverbindung über die die Einbringung der RFS erfolgte, kann aber auch über eine andere Verbindung erfolgen. Die RFS muss dazu feststellen ob eine Verbindung verfügbar ist, den Rückübertragungsserver kontaktieren, eine verschlüsselte Verbindung aufbauen und mit der Übertragung beginnen. Dabei muss die Übertragung unentdeckt bleiben, darf also u.a. nur wenig Bandbreite in Anspruch nehmen.

2.4.2 Behinderungsmöglichkeiten

Die Rückübertragung kann so getarnt werden, dass sie im Übertragungskanal, je nach Medium wie eine andere gängige Anwendung aussieht[13]. Die Kommunikation kann nur vom Benutzer als verdächtig enttarnt werden, wenn dieser bemerkt, dass sie nicht mit der selbst initiierten Kommunikation übereinstimmt. Die Verbindung muss also auf dem betroffenen System vor den systemeigenen Diagnosewerkzeugen (z.B. `netstat` oder Personal Firewalls) versteckt werden, so dass keine Warnungen, Abfragen etc. auftauchen. Bei der Vielzahl an verfügbarer Software ist dies ein aufwendiges Verfahren. Wird dieser Aufwand allerdings nicht betrieben, so kann die Rückübertragung leicht durch Personal Firewalls verhindert oder aufgedeckt werden. Ist dies einmal erfolgt, so tritt der schlimmstmögliche Fall auf: Die Rückübertragung kann manipuliert werden. Es können zum einen fingierte Daten untergeschoben werden und zum anderen kann mit höherem Aufwand sogar in die Verbindung selbst eingegriffen und entlastendes oder sinnloses Material eingeschleust werden[14].

[13] z.B. wie ein Internet Explorer der mit einem Apache Server über SSL/HTTPS kommuniziert.

[14] Auf dem betroffenen System kann sich eine andere, u.U. selbst geschriebene Software in Datenstrom der RFS vor der Verschlüsselung einklinken. Diese Funktion entspricht der Funktion der Quellen-TKÜ, mit dem Zusatz des schreibenden Eingriffs in den Datenstrom.

2.5 Entfernung der RFS

2.5.1 Zielstellung und Methoden

Nach dem die RFS nicht mehr benötigt wird, muss sie wieder von dem System entfernt werden. Das per Anweisung passieren kann durch entsprechende Befehle, die an die RFS übertragen werden. Das selbstständige Entfernen ist auch möglich nach einer bestimmten Zeit, die über einen Zähler gezählt wird oder zu einem bestimmten Datum oder Uhrzeit, wobei da das Problem ist, welche Uhrzeit die Richtige für die RFS ist. Zur Sicherheit sollte die RFS eine genormte Zeit über einen Zeitserver beziehen, da die Systemzeit manipuliert sein kann.

2.5.2 Behinderungsmöglichkeiten

Wenn die RFS nicht nach einer bestimmten Zeit sondern auf Anweisung entfernt wird, sich das System aber nicht mehr im Netz befindet, kann die Entfernung verhindert werden. Ein großes Problem stellen auch Backups des eigenen Systems da. Sollte die Zielperson mitbekommen haben, dass sich die RFS auf seinem System befand, konnte diese zwar auf dem laufenden System entfernt werden, aber nicht auf den Backups. Das BKA ist gesetzlich dazu verpflichtet, die Zielperson nach Ablauf des Falles oder beim Feststellen der Unschuld zu benachrichtigen. Hier wäre die Möglichkeit über die Backups die RFS zu suchen und genauer mit den Methoden des Reverse Engineering zu untersuchen. Ein mögliches Ziel wäre z. B. herauszufinden, wie die Software arbeitet, wo die Daten hin zurückübertragen werden usw. .

3 Recht

Die Rechtsgrundlage für geplante, sowie bereits durchgeführte Online-Durchsuchungen, ordnet sich in die umfassende Diskussion um die Ausweitung staatlicher Überwachungsbefugnisse in den letzten Jahren ein. Im Gesamtkontext der geplanten neuen Befugnisse, die z.B. das Bundeskriminalamt im Zuge der Terrorismusprävention bzw. -fahndung erhält, erscheint die Erlaubnis der Online-Durchsuchung beinahe nebensächlich. Dennoch verbindet sich mit ihr eine eigene umfangreiche Diskussion, die unter anderem zur Einführung eines neuen Grundrechts führte und noch längst nicht abgeschlossen ist.

Die einzelnen Abschnitte der rechtlichen Entwicklung lassen sich logisch am besten aufarbeiten, wenn wir uns auf ihre chronologische Abfolge beziehen. Wir unterteilen in folgende Abschnitte: nicht-öffentliches Vorgehen ohne Gesetzesgrundlage; erste gesetzliche Formulierung im Verfassungsschutzgesetz NRW; Definition der rechtlichen Grundlage durch Bundesverfassungsgerichtsurteil hierzu; Neuformulierung des BKA-Gesetzes unter Bezugnahme auf dieses Urteil.

3.1 Vorgesetzliche Situation

Nach den Anschlägen des 11. September 2001 sah sich auch die deutsche Politik mit der Situation konfrontiert, dass die Befugnisse und technischen Möglichkeiten der Sicherheitsorgane scheinbar nicht mit den modernen Methoden der Gegenseite mithalten konnten. In den Augen der verantwortlichen Politiker war es nötig geworden neue Mittel und Methoden zu finden, welche es erlaubten, angemessen auf die neuen Bedrohungen zu reagieren. Als größte Lücke wurde das Fehlen von Regularien zur Überwachung von Computern und Internetverkehr ausgemacht. Da Erkenntnisse vorlagen, dass Terroristen zur Anschlagsplanung vorwiegend das Internet nutzten, musste ein Weg gefunden werden, diese neue Art der Kommunikation zu überwachen.

Da es noch keinerlei Gesetzgebung diesbezüglich gab, wandte sich im März 2005 das Bundesamt für Verfassungsschutz mit der Bitte um Erweiterung der zulässigen nachrichtendienstlichen Mittel an das Innenministerium. Die zulässigen Mittel sind in einer sogenannten Dienstvorschrift festgeschrieben. Diese Dienstvorschrift wurde auf die Bitte hin vom damaligen Innenminister Otto Schily und seinem Innenstaatssekretär Lutz Diwell (beide SPD) dahingehend geändert, dass eine „offensive Beobachtung des Internets“[1] möglich wurde. Beiden war angeblich nicht klar, dass sie mit ihrer Änderung dem Verfassungsschutz Mittel an die Hand gaben, welche verfassungswidrig dazu genutzt wurden, neben Internetforen auch die Computer von Verdächtigen zu durchsuchen. Und obwohl im Juli 2005 das Parlamentarische Kontrollgremium über die Änderung informiert wurde, konnte dieses aufgrund von fehlenden technischen Kompetenzen weder die Tragweite der Änderung noch deren Verfassungswidrigkeit erkennen. Da sich sowohl Verfassungsschutz als auch Innenministerium auf Geheimhaltungspflichten berufen, ist bis heute weder klar, welche Mittel damals angefordert wurden, noch ist der genaue Wortlaut der geänderten Dienstvorschrift bekannt. Das Innenministerium räumte im Mai 2007 allerdings ein, dass der Verfassungsschutz die neue Möglichkeit zur heimlichen Online-Durchsuchung in „weniger als einem Dutzend“ Fällen auch angewandt hat[2].

3.2 Verfassungsschutzgesetz NRW

Am 20.12.2006 wird ein neues Verfassungsschutzgesetz in Nordrhein-Westfalen verabschiedet. Es ist von Bedeutung, da es sich um das erste Gesetz handelt, das die Online-Durchsuchung explizit vorsieht. Dieser Versuch einer gesetzlichen Rahmensgebung für das umstrittene Vorgehen ist allgemein und unverbindlich. Erlaubt ist, „der heimliche Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel.“ (VSG NRW, gestrichener §5 Abs. 2). Dieser Nebensatz enthält keine der üblichen Vorbehalte gegenüber Grundrechtseingriffen. Der Status der Online-Durchsuchung als Grundrechtseingriff war zu diesem Zeitpunkt keineswegs festgeschrieben. Es gibt weder einen Richtervorbehalt, noch eine Benachrichtigungspflicht, weiterhin keine Regelung, wie mit erhaltenen Daten des Kernbereichs privater Lebensgestaltung zu verfahren

[1] Vgl. Rath (2007)
[2] Vgl. Rath (2007)

ist. Da diese Punkte in der öffentlichen Diskussion zu diesem Zeitpunkt durchaus geläufig waren, drängt sich die Vermutung auf, dass es in der Gesetzgebung zuerst darum ging, Fakten zu schaffen und die rechtliche Klärung dem Bundesverfassungsgericht (BVerfG) zu überlassen. Ein Verlauf, der abzusehen war und genau so eintrat. Gleich mehrere Verfassungsbeschwerden wurden eingereicht, das BVerfG klärte die Diskussion einige Monate später.

3.3 Urteil des Bundesverfassungsgerichts

Das BVerfG urteilt am 27. Februar 2008 und trifft eine Entscheidung, die für die weitere Entwicklung maßgebend ist. Die Beschwerden stützen sich im wesentlichen auf folgende Argumente: Die Online-Durchsuchung sei einem Eingriff in die Unverletzlichkeit der Wohnung (§13 GG) gleichzustellen[3]. Zudem mangele es an einem Richtervorbehalt, am Schutz des Kernbereichs privater Lebensgestaltung und an der Normenklarheit. Schließlich sei die Online-Durchsuchung unverhältnismäßig. Das BVerfG folgt dieser Argumentation weitgehend[4]. Wenn auch die Unverletzlichkeit der Wohnung für das Urteil keine Rolle spielt, so leitet das Gericht ein neues Grundrecht her, das die gleichen Erfordernisse stellt wie jedes Grundrecht. Das „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ leitet sich aus dem Allgemeinen Persönlichkeitsrecht[5] ab. Dieses dient im Grundgesetz als eine Art Auffangregel. Das allgemeine Persönlichkeitsrecht besagt, dass jeder „das Recht auf die freie Entfaltung seiner Persönlichkeit“ hat, soweit er „nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt“[6]. Insofern, als dass die Computernutzung inzwischen für die Persönlichkeitsentwicklung eine nicht bestreitbare Bedeutung erlangt hat, lässt sich ein eigener Rechtsgrundsatz herleiten, der die Computernutzung besonders schützt. Ähnlich dem Recht auf informationelle Selbstbestimmung handelt es sich bei dem neuen Grundrecht also um eines, das nicht direkt im Text des Grundgesetzes erwähnt wird, aber sich nach Ansicht des BVerfG unzweifelhaft daraus direkt herleitet. Der Umstrittene §5 ABs.2 Nr.11 des Verfassungsschutzgesetzes von NRW wird darauf hin für ungültig erklärt: Die für einen Grundrechtseingriff erforderlichen Schwel-

[3] zu dieser Diskussion siehe Borchers u. Kuri (2007)
[4] folgende Ausführungen sinngemäß aus Bundesverfassungsgericht (2008) entnommmen
[5] GG, Art.2 Abs.1 i.V.m. Art. 1 Abs. 1
[6] GG, Art.2 Abs.1

len sind hier nicht gegeben. Die weiteren Ausführungen des BVerfG erörtern die notwendigen Bedingungen. Diese Umfassen - wie in der Beschwerde gefordert - die Gebote der Normenklarheit und -bestimmtheit, die Verhältnismäßigkeit im engeren Sinn (z.B. muss ein überragend hohes Rechtsgut bedroht sein), und den Schutz des Kernbereiches der persönlichen Lebensgestaltung.

3.4 Entwurf eines neuen BKA-Gesetzes

Nach dem Urteil des Bundesverfassungsgerichts war klar, dass die Online-Durchsuchung einer wesentlich gründlicheren Rechtfertigung bedarf, als im gestrichenen Paragraphen des Verfassungsschutzgesetzes. Der Entwurf des neuen BKA-Gesetzes versucht die Vorgaben des BVerfG umzusetzen. Paragraph 20k regelt den Eingriff in informationstechnische Systeme: Grundsätzlich ist festgelegt, dass dieser nur in Fällen zulässig ist, in denen „Leib, Leben oder 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“[7] gefährdet sind. Ebenfalls wird klargestellt, dass solche Maßnahmen „nur auf Antrag des Präsidenten des Bundeskriminalamts oder seines Vertreters durch das Gericht angeordnet werden“ [8] dürfen. Hier ist allerdings eine Ausnahme vorgesehen, die sich auf Gefahr im Verzug bezieht. In diesem Fall kann die Maßnahme ohne die Zustimmung eines Richters durchgeführt werden. Seine Zustimmung ist nur nachträglich einzuholen, eine Frist von drei Tagen wird dazu eingeräumt. Weiter ist ein Kernbereichsschutz vorgesehen der darin besteht, dass sobald Erkenntnisse dafür vorliegen, dass die Maßnahme den Kernebereich privater Lebensgestaltung betrifft, diese auszusetzen sei. Da es sich offensichtlich bei einer zumindest teilautomatischen Überwachung nicht garantieren lässt, dass diese Erkenntnisse vor Erlangung der Daten vorliegen, sollen diese durch zwei BKA-Beamte, von denen einer die Befähigung zum Richteramt besitzen muss, auf Kernbereichsverletzungen geprüft und ggf. gelöscht werden. Erst in Zweifelsfällen müssen die Daten einem Richter vorgelegt werden. Ob diese Regelung - bei der das BKA letztlich Zugriff auf die Daten hat und selbst zuerst entscheidet, ob diese verwertet werden oder nicht - einen aus-

[7] (Deutscher Bundestag 2008, §20k)
[8] ebenda

reichenden Kernbereichsschutz darstellt ist umstritten[9]. Zuletzt ist vorgesehen, betroffene Personen von der Maßnahme im Nachhinein zu unterrichten sofern nicht eine der zahlreichen Ausnahmefälle vorliegt.

3.5 Aktueller Stand

Der oben vorgestellte Entwurf zur Novellierung des BKA-Gesetzes wurde am 04. Juni 2008 vom Regierungskabinett als Gesetz zur Ausweitung der BKA-Kompetenzen im Kampf gegen den Terror beschlossen. Damit ist die Online-Durchsuchung in Form des neuen BKA-Gesetzes in das Gesetztgebungsverfahren eingebracht. Ob das Gesetz in dieser Form jedoch überhaupt in Kraft tritt, bleibt aufgrund heftiger Kritik, auch aus den Reihen der SPD und der Opposition, bisher fraglich [10].

Mit der Feststellung der Verfassungswidrigkeit des §5 ABs.2 Nr.11 des Verfassungsschutzgesetzes von Nordrhein-Westfalen durch das Bundesverfassungsgericht gibt es also momentan auf Bundesebene keine rechtliche Grundlage für Online-Durchsuchungen. Jedoch sind neben der Novellierung des BKA-Gesetzes verschiedene Verfahren eingeleitet worden, um rechtliche Grundlagen für die Online-Durchsuchung zu schaffen.

Auf Bundesebene hat das Bayrische Justizministerium am 13. Juni 2008 einen Antrag zur Änderung der Strafprozessordnung im Bundesrat eingebracht. Dieser sieht den Einsatz der Online-Durchsuchung als Mittel der Behörden zur Ermittlung in Fällen schwerster Delikte der organisierten Kriminalität oder besonders schwerer Straftaten vor [11]. Dieser Antrag wurde am 04. Juli 2008 vom Bundesrat abgelehnt [12].

[9] Auch der Sinn einer „Gefahr im Verzug“–Ausnahme ist zweifelhaft für einen Einsatz der wochenlanger Vorbereitung bedarf. Siehe dazu Borchers u. Briegleb (2008)
[10] Vgl. Tagesschau (2008)
[11] Vgl. Krempl (2008b)
[12] Vgl. Krempl (2008c)

Auf Länderebene ist die Online-Durchsuchung zumindest in Bayern schon Realität. Am 03. Juli 2008 verabschiedete der bayrische Landtag sowohl ein neues Polizeiaufgabengesetz als auch eine Novellierung des Verfassungsschutzgesetzes des Landes. Damit ist Bayern das erste Bundesland, welches eine rechtliche Grundlage für die Online-Durchsuchung nicht nur für die Verbrechensbekämpfung durch die Polizei sondern auch für Ermittlungen des Verfassungsschutzes [13].

Aktuell gibt es ein weiteres Vorgehen zur Schaffung einer gesetzlichen Grundlage für die Online-Durchsuchung in Hessen. Das dortige Innenministerium strebt eine Anpassung des Hessischen Landesgesetzes über die öffentliche Sicherheit und Ordnung (HSOG) an. Der Antrag schreibt im § 15 b HSGO Rahmenbedingungen für die Online-Durchsuchung als Ermittlungsinstrument der Polizeibehörden fest. Vorgesehen ist die Befugnis zum Einsatz bei Ermittlungen im Terrorismusbereich und bei schweren Straftaten [14].

[13] Vgl. Krempl (2008a)
[14] Vgl. Innenministerium Hessen (2008)

4 Politik

Dieses Kapitel beschäftigt sich mit der politischen Dimension der Online-Durchsuchung. Neben der rechtlichen und sachlichen Argumentation wurde in den Medien teilweise stark emotional argumentiert. Eine echte und notwendige sowie aufklärende Diskussion über Grundwerte ist überfällig und soll hier mit angeschnitten werden.

4.1 Ziele der Online-Durchsuchung

Die Ziele der Online-Durchsuchung sind von der Politik keineswegs klar kommuniziert worden. Wir versuchen an dieser Stelle trotzdem einige Ziele bzw. Einsatzmöglichkeiten einer Online-Durchsuchung darzustellen.

Zunächst einmal ist eine Motivation für das Gesetz, welches die Online-Durchsuchung für Behörden zu einem legalen Mittel macht, dass die Lage bislang rechtlich unklar war. Bis zum Zeitpunkt als über ein Gesetz zur Online-Durchsuchung nachgedacht wurde gab es lediglich eine Dienstanweisung von Otto Schily, dem ehemaligen Bundesminister des Innern, welche dem Bundeskriminalamt (kurz: BKA) erlaubte in einigen Fällen Online-Durchsuchungen durchzuführen[1].

Politisch wurde als Legitimation für die Online-Durchsuchung der Kampf gegen der Terrorismus genannt. Auf der technischen Ebene ist die Online-Durchsuchung eines Computers der einzige Weg, um an verschlüsselte Daten zu kommen. Insbesondere ist die Quellen-TKÜ der einzige Weg, um verschlüsselte Kommunikation abzuhören, da die kommunizierten Daten jeweils entweder auf dem sendenden oder dem empfangenden Rechner abgegriffen werden müssen, da sie auf dem Weg von dem einen Rechner zum anderen verschlüsselt sind und somit zwar abgehört, aber nicht genutzt werden können, da gängige

[1] Siehe Krempl (2007)

Verschlüsselungstechniken als nicht brechbar gelten.

Weiter ist eine Online-Durchsuchung brauchbar, wenn keine herkömmliche Kommunikation stattfindet. Die zu kommunizierenden Daten werden also nicht, wie normalerweise, zum Beispiel beim Senden einer E-Mail, üblich, von einem Rechner zu einem anderen Rechner gesendet, sondern sie verlassen einen Rechner gar nicht und können somit auch nicht abgehört werden. Ein Beispiel für diese Art der nicht herkömmlichen Kommunikation könnte zum Beispiel der gemeinsame Zugriff auf ein und das selbe Postfach genannt werden. Die beiden Kommunikationspartner versenden dabei eine E-Mail nicht an eine andere E-Mail-Adresse und somit an einen anderen Rechner, sondern legen diese einfach im Postfach, zum Beispiel im *Entwürfe*-Ordner ab. Der zweite Kommunikationspartner loggt sich dann genauso in das Postfach ein und liest die Mail einfach aus diesem Ordner heraus. Wenn der Zugriff auf das E-Mail-Konto über eine verschlüsselte Verbindung aufgebaut wird (HTTPS bzw. SSL), so ist auch diese Verbindung abhörsicher.

4.2 Argumente

Im Folgenden soll nun etwas detaillierter auf die Argumente für bzw. gegen die Online-Durchsuchung eingegangen werden. Diese Argumente vermischen sich natürlich teilweise mit den Zielen der Online-Durchsuchung.

4.2.1 Pro

Wie schon bei den Zielen genannt ist ein Argument für die Online-Durchsuchung, dass die Welt sich vom sog. internationalen Terrorismus bedroht sieht. Da Anschläge in der Vergangenheit gezeigt haben, dass Terroristen primär über das Internet miteinander kommunizieren, sieht sich der Gesetzgeber in der Lage die aktuelle Gesetzgebung diesen Umständen anpassen zu müssen.

Gerade im Fall von terroristischen Anschlägen scheint es nötig diese im Vorfeld zu verhindern und nicht die Täter nach der Tat zu finden. Insbesondere für dieses Ziel ist es nötig die Kommunikation von potentiellen Tätern im Vorfeld abzuhören. Aus oben genannten technischen Gründen (Verschlüsselung) ist dies zum Teil nur auf dem Rechner der Kommunizierenden möglich.

Des weiteren reiht sich das Gesetz zur Online-Durchsuchung in eine Reihe weiterer Gesetze ein, die sich mit der Terror-Bekämpfung beschäftigen. Als Beispiel ist die Vorratsdatenspeicherung zu nennen, aber auch Konzepte wie die nationale Anti-Terror-Datei und Ähnliches.

Ein weiteres von der Politik genannten Argument für die Online-Durchsuchung ist die schnellere Ermittlung nach oder vor Straftaten, da eine Online-Durchsuchung nicht mit aufwändigen Hausdurchsuchungen verbunden ist, sondern verdeckt von der Ermittlern durchgeführt werden kann.

4.2.2 Contra

Eben diese verdeckte Art zu Ermitteln führt allerdings zu den Argumenten gegen die Online-Durchsuchung. So handelt es sich nach §20 Abs. (1) des BKA-Gesetzes eben um eine verdeckte Ermittlung von der die überwachte Person ersteinmal nichts erfährt. Die Benachrichtigung eben dieser überwachten Person kann nach §20 Abs. (1) Nr. 6 unter bestimmten Umständen ausbleiben. Dies steht allerdings im Widerspruch zur Entscheidung des Bundesverfassungsgerichtes[2].

Weitere Argumente gegen die Online-Durchsuchung betreffen dessen Wirksamkeit. So ist es relativ einfach sich gegen eine Online-Durchsuchung zu schützen. Dies kann zum Beispiel durch die Nutzung von Internet-Cafés geschehen. In so einem Fall würde die kommunizierende Person bei jedem Kommunikationsvorgang einen anderen Rechner benutzen, so dass die Installation einer entsprechenden Überwachungssoftware nicht zielführend wäre. Im Gegenteil es würde sogar dazu kommen, dass unbeteiligte Dritte, welche auch diesen Rechner in dem Internet-Café benutzen mit überwacht werden würden.

Des weiteren könnte man unverschlüsselte Inhalte nur auf Rechnern vorhalten, die nicht ans Internet angeschlossen sind. Somit wäre in diesem Fall eine Online-Durchsuchung unmöglich. Zur Kommunikation könnten verschlüsselte Inhalte „händisch“ auf einen an das Internet angeschlossenen Rechner übertragen werden, um von dort aus gesendet werden zu können. Der Effekt wäre, dass auf dem an das Internet angeschlossenen Rechner nur die verschlüsselten Inhalte vorhanden wären. Somit können auch nur diese von einer Überwachungssoftware gefunden werden. Dies ist allerdings wie oben schon erwähnt

[2] vgl. BVerfGE, 109, 279, 363ff

nutzlos, da verschlüsselte Inhalte nicht entschlüsselt werden können.

Ein weiteres Argument gegen die Online-Durchsuchung ist das „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“, wie es im Urteil zum entsprechenden NRW-Gesetz von Bundesverfassungsgericht postuliert wurde und das bei einer Online-Durchsuchung grundsätzlich verletzt wird.

Staatsrechtliche Bedenken

Die Aufgabe des BKA ist nach eigenen Angaben „als zentrale Kriminalpolizei in Deutschland die Verbrechensbekämpfung auf nationaler und internationaler Ebene zu koordinieren“[3]. Das Instrument der Online-Durchsuchung würde allerdings über die reine Koordinierung hinausgehen, da es sich um eine Ermittlungsmaßnahme handelt.

Der Polizeibrief[4] vom 14.04.1949 besagt außerdem, dass der Bund nur die Koordinierung der Verbrechensbekämpfung übernehmen darf und ihm keine Exekutiven Aufgaben übertragen werden dürfen. Ziel der Polizeibriefes ist die Schaffung einer Staatspolizei zu unterbinden.

Bei der Online-Durchsuchung handelt es sich, da das Ziel ist Straftaten im Vorfeld zu verhindern, um eine präventive Maßnahme. Präventive Maßnahmen sind im Allgemeinen allerdings dem Verfassungsschutz vorbehalten. Würde eine Polizeibehörde, wie das BKA eine ist, eine solche Maßnahme durchführen, wäre sie bei einem Hinweis auf eine Straftat gezwungen zu ermitteln.

4.3 Zusammenhang zum Datenschutz

In diesem Abschnitt soll ein Zusammenhang des Sachverhalts zum Datenschutz und dessen grundlegenden Prinzipien hergestellt werden.

Aus dem BKA Gesetz §20 Abs. 7:

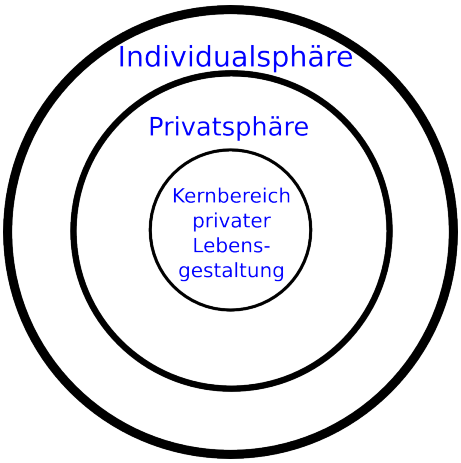
> *Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch die*

[3] Siehe Bundeskriminalamt (2008)
[4] Siehe Clay u. a. (1949)

Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig.

Problematisch ist, dass die Prüfung, ob Daten aus dem Kernbereich privater Lebensgestaltung erhoben werden, von zwei BKA-Beamten vollzogen wird. Diese Prüfung kann schwerlich objektiv durchgeführt werden, da die BKA-Beamten im Zweifelsfall in die Ermittlungen involviert sind und somit in einem Interessenkonflikt stehen.

Zur Veranschaulichung der verschiedenen Ebenen das Sphären-Modell:



4.4 Politische Kultur

Abschließend ein paar Worte zur politischen Kultur Deutschlands, die wir eng verknüpft mit der Online-Durchsuchun, aber auch allgemein mit den sog. Anti-Terror-Gesetzen, sehen.

In der Bundesrepublik Deutschland schlagen die Verabschiedungen von Gesetzes in den Medien immer häufiger hohe Wellen. Allerdings nicht nur, weil es sich um umstrittene Gesetze handelt, sondern vor allen Dingen, weil die Verfassungkonformität von Gesetzen in der Vergangenheit immer häufiger vom Bundesverfassungsgericht entschieden werden musste.

Hinter diesem Vorgehen könnte politisches Kalkül stecken. Da es mitunter schwierig ist umstrittene politische Forderungen in Gesetzen unterzubringen, kann es zur politischen Strategie werden Gesetze schärfer zu formulieren als eigentlich gewollt. Das Bundesverfassungsgericht wird dann nach einer entsprechenden Klage die Grenzen aufzeigen, so dass das Gesetz im Nachhinein entsprechend angepasst werden muss. Dieses Vorgehen ist insofern kritikwürdig, als dass die Politik sich nicht vertrauenswürdiger macht wenn sie offensichtlich Grundrechte missachtet.

Ein Beispiel für einen solchen Fall ist die Vorratsdatenspeicherung. So hat die SPD laut dem stenographischen Bericht der 124. Sitzung des Bundestages dem Gesetz trotz *"'trotz schwerwiegender politischer und verfassungsrechtlicher Bedenken"'* zugestimmt. Weiter sagt die SPD in diesem Bericht, dass die Vorschläge zur Vorratsdatenspeicherung den *"'Makel der offensichtlichen Verfassungswidrigkeit"'* tragen. Trotzdem hat die SPD für diese Vorschläge gestimmt[5]. In diesem Verhalten ist ein Paradigmenwechsel in der Politik zu sehen. Die demokratische Grundordnung wird auch mit verfassungswidrigen Mitteln versucht zu verteidigen. Freiheit durch Sicherheit.

Diese Veränderung der politischen Kultur wird auch in Zitaten von einigen Politikern deutlich welche an dieser Stelle nocheinmal wiedergegeben werden sollen.

Hans-Christian Ströbele, Grüne:

> *Unser Privates stirbt ganz offensichtlich scheibchenweise.*

Max Stadler, FDP:

> *Wenn ein Verdächtiger heimlich ausgespäht wird, dann müsste der Betroffene zumindest nachträglich darüber informiert werden, um die Maßnahme im Zweifelsfall gerichtlich überprüfen zu lassen.*[6]

Brigitte Zypries, SPD (vor der Debatte am 20. Juni):

> *Insgesamt geht es um graduelle Veränderungen in einzelnen Punkten, nicht um die Substanz des Gesetzes.*[7]

[5] Siehe Deutscher Bundestag (2007, Anlage 4)
[6] Siehe Sawall (2008)
[7] Siehe Sawall (2008)

Wolfgang Schäuble, CDU:

> *... ich komme in keinen Computer rein, ich weiß auch kaum wie die Polizei das macht. Ich weiß gerade mal was so ein Trojaner ist*[8].

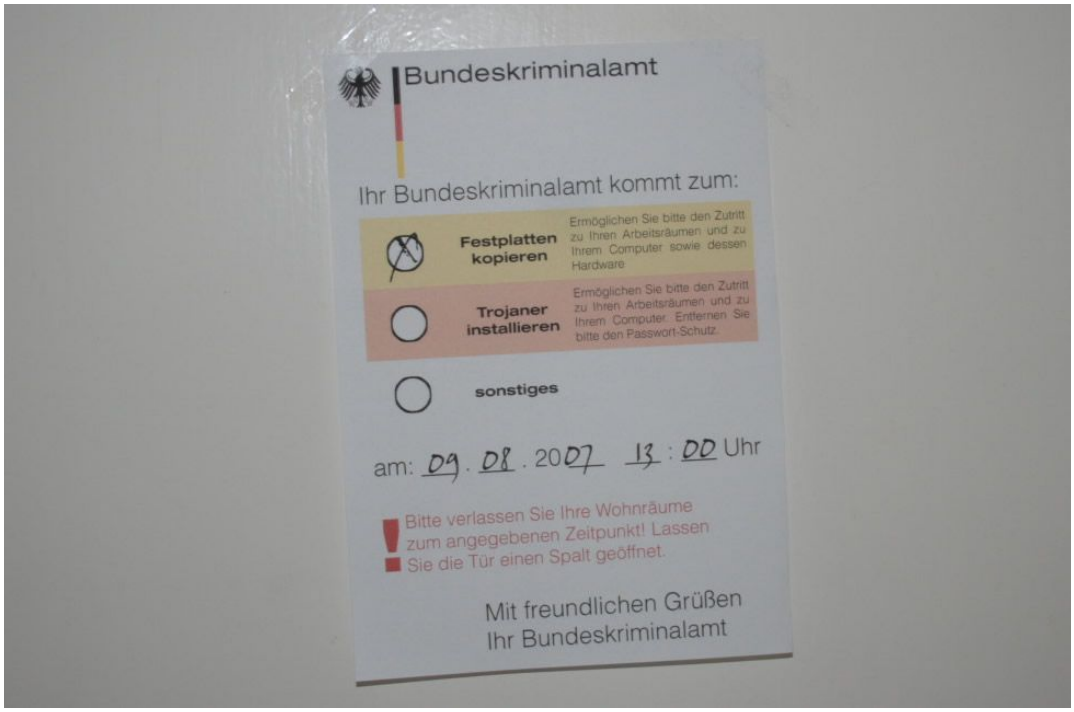
4.5 Blick in die Zukunft

Im Gesetzesentwurf ist, wenn es um die Zielsysteme geht, welche abgehört werden dürfen, ganz allgemein von *informationstechnischen Systemen* die Rede. Dieser Terminus ist nicht ganz unproblematisch, da er keine sonderlich scharfe Definition darstellt. So könnte zum Beispiel auch ein Herzschrittmacher ein solches Informationstechnisches System darstellen.

Dies würde dazu führen, dass nicht nur herkömmliche Computer von diesem Gesetz betroffen sind, sondern auch Systeme die auf den ersten Blick nicht als Computer wahrgenommen werden, wie zum Beispiel Herzschrittmacher[9].

Klar wird, die Folgen eines solches Gesetzes, wenn es nicht an allen Stellen klar formuliert ist, sind nicht absehbar. In Zukunft könnten solche Gesetze auch für Dinge genutzt werden für die sie nicht entworfen worden sind.

[8] Siehe Rath u. Schäuble (2007)
[9] Siehe Schulz u. Pfitzmann (2008)


Bundeskriminalamt
Ihr Bundeskriminalamt kommt zum:
Festplatten kopieren
Ermöglichen Sie bitte den Zutritt zu Ihren Arbeitsräumen und zu Ihrem Computer sowie dessen Hardware
Trojaner installieren
Ermöglichen Sie bitte den Zutritt zu Ihren Arbeitsräumen und zu Ihrem Computer. Entfernen Sie bitte den Passwort-Schutz.
sonstiges
am: 09. 08. 2007 13 : 00 Uhr
Bitte verlassen Sie Ihre Wohnräume zum angegebenen Zeitpunkt! Lassen Sie die Tür einen Spalt geöffnet.
Mit freundlichen Grüßen
Ihr Bundeskriminalamt

5 Literaturverzeichnis

GG

Grundgesetz der Bundesrepublik Deutschland. – http://www.bundestag.de/parlament/funktion/gesetze/grundgesetz/gg_01.html

Aleph One 1996

ALEPH ONE: Smashing the stack for fun and profit. In: *Phrack Magazine* 7 (1996), S. 49

Anderson 2001

ANDERSON, Ross J.: *Security Engineering: A Guide to Building Dependable Distributed Systems*. John Wiley & Sons, Inc. New York, NY, USA, 2001

Borchers u. Briegleb 2008

BORCHERS, Detlef ; BRIEGLEB, Volker: SPD will BKA-Gesetz korrigieren. In: *heise online* (2008), Juni. http://www.heise.de/newsticker/meldung/109623

Borchers u. Kuri 2007

BORCHERS, Detlef ; KURI, Jürgen: Online-Durchsuchung: Ist die Festplatte eine Wohnung? In: *heise online* (2007), Juli. http://www.heise.de/newsticker/meldung/93307

Buermeyer 2007

BUERMEYER, Ulf: Die Online-Durchsuchung. Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme. In: *HRRS – Onlinezeitschrift für Höchstrichterliche Rechtsprechung im Strafrecht* 4 (2007), S. 154–166

Bundeskriminalamt 2008

BUNDESKRIMINALAMT: *Profil*. Webseite. http://www.bka.de/profil/profil1.html. Version: Oktober 2008

Bundesministerium des Innern 2007a
BUNDESMINISTERIUM DES INNERN: *Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien*. August 2007

Bundesministerium des Innern 2007b
BUNDESMINISTERIUM DES INNERN: *Fragenkatalog des Bundesministeriums der Justiz*. August 2007

Bundesverfassungsgericht 2008
BUNDESVERFASSUNGSGERICHT: *Urteil zum VSG NRW (BVerfG, 1 BvR 370/07 vom 27.2.2008)*. Februar 2008. – `http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html`

BVerfGE
BVERFGE: *Entscheidungen des Bundesverfassungsgerichts*. Bd. 109. J. C. B. Mohr (Paul Siebeck). – S. 279, 363ff

Chaos Computer Club e.V. 2007
CHAOS COMPUTER CLUB E.V.: *Bundestrojaner in ELSTER-Software entdeckt*. Presseerklärung, 1. April 2007

Clay u. a. 1949
CLAY, Lucius D. ; ROBERTSON, B. H. ; KOENIG, Pierre: *Schreiben der Militärgouverneure zum Grundgesetz („Polizei-Brief")*. `http://www.verfassungen.de/de/de49/grundgesetz-schreiben49-3.htm`. Version: April 1949. – Aus: E.R. Huber, Quellen zum Staatsrecht der Neuzeit, Bd. II, Deutsche Verfassungsdokumente der Gegenwart (1919–1951), Matthiesen Tübingen, 1951, S.216 (deutsche Fassung)

Deutscher Bundestag 2007
DEUTSCHER BUNDESTAG: *Plenarprotokoll 16/124 – Stenographischer Bericht der 124. Sitzung in der 16. Wahlperiode*. November 2007

Deutscher Bundestag 2008
DEUTSCHER BUNDESTAG: *Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt*. Drucksache des Deutschen Bundestages, DIP 16/9588. `http://dip21.bundestag.de/dip21/btd/16/095/1609588.pdf`. Version: 2008

Fox 2007a

FOX, Dirk: Realisierung, Grenzen und Risiken der Online-Durchsuchung. In: *DuD - Datenschutz und Datensicherheit* 31 (2007), S. 827–834

Fox 2007b

FOX, Dirk: *Stellungnahme zur „Online-Durchsuchung" (Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07)*. September 2007. – Version 1.1

Hoglund u. McGraw 2004

HOGLUND, Greg ; MCGRAW, Gary: *Exploiting Software: How to Break Code*. 1st Ed. Pearson Higher Education, Addison-Wesley, 2004

Innenministerium Hessen 2008

INNENMINISTERIUM HESSEN: *Vorschläge der Landesregierung zur Anpassung des HSOG an aktuelle Erfordernisse*. Pressemitteilung. http://www.hessen.de/irj/hessen_Internet?rid=HStK_15/hessen_Internet/nav/5ef/5ef5072f-a961-6401-e76c-d1505eb31b65,2616008f-993c-ac11-2668-4144e9169fcc,,,11111111-2222-3333-4444-100000005004%26_ic_uCon_zentral=2616008f-993c-ac11-2668-4144e9169fcc.htm&uid=5ef5072f-a961-6401-e76c-d1505eb31b65. Version: Sep 2008

Krempl 2007

KREMPL, Stefan: Bundesregierung gibt zu: Online-Durchsuchungen laufen schon. In: *heise online* 25.04. (2007). http://www.heise.de/newsticker/meldung/88824

Krempl 2008a

KREMPL, Stefan: Bayerischer Landtag setzt den „Bayerntrojaner" frei. In: *heise-online* (2008), Juli. http://www.heise.de/newsticker/meldung/110426

Krempl 2008b

KREMPL, Stefan: Bayern bringt Entwurf zu heimlichen Online-Durchsuchungen in den Bundesrat ein. In: *heise-online* (2008), Jun. http://www.heise.de/newsticker/meldung/109424

Krempl 2008c

KREMPL, Stefan: Bundesrat will heimliche Online-Durchsuchungen auf Ter-

rorabwehr beschränken. In: *heise online* (2008), Juli. http://www.heise.de/newsticker/meldung/110466

von Leitner u. a. 2007
LEITNER, Felix von ; BOGK, Andreas ; KURZ, Constanze: *Der Bundestrojaner: Die Wahrheit haben wir auch nicht, aber gute Mythen*. Vortrag auf dem 24C3. http://events.ccc.de/congress/2007/Fahrplan/events/2363.en.html. Version: Dezember 2007

Lutz u. a. 2008
LUTZ, Martin ; JUNGHOLT, Thorsten ; ZIERKE, Jörg: BKA verteidigt Aufrüstung der Terrorfahnder. In: *WELT ONLINE* (2008), Juni. http://www.welt.de/politik/article2055826/BKA_verteidigt_Aufruestung_der_Terrorfahnder.html

Pfitzmann 2008
PFITZMANN, Andreas: Contra Online-Durchsuchung. In: *Informatik Spectrum* (2008), Januar, Nr. 31, S. 65–69

Rath 2007
RATH, Christian: Online-Schnüffeln ohne Freibrief? In: *taz* 02.05. (2007). http://www.taz.de/index.php?id=archivseite&dig=2007/05/02/a0210

Rath u. Schäuble 2007
RATH, Christian ; SCHÄUBLE, Wolfgang: „Terroristen sind auch klug“. In: *taz* 08.02. (2007). http://www.taz.de/index.php?id=archivseite&dig=2007/02/08/a0169

Rath u. Zierke 2007
RATH, Christian ; ZIERKE, Jörg: Am Computer des Täters ansetzen. In: *taz* 26.03. (2007)

Sawall 2008
SAWALL, Achim: FDP-Innenexperte: Überwachung privater Computer sinnlos. In: *Golem.de* 20.06. (2008). http://www.golem.de/0806/60535.html

Schulz u. Pfitzmann 2008
SCHULZ, Daniel ; PFITZMANN, Andreas: Datenschutz-Forscher über

Online-Schnüffelei: „Der Staat könnte in Körper eindringen“. In: *taz* 28.05. (2008). http://www.taz.de/1/archiv/dossiers/dossier-ueberwachung/online-durchsuchung/artikel/1/der-staat-koennte-in-koerper-eindringen/

Tagesschau 2008
TAGESSCHAU: *Grünes Licht für Späh-Befugnisse - Kabinett verabschiedet Gesetzentwurf*. http://www.tagesschau.de/inland/kabinett34.html. Version: Jun 2008

Wikipedia 2008
WIKIPEDIA: *Trusted Computing*. http://de.wikipedia.org/wiki/Trusted_Computing. Version: Oktober 2008

Zierke 2008
ZIERKE, Jörg: Pro Online-Durchsuchung. In: *Informatik Spectrum* 1 (2008), S. 62–64